

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Electra Zoe Karamargin 184677IVCM

**GOING DARKER:
A FORENSIC ANALYSIS OF SMART EYEWEAR BIOMETRIC
ASSET MANAGEMENT, TOWARD THE RISING CONFLICT
BETWEEN SECURITY THROUGH PRIVACY BY DESIGN AND
FORENSIC INVESTIGATION**

Master's thesis

Supervisor: Hayretdin Bahsi
PhD Cyber Security
Digital Forensics

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Electra Karamargin

12/21/2020

Abstract

Leading consumer centric technology firms and law enforcement agencies have been deploying or are projected to deploy smart eyewear devices, as these hands-free recording devices enable the wearer to effortlessly capture a first-person point-of-view of their surrounding environment.

As recording and capturing devices trend toward concealment in all sectors, from governmental to corporate to private, privacy concerns heighten not only for the end user of the device and their interpersonal network, but additionally relative to bystanders who are either inadvertently or deliberately recorded by smart eyewearers.

In attempts to mitigate the privacy concerns and comply with relative data protection legislation, it is in the device developer's best interest to provide their consumer base with products possessing stringent data protections.

As a result, forensic investigators and law enforcement entities are increasingly left in the dark as privacy by design modeling and technology outpaces their technical and legal capabilities and capacity.

Individual privacy rights and forensic investigation conflict concerning the management of biometric assets through privacy by design and privacy by default.

The privacy versus investigative forensics problem of Going Dark is explored via network and mobile systems forensic analysis of biometric asset management within a smart eyewear ecosystem. The study determines if forensic investigations are deterred or enabled by the systems' privacy by design security features or privacy risks.

The National Institute of Standards and Technology's Privacy Framework is used in conjunction with the International Organization for Standardization's 19510:2013 standard to identify, map, and analyze biometric asset data processing within the product's design and system environment.

Similar recent studies and research of this nature have yet to be conducted on smart eyewear devices nor the exact device examined and analyzed in this study, a Snapchat Spectacles version 2.

This thesis is written in English and is X pages long, including X chapters, X figures and X tables.

Abstraktne

Juhtivad tarbijakesksed tehnoloogiaettevõtted ja õiguskaitseorganid on kasutusele võtnud või kavatsevad juurutada nutikaid prilliseadmeid, kuna need käed-vabad salvestusseadmed võimaldavad kasutajal vaevata jäädvustada esimese inimese vaatepilti ümbritsevast keskkonnast.

Kuna seadmete salvestamine ja hõivamine suundub varjamineks kõigis sektorites, alates valitsusasutustest ja lõpetades eraettevõtetega, suurenevad privaatsusprobleemid mitte ainult seadme ja nende suhtlusvõrgu lõppkasutaja jaoks, vaid ka kõrvalseisjate suhtes, keda nutikad kas tahtmatult või tahtlikult salvestavad prillid.

Püüdes leevendada privaatsusprobleeme ja järgida suhtelisi andmekaitsealaseid õigusakte, on seadme arendaja huvides pakkuda oma tarbijabaasile tooteid, millel on range andmekaitse.

Selle tulemusel jäävad kohtuekspertiisid ja õiguskaitseorganid üha enam pimedusse, kuna disainimudelite ja tehnoloogia abil privaatsus ületab nende tehnilised ja õiguslikud võimalused ning võimekuse.

Individuaalsed privaatsusõigused ja kohtuekspertiisi uurimise konfliktid seoses biomeetriliste varade haldamisega disainilahenduse ja vaikimisi privaatsuse kaudu.

Going Darki privaatsuse versus uuriva kohtuekspertiisi probleemi uuritakse võrgu- ja mobiilsüsteemide kaudu biomeetrilise varahalduse kohtuekspertiisi analüüsi abil nutikate prillide ökosüsteemis. Uuringus tehakse kindlaks, kas kohtuelu uurimist takistavad või võimaldavad süsteemide privaatsus disaini turvaelementide või privaatsusriskide tõttu.

Riikliku standardite ja tehnoloogiainstituudi privaatsusraamistikku kasutatakse koos Rahvusvahelise Standardiorganisatsiooni standardiga 19510: 2013, et tuvastada, kaardistada ja analüüsida toote disaini ja süsteemikeskkonna biomeetriliste varade andmete töötlemist.

Sarnased hiljutised uuringud ja sedalaadi uuringud ei ole veel läbi viidud nutikate prilliseadmetega ega ka selles uuringus uuritud ja analüüsitud täpse seadmega, Snapchati prillide versiooniga 2.

See lõputöö on kirjutatud inglise keeles ja see on X lehekülge pikk, sisaldades X peatükki, X joonist ja X tabelit.

List of abbreviations

ADB	Android Debug Bridge
BLE	Bluetooth Low Energy
BPMN	Business Process Model and Notation
ENISA	The European Union Agency for Cybersecurity Formerly: European Network and Information Security Agency
IC	integrated circuit
HS	High Speed
ISO	International Organization for Standardization
MU-MIMO	Multi-User Multiple Input Multiple Output
NBDDO	Never been “deleted” or “deleted, overwritten”
NIST	National Institute of Standards and Technology
NVM	Non-volatile memory
PCM	protection circuit module
SOC	System-on-chips

List of terms

Biometric	<p>“Measurable physical characteristics [, physiological characteristics,] or personal behavioral traits used to [uniquely] identify, or verify the claimed [unique] identity of, an individual.” [1] [2]</p> <p>Biometric data/assets may include, but are not limited to: facial images, ear images, ocular images, tongue images, speaker/speech audio/video recordings, emotive facial movements/gestures captured in the form of images/audio/video recordings, and gait video recordings.</p>
Confidentiality	<p>“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.” [3]</p>
Personal data	<p>“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” [4]</p>
Privacy	<p>“Freedom from unauthorized intrusion.” [5]</p> <p>“The right of a party to maintain control over and confidentiality of information about itself.”[6]</p>
Privacy by design	<p>The implementation of personal data protection throughout a product or system lifecycle [4].</p>

Privacy by default

The assurance personal data is automatically protected by a product or system, without need for an individual to alter the data processing product or system.

Additionally, the limitation on the amount of: personal data collected, personal data processing, the storage duration, and accessibility duration [4].

Privacy enhancing technologies

“software and hardware solutions, i.e. systems encompassing technical processes, methods, or knowledge to achieve specific privacy or data protection functionality or to protect against risks to privacy of an individual or a group of natural persons.” [7] [8]

Processing

“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” [4]

Public domain

“creative materials that are not protected by intellectual property laws such as copyright, trademark, or patent laws. The public owns these works, not an individual author or artist. Anyone can use a public domain work without obtaining permission, but no one can ever own it.” [9]

Table of Contents

Author's declaration of originality	2
Abstract	3
Abstraktne	4
List of abbreviations	5
List of terms	6
Table of Contents	8
List of figures	11
List of tables	14
Introduction	16
Topic	16
Motivation	16
Research Problems	17
Main Objectives	17
Scope	17
Ethical Issues	18
Key Assumptions	18
Literature Review	19
Methodology	19
Keywords: Inclusion and exclusion criteria	19
Search techniques	22
Digital Libraries	22
Journals and conferences	23
Grey Literature	23
Related works	24
Related works: Research methods	24
Related works: Data sources and tools	25
Related works: Data analysis methods and tools	26
Triangulation of methods and tools	26
Privacy risk management analysis methodology	26
NIST Privacy Framework	26
Business Process Modeling & Notation (BPMN) v2.0.1	28
Related works: Research gap analysis	29
Background information	30
Smart eyewear company profile	30

Smart eyewear data protection and privacy policies	30
Snap Inc. privacy violation timeline and risk management	31
Smart eyewear hardware	32
Research methods	37
Data collection methods	38
Participant observer simulated biometric data	38
Forensic Examinations	40
Forensic exam I: Wi-Fi scanning and enumeration	40
Forensic exam I: Methods and tools	41
Forensic exam I: Analysis, results, and discussion	41
Forensic exam II: BLE scanning & enumeration	50
Forensic exam II: Methods and tools	51
Forensic exam II: Analysis, results, and discussion	52
Forensic exam III: BLE scanning and enumeration with nRF Sniffer	58
Forensic exam III: Methods and tools	59
Forensic exam III: Analysis, results, and discussion	61
Forensic exam IV: Decrypting Bluetooth Low Energy	71
Forensic exam IV: Methods and tools	72
Forensic exam IV: Analysis, results, and discussion	72
Forensic exam V: HCI BTSnoop logs	76
Forensic exam V: Methods and tools	77
Forensic exam V: Analysis, results, and discussion	78
Forensic exam VI: Non-Rooted extraction via ADB Pull and ADB Backup	82
Forensic exam VI: Methods and tools	83
Forensic exam VI: Analysis, results, and discussion	84
Forensic exam VII: ADB dumpsys meminfo	87
Forensic exam VII: Methods and tools	88
Forensic exam VII: Analysis, results, and discussion	89
Forensic exam VIII: Data request	91
Forensic exam VIII: Methods and tools	92
Forensic exam VIII: Analysis, results, and discussion	93
Forensic exam IX: Acquiring system administration privilege	100
Forensic exam IX: Methods and tools	100
Forensic exam IX: Analysis, results, and discussion	102
Forensic exam X: Acquiring smart eyewear cloud data with a rooted sandbox smartphone and parallel APK	105
Forensic exam X: Methods and tools	106
Forensic exam X: Analysis, results, and discussion	111
Forensic exam XI: Rooted extraction via ADB pull	117

Forensic exam XI: Methods and tools	118
Forensic exam XI: Analysis, results, and discussion	118
Forensic exam XII: Rooted extraction via TWRP copy and ADB backup	120
Forensic exam XII: Methods and tools	121
Forensic exam XII: Analysis, results, and discussion	122
Forensic exam XIII: Rooted physical extraction via Axiom Magnet Process and Examine	124
Forensic exam XIII: Methods and tools	124
Forensic exam XIII: Analysis, results, and discussion	125
Validation via triangulation	128
Pre-extraction metadata	131
Post-extraction metadata	132
SHA digest matching	142
Biometric detection	146
Biometric detection on non-rooted logical extraction	147
Biometric detection on rooted physical extraction	152
Database metadata	164
Artifact inventory count	171
Results and Discussion	172
Identify & map: Business Process Modeling & Notation (BPMN)	172
NIST Privacy Framework Profile	182
Synopsis	188
Main goal	189
Limitations	189
Analysis Bias	189
Novelty	189
Main contribution	189
Future work	190
References	190
Appendix	209

List of figures

- Figure 1. NIST Privacy Framework's Core Functions and Categories. [97]
- Figure 2. Snap Inc. privacy violation timeline: 2013:[134][135][136][137]; 2014:[138][132][139][140][141][142]; 2016:[143]; 2018: [144]; 2019: [133]
- Figure 3. Snapchat Spectacles version 2 teardown - Sunglasses and camera [146][147]
- Figure 4. Snapchat Spectacles version 2 internal hardware [146][147] [150]
- Figure 5. Snapchat Spectacles version 2 internal hardware - Reverse side [146][147] [150]
- Figure 6. Bystander notification of (a) camera photographing (all lights, 1 blink) or (b) video recording (all lights, rotating swirl). [155]
- Figure 7. Snapchat Spectacles version 2 - Malibu lithium-ion battery Model SC03 [146][147] [150]
- Figure 8. Hardware setup for simulated biometric capture and collection [161] [151]
- Figure 9. Forensic exam I: WiFi Monitor v1.11 network scan results
- Figure 10. Forensic exam I: Network addresses from Samsung Galaxy S10e
- Figure 11. Forensic exam I: Confirmation of paired smartphone's OUI (a) Wireshark OUI lookup tool (b) System defined MAC-48 (c) Network scanned EUI-48 [165]
- Figure 12. Forensic exam I: Network Analyzer Lite v3.7 scan results for smart eyewear paired smartphone
- Figure 13. Forensic exam I: Network Analyzer Lite v3.7 Port Scanner results for smart eyewear paired smartphone (a) Port Scanner: Query (b) Port Scanner results
- Figure 14. Forensic exam I: NMAP v7.80 results from host discovery ping scan with disabled port scanning for smart eyewear paired smartphone
- Figure 15. Forensic exam I: NMAP v7.80port and device fingerprinting scan results for smart eyewear paired smartphone
- Figure 16. Forensic exam I: Wireshark Wireshark win64 v3.0.10-0-gaa0261e8ddf3 Wi-Fi scan results for smart eyewear paired smartphone
- Figure 17. Forensic exam II: nRF Connect (a)"SCANNER" and (b)"FLAGS & SERVICES" screenshots of Spectacles version 2 smart eyewear BLE communications
- Figure 18. Forensic exam II: nRF Connect "SCANNER: Raw data" results
- Figure 19. Forensic exam II: BLE network services and characteristics data extracted via nRF Connect and nRF Logger from smart eyewear
- Figure 20. Forensic exam II: Results from Wireshark's OUI Lookup Tool for smart eyewear 48-bit EUI-48 BLE address (a)nRF Connect EUI-48 results (b)nRF Connect EUI-48 results (c) Lookup of Snap Inc. OUI
- Figure 21. Forensic exam III: Bluetooth Low Energy Extraction hardware configuration. [195] [196][161]
- Figure 22. Forensic exam III:
- Figure 23. Forensic exam III:
- Figure 24. Forensic exam III:
- Figure 25. Forensic exam III:
- Figure 26. Forensic exam III:
- Figure 27. Forensic exam III:
- Figure 28. Forensic exam III: Encrypted PDU communications sent between smartphone and smart eyewear
- Figure 29. Forensic exam III: Encrypted PDU write request command sent from smartphone/master to smart eyewear/slave
- Figure 30. Forensic exam III: Encrypted PDU notification sent from smart eyewear/slave to smartphone/master
- Figure 31. Forensic exam IV: Incompatible BLE frame format produced from nRF52840 DK
- Figure 32. Forensic exam IV: Crackle decryption input command
- Figure 33. Forensic exam IV: "Unpair Spectacles"
- Figure 34. Forensic exam IV: Snapchat Spectacles version 2 smart eyewear initial pairing requires naming
- Figure 35. Forensic exam IV: Wireshark pcap of BLE smart eyewear pairing to smartphone (a) Frames 1301-1339 (b) Frames 1340-1395
- Figure 36. Forensic exam IV: Attempted BLE packet decryption with Crackle on Kali Linux virtual system

Figure 37. Forensic exam V: ADB Bugreport generation to extract Bluetooth HCI Snoop Log from smart eyewear's paired smartphone

Figure 38. Forensic exam V: Detail of Frame 563, Bluetooth Pairing request sent from Samsung Galaxy S10e to Snapchat Spectacles version 2 smart eyewear (a-b)

Figure 39. Forensic exam V: Detail of Frame 574, Bluetooth SMP pairing failure from Snapchat Spectacles version 2 smart eyewear to Samsung Galaxy S10e

Figure 40. Forensic exam V: Summary of Frame 24176, Nordic UART Tx Write Command sent from Samsung Galaxy S10e to Snapchat Spectacles version 2 smart eyewear (a-b)

Figure 41. Forensic exam V: Detail of Frame 24176, of Nordic UART Tx Write Request Command sent from Samsung Galaxy S10e to Snapchat Spectacles version 2 smart eyewear.

Figure 42. Forensic exam VI: ADB Pull

Figure 43. Forensic exam VI: ADB Backup command for non-rooted data extraction.[208]

Figure 44. Forensic exam VI: Command for conversion of ADB backup.ab file to backup.tar file.

Figure 45. Forensic exam VI: ADB backup.ab, backup.tar, and Z-Zip extracted files from paired smartphone.

Figure 46. Forensic exam VI: ADB Pull results from targeted non-rooted smartphone.

Figure 47. Forensic exam VI: ADB Shell results from targeted non-rooted smartphone.

Figure 48. Forensic exam VI: ADB Backup extraction of "apps" and "shared" file directories from the paired smartphone

Figure 49. Forensic exam VI: Extracted photographs (.jpg) and videos (.mp4) containing biometric information within \shared\0\Spectacles directory

Figure 50. Forensic exam VI: Extracted thumbnails (.jpg), from smart eyewear videos, containing biometric information within \shared\0\Movies\thumbnails directory

Figure 51. Forensic exam VI: Extracted thumbnails (.jpg), from smart eyewear photographs, containing biometric information within \shared\0\Pictures\thumbnails directory

Figure 52. Forensic exam VI: Extracted thumbnails (.jpg), from smart eyewear videos, containing biometric information within \shared\0\DCIM\thumbnails directory

Figure 53. ADB shell dumpsys meminfo command.

Figure 54. ADB Dumpsys meminfo report for com.snapchat.android

Figure 55. Forensic exam VIII: "Account History" and "Spectacles" excerpts from smart eyewear "Data Request" (a) Action(s): "Paired" and "Deleted"; (b) Action: "Not Paired" ; (c) Action: "Firmware Updated"

Figure 56. Forensic exam VIII: HTTP 403 response after requesting smart eyewear data past 7th day.

Figure 57. Forensic exam VIII: Autopsy 4.13.0 metadata from a (a) JPEG image and (b) MP4 video, extracted from smart eyewear Data Request

Figure 58. Forensic exam IX: (a) Warning before entering "Device unlock mode" (b) "Unlock bootloader" warning

Figure 59. Forensic exam IX: Screenshot of "Strong protection" (encryption) and "Security policy updates" (a) Enabled (b) Disabled

Figure 60. Forensic exam IX: Failed attempt to flash TWRP .tar file to S10E

Figure 61. Forensic exam X: Verification of Snapchat APK allowBackup="false" flag via Android Studio [228]

Figure 62. Forensic exam X: 103 total data assets in Snapchat's "Memories" before logout on target smartphone (Samsung Galaxy S10e) (a) July 2020(b) August 2020 (c) Total July - August 2020

Figure 63. Forensic exam X: 164 total data assets in Snapchat "Memories" after login on sandbox smartphone (Xiaomi Redmi Note 7) (a) July 2020(b) August 2020 (c) Total July - August 2020

Figure 64. Logout/Login Eyewear Cloud Server Data Discrepancy

Figure 65. Forensic exam X: Pertinent directory results excerpted from ADB Shell recursive directory tree listing as rooted superuser of sandbox smartphone (Xiaomi Redmi Note 7)

Figure 66. Forensic exam X: As rooted superuser of sandbox smartphone, determined number of files within Snapchat APK's select directories likely holding pertinent biometric assets.

Figure 67. Forensic exam XI: Excerpted ADB Pull errors encountered on rooted sandbox smartphone, while logged into smart eyewear user account

Figure 68. Forensic exam XI: Error prone file workaround - Separate ADB Pulls on rooted sandbox smartphone, while logged into smart eyewear user account

Figure 69. Forensic exam XII: TWRP procedure to copy com.snapchat.android directory to external storage (a) Located and selected com.snapchat.android file (b) Selected Action: Copy Folder (c) Selected Destination Folder: /sdcard1 (d) Confirmed Action

Figure 70. Forensic exam XII: ADB Backup procedure on rooted sandbox smartphone logged into smart eyewear cloud account

Figure 71. Forensic exam XII: ADB Backup failure after rooting smartphone due to Android Manifest control set

Figure 72. Forensic exam XII: Successful ADB Backup of com.snapchat.android TWRP directory copy from rooted sandbox smartphone logged into smart eyewear cloud account

Figure 73. Forensic exam XII: Truncation of file names and extensions within “memories_mini_thumbnail” directory after TWRP copy/ADB Backup method

Figure 74. Forensic exam XII: Truncation of file names and extensions within “memories_thumbnail” directory after TWRP copy/ADB Backup method

Figure 75. Forensic exam XII

Figure 76. Excerpts of stat data for “.0” files via ADB shell on rooted sandbox smartphone (Xiaomi Redmi Note 7)

Figure 77. Excerpts of hexadecimal data for “.0” files via ADB shell on rooted sandbox smartphone (Xiaomi Redmi Note 7)

Figure 78. Biometric detection: Scan of non-rooted target smartphone (Samsung Galaxy S10e SM-G970F) with Magnet Axiom’s Magnet.AI Categorization module found 24 “Possible human faces”

Figure 79. Biometric detection: Magnet Axiom extraction via adb-data.tar (a) Exported Spectacles .jpg and .mp4 files (b) “Pictures” > .thumbnails (c) “DCIM” > .thumbnails (d) “Movies” > .thumbnails

Figure 80. Biometric detection: Magnet Axiom extraction via sdcard.tar.gz (a) Exported Spectacles .jpg and .mp4 files (b) “Pictures” > .thumbnails (c) “DCIM” > .thumbnails (d) “Movies” > .thumbnails

Figure 81. Biometric detection: 60 confirmed total artifacts within file system after manually tagging missed biometric images (a) Magnet AI Categorization summary (b) Details of JPG file from /Spectacles directory (c) Details of MP4 file from /Spectacles directory

Figure 82. Biometric detection: Magnet Axiom’s detection of “possible human faces” within physical image of sandbox smartphone from Forensic exam XIII

Figure 83. Biometric detection: File signature mismatch identification by Autopsy 4.13.0 (a) image/jpeg and image/png MIME Types (b) text/plain MIME Types

Figure 84. Biometric detection: File signature mismatch identification by Magnet Axiom v4.7.0.22371

Figure 85. Biometric detection: File signature mismatches containing “possible human faces” detected by Magnet Axiom, from physical image of sandbox smartphone

Figure 86. Addition of WEBP MIME type with a .0 extension to Magnet Axiom’s Custom File Types list

Figure 87. Results of Magnet.AI facial detection after addition of WEBP MIME type with a .0 extension to Magnet Axiom’s Custom File Types list (a) Preview and details for file within “/memories_media” directory (b) Preview and details for file within “/memories_thumbnail” directory

Figure 88. Biometric detection: Example of a webp file, with mismatched “.0” extension, from the “/memories_thumbnail” directory dragged and dropped into offline web browser

Figure 89. Failed facial detection with Magnet.AI after changing file extensions to .jpg

List of tables

- Table 1. Initial seed set of keywords and derivation examples.
- Table 2. High ranking journals and conferences referenced within study.
- Table 3. BPMN's OMG specification and ISO standard details. ,[98], [113], [114]
- Table 4. Spectacles version 2 smart eyewear wireless network SoCs Specifications [152], [153], [154],[151]
- Table 5. Public domain photographs used in simulation [159] [160]
- Table 6. Public domain videos used in simulation [159] [160]
- Table 7. Forensic exam I: Chain of custody, network access, system administration status
- Table 8. Forensic exam I: WiFi scanning and enumeration tools.
- Table 9. Forensic exam I: 48-bit Extended Unique Identifiers (EUI-48) [166]
- Table 10. Forensic exam I: NMAP v7.8 TCP/IP SCAN fingerprint results for smart eyewear paired smartphone [169]
- Table 11. Forensic exam II: Chain of custody, network access, system administration status
- Table 12. Forensic exam II: BLE scanning and enumeration tools
- Table 13. Forensic exam II: Smart eyewear BLE data obtained from nRF Connect "SCANNER" and "FLAGS & SERVICES"
- Table 14. Forensic exam II: nRF Connect "SCANNER: Raw data" results and Bluetooth generic access profile specifications.[180][181][182][183]
- Table 15. Forensic exam II: Data obtained from nRF Logger results, descriptions, and Nordic Semiconductor's Assigned Values for BLE UUIDs [184]
- Table 16. Forensic exam II: 48-bit Extended Unique Identifiers (EUI-48) for smart eyewear [166]
- Table 17. Forensic exam III: Chain of custody, network access, system administration status
- Table 18. Forensic exam III: nRF52840 and Wireshark: BLE scanning and enumeration tools
- Table 18. Forensic exam III:
- Table 19. Forensic exam III:
- Table 20. Forensic exam III:
- Table 21. Forensic exam III:
- Table 22. Forensic exam IV: Bluetooth Low Energy decryption tools.
- Table 23. Forensic exam V: Chain of custody, network access, system administration status
- Table 24. Forensic exam V: Bluetooth HCI Snoop Log Extraction tools.
- Table 25. Forensic exam V: TX and RX Characteristics
- Table 26. Forensic exam VI: Chain of custody, network access, system administration status
- Table 27. Forensic exam VI: Non-Rooted Data Extraction tools.
- Table 28. Forensic exam VII: Chain of custody, network access, system administration status
- Table 29. Forensic exam VII: Adb dumpsys meminfo tools.
- Table 30. Forensic exam VIII: Chain of custody, network access, system administration status
- Table 31. Forensic exam VIII: Procedure used to request and examine smart eyewear user's mobile application data from Snap Inc.
- Table 32. Forensic exam VIII: Tools used fused to request and examine smart eyewear user's mobile application data from Snap Inc.
- Table 33. Forensic exam VIII: ExifTool v12.07 metadata from a JPEG image extracted from smart eyewear Data Request
- Table 34. Forensic exam VIII: ExifTool v12.07 metadata from a MP4 video extracted from smart eyewear Data Request
- Table 35. Forensic exam IX: Chain of custody, network access, system administration status
- Table 36. Forensic exam IX: Tools used for rooted data acquisition of targeted smartphone.
- Table 37. Forensic exam IX: Attempted procedure used for rooted data acquisition of targeted smartphone. [218]
- Table 38. Forensic exam IX: Tools used for "Odin Install Method (No Root Required)" of targeted smartphone.
- Table 39. Forensic exam IX: Procedure used for "Odin Install Method (No Root Required)" of targeted smartphone.
- Table 40. Forensic exam X: Chain of custody, network access, system administration status
- Table 41. Forensic exam X: Tools used for rooting, installing a smart eyewear APK, and examining cloud data on an investigator's sandbox device.
- Table 42. Forensic exam X: Procedure used for rooting investigator's sandbox device.

Table 43. Forensic exam X: Procedure used for installing smart eyewear APK on investigator's sandbox device.

Table 44. Forensic exam X: Procedures used for manual acquisition and logical examinations of smart eyewear cloud data

Table 45. Forensic exam XIII: Additional tools used for rooted physical extraction via Axiom Magnet Process and Examine.

Table 46. Data analysis methods: Additional tools used for validation via triangulation.

Table 47. Validation via triangulation procedure

Table 48. Files selected from /memories_mini_thumbnail and /memories_thumbnail to be audited

Table 49. Metadata results for 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

Table 50. Metadata results for BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

Table 51. Extraction method comparison of a file within "memories_mini_thumbnail" directory

Table 52. Extraction method comparison of a file within "memories_thumbnail" directory

Table 53. Extraction method comparison of a file's hexadecimal content within "memories_mini_thumbnail" directory

Table 54. Extraction method comparison of a file's hexadecimal content within "memories_thumbnail" directory

Table 55. SHA Extraction method comparison for webp image file from /memories_mini_thumbnail

Table 56. SHA Extraction method comparison for webp image file from /memories_thumbnail

Table 57. Biometric detection: Additional tools required for facial recognition analysis

Table 58. Biometric detection: Imaging tool comparison for 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

Table 59. Biometric detection: Imaging tool comparison for BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

Table 60. Biometric detection: Extraction method comparison of webp thumbnail and mini thumbnail with offline web browser

Table 61. Database metadata 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

Table 62. Database metadata BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

Table 63. Database metadata screenshots 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

Table 64. Database metadata screenshots BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

Table 65. Artifact inventory counts before and after data extractions from /data/data/com.snapchat.android

1 Introduction

1.1 Topic

Forensic analyses have been conducted on a single smart eyewear device to determine how the acquisition and analysis of the device's biometric assets, in the form of image captures and video recordings of individuals, is either deterred by smart eyewear's privacy by design features or enabled by the smart eyewear ecosystem's privacy risks.

NIST's Privacy Framework [97], in conjunction with ISO/IEC 19510:2013 (BPMN v2.0.1) [98] and "Security Risk-Oriented BPMN" [255], have been used to model and understand current privacy practices and set targeted privacy objectives for the smart eyewear's privacy ecosystem.

1.2 Motivation

Individual privacy rights and forensic investigation conflict concerning the management of biometric assets through *privacy by design* and *privacy by default*.

Forensic investigators and law enforcement entities are increasingly left in the dark as privacy by design and privacy by default modeling and technology outpaces their technical and legal capabilities and capacity. The aforementioned concept and challenge has been coined from the military term of "Going Dark" [10].

In attempts to play catch-up, select law enforcement units are adopting screening devices, software, and databases reliant upon beta biometric recognition algorithms to match identities either in real time from surveillance footage or from historically sourced images and video datasets [11] [12] [13] [14] [15] [16] [17] [18] [19].

The privacy versus investigative forensics problem of *Going Dark* has been explored within the forensic analysis of smart eyewear, as many leading consumer centric technology firms [20] [21] [22] [23] [24] [25] [26] [27] [28] and law enforcement agencies [29] [30] [31] [32] [33] are rolling out smart eyewear as the next big trend in inconspicuous internet of things (IoT) devices [34] [35] [36] to interact, capture, record, store, transfer, and analyze public biometric assets.

As recording and capturing devices trend toward concealment in all sectors, from governmental to corporate to private, privacy concerns heighten not only for the end user of the device and their interpersonal network, but additionally relative to bystanders who are either inadvertently or deliberately recorded by smart eyewearers [37] [38] [39] [40] who likely have not granted consent to be captured in time.

When a single image or video capture of an individual may be utilized to identify [41] [42], harass [43], and/or incriminate [44] [45] [46] [47], a higher standard for biometric data management, procurement, and analysis must be observed.

1.3 Research Problems

Going Darker: A forensic analysis of smart eyewear biometric asset management, toward the rising conflict between security through privacy by design and forensic investigation.

RP1:

Conduct network and mobile systems forensic analysis of smart eyewear ecosystem to identify and map biometric asset data processing in congruence with NIST's Privacy Framework and BPMN v2.0.1.

RP2:

Analyze identified data actions, or lack thereof, which present biometric asset privacy risks within the smart eyewear ecosystem.

RP3:

Develop a NIST Privacy Framework Current to Target Profile to improve privacy risk management of biometric data assets processed by smart eyewear.

1.4 Main Objectives

Main objectives include the forensic investigation of a smart eyewear device leading to determinations concerning the device's *privacy by design* features, privacy risks, and loss of biometric asset privacy.

Privacy aware system models identifying and mapping the smart eyewear's current risk status and formulated from the smart eyewear biometric artifact acquisition and analysis results.

Current privacy risk management system models aiding in establishing targeted privacy objectives specific to the smart eyewear ecosystem.

1.5 Scope

The scope has been restricted to the forensic analysis of a single pair of smart eyewear due to the cost prohibitive nature of such devices. Snapchat Spectacles version 2 were chosen for their moderately affordable price range.

Open source forensic tools have been utilized to conduct the research to bypass further restrictive cost barriers. Commercial tools were procured as limited trial versions or by the university's procurement division.

Time prohibitive barriers restricted the study's scope by including neither the development of new forensic tools for data extraction and collection, nor the search for new exploits and attack methods, nor the privacy analysis of biometric audio samples captured within the recorded videos.

1.6 Ethical Issues

All efforts were made to ensure individual participant privacy rights are upheld according to local and national legislation; including but not limited to GDPR, national regulations, and an ethical committee review, such as an institutional review board (IRB).

Biometric data sourced for the study has been collected under a simulated operational environment to avoid infringing on individual privacy rights in a public field environment. Additionally, public domain videos and photographs of individuals were used as the subject matter within the smart eyewear video recording and photographic simulation captures to further ensure no individual privacy rights were infringed upon.

As no large-scale network scanning was performed, registering the IP utilized for scanning with required authorities was not required. Privacy risks discovered through forensic analysis, will be responsibly disclosed with all firms.

1.7 Key Assumptions

Key assumptions of the study include:

Test monitoring equipment:

Forensic software and hardware monitoring tools utilized are assumed to record and analyze data relative to their marketed and statistically supported product claims. Defects or bugs within forensic software could impact data collection from smart devices.

Geographical distance/Environmental disturbances:

Distance and disturbances between network communications could affect data collection.

Protocols:

Protocols used could impact data extraction and collection from the mobile smart devices.

Topology/architecture:

Topology and architecture of smart devices and the network they are located within could impact data extraction and collection.

Communication medium:

Communication mediums may impact data collection and extraction from smart devices. For instance, Wi-Fi, fluorescent lights, microwave ovens, and wireless devices within the same 2.4GHz ISM band could impact Bluetooth Low Energy (BLE) communications.

Software condition:

Smart device software could impact data extraction and retrieval if not free from design defects.

Hardware condition:

Smart device hardware could impact system and network communications. Equipment has been purchased or downloaded new, unused, and free from manufacturing defects; and is assumed to be as advertised.

Version of firmware/software:

Software versions could impact data extracted or collected from smart devices.

Bandwidth:

Bandwidth of mobile smart devices may impact data collection and extraction.

Equipment type/vendor:

Type of equipment and equipment vendor could impact data extraction and collection considering each entity could have different design and development standards.

Socio-economic disturbances:

Socio-economic disturbances could impact forensic tool procurement and data collection

2 Literature Review

2.1 Methodology

2.1.1 Keywords: Inclusion and exclusion criteria

The literature review began with an initial framework set of keywords excerpted from the overarching research problem.

A seed set of exact keyword phrases was searched for using Boolean operators within various digital library databases. The initial search included the following single keywords, bigrams, and trigrams:

“going dark” AND “forensic analysis” AND “smart eyewear” AND “biometric asset management” AND “security” AND “privacy by design” AND “forensic investigation”

This search produced zero results in most digital libraries except for Elsevier, which output around 63,188 webpages, books, and journals since their search function does not accurately utilize Boolean logic, thus creating false positives for the full inclusion of all selected keywords and keyword phrases. Elsevier claims ScienceDirect is their more search friendly digital library database for open access content [48].

As research progressed, the initial set of keywords and keyword phrases was modified and distilled. The identified body of literature excluded the keywords: “asset” and “management”, and the keyword phrase: “biometric asset management” from the initial set. Words linked to non-computational forensics disciplines were also excluded from the search. Additionally, select keywords or keyword phrases were included as substitute derivations for particular words within the initial seed set, see Table 1.

The following are a few examples of the many search queries performed:

(“smart eyewear” OR "smart glasses") AND (“forensic analysis” OR “forensic investigation”)
(“smart eyewear” OR "smart glasses" OR “smart glass” OR “google glass” OR wearable OR “iot devices”)
AND (“forensic analysis” OR “forensic investigation” OR forensic OR teardown)
AND (“security” OR cybersecurity OR “information security”)
AND (“privacy by design” OR privacy)
AND (biometric OR “facial recognition” OR “voice recognition” OR “gait recognition”)
AND (“going dark” OR “going dark debate” OR “access to encrypted”)
NOT (watches OR fitbit OR medicine OR pathology OR dna OR spectrometry OR assist)

Table 1. Initial seed set of keywords and derivation examples.

“going dark”	“biometric asset management”	“smart eyewear”	“security”	“privacy by design”	“forensic analysis”	“forensic investigation”
“going dark debate”	biometric	“smart glasses”	cybersecurity	privacy	forensic AND	
“lawful hacking”	“facial recognition”	“augmented reality” OR AR	security AND	“data privacy”	mobile	
“law enforcement”	“voice recognition”	“mixed reality”	Information	“privacy preservation”	“data analysis”	
“access to”	“speech recognition”	wearables	data	“user privacy”	iot	
hacking	“gait recognition”	“smart devices”	IoT	“bystander privacy”	digital	
encryption	“iris recognition”	“iot devices”	BLE	“other people’s privacy”	hardware	
“technology law review”	“biometric recognition”	“wearable devices”	challenges	“identity privacy”	network	
“access to encrypted”	“tongue recognition”	“google glass”	wearable	confidentiality	wifi	
“government access to”	“machine learning”	“smart glass”	“data breach”	“systems modeling”	wireless	
“government hacking”	“artificial intelligence” OR AI	“police body cams”	management	development	bluetooth	
enforcement	“deep learning”	snapchat AND spectacles	privacy AND risks vulnerabilities threats controls requirements	“design factors”	“BLE” OR “bluetooth low energy” OR “bluetooth smart” OR “bluetooth 4.0” AND forensic	
“public safety”	“biometric hash”	“mobile devices”	“IoT protocols”	“hardware engineering”	teardown	

2.1.2 Search techniques

Search techniques included beginning with an initial set of keywords and initial set of open access academic journals and conference sources when querying research databases.

A systematic literature review was performed wherein qualitative methods were strived for and in certain search queries achieved. Academic journals searched for included recent, high ranked journals (relative to the H Index), that possessed a high number of citations.

Discrepancies between H Index rankings between authoritative ranking entities [49] and [50] exist and thus the accuracy of rankings may vary.

Backward and forward snowballing techniques were applied to seed sets of papers to filter through results. For instance, backward snowballing was applied after the following query:

("smart eyewear" OR "smart glasses" OR "smart glass" OR "wearable" OR "google glass") AND forensic

which resulted in the discovery of the following reference [51] from the International Journal of Forensic Science & Pathology. Referenced within [51] was a piece of grey literature entitled "Google Glass Forensics" [52] providing in-depth details on the forensics tools and procedures utilized to acquire data artifacts from the Google Glass smart eyewear.

Forward snowballing was applied to the reference [52], which was cited by a piece of grey literature [53] which performed a detailed forensic examination on a pair of smart glasses entitled Ice Theia.

Quantitative data analysis [54] was performed on select studies when searching for derivations of keywords from the initial seed set.

2.1.3 Digital Libraries

Digital libraries utilized within the study initiated with Google Scholar and Scopus as the starting points for the search, which then filtered into publishing libraries: ACM Digital Library, Elsevier, IEEE Xplore Digital Library, ResearchGate, ScienceDirect, SemanticScholar, and SpringerLink.

As mentioned prior, Elsevier's search did not use boolean logic operators, ScienceDirect was preferred unless otherwise noted.

2.1.4 Journals and conferences

High ranking journals and conferences referenced within study are illustrated within Table 2.

Table 2. High ranking journals and conferences referenced within study.

Journals and Conferences	H Index
Journal of Business Research	158
IEEE Communications Surveys & Tutorials	147
ACM Computing Surveys (CSUR)	132
Presence: Teleoperators & Virtual Environments	78
2018 IEEE Symposium on Security and Privacy (SP)	72
IEEE Access	56
Multimedia Tools and Applications	52
IEEE Internet Things	47
ACM Transactions on Internet Technology (TOIT)	46
Digital Investigation	43
International Conference on Financial Cryptography and Data Security	43
Life Science Journal	21
2015 10th International Conference on Availability, Reliability and Security (ARES)	20
ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security	20

See *References* section for a comprehensive listing of all academic journals and conferences included within the study.

2.1.5 Grey Literature

Search Methods, Selected Keywords, and Inclusion/Exclusion criteria

Grey literature was sourced from the news media, technology industry, and governmental publications via prior mentioned digital libraries and snowballing techniques within those found queries. Google's search engine was also used to find grey literature providing greater background on current technological and law enforcement trends, news articles, forensic tools, software modeling languages, security frameworks, artifact acquisition methods, smart eyewear hardware components, privacy

standards, forensic guidelines, product test reports, privacy regulations, product and software patents, and product teardowns.

Keywords, keyword phrases, and their derivatives primarily followed Table 1; however, the following keyword terms were added to the grey literature search: NIST, ENISA, BPMN, ISO, ADB, guidelines, framework, patents, standards.

2.2 Related works

2.2.1 Related works: Research methods

Of the few studies discovered on the forensic analyses of smart eyewear, most of which were grey literature, observational exploratory or observational descriptive research methods were utilized to gain, a broad or specific in-depth, foundational understanding of these unexplored emerging wearable devices.

Observational descriptive forensic artifact acquisitions and analyses performed on a single pair of Google Glass Explorer Edition smart glasses include: a reconstruction of the smart eyewear end user's action history by organizing found forensic artifacts in chronological order [52]; the examination of a threat agent's ability, without administrative root access, to install a malicious application enabling photographs to be taken with and saved by the smart eyewear without alerting the end user of the device [55]; a study published within the *International Journal of Forensic Science & Pathology (IJFP)*, used varying methods of smart eyewear data acquisition to acquire artifacts after normal device usage [51].

Observational exploratory research includes studies on: post-adoption everyday use of smart eyewear [56] and wearable body cameras [57]; forensic acquisition and analysis of three wearable device types: smart glasses, smart watches, and fitness trackers [53].

Observational exploratory and descriptive forensic examinations of other wearable devices, such as smartwatches [58] [59] [60] [61] [62] [63] and fitness trackers [60] [63] [64][65][66][67][68], have been conducted with greater frequency and many recently published in higher ranking journals and conferences.

Observational exploratory surveys conducted include studies on: privacy and security within IoT wearable devices [69] [70] [71] [72] [73] [74] [75] fitness smart wearables [76], wearable biometric recognition systems [77], IoT forensics definitions, challenges, and future research directions [78], privacy issues in digital forensics [79], consumer acceptance and adoption of wearable devices [80], smart eyewear interaction methods [81], gestural bystander privacy mitigation from smart eyewear [82], tools for forensic investigations [83][84].

Although observational exploratory studies lack the specific in-depth analyses conducted within descriptive forensic examinations of systems, the aforementioned surveys provide a broad foundational understanding of emerging IoT wearable systems,

general privacy and security risks to wearable IoT devices, biometric device capacities, and conventional forensic methods and tools utilized within investigations.

A unique observational ethnographic research study, developed through Grounded Theory, was conducted on the socioethical impacts of law enforcement wearable cameras on the power and privacy concerns of surveilled Aboriginal communities around the world [85].

Applied observational exploratory and descriptive research on smart eyewear privacy include studies on: altering smart eyewear hardware and software designs [86] a granular privacy preference model with simulator to protect sensitive personal data within a single smartwatch [87], a privacy model to preserve personally identifiable biometric data of smart eyewear bystanders by obscuring facial features [88] [89].

An applied experimental security analysis of smart glasses and smart watches was conducted to analyze a security testbed framework for wearable IoT devices [90].

Theoretical research on smart eyewear privacy includes studies on: augmented reality smart glasses and privacy risks [91], long-term usage of smart eyewear [92], consumer acceptance and adoption of smart eyewear [93] and wearable devices [94].

Experimental research conducted on smart eyewear privacy include studies on the influence of smart glass design factors on device acceptance and adoption [95] and privacy risk impact on the adoption of wearable cameras used for personal life vlogging in South Africa [96].

2.2.2 Related works: Data sources and tools

Observational descriptive studies on the forensic analyses of smart eyewear [51] [55] [52] and wearable devices [58] [59] [61] collected data directly through the forensic examination of wearable IoT devices and the subsequent acquisition of data artifacts.

Related observational exploratory studies obtained data through various sources including the forensic analyses of wearable IoT devices [60] [53], surveys of literature [71] [72] [73] [79] [80] [74] [75], and a combination of interviews and/or questionnaires of individuals prefaced with literature reviews [56] [57] [78] [83].

Data for the observational ethnographic study on law enforcement wearable cameras was sourced through a comprehensive literature review and via researcher as Participant Observer partially structured interviews with worldwide participants over the course of five years [85].

Applied observational descriptive and exploratory studies on smart wearables and privacy sourced data through surveyed literature reviews [86] [87], questionnaires [86],

then applied findings into either theoretical models [86] [87] [89], simulations [87], or proof-of-concept examinations [88] .

Applied experimental research on a single smart eyewear device and two smartwatches collected data through an exploratory literature review on wearable devices and a proof-of-concept examination of the developed security testbed [90].

Theoretical research on smart eyewear and wearable devices sourced data from literature reviews [91][92] [93][94] and developed theoretical models tested through questionnaires [91] [93][94] and unstructured interviews [91].

Experimental studies on smart eyewear acceptance and adoption sourced data from literature reviews [95] [96]and questionnaires [95][96].

2.2.3 Related works: Data analysis methods and tools

Smart eyewear [51] [55] [52] and IoT wearable [53] [58] [59] [61] ecosystem privacy risks were identified, defined, and comparatively analyzed through forensic examination and artifact acquisition.

Human factors relative to privacy risks on wearable devices were identified, defined, and comparatively analyzed after eliciting responses from study participants within observational [56][57][78] [83][85], applied [86], theoretical [91] [93] [94], and experimental [95][96] studies.

Applied research methods utilized solution driven privacy risk management analysis methods, wherein theoretical models or proof-of-concept examinations were developed after conducting exploratory or descriptive literature reviews [86][90][87][88][89].

2.2.3.1 Triangulation of methods and tools

Forensic analysis of smart eyewear mobile systems and wireless networks were conducted with a variety of open source and commercial, software and hardware tools to enable cross examination and artifact triangulation.

Open source software utilized provided a cost free and easily accessible toolset, whereas commercial software tools offered efficient and automated solutions.

Magnet Axiom's commercial forensic suite was procured through TalTech's Centre of Digital Forensics and Cyber Security.

2.2.3.2 Privacy risk management analysis methodology

2.2.3.2.1 NIST Privacy Framework

NIST's Privacy Framework , see figure 1 [97], has been utilized to manage privacy risks within the smart eyewear ecosystem as it provides a clear and concise management

structure in which to analyze and mitigate privacy risks within systems, products, and services.

The framework’s five core functions of Identify, Govern, Control, Communicate, and Protect [97] provide a foundation on which to assess a product’s ability to effectively manage privacy risks throughout the data processing life cycle.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

Figure 1. NIST Privacy Framework’s Core Functions and Categories. [97]

The framework is flexible and to be deployed relative to the applied data processing environment and target privacy objectives. Not all core functions, categories, and subcategories are required to be utilized if not applicable to preserving data privacy within the system, product, and/or service.

Freedom to manipulate the framework is further stressed by the implementation’s developers concerning their Implementation Tiers, detailing “...the Privacy Framework is based upon achieving the outcomes described in an organization’s Target Profile(s) and not upon Tier determination.” [97]

Aligned with that perspective, NIST Privacy Framework’s utilization of Implementation Tiers have not applied within this study since outside the scope of this research. The Tiers are organizational tools meant for internal company management and budgeting of resources (ie. capital, staffing, technology, immaterial intellectual property assets) to support and achieve communication and decision-making processes concerning the evolution of one’s privacy risk management current profile to their target profile.

Focus has been placed on determining the smart eyewear’s current and target privacy risk management Profiles, Core Functions, Categories, and Subcategories.

2.2.3.2.2 Business Process Modeling & Notation (BPMN) v2.0.1

The NIST Privacy Framework Identify and Communicate Core Functions’ Subcategories recommend that all assets, actions, and individuals within the data processing ecosystem are inventoried, mapped, and communicated as a foundational starting point to understand the origins of privacy risks, account for, and manage those risks throughout the data processing life cycle [97].

Business Process Modeling & Notation (BPMN) version 2.0.1 [98] has been utilized in conjunction with the NIST Privacy Framework within this study since other engineering models and methodologies such as, Privacy Enhanced BPMN [99] [100], UML [101], SecureUML [102] [103], UMLsec [104] [105] [106] [107] [108], Misuse cases [109], Mal-activity diagrams [110] and Secure Tropos [111][112] fall short of BPMN’s infographic-like intuitive modeling standard which opens communications regarding privacy risks and management to everyone from the privacy security researcher to the device/biometric data owner to the forensics investigator.

Attesting to BPMN v2.0.1’s international acceptance and widespread utilization is the International Organization for Standardization’s adoption of the exact standard as ISO/IEC 19510:2013, see table 3 for the standard’s adoption dates, publishing status, and upcoming ISO version.

Table 3. BPMN’s OMG specification and ISO standard details [98] [113] [114].

Specification Title	Acronym	Version	Published Status	Adoption Date	OMG File ID	ISO Number
Business Process Model And Notation Superseded by: BPMN v2.0.2	BPMN™	2.0.1	formal	September 2013	formal/ 13-11-03	19510:2013
Business Process Model and Notation	BPMN™	2.0.2	formal	January 2014	formal/ 13-12-09	TBD

The only other engineering modeling methodology adopted by the ISO, within the aforementioned contending models cited above, is the Unified Modeling Language (UML) [115]; however, the UML standard is geared towards “provid[ing] system architects, software engineers, and software developers with tools for analysis, design, and implementation of software-based systems as well as for modeling business and similar processes.”[116]

In contrast, the BPMN v2.0.1 adopted ISO/IEC 19510:2013 standard’s

“primary goal... is to provide a notation that is readily understandable by all business users... creat[ing] a standardized bridge for the gap between the business process design and process implementation. ... The intent ... is to standardize a business process model and notation in the face of many different modelling notations and viewpoints. In doing so, ISO/IEC 19510:2013 will provide a simple means of communicating process information to other business users, process implementers, customers, and suppliers.”[98]

BPMN v2.0.1’s open communication objectives further align with NIST’s Communicate Core Function, a vital “privacy protection activity” [97], aiming to create greater transparency and accountability of data processing entities [97].

2.2.4 Related works: Research gap analysis

Similar studies of forensic device analysis, within the field of systems and network forensics, fail to address either one or more of the combined issues: (a) the significance of privacy by design modeling and features within smart eyewear (b) the privacy and security management of biometric assets on smart eyewear in the context of a forensic investigation.

J. Rongen and Z. Geradts’ “Extraction and Forensic Analysis of Artifacts on Wearables” within the International Journal of Forensic Science & Pathology examined an Explorer Edition pair of Google Glass smart eyewear (A developer version, not the consumer version) and did not explicitly mention the significance of privacy by design modeling and features nor biometric asset management, however, the study required the use of various methods in attempting to gain elevated administrative root privileges within Google Glass, with a major caveat of some methods being a complete erasure of the user data partition [51].

Walnycky et al., within Digital Investigation’s “Network and device forensic analysis of android social-messaging applications” were able to compromise the privacy and security of 16 out of the 20 instant messaging software applications for Android they examined [117]. Walnycky et al.’s study also examined the Snapchat Android application, which is utilized by the smart eyewear to be examined within this study. Within the study, Snapchat was determined to encrypt their network traffic with HTTPS and SSL certificates, which ultimately prevented data reconstruction (images/audio/video) from data storage (both hardware and server) and packet inspection from WiFi network traffic [117]. Ultimately the study was unable to acquire or reconstruct any user data from the Snapchat application. The aforementioned study delved into the importance of privacy by design and security concerns relative to Android applications on smartphones; however, it is clear smart eyewear was not analyzed within, as it was not within the study’s scope.

T. Alyahya and F. Kausar’s study, “Snapchat analysis to discover forensic artifacts on Android smartphone,” specifically targets the extraction of Snapchat application data and artifacts on smartphone internal memory using the open source forensic platform

Autopsy and a trial version of the commercial platform Axiom Process and Examine [118]. Alyahya and Kausar determined both forensic tools are capable of only extracting a fraction of full communications (photos/videos/messages) sent and received. Alyahya and Kausar's study did not focus on smart eyewear nor did it expand upon privacy by design nor biometric asset management within the smart device.

3 Background information

3.1 Smart eyewear company profile

Snap Inc., the developers of the smart eyewear, Spectacles, and smart eyewear mobile software application, Snapchat, define themselves as a camera company whose prime motivation is to reinvent the camera to empower people by enabling them to better communicate and express themselves [119].

According to Google Play, the Snapchat Android mobile application has been downloaded over 1 billion times [120]. As of the 3rd Quarter 2020 financial report (FORM 10-Q), the smart eyewear's mobile management application, Snapchat, possessed 249 million Daily Active Users (DAUs) [121]; however, it remains unclear how many of those DAUs possess and often utilize their companion peripheral smart eyewear device.

Smart eyewear worldwide sales contributed \$1.595 million in revenue to Snap Inc. over the last nine months, with the largest revenues emanating from North America (inclusive of Mexico, the Caribbean, and Central America) and Europe (inclusive of Russia and Turkey) [121].

Snap Inc.'s FORM 10-Q also details the firm does not possess any manufacturing capabilities, has limited quality control over their smart eyewear contract manufacturers within China, and any product redesigns require greater financial and time-intensive resources to re-qualify as an eyewear product with governmental regulatory entities, such as the U.S. Food and Drug Administration (FDA) [121].

3.2 Smart eyewear data protection and privacy policies

Snapchat Spectacles are sold worldwide, and as a result of conducting such business and sales, the firm is bound to the data protection and privacy regulations within each governmental subset wherein the smart eyewear is sold and the smart eyewear application is available for download and use.

Snap Inc.'s Data Processing Agreement [122] and Privacy Policy [123] [124] details how the firm aims to handle consumer data with respect to data protection legislation such as General Data Protection Regulation (GDPR) [125] , California Consumer

Privacy Act of 2018 ("CCPA") [126], Brexit [127] and EU-U.S. and Swiss-U.S. Privacy Shield Frameworks [128][129].

The smart eyewear firm provides the general public with a bi-annual Transparency Report detailing select statistics on government requests, such as subpoenas, court orders, search warrants, wiretaps, and summons, for consumer account information [130].

Snap Inc. also provides a Law Enforcement Guide detailing data storage, request, and processing protocols as mandated by the firm's internal policies, the Stored Communications Act, 18 U.S.C. § 2701 and § 2703(f), et seq. ("SCA"), and the Mutual Legal Assistance Treaty ("MLAT") [131].

3.3 Snap Inc. privacy violation timeline and risk management

The developing firm for Spectacles smart eyewear, Snap Inc., has a history of privacy policy deception [132], privacy violations [133], and data breaches on personal information [134][135][136][137][138][132][139][140][141][142][143] [144][133](see figure 2).

Millions of consumers' private accounts, photos, and videos, containing personally identifiable biometric data, have been exposed to exploitation (see figure 2) while in the care of Snap Inc.

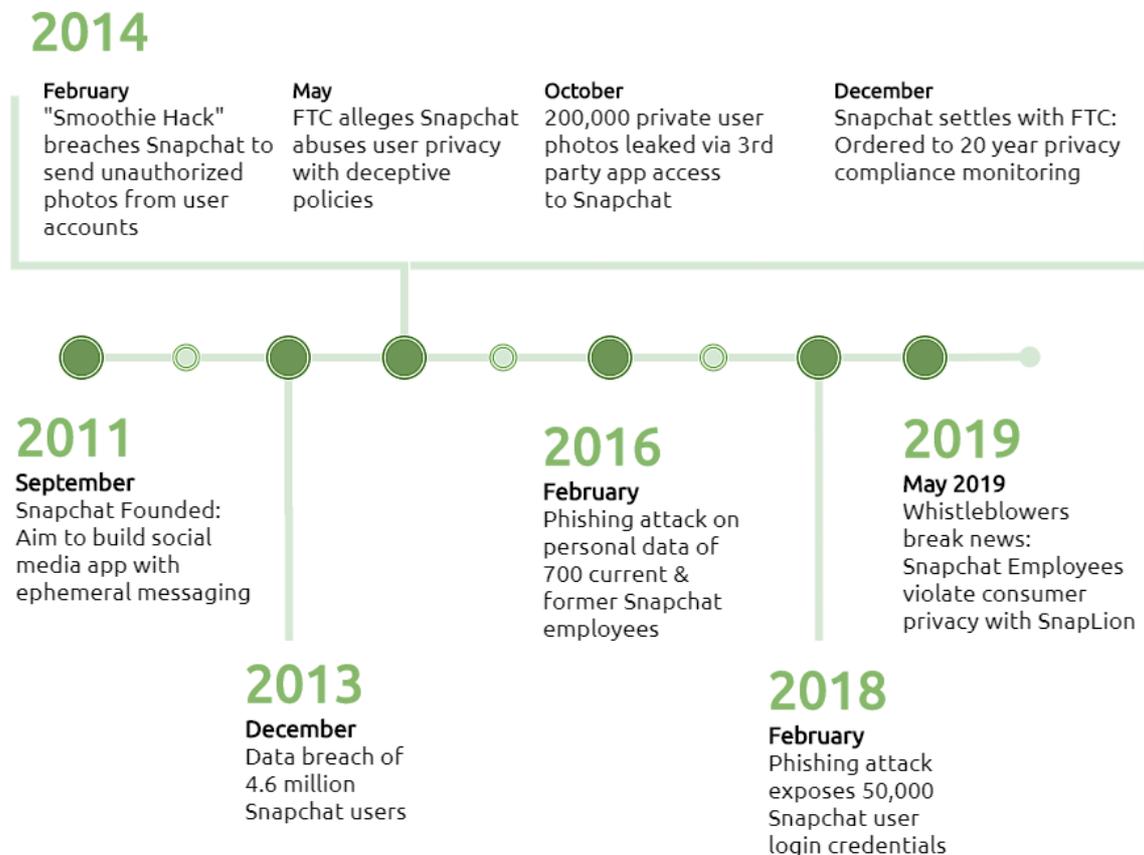


Figure 2. Snap Inc. privacy violation timeline: 2013:[134][135][136][137]; 2014:[138][132][139][140][141][142]; 2016:[143]; 2018: [144]; 2019: [133]

The firm's inability to manage privacy risks for their software and hardware products pushed the FTC to take action against the firm in May 2014, ultimately resulting in the imposition of a 20 year privacy compliance monitoring order [132].

Periodic privacy monitoring by the FTC failed to prevent Snap Inc. employees from violating consumers' privacy with an internal corporate tool, SnapLion, intended to aid law enforcement [133]. It was not the FTC alerting the general public nor the company's leadership, but rather whistleblowers within Snap Inc. who reported internal privacy incidents and violations to Vice Motherboard, a subsidiary science and tech news magazine of the Vice Media Group LLC broadcasting company, in May 2019 [133].

The full impact of Snap Inc.'s struggle to manage data protection and privacy risks is unknown, further studies are needed to gain understanding and solve unresolved privacy issues.

4 Smart eyewear hardware

Snapchat Spectacles version 2 smart eyewear is essentially a pair of sunglasses with a built in camera capable of taking photographs and videos, see figure 3. Depending on the sunglass frame style selected, Spectacles version 2 cost anywhere from 175€ to 230€ [145].



Figure 3. Snapchat Spectacles version 2 teardown - Sunglasses and camera [146][147]

All version 2 Spectacles possess an Android mobile operating system based on a custom Linux Kernel version 3.10.71 [148].

Spectacles version 2 smart eyewear do not possess a visual interface display to manage and view photos and videos captured and collected by the device. A paired smartphone is required to manage and view the photos and videos captured and collected by the smart eyewear.

Spectacles version 2 are compatible with iPhone 5 or greater, running iOS 10 or greater; most Android devices running Android 4.4 or greater, with BLE and Wi-Fi Direct;

however, not compatible with Samsung Galaxy models: A6+/J5/J7/J7 Perx/J7 Prime/J7 V [149].

Spectacles version 2 uses a Samsung KM1JX0019M 4GB flash memory chip with unknown camera processor [150][151] (figures 4-5) The smart eyewear camera and camera processor is capable of processing 1642 x 1642 px photos and 10-30 second 1216 x 1216 px video clips at 60 fps, all with a 105° field of view and 2.2 F-stop [151].

What makes Spectacles version 2 eyewear “smart” is the ability of the system to transmit and manage captured photographs and videos via wireless communication networks (Wifi, Bluetooth Low Energy, and location services). Spectacles version 2 contains two wireless networking System-on-chips (SoCs), the Qualcomm QCA9377 and the Nordic Semiconductor nRF52832, (see Table 4 and Figures 4-5).

Table 4. Spectacles version 2 smart eyewear wireless network SoCs Specifications [151] [152] [153] [154].

	Nordic Semiconductor nRF52832 Bluetooth SoC:	Qualcomm QCA9377 Wi-Fi/Bluetooth SoC:
CPU	ARM Cortex M4 32-bit processor with FPU, 64 MHz	Tensilica
Memory	Bluetooth: 512 kB flash/64 kB RAM 256 kB flash/32 kB RAM	One-Time-Programmable (OTP) Non-volatile memory (NVM) 1.5 KB Bluetooth: 192KB RAM/672KB ROM Wi-Fi: 1.2MB RAM/448KB ROM
Supported Interfaces	Bluetooth: Universal asynchronous receiver/transmitter (UART), SPI, TWI, PDM, I2S	Inter-IC Sound (I ² S) Bluetooth: PCM, Universal asynchronous receiver/transmitter (UART) Wi-Fi: Peripheral Component Interconnect Express (PCIe) 2.1
Bluetooth Versions	- Bluetooth 5.2 - Backward compatible with: - Bluetooth 4.x: Bluetooth Low Energy/Bluetooth Smart/Bluetooth High Speed (HS)/Bluetooth mesh/ANT	- Bluetooth 5.0 - Backward compatible with: - Bluetooth 4.x: Bluetooth Low Energy/Bluetooth Smart/Bluetooth High Speed (HS) - Bluetooth 2.x
Radio Spectral Band(s)	2.4GHz receiver / transmitter	2.4GHz and 5GHz

Bluetooth Class Support	Unknown	Class 2 and Class 1
Wi-Fi Standards	Not applicable	<ul style="list-style-type: none"> - 802.11ac Wave 2, Multi-User Multiple Input Multiple Output (MU-MIMO) - 802.11a/b/g/n
Wi-Fi Channel Utilization	Not applicable	20/40/80 MHz
Temperature sensor	Yes	Not applicable
Security	AES-128/ECB/CCM/AAR co-processor	Not applicable

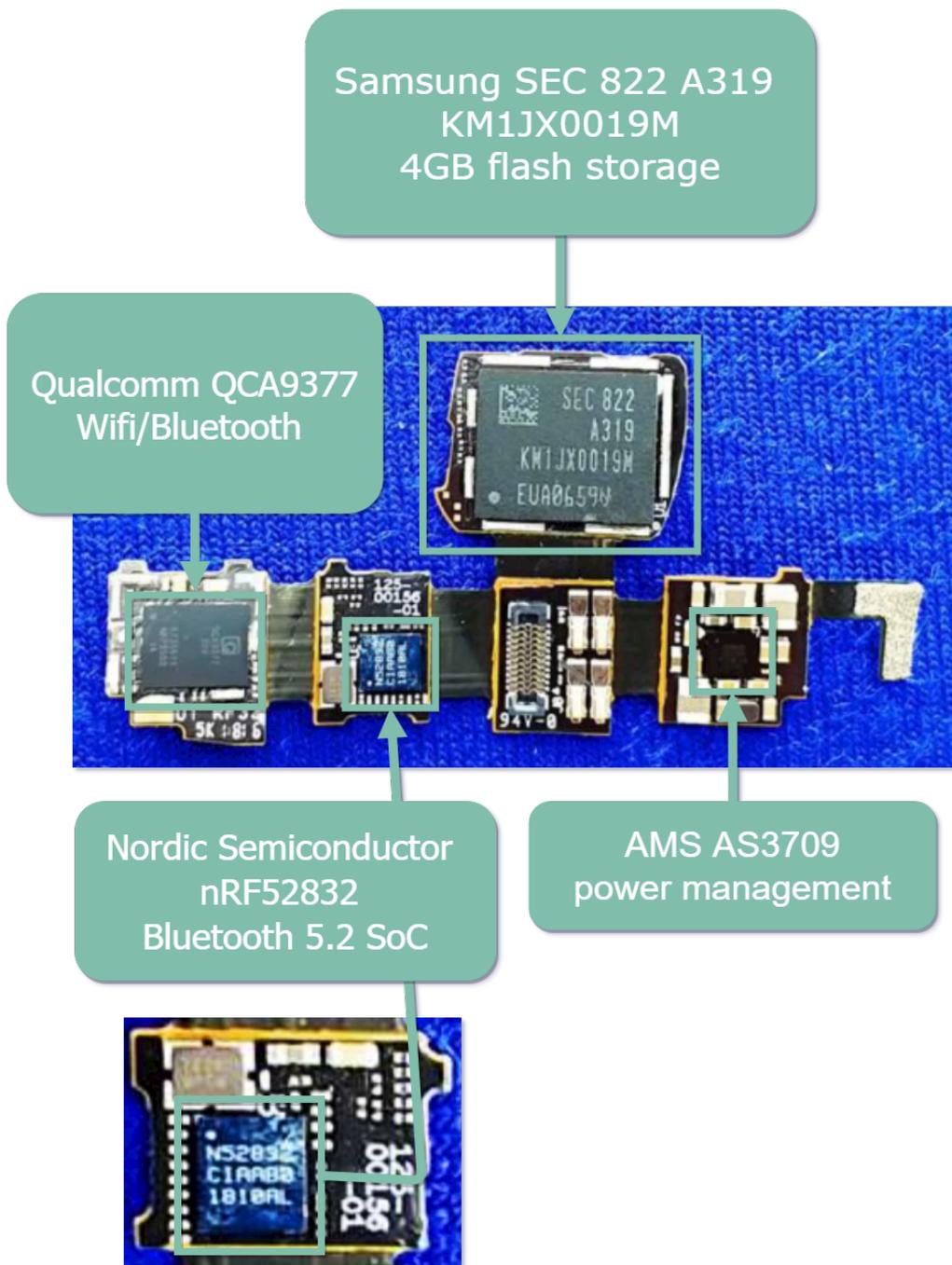


Figure 4. Snapchat Spectacles version 2 internal hardware [146][147] [150]

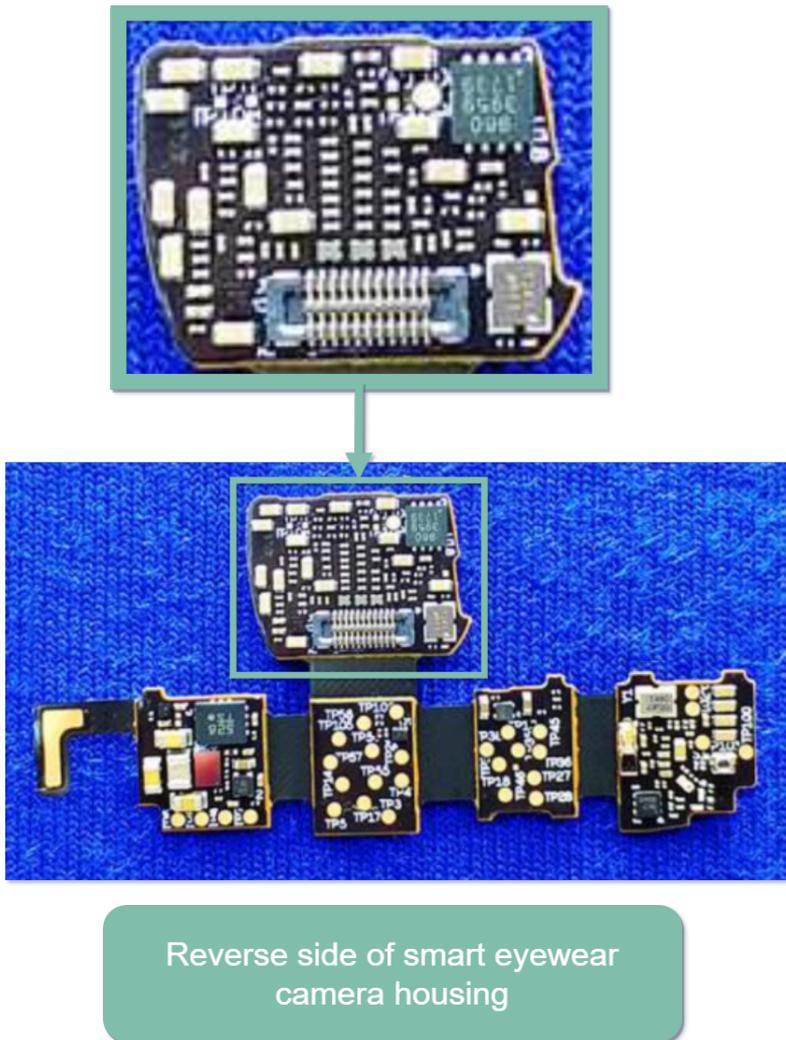


Figure 5. Snapchat Spectacles version 2 internal hardware - Reverse side [146][147] [150]

A single physical input button enables the smart eyewear to perform multiple actions including: capturing and storing photos and videos; smartphone pairing; restarting with a power cycle; hard resetting.

Inner sunglass LED signals notify device owner of: in progress and completion actions of photo and video capturing [155].

External sunglass LED signals notify of: low battery, no storage space, low/high extreme temperatures, initiated software updates, software errors [156].

External sunglass LED signals notify bystanders that photos and videos are being captured and recorded by the device [155] (figure 6).

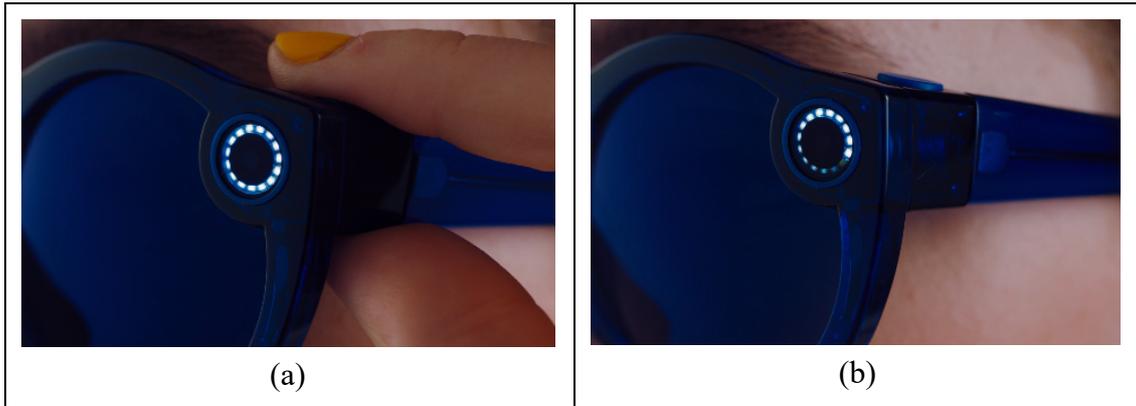


Figure 6. Bystander notification of (a) camera photographing (all lights, 1 blink) or (b) video recording (all lights, rotating swirl) [155].

The smart eyewear also requires GPS Location Services for pairing the device to an Android smartphone [157] ; however, it is unclear what IC chip was utilized.

Spectacles version 2 eyewear possess a built-in rechargeable Malibu lithium-ion battery Model SC03 PCM125-00132-01 with 3.8 rated voltage and a rated capacity of 96mAh/0.36Wh [150](figure 7) and an AMS AS3709 power management integrated chip (IC)[158] [151](figure 4) .

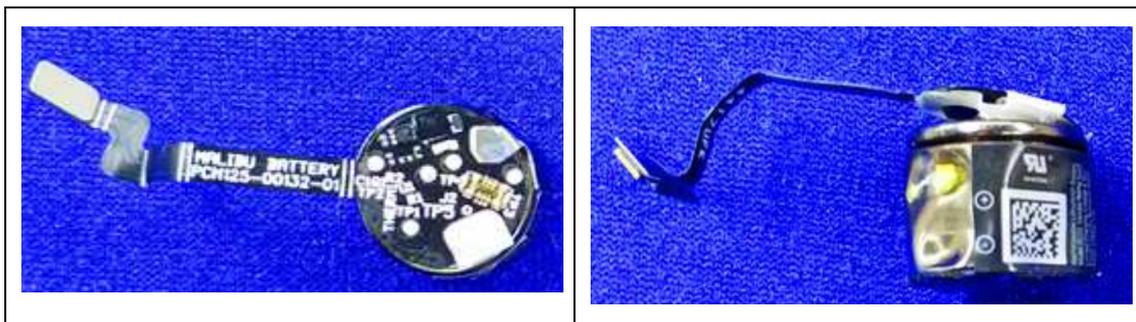


Figure 7. Snapchat Spectacles version 2 - Malibu lithium-ion battery Model SC03 [146][147] [150]

5 Research methods

Applied observational descriptive methods have been utilized to conduct a forensic case study, as the main objectives are to understand the smart eyewear's ability to manage privacy risks for biometric assets processed and apply the acquired understanding in the development of ISO/IEC 19510:2013 privacy risk models and NIST Privacy Framework Profiles to aid in resolving any found privacy risks.

Observational descriptive research methods are best suited to this study since access and resources to collect data from the smart eyewear's wireless communication networks and cloud are restricted, limited, and not fully controllable; due to the scale and complexity of wireless network variables and the smart eyewear cloud's restricted administrative privilege.

The observational scope of the study is descriptive versus exploratory, since the study's focus is limited to an in-depth and detailed systems examination on the privacy risk management of biometric assets processed by a single smart eyewear device.

6 Data collection methods

6.1 Participant observer simulated biometric data

Biometric data sourced for the study has been collected under a simulated operational environment to ensure any ethical concerns relative to capturing biometric data assets in a natural, unpredictable, and uncontrollable field environment are nullified.

Simulated biometric artifact collection reduced the time required to conduct the study since forensic tool testing and artifact acquisition was not contingent on the availability of biometric data subjects nor obtaining explicit permission consent forms to utilize an individual's personal data.

Simulations enabled the study's focus to remain on the forensic acquisition and analysis of the collected biometric artifacts as opposed to managing experiment test subjects, their personal biometric data, and the relative legal obligations surrounding such activities.

Photos and videos of individuals sourced from the public domain (Tables 5-6) were subsequently photographed and recorded by the researcher, acting as a participant observer, using the smart eyewear device as illustrated within Figure 8.



Table 5. Public domain photographs used in simulation [159] [160]

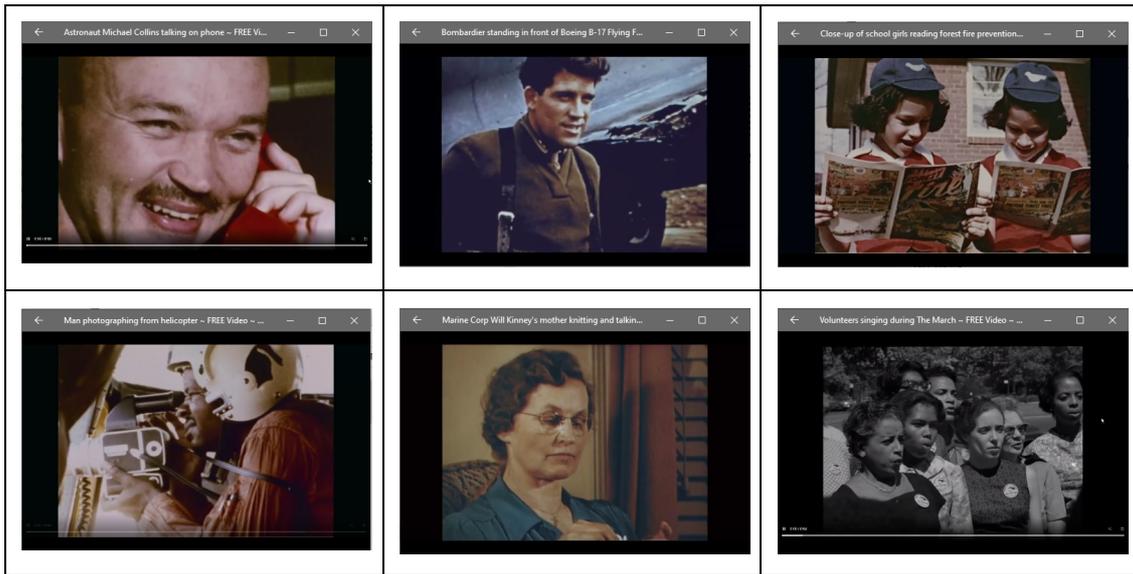


Table 6. Public domain videos used in simulation [159] [160]



Figure 8. Hardware setup for simulated biometric capture and collection [161] [151]

Since the smart eyewear does not possess any visual display hardware or cable port (enabling the connection to an external device with a visual display) to view, manage, or manually acquire images and video recordings directly from the wearable device's internal storage, a user test account has been generated within the smart eyewear's mobile management application, Snapchat, located on a wirelessly paired smartphone.

The test account enables the paired smartphone to manage the biometric photographs and videos collected by the smart eyewear. During the study, the smartphone application was prompted to: a.) export photographs and videos from the smart eyewear to the paired smartphone, thereafter the system auto-deletes transferred files from the smart eyewear and b.) delete photographs and videos stored on the smart eyewear and not send to the smartphone.

The collection of biometric assets by the smart eyewear facilitates the study's understanding of how an individual's personally identifiable data is subject to privacy risks within a forensic investigation.

6.2 Forensic Examinations

A series of forensic examinations have been conducted to observe, identify, and define network and system privacy risks within the Spectacles version 2 smart eyewear ecosystem.

The researcher, acting as participant observer, prompted the smart eyewear to transfer captured and stored photographs and videos of individuals over wireless communication networks, including the Internet, Wi-Fi, Bluetooth, BLE, and location services to the paired smartphone. Network forensics examinations have been conducted concurrently with the aforementioned actions, while systems forensics examinations thereafter.

Attempts have been made to extract biometric assets, in the form of .jpg images, .mp4 videos, and files containing relative data and metadata, from network communications, device hardware, and device software of the smart eyewear, paired smartphone, and the smart eyewear application cloud through a combination of open source and commercial forensic software and hardware.

6.2.1 Forensic exam I: Wi-Fi scanning and enumeration

Forensic exam I highlights a case wherein an investigator possesses access to open source 802.11 wireless local area network (WLAN) scanning and enumerating smartphone and laptop applications and is capable of locating themselves and their monitoring devices within the devices' 802.11 WLAN network range.

The forensic investigator has not obtained custody of a suspect or witnesses' smart eyewear nor their paired smartphone. The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table 7 for further detail.

Table 7. Forensic exam I: Chain of custody, network access, system administration status

Target Devices	Chain of Custody	Network Access	System Administration Status
Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	Access to open 802.11 WLAN networks	Not Rooted
Samsung Galaxy S10e smartphone (BLE paired to smart eyewear)	Device not possessed by forensic investigator	Access to open 802.11WLAN networks	Not Rooted

6.2.1.1 Forensic exam I: Methods and tools

Open source Wi-Fi scanning tools (WiFi Monitor v1.11 [162], Network Analyzer Lite v3.7 [163], Network Mapper (NMAP) v7.80 [175], and Wireshark win64 v3.0.10-0-gaa0261e8ddf3 [164]) were installed on monitoring devices in attempts to scan and enumerate target devices within the smart eyewear ecosystem, see Table 13, as they were capturing, storing, and transmitting simulated photographs and videos of individuals.

Table 8. Forensic exam I: WiFi scanning and enumeration tools.

Device	Software and peripherals
Target device: Snapchat Spectacles Version 2 smart eyewear	<ul style="list-style-type: none"> - Charging peripherals required for high battery use activities
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	<ul style="list-style-type: none"> - Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0 [120]
Monitoring smartphone	<ul style="list-style-type: none"> - Android v9 - WiFi Monitor v1.11 [162] - Network Analyzer Lite v3.7 [163]
Monitoring laptop	<ul style="list-style-type: none"> - Windows 10 Operating system - Wireshark OUI lookup tool [165] - Network Mapper (NMAP) v7.80 [175] - Wireshark win64 v3.0.10-0-gaa0261e8ddf3 [164]

6.2.1.2 Forensic exam I: Analysis, results, and discussion

WiFi Monitor v1.11 was incapable of gathering any information on the Snapchat Spectacles Version 2 smart eyewear and provided limited information on the paired Samsung Galaxy S10e smartphone.

The “SCAN” tab within WiFi Monitor v1.11 presented the Samsung Galaxy S10e’s dynamic internal IPv4 address 192.168.0.107 and the device’s 48-bit Extended Unique Identifier (EUI-48): a6:d0:e9:01:8c:ef, see Figure 2.

Note, “EUI-48... identifiers are most commonly used as globally unique network addresses (sometimes called MAC addresses)... For example, an EUI-48 is commonly

used as the address of a hardware interface according to IEEE Std 802, historically using the name “MAC-48”.”[166]

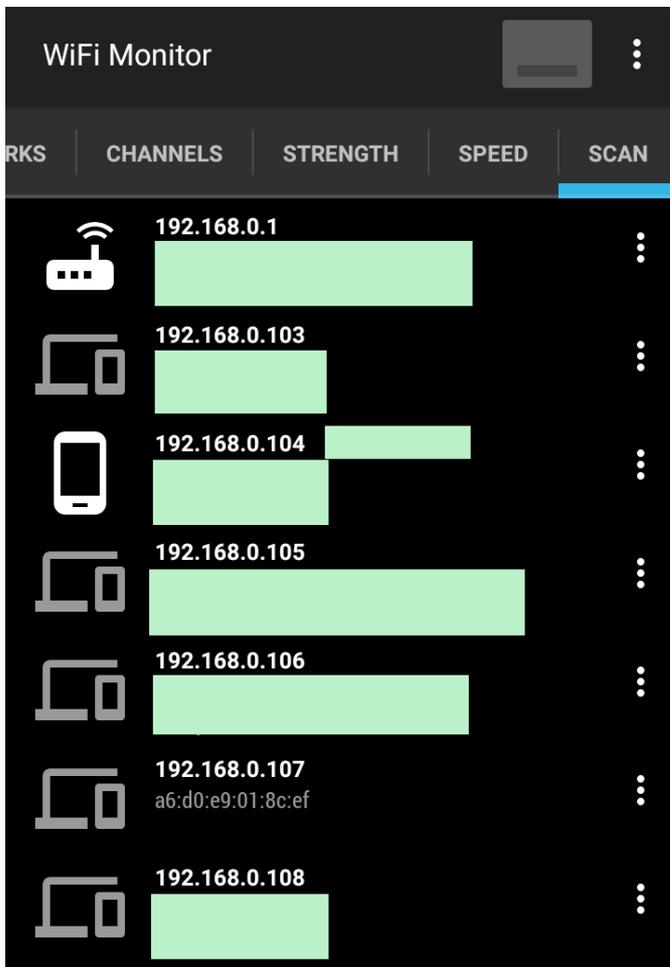


Figure 9. Forensic exam I: WiFi Monitor v1.11 network scan results

Figure 3 illustrates Samsung Galaxy S10e smartphone’s system defined 802.11 WLAN MAC-48 address, as depicted by a screenshot directly from the smartphone.

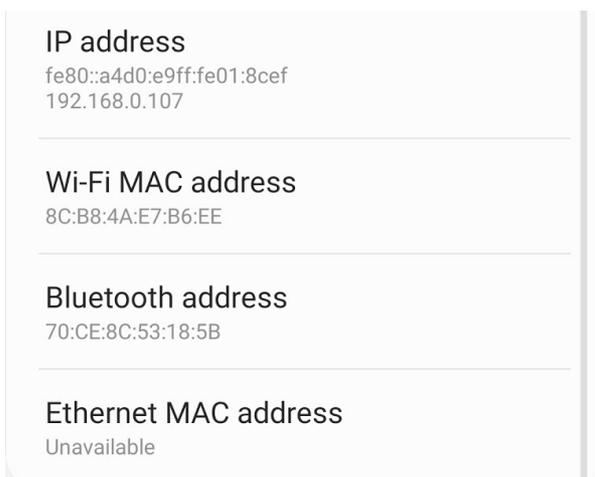


Figure 10. Forensic exam I: Network addresses from Samsung Galaxy S10e

The information within Figure 3 is not available to the network investigator within our scanning and enumeration scenario, as such, the process of eliminating non-target devices detected within a 802.11 WLAN network scan would require additional visual surveillance and identification of target devices carried by the device owner in question.

The paired Samsung Galaxy S10e smartphone’s network scanned and system defined EUI-48 addresses both indicated the device is an individual address, denoted by the least significant bit of Octet 0 (the I/G bit) being zero, see table x.

The paired Samsung Galaxy S10e smartphone’s system defined EUI-48 address indicates the device address is universally administered, denoted by the second least significant bit of Octet 0 (the U/L bit) being 0, see table x. As a universally administered address, it is a globally unique network address, and thus a factory default MAC-48 address, see table x.

The paired Samsung Galaxy S10e smartphone’s network scanned EUI-48 address indicated the device address is locally administered and not the factory default MAC-48 address, denoted by the second least significant bit of Octet 0 (the U/L bit) being 1, see table x.

Table 9. Forensic exam I: 48-bit Extended Unique Identifiers (EUI-48) [166]

EUI-48 specifics	MAC-48/EUI-48 address of paired Samsung Galaxy S10e smartphone	Scanned EUI-48 address of paired Samsung Galaxy S10e smartphone
Samsung Galaxy S10e smartphone EUI-48 addresses	8C:B8:4A:E7:B6:EE	a6:d0:e9:01:8c:ef
First octet (Octet 0) of hexadecimal Wi-Fi MAC address	xC :xx:xx:xx:xx:xx	x6 :xx:xx:xx:xx:xx
Least-significant bit of binary address: Individual address (I/G bit = 0) (Unicast) Group address (I/G bit = 1) (Multicast/Broadcast)	00001100 xxxxxxx 0	00000110 xxxxxxx 0
Second-least-significant bit of binary address: Universal administration of the address (U/L bit = 0) (Factory default) Local administration of the address (U/L bit = 1) (NOT factory default)	00001100 xxxxxxx 0 x	00000110 xxxxxxx 1 x

Wireshark OUI lookup tool [165] was used to cross verify Organizationally Unique Identifier (OUI) results from the WiFi Monitor v1.11 network scan, see Figure 4 (a)(b)(c). However, these tools provide greater information to investigators when

targeted devices use their MAC-48 address as their EUI-48 address, as illustrated in Figure 2 and Figure 4(b)(c).

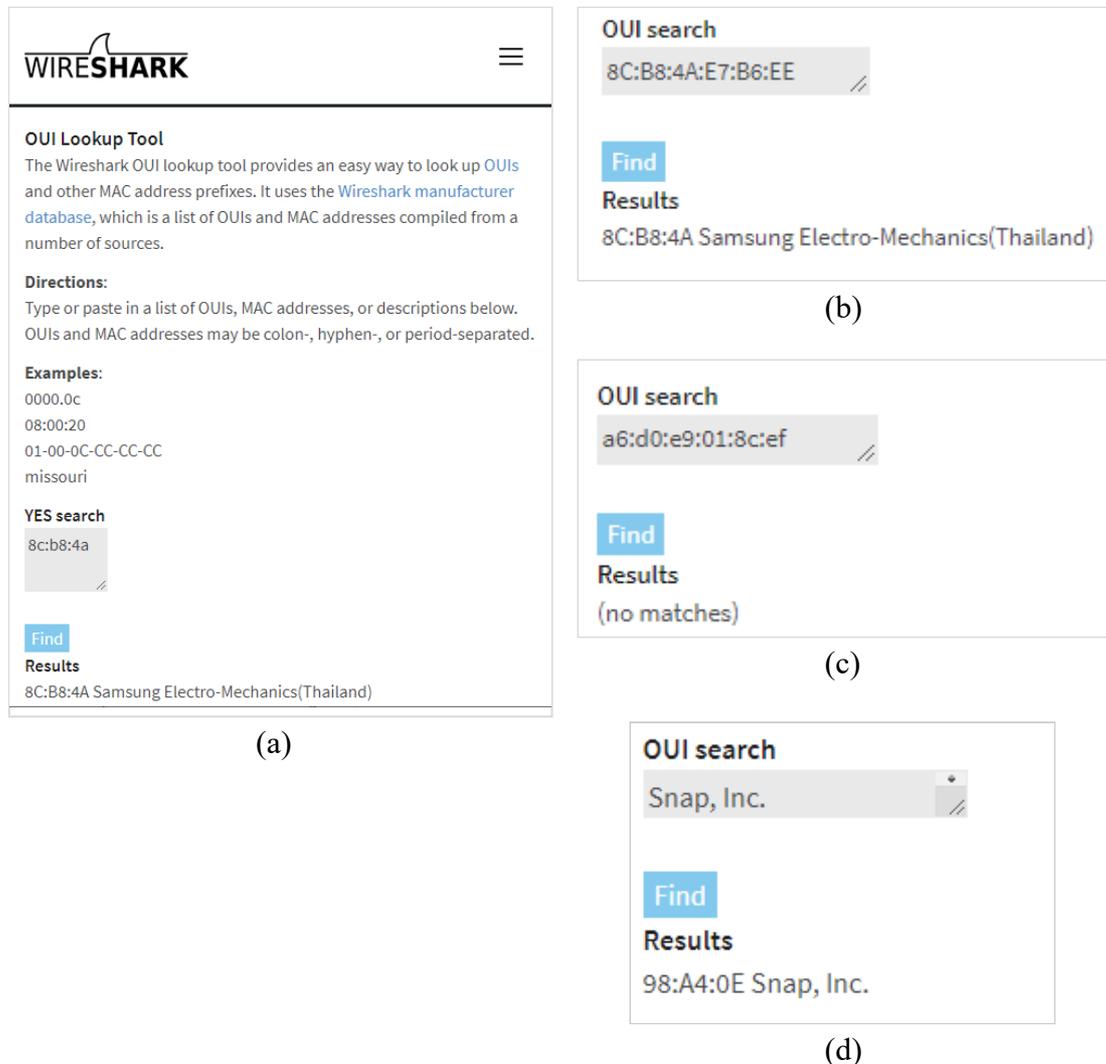


Figure 11. Forensic exam I: Confirmation of paired smartphone's OUI (a) Wireshark OUI lookup tool (b) System defined MAC-48 (c) Network scanned EUI-48 (d) Snap, Inc.'s OUI [165]

After initiating multiple scans with WiFi Monitor v1.11, the monitoring smartphone automatically disconnected from the Wi-Fi connection, requiring a connection reset to resume scanning.

In addition to scanning Wi-Fi networks, the smartphone application Network Analyzer Lite v3.7 [163] provided more enumeration tools than WiFi Monitor v1.11, such as port scanning to identify host network services and functions.

Nevertheless, attempts to gather any information on the smart eyewear device's Wi-Fi hostname, addresses, ports, or host network services with Network Analyzer Lite v3.7 also proved unsuccessful.

Parallel to WiFi Monitor v1.11's results, Network Analyzer Lite v3.7 provided Samsung Galaxy S10e's dynamic internal IPv4 address 192.168.0.103 (change is due to IP

dynamic assignment), the device's EUI-48 "a6:d0:e9:01:8c:ef ", and was unable to provide the device's OUI (denoted as "N/A"), see Figure 5.

Network Analyzer Lite v3.7 additionally determined there is a known IPv6 address for the device (denoted by the purple "6" flag) and that the device responds to ICMP ping requests (denoted by the green "P" flag), see Figure 5. The IPv6 address was not provided by Network Analyzer Lite v3.7, only a notification that it was known.

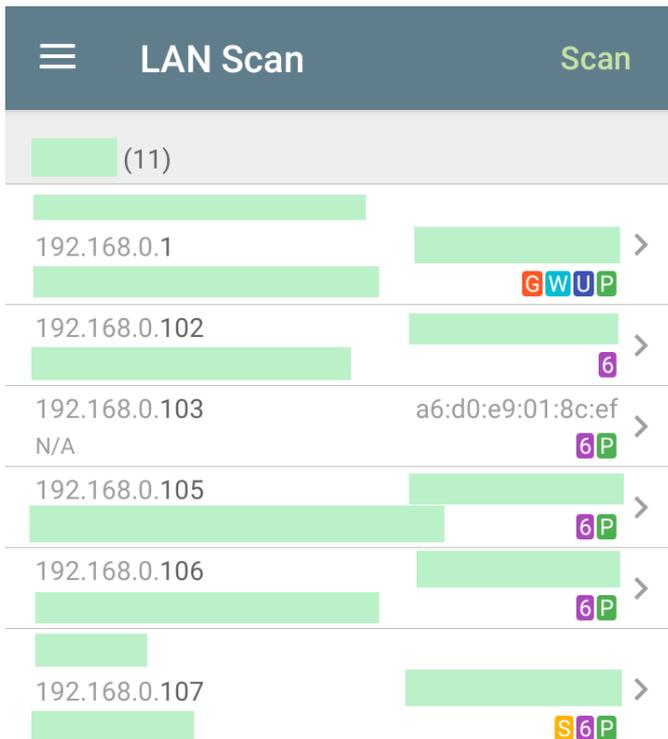


Figure 12. Forensic exam I: Network Analyzer Lite v3.7 scan results for smart eyewear paired smartphone

A port scan was performed on the target Samsung Galaxy S10e paired smartphone using Network Analyzer Lite v3.7. System ports 0-1023 on the mobile device were either closed or blocked, see Figure 6. The blocked ports indicate a firewall is in use.

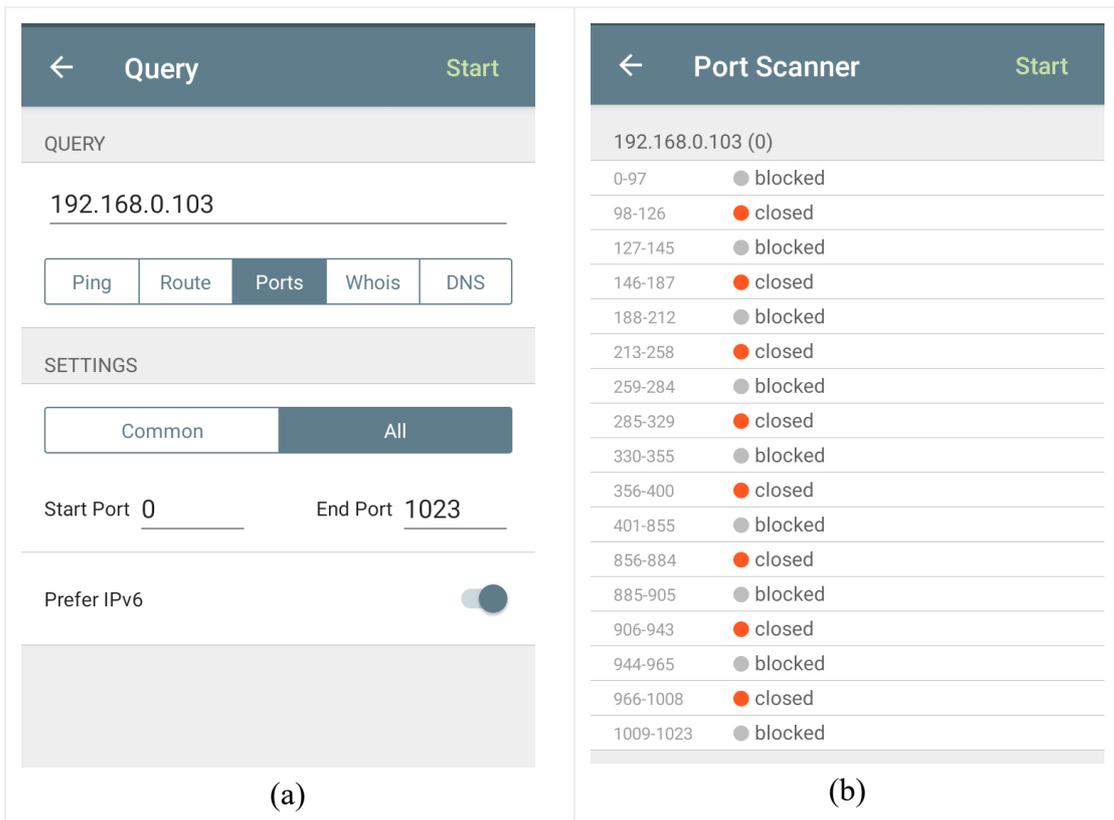


Figure 13. Forensic exam I: Network Analyzer Lite v3.7 Port Scanner results for smart eyewear paired smartphone (a) Port Scanner: Query (b) Port Scanner results

Note, Network Analyzer Lite v3.7 only permits scanning ports 0-1023.

Network Mapper (NMAP) v7.80 [175], loaded on a monitoring laptop, was utilized to cross verify scanning and enumeration results from WiFi Monitor v1.11 and Network Analyzer Lite v3.7, see Figures 7-8.

A host discovery ping scan that disables default port scanning was performed on 256 hosts within the specified “192.168.0.1/24” target by selecting the NMAP Scan Type, “-sn” [167] see Figure 7. Host discovery defaults for the -sn scan type include “an ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp request by default.” [167]

The NMAP v7.80 host discovery ping scan confirmed no enumerable smart eyewear hostname, IP addresses, EUI-48/MAC-48 addresses, ports, or host network services were determined; only the target paired smartphone was identified within the 6 available hosts (Figure 7).

NMAP v7.80 results matched WiFi Monitor v1.11 and Network Analyzer Lite v3.7 as follows: located an internal dynamic IP address “192.168.0.103”, a matching EUI-48 address “ A6:D0:E9:01:8C:EF ”, and a matching unknown OUI for the target paired smartphone, see figure x-x, tables x-x.

```

Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 16:27 FLE Daylight Time
Nmap scan report for 192.168.0.1
Host is up (0.0020s latency).
MAC Address: *****

Nmap scan report for 192.168.0.107
Host is up (0.079s latency).
MAC Address: *****

Nmap scan report for 192.168.0.120
Host is up (0.0020s latency).
MAC Address: ***** (****)

Nmap scan report for 192.168.0.254
Host is up (0.0030s latency).
MAC Address: *****

Nmap scan report for 192.168.0.111
Host is up.
Nmap done:          (          ) scanned in 4.66 seconds

```

Figure 14. Forensic exam I: NMAP v7.80 results from host discovery ping scan with disabled port scanning for smart eyewear paired smartphone

The following NMAP query, see figure x, scanned all TCP and UDP ports on the target paired smartphone to determine their status, the reasoning why a port is in such a state, and additionally requested a verbose detection of device fingerprinting information including operating system, version, script scanning, and traceroute [168] table x appendix X table x.

NMAP v7.80 reported that it received an arp-response indicating the target smartphone host is up, all host network service ports were closed; more specifically NMAP’s Open TCP ports (OT), Closed TCP ports (CT), and Closed UDP ports (CU) tests found no open TCP ports, 1 closed TCP port, and 38,462 closed UDP ports on target paired smartphone, see figure x-x, tables x-x, appendix X

NMAP v7.80 further reported “All 1000 scanned ports on 192.168.0.103 are closed because of 1000 resets” (figure x) and that “Too many fingerprints match this host to give specific OS details”(figure x).

```

Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 15:47 FLE Daylight Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Initiating ARP Ping Scan at 15:47
Scanning 192.168.0.103 [1 port]
Completed ARP Ping Scan at 15:47, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:47
Completed Parallel DNS resolution of 1 host. at 15:47, 0.01s elapsed
Initiating SYN Stealth Scan at 15:47
Scanning 192.168.0.103 [1000 ports]
Completed SYN Stealth Scan at 15:47, 4.62s elapsed (1000 total ports)
Initiating Service scan at 15:47
Overriding exclude ports option! Some undesirable ports may be version scanned!
Initiating OS detection (try #1) against 192.168.0.103
Retrying OS detection (try #2) against 192.168.0.103
NSE: Script scanning 192.168.0.103.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Nmap scan report for 192.168.0.103
Host is up, received arp-response (0.042s latency).
All 1000 scanned ports on 192.168.0.103 are closed because of 1000 resets
MAC Address: A6:D0:E9:01:8C:EF (Unknown)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=4/21%OT=%CT=1%CU=38462%PV=Y%DS=1%DC=D%G=N%M=A6D0E9%TM=5E9EEB6F%P=***
*-pc-windows-windows)
SEQ(CI=Z%II=I)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 42.47 ms 192.168.0.103
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.93 seconds
Raw packets sent: 1124 (50.580KB) | Rcvd: 1061 (43.552KB)

```

Figure 15. Forensic exam I: NMAP v7.80 port and device fingerprinting scan results for smart eyewear paired smartphone

Table 10. Forensic exam I: NMAP v7.8 TCP/IP SCAN fingerprint results for smart eyewear paired smartphone [169]

SCAN test names	SCAN test results
Nmap version number (V):	V=7.80
IPvX fingerprint:	E=4
Date of scan (D) (month/day):	D=4/21
Open TCP ports (OT):	OT= Empty since Nmap found no open TCP ports on target
Closed TCP ports (CT):	CT=1 Nmap found 1 closed TCP port on target
Closed UDP ports (CU):	CU=38462 Nmap found 38,462 closed UDP ports on target
Private IP space (PV):	PV=Y The target is on the 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 private networks (RFC 1918).
Network distance (DS):	DS= 1 = Directly connected on an ethernet network. Network hop distance from the target.
Distance calculation method (DC):	DC= D = Direct subnet connection (DS=1) Indicates how network distance (DS) was calculated by verifying the host is truly directly connected and no ICMP TTL miscalculation occurred when intermediate machines changed TTL.
Good results (G):	G=N = No , results were not good enough to submit fingerprint to Nmap.Org.
Target MAC prefix (M):	M=A6D0E9 Probe returned the first six hex digits of target MAC address. Since the target is on the same ethernet network, results were not omitted. (DS=1).
The OS scan time (TM) (Unix time_t format, in hexadecimal):	TM=5E9EEB6F Decimal format: 1587473263 04/21/2020 @ 12:47pm (UTC)
Platform Nmap was compiled for (P):	P=****-pc-windows-windows

Wireshark win64 v3.0.10-0-gaa0261e8ddf3 [164] provided additional verification and data validation for 802.11 wireless local area network (WLAN) scanning and enumeration. Wireshark results matched WiFi Monitor v1.11, Network Analyzer Lite v3.7, and NMAP v7.80 as follows: located an internal dynamic IP address “192.168.0.107” and a matching EUI-48 address “ A6:D0:E9:01:8C:EF ”, see figures X-X.

However, in contrast, Wireshark’s capture of Dynamic Host Configuration Protocol (DHCP) Discover and Request Message Type communications additionally provided

vendor-specific information on the target smart eyewear paired smartphone including: Vendor Class Identifier: “android-dhcp-10” and Host Name: “Galaxy-S10e”, see figures x-x.

No 802.11 WLAN communications were detected from the smart eyewear.

Restrictions on altering the 802.11 WLAN capture modes on the monitoring laptop running Windows 10 [170] [171] [172] resulted in the incorrect display of “Encapsulation Type” as “Ethernet” in instances where “IEEE 802.11 plus radiotap radio header” should be displayed, as seen within Figure x-x.

The image shows two Wireshark packet capture windows. The top window is filtered for 'eth.src == a6:d0:e9:01:8c:ef' and displays four packets:

No.	Source	eth.src Source	Destination address	eth.dst Destination	Protocol	Info
765	0.0.0.0	a6:d0:e9:01:8c:ef	255.255.255.255	ff:ff:ff:ff:ff:ff	DHCP	DHCP Discover - Transaction ID 0x8b67c51c
772	0.0.0.0	a6:d0:e9:01:8c:ef	255.255.255.255	ff:ff:ff:ff:ff:ff	DHCP	DHCP Request - Transaction ID 0x8b67c51c
775	a6:d0:e9:01:8c:ef	a6:d0:e9:01:8c:ef	Broadcast	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.0.1? Tell 192.168.0.107
776	a6:d0:e9:01:8c:ef	a6:d0:e9:01:8c:ef	Broadcast	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.0.1? Tell 192.168.0.107

The bottom window is also filtered for 'eth.src == a6:d0:e9:01:8c:ef' and displays four Ethernet packets:

Encapsulation type	Vendor class identifier	Host Name	Time	Arrival Time
Ethernet	android-dhcp-10	Galaxy-S10e	2020-07-21 14:51:00.401108000	Jul 21, 2020 17:51:00.401108000 FLE Daylight Time
Ethernet	android-dhcp-10	Galaxy-S10e	2020-07-21 14:51:01.580252000	Jul 21, 2020 17:51:01.580252000 FLE Daylight Time
Ethernet			2020-07-21 14:51:01.744500000	Jul 21, 2020 17:51:01.744500000 FLE Daylight Time
Ethernet			2020-07-21 14:51:01.864843000	Jul 21, 2020 17:51:01.864843000 FLE Daylight Time

Figure 16. Forensic exam I: Wireshark Wireshark win64 v3.0.10-0-gaa0261e8ddf3 Wi-Fi scan results for smart eyewear paired smartphone

None of the Wi-Fi scanning tools were capable of intercepting any Wi-Fi communication packets containing photographs or videos between the smart eyewear and paired smartphone.

6.2.2 Forensic exam II: BLE scanning & enumeration

Forensic exam II highlights a case wherein an investigator possesses access to open source Bluetooth Low Energy (BLE) scanning and enumerating smartphone applications and is capable of locating themselves and their monitoring device within the smart eyewear’s BLE network range.

The forensic investigator has not obtained custody of a suspect or witnesses’ smart eyewear nor their paired smartphone. The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table x for further detail.

Table 11. Forensic exam II: Chain of custody, network access, system administration status

Devices	Chain of Custody	Network Access	System Administration Status
Target device: Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	Access to open Bluetooth Low Energy networks	Not Rooted
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	Device not possessed by forensic investigator	Access to open Bluetooth Low Energy networks	Not Rooted

6.2.2.1 Forensic exam II: Methods and tools

Open source Bluetooth Low Energy tools, see Table 14, were installed and initiated on a monitoring smartphone to scan and enumerate the following target devices: Snapchat Spectacles Version 2 smart eyewear and the paired Samsung Galaxy S10e smartphone.

While scanning and enumerating for BLE communications, the researcher, as a participant observer, captured simulated photos and videos of individuals with the smart eyewear, paired the smart eyewear and smartphone, and sent the images and videos from the smart eyewear to the paired smartphone.

Table 12. Forensic exam II: BLE scanning and enumeration tools

Device	Software and peripherals
Target device: Snapchat spectacles Version 2 smart eyewear	- Charging peripherals required for high battery use activities
Target device: Samsung Galaxy S10e smartphone (BLE paired to smart eyewear)	- Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0 [120]
Monitoring smartphone	- Android v9 - nRF Connect v4.24.3 [173] - nRF Logger v1.9.0 [174]

nRF Connect v4.24.3, used in conjunction with nRF Logger v1.9.0, require permissions to use the monitoring smartphone's location and Bluetooth adapters. Once permissions are enabled, scanning for host devices can be initiated.

6.2.2.2 Forensic exam II: Analysis, results, and discussion

Advertising packets sent by the smart eyewear to the paired Samsung Galaxy S10e smartphone were intercepted by the nRF Connect Scanner via the monitoring smartphone, see Figures x (a)(b)for BLE scan results.

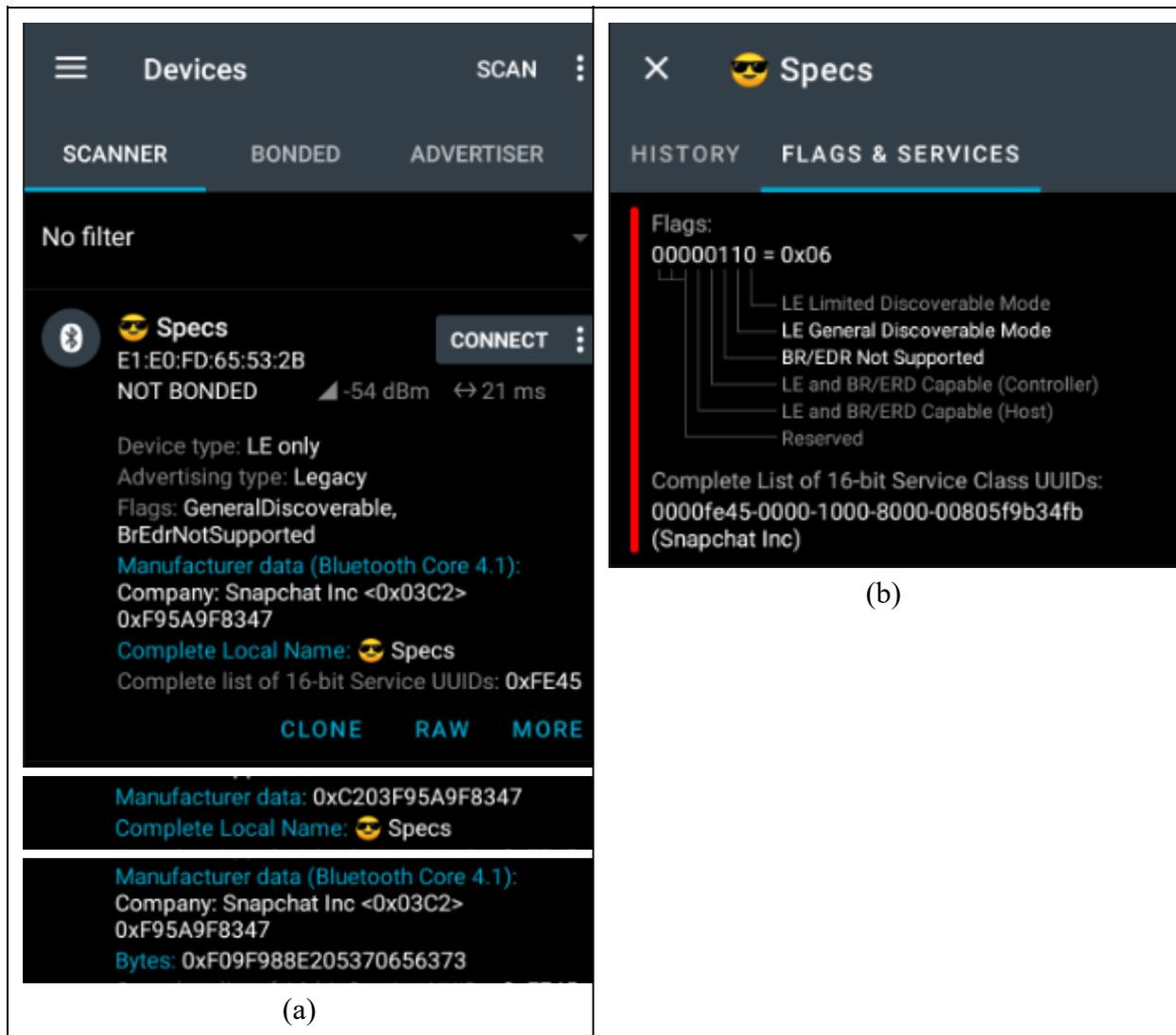


Figure 17. Forensic exam II: nRF Connect (a)“SCANNER” and (b)“FLAGS & SERVICES” screenshots of Spectacles version 2 smart eyewear BLE communications

Nordic Semiconductor’s nRF Connect scan and enumeration of Snapchat Spectacles version 2 smart eyewear provided crucial information needed to identify the: IoT mobile device; the device’s BLE network communication details; the device’s supported network services and characteristics, see Tables x-x and Figures x-x.

Table 13. Forensic exam II: Smart eyewear BLE data obtained from nRF Connect “SCANNER” and “FLAGS & SERVICES”

Description	Data obtained from nRF Connect scan results
Complete Local Name	 Specs Bytes (Hexadecimal):0xF09F988E205370656373 Hexadecimal to UTF-8: F0 9F 98 8E: “  ” 20: “ ” 53 70 65 63 73: “ Specs ”
BLE EUI-48 ADDRESS	E1:E0:FD:65:53:2B
Bonded/Not Bonded	Not bonded
Device Type	LE only (Low Energy only)
Advertising Type	Legacy
Flags	GeneralDiscoverable, BrEdrNot Supported
Bluetooth version	Bluetooth Core 4.1
Snapchat’s Company Identifier	Hexadecimal notation: 0x03C2 Decimal notation: 962
Manufacturer data: (Portion of Serial Number as noted by Forensic Exam VIII)	0x*****
16-bit Universally Unique Identifier (UUID) Value (Also the abbreviated alias of Snapchat Inc.’s full 128-bit Bluetooth SIG UUID)	Hexadecimal notation: 0xFE45 Decimal notation: 65093
Snapchat Inc’s full 128-bit Bluetooth SIG Universally Unique Identifier (UUID)	0000 FE45 -0000-1000-8000-00805F9B34FB

Bluetooth SIG’s assigned numbers online database confirmed, Snapchat was allocated their 16-bit Universally Unique Identifier (UUID), “FE45”, on 04/10/2016 [176].

Snapchat Inc.’s Company Identifier of “0x03C2”, in hexadecimal notation (Decimal notation: 962), was also confirmed by Bluetooth SIG [177].

Bluetooth Special Interest Group (SIG) adopted a standard Bluetooth Base UUID of “00000000-0000-1000-8000-00805F9B34FB” to reduce the amount of data sent with each communication [178]. The first 16-bits are zero for 16-bit UUIDs, like Snapchat Inc’s 0xFE45. The full 128-bit Bluetooth SIG UUID is derived as follows:

$$128\text{-bit value} = \mathbf{0000FE45} + 00000000\text{-}0000\text{-}1000\text{-}8000\text{-}00805F9B34FB$$

Snapchat Inc’s Bluetooth SIG UUID version and variant are, Version 1 (1xxx) and Variant 8 (8xxx) [179].

Raw data obtained from the smart eyewear’s advertising packets (Figure x) is clarified within Table x. Note, nRF Connect concisely converts raw data packets and displays most of this information in human readable form within the “SCANNER” tab (Figure 9) without requiring a search for Bluetooth core specifications.

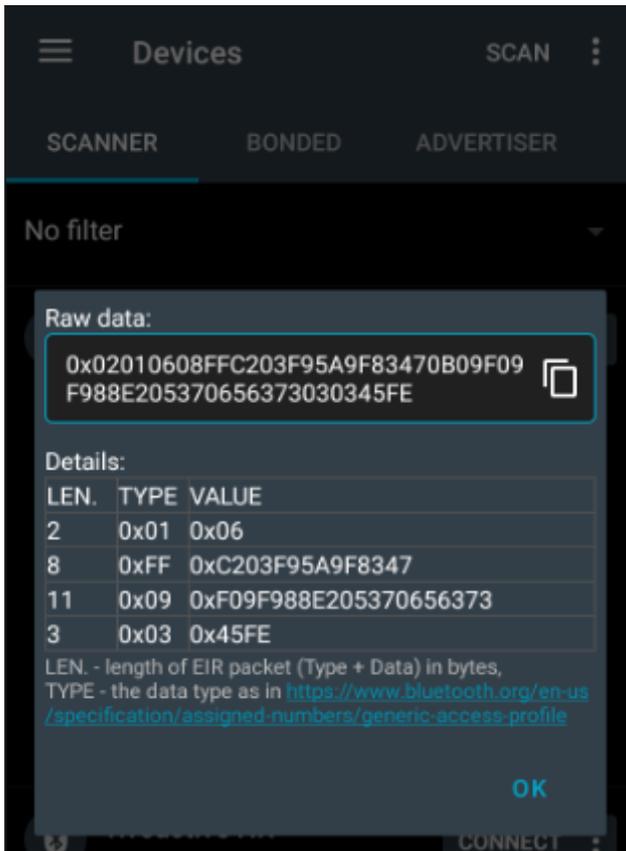


Figure 18. Forensic exam II: nRF Connect “SCANNER: Raw data” results

Table 14. Forensic exam II: nRF Connect “SCANNER: Raw data” results and Bluetooth generic access profile specifications [180][181][182][183].

Length of EIR packet (Type + Data) in bytes	Data Type Value	Data Type Name	Value	Description
2	0x01	«Flags»	06	Flag “06”: General Discoverable; Bluetooth Basic Rate/ Enhanced Data Rate Not Supported
8	0xFF	«Manufacturer Specific Data»	C2 03	First 2 octets: Company Identifier Code (Encoded in Little-endian)

				Hexadecimal: 0x03C2 Decimal: 962 Snapchat Inc Second 2 octets: Additional manufacturer specific data
11	0x09	«Complete Local Name»	F0 9F 98 8E 20 53 70 65 63 73	Complete local name of BLE smart eyewear device UTF-8: 😊 Specs
3	0x03	«Complete List of 16-bit Service Class UUIDs»	45 FE	Bluetooth SIG Member 16-bit Assigned UUID (Encoded in Little-endian) Hexadecimal: 0xFE45 Snapchat Inc

nRF Connect and nRF Logger provided the enumeration of the smart eyewear’s BLE network services and characteristics within a log file (Figure x). See Table x-x for a detailed breakdown of all services and characteristics extracted from nRF Logger.

```
nRF Connect, 2020-03-28
😊 Specs (EE:FD:FE:5B:FB:0A)
V 12:20:03.877 Connecting to EE:FD:FE:5B:FB:0A...
D 12:20:03.877 gatt = device.connectGatt(autoConnect = false, TRANSPORT_LE, preferred PHY = LE
LM)
D 12:20:04.040 [Callback] Connection state changed with status: 0 and new state: CONNECTED (2)
I 12:20:04.040 Connected to EE:FD:FE:5B:FB:0A
D 12:20:04.041 [Broadcast] Action received: android.bluetooth.device.action.ACL_CONNECTED
V 12:20:04.127 Discovering services...
D 12:20:04.127 gatt.discoverServices()
I 12:20:04.658 Connection parameters updated (interval: 7.5ms, latency: 0, timeout: 5000ms)
D 12:20:04.805 [Callback] Services discovered with status: 0
I 12:20:04.806 Services discovered
V 12:20:04.837 Generic Access (0x1800)
- Device Name [R W] (0x2A00)
- Appearance [R] (0x2A01)
- Peripheral Preferred Connection Parameters [R] (0x2A04)
- Central Address Resolution [R] (0x2AA6)
Generic Attribute (0x1801)
- Service Changed [I] (0x2A05)
Client Characteristic Configuration (0x2902)
Unknown Service (0000fe45-0000-1000-8000-00805f9b34fb)
- RX Characteristic [W WNR] (6e400002-b5a3-f393-e0a9-e50e24dcca9e)
- TX Characteristic [N] (6e400003-b5a3-f393-e0a9-e50e24dcca9e)
Client Characteristic Configuration (0x2902)
D 12:20:04.842 gatt.setCharacteristicNotification(00002a05-0000-1000-8000-00805f9b34fb, true)
D 12:20:04.845 gatt.setCharacteristicNotification(6e400003-b5a3-f393-e0a9-e50e24dcca9e, true)
I 12:20:04.857 Connection parameters updated (interval: 15.0ms, latency: 30, timeout: 6000ms)
```

Figure 19. Forensic exam II: BLE network services and characteristics data extracted via nRF Connect and nRF Logger from smart eyewear

Table 15. Forensic exam II: Data obtained from nRF Logger results, descriptions, and Nordic Semiconductor's Assigned Values for BLE UUIDs [184]

Data obtained from nRF Logger	Description
☺ Specs	Complete Local Name
EE:FD:FE:5B:FB:0A	BLE EUI-48 ADDRESS
TRANSPORT_LE	Prefer Bluetooth Low Energy transport for Generic Attribute Profile (GATT) connections to remote dual-mode devices, Constant Value: 2 (0x00000002) [185]
preferred PHY = LE 1M	Bluetooth Low Energy 1 mega symbol per second (Ms/s) [186] Physical Channel for advertising, scanning or connection Constant Value: 1 (0x00000001)[187]
[Broadcast] Action received: android.bluetooth.device.action.ACL_CONNECTED	Broadcast Action: Indicates a low level Asynchronous Connection-Less (ACL) connection has been established with a remote device [188] "ACL connections are managed automatically by the Android Bluetooth stack." [189]
Generic Access (0x1800)	Generic Access Profile BLE_UUID_GAP
Device Name [R W] (0x2A00)	Device Name Characteristic BLE_UUID_GAP_CHARACTERISTIC_DEVICE_NAME
Appearance [R] (0x2A01)	Appearance Characteristic BLE_UUID_GAP_CHARACTERISTIC_APPEARANCE
Peripheral Preferred Connection Parameters [R] (0x2A04)	Peripheral Preferred Connection Parameters Characteristic BLE_UUID_GAP_CHARACTERISTIC_PPCP
Central Address Resolution [R] (0x2AA6)	Central Address Resolution Characteristic BLE_UUID_GAP_CHARACTERISTIC_CAR
Generic Attribute (0x1801)	Generic Attribute Profile BLE_UUID_GATT
Service Changed [I] (0x2A05)	Service Changed Characteristic BLE_UUID_GATT_CHARACTERISTIC_SERVICE_CHANGED
Client Characteristic Configuration (0x2902)	Client Characteristic Configuration Descriptor BLE_UUID_DESCRIPTOR_CLIENT_CHAR_CONFIG
Unknown Service (0000fe45-0000-1000-8000-00805f9b34fb)	Snapchat Inc.'s full 128-bit Bluetooth SIG Universally Unique Identifier (UUID)
RX Characteristic [W WNR] (6e400002-b5a3-f393-e0a9-e50e24dcca9e)	RX Characteristic <ul style="list-style-type: none"> - Write [W] or Write Without Response [WNR] - Write data to the RX Characteristic to send it on to the Universal Asynchronous Receiver/Transmitter (UART) interface. [190]
TX Characteristic [N] (6e400003-b5a3-f393-e0a9-e50e24dcca9e)	TX Characteristic <ul style="list-style-type: none"> - Notify [N]

	<ul style="list-style-type: none"> - Enable notifications for the TX Characteristic to receive data from the application. The application transmits all data that is received over Universal Asynchronous Receiver/Transmitter (UART) as notifications. <p>[190]</p>
gatt.setCharacteristicNotification(00002a05-0000-1000-8000-00805f9b34fb, true)	gatt.setCharacteristicNotification BLE_UUID_GATT_CHARACTERISTIC_SERVICE_CHANGED “Service Changed Characteristic”
gatt.setCharacteristicNotification(6e400003-b5a3-f393-e0a9-e50e24dcca9e, true)	gatt.setCharacteristicNotification Service changed to TX Characteristic

Wireshark’s OUI Lookup Tool was unable to locate Snap Inc.’s OUI “98:A4:0E” (FigureX(c)) from neither nRF Connect EUI-48 results (FigureX(a)) nor nRF Logger EUI-48 results (Figure(b)).

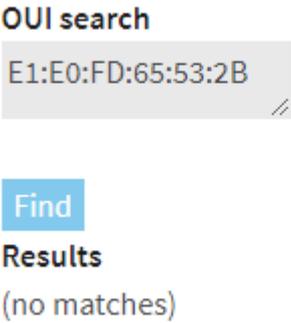
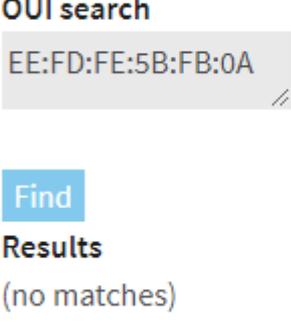
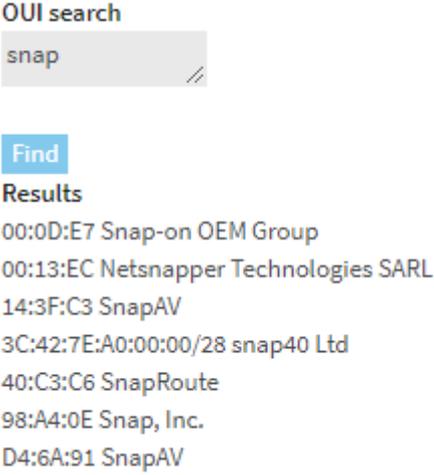
 <p>(a)</p>	 <p>(b)</p>
 <p>(c)</p>	

Figure 20. Forensic exam II: Results from Wireshark’s OUI Lookup Tool for smart eyewear 48-bit EUI-48 BLE address (a)nRF Connect EUI-48 results (b)nRF Connect EUI-48 results (c) Lookup of Snap Inc. OUI

nRF Connect and nRF Logger EUI-48 addresses possess conflicting information regarding the smart eyewear’s Individual/Group and Universal/Local designations, see Table x. The EUI-48 from nRF Connect claims the smart eyewear is a Group address that is Universally administered while EUI-48 results from nRF Logger claim the smart eyewear is an Individual address which is Locally administered.

Table 16. Forensic exam II: 48-bit Extended Unique Identifiers (EUI-48) for smart eyewear [166].

EUI-48 specifics	EUI-48 address from nRF Connect application interface	EUI-48 address from nRF Logger log file
Spectacles version 2 smart eyewear EUI-48 addresses	E1:E0:FD:65:53:2B	EE:FD:FE:5B:FB:0A
First octet (Octet 0) of hexadecimal BLE EUI-48 address	x1 :xx:xx:xx:xx:xx	xE :xx:xx:xx:xx:xx
Least-significant bit of binary address: Individual address (I/G bit = 0) (Unicast) Group address (I/G bit = 1) (Multicast/Broadcast)	00000001 xxxxxxx1	00001110 xxxxxxx0
Second-least-significant bit of binary address: Universal administration of the address (U/L bit = 0) (Factory default) Local administration of the address (U/L bit = 1) (NOT factory default)	00000001 xxxxxxx0x	00001110 xxxxxxx1x

Neither nRF Connect v4.24.3 [173] nor nRF Logger v1.9.0 [174] were capable of intercepting any BLE communication packets containing photographs or videos between the smart eyewear and paired smartphone.

6.2.3 Forensic exam III: BLE scanning and enumeration with nRF Sniffer

Forensic exam III highlights a scenario wherein an forensic investigator possesses access to a low cost Bluetooth Low Energy sniffing device, open source Bluetooth Low Energy (BLE) scanning and enumerating smartphone applications, and is capable of locating themselves and their monitoring device within the smart eyewear’s BLE network range.

The forensic investigator has not obtained custody of a suspect or witnesses’ smart eyewear nor their paired smartphone. The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table x for further detail.

Table 17. Forensic exam III: Chain of custody, network access, system administration status

Devices	Chain of Custody	Network Access	System Administration Status
Target device: Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	Access to open Bluetooth Low Energy networks	Not Rooted
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	Device not possessed by forensic investigator	Access to open Bluetooth Low Energy networks	Not Rooted

6.2.3.1 Forensic exam III: Methods and tools

Forensic exams I and II failed to acquire any photographs and videos from the smart eyewear ecosystem; however, results from scanning and enumerating the devices and obtained background information enabled the informed selection and purchase of the Nordic Semiconductor nRF52840 Development Kit (PCA10056)[192].

Snapchat Spectacles version 2 smart eyewear contains a Nordic Semiconductor nRF52 Series [193] nRF52832 Bluetooth SoC along with a Qualcomm QCA9377 Wi-Fi/Bluetooth SoC, both of which are Bluetooth version 5.0 dual mode SoCs with backwards compatibility for Bluetooth 4.x (Bluetooth Low Energy/Bluetooth mesh). The Bluetooth SoCs within the smart eyewear also support the 2.4GHz Universal asynchronous receiver/transmitter (UART) interface.

Scanning and enumeration results from Forensic exam II detailed the smart eyewear deploys Bluetooth version “Bluetooth Core 4.1”, uses General Discoverable mode to send Legacy Bluetooth Advertising packets to establish BLE connections between devices, and does not support Bluetooth Classic Radio’s Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR).

Conflicting information was collected from the nRF Connect application interface and log file generated by nRF Logger concerning the smart eyewear either only using BLE or preferring BLE transport for Generic Attribute Profile (GATT) connections. However, since the device does not support BR/EDR, the only option is BLE physical transport for GATT connections to remote dual-mode devices.

The Nordic Semiconductor nRF52840 Development Kit, also within their nRF52 series of System-on-Chip (SoC) devices [193], supports Bluetooth 5.x and 4.x, inclusive of Bluetooth Low Energy [192].

Data acquisition and extraction followed Nordic Semiconductor guidelines for their nRF Sniffer for Bluetooth LE software and the nRF52840 Development Kit (DK) [194], see Figure 11 for hardware configuration and Table 16 for tools utilized.

The nRF52840 Development Kit [192] and Wireshark [164], equipped with nRF Sniffer for Bluetooth LE [248], were utilized to scan and intercept BLE communications between the following target devices: Snapchat Spectacles Version 2 smart eyewear and the paired Samsung Galaxy S10e smartphone, see Table x.

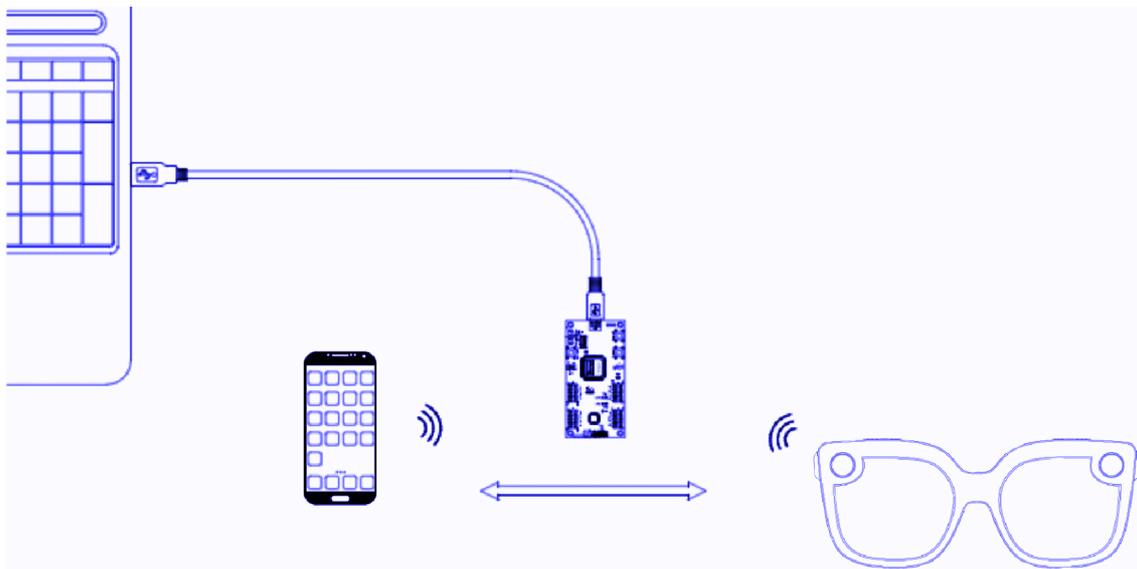


Figure 21. Forensic exam III: Bluetooth Low Energy Extraction hardware configuration [195] [196][161].

While scanning and enumerating for BLE communications, the researcher, as a participant observer, captured simulated photos and videos of individuals with the smart eyewear, paired the smart eyewear and smartphone, and sent the images and videos from the smart eyewear to the paired smartphone.

Table 18. Forensic exam III: nRF52840 and Wireshark: BLE scanning and enumeration tools

Device	Software and peripherals
Target device: Snapchat spectacles Version 2 smart eyewear	- Charging peripherals required for high battery use activities
Target device: Samsung Galaxy S10e smartphone	- Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0 [120]

(BLE paired to smart eyewear)	
Monitoring laptop	<ul style="list-style-type: none"> - Windows 10 Operating system - Wireshark win64 v3.0.10-0 [164] <ul style="list-style-type: none"> - equipped with nRF Sniffer for Bluetooth LE [248] - nRF Connect Bluetooth Low Energy [173] - J-Link Commander v6.80b [246] - Python-3.7.7 (32-bit) [247] - Windows Command Processor
nRF52840 Development Kit (PCA10056) Single board development kit for Bluetooth Low Energy/ Bluetooth 5/Bluetooth mesh/ Thread/Zigbee/802.15.4/ANT/2.4 GHz [192]	<ul style="list-style-type: none"> - USB cable Type A & Micro-B 5 pin connectors to connect the nRF52840 Development Kit to the laptop

6.2.3.2 Forensic exam III: Analysis, results, and discussion

Bluetooth Low Energy Link Layer > Advertising State

The nRF52840 enabled capture of the smart eyewear's bluetooth low energy link layer advertising state packets (ADV_IND and ADV_NONCONN_IND) via Wireshark. The smart eyewear publicly advertises the device's company ID (Snapchat Inc) and device's name (☺ Specs) without any encryption or anonymization. Failure to maintain anonymization of such a unique device within wireless communications presents a privacy concern for the end user, as their device is easily identifiable by anyone, including forensic investigators listening in on their BLE communications and data transfers.

The screenshot shows the Wireshark interface with a packet capture filter: `btcommon.eir_ad.entry.device_name == "\xf0\x9f\x98\x8e Specs"`. Below the filter, a table displays the captured packets:

No.	Company ID	Time	Source	btle.advertising_address
23	Snapchat Inc	2020-04-11 16:22:27.554216000	ee:fd:fe:5b:fb:0a	ee:fd:fe:5b:fb:0a

Destination address	Protocol	bt.le.length	Info	CRC	Device Name	LE General Discoverable Mode	Data
Broadcast	LE LL	30	ADV_IND	OK	Specs	true	f95a9f8347

Figure 22. Forensic exam III:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

btcommon.eir_ad.entry.device_name == "\xf0\x9f\x98\x8e Specs"

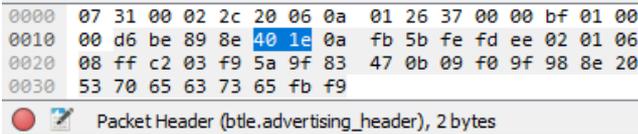
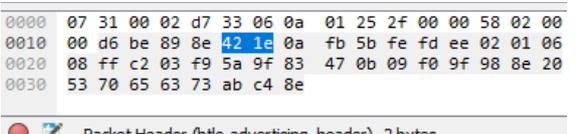
No.	Company ID	Time	Source	bt.le.advertising_address
5058	Snapchat Inc	2020-04-11 16:23:28.234186000	ee:fd:fe:5b:fb:0a	ee:fd:fe:5b:fb:0a

Destination address	Protocol	bt.le.length	Info	CRC	Device Name	LE General Discoverable Mode	Data
Broadcast	LE LL	30	ADV_NONCONN_IND	OK	Specs	true	f95a9f8347

Figure 23. Forensic exam III:

The smart eyewear is utilizing the following legacy advertising protocol data unit types (ADV_IND and ADV_NONCONN_IND) [178].

Table 18. Forensic exam III:

Advertising PDU type and length values utilized by smart eyewear			
ADV_IND		ADV_NONCONN_IND	
			
Figure x.		Figure x.	
Hexadecimal		Hexadecimal	
40	1E	42	1E
Binary		Binary	
0x1e40		0x1e42	
01000000	00011110	01000010	00011110

ADV_IND advertises an undirected, scannable, and connectable indication which does not expect a reply; while ADV_NONCONN_IND advertises an undirected, non-scannable, and non-connectable indication which does not expect a reply.

According to the Bluetooth Core Specifications [178], an advertising payload contains an advertiser’s public or random device address which is transmitted with the least significant octet first followed by the remaining octets in increasing order, see figure x. A bluetooth address is a 48-bit length value which uniquely identifies a device and can be public and/or random, but must at least be one of those types.

Table 19. Forensic exam III:

Advertising Payload	
AdvA: The smart eyewear’s advertised random device address as indicated by TxAdd within the advertising packet header (6 octets)	AdvData: Advertising data from advertising host, if not empty (0-31 octets)


```

Advertising Address: ee:fd:fe:5b:fb:0a (ee:fd:fe:5b:fb:0a)
> Advertising Data
CRC: 0xa6df9f

0000  07 31 00 02 2c 20 06 0a 01 26 37 00 00 bf 01 00  .1., . . &7.....
0010  00 d6 be 89 8e 40 1e 0a fb 5b fe fd ee 02 01 06  .....@. [.....
0020  08 ff c2 03 f9 5a 9f 83 47 0b 09 f0 9f 98 8e 20  .....Z. G.....
0030  53 70 65 63 73 65 fb f9                               Specse..

Advertising Address (bt.le.advertising_address), 6 bytes
  
```

Figure x. Forensic exam III:

The smart eyewear BLE developers enabled bluetooth random addressing, a privacy by design feature. This privacy feature was detected within the BLE pcaps collected, as illustrated in figures x and x, denoted as “Tx Address: Random”. Random BLE addresses do not require registration with IEEE.

Table 20. Forensic exam III:

Smart Eyewear Advertising PDU Type: ADV_IND				
Advertising Type	When	How	Version	Parameter Description
ADV_IND	Advertising	Indication	Legacy	Connectable and Scannable

	device state	w/ No reply expected		undirected advertising events
<pre> > Frame 23: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) > Nordic BLE Sniffer v Bluetooth Low Energy Link Layer Access Address: 0x8e89bed6 v Packet Header: 0x1e40 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random) 0000 = PDU Type: ADV_IND (0x0) ...0 = RFU: 0 ..0. = Channel Selection Algorithm: #1 .1.. = Tx Address: Random 0... = Reserved: False Length: 30 Advertising Address: ee:fd:fe:5b:fb:0a (ee:fd:fe:5b:fb:0a) </pre>				
Figure x. Forensic exam III:				

Table 21. Forensic exam III:

Smart Eyewear Advertising PDU Type: ADV_NONCONN_IND				
Advertising Type	When	How	Version	Parameter Description
ADV_NONCONN_IND	Advertising device state	Indication, w/ No reply expected	Legacy	Non-connectable and Non-scannable undirected advertising events
<pre> > Frame 5058: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) > Nordic BLE Sniffer v Bluetooth Low Energy Link Layer Access Address: 0x8e89bed6 v Packet Header: 0x1e42 (PDU Type: ADV_NONCONN_IND, ChSel: #1, TxAdd: Random) 0010 = PDU Type: ADV_NONCONN_IND (0x2) ...0 = RFU: 0 ..0. = Channel Selection Algorithm: #1 .1.. = Tx Address: Random 0... = Reserved: False Length: 30 Advertising Address: ee:fd:fe:5b:fb:0a (ee:fd:fe:5b:fb:0a) </pre>				
Figure x. Forensic exam III:				

Since the smart eyewear possesses a random BLE advertising address, it has a static address and may have a private address. If private, it is either resolvable or non-resolvable.

According to the Bluetooth Core Specifications [178], the smart eyewear's random static address can be changed to a new value upon a hard reset of the device, thus providing the end user with more options to inhibit tracking of their device [203].

To verify BLE fresh address generation, the smart eyewear's BLE hard reset feature was initiated, the device's random static address changed, and connectivity to its old address was lost within the smartphone, as illustrated when comparing the following BLE pcap (figure x) to a BLE pcap taken prior to a hard reset of the device (figure x) :

No.	Time	Source	btle.advertising_address
1	2020-07-29 18:19:41.284180000	d0:70:fe:a6:32:5e	d0:70:fe:a6:32:5e

Destination address	Protocol	btle.length	Info	CRC	Device Name	LE General Discoverable Mode	Data
Broadcast	LE LL	30	ADV_IND	OK	👤 Specs	true	f95a9f8347

Figure 24. Forensic exam III:

While the device developers enabled random BLE addressing for the device to deter device tracking, the device can still be tracked by the obvious device name and company id values sent publicly via BLE Broadcast, without encryption, during the advertising state.

A BLE pcap between the communications of the smart eyewear and the smartphone during and after advertising, scanning, and connection states illustrated the smart eyewear fails to utilize the BLE Link Layer privacy feature of private addressing.

No.	Time	initiator_address	Source
1306	2020-04-11 14:11:24.536	5e:9b:7f:e8:46:73	5e:9b:7f:e8:46:73

btle.advertising_address	Destination	PHY	Protocol	Info
ee:fd:fe:5b:fb:0a	ee:fd:fe:5b:fb:0a	LE 1M	LE LL	CONNECT_REQ

Nordic BLE Sniffer

Board: 7

▼ Header Version: 2, Packet counter: 6766

Length of payload: 53

Protocol version: 2

Packet counter: 6766

Packet ID: 6

Length of packet: 10

▼ Flags: 0x01

.... .01 = CRC: OK

.... ..0. = Direction: Slave -> Master

.... .0.. = Encrypted: No

.... 0... = MIC: Only relevant when encrypted

.000 = PHY: LE 1M (0)

0... = RFU: 0

Channel: 37

RSSI (dBm): -23

Event counter: 0

Delta time (μ s end to start): 150

[Delta time (μ s start to start): 470]

Bluetooth Low Energy Link Layer

Access Address: 0x8e89bed6

▼ Packet Header: 0x22c5 (PDU Type: CONNECT_REQ, ChSel: #1, TxAdd: Random, RxAdd: Random)

.... 0101 = PDU Type: CONNECT_REQ (0x5)

...0 = RFU: 0

..0. = Channel Selection Algorithm: #1

.1.. = Tx Address: Random

1... = Rx Address: Random

Length: 34

Initiator Address: 5e:9b:7f:e8:46:73 (5e:9b:7f:e8:46:73)

Advertising Address: ee:fd:fe:5b:fb:0a (ee:fd:fe:5b:fb:0a)

▼ Link Layer Data

Access Address: 0x50656550

CRC Init: 0xde07d4

Window Size: 3 (3.75 msec)

Window Offset: 2 (2.5 msec)

Interval: 39 (48.75 msec)

Latency: 0

Timeout: 500 (5000 msec)

▼ Channel Map: ff07c0ff1f

```

.... .1. = RF Channel 1 (2404 MHz - Data - 0): True
.... ..1. = RF Channel 2 (2406 MHz - Data - 1): True
.... .1.. = RF Channel 3 (2408 MHz - Data - 2): True
.... 1... = RF Channel 4 (2410 MHz - Data - 3): True
...1 .... = RF Channel 5 (2412 MHz - Data - 4): True
..1. .... = RF Channel 6 (2414 MHz - Data - 5): True
.1.. .... = RF Channel 7 (2416 MHz - Data - 6): True
1... .... = RF Channel 8 (2418 MHz - Data - 7): True
.... ...1 = RF Channel 9 (2420 MHz - Data - 8): True
.... ..1. = RF Channel 10 (2422 MHz - Data - 9): True
.... .1.. = RF Channel 11 (2424 MHz - Data - 10): True
.... 0... = RF Channel 13 (2428 MHz - Data - 11): False
...0 .... = RF Channel 14 (2430 MHz - Data - 12): False
..0. .... = RF Channel 15 (2432 MHz - Data - 13): False
.0.. .... = RF Channel 16 (2434 MHz - Data - 14): False
0... .... = RF Channel 17 (2436 MHz - Data - 15): False
.... ...0 = RF Channel 18 (2438 MHz - Data - 16): False
.... ..0. = RF Channel 19 (2440 MHz - Data - 17): False
.... .0.. = RF Channel 20 (2442 MHz - Data - 18): False
.... 0... = RF Channel 21 (2444 MHz - Data - 19): False
...0 .... = RF Channel 22 (2446 MHz - Data - 20): False
..0. .... = RF Channel 23 (2448 MHz - Data - 21): False
.1.. .... = RF Channel 24 (2450 MHz - Data - 22): True
1... .... = RF Channel 25 (2452 MHz - Data - 23): True
.... ...1 = RF Channel 26 (2454 MHz - Data - 24): True
.... ..1. = RF Channel 27 (2456 MHz - Data - 25): True
.... .1.. = RF Channel 28 (2458 MHz - Data - 26): True
.... 1... = RF Channel 29 (2460 MHz - Data - 27): True
...1 .... = RF Channel 30 (2462 MHz - Data - 28): True
..1. .... = RF Channel 31 (2464 MHz - Data - 29): True
.1.. .... = RF Channel 32 (2466 MHz - Data - 30): True

```

```

0000 07 35 00 02 6e 1a 06 0a 01 25 17 00 00 96 00 00  .5..n...-%.....
0010 00 d6 be 89 8e c5 22 73 46 e8 7f 9b 5e 0a fb 5b  .....s F...^...[
0020 fe fd ee 50 65 65 50 d4 07 de 03 02 00 27 00 00  ...PeeP...'....'
0030 00 f4 01 ff 07 c0 ff 1f 27 df ed a0  .....'.

```

Packet Header (btle.advertising_header), 2 bytes

Figure 25. Forensic exam III:

After the smartphone initiated a connection request, CONNECT_REQ, with the smart eyewear, the smartphone sent a LL_FEATURE_REQ PDU while acting as the Master device within the connection, see figure x.

No.	Time	Source	Destination address
1346	2020-04-11 14:11:25.377458000	Master_0x50656550	Slave_0x50656550
1347	2020-04-11 14:11:25.380456000	Slave_0x50656550	Master_0x50656550
1348	2020-04-11 14:11:25.392449000	Master_0x50656550	Slave_0x50656550
1349	2020-04-11 14:11:25.394447000	Slave_0x50656550	Master_0x50656550

btle.master_bd_addr	btle.slave_bd_addr	Protocol	Info	CRC
5e:9b:7f:e8:46:73	ee:fd:fe:5b:fb:0a	LE LL	Control Opcode: LL_FEATURE_REQ	OK
5e:9b:7f:e8:46:73	ee:fd:fe:5b:fb:0a	ATT	Rcvd Read By Type Response, Attrib...	OK
5e:9b:7f:e8:46:73	ee:fd:fe:5b:fb:0a	ATT	Sent Read By Type Request, GATT Ch...	OK
5e:9b:7f:e8:46:73	ee:fd:fe:5b:fb:0a	LE LL	Control Opcode: LL_FEATURE_RSP	OK

Figure 26. Forensic exam III:

The smart eyewear responded with the LL_FEATURE_RSP PDU (figure x and figure x) which demonstrated the smart eyewear, acting as the Slave device after the BLE Link Layer connection event, fails to possess “LL Privacy” as demonstrated by the “False” marker.

The Bluetooth Core Specification states the BLE Link Layer provides privacy by using private addresses [178]; however, private addresses implemented by default are at the discretion and implementation of the BLE device developers, not the end users.

No.	Time	Source	Destination address
1349	2020-04-11 14:11:25.394447000	Slave_0x50656550	Master_0x50656550
<ul style="list-style-type: none"> > Frame 1349: 35 bytes on wire (280 bits), 35 bytes captured (280 bits) > Nordic BLE Sniffer ▼ Bluetooth Low Energy Link Layer <ul style="list-style-type: none"> Access Address: 0x50656550 [Master Address: 5e:9b:7f:e8:46:73 (5e:9b:7f:e8:46:73)] [Slave Address: ee:fd:fe:5b:fb:0a (ee:fd:fe:5b:fb:0a)] > Data Header: 0x090b Control Opcode: LL_FEATURE_RSP (0x09) ▼ Feature Set: 0x0000000000000021 <ul style="list-style-type: none">1 = LE Encryption: True0. = Connection Parameters Request Procedure: False0.. = Extended Reject Indication: False 0... = Slave Initiated Features Exchange: False ...0 = LE Ping: False ..1. = LE Data Packet Length Extension: True .0.. = LL Privacy: False 0... = Extended Scanner Filter Policies: False0 = LE 2M PHY: False0. = Stable Modulation Index - Transmitter: False0.. = Stable Modulation Index - Receiver: False 0... = LE Coded PHY: False ...0 = LE Extended Advertising: False ..0. = LE Periodic Advertising: False .0.. = Channel Selection Algorithm #2: False 0... = LE Power Class 1: False0 = Minimum Number of Used Channels Procedure: False 0000 000. = Reserved: 0 Reserved: 0000000000 			

Figure 27. Forensic exam III:

Greater privacy controls are afforded when BLE device developers deploy private addressing by default.

Bluetooth Low Energy Link Layer > Connection State

The smart eyewear’s LL_FEATURE_RSP PDU (figure x) also provided details that the device possesses “LE Encryption”.

According to the Bluetooth Core Specifications, BLE Link Layer Hosts can enable packet encryption after entering into the Connection state by exchanging the master (smart phone) and slave (smart eyewear) initialization vectors (IV) and session key diversifiers (SKD) [178]. The master/smartphone’s IVm and SKDm are sent within the LL_ENC_REQ PDU and the slave/smart eyewear’s IVs and SKDs are sent within the LL_ENC_RSP PDU [178].

However, none of the aforementioned encryption request and response PDUs were observed within the actual BLE packets captured by the nRF52840 DK and Wireshark; nevertheless, the intercepted packets contained encrypted data as illustrated within (figures X, X, and X).

No.	Time	Source	Destination address	Protocol	Info
1405	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1406	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1407	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1408	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1409	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1410	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1411	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1414	2020-04-11 14..	Slave_0x50656550	Master_0x50656550	ATT	Rcvd Handle Value Notification, Handle: 0x0012 (Snapchat Inc: Nordic UART Rx)
1416	2020-04-11 14..	Slave_0x50656550	Master_0x50656550	ATT	Rcvd Handle Value Notification, Handle: 0x0012 (Snapchat Inc: Nordic UART Rx)
1417	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1419	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1422	2020-04-11 14..	Slave_0x50656550	Master_0x50656550	ATT	Rcvd Handle Value Notification, Handle: 0x0012 (Snapchat Inc: Nordic UART Rx)
1423	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1425	2020-04-11 14..	Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
1428	2020-04-11 14..	Slave_0x50656550	Master_0x50656550	ATT	Rcvd Handle Value Notification, Handle: 0x0012 (Snapchat Inc: Nordic UART Rx)
1430	2020-04-11 14..	Slave_0x50656550	Master_0x50656550	ATT	Rcvd Handle Value Notification, Handle: 0x0012 (Snapchat Inc: Nordic UART Rx)

Figure 28. Forensic exam III: Encrypted PDU communications sent between smartphone and smart eyewear

```

> Frame 1405: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
> Nordic BLE Sniffer
  Bluetooth Low Energy Link Layer
    Access Address: 0x50656550
    [Master Address: 5e:9b:7f:e8:46:73 (5e:9b:7f:e8:46:73)]
    [Slave Address: ee:fd:fe:5b:fb:0a (ee:fd:fe:5b:fb:0a)]
  > Data Header: 0x130e
    [L2CAP Index: 50]
    CRC: 0x2d4471
  Bluetooth L2CAP Protocol
    Length: 15
    CID: Attribute Protocol (0x0004)
  Bluetooth Attribute Protocol
    Opcode: Write Command (0x52)
      0... .... = Authentication Signature: False
      .1.. .... = Command: True
      ..01 0010 = Method: Write Request (0x12)
    Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
      [Service UUID: Snapchat Inc (0xfe45)]
      [UUID: 6e400002b5a3f393e0a9e50e24dcca9e]
    UART Tx: @Fq\003\026'
0000 07 26 00 02 d1 1a 06 0a 03 05 1a 4f 00 b0 39 00  .&..... ..O..9.
0010 00 50 65 65 50 0e 13 0f 00 04 00 52 10 00 40 c3  .PeeP... ..R..@.
0020 b5 46 e2 71 c7 89 03 de 16 27 b4 22 8e          .F.q.... .'.".
UART Tx (btgatt.nordic.uart_tx), 12 bytes

```

Figure 29. Forensic exam III: Encrypted PDU write request command sent from smartphone/master to smart eyewear/slave

```

> Frame 1416: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Nordic BLE Sniffer
  Bluetooth Low Energy Link Layer
    Access Address: 0x50656550
    [Master Address: 5e:9b:7f:e8:46:73 (5e:9b:7f:e8:46:73)]
    [Slave Address: ee:fd:fe:5b:fb:0a (ee:fd:fe:5b:fb:0a)]
  > Data Header: 0x350a
    [L2CAP Index: 58]
    CRC: 0x3620e6
  Bluetooth L2CAP Protocol
    Length: 49
    CID: Attribute Protocol (0x0004)
  Bluetooth Attribute Protocol
    Opcode: Handle Value Notification (0x1b)
      0... .... = Authentication Signature: False
      .0.. .... = Command: False
      ..01 1011 = Method: Handle Value Notification (0x1b)
    Handle: 0x0012 (Snapchat Inc: Nordic UART Rx)
      [Service UUID: Snapchat Inc (0xfe45)]
      [UUID: 6e400003b5a3f393e0a9e50e24dcca9e]
    UART Rx: ` \020gqj\034X\003}\tzz\005\024

```

0000	07 48 00 02 dc 1a 06 0a 01 02 39 69 00 97 00 00	.H..... .9i....
0010	00 50 65 65 50 0a 35 31 00 04 00 1b 12 00 60 10	.PeeP.51
0020	c7 67 bc 8c 71 ac 6a 1c 58 ce 03 7d b4 09 b0 84	.g.q.j X..}....
0030	cd 7a c6 c4 05 14 00 00 38 d6 44 05 7f cf 15 d9	.z..... 8.D.....
0040	82 05 15 00 ad 9e d7 b3 7f 14 fc 7f 6c 04 67l.g

UART Rx (btgatt.nordic.uart_rx), 46 bytes

Figure 30. Forensic exam III: Encrypted PDU notification sent from smart eyewear/slave to smartphone/master

The LE Encryption enabled by default by the smart eyewear developers provided a privacy enhancing layer of security around the biometric data captured and transmitted by the smart eyewear device. Packet decryption must be performed in order to obtain access to the images and videos containing the biometric dataset.

Ascertained from the scanning were the devices' Bluetooth address and address type, complete or shortened name, and RSSI in addition to the extraction of Bluetooth packets from both devices.

6.2.4 Forensic exam IV: Decrypting Bluetooth Low Energy

Intercepted BLE communications from the smart eyewear to the smartphone were confirmed as encrypted within Forensic exam III; as such, no photographs or videos containing biometric information were capable of being acquired by intercepting and eavesdropping on communications between the two mobile devices.

Scanning, enumeration, and BLE communication interception results from Forensic exams II and III illustrated the devices were utilizing Bluetooth 4.1 and LE Legacy Pairing.

Bluetooth 4.1 and LE Legacy Pairing security options for product and system developers possess greater risks than security options afforded within Bluetooth 4.2 (LE

Secure Connections was introduced in v4.2, which uses Elliptic Curve Diffie Hellman (ECDH) for BLE key generation, a Federal Information Processing Standards (FIPS) compliant algorithm) to 5.x [178] [197][198].

Crackle, an open source Bluetooth Low Energy decryption tool, proven to exploit vulnerabilities within Bluetooth versions 4.0 - 4.1 [199][200], was used in an attempt to decrypt BLE communications sent between the smart eyewear and the paired smartphone.

6.2.4.1 Forensic exam IV: Methods and tools

Forensic Exam III should be conducted prior to Forensic exam IV to obtain Wireshark BLE packet capture (pcap) files between the smart eyewear and smartphone.

Scenario conditions within Forensic exam IV (chain of custody, network access, system administration status, tools, and methods) parallel Forensic exam III, as prior BLE pcap generation is required in order to decrypt communications.

Kali GNU/ Linux Rolling v2020.3 was installed on Oracle VM Virtualbox, a virtual computer, in order to test Crackle, see Table 21 for tools used.

Table 22. Forensic exam IV: Bluetooth Low Energy decryption tools.

Device	Software, peripherals, pcap files
Host laptop	<ul style="list-style-type: none"> - Wireshark v3.2.5 [164] - Windows 10 operating system - Oracle VM Virtualbox
Virtual computer Oracle VM Virtualbox	<ul style="list-style-type: none"> - Kali GNU/ Linux Rolling v2020.3 [201] - Crackle (Original) [200] - Crackle (with added support for Nordic's nRF52840 DK) [202] - Bluetooth Low Energy Extracted PCAP files from Forensic exam III

6.2.4.2 Forensic exam IV: Analysis, results, and discussion

Initial testing of BLE pcap files proved Crackle, as developed by Mike Ryan, was not capable of analyzing pcap files generated utilizing the Nordic nRF52840 DK to intercept BLE communications, see Figure X.

```
# crackle -i './Downloads/Wireshark_BLE.pcap'
Warning: No output file specified. Decrypted packets will be lost to
the ether.

Frames inside PCAP file not supported ! dlt_name=(NORDIC_BLE)
Frames format supported:
 [256] BLUETOOTH_LE_LL_WITH_PHDR
 [192] PPI
```

Figure 31. Forensic exam IV: Incompatible BLE frame format produced from nRF52840 DK

The crackle.c file required updates to include various parameters to provide support for the Nordic nRF52840 DK. Gerhard Klostermeier's (known as ikarus23 on Github) Crackle updates [202] were used to assist in analyzing pcaps generated by the Nordic Semiconductor nRF52840 DK.

After updating the crackle.c file, captured BLE pcap files from Forensic exam III were loaded into Crackle with the following decryption input command, see Figure X.

```
crackle -i [path-to-new-file.pcap]
```

Figure 32. Forensic exam IV: Crackle decryption input command

BLE communications captured and tested within Crackle failed to contain the initial pairing's Long Term Key required to decrypt the data between the smart eyewear and smartphone.

Numerous attempts were made to capture BLE communications prior to the initial pairing between smart eyewear and smartphone, however, all attempts to decrypt the transferred data were unsuccessful.

The initial pairing point occurs after unpairing the smart eyewear from the smartphone (Figure x.) and the "Name your Spectacles" input screen is triggered (Figure x (b)) between the "Connecting..."(Figure x (a)) and "Pairing Successful!"(Figure x (c)) screens.

The "Name your Spectacles" splash screen (Figure x (b)) does not always pop-up after unpairing and re-pairing, meaning that an initial pairing may or may not be triggered and the smart eyewear may have to be hard reset [203] in order to achieve this course of action.

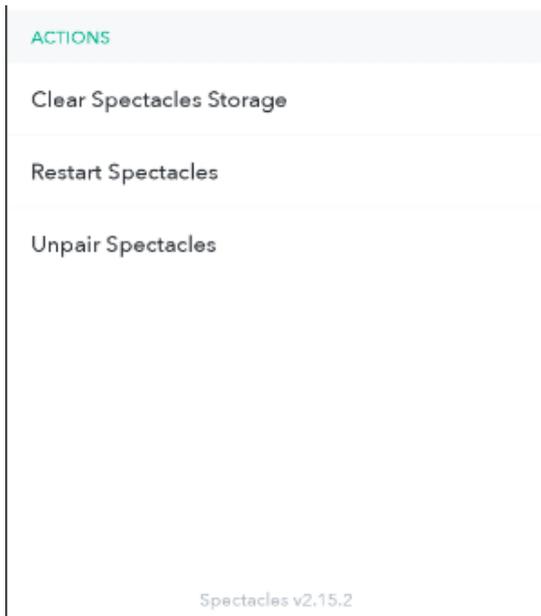


Figure 33. Forensic exam IV: “Unpair Spectacles”

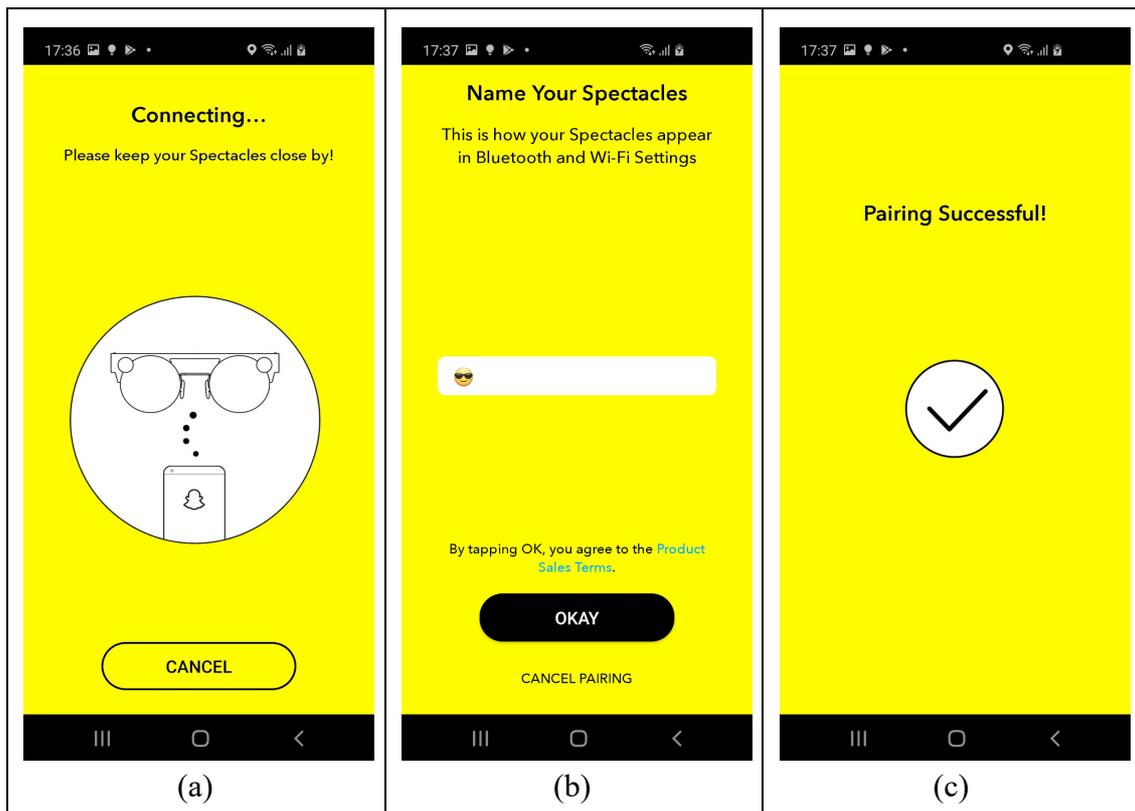


Figure 34. Forensic exam IV: Snapchat Spectacles version 2 smart eyewear initial pairing requires naming

Wireshark’s pcap confirmed the initial pairing point (Figure X(a)(b)) when the devices are no longer referred to by their EUI-48 addresses but rather as slave and master.

Title:	Protocol	Type:	Protocol	Fields:	Enter a field ...	Occurrence:	OK	Can
No.	Time	Device Name	Source	Destination address	Protocol	Info	UART Tx	UART Rx
1301	2020-04-11 14:11:24.513203000		5e:9b:7f:e8:46:73	ee:fd:fe:5b:f0:0a	LE LL	SCAN_REQ		
1302	2020-04-11 14:11:24.514203000		ee:fd:fe:5b:f0:0a	Broadcast	LE LL	SCAN_RSP		
1303	2020-04-11 14:11:24.515202000	Specs	ee:fd:fe:5b:f0:0a	Broadcast	LE LL	ADV_IND		
1304	2020-04-11 14:11:24.516201000	Specs	ee:fd:fe:5b:f0:0a	Broadcast	LE LL	ADV_IND		
1305	2020-04-11 14:11:24.534450000	Specs	ee:fd:fe:5b:f0:0a	Broadcast	LE LL	ADV_IND		
1306	2020-04-11 14:11:24.536452000		5e:9b:7f:e8:46:73	ee:fd:fe:5b:f0:0a	LE LL	CONNECT_REQ		
1307	2020-04-11 14:11:24.540448000		Master_0x50656550	Slave_0x50656550	LE LL	Control Opcode: LL_VERSION_IND		
1308	2020-04-11 14:11:24.541445000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Exchange MTU Request, Client Rx MTU: 64		
1309	2020-04-11 14:11:24.590425000		Master_0x50656550	Slave_0x50656550	ATT	Sent Exchange MTU Response, Server Rx MTU: 64		
1310	2020-04-11 14:11:24.592430000		Slave_0x50656550	Master_0x50656550	LE LL	Control Opcode: LL_VERSION_IND		
1311	2020-04-11 14:11:24.594428000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Group Type Request, GATT Primary Service Declara...		
1312	2020-04-11 14:11:24.640691000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Group Type Request, GATT Primary Service Declara...		
1314	2020-04-11 14:11:24.687662000		Master_0x50656550	Slave_0x50656550	LE LL	Control Opcode: LL_CONNECTION_UPDATE_REQ		
1315	2020-04-11 14:11:24.689661000		Slave_0x50656550	Master_0x50656550	LE LL	Control Opcode: LL_LENGTH_REQ		
1316	2020-04-11 14:11:24.7365632000		Master_0x50656550	Slave_0x50656550	LE LL	Control Opcode: LL_LENGTH_RSP		
1317	2020-04-11 14:11:24.737631000		Slave_0x50656550	Master_0x50656550	L2CAP	Connection Parameter Update Request		
1320	2020-04-11 14:11:24.785601000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Read By Group Type Response, Attribute List Length: 3, G...		
1321	2020-04-11 14:11:24.786601000		Master_0x50656550	Slave_0x50656550	L2CAP	Connection Parameter Update Response (Accepted)		
1322	2020-04-11 14:11:24.832573000		Master_0x50656550	Slave_0x50656550	L2CAP	Connection Parameter Update Response (Accepted)		
1324	2020-04-11 14:11:24.834571000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Include Declaration, Handles:...		
1327	2020-04-11 14:11:24.882541000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Error Response - Attribute Not Found, Handle: 0x0001 (Ge...		
1328	2020-04-11 14:11:24.930512000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Characteristic Declaration, H...		
1331	2020-04-11 14:11:24.982624000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Read By Type Response, Attribute List Length: 4, Device ...		
1332	2020-04-11 14:11:25.027994000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Characteristic Declaration, H...		
1335	2020-04-11 14:11:25.079067000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Error Response - Attribute Not Found, Handle: 0x0009 (Ge...		
1336	2020-04-11 14:11:25.126296000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Include Declaration, Handles:...		
1339	2020-04-11 14:11:25.177351000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Error Response - Attribute Not Found, Handle: 0x000a (Ge...		

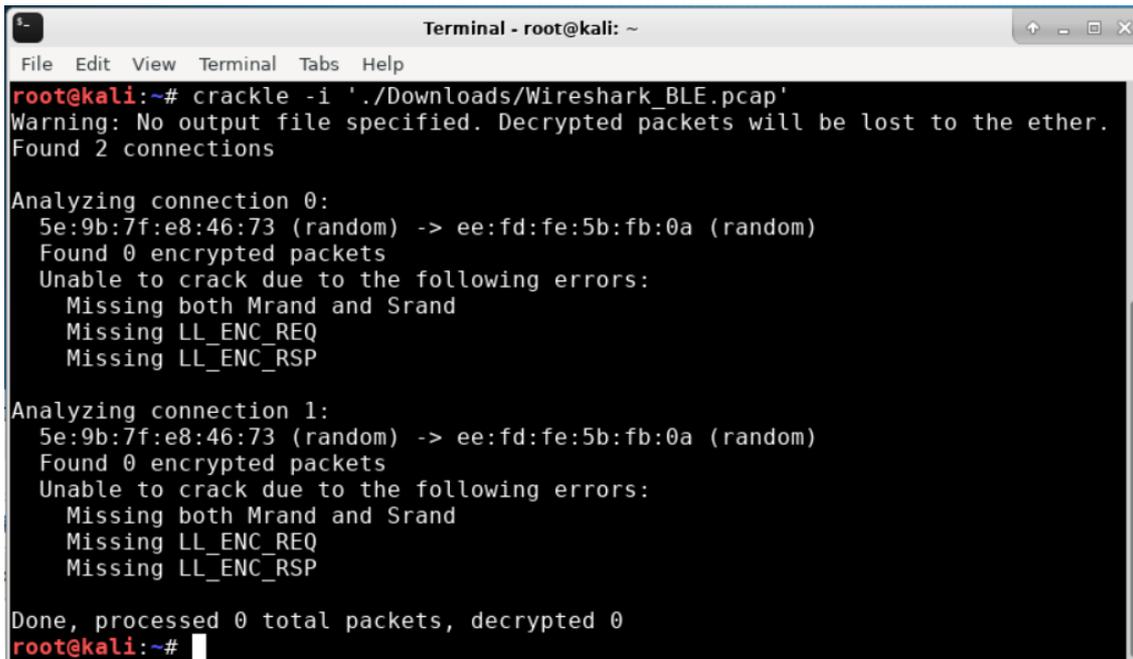
(a)

No.	Time	Device Name	Source	Destination address	Protocol	Info	UART Tx	UART Rx
1340	2020-04-11 14:11:25.223574000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Characteristic Declaration, H...		
1346	2020-04-11 14:11:25.377458000		Master_0x50656550	Slave_0x50656550	LE LL	Control Opcode: LL_FEATURE_REQ		
1347	2020-04-11 14:11:25.380456000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Read By Type Response, Attribute List Length: 1, Service...		
1348	2020-04-11 14:11:25.392449000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Characteristic Declaration, H...		
1349	2020-04-11 14:11:25.394447000		Slave_0x50656550	Master_0x50656550	LE LL	Control Opcode: LL_FEATURE_RSP		
1352	2020-04-11 14:11:25.424478000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Error Response - Attribute Not Found, Handle: 0x000c (Ge...		
1353	2020-04-11 14:11:25.437473000		Master_0x50656550	Slave_0x50656550	ATT	Sent Find Information Request, Handles: 0x000d..0x000d		
1356	2020-04-11 14:11:25.454459000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Find Information Response, Handle: 0x000d (Generic Attri...		
1357	2020-04-11 14:11:25.467450000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Include Declaration, Handles:...		
1360	2020-04-11 14:11:25.484447000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Error Response - Attribute Not Found, Handle: 0x000e (Sn...		
1361	2020-04-11 14:11:25.496432000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Characteristic Declaration, H...		
1364	2020-04-11 14:11:25.512422000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Read By Type Response, Attribute List Length: 2, Nordic ...		
1365	2020-04-11 14:11:25.526432000		Master_0x50656550	Slave_0x50656550	ATT	Sent Read By Type Request, GATT Characteristic Declaration, H...		
1368	2020-04-11 14:11:25.542525000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Error Response - Attribute Not Found, Handle: 0x0012 (Sn...		
1369	2020-04-11 14:11:25.557517000		Master_0x50656550	Slave_0x50656550	ATT	Sent Find Information Request, Handles: 0x0013..0xffff		
1372	2020-04-11 14:11:25.574506000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Find Information Response, Handle: 0x0013 (Snapchat Inc:...		
1373	2020-04-11 14:11:25.586498000		Master_0x50656550	Slave_0x50656550	ATT	Sent Find Information Request, Handles: 0x0014..0xffff		
1376	2020-04-11 14:11:25.602504000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Error Response - Attribute Not Found, Handle: 0x0014 (Sn...		
1377	2020-04-11 14:11:25.616540000		Master_0x50656550	Slave_0x50656550	LE LL	Control Opcode: LL_CONNECTION_UPDATE_REQ		
1379	2020-04-11 14:11:25.631531000		Master_0x50656550	Slave_0x50656550	ATT	Sent Write Request, Handle: 0x0013 (Snapchat Inc: Nordic UART...		
1382	2020-04-11 14:11:25.647540000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Write Response, Handle: 0x0013 (Snapchat Inc: Nordic UAR...		
1385	2020-04-11 14:11:25.663573000		Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART... \001\025		
1387	2020-04-11 14:11:25.676615000		Slave_0x50656550	Master_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART... \036\033.)		
1390	2020-04-11 14:11:25.692691000		Slave_0x50656550	Master_0x50656550	ATT	Rcvd Handle Value Notification, Handle: 0x0012 (Snapchat Inc:...		\001\026
1391	2020-04-11 14:11:25.709015000		Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART... \005\034		
1393	2020-04-11 14:11:25.724014000		Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART... @@@F@@@		
1394	2020-04-11 14:11:25.739068000		Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART... @@@F@@@		
1395	2020-04-11 14:11:25.754288000		Master_0x50656550	Slave_0x50656550	ATT	Sent Write Command, Handle: 0x0010 (Snapchat Inc: Nordic UART... @@@F@@@		

(b)

Figure 35. Forensic exam IV: Wireshark pcap of BLE smart eyewear pairing to smartphone (a) Frames 1301-1339 (b) Frames 1340-1395

However, even after determining the initial pairing point and numerous attempts at unpairing and re-pairing the two devices, capturing simulated photographs and videos of individuals with the smart eyewear, and transferring them to the smartphone thereafter failed to generate the following LE Link Layer values required by Crackle to decrypt the payloads: Mrand; Srand; LL_ENC_REQ; LL_ENC_RSP (Figure X).



```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# crackle -i './Downloads/Wireshark_BLE.pcap'
Warning: No output file specified. Decrypted packets will be lost to the ether.
Found 2 connections

Analyzing connection 0:
5e:9b:7f:e8:46:73 (random) -> ee:fd:fe:5b:fb:0a (random)
Found 0 encrypted packets
Unable to crack due to the following errors:
  Missing both Mrand and Srand
  Missing LL_ENC_REQ
  Missing LL_ENC_RSP

Analyzing connection 1:
5e:9b:7f:e8:46:73 (random) -> ee:fd:fe:5b:fb:0a (random)
Found 0 encrypted packets
Unable to crack due to the following errors:
  Missing both Mrand and Srand
  Missing LL_ENC_REQ
  Missing LL_ENC_RSP

Done, processed 0 total packets, decrypted 0
root@kali:~#
```

Figure 36. Forensic exam IV: Attempted BLE packet decryption with Crackle on Kali Linux virtual system

Crackle's failure to decrypt data payloads transferred between the smart eyewear and smartphone results from either:

- Encryption occurring outside the Bluetooth LE Link Layer
- Device pairing is using a custom algorithm, specific to the smartwear device/application

6.2.5 Forensic exam V: HCI BTSnoop logs

Forensic Exam IV provided inconclusive results regarding the smart eyewear's Bluetooth encryption; however, the study did inform that HCI Snoop logs contain data before it is encrypted by the BLE Link Layer [204].

If the BT HCI Snoop log details the data payload is encrypted, it can be deduced the smart eyewear developers have not encrypted their communications within the BLE Link Layer.

Forensic exam V highlights a case wherein an investigator briefly gains access to the target smartphone (paired to the smart eyewear) to enable Bluetooth log generation unbeknownst to the device owner.

After an allotted time range has passed to collect sufficient evidence, the investigator, once again, briefly obtains the device to retrieve the generated Bluetooth log file.

The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table x for further detail.

Table 23. Forensic exam V: Chain of custody, network access, system administration status

Devices	Chain of Custody	Network Access	System Administration Status
Target device: Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	No access to device's used networks	Not Rooted
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	Briefly obtained by forensic investigator on two occasions: First, to enable Bluetooth log file capturing and generation. Second, to collect the Bluetooth log file.	No access to device's used networks	Not Rooted

6.2.5.1 Forensic exam V: Methods and tools

The researcher, acting as participant observer, performed the following actions:

As forensic investigator:

Enabled the target smartphone's "Developer Options" and "Bluetooth Host Controller Interface (BT HCI) Snoop log" were enabled [205].

As smart eyewear owner:

Captured simulated photos and videos of individuals with the smart eyewear, paired the smart eyewear and smartphone, and sent the images and videos from the smart eyewear to the paired smartphone.

As forensic investigator:

Extracted a BT HCI Snoop log from the target smartphone's Bugreport via Android Debug Bridge (ADB). Connected the laptop and smartphone with the USB connection cable, the following commands were entered within cmd.exe:

```
>adb devices
List of devices attached
RF8N11P3CGH    device

>adb bugreport "[filepath]"
```

Figure 37. Forensic exam V: ADB Bugreport generation to extract Bluetooth HCI Snoop Log from smart eyewear's paired smartphone

Wireshark was then used to open, view, and analyze the generated BT HCI Snoop log.

See Table 24 for extraction tools and Figure x for commands used.

Table 24. Forensic exam V: Bluetooth HCI Snoop Log Extraction tools.

Device	Software and peripherals
Target device: Samsung Galaxy S10e smartphone (BLE paired to smart eyewear)	<ul style="list-style-type: none"> - Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0 [120]
Laptop	<ul style="list-style-type: none"> - Windows 10 Operating system - Windows Command Processor (cmd.exe) - Android Debug Bridge (ADB)[206] - Wireshark v3.2.5 [164] - USB cable Type A & Micro-B 5 pin connectors to connect target smartphone to the laptop

6.2.5.2 Forensic exam V: Analysis, results, and discussion

After entering the command “adb devices”, ADB encountered device recognition issues when the targeted smartphone was not included within the “List of devices attached” output; however, the following procedure was used to solve the connectivity issue [207].

Bluetooth HCI Snoop Log results clarified that BLE communications between the smart eyewear and smartphone do not permit Bluetooth Security Manager Protocol (SMP) pairing requests since the smart eyewear does not support SMP pairing. (Figure X,X,X)

No.	Source Device Name	Source Device Name	Protocol	Info
563	Galaxy S10e	Galaxy S10e	SMP	Sent Pairing Request: AuthReq: Bonding, MITM, SecureConnection
574	Specs	Specs	SMP	Rcvd Pairing Failed: Pairing Not Supported
581	Galaxy S10e	Galaxy S10e	SMP	Sent Pairing Request: AuthReq: Bonding, MITM, SecureConnection
592	Specs	Specs	SMP	Rcvd Pairing Failed: Pairing Not Supported
599	Galaxy S10e	Galaxy S10e	SMP	Sent Pairing Request: AuthReq: Bonding, MITM, SecureConnection
610	Specs	Specs	SMP	Rcvd Pairing Failed: Pairing Not Supported
649	Galaxy S10e	Galaxy S10e	SMP	Sent Pairing Request: AuthReq: Bonding, MITM, SecureConnection
660	Specs	Specs	SMP	Rcvd Pairing Failed: Pairing Not Supported
1266	Galaxy S10e	Galaxy S10e	SMP	Sent Pairing Request: AuthReq: Bonding, MITM, SecureConnection
1278	Specs	Specs	SMP	Rcvd Pairing Failed: Pairing Not Supported
1341	Galaxy S10e	Galaxy S10e	SMP	Sent Pairing Request: AuthReq: Bonding, MITM, SecureConnection

(a)

```

> Frame 563: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
▼ Bluetooth L2CAP Protocol
  Length: 7
  CID: Security Manager Protocol (0x0006)
▼ Bluetooth Security Manager Protocol
  Opcode: Pairing Request (0x01)
  IO Capability: Keyboard, Display (0x04)
  OOB Data Flags: OOB Auth. Data Not Present (0x00)
  > AuthReq: 0x0d, Secure Connection Flag, MITM Flag, Bonding Flags: Bonding
  Max Encryption Key Size: 16
  ▼ Initiator Key Distribution: 0x0f, Link Key, Signature Key (CSRK), Id Key (IRK), Encryption Key (LTK)
    0000 .... = Reserved: 0x0
    .... 1... = Link Key: True
    .... .1.. = Signature Key (CSRK): True
    .... ..1. = Id Key (IRK): True
    .... ...1 = Encryption Key (LTK): True
  ▼ Responder Key Distribution: 0x0f, Link Key, Signature Key (CSRK), Id Key (IRK), Encryption Key (LTK)
    0000 .... = Reserved: 0x0
    .... 1... = Link Key: True
    .... .1.. = Signature Key (CSRK): True
    .... ..1. = Id Key (IRK): True
    .... ...1 = Encryption Key (LTK): True

```

```

0000 02 40 00 0b 00 07 00 06 00 01 04 00 0d 10 0f 0f  .@.....:....

```

Opcode (bt SMP opcode), 1 byte

(b)

Figure 38. Forensic exam V: Detail of Frame 563, Bluetooth Pairing request sent from Samsung Galaxy S10e to Snapchat Spectacles version 2 smart eyewear (a-b)

Interface	Hop 37,38,39			Help	Defaults	Log
No.	Service UUID	UART Tx	UART Rx			
24172	Snapchat Inc					
24173	Snapchat Inc					
24174	Snapchat Inc					
24175	Snapchat Inc	\0017				
24176	Snapchat Inc	xf:\022 (W6\02_				
24177	Snapchat Inc	6&dR\002` \020y\031+_				
24178						
24179						
24180	Snapchat Inc		\0018			
24181						
24182	Snapchat Inc		s5t\037\022 w\TM\0259			
24183	Snapchat Inc		z\0220.wnK\bxr\			
24184	Snapchat Inc	\001#				
24185	Snapchat Inc	8c'\022\fv\021_				
24186						
24187	Snapchat Inc		\0015\003			
24188	Snapchat Inc		vy\034\022\0069			
24189	Snapchat Inc		SS]F&' \003			

Figure 40. Forensic exam V: Summary of Frame 24176, Nordic UART Tx Write Command sent from Samsung Galaxy S10e to Snapchat Spectacles version 2 smart eyewear (a-b)

```

<
> Frame 24176: 32 bytes on wire (256 bits), 32 bytes captured (256 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth Attribute Protocol
  v Opcode: Write Command (0x52)
    0... .... = Authentication Signature: False
    .1.. .... = Command: True
    ..01 0010 = Method: Write Request (0x12)
  v Handle: 0x0010 (Snapchat Inc: Nordic UART Tx)
    [Service UUID: Snapchat Inc (0xfe45)]
    [UUID: 6e40002b5a3f393e0a9e50e24dcca9e]
    UART Tx: xf:\022 (W6\02_
0000  02 40 00 1b 00 17 00 04 00 52 10 00 81 78 66 3a  .@.....R..xf:
0010  88 12 20 28 f0 57 e0 36 89 fb 9c da de 10 8e 17  ..(W.6.....
UART Tx (btgatt.nordic.uart_tx), 20 bytes

```

Figure 41. Forensic exam V: Detail of Frame 24176, of Nordic UART Tx Write Request Command sent from Samsung Galaxy S10e to Snapchat Spectacles version 2 smart eyewear.

Table 25. Forensic exam V: TX and RX Characteristics

RX Characteristic [W WNR] (6e400002-b5a3-f393-e0a9-e50e24dcca9e)	RX Characteristic <ul style="list-style-type: none"> - Write [W] or Write Without Response [WNR] - Write data to the RX Characteristic to send it on to the UART interface. [190]
TX Characteristic [N] (6e400003-b5a3-f393-e0a9-e50e24dcca9e)	TX Characteristic <ul style="list-style-type: none"> - Notify [N] - Enable notifications for the TX Characteristic to receive data from the application. The application transmits all data that is received over UART as notifications. [190]

6.2.6 Forensic exam VI: Non-Rooted extraction via ADB Pull and ADB Backup

Forensic exam VI highlights a case wherein an investigator has gained access to the smart eyewear owner’s paired smartphone to create copies of select files.

The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table x for further detail.

Table 26. Forensic exam VI: Chain of custody, network access, system administration status

Devices	Chain of Custody	Network Access	System Administration Status
Target device: Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	No access to device’s used networks	Not Rooted
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	Device obtained by forensic investigator	No access to device’s used networks	Not Rooted

6.2.6.1 Forensic exam VI: Methods and tools

The non-rooted data extraction method was performed with Android Debug Bridge (ADB) Pull and Backup.

ADB Backup and ADB Pull are logical extraction methods which copy only available files such as: visible, hidden, and system. These methods do not recover deleted files.

ADB Backup and ADB Pull do not require system administrative privileges; however, such escalated privileges provide availability to personal application data within the /data/data file.

Table 27. Forensic exam VI: Non-Rooted Data Extraction tools.

Device	Software and peripherals
Target device: Samsung Galaxy S10e smartphone (BLE paired to smart eyewear)	<ul style="list-style-type: none">- Android v10.0; One UI v2.0- Snapchat application v10.77.5.0 [120]
Laptop	<ul style="list-style-type: none">- Windows 10 operating system- Windows Command Processor- Android Debug Bridge [206]<ul style="list-style-type: none">- Shell [249]- Pull [250]- Android Backup Extractor v20180521 [208]- 7-Zip File Manager [209]- USB cable Type A & Micro-B 5 pin connectors to connect target smartphone to the laptop

ADB pull was performed by connecting the target smartphone to laptop and entering the following command within cmd.exe :

```
> adb pull -a /data/data/com.snapchat.android "C:\path_to_new_file"
```

Figure 42. Forensic exam VI: ADB Pull

The ADB Backup method used within this scenario was adapted and modified from the following guidelines [210].

Connected target smartphone to laptop and entered the following commands within cmd.exe:

```
>adb backup -apk -shared -all -f "\path_to_file\backup.ab"  
WARNING: adb backup is deprecated and may be removed in a future release  
Now unlock your device and confirm the backup operation...
```

Figure 43. Forensic exam VI: ADB Backup command for non-rooted data extraction [208].

An archive, entitled “backup.ab”, was created of the paired smartphone’s data contained within Android application package (.apk) files, shared storage, all installed apps, and system apps.

Converted the ADB “backup.ab” file to a “backup.tar” file with the following command within cmd.exe (Figures x-x):

```
>java.exe -jar "\path_to_file\abe.jar" unpack "\path_to_file\backup.ab"  
"\path_to_file\backup.tar":\
```

Figure 44. Forensic exam VI: Command for conversion of ADB backup.ab file to backup.tar file.

The paired smartphone’s files were extracted from the backup.tar file with 7-Zip File Manager (7zFM.exe) (Figure X).

Name	Type	Size
backup	File folder	
backup.ab	AB File	680,370 KB
backup.tar	TAR File	813,008 KB

Figure 45. Forensic exam VI: ADB backup.ab, backup.tar, and Z-Zip extracted files from paired target smartphone.

6.2.6.2 Forensic exam VI: Analysis, results, and discussion

ADB pull did not produce any viable data acquisitions from the “/data/data/com.snapchat.android directory” on the non-rooted target device, results output “Permission denied” (Figure x).

```
> adb devices -l  
List of devices attached  
RF8N11P3CGH          device product:beyond0lteeea model:SM_G970F  
device:beyond0 transport_id:3  
  
> adb pull -a /data/data/com.snapchat.android "C:\path_to_new_file"  
adb: error: failed to stat remote object '/data/data/com.snapchat.android':  
Permission denied
```

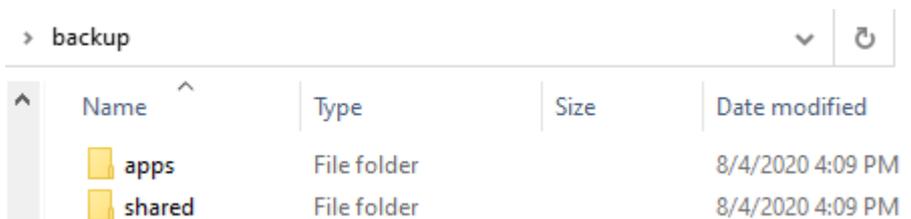
Figure 46. Forensic exam VI: ADB Pull results from targeted non-rooted smartphone.

ADB shell commands were also issued to access and view the directory; however, results were no different from ADB pull command (Figure x).

```
>adb shell
1|beyond0:/data/data $ cd /data/data/com.snapchat.android
/system/bin/sh: cd: /data/data/com.snapchat.android: Permission denied
```

Figure 47. Forensic exam VI: ADB Shell results from targeted non-rooted smartphone.

ADB Backup generated a “backup” file folder containing “apps” and “shared” file directories from the paired smartphone (Figure x).



Name	Type	Size	Date modified
apps	File folder		8/4/2020 4:09 PM
shared	File folder		8/4/2020 4:09 PM

Figure 48. Forensic exam VI: ADB Backup extraction of “apps” and “shared” file directories from the paired smartphone

The “apps” directory did not contain the “com.snapchat.android” application file, and as such, no photographs or videos, previously exported from the smart eyewear, were acquired within the /com.snapchat.android directory.

Photographs and videos containing biometric information, were located within the “shared” directory’s subfolders as illustrated within Figures x-x.

The aforementioned photographs and videos, within the “shared” directory, were previously exported from the smart eyewear to the smartphone’s Snapchat mobile application “Memories” folder, and from that location .jpg and .mp4 files were exported to the smartphone’s internal storage directory: \shared\0\Spectacles (referred to as the “Camera Roll” within com.snapchat.android application) (Figure X).

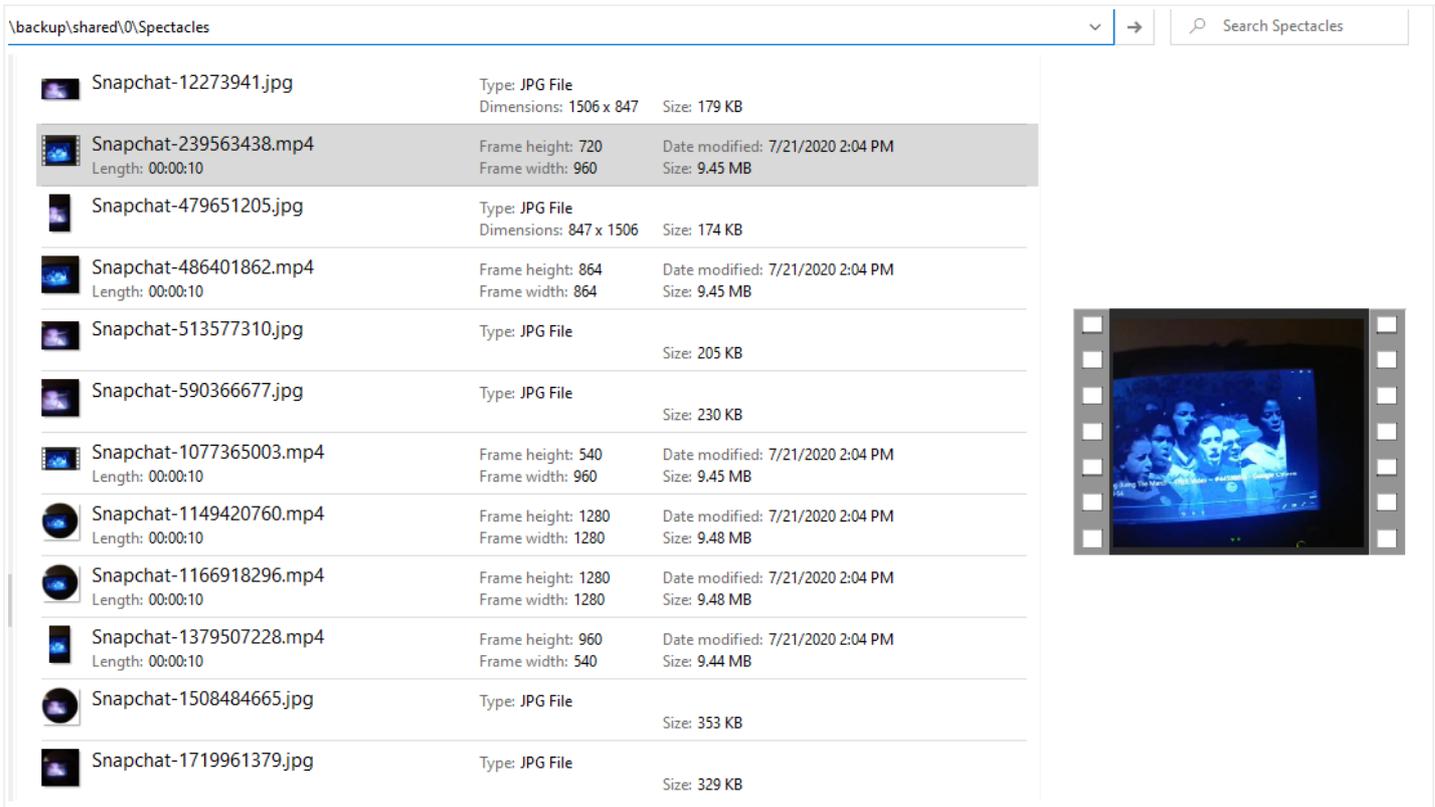


Figure 49. Forensic exam VI: Extracted photographs (.jpg) and videos (.mp4) containing biometric information within `\shared\0\Spectacles` directory

Exportation from “Memories” within `com.snapchat.android`, triggered the system to concurrently auto-create thumbnails for the exported .jpg and .mp4 files, which then stored the photographs and videos within their relative directories Figures x-x.

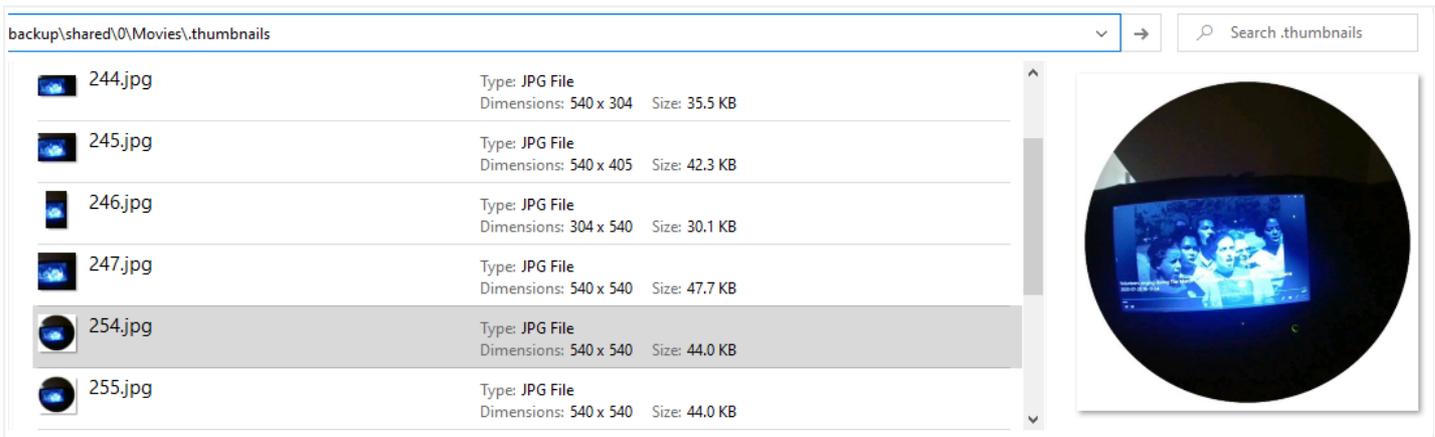


Figure 50. Forensic exam VI: Extracted thumbnails (.jpg), from smart eyewear videos, containing biometric information within `\shared\0\Movies\.thumbnails` directory

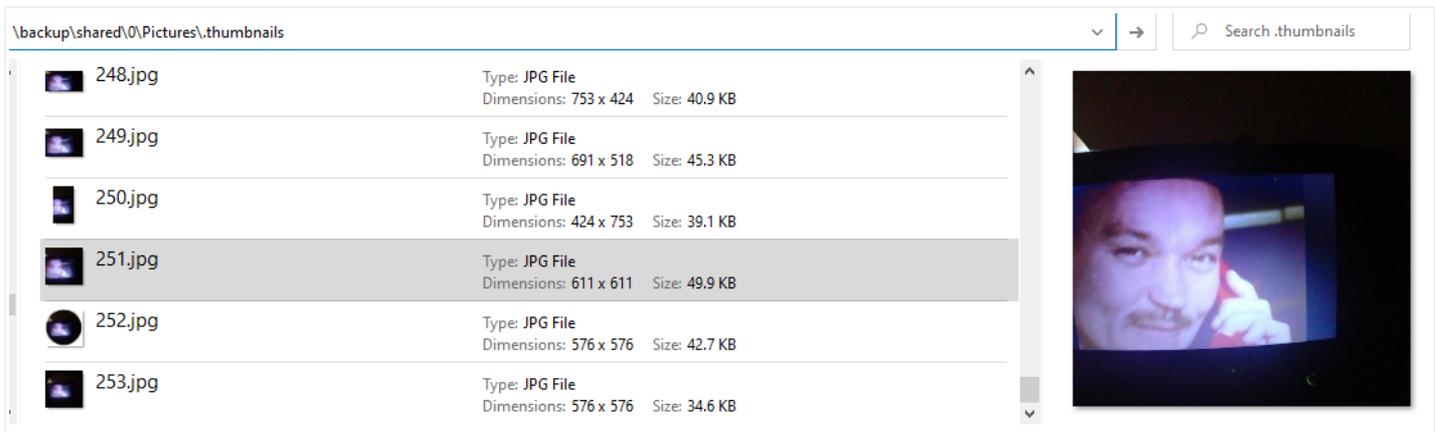


Figure 51. Forensic exam VI: Extracted thumbnails (.jpg), from smart eyewear photographs, containing biometric information within \\shared\0\Pictures\.thumbnails directory

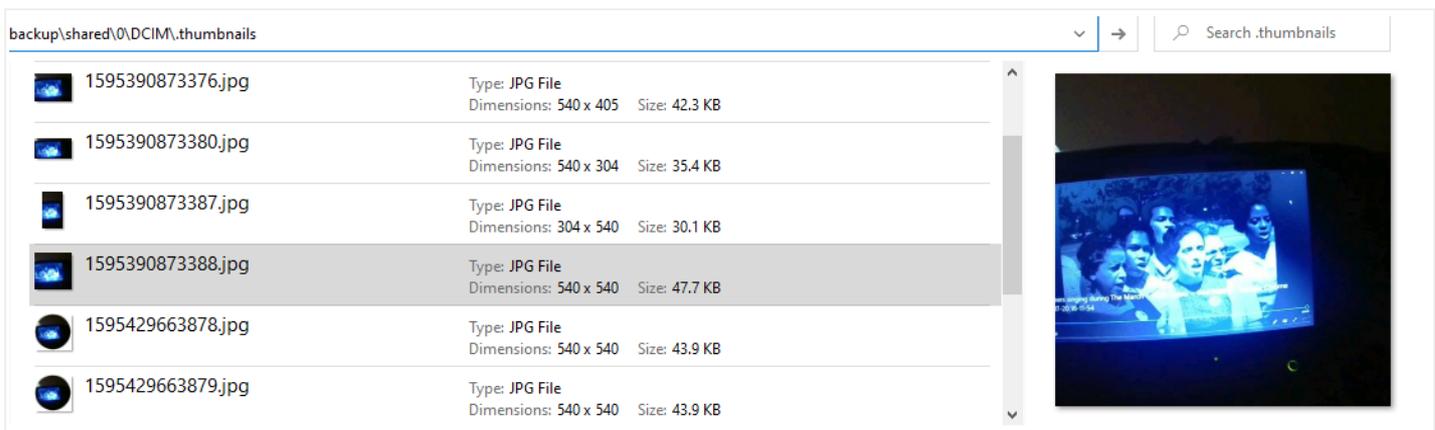


Figure 52. Forensic exam VI: Extracted thumbnails (.jpg), from smart eyewear videos, containing biometric information within \\shared\0\DCIM\.thumbnails directory

30 files containing biometric content were extracted from the /shared/0 directory, 6 being .mp4 video files within the /Spectacles directory, another 6 being .jpg image files within the /Spectacles directory, and 18 .jpg thumbnails divided evenly amongst the /Movies, /Pictures, /DCIM directories.

Forensic exam VI failed to extract and acquire any photographs or videos from the smart eyewear's /data/data directory; nor did it provide any information on the smart eyewear's internal device storage, cloud databases, or memory used to store the photographs and videos on the smart eyewear's paired smartphone.

6.2.7 Forensic exam VII: ADB dumpsys meminfo

Forensic exam VII highlights a case wherein an investigator gains access to the target smart eyewear's paired smartphone to obtain a memory information and database report, ADB Dumpsys meminfo, on the smart eyewear and the smart eyewear's mobile application prior to rooting the device.

The ADB dumpsys meminfo report provides a cross reference information source to aid in validating biometric assets and database files found after obtaining administrative root access to the smart eyewear paired smartphone.

The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table 28 for further detail.

Table 28. Forensic exam VII: Chain of custody, network access, system administration status

Devices	Chain of Custody	Network Access	System Administration Status
Target device: Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	No access to device's used networks	Not Rooted
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	Device obtained by forensic investigator	No access to device's used networks	Not Rooted

6.2.7.1 Forensic exam VII: Methods and tools

The ADB dumpsys meminfo report on the smart eyewear's mobile application, com.snapchat.android, provides information on the smart eyewear and application's memory usage, in addition to database locations, names, sizes, and caches (Figure X).

Target paired smartphone was connected to the laptop and the following command was used with option -d to provide additional information on the smart eyewear mobile application's Android Run Time (ART) and Dalvik memory usage [211].

```
adb shell dumpsys meminfo com.snapchat.android -d
```

Figure 53. ADB shell dumpsys meminfo command.

Table 29. Forensic exam VII: Adb dumpsys meminfo tools.

Device	Software and peripherals
Target device:	- Android v10.0; One UI v2.0

Samsung Galaxy S10e smartphone (BLE paired to smart eyewear)	<ul style="list-style-type: none"> - Snapchat application v10.77.5.0 [120]
Laptop	<ul style="list-style-type: none"> - Windows 10 Operating system - Windows Command Processor - Android Debug Bridge [206] <ul style="list-style-type: none"> - Shell [249] - Dumpsys [211] - Meminfo [212] - USB cable Type A & Micro-B 5 pin connectors to connect target smartphone to the laptop

6.2.7.2 Forensic exam VII: Analysis, results, and discussion

The ADB Dumpsys meminfo report extracted the following database names from the smart eyewear's mobile application:

```
(attached) temp
0a8efa36-be51-e029-0f09-30f0af6d4287_fidelius.db
androidx.work.workdb
cognac
core.db
durable_job
feature
fidelius_database.db
journal.db
main.db
media_packages
memories.db
simple_db_helper.db
SPECTACLES_SQLITE
```

All databases were stored within the following directory:

/data/user/0/com.snapchat.android/databases/

```
Microsoft Windows [Version 10.0.18363.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>adb devices
List of devices attached
RF8N11P3CGH    device

C:\WINDOWS\system32>adb shell dumpsys meminfo com.snapchat.android -d
```

Applications Memory Usage (in Kilobytes):
Uptime: 89859242 Realtime: 1194006404

```
** MEMINFO in pid 25949 [com.snapchat.android] **
      Pss Private Private SwapPss Heap Heap Heap
      Total Dirty Clean Dirty Size Alloc Free
-----
Native Heap 72856 72784 0 17183 101444 90176 11267
Dalvik Heap 20535 20504 0 348 23331 17515 5816
Dalvik Other 4648 4648 0 8
Stack 44 44 0 12
Ashmem 190 172 0 0
Other dev 36 4 28 0
.so mmap 25297 1180 15892 3666
.jar mmap 3457 0 1108 0
.apk mmap 38147 196 36312 0
.ttf mmap 516 0 480 0
.dex mmap 71552 28 71516 16
.oat mmap 837 0 60 0
.art mmap 25891 25336 188 2014
Other mmap 3017 200 2384 0
GL mtrack 18798 18798 0 0
Unknown 4728 4712 0 2952
TOTAL 316748 148606 127968 26199 124775 107691 17083
```

App Summary

```
      Pss (KB)
-----
Java Heap: 46028
Native Heap: 72784
Code: 126772
Stack: 44
Graphics: 18798
Private Other: 12148
System: 40174

TOTAL: 316748 TOTAL SWAP PSS: 26199
```

Objects

```
Views: 229 ViewRootImpl: 2
AppContexts: 13 Activities: 1
Assets: 24 AssetManagers: 0
Local Binders: 82 Proxy Binders: 67
Parcel memory: 60 Parcel count: 205
Death Recipients: 2 OpenSSL Sockets: 0
WebViews: 0
```

SQL

```
MEMORY_USED: 8189
PAGECACHE_OVERFLOW: 844 MALLOC_SIZE: 117
```

DATABASES

```
pgsz dbsz Lookaside (b) cache Dbname
4 60 34 2/38/3
/data/user/0/com.snapchat.android/databases/0a8efa36-be51-e029-0f09-30f0af6d4287_fidelius.db
4 60 48 11/30/3
/data/user/0/com.snapchat.android/databases/0a8efa36-be51-e029-0f09-30f0af6d4287_fidelius.db (1)
4 176 19 0/130/1
/data/user/0/com.snapchat.android/databases/simple_db_helper.db
4 1016 69 1576/298/25
/data/user/0/com.snapchat.android/databases/main.db
4 1016 109 655/3336/12
/data/user/0/com.snapchat.android/databases/main.db (3)
4 1016 91 3676/633/25
/data/user/0/com.snapchat.android/databases/main.db (1)
4 1016 105 3980/480/25
/data/user/0/com.snapchat.android/databases/main.db (2)
4 60 28 2/40/3
/data/user/0/com.snapchat.android/databases/fidelius_database.db
4 60 18 1/28/1
/data/user/0/com.snapchat.android/databases/fidelius_database.db (1)
4 3280 102 12442/4722/25
/data/user/0/com.snapchat.android/databases/memories.db
4 3280 48 601/16191/1
/data/user/0/com.snapchat.android/databases/memories.db (3)
4 3280 109 19649/3319/25
/data/user/0/com.snapchat.android/databases/memories.db (1)
4 3280 109 20932/2623/25
/data/user/0/com.snapchat.android/databases/memories.db (2)
4 244 22 28/93/2
```

```

/data/user/0/com.snapchat.android/databases/feature
4      244      25      136/28/1
/data/user/0/com.snapchat.android/databases/feature (1)
4      244      25      59/25/1
/data/user/0/com.snapchat.android/databases/feature (2)
4      640      66      1177/1661/6
/data/user/0/com.snapchat.android/databases/media_packages
4      640      25      95/230/1
/data/user/0/com.snapchat.android/databases/media_packages (2)
4      640      65      747/32/4
/data/user/0/com.snapchat.android/databases/media_packages (1)
4      1960     108    32999/11717/12
/data/user/0/com.snapchat.android/databases/journal.db
4      1960     60     21792/31/2
/data/user/0/com.snapchat.android/databases/journal.db (3)
4      1960     85     26786/38/4
/data/user/0/com.snapchat.android/databases/journal.db (1)
4      1960     44     25314/84/1
/data/user/0/com.snapchat.android/databases/journal.db (2)
4      76       97     9/82/7
/data/user/0/com.snapchat.android/databases/androidx.work.workdb
4      12       0/0/0   (attached) temp
4      48       104    4024/4884/7
/data/user/0/com.snapchat.android/databases/durable_job
4      48       108    11957/52/8
/data/user/0/com.snapchat.android/databases/durable_job (1)
4      48       82     5880/5847/3
/data/user/0/com.snapchat.android/databases/durable_job (3)
4      48       93     11429/320/6
/data/user/0/com.snapchat.android/databases/durable_job (2)
4      40       22     1/41/2
/data/user/0/com.snapchat.android/databases/cognac
4      828      109    2080/1723/22
/data/user/0/com.snapchat.android/databases/core.db
4      828      62     54/1455/2
/data/user/0/com.snapchat.android/databases/core.db (1)
4      828      56     1954/340/2
/data/user/0/com.snapchat.android/databases/core.db (3)
4      828      109    975/878/7
/data/user/0/com.snapchat.android/databases/core.db (2)
4      132     100    12404/12666/25
/data/user/0/com.snapchat.android/databases/SPECTACLES_SQLITE
4      12       0/0/0   (attached) temp
4      132     83     60140/3429/25
/data/user/0/com.snapchat.android/databases/SPECTACLES_SQLITE (2)
4      132     97     59381/3833/25
/data/user/0/com.snapchat.android/databases/SPECTACLES_SQLITE (3)
4      132     109    40152/20690/14
/data/user/0/com.snapchat.android/databases/SPECTACLES_SQLITE (4)

Asset Allocations
: 271K
: 319K
: 258K
: 411K

```

Figure 54. ADB Dumpsys meminfo report for com.snapchat.android

6.2.8 Forensic exam VIII: Data request

By requesting user account data directly from the smart eyewear firm, Forensic exam VIII aids in collecting biometric information, cross correlating evidence, finding discrepancies in data storage and BLE transfer integrity, and determining smart eyewear camera hardware.

As described within Snap Inc.'s "Law Enforcement Guide" [213], the smart eyewear's Law Enforcement Service System (LESS)[214] handles direct requests for data as follows:

“For use only by SWORN LAW ENFORCEMENT OFFICERS (or other appropriate governmental entities) requesting Snap's disclosure of Snapchat account records. Please note a valid identifier is required in order for Snap to locate a Snapchat account and process your request. We are unable to locate Snapchat accounts based on any of the following: display name, real name, date of birth, street address, social security number, and photos.”

and as such, data from the LESS system has not been examined for the purpose of this study due to restricted availability.

An alternative data request method [215] is available and has been utilized within this study, as the researcher is not a “sworn law enforcement officer” nor “other appropriate governmental entity”.

This alternative method may be used by a forensic investigator who legally obtains access to the smart eyewear owner’s user account login information (Snapchat username/verified email address and password [216]) and linked email account.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner. The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices, see Table x for further detail.

Table 30. Forensic exam VIII: Chain of custody, network access, system administration status

Devices	Chain of Custody	Snapchat Login Access	Gmail Account Access (Linked to Snapchat)	Network Access	System Administration Status
Target device: Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	Not Applicable	Not Applicable	No access to device’s used networks	Not Rooted
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	Obtained by forensic investigator	Obtained by forensic investigator	Obtained by forensic investigator	No access to device’s used networks	Not Rooted

6.2.8.1 Forensic exam VIII: Methods and tools

See Tables x-x for procedures and tools to request and examine the smart eyewear user’s mobile application data from Snap Inc.

Table 31. Forensic exam VIII: Procedure used to request and examine smart eyewear user’s mobile application data from Snap Inc.

1.	Obtained target smartphone and access to open emails within Gmail account linked to smart eyewear mobile application
2.	Obtained access to smart eyewear owner’s Snap Inc. account username/verified email address and login password

3.	Requested data download via Snap Inc.'s procedural guide [215] [216]
4.	Downloaded data request ZIP file via link provided in smart eyewear owner's linked Gmail account to investigator's external microSDXC card within target smartphone
5.	Transferred ZIP file from microSDXC card to laptop for further examination
6.	Extracted data request from ZIP file
7.	Examined data request within Autopsy 4.13.0 [251], ExifTool v12.07 [252], and VLC Media Player (64-bit) [253]

Table 32. Forensic exam VIII: Tools used fused to request and examine smart eyewear user's mobile application data from Snap Inc.

Device	Software, peripherals, tools, files
Target device: Samsung Galaxy S10e smartphone (BLE paired to smart eyewear)	<ul style="list-style-type: none"> - Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0 - microSDXC card (Investigator's non-volatile memory card)
Laptop	<ul style="list-style-type: none"> - Windows 10 Operating system - ZIP file requested from Snap Inc. - Autopsy 4.13.0 [251] - ExifTool v12.07 [252] - VLC Media Player (64-bit) [253]

6.2.8.2 Forensic exam VIII: Analysis, results, and discussion

The data request provided a historic archive of the smart eyewear user's mobile application actions (Figure X (a)(b)). The list on the left, under the Snap Inc. logo, is composed of links to data and information types stored within the smart eyewear cloud.

The manufacturer data extracted from BLE scanning and enumeration within Forensic exams II-III (Figures X-X) matched the first 10 characters of the 16 character Spectacles smart eyewear Serial Number (Figure X). This data has been obscured for purposes of anonymity.



Account History

This section includes an overview of your current and previous display name, mobile number, and email address — as well as information about when you've changed your password, linked your Bitmoji, or paired Spectacles.

- Login History and Account Information
- Snap History
- Chat History
- Our Story and Crowd-Sourced Content
- Purchase History
- Shop History
- Snapchat Support History
- User Profile
- Friends
- Ranking
- Story History

Display Name Change

Date	Display Name
2020-02-17 15:20:28 UTC	S Tene

Email Change

Date	Email Address
2020-02-17 15:21:23 UTC	stene000@gmail.com

Password Change

Date
2020-09-18 21:31:20 UTC
2020-09-18 21:24:27 UTC

Account History

Location

Search History

Terms History

Subscriptions

Bitmoji

In-app Surveys

Reported Content

Bitmoji Kit

Connected Apps

Talk History

Ads Manager

Snap Games and Minis

My Lenses

Memories

Cameos

Email Campaign History

Frequently Asked Questions

Spectacles

Date	Action
2020-09-18 21:17:49 UTC	Paired
2020-09-17 11:41:29 UTC	Paired
2020-08-04 14:33:00 UTC	Paired
2020-08-04 11:11:42 UTC	Paired
2020-08-04 11:05:53 UTC	Deleted
2020-08-04 11:05:35 UTC	Paired
2020-08-04 11:03:24 UTC	Deleted
2020-08-04 11:03:06 UTC	Paired
2020-08-04 10:59:12 UTC	Paired
2020-08-04 10:51:52 UTC	Paired
2020-08-03 22:48:22 UTC	Paired
2020-08-03 22:46:27 UTC	Paired

(a)

2020-07-30 10:19:13 UTC	Not Paired
-------------------------	------------

(b)

2020-02-17 15:43:31 UTC	Firmware Updated
2020-02-17 15:40:04 UTC	Paired

(c)

Figure 55. Forensic exam VIII: “Account History” and “Spectacles” excerpts from smart eyewear “Data Request” (a) Action(s): “Paired” and “Deleted”; (b) Action: “Not Paired” ; (c) Action: “Firmware Updated”

The data request provided a smart eyewear log which included the following system actions occurring between the time range of 2020-02-17 15:40:04 UTC and 2020-09-18 21:17:49 UTC: 141 “Paired” events; 24 “Deleted” events; 2 “Not Paired” events; 1 “Firmware Updated” event, see Figure X (a)(b)(c) for action excerpts.

Smart eyewear actions found within the data request can be cross referenced with BLE pairing events within Forensic exam III.

87 photos and 77 videos (164 artifacts total) were extracted from Snapchat Memories, possessing timestamps between 2020-07-21 14:53:02 UTC and 2020-08-04 11:13:01 UTC. (Figure X)

Download links were tested after 7 days to verify Snap Inc.’s data minimization expiration policy. As warned, an HTTP “... Status 403” response code was provided, alerting access to the requested resources is forbidden. (Figure X)

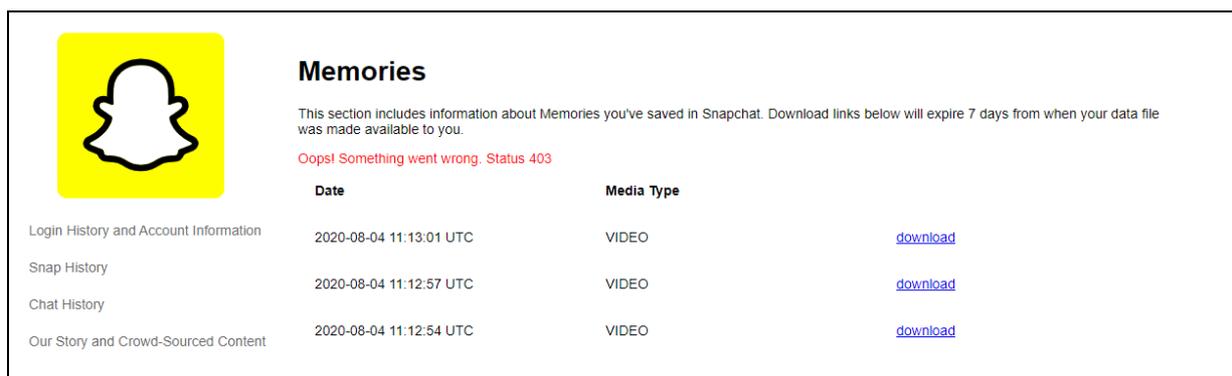


Figure 56. Forensic exam VIII: HTTP 403 response after requesting smart eyewear data past 7th day.

The “Data Request” was examined within Autopsy v4.13.0 and ExifTool v12.07 which provided great detail on the original photographs and videos captured by the smart eyewear, including the camera make (Ambarella) and model (Amba_camera_h2) within the smart eyewear (Figure X and Table X).

Autopsy v4.13.0 was incapable of generating a thumbnail preview for the MP4 video files.

Preliminary background research compiled for this study was incapable of identifying the smart eyewear’s video processing SoC; however, a quick lookup of “Ambarella h2” provided the Ambarella H2 Video SoC product brief [217] without having to perform an invasive device teardown.

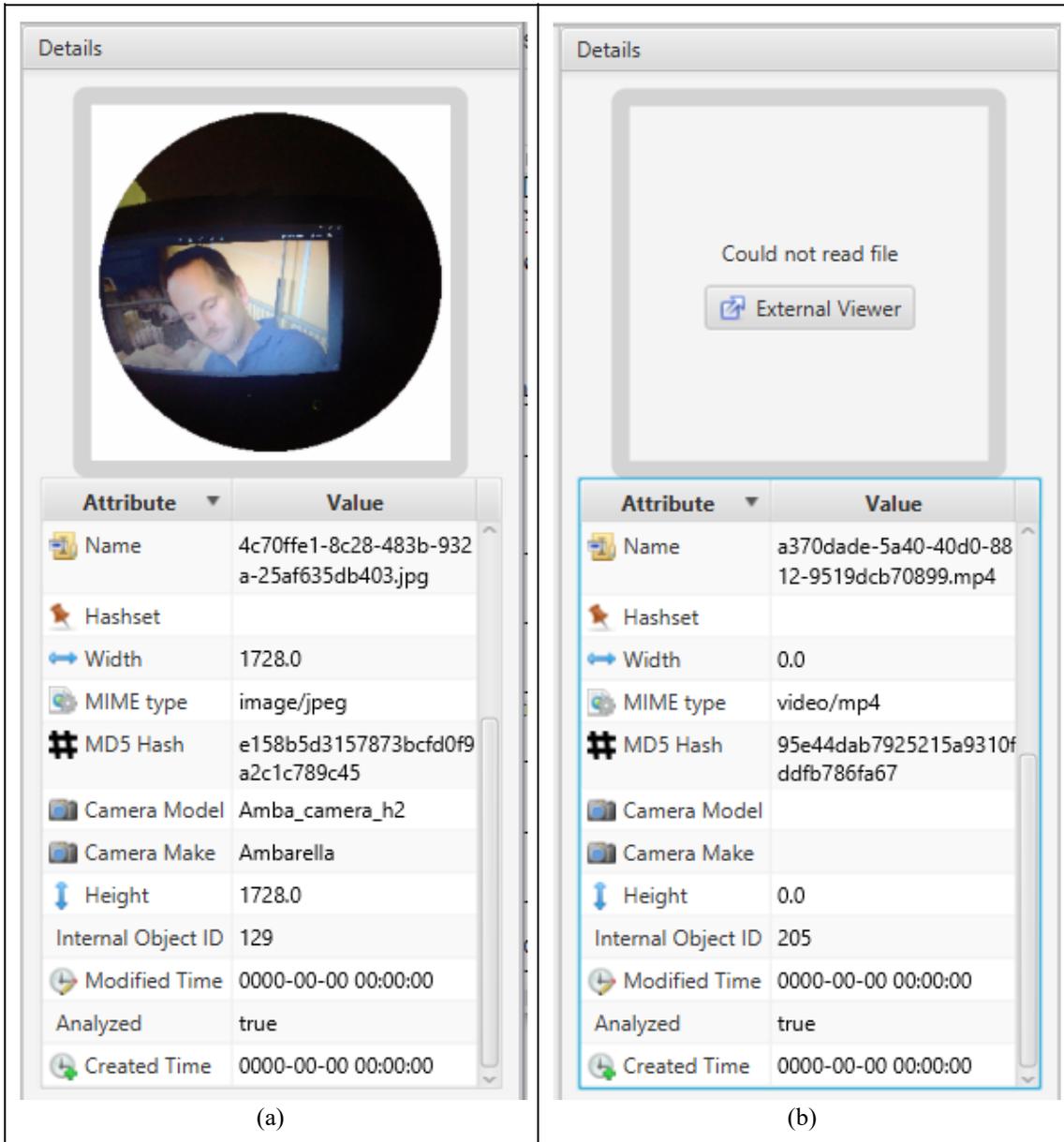


Figure 57. Forensic exam VIII: Autopsy 4.13.0 metadata from a (a) JPEG image and (b) MP4 video, extracted from smart eyewear Data Request

Snap Inc. developers did not include any metadata values for the following JPEG image tags: “Date/Time Original” and “Create Date”. The lack of this information heightens the difficulty of triangulating biometric artifact evidence, as there is no point of reference for the exact time the photograph was captured by the smart eyewear.

Table 33. Forensic exam VIII: ExifTool v12.07 metadata from a JPEG image extracted from smart eyewear Data Request

Tag	Value	Tag	Value	Tag	Value
File Name	4c70ffe1-8c28-483b-932a-25af635db403.jpg	Shutter Speed Value	1/60	Device Setting Description	(Binary data 4 bytes, use -b option to extract)
Directory	C:/path-to-file	Aperture Value	2	Subject Distance Range	Unknown

File Size	606 kB	Exposure Compensation	0	Compression	JPEG (old-style)
File Modification Date/Time	2020:09:21 00:54:45+03:00	Max Aperture Value	2	Thumbnail Offset	41984
File Access Date/Time	2020:12:03 13:29:59+02:00	Subject Distance	0 m	Thumbnail Length	10734
File Creation Date/Time	2020:09:21 00:54:44+03:00	Metering Mode	Spot	MPF Version	10
File Permissions	rw-rw-rw-	Light Source	Unknown	Number Of Images	2
File Type	JPEG	Flash	No flash function	MP Image Flags	Dependent child image
File Type Extension	jpg	Focal Length	0.0 mm	MP Image Format	JPEG
MIME Type	image/jpeg	Warning	[minor] Unrecognized MakerNotes	MP Image Type	Large Thumbnail (VGA equivalent)
Exif Byte Order	Little-endian (Intel, II)	Flashpix Version	10	MP Image Length	111511
Image Description	UserContent\6a414fbff9	Color Space	sRGB	MP Image Start	509003
Make	Ambarella	Exif Image Width	1728	Dependent Image 1 Entry Number	0
Camera Model Name	Amba_Camera_H2	Exif Image Height	1728	Dependent Image 2 Entry Number	0
Orientation	Horizontal (normal)	Interoperability Index	R98 - DCF basic file (sRGB)	Image UID List	(Binary data 66 bytes, use -b option to extract)
X Resolution	72	Interoperability Version	10	Total Frames	1
Y Resolution	72	Exposure Index	undef	Image Width	1728
Resolution Unit	inches	Sensing Method	One-chip color area	Image Height	1728
Software	0.8.0001	File Source	Digital Camera	Encoding Process	Baseline DCT, Huffman coding
Modify Date	000M0000.JPG	Scene Type	Directly photographed	Bits Per Sample	8
Y Cb Cr Positioning	Centered	Custom Rendered	Normal	Color Components	3
Exposure Time	1/60	Exposure Mode	Auto	Y Cb Cr Sub Sampling	YCbCr4:2:2 (2 1)
F Number	2.8	White Balance	Auto	Aperture	2.8
Exposure Program	Program AE	Digital Zoom Ratio	undef	Image Size	1728x1728
ISO	295	Focal Length In 35mm Format	28 mm	Megapixels	3
Exif Version	1220	Scene Capture Type	Landscape	Shutter Speed	1/60
Date/Time Original	Empty Field	Gain Control	None	Thumbnail Image	(Binary data 10734 bytes, use -b option to extract)

Create Date	Empty Field	Contrast	Normal	Preview Image	(Binary data 111511 bytes, use -b option to extract)
Components Configuration	-, Cr, Cb, Y	Saturation	Normal	Focal Length	0.0 mm
Compressed Bits Per Pixel	21474831.48	Sharpness	Normal	Light Value	7.3

Conversely, Snap Inc. developers did include metadata values for the following MP4 video timestamp tags: “Create Date”; “Modify Date”; “Media Create Date”; “Media Modify Date”; “Track Create Date”; “Track Modify Date”. All of which possessed the exact same timestamp that fell within the correct time range the photos and videos were captured by the smart eyewear July to August 2020; however, this timestamp did not match any of the timestamps within the Data Request index.html file.

Table 34. Forensic exam VIII: ExifTool v12.07 metadata from a MP4 video extracted from smart eyewear Data Request

Tag	Value	Tag	Value
File Name	a370dade-5a40-40d0-8812-9519dcb70899.mp4	Track Duration	10.09 s
Directory	C:/path-to-file	Track Layer	0
File Size	2.9 MB	Track Volume	0.00%
File Modification Date/Time	2020:09:21 01:05:13+03:00	Image Width	1280
File Access Date/Time	2020:12:03 15:27:39+02:00	Image Height	1280
File Creation Date/Time	2020:09:21 01:05:12+03:00	Graphics Mode	srcCopy
File Permissions	rw-rw-rw-	Op Color	0 0 0
File Type	MP4	Compressor ID	hvc1
File Type Extension	mp4	Source Image Width	1280
MIME Type	video/mp4	Source Image Height	1280
Major Brand	MP4 v1 [ISO 14496-1:ch13]	X Resolution	72
Minor Version	2013.10.18	Y Resolution	72
Compatible Brands	mp41	Compressor Name	HEVC Coding
Media Data Size	3002462	Bit Depth	24
Media Data Offset	28	Video Frame Rate	59.94
Movie Header Version	0	Matrix Structure	1 0 0 0 1 0 0 0 1
Create Date	2020:07:21 11:03:54	Media Header Version	0
Modify Date	2020:07:21 11:03:54	Media Create Date	2020:07:21 11:03:54
Time Scale	60000	Media Modify Date	2020:07:21 11:03:54
Duration	10.09 s	Media Time Scale	44100

Preferred Rate	1	Media Duration	10.08 s
Preferred Volume	100.00%	Handler Class	Media Handler
Preview Time	0 s	Handler Type	Audio Track
Preview Duration	0 s	Handler Description	AAC Media Handle
Poster Time	0 s	Balance	0
Selection Time	0 s	Audio Format	mp4a
Selection Duration	0 s	Audio Channels	1
Current Time	0 s	Audio Bits Per Sample	16
Next Track ID	3	Audio Sample Rate	44100
Track Header Version	0	Image Size	1280x1280
Track Create Date	2020:07:21 11:03:54	Megapixels	1.6
Track Modify Date	2020:07:21 11:03:54	Avg Bitrate	2.38 Mbps
Track ID	1	Rotation	0

VLC Media Player (64-bit) [253] was used to preview the .mp4 files, as Autopsy 4.13.0 [251] and ExifTool v12.07 [252] did not provide a means to view thumbnails of the video files nor the video files themselves.

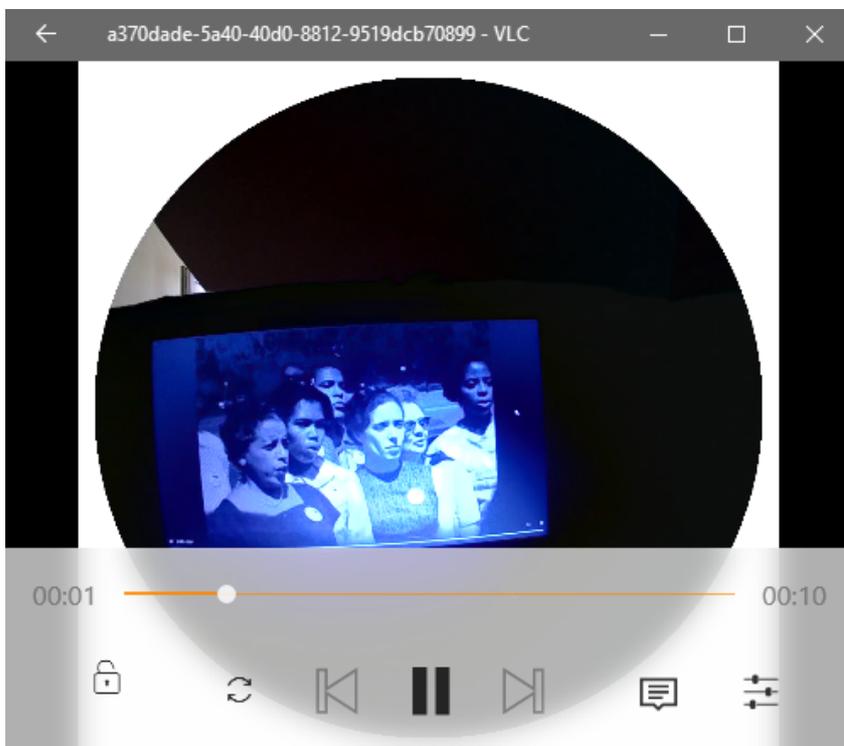


Figure x. Forensic exam VIII: VLC Media Player (64-bit) preview of .mp4 file

Of the 164 total artifacts extracted from Snapchat Memories, 103 were biometric artifacts, 53 .jpg image files contained biometric content and 50 .mp4 video files contained biometric content.

6.2.9 Forensic exam IX: Acquiring system administration privilege

Forensic exam IX highlights a scenario wherein an investigator physically possesses the smart eyewear owner’s paired smartphone and attempts to gain system administrative privileged access to the device’s file system to locate and acquire protected personal data, such as the photographs and videos transferred from the smart eyewear to the smartphone’s /data/data directory.

Two methods of gaining system administrative access to the file system are examined. The first method attempts to acquire root access to the device and the second method flashes a custom firmware recovery installation on the smart eyewear’s paired smartphone without having to unlock the device’s bootloader to root the device.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table x for further detail.

Table 35. Forensic exam IX: Chain of custody, network access, system administration status

Devices	Chain of Custody	Network Access	System Administration Status
Target device: Spectacles version 2 smart eyewear	Device not possessed by forensic investigator	No access to device’s used networks	Not Rooted
Target device: Samsung Galaxy S10e smartphone (BLE paired to smart eyewear)	Obtained by forensic investigator	No access to device’s used networks	Root Attempted

6.2.9.1 Forensic exam IX: Methods and tools

See tables x-x for tools and attempted procedures used for the rooted data acquisition of targeted smartphone.

Table 36. Forensic exam IX: Tools used for rooted data acquisition of targeted smartphone.

Device	Software and peripherals
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte	<ul style="list-style-type: none"> - Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0

Table 37. Forensic exam IX: Attempted procedure used for rooted data acquisition of targeted smartphone [218] [219].

1.	Created ADB partial backup of targeted smartphone within Forensic exam VI
2.	Ensure Samsung S10e driver is installed on computer to enable connection between smartphone and computer
3.	Ensure smartphone has at least 80% battery charge
4.	Enable “Developer options” on smartphone: Settings > About Phone > Build Number (tap 7 times)
5.	Enable “USB debugging mode”: Settings > Developer options > USB debugging
6.	Enable “OEM unlocking”: (Original Equipment Manufacturer) Settings > Developer Options > OEM unlocking
7.	Unlock the Bootloader
8.	Powered off smartphone, booted into “Download mode”, entered into “Unlock mode”
9.	Encountered “Unlock Bootloader” warning regarding deletion of “...all personal data”
10.	Aborted attempt to root device

The “Odin Install Method (No Root Required)” [218] was utilized after aborting acquiring root access to the target smartphone, see tables x-x for tools and attempted procedures used.

Table 38. Forensic exam IX: Tools used for “Odin Install Method (No Root Required)” of targeted smartphone.

Device	Software and peripherals
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte	<ul style="list-style-type: none"> - Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0
Laptop	<ul style="list-style-type: none"> - Windows 10 Operating system - Odin3_v3.13.1.zip [254] - Team Win Recovery Project (TWRP) Recovery

	<ul style="list-style-type: none"> - Twrp-3.4.0-0-beyond0lte.img.tar [220] - USB cable Type A & Micro-B 5 pin connectors to connect target smartphone to the laptop
--	---

Table 39. Forensic exam IX: Procedure used for “Odin Install Method (No Root Required)” of targeted smartphone.

1.	Downloaded and installed Odin3_v3.13.1 on laptop
2.	Downloaded Team Win Recovery Project (TWRP) Recovery file for Samsung Galaxy S10e (Exynos) (Twrp-3.4.0-0-beyond0lte.img.tar [220]) via laptop
3.	Powered off smartphone
4.	Entered S10e into “Download mode” and connected device to laptop with USB cable
5.	Opened Odin, clicked “AP” (Android Processor) button, selected Twrp-3.4.0-0-beyond0lte.img.tar firmware file
6.	Pressed “Start” to flash .tar firmware file to the smartphone’s system partition

6.2.9.2 Forensic exam IX: Analysis, results, and discussion

Gaining root access was not possible on the targeted paired smartphone, which was initially utilized to import all biometric assets from the smart eyewear.

Unlocking the Samsung Galaxy S10e’s locked bootloader would have resulted in the deletion of all personal application data within the smart eyewear mobile application prior to attempting to root the device; as disclaimed by the device’s “Unlock bootloader” warning: “Unlock Bootloader? ...To prevent unauthorized access to your personal data, unlocking the bootloader will also delete all personal data from your phone (a “factory data reset”)”, see Figure x (a)(b).

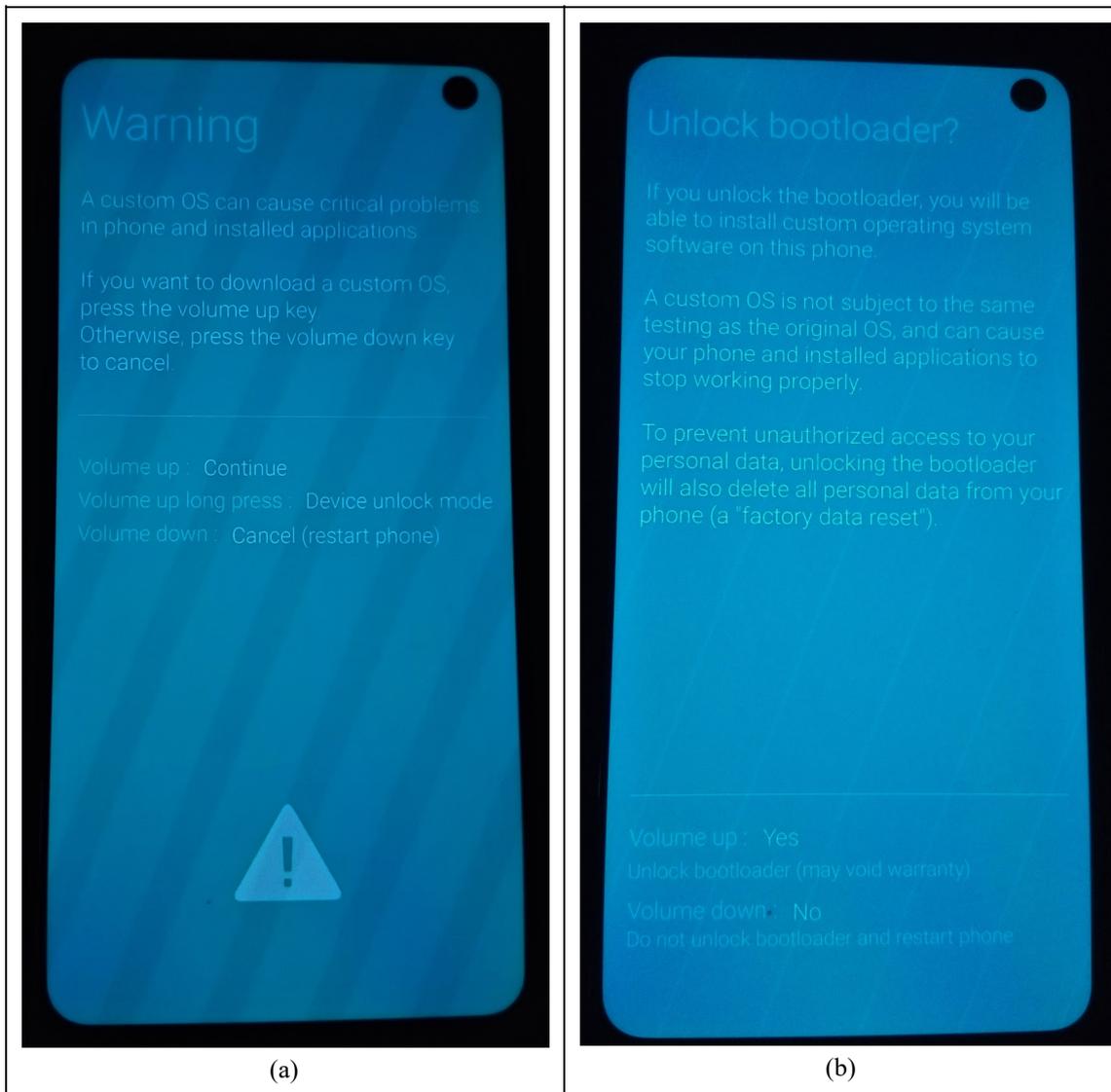


Figure 58. Forensic exam IX: (a) Warning before entering “Device unlock mode” (b) “Unlock bootloader” warning

The aforementioned method to root the device was aborted and various attempts were made to flash a TWRP .tar recovery file to the smart eyewear’s paired smartphone without unlocking the bootloader in order to preserve data integrity; however, this “Odin Install Method (No Root Required)” also proved to be a fruitless endeavor.

In the last attempts to flash the recovery software to the S10e, “Strong protection” (encryption) and “Security policy updates” were turned off on the S10e (figure x).

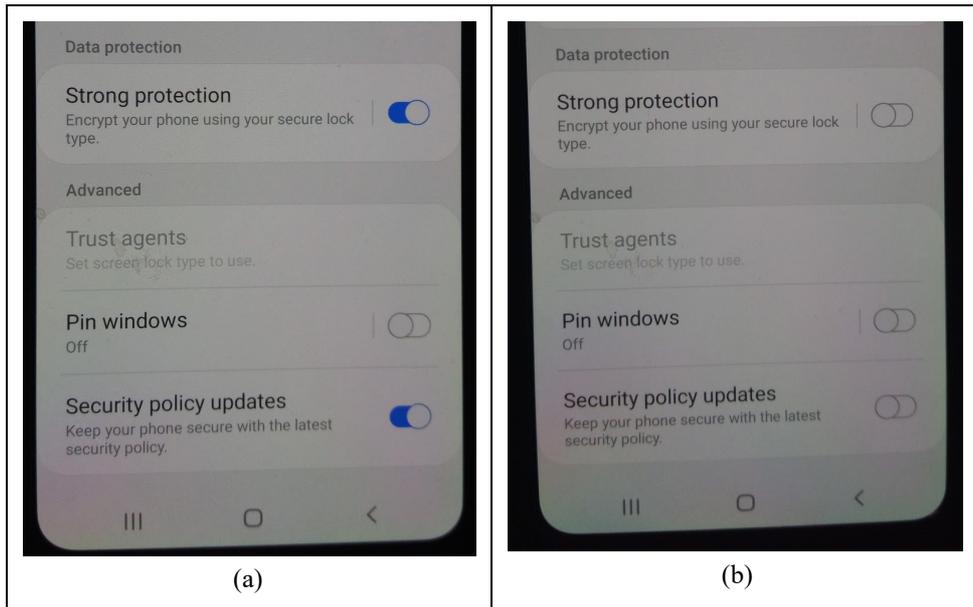


Figure 59. Forensic exam IX: Screenshot of “Strong protection” (encryption) and “Security policy updates” (a) Enabled (b) Disabled

Nevertheless, all attempts to flash the TWRP .tar recovery via Odin to the S10e without unlocking the bootloader were unsuccessful, as illustrated in the last attempt in figure x.

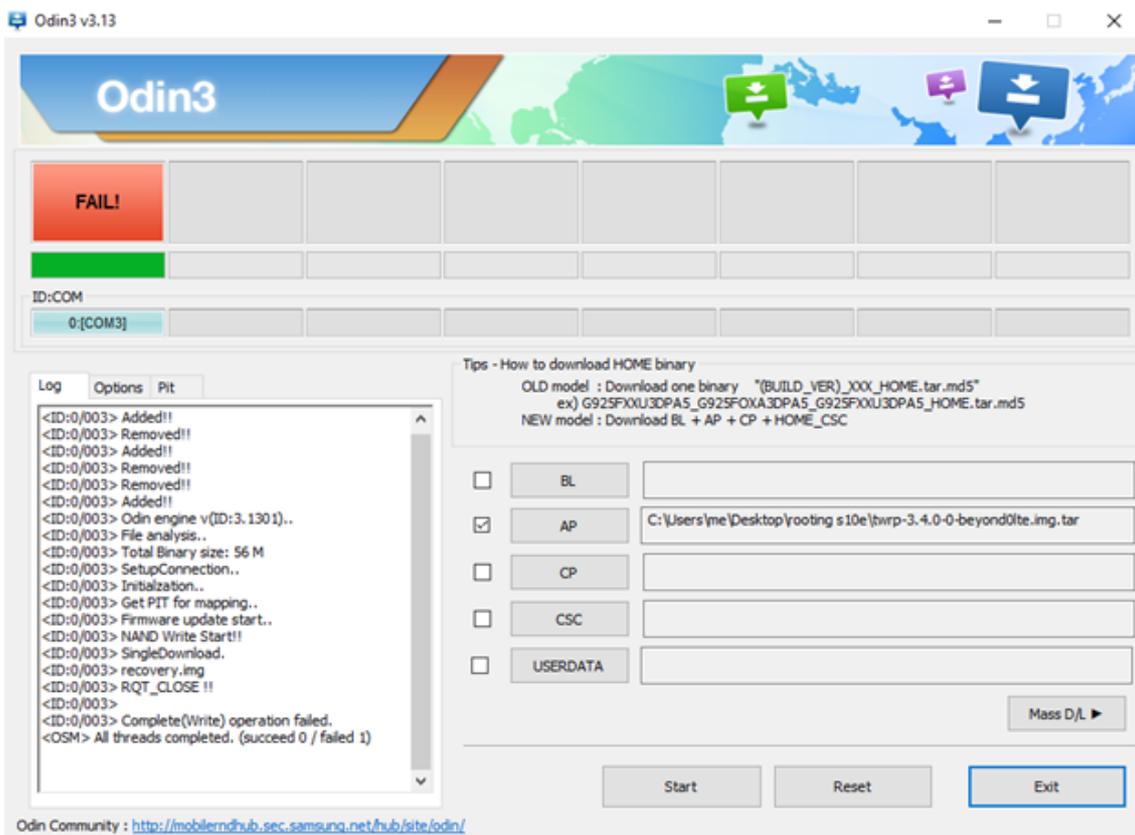


Figure 60. Forensic exam IX: Failed attempt to flash TWRP .tar file to S10E

The escalation of administrative file system privilege by obtaining root access to a mobile smart device in a forensically sound manner which preserves data integrity, has been investigated and contentiously debated among computer forensics professionals.

The following study, [221], concludes that rooting an android smartphone during the boot process with a custom recovery image preserves data integrity, whereas other studies, [51] [191], conclude acquiring root access to smart devices results in loss of data through either data manipulation or erasure of user data.

Contention within the forensic community further reinforces the need to exercise preventative due diligence when acquiring forensic assets. NIST’s guidelines on mobile forensics were followed, as identifying mobile devices and understanding the situational environment of the device ecosystem within a forensic investigation [222] enables an investigator to make informed and tailored choices when extracting and attempting to preserve device data.

Refraining from rooting the initially paired smartphone, was a choice made only after further system observation and identification, in an attempt to preserve data integrity.

No additional photos or videos were extracted from the smart eyewear’s paired smartphone due to the system’s locked bootloader and the inability to flash a custom firmware recovery installation on the smartphone.

6.2.10 Forensic exam X: Acquiring smart eyewear cloud data with a rooted sandbox smartphone and parallel APK

Forensic exam X explores acquiring access to the smart eyewear owner’s cloud data after installing the same version of the com.snapchat.android Android Application package (APK) which was on the paired smartphone, on a rooted sandbox smartphone.

The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices. The forensic investigator only possesses administrative privilege to their sandbox smartphone.

The researcher as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner, see Table x for further detail.

Table 40. Forensic exam X: Chain of custody, network access, system administration status

Devices	Chain of Custody	Snapchat APK Login Access	Network Access	System Administration Status
Target device: Spectacles version 2	Device not possessed by	Not Applicable	No access to device’s used	Not Rooted

smart eyewear	forensic investigator		networks	
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	Obtained by forensic investigator	Obtained by forensic investigator	No access to device's used networks	Not Rooted
Sandbox device: Xiaomi Redmi Note 7 Smartphone Code Name: lavender	Not Applicable: Investigator's device	Not Applicable: Investigator's device	Not Applicable: Investigator's device	Rooted

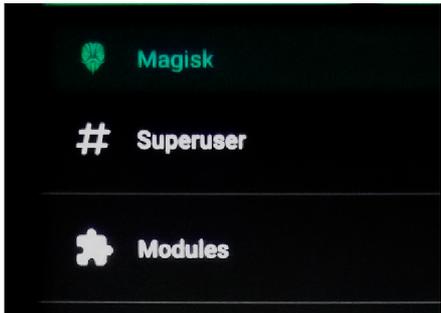
6.2.10.1 Forensic exam X: Methods and tools

See tables x-x for tools procedures used for rooting, installing a smart eyewear APK, and examining cloud data on an investigator's sandbox device.

Table 41. Forensic exam X: Tools used for rooting, installing a smart eyewear APK, and examining cloud data on an investigator's sandbox device.

Device	Software and peripherals
Target device: Samsung Galaxy S10e (Exynos) Smartphone Code Name: beyond0lte (BLE paired to smart eyewear)	<ul style="list-style-type: none"> - Android v10.0; One UI v2.0 - Snapchat application v10.77.5.0
Investigator's sandbox device: Xiaomi Redmi Note 7 (model: M1901F7G) smartphone Code Name: lavender	<ul style="list-style-type: none"> - Android v9 PKQ1.180904.001 - Snapchat application v10.77.5.0 [223] - Team Win Recovery Project (TWRP) Recovery image for Xiaomi Redmi Note 7 (lavender) [224] - Magisk Manager v7.5.1[225] - Magisk-v20.4.zip [226]
Laptop	<ul style="list-style-type: none"> - Windows 10 Operating system - Windows Command Processor - Android Debug Bridge - Odin3_v3.13.1.zip [254] - Android Studio [228] - USB cable Type A & Micro-B 5 pin connectors to connect target smartphone to the laptop
Camera	<ul style="list-style-type: none"> - Micro SD memory card to transfer photos to laptop

Table 42. Forensic exam X: Procedure used for rooting investigator’s sandbox device.

1.	Ensure Xiaomi Redmi Note 7 driver is installed on computer to enable connection between smartphone and computer
2.	Ensure smartphone has at least 80% battery backup before rooting
3.	Enable “Developer Options” on smartphone: Settings > About Phone > Build Number (tap 7 times)
4.	Enable “USB debugging mode”: Settings > Developer Options > USB Debugging
5.	Enable “OEM Unlocking”: (Original Equipment Manufacturer) Settings > Developer Options > OEM Unlocking
6.	Unlocked Bootloader on Xiaomi Redmi Note 7 [229]
7.	Installed TWRP Recovery file [224] on Xiaomi Redmi Note 7
8.	Installed Magisk Manager v7.5.1[225]and Magisk-v20.4.zip [226] on Xiaomi Redmi Note 7
9.	Installed Odin on laptop
10.	Rooted Xiaomi Redmi Note 7 with TWRP, ADB, Magisk Manager, and Magisk-v20.4.zip [230]
11.	<p>Connected sandbox smartphone to laptop via USB cable, then sent the following ADB commands:</p> <pre>>adb devices -l List of devices attached 2da4da73 device product:lavender_eea model:Redmi_Note_7 device:lavender transport_id:1 >adb shell 13 lavender:/ \$ su Permission denied</pre> <p>Figure x. Forensic exam X: Testing administrative privilege within sandbox smartphone via ADB shell su command</p>
12.	<p>Opened Magisk Manager, clicked 3 bars icon, selected “# Superuser” from the drop down menu, and enabled “Shell - com.android.shell” toggle button (Figure x (a)(b)(c)).</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>(a)</p> </div> <div style="text-align: center;">  <p>(b)</p> </div> </div>

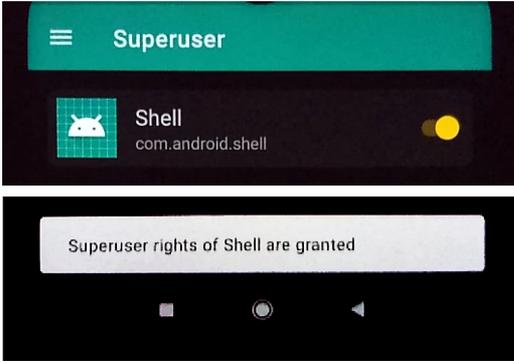
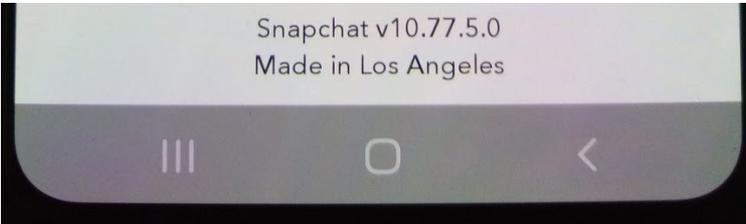
	 <p style="text-align: center;">(c)</p> <p>Figures x. Forensic exam X: Magisk superuser rights granted (a) 3 bars icon (b) # Superuser (c) Shell</p>
13.	<p>Re-sent ADB Shell “su” command to acquire administrative system privilege on the sandbox smartphone.</p> <p>Then installed smart eyewear APK, see Table 14 for detail.</p>

Table 43. Forensic exam X: Procedure used for installing smart eyewear APK on investigator’s sandbox device.

1.	<p>Determined com.snapchat.android APK version number from targeted smartphone Open Snapchat > Settings > Scroll to page end</p>  <p>Figure x. Forensic exam X: Verification of com.snapchat.android version 10.77.5.0 on targeted smartphone (Samsung Galaxy S10e)</p> <p>The intent behind APK version verification is to simulate as much of the targeted paired smartphone and smart eyewear’s ecosystem and operational environment as possible, prior to accessing data stored on the cloud.</p> <p>Additionally, developers of the Snapchat mobile application (com.snapchat.android) updated the software numerous times throughout the testing process, requiring the installation of a deprecated version of Snapchat, as opposed to downloading the software directly from Snap Inc. on Google Play.</p>
2.	<p>Locating and installing a compatible deprecated Snapchat APK file on the sandbox smartphone requires the device’s most preferred Application Binary Interface (ABI).</p> <p>Determined target and sandbox smartphone most preferred Application Binary Interface (ABI) by connecting both devices to the laptop and using ADB command:</p> <pre style="text-align: center;">adb shell getprop findstr ro.product.cpu.abi</pre>

Android Developers detailed that Android’s build information, extracted from system properties, possesses “... ordered list[s] of ABIs supported by this device. The most preferred ABI is the first element in the list.” [231] , see Figures x-x.

```
>adb devices -l
List of devices attached
RF8N11P3CGH      device product:beyond0lteeea model:SM_G970F
device:beyond0 transport_id:17

>adb shell getprop | findstr ro.product.cpu.abi
[ro.product.cpu.abi]: [arm64-v8a]
[ro.product.cpu.abi.list]: [arm64-v8a,armeabi-v7a,armeabi]
[ro.product.cpu.abi.list32]: [armeabi-v7a,armeabi]
[ro.product.cpu.abi.list64]: [arm64-v8a]
```

Figure x. Forensic exam X: Target smartphone (Samsung Galaxy S10e:beyond0lteeea) Application Binary Interface

```
>>adb devices -l
List of devices attached
2da4da73         recovery product:omni_lavender model:Redmi_Note_7
device:lavender transport_id:18

>adb shell getprop | findstr ro.product.cpu.abi
[ro.product.cpu.abi]: [arm64-v8a]
[ro.product.cpu.abi.list]: [armeabi-v7a,armeabi]
[ro.product.cpu.abi.list32]: [armeabi-v7a,armeabi]
[ro.product.cpu.abi.list64]: []
```

Figure x. Forensic exam X: Sandbox smartphone (Xiaomi Redmi Note 7: Lavender) Application Binary Interface

The target and sandbox smartphones coincidentally possessed the same ABI, “arm64-v8a”, Figures x-x.

3. Verified com.snapchat.android APK file was cryptographically signed by Snap Inc. See APK certificate fingerprints in Figure x [223].

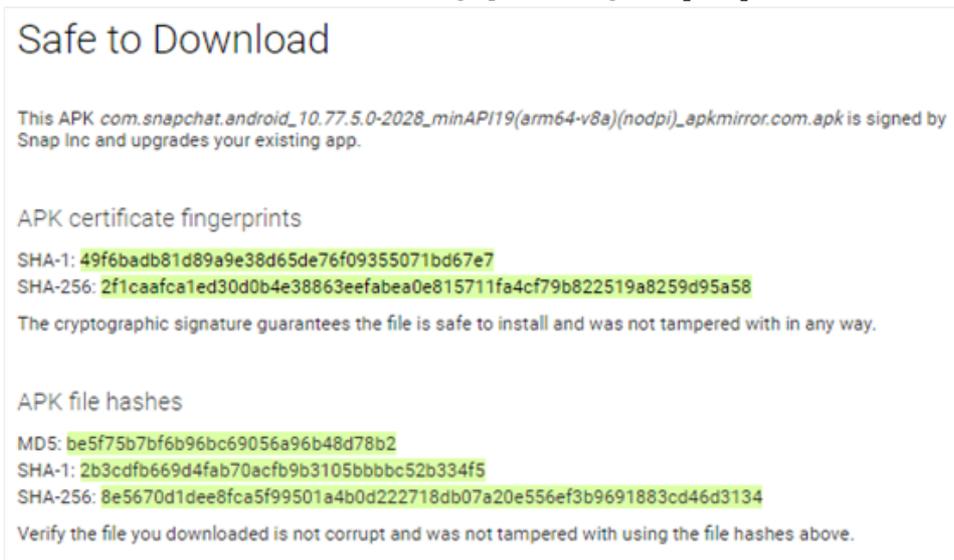
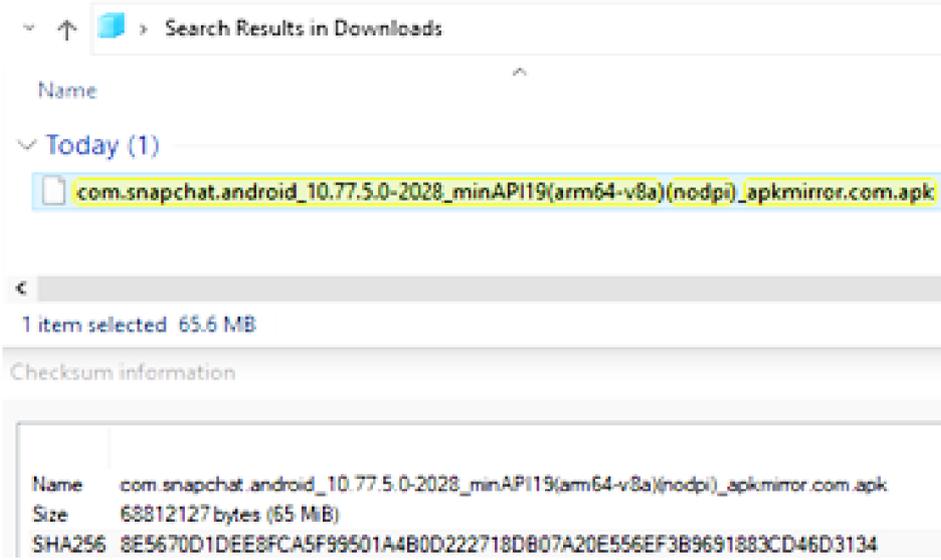


Figure x. Forensic exam X: Snapchat 10.77.5.0 APK cryptographic certificate fingerprints and file hashes [223]

4. Downloaded the deprecated 10.77.5.0 version of the com.snapchat.android APK file

	<p>from apkmirror.com: com.snapchat.android_10.77.5.0-2028_minAPI19(arm64-v8a)(nodpi)_apkmirror.com.apk [223]</p>
5.	<p>Verified application product integrity of downloaded Snapchat APK file's SHA256 hash with the Windows 10 CRC SHA tool, see Figure x.</p>  <p>Figure x. Forensic exam X: SHA256 hash results for Snapchat 10.77.5.0 apk file via Windows 10 CRC SHA tool</p> <p>Results from Figure x match Figure x, thus verifying integrity of the APK file: com.snapchat.android_10.77.5.0-2028_minAPI19(arm64-v8a)(nodpi)_apkmirror.com.apk [223]</p>
6.	<p>Downloaded Android Studio [228] and verified Snapchat APK's backup settings within the AndroidManifest.xml file</p>
7.	<p>Installed com.snapchat.android_10.77.5.0-2028_minAPI19(arm64-v8a)(nodpi)_apkmirror.com.apk [223] on the rooted sandbox smartphone with TWRP and ADB</p>

See Table x for procedures used to manually acquire and logically examine smart eyewear cloud data.

Table 44. Forensic exam X: Procedures used for manual acquisition and logical examinations of smart eyewear cloud data

1.	Obtained Snapchat APK user login credentials (username/email and password)
2.	Manually traversed smart eyewear APK display interface and photographed found biometric evidence on the target BLE paired smartphone (Samsung Galaxy S10e)
3.	Logged out of smart eyewear mobile application user account on target smartphone
4.	Logged into smart eyewear mobile application user account on sandbox smartphone

5.	Manually traversed smart eyewear APK display interface and photographed found biometric evidence on sandbox smartphone
6.	<p>As a rooted superuser, logically examined Snapchat APK cloud data by making file management system calls to open and read directories and file names within the sandbox smartphone's file system.</p> <p>The following ADB commands were used to list Snapchat's directory tree recursively:</p> <pre data-bbox="335 481 1300 728"> >adb devices -l List of devices attached 2da4da73 device product:lavender_eea model:Redmi_Note_7 device:lavender transport_id:1 >adb shell 13 lavender:/ \$ su lavender:/ # cd /data/data/com.snapchat.android lavender:/data/data/com.snapchat.android # ls -R </pre> <p>Figure x. Forensic exam X: ADB Shell command to recursively list all Snapchat APK directories as rooted superuser</p>

6.2.10.2 Forensic exam X: Analysis, results, and discussion

After downloading and hash verifying the deprecated 10.77.5.0 version of Snapchat's APK, Android Studio [228] was downloaded to access the application's AndroidManifest.xml file and verify the software's backup settings prior to installing the APK on the sandbox smartphone, Table 14 #6 and Figure x.

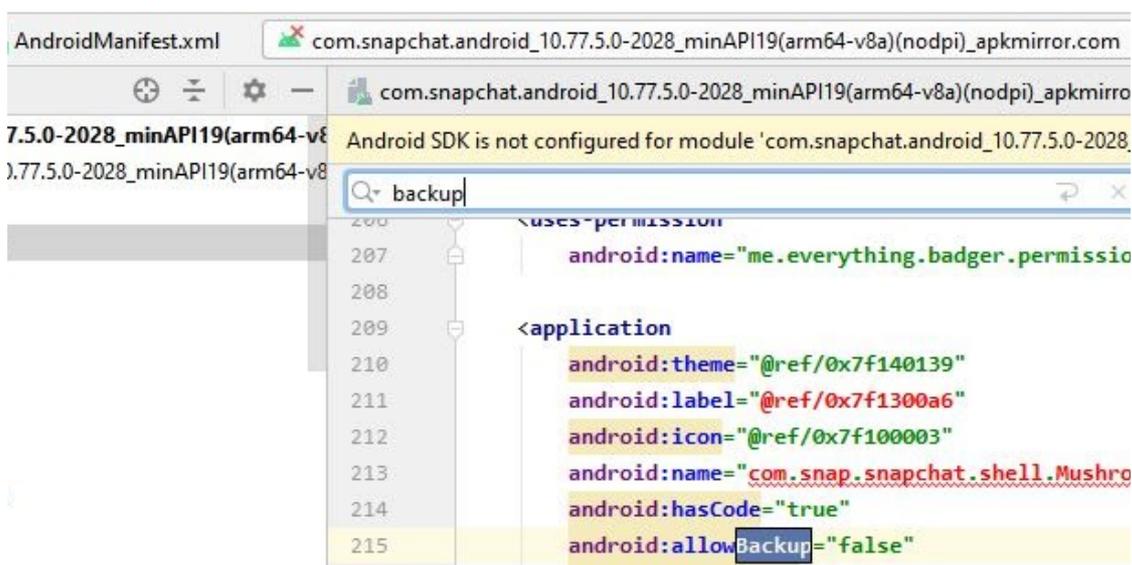


Figure 61. Forensic exam X: Verification of Snapchat APK allowBackup="false" flag via Android Studio [228]

As expected from results within Forensic exam VI, the "allowBackup" flag was set to "false" (Figure X). Snap Inc.'s developers set a privacy-by-default/privacy-by-design control on their Snapchat mobile application, thus preventing ADB backups.

Manual examinations and acquisitions of photographs and videos containing biometric data within the target and sandbox smartphone Snapchat APKs were performed in order to cross reference results.

After installing the deprecated version of Snapchat and logging into the smart eyewear's smartphone application on the sandbox device, an unintended determination illustrated the smart eyewear's cloud did not accurately and timely communicate and provide availability to many images and videos it was responsible for collecting and storing.

It was not until after the Snapchat APK (com.snapchat.android) was logged out of, on the target smartphone, and logged back in, on the sandbox smartphone, did prior BLE transferred images and videos from the smart eyewear to the cloud database become available.

Prior to logging out of the smart eyewear mobile APK on the target smartphone (Samsung Galaxy S10e) there were 22 assets saved in July and 81 assets saved in August 2020 (Figure x).

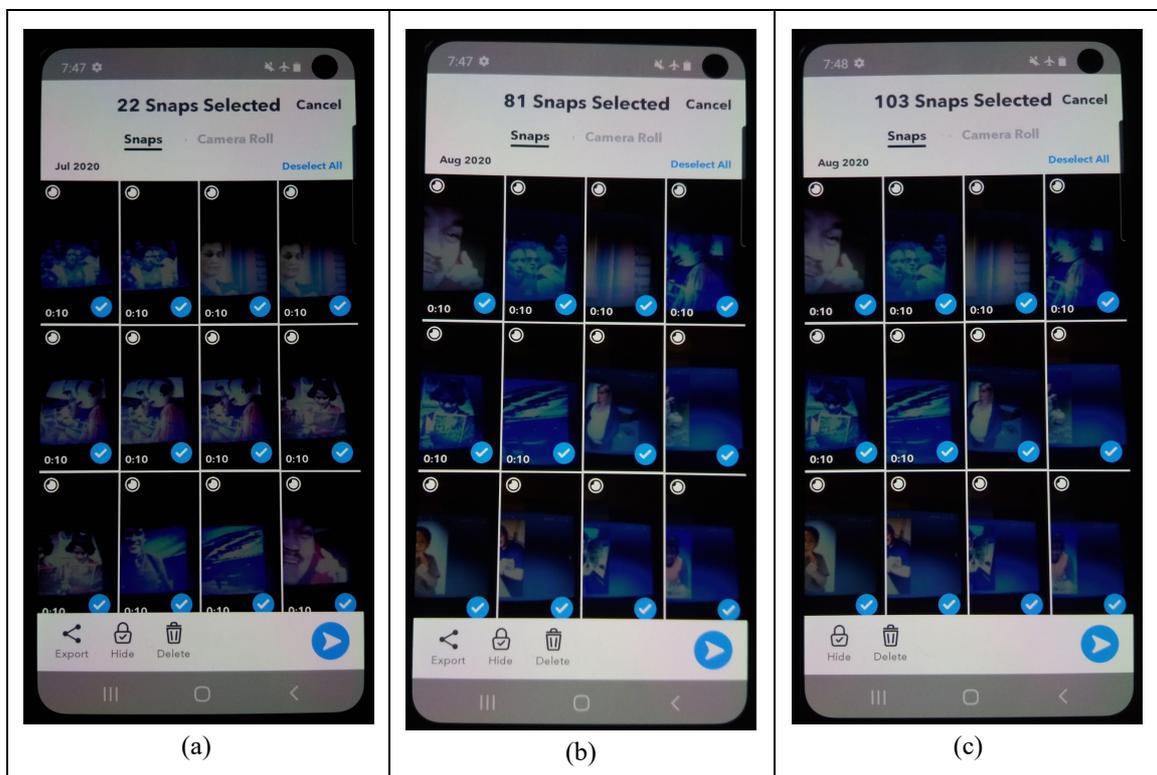


Figure 62. Forensic exam X: 103 total data assets in Snapchat's "Memories" before logout on target smartphone (Samsung Galaxy S10e) (a) July 2020(b) August 2020 (c) Total July - August 2020

After logging into the smart eyewear application on the sandbox smartphone (Xiaomi Redmi Note 7) there were 65 assets saved in July and 99 assets saved in August 2020, for a total of 164, see figure x.

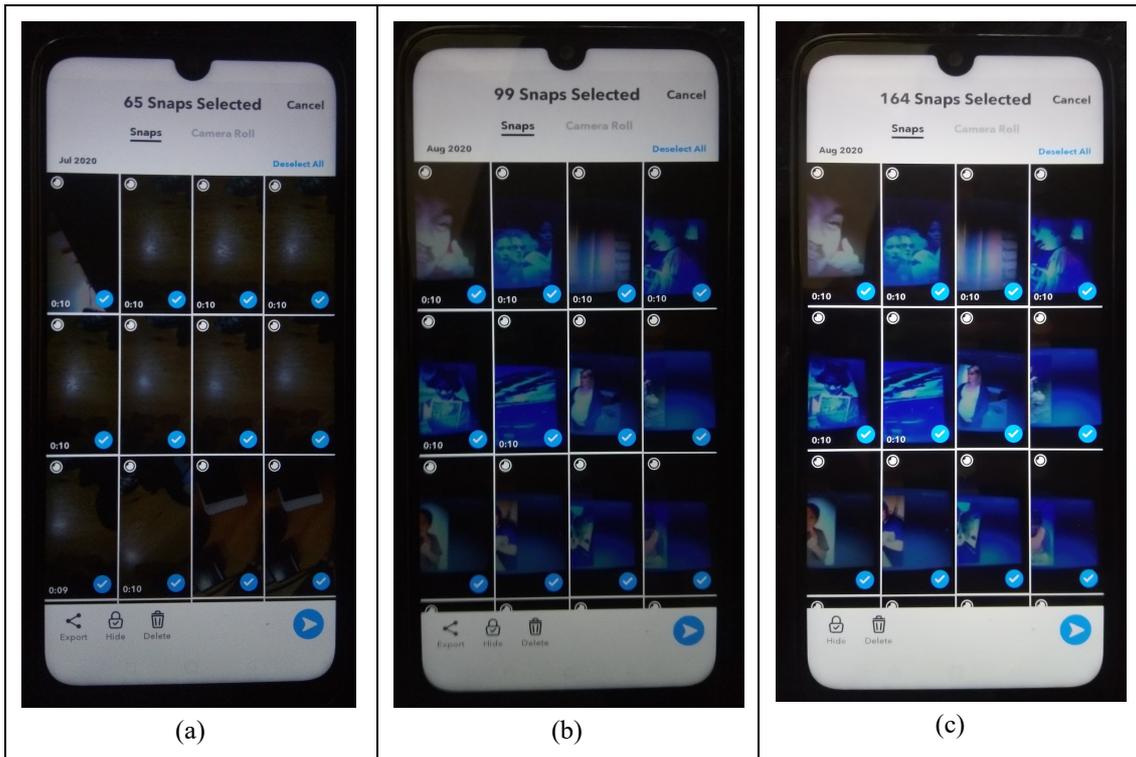


Figure 63. Forensic exam X: 164 total data assets in Snapchat “Memories” after login on sandbox smartphone (Xiaomi Redmi Note 7) (a) July 2020 (b) August 2020 (c) Total July - August 2020

A total of 61 smart eyewear photos and videos were not made available until after logging out and logging back into the application. The data assets did not become available until after logging out of the smart eyewear application user account on the target smartphone and logging back into the account via the sandbox smartphone.

Figure x graphically displays the discrepancy of available smart eyewear data assets before logging out of the Snapchat APK and after logging back in.

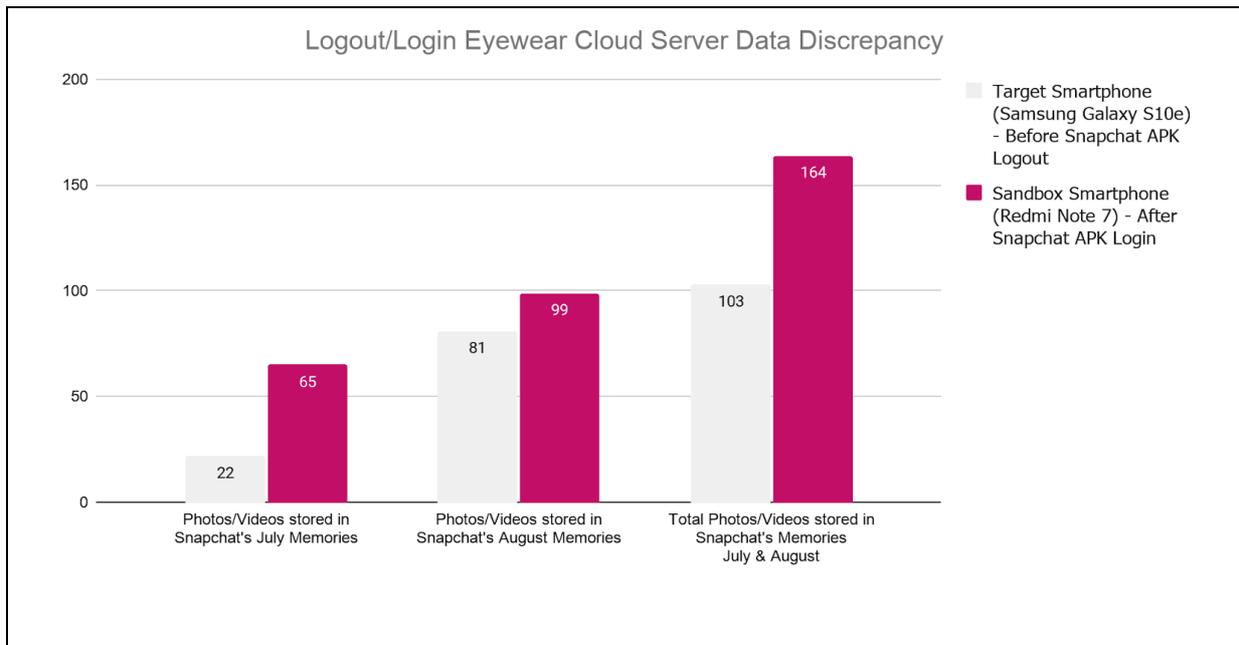


Figure 64. Logout/Login Eyewear Cloud Server Data Discrepancy

Additionally, a quick logical examination of the smart eyewear's cloud data was performed as a rooted superuser on the sandbox smartphone (See Table 15 #6 for commands used and Figure x for results).

```
./databases:
SPECTACLES_SQLITE          cognac          feature-shm      media_packages
SPECTACLES_SQLITE-shm     cognac-shm     feature-wal      media_packages-shm
SPECTACLES_SQLITE-wal     cognac-wal     fidelius_database.db  media_packages-wal
aab888f1-86bc-b786-2985-2dea8d198c5f_fidelius.db  core.db        fidelius_database.db-shm  memories.db
aab888f1-86bc-b786-2985-2dea8d198c5f_fidelius.db-shm core.db-shm    fidelius_database.db-wal  memories.db-shm
aab888f1-86bc-b786-2985-2dea8d198c5f_fidelius.db-wal core.db-wal    journal.db              memories.db-wal
adb                        cronet         journal.db-shm      simple_db_helper.db
androidx.work.workdb     durable_job    journal.db-wal      simple_db_helper.db-shm
androidx.work.workdb-shm durable_job-shm main.db              simple_db_helper.db-wal
androidx.work.workdb-wal durable_job-wal main.db-shm
arroyo.db                feature       main.db-wal

./databases/cronet:
prefs version

./databases/cronet/prefs:
local_prefs.json

./files/file_manager/media:
0b8ace4a-13d6-d53b-49c-0d4aec963101.edits.0  7f3f99c1-08ba-3da8-df31-dafa6d7d77ff.edits.0
c53929e5-41a4-039d-1aef-efabac055504.media.0
13c5f2e4-73eb-fa5a-b3bf-fa6de0cf7663.edits.0  8448c9bd-cf64-2b0b-73b8-4a4909fba7b9.media.0
f009221b-dc07-dd3b-5089-c30413f7e160.media.0
4a002e22-f28e-749e-7878-cd14b2d551e4.media.0  95f5c8ed-983e-3d0e-3856-13d9655980c2.edits.0
4d30341e-6b8a-9d87-d6f6-c5e25e54bf65.edits.0  a6eba6fe-3dba-c66f-37f2-935a242894d7.media.0

./files/file_manager/memories_media:
27D9544FC224C254D2EFA44918103C87.media.0  57F4270924A6BB758DC1D51AAF43EC84.media.0  BDE0BD70916DCF9A5476ECACE3F7528E.media.0
296A9E884ABAC40AECCF8655169016A3.media.0  63345E64B7972415E7BF74657F608437.media.0  BE8DAC4B9D843981DA80DB5533FF3128.media.0
37AA06CE2E4F9EC003040717CBA8B2E8.media.0  9462C63EEB60E63F2520BE8DA0FCEAAD.media.0  C082F6F30F3DBFBA14E21D09C37A624.media.0
458A067D15EFB608ADF16AB3E75792B8.media.0  E308BF7C14861C7DA95A606BEA14754E.media.0

./files/file_manager/memories_mini_thumbnail:
0237CACF772391EB779E6041AB5E775F.mini_thumbnail.0  8D8E3F19FCD5D7FA77E5011AF68330C.mini_thumbnail.0
03B80EC2154AD99C63FD94094CBA2530.mini_thumbnail.0  8FE8A8965651122FBD0A5C30A6349754.mini_thumbnail.0
03CAF1AB739D2CDAS8C783DC8BC6EDC.mini_thumbnail.0  92F8D1A05CF55041A803550F6352953C.mini_thumbnail.0
05B4414E845DF63E9268FB2B1F832F26.mini_thumbnail.0  976FC07E65396648A048E8CC8AEED0DB.mini_thumbnail.0
05B589885228FB0EBE20DDFB5D2F748D6.mini_thumbnail.0  9A40070118DB1908C1779B150B33DF0B.mini_thumbnail.0
068A5170A1B23F0CC179CBE06C283307.mini_thumbnail.0  9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
08FFAC0646C3DC0C734DC322E0C09CFD.mini_thumbnail.0  9BEA8FFB12BBFDAAC9AC45B1A4BB7C2F.mini_thumbnail.0
0C010F1D2B12B336D469AFA466355F44.mini_thumbnail.0  9C3546074CD7610FF845012999871E83.mini_thumbnail.0
0C1D9FC52158B4FFB8D46A93AFFD0F42.mini_thumbnail.0  9CB94784B023F5F50CB48CCA45DE1FD9.mini_thumbnail.0
0ECD1EAAE669893B0DFB931B2BE6F04.mini_thumbnail.0  9F161D0BE6EF26C79B2EC1F0C722BC3D.mini_thumbnail.0
0ECD539521D55823AAA4F4EAE4DEF8.mini_thumbnail.0  A3971F5843C86F5C20FCE65FF931386A.mini_thumbnail.0
0F91EFEE94784AC99C71E932ECC70B3E.mini_thumbnail.0  A73F847715EC899C95692265FB04C29F.mini_thumbnail.0
12B1FC827A7949E5243499B5332C1F.mini_thumbnail.0  A95688027B9BE1FA19F6F79CE68D6B.mini_thumbnail.0
165DA3DF84F2DB09B64387AC98D3A60.mini_thumbnail.0  AA2713B249C39C15F8EA1EF8048CF377.mini_thumbnail.0
169523D54D6A9D8A3D88907C5A7FF2.mini_thumbnail.0  AB0E1B4470DB9C2918421F316677DBFB.mini_thumbnail.0
16CF75C85066F71871C35A506867EC70.mini_thumbnail.0  ACAF588AC8A237E58878858D6CAFAB9.mini_thumbnail.0
1813A6E422DB1A74CD8F987F55E787D3.mini_thumbnail.0  ADE40B29F95C0C4078FA9513BF638BE4.mini_thumbnail.0
1A2243DC96C7F30867E425D2369FDF.mini_thumbnail.0  AF57F42E3A89FBC22892B4C48B56B9C2.mini_thumbnail.0
1A63AD2EB2DC775B2C97E88C9036AE2.mini_thumbnail.0  B344ACFB73F0864EC1092461380B6A7.mini_thumbnail.0
1ACA8086ED74E76E24108614CA4A4156.mini_thumbnail.0  B3B8D9086FCD775399F60CB889485DD1.mini_thumbnail.0
1D38C01661B9C779B2540C995013638.mini_thumbnail.0  B4D275D7AD909CC60FDC5291BCAF4C37B.mini_thumbnail.0
202436985224611CA0B503A688A1BAC.mini_thumbnail.0  B61324302DE8F383D89DBFBE671AD6.mini_thumbnail.0
212DA2B606D151BBEBE0343E483A1.mini_thumbnail.0  B690782992290AAAC8789BCE21FD04A4.mini_thumbnail.0
222B118A0DC789FC0C7349366BBB74.mini_thumbnail.0  B89F210FCA2F0BBEC647530C5B613E8.mini_thumbnail.0
2862BD013F902A136872718CF6BB0E99.mini_thumbnail.0  B8F442A5935D3EC405EB0B047C4AF22E.mini_thumbnail.0
2BED98A6C4F35003FB5237D86A1B4FFB.mini_thumbnail.0  B9AA6E451FA49FF5B55247D2E40C7094.mini_thumbnail.0
2D4AF2F744028412591046291B15B971.mini_thumbnail.0  B9B26A536175462E7B277DF924F2B421.mini_thumbnail.0
2DDF2518753CF1606051DFD3664A1CE4.mini_thumbnail.0  BB043B51B84A8AFC86BEEBD49D981BED.mini_thumbnail.0
2E69EBCA9B25252F2CA5E33A92CBA4A9.mini_thumbnail.0  BB1889C5D1ADA5337EE89159B0B07985.mini_thumbnail.0
2F9CCBBE728B72D1CA67AE020B3E8F.mini_thumbnail.0  BC5AE5FD25C4647C57E0FF8B1776E02.mini_thumbnail.0
2FA32C9085729046B392F75E8A29810.mini_thumbnail.0  BE529A20ECA8AD530A5A46AAB375DEC4.mini_thumbnail.0
2FDD7128B9C6E214784AD3723C112A2.mini_thumbnail.0  BE8DF999567A77BCE6FD25A25F037080.mini_thumbnail.0
3082723AF817516BE6193531EFF101AE.mini_thumbnail.0  C12DA6999EA72C7D3EC8C1D0F48A4B7.mini_thumbnail.0
3275DE743F3A678DC5C9DE8FA89ADCEA.mini_thumbnail.0  C291A213C421835B8A0B35DFC9B6A4.mini_thumbnail.0
3597ADA6FA2A3112946C2B06D24AC7650.mini_thumbnail.0  C2A0CFD188541D2286F406C0CAC373A6.mini_thumbnail.0
3871992F5237E53F2E685DB07BC6953D.mini_thumbnail.0  C3A37946C7731C6E6CC5A345A8F67B0.mini_thumbnail.0
3C9BA482635562C15770F822F81B57B.mini_thumbnail.0  C4148598B0E34A7E65CF668082C28442.mini_thumbnail.0
3CA05F786458E926CEB920EAC812AAC.mini_thumbnail.0  C45576FD98781659BB3F0FE23D1AA761.mini_thumbnail.0
42C5569E03C6C0F67AR22149C68D883.mini_thumbnail.0  C50650488CC8B941AFB15CE66D6B97C.mini_thumbnail.0
4368572A00D0CFC8A8590F883E3DE6E55.mini_thumbnail.0  C52093E51C10E85908917A84C176780.mini_thumbnail.0
44F78B450356A97BE6417BFA28E4EF52.mini_thumbnail.0  C74CEF2279BE3F13743C4CA36634597F.mini_thumbnail.0
465D20C512897B7481A195CB48F4D7A9.mini_thumbnail.0  C800FF03E39DA04524B87C3E54498336.mini_thumbnail.0
47D05C7A49728D1F10047E807EBBC7B52.mini_thumbnail.0  C97D97E1554A63DD79E1BBECCD3C4E2.mini_thumbnail.0
4A569280B98AC476807E6670C6699BA.mini_thumbnail.0  CA0848C9787C91C58B6F5E66604578B0.mini_thumbnail.0
4A885E14FC1D84566E6FB5202F23F37.mini_thumbnail.0  CABFCACFD86E4A4F57AD47217BA0E7934.mini_thumbnail.0
4D2C6AE7BDBAF9A4014F2AA6B3A36.mini_thumbnail.0  CBE348B80529BA970150F30120CDB7C.mini_thumbnail.0
4FF430DCB2882C9BAF79742D23E4A6E.mini_thumbnail.0  CC298E632AA983FA4AC2B35B35876DE7.mini_thumbnail.0
5178778884CBCEA48662CBA719B13EBA.mini_thumbnail.0  CC5DFF1056DC20B16E210582CA79EBD3.mini_thumbnail.0
52BFB1FA8BCA1F49B9CDA95FCD52.mini_thumbnail.0  CC8229C0676C7C4182F3758F2408201.mini_thumbnail.0
530FF04DBA741F928CB9F3218E723B2.mini_thumbnail.0  CD2956BD99CD42822BA1975FACA2825.mini_thumbnail.0
533B37F526F7E6159227D3E7001626.mini_thumbnail.0  CDF5E041F81FE05676F949887E0884F8.mini_thumbnail.0
```

570CF347A90DC72E24FE8BE03D9BC344.mini_thumbnail.0 CE2FC2250B5A4E9FBABBA704B0D24C44.mini_thumbnail.0
59A6E9759P3C0AD76598DFC859882F0.mini_thumbnail.0 CE90DB96C303B2E3B1B31FD007601B22.mini_thumbnail.0
5661F36747704E12C57B4CAA1B6A6E790.mini_thumbnail.0 CF24D351D65B18E9EC2A34013C11C3F0.mini_thumbnail.0
56620F91252305886409E3B34D8984C23.mini_thumbnail.0 CF4F54FFEC08451D5444202698F71005.mini_thumbnail.0
61A8EF8078B67528AC7BC2700C215356.mini_thumbnail.0 CF5EC282086DB9A9F3520AA48F8E73A4.mini_thumbnail.0
65208154E8PDDC19413E6B8532348F1.mini_thumbnail.0 D02E7D68169663B378221986B58F2C22.mini_thumbnail.0
6873768A482A024504519CF9FA088A0A3.mini_thumbnail.0 D536FA626A06E1E7DF4F51219ADA90.mini_thumbnail.0
6963C5B72B90A01874D412E1FE011999.mini_thumbnail.0 D537DDF715337B45C7371EC13C4DBEC9.mini_thumbnail.0
69D1CDB3463622A6F64B1C313B35A67A.mini_thumbnail.0 D8678E1BA54E65AF9F7A2049962AF2B.mini_thumbnail.0
69F4E1CFA38B4B26536574A9C7DF740D.mini_thumbnail.0 D96430756C86A524BDBC476AD6AB92F5.mini_thumbnail.0
6C870D5C3603261AD22082AA02D28E95.mini_thumbnail.0 DB098C33C8A8C586D1F504A0446D4F40.mini_thumbnail.0
6F753427146FCA8AF66F3A2145FF7092.mini_thumbnail.0 DB82D22D59AC1B8BF6E85CE298007EA.mini_thumbnail.0
71D1D511F5E2CD5BFC950EA537F4DA60.mini_thumbnail.0 DC12537C2E3887CDBB97BA1BB5548E53.mini_thumbnail.0
722AAC10EAF08857A61BD6D9D75C5B5C8.mini_thumbnail.0 E1D59F66847AD666A80B9F69C6FEA36.mini_thumbnail.0
7597DDC26D38D2267241888E11FAA375.mini_thumbnail.0 E3126AA3D1A754C6D4FE2246BD4DEFA.mini_thumbnail.0
7619BBF2817608FBB48E4C823E7682D8.mini_thumbnail.0 E4BD0E725C101BB2392431F8155E4F41.mini_thumbnail.0
7C5E2ED045330BD9BAE55148A530DA26.mini_thumbnail.0 E5872481DD5CB57E9B10968BCC91E1F7.mini_thumbnail.0
7CFD602B4B0928C4F6D23CA65B6AAE4.mini_thumbnail.0 E820567B2C706892BC3F1646DED324E5.mini_thumbnail.0
7DA563B30344BE91AC37174FA536D3E0.mini_thumbnail.0 EA5E0D73A6D384D32C812D3BFA5F0DF5.mini_thumbnail.0
7DCBFDF520F5C66A36AFC6A584F9160.mini_thumbnail.0 EACD876CD63B944386C78E0A019CB920.mini_thumbnail.0
7EB023C1DBFC9C24BBA8B6BDFDE29DD8.mini_thumbnail.0 ECB901840C609AA21A4CFCC949C7E69.mini_thumbnail.0
80902D996CBDEDD58A3AF378267D9A15.mini_thumbnail.0 EE33BE6716BF4144B3F42896B8E634C.mini_thumbnail.0
81E09AC1D8C1F04C369456E89441339C.mini_thumbnail.0 F01C4D657A06F6EB334A8FCDCB42294.mini_thumbnail.0
81FFBF1B1DF42859F70EF81AFCE6A6393.mini_thumbnail.0 F0CEEFA4C29BAA88857FCDA58053C2955.mini_thumbnail.0
8269A9CA16C83BFBFC54B0120F7B53D07.mini_thumbnail.0 F1206ECD83AA771ECCDD2B067C101321.mini_thumbnail.0
82A7D6260714BC5920796434DC89F117.mini_thumbnail.0 F12E19434C96A2BC7EA4726985A3D3CB.mini_thumbnail.0
8418F44B7F6624DA8BE991DA1BF244F6.mini_thumbnail.0 F2E5B8373C2C2A497997644122261C.mini_thumbnail.0
88D9658CA49C72BA5570B1CDBE5847FBB.mini_thumbnail.0 F8809CB6474EADDB085970E0B35E744.mini_thumbnail.0
892E6788BE56A05D8DB394EFD7F351A.mini_thumbnail.0 FC214E1093466A6AF42C2E926FCE5AAB.mini_thumbnail.0
897E5846B19448289AB684DB624F89C1.mini_thumbnail.0 FDEF4F656732F5E5FFB2B0DD3F5195D.mini_thumbnail.0
8C8A5338AD795717DA5F2D9D45B876B.mini_thumbnail.0 FFAD7C5AD6EA621DA6505B55E1DEDEA.mini_thumbnail.0

./files/file_manager/memories_print_thumbnail:

./files/file_manager/memories_thumbnail:

0228660519E053AF8FBD40C82257D5FB.thumbnail.0 52FD981DFEED24AC8CA7CA9BDE2622D7.thumbnail.0
A3652D11A625730DA7E4F04A8C62CE1C.thumbnail.0
057C119889FC146EEFB7A753B771DCB.thumbnail.0 547A731CB084FF831A38F295C8DCDB8.thumbnail.0
A732840AC345D89F7D7F694204BE27BB.thumbnail.0
064FBB1F63925F349410B8BD38F9F339.thumbnail.0 5485C46CCC43B777A02563ECAD445.thumbnail.0
A7BFBC99EB6D83B087E9D93C5E45CA3.thumbnail.0
069C280ABE4CA581CA4831F4CAE1E257.thumbnail.0 5569A3C2083885E5B333B09BE0B3916.thumbnail.0
A7F653B78995B989825FFA4DF2C3A083.thumbnail.0
0AAAAA17CF42235EC8AD7E53A4ABB31.thumbnail.0 557AC50636A2F996EB392BF0717BDE3.thumbnail.0
A99F5713209239BF30C6EA73EBFB6683.thumbnail.0
0EC4C34BE81422D7D409924631880049.thumbnail.0 558CE4623F03EE2C50E1352D2A96D8C3.thumbnail.0
A63153EB101CB09DB71640329988D58.thumbnail.0
0F4EF052A445C8CF4731D2F5397D12C1.thumbnail.0 5884AF8A52B79101629238E44A79EF71.thumbnail.0
AD0B4EA1BDC4BE1EB15A637B2E088E0.thumbnail.0
12815E1CA70B983F7DC5F0B642708895.thumbnail.0 5974106ED1F5681805D5D29D3F986397.thumbnail.0
AEC52CC15B320F58FB0B53374A047390.thumbnail.0
15AFDD73AB4C07C99F16B93E892A60C3.thumbnail.0 6233D34BD331A5CB57D571CB71268EB3.thumbnail.0
B3159817FEC06139600BC7634F0E2507.thumbnail.0
15D832F7A17AE89B97DEBEE1733B0FC4.thumbnail.0 6478904B1855EF779776D888D820B8.thumbnail.0
B3484C1D7A053895A062C5B5B4EFC542.thumbnail.0
1765AE77A44002873BD87735F4264D0D.thumbnail.0 65C9A9FFC31C849FE4D51246C76EDA8E.thumbnail.0
B4C3B8EABEBF27B9CB26720D25C21BC9.thumbnail.0
19D0F40E4F0131E18C27BF32C506FC31.thumbnail.0 6684FC8EB5435C2FA2AA1B1F29BAE18F.thumbnail.0
B4EE5179E8BB1E8883BDADECAA41216B.thumbnail.0
1A19C77E6FB006E38FE555C6AC3CF641.thumbnail.0 6700F217E306EDA5B2A431C75F18C64F.thumbnail.0
B54EF71AA2DCDB263E51BEB32BAF761.thumbnail.0
1B86E1C82BCE2D267819ACB6CFC050C.thumbnail.0 674685E1ABD2C22E1EF78330562EF58A.thumbnail.0
B6EFD3C0F29F4EF7A9291C23C8F9D1C5.thumbnail.0
1D3F4393B4CD67A026FA3C621C443CC.thumbnail.0 69A964437158312C061F0E04E14179A2.thumbnail.0
B9FCF45AA6998968D246CD1536F77485.thumbnail.0
1DCA0AEF70513FA317B8E5482809C63.thumbnail.0 6D0938400277D31AF7F8392A5B288E58.thumbnail.0
BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
1E806D39F0E88078F2AF1607713752B3.thumbnail.0 6EA9C185111559A9271BE28854B3F0A2.thumbnail.0
BD79E05C338E646DEB47B9B28417C2D.thumbnail.0
1FCE740DD8CF390A90636B55C3CA370B.thumbnail.0 70A0E3C73CD81F373CED5A001A1C0B4D.thumbnail.0
BEFE851B4ED673FCCD0789CAB1943990.thumbnail.0
22F0CBF4EA5A668AE9F2D9EA42F2579.thumbnail.0 7340873AEC065ED613991FD8D06AA191.thumbnail.0
C0EB556720D08D571637012B70124363.thumbnail.0
25BD771AF7AF0A854AA9D7069D6FC979.thumbnail.0 7412807E4BB8FB2101839F5BE524377.thumbnail.0
C40A17CFDF777D2EE8F260FD977DA92B.thumbnail.0
2973175BF2C8DBF78F23A8AF856B002.thumbnail.0 74A31ADE504A60F3BB97879EF4E6471.thumbnail.0
C517F36553726600B5C5ED2480AE5B1B.thumbnail.0
2A2BDDFEA6677F1281C63B336E115F76.thumbnail.0 75A83B3A1373B1CB8FA8C18F41614005.thumbnail.0
C9CBEC40148F7AD621562F18CEE5F08.thumbnail.0
2DD87BA0E11A3423AA6F85C7C1D2CBD5.thumbnail.0 75F966B714B9A24C4A0EADBC3397DA0.thumbnail.0
CABD321198E3284726A9D414A020C6C7.thumbnail.0
2E55572BBF2CC616ACCFB4A1EBC362D.thumbnail.0 7787E46C0042B2B733C2166CBFB63E8.thumbnail.0
D0126AA91F8945EE7A3C3315AC672949.thumbnail.0
2F0503AF56FD4AD5C51D57C156A55BC2.thumbnail.0 77F6561B2DC9C3A5B9739F0E5E8A768D.thumbnail.0
D03EE10EF8CD989F40E41B90932AB956.thumbnail.0
3007023AED31C27100E049570C93BC39.thumbnail.0 8048363EA9155270B821550FB12375E2.thumbnail.0
D20E3D26F9EAC943DA3320E721C25CA8.thumbnail.0
30D2E4A641FD3DB3DD612FB18FA77AA8.thumbnail.0 80A4D8EE249654A62D3EEFA8FB749890.thumbnail.0
D357E7E4D0CACC092CCBF8C4F3D808BB.thumbnail.0
30E180C637D9E68EF48E6D286D4FAB73.thumbnail.0 8286AD7C1C91043A049FE9797E026A41.thumbnail.0
D4CB4F4296A100FE30D053463B0DBB8.thumbnail.0
3144193361CA1BAC9E6CC6BBD69CF17A.thumbnail.0 83DE5D47573D4A3B3B9828B8D5CEBF4E.thumbnail.0
D6B9502A8985DDA792589BEA2E26324.thumbnail.0
319E9A56B66AE0683DEA678759068223.thumbnail.0 8612A2D89034FAA0A3AE8AF30334BF32.thumbnail.0
D733F19801C3F2DED46E2000F038DA40.thumbnail.0
3294D79258C7CB01EAB06AF3248BFA8.thumbnail.0 88814CF30C3ADE0782A7A56781C2D695.thumbnail.0
D89D5C717C289535A15F858B198655BF.thumbnail.0
337BE3CA984984780722B189E3F1DF3.thumbnail.0 88FCC3459B9D445CC46C16169E305DC.thumbnail.0
DAAD7F59D87BAC6907964795E901DF3.thumbnail.0
33A448AB3FBA3A7BAE740BDDC1DE99.thumbnail.0 8A236E17770EEBB3CE16B6792F68C85A.thumbnail.0
EOAA07C8F98E2BCC5AE7C3EB984219.thumbnail.0

```

39957A6980FF4634B9BC085EFD8FF7D2.thumbnail.0 8A6E2257550E53C8539B0B56D70ADA58.thumbnail.0
E18B7B0EF3EF7ABE51B9BCC097F36E2D.thumbnail.0
3EBBD273A81A0F123A2D30924840DE2.thumbnail.0 8ACE100817E7E30B176AF80E814AEC8B.thumbnail.0
E74200F6ADECE8CD7EFEB6850945BEDE3.thumbnail.0
3F903A542BD4ECEA2B02C54E418C812.thumbnail.0 8C1EE510C301588F32D6F4930CA1CAFF.thumbnail.0
EAF97CAEFC08F8F2E24F17B15DBEA52.thumbnail.0
418962D85593EC889A14FDC7A516CA04.thumbnail.0 8C3B8D4B7B0C2AF82AEF3F0E2F5AEC4B.thumbnail.0
EE7D5ECDBD72F7CD3022F7DFACF985A8.thumbnail.0
425C1BEDB29CBB10869EBC737E5924C.thumbnail.0 8C5D1530C83A850B79CB9DFB9CC5594D.thumbnail.0
EF1AF38104CEE07C30ABD17098D6C5E.thumbnail.0
468E76FF19E65446D77CA787CB64AB23.thumbnail.0 8E08E426DF2DF6515897D6A42CDB6A21.thumbnail.0
F1ECD641AC25658DD96D4DD750A4ABD9.thumbnail.0
471E6C8B78EA8111F4910F4FEA5703E4.thumbnail.0 8EE8CE9030F9C68F281F21D3EBBEBA44.thumbnail.0
F45546530B3A0679C96699265472FFA6.thumbnail.0
48727CE45495E2A9DA4A96EDA2623928.thumbnail.0 8F3040ACAD8CF80D01694E31AB8CE230.thumbnail.0
F5FB12731FD4AEA3CDF3E16820588663.thumbnail.0
48C525AFEBE3225C99CFBCE14D4961.thumbnail.0 8F744482984DBEE3F8DAA77D1EF97934.thumbnail.0
F659EF7EDB516E64DF7C564754C9FBE0.thumbnail.0
48D79B90CEA65AAA93DDE01C0E61A80C.thumbnail.0 92B2A0FB74D81B8ACFE06222986CBB50.thumbnail.0
F9682046BDD23832CCDAD461D84CAC5.thumbnail.0
49175B6099BD3DFC5A2C94A3CF52114D.thumbnail.0 93A6E9E8C9BE8EFF04F0453E1D7639B.thumbnail.0
FAE983A9523445649F8966EEDF9AE675.thumbnail.0
4A4F17D3439E94E5B99AF3E4DCD7C9DF.thumbnail.0 94B45F93208E6F87BA752F6811E57712.thumbnail.0
FE1855675153CA79EDC8C767FE3BAFDD.thumbnail.0
4C4E9F78AB4FC4B9997D7271E86259A.thumbnail.0 9530AA55FDA69CD0E2043664FEB53712.thumbnail.0
FBEE233A96F9F06FD5BE6B0903E09D49.thumbnail.0
4F446F252FC4E36C9335C2807CA2D6F9.thumbnail.0 97D687C37D196FD1D3EBB4B3EA8EB870.thumbnail.0
FCE70EF7A2981E8C94C47227E994E2B2.thumbnail.0
51BEC8B8009D700B7D07FCF4F311D0BF.thumbnail.0 980793CDDF59EAFB07B05972DA8583CE.thumbnail.0
FDD3D6A21940DADB3787A431AF84DC1D.thumbnail.0
521AA4839FFDAB69BB038357036EC3C.thumbnail.0 9C7C5A53DD112A7E01FDD26E1F12A8AF.thumbnail.0
FED260DF6C72CE3D2DCEC437E7662CCA.thumbnail.0
523066F90AAA043DB21D4601A20794DB.thumbnail.0 9D655FF895C4D7C3C0406E1EFBAE53DE.thumbnail.0
52EDA3534417AB63DF3AA9D1DF153356.thumbnail.0 A16183682F1D29A41EE7D539E1FAF1D0.thumbnail.0

./files/file_manager/snap:

./files/file_manager/spectacles:

./files/file_manager/spectacles-files:

./files/file_manager/user_generated_assets:

./files/gallery:
files thumbnails

./files/gallery/files:

./files/gallery/thumbnails:

./shared_prefs:
APP_START_EXPERIMENT_PREFS.xml      androidx.work.util.preferences.xml
BLIZZARD_SAMPLING_PREFS.xml         channel_persistent_store.xml
BLIZZARD_V2_ACTIVATION.xml          com.crashlytics.preferences.xml
Composer.xml                          com.google.android.gms.appid.xml
DefaultOneTapLoginDialogManager.xml  com.snapchat.android.analytics.framework.com.snapchat.android.xml
Laguna.xml                           com.snapchat.android.preferences.xml
LanguageSettings.xml                dataMigrationConfig.xml
LoginSignupStore.xml                 hardware.gpu.com.snapchat.android.xml
MDP_EXO_PLAYER_CACHE_SIZE_PREF.xml  identity_persistent_store.xml
SharedPrefsOneTapLoginUserStore.xml  io.fabric.sdk.android.fabric:axxq.xml
TwitterAdvertisingInfoPreferences.xml user_device_identity_keys.xml
UUID_STORE.xml                       user_session_shared_pref.xml
WebViewChromiumPrefs.xml

```

Figure 65. Forensic exam X: Pertinent directory results excerpted from ADB Shell recursive directory tree listing as rooted superuser of sandbox smartphone (Xiaomi Redmi Note 7)

Listing Snapchat’s directory tree recursively provided a snapshot into what directories likely held the biometric assets captured by the smart eyewear. Some directories expected to hold biometric assets were found empty, including but not limited to the following:

- memories_print_thumbnail
- snap
- spectacles
- spectacles-files
- user_generated_assets
- gallery
- /gallery/files
- /gallery/thumbnails

Determined the number of files within Snapchat APK's select directories likely holding pertinent biometric data assets, see figure x.

```
lavender:/data/data/com.snapchat.android/databases # ls | wc -l
42

lavender:/data/data/com.snapchat.android/files/file_manager/memories_thumbnail # ls | wc -l
151

lavender:/data/data/com.snapchat.android/files/file_manager/memories_mini_thumbnail # ls | wc -l
164
```

Figure 66. Forensic exam X: As rooted superuser of sandbox smartphone, determined number of files within Snapchat APK's select directories likely holding pertinent biometric assets.

The directory entitled “ /files/file_manager/memories_thumbnail ” held 151 files with “thumbnail” in their filename.

The directory entitled “ /files/file_manager/memories_mini_thumbnail ” held 164 files with “mini_thumbnail” in their filename.

Relative to the 164 files manually examined within Snapchat's “Memories” storage (Figure x (c)), it is unclear why 13 of the 164 total files stored in Snapchat's cloud database were not made available as “thumbnail” files within the “/files/file_manager/memories_thumbnail” directory.

It is also unclear why only files entitled “thumbnail” and “mini_thumbnail” are stored and made available via the cloud, as opposed to the original photographs and videos captured, stored, and transferred by the smart eyewear.

6.2.11 Forensic exam XI: Rooted extraction via ADB pull

Forensic exam XI highlights a scenario wherein an investigator attempts to extract the smart eyewear personal data directory (/data/data/com.snapchat.android) via ADB Pull after acquiring access to a smart eyewear owner's user account on a rooted sandbox smartphone within Forensic exam X.

The researcher, as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner.

The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices. The forensic investigator only possesses administrative privilege to their sandbox smartphone. Chain of custody, network access, system administration status parallel Forensic exam X, see Table x.

6.2.11.1 Forensic exam XI: Methods and tools

Forensic exam XI is contingent on Forensic exam X being performed prior, as such, all methods and tools used prior are also required in order to perform this examination.

ADB pull of the “com.snapchat.android” file, located on the rooted sandbox smartphone (Xiaomi Redmi Note 7), was performed via cmd.exe on a Windows 10 laptop:

```
adb pull -a /data/data/com.snapchat.android C:\path_to_new_file
```

Figure x. Forensic exam XI: ADB Pull of com.snapchat.android directory on rooted sandbox smartphone, while logged into smart eyewear user account

6.2.11.2 Forensic exam XI: Analysis, results, and discussion

The ADB Pull extraction method resulted in the following errors, see Figure x below:

```
>adb pull -a /data/data/com.snapchat.android C:\path_to_new_file
adb: error: failed to create directory
'C:\path_to_new_file\com.snapchat.android\files\.Fabric\io.fabric.sdk.android:fabric\':
Invalid argument

>adb pull -a /data/data/com.snapchat.android/shared_prefs C:\path_to_new_file
adb: error: cannot create
'C:\path_to_new_file\shared_prefs\io.fabric.sdk.android:fabric:axxq.xml': No such file or
directory

>adb pull -a
/data/data/com.snapchat.android/shared_prefs/io.fabric.sdk.android:fabric:axxq.xml
C:\path_to_new_file
adb: error: cannot create 'C:\path_to_new_file\io.fabric.sdk.android:fabric:axxq.xml': No
such file or directory
```

Figure x. Forensic exam XI: Excerpted ADB Pull errors encountered on rooted sandbox smartphone, while logged into smart eyewear user account

The initial error listed above temporarily prevented acquiring access to the entire com.snapchat.android directory. To resolve this hindrance, all files were ADB pulled separately, excluding error prone files from each ADB Pull attempt after heeding warning messages, see Figure x below for further detail on data extraction:

```
>adb pull -a /data/data/com.snapchat.android/files/Snapchat C:\path_to_new_file
/data/data/com.snapchat.android/files/Snapchat/: 1 file pulled, 0 skipped. 0.0 MB/s (141
bytes in 0.006s)
>adb pull -a /data/data/com.snapchat.android/files/crash C:\path_to_new_file
/data/data/com.snapchat.android/files/crash/: 0 files pulled, 0 skipped.
>adb pull -a /data/data/com.snapchat.android/files/gallery C:\path_to_new_file
/data/data/com.snapchat.android/files/gallery/: 0 files pulled, 0 skipped.
>adb pull -a /data/data/com.snapchat.android/files/lookserly_user_data_cache
C:\path_to_new_file
/data/data/com.snapchat.android/files/lookserly_user_data_cache/: 0 files pulled, 0 skipped.
>adb pull -a /data/data/com.snapchat.android/files/splitcompat C:\path_to_new_file
/data/data/com.snapchat.android/files/splitcompat/: 0 files pulled, 0 skipped.
>adb pull -a /data/data/com.snapchat.android/files/blizzardv2 C:\path_to_new_file
/data/data/com.snapchat.android/files/blizzardv2/: 22 f...es pulled, 0 skipped. 0.3 MB/s
(154116 bytes in 0.471s)
>adb pull -a /data/data/com.snapchat.android/files/file_manager C:\path_to_new_file
/data/data/com.snapchat.android/files/file_manager/: 41...pulled, 0 skipped. 1.4 MB/s
(46625152 bytes in 31.499s)
```

```
>adb pull -a /data/data/com.snapchat.android/files/lookserty_sdk C:\path_to_new_file
/data/data/com.snapchat.android/files/lookserty_sdk/: 1 file pulled, 0 skipped. 0.1 MB/s (4096
bytes in 0.058s)
>adb pull -a /data/data/com.snapchat.android/files/scheduledLenses.proto C:\path_to_new_file
/data/data/com.snapchat.android/files/scheduledLenses.p...e pulled, 0 skipped. 10.8 MB/s
(183491 bytes in 0.016s)
>adb pull -a /data/data/com.snapchat.android/files/streaming C:\path_to_new_file
/data/data/com.snapchat.android/files/streaming/: 1 file pulled, 0 skipped.
>adb pull -a
/data/data/com.snapchat.android/files/.Fabric/com.crashlytics.sdk.android.crashlytics-core
C:\path_to_new_file
/data/data/com.snapchat.android/files/.Fabric/com.crashlytics.sdk.android.c...ytics-core/:
210 files pulled, 0 skipped. 0.0 MB/s (161894 bytes in 3.116s)
>adb pull -a /data/data/com.snapchat.android/files/.Fabric/com.crashlytics.settings.json
C:\path_to_new_file
adb: error: failed to stat remote object
'/data/data/com.snapchat.android/files/.Fabric/com.crashlytics.settings.json': No such file
or directory
>adb pull -a
/data/data/com.snapchat.android/files/.Fabric/io.fabric.sdk.android:fabric/com.crashlytics.se
ttings.json C:\path_to_new_file
/data/data/com.snapchat.android/files/.Fabric/io.fabric.sdk.android:fabric/...cs.settings.jso
n: 1 file pulled, 0 skipped. 0.0 MB/s (1553 bytes in 0.062s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/APP_START_EXPERIMENT_PREFS.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/APP_START_EXPERIMENT_PREFS.xml: 1 file pulled, 0
skipped. 0.0 MB/s (772 bytes in 0.051s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/BLIZZARD_SAMPLING_PREFS.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/BLIZZARD_SAMPLING_PREFS.xml: 1 file pulled, 0
skipped. 0.0 MB/s (120 bytes in 0.005s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/BLIZZARD_V2_ACTIVATION.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/BLIZZARD_V2_ACTIVATION.xml: 1 file pulled, 0
skipped. 0.0 MB/s (110 bytes in 0.053s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/Composer.xml C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/Composer.xml: 1 file pulled, 0 skipped. 0.0 MB/s
(144 bytes in 0.006s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/DefaultOneTapLoginDialogManager.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/DefaultOneTapLoginDialogManager.xml: 1 file
pulled, 0 skipped. 0.0 MB/s (167 bytes in 0.008s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/Laguna.xml C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/Laguna.xml: 1 file pulled, 0 skipped. 0.0 MB/s
(680 bytes in 0.049s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/LanguageSettings.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/LanguageSettings.xml: 1 file pulled, 0 skipped.
0.0 MB/s (65 bytes in 0.004s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/LanguageSettings.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/LanguageSettings.xml: 1 file pulled, 0 skipped.
0.0 MB/s (65 bytes in 0.004s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/LoginSignupStore.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/LoginSignupStore.xml: 1 file pulled, 0 skipped.
0.0 MB/s (65 bytes in 0.048s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/MDP_EXO_PLAYER_CACHE_SIZE_PREF.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/MDP_EXO_PLAYER_CACHE_SIZE_PREF.xml: 1 file
pulled, 0 skipped. 0.0 MB/s (134 bytes in 0.057s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/SharedPrefsOneTapLoginUserStore.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/SharedPrefsOneTapLoginUserStore.xml: 1 file
pulled, 0 skipped. 0.0 MB/s (118 bytes in 0.004s)
>adb pull -a
/data/data/com.snapchat.android/shared_prefs/TwitterAdvertisingInfoPreferences.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/TwitterAdvertisingInfoPreferences.xml: 1 file
pulled, 0 skipped. 0.1 MB/s (213 bytes in 0.004s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/UUID_STORE.xml C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/UUID_STORE.xml: 1 file pulled, 0 skipped. 0.0
MB/s (149 bytes in 0.103s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/WebViewChromiumPrefs.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/WebViewChromiumPrefs.xml: 1 file pulled, 0
```

```

skipped. 0.0 MB/s (127 bytes in 0.008s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/androidx.work.util.preferences.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/androidx.work.util.preferences.xml: 1 file
pulled, 0 skipped. 0.0 MB/s (136 bytes in 0.004s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/channel_persistent_store.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/channel_persistent_store.xml: 1 file pulled, 0
skipped. 0.0 MB/s (124 bytes in 0.051s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/com.crashlytics.preferences.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/com.crashlytics.preferences.xml: 1 file pulled, 0
skipped. 0.0 MB/s (251 bytes in 0.048s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/com.google.android.gms.appid.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/com.google.android.gms.appid.xml: 1 file pulled,
0 skipped. 0.3 MB/s (2514 bytes in 0.007s)
>adb pull -a
/data/data/com.snapchat.android/shared_prefs/com.snapchat.android.analytics.framework.com.sna
pchat.android.xml C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/com.snapchat.android.analytics...pchat.android.x
ml: 1 file pulled, 0 skipped. 0.1 MB/s (971 bytes in 0.007s)
>adb pull -a
/data/data/com.snapchat.android/shared_prefs/com.snapchat.android.preferences.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/com.snapchat.android.preferences.xml: 1 file
pulled, 0 skipped. 0.0 MB/s (65 bytes in 0.043s)
>adb pull -a
/data/data/com.snapchat.android/shared_prefs/com.snapchat.android.preferences.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/com.snapchat.android.preferences.xml: 1 file
pulled, 0 skipped. 0.0 MB/s (65 bytes in 0.004s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/dataMigrationConfig.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/dataMigrationConfig.xml: 1 file pulled, 0
skipped. 0.0 MB/s (65 bytes in 0.005s)
>adb pull -a
/data/data/com.snapchat.android/shared_prefs/hardware.gpu.com.snapchat.android.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/hardware.gpu.com.snapchat.android.xml: 1 file
pulled, 0 skipped. 0.1 MB/s (280 bytes in 0.004s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/identity_persistent_store.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/identity_persistent_store.xml: 1 file pulled, 0
skipped. 0.0 MB/s (825 bytes in 0.049s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/user_device_identity_keys.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/user_device_identity_keys.xml: 1 file pulled, 0
skipped. 0.1 MB/s (531 bytes in 0.007s)
>adb pull -a /data/data/com.snapchat.android/shared_prefs/user_session_shared_pref.xml
C:\path_to_new_file
/data/data/com.snapchat.android/shared_prefs/user_session_shared_pref.xml: 1 file pulled, 0
skipped. 0.0 MB/s (1000 bytes in 0.054s)

```

Figure 68. Forensic exam XI: Error prone file workaround - Separate ADB Pulls on rooted sandbox smartphone, while logged into smart eyewear user account

6.2.12 Forensic exam XII: Rooted extraction via TWRP copy and ADB backup

Despite gaining administrative root access to the sandbox smartphone (Xiaomi Redmi Note 7), creating an ADB Backup of the com.snapchat.android directory still proved cumbersome due to the allowBackup="false" flag set within the AndroidManifest.xml file of the 10.77.5.0 version of Snapchat's APK.

Forensic exam XII highlights a scenario wherein an investigator attempts to extract the smart eyewear personal data directory (/data/data/com.snapchat.android) via ADB

Backup after acquiring access to a smart eyewear owner’s mobile app user account on a rooted sandbox smartphone within Forensic exam X.

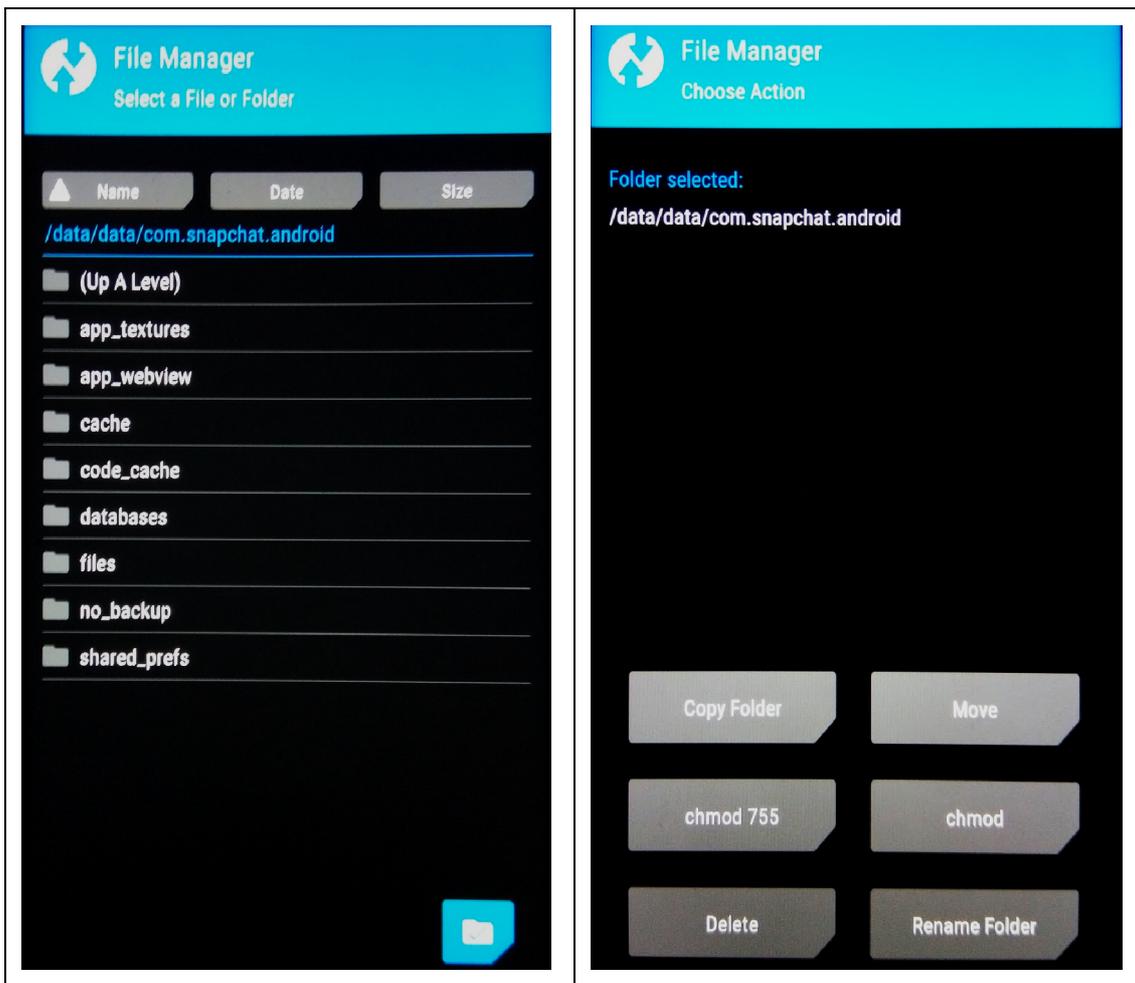
The researcher, as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner.

The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices. The forensic investigator only possesses administrative privilege to their sandbox smartphone. Chain of custody, network access, system administration status parallel Forensic exam X, see Table x.

6.2.12.1 Forensic exam XII: Methods and tools

Forensic exam XII is contingent on Forensic exam X being performed prior, as such, all methods and tools used prior are also required in order to perform this examination.

In order to bypass the allowBackup=“false” restriction set within the smart eyewear APK’s AndroidManifest.xml file, a copy of the “com.snapchat.android” directory was created within TWRP and saved outside the /data/data directory, see Figure X (a)(b)(c)(d) for procedure.



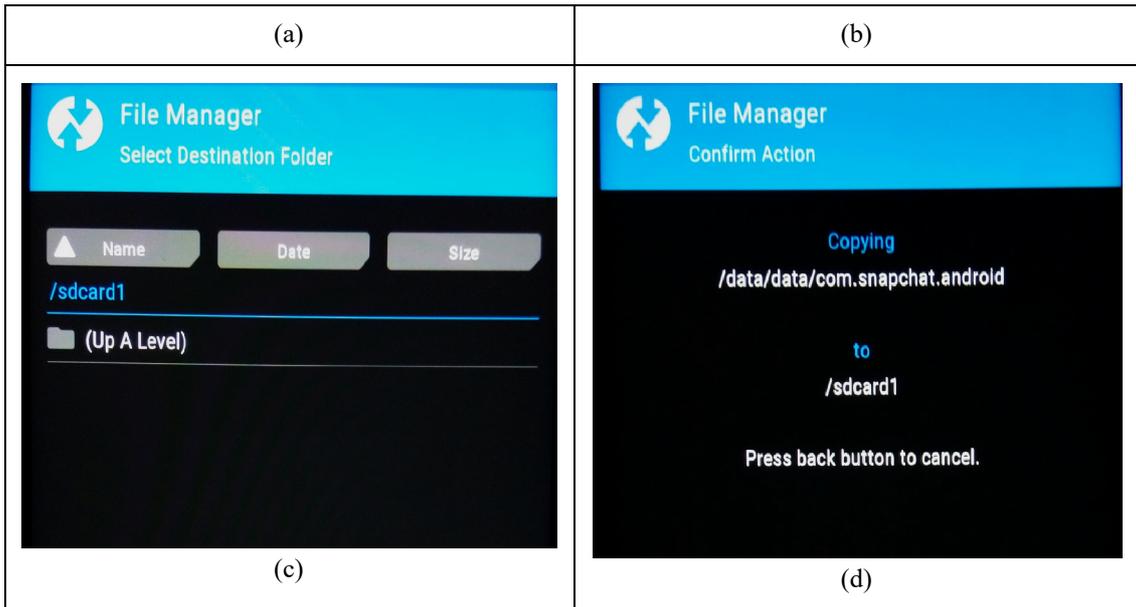


Figure 69. Forensic exam XII: TWRP procedure to copy com.snapchat.android directory to external storage (a) Located and selected com.snapchat.android file (b) Selected Action: Copy Folder (c) Selected Destination Folder: /sdcard1 (d) Confirmed Action

After a copy of the “com.snapchat.android” directory was made within TWRP and saved external to the /data/data directory, ADB Backup was performed as follows:

```
>adb devices -l
List of devices attached
2da4da73          device product:lavender_eea model:Redmi_Note_7
device:lavender transport_id:9

>adb backup -apk -shared -all -f "C:\path_to_new_file\backup.ab"
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

>java.exe -jar "C:\abe.jar"  unpack "C:\path_to_new_file\backup.ab"
"C:\path_to_new_file\backup.tar"
```

Figure 70. Forensic exam XII: ADB Backup procedure on rooted sandbox smartphone logged into smart eyewear cloud account

6.2.12.2 Forensic exam XII: Analysis, results, and discussion

Figure x illustrates a failed ADB Backup attempt on the rooted sandbox smartphone after logging into the smart eyewear mobile application.

Name	Date created	Size	Type
 backup.ab	9/21/2020 4:33 AM	0 KB	AB File

Figure 71. Forensic exam XII: ADB Backup failure after rooting smartphone due to Android Manifest control set

As mentioned prior, the allowBackup="false" flag set within the AndroidManifest.xml file continued to block access to the "/data/data/com.snapchat.android" directory when attempting to create an ADB Backup of the sandbox smartphone and transfer the file to laptop; only an empty .ab file was created (Figure x)

Figure x. depicts the successful ADB Backup of the "com.snapchat.android" TWRP directory copy, see figure x.

Name	Date created	Type	Size	Tags
backup	9/22/2020 8:19 PM	File folder		
backup.ab	9/22/2020 8:13 PM	AB File	223,884 KB	
backup.tar	9/22/2020 8:19 PM	TAR File	311,558 KB	

Figure x. Forensic exam XII: Successful ADB Backup of com.snapchat.android TWRP directory copy from rooted sandbox smartphone logged into smart eyewear cloud account

It is possible to change an APK's allowBackup="false" flag to "true" [232] [233] [234] within an APK's AndroidManifest.xml file; however, this action would alter the integrity of the APK and the signed cryptographic hash provided by the development firm, Snap Inc. and therefore was avoided.

The ADB Backup extraction method resulted in truncating select file names and extensions within the following two directories:

"com.snapchat.android/files/file_manager/memories_thumbnail" (Figure X)

"com.snapchat.android/files/file_manager/memories_mini_thumbnail" (Figure X)

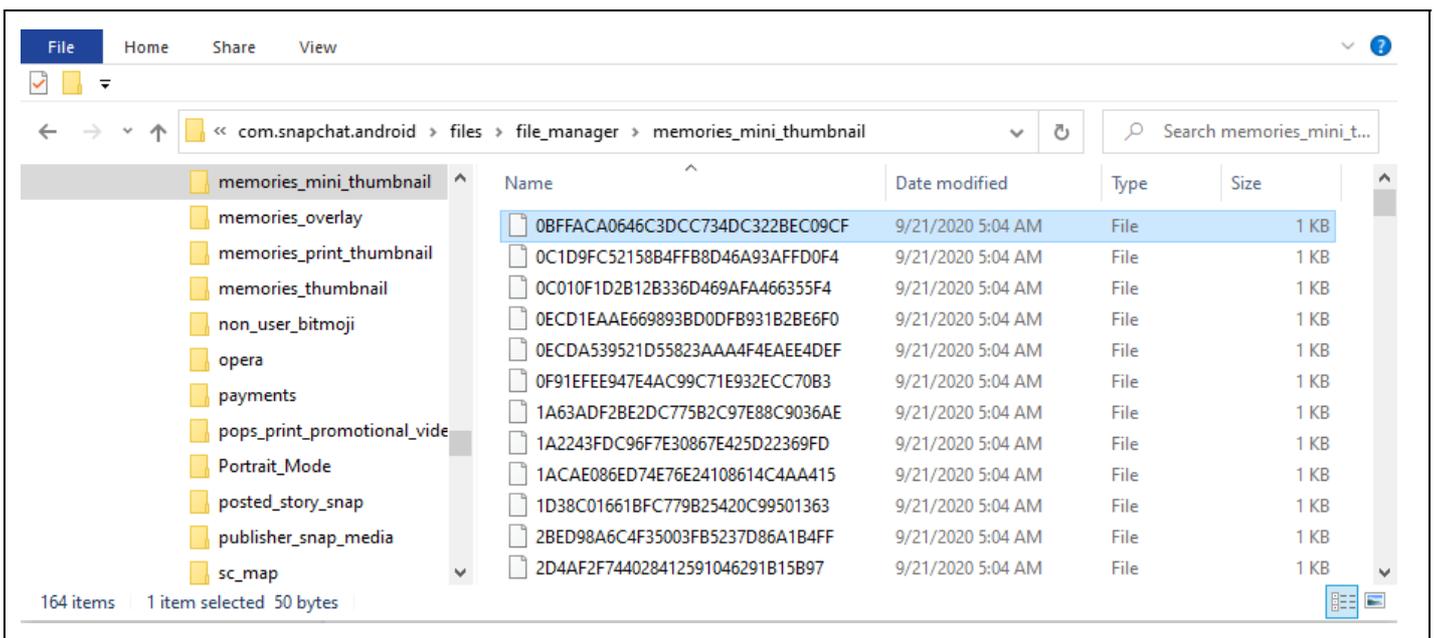


Figure 73. Forensic exam XII: Truncation of file names and extensions within "memories_mini_thumbnail" directory after TWRP copy/ADB Backup method (Figure X)

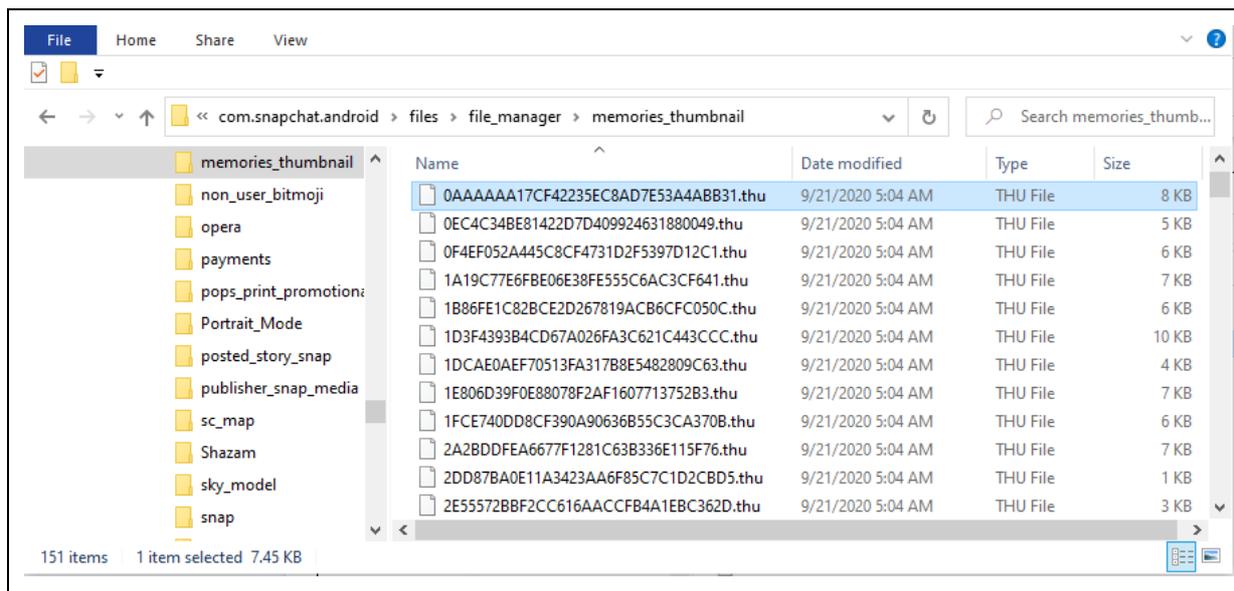


Figure 74. Forensic exam XII: Truncation of file names and extensions within “memories_thumbnail” directory after TWRP copy/ADB Backup method (Figure X)

6.2.13 Forensic exam XIII: Rooted physical extraction via Axiom Magnet Process and Examine

Manual and logical extractions made within Forensic exams X-XII were not capable of acquiring data from unallocated space, also known as deleted files. Forensic exam XIII attempts to acquire a complete bit-by-bit copy, or full image, of the sandbox smartphone in an attempt to extract any data missed within the logical extractions performed prior, inclusive of deleted data from unallocated space.

The researcher, as a participant observer of the smart eyewear ecosystem, acts as both the forensic investigator and the smart eyewear/smartphone/data owner.

The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices. The forensic investigator only possesses administrative privilege to their sandbox smartphone. Chain of custody, network access, system administration status parallel Forensic exam X, see Table x.

6.2.13.1 Forensic exam XIII: Methods and tools

Forensic exam XIII is contingent on Forensic exam X being performed prior, as such, all methods and tools used prior are also required in order to perform this examination.

In addition to all the tools and methods used within Forensic exam X, Magnet Axiom Process and Magnet Axiom Examine were used to extract and analyze data from the rooted sandbox smartphone. (Table ?)

Access to the Magnet Axiom commercial software was made possible via an OpenVPN connection to a server hosting TalTech’s acquisition of the software.

Table 45. Forensic exam XIII: Additional tools used for rooted physical extraction via Axiom Magnet Process and Examine.

Device	Software and peripherals
Laptop	<ul style="list-style-type: none"> - Magnet Axiom Process v4.7.0.22371 - Magnet Axiom Examine v4.7.0.22371 - USB cable Type A & Micro-B 5 pin connectors to connect target smartphone to the laptop - OpenVPN Connect

Magnet Axiom process uses the Linux DD command to recover a full physical image of the device’s flash memory, including file system data, deleted data from unallocated space, user data, and native data [235].

6.2.13.2 Forensic exam XIII: Analysis, results, and discussion

The rooted physical data extraction of the sandbox smartphone recovered data regarding “Deleted” and “Deleted, Overwritten” artifacts; however, only the file names, locations, and extensions were recovered. The “Deleted” and “Deleted, Overwritten” artifacts discovered were empty, containing no internal hexadecimal data from which to discern file signatures or any visible biometric information, see figures x-x.

EVIDENCE (11) Selected fold

Entire Disk (EXT-family, 21.75 GB) > data > com.snapchat.android > files > file_manager > media

Name	Deleted	Size (bytes)	Type	File ext
0b8ace4a-13d6-d53b-494c-0d4aec963101.edits.0	Deleted		File	.0
13c5f2e4-73eb-fa5a-b3bf-fa6de0cf7663.edits.0	Deleted		File	.0
4d002e22-f28e-749e-7878-cd14b2d551e4.media.0	Deleted		File	.0
4d002e22-f28e-749e-7878-cd14b2d551e4.media.0.tmp	Deleted		File	.tmp
4d30341e-6b8a-9d87-db6f-c5e25e54bf65.edits.0	Deleted		File	.0
7f3f99c1-08ba-3da8-df31-dafa6d7d77ff.edits.0	Deleted		File	.0
8448c9bd-cf64-2b0b-73b8-4a4909fba7b9.media.0	Deleted		File	.0
95f5c8ed-983e-3d0e-3856-13d9655980c2.edits.0	Deleted		File	.0
a6eba6fe-3dba-c66f-37f2-935a242894d7.media.0	Deleted		File	.0
c53929e5-41a4-039d-1aef-efabac055504.media.0	Deleted		File	.0
f009221b-dc07-dd3b-5089-c30413f7e160.media.0	Deleted		File	.0

Figure 75. Forensic exam XIII:
./files/file_manager/memories_media

EVIDENCE (12)

Selected folder only Column view

Name	Deleted	Size (bytes)	Type	File extension
C082F6F30F3DBFBA1D4E21D09C37A624.media.0.tmp	Deleted, Overwritten		File	.tmp
C082F6F30F3DBFBA1D4E21D09C37A624.media.0		5,255,856	File	.0
BE8DAC4B9D843981DA80DB5533FF3128.media.0		931,363	File	.0
BDE0BD70916DC9A5476ECACE3F7528E.media.0		877,356	File	.0
B308BFCB14861C7DA95A6068EA14754E.media.0		708,063	File	.0
9462C63EEB60E63F2520BE8DA0FCEAAD.media.0		672,127	File	.0
63345E64B7972415E7BF74657F608437.media.0		959,242	File	.0
57F4270924A68B758DC1D51AAF43EC84.media.0		931,430	File	.0
458A067D15EFB608ADF16AB3E75792B8.media.0		395,651	File	.0
37AA06CE2E4F9EC003040717CBA8B2E8.media.0		947,580	File	.0
296A9EE84ABAC40AECCF8655169016A3.media.0		567,249	File	.0
27D9544FC224C254D2EFA44918103C87.media.0		509,315	File	.0

Figure 76. Forensic exam XIII:

EVIDENCE (192)

Selected folder only Column view

Name	Deleted	Size (bytes)	Type	File extension
2F9CCBBECE728B72D1CA67AE020B3E8F.mini_thumbnail.0	Deleted		File	.0
2E69ECBA9B25252F2CA5E33A92CBA4A9.mini_thumbnail.0	Deleted, Overwritten		File	.0
2DDF2518753CF1606051DFD3664A1CE4.mini_thumbnail.0	Deleted		File	.0
2D4AF2F744028412591046291B158971.mini_thumbnail.0	Deleted		File	.0
2BED98A6C4F35003FB5237D86A1B4FFB.mini_thumbnail.0	Deleted		File	.0
2862BD013F902A136872718C6FB80E99.mini_thumbnail.0	Deleted		File	.0
222B1184A0DC789FOCF73493668BBB74.mini_thumbnail.0	Deleted		File	.0
222B1184A0DC789FOCF73493668BBB74.mini_thumbnail.0	Deleted		File	.0
212D4A2B606D151BEBE8B0343EC483A1.mini_thumbnail.0	Deleted		File	.0
202436985224611CA0B503A6B8A1BAAC.mini_thumbnail.0	Deleted		File	.0

Figure 77. Forensic exam XIII:

EVIDENCE (164)

Selected folder only Column view

Name	Deleted	Size (bytes)	Type	File extension
FD096812EEBA3233FDA4DA3FF0471407.spectacles.0	Deleted		File	.0
FD07B2FA50039F145539804B70F64849.spectacles.0	Deleted		File	.0
FD07B2FA50039F145539804B70F64849.spectacles.0	Deleted		File	.0
FCFFCD6D8F0B49A810135AD49AECD2CA.spectacles.0	Deleted		File	.0
FC8D3AC1355CE5F66A3A4D83926F9F93.spectacles.0	Deleted		File	.0
FBDF935C67385FF94D32BB235AD87EE5.spectacles.0	Deleted		File	.0
FBAF79D0668B31542BC50220ADCDE301.spectacles.0	Deleted		File	.0
FAA668C332C253B8F1B7557994CA4A60.spectacles.0	Deleted		File	.0
FAA55CE9B47DFOC05BCA569ABB2E0720.spectacles.0	Deleted		File	.0
F9126AB37E8191DAD31AEFB0116DFED2.spectacles.0	Deleted		File	.0
F86601533D55A51A597D586EC9A26D98.spectacles.0	Deleted		File	.0

Figure 78. Forensic exam XIII:

EVIDENCE (43)

Selected folder only

Entire Disk (EXT-family, 21.75 GB) > data > com.snapchat.android > files > gallery > thumbnails

Name	Deleted	Size (bytes)	Type	File
FED260DF6C72CE3D2DCEC437E7662CCA.thumbnail.0	Deleted, Overwritten		File	.0
FDD3D6A21940DAD83787A431AF84DC1D.thumbnail.0	Deleted, Overwritten		File	.0
F1ECD641AC25658DD96D4DD750A4ABD9.thumbnail.0	Deleted, Overwritten		File	.0
EF1AF38104CEE07C30ABD17098D6C5E.thumbnail.0	Deleted, Overwritten		File	.0
EAF97CAEFC08F8F2E24F187B15DBEA52.thumbnail.0	Deleted		File	.0
E18B7B0EF3EF7ABE51B98CC097F36E2D.thumbnail.0	Deleted, Overwritten		File	.0
D6B9502A89855DDA79258B9EA2E26324.thumbnail.0	Deleted, Overwritten		File	.0
D4CB4F4296A100FE30D053463B0BDBB8.thumbnail.0	Deleted, Overwritten		File	.0

Figure 79. Forensic exam XIII:

EVIDENCE (39)

Selected folder only

Entire Disk (EXT-family, 21.75 GB) > data > com.snapchat.android > files > gallery > files

Name	Deleted	Size (bytes)	Type
F9682046BDD23832CCDAD461D84CACE5.thumbnail.0	Deleted, Overwritten		File
F659EF7EDB516E64DF7C564754C9FBEO.thumbnail.0	Deleted, Overwritten		File
F1ECD641AC25658DD96D4DD750A4ABD9.thumbnail.0.tmp	Deleted, Overwritten		File
E0AA07C8F98E92BCC56AE7C3EB984219.thumbnail.0	Deleted, Overwritten		File
DD1F07E80DB99953DF5F15FC533AE18F.thumbnail.0	Deleted, Overwritten		File

Figure 80. Forensic exam XIII:

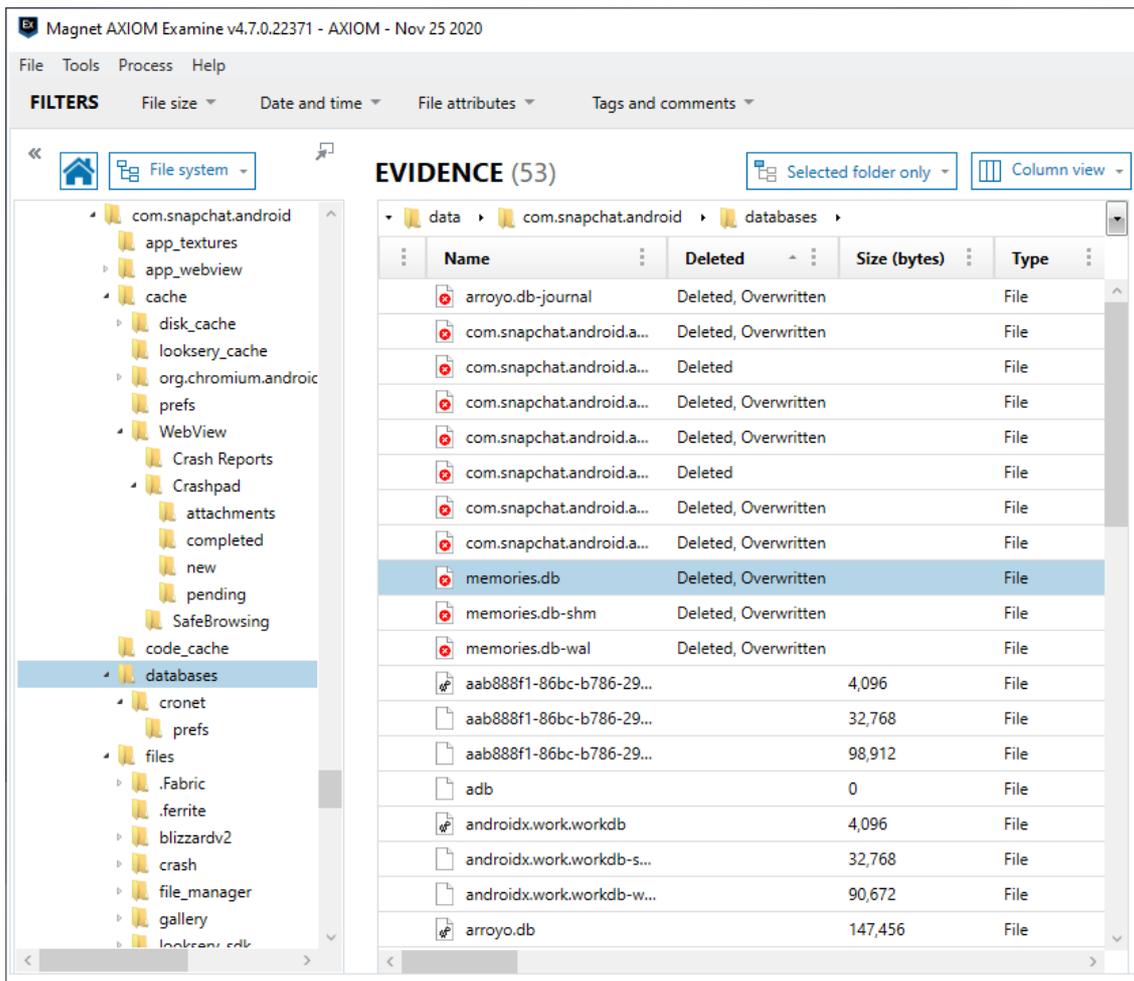


Figure 81. Forensic exam XIII:

The physical extraction acquired data regarding 53 artifacts from /databases; however, 2 were “Deleted” and 9 were “Deleted, Overwritten”, placing the complete artifacts extracted at a total of 42.

7 Validation via triangulation

Integrity of data sourced through the forensic examinations has been validated through a cross examination of SHA hashes, metadata, timestamps, visual observation, and artifact inventory counts.

Files within “/files/file_manager/memories_mini_thumbnail” and “/files/file_manager/memories_thumbnail” directories within /com.snapchat.android were examined as they were the only folders extracted which likely contained photograph or video files with viable biometric information.

Artifacts found within the following directories were not further examined due to either the files being “Deleted”, “Deleted, Overwritten”, and/or lacked biometric information after previewing image content:

./files/file_manager/media
 ./files/file_manager/memories_media
 ./files/file_manager/spectacles
 ./files/gallery/files
 ./files/gallery/thumbnails

None of the original image files captured by the smart eyewear were discovered within the /data/data/com.snapchat.android directory on the sandbox smartphone (Xiaomi Redmi Note 7); however, thumbnails and mini thumbnails of the smart eyewear images and videos were accessed, extracted, and acquired. File metadata and naming conventions collected aided in making this determination, as illustrated below.

The TWRP Copy/ADB Backup Method, used within Forensic exam XII, truncated file extensions and portions of file names within the /memories_thumbnail directory and the /memories_mini_thumbnail directory (Table x-x); however, it was determined, through data and forensic method triangulation, truncation had little effect on the integrity of the files extracted. Apart from shortening the file names and file extensions, all other information within the webp image files retained integrity after data extraction, as denoted by the matching SHA checksum hashes, metadata, and visual parallels across all extraction methods (Tables x-x).

Data analysis and validation is contingent on Forensic exams I - XIII being performed prior, as such, all methods and tools used prior are also required in order to analyze and validate the data in its entirety.

See Tables X-X for validation via triangulation tools and procedures utilized to further analyze the files extracted.

Table 46. Data analysis methods: Additional tools used for validation via triangulation.

Device	Software and peripherals
Laptop	<ul style="list-style-type: none"> - Autopsy 4.13.0 [251] - ExifTool v12.07 [252] - Magnet Axiom v4.7.0.22371 - HxD Hex Editor v2.3.0.0 - Opera web browser disconnected from Internet - DB Browser for SQLite v3.11.2 <ul style="list-style-type: none"> - Built for x86_64-little_endian-llp64, running on x86_64 - Qt v5.11.3 - SQLite v3.27.2

Table 47. Validation via triangulation procedure

1.	Randomly selected one file from each relative directory (/memories_thumbnail and /memories_mini_thumbnail)
2.	Collected pre-extraction metadata via ADB shell commands on sandbox smartphone
3.	Extracted SHA hashes for both webp files on the rooted sandbox smartphone within ADB shell (Figure x-x)
4.	Analyzed each selected file's post-extraction metadata with ExifTool v12.07, HxD Hex Editor v2.3.0.0, Autopsy v4.13.0, and Magnet Axiom v4.7.0.22371 (Figure x)
5.	Extracted SHA hashes for both webp files with Windows' CRC SHA on the Windows 10 laptop (Table x)
6.	Compared and matched SHA hashes for webp images
7.	Analyzed logical and physical data extractions with Magnet Axiom's Magnet.AI facial detection scanner
8.	Added the WEBP MIME type combined with the ".0" file type extension as a custom file type to Magnet Axiom's CustomFileTypeArtifacts.xlsx file and re-ran Magnet.AI facial detection scanner
9.	Ensured laptop was disconnected from the Internet, then dragged and dropped webp files into Opera web browser to visually inspect and match images extracted via differing forensic methods
10.	Extracted copies of NBDDO files with ".0" file extensions from Magnet Axiom, changed file extensions to .webp to match their file header signature, then imported altered files back into the Magnet Axiom case file to scan and categorize as "possible human faces" by the Magnet.AI module.
11.	Step 9 was repeated; however, in this instance the file extensions were changed to .jpg to determine if the webp extension was preventing facial detection within examined files
12.	Searched for and located selected webp files within smart eyewear databases with HxD Hex Editor, DB Browser for SQLite, and Magnet Axiom
13.	Totaled artifact inventory counts for each relative file extracted

Table X illustrates the two files selected from /com.snapchat.android to be analyzed.

Table 48. Files selected from /memories_mini_thumbnail and /memories_thumbnail to be audited

File path	File Name	File Extension
/com.snapchat.android/files/file_manager/memories_thumbnail/	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail	.0
/com.snapchat.android/files/file_manager/memories_mini_thumbnail/	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail	.0

7.1.1 Pre-extraction metadata

Metadata from each file with a “.0” extension, within /memories_mini_thumbnail and /memories_thumbnail directories on the rooted sandbox smartphone, was collected prior to performing data extractions (within Forensic exams XI-XIII) via ADB shell’s “stat” [236] and “od”[237] commands (Figure x). The sandbox smartphone did not possess the “hexdump” [238]Linux command.

Creation or birth timestamps for files are not implemented within Linux systems; however, the system notes the time a file’s contents were last modified, “2020-09-21 01:18” (Figure X).

These timestamps do not match the point-in-time the photographs and videos were captured, collected, and stored by the smart eyewear hardware; which was between July and August 2020 according to Forensic exams VIII and X.

Within Figures x-x, commands are denoted in white, pertinent information is denoted in yellow, while other matching colors denote matching timestamps.

```
>adb devices -l
List of devices attached
2da4da73                device  product:lavender_eea  model:Redmi_Note_7
device:lavender transport_id:1

>adb shell
lavender:/ $ su
lavender:/ # cd
/data/data/com.snapchat.android/files/file_manager/memories_mini_thumbnail
lavender:/data/data/com.snapchat.android/files/file_manager/memories_mini_thumbnail
# stat 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
  File: `9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0'
  Size: 96      Blocks: 8      IO Blocks: 512 regular file
Device: fc01h/64513d      Inode: 262480      Links: 1
Access: (600/-rw-----)      Uid: (10170/ u0_a170)      Gid: (10170/ u0_a170)
Access: 2020-09-21 01:54:18.782134410
Modify: 2020-09-21 01:18:40.012999990
Change: 2020-09-21 01:18:40.012999990

lavender:/data/data/com.snapchat.android/files/file_manager/memories_thumbnail # cd
/data/data/com.snapchat.android/files/file_manager/memories_thumbnail
lavender:/data/data/com.snapchat.android/files/file_manager/memories_thumbnail #
stat BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
  File: `BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0'
  Size: 4820     Blocks: 16      IO Blocks: 512 regular file
Device: fc01h/64513d      Inode: 262626      Links: 1
Access: (600/-rw-----)      Uid: (10170/ u0_a170)      Gid: (10170/ u0_a170)
Access: 2020-09-21 01:54:08.805466750
Modify: 2020-09-21 01:18:45.772999988
Change: 2020-09-21 01:18:45.772999988
```

Figure 76. Excerpts of stat data for “.0” files via ADB shell on rooted sandbox smartphone (Xiaomi Redmi Note 7)

Hexadecimal data acquired with the “od” command confirmed both “.0” files were originally created with the WebP [239] image format, as denoted by the file header signature [240]. (Figure x) Snap Inc. developers purposely changed the file extension from the original “.webp” to “.0” in order to conceal the file’s image properties and mismatch the file’s content and file extension.

```
lavender:/data/data/com.snapchat.android/files/file_manager/memories_mini_th
umbnail # hexdump -C 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
/system/bin/sh: hexdump: not found

lavender:/data/data/com.snapchat.android/files/file_manager/memories_mini_th
umbnail # od -ct x1 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
0000000  52 49 46 46 58 00 00 00 57 45 42 50 56 50 38 20
          R  I  F  F  X  \0 \0 \0  W  E  B  P  V  P  8

lavender:/data/data/com.snapchat.android/files/file_manager/memories_thumbnai
l # od -ct x1 BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
0000000  52 49 46 46 cc 12 00 00 57 45 42 50 56 50 38 20
          R  I  F  F 314 022 \0 \0  W  E  B  P  V  P  8
```

Figure 77. Excerpts of hexadecimal data for “.0” files via ADB shell on rooted sandbox smartphone (Xiaomi Redmi Note 7)

7.1.2 Post-extraction metadata

ExifTool v12.07, Autopsy 4.13.0, Magnet Axiom v4.7.0.22371, and HxD Hex Editor v2.3.0.0 were used to acquire and analyze metadata from files, which possibly contained biometric information, after logical or physical extraction from the rooted sandbox smartphone. (Tables x-x)

Matching colors within Tables x-x denote matching timestamps. All other pertinent information is denoted in yellow (File: names, types, extensions, errors). Blacked out fields denote attributes not supported by the metadata tool utilized.

Timestamps found within metadata post-extraction were not generated at the point-in-time the smart eyewear captured the photographs and videos (Tables x-x). Time stamps that matched included: The mini_thumbnail’s “File Modification Date/Time” from the ADB Pull extraction method and “File Creation Date/Time” from the “Deleted” file extracted by Magnet Axiom (Table x); additionally, the thumbnail’s “File Modification Date/Time” from the ADB Pull extraction method matched Magnet Axiom’s “File Modification” and “File Creation” Date/Time (Table x). Deleted files examined by Magnet Axiom possessed timestamps of the deletion time, whereas “Deleted, Overwritten” files did not. Autopsy 4.13.0 was incapable of acquiring timestamps and image dimensions.

ExifTool v12.07, Autopsy 4.13.0, HxD Hex Editor v2.3.0.0 confirmed the original File Type as “WEBP”, File Type Extension as “.webp”, and MIME Type as “image/webp” for the mini thumbnail and thumbnail files audited whose contents were intact. (Tables x-x) Magnet Axiom v4.7.0.22371 did not catch the mismatch between the file extension (“.0”) and file header signature (Hexadecimal: 52 49 46 46 -- -- -- -- 57 45 42 50 ; ASCII: RIFF -- -- -- -- WEBP) on both file names examined; however, this data was displayed within the software’s “Preview” and “Text and Hex” modules even though not

automatically parsed and organized as such. (Tables x-x) “Deleted” and “Deleted, Overwritten” files did not possess file type attributes. (Tables x-x)

The data request performed within Forensic exam VIII, via Autopsy v4.13.0, provided metadata on the smart eyewear’s video camera processing SoC, whereas the metadata captured from the sandbox smartphone did not contain any camera information (Tables X-X), further evidencing the webp files were not originally captured by the smart eyewear but generated as thumbnails thereafter.

As noted in Forensic exam XII, File Names were truncated within the TWRP copy/ADB Backup extraction method.

Table 49. Metadata results for 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

Results for /data/com.snapchat.android/files/file_manager/memories_mini_thumbnail/ 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0								
	Rooted acquisition method							
	Logical extraction of file via ADB pull		Logical extraction of file via TWRP copy/ADB Backup		Physical extraction of file via Magnet Axiom	Physical extraction and exportation of “Deleted” file via Magnet Axiom	Physical extraction of “Deleted” file via Magnet Axiom	
	Metadata Tool							
	ExifTool v12.07	Autopsy v4.13.0	ExifTool v12.07	Autopsy v4.13.0	Not Applicable	ExifTool v12.07	Magnet Axiom v4.7.0.22371	
Details								
File Name & File Extension	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	9A60BAE3104F32B5710B58A16B76AC7	9A60BAE3104F32B5710B58A16B76AC7	Not Available	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	
Deleted								Deleted
File Size	96 bytes	96 bytes	96 bytes	96 bytes			0 bytes	Empty Field
File Modification Date/Time	2020:09:21 01:18:40+03:00	0000-00-00 00:00:00	2020:09:21 05:04:06+03:00	0000-00-00 00:00:00			2020:11:28 12:35:33+02:00	2020:11:25 11:49:16PM
File Deleted Date/Time								2020:11:25 11:49:16PM
File Access Date/Time	2020:10:10 14:35:28+03:00	0000-00-00 00:00:00	2020:10:10 16:42:45+03:00	0000-00-00 00:00:00			2020:11:28 12:35:33+02:00	2020:09:21 01:54:18AM
File Creation Date/Time	2020:09:21 02:09:33+03:00	0000-00-00 00:00:00	2020:09:22 20:21:46+03:00	0000-00-00 00:00:00			2020:11:28 12:35:33+02:00	2020:09:21 01:18:40AM
File Permissions	rw-rw-rw-		rw-rw-rw-				rw-rw-rw-	
Error :	Empty Field		Empty Field				"File is empty"	
File Type	WEBP		WEBP				Empty Field	File
File Type Extension	webp		webp			Empty Field	.0	
MIME Type	image/webp	image/webp	image/webp	image/webp		Empty Field		
VP8 Version	0 (bicubic reconstruction, normal loop)		0 (bicubic reconstruction, normal loop)			Empty Field		
Image Width	5	-1.0	5	-1.0		Empty Field		

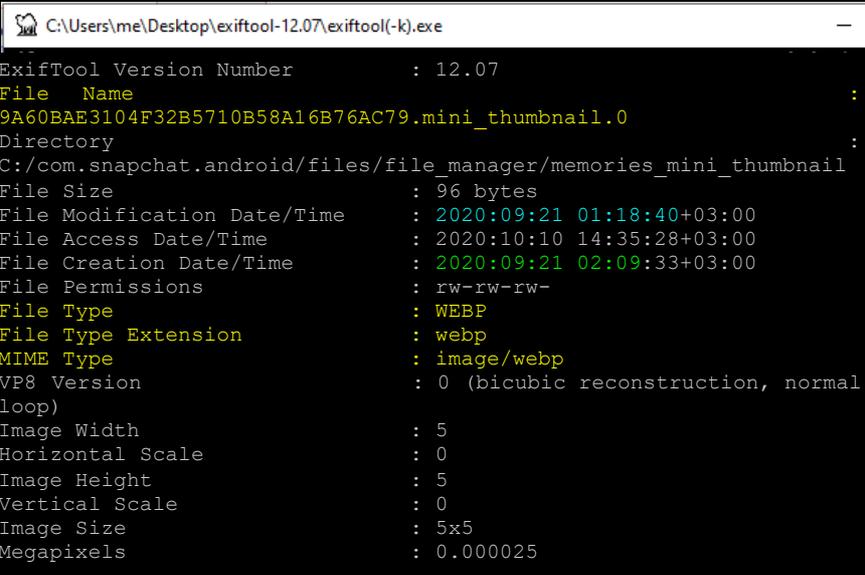
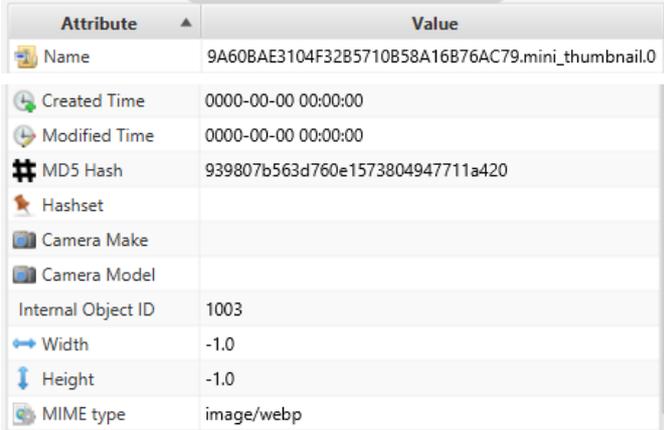
Horizontal Scale	0		0			Empty Field	
Image Height	5	-1.0	5	-1.0		Empty Field	
Vertical Scale	0		0			Empty Field	
Image Size	5x5		5x5			Empty Field	
Megapixels	0.000025		0.000025			Empty Field	
Camera Make		Empty Field		Empty Field			
Camera Model		Empty Field		Empty Field			

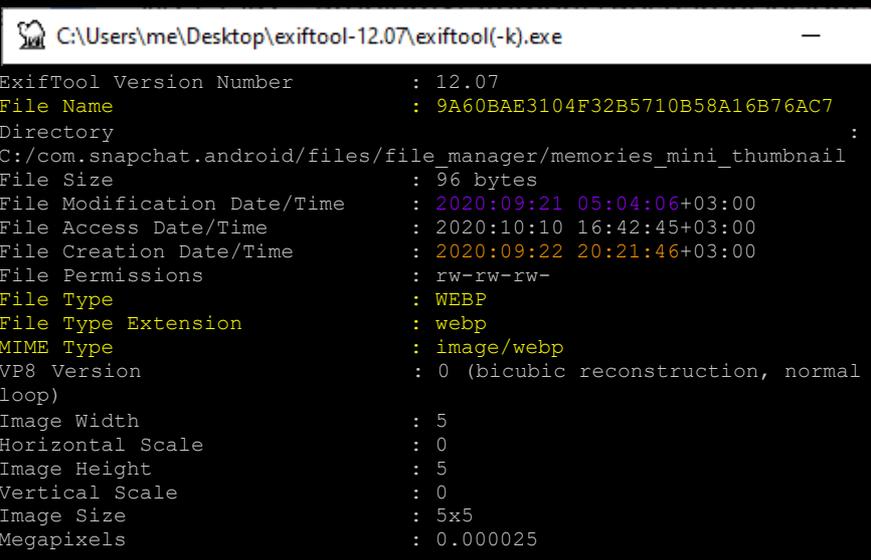
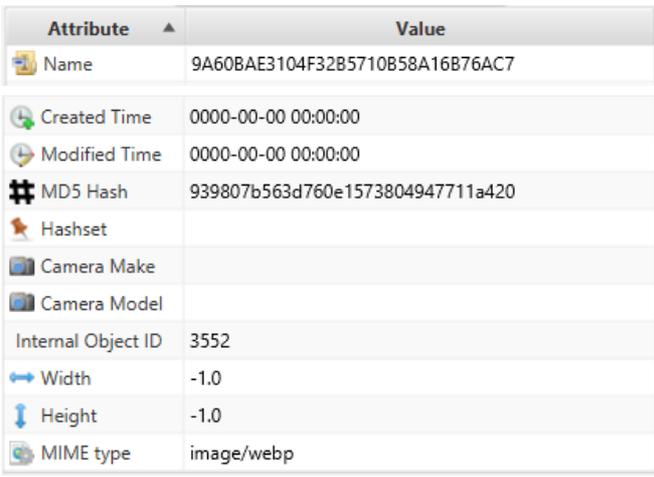
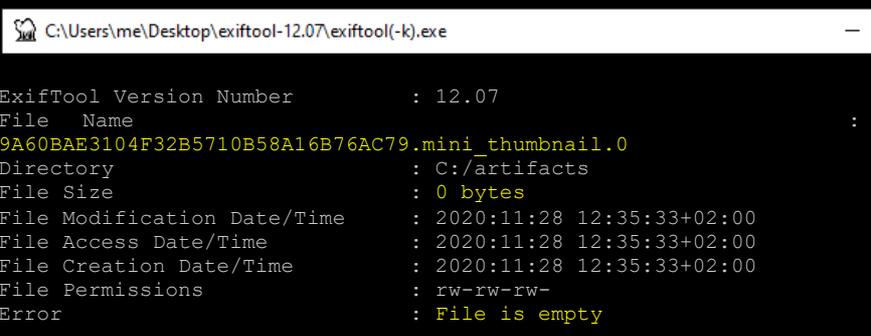
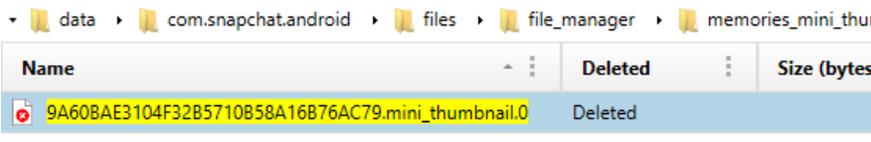
Table 50. .Metadata results forBB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

Results for /data/com.snapchat.android/files/file_manager/memories_thumbnail/ BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0								
	Rooted acquisition method							
	Logical extraction of file via ADB pull		Logical extraction of file via TWRP copy/ADB Backup		Physical extraction and exportation of file via Magnet Axiom Examine	Physical extraction of file via Magnet Axiom	Physical extraction and exportation of "Deleted, Overwritten" file via Magnet Axiom	Physical extraction of "Deleted, Overwritten" file via Magnet Axiom
	Metadata Tool							
	ExifTool v12.07	Autopsy v4.13.0	ExifTool v12.07	Autopsy v4.13.0	ExifTool v12.07	Magnet Axiom v4.7.0.22371	ExifTool v12.07	Magnet Axiom v4.7.0.22371
Details								
File Name & File Extension	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	BB0AFDFA15F475D761CAE9D1A843AF2A.thu	BB0AFDFA15F475D761CAE9D1A843AF2A.thu	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
Deleted						Empty Field		"Deleted, Overwritten"
File Size	4.7 kB	4,820 bytes	4.7 kB	4,820 bytes	4.7 kB	4,820 bytes	0 bytes	Empty Field
File Modification Date/Time	2020:09:21 01:18:45+03:00	0000-00-00 00:00:00	2020:09:21 05:04:06+03:00	0000-00-00 00:00:00	2020:11:28 00:28:16+02:00	2020:09:21 01:18:45 AM	2020:11:28 00:29:50+02:00	Empty Field
File Deleted Date/Time						Empty Field		Empty Field
File Access Date/Time	2020:10:05 23:08:43+03:00		2020:10:05 23:20:49+03:00		2020:11:28 00:28:16+02:00	2020:09:21 01:54:08 AM	2020:11:28 00:29:50+02:00	Empty Field
File Creation Date/Time	2020:09:21 02:09:17+03:00	0000-00-00 00:00:00	2020:09:22 20:21:46+03:00	0000-00-00 00:00:00	2020:11:28 00:28:16+02:00	2020:09:21 01:18:45 AM	2020:11:28 00:29:50+02:00	Empty Field
File Permissions	rw-rw-rw-		rw-rw-rw-		rw-rw-rw-		rw-rw-rw-	
Error :	Empty Field		Empty Field		Empty Field		"File is empty"	
File Type	WEBP		WEBP		WEBP	File	Empty Field	File
File Type Extension	webp		webp		webp	.0	Empty Field	.0
MIME Type	image/webp	image/webp	image/webp	image/webp	image/webp		Empty Field	

VP8 Version	0 (bicubic reconstruction , normal loop)		0 (bicubic reconstruction , normal loop)		0 (bicubic reconstruction , normal loop)		Empty Field
Image Width	270	-1.0	270	-1.0	270		Empty Field
Horizontal Scale	0		0		0		Empty Field
Image Height	270	-1.0	270	-1.0	270		Empty Field
Vertical Scale	0		0		0		Empty Field
Image Size	270x270		270x270		270x270		Empty Field
Megapixels	0.073		0.073		0.073		Empty Field
Camera Make		Empty Field		Empty Field			
Camera Model		Empty Field		Empty Field			

Table 51. Extraction method comparison of a file within “memories_mini_thumbnail” directory

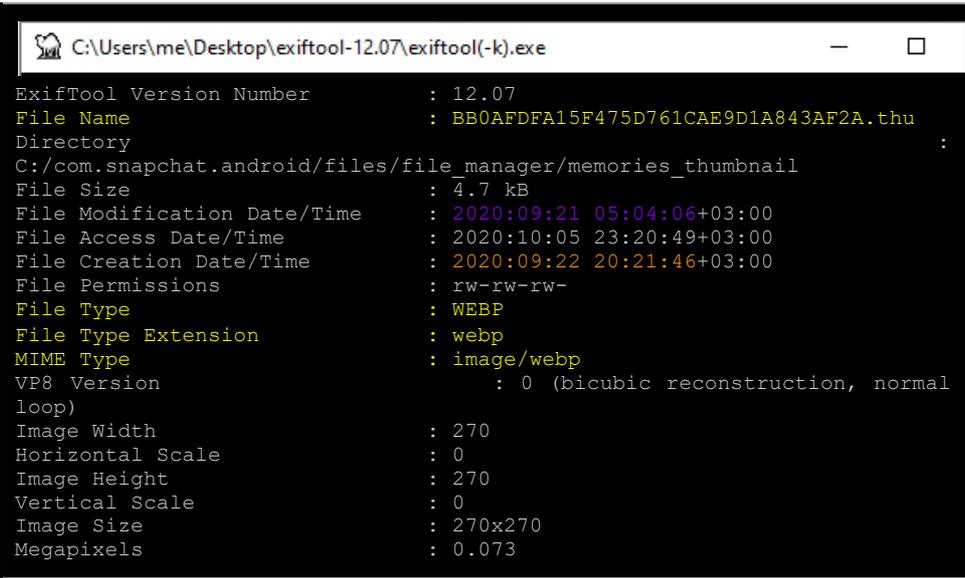
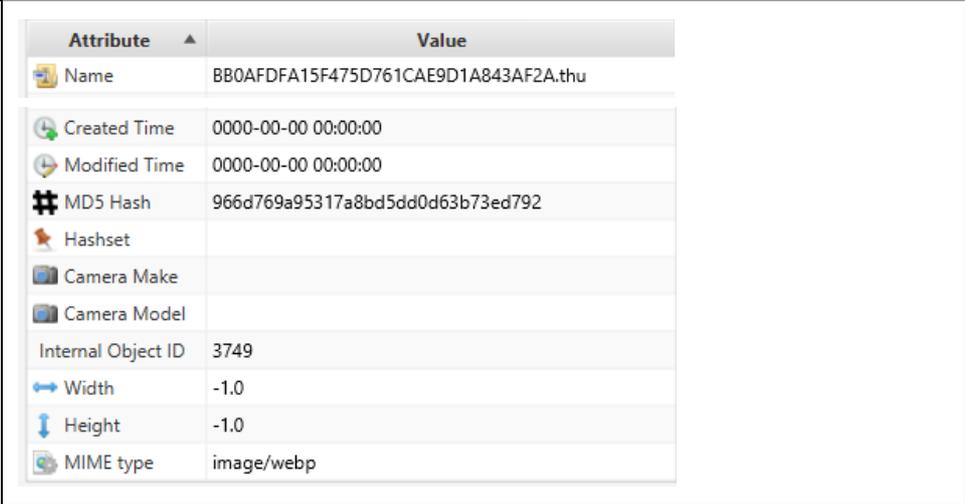
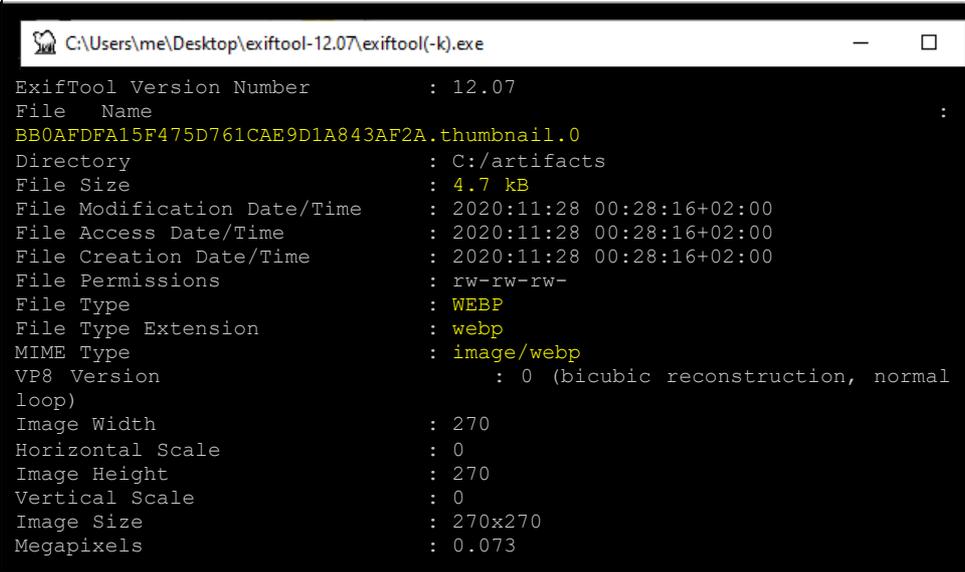
Acquisition method	Metadata Tool	Results for 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0																								
Rooted logical extraction via ADB pull	ExifTool v12.07	 <pre> C:\Users\me\Desktop\exiftool-12.07\exiftool(-k).exe ExifTool Version Number : 12.07 File Name : 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 Directory : C:/com.snapchat.android/files/file_manager/memories_mini_thumbnail File Size : 96 bytes File Modification Date/Time : 2020:09:21 01:18:40+03:00 File Access Date/Time : 2020:10:10 14:35:28+03:00 File Creation Date/Time : 2020:09:21 02:09:33+03:00 File Permissions : rw-rw-rw- File Type : WEBP File Type Extension : webp MIME Type : image/webp VP8 Version : 0 (bicubic reconstruction, normal loop) Image Width : 5 Horizontal Scale : 0 Image Height : 5 Vertical Scale : 0 Image Size : 5x5 Megapixels : 0.000025 </pre>																								
Rooted logical extraction via ADB pull	Autopsy v4.13.0	 <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0</td> </tr> <tr> <td>Created Time</td> <td>0000-00-00 00:00:00</td> </tr> <tr> <td>Modified Time</td> <td>0000-00-00 00:00:00</td> </tr> <tr> <td>MD5 Hash</td> <td>939807b563d760e1573804947711a420</td> </tr> <tr> <td>Hashset</td> <td></td> </tr> <tr> <td>Camera Make</td> <td></td> </tr> <tr> <td>Camera Model</td> <td></td> </tr> <tr> <td>Internal Object ID</td> <td>1003</td> </tr> <tr> <td>Width</td> <td>-1.0</td> </tr> <tr> <td>Height</td> <td>-1.0</td> </tr> <tr> <td>MIME type</td> <td>image/webp</td> </tr> </tbody> </table>	Attribute	Value	Name	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	Created Time	0000-00-00 00:00:00	Modified Time	0000-00-00 00:00:00	MD5 Hash	939807b563d760e1573804947711a420	Hashset		Camera Make		Camera Model		Internal Object ID	1003	Width	-1.0	Height	-1.0	MIME type	image/webp
Attribute	Value																									
Name	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0																									
Created Time	0000-00-00 00:00:00																									
Modified Time	0000-00-00 00:00:00																									
MD5 Hash	939807b563d760e1573804947711a420																									
Hashset																										
Camera Make																										
Camera Model																										
Internal Object ID	1003																									
Width	-1.0																									
Height	-1.0																									
MIME type	image/webp																									

<p>Rooted logical extraction via TWRP copy/ADB Backup</p>	<p>ExifTool v12.07</p>	 <pre> C:\Users\me\Desktop\exiftool-12.07\exiftool(-k).exe ExifTool Version Number : 12.07 File Name : 9A60BAE3104F32B5710B58A16B76AC7 Directory : C:/com.snapchat.android/files/file_manager/memories_mini_thumbnail File Size : 96 bytes File Modification Date/Time : 2020:09:21 05:04:06+03:00 File Access Date/Time : 2020:10:10 16:42:45+03:00 File Creation Date/Time : 2020:09:22 20:21:46+03:00 File Permissions : rw-rw-rw- File Type : WEBP File Type Extension : webp MIME Type : image/webp VP8 Version : 0 (bicubic reconstruction, normal loop) Image Width : 5 Horizontal Scale : 0 Image Height : 5 Vertical Scale : 0 Image Size : 5x5 Megapixels : 0.000025 </pre>																								
<p>Rooted logical extraction via TWRP copy/ADB Backup</p>	<p>Autopsy v4.13.0</p>	 <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>9A60BAE3104F32B5710B58A16B76AC7</td> </tr> <tr> <td>Created Time</td> <td>0000-00-00 00:00:00</td> </tr> <tr> <td>Modified Time</td> <td>0000-00-00 00:00:00</td> </tr> <tr> <td>MD5 Hash</td> <td>939807b563d760e1573804947711a420</td> </tr> <tr> <td>Hashset</td> <td></td> </tr> <tr> <td>Camera Make</td> <td></td> </tr> <tr> <td>Camera Model</td> <td></td> </tr> <tr> <td>Internal Object ID</td> <td>3552</td> </tr> <tr> <td>Width</td> <td>-1.0</td> </tr> <tr> <td>Height</td> <td>-1.0</td> </tr> <tr> <td>MIME type</td> <td>image/webp</td> </tr> </tbody> </table>	Attribute	Value	Name	9A60BAE3104F32B5710B58A16B76AC7	Created Time	0000-00-00 00:00:00	Modified Time	0000-00-00 00:00:00	MD5 Hash	939807b563d760e1573804947711a420	Hashset		Camera Make		Camera Model		Internal Object ID	3552	Width	-1.0	Height	-1.0	MIME type	image/webp
Attribute	Value																									
Name	9A60BAE3104F32B5710B58A16B76AC7																									
Created Time	0000-00-00 00:00:00																									
Modified Time	0000-00-00 00:00:00																									
MD5 Hash	939807b563d760e1573804947711a420																									
Hashset																										
Camera Make																										
Camera Model																										
Internal Object ID	3552																									
Width	-1.0																									
Height	-1.0																									
MIME type	image/webp																									
<p>Rooted physical extraction and exportation of file via Magnet Axiom Examine</p>	<p>Not Applicable</p>	<p>Not Available</p>																								
<p>Rooted physical extraction and exportation of "Deleted" file via Magnet Axiom Examine</p>	<p>ExifTool v12.07</p>	 <pre> C:\Users\me\Desktop\exiftool-12.07\exiftool(-k).exe ExifTool Version Number : 12.07 File Name : 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 Directory : C:/artifacts File Size : 0 bytes File Modification Date/Time : 2020:11:28 12:35:33+02:00 File Access Date/Time : 2020:11:28 12:35:33+02:00 File Creation Date/Time : 2020:11:28 12:35:33+02:00 File Permissions : rw-rw-rw- Error : File is empty </pre>																								
<p>Rooted physical extraction of "Deleted" file via Magnet Axiom Examine</p>		 <p>data > com.snapchat.android > files > file_manager > memories_mini_thun</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Deleted</th> <th>Size (bytes)</th> </tr> </thead> <tbody> <tr> <td>9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0</td> <td>Deleted</td> <td></td> </tr> </tbody> </table>	Name	Deleted	Size (bytes)	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	Deleted																			
Name	Deleted	Size (bytes)																								
9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	Deleted																									

--	--	--

Table 52. Extraction method comparison of a file within “memories_thumbnail” directory

Acquisition method	Metadata Tool	Results for BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
Rooted logical extraction via ADB pull	ExifTool v12.07	
Rooted logical extraction via ADB pull	Autopsy v4.13.0	

<p>Rooted logical extraction via TWRP copy/ADB Backup</p>	<p>ExifTool v12.07</p>	 <pre> C:\Users\me\Desktop\exiftool-12.07\exiftool(-k).exe ExifTool Version Number : 12.07 File Name : BB0AFDFA15F475D761CAE9D1A843AF2A.thu Directory : C:/com.snapchat.android/files/file_manager/memories_thumbnail File Size : 4.7 kB File Modification Date/Time : 2020:09:21 05:04:06+03:00 File Access Date/Time : 2020:10:05 23:20:49+03:00 File Creation Date/Time : 2020:09:22 20:21:46+03:00 File Permissions : rw-rw-rw- File Type : WEBP File Type Extension : webp MIME Type : image/webp VP8 Version : 0 (bicubic reconstruction, normal loop) Image Width : 270 Horizontal Scale : 0 Image Height : 270 Vertical Scale : 0 Image Size : 270x270 Megapixels : 0.073 </pre>																								
<p>Rooted logical extraction via TWRP copy/ADB Backup</p>	<p>Autopsy v4.13.0</p>	 <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>BB0AFDFA15F475D761CAE9D1A843AF2A.thu</td> </tr> <tr> <td>Created Time</td> <td>0000-00-00 00:00:00</td> </tr> <tr> <td>Modified Time</td> <td>0000-00-00 00:00:00</td> </tr> <tr> <td>MD5 Hash</td> <td>966d769a95317a8bd5dd0d63b73ed792</td> </tr> <tr> <td>Hashset</td> <td></td> </tr> <tr> <td>Camera Make</td> <td></td> </tr> <tr> <td>Camera Model</td> <td></td> </tr> <tr> <td>Internal Object ID</td> <td>3749</td> </tr> <tr> <td>Width</td> <td>-1.0</td> </tr> <tr> <td>Height</td> <td>-1.0</td> </tr> <tr> <td>MIME type</td> <td>image/webp</td> </tr> </tbody> </table>	Attribute	Value	Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thu	Created Time	0000-00-00 00:00:00	Modified Time	0000-00-00 00:00:00	MD5 Hash	966d769a95317a8bd5dd0d63b73ed792	Hashset		Camera Make		Camera Model		Internal Object ID	3749	Width	-1.0	Height	-1.0	MIME type	image/webp
Attribute	Value																									
Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thu																									
Created Time	0000-00-00 00:00:00																									
Modified Time	0000-00-00 00:00:00																									
MD5 Hash	966d769a95317a8bd5dd0d63b73ed792																									
Hashset																										
Camera Make																										
Camera Model																										
Internal Object ID	3749																									
Width	-1.0																									
Height	-1.0																									
MIME type	image/webp																									
<p>Rooted physical extraction and exportation of file via Magnet Axiom Examine</p>	<p>ExifTool v12.07</p>	 <pre> C:\Users\me\Desktop\exiftool-12.07\exiftool(-k).exe ExifTool Version Number : 12.07 File Name : BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0 Directory : C:/artifacts File Size : 4.7 kB File Modification Date/Time : 2020:11:28 00:28:16+02:00 File Access Date/Time : 2020:11:28 00:28:16+02:00 File Creation Date/Time : 2020:11:28 00:28:16+02:00 File Permissions : rw-rw-rw- File Type : WEBP File Type Extension : webp MIME Type : image/webp VP8 Version : 0 (bicubic reconstruction, normal loop) Image Width : 270 Horizontal Scale : 0 Image Height : 270 Vertical Scale : 0 Image Size : 270x270 Megapixels : 0.073 </pre>																								

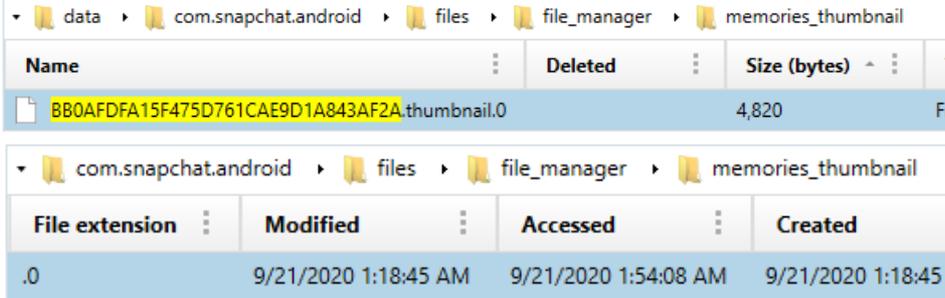
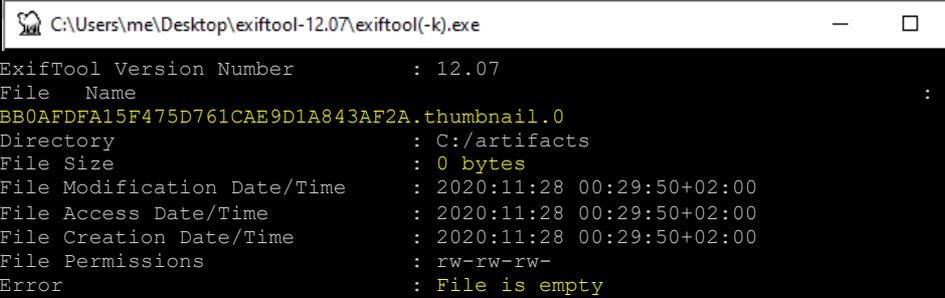
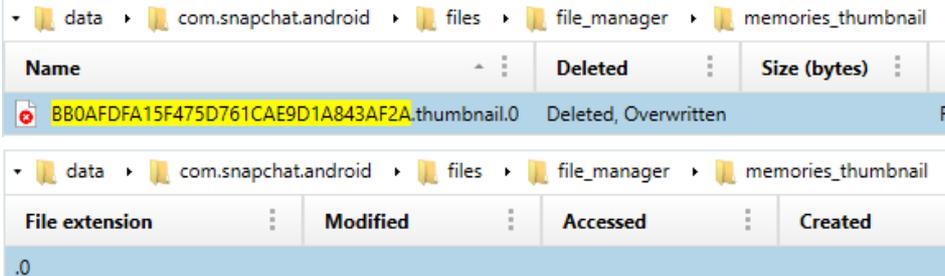
<p>Rooted physical extraction of file via Magnet Axiom Examine</p>	<p>Magnet Axiom v4.7.0.22371</p>	
<p>Rooted physical extraction and exportation of “Deleted, Overwritten” file via Magnet Axiom Examine</p>	<p>ExifTool v12.07</p>	
<p>Rooted physical extraction of “Deleted, Overwritten” file via Magnet Axiom Examine</p>	<p>Magnet Axiom v4.7.0.22371</p>	

Table 53. Extraction method comparison of a file’s hexadecimal content within “memories_mini_thumbnail” directory

<p>Acquisition method</p>	<p>Text and Hexadecimal Tool</p>	<p>Results for 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0</p>
---------------------------	----------------------------------	--

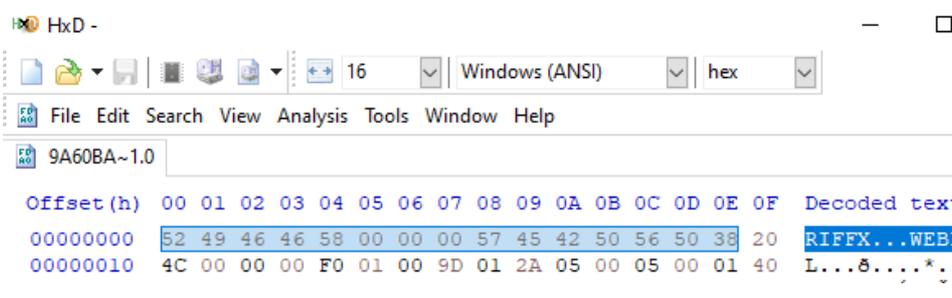
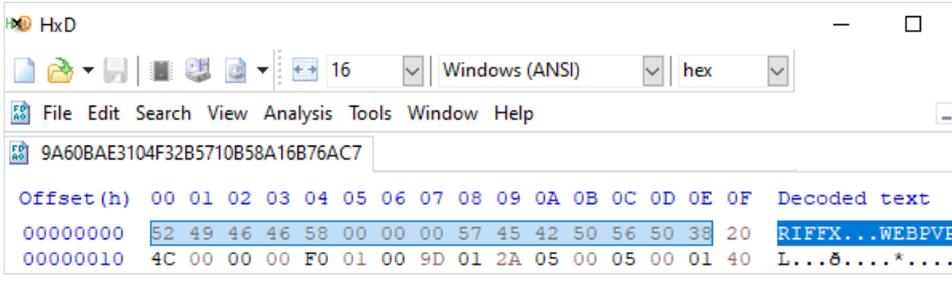
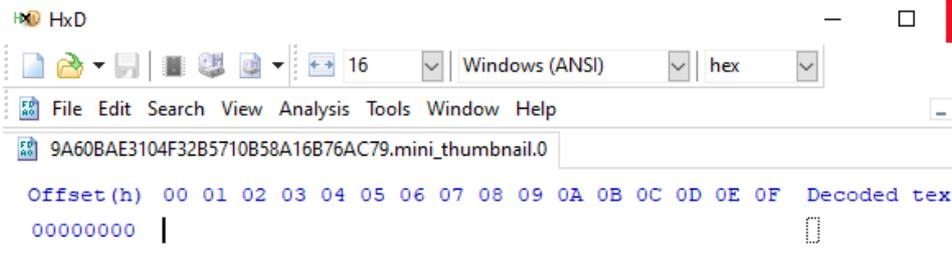
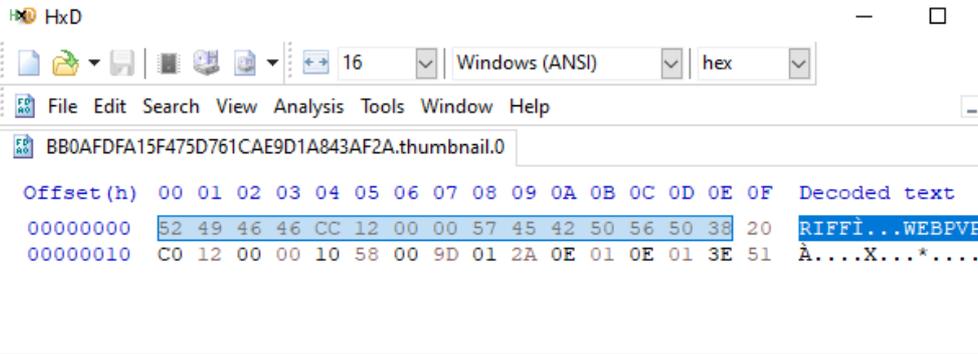
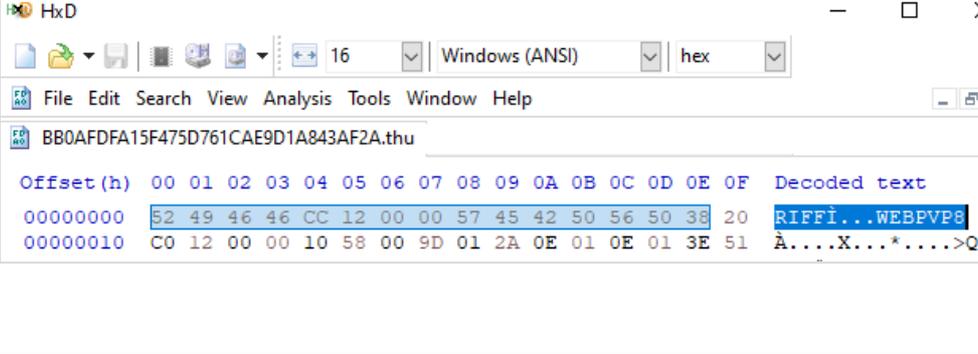
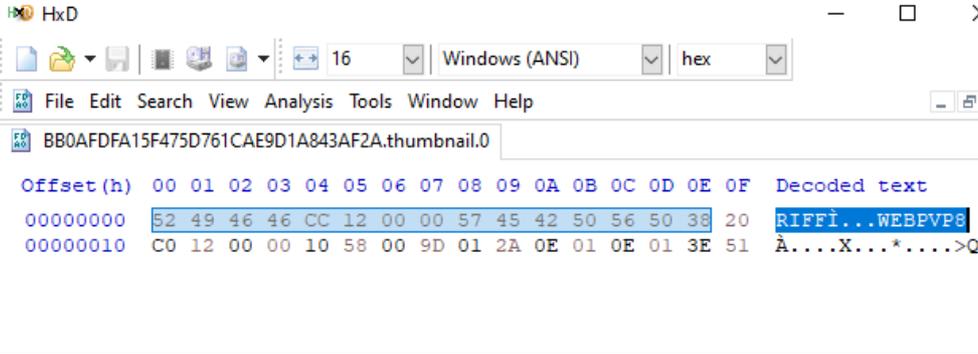
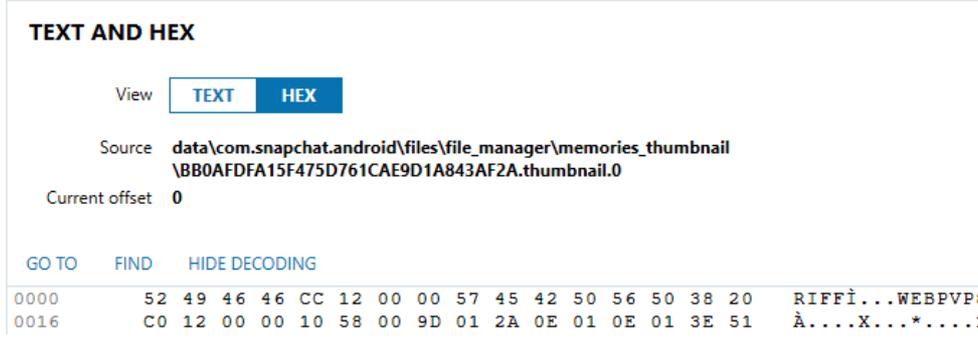
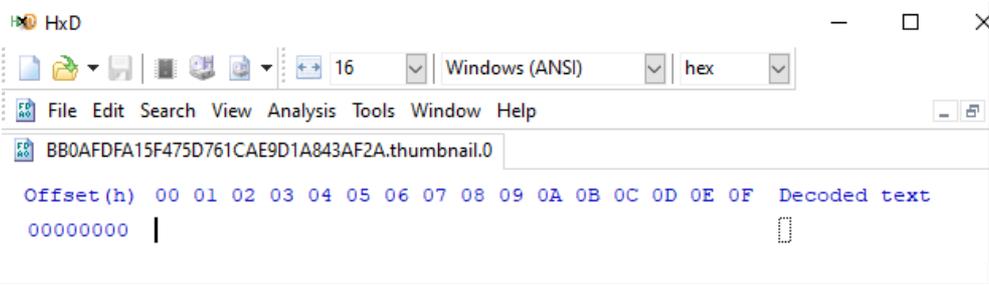
Rooted logical extraction via ADB pull	HxD Hex Editor v2.3.0.0	
Rooted logical extraction via TWRP copy/ADB Backup	HxD Hex Editor v2.3.0.0	
Rooted physical extraction and exportation of file via Magnet Axium Examine	Magnet Axium v4.7.0.22371	Not Available
Rooted physical extraction and exportation of “Deleted” file via Magnet Axium Examine	HxD Hex Editor v2.3.0.0	
Rooted physical extraction of “Deleted” file via Magnet Axium Examine	Magnet Axium v4.7.0.22371	No data to display within Magnet Axium Examine’s “Preview” and “Text and Hex” Modules.

Table 54. Extraction method comparison of a file’s hexadecimal content within “memories_thumbnail” directory

Acquisition method	Text and Hexadecimal Tool	Results for BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
Rooted logical extraction via ADB pull	HxD Hex Editor v2.3.0.0	
Rooted logical extraction via TWRP copy/ADB Backup	HxD Hex Editor v2.3.0.0	
Rooted physical extraction and exportation of file via Magnet Axium Examine	HxD Hex Editor v2.3.0.0	
Rooted physical extraction of file via Magnet Axium Examine	Magnet Axium v4.7.0.2237 1	

Rooted physical extraction and exportation of “Deleted, Overwritten” file via Magnet Axiom Examine	HxD Hex Editor v2.3.0.0	
Rooted physical extraction of “Deleted, Overwritten” file via Magnet Axiom Examine	Magnet Axiom v4.7.0.2237 1	No data to display within Magnet Axiom Examine’s “Preview” and “Text and Hex” Modules.

7.1.3 SHA digest matching

ADB shell’s sha[x]sum command and Windows CRC SHA program were utilized to verify file integrity of the “.0” webp image files via hash value matching.

ADB shell’s sha256sum and sha1sum commands were used to determine 256-bit and 160-bit digests (hash values) of the files on the sandbox smartphone prior to data extractions (Figures X-X).

Windows CRC SHA program, with wildcard asterisk “*” option selected, determined 256-bit and 160-bit digests after extracting the files from the sandbox smartphone. (Tables X-X)

Empty files with 0 byte file sizes, naturally did not match digest values for complete, never been “Deleted” nor “Deleted, Overwritten” files.

Table 55. SHA Extraction method comparison for webp image file from /memories_mini_thumbnail

Acquisition method	SHA Tool	SHA digests for 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
Rooted logical examination of sandbox smartphone file system	ADB shell sha[x]sum	<pre> >adb shell lavender:/ \$ su lavender:/ # cd /data/data/com.snapchat.android/files/file_manager/memories_mini_thumbnail lavender:/data/data/com.snapchat.android/files/file_manager/memories_mini_thumbnail # sha256sum 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 a58640187b69136300c6fb287b84a12ff21c6c049d3b752390ecc1323c913992 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 lavender:/data/data/com.snapchat.android/files/file_manager/memories_mini_thumbnail # sha1sum 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 </pre>

		<p>25a9c442b21f6a04eef8af0fa729912a5030105b 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0</p>						
Rooted logical extraction via ADB pull	Windows CRC SHA	<p>Checksum information</p> <p>Name 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 Size 96 bytes CRC32 AF9E1337 CRC64 0C6A905880E43676 SHA256 A58640187B69136300C6FB287B84A12FF21C6C049D3B752390ECC1323C913992 SHA1 25A9C442B21F6A04EEF8AF0FA729912A5030105B BLAKE2sp 6EFB1B480DEC305773F45353C471D0B4A440059EA24F0D32276B77696F449385</p>						
Rooted logical extraction via TWRP copy/ADB Backup	Windows CRC SHA	<p>Checksum information</p> <p>Name 9A60BAE3104F32B5710B58A16B76AC79 Size 96 bytes CRC32 AF9E1337 CRC64 0C6A905880E43676 SHA256 A58640187B69136300C6FB287B84A12FF21C6C049D3B752390ECC1323C913992 SHA1 25A9C442B21F6A04EEF8AF0FA729912A5030105B BLAKE2sp 6EFB1B480DEC305773F45353C471D0B4A440059EA24F0D32276B77696F449385</p>						
Rooted physical extraction of file via Magnet Axiom Examine		Not Available						
Rooted physical extraction of "Deleted" file via Magnet Axiom Examine	Magnet Axiom	<p>data > com.snapchat.android > files > file_manager > memories_mini_thumbnail</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Deleted</th> <th>SHA1 hash</th> </tr> </thead> <tbody> <tr> <td>9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0</td> <td>Deleted</td> <td>da39a3ee5e6b4b0d3255bfef95601890</td> </tr> </tbody> </table>	Name	Deleted	SHA1 hash	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	Deleted	da39a3ee5e6b4b0d3255bfef95601890
Name	Deleted	SHA1 hash						
9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0	Deleted	da39a3ee5e6b4b0d3255bfef95601890						
Rooted physical extraction and exportation of "Deleted" file via Magnet Axiom Examine	Windows CRC SHA	<p>Checksum information</p> <p>Name 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 Size 0 bytes CRC32 00000000 CRC64 0000000000000000 SHA256 E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B85 SHA1 DA39A3EE5E6B4B0D3255BFEF95601890AFD80709 BLAKE2sp DD0E891776933F43C7D032B08A917E25741F8AA9A12C12E1CAC8801500F2CA</p>						

The following 256-bit digest matched across all logical forensic data acquisition methods for the file entitled "9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0":

SHA256:

A58640187B69136300C6FB287B84A12FF21C6C049D3B752390ECC1323C913992

The following 160-bit digest matched across all logical forensic data acquisition methods for the file entitled “9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0”:

SHA1:

25a9c442b21f6a04eef8af0fa729912a5030105b

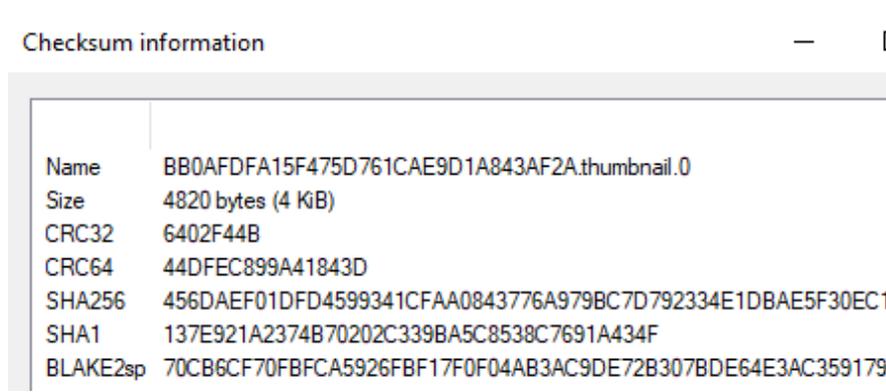
WEBP image files with “mini_thumbnail” in their file name and “.0” as their extension, were not extracted by Magnet Axiom since photographs and videos within Snapchat Memories must be opened and recently accessed to generate those particular files. Past “mini_thumbnail” files generated were deleted by the cloud server.

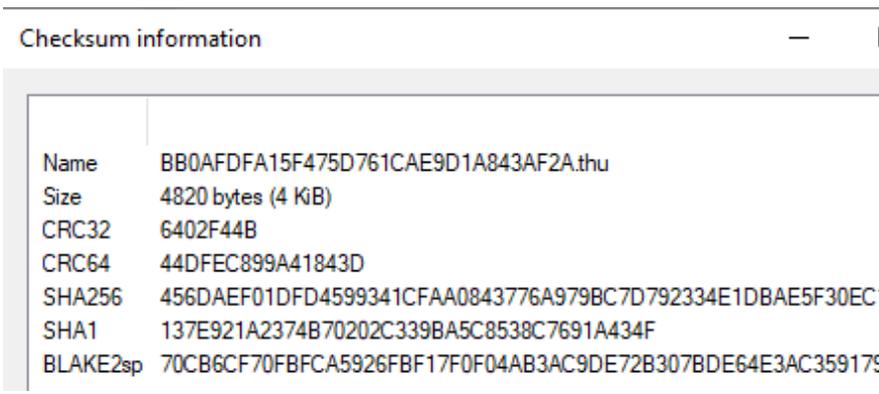
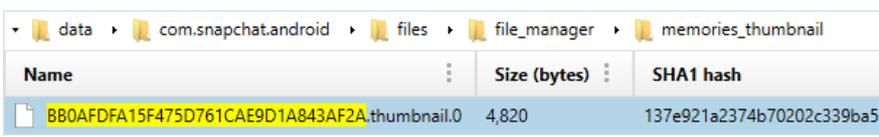
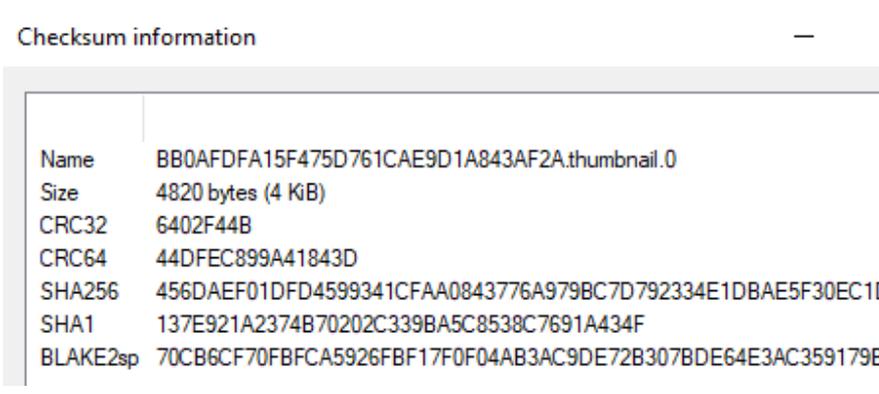
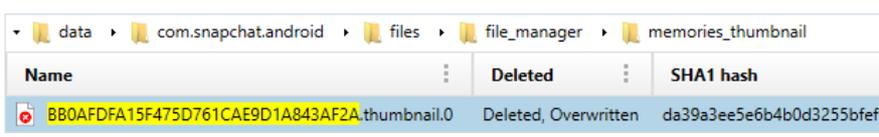
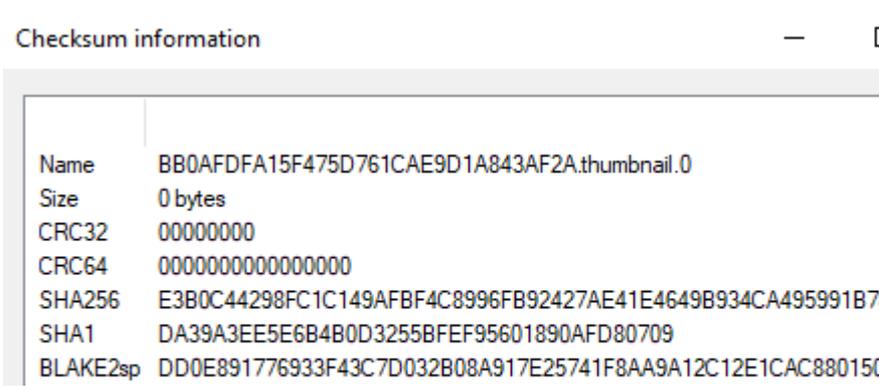
Windows CRC SHA and Magnet Axiom Examine’s 160-bit digest matched for the “deleted” file entitled “9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0”:

SHA1:

da39a3ee5e6b4b0d3255bfef95601890afd80709

Table 56. SHA Extraction method comparison for webp image file from /memories_thumbnail

Acquisition method	SHA Tool	SHA digests for BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0														
Rooted file system access to sandbox smartphone	ADB shell sha[x]sum	<pre>>adb shell lavender:/ \$ su lavender:/ # cd /data/data/com.snapchat.android/files/file_manager/memories_thumbnail lavender:/data/data/com.snapchat.android/files/file_manager/memories_thumbnail # sha256sum BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0 456daef01dfd4599341cfaa0843776a979bc7d792334e1dbae5f30ec1d0cb221 BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0 lavender:/data/data/com.snapchat.android/files/file_manager/memories_thumbnail # sha1sum BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0 137e921a2374b70202c339ba5c8538c7691a434f BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0</pre>														
Rooted logical extraction via ADB pull	Windows CRC SHA	 <p>Checksum information</p> <table border="1"><tr><td>Name</td><td>BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0</td></tr><tr><td>Size</td><td>4820 bytes (4 KiB)</td></tr><tr><td>CRC32</td><td>6402F44B</td></tr><tr><td>CRC64</td><td>44DFEC899A41843D</td></tr><tr><td>SHA256</td><td>456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1D0CB221</td></tr><tr><td>SHA1</td><td>137E921A2374B70202C339BA5C8538C7691A434F</td></tr><tr><td>BLAKE2sp</td><td>70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179</td></tr></table>	Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	Size	4820 bytes (4 KiB)	CRC32	6402F44B	CRC64	44DFEC899A41843D	SHA256	456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1D0CB221	SHA1	137E921A2374B70202C339BA5C8538C7691A434F	BLAKE2sp	70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179
Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0															
Size	4820 bytes (4 KiB)															
CRC32	6402F44B															
CRC64	44DFEC899A41843D															
SHA256	456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1D0CB221															
SHA1	137E921A2374B70202C339BA5C8538C7691A434F															
BLAKE2sp	70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179															

<p>Rooted logical extraction via TWRP copy/ADB Backup</p>	<p>Windows CRC SHA</p>	 <p>Checksum information</p> <table border="1"> <tr><td>Name</td><td>BB0AFDFA15F475D761CAE9D1A843AF2A.thu</td></tr> <tr><td>Size</td><td>4820 bytes (4 KiB)</td></tr> <tr><td>CRC32</td><td>6402F44B</td></tr> <tr><td>CRC64</td><td>44DFEC899A41843D</td></tr> <tr><td>SHA256</td><td>456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1</td></tr> <tr><td>SHA1</td><td>137E921A2374B70202C339BA5C8538C7691A434F</td></tr> <tr><td>BLAKE2sp</td><td>70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179</td></tr> </table>	Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thu	Size	4820 bytes (4 KiB)	CRC32	6402F44B	CRC64	44DFEC899A41843D	SHA256	456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1	SHA1	137E921A2374B70202C339BA5C8538C7691A434F	BLAKE2sp	70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179
Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thu															
Size	4820 bytes (4 KiB)															
CRC32	6402F44B															
CRC64	44DFEC899A41843D															
SHA256	456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1															
SHA1	137E921A2374B70202C339BA5C8538C7691A434F															
BLAKE2sp	70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179															
<p>Rooted physical extraction of file from Magnet Axiom Examine</p>	<p>Magnet Axiom</p>	 <p>data > com.snapchat.android > files > file_manager > memories_thumbnail</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Size (bytes)</th> <th>SHA1 hash</th> </tr> </thead> <tbody> <tr> <td>BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0</td> <td>4,820</td> <td>137e921a2374b70202c339ba5c8538c7691a434f</td> </tr> </tbody> </table>	Name	Size (bytes)	SHA1 hash	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	4,820	137e921a2374b70202c339ba5c8538c7691a434f								
Name	Size (bytes)	SHA1 hash														
BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	4,820	137e921a2374b70202c339ba5c8538c7691a434f														
<p>Rooted physical extraction and exportation of file from Magnet Axiom Examine</p>		 <p>Checksum information</p> <table border="1"> <tr><td>Name</td><td>BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0</td></tr> <tr><td>Size</td><td>4820 bytes (4 KiB)</td></tr> <tr><td>CRC32</td><td>6402F44B</td></tr> <tr><td>CRC64</td><td>44DFEC899A41843D</td></tr> <tr><td>SHA256</td><td>456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1</td></tr> <tr><td>SHA1</td><td>137E921A2374B70202C339BA5C8538C7691A434F</td></tr> <tr><td>BLAKE2sp</td><td>70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179B</td></tr> </table>	Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	Size	4820 bytes (4 KiB)	CRC32	6402F44B	CRC64	44DFEC899A41843D	SHA256	456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1	SHA1	137E921A2374B70202C339BA5C8538C7691A434F	BLAKE2sp	70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179B
Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0															
Size	4820 bytes (4 KiB)															
CRC32	6402F44B															
CRC64	44DFEC899A41843D															
SHA256	456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1															
SHA1	137E921A2374B70202C339BA5C8538C7691A434F															
BLAKE2sp	70CB6CF70FBFCA5926FBF17F0F04AB3AC9DE72B307BDE64E3AC359179B															
<p>Rooted physical extraction of "Deleted, Overwritten" file from Magnet Axiom Examine</p>	<p>Magnet Axiom</p>	 <p>data > com.snapchat.android > files > file_manager > memories_thumbnail</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Deleted</th> <th>SHA1 hash</th> </tr> </thead> <tbody> <tr> <td>BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0</td> <td>Deleted, Overwritten</td> <td>da39a3ee5e6b4b0d3255bfe9</td> </tr> </tbody> </table>	Name	Deleted	SHA1 hash	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	Deleted, Overwritten	da39a3ee5e6b4b0d3255bfe9								
Name	Deleted	SHA1 hash														
BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	Deleted, Overwritten	da39a3ee5e6b4b0d3255bfe9														
<p>Rooted physical extraction and exportation of "Deleted, Overwritten" file from Magnet Axiom Examine</p>	<p>Windows CRC SHA</p>	 <p>Checksum information</p> <table border="1"> <tr><td>Name</td><td>BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0</td></tr> <tr><td>Size</td><td>0 bytes</td></tr> <tr><td>CRC32</td><td>00000000</td></tr> <tr><td>CRC64</td><td>0000000000000000</td></tr> <tr><td>SHA256</td><td>E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B93CA495991B78</td></tr> <tr><td>SHA1</td><td>DA39A3EE5E6B4B0D3255BFE95601890AFD80709</td></tr> <tr><td>BLAKE2sp</td><td>DD0E891776933F43C7D032B08A917E25741F8AA9A12C12E1CAC880150</td></tr> </table>	Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	Size	0 bytes	CRC32	00000000	CRC64	0000000000000000	SHA256	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B93CA495991B78	SHA1	DA39A3EE5E6B4B0D3255BFE95601890AFD80709	BLAKE2sp	DD0E891776933F43C7D032B08A917E25741F8AA9A12C12E1CAC880150
Name	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0															
Size	0 bytes															
CRC32	00000000															
CRC64	0000000000000000															
SHA256	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B93CA495991B78															
SHA1	DA39A3EE5E6B4B0D3255BFE95601890AFD80709															
BLAKE2sp	DD0E891776933F43C7D032B08A917E25741F8AA9A12C12E1CAC880150															

The following 256-bit digest matched across all forensic data acquisition methods for the file entitled "BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0":

SHA256:

456DAEF01DFD4599341CFAA0843776A979BC7D792334E1DBAE5F30EC1D0CB221

The following 160-bit digest matched across all forensic data acquisition methods for the file entitled “BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0”:

SHA1:

137E921A2374B70202C339BA5C8538C7691A434F

Windows CRC SHA and Magnet Axiom Examine’s 160-bit digest matched for the “Deleted, Overwritten” file entitled “BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0”:

SHA1:

Da39a3ee5e6b4b0d3255bfef95601890afd80709

7.1.4 Biometric detection

Biometric facial detection is contingent on Forensic exams X and XIII being performed prior, as such, all methods and tools used prior are also required in order to perform facial recognition analysis on the data extracted. See Table X for additional tools required for facial recognition analysis.

Table 57. Biometric detection: Additional tools required for facial recognition analysis

Device	Software and peripherals
Laptop	<ul style="list-style-type: none">- Autopsy 4.13.0 [251]- Magnet Axiom v4.7.0.22371<ul style="list-style-type: none">- Magnet.AI module- Opera web browser v72.0.3815.400

Magnet Axiom’s Magnet.AI module was used to detect, categorize, and tag evidence artifacts of “possible human faces” [241].

Magnet.AI is not capable of uniquely identifying individual’s faces, it is only able to detect “possible human faces” and “pictures that are generally similar, such as pictures of the same room or pictures with similar scenery” [242] which is “based on a picture's general attributes, rather than specific details such as small objects or faces” [242].

An initial facial detection scan was performed on a “Quick Image” logical extraction from the non-rooted Samsung Galaxy S10e (SM-G970F) with Magnet Axiom’s Magnet.AI software.

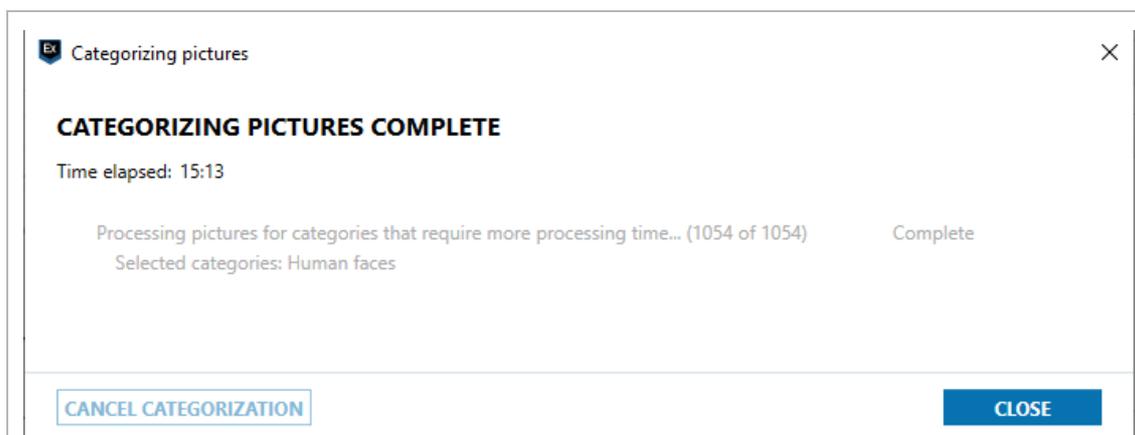
A second facial detection scan was performed with Magnet.AI on the rooted sandbox smartphone (Xiaomi Redmi Note 7) while logged into the smart eyewear’s cloud server.

The researcher, as a participant observer of the smart eyewear ecosystem, acted as both the forensic investigator and the smart eyewear/smartphone/data owner. The smart eyewear and the paired smartphone have not been rooted; neither the owner of the devices nor the forensic investigator have administrative privilege to those devices. The forensic investigator only possesses administrative privilege to their sandbox smartphone. Chain of custody, network access, system administration status parallel Forensic exam X, see Table x.

7.1.4.1 Biometric detection on non-rooted logical extraction

The Magnet.AI facial recognition scan of a “Quick Image” logical extraction from the non-rooted target smartphone (Samsung Galaxy S10e SM-G970F) with Magnet Axiom’s Process software detected 24 .jpg image files of “possible human faces”, out of 1,054 pictures within 15 minutes and 13 seconds, see Table x and figures x-x.

Files containing “possible human faces” are tagged with the color orange by Magnet.AI; however, the facial recognition scan only detected and accurately tagged .jpg files exported from the smart eyewear within the /Spectacles directory and relative thumbnails within the /Pictures/.thumbnails directory. (Table x) Magnet.AI failed to detect any “possible human faces” within the .mp4 video files and any other thumbnail directories. (Tables x-x)



(a)

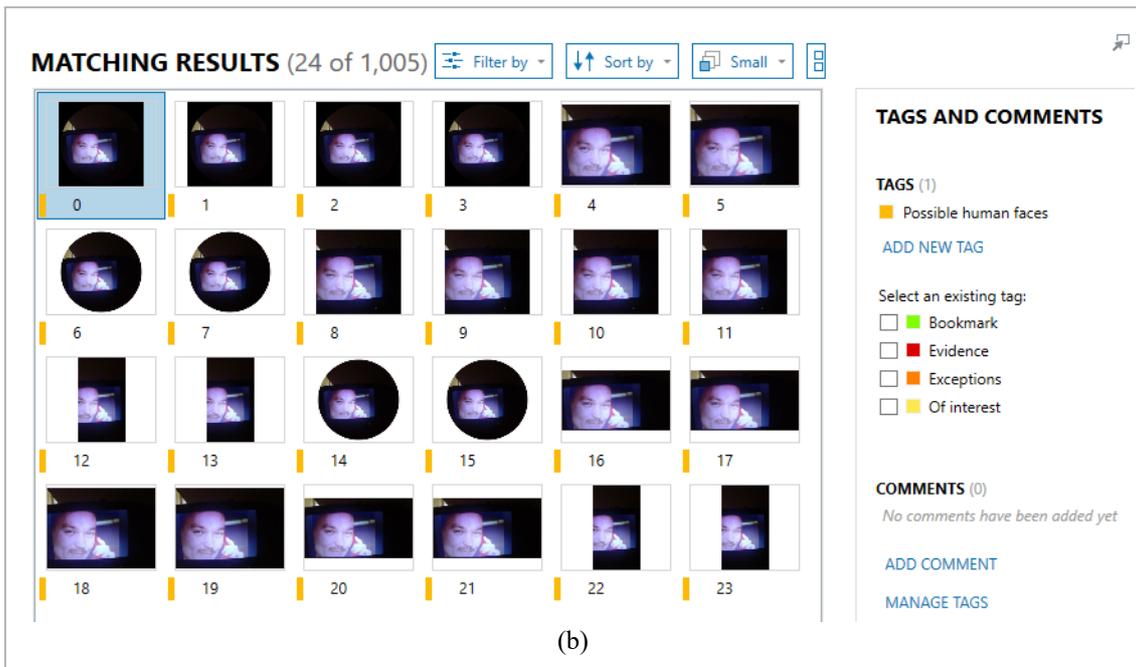


Figure 78. Biometric detection: Scan of non-rooted target smartphone (Samsung Galaxy S10e SM-G970F) with Magnet Axiom’s Magnet.AI Categorization module found 24 “Possible human faces”

Of the 24 images found, 12 were duplicates created by Magnet Axiom’s two differing extraction zipping methods: adb-data.tar and sdcard.tar.gz, 6 were .jpg images, and 6 were relative .jpg thumbnails.

The “Quick Image” extraction parallels results from Forensic exam VI., minus the duplicates.

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
Snapchat-12273941.jpg	File	.jpg	183,880	7/21/2020 1:58:12 PM	4edce4673d13ecf5
Snapchat-1508484665.jpg	File	.jpg	361,667	7/21/2020 1:58:12 PM	a0eaea4f18b0f2fac
Snapchat-1719961379.jpg	File	.jpg	337,005	7/21/2020 1:58:12 PM	551eb55a926d823
Snapchat-479651205.jpg	File	.jpg	179,029	7/21/2020 1:58:12 PM	954332435f79900e
Snapchat-513577310.jpg	File	.jpg	210,090	7/21/2020 1:58:12 PM	1581c275eec87f55
Snapchat-590366677.jpg	File	.jpg	236,405	7/21/2020 1:58:12 PM	bc946bd7eb1d8d4
Snapchat-1077365003.mp4	File	.mp4	9,911,818	7/21/2020 2:04:04 PM	b9777046f973db2
Snapchat-1149420760.mp4	File	.mp4	9,943,765	7/21/2020 2:04:04 PM	1ecb091e8b4951e
Snapchat-1166918296.mp4	File	.mp4	9,943,765	7/21/2020 2:04:04 PM	78b1017adfd5a13i
Snapchat-1379507228.mp4	File	.mp4	9,903,289	7/21/2020 2:04:04 PM	8c48f9a43966afdfc
Snapchat-239563438.mp4	File	.mp4	9,913,400	7/21/2020 2:04:04 PM	0a386474090702f5
Snapchat-486401862.mp4	File	.mp4	9,914,177	7/21/2020 2:04:04 PM	de20aad28f2aa4d

ALL EVIDENCE > samsung SM-G970F Quick Image.zip > adb-data.tar > shared > 0 > Pictures > .thumbnails

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
248.jpg	File	.jpg	41,979	7/31/2020 1:55:44 AM	58b4ba3caeebef0b0e
249.jpg	File	.jpg	46,419	7/31/2020 1:55:44 AM	c7c542ee52c4ec0300
250.jpg	File	.jpg	40,048	7/31/2020 1:55:44 AM	1a6d1a8f9e515c3560
251.jpg	File	.jpg	51,113	7/31/2020 1:55:44 AM	3ac2c7f69774eb3e9e
252.jpg	File	.jpg	43,778	7/31/2020 1:55:44 AM	3c6c7ef5738c26ea96
253.jpg	File	.jpg	35,434	7/31/2020 1:55:44 AM	099fc2f94043517d14

(b.)

ALL EVIDENCE > samsung SM-G970F Quick Image.zip > adb-data.tar > shared > 0 > DCIM > .thumbnails

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
1595390873376.jpg	File	.jpg	43,320	7/22/2020 7:07:53 AM	e34fd3bcaef571c72
1595390873380.jpg	File	.jpg	36,349	7/22/2020 7:07:53 AM	437666032af45a21
1595390873387.jpg	File	.jpg	30,849	7/22/2020 7:07:53 AM	e66e96c35c9f9b8c
1595390873388.jpg	File	.jpg	48,870	7/22/2020 7:07:53 AM	88f9ec43c7730acf4
1595429663878.jpg	File	.jpg	45,019	7/22/2020 5:54:23 PM	796ce8f3dd8f2c1e7
1595429663879.jpg	File	.jpg	45,019	7/22/2020 5:54:23 PM	796ce8f3dd8f2c1e7

(c.)

ALL EVIDENCE > samsung SM-G970F Quick Image.zip > adb-data.tar > shared > 0 > Movies > .thumbnails

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
244.jpg	File	.jpg	36,435	7/22/2020 7:07:53 AM	3341d2fc82d2e2cc34
245.jpg	File	.jpg	43,405	7/22/2020 7:07:53 AM	905ecaef4d1cd5a21c
246.jpg	File	.jpg	30,908	7/22/2020 7:07:53 AM	bccbc34d60dabb27b
247.jpg	File	.jpg	48,845	7/22/2020 7:07:53 AM	d314950254216e57a
254.jpg	File	.jpg	45,090	7/22/2020 5:54:23 PM	ce204ed961cf01b9d
255.jpg	File	.jpg	45,090	7/22/2020 5:54:23 PM	ce204ed961cf01b9d

(d.)

Figure 79. Biometric detection: Magnet Axiom extraction via adb-data.tar (a) Exported Spectacles .jpg and .mp4 files (b) “Pictures” > .thumbnails (c) “DCIM” > .thumbnails (d) “Movies” > .thumbnails

ALL EVIDENCE > samsung SM-G970F Quick Image.zip > sdc card.tar.gz > sdc card > Spectacles

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
Snapchat-12273941.jpg	File	.jpg	183,880	7/21/2020 1:58:12 PM	4edce4673d13ecf
Snapchat-1508484665.jpg	File	.jpg	361,667	7/21/2020 1:58:12 PM	a0eaea4f18b0f2fa
Snapchat-1719961379.jpg	File	.jpg	337,005	7/21/2020 1:58:12 PM	551eb55a926d823
Snapchat-479651205.jpg	File	.jpg	179,029	7/21/2020 1:58:12 PM	954332435f79900
Snapchat-513577310.jpg	File	.jpg	210,090	7/21/2020 1:58:12 PM	1581c275eec87f5f
Snapchat-590366677.jpg	File	.jpg	236,405	7/21/2020 1:58:12 PM	bc946bd7eb1d8d
Snapchat-1077365003.mp4	File	.mp4	9,911,818	7/21/2020 2:04:04 PM	b9777046f973db2
Snapchat-1149420760.mp4	File	.mp4	9,943,765	7/21/2020 2:04:04 PM	1ecb091e8b4951e
Snapchat-1166918296.mp4	File	.mp4	9,943,765	7/21/2020 2:04:04 PM	78b1017adfd5a13
Snapchat-1379507228.mp4	File	.mp4	9,903,289	7/21/2020 2:04:04 PM	8c48f9a43966afdf
Snapchat-239563438.mp4	File	.mp4	9,913,400	7/21/2020 2:04:04 PM	0a386474090702f
Snapchat-486401862.mp4	File	.mp4	9,914,177	7/21/2020 2:04:04 PM	de20aad28f2aa4d

(a.)

ALL EVIDENCE > samsung SM-G970F Quick Image.zip > sdc card.tar.gz > sdc card > Pictures > .thumbnails

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
248.jpg	File	.jpg	41,979	7/31/2020 1:55:44 AM	58b4ba3caeebef01
249.jpg	File	.jpg	46,419	7/31/2020 1:55:44 AM	c7c542ee52c4ec03
250.jpg	File	.jpg	40,048	7/31/2020 1:55:44 AM	1a6d1a8f9e515c3f
251.jpg	File	.jpg	51,113	7/31/2020 1:55:44 AM	3ac2c7f69774eb3e
252.jpg	File	.jpg	43,778	7/31/2020 1:55:44 AM	3c6c7ef5738c26ea
253.jpg	File	.jpg	35,434	7/31/2020 1:55:44 AM	099fc2f94043517d

(b.)

ALL EVIDENCE > samsung SM-G970F Quick Image.zip > sdc card.tar.gz > sdc card > DCIM > .thumbnails

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
1595390873376.jpg	File	.jpg	43,320	7/22/2020 7:07:53 AM	e34fd3bcaef571c72
1595390873380.jpg	File	.jpg	36,349	7/22/2020 7:07:53 AM	437666032af45a21f
1595390873387.jpg	File	.jpg	30,849	7/22/2020 7:07:53 AM	e66e96c35c9f9b8c5
1595390873388.jpg	File	.jpg	48,870	7/22/2020 7:07:53 AM	88f9ec43c7730acf4f
1595429663878.jpg	File	.jpg	45,019	7/22/2020 5:54:23 PM	796ce8f3dd8f2c1e7
1595429663879.jpg	File	.jpg	45,019	7/22/2020 5:54:23 PM	796ce8f3dd8f2c1e7

(c.)

ALL EVIDENCE > samsung SM-G970F Quick Image.zip > sdc card.tar.gz > sdc card > Movies > .thumbnails

Name	Type	File extension	Size (bytes)	Modified	SHA1 hash
244.jpg	File	.jpg	36,435	7/22/2020 7:07:53 AM	3341d2fc82d2e2cc
245.jpg	File	.jpg	43,405	7/22/2020 7:07:53 AM	905ecaef4d1cd5a2
246.jpg	File	.jpg	30,908	7/22/2020 7:07:53 AM	bccbc34d60dabb27
247.jpg	File	.jpg	48,845	7/22/2020 7:07:53 AM	d314950254216e57
254.jpg	File	.jpg	45,090	7/22/2020 5:54:23 PM	ce204ed961cf01b9
255.jpg	File	.jpg	45,090	7/22/2020 5:54:23 PM	ce204ed961cf01b9

(d.)

Figure 80. Biometric detection: Magnet Axiom extraction via sdc card.tar.gz (a) Exported Spectacles .jpg and .mp4 files (b) "Pictures" > .thumbnails (c) "DCIM" > .thumbnails (d) "Movies" > .thumbnails

It was necessary to manually tag 36 files containing facial biometric information, missed by Magnet.AI's automated process [242].

Filters: Evidence, Artifacts, Content types, Date and time, Possible human faces, Profiles, Partial results, CLEAR FILTERS, Type a search term..., GO, ADVANCED

Matched Files: Keyword lists, Skin tone, Media categorization, Media attributes (VICs), Similar pictures

MATCHING RESULTS (60 of 18,048)

Item	Type
Snapshot-12273941.jpg	Pictures
Snapshot-1508484665.jpg	Pictures
Snapshot-590366677.jpg	Pictures
Snapshot-479651205.jpg	Pictures
Snapshot-513577310.jpg	Pictures
Snapshot-1719961379.jpg	Pictures
249.jpg	Pictures
252.jpg	Pictures
250.jpg	Pictures
253.jpg	Pictures
251.jpg	Pictures
1595390873380.jpg	Pictures
248.jpg	Pictures
1595390873388.jpg	Pictures
1595429663879.jpg	Pictures
1595429663878.jpg	Pictures
1595390873387.jpg	Pictures
1595390873376.jpg	Pictures
254.jpg	Pictures

Preview: Snapchat-513577310.jpg

Tags, Profiles & Media Categories:

Time zone UTC+2:00

(a)

Filters: Evidence, Artifacts, Content types, Date and time, Possible human faces, Profiles, Partial results, CLEAR FILTERS, Type a search term..., GO, ADVANCED

Matched Files: Keyword lists, Skin tone, Media categorization, Media attributes (VICs), Similar pictures

MATCHING RESULTS (60 of 18,048)

Item	Type
1595390873376.jpg	Pictures
254.jpg	Pictures
244.jpg	Pictures
246.jpg	Pictures
255.jpg	Pictures
247.jpg	Pictures
245.jpg	Pictures
Snapshot-1077365003.mp4	MP4
Snapshot-1149420760.mp4	MP4
Snapshot-1166918296.mp4	MP4
Snapshot-1379507228.mp4	MP4
Snapshot-239563438.mp4	MP4
Snapshot-486401862.mp4	MP4
Snapshot-1077365003.mp4	MP4
Snapshot-1149420760.mp4	MP4
Snapshot-1166918296.mp4	MP4
Snapshot-1379507228.mp4	MP4
Snapshot-239563438.mp4	MP4
Snapshot-486401862.mp4	MP4

Preview: Samsung SM-G970F Quick Image

Details: ARTIFACT INFORMATION

Time zone UTC+2:00

(b)

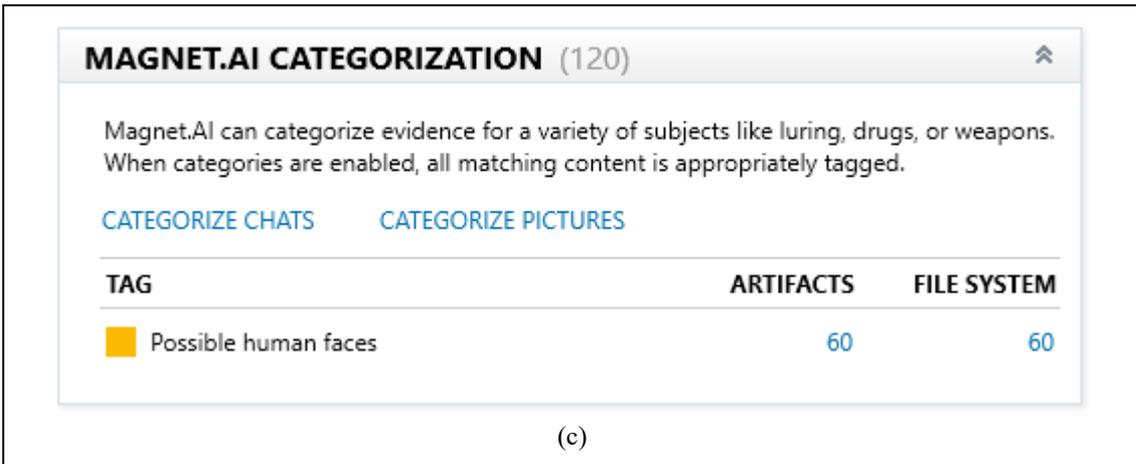


Figure 81. Biometric detection: 60 confirmed total artifacts within file system after manually tagging missed biometric images (a) Magnet AI Categorization summary (b) Details of JPG file from /Spectacles directory (c) Details of MP4 file from /Spectacles directory

7.1.4.2 Biometric detection on rooted physical extraction

Magnet.AI’s facial detection scan of a full image physical extraction from Forensic exam XIII detected 137 files of “possible human faces”, out of 44,400 pictures (carved .png and .jpg files) and 181 videos (carved .mp4 files) within 14 minutes, see Table x and figures x-x.

However, none of 137 files detected by Magnet Axiom were captured by the smart eyewear and stored by the smart eyewear cloud server within the smart eyewear mobile application.

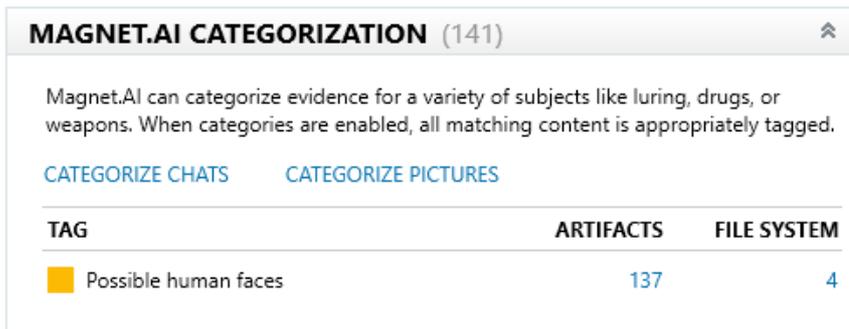
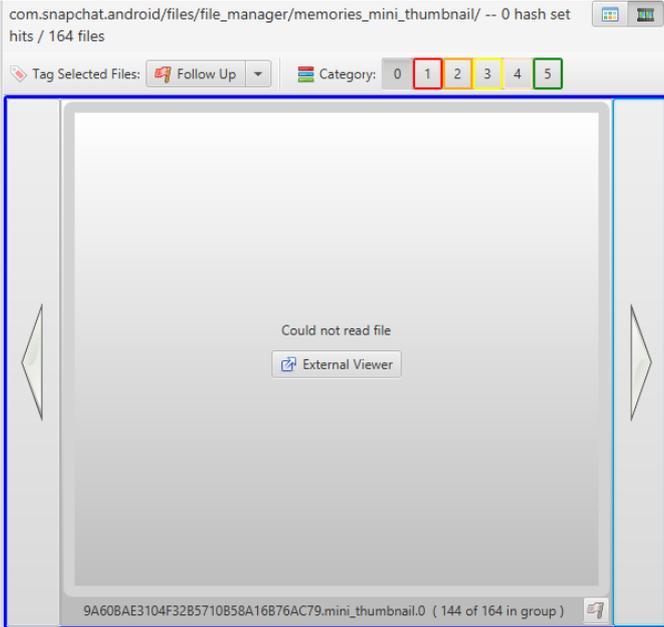
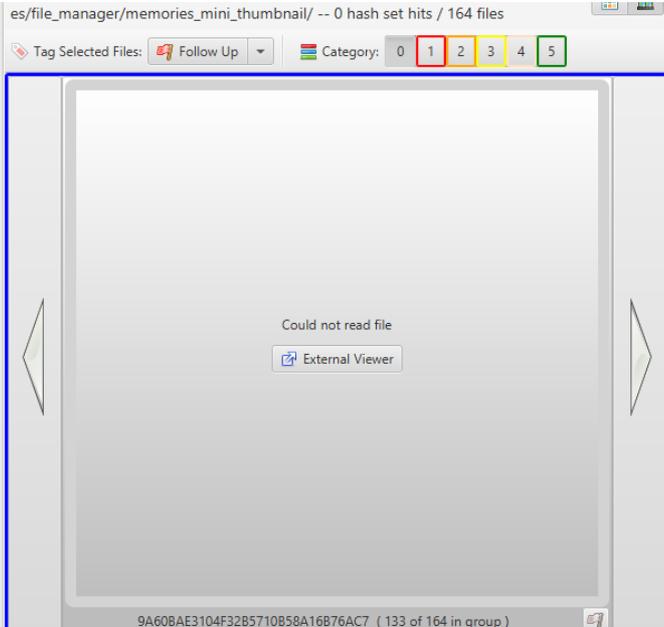


Figure X. Biometric detection: Magnet Axioms detection of “possible human faces” within physical image of sandbox smartphone from Forensic exam XIII

Neither Autopsy 4.13.0 nor Magnet Axiom v4.7.0.22371 were capable of automatically generating and displaying visual images of the webp image files concealed by Snap Inc. developers with “.0” file type extensions (Tables X-X).

The inability to display webp images could be attributed to the inability to identify file signature mismatches between files with “.0” file type extensions and “image/webp” MIME file types within file signature headers (Tables X-X).

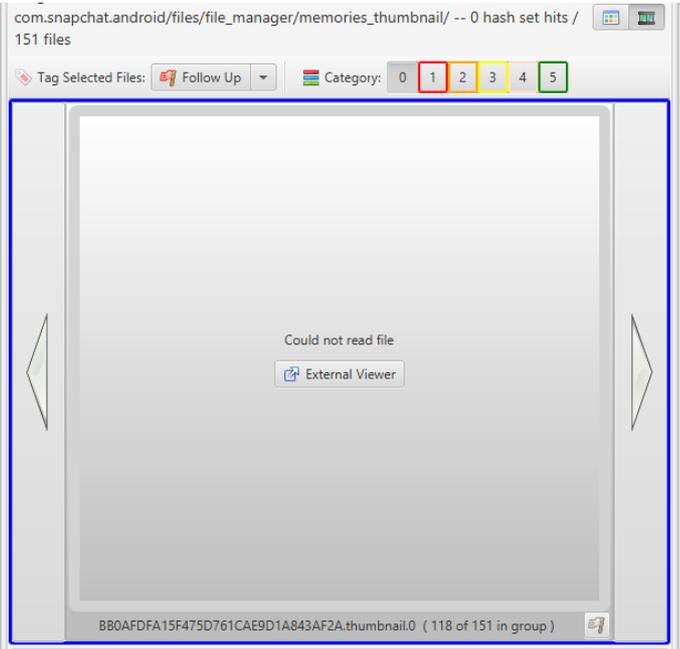
Table 58. Biometric detection: Imaging tool comparison for 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

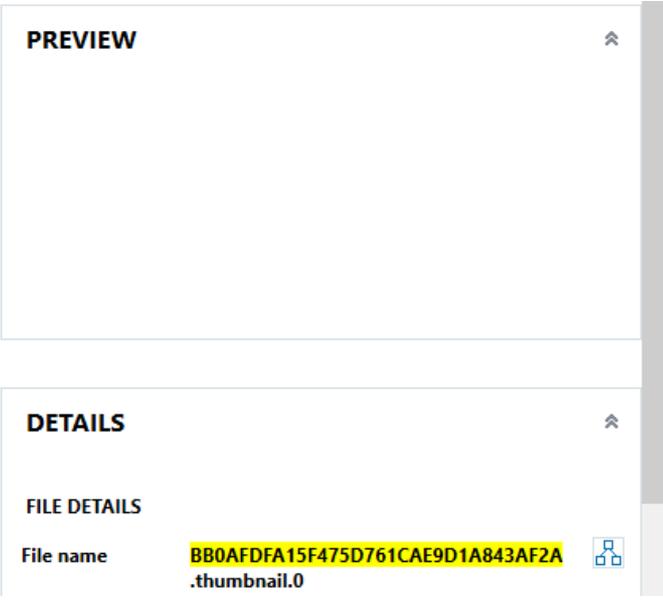
Acquisition method	Imaging Tool	Image Preview of: 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
Rooted logical extraction via ADB Pull	Autopsy v4.13.0	
Rooted logical extraction via TWRP copy/ADB Backup	Autopsy v4.13.0	
Rooted physical extraction of file via Magnet Axiom Examine	Magnet Axiom v4.7.0.22371	Not Available*

<p>Rooted physical extraction of "Deleted" file via Magnet Axiom Examine</p>	<p>Magnet Axiom v4.7.0.22371</p>	<div data-bbox="651 215 1289 551"> <p>PREVIEW </p> </div> <div data-bbox="651 600 1289 810"> <p>DETAILS </p> <p>FILE DETAILS</p> <p>File name 9A60BAE3104F32B5710B58A16B76AC79.  mini_thumbnail.0</p> </div>
--	----------------------------------	--

* Initial thumbnails and mini thumbnails generated prior to the physical extraction via Magnet Axiom were respectively "Deleted, Overwritten" or "Deleted" when the physical image of the device was created; this may be attributed to two possible factors: (a) photographs and videos within Snapchat Memories had not recently been opened and thus failed to generate or (b) the need to connect to the university's server to access the Magnet Axiom program resulted in deleting, overwriting, and replacing the thumbnails and deleting mini thumbnails without replacing those artifacts.

Table 59. Biometric detection: Imaging tool comparison for BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

Acquisition method	Imaging Tool	Image Preview of: BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
Rooted logical extraction via ADB Pull	Autopsy v4.13.0	
Rooted logical extraction via TWRP copy/ADB Backup	Autopsy v4.13.0	

<p>Rooted physical extraction of file via Magnet Axiom Examine</p>	<p>Magnet Axiom v4.7.0.22371</p>	 <p>PREVIEW</p> <pre> WEBPVP8 hp en >I^[0r] i 6*{4-" Cs5* X_?_[H </pre> <p>DETAILS</p> <p>FILE DETAILS</p> <p>File name BB0AFDFA15F475D761CAE9D1A843AF2A  .thumbnail.0</p>
<p>Rooted physical extraction of "Deleted, Overwritten" file via Magnet Axiom Examine</p>	<p>Magnet Axiom v4.7.0.22371</p>	 <p>PREVIEW</p> <p>DETAILS</p> <p>FILE DETAILS</p> <p>File name BB0AFDFA15F475D761CAE9D1A843AF2A  .thumbnail.0</p>

Although Autopsy 4.13.0 and Magnet Axiom v4.7.0.22371 were not capable of identifying file signature mismatches between files with “.0” file type extensions and “image/webp” MIME file types within file signature headers the programs were capable of identifying the following mismatches:

Autopsy v4.13.0 was capable of detecting file signature mismatches for “image/jpeg”; “image/png”; “text/plain” MIME file types with various file type extensions including “.0” and blank fields. (Figure x) And Magnet Axiom v4.7.0.22371 was capable of detecting file signature mismatches for “image/png”; “image/jpeg”; “image/webp” MIME file types but only if they possessed file extension types of “application/octet-stream” (which in all cases, the file extension was left empty) (Figure x).

Extension Mismatch Detected		
Table Thumbnail		
Source File	Extension	△ MIME Type
wallpaper-stage		image/jpeg
7d950f9a3692cf7df227d883a47e352b.0	0	image/jpeg
CA45749B9B0B04019A09DB44A30AAC19.static-map_	static-map_	image/jpeg
CA45749B9B0B04019A09DB44A30AAC19.static-map.0	0	image/jpeg
1023196729		image/png
4244383362		image/png
d2b89730b525093f070df7dbe8bbefb3.0	0	image/png
4244383362		image/png
1023196729		image/png
1023196729		image/png
4244383362		image/png
4244383362		image/png
1023196729		image/png
4244383362		image/png
1023196729		image/png
BFE574266146A632FB7CAF2768D918E5.silho	silho	image/png
BFE574266146A632FB7CAF2768D918E5.silhouette.0	0	image/png

(a)

Extension Mismatch Detected		
Table Thumbnail		
Source File	Extension	△ MIME Type
0228660519E053AF8FBD40C82257D5FB.thumbnail.0	0	text/plain
0237CACF772391EB779E6041AB5B775F.mini_thumbnail.0	0	text/plain
03880EC2154AD99C63FD94094CBA2530.mini_thumbnail.0	0	text/plain
03CAF1AB739D2CDA58C7873DC8CBE6DC.mini_thumbnail.0	0	text/plain
057C119889FC146EEFB7A75B3F771DCB.thumbnail.0	0	text/plain
05B4414E845DF63E9268FB2B1F832F26.mini_thumbnail.0	0	text/plain
05B589B85228F0EBC20DDFB5D2F748D6.mini_thumbnail.0	0	text/plain
064FBB1F63925F349410B8BD38F9F339.thumbnail.0	0	text/plain
068A5170A1B23F0CC179CBE06C283307.mini_thumbnail.0	0	text/plain
069C280ABE4CA581CA4831F4CAE1E257.thumbnail.0	0	text/plain

(b)

Figure 83. Biometric detection: File signature mismatch identification by Autopsy 4.13.0 (a)image/jpeg and image/png MIME Types (b) text/plain MIME Types

The screenshot shows the Magnet Axiom interface with a sidebar on the left and a main results pane. The sidebar includes a home icon, an 'Artifacts' dropdown, and a list of categories: MATCHING RESULTS (45,110), CHAT (1), MEDIA (44,640), OPERATING SYSTEM (469), Application Activity - Android (2), and File Signature Mismatch (Picture) (467). The main pane is titled 'MATCHING RESULTS (467 of 467)' and contains a table with columns for File Name, File Extension, File Type, and File Extension Type. The table lists several files, with the one having ID 158150bebf60e5c092055b0301... highlighted in blue.

File Name	File Extension	File Type	File Extension Type
12d88dd515b7b07567a8430175...		image/webp	application/octet-stream
12mps7x7d6w0860lzit9g1siw0		image/png	application/octet-stream
13s7g11v3mj6rkqpvwfczh4e0		image/png	application/octet-stream
13tct239b3vaxidb717bwjp4u0		image/png	application/octet-stream
158150bebf60e5c092055b0301...		image/webp	application/octet-stream
16rxerlrtdkxupwt6pwc6yvy40		image/png	application/octet-stream
172qlrmwvs148cifoltdlvno20		image/png	application/octet-stream
174a325fa3f		image/jpeg	application/octet-stream

Figure 84. Biometric detection: File signature mismatch identification by Magnet Axiom v4.7.0.22371

Of 467 file signature mismatches found by Magnet Axiom, 4 files were also flagged for containing “possible human faces” by the Magnet.AI module, none of which captured by the smart eyewear, nor did any contain biometric data from actual humans (but rather drawings of humans), see Figure X for results.

The screenshot shows the Magnet Axiom interface with a sidebar on the left and a main results pane. The sidebar includes a home icon, an 'Artifacts' dropdown, and a list of categories: MATCHING RESULTS (4), OPERATING SYSTEM (4), and File Signature Mismatch (Picture) (4). The main pane is titled 'MATCHING RESULTS (4 of 467)' and displays four items, each with a thumbnail image and text indicating a 'FILE SIGNATURE MISMATCH (PICTURE)'. The items are: 5p5s3kqwwwuwg9y7nz8kjwcw0 (Mario), 52bqp9gb3ygb46iv2vvmx5hs0 (woman's face), 12mps7x7d6w0860lzit9g1siw0 (woman's face), and 24bsz5p2zaf6oxoftqi2p23250 (man's face).

Figure 85. Biometric detection: File signature mismatches containing “possible human faces” detected by Magnet Axiom, from physical image of sandbox smartphone

Adding the WEBP MIME type combined with the “.0” file type extension as a custom file type to Magnet Axiom’s CustomFileTypeArtifacts.xlsx file failed to assist Magnet.AI in identifying, categorizing, and tagging any additional “possible human faces”, as illustrated in Tables x-x. However, this action did result in generating image content within Magnet Axiom’s Preview module for files within the “/memories_media” directory.

Red tags denote “evidence” files tagged by the researcher prior to adding the custom file type in order to flag all NBDDO files within the “/memories_media” and the “/memories_thumbnail” directories. No orange tags denoting “possible human faces” were generated by the system after re-running the Magnet.AI facial detection scan.

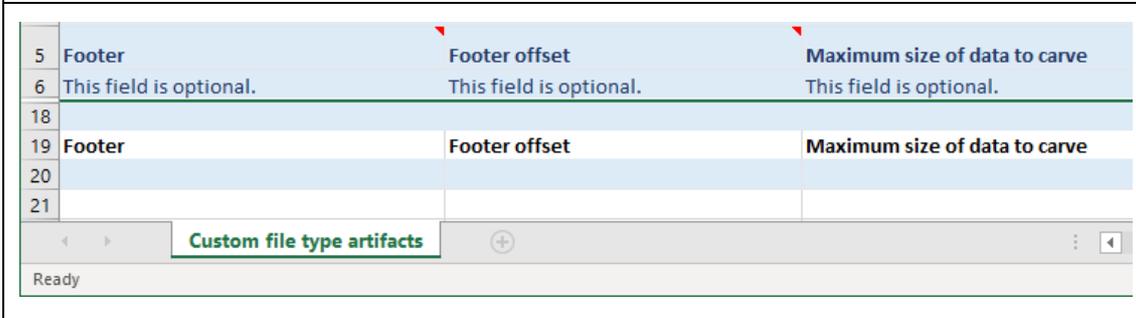
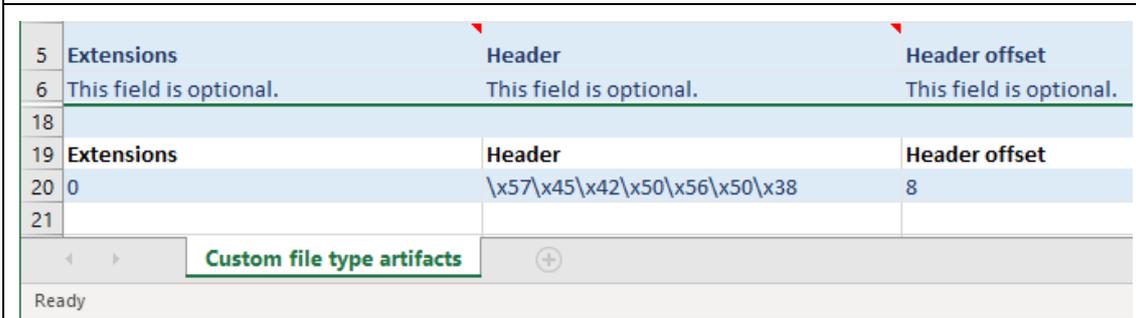
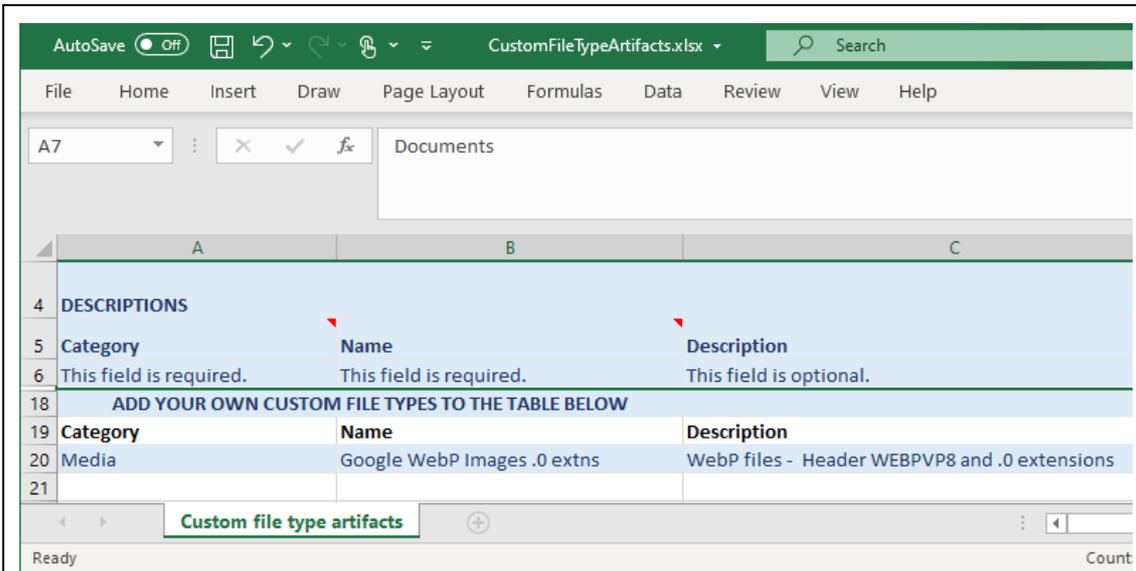


Figure 86. Addition of WEBP MIME type with a .0 extension to Magnet Axiom's Custom File Types list

MATCHING RESULTS (162 of 567,260) Column view **48C525AFEBE3225C89CFBFCED14...**

Item	Type	Artifact category
558CE4623F03EE2C50E1352D2A96D8C3.thumbnail.0	Files	Examiner defined
3007023AED31C27100E049570C93BC39.thumbnail.0	Files	Examiner defined
25BD771AF7AFA0A854AA9D7069D6FC979.thumbnail.0	Files	Examiner defined
980793CDDF59EAF807B05972DA8583CE.thumbnail.0	Files	Examiner defined
AEC52CC15B320F58FB0B53374A047390.thumbnail.0	Files	Examiner defined
48C525AFEBE3225C89CFBFCED14D4961.thumbnail.0	Files	Examiner defined
6684FC8EB5435C2FA2AA1B1F29BAE18F.thumbnail.0	Files	Examiner defined
3294D79258C87C801EAE06AF3248BFA8.thumbnail.0	Files	Examiner defined
57F4270924A6BB758DC1D51AAF43EC84.media.0	0	Tagged from file system
B308BFCB14861C7DA9A5A606BEA14754E.media.0	0	Tagged from file system
458A067D15EFB608ADF16AB3E75792B8.media.0	0	Tagged from file system
296A9EE84ABAC40AECCF8655169016A3.media.0	0	Tagged from file system
9462C63EEB60E63F2520BE8DA0FCEAAD.media.0	0	Tagged from file system
BE8DAC489D843981DA80DB5533FF3128.media.0	0	Tagged from file system
BDE0BD70916DCF9A5476ECACE3F7528E.media.0	0	Tagged from file system
63345E64B7972415E7BF74657F608437.media.0	0	Tagged from file system
27D9544FC224C254D2EFA44918103C87.media.0	0	Tagged from file system
37AA06CE2E4F9EC003040717CBA8B2E8.media.0	0	Tagged from file system
C082F6F30F3DBFBA1D4E21D09C37A624.media.0	0	Tagged from file system

PREVIEW

FIND

```

WEBPVP8
4z'p
e
9NjXas
i?)8hBW
TYvÛ2j7ÆÛq`©RM-[]NE

```

DETAILS

ARTIFACT INFORMATION

Name: 48C525AFEBE3225C89CFBFCED14D4961.thumbnail.0

Type: File

File extension: .0

File size: 6932

Created: 9/21/2020 1:18:55 AM

Time zone: UTC+2:00

Figure 87. Results of Magent.AI facial detection after addition of WEBP MIME type with a .0 extension to Magnet Axiom’s Custom File Types list Preview and details for file within “/memories_thumbnail” directory

In order to view image content for the WEBP files with mismatched file type extensions and file header signatures, the files were copied from the “/memories_mini_thumbnail” and “/memories_thumbnail” directories created after each data extraction and viewed within an offline web browser (Figure x).

The web browser was not connected to the Internet when viewing the files to ensure the artifacts remained isolated from any network connections, additionally, this viewing method did not require any modifications to each file’s file extension.

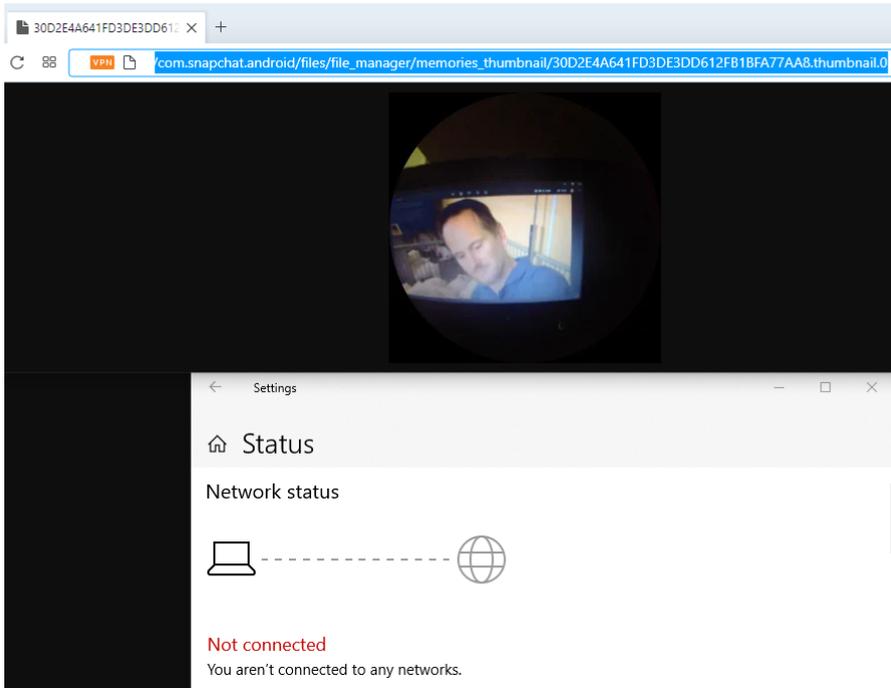


Figure 88. Biometric detection: Example of a webp file, with mismatched “.0” extension, from the “/memories_thumbnail” directory dragged and dropped into offline web browser

Visual observation provided additional validation that files extracted through differing forensic extraction methods yielded the same image content results (Table x). No biometric information could be discerned from files named “mini_thumbnail”, as the image size was too small to garner any viable information.

Table 60. Biometric detection: Extraction method comparison of webp thumbnail and mini thumbnail with offline web browser

Acquisition method	Web browser display of BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0	Web browser display with 500% enlargement of 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
Logical extraction via ADB pull		

<p>Logical extraction via TWRP copy/ADB Backup</p>		
<p>Physical extraction and exportation of file via Magnet Axiom Examine</p>		<p>Not Available*</p>
<p>Physical extraction and exportation of "Deleted, Overwritten" file via Magnet Axiom Examine</p>	<p>Empty file</p>	<p>Not applicable</p>
<p>Physical extraction and exportation of "Deleted" file via Magnet Axiom Examine</p>	<p>Not applicable</p>	<p>Empty file</p>

Changing the mismatched files' file extensions to match their file header signatures was attempted to try and garner more accurate facial detection results with Magnet Axiom's Magnet.AI.

11 NBDDO files from the
"/data/data/com.snapchat.android/files/file_manager/memories_media" directory and
151 NBDDO files from the
"/data/data/com.snapchat.android/files/file_manager/memories_thumbnail" directory

were exported as copies from Magnet Axiom. The “.0” file extensions on those files were bulk changed to “.webp” with the following cmd.exe command:

```
>ren *.0 *.webp
```

The altered files were then imported as new evidence into the Magnet Axiom case file to be scanned and categorized as “possible human faces” by the Magnet.AI module.

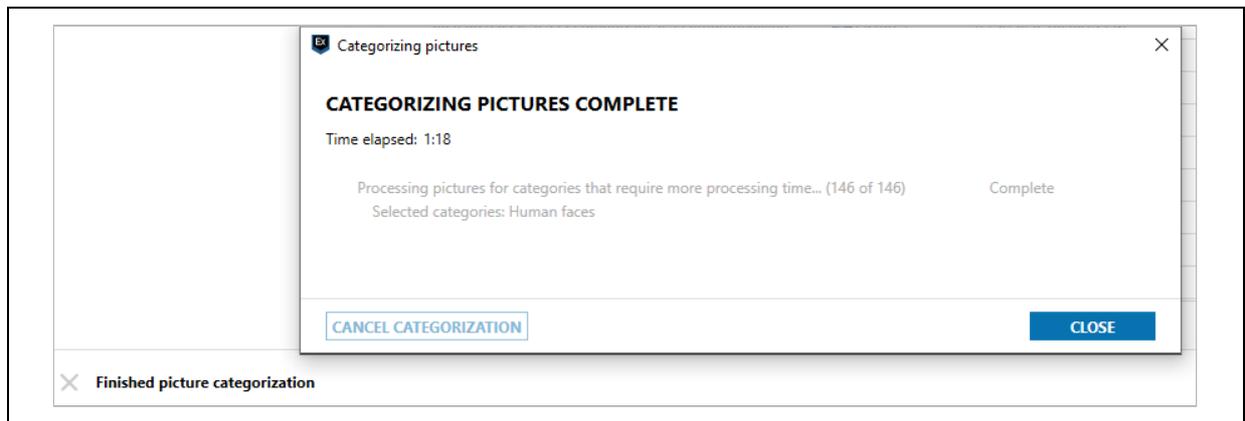
Table x

The facial detection module failed to categorize any of the .webp files as possessing biometric content, when various files did contain such content.

The aforementioned file extension altering process was repeated; however, in this instance the files’s file extensions were then changed to .jpg. This alteration enabled Magnet Axiom to accurately label each file as a picture and display its relative image content in the form of thumbnails; however, the Magnet.AI module still failed to recognize any biometric facial content within the files, as illustrated in Table x where no orange tags exist.

The Preview module also failed to accurately display the file’s image content, instead displaying the file’s text content.

```
>ren *.0 *.jpg
```



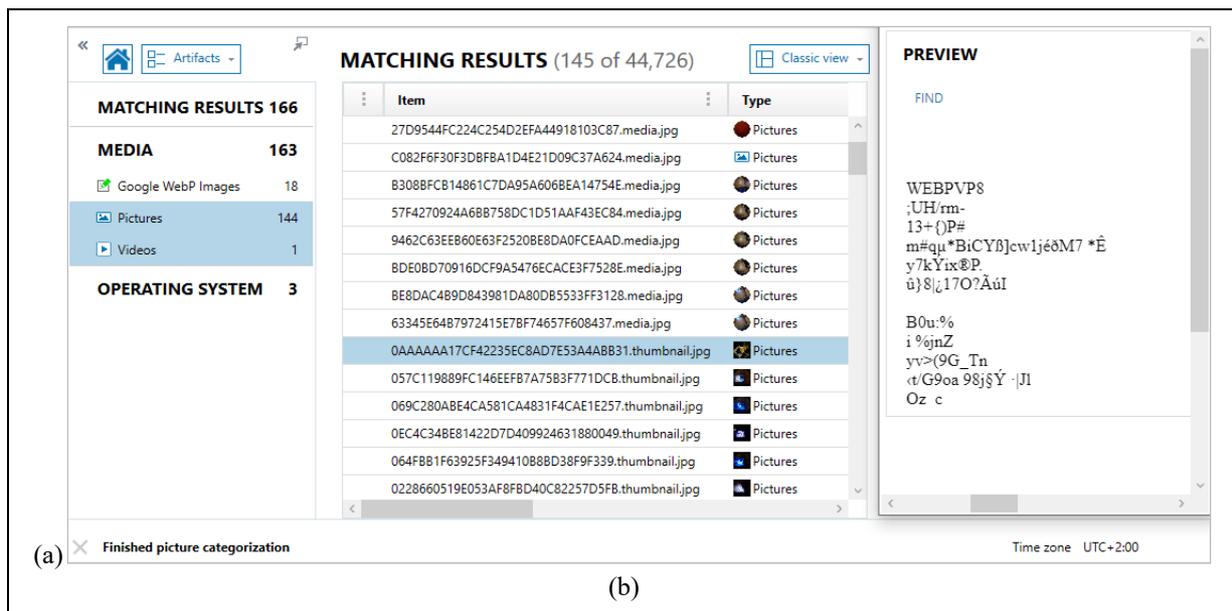


Figure 89. Failed facial detection with Magnet.AI after changing file extensions to .jpg

7.1.5 Database metadata

HxD Hex Editor v2.3.0.0 was used to locate each select mini thumbnail and thumbnail amongst all smart eyewear databases with the program’s “Find” search module. Both files were located within the database entitled “journal.db”.

DB Browser for SQLite v3.11.2 and the Journal module within Magnet Axiom v4.7.0.22371 were used to further examine and analyze the artifacts’ relative metadata. (Table x)

Matching metadata within “journal.db” provided further integrity verification of data extracted across various methods.

Table 61. Database metadata 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

/com.snapchat.android/files/file_manager/memories_mini_thumbnail/ 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0				
Rooted acquisition method				
	Logical extraction via ADB pull	Logical extraction via TWRP copy/ADB Backup	Physical extraction of file via Magnet Axiom Examine	Physical extraction and exportation of file via Magnet Axiom Examine
Metadata Tool				

	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-lp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-lp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2	Magnet Axiom v4.7.0.22371 Journal module	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-lp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2
Details				
id	698	698	Not available	Not available
journal_id	104	104		
key	9A60BAE3104F32B5710B58A16B76AC79. mini_thumbnail	9A60BAE3104F32B5710B58A16B76AC79. mini_thumbnail		
sequence_number	69	69		
value_count	1	1		
status	1	1		
last_update_time	1600640320024	1600640320024		
last_update_time [244]	Monday, September 21, 2020 1:18:40.024 AM GMT+03:00 DST	Monday, September 21, 2020 1:18:40.024 AM GMT+03:00 DST		
last_read_time	1600641510009	1600641510009		
last_read_time [244]	Monday, September 21, 2020 1:38:30.009 AM GMT+03:00 DST	Monday, September 21, 2020 1:38:30.009 AM GMT+03:00 DST		
lock_count	0	0		
total_size	96	96		
value_sizes (Binary)	Blob	Blob		
value_sizes (HEX)	0000 00 00 00 00 00 00 00 60	0000 00 00 00 00 00 00 00 60		
value_sizes (ASCII)``		
value_sizes (Decimal)	96	96		
expiration	1601851110009	1601851110009		
expiration [244]	Monday, October 5, 2020 1:38:30.009 AM GMT+03:00 DST	Monday, October 5, 2020 1:38:30.009 AM GMT+03:00 DST		
last_consumed_time	1600641510009	1600641510009		
last_consumed_time [244]	Monday, September 21, 2020 1:38:30.009 AM GMT+03:00 DST	Monday, September 21, 2020 1:38:30.009 AM GMT+03:00 DST		

Table 62. Database metadata BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

/com.snapchat.android/files/file_manager/memories_thumbnail/ BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0				
Rooted acquisition method				
	Logical extraction via ADB pull	Logical extraction via TWRP copy/ADB Backup	Physical extraction of file via Magnet Axiom Examine	Physical extraction and exportation of file via Magnet Axiom Examine

	Metadata Tool			
	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-lp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-lp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2	Magnet Axiom v4.7.0.22371 Journal module	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-lp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2
Details				
id	835	835	835	835
journal_id	105	105	105	105
key	BB0AFDFA15F475D761CAE9D1A843AF2 A.thumbnail	BB0AFDFA15F475D761CAE9D1A843AF2 A.thumbnail	BB0AFDFA15F475D761CAE9D1A843AF2 A.thumbnail	BB0AFDFA15F475D761CAE9D1A843AF2 A.thumbnail
sequence_number	72	72	72	72
value_count	1	1	1	1
status	1	1	1	1
last_update_time	1600640325784	1600640325784	1600640325784	1600640325784
last_update_time [244]	Monday, September 21, 2020 1:18:45.784 AM GMT+03:00 DST	Monday, September 21, 2020 1:18:45.784 AM GMT+03:00 DST	Monday, September 21, 2020 1:18:45.784 AM GMT+03:00 DST	Monday, September 21, 2020 1:18:45.784 AM GMT+03:00 DST
last_read_time	1600640424185	1600640424185	1602873332238	1602873332238
last_read_time [244]	Monday, September 21, 2020 1:20:24.185 AM GMT+03:00 DST	Monday, September 21, 2020 1:20:24.185 AM GMT+03:00 DST	Friday, October 16, 2020 9:35:32.238 PM GMT+03:00 DST	Friday, October 16, 2020 9:35:32.238 PM GMT+03:00 DST
lock_count	0	0	0	0
total_size	4820	4820	4820	4820
value_sizes (Binary)	Blob	Blob	?	Blob
value_sizes (HEX)	0000 00 00 00 00 00 00 12 d4	0000 00 00 00 00 00 00 12 d4		0000 00 00 00 00 00 00 12 d4
value_sizes (ASCII)
value_sizes (Decimal)	4820	4820		4820
expiration	1605824424185	1605824424185	1608057332238	1608057332238
expiration [244]	Friday, November 20, 2020 12:20:24.185 AM GMT+02:00	Friday, November 20, 2020 12:20:24.185 AM GMT+02:00	Tuesday, December 15, 2020 8:35:32.238 PM GMT+02:00	Tuesday, December 15, 2020 8:35:32.238 PM GMT+02:00
last_consumed_time	1600640424185	1600640424185	1602873332238	1602873332238
last_consumed_time [244]	Monday, September 21, 2020 1:20:24.185 AM GMT+03:00 DST	Monday, September 21, 2020 1:20:24.185 AM GMT+03:00 DST	Friday, October 16, 2020 9:35:32.238 PM GMT+03:00 DST	Friday, October 16, 2020 9:35:32.238 PM GMT+03:00 DST

“Last_update_time” for the 9A60BAE3104F32B5710B58A16B76AC79.thumbnail.0 file found within the “journal.db” matched the following timestamps:

- “Modify” and “Change” timestamps from rooted logical examination of file via ADB shell’s stat command
- "File Modification Date/Time" from ExifTool v12.07 after rooted logical extraction of file via ADB Pull

- "File Creation Date/Time" from rooted physical extraction of "Deleted" file via Magnet Axiom v4.7.0.22371

"Last_update_time" for the BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0 file found within the "journal.db" matched the following timestamps:

- "Modify" and "Change" timestamps from rooted logical examination of file via ADB shell's stat command
- "File Modification Date/Time" from ExifTool v12.07 after rooted logical extraction of file via ADB Pull
- "File Modification Date/Time" from rooted physical extraction of file via Magnet Axiom v4.7.0.22371
- "File Creation Date/Time" from rooted physical extraction of file via Magnet Axiom v4.7.0.22371

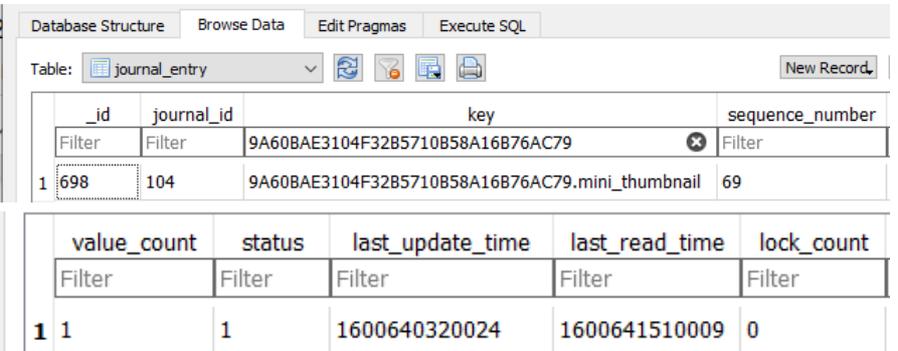
"Total_size" and "Value_sizes" for the 9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0 file found within the "journal.db" matched the following timestamps:

- "Size" from rooted logical examination of file via ADB shell's stat command
- "File Size" from ExifTool v12.07 after rooted logical extraction of file via ADB Pull
- "File Size" from Autopsy v4.13.0 after rooted logical extraction of file via ADB Pull
- "File Size" from ExifTool v12.07 after rooted logical extraction of file via TWRP copy/ADB Backup
- "File Size" from Autopsy v4.13.0 after rooted logical extraction of file via TWRP copy/ADB Backup

"Total_size" and "Value_sizes" for the BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0 file found within the "journal.db" matched the following timestamps:

- "Size" from rooted logical examination of file via ADB shell's stat command
- "File Size" from Autopsy v4.13.0 after rooted logical extraction of file via ADB Pull
- "File Size" from Autopsy v4.13.0 after rooted logical extraction of file via TWRP copy/ADB Backup
- "File Size" from rooted physical extraction of file via Magnet Axiom v4.7.0.22371

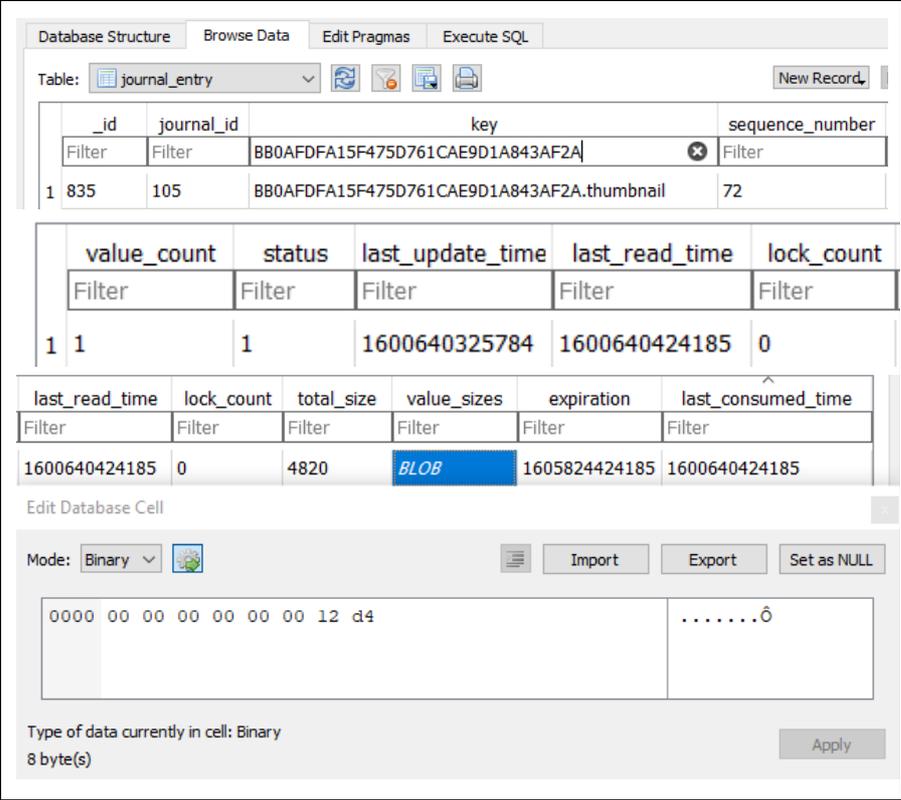
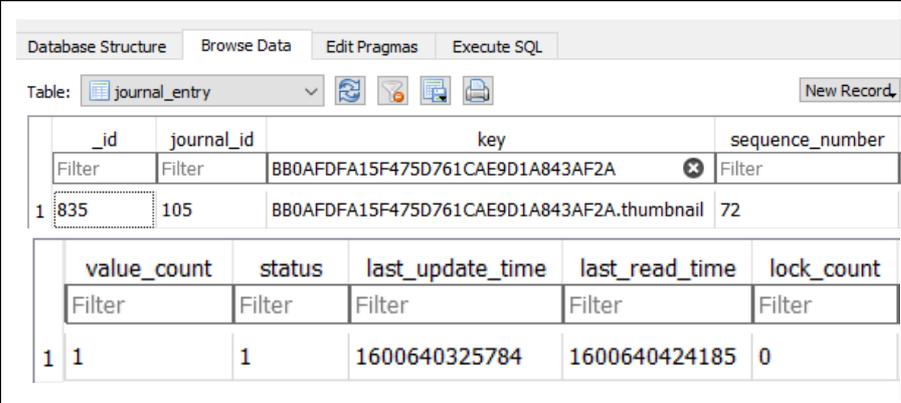
Table 63. Database metadata screenshots
9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0

Acquisition method	Database tool	9A60BAE3104F32B5710B58A16B76AC79.mini_thumbnail.0
Logical extraction via ADB pull	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-llp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2	

<p>Logical extraction via TWRP copy/ADB Backup</p>	<p>DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-llp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2</p>	
<p>Physical extraction of file via Magnet Axiom Examine</p>	<p>Magnet Axiom v4.7.0.22371 Journal module</p>	<p>Not available</p>
<p>Physical extraction and exportation of file via Magnet Axiom Examine</p>	<p>DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-llp64, running on x86_64 Qt v5.11.3</p>	<p>Not available</p>

	SQLite v3.27.2	
--	----------------	--

Table 64. Database metadata screenshots
BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0

Acquisition method	Database tool	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail.0
Logical extraction via ADB pull	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-llp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2	 <p>The screenshot shows the 'journal_entry' table in DB Browser for SQLite. The table has columns: _id, journal_id, key, sequence_number, value_count, status, last_update_time, last_read_time, lock_count, total_size, value_sizes, expiration, and last_consumed_time. The row with _id=1 is selected, and the 'value_sizes' column contains the value 'BLOB'. The 'Edit Database Cell' dialog is open, showing the binary data '0000 00 00 00 00 00 00 12 d4' and '.....ô'.</p>
Logical extraction via TWRP copy/ADB Backup	DB Browser for SQLite v3.11.2 Built for x86_64-little_endian-llp64, running on x86_64 Qt v5.11.3 SQLite v3.27.2	 <p>The screenshot shows the 'journal_entry' table in DB Browser for SQLite. The table has columns: _id, journal_id, key, sequence_number, value_count, status, last_update_time, last_read_time, lock_count, total_size, value_sizes, expiration, and last_consumed_time. The row with _id=1 is selected, and the value '835' in the _id column is highlighted with a dashed border.</p>

last_read_time	lock_count	total_size	value_sizes	expiration	last_consumed_time
Filter	Filter	Filter	Filter	Filter	Filter
1600640424185	0	4820	BLOB	1605824424185	1600640424185

Edit Database Cell ✕

Mode: Binary Import Export Set as NULL

0000 00 00 00 00 00 00 12 d4ô
------------------------------	--------

Type of data currently in cell: Binary
8 byte(s)

Apply

Physical extraction of file via Magnet Axiom Examine

Magnet Axiom v4.7.0.22371
Journal module

journal.db

Select table: journal_entry

FIND BUILD QUERY EXPORT CLEAR FILTERS SHOW / HIDE C

#	_id	journal_id	key	sequence_number
1	835	105	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail	72

value_count	status	last_update_time	last_read_time	lock_count
1	1	1600640325784	1602873332238	0

total_size	value_sizes	expiration	last_consumed_time
4820	?	1608057332238	1602873332238

Physical extraction and exportation of file via Magnet Axiom Examine

DB Browser for SQLite v3.11.2
Built for x86_64-little_endian-llp64, running on x86_64
Qt v5.11.3
SQLite v3.27.2

Database Structure Browse Data Edit Pragma Execute SQL

Table: journal_entry

_id	journal_id	key	sequence_number
Filter	Filter	BB0AFDFA15F475D761CAE9D1A843AF2A	Filter
1	835	105	BB0AFDFA15F475D761CAE9D1A843AF2A.thumbnail

value_count	status	last_update_time	last_read_time	lock_count
Filter	Filter	Filter	Filter	Filter
1	1	1	1600640325784	1602873332238

last_read_time	lock_count	total_size	value_sizes	expiration	st_consumed_tin
Filter	Filter	Filter	Filter	Filter	Filter
1602873332238	0	4820	BLOB	1608057332238	1602873332238

Edit Database Cell ✕

Mode: Binary Import Export Set as NULL

0000 00 00 00 00 00 00 12 d4ô
------------------------------	--------

Type of data currently in cell: Binary
8 byte(s)

Apply

7.1.6 Artifact inventory count

Forensic exams X - XIII provided artifact inventory counts before and after data extractions from /data/data/com.snapchat.android directory on the rooted sandbox smartphone (Table X).

All examination and extraction methods tested acquired 151 complete, never been “deleted”, or “deleted, overwritten” artifacts from the “./files/file_manager/memories_thumbnail” directory.

The rooted full image physical extraction of the sandbox smartphone was capable of acquiring file name, extension, and location information on “Deleted” and “Deleted, Overwritten” files; however, since the files were empty, no other information was extracted on those files.

Table 65. Artifact inventory counts before and after data extractions from /data/data/com.snapchat.android

Path to file: /data/data/com.snapchat.android	ADB Shell Logical Exam Before Data Extraction	Rooted Logical Extraction ADB pull	Rooted Logical Extraction TWRP copy & ADB Backup	Rooted Full Image Extraction Magnet Axiom Process			
				NBDDO	"Deleted"	"Deleted, Overwritten"	Total
./databases	42	30	28	42	2	9	53
./files/file_manager/media	10	0	0	0	11	0	11
./files/file_manager/memories_media	11	0	0	11	0	1	12
./files/file_manager/memories_mini_thumbnail	164	164	164	0	191	1	192
./files/file_manager/memories_print_thumbnail	0	0	0	0	0	0	0
./files/file_manager/memories_thumbnail	151	151	151	151	1	78	230
./files/file_manager/snap	0	0	0	0	0	0	0
./files/file_manager/spectacles	0	0	0	0	164	0	164
./files/file_manager/spectacles-files	0	0	0	0	0	0	0
./files/file_manager/user_generated_assets	0	0	0	0	0	0	0
./files/gallery/files	0	0	0	0	0	39	39
./files/gallery/thumbnails	0	0	0	0	1	42	43
./shared_prefs	25	24	25	27	0	1	28

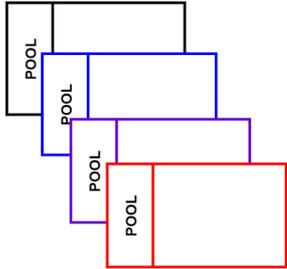
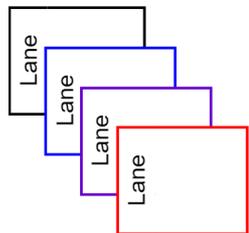
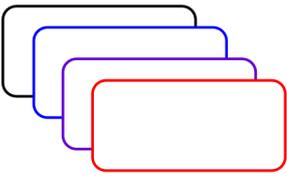
8 Results and Discussion

8.1 Identify & map: Business Process Modeling & Notation (BPMN)

Forensic analyses of the smart eyewear’s network communications and mobile systems provided key detailed insights to identify, map, and analyze biometric asset processing and privacy risks within the smart eyewear ecosystem.

Granular BPMN mappings of forensic exam processes within the smart eyewear ecosystem were created to summarize and clearly identify privacy risk origin points (figures x-x) to aid in formulating a NIST Privacy Framework Profile.

Table x. BPMN inventory legend

Item	Description	Icon(s)
Device systems and stakeholder(s)	<ul style="list-style-type: none"> - Target smartphone - Forensic laptop - Sandbox smartphone - TWRP - Forensic investigator/law enforcement 	
Software and hardware tools	<ul style="list-style-type: none"> - ADB Pull - ADB Shell - ADB Backup - ADB Dumpsys Meminfo - Magnet Axiom - Smart eyewear mobile application - ODIN 3_v3.13.1 - accounts.snapchat.com - Investigator’s micro SDXC card - Magnet.AI 	
Data processes/actions (As specified within pool, lane, and/or data action)	Data processing actions taken by smart eyewear ecosystems, smart eyewear organization, or forensic investigator/law enforcement	
Stakeholders (As specified within pool, lane, and/or data action)	<ul style="list-style-type: none"> - Smart eyewear owner - Bystanders - Forensic investigator/law enforcement - Smart eyewear organization (Snap Inc.) 	

Cloud storage service	Snap Inc.'s Snapchat "Memories" cloud storage service	
Network services	Network services required for communication between smart eyewear and paired smartphone <ul style="list-style-type: none"> - Wi-Fi - Bluetooth Low Energy - Location services 	
Privacy process status	Black = Privacy neutral Blue = Privacy maintained Purple = Privacy lost & maintained Red = Privacy lost	
Lost: <ul style="list-style-type: none"> - Privacy (P) - Confidentiality (C) - Integrity (I) - Availability (A) 		
Maintained: <ul style="list-style-type: none"> - Privacy (P) - Confidentiality (C) - Integrity (I) - Availability (A) 		
Smart eyewear Biometric assets (Privacy maintained)	JPG image files and MP4 video files containing biometric content of smart eyewear owner or bystanders whose privacy is maintained	
Smart eyewear Biometric assets (Privacy lost)	JPG image files and MP4 video files containing biometric content of smart eyewear owner or bystanders whose privacy is lost	
Data assets (Privacy lost)	Data assets containing relative file data or metadata for biometric assets	
Missing data assets	Missing data assets preventing availability of biometric assets	

See figures x-x for BPMN mappings of each forensic exam attributed to privacy loss for the smart eyewear owner and bystanders captured by their device.

Forensic exam VI: Non-Rooted extraction via ADB

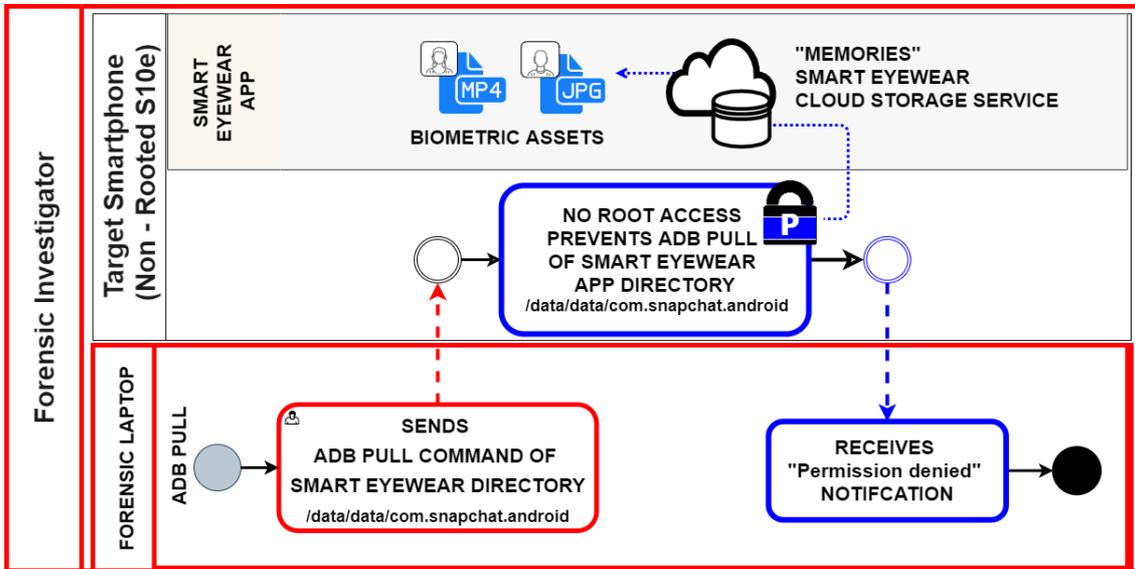


Figure x. BPMN of Forensic exam VI: Non-Rooted extraction via ADB Pull

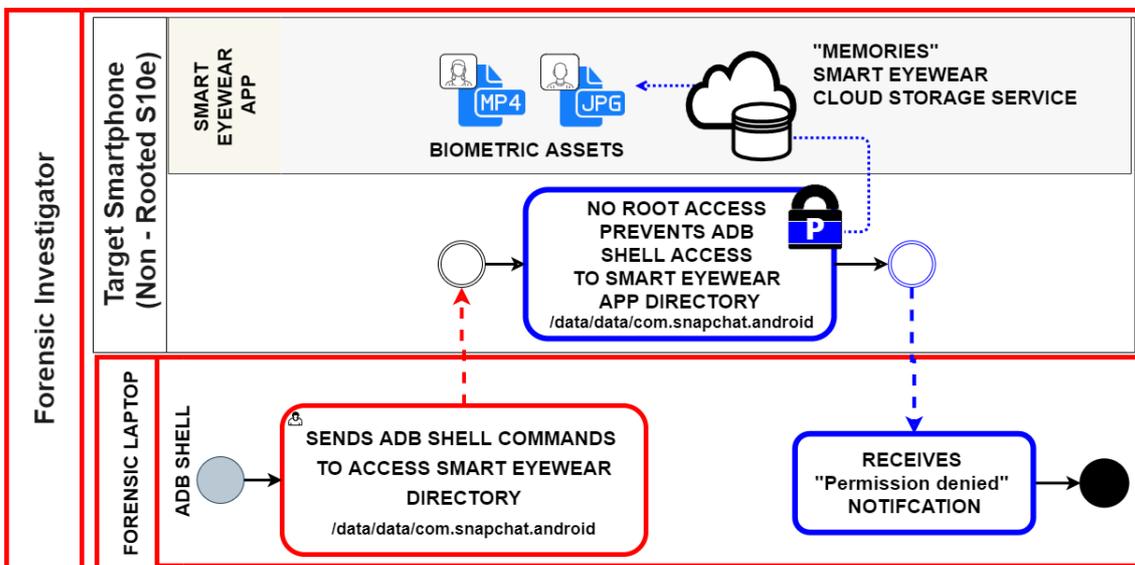


Figure x. BPMN of Forensic exam VI: Non-Rooted extraction via ADB Shell

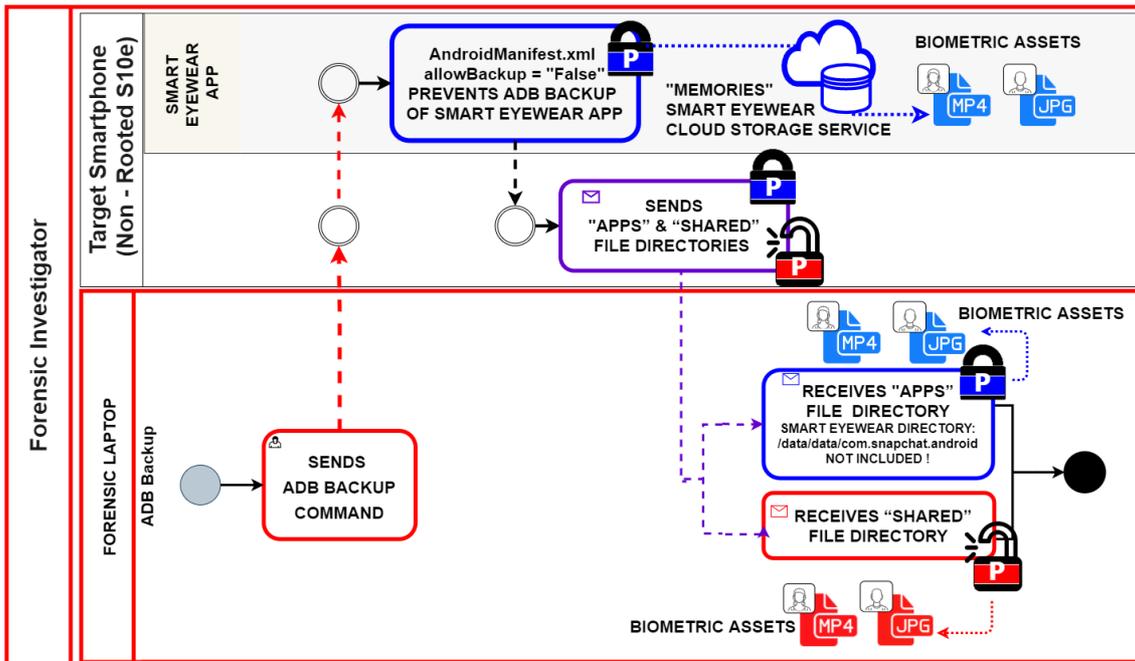


Figure x. BPMN of Forensic exam VI: Non-Rooted extraction via ADB Backup

Forensic exam VII: ADB dumphsys meminfo

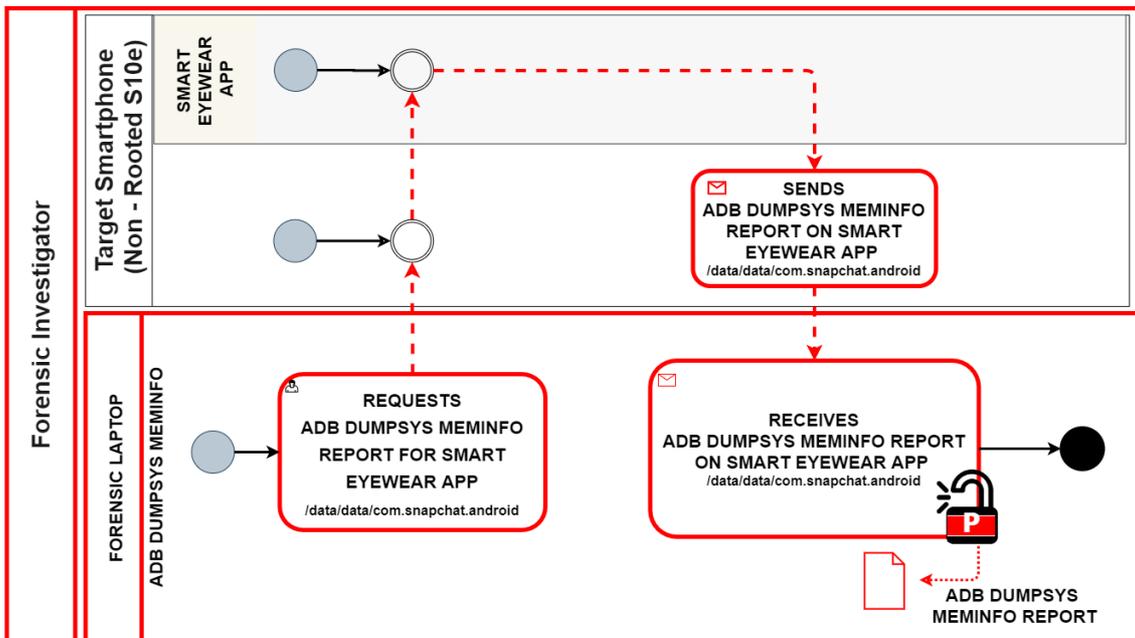


Figure x. BPMN of Forensic exam VII: ADB dumphsys meminfo

Forensic exam VIII: Data request

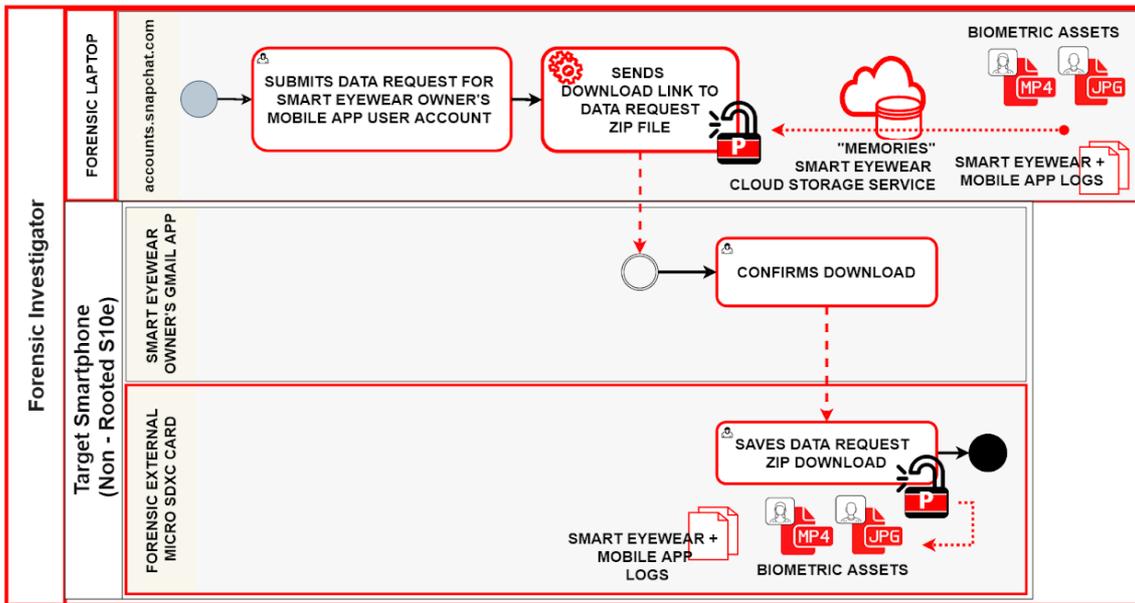


Figure x. BPMN of Forensic exam VIII: Data request

Forensic exam IX: Acquiring system administration privilege

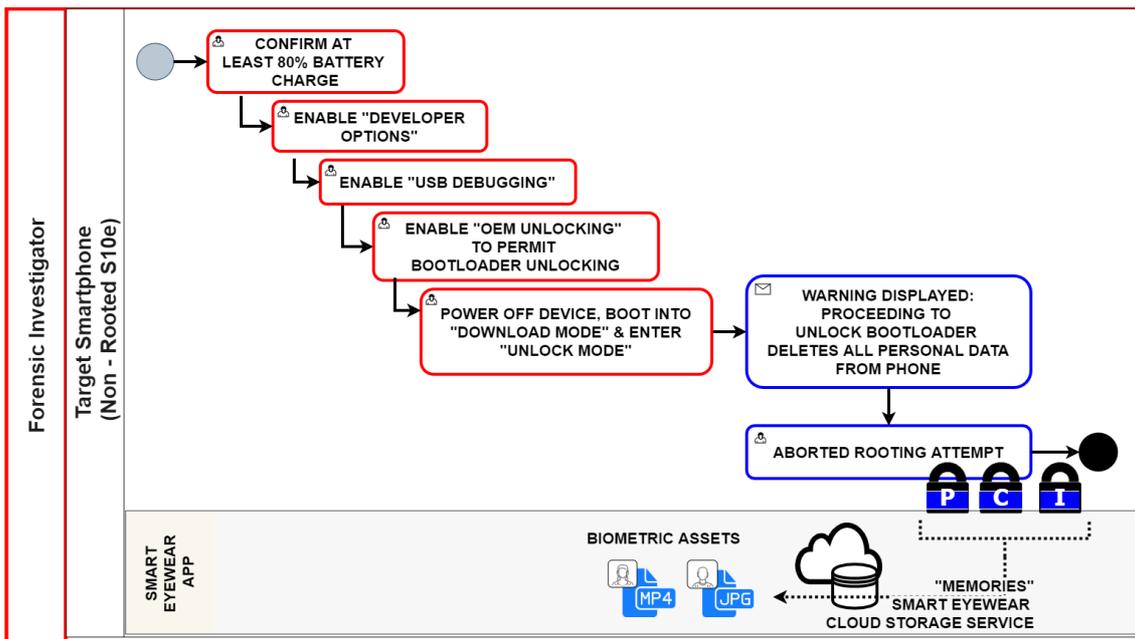


Figure x. BPMN of Forensic exam IX: Acquiring system administration privilege

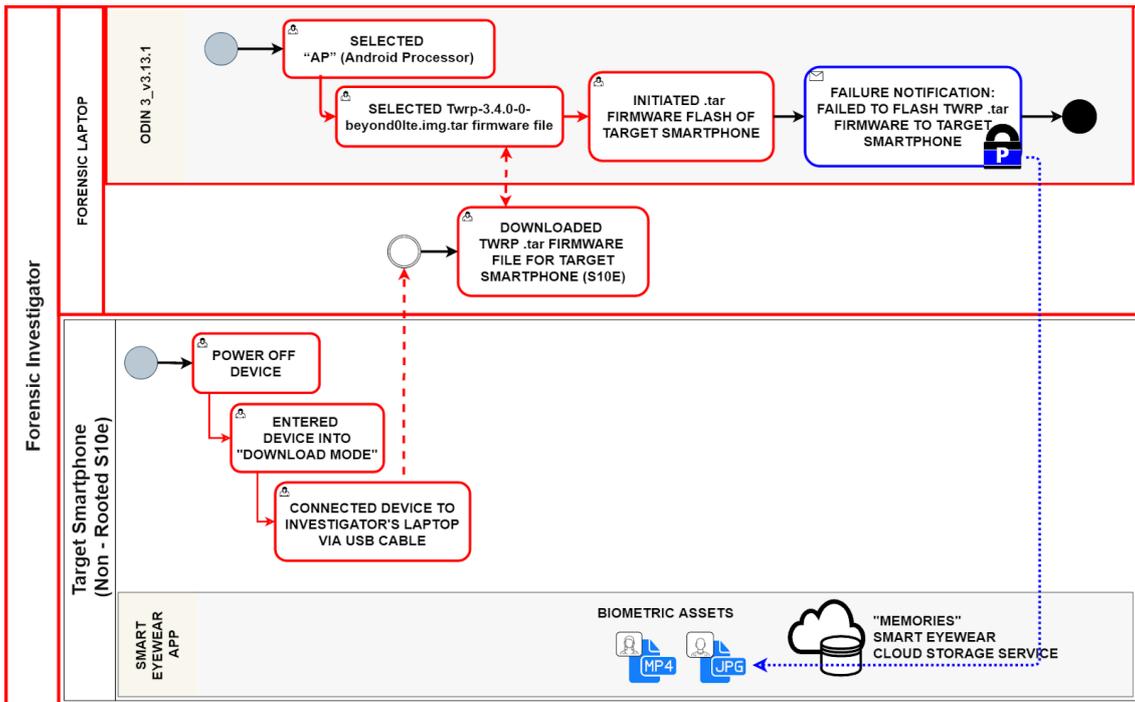


Figure x. BPMN of Forensic exam IX: Acquiring system administration privilege

Forensic exam X: Acquiring smart eyewear cloud data with a rooted sandbox smartphone and parallel APK

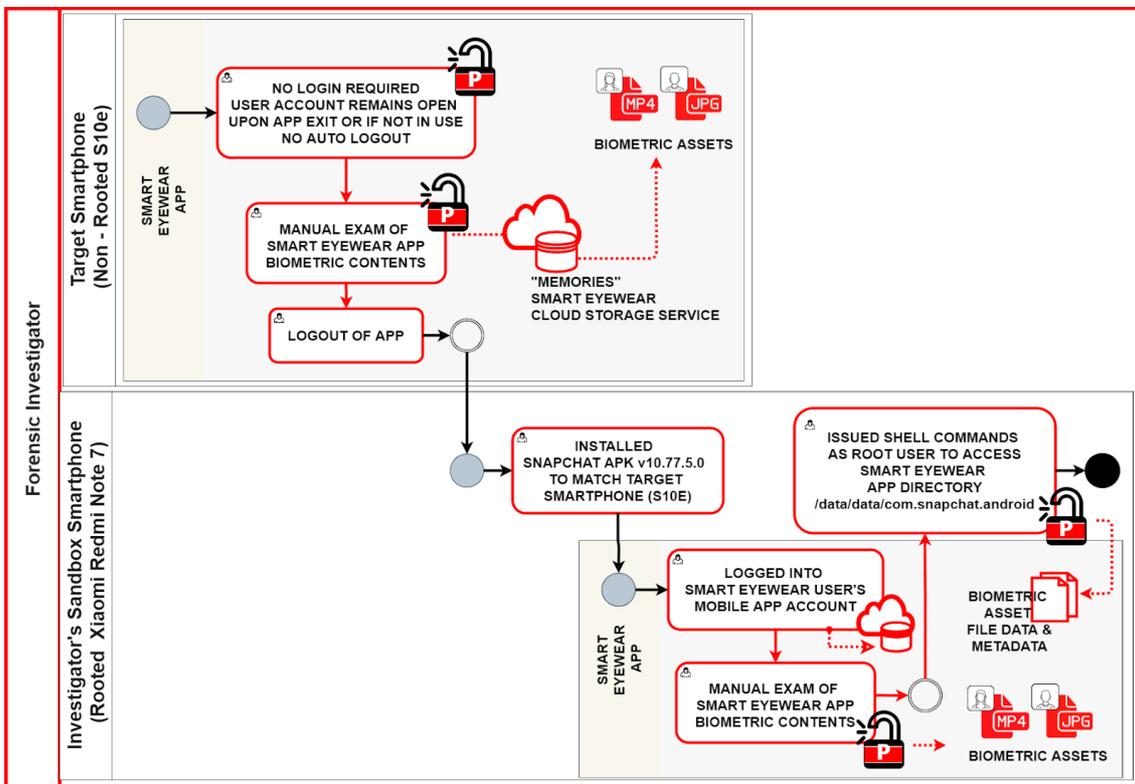


Figure x. BPMN of Forensic exam X: Acquiring smart eyewear cloud data with a rooted sandbox smartphone and parallel APK

Forensic exam XI: Rooted extraction via ADB pull

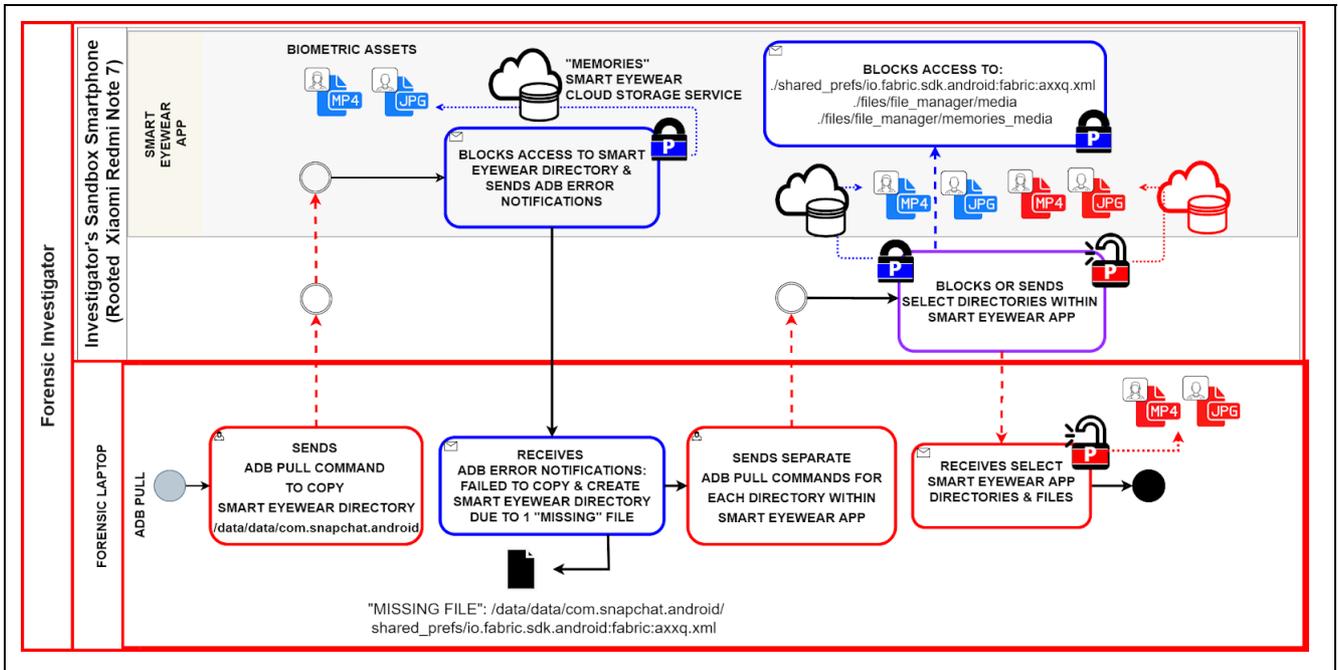


Figure x. BPMN of Forensic exam XI: Rooted extraction via ADB pull

Forensic exam XII: Rooted extraction via TWRP copy and ADB backup

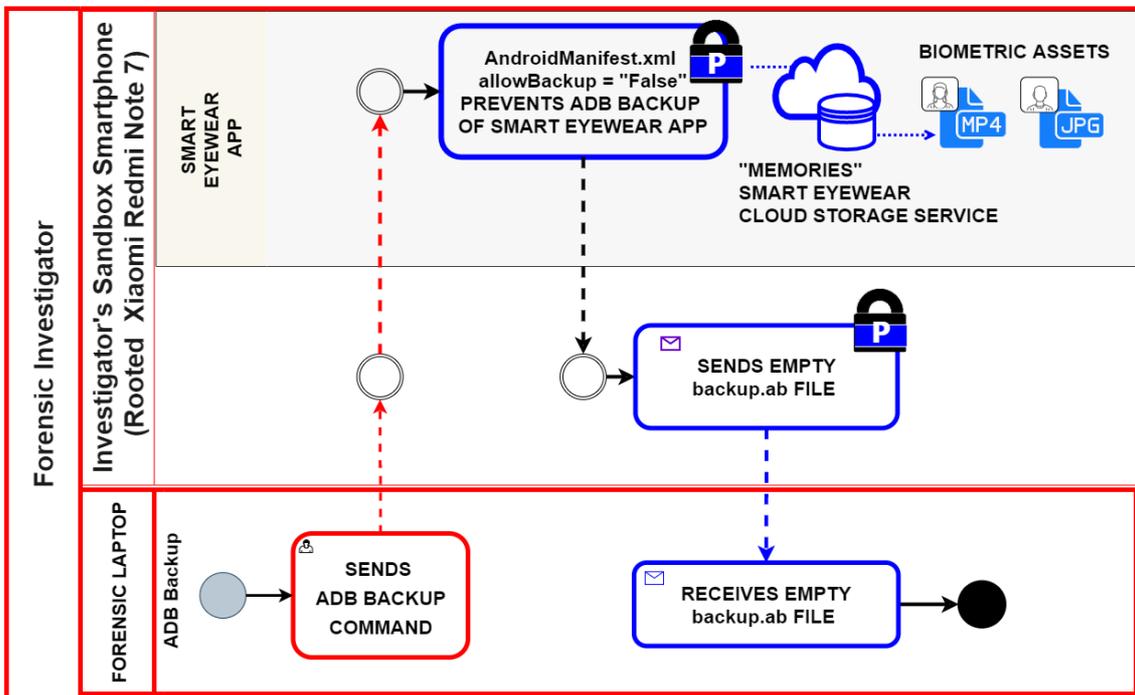


Figure x. BPMN of Forensic exam XII: Rooted extraction via ADB backup

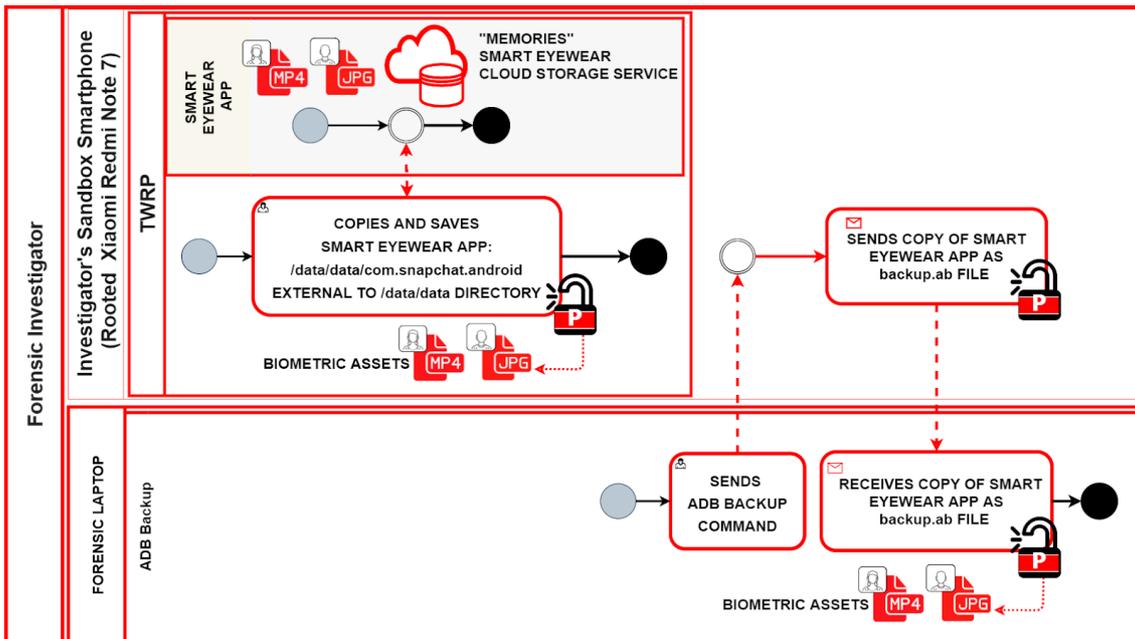


Figure x. BPMN of Forensic exam XII: Rooted extraction via TWRP copy and ADB backup

Forensic exam XIII: Rooted physical extraction via Magnet Axiom Process and Examine

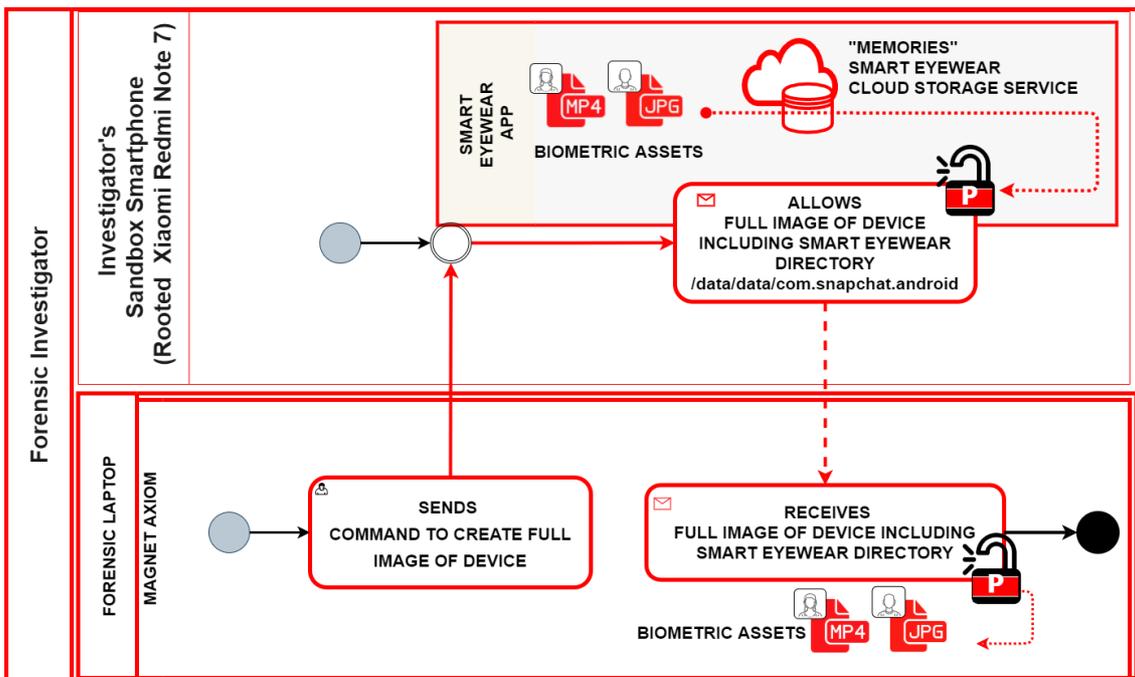


Figure x. BPMN of Forensic exam XIII: Rooted physical extraction via Magnet Axiom Process and Examine

Biometric detection

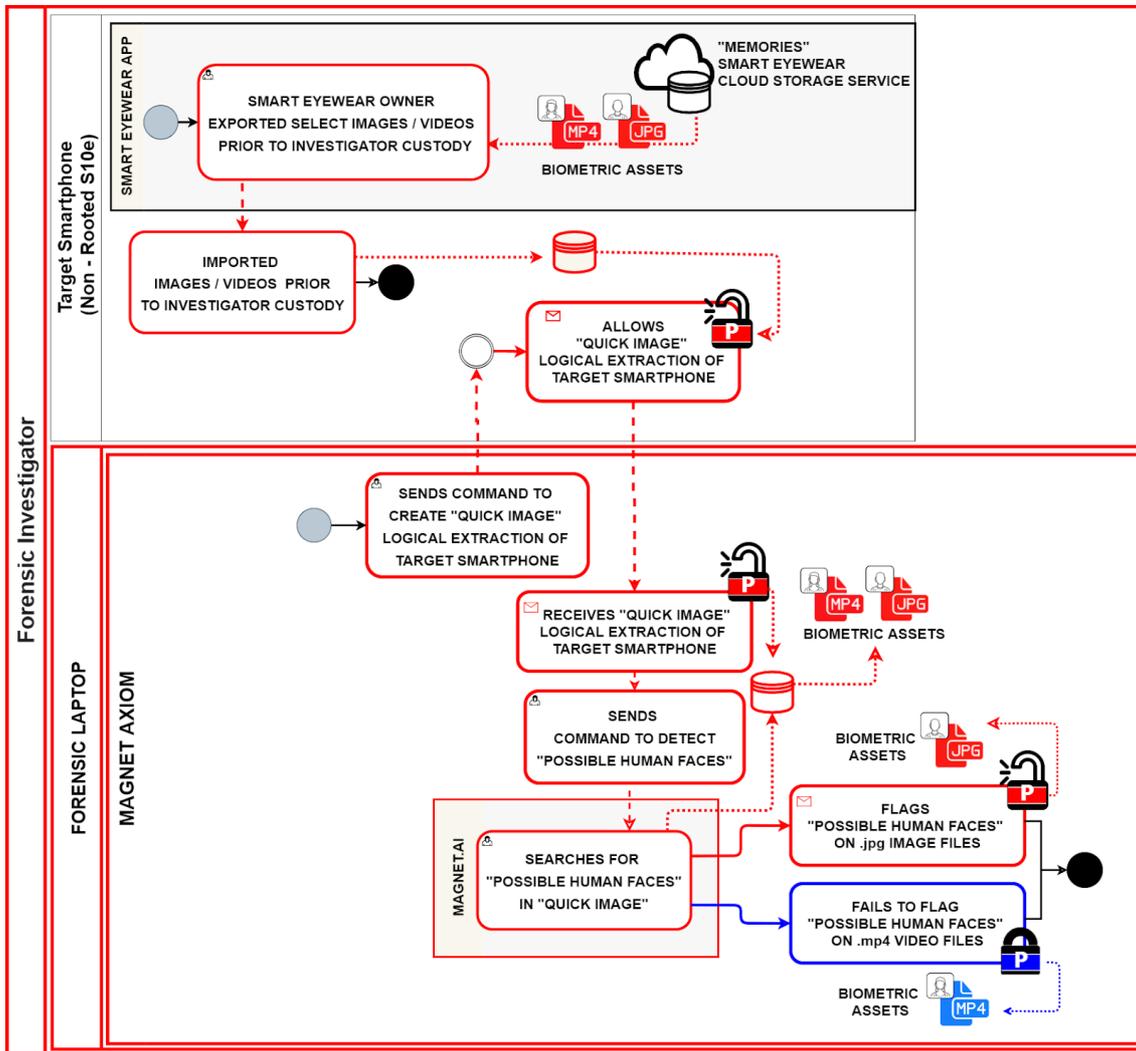


Figure x. BPMN of biometric detection on non-rooted logical extraction

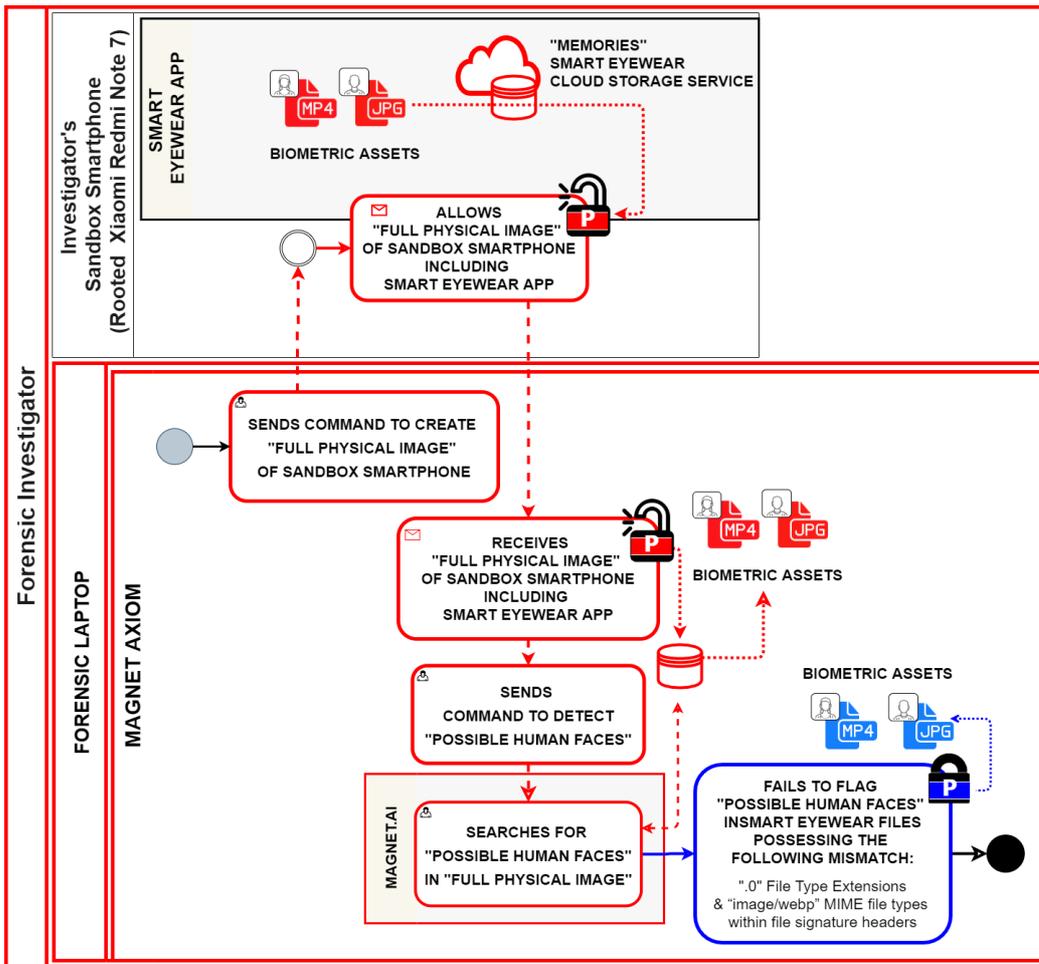


Figure x. BPMN of biometric detection on rooted physical extraction

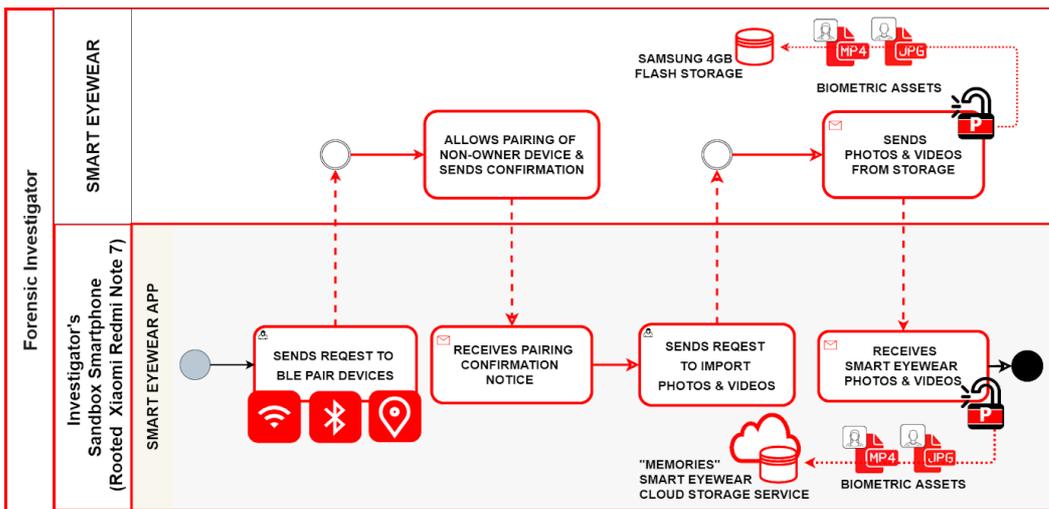


Figure x. BPMN of BLE transfer from smart eyewear to investigator sandbox smartphone

8.2 NIST Privacy Framework Profile

Biometric privacy risks found within the smart eyewear are best summarized within the NIST Privacy Framework Current to Target Profile, see table x.

The addition of following icons, see Table X, to NIST Privacy Framework profiles aid in communicating to smart eyewear stakeholders, a Privacy Profile’s Subcategory status concerning the product’s stage in meeting privacy risk objectives.

Table x. Profile Subcategory stage status icons [161]

Profile Subcategory Stage Statuses		
 Satisfied	 Needs Work	 Missing

Details concerning the Current and Target Profile Subcategory stage statuses have been comprehensively outlined below; however, the infographic icons provide a quick reference means for all stakeholders to immediately understand where privacy is at risk within the smart eyewear ecosystem.

Table x. Privacy Framework Current to Target Profile [97]

Privacy Framework Current to Target Profile for Snapchat Spectacles Smart Eyewear			
Function	Category	Subcategory	Subcategory Status
Identify-P (ID-P)	ID.IM-P	ID.IM-P1	 Satisfied <p>Inventoried Systems/products/services that process biometric data within this study.</p>
Identify-P (ID-P)	ID.IM-P	ID.IM-P2	 Satisfied <p>Inventoried individual product stakeholders (e.g., device owners/operators, the organization, or third parties such as forensic investigators and law enforcement) and their roles relative to the systems/products/services and</p>

				components (e.g., internal or external) that process biometric data within this study.
Identify-P (ID-P)	ID.IM-P	ID.IM-P3	 Satisfied	Inventoried categories of individuals (e.g., product owners, product operators, bystanders) whose biometric data are being processed within this study.
Identify-P (ID-P)	ID.IM-P	ID.IM-P4	 Satisfied	Inventoried data actions of the systems/products/services within this study.
Identify-P (ID-P)	ID.IM-P	ID.IM-P5	 Satisfied	Purposes for forensic investigator data actions were detailed within this study.
Identify-P (ID-P)	ID.IM-P	ID.IM-P6	 Satisfied	Inventoried data elements within the data actions within this study.
Identify-P (ID-P)	ID.IM-P	ID.IM-P7	 Satisfied	Identified the data processing environment (e.g., target devices, sandbox devices, third parties) within this study.
Identify-P (ID-P)	ID.IM-P	ID.IM-P8	 Satisfied	This study mapped smart eyewear ecosystem: <ul style="list-style-type: none"> - data processing - data actions - data elements - systems/products/services - components - roles of smart eyewear stakeholders

Identify-P (ID-P)	ID.RA-P	ID.RA-P1	 Satisfied	<p>Identified contextual factors related to data actions within smart eyewear ecosystem (e.g., individuals' privacy, data confidentiality, visibility of data processing to external parties).</p>
Identify-P (ID-P)	ID.RA-P	ID.RA-P3	 Satisfied	<p>Identified potential problematic data actions and associated problems within this study.</p>
Govern-P (GV-P)	GV.PO-P	GV.PO-P1	 Needs Work	<p>Currently established and communicated data retention periods of 30 days result in greater privacy risk vulnerabilities and threats, ultimately increasing negative impacts for consumers and business.</p> <p>Data retention periods should be shortened to further minimize the timeframe consumer data is held.</p>
Control-P (CT-P)	CT.DM-P	CT.DM-P1	 Missing	<p>Some data elements containing biometric assets were not accessible to smart eyewear owner for review after transferring from smart eyewear to smartphone mobile application, these elements were stored in Memories, the smart eyewear's cloud-storage service.</p> <p>These biometric assets were available to the smart eyewear firm via their cloud and thus available to forensic investigators/law enforcement.</p>

<p>Control-P (CT-P)</p>	<p>CT.DM-P</p>	<p>CT.DM-P2</p>	 <p>Needs Work</p>	<p>Data elements within Data Request were accessible for transmission and disclosure for 7 days.</p>
<p>Control-P (CT-P)</p>	<p>CT.DP-P</p>	<p>CT.DM-P8</p>	 <p>Needs Work</p>	<p>Data request audit/log records 7 day retention policy should be reviewed and altered to minimize biometric asset privacy risk to the time required to download the Data Request.</p> <p>Established and communicated personal data retention periods for Data Requests should be shortened to the exact time it takes to transfer the data request, as opposed to 7 days, in order to control and reduce privacy risk vulnerabilities and threats by minimizing the timeframe consumer data is held.</p>
<p>Control-P (CT-P)</p>	<p>CT.DP-P</p>	<p>CT.DP-P1</p>	 <p>Missing</p>	<p>Smart eyewear data processing by Memories, cloud-storage service, does not limit observability and linkability.</p> <p>Biometric data processing managed by Memories, the smart eyewear's cloud-storage service is not end-to-end encrypted by privacy-preserving Cryptography.</p> <p>There is no option (e.g. physical port/USB cable/software) to manually transfer photos and videos containing biometric data manually between local devices without being required to use the smart eyewear's cloud-storage.</p>

Control-P (CT-P)	CT.DP-P	CT.DP-P2	 Missing	<p>Data are not processed to limit the identification of individuals.</p> <p>No end-to-end encryption of photos and/or videos containing biometric content the individual or bystanders transferred to the smart eyewear cloud would identify them.</p>
Control-P (CT-P)	CT.DP-P	CT.DP-P3	 Missing	<p>Data are not processed to limit the formulation of inferences about individuals' behavior or activities.</p> <p>Metadata linked to biometric images and videos within smart eyewear database contained exact latitude and longitude coordinate location information of capture.</p>
Control-P (CT-P)	CT.DP-P	CT.DP-P4	 Missing	<p>Smart eyewear ecosystem configurations do not permit selective collection or disclosure of biometric data elements, as all elements must be transferred to the smart eyewear cloud database from the smart eyewear in order to access them.</p>
Communicate-P (CM-P)	CM.PO-P	CM.PO-P1	 Needs Work	<p>Vague non-transparent data retention policy for photos and videos containing biometric content stored then deleted from Snapchat Memories. The following statement is unclear to all smart eyewear stakeholders: "If you delete a Snap from your Memories, Snapchat servers are designed to erase that Snap as soon as possible." [256]</p>

<p>Communicate-P (CM-P)</p>	<p>CM.PO-P</p>	<p>CM.PO-P1</p>	<p> Satisfied</p>	<p>Transparent data availability policy regarding Data Request zip file download links: "Download links below will expire 7 days from when your file was made available to you."</p>
<p>Communicate-P (CM-P)</p>	<p>CM.AW-P</p>	<p>CM.AW-P4</p>	<p> Satisfied</p>	<p>Snap Inc. provides a public transparency report regarding records of data disclosures and data sharing with law enforcement and governmental agencies. [130]</p>
<p>Communicate-P (CM-P)</p>	<p>CM.AW-P</p>	<p>CM.AW-P7</p>	<p> Needs Work</p>	<p>Not all impacted individuals and organizations are notified about investigative privacy breaches or events regarding their data, as detailed: "Since November 15, 2015, our policy has been to notify Snapchatters when we receive legal process seeking their account information, with exceptions for cases where we are legally prohibited from doing so, or when we believe there are exceptional circumstances (like child exploitation or an imminent risk of death or bodily injury)." [257]</p>
<p>Protect-P (PR-P)</p>	<p>PR.AC-P</p>	<p>PR.AC-P1</p>	<p> Needs Work</p>	<p>Account creation requires strength tested password requirements upon issuance of smart eyewear identity creation.</p>
<p>Protect-P (PR-P)</p>	<p>PR.DS-P</p>	<p>PR.DS-P1</p>	<p> Missing</p>	<p>Smart eyewear biometric assets at-rest are not protected from forensic examinations once smart eyewear or paired smartphone has been</p>

				obtained, or data has been transferred from smart eyewear to cloud storage.
Protect-P (PR-P)	PR.DS-P	PR.DS-P2	 Satisfied	Biometric images and videos transferred from the smart eyewear to the paired smartphone using Wi-Fi communications are protected
Protect-P (PR-P)	PR.DS-P	PR.DS-P2	 Satisfied	Biometric images and videos transferred from the smart eyewear to the paired smartphone using BLE communications are protected
Protect-P (PR-P)	PR.DS-P	PR.DS-P4	 Missing	Smart eyewear ecosystem lacks capacity to ensure availability of transferred smart eyewear biometric assets is maintained.
Protect-P (PR-P)	PR.DS-P	PR.DS-P6:	 Missing	<p>Smart eyewear ecosystem lacks integrity checking mechanisms used to verify information integrity between smart eyewear and paired smartphone after transferring data from the former to the latter.</p> <p>Images and videos containing biometric content were stored on smart eyewear cloud storage after transfer from smart eyewear; however, never transferred to paired smartphone.</p>

9 Synopsis

9.1 Main goal

The study determined what design features were utilized to ensure the privacy of the biometric assets recorded on smart eyewear from external actors, specifically forensic investigation and law enforcement entities.

The study also determined vulnerabilities in design where privacy controls have fallen short and where a forensic investigator's actions during an investigation of smart eyewear lead to biometric asset loss of privacy.

9.2 Limitations

Budgetary and time constraints limited the amount of research that could be achieved relative to data processing, analysis, and validation. A larger budget and more time would have afforded the ability to test Bluetooth low energy tracking tools at the enterprise commercial level and cross compare results and devices, as well as numerous commercial systems forensics software packages. And additionally conduct a privacy cross examination on the ability of facial recognition tools, such as FindFace by NtechLab and Amazon Rekognition by Amazon, Inc. and Amazon Web Services, to uniquely identify individuals.

Additionally, initial research plans were to test law enforcement smart eyewear, in a live field study in various busy public venues; this proposed plan was restricted by product procurement, cost, a worldwide pandemic, and GDPR legal barriers.

9.3 Analysis Bias

Selecting open access journals, conferences, and grey literature within this study's literature review contributed to systemic bias within the selection related works [243]. The impact of restricted access to "paywalled"[243] literature on this study is unknown.

Utilization of select simulated biometric data sourced from the public domain in a semi-controlled testing environment, created data sampling bias within the study. Providing greater resources were possessed to conduct this study with a diverse selection of smart eyewear test subjects in numerous environmental situations, this sample bias may be eliminated.

9.4 Novelty

9.4.1 Main contribution

One of the main scientific novel contributions of the study is the identification and mapping of privacy by design features, within a pair of smart eyewear, that either aid in securing biometric asset privacy or create privacy risks, leaving the assets vulnerable for exploitation.

Honing in on privacy by design and default features through forensic examination establishes current security design norms deployed to protect biometric assets, collected via smart eyewear, from privacy loss relative to all external actors, including those within law enforcement and forensics investigation entities.

The study's next novel contribution is the application of NIST's Privacy Framework Profiles to the smart eyewear ecosystem in the context of a forensic investigation case study.

The forensic analyses conducted illustrates how design features working to protect the privacy of an end user or a recorded bystander, inhibit law enforcement and forensic investigators from ascertaining evidence from such devices. Or conversely, how lack of privacy design features enable law enforcement and forensic investigators to easily obtain evidence.

9.5 Future work

Avenues for continued research and future work involves a full forensic analysis and survey of all prospective smart eyewear devices currently on the market and those yet to emerge. The dearth of privacy management information on these devices leaves all stakeholders of such products in the dark as more and more individuals, government agencies, and corporations begin to utilize these hands free audio and video capturing devices.

This study provided a preliminary exploration of privacy risk management within smart eyewear. Further studies of privacy risk management validation via triangulation should be explored through comparisons of differing modeling, mapping, and framework tools and methodologies.

A comparative analysis of low and high end bluetooth sniffing devices relative to scanning and extracting data from smart eyewear will assist in validating the forensic equipment.

Greater technical depths should be explored within chip off forensics analysis on all current and emerging smart eyewear devices.

References

- [1] C. C. Editor, “biometric - Glossary,” Nist.gov. [Online]. Available: <https://csrc.nist.gov/glossary/term/biometric>. [Accessed: 2020].
- [2] “Art. 4 GDPR – definitions,” Gdpr-info.eu, 12-Jul-2016. [Online]. Available: <https://gdpr-info.eu/art-4-gdpr/>. [Accessed: 2020].
- [3] C. C. Editor, “confidentiality - Glossary,” Nist.gov. [Online]. Available: <https://csrc.nist.gov/glossary/term/confidentiality>. [Accessed: 2020].
- [4] “EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex,” Europa.eu. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:02016R0679-20160504>. [Accessed: 2020].
- [5] “Definition of PRIVACY,” Merriam-webster.com. [Online]. Available: <https://www.merriam-webster.com/dictionary/privacy>. [Accessed: 2020].
- [6] Nist.gov. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4734.pdf>. [Accessed: 2020].
- [7] *Europa.eu*. [Online]. Available: <https://www.enisa.europa.eu/publications/pets>. [Accessed: 2020].
- [8] R. Commissioner/Ontario, “Privacy-enhancing technologies: The path to anonymity,” Ola.org. [Online]. Available: <https://collections.ola.org/mon/10000/184530.pdf>. [Accessed: 2020].
- [9] R. Stim, Website, Twitter, and LinkedIn, “Welcome to the public domain - copyright overview by rich stim - Stanford copyright and fair use center,” Stanford.edu, 04-Apr-2013. [Online]. Available: <https://fairuse.stanford.edu/overview/public-domain/welcome/>. [Accessed: 15-Nov-2019].
- [10] “Going dark: Are technology, privacy, and public safety on a collision course?,” Fbi.gov, 16-Oct-2014. [Online]. Available: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>. [Accessed: 08-Dec-2019].
- [11] “Emails show how Amazon is selling facial recognition system to law enforcement,” Aclunc.org. [Online]. Available: <https://www.aclunc.org/news/emails-show-how-amazon-selling-facial-recognition-system-law-enforcement>. [Accessed: 2020].
- [12] L. B. Baldwin, “Ear recognition as device input,” 9049983, 09-Jun-2015.
- [13] D. Kang, “Chinese ‘gait recognition’ tech IDs people by how they walk,” Associated Press, 06-Nov-2018. [Online]. Available: <https://apnews.com/bf75dd1c26c947b7826d270a16e2658a>. [Accessed: 2020].
- [14] “Russian court rules in favor of facial recognition over privacy claims,” Reuters, 03-Mar-2020.

- [15] C. Zakrzewski, “Technology 202: Other countries use surveillance to fight coronavirus. Privacy advocates worry the U.S. could follow,” Washingtonpost.com, 17-Mar-2020. [Online]. Available: <https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/03/17/the-technology-202-other-countries-use-surveillance-to-fight-coronavirus-privacy-advocates-worry-the-u-s-could-follow/5e70268c88e0fa101a74acf2/>. [Accessed: 2020].
- [16] A. Glaser, “‘Fever detection’ cameras to fight coronavirus? Experts say they don’t work,” NBC News, 27-Mar-2020. [Online]. Available: <https://www.nbcnews.com/tech/security/fever-detection-cameras-fight-coronavirus-experts-say-they-don-t-n1170791>. [Accessed: 2020].
- [17] M. Murphy, “Fever surveillance ‘to become as common as CCTV,’” The Telegraph, 15-Apr-2020. [Online]. Available: <https://www.telegraph.co.uk/technology/2020/04/15/fever-surveillance-become-common-cctv/>. [Accessed: 2020].
- [18] K. Hill, “The secretive company that might end privacy as we know it,” The New York Times, The New York Times, 18-Jan-2020.
- [19] R. M. Kirsten Grind and A. W. Mathews, “To track virus, governments weigh surveillance tools that push privacy limits,” Wall Street journal (Eastern ed.), wsj.com, 17-Mar-2020.
- [20] A. D. Rayome, “Amazon’s \$180 Echo Frames are Alexa’s first take on smart glasses,” CNET, 26-Sep-2019. [Online]. Available: <https://www.cnet.com/news/amazons-180-echo-frames-are-alexas-first-take-on-smart-glasses/>. [Accessed: 08-Dec-2019].
- [21] “Spectacles by Snap Inc. • Capture your world in 3D,” Spectacles.com. [Online]. Available: <https://www.spectacles.com/>. [Accessed: 06-Oct-2019].
- [22] “Glass – Glass,” Google.com. [Online]. Available: <https://www.google.com/glass/start/>. [Accessed: 08-Dec-2019].
- [23] “Can these smart glasses do what Google couldn’t?,” 14-Feb-2019. [Online]. Available: <https://www.youtube.com/watch?v=5dsVwXzOIjk>. [Accessed: 2020].
- [24] S. Rodriguez, “Facebook working on smart glasses with Ray-Ban, code-named ‘Orion,’” CNBC, 17-Sep-2019. [Online]. Available: <https://www.cnbc.com/2019/09/17/facebook-enlists-ray-ban-maker-luxottica-to-make-orion-ar-glasses.html>. [Accessed: 2020].
- [25] “Exclusive: Intel’s new smart glasses hands-on,” 05-Feb-2018. [Online]. Available: <https://www.youtube.com/watch?v=bnfwClgheF0>. [Accessed: 2020].
- [26] “Microsoft HoloLens,” Microsoft.com. [Online]. Available: <https://www.microsoft.com/en-us/hololens>. [Accessed: 2020].
- [27] D. Phelan, “Apple smart glasses may be coming, but not until 2022 or 2023,” Forbes Magazine, 11-Nov-2019.

- [28] Trevor and G. Giant, “Bosen puettavat laitteet – klassiset aurinkolasit Bluetooth-äänellä,” Bose.fi, 15-Jul-2020. [Online]. Available: https://www.bose.fi/fi_fi/products/frames/bose-frames-alto.html. [Accessed: 2020].
- [29] S. Liao, “Chinese police are expanding facial recognition sunglasses program,” The Verge, 12-Mar-2018. [Online]. Available: <https://www.theverge.com/2018/3/12/17110636/china-police-facial-recognition-sunglasses-surveillance>. [Accessed: 01-Dec-2019].
- [30] C. Burt, “Police in Miami, India, Macau expand facial recognition use amid further warnings,” BiometricUpdate.com, 11-Nov-2019. [Online]. Available: <https://www.biometricupdate.com/201911/police-in-miami-india-macau-expand-facial-recognition-use-amid-further-warnings>. [Accessed: 01-Dec-2019].
- [31] D. Zeqiri, J. Kinsman, N. Trend, D. Penna, and A. Singh, “Brazilian police to use ‘Robocop-style’ glasses at World Cup,” Sunday telegraph, 12-Apr-2011.
- [32] “Video: Scan faces, take photos with these glasses in Dubai,” Khaleejtimes.com, 16-Oct-2018. [Online]. Available: <https://www.khaleejtimes.com/technology/video-scan-faces-take-photos-with-these-glasses-in-dubai-123>. [Accessed: 01-Dec-2019].
- [33] М. Солопов and Е. Кузнецова, “Мэрия Москвы закажет для полицейских очки с распознаванием лиц,” Rbc.ru. [Online]. Available: <https://www.rbc.ru/society/15/02/2019/5c6526369a79471a20e2fee7>. [Accessed: 01-Dec-2019].
- [34] Fox News, “Big tech racing to replace smartphones with smart glasses,” New York post, New York Post, 12-Nov-2019.
- [35] T. Haselton, “There’s a race to replace our iPhones with smart glasses we wear everywhere,” Cnbc.com, 11-Nov-2019. [Online]. Available: <https://www.cnbc.com/2019/11/11/smart-glasses-that-replace-phones-may-be-the-next-hottest-tech-trend.html>. [Accessed: 08-Dec-2019].
- [36] N. Osorio, “Next big computing device after smartphones is just 2 years away,” Ibtimes.com, 01-Dec-2019. [Online]. Available: <https://www.ibtimes.com/next-big-computing-device-after-smartphones-just-2-years-away-2876844>. [Accessed: 08-Dec-2019].
- [37] S. Chowdhury, M. S. Ferdous, and J. M. Jose, “Bystander Privacy in Lifelogging,” in Proceedings of the 30th International BCS Human Computer Interaction Conference (HCI), 2016, pp. 1–3.
- [38] A. J. Perez, S. Zeadally, and S. Griffith, “Bystanders’ Privacy,” IT Prof., vol. 19, no. 3, pp. 61–65, 2017.
- [39] I. Flammer, “Genteel wearables: Bystander-centered design,” IEEE Secur. Priv., vol. 14, no. 5, pp. 73–79, 2016.

- [40] M. Dimiccoli, J. Marín, and E. Thomaz, “Mitigating bystander privacy concerns in egocentric activity recognition with deep learning and intentional image degradation,” *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 1, no. 4, pp. 1–18, 2018.
- [41] V. Biryukov, “You can’t replace your face, says face recognition,” *Kaspersky.com*, 22-Apr-2016. [Online]. Available: <https://www.kaspersky.com/blog/findface-experiment/11916/>. [Accessed: 2020].
- [42] A. Novobranets, K. Теллер, A. Vizkovskii, and O. Bubich, “Конец анонимности: Идентификация случайных попутчиков,” *Birdinflight.com*, 09-Dec-2020. [Online]. Available: <https://birdinflight.com/ru/vdohnovenie/fotoproect/06042016-face-big-data.html>. [Accessed: 2020].
- [43] A. Cuthbertson, “Porn stars and sex workers targeted with facial recognition app,” *Newsweek*, 29-Apr-2016. [Online]. Available: <https://www.newsweek.com/porn-actress-facial-recognition-findface-sex-worker-453357>. [Accessed: 2020].
- [44] “James Bain - National Registry of Exonerations,” *Umich.edu*. [Online]. Available: <https://www.law.umich.edu/special/exoneration/Pages/casedetail.aspx?caseid=3008>. [Accessed: 2020].
- [45] “David Brian Sutherlin - national registry of exonerations,” *Umich.edu*. [Online]. Available: <https://www.law.umich.edu/special/exoneration/Pages/casedetail.aspx?caseid=3671>. [Accessed: 2020].
- [46] “Thomas McGowan - national registry of exonerations,” *Umich.edu*. [Online]. Available: <https://www.law.umich.edu/special/exoneration/Pages/casedetail.aspx?caseid=3455>. [Accessed: 2020].
- [47] “Robert Lamar Watson - national registry of exonerations pre 1989,” *Umich.edu*. [Online]. Available: <https://www.law.umich.edu/special/exoneration/Pages/casedetailpre1989.aspx?caseid=373>. [Accessed: 2020].
- [48] Elsevier, “6 ways to find Elsevier’s open access content,” *Elsevier.com*, 01-Oct-2013. [Online]. Available: <https://www.elsevier.com/authors-update/story/access-to-research/6-ways-to-find-elseviers-open-access-content>. [Accessed: 2020].
- [49] “Scimago Journal & Country Rank,” *Scimagojr.com*. [Online]. Available: <https://www.scimagojr.com>. [Accessed: 2020].
- [50] I. Bouchrika and +, “Guide2Research - leading research portal for computer science,” *Guide2research.com*. [Online]. Available: <http://www.guide2research.com/>. [Accessed: 2020].

- [51] J. Rongen and Z. Geradts, "Extraction and forensic analysis of artifacts on wearables," *International Journal of Forensic Science & Pathology (IJFP)*, pp. 312–318, 2017.
- [52] J. Desautels, "Google Glass Forensics," *Smarterforensics.com*. [Online]. Available: <https://smarterforensics.com/wp-content/uploads/2014/06/Google-Glass-Forensics.pdf>. [Accessed: 2020].
- [53] M. E. Loomis, "Wearable device forensics," The University of Tulsa, 2019.
- [54] "WordCounter," *Databasic.io*. [Online]. Available: <https://databasic.io/en/wordcounter/>. [Accessed: 2020].
- [55] K. Behel, N. Altom, and R. Ginsburg, "Google Glass Security Analysis," *Insurehub.org*. [Online]. Available: <http://insurehub.org/sites/default/files/reports/glass-report.pdf>. [Accessed: 2020].
- [56] T. Bipat, M. W. Bos, R. Vaish, and A. Monroy-Hernández, "Analyzing the use of camera glasses in the wild," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 2019.
- [57] M. Koelle, W. Heuten, and S. Boll, "Are you hiding it?: Usage habits of lifelogging camera wearers," in *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '17*, 2017.
- [58] J. Gregorio, B. Alarcos, and A. Gardel, "Forensic analysis of Nucleus RTOS on MTK smartwatches," *Digit. investig.*, vol. 29, pp. 55–66, 2019.
- [59] I. Baggili, J. Oduro, K. Anthony, F. Breitingner, and G. McGee, "Watch what you wear: Preliminary forensic analysis of smart watches," in *2015 10th International Conference on Availability, Reliability and Security*, 2015.
- [60] A. MacDermott, S. Lea, F. Iqbal, I. Idowu, and B. Shah, "Forensic analysis of wearable devices: Fitbit, Garmin and HETP watches," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2019, pp. 1–6.
- [61] N. R. Odom, J. M. Lindmar, J. Hirt, and J. Brunty, "Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices," *J. Forensic Sci.*, vol. 64, no. 6, pp. 1673–1686, 2019.
- [62] S. Becirovic and S. Mrdovic, "Manual IoT forensics of a Samsung gear S3 frontier smartwatch," in *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2019, pp. 1–5.
- [63] "Projects:2017s1-165 forensic investigation of fitness devices," *Edu.au*. [Online]. Available: https://projectswiki.eleceng.adelaide.edu.au/projects/index.php/Projects:2017s1-165_Forensic_Investigation_of_Fitness_Devices. [Accessed: 2020].
- [64] J. Classen, D. Wegemer, P. Patras, T. Spink, and M. Hollick, "Anatomy of a vulnerable fitness tracking system: Dissecting the Fitbit cloud, app, and firmware,"

Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., vol. 2, no. 1, pp. 1–24, 2018.

[65] S. Kang, S. Kim, and J. Kim, “Forensic analysis for IoT fitness trackers and its application,” *Peer Peer Netw. Appl.*, vol. 13, no. 2, pp. 564–573, 2020.

[66] Y. H. Yoon and U. Karabiyik, “Forensic analysis of Fitbit Versa 2 data on android,” *Electronics (Basel)*, vol. 9, no. 9, p. 1431, 2020.

[67] J. Orlosky, O. Ezenwoye, H. Yates, and G. Besenyi, “A look at the security and privacy of Fitbit as a health activity tracker,” in *Proceedings of the 2019 ACM Southeast Conference on ZZZ - ACM SE '19*, 2019.

[68] A. Almogbil, A. Alghofaili, C. Deane, T. Leschke, A. Almogbil, and A. Alghofaili, “The accuracy of GPS-enabled Fitbit activities as evidence: A digital forensics study,” in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2020, pp. 186–189.

[69] B. A. Delail and C. Y. Yeun, “Recent advances of smart glass application security and privacy,” in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, pp. 65–69.

[70] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner, “Towards security and privacy for multi-user augmented reality: Foundations with end users,” in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 392–408.

[71] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in internet-of-things,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017.

[72] S. Seneviratne et al., “A survey of wearable devices and challenges,” *IEEE Commun. Surv. Tutor.*, vol. 19, no. 4, pp. 2573–2620, 2017.

[73] J. A. De Guzman, K. Thilakarathna, and A. Seneviratne, “Security and privacy approaches in mixed reality: A literature survey,” *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–37, 2020.

[74] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations,” *IEEE Commun. Surv. Tutor.*, vol. 21, no. 3, pp. 2702–2733, 2019.

[75] K. W. Ching and M. M. Singh, “Wearable technology devices security and privacy vulnerability analysis,” *Int. j. netw. secur. appl.*, vol. 8, no. 3, pp. 19–30, 2016.

[76] H. Qiu, X. Wang, and F. Xie, “A survey on smart wearables in the application of fitness,” in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, 2017, pp. 303–307.

- [77] J. Blasco, T. M. Chen, J. Tapiador, and P. Peris-Lopez, "A survey of wearable biometric recognition systems," *ACM Comput. Surv.*, vol. 49, no. 3, pp. 1–35, 2016.
- [78] T. Wu, F. Breitingner, and I. Baggili, "IoT ignorance is digital forensics research bliss: A survey to understand IoT forensics definitions, challenges and future research directions," in *Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19*, 2019.
- [79] A. Aminnezhad, A. Dehghantanha, and M. T. Abdullah, "A Survey on Privacy Issues in Digital Forensics," *International Journal of Cyber-Security and Digital Forensics*, vol. 1, no. 4, pp. 311–323, May 2015.
- [80] M. Kalantari, "Consumers adoption of wearable technologies: literature review, synthesis, and future research agenda," *Int. J. Technol. Mark.*, vol. 12, no. 1, p. 1, 2017.
- [81] L.-H. Lee and P. Hui, "Interaction methods for smart glasses: A survey," *IEEE Access*, vol. 6, pp. 28712–28732, 2018.
- [82] M. Koelle, S. Ananthanarayan, S. Czupalla, W. Heuten, and S. Boll, "Your smart glasses' camera bothers me!: Exploring opt-in and opt-out gestures for privacy mediation," in *Proceedings of the 10th Nordic Conference on Human-Computer Interaction - NordiCHI '18*, 2018.
- [83] L. Sanchez, C. Grajeda, I. Baggili, and C. Hall, "A practitioner survey exploring the value of forensic tools, AI, filtering, & safer presentation for investigating child sexual abuse material (CSAM)," *Digit. investig.*, vol. 29, pp. S124–S142, 2019.
- [84] H.-E. Lee, T. Ermakova, V. Ververis, and B. Fabian, "Detecting child sexual abuse material: A comprehensive survey," *Forensic Science International: Digital Investigation*, vol. 34, no. 301022, p. 301022, 2020.
- [85] A. Hayes, "The Socioethical Implications of Body Worn Computers: An Ethnographic Study," University of Wollongong, NSW, Australia, 2020.
- [86] S. Safavi and Z. Shukur, "Improving Google glass security and privacy by changing the physical and software structure," *Life Science Journal*, vol. 11, no. 5, pp. 109–117, May 2014.
- [87] K. Ghazinour, E. Shirima, V. R. Parne, and A. BhoomReddy, "A model to protect sharing sensitive information in smart watches," *Procedia Comput. Sci.*, vol. 113, pp. 105–112, 2017.
- [88] R. Yus, P. Pappachan, P. K. Das, E. Mena, A. Joshi, and T. Finin, "Demo: FaceBlock: privacy-aware pictures for google glass," in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services - MobiSys '14*, 2014.
- [89] P. Pappachan, R. Yus, P. K. Das, T. Finin, E. Mena, and A. Joshi, "A semantic context-aware privacy model for FaceBlock," 2014.

- [90] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, “Advanced security testbed framework for wearable IoT devices,” *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–25, 2016.
- [91] P. A. Rauschnabel, J. He, and Y. K. Ro, “Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks,” *J. Bus. Res.*, vol. 92, pp. 374–384, 2018.
- [92] N. Zuidhof, S. Ben, O. Peters, and P.-P. Verbeek, “A theoretical framework to study long-term use of smart eyewear,” in *Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers - UbiComp/ISWC '19*, 2019.
- [93] P. A. Rauschnabel, A. Brem, and B. S. Ivens, “Who will buy smart glasses? Empirical results of two pre-market-entry studies on the role of personality in individual awareness and intended adoption of Google Glass wearables,” *Comput. Human Behav.*, vol. 49, pp. 635–647, 2015.
- [94] H. Li, J. Wu, Y. Gao, and Y. Shi, “Examining individuals’ adoption of healthcare wearable devices: An empirical study from privacy calculus perspective,” *Int. J. Med. Inform.*, vol. 88, pp. 8–17, 2016.
- [95] A. E. Ok, N. A. Basoglu, and T. Daim, “Exploring the design factors of smart glasses,” in *2015 Portland International Conference on Management of Engineering and Technology (PICMET)*, 2015, pp. 1657–1664.
- [96] S. Parker and J.-P. Van Belle, “Lifelogging and lifeblogging: Privacy issues and influencing factors in South Africa,” in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 2015, pp. 111–117.
- [97] National Institute of Standards and Technology, “Nist privacy framework:: A tool for improving privacy through enterprise risk management, version 1.0,” National Institute of Standards and Technology, Gaithersburg, MD, 2020.
- [98] “ISO/IEC 19510:2013,” Iso.org, 2018. [Online]. Available: <https://www.iso.org/standard/62652.html>. [Accessed: 2020].
- [99] P. Pullonen, R. Matulevičius, and D. Bogdanov, “PE-BPMN: Privacy-enhanced business process model and notation,” in *Lecture Notes in Computer Science*, Cham: Springer International Publishing, 2017, pp. 40–56.
- [100] P. Pullonen, J. Tom, R. Matulevičius, and A. Toots, “Privacy-enhanced BPMN: enabling data privacy analysis in business processes models,” *Softw. Syst. Model.*, vol. 18, no. 6, pp. 3235–3264, 2019.
- [101] E. Mouggiakou and M. Virvou, “Based on GDPR privacy in UML: Case of e-learning program,” in *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 2017, pp. 1–8.
- [102] T. Lodderstedt, D. A. Basin, and J. Doser, “SecureUML: A UML-based modeling language for model-driven security,” in *UML 2002 - The Unified Modeling Language*, 5th International Conference on the Unified Modeling Language, 2002, pp. 426–441.

- [103] D. A. Basin, J. Doser, and T. Lodderstedt, "Model Driven Security: From UML models to access control infrastructures," *ACM Transactions on Software Engineering and Methodology*, vol. 15, no. 1, pp. 39–91, Jan. 2006.
- [104] J. Jürjens and J. Jurjens, *Secure systems development with UML*. New York, NY: Springer, 2005.
- [105] J. Jürjens, "Model-Based Security Engineering with UML," in *Foundations of Security Analysis and Design III, FOSAD 2004/2005 Tutorial Lectures*, 2004.
- [106] J. Jürjens, "UMLsec: Extending UML for secure systems development," in *«UML» 2002 — The Unified Modeling Language*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 412–425.
- [107] J. Jürjens, "Towards development of secure systems using UMLsec," in *Fundamental Approaches to Software Engineering*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 187–200.
- [108] R. Matulevičius and M. Dumas, "A comparison of SecureUML and UMLsec for role-based access control," *Cs.ut.ee*. [Online]. Available: <https://courses.cs.ut.ee/2010/is/uploads/Main/RBAC-for-UML.pdf>. [Accessed: 2020].
- [109] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requir. Eng.*, vol. 10, no. 1, pp. 34–44, 2005.
- [110] G. Sindre, "Mal-activity diagrams for capturing attacks on business processes," in *Requirements Engineering: Foundation for Software Quality*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 355–366.
- [111] V. Diamantopoulou, M. Pavlidis, and H. Mouratidis, "Evaluation of a security and privacy requirements methodology using the physics of notation," in *Computer Security*, Cham: Springer International Publishing, 2018, pp. 210–225.
- [112] H. Mouratidis and P. Giorgini, "Secure Tropos: A security-oriented extension of the Tropos methodology," *Int. j. softw. eng. knowl. eng.*, vol. 17, no. 02, pp. 285–309, 2007.
- [113] "About the business process model and notation specification version 2.0.1," *Omg.org*. [Online]. Available: <https://www.omg.org/spec/BPMN/2.0.1/>. [Accessed: 2020].
- [114] "About the business process model and notation specification version 2.0.2," *Omg.org*. [Online]. Available: <https://www.omg.org/spec/BPMN/2.0.2/>. [Accessed: 2020].
- [115] "Information technology - Object Management Group Unified Modeling Language (OMG UML), Superstructure," *Omg.org*, Apr-2012. [Online]. Available: <https://www.omg.org/spec/UML/ISO/19505-2/PDF>. [Accessed: 2020].
- [116] "ISO/IEC 19505-2:2012," *Iso.org*, 2017. [Online]. Available: <https://www.iso.org/standard/52854.html>. [Accessed: 2020].

[117] D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger, “Network and device forensic analysis of Android social-messaging applications,” *Digit. investig.*, vol. 14, pp. S77–S84, 2015.

[118] T. Alyahya and F. Kausar, “Snapchat analysis to discover digital forensic artifacts on android smartphone,” *Procedia Comput. Sci.*, vol. 109, pp. 1035–1040, 2017.

[119] “Snap Inc,” *Snap.com*. [Online]. Available: <https://www.snap.com/en-US>. [Accessed: 2020].

[120] Snap, Inc., “Snapchat,” <https://play.google.com/>. [Online]. Available: <https://play.google.com/store/apps/details?id=com.snapchat.android&hl=en&gl=ee>. [Accessed: 2020].

[121] Q4cdn.com. [Online]. Available: https://s25.q4cdn.com/442043304/files/doc_financials/2020/q3/461758eb-1c14-400e-a425-08873e878de9.pdf. [Accessed: 2020].

[122] “Data processing agreement – snap inc,” *Snap.com*. [Online]. Available: <https://www.snap.com/en-US/terms/data-processing-agreement/>. [Accessed: 2020].

[123] “Privacy center – snap inc,” *Snap.com*. [Online]. Available: <https://www.snap.com/en-US/privacy/privacy-policy/>. [Accessed: 2020].

[124] “Snap Privacy and Security FAQs,” *Snapchat.com*. [Online]. Available: <https://businesshelp.snapchat.com/en-US/article/snap-privacy-faq>. [Accessed: 2020].

[125] “Snap and the GDPR,” *Snapchat.com*. [Online]. Available: https://businesshelp.snapchat.com/s/article/gdpr?language=en_US. [Accessed: 2020].

[126] “Snap and The CCPA,” *Snapchat.com*. [Online]. Available: <https://businesshelp.snapchat.com/en-US/article/ccpa>. [Accessed: 2020].

[127] “Snap and Brexit,” *Snapchat.com*. [Online]. Available: https://businesshelp.snapchat.com/s/article/snap-brexit?language=en_US. [Accessed: 2020].

[128] “Snap Inc. and Privacy Shield,” *Snap.com*. [Online]. Available: <https://www.snap.com/en-US/privacy/privacy-shield/>. [Accessed: 13-Mar-2019].

[129] “Privacy Shield,” *Privacyshield.gov*. [Online]. Available: <https://www.privacyshield.gov/participant?id=a2zt0000000TNPxAAO&status=Active>. [Accessed: 11-Nov-2019].

[130] “Transparency Report,” *Snap.com*. [Online]. Available: <https://www.snap.com/en-US/privacy/transparency/>. [Accessed: 2020].

[131] Related Inquiries, “Contact Information for Law Enforcement,” *Googleapis.com*. [Online]. Available: <https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf>. [Accessed: 2020].

- [132] “Snapchat, inc., in the matter of,” Ftc.gov, 08-May-2014. [Online]. Available:
<https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter>. [Accessed: 2020].
- [133] “Snapchat employees abused data access to spy on users,” Vice.com. [Online]. Available:
<https://www.vice.com/en/article/xwnva7/snapchat-employees-abused-data-access-spy-on-users-snaplion>. [Accessed: 2020].
- [134] V. Blue, “Researchers publish Snapchat code allowing phone number matching after exploit disclosures ignored,” ZDNet, 25-Dec-2013. [Online]. Available:
<https://www.zdnet.com/article/researchers-publish-snapchat-code-allowing-phone-number-matching-after-exploit-disclosures-ignored/>. [Accessed: 2020].
- [135] Gibson Security, “@Snapchat Full disclosure release, complete API documentation + 2 exploits,” Twitter.com, 24-Dec-2013. [Online]. Available:
<https://twitter.com/gibsonsec/status/415596725290532865>. [Accessed: 2020].
- [136] “Snapchat - GSFD,” Gibsonsec.org. [Online]. Available:
<https://gibsonsec.org/snapchat/fulldisclosure/>. [Accessed: 2020].
- [137] C. Shu, “Confirmed: Snapchat Hack Not A Hoax, 4.6M Usernames And Numbers Published,” TechCrunch, 01-Jan-2014.
- [138] C. Shu, “Snapchat Hacked By Fruit Smoothie Enthusiast,” TechCrunch, 12-Feb-2014.
- [139] J. Cook, “Hackers access at least 100,000 snapchat photos and prepare to leak them, including underage nude pictures,” Business Insider, 10-Oct-2014.
- [140] S. Gallagher, “Snapchat images stolen from third-party Web app using hacked API [Updated],” Arstechnica.com, 10-Oct-2014. [Online]. Available:
<https://arstechnica.com/information-technology/2014/10/snapchat-images-stolen-from-third-party-web-app-using-hacked-api/>. [Accessed: 2020].
- [141] J. Crook, “Snapsaved Takes Responsibility For Latest Snapchat Leak,” TechCrunch, 13-Oct-2014.
- [142] J. Crook, “Snapchat Reminds Us That Users Are To Blame For Photo Leaks,” TechCrunch, 14-Oct-2014.
- [143] P. Dave, “Snapchat employee data compromised in phishing attack,” The Los Angeles times, Los Angeles Times, 29-Feb-2016.
- [144] C. Newton, “A phishing attack scored credentials for more than 50,000 Snapchat users,” The Verge, 16-Feb-2018. [Online]. Available:
<https://www.theverge.com/2018/2/16/17017078/snapchat-phishing-attack-klkviral-dominican-republic>. [Accessed: 2020].
- [145] “Spectacles by snap inc. • shop,” Spectacles.com. [Online]. Available:
<https://www.spectacles.com/fi/shop>. [Accessed: 2020].

- [146] “002 Wearable video camera, 002 Teardown Internal Photos Internal picture Snap,” Fccid.io, 20-Aug-2018. [Online]. Available: <https://fccid.io/2AIRN-002/Internal-Photos/Internal-picture-3974560>. [Accessed: 2020].
- [147] “002 Wearable video camera, 002 Teardown Internal Photos Internal picture Snap,” Fccid.io, 20-Aug-2018. [Online]. Available: <https://fccid.io/2AIRN-002/Internal-Photos/Internal-picture-3974899>. [Accessed: 2020].
- [148] A. O’Neill, “Open Source Software,” in *Encyclopedia of Applied Ethics*, Elsevier, 2012, pp. 281–287.
- [149] “Compatibility Guide,” Spectacles.com. [Online]. Available: <https://support.spectacles.com/hc/en-us/articles/360033763231-Compatibility-Guide>. [Accessed: 2020].
- [150] K. Scharfglass, “Snap Spectacles V2 Teardown: A feat in space-constrained hardware engineering,” Mindtribe, 19-Mar-2019. [Online]. Available: <https://mindtribe.com/2019/03/snap-spectacles-v2-teardown-a-feat-in-space-constrained-hardware-engineering>. [Accessed: 2020].
- [151] “Shop • Spectacles 2 (Veronica),” Spectacles.com. [Online]. Available: <https://www.spectacles.com/fi/shop/veronica#tech-specs>. [Accessed: 2020].
- [152] “QCA9377,” Qualcomm.com, 02-Oct-2018. [Online]. Available: <https://www.qualcomm.com/products/qca9377>. [Accessed: 2020].
- [153] “nRF52832 - Nordic Semiconductor,” Nordicsemi.com. [Online]. Available: <https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52832>. [Accessed: 2020].
- [154] “Nordic Semiconductor Infocenter,” Nordicsemi.com. [Online]. Available: https://infocenter.nordicsemi.com/index.jsp?topic=%2Fstruct_nrf52%2Fstruct%2Fnrf52832.html&cp=3_2. [Accessed: 2020].
- [155] “Capturing Snaps,” Spectacles.com. [Online]. Available: <https://support.spectacles.com/hc/en-us/articles/360000412923-Capturing-Snaps>. [Accessed: 2020].
- [156] “Spectacles LED Messages,” Spectacles.com. [Online]. Available: <https://support.spectacles.com/hc/en-us/articles/360000413863-Spectacles-LED-Messages>. [Accessed: 2020].
- [157] “Pairing Your Spectacles,” Spectacles.com. [Online]. Available: <https://support.spectacles.com/hc/en-us/articles/360000407246>. [Accessed: 2020].
- [158] “AS3709,” Ams.com. [Online]. Available: <https://ams.com/search#/AS3709>. [Accessed: 2020].
- [159] “Photos - People : USDA ARS,” Usda.gov. [Online]. Available: <https://www.ars.usda.gov/oc/images/photos/photos-people/>. [Accessed: 2020].
- [160] “The Public Domain Project,” Pond5.com. [Online]. Available: <https://www.pond5.com/free>. [Accessed: 2020].

- [161] "Flowchart maker & online diagram software," Diagrams.net. [Online]. Available: <https://app.diagrams.net/>. [Accessed: 2020].
- [162] "WiFi Monitor: analyzer of WiFi networks," Google.com. [Online]. Available: <https://play.google.com/store/apps/details?id=com.signalmonitoring.wifimonitoring&hl=en>. [Accessed: 2020].
- [163] "Network Analyzer," Google.com. [Online]. Available: <https://play.google.com/store/apps/details?id=net.techet.netanalyzerlite.an&hl=en>. [Accessed: 2020].
- [164] "Wireshark · Go Deep," Wireshark.org. [Online]. Available: <https://www.wireshark.org>. [Accessed: 2020].
- [165] "Wireshark · OUI Lookup Tool," Wireshark.org. [Online]. Available: <https://www.wireshark.org/tools/oui-lookup.html>. [Accessed: 2020].
- [166] "IEEE Registration Authority Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)," Ieee.org, 03-Aug-2017. [Online]. Available: <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf>. [Accessed: 2020].
- [167] "Host Discovery," Nmap.org. [Online]. Available: <https://nmap.org/book/man-host-discovery.html>. [Accessed: 2020].
- [168] "Options Summary," Nmap.org. [Online]. Available: <https://nmap.org/book/man-briefoptions.html>. [Accessed: 2020].
- [169] "Understanding an Nmap Fingerprint," Nmap.org. [Online]. Available: <https://nmap.org/book/osdetect-fingerprint-format.html>. [Accessed: 2020].
- [170] "CaptureSetup/WLAN - The Wireshark Wiki," Wireshark.org. [Online]. Available: <https://wiki.wireshark.org/CaptureSetup/WLAN>. [Accessed: 2020].
- [171] "Wi-Fi - The Wireshark Wiki," Wireshark.org. [Online]. Available: <https://wiki.wireshark.org/Wi-Fi>. [Accessed: 2020].
- [172] "HowToDecrypt802.11 - The Wireshark Wiki," Wireshark.org. [Online]. Available: <https://wiki.wireshark.org/HowToDecrypt802.11>. [Accessed: 2020].
- [173] "nRF Connect for Mobile," Google.com. [Online]. Available: <https://play.google.com/store/apps/details?id=no.nordicsemi.android.mcp&hl=en>. [Accessed: 2020].
- [174] "nRF Logger," Google.com. [Online]. Available: <https://play.google.com/store/apps/details?id=no.nordicsemi.android.log>. [Accessed: 2020].
- [175] "Download the Free Nmap Security Scanner for Linux/mac/windows," Nmap.org. [Online]. Available: <https://nmap.org/download.html>. [Accessed: 2020].
- [176] "Assigned Numbers," Bluetooth.com. [Online]. Available: <https://www.bluetooth.com/specifications/assigned-numbers/>. [Accessed: 2020].

- [177] “Company Identifiers,” Bluetooth.com. [Online]. Available: <https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers/>. [Accessed: 2020].
- [178] “Core Specifications,” Bluetooth.com. [Online]. Available: <https://www.bluetooth.com/specifications/bluetooth-core-specification/>. [Accessed: 2020].
- [179] P. J. Leach, M. Mealling, and R. Salz, “A Universally Unique Identifier (UUID) URN Namespace,” 2005.
- [180] “Generic Access Profile,” Bluetooth.com. [Online]. Available: <https://www.bluetooth.com/specifications/assigned-numbers/generic-access-profile/>. [Accessed: 2020].
- [181] “Supplement to the Bluetooth Core Specification Version 4,” Bluetooth.org, 03-Dec-2013. [Online]. Available: https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=282152. [Accessed: 2020].
- [182] T. Whitlock, “Emoji unicode characters for use on the web,” Timwhitlock.info. [Online]. Available: <https://apps.timwhitlock.info/emoji/tables/unicode>. [Accessed: 2020].
- [183] “Hex to ASCII,” Rapidtables.com. [Online]. Available: <https://www.rapidtables.com/convert/number/hex-to-ascii.html>. [Accessed: 2020].
- [184] “Nordic Semiconductor Infocenter,” Nordicsemi.com. [Online]. Available: https://infocenter.nordicsemi.com/index.jsp?topic=%2Fcom.nordic.infocenter.s132.api.v4.0.2%2Fgroup__b_l_e__u_u_i_d__v_a_l_u_e_s.html. [Accessed: 2020].
- [185] “TRANSPORT_LE,” Android.com. [Online]. Available: https://developer.android.com/reference/android/bluetooth/BluetoothDevice#TRANSPORT_LE. [Accessed: 2020].
- [186] “PHY_LE_1M,” Android.com. [Online]. Available: https://developer.android.com/reference/android/bluetooth/BluetoothDevice#PHY_LE_1M. [Accessed: 2020].
- [187] M. Woolley, “Exploring Bluetooth 5 -going the distance,” Bluetooth.com, 13-Feb-2017. [Online]. Available: <https://www.bluetooth.com/blog/exploring-bluetooth-5-going-the-distance/>. [Accessed: 2020].
- [188] “ACTION_ACL_CONNECTED,” Android.com. [Online]. Available: https://developer.android.com/reference/android/bluetooth/BluetoothDevice#ACTION_ACL_CONNECTED. [Accessed: 2020].
- [189] “BluetoothDevice,” Android.com. [Online]. Available: <https://developer.android.com/reference/android/bluetooth/BluetoothDevice>. [Accessed: 2020].

- [190] “Nordic UART Service (NUS) — nRF Connect SDK 1.4.99 documentation,” Nordicsemi.com. [Online]. Available: https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/include/bluetooth/services/nus.html. [Accessed: 2020].
- [191] T. Vidas, C. Zhang, and N. Christin, “Toward a general collection methodology for Android devices,” *Digit. investig.*, vol. 8, pp. S14–S24, 2011.
- [192] “nRF52840 DK,” Nordicsemi.com. [Online]. Available: <https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF52840-DK>. [Accessed: 2020].
- [193] “nRF52 Series.” [Online]. Available: https://infocenter.nordicsemi.com/topic/struct_nrf52/struct/nrf52.html. [Accessed: 2020].
- [194] “nRF Sniffer for Bluetooth LE.” [Online]. Available: https://infocenter.nordicsemi.com/topic/ug_sniffer_ble/UG/sniffer_ble/intro.html. [Accessed: 2020].
- [195] “Running nRF Sniffer.” [Online]. Available: https://infocenter.nordicsemi.com/topic/ug_sniffer_ble/UG/sniffer_ble/running_sniffer.html. [Accessed: 2020].
- [196] “Spectacles Look and Fit,” Spectacles.com. [Online]. Available: <https://support.spectacles.com/hc/en-us/articles/360001297463-Spectacles-Look-and-Fit>. [Accessed: 2020].
- [197] J. Marcel and M. Afaneh, “The Bluetooth LE security study guide,” Bluetooth.com, 25-Oct-2019. [Online]. Available: <https://www.bluetooth.com/bluetooth-resources/le-security-study-guide/>. [Accessed: 2020].
- [198] J. Padgett et al., “Guide to bluetooth security,” National Institute of Standards and Technology, Gaithersburg, MD, 2017.
- [199] M. Ryan, “Bluetooth: With Low Energy comes Low Security,” Usenix.org. [Online]. Available: <https://www.usenix.org/system/files/conference/woot13/woot13-ryan.pdf>. [Accessed: 2020].
- [200] M. Ryan, Crackle - Crack and decrypt BLE encryption. .
- [201] “Kali Linux Downloads,” Kali.org. [Online]. Available: <https://www.kali.org/downloads/>. [Accessed: 2020].
- [202] M. Ryan, crackle - add support for PCAPs generated by the Nordic BLE sniffer. #44. .
- [203] “Hard Reset your Spectacles,” Spectacles.com. [Online]. Available: <https://support.spectacles.com/hc/en-us/articles/360000479226-Hard-Reset-Your-Spectacles>. [Accessed: 2020].
- [204] M. Ryan, crackle - Crackle not decrypting the Android BT snooping enabled packet dumps ? #37. .

- [205] “Capture and read bug reports,” Android.com. [Online]. Available: <https://developer.android.com/studio/debug/bug-report>. [Accessed: 2020].
- [206] “Android Debug Bridge (adb),” Android.com. [Online]. Available: <https://developer.android.com/studio/command-line/adb>. [Accessed: 2020].
- [207] “Fix ADB Devices Not Shown|USB Debugging issue| Device is not listed in adb devices Camand| Miui8,” 26-Feb-2017. [Online]. Available: https://www.youtube.com/watch?v=JR4fBbcB_AU. [Accessed: 2020].
- [208] “Android Debug Bridge (adb) | Android Developers | Backup and Restore Commands.” [Online]. Available: <https://web.archive.org/web/20180426100826/https://developer.android.com/studio/command-line/adb>. [Accessed: 2020].
- [209] “7-Zip,” 7-Zip.org. [Online]. Available: <https://www.7-zip.org/>. [Accessed: 2020].
- [210] Bhardwaj, “Android Backup File(.ab) Analysis,” Digitalforensicforest.com. [Online]. Available: <https://digitalforensicforest.com/2016/01/28/android-backup-file-ab-analysis/>. [Accessed: 2020].
- [211] “Dumpsys,” Android.com. [Online]. Available: <https://developer.android.com/studio/command-line/dumpsys>. [Accessed: 2020].
- [212] “meminfo,” Android.com. [Online]. Available: <https://developer.android.com/studio/command-line/dumpsys#meminfo>. [Accessed: 2020].
- [213] Related Inquiries, “Contact Information for Law Enforcement,” Snapchat.com. [Online]. Available: <https://www.snapchat.com/lawenforcement>. [Accessed: 2020].
- [214] “Law Enforcement Service System,” Snapchat.com. [Online]. Available: <https://less.snapchat.com/>. [Accessed: 2020].
- [215] “Snapchat Support - Download my data,” Snapchat.com. [Online]. Available: <https://support.snapchat.com/en-US/a/download-my-data>. [Accessed: 2020].
- [216] “Log In • Snapchat,” Snapchat.com. [Online]. Available: <https://accounts.snapchat.com>. [Accessed: 2020].
- [217] K. Features, “H2 Video SoC for Consumer Applications,” Ambarella.com. [Online]. Available: <https://www.ambarella.com/wp-content/uploads/H2-Product-Brief.pdf>. [Accessed: 2020].
- [218] “Samsung Galaxy S10e (Exynos),” Twrp.me. [Online]. Available: <https://twrp.me/samsung/samsunggalaxys10e.html>. [Accessed: 13-Dec-2020].
- [219] “Magisk Installation: Samsung (System-as-root).” [Online]. Available: <https://topjohnwu.github.io/Magisk/install.html#samsung-system-as-root>. [Accessed: 2020].

- [220] “Download twrp-3.4.0-0-beyond0lte.img.tar,” Twrp.me. [Online]. Available: <https://eu.dl.twrp.me/beyond0lte/twrp-3.4.0-0-beyond0lte.img.tar.html>. [Accessed: 2020].
- [221] M. Hassan and L. Pantaleon, “An investigation into the impact of rooting android device on user data integrity,” in 2017 Seventh International Conference on Emerging Security Technologies (EST), 2017.
- [222] R. Ayers, S. Brothers, and W. Jansen, “Guidelines on mobile device forensics,” National Institute of Standards and Technology, 2014.
- [223] “Snapchat 10.77.5.0 (arm64-v8a) (nodpi) (Android 4.4+),” Apkmirror.com. [Online]. Available: <https://www.apkmirror.com/apk/snap-inc/snapchat/snapchat-10-77-5-0-release/snapchat-10-77-5-0-2-android-apk-download>. [Accessed: 2020].
- [224] “TWRP for lavender,” Twrp.me. [Online]. Available: <https://eu.dl.twrp.me/lavender/>. [Accessed: 2020].
- [225] J. Wu, Magisk Manager v7.5.1. 2020.
- [226] J. Wu, Magisk v20.4. 2020.
- [227] “[GUIDE]: Flash Oreo (G955FXXU1CRB7) using new Odin (3.13.1),” Xda-developers.com. [Online]. Available: <https://forum.xda-developers.com/galaxy-s8+/how-to/guide-flash-oreo-g955fxxu1crb7-using-t3755789>. [Accessed: 2020].
- [228] “Android Studio Download,” Android.com. [Online]. Available: <https://developer.android.com/studio>. [Accessed: 2020].
- [229] “Apply for unlocking Mi devices,” Miui.com. [Online]. Available: <https://en.miui.com/unlock/>. [Accessed: 2020].
- [230] “Xiaomi Redmi Note 7,” Twrp.me. [Online]. Available: <https://twrp.me/xiaomi/xiaomiredminote7.html>. [Accessed: 2020].
- [231] “Build,” Android.com. [Online]. Available: <https://developer.android.com/reference/android/os/Build.html>. [Accessed: 2020].
- [232] “[GUIDE] How to enable adb backup for any app changing android:allowBackup,” Xda-developers.com. [Online]. Available: <https://forum.xda-developers.com/android/software-hacking/guide-how-to-enable-adb-backup-app-t3495117>. [Accessed: 2020].
- [233] M. Ibrahim, “Android: Enable ADB backup for any app,” Stackpointer.io, 02-May-2015. [Online]. Available: <https://stackpointer.io/mobile/android-enable-adb-backup-for-any-app/462/>. [Accessed: 2020].
- [234] “How to force any android app to allow adb backup,” Blogspot.com. [Online]. Available: <http://dalvikplanet.blogspot.com/2020/05/how-to-force-any-android-app-to-allow.html>. [Accessed: 2020].

- [235] “Acquiring an Android device,” Magnetforensics.com. [Online]. Available: https://www.magnetforensics.com/docs/axiom/html/Content/en-us/acquire-mobile/acquiring-android.htm?tocpath=Magnet%20AXIOM%7CAcquiring%20and%20loading%20evidence%7CAcquiring%20mobile%20evidence%7CAcquiring%20an%20Android%20device%7C_____0. [Accessed: 2020].
- [236] “stat(1): file/file system status - Linux man page,” Die.net. [Online]. Available: <https://linux.die.net/man/1/stat>. [Accessed: 2020].
- [237] “od(1): dump files in octal/other formats - Linux man page,” Die.net. [Online]. Available: <https://linux.die.net/man/1/od>. [Accessed: 2020].
- [238] “hexdump(1) - Linux man page,” Die.net. [Online]. Available: <https://linux.die.net/man/1/hexdump>. [Accessed: 2020].
- [239] “WebP Container Specification - Naming,” Google.com. [Online]. Available: https://developers.google.com/speed/webp/docs/riff_container. [Accessed: 2020].
- [240] “WebP Container Specification - WebP File Header,” Google.com. [Online]. Available: https://developers.google.com/speed/webp/docs/riff_container. [Accessed: 2020].
- [241] “Categorizing evidence with magnet.AI,” Magnetforensics.com. [Online]. Available: <https://www.magnetforensics.com/docs/axiom/html/Content/en-us/magnet-ai/categorize-evidence-magnet-ai.htm?Highlight=possible%20human%20faces>. [Accessed: 2020].
- [242] “Finding similar pictures with Magnet.AI,” Magnetforensics.com. [Online]. Available: https://www.magnetforensics.com/docs/axiom/html/Content/en-us/magnet-ai/finding-similar-pictures-magnet-ai.htm?tocpath=Magnet%20AXIOM%7CAnalyzing%20evidence%20with%20Magnet.AI%7C_____2. [Accessed: 2020].
- [243] T. W. Edgar and D. O. Manz, Research methods for cyber security. Rockland, MA: Syngress Media, 2017.
- [244] “Epoch Converter,” Epochconverter.com. [Online]. Available: <https://www.epochconverter.com/>. [Accessed: 2020].
- [245] “TCP/IP Fingerprinting Methods Supported by Nmap,” Nmap.org. [Online]. Available: <https://nmap.org/book/osdetect-methods.html>. [Accessed: 2020].
- [246] “SEgger - the embedded experts - downloads - J-link / J-trace,” Segger.com. [Online]. Available: <https://www.segger.com/downloads/jlink/>. [Accessed: 15-Dec-2020].
- [247] “Python Release Python 3.7.7,” Python.org. [Online]. Available: <https://www.python.org/downloads/release/python-377/>. [Accessed: 15-Dec-2020].
- [248] “nRF Sniffer for Bluetooth LE - Downloads,” Nordicsemi.com. [Online]. Available:

<https://www.nordicsemi.com/Software-and-tools/Development-Tools/nRF-Sniffer-for-Bluetooth-LE/Download>. [Accessed: 2020].

[249] “Issue shell commands,” Android.com. [Online]. Available: <https://developer.android.com/studio/command-line/adb#shellcommands>. [Accessed: 2020].

[250] “Copy files to/from a device,” Android.com. [Online]. Available: <https://developer.android.com/studio/command-line/adb#copyfiles>. [Accessed: 2020].

[251] “Autopsy,” Autopsy.com, 12-Aug-2019. [Online]. Available: <https://www.autopsy.com/download/>. [Accessed: 2020].

[252] “ExifTool by Phil Harvey,” Exiftool.org. [Online]. Available: <https://exiftool.org/>. [Accessed: 2020].

[253] “VLC Media Player (64-bit),” Cnet.com. [Online]. Available: https://download.cnet.com/VLC-Media-Player-64-bit/3000-13632_4-75761094.html. [Accessed: 15-Dec-2020].

[254] “Odin3 v3.13.1,” Xda-developers.com. [Online]. Available: <https://forum.xda-developers.com/t/odin3-v3-13-1.2711451/>. [Accessed: 2020].

[255] R. Matulevičius, Fundamentals of secure system modelling, 1st ed. Cham, Switzerland: Springer International Publishing, 2017.

[256] “Snapchat Support - When does Snapchat delete Snaps and Chats?,” Snapchat.com. [Online]. Available: <https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted>. [Accessed: 2020].

[257] “About Transparency Reporting: History of Snap’s Transparency Reporting,” Snap Inc. [Online]. Available: <https://www.snap.com/en-US/privacy/transparency/about>.

Appendix

The IP ID sequence generation algorithm (SEQ) conducted two tests (**CI**, **II**) examining the IP header ID field of responses.[245]

Table x. NMAP v7.80 IP ID sequence generation algorithm (SEQ) fingerprint results for smart eyewear paired smartphone [245]

SEQ test names	SEQ test results
(CI) Responses from the three TCP probes sent to a closed port: T5, T6, and T7. At least two responses are required.	CI= Z = All of the ID numbers were zero
(II) Responses from the ICMP responses to the two IE ping probes Both ICMP responses must be received	II= I = Incremental, since all differences were less than 10.

Table x. NMAP v7.8 TCP/IP T5-T7, U1, and IE fingerprint results for smart eyewear paired smartphone [245]

	T5	T6	T7	U1	IE
(R)	R=Y Target responded to probe	R=Y Targets responded to both ICMP echo request packets			
(DF) IP don't fragment bit. IP header contains a single bit forbidding routers from fragmenting a packet.	DF=Y YES, bit is set	DF=Y YES, bit is set	DF=Y YES, bit is set	DF=N NO, bit is NOT set	
(DFI) Custom test for special dual-probe ICMP					DFI=N Neither target set DF bit
(T) IP packet initial time-to-live Used for OS detection	T=40	T=40	T=40	T=40	T=40 for 1st ICMP echo request packet probe
(CD) ICMP response code value of an ICMP echo reply					CD=S for 1st ICMP echo request packet probe. S = Both code values are the same
(TG) IP initial					

time-to-live guess					
(W)	W=0	W=0	W=0		
(S) Exam of how 32-bit TCP sequence number field in the TCP header compares to TCP acknowledgment number from probe	S=Z Sequence number is zero	S=A Sequence number matches acknowledgment number in probe	S=Z Sequence number is zero		
(A) Tests how TCP acknowledgment number in the response compares to the sequence number in probe	A=S+ Acknowledgment number matches sequence number in probe plus one	A=Z Acknowledgment number is zero	A=S+ Acknowledgment number matches sequence number in probe plus one		
(F) TCP flags from probe response recorded. Each letter is one flag in same order as TCP packet	F=AR Flag name: Acknowledgment (ACK) Flag byte value: 16 Flag name: Reset (RST) Flag byte value: 4	F=R Flag name: Reset (RST) Flag byte value: 4	F=AR Flag name: Acknowledgment (ACK) Flag byte value: 16 Flag name: Reset (RST) Flag byte value: 4		
(O)	O=	O=	O=		
(RD) TCP RST data checksum	RD=0 No ASCII data, such as error messages, returned in reset packets	RD=0 No ASCII data, such as error messages, returned in reset packets	RD=0 No ASCII data, such as error messages, returned in reset packets		
(Q) TCP miscellaneous quirks	Q= Since empty, no quirks are present	Q= Since empty, no quirks are present	Q= Since empty, no quirks are present		
(IPL) IP total length (in octets) of an IP packet				IPL=164	
(UN) Unused port unreachable field nonzero				UN=0 Last four bytes of ICMP port unreachable message header are confirmed as zero	
(RIPL) Returned probe IP total length value				RIPL=G G = good, since correct IP total length value of 0x148 (328)	

(RID) Returned probe IP ID value				RID=G G = good, since returned static value of 0x1042 in port unreachable message	
(RIPCK) Integrity of returned probe IP checksum value				RIPCK=G G = good, since checksum matches enclosed IP packet	
(RUCK) Integrity of returned probe UDP checksum				RUCK=G G = good, since UDP header checksum value matches sent value	
(RUD) Integrity of returned UDP data				RUD=G G = good, since all payload bytes are the expected 'C' (0x43), or if the payload was truncated to zero length	