TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Cybersecurity Curriculum

Gustav Gretškov

Portless Device Forensics in the Future

Master's Thesis

Supervisor: Matthew James Sorell, PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Küberturve ainekava

Gustav Gretškov

Juhtmeteta seadmete kriminalistika tulevikus

Magistritöö

Juhendaja: Matthew James Sorell, PhD

Tallinn 2025

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.

Author: Gustav Gretškov

18.05.2025

Portless Device Forensics in the Future

Abstract:
Device forensics has been a key process in crime investigation since the emergence of computer systems into the mainstream ever since the 80s and has only been growing since. This process was enabled from the start by the I/O ports on devices allowing for data extraction. While software and procedures regarding this process have changed over the years, the core principle has remained the same. However, the rise of the Internet of Things (IoT) along with the development of wireless technologies presents the threat of devices without ports. This may potentially become a serious problem in digital forensics and hinder the operations of crime investigations which already rely heavily on the speed of every process involved. This paper performs a systematic literature review to determine the currently possible alternatives and strategies to portless data extraction as well as understand the prevalence of portless devices. It then contrasts the results with answers obtained from a round of interviews with police forensics specialists in order to compare theoretical results with real experience. The potential final scope of the portless device problem is then demonstrated through an overview of a selection of fully portless devices and the methods of extracting data from them. This kind of approach will provide forensics teams with a good overview of the existing possible methods in order to expedite the data recovery process while also offering insight into the severity of portless devices. Because the efficiency of the recovery process is key to crime investigations, this paper's contribution will allow insight into the optimizations to be researched within the process and hence improve the productivity of such teams in the future.

Keywords:
Internet of things, forensics, portless devices, data extraction

Juhtmeteta seadmete kriminalistika tulevikus

Lühikokkuvõte:
Seadmete kriminalistika on olnud võtmetähtsusega protsess kuritegude uurimises alates arvutisüsteemide peavoolu sattumisest 80ndatel ja on sellest ajast saati ainult kasvanud. Algusest peale on seda andmeekstraheerimisprotsessi võimaldanud seadmetel olev sisend-väljundport. Selle protsessiga seotud tarkvara ja protseduurid on üle aastate muutnud aga põhiprintsiip on jäänud samaks. Nüüd toob asjade internet koos traadita tehnoologiate arendusega juhtmeteta seadmete ohu. Sellel on potentsiaal areneda digitaalkriminalistika väljas tõsiseks probleemiks ja pidurdada kuriteouurimisi, mis juba praegugi nõuavad kiirust igas protsessi sammus. See uurimistöö teeb süstemaatilise kirjandusarvustuse, et leida hetkel võimalikke alternatiive ja strateegiaid juhtmeteta seadmetest info eraldamiseks ja nende seadmete populaarsusest arusaamiseks. Selle järel võrreldakse saadud tulemusi politseispetsialistidelt saadud vastustega et leida kui palju on teeorial praktikaga kattumist. Potentsiaalne lõplik probleemi ulatuslikus on demonstreeritud ülevaatega erinevatest juhtmeteta seadmetest ja nendest info eraldamise võimalustest. Selline meetod annab kriminalistidele hea ülevaate hetkel olevatest võimalikest meetoditest andmete kiiremaks eraldamiseks. Samal ajal pakub uurimistöö ka arusaama juhtmeteta seadmete tõsidusest. Kuna andmete saamise kiirus on võtmetähtsusega kuriteouurimistes annab see uurimus pilgu erinevatesse optimiseeringutesse mida saab tulevikus uurida ja mille kaudu on võimalik tiimide produktiivsust suurendada.

Võtmesõnad:
Asjade internet, kriminalistika, juhtmeteta seadmed, andmete ekstraheerimine

Glossary

5G 5th Generation (Mobile Network). 1

APDU Application Protocol Data Unit. 1

CFTT Computer Forensics Tool Testing. 1

DoS Denial of Service. 1

ECG Electrocardiogram. 1

eSE Embedded Secure Element. 1

GDPR General Data Protection Regulation. 1

GPS Global Positioning System. 1

HDD Hard Disk Drive. 1

I/O Input/Output. 1

ISO International Standard Organization. 1

JTAG Joint Test Action Group. 1

LEO Low Earth Orbit. 1

LISL Laser Inter-Satellite Link. 1

LPWAN Low-Power Wide-Area Network. 1

NFC Near Field Communication. 1

NIST National Institute of Standards and Technology. 1

NR New Radio. 1

PC Personal Computer. 1

RAM Random Access Memory. 1

RQ Research Question. 1

SD Secure Digital (Card). 1

SDN Software Defined Network. 1

SG Smart Grid. 1

SLR Systematic Literature Review. 1

SSD Solid State Drive. 1

USB Universal Serial Bus. 1

Wi-Fi Wireless Fidelity. 1

WPC Wireless Power Consortium. 1

Contents

List of Figures

List of Tables

1 Introduction

Portless devices are an all-encompassing term covering any form of device that does not come with an input/output (I/O) port. Such devices transmit data solely wirelessly and do not utilize a port capable of data transfer, though for the purposes of this paper these devices may still have a solely power-transmitting port. The most common form of such devices can be seen in IoT devices that communicate solely over a wireless network - most commonly the Wi-Fi of the home they are installed in. The popularity of these is ever-increasing as more than 70% of Americans in 2019 were reported to have at least one network-connected device, with the amount of devices connected globally having predicted to nearly be doubled from 2019 as of 2024. [KSC+19, Sin23] IoT devices commonly used in households can range from smart televisions, often having a data transfer port or several, all the way to security cameras which may operate solely on a power cable and wireless network. [AZZ+17]

Aside from the much larger and wider IoT scene, a pioneer in pushing for portless devices that are potentially more mobile than the stationary, home-attached IoT devices has been Apple. These already exist in the form of the more recent Apple Watches (7 and above) that feature magnetic charging through the MagSafe technology. However, the technology is being held back by numerous accusations and concerns of interference with cardiac implantable electromagnetic devices. [NNGTTW21] On the mobile phone front, Apple has been showing a public interest in migrating its phones to being solely portless for the past few years. [GB20] Regardless, hopes of that have also been slowed by a new EU regulation mandating the inclusion of USB-C chargers in every such mobile device by fall 2024. [Par22]

The various sources of forensics (Extraction of data from the device itself and analysis of it) data acquisition can be categorized loosely into data straight from the device's local hardware, network data in transit over various local or wider networks (generally through logs of such), and cloud data at rest at its final location. [KR16] The lack of an input port presents a challenge particularly in acquiring the first form of data.

1.1 Task

The main research question of the paper is "How will portless devices affect forensics in the future?" Remedying the issue of acquiring the physical data present on the device is the main focus of this paper, though regardless of the particular focus, network and cloud data acquisition will also be considered and touched upon. The more specific methodology involved in doing so is mentioned in section 3.

1.2 Structure

The rest of the thesis is divided into five additional sections. Chapter 2 will provide an overview of the fundamental knowledge regarding core concepts handled in the paper, as well as any adjacent research or information that is required to know in order to understand what is to follow. After that, chapter 3 explains the precise methods chosen to carry out this paper and how the results will be validated. Chapter 4.1 presents the findings of the paper by following the research questions set out in the methodology chapter and the practices in the state of the art chapter. Each subsection will present its findings on the relevant research for a specific research question, analyzing the benefits and shortcomings of each in order to develop a full whole which will be used to answer the overarching research question. This is followed by chapter 5 bringing specific examples of portless devices and their data acquisition methods in order to establish a scope of the problem. Chapter 6 goes over the final answer to the main research question, recommends future research related to the field, as well as gives critical overview of the limitations of the work. The entire thesis is concluded and summarized in chapter 7.

1.3 Novelty

The study presents a unique overview of portless devices from a primarily forensic point of view. While some existing studies do go over the currently existing methods for IoT or wireless devices in general, they do not provide insight into neither the more technical aspects of the methods nor the design philosophies that guide them. Looking at portless devices as a whole, including mobile devices and laptops, does not exist in the current research space. None of the existing papers that analyze current methods provide a solid guideline on how to develop a new one based on the weaknesses and strengths of current ones, and as such this paper finds a unique niche in exploring the usefulness of methods against current and future devices as well as in going over in detail the process of developing a utility for data extraction in the field.

2 Background

2.1 Internet of Things

The beginning of an ever-increasingly connected world has brought the need to birth the Internet of Things concept. This refers to the entire concept of common everyday objects such as televisions, cameras, doorbells and such, along with not-so-common objects like industrial components, sensors, and machines all being interconnected through the global Internet. The former capability is also often combined with data analysis capabilities, whether they be local on the particular machine itself or in the cloud. As such, the Internet of Things bridges the definition of what is normally considered a computer as processing power is starting to extend to objects that never had any. It is important to note, however, that while the Internet of Things can and does refer to by name as devices connecting to the Internet, in practice it applies to a device having any communicative capabilities with other devices, even if not necessarily through such a wide network. [REC15, AQPMS15]

It is important to understand that in order for a system to be truly IoT, there should be a multitude of networks communicating with each other in an interoperable manner. [MAEP15] This sort of interoperability is one of the founding pillars of the IoT architecture and is a significant contributing factor to the purpose of this paper as data becomes more dissipated and harder to both track and acquire. This issue is further enhanced by the members of an IoT network often working together in order to utilize the resources of multiple networks [LHZ$^+$16] as efficiently as possible at the same time, making provenance of data incredibly difficult. While IoT architecture can vary heavily, the most basic and common is the three-layer architecture where a distinction is made between the perception layer, the network layer, and then the application layer. [LYZ$^+$17] The architecture can be seen illustrated in figure 1.

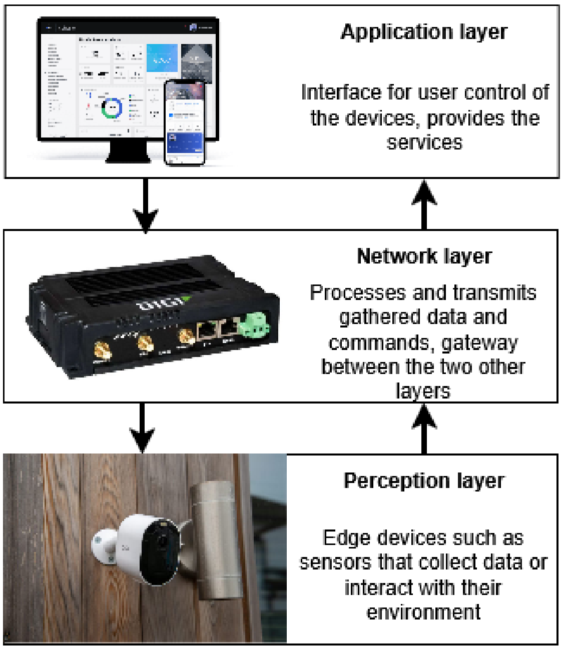

Application layer
Interface for user control of the devices, provides the services
Network layer
Processes and transmits gathered data and commands, gateway between the two other layers
Perception layer
Edge devices such as sensors that collect data or interact with their environment

Figure 1. IoT Three-Layer Architecture [Lud23] [5Gs25] [Coh25]

The emergence of IoT as such has forced the forensics community to adapt to an exponentially bigger range of devices with their own unique quirks - some not having any input ports at all. As such, network and cloud forensics have become more important as extracting data from a device solely by plugging it in gets left more in the past by each passing year. Standard tools and methodologies that worked on normal personal computers (PCs) and mobile devices can not be applied to this vast variety. Furthermore, the devices often spit out enormous amounts of highly unorganized data, often in very specific formats uniquely tailored to the devices' vendors, adding to the complexity of successful analysis. [YHA$^+$19]

Because the technology is developing so rapidly, there is a lack of standardization amongst it. Several new standards are being worked on and have been presented, yet companies are afraid to follow any of them in fears of being locked into one single standard that will likely be obsolete in a few years [VT18]. The current ISO standard for IoT devices is ISO/IEC 30141 [ISOb] which replaces the previous, rudimentary 30141:2018 version. With a six year period from the evolution of the previous version, it is clear that the development is rather slow given the pace of the technology itself. As of right now, industrial sectors are most prevalently adhering to their own visions and needs and primarily tend to not follow any global standards for their respective industries. [ASB20]

2.2 Mobile and digital forensics

Digital forensics is the scientifically (and legally) sound analysis of traces and evidence left by crimes committed through computer systems. [AKPL21] Originally called computer forensics, the field evolved into a more general digital forensics that then branched off into various subsets of such evidence such as computer systems, networks, mobile devices etc. The four main tenets of digital forensics are acquisition, preservation, analysis, and presentation. [DD12].

The first tenet, acquisition, is largely the main focus of this paper. As it is preliminary to anything else, it could be considered the most important. It involves the collection of the electronic data in any shape or form such as seizing a device at a crime scene or accessing cloud data related to an investigation. This is the stage where data is at its most sensitive state and the likeliest to be damaged or lost. [KFF24] The integrity and speed of this step is paramount especially when dealing with IoT systems where a large share of the data might be volatile in nature due to limited storage or high mobility. [CAG18]

The preservation tenet involves storing the data in such a manner that is retains its validity to be used as evidence in a court setting. Provenance and keeping a chain of custody are are the biggest issues along this step, as any issues along the line might result to doubts towards the validty of the evidence. [LCHW14].

Analysis involves looking over the data and gathering actionable evidence from it. For example in the case of a murder this could involve looking over the suspect's chat logs or history to find traces of planning or deliberation - important in order to tell the difference between a homicide and a murder. It is also the main bottleneck in being able to use digital evidence in an effective manner. [Est25] The sheer volume of data that can be gathered from devices is enormous and there are too many investigations that demand police attention to be able to thoroughly go through digital evidence in an in-depth, personal manner. Solutions must be automated to a good degree and intuitive to use for staff. [HD24]

The final presentation step is of least relevance to the paper as it involves the mostly legal aspect of preparing and writing a forensic report as well as defending it in court. A proper methodology must be tracked in order for this step to be successful, and the burden relies largely on stage 2 of the investigation for doing so. All the different tenets of a forensic investigation are outlined in figure 2. Note that the tenets are not the same as the steps outlined in the ISO-IEC 27037/2012 digital evidence processing standard. The grouping is slightly different, though the content is similar. [ISOa]

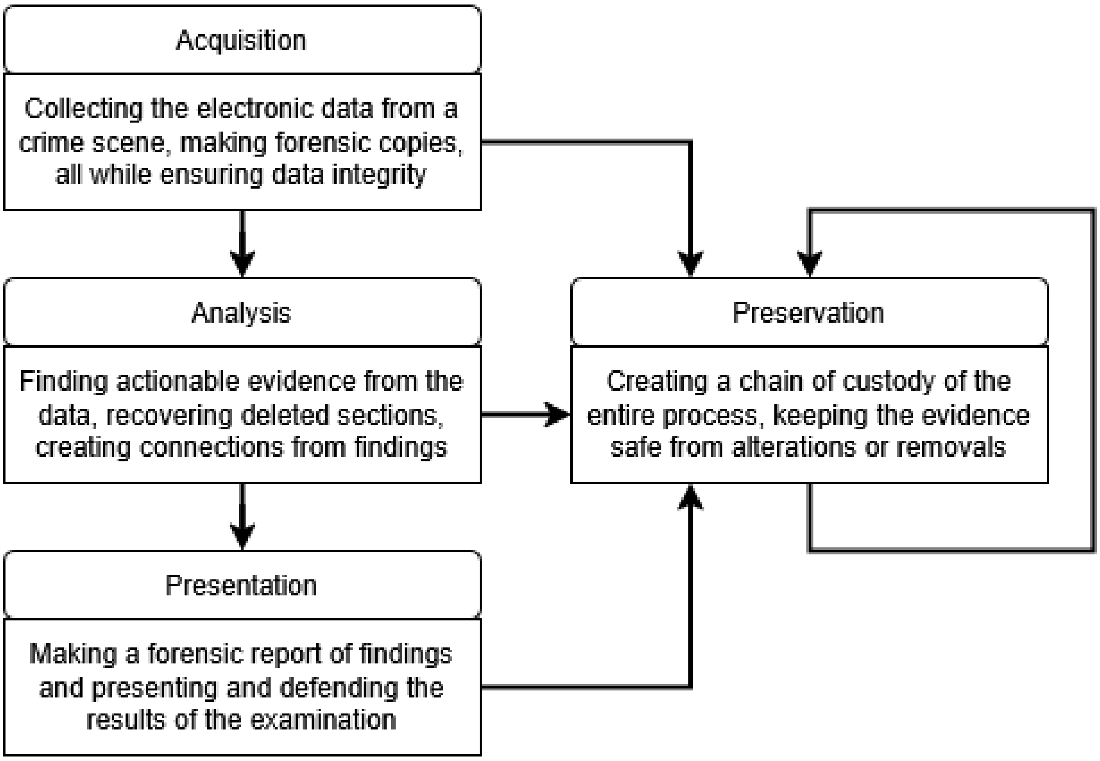

Acquisition
Collecting the electronic data from a crime scene, making forensic copies, all while ensuring data integrity
Analysis
Finding actionable evidence from the data, recovering deleted sections, creating connections from findings
Presentation
Making a forensic report of findings and presenting and defending the results of the examination
Preservation
Creating a chain of custody of the entire process, keeping the evidence safe from alterations or removals

Figure 2. The four tenets of digital forensics

Historically mobile phone forensics has relied in large part on physical access to the phone. A classical forensics process must first and foremost focus on keeping the device from getting contaminated and generating further information, usually placed into a Faraday bag while in Airplane mode, disabling most communications by software and by hardware. The device then gets imaged and said image gets analyzed in a lab, providing a good overview of the files and information inside. In some ways, one might imagine that having a portless device might make the device more secure to analysis, however - more often than not, permission to analyze the device is in one way or another received from the device's owner, therefore bypassing the need to overcome security. This device data is then backed up by network records and other available forensic data. [Hre21, Kum21]

A concerning trend in the market has been the minimization of the amount of ports on a phone, leading to very recent current-day pushes for and against entirely portless phones. The technology for such has been developed by Apple through MagSafe. While the current models do not yet support data transfer, Apple's recent patents suggest that plans to include such capabilities are in the works, which could potentially help break into the concept of portless phones. [Inc24] The pairing of such a device would help act as a potential forensic failsafe, giving the chance to extract data even when a device might not boot up anymore. Even then, portless mobile devices such as the newer Apple Watches have appeared on the market along with fully portless phones from currently less known companies, prompting an investigation into new forensic tools and methods for analyzing the data. The concerns extend also to other mobile devices such as smart watches and other wearables, tablets, sensors and the like as they are becoming more prevalent in investigations. Being able to easily interface with such devices could significantly improve police operations. [JSE24]

2.3 Related work

This literature review will focus on analyzing existing methods, both older and newer, while the full paper will potentially also include a self-developed method to provide insight into the process of developing a tool and filling gaps in the current ones. Some relevant, albeit more general papers are outlined below.

Brunty J. [Bru23] dives deep into methodologies for validating methods used in digital forensics. The study provides a critical analysis of the various standards available that relate to digital forensic procedures and then creates a concise plan for developing a forensically-sound methodology that would be accepted in the scientific community.

Rani et al., [RG20] gives an overview of the forensic characteristics of IoT devices and general process steps and guidelines for performing an examination. It also highlights the need for security in said devices through different example groupings such as the smart transportation or personal life categories.

Waseem et al., [WAN+21] gives an overview of the fundamentals of performing forensics in software-defined networks (SDN). Although the thought process used is useful, the paper lacks technical depth and covers an architecture not yet widely used and still in its infancy stages.

While these papers support the making of this one, they do not provide any specific forensic methods to follow in terms of technical procedures. These merely provide a framework and additional insight into the context surrounding the topic, as well as a methodological framework. Papers covering such will be analyzed further on in this systematic literature review (SLR).

3 Methodology

The study utilizes a systematic literature review in order to understand the gaps that exist in existing implementations as well as take away from their strengths while avoiding weaknesses discovered, then supporting the information found with answers from police interviews as well as specific device examples to establish potential scope. The focus is on the usefulness of the information in future law enforcement to perform forensics in the field and all research will be went over through that lens. The emphasis is placed on the practicality of solutions and information instead of solely a general analysis, as well as determining the scale of the threat that such devices pose to the forensic access and acquisition of the data present on devices for investigations.

3.1 Systematic Literature Review

A literature review is conducted in order to cover the earlier established research question and the derived sub-questions. The aim is to confirm or disprove the assumptions made in the hypothesis and to draw out any information relevant to the construction of a prototype, both in the context of this paper as well as any other interested parties.

In order to optimize the process of the SLR a review protocol was created. Doing so helps overcome the inherent biases of researchers and streamline the selection. [BSCMSJ21] A wide variety of search engines and databases are used in order to avoid publisher bias as well as get methods outside of solely the research community, particularly given the practical nature of the issue. The most widely-used terms for the searches were (("IoT" OR "digital" OR "mobile" OR "wireless") AND ("security" OR "forensics" OR "data extraction")), as well as ("IoT" AND ("popularity" OR "trends" OR "future")). The specific exclusion criteria then used are listed in Table 2. These searches will mainly be conducted in ScienceDirect, Google Scholar, ResearchGate, Science.gov, IEEE, Researchgate, and Springer. Sources related to RQ1 are mostly pulled from Google, Youtube, and other less academic mediums as trendsetting is in majority in the control of companies looking forwards and social media talking about it [IS20].

The findings from these results are compared to data gathered from interviewing police specialists in Estonia to see how the hypothesis gathered from theory compares to reality. The interviews include four police forensics specialists working at high level positions that are capable of answering on behalf of many and having a large amount of experience in the field.

After that examples of specific portless devices are given in order to demonstrate the scope of the problems caused by such devices with an overview of how the data present on them could physically be accessed.

[RQ1] How likely are portless devices to exist in the future?

This research question puts an emphasis on the necessity for this paper. With such a novel field, it is important to know how many resources from law enforcement are worth to put into pursuing the topic. The RQ1 covers

- i) How prevalent are portless devices in the present?
- ii) What kind of portless devices and technologies are seeing development?
- iii) What obstructs the adoption of portless devices?
- iv) Is there anything enabling or driving the adoption of portless devices?
- v) What are the timelines within which portless devices might become available?

[RQ2] What indirect extraction methods can be used to access data relating to a portless device?
While direct access to the device might prove difficult to achieve, the ever-growing connectivity of the world provides several alternatives that might help provide data assisting in an investigation without ever gaining any data that resides on the device itself. The objective of this RQ is to identify these methods and compare their use cases and practicality.

[RQ3] What extraction methods could be used to access data physically present on a portless device?
RQ3 focuses on the ultimate practical goal of this paper - extraction of data from the device itself. This RQ will help gain an insight into how it might already be done in the present, as well as a foundation to any researchers seeking to create solutions to the issues.

In order to optimize the process of the SLR a review protocol was created. Doing so helps overcome the inherent biases of researchers and streamline the selection. [BSCMSJ21] A wide variety of search engines and databases are used in order to avoid publisher bias as well as get methods outside of solely the research community, particularly given the practical nature of the issue. The terms used for the the searches were (("IoT" OR "digital" OR "mobile" OR "wireless") AND ("security" OR "forensics" OR "data extraction")), as well as ("IoT" AND ("popularity" OR "trends" OR "future")). The specific exclusion criteria then used are listed in Table 2. These searches were conducted in ScienceDirect, Science.gov, IEEE, Researchgate, and Springer. Sources related to RQ1 were mostly pulled from Google, Youtube, and other less academic mediums as trendsetting is in majority in the control of companies looking forwards. The search criteria can be seen summarized in table 1. The database selection was mainly guided by the size of the databases themselves as well as the quality and appropriateness [KPBB$^+$09] of the studies contained in the databases.

Databases used	ScienceDirect ResearchGate Science.gov IEEE Springer
Searched literature types	Journals and conference papers
Search strings	(("IoT" OR "digital" OR "mobile" OR "wireless") AND ("security" OR "forensics" OR "data extraction")) ("IoT" AND ("popularity" OR "trends" OR "future"))
Study languages	English
Publication period	January 2018 to May 2025

Table 1. Academic literature search strategy

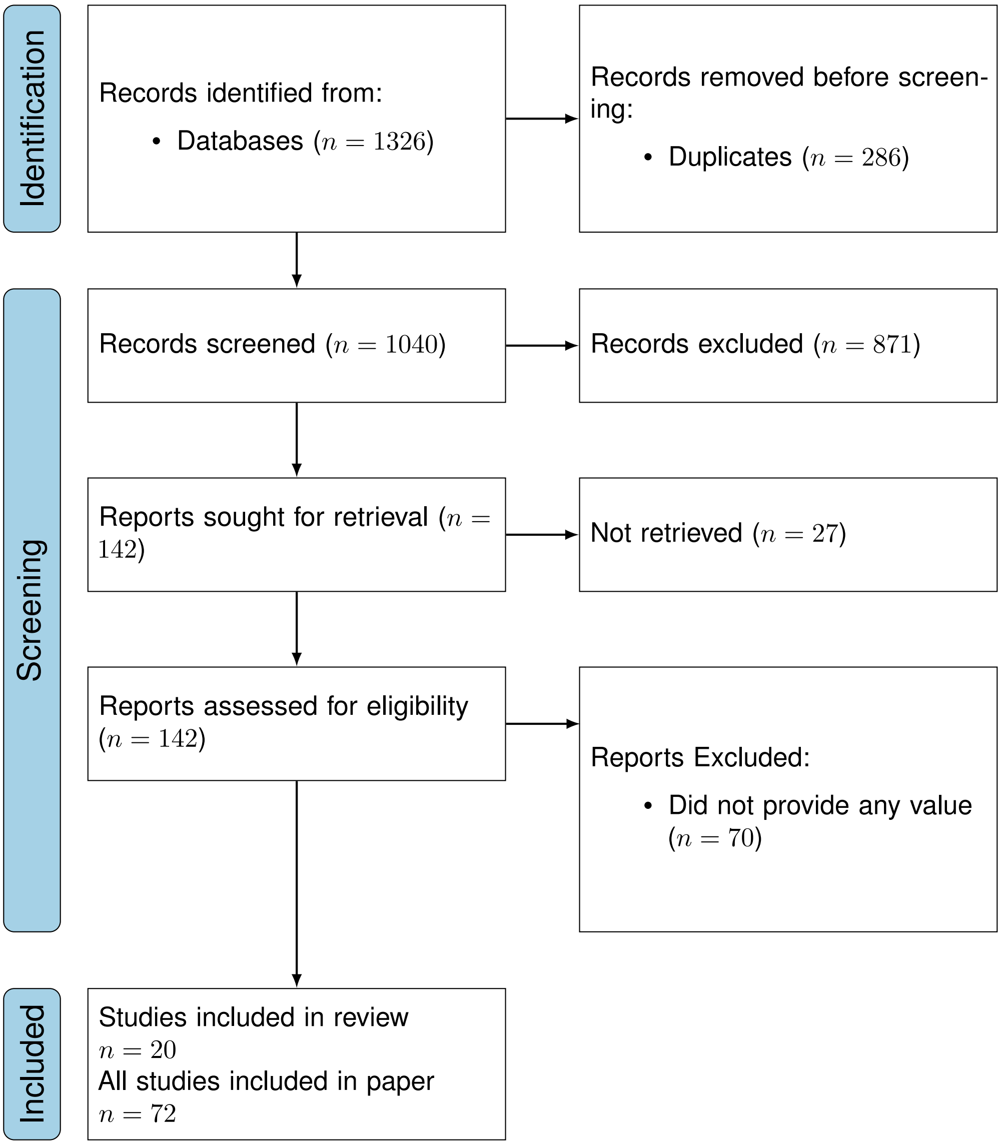
3.2 Scope and Goal

The scope of this study includes the research questions defined earlier along with the development of a prototype version of a device to fulfill a gap identified by answering the research questions. The research questions are intended solely to provide guidance and identify the gaps and future trends of the subject matter in an effort to guide other research in the field, as well as to support the prototype. The prototype is developed to provide insight into the development process of solving these shortcomings, not to be a final solution to every problem identified. The paper will prove or disprove the assumptions made in the hypothesis and concentrate the available research that exists on the topics, providing a critical overview of the strengths and weaknesses of the papers and establishing future directions to look into based on the results.

Inclusion criteria	**Exclusion criteria**
Papers about digital forensics methods	Papers older than 2015
Papers relating to IoT trends	Papers not in English
Papers about network foreniscs	Research papers with less than 5 sources

Table 2. Inclusion and exclusion criteria

All rounds of filtering were done manually without the assistance of scripts. Papers that did not fit the purposes of the research questions were filtered out immediately. Papers that supported the collection of data and information for the purposes of background and general knowledge were put to the side and later used in the making of this paper. Zotero was used to manage references and keep track of all the papers that were sifted through. Figure 3 shows an overview of the process and study count.



Identification
Records identified from:
• Databases ($n = 1326$)
Records removed before screening:
• Duplicates ($n = 286$)
Screening
Records screened ($n = 1040$)
Records excluded ($n = 871$)
Reports sought for retrieval ($n = 142$)
Not retrieved ($n = 27$)
Reports assessed for eligibility ($n = 142$)
Reports Excluded:
• Did not provide any value ($n = 70$)
Included
Studies included in review $n = 20$
All studies included in paper $n = 72$

Figure 3. PRISMA model of literature selection

4 Analysis

Section 4.1 goes over the final results of performing the SLR and outlines the included papers in Tables 3, 4, 5, and 6 along with their purpose in the final paper and their shortcomings. The subset of papers is then analyzed more thoroughly and their findings used to support answering the research questions. Chapter 4.2 brings up the main findings from police interviews and contrasts them to available research, and chapters 4.3, 4.4, 4.5 go over the main findings of the SLR with regard to the research questions.

4.1 Systematic Literature Review

This section of the paper outlines the papers included to be analyzed for the systematic literature review and then an analysis of their shortcomings, usefulness, study designs, and findings.

Source	Study design	Area	Purpose	Main findings	Shortcomings
Sikos, Leslie F. [Sik20]	Review	RQ2	Viability and methods of packet analysis	Packet data could potentially be spoofed, though if not spoofed then they can contribute a wealth of evidence directly and indirectly	Shallow specifics, giving the briefest overview of a myriad of solutions
Dykstra J., Sherman A. [DS13]	Prototype, laboratory study	RQ2	Creating digital forensic tools for the cloud	Developed a set of tools to obtain forensic data from the cloud while bypassing the usual wait and long process in acquiring them	Stack-specific, needs to be already existing in infrastructure. Never developed past the initial publication.
Yacooub et al. [YNSC22]	Literature review	RQ2-3	Anti-forensics techniques and solutions	Anti-forensic activities have been steadily rising over the last years, current specialists are not sufficiently equipped to deal with these techniques	Wide, not technically deep in the context of solutions. Large amount of solutions boil down to "more funding and/or time"
Abiodun, Oludare Isaac, et al. [IAEA22]	Literature review	RQ2-3	Highlight and solve cloud data provenance issues	Hard to provide provenance while ensuring appropriate confidentiality and privacy, interoperability of devices yet lack of interoperability in manufacturers complicates chaining data	Does not solve any of the novel issues, particularly in the realm of privacy
NIST [NIS21]	Laboratory study	RQ3	Direct hardware data extraction	Most social media data was either only partially captured or not at all, though most other deleted data was recovered as expected	Lack of methodological details, the process is potentially capable of damaging the source, too time-intensive for real investigations

Table 3. Included studies I

Source	**Study design**	**Area**	**Purpose**	**Main findings**	**Shortcomings**
Aji et al., [AHR20]	Laboratory study	RQ3	APK for Android data extraction	Successful rapid data extraction using two open-source tools, though both are found to be lacking in one respect the other has	Technically shallow, requires source editing, and does not work in full without rooting
Zohourian et al. [ZDN$^+$23]	Literature review	RQ3	Zigbee network security assessment	The widely-used Zigbee protocol has significant key management weaknesses and manufacturers often minimize security investment	Wide, the forensic data acquired might be of limited use due to involved device storage sizes being minimal
Lin, James C. [Lin21]	Laboratory study	RQ1	Wireless power transfer future insight	Completely wireless power for electric appliances is a sustainable prospect, though some methods are not safe for humans	Not a cybersecurity focused paper, solely a potentially enabling technology. Study not thorough enough on human safety
Zhang H. [Zha24]	Laboratory study	RQ2	Wireless sensor network forensics	Automated forensic systems are far better at detecting DOS or probing attacks than anything more complicated such as user-to-root attacks	Relies very heavily on training data and as such will always lag behind, 80-90% accuracy is low
Mahmood H. et al [MAA$^+$24]	Literature Review	RQ2	Analysis of IoT forensics research	Traditional data collection is ineffective on IoT devices, no framework caters to every aspect of IoT forensics	No practical use, overview of already popular techniques

Table 4. Included studies II

Source	**Study design**	**Area**	**Purpose**	**Main findings**	**Shortcomings**
Chettri and Bera [CB20]	Review	RQ1	Provide overview of the technologies that enable IoT in 5G as well as the challenges making it more difficult to implement	The devices involved generate enormous amounts of data, present a far wider attack surface, and bring faster software elasticity	Quantitive assumptions with invalid citation support, somewhat outdated for current era
Gupta et al. [GNSV22]	Review and framework	RQ3	Designing a better framework for learning digital forensics	Digital forensics education is too theoretical, lacks a pedagogical model, and is severely unsupported among organizations	The practical material provided as an output to the research is ephemeral due to the nature of the field
Chi et al. [CAG18]	Review and framework	RQ2	Creating a framework to provide a timeline of forensically significant events	Lifespan of data in an IoT system is far shorter than traditionally, application created to provide a timeline using artifacts from the network	Outdated sources used to state present claims, lack of insight into the operation of the application
Sharma and Awasthi [SA24]	Laboratory study	RQ3	Assess the security of a field of IoT devices and showcase a process to extract data from them	Created a lightweight forensic investigation model, showcased extracting Wi-i passwords, activity logs, phone models etc from smart bulbs	Very time-intensive method involving manually connecting pins from extracted Wi-Fi module and finding device-specific logs
Zhang et al. [ZUBC20]	Laboratory study	RQ2-3	Explore threat actor process	In the case of the Mirai botnet, the CNC or MySQL servers contain logins for other servers which lead to finding the list of active bots as well as a history of the attacks	Does not take into account any evolutions or potential modifications to the original attack

Table 5. Included studies III

Source	Study design	Area	Purpose	Main findings	Shortcomings
Cuomo R. et al. [CDI22]	Laboratory study	RQ3	Mobile forensics technical assessments overview	Full access to memory is prohibitively difficult, extraction with the analyzed method is repeatable despite hash changes	Processes used involve rooting the phone and only apply to Android
Alendal et al. [AAD21]	Laboratory study	RQ3	Breaking the embedded secure chip	Provides an approach to discover an exploitable vulnerability leverage it to bypass embedded security	Approach could be adapted but is too careless and slow for investigations
Shayea et al. [SESE^{+}24]	Literature review	RQ1	5G and IoT integration with LEO networks	Unclear if LEO satellites can satisfy 5G requirements properly, large push towards launching LEO constellations with 5G	No security implications of the integration explored
Qays et al. [QAAS^{+}23]	Literature review	RQ1	Exploring IoT-assisted smart grids	Data inconsistency in IoT raises complexity, lack of prototypes and accessible field data for research	Solutions are discussed with little to no regard to their security
Gopinath et al. [GKSSJ23]	Laboratory study	RQ3	Investigate shortcomings of IoT forensics	Provides an experiment on data retrieval and image creation times along with a short overview of the process	Experiment does not adhere to any specifics of IoT systems

Table 6. Included studies IV

Sikos, Leslie F. "Packet analysis for network forensics: A comprehensive survey." [Sik20]
This article provides an understanding of the operation of tools designed for packet analysis down to a technical level and helps understand the data provided by such. It goes over both software and hardware opportunities for performing packet sniffing as well as their operating principles and use cases. The article gives an extensive overview of the choices available to a forensics specialist, but does not dive deep into any particular one, and as such may be somewhat shallow. Regardless, it provides good starting points based on the exact operation and circumstances of the device in question.

Dykstra J., Sherman A. "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform" [DS13]
The paper goes into detail on the creation and operating principles of a forensic tool suite called FROST. It expands on an earlier paper done by the same people that established necessity for such a tool that would gather data from the management plane. The concept shows promise as a way to bypass the otherwise lengthy acquisition processes for cloud data for investigators and law enforcement. Having a general concept on how such a tool was developed helps bring insight into the processes behind such an endeavor and the community's expectations from a forensic tool. Data would be easily accessible to users of the cloud and, as such, with permission from the victim/suspect, cloud data extraction could be significantly easier. The suite is held back by the necessity to have it incorporated into the cloud provider, as well as only working on the OpenStack infrastructure. As of 2025, FROST has not seen any updates since the original publication of the related paper and is not available anywhere online. The project was included in the systematic literature review as an example due to its unique role in bridging the gap with cloud data acquisition, as well as an example of prototypes in the field that never get developed despite their necessity.

Yacooub et al., "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations" [YNSC22]
[YNSC22] is unique in the inclusion of anti-digital forensics systems, especially adopted to the IoT framework which can often hold portless devices. It is an exceptionally long paper providing a comprehensive overview of the different types of IoT devices, associated forensics, their challenges, and anti-forensic tools. However, despite its size it suffers from the general drawback of wider papers in that no particular system is discussed to a technical depth. Instead it is a cornucopia of techniques used by both law enforcement and those attempting to evade detection. It essentially provides a wiki of jumping points for more detailed analysis and gives reminders of concepts to keep in mind when developing one's own tools, its final contribution being a list of suggestions for forensics teams. Even so, the final suggestions of the paper are very general and

not of much practical use - its main practicality instead lying in the plethora of general, sourced information that can be used as a jumping point into a deeper dive of whatever technique is needed to be used.

Abiodun, Oludare Isaac, et al."Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey [IAEA22]
This survey goes over the challenges of establishing data provenance in a cloud context - a concept very important for a forensic analyst as provenance refers to the origins of data, helping track down who a particular piece of evidence might be coming from or where it came from. Aside from establishing the requirements for keeping good provenance and the tools and suggestions to do so, the paper also highlights ways to make sense of provenance data or collect it on one's own. However, most of these techniques require tampering with the device(s) in question and, as such, are much less attractive for the purposes of a forensic investigation due to the contamination of source material. As such, the ultimate conclusion is that forensics analysts are still at the mercy of the service providers themselves and their organization of data, but should push for better standards to be followed according to the requirements set out in the paper.

NIST, "Test Results for Binary Image JTAG, Chip-Off Decoding and Analysis Tool [NIS21]
While not exactly a research paper on its own, this group of NIST's Computer Forensics Tool Testing (CFTT) project reports provides good experimental results for the extraction of data on a damaged mobile device using an assortment of different tools. While the methodology is not precisely described in any of the results, the results themselves offer a good overview of the basic environment used as well as the specific technique. The main allure of this lies in the successful results outlined in these reports, providing reason for further analysis into the extraction methods used in the case of a portless or damaged device. The sensitive, specific technique used for extraction, however, is very time consuming and damaging to the source device and as such may prove ineffective for day-to-day forensics aside from the most extreme cases.

Aji et al., "Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software [AHR20]
The paper introduces the working concepts of an apk file that can be ran on the target device in order to extract selected types of data from it into an SD card. This approach comes with a big downside of requiring an SD card. Due to the program itself being open source, it could potentially be modified to not require an SD card or even transmit its data to another device either through a local connection or the Internet after creating it. The downside of this paper is the lack of detail in the actual process of extraction, only comparing it with one other extraction method and never going into depth on how

the program itself functions deep down. As such, modifications to it relying solely on this paper may prove difficult.

Zohourian et al., "IoT Zigbee device security: A comprehensive review" [ZDN$^+$23]
This review serves to provide a solid foundational knowledge of the Zigbee system commonly used in IoT devices, especially with regards to its security. As such, the paper indirectly provides approaches on how a forensic expert could extract data from such devices. This is significant due to the prevalence of this technology in small IoT devices which very commonly do not have any input ports for diagnostics nor do they use common wireless protocols such as Bluetooth or Wi-Fi. In terms of criminalistics, the technology is popular in motion sensors or home alarms, providing very tangible benefit to a criminal case. However, the size of associated devices means that often times local storage might be too lacking and as such, the majority of attack vectors focus on disabling the device in one form or another or using it as an entry point, limiting its usefulness in forensics, which target the past.

Lin, James C., "Safety of Wireless Power Transfer" [Lin21]
While [Lin21] is not a cybersecurity specific paper, it provides good insight into the future of wireless charging - and as such, wireless devices as a whole. Aside from setting up the operating principles of wireless charging, the paper establishes a bright future for the technology and shows its potential. Special highlight is given to the capability of fully wireless power supply between various types of devices ranging from phones to electric appliances, with the capability of real-time data transfer and even calls with little to no risk to personal health. As such, the paper significantly supports migration to portless devices, even without a power port.

Zhang H., "Simulation of network forensics model based on wireless sensor networks and inference technology" [Zha24]
In this paper an alternative method of analyzing for suspicious network traffic in a setup of wireless sensors is proposed. [Zha24] outlines a network intrusion forensic system based on a fuzzy logic-based decision tree data mining system. The experiments conducted in the paper show a high degree of precision and true positive rates for most common attack types such as DoS. However, not specifically brought out in the paper are its weaknesses, most notably the reliance on training data. As such, its performance drops significantly when it comes to noticing and identifying more sophisticated attacks that training data might be lacking on or diverge heavily for, such as spy attacks and other remote-to-local attacks which try to send packets from outside the network without authorization.

Mahmood H. et al, "Comparative study of IoT forensic frameworks" [MAA$^+$24]
The comparative study done by Mahmood H. et al goes over a wide range of literature surrounding IoT forensics, but fails to deliver a focus on any specific area. The study finds that the past and current research on the topic is trying to find a general solution to forensics in the area despite lacking even a specialized solution. It highlights the need for a standardized framework for data extraction from even a similar set of devices, let alone a wider group, as most data extraction in the field is still done physically or otherwise manually depending on the device. The paper focuses on naming different tools and the like used without giving any overview into the actual process of data extraction, and therefore also missing out on providing insight into more efficient methods by principle.

Chettri and Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems" [CB20]
The review carried out by Chettri L. and Bera R. establishes a solid overview of both the recently developing as well as established technologies that enable IoT in 5G. It goes into detail about the operations of 5G New Radio (5G NR), multiple input and multiple output (MIMO), cloud computing, as well as mm-wave communication. The operation of LPWAN networks and types of alternatives are highlighted, yet their significance is not highlighted to a low degree, making it unclear which technologies are spearheading the competition or have the most relevance in their respective subareas such as low-range vs high-range communications. The paper also states claims such as an 80-billion device milestone by 2030 with the sources referenced not backing up the claim or being too old to support it.

Gupta et al., "Digital Forensics Lab Design: A framework" [GNSV22]
The purpose of Gupta and his co-researcher's paper is to provide a framework for the teaching of digital forensics. It highlights the obstacles faced such as the cost of related soft- and hardware and the effort required to set up effective laboratory teaching environments, coupled with the contemporary nature of the field making the high amounts of work required quickly expiring. The paper sets out an outline program for educating students using open-source software starting with acquiring forensically sound images and ending with writing reports. However, despite outlining the problems faced in the field - it does not do much to solve them in a more permanent matter. The curriculum outlined in the paper could perhaps be of use for some time until it expires, but the fundamental contribution is minimal save for the potential shift in headspace encouraging collaboration between researchers and educators in sharing materials.

Chi et al., "A Framework for IoT Data Acquisition and Forensics Analysis" [CAG18]

The framework created by Chi H., Aderibigbe T., and Granville B.C. attempts to establish a more universal data collection framework that is compatible with a variety of IoT devices. The paper mentions a desktop and a mobile application for extracting artifacts from the network, device, and cloud sources. Two scenarios are outlined for the purposes of testing the framework, though the methodology on how this is done is entirely unclear. The body of the paper focuses on describing the attacks occuring within the scenarios but makes no mention of how their application extracts artifacts or acquired forensic data from the incidents save for a brief mention of the application merely being able to do so. As such, the value generated by the paper is low and can only be used to gather small amounts of insights into the prerequisites or considerations for making a framework - such as the locations of data, formats, or their lifespan.

Sharma and Awasthi, "Unveiling the hidden dangers: Security risks and forensic analysis of smart bulbs" [SA24]
Sharma and Awasthi's laboratory study explores the potential threats and evidence provided by discarded smart devices. The analysis looks at seven different smart light bulbs and attempts to reverse engineer them as well as gather remnant data present on the bulbs. While the point of the paper is to demonstrate the risk of discarding the devices, the results and especially process in the way of thinking could be adapted to field use with devices still present and connected. It reveals how the devices store plaintext wifi passwords, activity logs, creation times, phone connections etc. While the exact results are not very useful in day-to-day use due to the time complexity of extracting the data, involving the manual connection of pins as well as removing the Wi-Fi module - it could potentially be of use in a high profile case when all other evidence is insufficient. The modules analyzed in the paper are also somewhat common, and thus could be of use in both present and future IoT devices other than the analyzed smart bulbs.

Zhang et al., "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers" [ZUBC20]
The paper by Zhang et al. creates a reconstruction of the Mirai botnet attacks that devastated a majority of the internet in 2016 [Mal] and replicates its architecture. It finds that the botnet server itself can be used to find the IP addresses and credentials of infected devices and outlines the exact methods of finding them from the server's memory, as well as the network by tracking the packets and payloads contained therein. However, the analysis of the botnet is only done in its entirely unedited form and therefore its direct outputs have limited value as alterations were not even considered. Nevertheless the techniques used in acquiring the data could be replicated and the research provides a roadmap that assists in navigating the environment. This can also be used for analyzinng other similar attacks.

Cuomo R. et al., "Mobile Forensics: Repeatable and Non-Repeatable Technical Assessments " [CDI22]
Cuomo et al.'s laboratory study analyses the effects of different methods of acquisition as well as the steps taken during them to analyze the repeatability of extracting the data. As an example, a restart of the device caused around 0.9% of files to generate a different hash code. Analyzing the files it was found that a majority of the difference is a result of the extraction software itself and the files on the mobile phone have not changed in reality. The biggest culprit in doing this are the timestamps tied to the files themselves or the generation of more forensically readable chat logs from application data, as well as extracting information from binary files. It was found that the actual forensic content of the files did not change through a restart (in Airplane mode).

Alendal et al., "Chip chop — smashing the mobile phone secure chip for fun and digital forensics" [AAD21]
This paper attempts to break the embedded secure element (eSE) on a Samsung mobile device. It manages to accomplish it in a remote manner, being forensically significant as it does not require physical access to the device and the techniques can therefore be applied even to portless devices. The significance is even further as it worked against a powered off device without user credential knowledge. The paper analyzed the behaviour of the eSE in response to various attacks using two oracles, most notably through the application protocol data unit (APDU) handlers. Doing so a stack buffer overflow was found and from there the RAM memory could be read to find a gadget to read the entirety of the eSE flash and RAM. The vulnerability has been patched since, and the method used by the researchers in finding the vulnerability is very destructive. As such, it would not be suitable for a forensic analysis of a device directly, however the process can be replicated on an identical device to find vulnerabilities to apply to the collected evidence device in a safe manner. The process is very time-consuming though and is likely left more to the fields of hobbyists or researchers as police would not have the resources to perform such experimentation.

Shayea et al., "Integration of 5G, 6G and IoT with Low Earth Orbit (LEO) networks: Opportunity, challenges and future trends" [SESE$^+$24]
The literature review performed by Shayea et al. concentrates on the current state of the most recent and rapidly emerging Low Earth Orbit (LEO) section of space with regards to 5/6G and IoT. It finds that the current frameworks for 5G are not well enough adapted for a LEO environment as the latency alone falls out of the standard. The distances involved make the doppler shift problem already present in 5G far worse and have the potential to harm the integrity of data if it is not manipulated carefully enough. The innovation discussed in the paper is Laser Inter-Satellite Link (LISL) technology which uses laser beams instead of more traditional wireless communication. The widespread

adoption of this technology could offer far reduced latency and much higher data rates, though line of sight issues could completely cut off data flow if not worked around.

Qays et al., "Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review" [QAAS^{+}23]
This research focuses on reviewing the cutting-edge of design, protocols, and technology that assist and enable Smart Grids (SG). Among its most relevant findings are a lack of proper authentication between the smart devices involved in the systems. Due to the SG system potentially being the cornerstone of power transfer, accessing device logs and getting authoritative control when it should not be provided has the potential to tamper with evidence acquired by the police as it could be falsified within the SG system itself. Since the data transfer in such a system is two-way, much more care should be put into securing the data flow especially when device power logs could, for example, back up alibis of suspects.

Gopinath et al., "Explainable IoT Forensics: Investigation on Digital Evidence" [GKSSJ23]

The experiment done by Gopinath et al. attempts to achieve an understanding of retrieving data from an SSD with lost information. Two common forensic tools are used to achieve this - Autopsy and FTK Imager. Data was intentionally lost and attempted to be retrieved. The tools succeeded in recovering data from a USB drive, an HDD, and an SSD. However, the methodology of the experiment is not clear enough on what exact devices were used, or what the content of the data was. It does not show any comparisons or outliers in the extraction process either and, despite specifically outlining IoT forensics, none of the extracted devices have anything to do with the smaller IoT devices outlined at the beginning of the paper. As such, its main value stems from the literature review that can be used to aggregate similar sources and data for the purposes of this paper.

4.2 Police interview insights

Collecting digital evidence happens in almost every criminal case
The interviewed specialists unanimously agreed that digital evidence is collected in almost every single case, often several times throughout the different stages of an investigation. The situation is supported by a United States survey done in 2022 with data going back as far as to 2020 [Mil22], though contrasted by an English survey done in 2023 which claims that on average evidence from a mobile phone was used only in approximately 50% of cases by the prosecution and 31% of cases by the defence.

Other digital evidence types were used even less, though the report makes no mention of how often digital evidence of any form in general was used during a trial [WKHGR23].

The research can be considered an outlier in the general space of digital forensics, as even in 2018 the European Commission found that 85% of all criminal investigations have digital evidence of any type be used in a manner relevant to the case. [Uni18]

The most prevalent evidence collected are mobile phones, computers, cloud data, data carriers (e.g. USB sticks), and camera recordings

The above devices were mentioned in every interview, generally in that exact order. While the question had some bias in the form of naming a few example device types, they were not in this order. These exact answers also match the responses set out in the Uniform Principles and Guidelines for Investigations in 2021 [oII], though the questioned police specialists also had some stray answers including drones, servers, and recorders. All of the mentioned data sources can also be seen to be common evidence according to the International Association of Chiefs of Police. [oCoP]. A study done by Hargreaves et al. found a similar ordering of digital evidence sources with smartphones encountered in 86.9% of cases. The prevalence of other sources dropped significantly, going down to roughly 20% for wearables and less than 10% for smart home devices. [HBD^{+}24]

Data acquisition is mostly hindered by encryption or damaged devices

The police specialists' answers almost all included a mention of difficulties with encrypted devices, generally in the case of an unknown password. In the case of unencrypted data, the lack of a passcode is generally not a significant issue for law enforcement should there really be a need to access the data. [ASAR^{+}24] In the case of more complex extractions, solutions such as In-System Programming (ISP) or Chip-Off were mentioned, though they carry the caveat of whether the potential evidence is worth the manpower. Another heavily mentioned issue was the data storage device itself being damaged either physically and therefore difficult or impossible to access or in the form of bad sectors in the case of HDDs. One of the interviewed specialists also specifically brought out portless devices as an encountered issue in the sense of not having any data transfer ports.

On the legal side police have little to no help from the law when it comes to acquiring the data. A somewhat recent Supreme Court of Estonia ruling stated that police have to make it clear to a suspect and their relatives that they do not have to provide their PINs. The situation falls under the right of the accused and their relatives to refrain from helping the investigation. However, the possibility of forcefully gaining access to the digital data due to biometric identification such as making the suspect give fingerprints or facial scans was presented. The opportunity however does potentially infringe on the suspect's rights and should currently be solved on a case by case basis. [oE]

While basic data acquisition is quick to teach, becoming an expert in the field takes several years.

The basics of acquiring data in the field are not particularly complicated and can be taught in even a week or less. Despite that, gaining a working knowledge of the different edge cases that an officer can run into during their work takes several years and even then there is never a resting point for the knowledge due to the fast development of digital forensics. Overall the amount of direct education given even in training is very limited and most of what is learned is through co-workers or experience in the field. This problem in digital forensics runs deep and is prevalent in the education system as well, as most educational programs do not offer relevant real-life experience nor prepare students for entering the workforce in the field. [MAOB21] This can be partly attributed to the high complexity and low funding available to digital forensics training, though the lack of publicly accessible data and tools is a significant contributing factor as well. [GNSV22]

Expert specialists with a far higher proficiency are involved in almost every large-scale case

While the definition of large-scale is somewhat fuzzy, it includes nearly every case from the central police department. These specialists are quite regularly external to the police department itself, highlighting the already complex and diverse environment of digital forensics and the need for more specialized training in every department.

Portless devices exist in the field, though occurrences with them are very rare

Every interviewed specialist reported experience with some sort of portless device on the field. The most prevalent ones are security cameras, smart home devices, or various sensors. These situations only arise once a month at best, though there have been cases with non-standard ports such as iWatches or drones that require specialized adapters and/or software. Despite the existence of various standards, such devices have a high degree of difference in the structure of their data as well as a multitude of locations from where the data could be extracted from. [Ree23]. The most general solution used in dealing with not well known devices or ones with extraction difficulties has been taking pictures of the screens themselves. In very rare occasions have devices been dismantled in search of an onboard storage device due to the time required to do so.

The absence of ports is mitigated by access to cloud data

The police regularly access cloud data of suspects, largely through cooperation with them though the possibility to acquire data through a formal data request exists. This can help mitigate navigating the highly varied environment of different IoT or otherwise hard to physically access devices, though it comes at the cost of a high waiting time in order to acquire the data and requires a legally valid and especially compelling reason.

Free forensic software can be limited and commercial solutions are incredibly costly

This was reported by almost every interviewed specialist. While the cost of such solutions is of less issue to a government organization such as the police, the overall lack of availability of free tools is of harm to the digital forensics community in general. This is particularly highlighted in the time it takes to keep the tools up to date. [WBO20]The police specialists reported that often times the software that is being used is incapable of always keeping up to date with the latest advancements in technology. Having more open source tools would alleviate the issue as there would be a larger workforce with more frequent updates that is capable of staying somewhat on top of recent events. [WSC15]

A minor additional described problem unique to the Estonian (and other small countries') forensic teams is the delay in localization. While the official language for investigations is in Estonian, software often takes a long time to get localized if at all. Even though it is not a significant problem, any delay such differences cause on a case-by-case basis can compound to a significant time loss for the police department in the long run.

4.3 RQ1: How likely are portless devices to exist in the future?

This subsection looks over the different aspects relating to the first research question - the likeliness of portless devices in the future and any trends or enabling technologies and events supporting or hindering its growth.

4.3.1 Legislation

This subsection analyzes some of the current hurdles or supporting legislation on the topic. The most prevalent of these is the EU directive on device ports [Par22]. The directive states that "devices that use wired charging must use a USB-C port". While it might seem to be off-putting for the development of non-standard ports as one of the pioneers of the market, Apple, has stated on multiple accounts that they do not wish to use the USB-C port device [Ste22]. However, the specific subclause on "that use wired charging" is of interest. While the directive in general was enough to stop Apple from releasing their iPhone 17 Air without a charging port out of initial fear - the mindset has remained the same. [Gur25]

In an interview done with the European Commission press officer Federica Miccoli it was ultimately confirmed that a portless phone would be compliant as it cannot be recharged through wired methods, and therefore does not need a harmonized charging solution. However, the EU still encourages developing a united wireless charging standard in the stead of proprietary solutions. [Lov25] Legislation is important to keep an eye on in the future as the proper market-stimulating policies can drastically alter the cost-benefit evaluations for companies as well as decrease the final price for the consumer. [KMT18]

4.3.2 Emerging technologies

This subsection covers some recent technologies that support the growth of portless devices.

QI2 standard, wireless power
An evolution of the Magsafe standard initially drafted up by Apple in 2007 [RDA+07], the Qi2 standard is a result of cooperation between Apple and the Wireless Power Consortium (WPC). The standard as such is essentially a result of the donation of the Magsafe technology to the WPC. [Con]The goal of the standard is to unify the wireless charging industry in order to provide more interoperability between devices. The standard is backwards compatible and, as such, already supports Apple's iPhone 12 all the way to iPhone 16 and any future devices. The collaboration and development of a solid standard before portless mobile phones are even introduced to the market has the potential to smoothen their release as well as make legislative support easier.

Wireless power transfer using solar satellites has also been looked into, though the underlying technology could not be adopted for widespread home use just yet as the microwave beams used would have very high power densities that can be harmful to humans. [Lin21] Despite that, wireless power transmission is increasing in popularity and demand as more devices become interconnected in a portless manner. [Shi21] As of right now though the technology seems most useful for powering remote locations or potentially charging electric vehicles or other larger scale consumers. [ea]

LEO constellations
One potential prospect for technically portless devices are low earth orbit satellites due to their distance and physical inaccessibility. Their large scale of coverage has the potential to supply a wide area of IoT devices at once as there are already steps being taken towards integrating LEO constellations into 5G networks. While standards do not quite yet match, work is being done to improve on the fact and better integrate them into the 5G ecosystem. [SESE+24] We can see that the somewhat recent release 16 and 17 from 3GPP have had significant improvements on this part by for example integrating NR over non-terrestrial networks. [3GP].

As satellites are becoming more prevalent as an option even for more basic consumers through the addition of companies that provide satellite-operations-as-a-service such as SpaceIt [spa], researchers and forensics specialists should put consideration into potentially exploring the field further as it starts to become more accessible. While doppler shift is somewhat of an issue for data integrity for such operations both normally and in terms of extracting forensic data due to the high orbital velocity of the satellites, careful development considering the matter could help offset it. [BNX+19]

The recent investigations into laser inter-satellite links has the potential to drastically increase the area of devices that are connected with each other in an IoT network due to the range covered by satellite systems and the extremely low latency provided by laser communications. [CY21] Care must be taken to prevent loss of line of sight though as that could result in a significant loss of data useful for forensics, and as such redundant data pathways must exist.

4.3.3 Market trends

This section focuses on analyzing the market trends present in relevant devices to see what the data in the future might look like. The most relevant chosen statistics were the overall number of IoT devices as well as the count of wireless smart home cameras. These two seem most prudent to investigate as one gives a general idea on the growth of IoT, which largely encompasses wireless devices or things without a traditional input port that is easy to extract from. The latter gives insight into one of the most important types of IoT devices for criminal cases [Est25] and the most likely to be wanted to gather evidence from.

Data about IoT popularity was gathered from IoT analytics and Transforma. The Wayback Machine [Arc] had to be used as the sites paywall information from past years as the years progress, even if it was free in the time when it was the latest information. Figures 4 and 5 show a mix of both real data and future forecasts based on the year of the study.

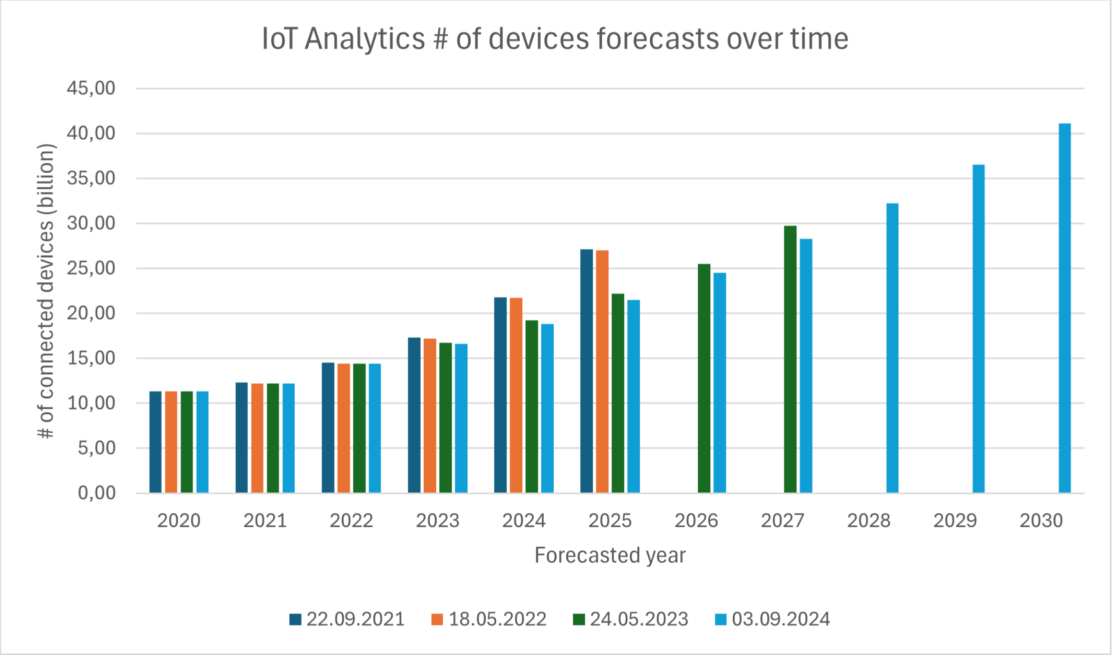


Figure 4. IoT Analytics IoT connections forecasts [Sin24]

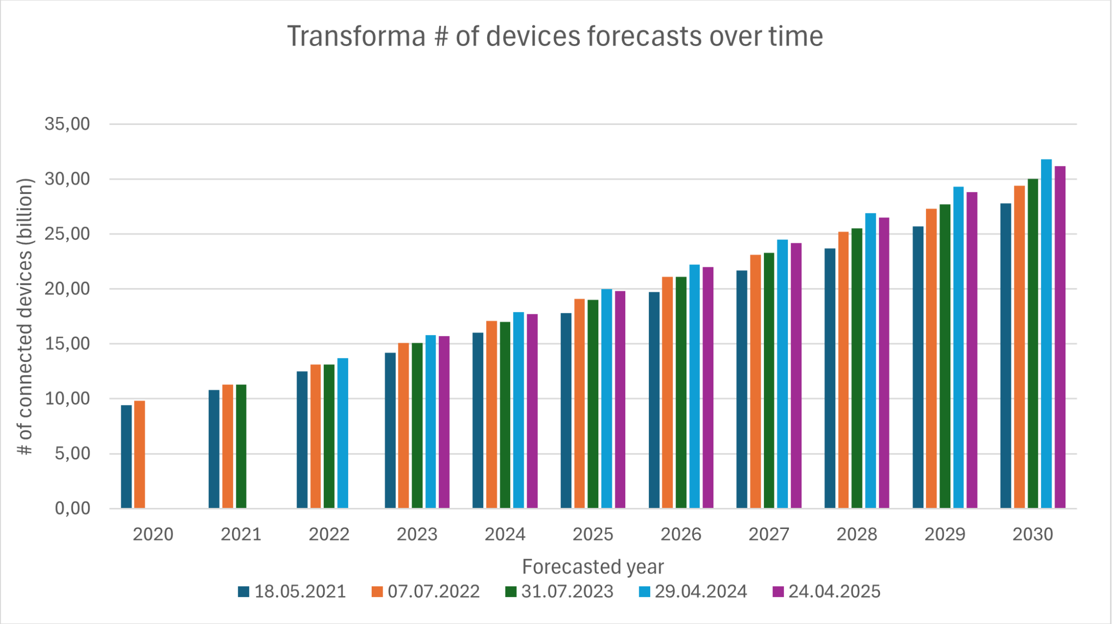


Figure 5. Transforma IoT connections forecasts [Ins]

Some things to note are that real data generally only applies up until half a year before the study was performed, so in the case of an IoT analytics study from 2023, real data only goes up to the end of 2022. While we can observe a steady and slightly exponential growth of devices over the years on both graphs, interesting properties can be noted. In the IoT analytics forecasts, the forecasts get less ambitious every year with a roughly 15% difference in the amount of predicted devices for 2025 from the study done in 2021 and the study done in 2024.

The Transforma forecasts are more consistent with their predictions, however it is important to notice the significant drop between the reports done in 2024 and 2025. Both of these suggest that the IoT trends are not quite as rapidly growing as initially expected. Figure 6 highlights the difference between the latest reports from the two companies.

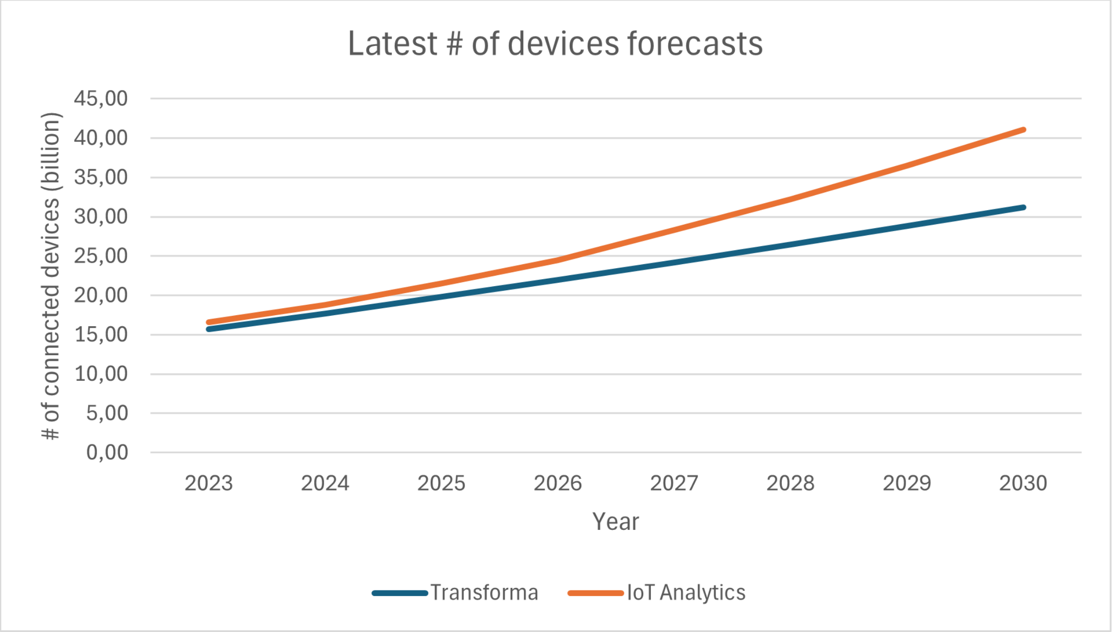
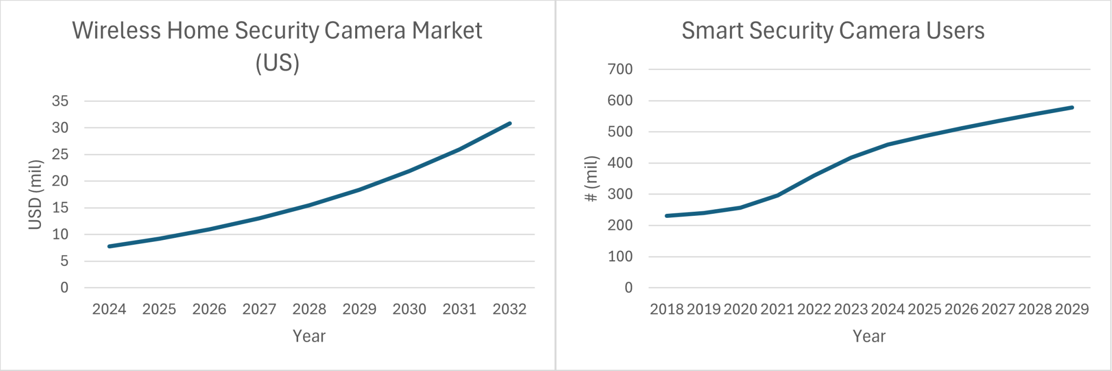


Figure 6. IoT Analytics vs Transforma latest IoT connections forecasts

The key insight to note is the difference in growth. IoT analytics predicts a strongly exponential growth in the number of devices even though they have had to tone down their numbers year after year. Transforma's growth is barely exponential - almost a linear line. Due to the accuracy of Transforma's forecasts so far, the trend being softer than expected is likely.

The smart home security camera market shows a steady increase in the adoption of wireless cameras as can be seen in figure 7b. Figure 7a shows the current market trends for wireless cameras in the United States.



(a) US Wireless Camera Market [Res25]

(b) Smart Security Camera users [Sta]

Figure 7. Wireless Camera Market Research

In both cases, the growth is significant especially in the recent years, though the research done in the US predicts a compound annual growth rate of 18.8% consistently. Data about previous years was unable to be obtained. Statista's research shows the growth rate decaying over time, likely as a result of people who wanted to adopt the technology already doing so as it gets cheaper, but once they have it they are less likely to replace it and so the customer base declines.

4.4 RQ2: What indirect extraction methods can be used to access data relating to a portless device?

This research question looks into the potential ways to get data from a portless device without having to physically extract information from it. The potential paths of action can largely be grouped in two: Cloud data and network data.

4.4.1 Cloud

Cloud data extraction is the main source of acquiring information when access to the device cannot be obtained neither through voluntary password sharing nor physical extraction. [Est25] Despite that, forensics analysts are held back from the acquisition of cloud data by the lengthy request periods for it. While there exist methods around the request periods [DS13], these require integration with the infrastructure itself and, as such, still put analysts at the mercy of the service providers' choices in terms of architecture and included systems. As of right now the only real way to get cloud data is through voluntary account access or through a formal request from the provider itself. When dealing with cloud data, provenance should be considered with special caution as well as the line of when and from what device data was acquired from can become somewhat muddy. [LCHW14]

4.4.2 Network

The most prevalent use of network data that is often used in criminal investigations is the use of cellular data logs. This encompasses things such as call logs, messages, connected cell towers and the like. While these are useful for constructing a potential timeline of events, they do not provide value through the messages contained and cannot provide custom data for use in investigations. As such, their use is limited to a supportive role in investigations. Care should also be taken when using it to determine suspect locations as the data gathered is heavily unreliable, even in cities where cell tower intensity is denser. [ZYZC24] Other methods of gathering data through the network rely on finnicky and time-expensive extraction methods often requiring prolonged presence in or extensive analysis of the network [Sik20]. The majority of research on the field also assumes an I/O port existing, and even in the case of network data relies on a physical connection to the device, whereas methods of data extraction focused on solely acquiring it through the network are too limited or primitive for general use and would have to be far further refined to be usable in the field [MAA+24], and as such the research on portless device forensics through these indirect methods is largely insufficient.

4.5 RQ3: What extraction methods could be used to access data physically present on a portless device?

NIST has very clearly demonstrated exceeding success in extracting data from an otherwise broken mobile device through JTAG and chip-off decoding. [NIS21] This process however is incredibly time-intensive and the latter malforms the source data, making it unusable for normal forensic investigations unless somehow further optimized or modified.

Wirelessly transmitting a tool for the extraction of data can work [AHR20], but relies on the device being in working condition and may struggle to be adopted for the more scrutinizing Apple ecosystem that is harsher on app control, that is if attempts to modify it to suit forensic needs even on an Android system are successful.

Some success has been found with direct analysis of logs present on the storages of IoT devices such as smart bulbs, though the data contained therein is extremely volatile and might not date back far. [SA24] Furthermore, the most useful data such as network passwords that are stored in plaintext must be acquired through extracting the WiFI module from the device itself and connecting it to one's own device - an investment of time that the police do not have for most investigations. The research done on this field does however emphasize that the lack of standardization. The former brings a lack of plug and play solutions for easy analysis but also opens the gateway for being able to break into systems when there is a dire need to do so due to the much less tested standards and lower attention to security present in these devices.

In the absence of other solutions such as IoT devices that are difficult to extract data from, the remaining choices boil down to taking pictures of the device in question or manually attempting to extract the storage medium from the device. [Est25] The solutions available may wary from device to device and some overview of potential examples are given in chapter 5.

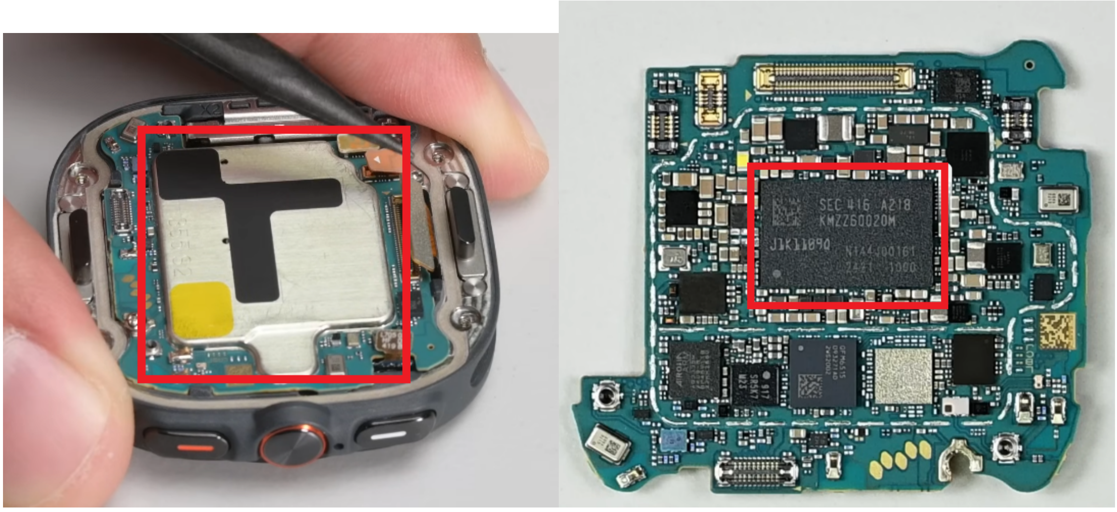
5 Portless device examples

In order to establish the potential scale of portless devices, specific examples have to be considered as well as their success in their respective fields and what ways exist to extract data from them. This section will look at an example or two from the following categories which could be considered most relevant to a forensic investigation [Est25]: wearables, phones, sensors, other IoT devices. In addition there is also a brief overview of bio-integrated wearables which are largely in the research phase but could prove a useful tool in cases where they are involved.

5.1 Wearable

Galaxy Watch Ultra

The Galaxy Watch Ultra is a fully wireless watch from Samsung released in 2024. The specifications of the device are very similar to the Apple Watch Ultra all the way down to the design. As a smartwatch it can measure most basic biological information from heart rate to oxygen saturation. What is of note is the 32GB storage in the on-board Exynos W1000 processor together with 2GB of RAM. The problem is that accessing it requires disassembly of the device and the components themselves are shielded by a firm metal cover. Even with it exposed, there are no clear points of entry. The shielding and the processor underneath can be seen in figures 8a and 8b



(a) Shielded processor

(b) Uncovered processor

Figure 8. Galaxy Watch Ultra Mainboard. Footage courtesy of [iFi24]

Zio XT heart monitor

The Zio XT is a long-term monitoring service mostly intended for keeping tabs on the health of the elderly. It is mostly an ECG monitor that connects to a device through Bluetooth. The main draw of the device is the comfort of it, being able to be kept on even during the shower or sleep. Due to the non-intrusive nature of it, users have shown a 98% compliance rate in keeping the device on, proving it to be reliable in monitoring a person's health at any point. [Zio] Within the device we can also find onboard flash storage, though extracting data from it would be incredibly cumbersome. Therefore the only real solution is having willing help from the victim's relatives or the company itself. Due to the device being comfortable to keep on and the memory being able to store weeks of data, it would be helpful in determining a patient's state and time of distress or death. A picture of the mainboard can be seen in figure 9.

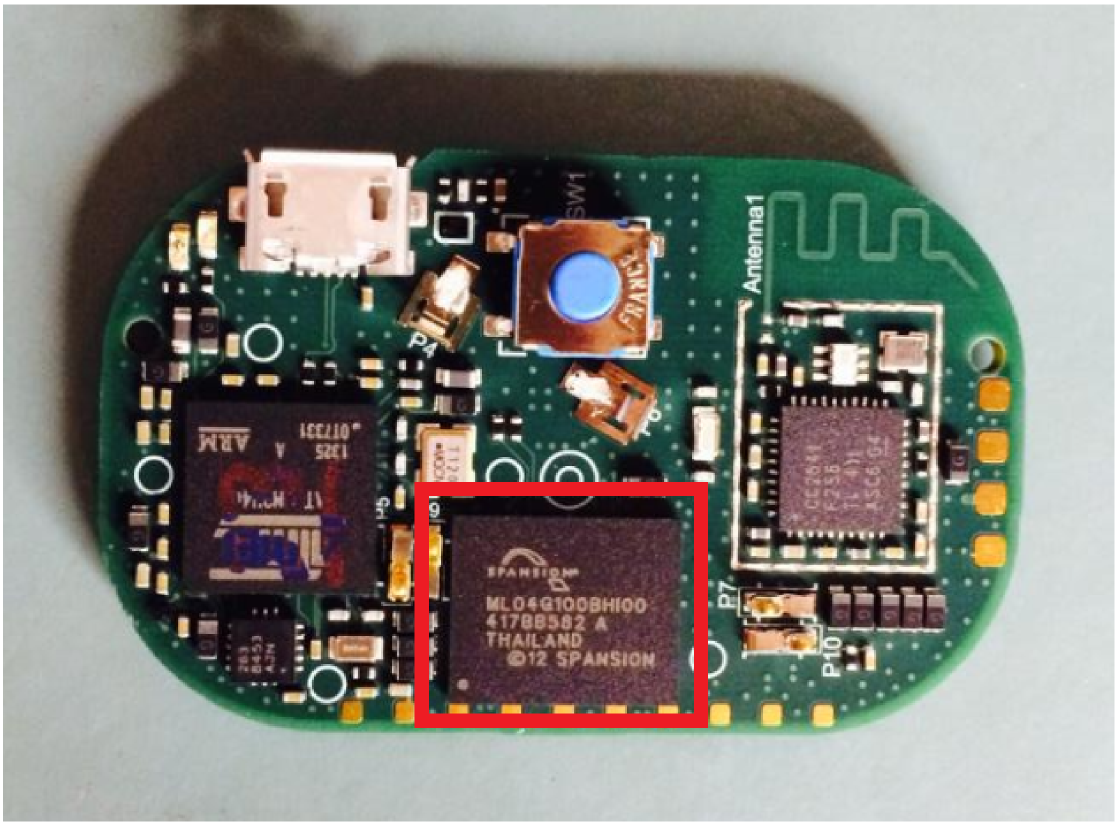


Figure 9. Zio XT mainboard. Base image courtesy of [ID]

5.2 Phone

The MeiZu Zero was the first and so far only portless phone introduced into the public market. It was highly marketed as the smartphone of the future featuring no buttons, holes, ports, or outer wire connections. The phone used the company's own 18W wireless charging solution, far faster than the other alternatives at the time and even faster than the current Qi2 standard that stands at 15W. [GSM] The phone was attempted to be funded by a 100k USD kickstarter but ultimately met only 45% of its goal.

As only a limited amount of demo versions of the phone were released, no disassembly can be found. The only extraction that could be done on the phone would have to be indirect through a network medium as the phone does not even support a physical SIM. It might be potentially possible to dismantle the device and take the storage module out of it, but without any disassembly information available it is hard to estimate the forensic soundness of doing so. The failure of its kickstarter despite the widespread media attention it received, reaching even Estonia [Man], shows a lack of consumer interest in such a device at the time. This could also be attributed to the relative obscruity of the company as well.

5.3 Sensor

The JioTag Air is a GPS tracker similar to the Apple Airtag. It is advertised as a cheaper and more powerful alternate to the Apple Airtag. Despite being a competitor to Apple, it uses the same Find My ecosystem in order to provide its services, with the caveat that it's also compatible with Android devices through its own application. The device is powered entirely with a battery cell and therefore has no ports to connect to. Forensics would have to be conducted using data from the cloud or the mobile phone the device is paired with. [Jio] However, opening the device up reveals a multitude of test pins that could be connected to [Agg24], though there is no documentation available online on the process of doing so, nor would it be particularly time efficient for the police. The pins can be seen highlighted in figure 10.

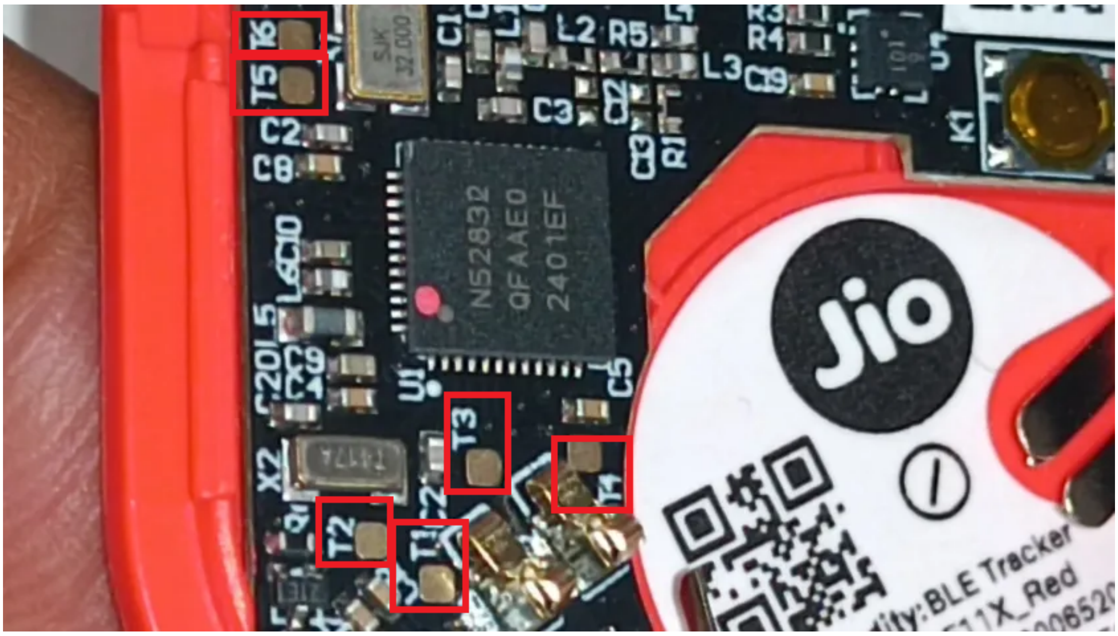


Figure 10. JioTag test pins. Base image courtesy of [Agg24]

5.4 Other IoT

The Wyze Smart Plug is a simple outlet add-on that allows remote control of any device connected to it. It does not interface with devices in any special way other than cutting off power supply to the device based on commands received. The circuit board inside the plug contains an ESP8266 Wi-Fi microcontroller. The controller contains a small amount of memory (80 KiB) that could potentially store some data about the user's operations or recent history. Physical access to the module is cumbersome as it requires slightly malforming the container and then manually connecting pins to the module that is in a somewhat uncomfortable position as it is blocked off by the socket's relay. While the controller is subject to several vulnerabilities, none of them are of particular forensic interest in the context of a smart plug as the most they could do is disable the device from transmitting power (or vice versa). The circuit board can be seen on figure 11 with the microcontroller highlighted.

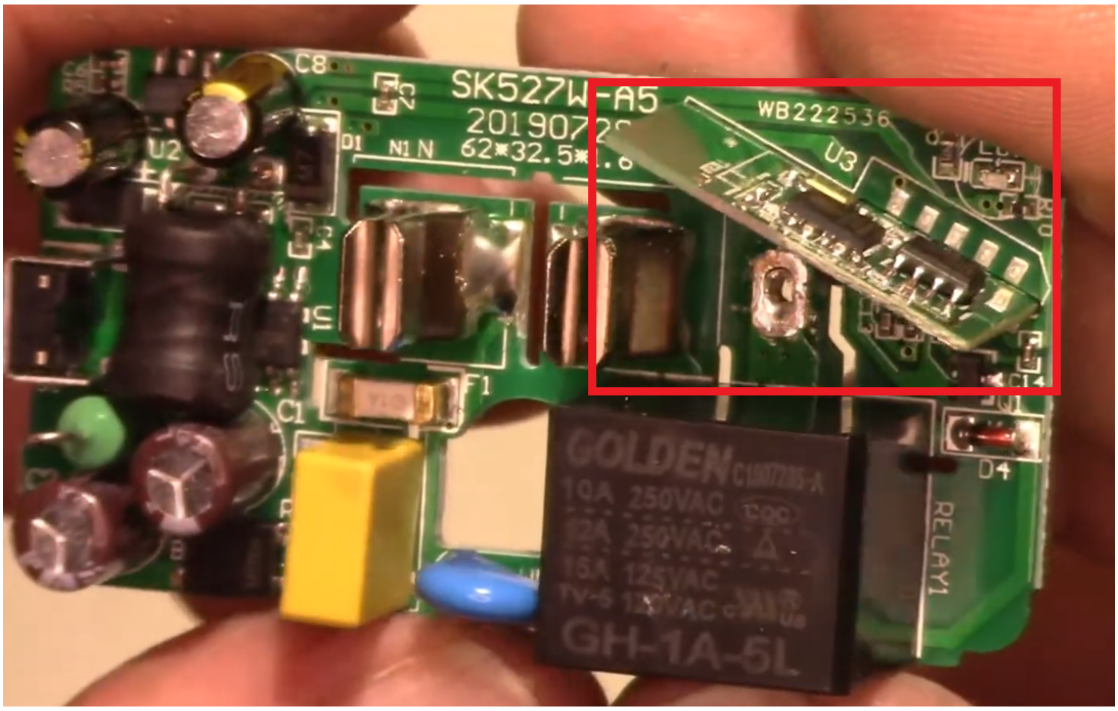


Figure 11. WYZE smart plug circuit board. Base image courtesy of [Fix19]

5.5 Bio-Integrated Wearable

Another potential future avenue of portless health devices that could carry a significant amount of forensically important data are bio-integrated wearables. These would measure the biophysical and biochemical signals of the human body in a far more efficient manner than any form of smart watch can and are made possible by recent advances into ultrathin electronic systems that are flexible enough to stay intimately connected with the human skin through its movements and bends [ZLY+18]. These advances can be dated back as early as 2007. [MGB+07] Despite that they are still not ready for widespread manufacture due to the high amount of complexity and the interdisciplinary knowledge and cooperation required to develop such devices. [RCB+19]. These devices can utilize any of the wireless communication channels available to normal IoT hardware such as NFC, Wi-Fi, or Bluetooth. [LY16] While the security concerns of Bluetooth are heavy [Yin23], new wearable technology is still being proposed using those modules [HCL+24] and as such forensic specialists should be prepared for that in the future, as the wearables are unlikely to have any form of wired data port.

6 Discussion

6.1 Research Question Answer

How will portless devices affect forensics in the future?
As of right now, portless devices are not the most prevalent issue in digital forensics. Actual field contact with them is relatively rare. While the first pushes towards a fully portless mobile phone were largely a stunt and failed, Apple's own attempts are likely to have a much more significant impact on the trends to follow and may make encountering these devices far more common in investigations, given as mobile phones are the most common form of digital evidence. The commitment to adopting portless devices can be seen in working on a unified standard for wireless charging before having released a fully portless phone, preventing further obstacles from very likely future EU regulations on the structure of such devices.

Several supporting technologies such as laser communication for LEO satellites that are being integrated with 5G systems support the growth of wireless devices. Every trend report predicts a heavy growth of portless devices of one form or another. Looking at examples of individual portless devices shows that aside from cloud data, physical data extraction is incredibly cumbersome if not entirely forensically inviable for the purposes of criminal investigations.

With all that considered - while forensic devices are not a problem right now, they will be in a few years unless new methods are developed to extract data from them or work with cloud providers.

6.2 Limitations

This paper has several limitations that threaten its validity. While attempts were made to gather data from a variety of sources ranging from both academic to industry-specific all the way to interviews, a bias in study selection will always exist even subconsciously within the researcher as they might unknowingly exclude fitting sources or might not have applied or even formulated the exclusion/inclusion criteria correctly. Furthermore, data extracted from the gathered studies might also suffer from the researcher's subjectivity in interpretation as full papers cannot be represented in this format and the analytical nature of the SLR demands interpreting the results and implications of chosen papers, which happens through the eyes of the researcher.

Another particular issue is the novelty of the topic itself - the amount of data available on it being minimal, making academic sources on the topic hard to find and forcing the researcher to even rely on patents and interviews for information. Very few sources are directly about the forensics of a portless device and as such, conclusions had to be drawn from papers about adjacent and supporting topics such as 5G. Direct research queries on the exact field of study yield no results in research databases.

The small sample size of interviewees must be considered as well. While the nature of their positions means that they speak for many, four is regardless still a statistically small number and lends itself to potential bias in the answers of every interviewee.

This work presents a light analysis of the papers covered, as well as a current background of the topic and the researcher's interpretation of the state of the future of forensics in the area. As a result, it goes through multiple layers of interpretation and must be critically judged as doing so.

6.3 Future Research

Due to the novelty of the field in question, much more research could be conducted on the topic at hand

- A deep analysis of Apple's new portless phone when it launches, as it has the potential to shape the entire market
- The legal side of portless forensics - how could investigations be assisted in a manner that retains a suspect's rights?
- An assessment of the communication technologies in use by portless IoT devices - particularly developing replacements or evolutions to Bluetooth
- Experimental laboratory dismantlings of multiple types of portless devices in order to find common and easy to access entry points
- A timeless or long-lived framework on teaching digital forensics and sharing information regarding it with educators instead of one that relies solely on current technologies
- A large scale survey of investigators in the field on the effects of portless devices and their prevalence. The closest research is [Mil22] which focuses more on the relationship between prosecutors and investigators and general digital evidence without specific device types.

7 Conclusion

The work set out to find an answer to the effect portless devices will have in the future. To that end, a large number of research papers as well as commercial sources were investigated and their findings combined for a bigger picture. A police interview was conducted in order to contrast the practical experiences of police specialists with the theoretical findings to test their validity in Estonia as well as in general.

Based on the information provided by the various sources analyzed in the paper, the general view for the future count of portless devices is growing, however not as ambituously as initially thought.

Advancements in a standardized wireless charging protocol show potential in adopting the technology over a wider range of devices from ones as small as sensors through Qi2 technology to as large as electric vehicles through solar satellites. Technologies that support integrating LEO satellite constellations into 5G interactions make the reach of IoT networks far wider and prevalent. While prior in the paper some hurdles such as the new EU law mandating the use of USB-C chargers were mentioned, general trends within device manufacturers favour minimizing the space used for ports, especially in the world of IoT. It has also been clarified that the directive demanding the use of USB-C does not apply to entirely portless devices, clearing the way for Apple to release their new portless mobile phone and shake the market.

The study found that there is a lack of direct data extraction methods for purely portless devices in general. Furthermore, methods that do exist tend to be too time-consuming to be applied to a criminal case where the amount of time that can be spent on any particular piece of evidence is limited, especially when considering that extracting data only yields potential, not guaranteed evidence. A number of portless devices come without any significant on-board storage at all, and those that do come with storage often have it tightly attached to the processor or the mainboard and are difficult to extract from.

The current main viable indirect extraction method is merely asking cloud providers for the data through a formal request. This method takes a significant amount of time both in terms of waiting for the reply and the data itself, as well as crafting a valid request. The research on ways to mitigate this relies on solutions that have already been built into the architecture of the systems and have not seen any success in practice. Capturing network data can be considered but the research on the topic is not mature enough to have yielded any prompt ways of doing so.

The current forensic scene is ill-prepared for the advent of portless devices as police investigations do not have the resources to tailor custom-made solutions for the extraction of data from a diverse set of devices without a unified standard. Of utmost importance is being able to have plug-and-play solutions for data acquisition and there is a complete lack of any such method for a portless device. While service pins exist for some devices, even using them can take time and a large number of portless devices do not have them in the first place. The recent jump in supporting technologies as well as commercial push suggests a significant rise in the amount of portless devices in everyday life, and there are no efficient enough tools or methods in the forensic community to deal with it at present time.

References

[3GP] 3GPP. Release 17.

[5Gs25] 5Gstore. Digi ix15 iot gateway, 2025. [Online; accessed April 27, 2025].

[AAD21] Gunnar Alendal, Stefan Axelsson, and Geir Olav Dyrkolbotn. Chip chop — smashing the mobile phone secure chip for fun and digital forensics. *Forensic Science International: Digital Investigation*, 37:301191, July 2021.

[Agg24] Pallav Aggarwal. What's Inside The JioTag Air? A Complete Hardware Teardown, September 2024. Section: Teardown.

[AHR20] Mukhlis Prasetyo Aji, Dedy Hariyadi, and Tri Rochmadi. Logical acquisition in the forensic investigation process of android smartphones based on agent using open source software. In *IOP Conference Series: Materials Science and Engineering*, volume 771, page 012024. IOP Publishing, 2020.

[AKPL21] Dr-Abdullah Ayub Khan Ph.D and Asif Laghari. Digital Forensics and Cyber Forensics Investigation: Security Challenges, Limitations, Open Issues, and Future Direction. *International Journal of Electronic Security and Digital Forensics*, 1, October 2021.

[AQPMS15] Antar Shaddad Abdul-Qawy, PJ Pramod, E Magesh, and T Srinivasulu. The internet of things (iot): An overview. *International Journal of Engineering Research and Applications*, 5(12):71–82, 2015.

[Arc] The Internet Archive. Wayback Machine.

[ASAR+24] Mohammed Amin Almaiah, Leen Mohammad Saqr, Leen Ahmad Al-Rawwash, Layan Ahmed Altellawi, Romel Al-Ali, and Omar Almomani. Classification of Cybersecurity Threats, Vulnerabilities and Countermeasures in Database Systems. *Computers, Materials and Continua*, 81(2):3189–3220, November 2024.

[ASB20] Abdullah Aziz, Olov Schelén, and Ulf Bodin. A Study on Industrial IoT for the Mining Industry: Synthesized Architecture and Open Research Directions. *IoT*, 1(2):529–550, December 2020. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

[AZZ+17] Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, and M.L.M. Kiah. A review of smart home applications based on internet of things. *Journal of Network and Computer Applications*, 97:48–65, 2017.

[BNX$^+$19] Hamza Benzerrouk, Quang Nguyen, Fang Xiaoxing, abdessamad amrhar, Hamza Rasaee, and Rene. Jr Landry. LEO satellites Based Doppler Positioning Using Distributed nonlinear Estimation. *IFAC-PapersOnLine*, 52(12):496–501, January 2019.

[Bru23] Josh Brunty. Validation of forensic tools and methods: A primer for the digital forensics examiner. *Wiley Interdisciplinary Reviews: Forensic Science*, 5(2):e1474, 2023.

[BSCMSJ21] Andrew Booth, Anthea Sutton, Mark Clowes, and Marrissa Martyn-St James. Systematic approaches to a successful literature review. 2021.

[CAG18] Hongmei Chi, Temilola Aderibigbe, and Bobby C. Granville. A Framework for IoT Data Acquisition and Forensics Analysis. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 5142–5146, December 2018.

[CB20] Lalit Chettri and Rabindranath Bera. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet of Things Journal*, 7(1):16–32, January 2020.

[CDI22] Raffaele Cuomo, Davide D'Agostino, and Mario Ianulardo. Mobile Forensics: Repeatable and Non-Repeatable Technical Assessments. *Sensors*, 22(18):7096, January 2022. Number: 18 Publisher: Multidisciplinary Digital Publishing Institute.

[Coh25] Cohesion. Cohesion unified software platform, 2025. [Online; accessed April 27, 2025].

[Con] Wireless Power Consrtium. Qi Wireless charging.

[CY21] Aizaz U. Chaudhry and Halim Yanikomeroglu. Laser Intersatellite Links in a Starlink Constellation: A Classification and Analysis. *IEEE Vehicular Technology Magazine*, 16(2):48–56, June 2021.

[DD12] Larry E. Daniel and Lars E. Daniel. Chapter 2 - Overview of Digital Forensics. In Larry E. Daniel and Lars E. Daniel, editors, *Digital Forensics for Legal Professionals*, pages 11–16. Syngress, Boston, January 2012.

[DS13] Josiah Dykstra and Alan T. Sherman. Design and implementation of frost: Digital forensic tools for the openstack cloud computing platform. *Digital Investigation*, 10:S87–S95, 2013. The Proceedings of the Thirteenth Annual DFRWS Conference.

[ea] Hutchinson et al. Potential of wireless power transfer for dynamic charging of electric vehicles.

[Est25] Estonian Police and Border Guard. Interviews of Estonian Police and Border Guard Digital Forensics Specialists, 2025. Conducted by Gustav Gretškov.

[Fix19] FixitFrank. WYZE Smart Socket Teardown -YASS, September 2019.

[GB20] Mark Gurman and Marques Brownlee. A portless iphone chat with mark gurman, $500 airpods max, & samsung's disappearing charging brick. Apple Podcasts, 2020.

[GKSSJ23] Achuth Gopinath, Kukatlapalli Pradeep Kumar, K M Shehan Saleem, and Justin John. Explainable IoT Forensics: Investigation on Digital Evidence. In *2023 IEEE International Conference on Contemporary Computing and Communications (InC4)*, volume 1, pages 1–6, April 2023.

[GNSV22] Khushi Gupta, Ashar Neyaz, Narasimha Shashidhar, and Cihan Varol. Digital Forensics Lab Design: A framework. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6, June 2022.

[GSM] GSMArena. Meizu Zero - Full phone specifications.

[Gur25] Mark Gurman. Apple's iPhone 17 'Air' Is a Step Toward a Slimmer, Port-Free Era. *Bloomberg.com*, March 2025.

[HBD$^+$24] Christopher Hargreaves, Frank Breitinger, Liz Dowthwaite, Helena Webb, and Mark Scanlon. DFPulse: The 2024 digital forensic practitioner survey. *Forensic Science International: Digital Investigation*, 51:301844, December 2024.

[HCL$^+$24] Xinyang He, Jiaxin Cai, Mingyuan Liu, Xuepeng Ni, Wendi Liu, Hanyu Guo, Jianyong Yu, Liming Wang, and Xiaohong Qin. Multifunctional, Wearable, and Wireless Sensing System via Thermoelectric Fabrics. *Engineering*, 35:158–167, April 2024.

[HD24] Graeme Horsman and Andrew Dodd. Competence in digital forensics. *Forensic Science International: Digital Investigation*, 51:301840, December 2024.

[Hre21] Andrew Hrenak. Mobile device forensics: An introduction. In *Cyber Forensics*, pages 291–322. CRC Press, 2021.

[IAEA22] Oludare Isaac Abiodun, Moatsum Alawida, Abiodun Esther Omolara, and Abdulatif Alabdulatif. Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10, Part B):10217–10245, 2022.

[ID] FCC ID. SR15P ZIO SR ECG PATCH Teardown Internal Photos iRhythm Technologies, .

[iFi24] iFixit. Galaxy Watch Ultra Teardown - Not Just An Apple Watch Clone, August 2024.

[Inc24] Apple Inc. Accessory devices that communicate with electronic devices, 2024.

[Ins] Transforma Insights. Current IoT Forecast Highlights - Transforma Insights.

[IS20] Selay Ilgaz Sümer. A New Marketing Trend in the Digital Age: Social Media Marketing. In Umit Hacioglu, editor, *Digital Business Strategies in Blockchain Ecosystems: Transformational Design and Future of Global Business*, pages 133–151. Springer International Publishing, Cham, 2020.

[ISOa] ISO. ISO/IEC 27037:2012.

[ISOb] ISO. ISO/IEC 30141:2024.

[Jio] Jio. JioTag Air for iOS - Location Tracker: Mini Tracking Device.

[JSE24] Luke Jennings, Matthew Sorell, and Hugo G. Espinosa. The provenance of Apple Health data: A timeline of update history. *Forensic Science International: Digital Investigation*, 50:301804, October 2024.

[KFF24] Lena Klasén, Niclas Fock, and Robert Forchheimer. The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, 362:112133, September 2024.

[KMT18] Goksin Kavlak, James McNerney, and Jessika E. Trancik. Evaluating the causes of cost reduction in photovoltaic modules. *Energy Policy*, 123:700–710, December 2018.

[KPBB$^+$09] Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, 51(1):7–15, January 2009.

[KR16] Victor R. Kebande and Indrakshi Ray. A generic digital forensic investigation framework for internet of things (iot). In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 356–362, 2016.

[KSC$^+$19] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. All things considered: An analysis of IoT devices on home networks. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1169–1185, Santa Clara, CA, August 2019. USENIX Association.

[Kum21] Manish Kumar. Mobile forensics: Tools, techniques and approach. In *Crime Science and Digital Forensics*, pages 102–116. CRC Press, 2021.

[LCHW14] Jin Li, Xiaofeng Chen, Qiong Huang, and Duncan S. Wong. Digital provenance: Enabling secure data forensics in cloud computing. *Future Generation Computer Systems*, 37:259–266, July 2014.

[LHZ$^+$16] Hang Liu, Sha Hua, Xuejun Zhuo, Dechang Chen, and Xiuzhen Cheng. Cooperative spectrum sharing of multiple primary users and multiple secondary users. *Digital Communications and Networks*, 2(4):191–195, November 2016.

[Lin21] James C. Lin. Safety of wireless power transfer. *IEEE Access*, 9:125342–125347, 2021.

[Lov25] Ben Lovejoy. EU confirms Apple can make a portless iPhone without USB-C, March 2025.

[Lud23] David Ludlow. Arlo pro 5 review, 2023. [Online; accessed April 27, 2025].

[LY16] Ting Liang and Yong J. Yuan. Wearable Medical Monitoring Systems Based on Wireless Networks: A Review. *IEEE Sensors Journal*, 16(23):8186–8199, December 2016.

[LYZ$^+$17] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 4(5):1125–1142, October 2017.

[MAA$^+$24] Haroon Mahmood, Maliha Arshad, Irfan Ahmed, Sana Fatima, and Hafeez ur Rehman. Comparative study of iot forensic frameworks. *Forensic Science International: Digital Investigation*, 49:301748, 2024.

[MAEP15] Mahdi H. Miraz, Maaruf Ali, Peter S. Excell, and Rich Picking. A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In *2015 Internet Technologies and Applications (ITA)*, pages 219–224, September 2015.

[Mal] Malwarebytes. What was the Mirai botnet?

[Man] Jan-Matthias Mandri. Meizu Zero: tulevikutelefon, millel pole ühtegi pesa ega nuppu. Section: Forte, Digi.

[MAOB21] Syria McCullough, Stella Abudu, Ebere Onwubuariri, and Ibrahim Baggili. Another brick in the wall: An exploratory analysis of digital forensics programs in the United States. *Forensic Science International: Digital Investigation*, 37:301187, July 2021.

[MGB^{+}07] C. Müller, S. Goffri, Dag Werner Breiby, Jens Wenzel Andreasen, H.D. Chanzy, R.A.J. Janssen, Martin Meedom Nielsen, C.P. Radano, H. Sirringhaus, P. Smith, and N. Stingelin-Stutzmann. Tough, semiconducting polyethylene-poly(3-hexylthiophene) diblock copolymers. *Advanced Functional Materials*, 17(15):2674–2679, 2007.

[Mil22] Christa M. Miller. A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, 6:100296, December 2022.

[NIS21] NIST. Test results for binary image jtag, chip-off decoding and analysis tool, 2019-2021.

[NNGTTW21] Fahd Nadeem, Arismendy Nunez Garcia, Cao Thach Tran, and Michael Wu. Magnetic interference on cardiac implantable electronic devices from apple iphone magsafe technology. *Journal of the American Heart Association*, 10(12):e020818, 2021.

[oCoP] International Association of Chiefs of Police. Common Electronic Devices that Generate Digital Evidence.

[oE] Supreme Court of Estonia. 1-20-1208/172.

[oII] The Conference of International Investigators. General Principles for Digital Evidence.

[Par22] The European Parliament. Directive (eu) 2022/2380 of the european parliament and of the council of 23 november 2022. 2022.

[QAAS$^+$23] Md. Ohirul Qays, Iftekhar Ahmad, Ahmed Abu-Siada, Md. Liton Hossain, and Farhana Yasmin. Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review. *Energy Reports*, 9:2440–2452, December 2023.

[RCB$^+$19] Tyler R. Ray, Jungil Choi, Amay J. Bandodkar, Siddharth Krishnan, Philipp Gutruf, Limei Tian, Roozbeh Ghaffari, and John A. Rogers. Bio-Integrated Wearable Systems: A Comprehensive Review. *Chemical Reviews*, 119(8):5461–5533, April 2019. Publisher: American Chemical Society.

[RDA$^+$07] Matthew Dean Rohrbach, Mark Edward Doutt, Bartley K. Andre, Kanye Lim, John C. DiFonzo, and Jean-Marc Gery. Magnetic connector for electronic device, December 2007.

[REC15] Karen Rose, Scott Eldridge, and Lyman Chapin. The internet of things: An overview. *The internet society (ISOC)*, 80(15):1–53, 2015.

[Ree23] Paul Reedy. Internet of Things (IoT) Forensics. In Max M. Houck, editor, *Encyclopedia of Forensic Sciences, Third Edition (Third Edition)*, pages 286–293. Elsevier, Oxford, January 2023.

[Res25] Credence Research. Wireless Home Security Camera Market Size, Share and Forecast 2032, May 2025.

[RG20] Deepti Rani and Nasib Singh Gill. Internet of things (iot) characteristics, applications, and digital forensics investigation process: A review. *International Journal*, 8(9), 2020.

[SA24] Pankaj Sharma and Lalit Kumar Awasthi. Unveiling the hidden dangers: Security risks and forensic analysis of smart bulbs. *Forensic Science International: Digital Investigation*, 50:301794, September 2024.

[SESE$^+$24] Ibraheem Shayea, Ayman A. El-Saleh, Mustafa Ergen, Bilal Saoud, Riad Hartani, Derya Turan, and Adnan Kabbani. Integration of 5G, 6G and IoT with Low Earth Orbit (LEO) networks: Opportunity, challenges and future trends. *Results in Engineering*, 23:102409, September 2024.

[Shi21] Naoki Shinohara. Trends in wireless power transfer: Wpt technology for energy harvesting, mllimeter-wave/thz rectennas, mimo-wpt, and advances in near-field wpt applications. *IEEE Microwave Magazine*, 22:46–59, 01 2021.

[Sik20] Leslie F Sikos. Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, 32:200892, 2020.

[Sin23] Satyajit Sinha. State of iot 2023: Number of connected iot devices growing 16Technical report, IoT Analytics GmbH, 2023.

[Sin24] Satyajit Sinha. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally, September 2024.

[spa] Spaceit.

[Sta] Statista. Smart Security Cameras - Worldwide | Market Forecast.

[Ste22] Joanna Stern. Apple's reasoning on usb-c charging ports and privacy (interview), 2022.

[Uni18] European Union. COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 2018.

[VT18] Steve Van Till. Chapter 10 - IoT Technology and Standards. In Steve Van Till, editor, *The Five Technological Forces Disrupting Security*, pages 107–125. Butterworth-Heinemann, January 2018.

[WAN+21] Quadri Waseem, Sultan S. Alshamrani, Kashif Nisar, Wan Isni Sofiah Wan Din, and Ahmed Saeed Alghamdi. Future technology: Software-defined network (sdn) forensic. *Symmetry*, 13(5), 2021.

[WBO20] Tina Wu, Frank Breitinger, and Stephen O'Shaughnessy. Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation*, 34:300999, September 2020.

[WKHGR23] Dana Wilson-Kovacs, Rebecca Helm, Beth Growns, and Lauren Redfern. Digital evidence in defence practice: Prevalence, challenges and expertise. *The International Journal of Evidence & Proof*, 27(3):235–253, July 2023. Publisher: SAGE Publications Ltd.

[WSC15] Jing Wang, Patrick C. Shih, and John M. Carroll. Revisiting Linus's law: Benefits and challenges of open source software peer review. *International Journal of Human-Computer Studies*, 77:52–65, May 2015.

[YHA+19] Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Arif Ahmed, S.M. Ahsan Kazmi, and Choong Seon Hong. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, 92:265–275, 2019.

[Yin23] Haotian Yin. Security analysis of Bluetooth Secure Simple Pairing protocols with extended threat model. *Journal of Information Security and Applications*, 72:103385, February 2023.

[YNSC22] Jean-Paul A Yaacoub, Hassan N Noura, Ola Salman, and Ali Chehab. Advanced digital forensics and anti-digital forensics for iot systems: Techniques, limitations and recommendations. *Internet of Things*, 19:100544, 2022.

[ZDN+23] Alireza Zohourian, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Hassan Mahdikhani, Priscilla Kyei Danso, Heather Molyneaux, and Ali A. Ghorbani. Iot zigbee device security: A comprehensive review. *Internet of Things*, 22:100791, 2023.

[Zha24] Hao Zhang. Simulation of network forensics model based on wireless sensor networks and inference technology. *Measurement: Sensors*, 34:101261, 2024.

[Zio] Zio. Zio® XT Monitor | Long-Term Continuous Heart Monitoring.

[ZLY+18] Heng Zhang, Youdi Liu, Chao Yang, Li Xiang, Youfan Hu, and Lian-Mao Peng. Wafer-Scale Fabrication of Ultrathin Flexible Electronic Systems via Capillary-Assisted Electrochemical Delamination. *Advanced Materials (Deerfield Beach, Fla.)*, 30(50):e1805408, December 2018.

[ZUBC20] Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, and Kim-Kwang Raymond Choo. IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, 32:300926, April 2020.

[ZYZC24] Xiangkai Zhou, Linlin You, Shuqi Zhong, and Ming Cai. From cell tower location to user location: Understanding the spatial uncertainty of mobile phone network data in human mobility research. *Computers, Environment and Urban Systems*, 111:102130, July 2024.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Gustav Gretškov

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Portless Device Forensics in the Future", supervised by Matthew James Sorell, PhD

    1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

    1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

18.05.20225

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - Interview Questions

1. Kui tihti tekib vajadus sündmuskohalt digitaalseid tõendeid koguda?
2. Milliseid tõendeid kogutakse? (Telefonid, IoT seadmed, salvestised, HDD/SSD, salvestatud andmed)
3. Kas seadmetelt on raske andmeid välja saada?
   - Tehniliselt poolelt
     - Millised takistused esinevad?
     - Kas takistuste lahendamiseks on hetkel teostatavaid (isegi kui raskeid) lahendusi)?
   - Juriidiliselt poolelt
     - Millised takistused esinevad?
     - Kas neist saaks ümber nt seadmetest kaudset infot salvestades?
4. Kui palju aega kulub selle jaoks, et politseinikut õpetada sündmuskohalt just digitaalseid tõendeid koguma?
5. Kas tuleb ette olukordi millal saadetakse eriteadmistega spetsialist(e) sündmuskohalt digitaalseid andmeid turvaliselt koguma?
6. Kas on tulnud ette vajadust koguda andmeid füüsiliste sisenditeta seadmelt? (IoT seadmed nagu kaamerad ja sensorid)
   - Milliste selliste seadmetega on kokku puudutud?
   - Kui tihti selline olukord esineb?
   - Kuidas sellises olukorras andmekogumisprotsess käib?
     - Kui tihti see õnnestub?
     - Kui tihti saab sellistelt seadmetelt kasulikku infot?
     - Kas on kokkuleppeid pilveteenuste pakkujatega infole ligipääsemiseks?
     - Kui tihti on improviseeritud sellistelt seadmetelt andmete leidmiseks lahendusi?
     - Kas on kasutusel lahendus selliste seadmete leidmiseks?
       (a) Mis on selle lahenduse tugevad küljed?
       (b) Mis on selle lahenduse nõrgad küljed?
       (c) Kui ei, kas selline lahendus oleks kasulik?
7. Kas on kasutusel kommerts- või isetehtud riist- ja/või tarkvara sündmuskohalt andmete kogumiseks?

- Mis on nende lahenduste ligikaudne maksuvus?
- Mis on nende lahenduste nõrgad küljed? Millest jääb tunne, et on puudu?

Appendix 3 - Translated Interview Questions

1. How often is there a need to collect digital evidence from a crime scene?
2. What kind of evidence is collected? (Phones, IoT devices, recordings, HDD/SSD, recorded data)
3. Is it difficult to extract data from devices?
    - From a technical side
        - What kind of obstacles are there?
        - Are there any possible workable solutions to the obstacles (even if very difficult)?
    - From a legal side
        - What kind of obstacles are there?
        - Could they be bypassed by for example recording indirect data from devices?
4. How much time does it take to train an officer to extract specifically digital data from a crime scene?
5. Are there situations when a more trained specialist(s) is sent to extract digital data securely from a crime scene?
6. Has there been a need to collect data from devices without a physical port (IoT devices such as cameras or sensors)
    - Which such devices have you had to deal with?
    - How often does such a situation occur?
    - How does the data collection process go in that situation?
        - How often does it succeed?
        - How often do you get useful information from such a device?
        - Are there any arrangements with cloud service providers to access information?
        - How often have you improvised solutions in order to extract data from such devices?
        - Is there a solution in use to find such devices?
            (a) What are the strong sides of that solution?
            (b) What are the weak sides of that solution?
            (c) If no, would such a solution be useful?

7. Is there a commercial or in-house tool/software in use for collecting data from a crime scene?
    - What is the approximate cost of such solutions?
    - What are the weak sides of such solutions? What do you feel is missing?

Appendix 4 - GDPR consent for interviews

Andmekaitse nõusolek

Gustav Gretškovi lõputööga seoses

Lõputöö nimi on „Juhtmeteta seadmete kriminalistika tulevikus“, juhendaja Matthew James Sorell, PhD. Lõputöö eesmärk on määrata, kui ulatuslik ja aktuaalne on juhtmeteta (portless) seadmete oht digitaalse kriminalistika effektiivsele läbiviimisele. Lõputöö on kirjutatud ja teostatakse inglise keeles. Intervjuu teostab Gustav Gretškov lõputöö raames, olles saanud uurimistööde kooskõlastamise komisjonilt loa (25.04.2025, nr 1.1-14/70-3).
Gustav Gretškov, isikukood 50101210871, on vastutav töötleja, kes määrab kindlaks, milliseid andmeid tuleb lõputöö tarvis koguda ning millised on kogumise eesmärgid ja vahendid.
Talletatakse järgnevat informatsiooni:

- Intervjuu vastused kas kirjalikul või suulisel (salvestatud) kujul
- Intervjueeritavate töökohanimetused

Talletatud informatsiooni ei avaldata kolmandatele osapooltele ega ei lisata puhtas kujus lõputööle. Lõputöös on intervjuu vastused puhtalt üldistatud ja kokkuvõetud kujul ning lõputöö ei sisalda ühegi andmesubjekti isikuandmeid. Kaks kuud pärast lõputöö kaitsmist anonümiseeritakse intervjuude vastused täielikult. Lisaks sellele võib andmesubjekt oma nõusoleku ükskõik millisel hetkel tagasi võtta kirjutades sellest e-mailiaadressile gustavgretskov@protonmail.com. Sellisel juhul ei kasutata ka tema intervjuu vastuseid lõputöös toimuvas analüüsis kui see veel valminud ei ole. Lõputöösse ei saa pärast 11. maid muudatusi teha.
Allkirjastades seda dokumenti annab andmesubjekt nõusoleku oma andmete töötlemiseks Gustav Gretškovi lõputööga seoses.