TALLINN UNIVERSITY OF TECHNOLOGY
Department of Software Science

Alla Sedneva 143018IABB

ANALYSIS OF INTERNET PRIVACY PROTECTION METHODS AND PRIVATE BROWSING MODE

Bachelor's thesis

Supervisor: Karin Rava

MSc. Eng

Tallinn 2017

TALLINNA TEHNIKAÜLIKOOL
Tarkvarateaduse instituut

Alla Sedneva 143018IABB

INTERNETI PRIVAATSUSE KAITSMISE MEETODITE JA PRIVAATSE SIRVIMISE REŽIIMI ANALÜÜS

Bakalaurusetöö

Juhendaja: Karin Rava

MSc. Eng

Tallinn 2017

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: Alla Sedneva

22 May 2017

Abstract

The subject of Internet privacy attracts many concerns. [26] In order to retain their privacy online, there are various methods available for users. Extensive research is required to find the method best suited for one's needs. This work explores and briefly describes some of the well-known methods and presents a table summarizing the criteria for each one for easy-to-understand visual overview.

One of the methods of protection is Private Browsing Mode, which found its way into every major browser. [4] Supposedly, it should leave no traces of surfing activities on the user's device. [3] [21] Such claim would be tested by using memory forensics analysis. Browsing artifacts will be examined and it will be found that every browser left essential browsing data on user's device and each that results varied for each browser.

For this work, survey was conducted by the Author to observe user's perceptions of Internet privacy in general as well as get to know the preferences with respect to the same. It was revealed that people are concerned about Internet privacy and most of the users use at least one method of protection on the regular basis; unsurprisingly, due to its ease of use, PBM was revealed to be the most popular choice among the respondents and Google Chrome took the number one spot as the most-user browser (despite if showing the worst result of all the browsers tested). It is concluded that not enough is done by users to achieve privacy online.

This thesis is written in English and is **35** pages long, including 6 chapters, 23 figures and 5 tables.

Annotatsioon

Interneti privaatsuse kaitsmise meetodite ja privaatse sirvimise režiimi analüüs

Interneti privaatsuse teema äratab huvi ja tekitab palju vaidlusi. Selleks, et hoida kasutajate privaatsust Internetis, on tänapäeval palju erinevaid meetodeid [26]. Kasutajate vajaduste rahuldamiseks parima viisi leidmiseks on vaja laiaulatuslikku uuringut.

Käesolev töö sisaldab endas mõnede tuntud meetodite uurimist. Töös on esitatud tabel, milles on välja toodud kriteeriumid, mis tulevad abiks sobiva meetodi valimisel. Selline tabel annab hea visuaalse ülevaate kõikidest võimalustest ja igal kasutajal on sellest lihtne aru saada. Töös on jõutud järelduseni, et mitte ükski viis ei garanteeri absoluutset privaatsust ja tuleb kasutada erinevaid meetmeid sõltuvalt situatsioonist ning selleks, et saavutada rohkem privaatsust, võib mõnesid meetmeid kombineerida.

Privaatse sirvimise režiim on üks populaarsemaid privaatsuse kaitsmise meetodeid, mis on saadaval enamuses tuntud brauserites [4]. Väidetavalt ei jää selle režiimi kasutamisel kasutaja seadmetesse mingit surfamise informatsiooni [3], [21]. Seda väidet kontrollitakse kasutades arvutimälu kriminalistika analüüsi. Sirvimise artefakte uuritakse ja pärast nende analüüsi leitakse, et iga brauser jätab olulisi ja individuaalseid andmeid kasutaja seadmesse. Kõikide brauserite tulemused on erinevad.

Selle töö jaoks oli läbi viidud küsitlus, et uurida kasutajate arusaama interneti privaatsuse kohta üldiselt ning välja selgitada nende eelistused privaatsuse kaitsmise meetodite suhtes. Selgus, et inimeste jaoks on privaatsus internetis oluline ja enamus neist kasutab vähemalt ühte meetodit regulaarselt; pole üllatav, et privaatse sirvimise režiim on kõige populaarsem valik, sest selle kasutamine on kõige lihtsam ja Google Chrome on enim valitud brauser (vaatamata sellele, et kõikide brauserite seast näitas see kõige halvemaid tulemusi). Jõuti järelduseni, et kasutajate poolt ei ole tehtud piisavalt privaatsuse saavutamiseks Internetis.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti **35** leheküljel, 6 peatükki, 16 joonist, 5 tabelit.

List of abbreviations and terms

TUT	Tallinn University of Technology
URL	Uniform Resource Locator
PBM	Private Browsing Mode
ISP	Internet Service Provider
DNS	Domain Name System
IOT	Internet of Things
I2P	Invisible Internet Project
VPN	Virtual Private Network
IE	Internet Explorer
TCP	The Transmission Control Protocol
UDP	User Datagram Protocol
IP	Internet Protocol
OS	Operating System

Table of Contents

1 Introduction 11
2 Privacy Background and Overview 12
2.1 Privacy and Internet Privacy 12
2.2 Law and Internet Privacy 14
3 Methods of Privacy Protection on the Internet 16
3.1 Tor 16
3.1.1 Tor Principle of Work 17
3.2 I2P 20
3.2.1 I2P Principle of Work 20
3.3 VPN 21
3.3.1 VPN Principle of Work 22
3.4 Private Browsing Mode 23
3.4.1 PBM Principle of Work 24
3.5 Analysis of Privacy Protection Methods 24
4 Private Browsing Mode Testing 28
4.1 Methodology 28
4.2 Google Chrome 30
4.3 Mozilla Firefox 32
4.4 Internet Explorer 33
4.5 Microsoft Edge 34
4.6 BPM Testing Analysis 35
5 Survey 37
5.1 Survey Content 37
5.2 Survey Analysis 38
6 Conclusion 44
References 46

List of figures

Figure 1 Relay types 18

Figure 2 Onion Routing 19

Figure 3 I2P Tunnels 21

Figure 4 VPN Connection Scheme 22

Figure 5 Google Chrome first full URL found 31

Figure 6 Google Chrome product details found 31

Figure 7 Google Chrome username, email and password found 31

Figure 8 Google Chrome second full URL found 31

Figure 9 Mozilla Firefox first full URL found 32

Figure 10 Mozilla Firefox product details found 32

Figure 11 Mozilla Firefox second full URL found 33

Figure 12 Internet Explorer second full URL found 33

Figure 13 Internet Explorer search result found 33

Figure 14 Microsoft Edge first full URL found 34

Figure 15 Microsoft Edge second full URL found 34

Figure 16 Microsoft Edge product details found 35

Figure 17 Survey question 1 39

Figure 18 Survey question 2 39

Figure 19 Survey question 3 40

Figure 20 Survey question 4 40

Figure 21 Survey question 5 41

Figure 22 Survey question 6 41

Figure 23 Survey question 7 42

List of tables

Table 1 Comparison of Privacy Protection Methods 27

Table 2 Google Chrome experiment data 30

Table 3 Mozilla Firefox experiment data 32

Table 4 Internet Explorer experiment data 33

Table 5 Microsoft Edge experiment data 34

1 Introduction

Privacy is important; everybody agrees on that. Everybody wants to have control over their personal information. Because of that, it was made a fundamental human right, recognized everywhere in the world. [37] With the development of technology, however, it is much harder to protect your own privacy as often users have no idea where and how their private information is leaking. In order to combat that, users have a number of privacy protection methods to choose from, all of them using different technologies and achieve different results. To find the best method, users must browse through a lot of materials to determine the strengths and weaknesses of each one. After all, each of the methods would be best suited for different needs. As such, the first goal of the present work is to summarize each of the widespread selected methods of protection, describe its technology and determine for what goals a certain method would be suited best. The analysis would be summarized by the table made by the Author based on the literature review to give the summarization a visual representation.

The second goal of this work is to test the security merits of one of the protection methods – Private Browsing Mode, which is an essential privacy-protection feature in every major browser. Supposedly, it should leave no traces of surfing activity on users' computer. [3] [21] This claim would be tested by conducting a memory forensics analysis using *FTK Imager* software and later examined in the Hexadecimal editor called *HxD*. The testing will occur on 64-bit Windows 10 OS and on various browsers such as Firefox, Google Chrome, IE and Edge to test out the description of the same on the browsers' webpages as well as to put to rest some misconceptions about PBM that users might have with respect to the scope of protection PBM offers.

The final part of this paper will consist of the survey conducted by the Author. The survey is needed to establish the perceptions of the users on the subject of the internet privacy as well as to reveal the most popular methods of protection. The survey will be then juxtaposed with the Chapters of this work in order to determine whether the users secure their privacy effectively.

2 Privacy Background and Overview

The aim of this chapter is to give a relevant background to the subject of privacy. As such, this Chapter will explore the concept of privacy in general. The definitions of the term will be examined and compared to find the common characteristics that scholars attribute to it. Next, the Author will research of what consists the privacy on the Internet. The importance of privacy will be outlined and major threats will be identified. Second part of this Chapter deals with the subject of law and internet privacy; this is important part of the background information, as law and privacy are closely connected.

2.1 Privacy and Internet Privacy

As mentioned in the Introduction, the primary topic of this paper is privacy on the internet. Before this can be explored, however, it’s important to understand the concept of privacy at large. The notion of privacy is hard for people to understand in full and difficult to define, yet nonetheless very important to do. It has been a struggle for many scholars, activists and policymakers to do so. [24] Privacy was and still is a front-line issue, especially now with the development of technologies and in order to properly regulate it, a clear and agreed-on definition is of prime importance.

Westin gives the following definition of privacy: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others”. [5] Another definition of similar nature is given by Charles Fried: “Privacy as the control we have over information about ourselves”. [25] This is very broad definition and goes for all situations, including for the privacy on the Internet. The main element in both of those definitions is control. Therefore, privacy cannot exist without the control over the information. [26] From those definitions, it’s evident that privacy is not just for individuals who have something to hide – it’s about feeling safe on the internet, knowing that your personal information is not being leaked and you actions are not tracked for somebody to judge or exploit.

Privacy on the internet is likewise difficult to define and it arises many questions, such as what information may be constituted as ‘private’ and whether there is a difference between ‘personal’ and ‘private’ information. On the internet, those concepts became blurry and the struggle to find the answer to those questions continues to this day. The personal information found on the internet can also vary in sensitivity. For instance, medical data is one of the most sensitive kind, however user’s shopping habits much less so. That is not to say that such information is not of value – companies exploit this information to impose target advertising in order to promote their products or services to users. Moreover, seemingly innocuous information can become increasingly sensitive. From those same shopping habits, your qualities and possible medical conditions can be deducted by special algorithms. For example, when user is shopping for the medicine called Digoxin it can be deducted that he may have a heart condition. That is not to say that all personal information should be highly classified, however it does mean that companies and individuals need to be careful about assuming that information that humdrum or supposedly innocuous information requires little or no protection. [27]

Internet privacy is not limited only between user and his computer. Privacy of the internet became critical for big corporations such as Apple or Google, since the majority of their technologies are based on Internet. Data breaches and incorrect handling of users’ information could occur and this could reflect on companies’ reputation and users may suffer in the result. [27] Such data breaches and irresponsible handling of users’ private information may cause the feeling of distrust in their respective service and as a result corporations could lose their clientele. A good and recent example of that is the service called Unroll.me, which had access to your inbox to quickly unsubscribe users from various newsletters that that email address was unwantedly subscribed to. A big scandal and boycott started when it was revealed that this service was selling user’s private information to third parties, such as Uber. [47] As such, both businesses and governments are beginning to take privacy very seriously.

Another danger to the internet privacy is the ever-growing popularity of the Internet of Things (IOT) technology and devices. Analysts forecast that by the year 2020, 20-25 billion IOT devices will be in use globally. [7] [8] To contrast this, this number is estimated to be just 8 billion in 2017. While the benefits of the IOT devices is out of scope of the present work, it certainly is an enormous threat to the internet privacy. Consequently, the amount of data generated by those devices is vast, which create more entry points for hackers. It also cannot be said that IOT devices are hacker-proof at the moment; as of 2016, only 10% of IOT device manufacturers were confident that their products cannot be hacked. [40] The problem also lies in the fact that not just the device itself must be secure, but also the network that it is connected to as well as software application for it. This offers hackers, governments and even manufacturers potential access to the control of the device, including its functionality, such as microphone access, and the data generated by it. Because IOT devices are also domestic personal items, it makes the data increasingly sensitive and personal. [9]

The internet is now a major part of our daily routine and its role increases each year. Increasingly more functions are available online today, such as interaction with the government. In case of Estonia, most of the government functions connected with one's health, tax returns, education and 'personal' information in general are available through the e-government portal [28], which increases the need to handle information carefully and safeguard it from leakage from the government's side. As the boundaries between our online and offline lives are becoming more blurred, our security and privacy online is likewise reflected on our 'real life'. Where one is restricted or compromised, the result can be that our 'real life' activities are also likewise reflected.

2.2 Law and Internet Privacy

It's impossible to talk about Internet Privacy without discussing its legal aspects. After all, privacy is an ancient right, which finds its beginning in the earliest Muslim, Christian and Jewish traditions. Earliest forms of privacy existed in England as far back as 1361, when King Edward criminalized the eavesdropping. [29] Privacy is also considered as a basic human right and is found in various international law instruments, such as Universal Declaration of Human Rights [37] and International Covenant on Civil and Political Rights. [38]

Laws work to protect individual's privacy and sometimes it's the only thing preventing big corporations from leaking your personal data to some third party in order to make a profit and exploit your privacy as a result. The effectiveness of law is, nevertheless, very limited due to a number of reasons. First of all, the technology is evolving really fast and the law-making process generally is very slow; in other words, the law simply cannot keep up with the technological progress. Secondly, we need to consider that lawmakers are not always tech-savvy and therefore often lack the knowledge in order to make the law effective and long-lasting. Another thing to keep in mind is that it’s often quite easy to get around law with a simple tweak in technology, however it’s much more difficult to amend the law to account for such tweak. [30]

Another point to consider is that the law is not always there to protect an Internet user and often does the contrary to protecting their privacy. At the time of writing this thesis, for instance, in US a privacy protection law is being repealed and is expected to be signed by the US President. [32] Should this go forward, this would allow Internet Service Providers (ISPs) to share personal information and location data of their users without users’ approval. This could have major consequences, as the private data of millions of users could be compromised. [6] This move is scheduled to take effect by the end of 2017. It’s important to understand that ISPs have direct access to all your browsing history and can track every click and action you make on the Internet. This is valuable information for various advertising companies and other third parties and this policy does nothing but harm the Internet users. Naturally, public is concerned about this and privacy-advocacy groups express their outrage. [31]

Another concept closely related to the notion of privacy is data protection. Unlike the right to privacy, this is a relatively modern invention which was brought to life by the emergence and development of information technology, the Internet in particular. [43] The first data protection law was put forward as recently as 1970 in Germany. [39] In a nutshell, the idea of data protection is that the individuals should have control over their personal data. That includes the collection by the computer of user’s personal information as well as use thereof. [22] That doesn’t mean that the information cannot be tracked at all, rather that individuals should give their consent on whether it could be tracked and if yes, then know how and where it is going to be used to make a rational weighted decision.

3 Methods of Privacy Protection on the Internet

As mentioned in the Chapter 2, the Internet can be a pitfall for privacy violations. All kinds of viruses and malicious software grow increasingly every day. We live in a global economy and often firms will store or move data to different parts of the world. In the meanwhile, individuals may use basic respectable web sites and don’t even suspect that their data can be collected, tracked, stored and forwarded to a third party.

There are various ways of privacy protection, the most popular of them are discussed and compared in this paper. Every method is designed for the specific audiences, depending on users’ tasks, technical skills and level of security they require. Not a single method existing today and available for a common user is a hundred percent secure, but each one of them decreases chances of user’s data being compromised.

Some of the privacy-protection methods could be combined, as they can be working alongside each other. Using two in combination, one could get the best out of them to strive for absolutely privacy protection, however also to bear the inconveniences which inevitably come with all of the methods described below.

The present work does not explore, nor sets a goal of exploring every privacy-protection method available. Here we are just exploring the popular privacy-protection methods utilizing different technology along with various results and levels of protection achieved and directed at their certain user-base.

Finally, the analysis of the methods will be conducted in order to highlight the strength and weaknesses of every privacy-protection method explored in the present work. Based on the findings, a table will be set out in the end of this chapter to give a comprehensive review of the same. This table could be useful to give an average user all the necessary information to choose the best suitable software based on the user’s requirements and level of security desired.

3.1 Tor

Tor is known as network with high level of anonymity that protects private information of users and provides data security. [18] Using Tor allows people to protect their privacy and security rights on the Internet. Individual users and other people who share the same device use Tor in order to avoid being tracked by websites or ISPs. Tor can also be used to access websites, which could be unavailable using other web-browsers for various reasons. [18] Traffic analysis gets information about individual’s contacts and their habits, by identifying source and destination points of Internet traffic. Traffic surveillance and network analysis can be stopped by Tor in order to retain the anonymity of its users.

Tor is an open-source software developed under Berkley Software Distribution license. Tor is an acronym that spells out as “The Onion Router”; this is a reference to their encryption layers, as depicted in Figure 2 as the mechanism resembles onion peeling process. [33] The concept of onion routing was first put forward in year 1995. Initially, the technology was financed by United States Naval Research Laboratory. Two years later, Defense Advanced Research Projects Agency (DARPA), US government agency, joined to this project. [34]

3.1.1 Tor Principle of Work

According to the description in Tor Browser itself, it is based on the Mozilla Firefox browser. In fact, Tor and Firefox developers collaborated on the development of the Tor Browser and in the result 95% of code in Tor browser comes from Mozilla Firefox. This collaboration was fruitful, and in the result, both Firefox and Tor have become safer in terms of privacy for the users. [19] Therefore, by using Tor, users automatically use Firefox privacy-protection function called Private Browsing, which will be discussed later in this paper in Chapter 3.4. [20]

On the highest level of the work process, Tor transfers the connection of individual’s computer with its destination (website) through numerous computer relays (also referred to as nodes). As of 2015, there are about 6000 routers responsible for data traffic in Tor network. They are located all over the world and operate due to volunteers sharing part of their traffic. It is notable that the majority of relays do not have any specific hardware or software installed, as they are all working using the same Tor software, just in the role of a relay.

The speed and security of Tor network depend on the number of relays - the more the better. This is due to the fact that traffic of a single relay is limited. The more relays a connection is going through, the harder it is to track it. [26] This is described by the probability theory as the more options you have the harder it is to guess a particular one.

As depicted in the Figure 1, Tor directs traffic through three relays, each having its role. Guard or Entry relay is the entry point to the network. Guard relays are chosen among those who remained in operation for a long time and have shown to be stable and having high speed. Middle relay routes the signal from Guard to Exit relays. As such, first relays do not have information about last ones and otherwise. Exit relay is the exit point of the network; it sends the traffic to the point of destination requested by the client. [45]

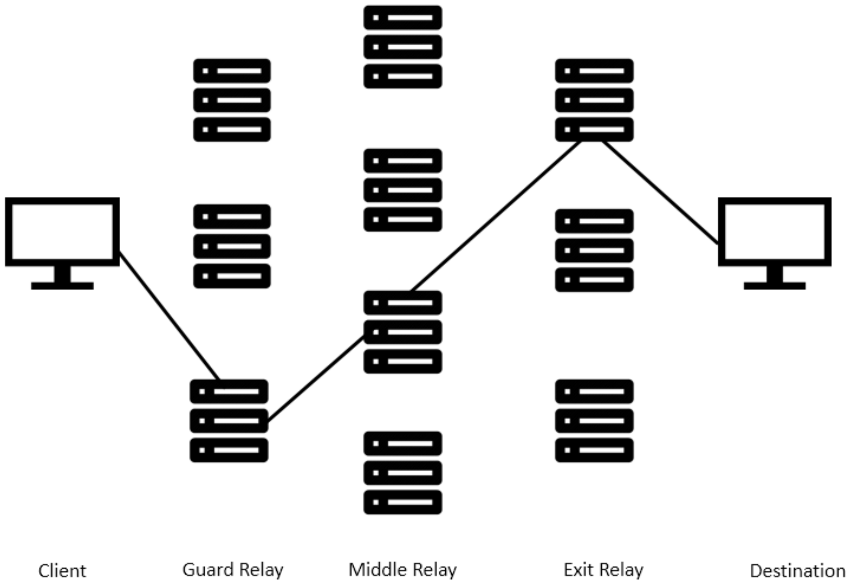


Figure 1 Relay types

Special responsibility lies with exit relays. As they are the once who send traffic to its destination, all of the potentially illegal activity going through Tor network will be connected to that exit relay. Therefore, they could be subject to raids by the police or notifications of the illegal activity.

Tor network is structured in such way that data cannot be accessed by relays; this is achieved through encryption. Client encrypts the data so that only Exit relay can decrypt it. After that, the data is once again encrypted for the Middle relay to decrypt. Finally, the data is encrypted one more time for the Entry relay.

In result, data is wrapped in encryption layers – just like an onion. In the end, every relay has only the information it needs – where the data has come from and where to send it. Such encryption is beneficial to all - client's traffic is hidden and relays do not bear responsibility for the data content. It is important to note that an Exit relay has access to the outgoing data as they have to send it to the destination point. [11] Figure 2 depicts the visual representation of the onion encryption method. [45]

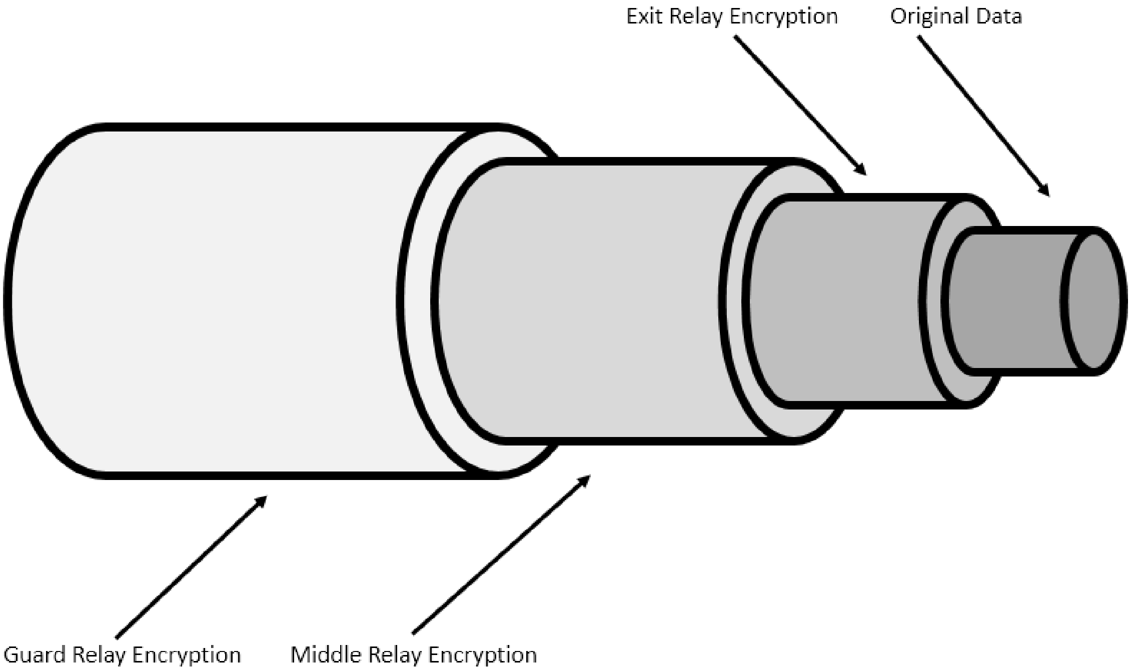


Figure 2 Onion Routing

Normally, the list of relays is public and that itself is problematic. That way, service providers can block users either entering or exiting Tor by filtering connections. However, there are also so-called Bridge relays (or bridges), which are Tor relays that are not indicated in the main directory. That allows for the users to access Tor even if the ISP is trying to block the access to the network. The latest version of Tor now provides user with a couple of bridges in order to gain access to the Tor network. In case the ISP blocks some bridges, the client will find another ones to connect. The full directory of bridges is highly classified. If any service provider gains access to it, he could block all of them and Tor network would collapse.

3.2 I2P

I2P is one of the lesser-known methods of personal data protection on the Internet. [27] It is a network of much smaller proportions than Tor and it has never received funding from the US Government or any big corporation. This project was started with a purpose of creating an anonymous network. I2P is available for everyone; however it is far from being user-friendly. Specific hardware is not required in order to use it. The name I2P stands for "Invisible Internet Project". I2P has own web-sites, blogs, chats, forums and torrent trackers and it fundamentally differs from a common network in terms of anonymity and security of browsing. In simplest terms, I2P is a “network within the Internet”.

3.2.1 I2P Principle of Work

I2P is a secure communication protocol working on top of the usual TCP/IP and UDP protocols. I2P has multiple functionalities:

1. I2P hides the IP address of the server, on which the website operates;

2. Decentralizes storage of domain names; numerous servers (so-called “address books”) are used instead of DNS.

3. End-to-end encryption data packages, making data interception pointless.

Those functions tackle the issue of anonymity. Using I2P, users can browse under another users’ IP addresses, thus avoiding blocked web pages in specific countries. [1]

I2P protocols use so-called “garlic routing”. In this case every package, which is transferred through the network is encrypted and packed into a larger package (analogue for garlic), which contains several more such smaller packages (cloves of garlic) for transferring to different relays. Suchwise, when a user receives a garlic, he pulls out a clove destined for himself and lets other cloves pass on. Since all cloves are encrypted, only the destined recipient knows what to do with it. Intermediate relays do not know what will happen next to any of the packages at the next relay and whether it will be the final one. Thereby, using only interceptions and analysis of the packages, it is strenuous to determine the physical location of the server and the latter, in turn, knows nothing of the user who appeals to him.

The data interception gets more complicated by the fact that each user changes the tunnel after a period of time, by default it is every 10 minutes. Tunnel is a chain of intermediate servers through which packages will be sent from the user to the end-server. More often than not, users act as a router, making I2P a fully decentralized service. In an online interaction I2P uses tunnels to hide IP addresses. Inbound and outbound tunnels are used for bidirectional communication. Inbound tunnels are used for transferring data to the peer who has created the tunnel while outbound tunnels are used for the opposite direction. [35]

Figure 3 illustrates a data transfer between two users in I2P network, demonstrating the functions of inbound and outbound channels. The message is sent from the User 2, aiming at first user's inbound tunnel's gateway. Once the message reaches the gateway, which is the entry point to his tunnel, it is dispatched all the way through his router. User 2 does not have knowledge about other user's inbound tunnel, but only about the entry point to his inbound channel. [35]

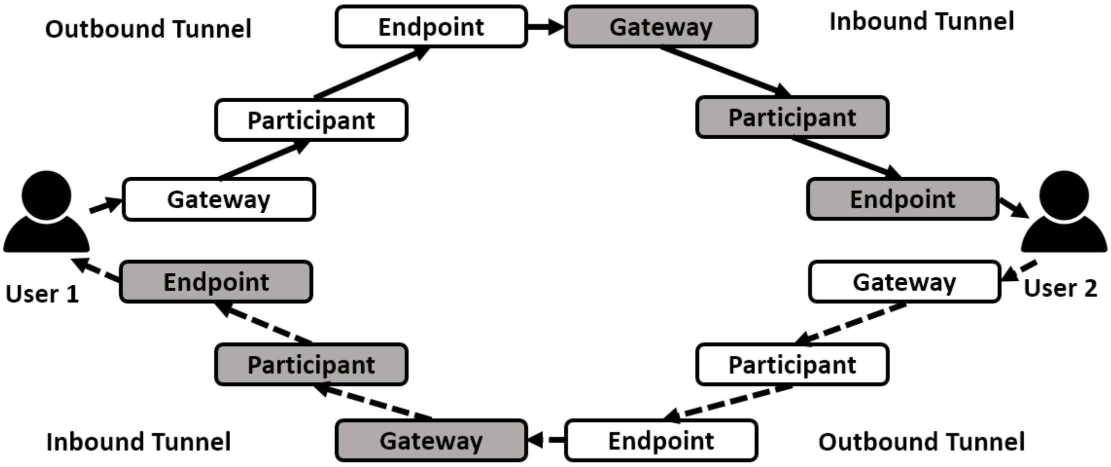


Figure 3 I2P Tunnels

3.3 VPN

VPN is an acronym for "Virtual Private Network". In simplest terms, VPN is a separate network constructed within a public network, such as Internet. [2] Through VPN, a user can securely connect to others on a public network as if they were a part of the same private network. Initially, the VPN was used mostly by the corporate employees to access their working computers remotely when they are needed to access sensitive information securely. In time, VNP technology became widely accessible for regular Internet users. VPN allows for a secure and encrypted connection to become anonymous online and keep private traffic data safe from any unwanted interference such as government or hackers. It is also a very widely used method to access geolocation-related blocked content on the Internet. Using a VNP allows users to connect to a server located in another place (for example when a certain content is available) and gain access to a previously-blocked content. This is especially relevant for countries with strict Internet and censorship laws. Most security experts recommend using VPN as an easy privacy and security solution when using public Wi-Fi hotspots, especially when accessing sensitive information such as online shopping or banking. [23]

3.3.1 VPN Principle of Work

Figure 4 illustrates the structure of a typical VPN network. This describes how the connected to the VPN server is made, which assigns a new public IP address to the user's device. When using the VPN, the traffic passes through your ISP and goes onto the VPN server. From thereon, your traffic is encrypted, different IP address is assigned and ISP cannot keep track of your actions anymore. [46]

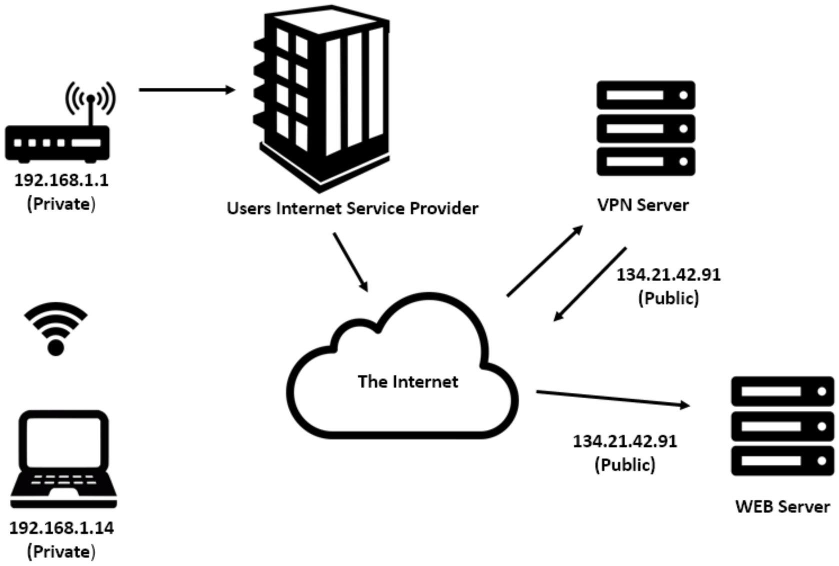


Figure 4 VPN Connection Scheme

Similar to the structure of I2P, VPN also utilizes tunneling. In VPN connection, packets of data are encrypted in a selected carrier protocols and transmitted between VPN client and server and decoded at the receiving end. In Internet types of VPN, an IP protocol is used. VPN protocols encrypt and authenticate data that is being sent through the tunnel.

There are various VPN protocols, each having their own principle of work, security and features.

- IPSec – a collection of various related protocols that feature encryption and authentication capacity. Essentially, IPSec is an addition to the standard IP protocol to include the VPN capability for the connection.

- PPTP (Point-to-Point-Tunneling-Protocol) – this protocol secures the data transfer from a VPN client to the network server via IP network. PPTP uses standard Point-to-Point protocol, but at the same time supports VPN. PPTP does not support the encryption of data. It is especially popular on Windows computers, because it is included by default in the OS. [10] PPTP has two types of data, namely control messages and data packets. Data packets are used to transfer user data through the tunnel. Control messages maintain the VPN connection and are used for signaling and status queries between the server and VPN client.

- L2TP (Layer Two Tunneling Protocol) – similarly to PPTP, L2TP does not support the encryption of data. It can be used in conjunction with IPsec in order to create a secure network, so L2TP would be creating a tunnel and IPsec handling the encryption.

In order to create a VPN tunnel, specific software must be installed on the user’s device. There are a number of options to choose from such as Open VPN, Cisco VPN, Hola.

3.4 Private Browsing Mode

Private Browsing Mode (PBM) is one of the most simplistic yet increasingly popular way of protecting your privacy online. As of 2017, it is a feature of every major browser, such as Google Chrome, Firefox, Internet Explorer and it even found its way in the mobile OS browsers. The name differs slightly, with Chrome calling it “Incognito mode”, Firefox “Private Browsing” and “InPrivate Mode” in IE. Unlike Tor, I2P and VPN, Private Browsing Mode does not protect privacy the same way, as it will leave traces of your activity on the Internet to the service providers, websites or employers, if browsing from the working computer. The following is the description of PBM as indicated on the Mozilla Support website: “Private Browsing Mode allows to browse the Internet without saving any information about which sites and pages you’ve visited.” [3] As seen from that description, its main demographics are people who share the user of one computer and other devices and do not want to the other party to trace the websites visited. Another important goal of the PBM is to prevent local attackers from accessing the information about PBM actions on the user’s computer. [4] As the description is quite ambiguous as well, it’s not hard to see why many users have certain misconceptions about the extent of its functionality and possible wrong impression about the scope of security it offers.

3.4.1 PBM Principle of Work

Despite each browser using a different name, one can expect this technology to be the same on every browser: according to the description on the respective browsers website, it should leave no traces of the browsing session after its termination. [21] That includes browsing history, cookies, form data, cached web content and downloads. The last comes with its limitations, as the downloaded files will be stored on users computer, however the browser will keep no record of them. In simple terms, that would mean that the browser would act as if the browsing session didn’t happen, instead making it a completely isolated.

It is important to mention that in order to make this mode workable, cookies are being saved while the session is in progress. That means that if one is logged in a certain website and later accesses this webpage while in the same session, he would remain logged in. As PBM doesn’t support any additional encryption, your ISP can still see you browsing activity. [21]

3.5 Analysis of Privacy Protection Methods

Tor has no traffic encryption because it can be tracked after leaving the exit relay. [12] This method hides user’s IP address which provides anonymity on the web. It can also be used to manipulate a geo-location, but users have to do a re-connection a number of times until the suitable country is reached. [13] It is free and easy to install because users simply have to download the software from the official webpage and no additional settings are required. Tor is sometimes perceived to be hard-to-use but after installing, it comes in a standard browser form much resembling Firefox and is normally used just like any other browser. Because of its structure, the speed is not great. It also has a very large user base and community with additional tutorials and discussions readily available online. Because the list of the relays is public, ISPs can also detect that you're using Tor and deny you the access to a certain website – one would have to use Bridge relays to get around that.

I2P can be rightfully considered to be for more advanced users, which also makes it the least popular. I2P does not let you browse the 'normal' web anonymously – it is not designed to do so. Instead, the anonymity can only be achieved when a website is hosted on the I2P network. It is easy to install but hard to use. Its current user-base is mostly advanced users. The user must also have a specific .i2p address of a specific webpage he is trying to reach, which is quite inconvenient and makes it hard to navigate inside. [1] It's not easy to configure as well due to a lot of settings involved; even though it supports P2P, it must also use specific torrent files, so the mainstream torrent trackers such as PirateBay will not work with it. The users are also limited to the maximum speed of a single hop in a single tunnel – if one hop has the maximum speed of 5kbps, the whole tunnel is likewise limited to that speed. [14] In terms of security, I2P technology with its combination of garlic routing, multilayer encryption and its random padding on data packets makes the I2P traffic extremely secure.

VPN encrypts traffic and hides user's IP address, which provides high level of anonymity on the web. The main advantage of VPN is how easy it is to manipulate user's location. Unlike Tor, this can be done in swiftly and without any difficulties and users also have the ability to choose any location from the VPN server list, instead of relogging into the system until the desired country appears. It is the only method in the list which costs money, with the prices averaging on 10USD/month for high-bandwidth service. [16] It must be said that VPN can technically be used for free, but it either will be a trial version of it, or the bandwidth and server list will be very limited. Its disadvantages are that logs of user's activity can be kept by the VPN service provider (and sometimes it is mandatory to keep them by law and to provide them to the law enforcement on request, which can compromise the user). [15] Similarly to Tor, some web portals can detect that VPN is used and block the access to its contents; such is, for example, the case of Netflix. [17]

The main advantages of PBM are simplicity to set up and use because it is included in the most popular browsers by default. According to the description, it also cleans all the history from the browser and all logs from the device after the session is over. [3] [21] PBM does not provide anonymity online because it does not hide user's IP nor encrypts traffic; PBM does not provide any location spoofing capabilities. User's information is available to ISP and visited websites. PBM places no limits on the bandwidth, therefore users can use the full potential of their internet speed.

As mentioned in the beginning, below is the table that reflects all the findings in this Chapter. This table was made by the author of the present paper based on the information collected from the reviewed literature as well as the underlying principle of work of each privacy-protection method overviewed above. The criteria for this table were chosen based on the most relevant requirements of this pieces of software along with the criteria that would demonstrate the strengths and weaknesses of each one.

Table 1 Comparison of Privacy Protection Methods

Criteria	**Tor**	**I2P**	**VPN**	**PBM**
Traffic encrypted	🟥	🟩	🟩	🟥
Hides IP address	🟩	🟩	🟩	🟥
Location spoofing	🟩	🟥	🟩	🟥
Activity logs are not saved on computer	🟩	🟥	🟥	🟩
Easy set up	🟩	🟥	🟩	🟩
Easy to use	🟩	🟥	🟩	🟩
Freeware	🟩	🟩	🟥	🟩
Additional software not needed	🟥	🟥	🟥	🟩
Cannot be blocked	🟥	🟩	🟥	🟩
High bandwidth	🟥	🟥	🟩	🟩
Information is hidden from ISP	🟩	🟩	🟩	🟥
P2P friendly	🟥	🟩	🟩	🟥
Hard to attack	🟩	🟩	🟩	🟥
Big community	🟩	🟥	🟩	🟩
Protects traffic outside browser	🟥	🟩	🟩	🟥
Logs are hidden from service provider	🟩	🟩	🟥	🟥

4 Private Browsing Mode Testing

A technical experiment is conducted in this work in order to determine whether PBM ‘works as advertised’ and how secure it is as a method of privacy protection. Another goal of this is to find out and outline the difference of PBM across different browsers.

The following experiment is carried out to find out whether the data and actions while being in PBM are stored in the computer memory. If the information is found, the definition of the PBM given by the developer might be put under question, since the information must not be reflected anywhere in the users’ computer, not only in the respective browser’s history. If private information while in PBM can be found in the RAM, the effectiveness of the same is debatable.

4.1 Methodology

A method called memory forensics will be used in order to find residual traces of the surfing activities. Memory forensics method is used in order to first extract and then to examine the computer’s memory (RAM). Given the right circumstances and proper legal procedure, it could produce evidence that is admissible in the court of law in criminal investigations. [44] As the computer functions register in RAM, it is a perfect way to extract useful information about the system and users’ actions in it. Depending on the RAM size and type, each action often exists for a long time after it has been done. Many types of data exist only in RAM, such as disk encryption keys, memory-resident injected code fragments, chat messages, unencrypted e-mail messages and Internet history records.

In the present research, the tests were performed on different Internet browsers. Namely, the following software was used:

Internet browsers:

- Google Chrome, version 57.0.2987.133
- Internet Explorer, version 11.1066.14393.0

- Mozilla Firefox, version 52.0.2
- Microsoft Edge, version 38.14393.1066.0

As Safari browser is not available for Windows, it was not included in this testing.

Operating Systems:

- Microsoft Windows 10 Home, 64-bit

First of all, the RAM had to be fully erased to a clean state. The most common method of clearing out the RAM is simply unplugging the computer from the power source for a couple of minutes; that was done in the beginning of the experiment to ensure the clarity of the results.

Then, various actions of similar nature were performed in every Internet Browsers concerned. Each of the action performed will be presented later in this Chapter. Each browser was tested separately and subsequently.. The memory was likewise cleared after each session to make sure that no results between each browser intertwined in any way.

The first step is to enable PBM. After that, the following actions were performed:

1. Google search of a particular information
2. Selecting a website from the list of results
3. Browsing the selected website, accessing random pages on the website
4. Accessing a pre-selected URL
5. Browsing the selected website, accessing random pages on the website
6. Creating an account by filling a registration form on popular shopping website https://www.shopspring.com/
7. Adding a random product to the shopping cart
8. Filling out shipping information by filling a form

9. Closing the PBM window

In order to analyze the RAM, the memory dump had to be created. That was accomplished using *AccessData FTK Imager 3.4.0.1*, which a software that could be used for Memory forensics. For the present work, a complete memory dump was captured using that software. The output file was 9,49 GB, which amounts to a complete memory dump to ensure the full picture. The memory dump had a “.mem” extension and was extracted to a designated folder.

After that, a separate piece of software named *HxD 1.7.7.0* was used. *HxD* is a hex editor that could be used, *inter alia*, to decipher the memory dump generated. With *HxD*, the author could search through the output file to find the desired information, or parts of the same. With *HxD* the memory dump was ‘translated’ into ASCII encoding standard, which made it readable. The general premise is to attempt to find the data in this memory dump that could contain traces of the actions performed in the PBM after the session has been terminated.

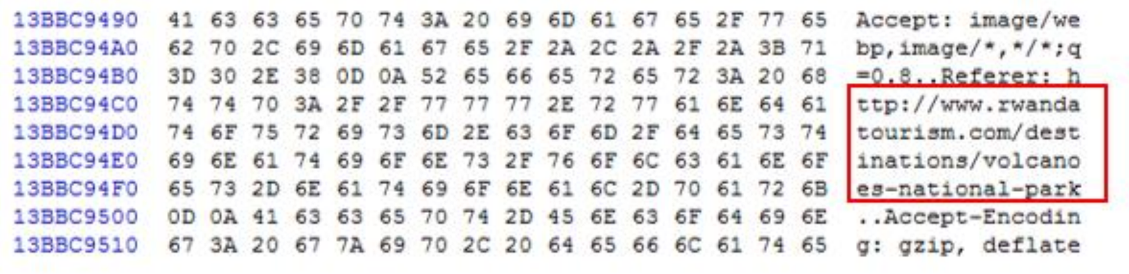
4.2 Google Chrome

The first browser subjected to the PBM testing was Google Chrome. Table 2 indicates the summary of the actions performed while in PBM session with exact URLs and user information.

Table 2 Google Chrome experiment data

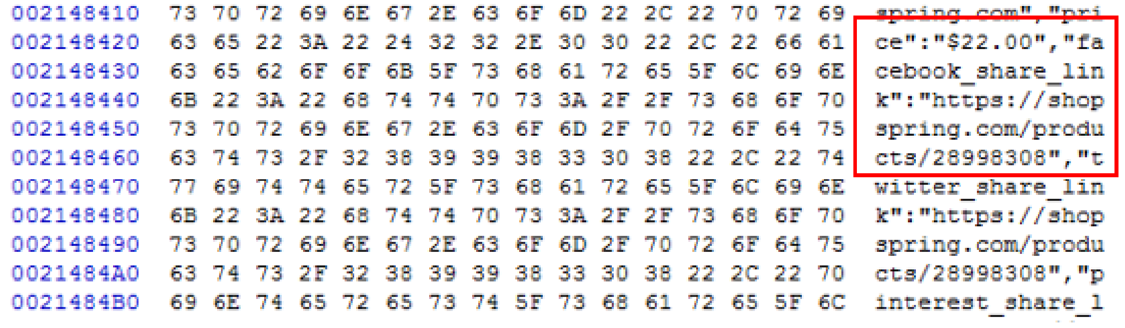
Google search	Rwanda sightseeings
First webpage	Rwandatourism.com
Second webpage	https://en.wikipedia.org/wiki/Boeing_747
Name	Zinzin
Surname	Buffetce
E-Mail	Geoeiebei897@rambler.ru
Password	Spehrbir8

When the session was finished, the RAM was extracted and opened in *Hxd*. Upon searching for the keywords above, the information that was revealed is shown in Figure 5-8.



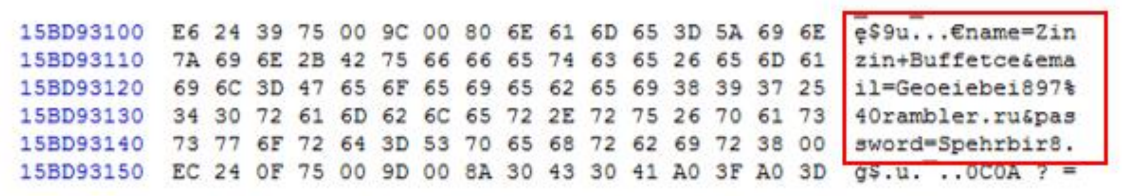
```
13BBC9490  41 63 63 65 70 74 3A 20 69 6D 61 67 65 2F 77 65  Accept: image/we
13BBC94A0  62 70 2C 69 6D 61 67 65 2F 2A 2C 2A 2F 2A 3B 71  bp,image/*,*/*;q
13BBC94B0  3D 30 2E 38 0D 0A 52 65 66 65 72 65 72 3A 20 68  =0.8..Referer: h
13BBC94C0  74 74 70 3A 2F 2F 77 77 77 2E 72 77 61 6E 64 61  ttp://www.rwanda
13BBC94D0  74 6F 75 72 69 73 6D 2E 63 6F 6D 2F 64 65 73 74  tourism.com/dest
13BBC94E0  69 6E 61 74 69 6F 6E 73 2F 76 6F 6C 63 61 6E 6F  inations/volcano
13BBC94F0  65 73 2D 6E 61 74 69 6F 6E 61 6C 2D 70 61 72 6B  es-national-park
13BBC9500  0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E  ..Accept-Encodin
13BBC9510  67 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65  g: gzip, deflate
```

Figure 5 Google Chrome first full URL found



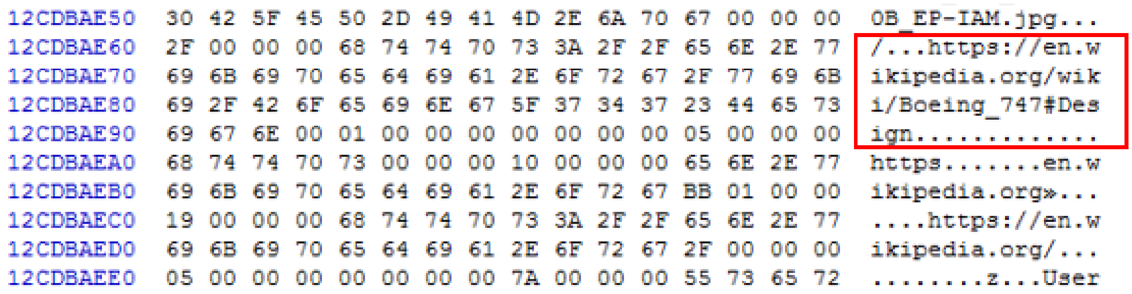
```
002148410  73 70 72 69 6E 67 2E 63 6F 6D 22 2C 22 70 72 69  spring.com","pri
002148420  63 65 22 3A 22 24 32 32 2E 30 30 22 2C 22 66 61  ce":"$22.00","fa
002148430  63 65 62 6F 6F 6B 5F 73 68 61 72 65 5F 6C 69 6E  cebook_share_lin
002148440  6B 22 3A 22 68 74 74 70 73 3A 2F 2F 73 68 6F 70  k":"https://shop
002148450  73 70 72 69 6E 67 2E 63 6F 6D 2F 70 72 6F 64 75  spring.com/produ
002148460  63 74 73 2F 32 38 39 39 38 33 30 38 22 2C 22 74  cts/28998308","t
002148470  77 69 74 74 65 72 5F 73 68 61 72 65 5F 6C 69 6E  witter_share_lin
002148480  6B 22 3A 22 68 74 74 70 73 3A 2F 2F 73 68 6F 70  k":"https://shop
002148490  73 70 72 69 6E 67 2E 63 6F 6D 2F 70 72 6F 64 75  spring.com/produ
0021484A0  63 74 73 2F 32 38 39 39 38 33 30 38 22 2C 22 70  cts/28998308","p
0021484B0  69 6E 74 65 72 65 73 74 5F 73 68 61 72 65 5F 6C  interest_share_l
```

Figure 6 Google Chrome product details found



```
15BD93100  E6 24 39 75 00 9C 00 80 6E 61 6D 65 3D 5A 69 6E  ę$9u...€name=Zin
15BD93110  7A 69 6E 2B 42 75 66 66 65 74 63 65 26 65 6D 61  zin+Buffetce&ema
15BD93120  69 6C 3D 47 65 6F 65 69 65 62 65 69 38 39 37 25  il=Geoeiebei897%
15BD93130  34 30 72 61 6D 62 6C 65 72 2E 72 75 26 70 61 73  40rambler.ru&pas
15BD93140  73 77 6F 72 64 3D 53 70 65 68 72 62 69 72 38 00  sword=Spehrbir8.
15BD93150  EC 24 0F 75 00 9D 00 8A 30 43 30 41 A0 3F A0 3D  g$.u. ..0C0A ? =
```

Figure 7 Google Chrome username, email and password found



```
12CDBAE50  30 42 5F 45 50 2D 49 41 4D 2E 6A 70 67 00 00 00  0B_EP-IAM.jpg...
12CDBAE60  2F 00 00 00 68 74 74 70 73 3A 2F 2F 65 6E 2E 77  /...https://en.w
12CDBAE70  69 6B 69 70 65 64 69 61 2E 6F 72 67 2F 77 69 6B  ikipedia.org/wik
12CDBAE80  69 2F 42 6F 65 69 6E 67 5F 37 34 37 23 44 65 73  i/Boeing_747#Des
12CDBAE90  69 67 6E 00 01 00 00 00 00 00 00 00 05 00 00 00  ign.............
12CDBAEA0  68 74 74 70 73 00 00 00 10 00 00 00 65 6E 2E 77  https.......en.w
12CDBAEB0  69 6B 69 70 65 64 69 61 2E 6F 72 67 BB 01 00 00  ikipedia.org»...
12CDBAEC0  19 00 00 00 68 74 74 70 73 3A 2F 2F 65 6E 2E 77  ....https://en.w
12CDBAED0  69 6B 69 70 65 64 69 61 2E 6F 72 67 2F 00 00 00  ikipedia.org/...
12CDBAEE0  05 00 00 00 00 00 00 00 7A 00 00 00 55 73 65 72  ........z...User
```

Figure 8 Google Chrome second full URL found

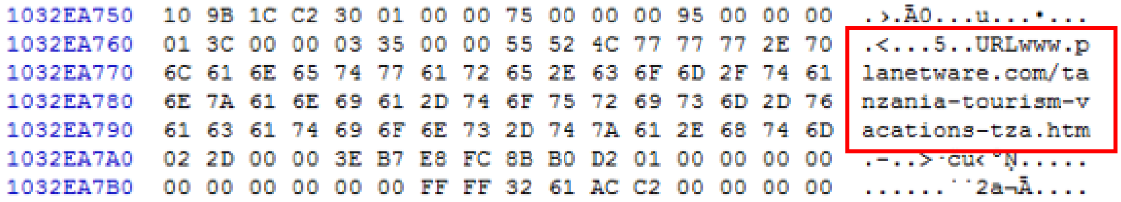
4.3 Mozilla Firefox

After the Chrome session, the RAM was completely wiped out and testing continued in the Firefox Browser. As mentioned in the beginning of this Chapter, the information changes for each browser to ensure the full clarity of the results. Table 3 indicates the data used for the Firefox's part of the testing.

Table 3 Mozilla Firefox experiment data

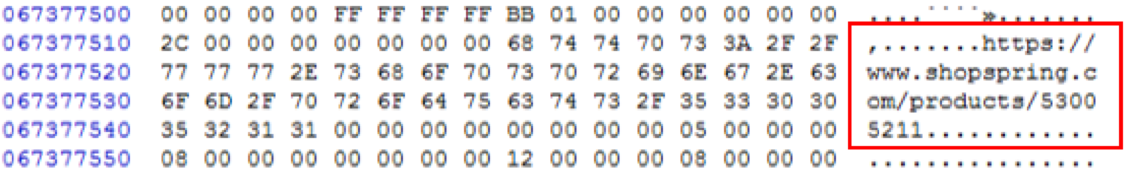
Google search	Tanzania sightseeing
First webpage	planetware.com
Second webpage	http://www.nationalgeographic.com/
Name	Dundun
Surname	Bigby
E-Mail	uqb@itmtx.com
Password	Ahrtui42

On Figure 9-11 the information that was found is indicated.



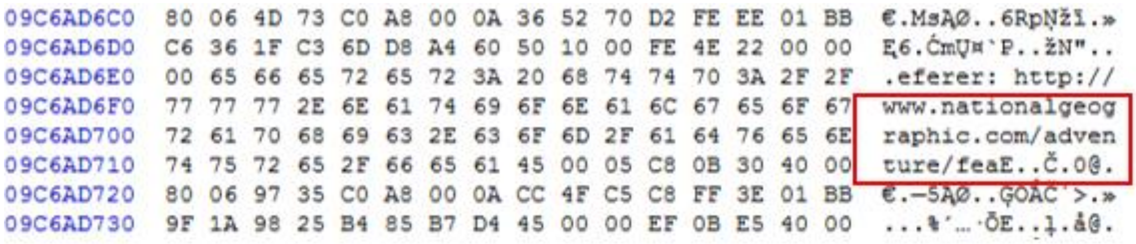
```
1032EA750  10 9B 1C C2 30 01 00 00 75 00 00 00 95 00 00 00  .›.Â0...u...•...
1032EA760  01 3C 00 00 03 35 00 00 55 52 4C 77 77 77 2E 70  .<...5..URLwww.p
1032EA770  6C 61 6E 65 74 77 61 72 65 2E 63 6F 6D 2F 74 61  lanetware.com/ta
1032EA780  6E 7A 61 6E 69 61 2D 74 6F 75 72 69 73 6D 2D 76  nzania-tourism-v
1032EA790  61 63 61 74 69 6F 6E 73 2D 74 7A 61 2E 68 74 6D  acations-tza.htm
1032EA7A0  02 2D 00 00 3E B7 E8 FC 8B B0 D2 01 00 00 00 00  .-..>·èü‹°Ò.....
1032EA7B0  00 00 00 00 00 00 FF FF 32 61 AC C2 00 00 00 00  ......ÿÿ2a¬Â....
```

Figure 9 Mozilla Firefox first full URL found



```
067377500  00 00 00 00 FF FF FF FF BB 01 00 00 00 00 00 00  ....ÿÿÿÿ».......
067377510  2C 00 00 00 00 00 00 00 68 74 74 70 73 3A 2F 2F  ,.......https://
067377520  77 77 77 2E 73 68 6F 70 73 70 72 69 6E 67 2E 63  www.shopspring.c
067377530  6F 6D 2F 70 72 6F 64 75 63 74 73 2F 35 33 30 30  om/products/5300
067377540  35 32 31 31 00 00 00 00 00 00 00 00 05 00 00 00  5211............
067377550  08 00 00 00 00 00 00 00 12 00 00 00 08 00 00 00  ................
```

Figure 10 Mozilla Firefox product details found



```
09C6AD6C0  80 06 4D 73 C0 A8 00 0A 36 52 70 D2 FE EE 01 BB  €.MsĄØ..6RpŅžî.»
09C6AD6D0  C6 36 1F C3 6D D8 A4 60 50 10 00 FE 4E 22 00 00  Ę6.ĆmŲ¤`P..žN"..
09C6AD6E0  00 65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F  .eferer: http://
09C6AD6F0  77 77 77 2E 6E 61 74 69 6F 6E 61 6C 67 65 6F 67  www.nationalgeog
09C6AD700  72 61 70 68 69 63 2E 63 6F 6D 2F 61 64 76 65 6E  raphic.com/adven
09C6AD710  74 75 72 65 2F 66 65 61 45 00 05 C8 0B 30 40 00  ture/feaE..Č.0@.
09C6AD720  80 06 97 35 C0 A8 00 0A CC 4F C5 C8 FF 3E 01 BB  €.—5ĄØ..ĢOÅČ˙>.»
09C6AD730  9F 1A 98 25 B4 85 B7 D4 45 00 00 EF 0B E5 40 00  ...‰´…·ŌE..ļ.å@.
```

Figure 11 Mozilla Firefox second full URL found

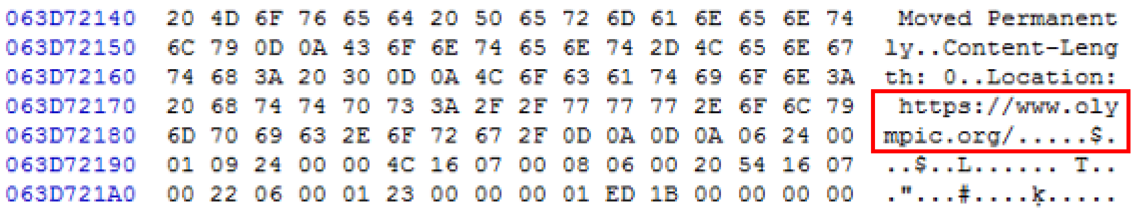
4.4 Internet Explorer

Table 4 indicates the data used for the IE part of the experiment.

Table 4 Internet Explorer experiment data

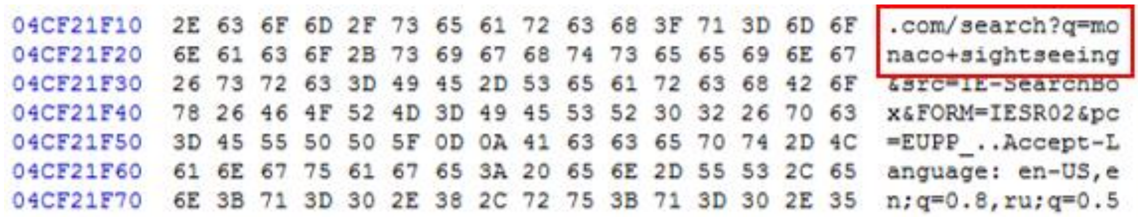
Google search	Monaco sightseeing
First webpage	lonelyplanet.com
Second webpage	https://www.olympic.org/
Name	Berkinson
Surname	Malzingo
E-Mail	bsb@reddit.usa.cc
Password	587Asdgw

The revealed information is shown in Figure 12-13.



```
063D72140  20 4D 6F 76 65 64 20 50 65 72 6D 61 6E 65 6E 74   Moved Permanent
063D72150  6C 79 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67  ly..Content-Leng
063D72160  74 68 3A 20 30 0D 0A 4C 6F 63 61 74 69 6F 6E 3A  th: 0..Location:
063D72170  20 68 74 74 70 73 3A 2F 2F 77 77 77 2E 6F 6C 79   https://www.oly
063D72180  6D 70 69 63 2E 6F 72 67 2F 0D 0A 0D 0A 06 24 00  mpic.org/.....$.
063D72190  01 09 24 00 00 4C 16 07 00 08 06 00 20 54 16 07  ..$..L...... T..
063D721A0  00 22 06 00 01 23 00 00 00 01 ED 1B 00 00 00 00  ."...#....ķ.....
```

Figure 12 Internet Explorer second full URL found



```
04CF21F10  2E 63 6F 6D 2F 73 65 61 72 63 68 3F 71 3D 6D 6F  .com/search?q=mo
04CF21F20  6E 61 63 6F 2B 73 69 67 68 74 73 65 65 69 6E 67  naco+sightseeing
04CF21F30  26 73 72 63 3D 49 45 2D 53 65 61 72 63 68 42 6F  &src=IE-SearchBo
04CF21F40  78 26 46 4F 52 4D 3D 49 45 53 52 30 32 26 70 63  x&FORM=IESR02&pc
04CF21F50  3D 45 55 50 50 5F 0D 0A 41 63 63 65 70 74 2D 4C  =EUPP_..Accept-L
04CF21F60  61 6E 67 75 61 67 65 3A 20 65 6E 2D 55 53 2C 65  anguage: en-US,e
04CF21F70  6E 3B 71 3D 30 2E 38 2C 72 75 3B 71 3D 30 2E 35  n;q=0.8,ru;q=0.5
```

Figure 13 Internet Explorer search result found

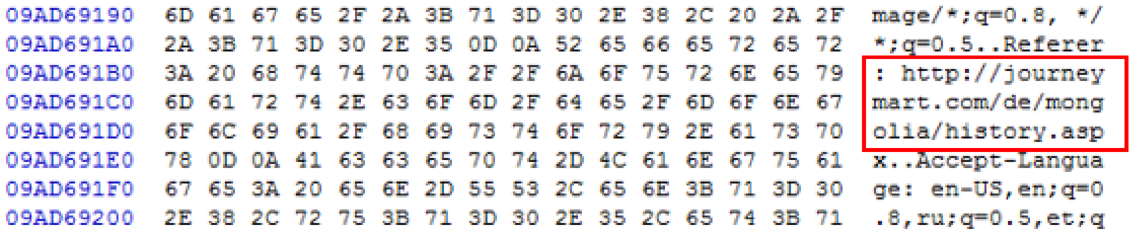
4.5 Microsoft Edge

Table 5 indicates the data used for Microsoft Edge.

Table 5 Microsoft Edge experiment data

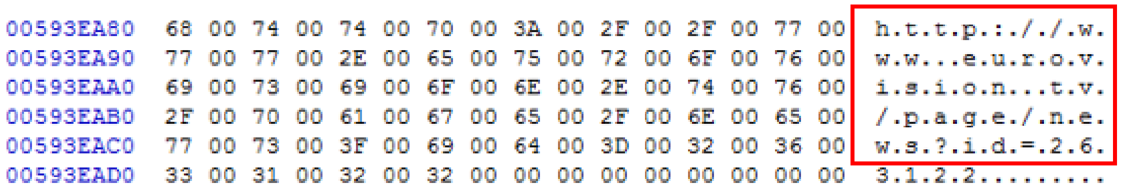
Google search	Mongolia sightseeings
First webpage	journeymart.com
Second webpage	https://eurovision.tv/
Name	Brendazra
Surname	Oliskovecno
E-Mail	wqs@bst-72.com
Password	Werghk90

Information revealed in Microsoft Edge is indicated in Figure 14-16.



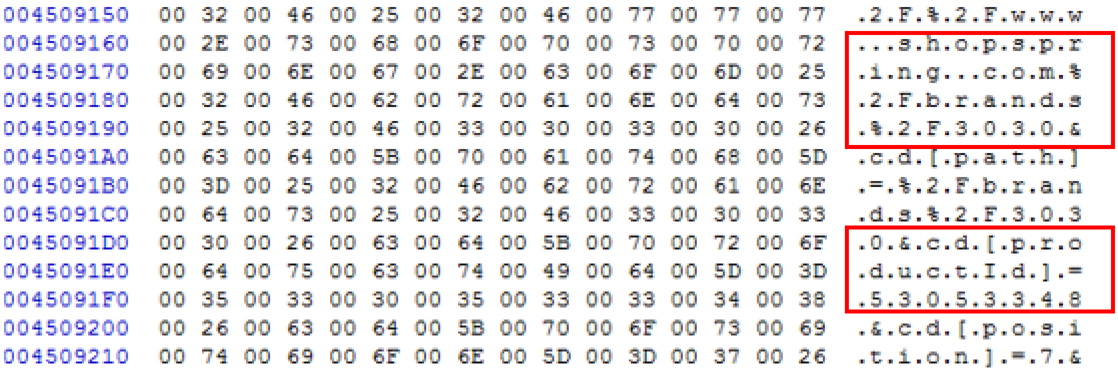
```
09AD69190  6D 61 67 65 2F 2A 3B 71 3D 30 2E 38 2C 20 2A 2F  mage/*;q=0.8, */
09AD691A0  2A 3B 71 3D 30 2E 35 0D 0A 52 65 66 65 72 65 72  *;q=0.5..Referer
09AD691B0  3A 20 68 74 74 70 3A 2F 2F 6A 6F 75 72 6E 65 79  : http://journey
09AD691C0  6D 61 72 74 2E 63 6F 6D 2F 64 65 2F 6D 6F 6E 67  mart.com/de/mong
09AD691D0  6F 6C 69 61 2F 68 69 73 74 6F 72 79 2E 61 73 70  olia/history.asp
09AD691E0  78 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61  x..Accept-Langua
09AD691F0  67 65 3A 20 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30  ge: en-US,en;q=0
09AD69200  2E 38 2C 72 75 3B 71 3D 30 2E 35 2C 65 74 3B 71  .8,ru;q=0.5,et;q
```

Figure 14 Microsoft Edge first full URL found



```
00593EA80  68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 77 00  h.t.t.p.:././.w.
00593EA90  77 00 77 00 2E 00 65 00 75 00 72 00 6F 00 76 00  w.w...e.u.r.o.v.
00593EAA0  69 00 73 00 69 00 6F 00 6E 00 2E 00 74 00 76 00  i.s.i.o.n...t.v.
00593EAB0  2F 00 70 00 61 00 67 00 65 00 2F 00 6E 00 65 00  /.p.a.g.e./.n.e.
00593EAC0  77 00 73 00 3F 00 69 00 64 00 3D 00 32 00 36 00  w.s.?.i.d.=.2.6.
00593EAD0  33 00 31 00 32 00 32 00 00 00 00 00 00 00 00 00  3.1.2.2.........
```

Figure 15 Microsoft Edge second full URL found



```
004509150  00 32 00 46 00 25 00 32 00 46 00 77 00 77 00 77  .2.F.%.2.F.w.w.w
004509160  00 2E 00 73 00 68 00 6F 00 70 00 73 00 70 00 72  ...s.h.o.p.s.p.r
004509170  00 69 00 6E 00 67 00 2E 00 63 00 6F 00 6D 00 25  .i.n.g...c.o.m.%
004509180  00 32 00 46 00 62 00 72 00 61 00 6E 00 64 00 73  .2.F.b.r.a.n.d.s
004509190  00 25 00 32 00 46 00 33 00 30 00 33 00 30 00 26  .%.2.F.3.0.3.0.&
0045091A0  00 63 00 64 00 5B 00 70 00 61 00 74 00 68 00 5D  .c.d.[.p.a.t.h.]
0045091B0  00 3D 00 25 00 32 00 46 00 62 00 72 00 61 00 6E  .=.%.2.F.b.r.a.n
0045091C0  00 64 00 73 00 25 00 32 00 46 00 33 00 30 00 33  .d.s.%.2.F.3.0.3
0045091D0  00 30 00 26 00 63 00 64 00 5B 00 70 00 72 00 6F  .0.&.c.d.[.p.r.o
0045091E0  00 64 00 75 00 63 00 74 00 49 00 64 00 5D 00 3D  .d.u.c.t.I.d.].=
0045091F0  00 35 00 33 00 30 00 35 00 33 00 33 00 34 00 38  .5.3.0.5.3.3.4.8
004509200  00 26 00 63 00 64 00 5B 00 70 00 6F 00 73 00 69  .&.c.d.[.p.o.s.i
004509210  00 74 00 69 00 6F 00 6E 00 5D 00 3D 00 37 00 26  .t.i.o.n.].=.7.&
```

Figure 16 Microsoft Edge product details found

4.6 BPM Testing Analysis

First of all, it is important to notice that retrievable artifacts about the browsing session were found in all of the browsers tested. The type and the amount of data varied slightly among browsers, but most of the browsers were on comparable level – all of them revealed crucial information about the browsing session. If the goal of this work were to find a winner in terms of PBM that would be indeed quite difficult, as no browser was significantly better than others and all of them revealed browsing data when subjected to memory analysis.

The most surprising result came from Google Chrome. Despite being the most used browser of all [42], it was the only browser that revealed completed form fields data, thus indicating both the users' email address and password. It also revealed not just the entered URL, but some information from the webpage itself, such as price of the ordered item; this information was not found on any other browser.

Another interesting feature is shown by Microsoft Edge. Upon examining the memory dump, it was found that some data was represented differently from others – namely that there were dots (or 00 in Hex) between every symbol. To the Author this made the forensics procedure more difficult. Other browsers were likewise checked for the similar features, however it was revealed that only data that came from Microsoft Edge has such format.

By this research, it follows that PBM does not delete the complete information about the browsing activities after the session has been terminated thus resulting in possible privacy leakage. In fact, the crucial information is still available to anyone who can access the RAM on user’s computer. This could be anyone who, for examples, shares the computer or the retrieved data from the RAM could be collected by the police forces to collect information about suspect’s activities online. [41]

This experiment gives grounds to contradict the description of PBM on the browsers’ webpages, which claimed that all data is erased after finishing session. [3] [21] This has certain implications. First of all, users who use PBM might be misconceptioned about the PBM functions and this could affect their perception of security online. Secondly, as mentioned in the Chapter 3, other methods of privacy protection may use PBM in order to strenghten their own security (such as PBM actually being a security feature of Tor browser). Therefore, If PBM is not as secure as it claims to be, it also could compromise the security level of other methods of protection that rely on it.

5 Survey

The final part of this work is a survey, which was conducted using SurveyMonkey online software and questionnaire tool. The main purpose of this survey is to determine a significance of the problem and to attract more attention to the privacy on the Internet. Also, it is important to figure out current situation, specifically how much users care about privacy today and what measures are taken to hold private data in safety. This Chapter is divided into two subchapters: one will describe the contents of the survey in details. The analysis of the survey will be presented in the second chapter, along with the pie charts summarizing the results.

5.1 Survey Content

Survey consists of 7 questions with answer options. Some questions allow choosing several options. [36] The questions were crafted in order to determine the understanding of the respondents with respect to the notion of privacy, to determine its importance in their lives and to see how the answers relate to the other parts of the present paper in terms of security and other aspects.

A total of 89 respondents took part in this survey. The majority of the participants are TUT students from different faculties. The survey was mainly disseminated on social networks and by the word of mouth. The results of the survey affirm the importance of internet privacy and necessity of this research.

The questionnaire is set out below:

1. **Which browser do you normally use?**
   Google Chrome
   Microsoft Edge
   Internet Explorer
   Safari
   Firefox
2. **Are you concerned about internet privacy?**

Yes

No

3. **Do you feel that your privacy is secure when you are browsing the web?**

   Yes

   No

   I have not thought about it

4. **Which methods of privacy protection do you know?**

   Private Browsing Mode

   Tor

   VPN

   I2P

   Neither of them

5. **Which methods do you use?**

   Private Browsing Mode

   Tor

   VPN

   I2P

   Neither of them

6. **How often do you clean browser history?**

   Every day

   Every week

   Every month

   Rarer than once a month

7. **What is the main reason you clean your history?**

   Privacy and security concerns

   Do not want friends/family to see my history (personal computer)

   Do not want employer to see my history (work computer)

5.2 Survey Analysis

Below are presented the diagrams summarizing the responses for each question. The diagrams (Figure 17-23) will be discussed later in this chapter in detail.

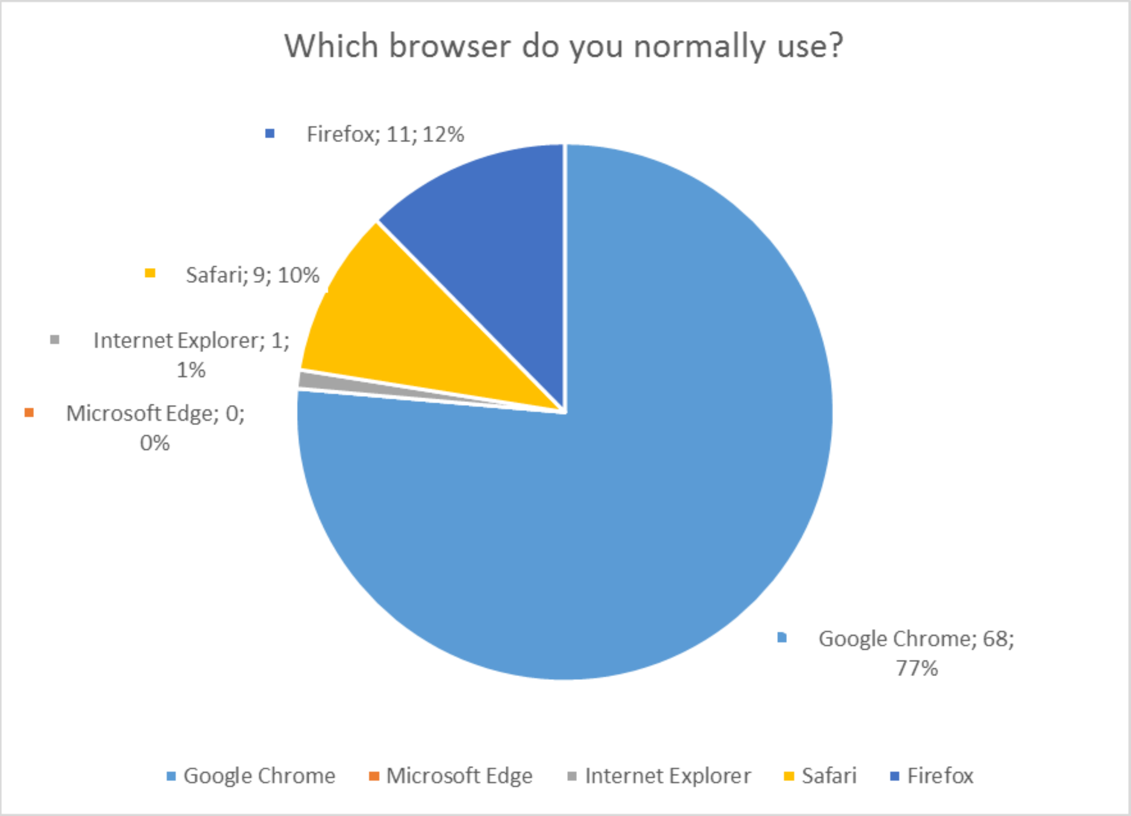


Figure 17 Survey question 1

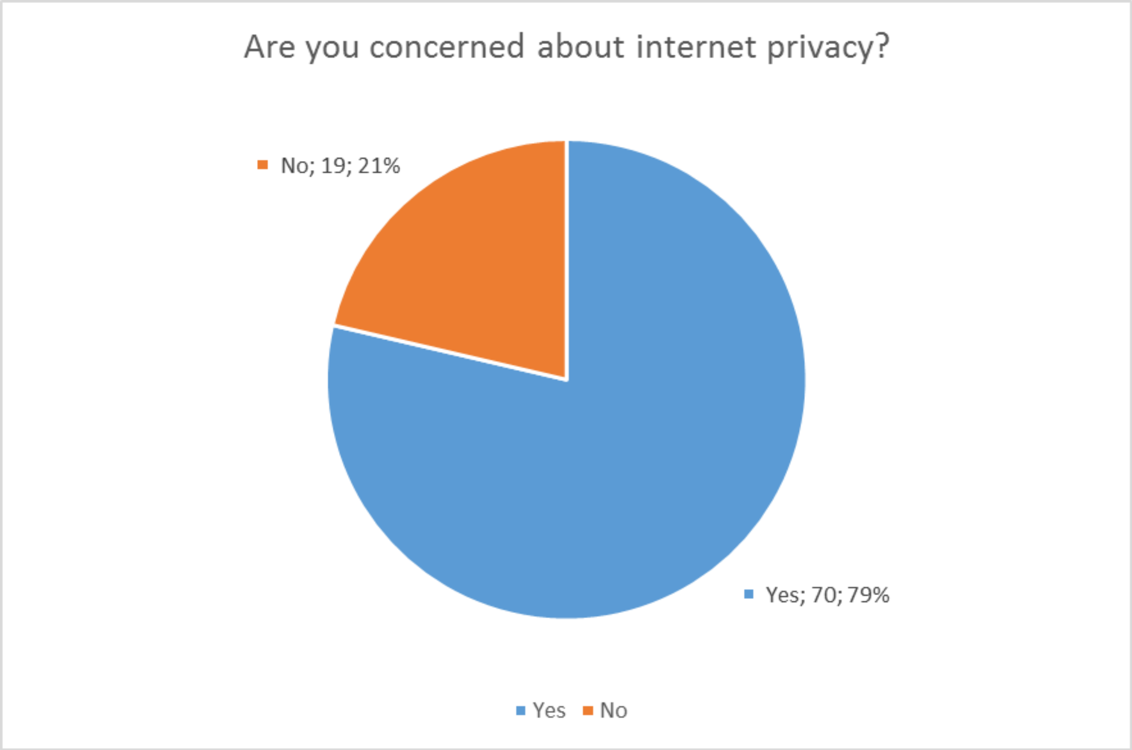


Figure 18 Survey question 2

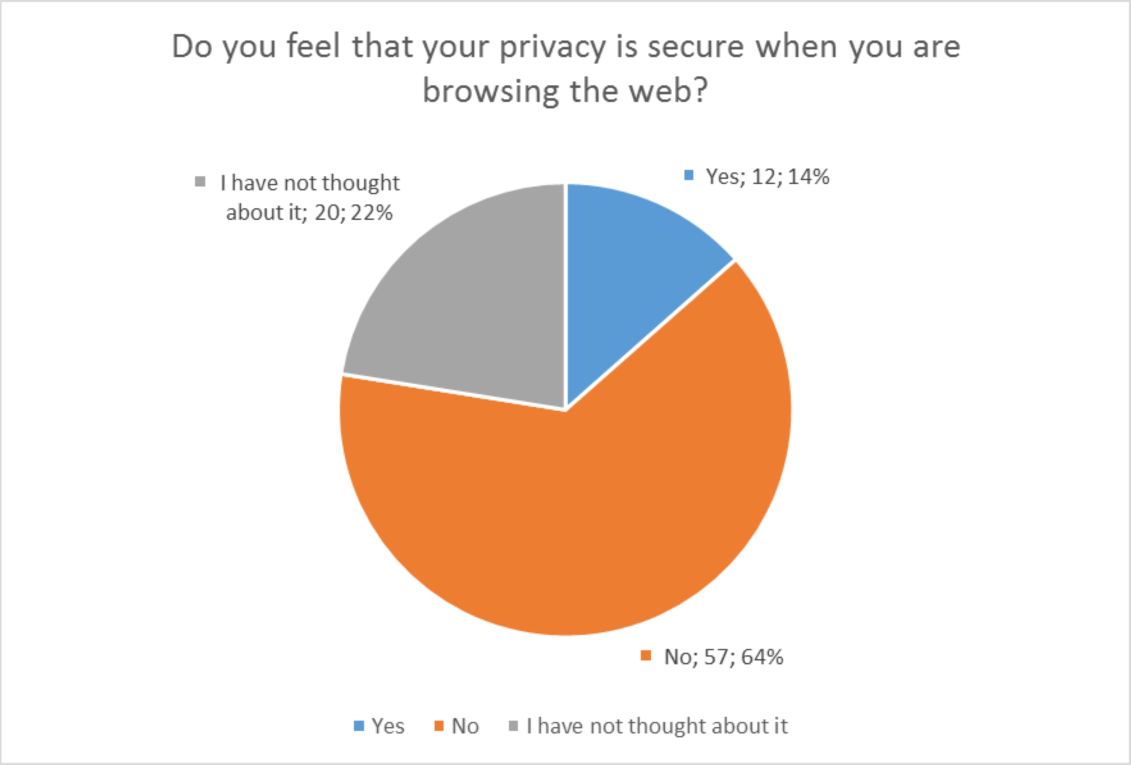


Figure 19 Survey question 3

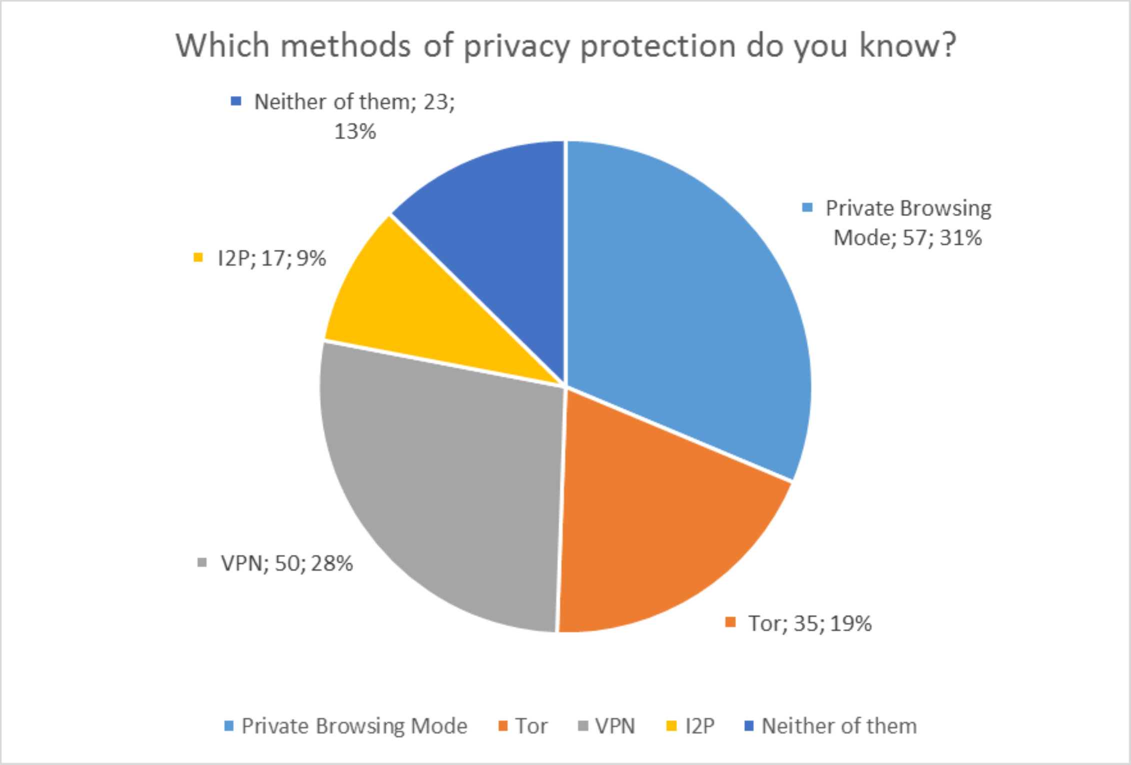


Figure 20 Survey question 4

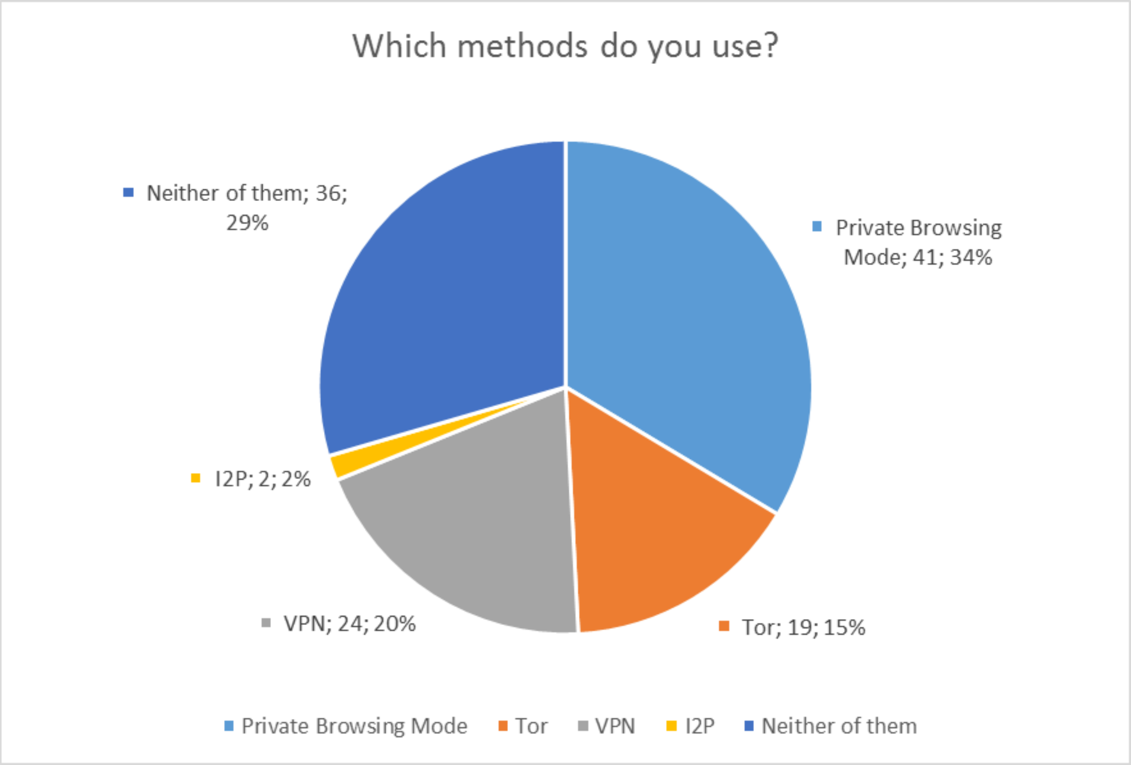


Figure 21 Survey question 5

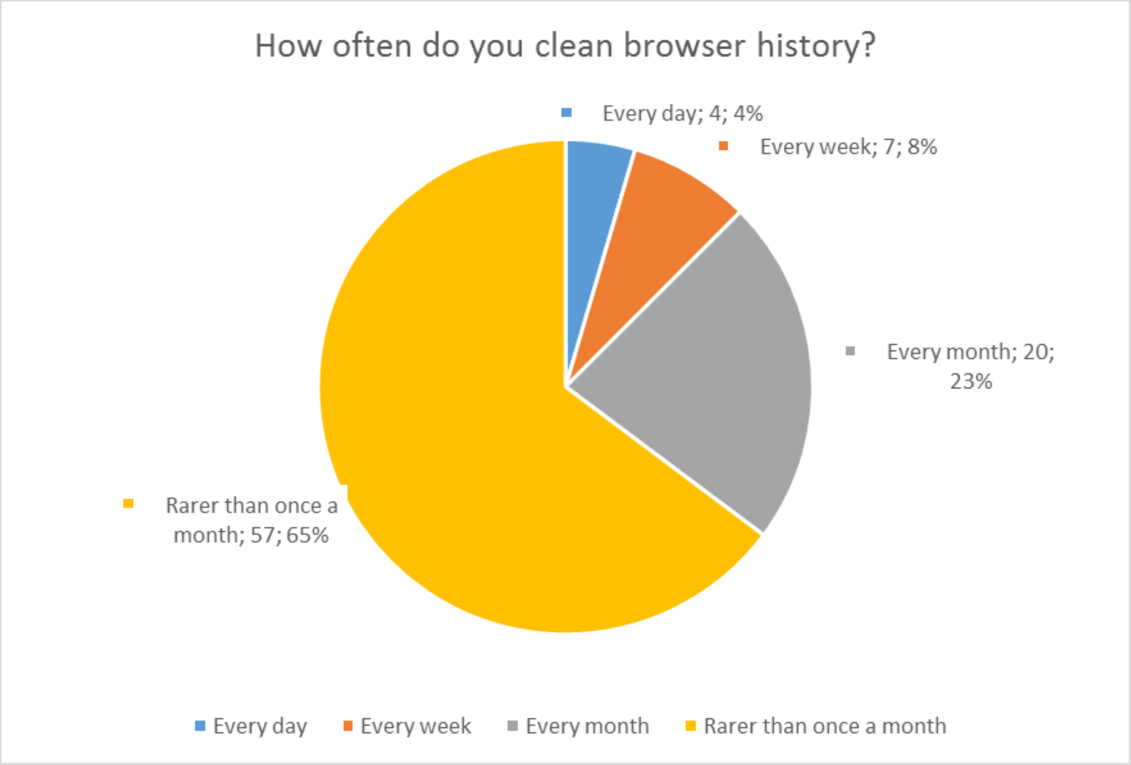


Figure 22 Survey question 6

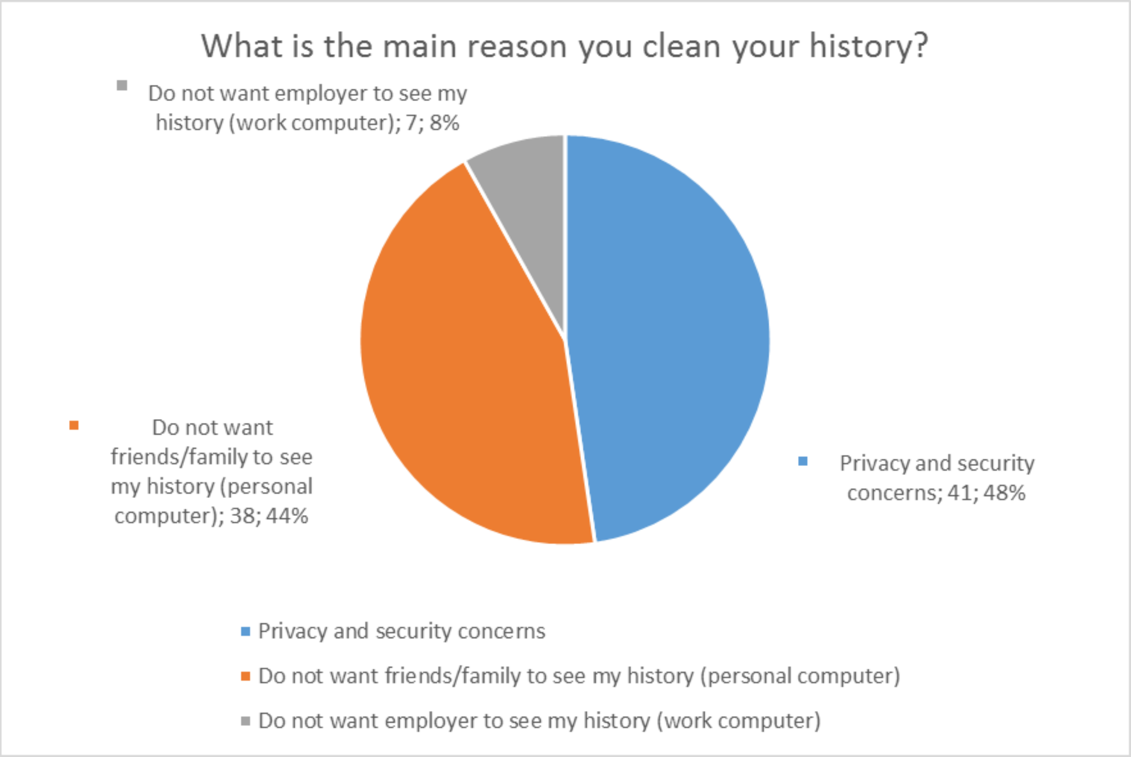


Figure 23 Survey question 7

The most popular privacy protection method is PBM - 64% of respondents know it and 46% use it regularly. That confirms the significance of the experiment described in detail in Chapter 4. Survey reveals that 30% do not use any privacy protection methods whatsoever. This is astonishing result, especially taking into consideration the fact that about 80% of respondents answered that they are concerned about internet privacy. The respondents noted that they do not feel secure while browsing the web as only 13% of them believe that their data is safe.

Another part of the survey consists of technical questions in order to get information about the preferences of Internet browsers people normally use. This information is required in order to determine the most favoured browser and to further see in the experiment how it bodes against the others in terms of PBM security features. According to the survey, Google Chrome is a favoured choice of browser - 76%; Firefox came second with a big gap; only 12% use it.

The survey also includes questions about browsing history, to be informed of how often people clean their history and for what reasons they do this. 65% of the responses indicated that people clean their browsing history rarer the once a month. As can be seen from the last chart, users clean their history because of privacy and security concerns and to prevent access to the information from people with whom they share devices.

To summarize, the majority of respondents answered that they are concerned about privacy on the Internet, however answers to other questions reveal that about 30% do not use any methods to protect their data and 65% clear their history rarer than once a month. That is astonishing results, because 80% answered that privacy is important for them. PBM, as expected, is the most important method of privacy protection online. To the uthor, that shows that while the majority of people value their privacy, not enough is done in order to ensure it.

6 Conclusion

The goal of this work was to analyze privacy protection methods on the subject of their strengths, weaknesses and differences in the methods of work. In order to achieve that, a comprehensive review was given for each one of them and then they were compared against each other based on literature review. To best summarize the review, Author presented a table which compared properties of each method to see how they fare against each other. It was established, that there is no go-to method for all scenarios; rather the best method of choice would depend on the preferences, goals and skill set of the user. It was further found that not a single method would make the user absolutely secure in terms of privacy protection online; this could only be achieved when using several privacy protection methods in combination. Of course, this protection does come at a price – each of the methods comes with its own downfalls, either in terms of speed or just convenience of use. Subsequently, when using several protection methods at the same time the inconvenience grows proportionally.

The second goal was to focus on one method of protection in particular – Private Browsing Mode, which is supposed to protect the user against local attacker, who could take control of the machine and its contents. It was found that important browsing artifacts could be recovered after the browsing session using memory forensics, which, assuming that the procedure itself was completed following the proper legal procedure, could be admissible as evidence in the court of law. [44] According to the results of the conducted research, it was revealed that Google Chrome revealed the most browsing information; other browsers showed relatively comparative results, but they all revealed various grades of information, such as URLs, website data, Google search results and, in the case of Google Chrome, even completed form field information that contained, *inter alia*, username and password of the user.

Essentially, it was established that memory forensics could, depending on the browser, completely or partially diminish the benefits of using Private Browsing Mode, despite the description of the service given. [3] [21] As such, PBM could be useful if one completely wipes off the RAM after the session – simply closing the browser window will not get rid of the artifacts and given the right tools, one could recover all the valuable information of the browsing session. Given the results, the PBM service description could be likewise improved to offer better account of its features to avoid giving users incorrect presumptions about the scope of the service.

The final part of the work consisted of the survey conducted by the Author. In total, 89 respondents took part in this survey. It was revealed that people are concerned about Internet privacy and most of the users use at least one method of protection on the regular basis; unsurprisingly, due to its ease of use, PBM was revealed to be the most popular choice among the respondents and Google Chrome took the number one spot as the most-user browser (despite if showing the worst result of all the browsers tested). Putting this together with the research, it can be said that not enough is done by the users in order to secure their privacy online, thus highlighting the importance of the present work.

In general, it could be safely said that both goals were accomplished successfully. The present work could be used both in terms of finding the right privacy protection method for a concerned user or to dispute the effectiveness of PBM. Based on this work and its findings, it can be said that in order to protect oneself online, one must go to great lengths in order to do so, both in terms of finding the right technology and sacrificing the convenience of browsing normally.

References

[1] K. Knibbs, "I2P: The Super-Anonymous Network That Silk Road Calls Home", *Gizmodo*, 2017. [Online]. Available: http://gizmodo.com/i2p-the-super-anonymous-network-that-silk-road-calls-h-1680940282. [Accessed: 10- Apr- 2017].

[2] H. Bidgoli, *Handbook of Information Security Volume 3*. Hoboken: John Wiley & Sons, 2006.

[3] "Private Browsing - Use Firefox without saving history", *Support.mozilla.org*, 2017. [Online]. Available: https://support.mozilla.org/t5/Protect-your-privacy/Private-Browsing-Use-Firefox-without-saving-history/ta-p/4473. [Accessed: 14- Apr- 2017].

[4] G. Aggarwal, E. Burzstein, C. Jackson and D. Boneh, *An Analysis of Private Browsing Modes in Modern Browsers*, 1st ed. .

[5] A. Westin and D. Solove, *Privacy and freedom*, 1st ed. 1967, p. 7.

[6] T. Wheeler, "Opinion | How the Republicans Sold Your Privacy to Internet Providers", *Nytimes.com*, 2017. [Online]. Available: https://www.nytimes.com/2017/03/29/opinion/how-the-republicans-sold-your-privacy-to-internet-providers.html?_r=0. [Accessed: 23- Apr- 2017].

[7] Business Insider Intelligence, "There will be 24 billion IoT devices installed on Earth by 2020", *Business Insider*, 2017. [Online]. Available: http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5. [Accessed: 23- Apr- 2017].

[8] "Gartner Says 8.4 Billion Connected", *Gartner.com*, 2017. [Online]. Available: http://www.gartner.com/newsroom/id/3598917. [Accessed: 23- Apr- 2017].

[9] A. Meola, "How the Internet of Things will affect security & privacy", *Business Insider*, 2017. [Online]. Available: http://www.businessinsider.com/internet-of-things-security-privacy-2016-8. [Accessed: 23- Apr- 2017].

[10] How PPTP makes Virtual Private Networks work", *Lifewire*, 2017. [Online]. Available: https://www.lifewire.com/pptp-point-to-point-tunneling-protocol-818182. [Accessed: 26- Apr- 2017].

[11] "Tor Exit Relays Mapped and Located | HackerTarget.com", *HackerTarget.com*, 2017. [Online]. Available: https://hackertarget.com/tor-exit-node-visualization/. [Accessed: 29- Apr- 2017].

[12] "VPN vs. Tor Comparison Chart - GreyCoder", *GreyCoder*, 2017. [Online]. Available: https://greycoder.com/tor-versus-vpn/. [Accessed: 29- Apr- 2017].

[13] D. Crawford, "Tor vs. VPN - BestVPN.com", *BestVPN.com*, 2017. [Online]. Available: https://www.bestvpn.com/blog/5888/tor-vs-vpn/. [Accessed: 29- Apr- 2017].

[14] "Performance - I2P", *Geti2p.net*, 2017. [Online]. Available: https://geti2p.net/en/about/performance. [Accessed: 29- Apr- 2017].

[15] P. Zaborszky, "Data retention and VPN logging in the United States - BestVPN.com", *BestVPN.com*, 2017. [Online]. Available: https://www.bestvpn.com/blog/5539/data-retention-and-vpn-logging-in-the-united-states/. [Accessed: 30- Apr- 2017].

[16] "Best VPN Services 2017 - Compare Reviews and Pricing", *Vpn-services.softwareinsider.com*, 2017. [Online]. Available: http://vpn-services.softwareinsider.com/. [Accessed: 30- Apr- 2017].

[17] "Evolving Proxy Detection as a Global Service", *Netflix Media Center*, 2017. [Online]. Available: https://media.netflix.com/en/company-blog/evolving-proxy-detection-as-a-global-service. [Accessed: 30- Apr- 2017].

[18] I. The Tor Project, "Tor Project: Overview", *Torproject.org*, 2017. [Online]. Available: https://www.torproject.org/about/overview.html.en. [Accessed: 01- May- 2017].

[19] "Tor at the Heart: Firefox | The Tor Blog", *Blog.torproject.org*, 2017. [Online]. Available: https://blog.torproject.org/blog/tor-heart-firefox. [Accessed: 01- May- 2017].

[20] "The Design and Implementation of the Tor Browser [DRAFT]", *Torproject.org*, 2017. [Online]. Available: https://www.torproject.org/projects/torbrowser/design/#disk-avoidance. [Accessed: 01- May- 2017].

[21] "Browse in private with Incognito mode - Computer - Chromebook Help", *Support.google.com*, 2017. [Online]. Available: https://support.google.com/chromebook/answer/95464?co=GENIE.Platform%3DDesktop&hl=en. [Accessed: 01- May- 2017].

[22] "Data Protection | Privacy International", *Privacyinternational.org*, 2017. [Online]. Available: https://www.privacyinternational.org/node/44. [Accessed: 03- May- 2017].

[23] M. Waschke, *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*, 1st ed. Apress, 2017, p. 207.

[24] S. Gutwirth, *Privacy and the information age*, 1st ed. Lanham, Md. [u.a.]: Rowman & Littlefield, 2002, pp. 33-35.

[25] F. Schoeman, *Philosophical dimensions of privacy*, 1st ed. Cambridge: Cambridge University Press, 1984, p. 209.

[26] B. Rössler, *The value of privacy*, 1st ed. [Place of publication not identified]: Polity Press, 2015, pp. 7-8.

[27] P. Bernal, *Internet privacy rights*, 1st ed. Cambridge: Cambridge University Press, 2014, p. 34.

[28] R. Amet, "Avaleht - eesti.ee", *Eesti.ee*, 2017. [Online]. Available: http://Eesti.ee. [Accessed: 30- Mar- 2017].

[29] J. Michael, *Privacy and human rights*, 1st ed. Aldershot: Darmouth, 1994.

[30] R. Giblin, *Code wars*, 1st ed. Northampton, Mass.: Edward Elgar Pub., 2011, pp. 92-94.

[31] O. Solon, "Here's how to protect your internet browsing data now that it's for sale", *the Guardian*, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/mar/30/privacy-protection-web-browsing-history-data-congress. [Accessed: 01- Apr- 2017].

[32] "Anger as US internet privacy law scrapped - BBC News", *BBC News*, 2017. [Online]. Available: http://www.bbc.com/news/technology-39427026. [Accessed: 01- Apr- 2017].

[33] *Performance of Tor*, 1st ed. Paul Buder, Daniel Heyne, and Martin Peter Stenzel, 2017, p. 2.

[34] M. Ligh, *Malware analyst's cookbook and dvd*, 1st ed. Indianapolis: Wiley, 2013.

[35] "A Bird’s Eye View on the I2P Anonymous File-sharing Environment", 2012. [Online]. Available: https://hal.inria.fr/hal-

00744919/PDF/A_Birda_s_Eye_View_on_the_I2P_Anonymous_0AFile-sharing_Environment_0A.pdf. [Accessed: 09- May- 2017].

[36] "Internet Privacy Survey", *Surveymonkey.com*, 2017. [Online]. Available: https://www.surveymonkey.com/r/N3YC3ZY. [Accessed: 09- May- 2017].

[37] U. Assembly, "A/RES/3/217 A - Universal Declaration of Human Rights - UN Documents: Gathering a body of global agreements", *Un-documents.net*, 1948. [Online]. Available: http://www.un-documents.net/a3r217a.htm. [Accessed: 09- May- 2017].

[38] U. Assembly, "A/RES/21/2200 - International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights - UN Documents: Gathering a body of global agreements", *Un-documents.net*, 1966. [Online]. Available: http://www.un-documents.net/a21r2200.htm. [Accessed: 09- May- 2017].

[39] H. Burkert, *Pricacy-data protection. Governance of Global Networks in the Light of Different Local Values*, 1st ed. [S.l.]: [s.n.], 2000, pp. 43-70.

[40] "The CEO's Guide to Securing the Internet of Things", 2015. [Online]. Available: https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf. [Accessed: 09- May- 2017].

[41] J. Oh, S. Lee and S. Lee, "Advanced evidence collection and analysis of web browser activity", Digital Investigation, vol. 8, pp. S62-S70, 2011, pp. 62-70

[42] "Google Chrome Is Now the Most Popular Web Browser", Gizmodo.com, 2016. [Online]. Available: http://gizmodo.com/google-chrome-is-now-the-most-popular-web-browser-1774266161. [Accessed: 11- May- 2017].

[43] S. Gutwirth, Reinventing data protection?, 1st ed. Dordrecht: Springer, 2010, p. 4.

[44] B. '16, "Computer Forensics in Criminal Investigations", DUJS Online, 2017. [Online]. Available: http://dujs.dartmouth.edu/2013/03/computer-forensics-in-criminal-investigations/#.WRyWr2iGOUk. [Accessed: 17- May- 2017].

[45] "How Tor Works (Translation)", Geektimes.ru, 2016. [Online]. Available: https://geektimes.ru/post/277578/. [Accessed: 18- May- 2017].

[46] "How VPN Works - riseup.net", Riseup.net. [Online]. Available: https://riseup.net/en/vpn/how-vpn-works. [Accessed: 18- May- 2017].

[47] S. Biddle, "Stop Using Unroll.me, Right Now. It Sold Your Data to Uber.", The Intercept, 2017. [Online]. Available: https://theintercept.com/2017/04/24/stop-using-unroll-me-right-now-it-sold-your-data-to-uber/. [Accessed: 19- May- 2017].