

# Accepted Manuscript

Title: Exploring the protection of private browsing in desktop browsers

Author: Nikolaos Tsalis, Alexios Mylonas, Antonia Nisioti, Dimitris Gritzalis, Vasilios Katos

PII: S0167-4048(17)30059-7

DOI: <http://dx.doi.org/doi: 10.1016/j.cose.2017.03.006>

Reference: COSE 1121

To appear in: *Computers & Security*

Received date: 24-3-2016

Revised date: 4-3-2017

Accepted date: 7-3-2017



Please cite this article as: Nikolaos Tsalis, Alexios Mylonas, Antonia Nisioti, Dimitris Gritzalis, Vasilios Katos, Exploring the protection of private browsing in desktop browsers, *Computers & Security* (2017), <http://dx.doi.org/doi: 10.1016/j.cose.2017.03.006>.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

# Exploring the protection of private browsing in desktop browsers

Nikolaos Tsalis<sup>1</sup>, Alexios Mylonas<sup>2</sup>, Antonia Nisioti<sup>2</sup>, Dimitris Gritzalis<sup>1</sup>, Vasilios Katos<sup>2</sup>

<sup>1</sup> *Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory  
Dept. of Informatics, Athens University of Economics & Business, Greece*

<sup>2</sup> *Faculty of Science and Technology  
Bournemouth University, United Kingdom*

{ntsalis, dgrit}@aueb.gr, {amylonas, anisioti, [vkatos](mailto:vkatos@bournemouth.ac.uk)}@bournemouth.ac.uk

Nikos Tsalis is a Ph.D. candidate with the Dept. of Informatics of the Athens University of Economics and Business, Greece.

Alexios Mylonas is a Lecturer with the Faculty of Science and Technology of the Bournemouth University, United Kingdom.

Dimitris Gritzalis is a Professor and the Director of the INFOSEC Laboratory with the Dept. of Informatics of the Athens University of Economics and Business, Greece. Dimitris is the Academic Editor of the Computers & Security Journal.

Vasilios Katos is a Professor with the Faculty of Science and Technology of the Bournemouth University, United Kingdom. Vasilios is an Associate Editor of the Computers & Security journal.

## Abstract

Desktop browsers have introduced *private browsing mode*, a security control which aims to protect users' data that are generated during a private browsing session, by not storing them in the file system. As the Internet becomes ubiquitous, the existence of this security control is beneficial to users, since privacy violations are increasing, while users tend to be more concerned about their privacy when browsing the web in a post-Snowden era. In this context, this work examines the protection that is offered by the private browsing mode of the most popular desktop browsers in Windows (*i.e.*, Chrome, Firefox, IE and Opera). Our experiments uncover occasions in which even if users browse the web with a private session, privacy violations exist contrary to what is documented by the browser. To raise the bar of privacy protection that is offered by web browsers, we propose the use of a virtual filesystem as the storage medium of browsers' cache data. We demonstrate with a case study how this countermeasure protects users from the privacy violations, which are previously identified in this work.

Keywords: Private Browsing, Web Browser, Web Security, Browsing Artefacts, Privacy.

## 1. INTRODUCTION

Since Internet penetration has risen in the last years (almost 3.4 million users by the end of 2015 (Internetworldstats, 2016)) it is important to preserve an adequate level of privacy to protect the average user while browsing the web. Average users, *i.e.*, those who are not technical, nor security savvy, rely on the default security countermeasures that are provided by the popular web browsers, such as protection from sites serving malware or hosting phishing at-

tacks. However, previous work has revealed that the actual protection offered by these controls is rather limited (Virvilis et al., 2014), (Tsalis et al., 2015a), (Virvilis et al., 2015), (Tsalis et al., 2015b) and (Mylonas et al., 2013).

*Private browsing* is a security control implemented by all popular web browsers, in order to provide enhanced privacy to the end user while browsing the web (Google, 2016a), (Google, 2016b) (Mozilla, 2016), (Microsoft, 2016a) and (Opera, 2016). Its primary goal is to protect the confidentiality of users' data, which are generated in a *private browsing session*, by avoiding to store them in the file system. In contrast, when the user is not under a private session (hereinafter this paper will refer this mode as *normal mode*), the data generated while she is browsing the web are stored in the filesystem for usability (e.g., facilitate authentication) and efficiency reasons (e.g., caching). Thus, private browsing can aid users to protect their privacy, against a local attacker who has access (temporal or permanent) to their device and attempts to uncover their online activities. After the revelations of state sponsored mass surveillance by Snowden (BBC, 2016), average users are concerned, more than ever, about protecting their privacy. In a recent survey (Gao et al., 2014), 200 people were asked about the use of private browsing. Nearly half of them (39.5%) stated that they use private browsing, so as to prevent their browsing history and any cookies from being saved.

This paper, examines the protection offered by private mode in popular web browsers, *i.e.*, *Chrome*, *Firefox*, *Internet Explorer* and *Opera*. A specific set of web artefacts was surveyed, which are typically created in a normal browsing session, to uncover if and where these are stored after the private session is terminated, contrary to the browser's documentation. Therefore, this work uncovers the deficiencies of the private browsing mode in web browsers and the respective privacy violations. In addition, to estimate the impact of the findings, a user survey was performed so as to note user opinion, based on the tested artefacts and their importance. Lastly, this work proposes the use of a virtual filesystem as a countermeasure against the privacy violations that have been uncovered.

The rest of the paper is structured as follows: Section 2 presents the related work. Section 3 includes our methodology. Section 4 contains the survey and test results. Section 5 presents our case study. Finally, Section 6 adds a discussion and concludes our work.

## 2. RELATED WORK

To the best of our knowledge, research regarding private mode and its effectiveness, is still limited and in an early stage. To begin with (Aggarwal et al., 2010) was among the first to cope with the analysis of private browsing and the artefacts that were exposed after the private session. More specifically, Aggarwal et al. tested a subset of the artefacts that are discussed in this work, in earlier versions of *Chrome*, *Firefox*, *Internet Explorer* and *Safari*. Also, the authors expanded their analysis in both extensions and plugins, so as to identify any security weaknesses. They concluded to the inadequate implementation of private mode in those browsers, which exposed users' activities. Additionally, they proposed a mechanism for *Firefox*, which protects against extensions that expose browsing artefacts after private mode.

In 2011, Oh et al. (2011) focused on analysing the log files created by the browser, focusing on timeline analysis (e.g., timestamps), search history, URL encoding, search keywords and the recovery of deleted data. The authors proposed WEFA, a tool for evidence collection and analysis. Their analysis was limited only on the normal browsing mode and also the browsers' versions used during the experiments are currently outdated. In (Said et al., 2011) the authors examined if private browsing artefacts were available in the system's memory. The work in (Ohana and Shashidhar, 2013) focused on portable browsers (e.g., stored on a USB flash drive) and whether artefacts are still available after the session terminates. The approach resembles the work in (Said et al., 2011), in terms of capturing and analysing RAM, while the artefacts tested included: history, credentials, images and videos.

The authors in (Heule et al., 2015) provided a control for that purpose, which is based on mandatory access control and protects sensitive data that may be accessed and used by *Chrome* extensions. Similarly, Lerner et al., (2013) focused on JavaScript extensions on *Firefox*, while in private mode. The authors verified a number of extensions, from a safety,

behavioural and debugging perspective that resulted in identifying which extensions could be malicious. Satvat et al., (2014) expanded the work in (Aggarwal et al., 2010), by performing RAM, file system and network analysis, which revealed a notable amount of inconsistencies in the private browsing implementation. The authors created extensions for Chrome, Internet Explorer, Safari and Firefox to evaluate whether browser extensions leave artefacts that violate user's privacy. Opera and Chrome's guest mode were not evaluated and only a subset of the artefacts of **Error! Reference source not found.** were considered.

Ruiz et al., (2015) focused on recovery techniques for page related data (*i.e.*, text and graphics) created during private browsing. The authors performed their tests within 4 individual phases: shutdown, freeze, kill process and power down, while each phase indicated the way the browser was terminated (*e.g.*, kill process - browser interruption). Their results showed that all phases included flaws regarding user's privacy, in terms of acquiring browsing artefacts. In addition, Montasari and Peltola, (2015) analysed both system's locations and RAM, in all browsers except Opera. Although the selected operating system is not clarified, it is implied that the authors used Windows for their experiments. Their results showed that Chrome is the most secure browser, since there are no artefacts available after private browsing, while Firefox only included low risk artefacts.

In a parallel work, Xu et al., (2015) studied private browsing using the threat model defined in (Aggarwal et al., 2010). They analysed the data flows that were generated by Firefox and Chrome with a system call tracer (for Linux) and detected the privacy violations that occurred, similarly to our work. To mitigate the identified privacy threats, they implemented UCOGNITO for Firefox and Chrome only, which also sandboxes the browser in order to control and delete the files that are created by the browser. UCOGNITO uses MBOX to redirect (write) access to the filesystem by rewriting file paths in a static location, which can be deleted after the private session. However, as in UCOGNITO the browsing artefacts are stored in the filesystem, they can be recovered even if they are deleted unless secure deletion is used (Gutmann, 1996), which is time consuming. In our work all the browsing artefacts are stored in a virtual filesystem, instead of a long term storage medium (*e.g.*, hard disk). As a result, any browsing artefact cannot be recovered when the electromagnetic load of the RAM is lost. In addition, secure deletion in the RAM is quicker compared to hard disks. Finally, the proposed solution can be used with any browser irrespective of its technology.

In a similar approach, recent works focused on the forensic perspective of mobile versions of web browser. Marrington et al. (2012) dealt with Chrome's normal and incognito mode and the forensic traces left behind in comparison to the installed and the portable version of the browser. The results showed that both versions revealed the same amount of artefacts, thereby concluding that the portable version of the browser does not offer enhanced security guarantees regarding the user's privacy. Moreover, Al Barghouthy et al. (2013) evaluated the available solutions that offer privacy protection to users. More specifically, they evaluated the Orweb browser that anonymizes network traffic and avoids saving the browsing history. Their results that the browsing artefacts (*e.g.*, visited URLs, login data, etc.) can be retrieved even when the Orweb browser is used.

In addition, a recent survey (Gao et al., 2014) focused on private browsing mode awareness from a user perspective. The authors surveyed 200 users regarding if, why and when they use this feature, and which are its benefits or drawbacks, if any.

This work expands our previous work that focuses on the security mechanisms offered by modern web browsers. Mylonas et al. (2013) enumerated the security and privacy controls that are offered by the most popular web browsers in both desktop and smartphone platforms, finding a considerable gap in their availability and configurability. Virvilis et al., (2014; 2015) and Tsalis et al., (2015a) evaluated the filtering mechanism that is offered by modern browsers in desktop and smartphone platforms against malware and phishing. Finally, Tsalis et al., (2015b) enumerated the available security and privacy add-ons and commented on the protection provided by modern web browsers.

### 3. METHODOLOGY

The scope of the analysis includes the popular desktop browsers (see **Error! Reference source not found.**)<sup>1</sup> for Windows, *i.e.*, Chrome v. 47, Firefox v. 43, Internet Explorer 11 and Opera v. 34. Windows 7 was selected as it was - at the time of conducting the analysis - the operating system with the largest user base (43.1% of the market share according to (W3schools, 2016b)).

This work assumes that a user browses the web with a desktop browser in which the attacker has temporal physical access (*e.g.*, Internet cafe, shared desktop). The user wishes to protect the details of her browser session and as such, she browses the web with private mode enabled and quits the browser without shutting down the workstation. It is also assumed that the attacker does not possess any forensic skills or tools, but is able to find any traces of the user's online activity by simply browsing the filesystem.

In this context, all the aforementioned browsers are used in private mode to evaluate whether they indeed provide the documented protection against privacy violations. To identify whether any traces of the user's online activities remain after a private session, each browser was executed in private mode and online activities were performed. More specifically, we assume that the user in her private session performs online activities that will create the artefacts of Table 2. For instance, when she visits a website, bookmarks it and downloads a file, then those actions will create artefacts regarding: bookmarking, browser cache memory, browsing history, cookies, download list and downloaded files.

Any changes to the filesystem as a result of these online activities were automatically monitored. The online activities that were performed aimed to create data which are typically left behind during a normal browsing session (see **Error! Reference source not found.**). More specifically the artefacts that were generated can be classified as: (a) *generic artefacts* (Aggarwal et al., 2010), which is a set similar to the set of protected data sources compiled from the browsers' documentation pages (*c.f.* **Error! Reference source not found.**) and includes simple browsing activities (*e.g.*, bookmarking a webpage, downloading a file, etc.), (b) *browser artefacts*, which describe changes in the browser itself (*e.g.*, installing a digital certificate, modifying browser settings) and (c) *website artefacts*, which include per site configurations, such as website translation or website zoom.

**Error! Reference source not found.** summarizes the set of artefacts that were examined by the authors of the relevant literature (see Section 2). To the best of our knowledge, no other work in the literature focuses on the superset of all the artefacts that we have tested. The majority of works in the relevant literature focuses on a subset of artefacts only, except for the work of Xu et al. (2015).

Lastly, to measure the impact of the corresponding findings, a survey was conducted that measured user awareness. Specifically, the survey collected the users' opinion about private browsing mode, and measured the impact of a privacy violation concerning the artefacts of Table 2. For readability reasons, the questionnaire that was used in the survey is available in the Appendix A.

#### 3.1 Analysis Environment

The browsers were monitored inside a virtual machine running Windows 7. Every browser was installed using the default installation settings in a different snapshot of the virtual machine. This initial clean state of the analysis environment was retained and was restored if needed in the analysis. As a result, this setup avoided any instances of cross contamination issues during the analysis.

<sup>1</sup> Apple offered a Safari for Windows but it was excluded from the analysis as it has been discontinued since 2012 (Apple, 2016).

To monitor any changes in the filesystem and the registry that occurred during the private sessions, all the relevant events created by the process of each browser were collected, in the same way dynamic malware analysis is conducted (Sikorski & Honig, 2012). To this end, bat scripts were facilitated that utilized process monitor v. 3.2 (Microsoft, 2016c), for the collection and parsing of all the modifications (events) occurred by the browsers' process.

## 4. RESULTS

### 4.1 User survey

As mentioned previously, a large percentage of users choose to enhance their privacy by utilizing the private mode for their browsing activities. Therefore, it is important to collect the users' perception regarding private browsing and its features. This will allow to compare the priorities set by the users against the ones set by the manufacturers of modern web browsers. In this context, this subsection presents the results of a survey that focused on capturing user opinions and perceptions regarding the artefacts of this work. Our survey included 153 participants, having the following demographics: 53.6% were men, 26.8% studied at MSc level and 73.2% at BSc level. 90.2% were Chrome users, 51% were Firefox users, 7% were Opera users and only 2.1% were using Internet Explorer.<sup>2</sup>

Amongst the participants, 71.2% were aware of the existence private browsing, 9.8% were unaware and 19% were not completely sure about the existence of the security control. Also, we examined whether users read the documentation of private mode, since this would inform them which artefacts are protected via the use of such mechanism. The corresponding results revealed that only 1.3% of the sample has read the whole online documentation, 11.8% of them quite read it, 30.7% hardly read it and 55.6% have not read it at all.

The following figure **Error! Reference source not found.** summarizes the sample's knowledge regarding the artefacts protected by private browsing. As the results indicate, the sample is more likely to consider that the artefacts remain after the private session if they are not mentioned in the documentation or the welcome page of private browsing. In addition, the figure summarizes the expectation of our sample with regards to the protection of their online privacy, in which sensitive data such as the browsing history and passwords should not be stored in the private session. However, this work proves that this expectation is not valid (see Section 4.4).

Table 4 **Error! Reference source not found.** summarizes the results from Q9 of the questionnaire regarding the number of respondents that would be very upset if an artefact was recovered by the attacker after the private session.<sup>3</sup> The results reveal that the *passwords* (80.4%) and *browsing history* (62.7%) artefacts are the ones that would upset the sample the most if they were collected by the attacker. Conversely, the sample expressed least concern about the *translation settings* (41.8%), *bookmarks* (34.6%) and *downloaded files* (32%). The results also suggest that the artefacts *auto-complete form data*, *browser cache memory*, *cookies*, *download list*, and *search terms*, would upset one out of two survey participants if they were exposed to an attacker.

### 4.2 Browser documentation

The documentation for each browser was enumerated regarding the protection that is offered by each private mode. It is worth clarifying that each browser refers to this control

<sup>2</sup> The questionnaire (see Appendix A) allowed more than one option to be selected in Q5 to reflect participants who were using multiple browsers.

<sup>3</sup> Table 1 in Appendix B includes all the results from Q9.

differently, namely: *incognito* and *guest* mode in Chrome (Google, 2016a; 2016b), *private* mode in Firefox (Mozilla, 2016), *InPrivate* mode in Internet Explorer (Microsoft, 2016a) and *private* mode in Opera (Opera, 2016). Even though all the examined browsers offer this documentation online, this documentation is rather limited. More specifically, only Firefox and Internet Explorer provide adequate documentation regarding the protection of almost all the artefacts that are in the scope of the analysis. The rest of the examined browsers have a very limited documentation regarding this control, especially Chrome that provides as little as one simple sentence regarding private mode.

In addition, users can get additional information regarding the private browsing within their browser. Specifically, when a user opens a new window in private mode, a welcome page is presented that informs the user regarding private mode and redirect her to the official documentation page. However, the user can be confused from inconsistencies between the information for this control, which is available in the online documentation and these welcome pages. More specifically, Chrome (*incognito* mode) mentions the deletion of cookies on the welcome page, but this is not available on the online documentation. The same applies for the protection of downloaded files. Moreover, Firefox does not document what happens with passwords created and used during a private session. Internet Explorer states that the extensions are disabled, which is something that is not available in the online documentation. Finally, Opera provides a generic message that states “*all the information connected with them will be erased*”, which is rather vague (and invalid, as will be proven).

**Error! Reference source not found.** includes only the artefacts mentioned in the documentation, while using the following notation: ● is used when the documentation states that the artefact is available after private mode, ○ when it is not and “-” when the documentation does not include any information about that specific artefact.

There is no consensus regarding the data that should be protected. In fact, each browser selects a different set of artefacts to protect. For instance, Opera does not protect the passwords that are created in a private session whereas Firefox and IE do. Chrome does not document the absence or the protection of this data.

### 4.3 Browser data sources

#### 4.3.1 Summary of modifications in the filesystem

By monitoring the events that were created by each browser process, all the interactions with the system were identified. **Error! Reference source not found.** summarizes the total interactions with the filesystem that occurred, with a breakdown of whether the browser created, deleted, or changed the attributes of a file or folder. One would consider that during a private session only a few or none changes should occur to the system. However, the results invalidate this assumption. **Error! Reference source not found.** summarizes the paths in the filesystem in which these modifications occurred.

#### 4.3.2 Location and analysis of artefacts

When a user browses the Internet, she performs specific activities, which generate artefacts based on the type of the performed activity. For instance, when the user bookmarks a website this action creates a new entry in the files which are used by the browser to store browsing data. Thus, if these entries are retrievable after the private session they constitute a privacy violation, revealing the user’s browsing actions.

##### 4.3.2.1 Generic artefacts

The analysis revealed that during a private session none of the browsers allow the user to save *auto-complete form data* and, with the exception of Opera, *passwords*. Opera in particular allows the user to store passwords in private mode (see **Error! Reference source**

**not found.**). Also, the username is stored in the “*LoginData*” file, but the password is only visible via the browser itself (*i.e.*, following the path in the browsers interface Settings → Privacy & Security → Manage Saved Passwords → Show). Session cookies and search terms do not remain in the filesystem after the private session.

The analysis revealed that all browsers protect the “*download list*” artefact, *i.e.*, all the browsers do not keep the list of files the user downloaded during the private session. However, as these files remain in the filesystem (see **Error! Reference source not found.**) the compilation of this list is straightforward. This holds true as, all the downloaded files can be found in the download folder of each browser after private mode, unless the user manually deletes them.

As summarized in **Error! Reference source not found.**, the bookmarks that are created during a private session remain in the filesystem, with the exception of Chrome’s *guest* mode that disallowed the creation of bookmarks. More specifically, in *Firefox* bookmarks are stored in the “*places.sqlite*” database, along with the creation timestamp of last access as shown in **Error! Reference source not found.**. In *Chrome*, bookmarks are saved in the “*bookmarks*” file (**Error! Reference source not found.**), along with their creation and/or modification timestamp. Similarly, in *Opera*, bookmarks are saved in the “*bookmarks*” file in the browser’s directory (**Error! Reference source not found.**). Lastly, *Internet Explorer* places the bookmarks in the Windows “*favourites*” folder (**Error! Reference source not found.**).

While all browsers attempt to delete the browsing history after the private session, the analysis revealed that it can be inferred from browser’s cache memory and bookmarks in *Firefox* and *Chrome*. Specifically, when a user bookmarks a webpage, *Chrome* and *Firefox* store additional data about the bookmarked website, which reveal that the activity was performed during private mode. *Chrome* creates a new profile page in the history database and it marks the hidden field with a “1” (**Error! Reference source not found.**), which suggests that the bookmark was created in private mode. Similarly, *Firefox* creates a new entry in the *moz\_bookmarks* field of the *places.sqlite* file (**Error! Reference source not found.**). This entry contains a unique id, which correlates with the *moz\_history\_visits* field of the same file (**Error! Reference source not found.**) and indicates the visit.

Finally, in almost all browsers the *cache memory* does not remain after the private session. In *Firefox* however the *ocsp* responses remain in the browser’s *cache* folder. The *ocsp* protocol is used by the browser to check the validity of a digital certificate (Santesson et al., 2013), but as shown in **Error! Reference source not found.** leaks part of the user’s browsing history.

#### 4.3.2.2 Browser artefacts

When a user modifies or views the browser’s settings, she is redirected to the same settings window that is used in normal mode. As a result, any changes in the browser’s settings will still be available after private browsing is terminated. Note that this applies to all of the tested browsers except *Chrome*’s *guest* mode, where the user can only configure the browser’s search engines (**Error! Reference source not found.**).



Furthermore, while Chrome's guest mode offered very limited access to the browser's settings, a user can manually access them via manually browsing to `chrome://settings/content` (**Error! Reference source not found.**). Note that the user can even update Chrome via the guest mode, by visiting the "about" field. These settings, except for the browser update, only apply to the guest mode and the changes are not available in normal mode. In contrast, these are available in the preferences file in Google's Guest profile folder. Thus, the user can manually visit and change the settings, which may result in revealing specific artefacts. For instance, if the user modifies the content settings and blocks the cookies from a specific website, this will still be available after the private session, and thus reveal the corresponding browsing activities.

The user can navigate in all browsers to the corresponding add-ons/extensions panel and interact with them in private mode. More specifically, the user can view, modify and delete existing ones, or even install new ones from the browser's repository. These will be available in normal mode, along with any changes in their settings. Thus, if she installs an add-on which is specific to one of the tested artefacts (e.g., history - ad-blocker), this will result in disclosing the user's activities performed (e.g., blocked website), since the change will also be available during normal mode. As a result, the blocked website will remain in the installed add-on and it is straightforward to infer that this website was visited (i.e., history)

While in private mode the user is able to delete existing certificates and add new ones. For instance, when a new certificate is added to Firefox, a new entry is created in the "cert8.db" file, while the same applies to the remaining browsers which use the system's certificates. And since the certificate includes the corresponding website, the user's history is available, as far as websites with certificates is concerned. During the analysis, only Chrome's guest mode does not offer the functionality to access the system's *certificates*.

Similarly, the user can access the browser's *plugins*, through the *settings* panel in any browser, which is already discussed earlier. Thus, any changes will still remain in normal mode in all browsers (why is this important). It should be noted that in the case of Chrome's Guest mode, any changes in these settings only apply to the guest profile and are stored in the preferences file in Google's Guest profile folder.

#### 4.3.2.3 Website artefacts

Both in normal and private mode, the user has the option to set settings that are valid for a specific web page/domain. These settings are referred as *permissions* and define how the browser will present specific content, such as images. Firefox is the only browser that groups these settings together in a panel, while the rest browsers allow a user to modify them either by visiting the "settings" panel, or by configuring them in an ad-hoc manner. For instance, full screen is set with a pop-up message. Note that in Chrome's guest mode, the changes are only available while guest mode is enabled, but are stored in the "preferences" file. Thus, since the permissions operate at a per-website basis, any change will include the website itself in the above mentioned file and as a result expose the "history" artefact. Similarly, Chrome, Internet Explorer and Opera store these changes in their default folders (as depicted in **Error! Reference source not found.**), while Firefox uses the "permissions.sqlite" file.

All browsers except for Firefox and Opera allow the user to translate a webpage or choose to never translate a web page. The analysis has revealed that this action in Internet Explorer does not leave any traces in its preferences folder. More specifically, the browser uses bing.com, which is automatically visited when the user translates a website. Thus, traces regarding this action can only be found in the DNS records (**Error! Reference source not found.**), where the translated website is also included. In contrast, in Chrome (in both incognito and guest mode) user's translation preferences are stored in the "preferences" file, which is available in each mode's folder. For instance, **Error! Reference source not found.** depicts data regarding the user's language preferences in incognito mode – i.e.,

blocked languages, blacklisted websites, etc. Lastly, the results suggest that a website's zoom level cannot be recovered in the file system after a private session.

#### 4.4 Summary of findings

**Error! Reference source not found.** summarizes the privacy protection that is offered by each web browser against an attacker who has unauthorized access to the user's device after the use of private mode. Moreover, the analysis of the privacy protection that is offered by private mode in each browser, uncovered inconsistencies in the documentation of this control, are summarized in **Error! Reference source not found.**. Both tables use a superset of symbols that have been used previously, namely define: the symbol ● is used when an artefact which is created/modified during private mode remains after the session terminates, the symbol ○ depicts that the artefact does not remain, the symbol ☐ indicates that the artefact is indirectly available after the session (see comments in the analysis), and the symbol ☒ is used when the browser does not allow the creation/modification of the artefact during the private mode. We mark with grey the cases in which there is a mismatch between the documentation and the analysis results or the cases in which we find an undocumented artefact remaining after the private session.

**Chrome.** During the analysis of *incognito* mode, almost all of the artefacts were revealed, except for: *browser cache memory*, *cookies*, *passwords* and *zoom level*. The same applies to the *guest* mode, where the browser did not offer the option to bookmark a webpage, while the permissions were not stored in the file system.

**Firefox.** The results were similar to Chrome's *incognito* mode, while there was not any website translation option available by Firefox. Also, the use of the *ocsp* protocol disclosed the browsing history within the *ocsp* responses.

**Internet Explorer.** Similarly, the analysis of *InPrivate* mode yields similar results to Chrome's *incognito* mode, with the exception of the "*download list*" artefact that was not saved in the filesystem.

**Opera.** The protection of the web artefacts in Opera's private mode is similar to Firefox's. However, the browser cache memory cannot be retrieved from the filesystem after the private session. In addition, only Opera enables the user to save her password during a private session, which is not deleted after the completion of the session.

The analysis revealed two facts regarding the protection that is offered to the user by private sessions: (a) some artefacts that are created in private sessions are *not included* in the documentation of this control and most of the cases remain after the end of the browsing session and (b) some artefacts remain in the filesystem after the private browsing session even though the documentation states otherwise. One should note that in both cases this results in a privacy violation, as these artefacts can be collected by the attacker. However, in the second case the control creates a false sense of privacy protection as the documentation promises to discard the data after the private session. Also, in the first case (assuming that a privacy concerned user will go through the relevant documentation pages) the user is not informed that the artefact is created and that it remains in the file system after using private browsing.

As proved through the survey presented in Section 4.4, users would be very upset if a specific subset of browsing artefacts could be retrieved after a private session, namely the browsing history and the passwords. According to our results the control's documentation states that the majority of these artefacts are unavailable after a private session. Our analysis however revealed instances in which these artefact are exposed to a local attacker even after the termination of the private session. This holds true, as (a) the browsing history in both Chrome and Firefox can be retrieved through the bookmarks, (b) passwords are not deleted

after the private session in Opera, and (c) the browsing history in Firefox can be retrieved from the ocsf responses.

In other words, our work uncovers that artefacts that are considered critical based on user perception can be indirectly retrieved through artefacts with lower criticality. Moreover, our analysis showed that the medium and low artefacts can be recovered after the private session in almost any browser. Therefore it is alarming that the users are unaware of this correlation that can be performed between the artefacts they consider of low importance in order to reveal the critical ones.

## 5. CASE STUDY: VIRTUAL FILESYSTEM VS. PRIVACY VIOLATIONS

This work proves that currently private sessions in all browsers fail to protect the confidentiality of the artefacts that are created while a user is browsing the web, even against a local attacker who has no forensic knowledge or tools. This holds true, as the artefacts are stored in the filesystem within each browser's folder that is used for data storage or caching. Thus, their unauthorized physical access is considered to be trivial. To mitigate this threat, this work proposes the use of a virtual filesystem as a countermeasure against the privacy violations that have been uncovered.

A virtual filesystem is stored in a volatile storage medium, *i.e.*, the RAM instead of a long term storage medium, *e.g.*, hard disk. Currently, software exists that creates a one-off volatile virtual filesystem that the browser can use to operate and support the browsing activities of the user. Such software is available in all popular operating systems for desktops, *e.g.*, RAMDisk (RAMDisk, 2016)) for Windows, *i.e.*, Linux (JamesCoyle, 2016) and OS X (Tanous, 2016).

This section will verify if the data that were stored in the virtual filesystem (*i.e.*, in the RAM) were properly deleted upon the termination of the private session. For this reason, we focus on two scenarios: a) using software that creates the virtual filesystem and erase its contents after its use and b) using a file shredder in order to securely erase the contents of the virtual filesystem. In each scenario, we locate the virtual filesystem in memory and examine if its contents have indeed been deleted.

### 5.1 Countermeasure setup

In this case study RAMDisk was selected to create the virtual filesystem in Windows. Windows was the selected operating system, as it has the largest user base. Upon installation of RAMDisk, the browser is configured to use a new destination path to store any data and settings to a RAM location, instead of the default filesystem location. All popular desktop browsers allow this configuration via their interface. Table 10, summarizes the configuration steps that are necessary for each browser in our scope.

### 5.2 Verification of the proposed countermeasure

The *first scenario* of the case study uses RAMDisk as the software that creates the virtual filesystem for storing the user's private browsing artefacts, while using the tool's capability of erasing the part of the memory where the virtual disk resides, after the process is terminated. Upon creating the virtual filesystem we enabled the tool's erase functionality in the software's configuration and created a volume having only a FAT partition. We configured a browser in the scope of analysis (Firefox in this scenario) to use the filesystem as described above. Also, we placed an existing browser cache in order to make the scenario realistic. We browsed the web and a JPEG file was downloaded to simulate the user's behaviour. While the RAMDisk process was still alive, a memory dump was acquired. After terminating RAMDisk's process,

another memory dump was acquired. In both cases, we identified and isolated the memory pages where the filesystem resides.

The two memory dumps were compared with the use of a hex editor in order to verify if the data that were stored in the virtual filesystem were indeed deleted. As demonstrated in Fig. 16, offset `0x19954000` of the first memory dump contains the boot sector of the virtual disk. At the same offset of the second memory dump, the boot sector has been replaced by zeros, as shown in Fig. 17. The same applies for all the data (e.g., files, folders) that have been stored in the virtual filesystem. For readability reasons, this is demonstrated with the aid of a snapshot of the image's contents, which was downloaded in this scenario. As shown in Fig. 18, the header of the file was found at offset `0x17C60000` of the first memory dump. The figure also shows part of the contents of the file. On the second dump, the header as well as the contents of the file have been replaced by zeros, as presented in Fig. 19. Consequently, our results prove that RAMDisk's erasing functionality indeed erases the virtual filesystem's data, and therefore all the browsing contents from memory. Therefore, RAMDisk or any other software that offers similar functionality, can be used as a countermeasure to protect the user from the privacy violations that have been discussed in Section 4.

In the *second scenario* we worked similarly but this time did not enable the tool's erasing functionality upon process termination. Instead, we securely deleted all the browser related files with the use of a file shredder (File Shredder, 2017). Again a real browser cache and a JPEG file were used replicating the *first scenario*. A first memory dump was acquired before the deletion of the files and a second after it, while the process was still alive – as otherwise the virtual disk would be inaccessible to the file shredder.

After the isolation of the corresponding process' memory space from both dumps, the extracted data were analysed via a hex editor. As expected, Figures 20-21 demonstrate that the boot sector of the virtual disk can be found in offset `0x14436036` in both dumps. This is not surprising as (i) the virtual disk is still mounted through the RAMDisk process and (ii) the file shredder does not erase the filesystem's structure. As before, the header and a part of the JPEG file are located in the first dump at offset `0x17845A00`, as shown in Fig. 22. After the secure deletion of the virtual filesystem this part of the memory is overwritten with zeros, as depicted in Figure 23. Consequently, the file shredder successfully erased any browsing related traces, thus protecting the web user's privacy.

It is worth noting that the complexity of the performed browsing actions does not affect the results of the erasing process in both scenarios. This holds true as in both cases all the involved files, folders and the filesystem data structures that describe them are securely deleted. More specifically, in the first scenario the whole filesystem (data structures along with metadata, files and folder) get nullified. In the second scenario the file shredder will securely wipe all the folders and files selected by the user. Thus, assuming that the browsing profile folder is selected, then the files, folders and their respective metadata in the file system structures will be wiped.

## 6. DISCUSSION AND CONCLUSIONS

Web browsers offer private browsing mode, a security control that protects user's privacy against an attacker who has physical access to the user's device. The presence of this security control allows the user to browse the Internet, without having concerns about whether her online actions will be available to another user who will subsequently use the same device.

This paper evaluates the level of protection against privacy violations that is provided by private sessions, as they are implemented by the current popular web browsers in the Windows platform. Windows was selected as it is currently the operating system with the largest user base in desktops, therefore, ensuring the representativeness of this work. Chrome, Firefox, Internet Explorer and Opera were monitored during private sessions that were mounted, with the aim to identify any browsing artefacts that remained after the termination of the private session. This work identifies instances in which the official documentation of

each browser is either (a) inadequate, as artefacts that are created during the private sessions were not part of the documentation, or (b) inconsistent, as artefacts that were documented to be deleted after the private session were found, directly or indirectly in the filesystem. In both cases, a user who has physical access to the device with moderate IT skills is able to access the profile directories of the aforementioned browser and access the browsing artefacts.

This work also includes a user survey with a two-fold purpose: (a) categorizing the findings based on user opinion regarding their importance and significance and (b) exploring whether the priorities in protecting web assets set forth by the web browsers are consistent with the priorities as collected by their users.

Overall, our results revealed that private mode has room for improvement, regarding desktop web browsers. The evaluation of the protection offered by each browser revealed inconsistencies regarding the artefacts documented not to be available after a private session is terminated. Specifically, as discussed in Section 4, there were artefacts that were not included in the documentation, as well as others that can be recovered after the private session, even though the documentation states otherwise. Thus, an average user who has read the browser's documentation for private browsing would be either ignorant about the existence of some browsing artefacts during private mode or misled as the security control is not efficient.

Almost none of the tested browsers documented or informed the user regarding the browser and website artefacts, as defined in **Error! Reference source not found.** As a result, all browsers have a considerable set of artefacts exposed to local attackers. More specifically, based on the results in **Error! Reference source not found.**, almost all browsers offered a similar protection to the artefacts that were tested, with the exception of Chrome's guest mode.

Our analysis revealed that all of the browsers protect the majority of the artefacts that the users consider as most important with regards to their privacy. However, as expected, during this impact valuation the users did not take into consideration the indirect impact of some artefacts with a low or medium valuation. For instance, the majority of the users were least concerned about the exposure of their bookmarks. However, as our results reveal, the bookmarks can be used to recover part of the browsing history, which was the second highest artefact in our survey results. Moreover, in principle, these were the web artefacts that the current implementation of the private mode in all browsers tends to forget to protect.

Furthermore, the user survey showed that the users' perceptions regarding the artefacts that are not available after the private session were consistent with the browsers' documentation. Indeed, web artefacts included in the documentation or the control's welcome screen were more likely to be identified by the sample as deleted after the private session. This is an interesting finding if one considers that the sample responses indicated that more than half of the participants did not read the documentation at all, while only 1.3% of them read it at a great extent.

Lastly, a case study was used in order to explore how a virtual filesystem can mitigate the privacy violations that were identified in this work. Specifically, it was proposed that browsing artefacts can be stored in a virtual filesystem within a volatile medium (*i.e.*, RAM) instead of a long term storage medium. Apart from the fact that any data cannot be recovered when the electromagnetic load of the RAM is lost, we examined two scenarios in which the contents of the virtual filesystem are erased (*i.e.*, they are replaced with zeros). The first scenario uses RAMDisk's integrated capability of erasing the memory occupied by the virtual disk. The second scenario utilizes a file shredder to securely delete the contents of the disk. Our memory analysis experiments did confirm that in both scenarios user's privacy was successfully preserved by replacing any browsing artefacts with zeros.

## 6.1 Limitations

Our work focuses on the latest versions (at the time of our experiments, *i.e.*, March 2016) of the desktop browsers in the Windows operating system only. Other browsers that are available in other desktop operating systems (*e.g.*, Linux, OS X) along with their mobile

counterparts (Android, iOS) fall outside the scope of this paper. Moreover, the dynamic nature of the web browsers due to their frequent updates, add another limitation to our work, as browser functionality – including security controls – may be altered or added in the future.

Also, the survey results provide only insights of the users' awareness and perceptions for the private mode and the impact of privacy violations regarding the artefacts that were examined in this work. In addition, the aforementioned results from the user survey are biased toward our sample demographics, but we regard these limitations as out of the scope of this work and we leave them for future work.

Finally, our experiments proved that the contents of the virtual filesystem will be erased from memory. However, any data related to browsing artefacts (directly, indirectly) might remain in memory in other processes (such as web browser), in clipboard, or in residues of received network packets. Nevertheless, this falls outside the scope of this work.

## 6.2 Future work

For future work, we plan to expand our survey and compare the views of both IT and non IT professionals, to investigate whether there is a notable difference among the two samples. Also, to further examine the privacy protection of private mode in modern browsers, we plan on including the analysis of web browsers in mobile devices, such as Android and iOS devices.

## REFERENCES

- Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010). Analysis of Private Browsing Modes in Modern Browsers. *USENIX Security Symposium* (pp. 79-94).
- Al Barghouthy, N., Marrington, A., & Baggili, I. (2013). The forensic investigation of android private browsing sessions using orweb. In *Computer Science and Information Technology (CSIT)*, 2013 5<sup>th</sup> International Conference on (pp. 33-37). IEEE.
- Amari, K. (2009). Techniques and tools for recovering and analyzing data from volatile memory. SANS Institute.
- Apple, (2016). *Safari 6 for PC? | Apple Support Communities*. [online] Available at: <https://discussions.apple.com/thread/5713095?tstart=0> [Accessed 16 Jan. 2016].
- Edward Snowden: *Leaks that exposed US spy programme - BBC News*. [online] Available at: <http://www.bbc.com/news/world-us-canada-23123964> [Accessed 13 Mar. 2016].
- Fileshredder.org. (2017). File Shredder. [online] Available at: <http://www.fileshredder.org/> [Accessed 27 Feb. 2017].
- Gao, X., Yang, Y., Fu, H., Lindqvist, J., & Wang, Y. (2014, November). Private Browsing: an Inquiry on Usability and Privacy Protection. In *Proc. of the 13<sup>th</sup> Workshop on Privacy in the Electronic Society* (pp. 97-106). ACM.
- Gartner, (2015). *Gartner Says 4.9 Billion Connected*. [online] Available at: <http://www.gartner.com/newsroom/id/2905717> [Accessed 13 Dec. 2015].
- Google, (2016). *Browse in private with incognito mode - Chrome Help*. [online] Available at: <https://support.google.com/chrome/answer/95464?hl=en> [Accessed 16 Jan. 2015].
- Google, (2016). *Let others browse Chrome as a guest - Chrome Help*. [online] Available at: <https://support.google.com/chrome/answer/6130773?hl=en> [Accessed 16 Jan. 2015].
- Gutmann, P. (1996, July). *Secure deletion of data from magnetic and solid-state memory*. In 6<sup>th</sup> USENIX Security Symposium, San Jose, CA (Vol. 14).

- JamesCoyle.net. (2013). *Create a RAM disk in Linux* / JamesCoyle.net. [online] Available at: <https://www.jamescoyle.net/how-to/943-create-a-ram-disk-in-linux> [Accessed 15 Jul. 2016].
- Heule, S., Rifkin, D., Russo, A., & Stefan, D. (2015). The most dangerous code in the browser. In *15<sup>th</sup> Workshop on Hot Topics in Operating Systems (HotOS XV)*. USENIX Association.
- Internetworldstats, (2016). *World Internet Users Statistics and 2015 World Population Stats*. [online] Available at: <http://www.internetworldstats.com/stats.htm> [Accessed 28 Feb. 2016].
- Lerner, B. S., Elbert, L., Poole, N., & Krishnamurthi, S. (2013). Verifying web browser extensions' compliance with private-browsing mode. In *Computer Security-ESORICS 2013* (pp. 57-74). Springer Berlin Heidelberg.
- Marrington, A., Baggili, I., Al Ismail, T., & Al Kaf, A. (2012). Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers. In *Computer Systems and Industrial Informatics (ICCSII)*, 2012 International Conference on (pp. 1-6). IEEE.
- Memory.dataram.com. (2016). *RAMDisk Product FAQ - RAMDisk Support Center - Support - Dataram*. [online] Available at: <http://memory.dataram.com/support/ramdisk-support-center/ramdisk-product-support-faq> [Accessed 8 Jul. 2016].
- Memory.dataram.com. (2016). *RAMDisk Product FAQ - RAMDisk Support Center - Support - Dataram*. [online] Available at: [http://ftp.raxco.com/pub/download/rd/UserGuides/RAMDISK\\_PLUS\\_HOW-TO\\_INSTRUCTIONS.pdf](http://ftp.raxco.com/pub/download/rd/UserGuides/RAMDISK_PLUS_HOW-TO_INSTRUCTIONS.pdf) [Accessed 8 Jul. 2016].
- Microsoft, (2016). *InPrivate Browsing - Microsoft Windows*. [online] Available at: <http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/in-private> [Accessed 16 Jan. 2015].
- Microsoft, (2016). *Translate websites*. [online] Available at: <http://onlinehelp.microsoft.com/en-us/bing/gg445029.aspx> [Accessed 16 Jan. 2015].
- Microsoft (2016). Process Monitor. [online] Available at: <https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx> [Accessed 16 Mar. 2016].
- Montasari, R., & Peltola, P. (2015). Computer Forensic Analysis of Private Browsing Modes. In *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security* (pp. 96-109). Springer International Publishing
- Mozilla, (2016). *Private Browsing - Use Firefox without saving history* / Firefox Help. [online] Available at: <https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history> [Accessed 16 Jan. 2015].
- Mylonas, A., Tsalis, N., & Gritzalis, D. (2013). Evaluating the manageability of web browsers controls. In *Security and Trust Management* (pp. 82-98). Springer Berlin Heidelberg.
- Oh, J., Lee, S. and Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. *Digital Investigation*, 8, pp.S62-S70.
- Ohana, D. and Shashidhar, N. (2013). Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artefacts from private and portable web browsing sessions. *EURASIP J Inform Secur*, 2013(1), p.6.
- Opera, (2016). *Opera Help*. [online] Available at: <http://help.opera.com/Mac/12.10/en/private.html> [Accessed 16 Jan. 2015].

- RAMDisk. (2016). *RAMDisk - Software that Accelerates, Protects, Optimizes - Server Memory Products & Services - Dataram*. [online] Available at: <http://memory.dataram.com/products-and-services/software/ramdisk> [Accessed 3 Mar. 2016].
- Ruiz, R. D. S., Amatte, F. P., Park, K. J. B., & Winter, R. (2015). Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode. *IJCSDF*, 4(3), pp.404-416.
- Said, H., Al Mutawa, N., Al Awadhi, I., & Guimaraes, M. (2011). Forensic analysis of private browsing artifacts. In *Innovations in information technology (IIT), 2011 International conference on* (pp. 197-202).
- Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (2013). *X. 509 Internet public key infrastructure online certificate status protocol-OCSP*. (No. RFC 6960).
- Satvat, K., Forshaw, M., Hao, F. and Toreini, E. (2014). On the privacy of private browsing – A forensic approach. *Journal of Information Security and Applications*, 19(1), pp.88-100.
- SearchDataManagement, (2016). *What is CRUD cycle (Create, Read, Update and Delete Cycle)? - Definition from WhatIs.com*. [online] Available at: <http://searchdatamanagement.techtarget.com/definition/CRUD-cycle> [Accessed 16 Jan. 2015].
- Sikorski, M. and Honig, A., (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press.
- Tanous, J. (2013). *How to Create a 4GB/s RAM Disk in Mac OS X - TekRevue*. [online] TekRevue. Available at: <https://www.tekrevue.com/tip/how-to-create-a-4gbs-ram-disk-in-mac-os-x/> [Accessed 15 Jul. 2016].
- Tsalis, N., Virvilis, N., Mylonas, A., Apostolopoulos, T., & Gritzalis, D. (2015). *Browser Blacklists: A utopia of phishing protection. Security and Cryptography*. In *Security and Cryptography*, M. Obaidad and A. Holzinger (Eds.), Lecture Notes (CCIS), Springer.
- Tsalis, N., Mylonas, A., & Gritzalis, D. An intensive analysis of security and privacy browser add-ons. In *Proc. of the 10th International Conference on Risks and Security of Internet and Systems (CRISIS-2015)*, Springer (LNCS).
- Virvilis, N., Tsalis, N., Mylonas, A., & Gritzalis, D. (2014). Mobile devices: A phisher's paradise. In *Proc. of the 11<sup>th</sup> International Conference on Security and Cryptography* (pp. 79-87).
- Virvilis, N., Mylonas, A., Tsalis, N. and Gritzalis, D. (2015). Security Busters: Web browser security vs. rogue sites. *Computers & Security*, 52, pp.90-105.
- W3schools, (2016). *Browser Statistics*. [online] Available at: [http://www.w3schools.com/browsers/browsers\\_stats.asp](http://www.w3schools.com/browsers/browsers_stats.asp) [Accessed 16 Jan. 2015].
- W3schools, (2016). *OS Platform Statistics*. [online] Available at: [http://www.w3schools.com/browsers/browsers\\_os.asp](http://www.w3schools.com/browsers/browsers_os.asp) [Accessed 16 Jan. 2015].
- Xu, M., Jang, Y., Xing, X., Kim, T., & Lee, W. (2015). UCognito: Private Browsing without Tears. In *22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 438-449). ACM.



## APPENDIX A

## QUESTIONNAIRE

**Athens University of Economics & Business, Dept. of Informatics  
Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory**

This is a voluntary and anonymous questionnaire. **Please read the following questions and answer honestly and responsibly.**

Researchers: **Nikolaos Tsalis**, Ph.D. Candidate ([ntsalis@aub.gr](mailto:ntsalis@aub.gr)), **Alexios Mylonas**, Lecturer ([amylonas@bournemouth.ac.uk](mailto:amylonas@bournemouth.ac.uk)), **Antonia Nisioti** ([anisioti@bournemouth.ac.uk](mailto:anisioti@bournemouth.ac.uk)), **Dimitris Gritzalis**, Professor ([dgrit@aub.gr](mailto:dgrit@aub.gr)), **Vasilis Katos**, Professor ([vkatos@bournemouth.ac.uk](mailto:vkatos@bournemouth.ac.uk))

1. **Sex:** Male ☐ Female ☐
2. **Age:** .....
3. **Education:** PhD ☐ MSc ☐ BSC ☐
4. Which is the **operating system** of your **personal computer**? (you can choose **more than one**)  
Windows ☐ Linux ☐ Mac OS ☐ Other (Please specify) .....
5. Which is the browser of your personal computer? (you can choose **more than one**)  
Google Chrome ☐ Mozilla Firefox ☐ Internet Explorer ☐  
Apple Safari ☐ Opera ☐ Other (Please specify) .....
6. Do you know what **private browsing** is?  
Yes ☐ No ☐ Not sure ☐
7. Have you read the **browser's electronic manual** about **private browsing**?  
Extensively ☐ Enough ☐ Little ☐ Not at all ☐

8. Which of the following artefacts, in your **opinion**, **do not remain** in your computer **after** a **private session**? (you can choose **more than one**)

- |                                  |                          |
|----------------------------------|--------------------------|
| 1. Auto-complete form data       | <input type="checkbox"/> |
| 2. Bookmarks                     | <input type="checkbox"/> |
| 3. Browser cache memory          | <input type="checkbox"/> |
| 4. Browsing history              | <input type="checkbox"/> |
| 5. Cookies                       | <input type="checkbox"/> |
| 6. Download list                 | <input type="checkbox"/> |
| 7. Download files                | <input type="checkbox"/> |
| 8. Passwords                     | <input type="checkbox"/> |
| 9. Search terms                  | <input type="checkbox"/> |
| 10. Add-ons/Extensions           | <input type="checkbox"/> |
| 11. Certificates                 | <input type="checkbox"/> |
| 12. Plugins                      | <input type="checkbox"/> |
| 13. Settings                     | <input type="checkbox"/> |
| 14. Permissions                  | <input type="checkbox"/> |
| 15. Translation                  | <input type="checkbox"/> |
| 16. Zoom level                   | <input type="checkbox"/> |
| 17. Other (Please specify) ..... | <input type="checkbox"/> |

9. How much would it **annoy** you if some artefacts **did remain** in your computer **after a private session**?

Artefact	Much	Medium	A little	Not at all	I do not know
Auto-complete form data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bookmarks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Browser cache memory	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Browsing history	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cookies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Download list	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Downloaded files	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Passwords	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Search terms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Add-ons/Extensions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certificates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Plugins	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Translation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zoom level	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (please specify) .....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Thank you for your time and effort**

## APPENDIX B

Table 1 summarizes the results from Q9 of the questionnaire that collected how upset the sample would become if an artefact was recovered by the attacker after the private session.

**Table 1** – Summary of the results regarding how upset the sample would be if an artefact is exposed.

Artefact	Very upset	Upset	Little upset	Not upset	I do not know
Auto-complete form data	45.1%	16.8%	16.7%	14.2%	7.2%
Bookmarks	17%	16.1%	27.1%	34.6%	5.2%
Browser cache memory	45.1%	23.5%	12.8%	8.8%	9.8%
Browsing history	62.7%	15%	9.2%	11.1%	2%
Cookies	52.3%	22.2%	11.1%	8.5%	5.9%
Download list	33.3%	24.2%	19.6%	20.3%	2.6%
Downloaded files	22.2%	22.9%	17.0%	32%	5.9%
Passwords	80.4%	5.2%	6.5%	5.2%	2.7%
Search terms	48.4%	18.3%	17.6%	13.1%	2.6%
Add-ons / Extensions	13.7%	18%	28.8%	28.1%	11.4%
Certificates	28.1%	22.2%	16.4%	16.3%	17%
Plugins	10.5%	19.6%	28.1%	23.5%	18.3%
Settings	14%	22.1%	25.8%	24.7%	13.4%
Permissions	20.3%	25.5%	22.2%	17.6%	14.4%
Translation	11.2%	12.4%	24.8%	41.8%	9.8%
Zoom level	10.5%	11%	24.2%	34%	20.3%

**Table 2** – Browsers' user base (February 2016, (W3schools, 2016a))

Browser	User base (%)
Chrome	69.0%
Firefox	18.6%
Internet Explorer	6.2%
Opera	1.3%

**Table 3** – User activity categorization.

Generic artefacts	Browser artefacts	Website artefacts
Auto-complete elements	Add-ons / Extensions	Permissions
Bookmarks	Certificates	Translation
Browser cache memory	Plugins	Zoom level
Browsing history	Settings	-
Cookies	-	-
Download list	-	-
Downloaded files	-	-
Passwords	-	-
Search terms	-	-

**Table 4** – Artefacts tested by authors.

Artefacts	(Aggarwal et al., 2010)	(Montasari and Peltola, 2015)	(Sarva et al., 2014)	(Ruiz et al., 2015)	(Ohana and Shashidhar, 2013)	(Said et al., 2011)	(Xu et al., 2015)	(Oheral, 2011)
<b>Generic artefacts</b>								
Auto-complete elements	x						x	
Bookmarks	x		x				x	x
Browser cache memory	x	x			x	x	x	x
Browsing history	x	x	x	x	x	x	x	x
Cookies	x						x	x
Download list	x						x	
Downloaded files	x	x		x	x			x
Passwords	x				x			
Search terms	x	x				x		x
<b>Browser artefacts</b>								
Add-ons / Extensions			x					
Certificates	x						x	
Plugins								
Settings								
<b>Website artefacts</b>								
Permissions								

Artefacts	(Aggarwal et al., 2010)	(Montasari and Peltola, 2015)	(Satvat et al., 2014)	(Ruiz et al., 2015)	(Ohara and Shashidhar, 2013)	(Said et al., 2011)	(Xu et al., 2015)	(Oh et al., 2011)
Translation							x	
Zoom level	x						x	

Accepted Manuscript

**Table 4** – The number of respondents who indicated they would be very upset if an artefact is exposed.

Artefact	Very Upset
Passwords	80.4%
Browsing history	62.7%
Cookies	52.3%
Search terms	48.4%
Auto-complete form data	45.1%
Browser cache memory	45.1%
Download list	33.3%
Certificates	28.1%
Downloaded files	22.2%
Permissions	20.3%
Bookmarks	17.0%
Settings	14.0%
Add-ons / Extensions	13.7%
Translation	11.2%
Plugins	10.5%
Zoom level	10.5%

**Table 5** – Browser documentation regarding private mode.

Artefact / Browser	Chrome		Firefox	Internet Explorer	Opera
	Private	Guest			
Add-ons / Extensions	-	-	-	○*	-
Auto-complete form data	-	-	○	○	-
Bookmarks	-	-	●	-	●
Browser cache memory	-	-	○	○	○
Browsing history	○	○	○	○	○
Cookies	○*	○	○	○	○
Download list	-	-	○	-	-
Downloaded files	●	-	●	-	●
Passwords	-	-	○	○	●
Search terms	-	-	○	○	-

\* This is available only at the welcome page of the private mode.

**Table 6** – Total interactions found in the filesystem during the private mode.

Action / Browser	Chrome		Firefox	Internet Explorer	Opera
	Private	Guest			
Create	20	161	62	100	99
Modify	34	28	24	13	20
Delete	2	2	2	2	2
<b>Total actions</b>	<b>67</b>	<b>202</b>	<b>94</b>	<b>116</b>	<b>125</b>

**Table 7** – Paths that were modified in the filesystem.

<b>Browser</b>	<b>Data source location</b>
<b>Chrome incognito</b>	AppData\Local\Google\Chrome\User Data\Default
	AppData\Local\Google\Chrome\User Data\Local State
	AppData\Local\Google\Chrome\User Data\ShaderCache
	HKEY_LOCAL_MACHINE\software\microsoft\SystemCertificates
<b>Chrome guest</b>	AppData\Local\Google\Chrome\User Data\Default
	AppData\Local\Google\Chrome\User Data\Guest Profile
	AppData\Local\Google\Chrome\User Data\System Profile\databases
<b>Firefox</b>	AppData\Local\Mozilla\Firefox\Profiles\nyaofkb5.default
	AppData\Roaming\Mozilla\Firefox\Profiles\nyaofkb5.default
<b>Internet Explorer</b>	AppData\Local\Microsoft\Feeds
	AppData\Local\Microsoft\Internet Explorer
	AppData\Local\Microsoft\Windows
	AppData\Local\Temp
	AppData\LocalLow\Microsoft
	AppData\Roaming\Microsoft\Internet Explorer
	HKEY_LOCAL_MACHINE\software\microsoft\SystemCertificates
<b>Opera</b>	AppData\Roaming\Microsoft\Windows
	AppData\Local\Opera Software\Opera Stable
	AppData\Roaming\Opera Software\Opera Stable
	HKEY_LOCAL_MACHINE\software\microsoft\SystemCertificates



**Table 8** – Overall results of the protection that is offered by private mode in each browser. †

Artefact / Browser	Chrome		Firefox	Internet Explorer	Opera
	Private	Guest			
Generic Artefacts					
Auto-complete form data	☒	☒	☒	☒	☒
Bookmarks	●	☒	●	●	●
Browser cache memory	○	○	●	○	○
Browsing history	☒	○	☒	○	○
Cookies	○	○	○	○	○
Download list	☒	☒	☒	☒	☒
Downloaded files	●	●	●	●	●
Passwords	☒	☒	☒	☒	●
Search terms	○	○	○	○	○
Browser Artefacts					
Add-ons / Extensions	●	☒	●	●	●
Certificates	●	☒	●	●	●
Plugins	●	●	●	●	●
Settings	●	●	●	●	●
Website Artefacts					
Permissions	●	○	●	●	●
Translation	●	●	☒	☒	☒
Zoom level	○	○	○	○	○

† ● is used when an artefact remains after the private session, ○ depicts that the artefact does not remain, ☒ indicates that the artefact is indirectly available after the session, and ☒ is used when the browser does not allow the creation/modification of the artefact during the private mode.

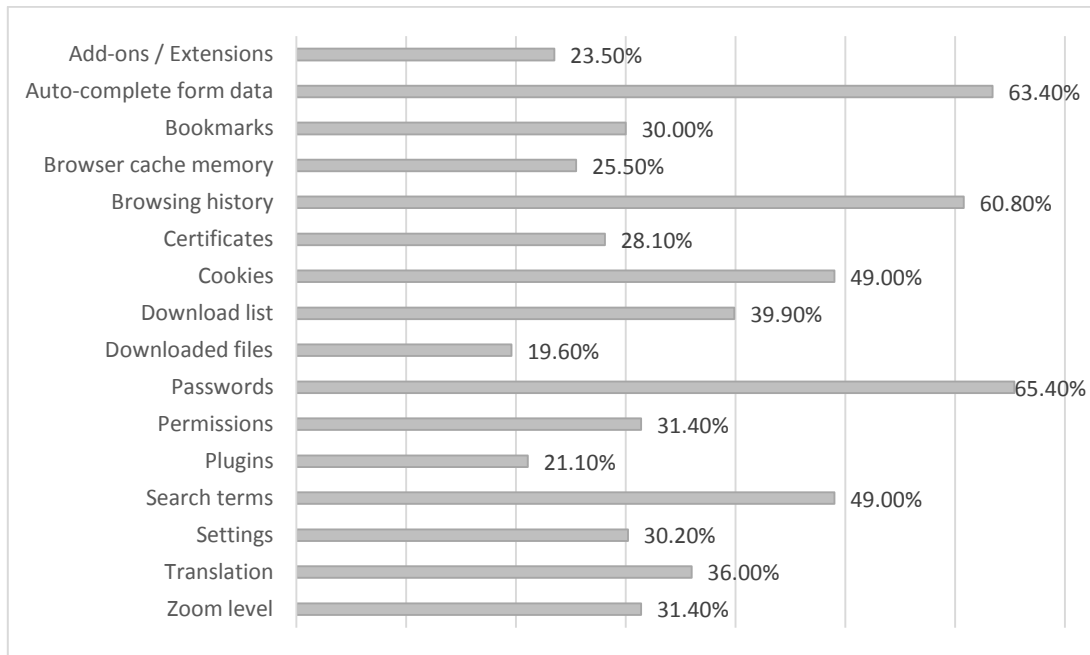
**Table 9** – Comparison of the documentation with the results from the analysis regarding the protection that is offered by private mode in each browser.<sup>†</sup>

Artefact / Browser	Chrome				Firefox		Internet Explorer		Opera	
	Private		Guest							
	Documentation	Analysis	Documentation	Analysis	Documentation	Analysis	Documentation	Analysis	Documentation	Analysis
<b>Generic Artefacts</b>										
Auto-complete form data	-	☒	-	☒	○	☒	○	☒	-	☒
Bookmarks	-	●	-	☒	●	●	-	●	●	●
Browser cache memory	-	○	-	○	○	●	○	○	○	○
Browsing history	○	☒	○	○	○	☒	○	○	○	○
Cookies	○	○	○	○	○	○	○	○	○	○
Download list	-	☒	-	☒	○	☒	-	☒	-	☒
Downloaded files	●	●	-	●	●	●	-	●	●	●
Passwords	-	☒	-	☒	○	☒	○	☒	●	●
Search terms	-	○	-	○	○	○	○	○	-	○
<b>Browser Artefacts</b>										
Add-ons / Extensions	-	●	-	○	-	●	○	●	-	●
Certificates	-	●	-	☒	-	●	-	●	-	●
Plugins	-	●	-	●	-	●	-	●	-	●
Settings	-	●	-	●	-	●	-	●	-	●
<b>Website artefacts</b>										
Permissions	-	●	-	○	-	●	-	●	-	●
Translation	-	●	-	●	-	☒	-	☒	-	☒
Zoom level	-	○	-	○	-	○	-	○	-	○

<sup>†</sup> ● is used when an artefact remains after the private session, ○ depicts that the artefact does not remain, ☒ indicates that the artefact is indirectly available after the session, and ☒ is used when the browser does not allow the creation/modification of the artefact during the private mode. We mark with grey the cases in which there is a mismatch between the documentation and the analysis results or the cases in which we find an undocumented artefact remaining after the private session.

**Table 5** – Browser configuration steps (RAMDisk, 2016)

<b>Google Chrome:</b>	<i>Right click Chrome icon → Properties → Add string "--user-data-dir=" folder path"" after "chrome.exe" → Replace "folder path" with the RAMDisk path</i>
<b>Mozilla Firefox:</b>	<i>about:config → Add string "browser.cache.disk.parent_directory" as preference name → Add the new path to the RAMDisk path</i>
<b>Internet Explorer:</b>	<i>Tools → Internet options → Settings → Move folder → Select RAMDisk path</i>
<b>Opera:</b>	<i>Properties → Target → Add "--disk-cache-dir=your folder path" after "launcher.exe" → Add the new path to the RAMDisk path</i>



**Figure 1** – Sample responses regarding the artefacts that do not remain after private browsing.

Table: logins

	origin_url	action_url	username_element	password_element	password_value
1	https://www.facebook.com/	https://www.facebook.com/login.php	email	pass	BLOB

**Figure 2** – Snapshot of password artefact in Opera.

Database Structure Browse Data Edit Pragmas Execute SQL

Table: moz\_bookmarks

	id	type	fk	parent	position	title	keyword_id	folder_type	dateAdded	lastModified	guid
1	16	1	11	5	0	Athens University of Economics and Business	NULL	NULL	1448463425922000	1448463425966000	CgncRTQbMLE

**Figure 3** – Snapshot of bookmark artefact in Firefox.

```
{
  "checksum": "e14ba1006bfee4eaf9c1ec27b66ef5a",
  "roots": {
    "bookmark_bar": {
      "children": [
        {
          "date_added": "13092937007244592",
          "id": "7",
          "name": "Athens University of Economics and Business",
          "type": "url",
          "url": "http://www.aueb.gr/"
        }
      ],
      "date_added": "13092936581775920",
      "date_modified": "13092937007244592",
      "id": "1",
      "name": "Bookmarks bar",
      "type": "folder"
    }
  },
}
```

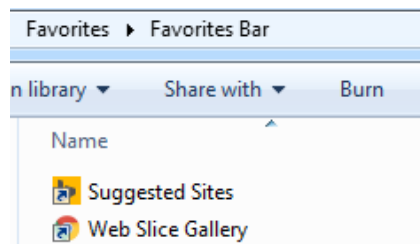
**Figure 4** – Snapshot of bookmark artefact in Chrome.

```

{
  "checksum": "56bca8efcf212214c53d007188634e05",
  "roots": {
    "bookmark_bar": {
      "children": [
        {
          "date_added": "13092937047283983",
          "id": "42",
          "meta_info": {
            "imageDataType": "2",
            "imageID": "B388FFA3274C23802FACA81D9256DB550E7AC675CDA2539CE7C08CD0889EADA9",
            "imageIdentifier": "2d44a4b8",
            "imageType": "2"
          },
          "name": "Athens University of Economics and Business",
          "type": "url",
          "url": "http://www.aueb.gr/"
        }
      ],
      "date_added": "13092756085109927",
      "date_modified": "13092937050810445",
      "id": "1",
      "name": "Bookmarks bar",
      "type": "Folder"
    }
  }
}

```

**Figure 5** – Snapshot of bookmark artefact in Opera.



**Figure 6** – Snapshot of bookmark artefact in IE.

Database Structure Browse Data Edit Pragma Execute SQL								
Table: urls								
	id	url	title	visit_count	typed_count	last_visit_time	hidden	favicon_id
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	http://www.aueb.gr/	Οικονομικό Πα...	0	0	1309293700724...	1	0

**Figure 7** – Snapshot of bookmark artefact revealing Chrome's history.

Database Structure Browse Data Edit Pragma Execute SQL											
Table: moz_bookmarks											
	id	type	fk	parent	position	title	keyword_id	folder_type	dateAdded	lastModified	guid
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	24	1	98	5	2	Athens University of Economics and Business	NULL	NULL	1448625622785...	1448625622988...	SKcAy1dnC-h6

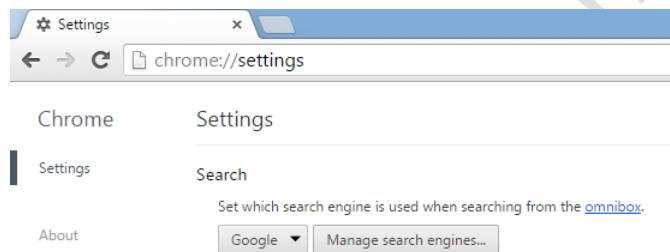
**Figure 8** – Location of bookmark artefact in moz\_bookmarks.

Database Structure Browse Data Edit Pragma Execute SQL					
Table: moz_historyvisits					
	id	from_visit	place_id	visit_date	visit_type
	Filter	Filter	Filter	Filter	Filter
1	24	0	18	1387285469455...	2

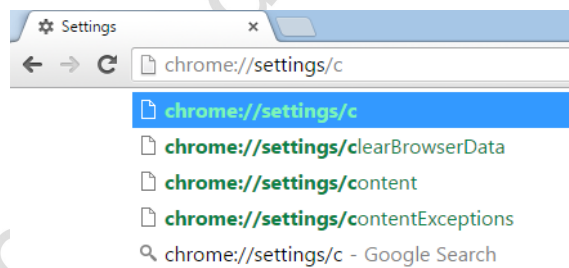
**Figure 9** – Website visit id in moz\_history\_visits.

<a href="http://anon&amp;id=1401978892&amp;suri=http://evsecure-ocsp.verisign.com/">anon&amp;id=1401978892&amp;suri=http://evsecure-ocsp.verisign.com/</a>
<a href="http://anon&amp;id=1401978891&amp;suri=http://evsecure-ocsp.verisign.com/">anon&amp;id=1401978891&amp;suri=http://evsecure-ocsp.verisign.com/</a>
<a href="http://anon&amp;id=1401978882&amp;suri=http://clients1.google.com/ocsp">anon&amp;id=1401978882&amp;suri=http://clients1.google.com/ocsp</a>
<a href="http://anon&amp;id=1401978878&amp;suri=http://clients1.google.com/ocsp">anon&amp;id=1401978878&amp;suri=http://clients1.google.com/ocsp</a>
<a href="http://anon&amp;id=1401978880&amp;suri=http://clients1.google.com/ocsp">anon&amp;id=1401978880&amp;suri=http://clients1.google.com/ocsp</a>
<a href="http://anon&amp;id=1401978885&amp;suri=http://clients1.google.com/ocsp">anon&amp;id=1401978885&amp;suri=http://clients1.google.com/ocsp</a>
<a href="http://anon&amp;id=1401978894&amp;suri=http://evsecure-ocsp.verisign.com/">anon&amp;id=1401978894&amp;suri=http://evsecure-ocsp.verisign.com/</a>
<a href="http://anon&amp;id=1401978881&amp;suri=http://clients1.google.com/ocsp">anon&amp;id=1401978881&amp;suri=http://clients1.google.com/ocsp</a>
<a href="http://anon&amp;id=1401978877&amp;suri=http://clients1.google.com/ocsp">anon&amp;id=1401978877&amp;suri=http://clients1.google.com/ocsp</a>
<a href="http://anon&amp;id=1401978876&amp;suri=http://ocsp.tcs.terena.org/">anon&amp;id=1401978876&amp;suri=http://ocsp.tcs.terena.org/</a>
<a href="https://www.google.com/uds/stats?r0=afcq%7C1&amp;nc=1401979006827_18130">https://www.google.com/uds/stats?r0=afcq%7C1&amp;nc=1401979006827_18130</a>
<a href="http://anon&amp;id=1401978883&amp;suri=http://clients1.google.com/ocsp">anon&amp;id=1401978883&amp;suri=http://clients1.google.com/ocsp</a>

**Figure 10** – OSCP responses' snapshot in Firefox cache memory.



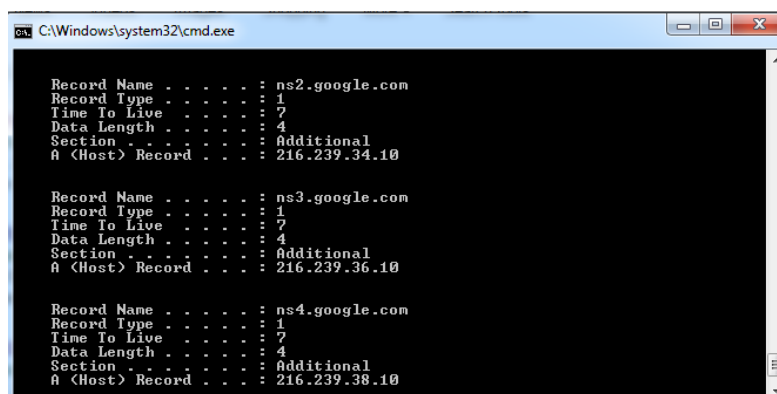
**Figure 11** – Snapshot of Chrome's guest settings.



**Figure 12** – Snapshot of Chrome's guest content settings.

Database Structure   Browse Data   Edit Pragma   Execute SQL							
Table: moz_perms							
	id	origin	type	permission	expireType	expireTime	modificationTime
	13	Filter	Filter	Filter	Filter	Filter	Filter
1	13	http://www.aueb.gr	plugin:npmeetingjoinpluginoc	1	0	0	1448634010918

**Figure 13** – Snapshot of permissions artefact in Firefox.



**Figure 14** - Snapshot from DNS records.

```

"translate_blocked_languages":["en","hy"],
"translate_denied_count_for_language":{"el":1},
"translate_last_denied_time_for_language":{"el":144889377596.927}},
"translate_site_blacklist":["mainichi.jp"],
"translate_whitelists":{}

```







[illegible][illegible]

Page 32 of 33

[illegible]

**Figure 8 – JPEG header and beginning of its contents of the Scenario 2 after the use of the file shredder**

**Figure 8 – JPEG header and beginning of its contents of the Scenario 2 after the use of the file shredder**