Exploring the protection of private browsing in desktop browsers

Nikolaos Tsalis[1], **Alexios Mylonas**[2], **Antonia Nisioti**[2], **Dimitris Gritzalis**[1], **Vasilios Katos**[2]

[1] Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business, Greece

[2] Faculty of Science and Technology
Bournemouth University, United Kingdom

{ntsalis, dgrit}@aueb.gr, {amylonas, anisioti, vkatos}@bournemouth.ac.uk

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 attacks. 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 Table 3 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. Marrignton 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 Table 1)[1] 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

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

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.

Table 1 – Browsers' user base (February 2016, (W3schools, 2016a))

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 Table 2). 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. Table 3) 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.

Table 2 – User activity categorization.

Table 3 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.

Table 3 – Artefacts tested by authors.

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.

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.[2]

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).

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

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.[3] 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.

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

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 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

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

[3] Table 11 in Appendix B includes all the results from Q9.

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).

Table 5 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.

Table 5 – Browser documentation regarding private mode.

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. Table 6 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. Table 7 summarizes the paths in the filesystem in which these modifications occurred.

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

Table 7 – Paths that were modified in the filesystem.

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 Figure 2). 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.

Figure 2 – Snapshot of password artefact in Opera.

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 Table 8) 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 Table 8, 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 Figure 3. In *Chrome*, bookmarks are saved in the *"bookmarks"* file (Figure 4), along with their creation and/or modification timestamp. Similarly, in Opera, bookmarks are saved in the *"bookmarks"* file in the browser's directory (Figure 5). Lastly, *Internet Explorer* places the bookmarks in the Windows *"favourites"* folder (Figure 6).

Figure 3 – Snapshot of bookmark artefact in Firefox.

Figure 4 – Snapshot of bookmark artefact in Chrome.

Figure 5 – Snapshot of bookmark artefact in Opera.

Figure 6 – Snapshot of bookmark artefact in IE.

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" (Figure 7), 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 (Figure 8). This entry contains a unique id, which correlates with the moz_history_visits field of the same file (Figure 9) and indicates the visit.

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

Figure 8 – Location of bookmark artefact in moz_bookmarks.

Figure 9 – Website visit id in moz_history_visits.

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 Figure 10 leaks part of the user's browsing history.

Figure 10 – OCSP responses' snapshot in Firefox cache memory.

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 (Figure 11).

Figure 11 – Snapshot of Chrome's guest settings.

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 (Figure 12). 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.

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

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 Table 8), while Firefox uses the *"permissions.sqlite"* file.

Figure 13 – Snapshot of permissions artefact in Firefox.

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 (Figure 14), 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, Figure 15 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.

Figure 14 – Snapshot from DNS records.

Figure 15 – Snapshot of translation in Google's Incognito mode.

4.4 Summary of findings

Table 8 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 Table 9. 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.

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

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.

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

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 ocsp 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.

Table 10 – Browser configuration steps (RAMDisk, 2016)

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 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.

Figure 16 – FAT boot sector of the Scenario 1 while RAMDisk's process is alive.

Figure 17 – FAT boot sector of the Scenario 1 after the termination of RAMDisk's process.

Figure 18 – JPEG header and beginning of its contents of the Scenario 1 while RAMDisk's process is alive**.**

Figure 19 – JPEG header and beginning of its contents of the Scenario 1 after the termination of RAMDisk's process.

Figure 20 – FAT boot sector of the Scenario 2 before the use of the file shredder.

Figure 21 – FAT boot sector of the Scenario 2 after the use of the file shredder.

Figure 22 – JPEG header and beginning of its contents of the Scenario 2 before the use of the file shredder.

Figure 23 – JPEG header and beginning of its contents of the Scenario 2 after the use of the file shredder.

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 Table 2. As a result, all browsers have a considerable set of artefacts exposed to local attackers. More specifically, based on the results in Table 8, 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 5th 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 13th Workshop on Privacy in the Electronic Societ*y (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 6th 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 *15th 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., Elberty, 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 [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 11th 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 [Accessed 16 Jan. 2015].

W3schools, (2016). *OS Platform Statistics*. [online] Available at: http:// 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@aueb.gr), **Alexios Mylonas**, Lecturer (amylonas@bournemouth.ac.uk), **Antonia Nisioti** (anisioti@bournemouth.ac.uk), **Dimitris Gritzalis**, Professor (dgrit@aueb.gr), **Vasilis Katos**, Professor (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 ☐
2. Bookmarks ☐
3. Browser cache memory ☐
4. Browsing history ☐
5. Cookies ☐
6. Download list ☐
7. Download files ☐
8. Passwords ☐
9. Search terms ☐
10. Add-ons/Extensions ☐
11. Certificates ☐
12. Plugins ☐
13. Settings ☐
14. Permissions ☐
15. Translation ☐
16. Zoom level ☐
17. Other (Please specify) …........ ☐

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	□	□	□	□	□
Bookmarks	□	□	□	□	□
Browser cache memory	□	□	□	□	□
Browsing history	□	□	□	□	□
Cookies	□	□	□	□	□
Download list	□	□	□	□	□
Downloaded files	□	□	□	□	□
Passwords	□	□	□	□	□
Search terms	□	□	□	□	□
Add-ons/Extensions	□	□	□	□	□
Certificates	□	□	□	□	□
Plugins	□	□	□	□	□
Settings	□	□	□	□	□
Permissions	□	□	□	□	□
Translation	□	□	□	□	□
Zoom level	□	□	□	□	□
Other (please specify)	□	□	□	□	□

Thank you for your time and effort

APPENDIX B

Table 11 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 11 – 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%

FIGURES AND TABLES

Table 12 – Browsers' user base (February 2016, (W3schools, 2016a))

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

Table 13 – 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 14 – Artefacts tested by authors.

Artefacts	(Aggarwal et al., 2010)	(Montasari and Peltola, 2015)	(Satvat et al., 2014)	(Ruiz et al., 2015)	(Ohana and Shashidhar, 2013)	(Said et al., 2011)	(Xu et al., 2015)	(Oh et al., 2011)
Generic artefacts								
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
Browser artefacts								
Add-ons / Extensions			x					
Certificates	x						x	
Plugins								
Settings								
Website artefacts								
Permissions								
Translation							x	
Zoom level	x						x	

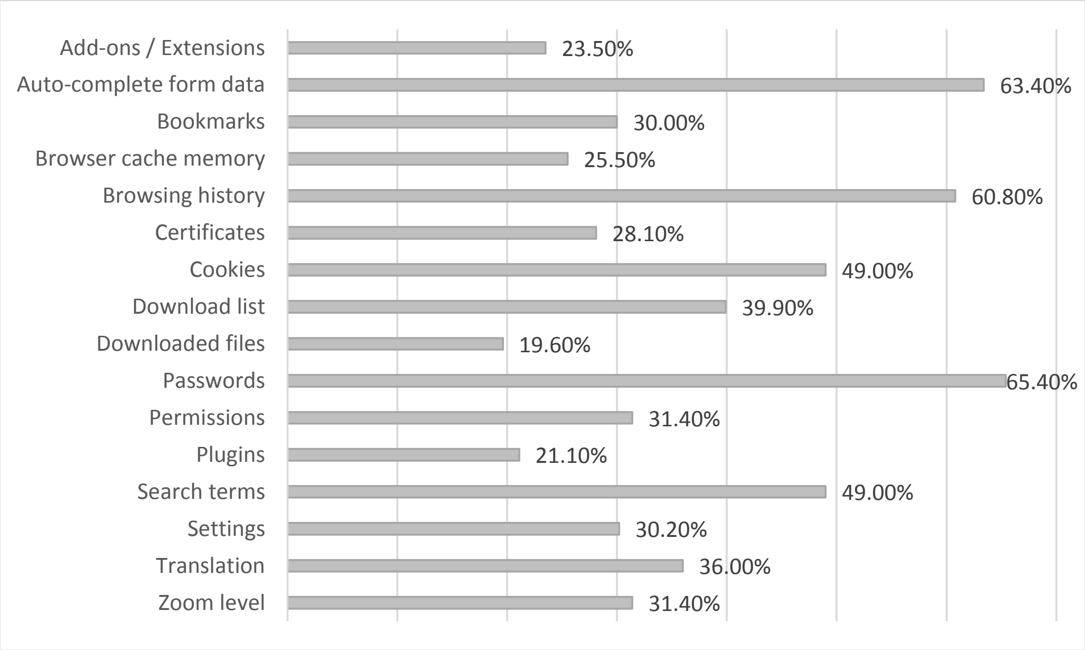


Figure 1 – Sample responses regarding the artefacts that do not remain after private browsing.

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
Total actions	**67**	**202**	**94**	**116**	**125**

Table 7 – Paths that were modified in the filesystem.

Browser	Data source location
Chrome incognito	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
Chrome guest	AppData\Local\Google\Chrome\User Data\Default
	AppData\Local\Google\Chrome\User Data\Guest Profile
	AppData\Local\Google\Chrome\User Data\System Profile\databases
Firefox	AppData\Local\Mozilla\Firefox\Profiles\nyaofkb5.default
	AppData\Roaming\Mozilla\Firefox\Profiles\nyaofkb5.default
Internet Explorer	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
Opera	AppData\Roaming\Microsoft\Windows
	AppData\Local\Opera Software\Opera Stable
	AppData\Roaming\Opera Software\Opera Stable
	HKEY_LOCAL_MACHINE\software\microsoft\SystemCertificates

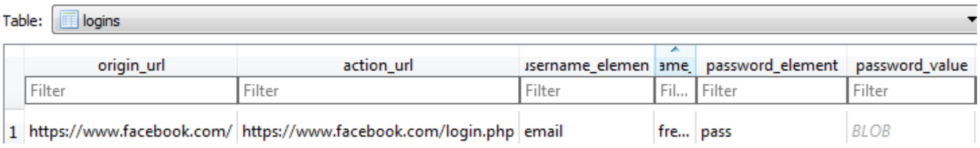


Table: logins

	origin_url	action_url	ısername_elemen	ame_	password_element	password_value
	Filter	Filter	Filter	Fil...	Filter	Filter
1	https://www.facebook.com/	https://www.facebook.com/login.php	email	fre...	pass	BLOB

Figure 2 – Snapshot of password artefact in Opera.

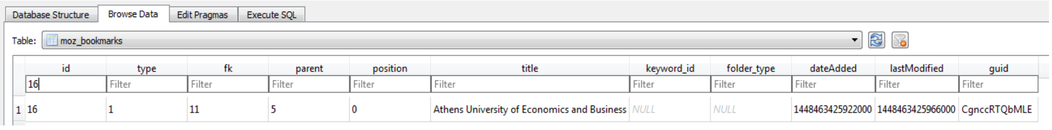
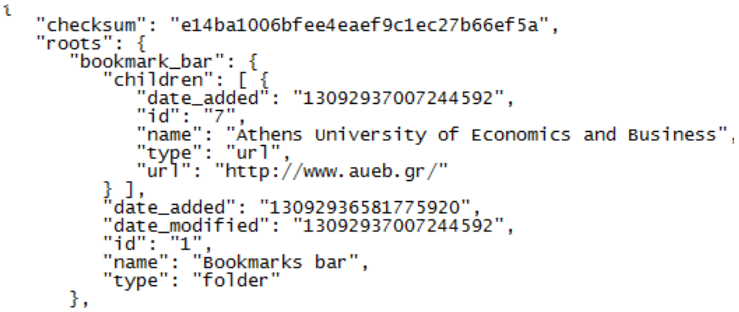


Table: moz_bookmarks

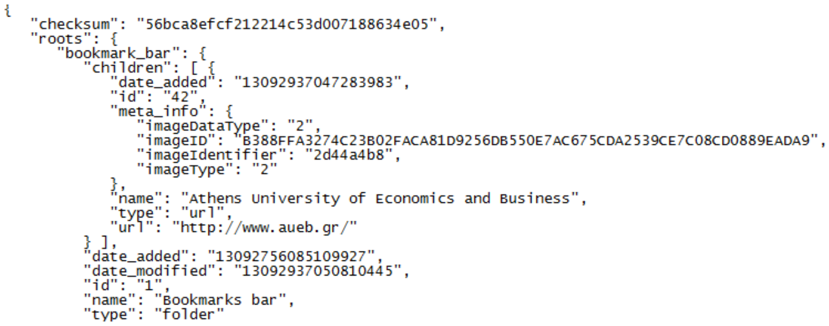
	id	type	fk	parent	position	title	keyword_id	folder_type	dateAdded	lastModified	guid
	16	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	16	1	11	5	0	Athens University of Economics and Business	NULL	NULL	1448463425922000	1448463425966000	CgnccRTQbMLE

Figure 3 – Snapshot of bookmark artefact in Firefox.



```
{
   "checksum": "e14ba1006bfee4eaef9c1ec27b66ef5a",
   "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": "B388FFA3274C23B02FACA81D9256DB550E7AC675CDA2539CE7C08CD0889EADA9",
               "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.

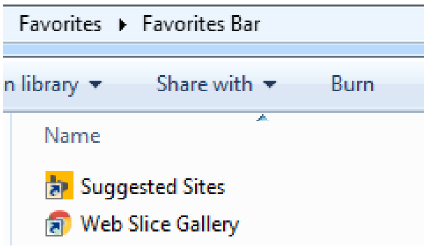


Figure 6 – Snapshot of bookmark artefact in IE.

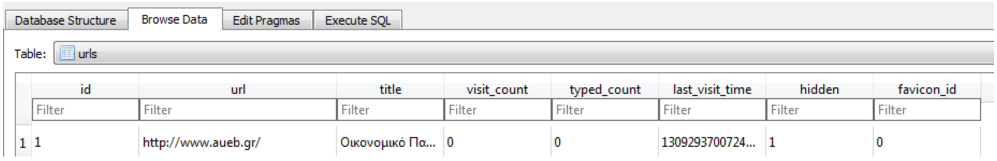


Table: urls

	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.

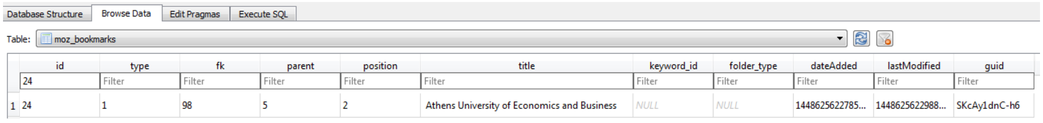


Table: moz_bookmarks

	id	type	fk	parent	position	title	keyword_id	folder_type	dateAdded	lastModified	guid
	24	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.

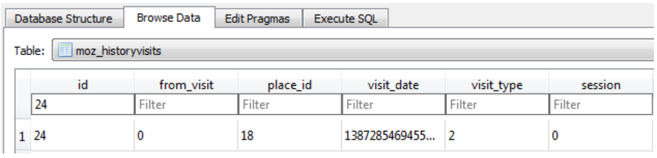
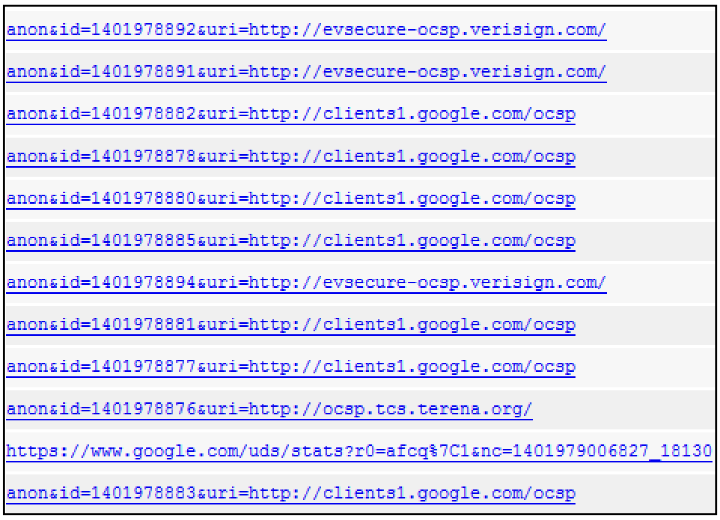


Table: moz_historyvisits

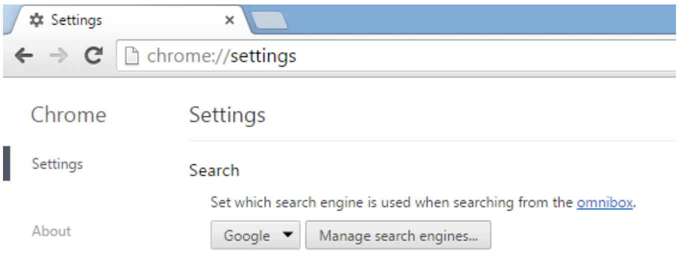
	id	from_visit	place_id	visit_date	visit_type	session
	24	Filter	Filter	Filter	Filter	Filter
1	24	0	18	1387285469455...	2	0

Figure 9 – Website visit id in moz_history_visits.



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

Figure 10 – OCSP responses' snapshot in Firefox cache memory.



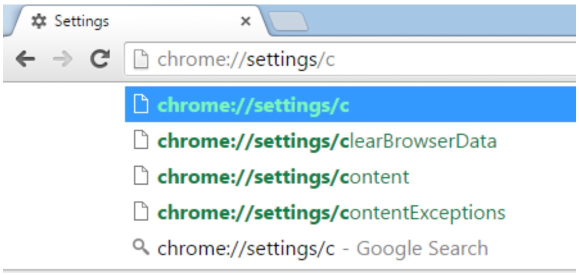
chrome://settings

Settings

Search

Set which search engine is used when searching from the omnibox.

Figure 11 – Snapshot of Chrome's guest settings.



chrome://settings/c

chrome://settings/c
chrome://settings/clearBrowserData
chrome://settings/content
chrome://settings/contentExceptions
chrome://settings/c - Google Search

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

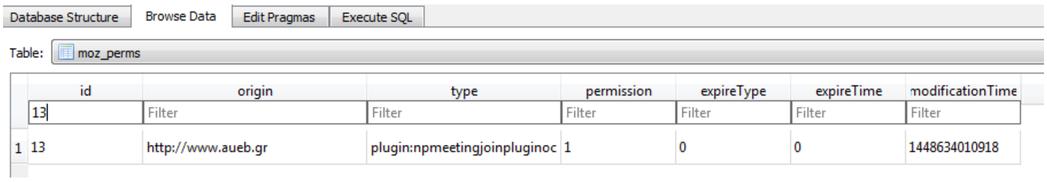
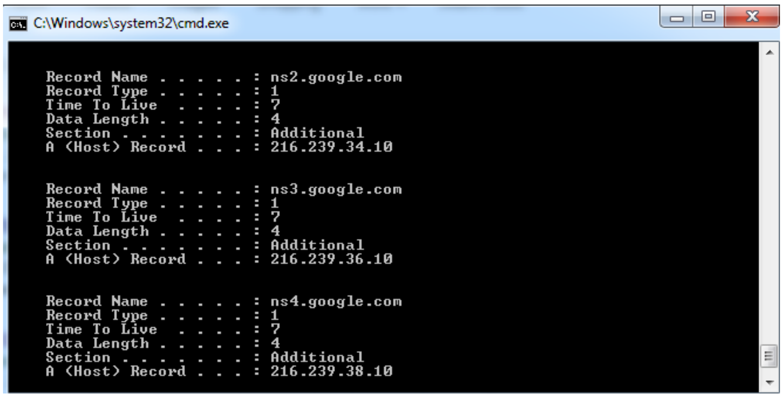


Table: moz_perms

	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.

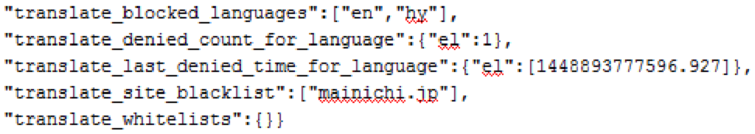


```
Record Name . . . . . : ns2.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 216.239.34.10

Record Name . . . . . : ns3.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 216.239.36.10

Record Name . . . . . : ns4.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 7
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 216.239.38.10
```

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":[1448893777596.927]},
"translate_site_blacklist":["mainichi.jp"],
"translate_whitelists":{}}
```

Figure 15 – Snapshot of translation in Google's Incognito mode.

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.

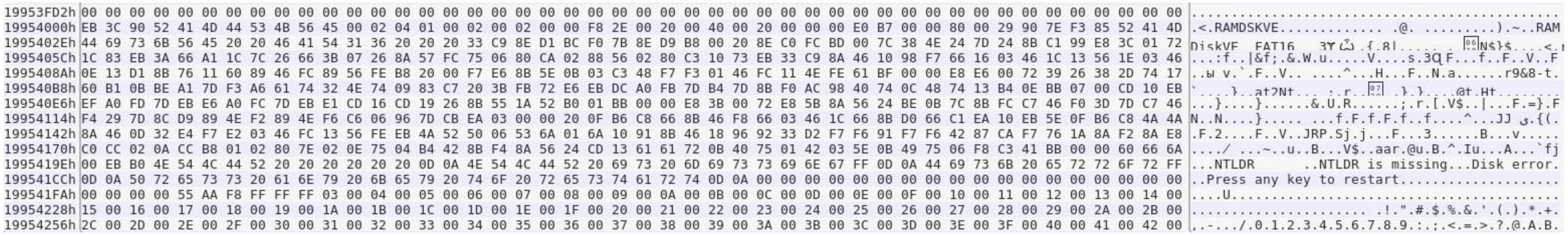
Table 9 – Comparison of the documentation with the results from the analysis regarding the protection that is offered by private mode in each browser. †

Artefact / Browser	**Chrome**				**Firefox**		**Internet Explorer**		**Opera**	
	Private		Guest							
	Documentation	Analysis	Documentation	Analysis	Documentation	Analysis	Documentation	Analysis	Documentation	Analysis
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. 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.

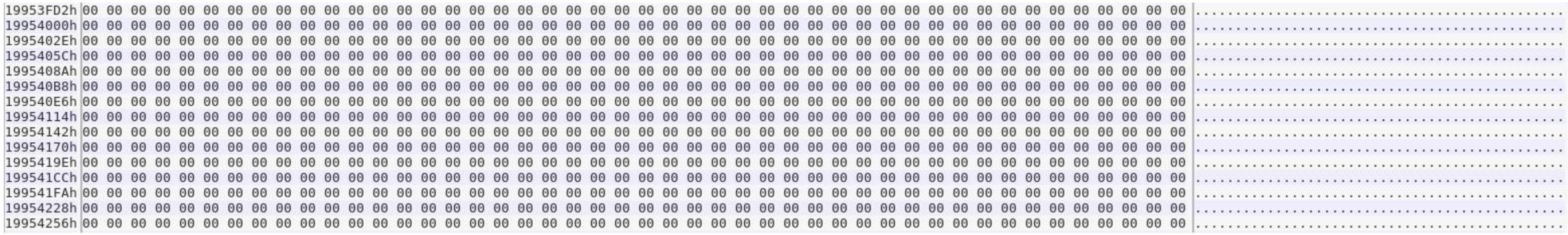
Table 15 – Browser configuration steps (RAMDisk, 2016)

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



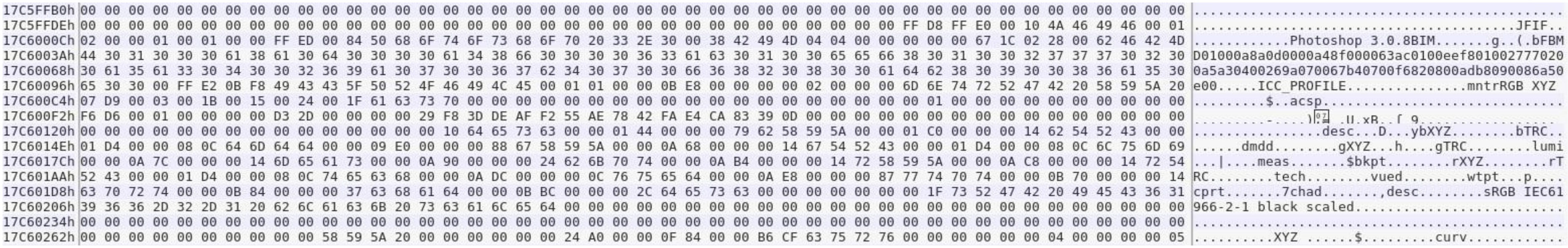
```
19953FD2h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
19954000h EB 3C 90 52 41 4D 44 53 4B 56 45 00 02 04 01 00 02 00 02 00 00 F8 2E 00 20 00 40 00 20 00 00 00 E0 B7 00 00 80 00 29 90 7E F3 85 52 41 4D .<.RAMDSKVE............. .@. .........).~..RAM
1995402Eh 44 69 73 6B 56 45 20 20 46 41 54 31 36 20 20 20 33 C9 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C 38 4E 24 7D 24 8B C1 99 E8 3C 01 72 DiskVE  FAT16   3ɣ ڤ .{.8|....... N$}$....<.r
1995405Ch 1C 83 EB 3A 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA 02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7 66 16 03 46 1C 13 56 1E 03 46 ...:f..|&f;.&.W.u.....V....s.3ɋF...f..F..V..F
1995408Ah 0E 13 D1 8B 76 11 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6 00 72 39 26 38 2D 74 17 ..ы v.`.F..V.. ....^...H...F..N.a......r9&8-t.
199540B8h 60 B1 0B BE A1 7D F3 A6 61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB DC A0 FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 13 B4 0E BB 07 00 CD 10 EB `....}..at2Nt... ;.r.. .}.}....@t.Ht........
199540E6h EF A0 FD 7D EB E6 A0 FC 7D EB E1 CD 16 CD 19 26 8B 55 1A 52 B0 01 BB 00 00 E8 3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0 3D 7D C7 46 ...}....}......&.U.R......;.r.[.V$..|...F.=}.F
19954114h F4 29 7D 8C D9 89 4E F2 89 4E F6 C6 06 96 7D CB EA 03 00 00 20 0F B6 C8 66 8B 46 F8 66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8 4A 4A N..N....}..... ...f.F.f.F.f..f....^...JJ ى.{(.
19954142h 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB 4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33 D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8 .F.2....F..V..JRP.Sj.j...F...3......B...v.....
19954170h C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42 8B F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A ..../ ...~..u..B...V$..aar.@u.B.^.Iu...A...`fj
1995419Eh 00 EB B0 4E 54 4C 44 52 20 20 20 20 20 20 0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69 6E 67 FF 0D 0A 44 69 73 6B 20 65 72 72 6F 72 FF ...NTLDR      ..NTLDR is missing...Disk error.
199541CCh 0D 0A 50 72 65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..Press any key to restart....................
199541FAh 00 00 00 00 55 AA F8 FF FF FF 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00 0F 00 10 00 11 00 12 00 13 00 14 00 ....U.........................................
19954228h 15 00 16 00 17 00 18 00 19 00 1A 00 1B 00 1C 00 1D 00 1E 00 1F 00 20 00 21 00 22 00 23 00 24 00 25 00 26 00 27 00 28 00 29 00 2A 00 2B 00 ...................... .!.".#.$.%.&.'.(.).*.+.
19954256h 2C 00 2D 00 2E 00 2F 00 30 00 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00 39 00 3A 00 3B 00 3C 00 3D 00 3E 00 3F 00 40 00 41 00 42 00 ,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.?.@.A.B.
```

Figure 24 – FAT boot sector of the Scenario 1 while RAMDisk's process is alive.



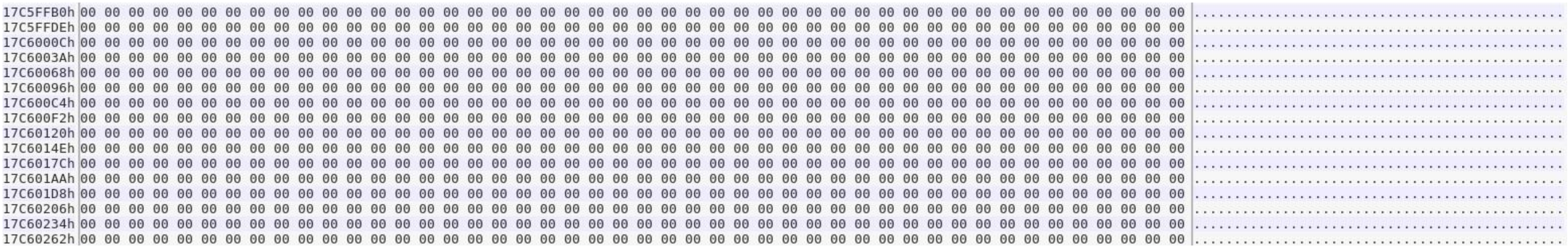
```
19953FD2h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
19954000h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
1995402Eh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
1995405Ch 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
1995408Ah 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
199540B8h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
199540E6h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
19954114h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
19954142h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
19954170h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
1995419Eh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
199541CCh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
199541FAh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
19954228h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
19954256h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
```

Figure 25 – FAT boot sector of the Scenario 1 after the termination of RAMDisk's process.



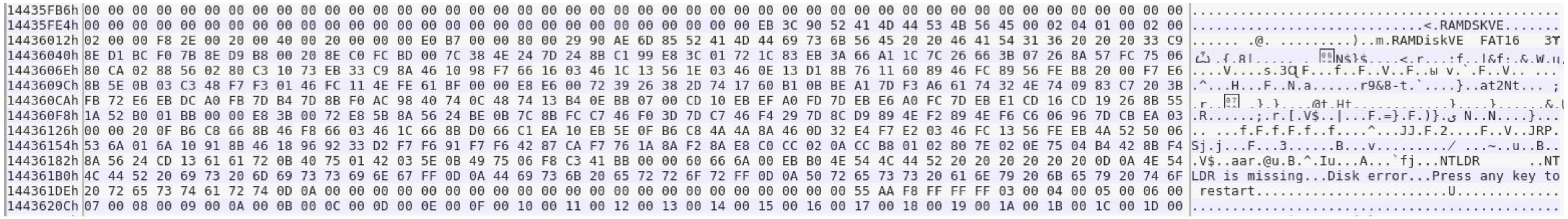
```
17C5FFB0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C5FFDEh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF D8 FF E0 00 10 4A 46 49 46 00 01 ....................................JFIF..
17C6000Ch 02 00 00 01 00 01 00 00 FF ED 00 84 50 68 6F 74 6F 73 68 6F 70 20 33 2E 30 00 38 42 49 4D 04 04 00 00 00 00 00 67 1C 02 28 00 62 46 42 4D ............Photoshop 3.0.8BIM.......g..(.bFBM
17C6003Ah 44 30 31 30 30 30 61 38 61 30 64 30 30 30 30 61 34 38 66 30 30 30 30 36 33 61 63 30 31 30 30 65 65 66 38 30 31 30 30 32 37 37 37 30 32 30 D01000a8a0d0000a48f000063ac0100eef801002777020
17C60068h 30 61 35 61 33 30 34 30 30 32 36 39 61 30 37 30 30 36 37 62 34 30 37 30 30 66 36 38 32 30 38 30 30 61 64 62 38 30 39 30 30 38 36 61 35 30 0a5a30400269a070067b40700f6820800adb8090086a50
17C60096h 65 30 30 00 FF E2 0B F8 49 43 43 5F 50 52 4F 46 49 4C 45 00 01 01 00 00 0B E8 00 00 00 00 02 00 00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 e00.....ICC_PROFILE..............mntrRGB XYZ 
17C600C4h 07 D9 00 03 00 1B 00 15 00 24 00 1F 61 63 73 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 .........$..acsp..............................
17C600F2h F6 D6 00 01 00 00 00 00 D3 2D 00 00 00 00 29 F8 3D DE AF F2 55 AE 78 42 FA E4 CA 83 39 0D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .........-....)  .U.xB..Ґ 9.................
17C60120h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 64 65 73 63 00 00 01 44 00 00 00 79 62 58 59 5A 00 00 01 C0 00 00 00 14 62 54 52 43 00 00 ................desc...D...ybXYZ........bTRC..
17C6014Eh 01 D4 00 00 08 0C 64 6D 64 64 00 00 09 E0 00 00 00 88 67 58 59 5A 00 00 0A 68 00 00 00 14 67 54 52 43 00 00 01 D4 00 00 08 0C 6C 75 6D 69 ......dmdd........gXYZ...h....gTRC........lumi
17C6017Ch 00 00 0A 7C 00 00 00 14 6D 65 61 73 00 00 0A 90 00 00 00 24 62 6B 70 74 00 00 0A B4 00 00 00 14 72 58 59 5A 00 00 0A C8 00 00 00 14 72 54 ...|....meas.......$bkpt........rXYZ........rT
17C601AAh 52 43 00 00 01 D4 00 00 08 0C 74 65 63 68 00 00 0A DC 00 00 00 0C 76 75 65 64 00 00 0A E8 00 00 00 87 77 74 70 74 00 00 0B 70 00 00 00 14 RC........tech........vued........wtpt...p....
17C601D8h 63 70 72 74 00 00 0B 84 00 00 00 37 63 68 61 64 00 00 0B BC 00 00 00 2C 64 65 73 63 00 00 00 00 00 00 00 1F 73 52 47 42 20 49 45 43 36 31 cprt.......7chad.......,desc........sRGB IEC61
17C60206h 39 36 36 2D 32 2D 31 20 62 6C 61 63 6B 20 73 63 61 6C 65 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 966-2-1 black scaled..........................
17C60234h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C60262h 00 00 00 00 00 00 00 00 00 00 58 59 5A 20 00 00 00 00 00 00 24 A0 00 00 0F 84 00 00 B6 CF 63 75 72 76 00 00 00 00 00 00 00 04 00 00 00 00 05 ..........XYZ ......$.........curv............
```

Figure 26 – JPEG header and beginning of its contents of the Scenario 1 while RAMDisk's process is alive**.**



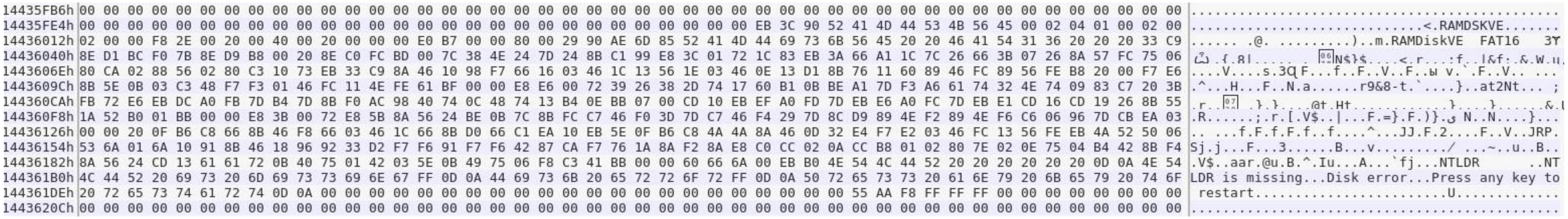
```
17C5FFB0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C5FFDEh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C6000Ch 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C6003Ah 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C60068h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C60096h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C600C4h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C600F2h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C60120h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C6014Eh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C6017Ch 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C601AAh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C601D8h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C60206h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C60234h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17C60262h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
```

Figure 27 – JPEG header and beginning of its contents of the Scenario 1 after the termination of RAMDisk's process.



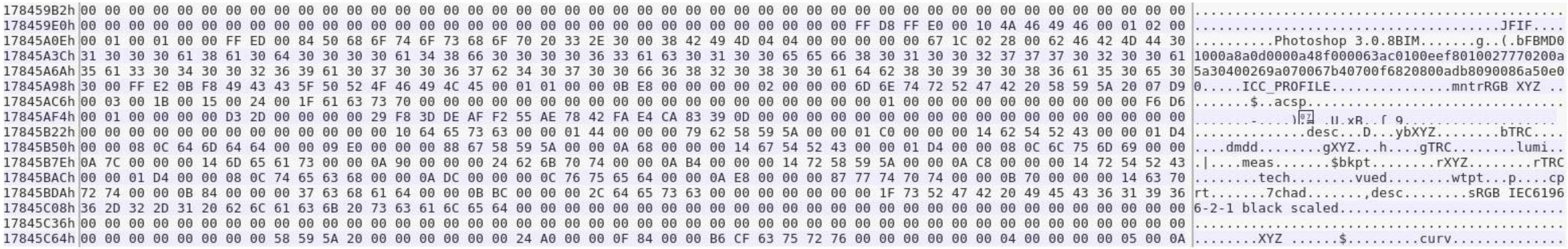
```
14435FB6h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
14435FE4h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 EB 3C 90 52 41 4D 44 53 4B 56 45 00 02 04 01 00 02 00 .............................<.RAMDSKVE.......
14436012h 02 00 00 F8 2E 00 20 00 40 00 20 00 00 00 E0 B7 00 00 80 00 29 90 AE 6D 85 52 41 4D 44 69 73 6B 56 45 20 20 46 41 54 31 36 20 20 20 33 C9 ...... .@. .........)..m.RAMDiskVE  FAT16   3ϒ
14436040h 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C 38 4E 24 7D 24 8B C1 99 E8 3C 01 72 1C 83 EB 3A 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 ᑕ.{.8l......  ␆N$}$....<.r...:f..|&f:.&.W.u.
1443606Eh 80 CA 02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 60 89 46 FC 89 56 FE B8 20 00 F7 E6 ....V....s.3Ɋ F...f..F..V..F..ы v.`.F..V.. ...
1443609Ch 8B 5E 0B 03 C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6 00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6 61 74 32 4E 74 09 83 C7 20 3B .^...H...F..N.a......r9&8-t.`....}..at2Nt... ;
144360CAh FB 72 E6 EB DC A0 FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 13 B4 0E BB 07 00 CD 10 EB EF A0 FD 7D EB E6 A0 FC 7D EB E1 CD 16 CD 19 26 8B 55 .r..␇ .}.}....@t.Ht...........}....}......&.U
144360F8h 1A 52 B0 01 BB 00 00 E8 3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0 3D 7D C7 46 F4 29 7D 8C D9 89 4E F2 89 4E F6 C6 06 96 7D CB EA 03 .R......;.r.[.V$..|...F.=}.F.)}.ى N..N....}...
14436126h 00 00 20 0F B6 C8 66 8B 46 F8 66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8 4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB 4A 52 50 06 .. ...f.F.f.F.f..f....^...JJ.F.2....F..V..JRP.
14436154h 53 6A 01 6A 10 91 8B 46 18 96 92 33 D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8 C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42 8B F4 Sj.j...F...3......B...v........./ ...~..u..B..
14436182h 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A 00 EB B0 4E 54 4C 44 52 20 20 20 20 20 20 0D 0A 4E 54 .V$..aar.@u.B.^.Iu...A...`fj...NTLDR      ..NT
144361B0h 4C 44 52 20 69 73 20 6D 69 73 73 69 6E 67 FF 0D 0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F LDR is missing...Disk error...Press any key to
144361DEh 20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA F8 FF FF FF 03 00 04 00 05 00 06 00  restart.......................U............
1443620Ch 07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00 0F 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1A 00 1B 00 1C 00 1D 00 ..............................................
```

Figure 28 – FAT boot sector of the Scenario 2 before the use of the file shredder.



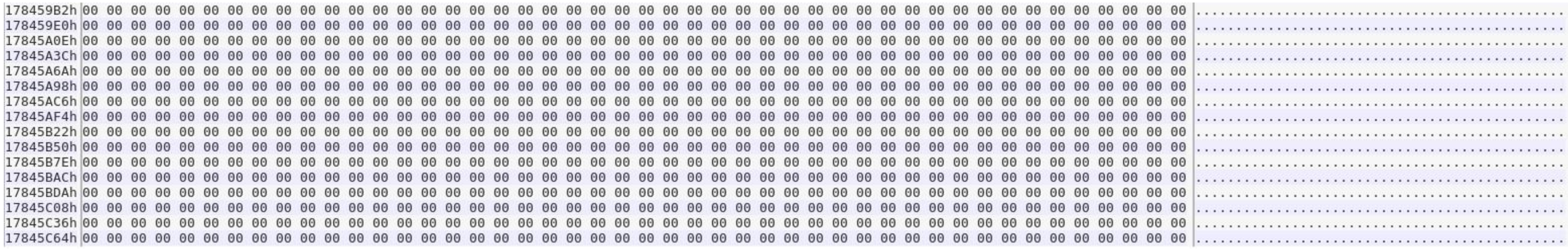
```
14435FB6h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
14435FE4h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 EB 3C 90 52 41 4D 44 53 4B 56 45 00 02 04 01 00 02 00 .............................<.RAMDSKVE.......
14436012h 02 00 00 F8 2E 00 20 00 40 00 20 00 00 00 E0 B7 00 00 80 00 29 90 AE 6D 85 52 41 4D 44 69 73 6B 56 45 20 20 46 41 54 31 36 20 20 20 33 C9 ...... .@. .........)..m.RAMDiskVE  FAT16   3ϒ
14436040h 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C 38 4E 24 7D 24 8B C1 99 E8 3C 01 72 1C 83 EB 3A 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 ᑕ.{.8l......  ␆N$}$....<.r...:f..|&f:.&.W.u.
1443606Eh 80 CA 02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 60 89 46 FC 89 56 FE B8 20 00 F7 E6 ....V....s.3Ɋ F...f..F..V..F..ы v.`.F..V.. ...
1443609Ch 8B 5E 0B 03 C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6 00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6 61 74 32 4E 74 09 83 C7 20 3B .^...H...F..N.a......r9&8-t.`....}..at2Nt... ;
144360CAh FB 72 E6 EB DC A0 FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 13 B4 0E BB 07 00 CD 10 EB EF A0 FD 7D EB E6 A0 FC 7D EB E1 CD 16 CD 19 26 8B 55 .r..␇ .}.}....@t.Ht...........}....}......&.U
144360F8h 1A 52 B0 01 BB 00 00 E8 3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0 3D 7D C7 46 F4 29 7D 8C D9 89 4E F2 89 4E F6 C6 06 96 7D CB EA 03 .R......;.r.[.V$..|...F.=}.F.)}.ى N..N....}...
14436126h 00 00 20 0F B6 C8 66 8B 46 F8 66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8 4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB 4A 52 50 06 .. ...f.F.f.F.f..f....^...JJ.F.2....F..V..JRP.
14436154h 53 6A 01 6A 10 91 8B 46 18 96 92 33 D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8 C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42 8B F4 Sj.j...F...3......B...v........./ ...~..u..B..
14436182h 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A 00 EB B0 4E 54 4C 44 52 20 20 20 20 20 20 0D 0A 4E 54 .V$..aar.@u.B.^.Iu...A...`fj...NTLDR      ..NT
144361B0h 4C 44 52 20 69 73 20 6D 69 73 73 69 6E 67 FF 0D 0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F LDR is missing...Disk error...Press any key to
144361DEh 20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA F8 FF FF FF 00 00 00 00 00 00 00 00 00 00  restart.......................U............
1443620Ch 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
```

Figure 29 – FAT boot sector of the Scenario 2 after the use of the file shredder.



```
178459B2h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
178459E0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF D8 FF E0 00 10 4A 46 49 46 00 01 02 00 ......................................JFIF....
17845A0Eh 00 01 00 01 00 00 FF ED 00 84 50 68 6F 74 6F 73 68 6F 70 20 33 2E 30 00 38 42 49 4D 04 04 00 00 00 00 00 67 1C 02 28 00 62 46 42 4D 44 30 ..........Photoshop 3.0.8BIM.......g..(.bFBMD0
17845A3Ch 31 30 30 30 61 38 61 30 64 30 30 30 30 61 34 38 66 30 30 30 30 36 33 61 63 30 31 30 30 65 65 66 38 30 31 30 30 32 37 37 37 30 32 30 30 61 1000a8a0d0000a48f000063ac0100eef8010027770200a
17845A6Ah 35 61 33 30 34 30 30 32 36 39 61 30 37 30 30 36 37 62 34 30 37 30 30 66 36 38 32 30 38 30 30 61 64 62 38 30 39 30 30 38 36 61 35 30 65 30 5a30400269a070067b40700f6820800adb8090086a50e0
17845A98h 30 00 FF E2 0B F8 49 43 43 5F 50 52 4F 46 49 4C 45 00 01 01 00 00 0B E8 00 00 00 00 02 00 00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07 D9 0.....ICC_PROFILE...............mntrRGB XYZ ..
17845AC6h 00 03 00 1B 00 15 00 24 00 1F 61 63 73 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 F6 D6 .......$..acsp................................
17845AF4h 00 01 00 00 00 00 D3 2D 00 00 00 00 29 F8 3D DE AF F2 55 AE 78 42 FA E4 CA 83 39 0D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......-....)□ .U.xB..ʃ.9.....................
17845B22h 00 00 00 00 00 00 00 00 00 00 00 00 00 10 64 65 73 63 00 00 01 44 00 00 00 79 62 58 59 5A 00 00 01 C0 00 00 00 14 62 54 52 43 00 00 01 D4 ..............desc...D...ybXYZ........bTRC....
17845B50h 00 00 08 0C 64 6D 64 64 00 00 09 E0 00 00 00 88 67 58 59 5A 00 00 0A 68 00 00 00 14 67 54 52 43 00 00 01 D4 00 00 08 0C 6C 75 6D 69 00 00 ....dmdd........gXYZ...h....gTRC........lumi..
17845B7Eh 0A 7C 00 00 00 14 6D 65 61 73 00 00 0A 90 00 00 00 24 62 6B 70 74 00 00 0A B4 00 00 00 14 72 58 59 5A 00 00 0A C8 00 00 00 14 72 54 52 43 .|....meas.......$bkpt........rXYZ........rTRC
17845BACh 00 00 01 D4 00 00 08 0C 74 65 63 68 00 00 0A DC 00 00 00 0C 76 75 65 64 00 00 0A E8 00 00 00 87 77 74 70 74 00 00 0B 70 00 00 00 14 63 70 ........tech........vued........wtpt...p....cp
17845BDAh 72 74 00 00 0B 84 00 00 00 37 63 68 61 64 00 00 0B BC 00 00 00 2C 64 65 73 63 00 00 00 00 00 00 00 1F 73 52 47 42 20 49 45 43 36 31 39 36 rt.......7chad.......,desc........sRGB IEC6196
17845C08h 36 2D 32 2D 31 20 62 6C 61 63 6B 20 73 63 61 6C 65 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6-2-1 black scaled............................
17845C36h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845C64h 00 00 00 00 00 00 00 00 58 59 5A 20 00 00 00 00 00 00 24 A0 00 00 0F 84 00 00 B6 CF 63 75 72 76 00 00 00 00 00 00 04 00 00 00 00 05 00 0A ........XYZ ......$.........curv..............
```

Figure 30 – JPEG header and beginning of its contents of the Scenario 2 before the use of the file shredder.



```
178459B2h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
178459E0h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845A0Eh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845A3Ch 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845A6Ah 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845A98h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845AC6h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845AF4h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845B22h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845B50h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845B7Eh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845BACh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845BDAh 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845C08h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845C36h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
17845C64h 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................................
```

Figure 31 – JPEG header and beginning of its contents of the Scenario 2 after the use of the file shredder