DOI: http://dx.doi.org/10.5769/C2011021

Webmail evidence recovery: a comparison among the most used Web browsers and webmail services

Pedro Monteiro da Silva Eleutério[a], Jane Dirce Alves Sandim Eleutério[b]
"(a) Brazilian Federal Police (DPF), pedro.pmse@dpf.gov.br, Campo Grande/MS – Brazil"
"(b) College of Computing - Federal University of Mato Grosso do Sul (FACOM-UFMS), jane@facom.ufms.br, Campo Grande/MS – Brazil"

Abstract — The content of electronic messages is often very useful in criminal investigations. Many Internet users use a free webmail service, which stores the electronic messages on remote servers. Thus, these messages are not directly stored on the digital devices seized by law enforcement. However, Web browsers have a caching function, which might store locally some hypertexts browsed by the user. The main objective of this work is to establish a relationship among the most used Web browsers and webmail services, helping forensic experts to recover such evidence more quickly and efficiently. The performed experiments showed this type of evidence may be find in different areas/files in hard disk drives and may vary depending on the Web browser and webmail service used.

Keywords — computer forensics, webmail recovery, caching function, Web browser, data carving.

1. Introduction

Forensic analysis on computer storage media are an important source of information for modern criminal investigations. The main storage digital device for computer forensics is the hard disk drive (HDD). Consequently, these devices can store plenty of evidence to assist in solving various types of crimes [1]. A type of evidence that often helps the investigations is the electronic message (email), which can contain a variety of information about the perpetrators, accomplices, and store relevant data.

The webmail services for electronic messaging are very used by Internet users. A recent research [2] showed that webmail is the most popular service on the World Wide Web, being used by 70% of all American Internet users in 2010. Several companies offer these services for free, just asking users to do a simple registration. After registered, users can initiate electronic message exchanging without difficulty, needing only a Web browser.

According to W3Schools [3], as shown in Figure 1(a), the three most used Web browsers in June 2011 are: Mozilla Firefox, Google Chrome and Microsoft Internet Explorer, with 42.2%, 27.9% and 23.2% of usage, respectively.

Another research [4] showed that Yahoo! Mail is the most used webmail service by American webmail users, with 44%. Microsoft Hotmail (Windows Live Mail) was in second place with 30%, followed by Google Gmail, in third place, with 15%, as show in Figure 1(b). Recent researches of the usage of webmail services in Brazil were not found in the literature, but it is known that these three webmail services are also very used, maybe in a different rank order.

All exchanged webmail messages are stored on remote computers (servers) of webmail provider companies, not being directly saved on the hard disk drive of the user's computer. However, the major Web browsers have the caching function, which can automatically save some of the browsed hypertexts

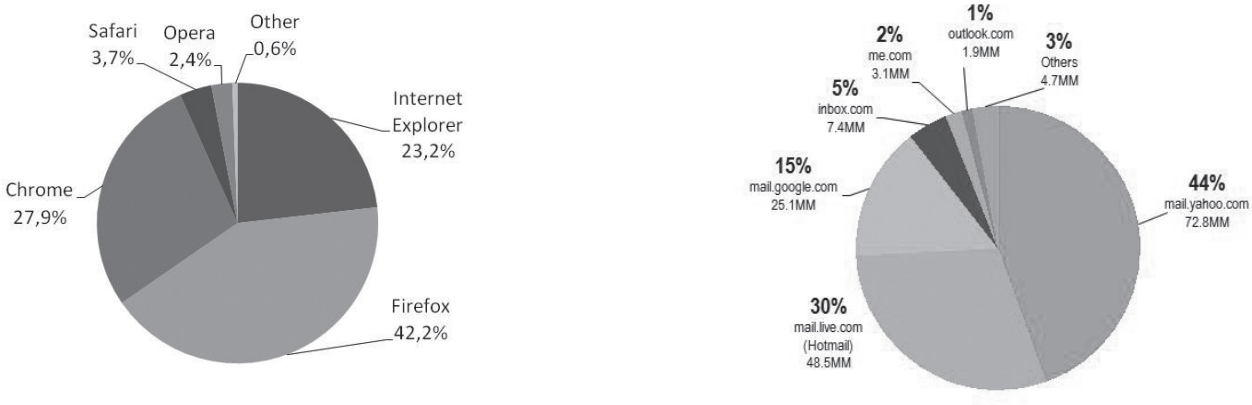

Fig. 1. (a) The most used Web browsers [3] and (b) the most used webmail services [4].

(and their elements) in the local hard disk drive [5]. Thus, forensic analysis in these hard disks can recover some data of browsed sites, especially with the technique of Data Carving [6], which can recover files based on the search for signatures of known file types in any digital storage device and any file system [7].

There are several Web browsers and each one has its own implementation of caching function. The major webmail services have different graphics user interfaces and use different technologies. Thus, it is unknown how and when webmail electronic messages will be stored on the local hard disk drive by browser caching functions. Another problem encountered by forensic examiners during analysis is the forensic tools. There is no guarantee that they will always recover and identify webmail hypertexts among the many other hypertexts stored on seized devices, which makes the task of finding webmail evidence harder.

Therefore, the main objective of this work is to establish a relationship among Web browsers and free webmail services in order to understand the behavior of browser caching function, helping forensic experts to find webmail evidence in a less arduous and more efficient way. To achieve the goals, experiments were conducted with the most used Web browsers on the market [3], such as Microsoft Internet Explorer 9, Mozilla Firefox 5 and Google Chrome 12, together with the most used free webmail services [4], such as Microsoft Hotmail, Google Gmail and Yahoo! Mail.

This article is organized as follows: section 2 presents some background concepts such as Data Carving, webmail and browser caching function. The various performed experiments, including the methodology used, are described in Section 3. The results and their analysis are discussed in Section 4. Finally, Sections 5 and 6 show the conclusions and ideas for future work related to the topic.

2. Background

This section shows a briefly description of concepts such as webmail, Web browsers and its caching function. In addition, Data Carving technique, widely used in computer forensics for data recovery, is discussed.

2.1. Webmail and Web Browser

Electronic messaging has always been one of the most used World Wide Web services by users. Today, the exchange of electronic messages among members of "old generations" is very popular. That means the use of emails is not restricted to new generations. A recent research [2] showed that the webmail usage of American people between 55 and 64 years increased 15% in the last year.

In recent years, with the advent of Cloud Computing [8] and Mobile Computing [9], several companies have emerged and started to provide webmail service for free, leading many people to use a webmail instead of local messaging programs, such as Microsoft Outlook and Mozilla Thunderbird. Because the webmail electronic messages are stored on remote servers, the biggest advantage of using them is that users can get access to their messages from any Internet-connected computer, requiring only a Web browser. As described before, webmail is the most popular service of the World Wide Web [2].

For computer forensics, it's more difficult to find webmail evidence, since the electronic messages are not explicitly saved to the hard disk of the user's computer. However, Web browsers have a caching function [5], which might store some data of browsed sites, including webmail, on the local hard disk. This function is discussed below.

2.2. Caching Function

One of the most active areas of research on the Internet is how to make effective caching function on Web pages [5]. From a client perspective, a page that can be recovered from a near location, such as the local hard disk, can be displayed more quickly than it needed to be downloaded from a remote server in the world. From the perspective of the server, when a caching function intercepts and answers a request, it reduces the server load [5].

The caching function can be implemented in many different places [10]. For example, a user's Web browser can use the caching function for recently accessed pages, as shown in Figure 2, and simply show a copy of them if the

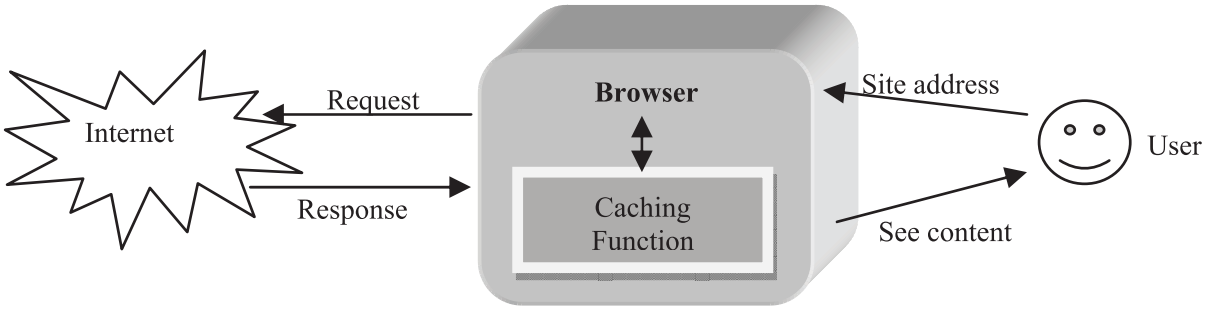

Fig. 2. When a user types a site address on the Web browser, it makes a request for content.
After getting the response, the browser might store the hypertexts and its elements locally for future use, leaving evidence that may be found by the forensic examiner.

user visits the same page again. It can also be implemented in an Internet Service Providers or in other network locations.

The caching function of Web pages is so important for the Internet. Thus, the HTTP protocol was designed to make this task easier [5]. The caching function needs to make sure that is not responding with an outdated version of the page. For example, the server assigns an expiration date for every page ("Expires" field) that sends back to the client. The caching function stores the date and does not need to check the page again until the expiration date is still valid. In addition, the HTTP protocol also supports the called "conditional get" ("If-Modified-Since" field) to check if there is a newer version of the page on the server, without download the entire page data [5].

However, setting the amount of time which pages should be on caching can be a little tricky. Some pages should never be stored by caching functions [11]. For example, a page containing the prices of exchange rates of major world currencies changes every second. If it was stored locally by caching function, a user who obtained a copy of the stored page will receive outdated information. Therefore, the caching function must used with care. Web pages that keep dynamic content, for example, generated by PHP / JSP scripts, should never be cached, because the parameters can be different next time [11]. Some webmail services can be classified into this category, because they are becoming more dynamic and with more usability, using new technologies such as Ajax [12], and combining some techniques, known as Dynamic HTML [13]. Thus, this may affect the local storage of webmail services, because the client-server communication can be performed directly by scripts, not being requested a new entire Web page to the server.

The browser caching function can save time and network bandwidth, making browsing faster, but on the other hand, requires processing and disk space on the user's computer. This entire process is done automatically by the browser, and it is invisible to the user [14]. The caching function is enabled by default on all major browsers. Most Internet users have no idea of this function and, for computer forensics, this is a very important factor, because it will be possible to recover data of browsed sites, which may include some exchanged webmail messages. One of the used techniques to recover data is Data Carving [6], which is described below.

2.3. Data Carving

Data Carving is a technique to recover files based on the search for signatures of known file types in a storage device. When a known file signature is found, it tries to search for the file contents, recovering the original information in whole or in part [6].

This technique relies on some assumptions [6]: (i) the beginning of the file, which includes the signature, must be present; (ii) "false hits" will occur in the attempt to recover files, because the file signatures can be found in many other files and in fragmented data; and (iii) the files to be recover must be contiguous and not fragmented.

Because this technique can be applied to cover every bit of a hard drive without the help of a file system [7], for example, this procedure allows recovering temporary files, including not directly saved files by the user. Hence, this technique can be applied in an attempt to retrieve the contents of browsed sites (hypertexts and its elements), since these files have a known format and, as already discussed, can be temporarily stored by browser caching function. Thus, this study also demonstrates the effectiveness of Data Carving for the recovery of webmail evidence.

3. Experiments and Methodology

In order to obtain a relationship among the most used Web browsers and webmail services, and to verify what and where evidence will be stored on local hard disks by browser caching function (or any other OS procedure), this section describes the material, the experiments performed and the methodology used in this work.

3.4. Material

The material (hardware) used in all the experiments were: a computer with an Intel i5 processor, motherboard Asus and 2GB RAM memory, plus six Seagate hard disk drives with a capacity of 20GB each.

The software used were: Microsoft Windows 7 Enterprise 64-bits; Microsoft Internet Explorer 9, build 9.0.8112.16421; Mozilla Firefox 5, build 5.0; Google Chrome 12, build 12.0.742.112, and; Forensic Tool Kit (FTK), version 1.81.6, for evidence recovery and forensic analysis.

3.5. Experiments

The major objective of the experiments is to check the evidence left by different webmail services in different Web browsers. Therefore, we considered the three most used Web browsers (Microsoft Internet Explorer, Mozilla Firefox and Google Chrome) [3] and the three most used free webmail services (Microsoft Hotmail, Google Gmail and Yahoo! Mail) [4]. During installation, configuration and usage, only the default options were chosen.

The following steps were performed in the experiments:

1. Three hard disk drives were formatted and received a completely new installation of Windows 7 Enterprise 64-bits. Only the default options were chosen. The option of automatic updates of Windows was disabled, so this service did not interfere with the temporary storage of data;
2. The first hard drive received a new installation of Microsoft Internet Explorer 9. On the second hard drive was installed Mozilla Firefox 5. Finally, Google Chrome 12 was installed on the third disk. All browsers were installed using default settings and the most current

versions at the time of the experiments, as described on the material section;

3. For each of the three hard disk drives, the following operations were done:
    a. Windows 7 OS was started and the installed Web browser (IE, Firefox or Chrome) was opened;
    b. The address *http://www.hotmail.com* was typed on browser and a new Hotmail account was created;
    c. The new Hotmail account was accessed and the introductory message was read;
    d. Two new emails to a common recipient were written;
    e. The Hotmail account was logged out;
    f. The address *http://www.gmail.com* was typed on browser and a new Gmail account was created;
    g. The new Gmail account was accessed and the introductory messages were read;
    h. Two new emails to a common recipient were written;
    i. The Gmail account was logged out;
    j. The address *http://mail.yahoo.com* was typed on browser and a new Yahoo! Mail account was created;
    k. The new Yahoo! Mail account was accessed and the introductory message was read;
    l. Two new emails to a common recipient were written;
    m. The Yahoo! Mail account was logged out;
    n. The browser was closed and the Windows 7 OS was turned off.
4. Using another computer, the authors accessed the email account which received the 18 emails written in Step 3 (six messages for each browser). All emails were read and the first message of each browser and each webmail service was replied;
5. Two new email messages were written for each of the nine email accounts created (three email accounts on each browser). The second message sent for each one had a text file attached;
6. For each of the three hard disk drives, the following operations were done:
    a. Windows 7 OS was started and the installed Web browser (IE, Firefox or Chrome) was opened;
    b. The address *http://www.hotmail.com* was typed on browser and the Hotmail account was accessed;
    c. The reply of first message sent (step 4) was read;
    d. The two messages received (written in step 5) was read. The first one was replied. The attachment contained in the second message received was read using only the "open" option, without save it on hard disk drive;
    e. The Hotmail account was logged out;
    f. The address *http://www.gmail.com* was typed on browser and the Hotmail account was accessed;
    g. The reply of first message sent (step 4) was read;
    h. The two messages received (written in step 5) was read. The first one was replied. The attachment contained in the second message received was read using only the "open" option, without save it on hard disk drive;
    i. The Gmail account was logged out;
    j. The address *http://mail.yahoo.com* was typed on browser and the Yahoo! Mail account was accessed;
    k. The reply of first message sent (step 4) was read;
    l. The two messages received (written in step 5) was read. The first one was replied. The attachment contained in the second message received was read using only the "open" option, without save it on hard disk drive;
    m. The Yahoo! Mail account was logged out;
    n. The browser was closed and the Windows 7 OS was turned off.
7. Subsequently, the three hard drives were duplicated (cloned) to other three HDDs for data preservation. With Forensic Tool Kit (FTK), three new cases were created for each cloned HDD with disk indexation option enabled and all types of Data Carving;
8. Each cloned HDDs were analyzed by the authors, who searched for webmail evidence, filling out the result tables.

To help understand the experiments, Figure 3 shows a diagram that summarizes the steps performed.

All written messages, including the replied ones, were different in order to be able to identify the evidence according to the browser and webmail service used. The time spent in the operations described in steps 3 and 6 was almost the same for each of the three hard drives (with different Web browsers) to not interfere with the results.

For each created case in FTK, the same searches were conducted in order to find traces of electronic messages, considering the differences among Web browsers. For example, in the case of Microsoft Internet Explorer, the temporally hypertexts were stored in the "*Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files*" folder, while in Firefox, the folder was "*Users\user\AppData\Local\Mozilla\Firefox\Profiles*". However, the entire hard disk drives were analyzed, including not allocated areas (free spaces), system files and fragmented files.

Data Carving function provided by Forensic Tool Kit was enabled in all three cases. The recovered files by this technique were especially analyzed.

During the search for evidence, the main goal was to recover the content of the exchanged messages. Thus, searches for the

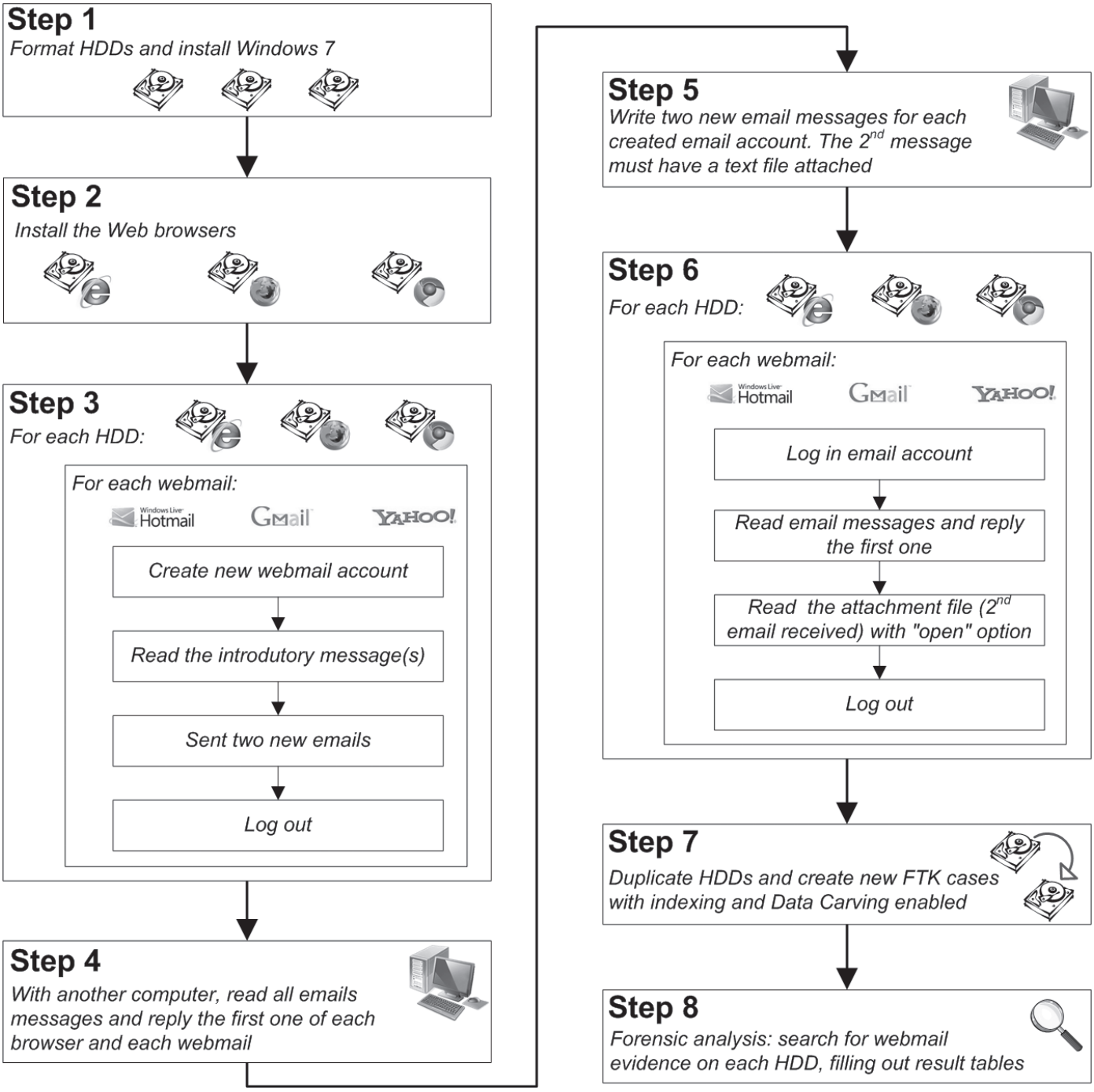

Fig. 3. Summary of performed steps on the experiments. In step 8 (forensic analysis), three tables were filled out with the results.

words contained in these messages were carried. Moreover, several searches for verification of the attached files (step 6.i) and email accounts used were performed too. During the forensic analysis, for each HDD, a result table was filled out with the results, as discussed below.

3.6. Methodology

In order to establish a relationship among the results obtained during step 8 of the experiments (forensic analysis), a result table for each one of the hard disk drives was filled out. Table 1 shows the answered questions and their descriptions, where it's possible to see that the experiments tried to find, especially, the content of exchanged messages, which is often what matters in an investigation.

For each question, the answers should indicate whether the contents of the emails were found (*Yes or No*) and where they were stored: in temporary hypertext files or recovered hypertexts by Data Carving (*hypertext file*), in free spaces of unallocated areas of hard disk drive or slack files (*free space*) or in other system files, like page files, swap or other OS files

Table 1. Questions to be answered for each one of the hard disk drives.

Question: What evidence was found?	Description (For each webmail service)
Email account creation (*steps 3.b, 3.f, 3.j*)	Is it possible to recover the email account creation page?
Webmail login page (*steps 3.c, 3.g, 3.k, 6.b, 6.f, 6.j*)	Is it possible to recover the page where the users log into the email account?
First email sent (*steps 3.d, 3.h, 3.l*)	Is it possible to recover the content of first email sent?
Second email sent (*steps 3.d, 3.h, 3.l*)	Is it possible to recover the content of second email sent?
Reply of first email sent (*steps 6.c, 6.g, 6.k*)	Is it possible to recover the content of the reply of first email sent?
First email received (*steps 6.d, 6.h, 6.l*)	Is it possible to recover the content of first email received?
Reply of first email received (*steps 6.d, 6.h, 6.l*)	Is it possible to recover the content of the response (reply) of first email received?
Second email received (*steps 6.d, 6.h, 6.l*)	Is it possible to recover the content of second email received?
Attachment file of second email received (*steps 6.d, 6.h, 6.l*)	Is it possible to recover the content of the file attached on second email received?
Inbox list (*steps 6.b, 6.f, 6.j*)	Is it possible to recover the inbox (list of messages)?

(*system file*). Therefore, when the answer is "*Yes*", there must be an indication of where the evidence was found (*hypertext file*, *free space* or *system file*).

4. Results and Analysis

As described before, a different Web browser was installed on each of the three hard disk drives. Thus, Table 1 has been filled out in accordance with the evidence found for each of the three HDDs. Tables 2, 3 and 4 show the results for the HDDs that contain, respectively, the installed Web browsers: Microsoft Internet Explorer 9, Mozilla Firefox 5 and Google Chrome 12.

The results showed many points of interest for content recovery of exchanged webmail messages. As expected, it was possible to recover webmail evidence. Moreover, webmail evidences were not found in the same format and in the same areas of the HDDs. Some temporary and Data Carving recovered hypertexts were actually found on the hard disks (indicated as "hypertext file" in the tables of results). However, other evidences were found in system files (indicated as "system file"), especially in page files, and also in the unallocated area of hard disk, including slack files (indicated as "free space"). These results are important for the forensic experts, because they must know that recovered hypertexts by Data Carving technique are not enough to find all the evidence that webmail services can produce.

As expected, the experiments showed there are differences in Web browsers caching function and webmail services. First, it's possible to see that Microsoft Internet Explorer caching function stored more information of the webmail

Table 2.
Results for hard disk drive with Microsoft Internet Explorer 9 installed.

Browser:	MICROSOFT INTERNET EXPLORER 9		
Question: What evidence was found?	**Microsoft Hotmail**	**Google Gmail**	**Yahoo! Mail**
Email account creation (*steps 3.b, 3.f, 3.j*)	Yes (hypertext file - empty form)	No	No
Webmail login page (*steps 3.c, 3.g, 3.k, 6.b, 6.f, 6.j*)	Yes (system file)	Yes (hypertext file)	No
First email sent (*steps 3.d, 3.h, 3.l*)	Yes (hypertext file and free space)	No	No
Second email sent (*steps 3.d, 3.h, 3.l*)	Yes (system file and free space)	No	No
Reply of first email sent (*steps 6.c, 6.g, 6.k*)	No	No	No
First email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Reply of first email received (*steps 6.d, 6.h, 6.l*)	Yes (free space)	No	No
Second email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Attachment file of second email received (*steps 6.d, 6.h, 6.l*)	Yes (text file)	Yes (text file)	Yes (text file)
Inbox list (*steps 6.b, 6.f, 6.j*)	Yes (hypertext file)	Yes (free space)	No

services than other browsers. On the other hand, Mozilla Firefox caching was the last: only an electronic message was found on the hard drive examined. Google Chrome caching function was in the second position.

Microsoft Hotmail produced more evidence on the three hard drives examined, regardless of browser used. For some reason, the content of Hotmail pages had been copied more easily by the browser caching functions (and the operating system procedures too). On the other hand, the results showed that the forensic analysis was not able to restore any content of exchanged electronic messages through Yahoo! Mail in the three hard drives examined, but this does not mean that caching function cannot store Yahoo! Mail pages, because an inbox page was recovery on the hard disk with Firefox. Another factor of interest is that only the hard disk with Google Chrome installed was possible to recover

Table 3. Results for hard disk drive with Mozilla Firefox installed.

Browser:	MOZILLA FIREFOX 5		
Question: What evidence was found?	**Microsoft Hotmail**	**Google Gmail**	**Yahoo! Mail**
Email account creation (*steps 3.b, 3.f, 3.j*)	No	No	No
Webmail login page (*steps 3.c, 3.g, 3.k, 6.b, 6.f, 6.j*)	No	No	No
First email sent (*steps 3.d, 3.h, 3.l*)	Yes (hypertext file)	No	No
Second email sent (*steps 3.d, 3.h, 3.l*)	No	No	No
Reply of first email sent (*steps 6.c, 6.g, 6.k*)	No	No	No
First email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Reply of first email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Second email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Attachment file of second email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Inbox list (*steps 6.b, 6.f, 6.j*)	Yes (hypertext file)	No	Yes (system file)

an electronic message from Google Gmail. This may be an indication that the Google browser could be optimized to work with Google's own products - or just be a coincidence.

There were no traces of email account creation in the three hard disks examined, except an empty form to create a Hotmail account using Microsoft Internet Explorer. However, all created email addresses were found in the hard disk drives examined. Therefore, despite the content of some emails have not been recovered, it was possible to prove that such email addresses were part of some operations performed on the computer.

The identification of text files sent as attachments of electronic messages was a surprising result. As described before, the attached files were opened directly from emails with the "open" option, without explicitly save these files on the hard drives. During forensic analysis, all attached files from Microsoft Internet Explorer and Google Chrome were found saved in temporary folders and with their original names. However, there were no traces of the attached files in

Table 4. Results for hard disk drive with Google Chrome installed.

Browser:	GOOGLE CHROME 12		
Question: What evidence was found?	**Microsoft Hotmail**	**Google Gmail**	**Yahoo! Mail**
Email account creation (*steps 3.b, 3.f, 3.j*)	No	No	No
Webmail login page (*steps 3.c, 3.g, 3.k, 6.b, 6.f, 6.j*)	No	No	No
First email sent (*steps 3.d, 3.h, 3.l*)	Yes (hypertext file)	No	No
Second email sent (*steps 3.d, 3.h, 3.l*)	No	Yes (free space)	No
Reply of first email sent (*steps 6.c, 6.g, 6.k*)	No	No	No
First email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Reply of first email received (*steps 6.d, 6.h, 6.l*)	Yes (free space)	No	No
Second email received (*steps 6.d, 6.h, 6.l*)	No	No	No
Attachment file of second email received (*steps 6.d, 6.h, 6.l*)	Yes (text file)	Yes (text file)	Yes (text file)
Inbox list (*steps 6.b, 6.f, 6.j*)	Yes (hyper-text file)	Yes (free space)	No

the HDD with Mozilla Firefox. This result can be explained by the usage of RAM memory by Firefox to display the attachment files.

As showed in Tables 2, 3 and 4, it was possible to recover some evidence from inbox (list of messages) in all browsers and webmail services. However, each inbox was found in specific areas of the disk: Hotmail in hypertext files; Gmail in free spaces, and; Yahoo! in a system file.

The Forensic Tool Kit has a tab of electronic messages (emails), where the tool tries to separate email messages from other files found on the hard drive, including webmail. However, the FTK was not able to identify any email in the three hard drives examined, displaying "0" (zero) for email statistics. This fact may be justified by the FTK version used and by natural changes of the user graphical interfaces of webmail services, including new Web technologies, such as previously cited Ajax [12] and Dynamic HTML [13].

5. Conclusions

The content of exchanged electronic messages on a hard disk drive is an important evidence for the investigation of various crimes. However, it's not trivial to forensic tools automatically identify and separate these type of evidence, which may lead forensic experts to error.

This work showed that the evidence left by webmail usage varies according to the chosen service and the Web browser. In addition, browser caching functions and OS procedures can store the content of webmail messages, including attached files, even without a direct user action in saving content on the computer. This fact is very important for the forensic expert to identify such evidence and assist in investigations.

The performed experiments in this work showed that the content of webmail messages can be stored in different areas of the HDDs and in different formats, such hypertexts (native World Wide Web format), system files, including page files, or also in the not allocated area from the hard drive, including slack files. This work also proved that using a single forensic technique, such as Data Carving, may not find all the existing evidence in this type of forensic analysis. If forensic experts don't have an idea of the keywords to be searched for webmail messages in seized storage devices, they can use expressions like "@hotmail.com", "@gmail.com" and "@yahoo.com". Some of found webmail messages would be also recovered with searches using these keywords. Other important results were described on Section 4.

Therefore, this work proved that is possible to recover the content of exchanged webmail messages. However, it's not easy to find such digital evidence and the forensic experts should use a lot of computer forensic techniques to find them.

6. Future Work

This work can be continued in various ways. One future work is to compare the main characteristics of the source code of webmail services to be easily searched by forensic experts. Another suggestion is to conduct experiments with real-time monitoring of the page files, browser caching function and hard disk I/O, while webmail services is been used in different Web browsers. Other idea is to build a new forensic tool to specifically search for webmail evidence, for example, or find out other keywords to search for these electronic messages in the search features provided by existing forensic tools.

Acknowledgements

The authors thank the Brazilian Federal Police (DPF) and the Federal University of Mato Grosso do Sul for financial and logistic support.

References

[1] Eleutério, P.M.S.; Machado, M.P. "Desvendando a Computação Forense". Novatec Editora, ISBN: 978-85-7522-260-7. Jan, 2011. [in portuguese]

[2] comScore Inc - Press Release. "Web-based Email Shows Signs of Decline in the U.S. While Mobile Email Usage on the Rise". Available from *http://www.comscore.com/Press_Events/Press_Releases/2011/1/Web-based_Email_Shows_Signs_of_Decline_in_the_U.S._While_Mobile_ Email_Usage_on_the_Rise*. Jan, 2011. [Visited Jul, 2011].

[3] W3schools.com. "Browser Statistics Month by Month". Available from *http://www.w3schools.com/browsers/browsers_stats.asp*. [Visited Jul, 2011].

[4] Compete - pulse. "Gmail's buzz – much bigger than its bite?". Available from *http://blog.compete.com/2010/11/11/gmails-buzz-much-bigger-than-its-bite/*. Nov, 2010. [Visited Jul, 2011].

[5] Peterson, L.L.; Davie, B.S. "Computer Networks: A System Approach". Second Edition. ISBN 978-1558605145. Morgan Kaufmann Press, 1999.

[6] Dickerman, D. "Advanced Data Carving". IRS Criminal Investigation – Electronic Crimes Program of DFRWS 2006. Jul, 2006.

[7] Veenman, C.J. "Statistical Disk Cluster Classification for File Carving," ias, pp.393-398, 2007 The Third International Symposium on Information Assurance and Security, 2007.

[8] Armbrust, M. et al. "A View of Cloud Computing". Communications of the ACM, Vol. 53, issue: 4, pg. 50-58. New York, Apr. 2010.

[9] Forman, G.H; Zahorjan, J. "The Challenges of Mobile Computing," Computer, vol. 27, no. 4, pp. 38-47, Apr. 1994.

[10] Cao, P.; Liu, C. "Maintaining strong cache consistency in the World Wide Web". IEEE Transactions on Computers. Vol. 47, issue: 4, pg. 445-457. Apr, 1998.

[11] Tanenbaum, A.S. "Computer Networks". Fourth Edition. ISBN 85-352-1185-3. Prentice Hall, 2002.

[12] Garrett, J.J. "Ajax: A New Approach to Web Application". Available from *http://www.robertspahr.com/teaching/nmp/ ajax_web_applications.pdf*. Feb, 2005. [Visited Jul, 2011].

[13] W3Schools.com. "DHTML Tutorial". Available from *http://www.w3schools.com/dhtml/default.asp*. [Visited Jul, 2011].

[14] Reddy, M.; Fletcher, G.P. "An adaptive mechanism for Web browser cache management". IEEE Internet Computing. Vol. 2, issue: 1, pg. 78-81, Feb, 1998.

Pedro Monteiro da Silva Eleutério: Computer Engineer by Federal University of São Carlos (UFSCar), Brazil. Master degree in Computer Science, hypermedia area, by University of São Paulo (USP), Brazil. Since 2006, he is a criminal forensic expert of Brazilian Federal Police (DPF). Author of the Computer Forensics book "Desvendando a Computação Forense" (in portuguese).

Jane Dirce Alves Sandim Eleutério: bachelor of System Analysis by Federal University of Mato Grosso do Sul (UFMS), Brazil. Master degree in Computer Science, hypermedia area, by University of São Paulo (USP), Brazil. She is currently following her Ph.D. program in Computer Science at University of Campinas (Unicamp), Brazil. Since 2010, she is a professor at College of Computing at Federal University of Mato Grosso do Sul (FACOM-UFMS).