RESIDUAL FACEBOOK DATA ANALYSIS IN BROWSERS

[1] J. RAJA SRI, [2] Dr.V. VALLI KUMARI

[1]M.tech, Department of Computer Science, Andhra University, Visakhapatnam, AP, India

[2]Proffessor, Department of Computer Science, Andhra University, Visakhapatnam, AP, India.

ABSTRACT: The Internet is an essential tool for everyday tasks. Aside from common use, the option to browse the Internet privately is a desirable attribute. However, this can create a problem when private Internet sessions become hidden from computer forensic investigators in need of evidence. Our primary focus in this research is to discover residual artifacts from private and portable web browsing sessions. In addition, the artifacts must contain more than just file fragments and enough to establish an affirmative link between user and session. As social media applications such as Facebook become an integral part of our society, they are also becoming an important source of information in a digital (forensics) investigation. In this paper, we examine the potential to recover artifacts of forensic interest after three popular browsers, namely: Mozilla Firefox, Google Chrome and Internet Explorer, have been used to access Facebook. Findings from this research will hopefully contribute to a better understanding to mobile device and app forensics. Certain aspects of this topic have triggered many questions, but there have never been enough authoritative answers to follow. As a result, we propose a new methodology for analyzing private and portable web browsing artifacts. Our research will serve to be a significant resource for law enforcement, computer forensic investigators, and the digital forensics research community.

KEYWORDS*:* Classification, Intrusion detection system, KDD dataset, Deep Learning Evaluation metrics, Machine Learning.

I. INTRODUCTION

The Internet is a necessary tool for everyday tasks involved in human life, as it is being used to connect others from different destinations for communicating, sharing information and many other activities. Web browsers are programs that are installed on operating systems to allow users around the globe to access, view, and communicate with websites, other users and other files stored on web servers. In addition, they are able to record and retain the browsing activity of users' sessions. The information includes storing files, storing images, URLs visited, search terms, emails, cookies and other types of information. The information related to users' browsing activities is stored on the local hard disk of the computer and can be accessed and retrieved easily by any user who has access to the same machine[1] (Said, Mutawa, Awadhi, & Guimaraes, 2011).

As users are becoming more concerned about their browsing activity while surfing the Internet, web browser companies have developed a feature that aims to leave no traces of the browsing activity relating to the private browsing session (Satvat, Forshaw, Hao, & Toreini, 2014). The feature is known as private browsing on common web browsers, which enables end consumers to have better control over their privacy. The feature has two main goals to achieve. The first and foremost goal is to leave no trace of the browsing session on the user's device. When a user visits a website there should not be any information related to that website in the browser's history, cache, or cookies on the local computer. More precisely, it aims to secure the private browsing session against a local attacker that takes control of the digital device at a specific time, as there should not be any information related to the private browsing session prior to that time. Secondly, it aims to secure against web attackers, which allows end consumers to hide their identity when visiting some websites [2] (Aggarwal, Bursztein, Jackson, & Boneh, 2010).

The feature was firstly introduced in 2005, in Safari browsers, and was then added to other Internet browsers such as Internet Explorer, Google Chrome, and Mozilla Firefox. Not all web browsers providing the private browsing feature are consistent in the type of privacy provided, as some browsers protect the user against local attackers only and others against web attackers, while yet another browser protects against both. For instance, Google Chrome and Mozilla Firefox provide privacy against a local attacker and some protection against a web attacker, whereas Safari provides privacy against local attackers only. Furthermore, there are inconsistencies within a single browser.

Technologically-minded offenders use the technology illegally to profit by using users' personal information or data for their own purposes. Offenders currently are using the technology in various ways and becoming more sophisticated and rigorous in avoiding being detected to achieve their crime[3] (Zainudin, Merabti, & Llwellyn-Jones, 2011). As the private browsing feature is being more recognized and used among consumers, there might be higher chance of misuse of the feature, which creates a new issue for digital forensic professionals, as users are able to hide their data when using the private browsing feature.

II. RELATED WORK

This section reviews similar approaches by other researchers. The related works are studied, and analyzed in order to understand the approaches that have been utilized in order to develop an appropriate methodology for this proposed research. As researchers and practitioners alike become increasingly becoming concerned with the residual data generated via social media interactions, residual data visibility in everyday life is bound to increase accordingly. Previous research indicates that residual data generated on devices can be used as a proxy to data that is being stored in cloud environments. Since many of these devices have browser capabilities, researchers are investigating social media services, specific browser forensics, and specific social media forensic opportunities. The importance of digital forensics, particularly in the context of social media forensics, is visible not only in news articles but in research activities as well [3].

This section reviews similar approaches by other researchers. Six related works are studied, and analyzed in order to understand the approaches that have been utilized in order to develop an appropriate methodology for this proposed research [4].

Weiss and Warner presented the results of their efforts to track criminals through Facebook activities. They successfully used a Facebook Application Programmer Interface (API) to query groups for specific key words. They reported that their activities led to the nine arrests by law enforcement. It was noted that the tool they created need open access to selected groups. If they did not have open access, then they attempted to join a group in order to execute their code.

Taylor et al made the point that both companies and individuals are utilizing these services and that these networking applications can also be abused. The authors pointed out that online information can be changed by a suspect prior to an analyst capturing relevant information. Hence, they went on to make the point that a range of devices from the suspect may need to be examined during an investigation. The authors also pointed out that the acquisition of evidence form a variety of platforms presents difficulties [15].

Yusuf et al specifically looked at the extraction of data from mobile device running Mozilla Firefox that interacted with social media services. The social media services that the researchers interacted with included Twitter and Facebook. They located account credentials from Facebook and Twitter in the device's volatile memory.

In 2011, Oh et al put forth the idea that forensic analyst should be able to collect evidence from multiple browsers through the analysis of log files. In order to achieve this, they developed a tool that worked with Internet Explorer, Firefox, Chrome, Safari and Opera. Their tool handles necessary decoding and time zone translations as needed. It also attempts to account for deleted logs by caring out deleted information. The authors did note that at the time of publication that it only worked on a Windows OS [8].

A number of other studies have emphasized the importance of the browser in social media interactions along with examining specific residual data generated by various browsers. For example, Mendoza et al studied how Google Chrome, Internet Explorer, Mozilla Firefox, Opera, and Apple's Safari implemented their web storage, as well as how web storage artifacts could be a source of information not present in other browser artifacts. The authors then presented a proof-of-concept tool, designed to facilitate the analysis of web storage artifacts on Windows platform[6,7,8].

Focusing on portable web browsers, Choi et al demonstrated how the use of such browsers can be detected via examining the 'User Assist' key value and prefetch file. Existing browser forensics literature, such as the study of Mahaju and Atkison who evaluated the effectiveness of five web browser forensics analysis tools for Firefox, provide instructional information that is relevant to extracting data. However, there is currently minimal or up-to-date research that examines the extraction of a range of data from multiple browsers that have interacted with a specific social media provider. Thus, this is the focus of this paper.

Uraz Yavanoglu, Busra Caglar, Ozlem Milletsever, Medine Colak, Semra Cakir and Seref Sag_roglu proposed the Intelligent Approach for Identifying Political Views over Social Networks. It is a research-based analysis of political views by analyzing Social Network data through Artificial Neural Networks: ANN model and Data mining. The data

used in this research is taken from Twitter which is a public data. Therefore, this work helps to analysis thoughts and ideas from Twitter users both supporting or opposing the government.

Chris Howden, Lu Liu, Zhijun Ding, Yongzhao Zhan and KP Lam proposed the Moments in Time: A Forensic View of Twitter which the Twitter is carried through the Python IDLE client with MySQL database and display the data from Twitter via the SQL Statement.

Shankar Setty, Rajendra Jadit, Sabya Shaikh, Chandan Mattikalli and Vma Mudenagudi proposed the Classification of Facebook News Feeds and Sentiment Analysis which presented a system for classification of Facebook news feeds and A learning based classifier is built using various classification algorithms such as Bi-nary Logistic Regression, Naive Bayes, Support Vector Machine (SVM), Bayes Net and J48 and This experiments on the live news feeds showed that the proposed approach could achieve significantly improved performance for structuring the data on Facebook using SVM classifier learning model.

Zhaochun Ren, David van Dijk, David Graus, Nina van der Knaap, Hans Henseler and Maarten de Rijke proposed the Semantic Linking and Contextualization for Social Forensic Text Analysis which is a research-based analysis of the connective data between two social networks and after that analysis data connection setting within the context.

Noora Al Mutawa, Ibtesam Al Awadhi, Ibrahim Baggili and Andrew Marrington proposed the Forensic artifacts of Facebook's instant messaging service which Facebook Chat conversations in Latin and Arabic character set were conducted using three major web browsers, and then forensically retrieved.

Reza Soltani and Abdolreza Abhari proposed the Identity Matching In Social Media Platforms which is a research-based analysis of the relationship of data users on Facebook, Twitter and Linkedin by dividing the data into three classes; Personal Identities (uses String Matching Algorithm and the Google Maps APIs), Social Identities, such as posted information and video files (NLP and Youtube APIs are used in this class), and Relational Identities such friend's information and group membership.

Aniello Castiglione, Giuseppe Cattaneo and Alfredo De Santis proposed A Forensic Analysis of Images on Online Social Networks which is a research-based analysis of visual information that may violate the copyright law or engage in illegal activity on social networks. In this research, the analysis mainly focuses on processing the uploaded images and what changes are made to some of the characteristics. The pixel resolution and related metadata are studied together.

Norulzahrah Mohd Zainudin and Madjid Merabti proposed the Online Social Networks As Supporting Evidence A Digital Forensic Investigation Model and Its Application Design. The application is designed to automatically search on social network, and the searched data is stored in order to analyze the evidence.

Early work on the forensic analysis of web browsers focused on Microsoft's Internet Explorer, for a long time the dominant browser on the web. For example, both Jones and Jones and Belani analyzed the structure of Internet Explorer activity files and developed the tool Pasco to parse these files.

Boyd and Forster focused on parsing the different date and time structures in these files. The interpretation of this data is rather straightforward. For example, Jones and Belani refer to the access timestamp in the browser history as follows: "Access Time - The moment in time the user browsed the website."

Similarly, Boyd and Forster states that the timestamps in the activity files "[. . .] represent the UTC date and time that the corresponding URL was last visited using Internet Explorer."

Other work continued to focus on the technical side of evidence collection. For example, for Firefox, Pereira analyzed history artifacts of version 3 and also proposed a method to recover deleted entries.

Mahaju and Atkison instead, compared different tools for analyzing Firefox browsing artifacts, and Oh et al. developed a new methodology to collect and analyze evidence from different browsers and to integrate all evidence in a single timeline. Sonntag also developed a tool which can extract and collect data from Internet Explorer, Chrome and Firefox. While they mention that the history of Internet Explorer may contain spurious elements which were not intentionally visited by a user and that Firefox and Chrome history entries have attributes which allow to distinguish intentional from unintentional visits, they do not investigate this systematically. Joseph et al. showed how to extract user credentials, visited sites and search strings from volatile memory (with the possibility of false positives when searching for URLs). Said et al. (2011) preferred the use of three available websites on the Internet to imitate users' behavior in real life, while other researchers preferred to create their own website that contained different forms of data (Mahendrakar et al. 2011). The other researchers Mahendrakar et al. (2011) wanted to create a website that would include all the various data forms, such as SSL certificates, text entry forms, password forms, 16MB HTML files, JPEG files, and cookies of different sizes that could be easily traced during the analysis. Both sets of researchers used unique URLs and keywords to enhance the accuracy of the experiment.

Said et al. (2011) used the private browsing feature on the selected website, an image of the physical memory was taken to analyze the different types of information that could be saved to the memory, such as the web browsing history and cache. This approach was beneficial, as Chivers (2014) stated that useful information could be retrieved using this approach. However, physical memory is often not captured by forensic experts as it is not often available. In the testing phase, encase was also utilized by Said et al. (2011), along with other tools, to capture an image of each hard disk used on the three workstations to further examine any artefacts on the hard disk. In addition, open source tools to view the history and cache of different browsers, such as MozillaCacheView, MozillaHistoryView, ChromeCacheView and IECacheView were used in the analysis. These cache viewer tools are capable of retrieving information about the web pages that have been visited and rebuilding them with the information stored in the Internet history file if they have been deleted (Lillard, Garrison, Schiller, & Steele, 2010).

Said et al. (2011) first examined the history and cache using open source tools that did not reveal any information about the visited websites during the private browsing session. The open source tools used only recovered records of the browsing in the normal mode. Therefore, the records that could be recovered are limited only to the browsing session mode utilized. The researchers did not only rely on the history and cache viewers to trace the information; they analyzed the physical memory using Win hex by searching for strings of the website typed in the private session mode, such as "ani-forensics.com", "Sindbad", and "kabamaro". They found that Mozilla Firefox had several entries in each string search. In addition, Google Chrome retrieved several entries from the physical memory of the visited websites during the private session mode after it had been analyzed by Win hex. Internet Explorer also gathered the same results after analyzing the physical memory.

Using a variety of tools to extract and analyze the digital evidence is useful to search for the different artefacts that could be left behind in a private session mode. Each tool has different functionalities in searching and retrieving information and has been designed for different purposes such as acquisition, validation and discrimination, extraction, reconstruction and reporting (Phillips, Godfrey, Steuart, & Brown, 2013). A criminal user, for instance, could change the trace of a particular piece of information on the computer being used to make the investigation of information harder for investigators. In addition, a criminal could overload his/her computer with a wide variety of data to make the analyzing phase more complicated for investigators to distinguish between relevant and irrelevant information. Therefore, using a range of forensics tools that are able to search for information is preferable so that an investigator can be certain that he/she searched and analyzed all the data being left that could be potential evidence in a legal case (Phillips et al., 2013).

Much research has been conducted in the area where web browser vendors claim that private browsing is secure and that information about the session will not be saved on a local machine. However, the results of Said et al.'s (2011) tests revealed that artefacts are able to be recovered. The research performed by Said et al. (2011) had similar findings to that of Ohana & Shashidhar (2013), as the experiments revealed that neither Chrome nor Firefox wrote any data to the file system, while data about the private session in Internet Explorer was able to be recovered. In addition, Malmstrom & Teveldal (2013) examined Internet Explorer version 10 and found that a private browsing session is recoverable, as the Extensible Storage Engine (ESE) database deletes the private session records after the session is ended by the user which exists on the local hard disk until it is overwritten with other data.

Mahendrakar et al. (2011) also examined four modern web browsers: Mozilla Firefox, Internet Explorer, Google Chrome, and Safari. They found that all four browsers retained information of the private session mode. However, the findings of the testing revealed that Safari retained more information from the private browsing session than other browsers. Noorulla's (2014) research looked at the information that could be left by users after using private mode in four modern web browsers, all of which could be important for investigators during an investigation. The results of their testing revealed a similar finding to that of Said et al. (2011). Internet Explorer versions 8 and 9 had information related to the browsing session and this was able to be recovered even though the database had deleted it, while Safari writes and stores the data to a "WebpageIcons.db" file. Thus, with appropriate tools, forensic experts are able to carve out and reconstruct the data that has been previously deleted.

However, nearly all the research that has been conducted in this area has resulted from the fact that Mozilla Firefox and Google Chrome are the web browsers that write and record the least data on either the hard disk or the physical memory, which could have an impact on an investigation if a criminal is trying to hide his/her browsing activity. These two web browsers are considered the most suitable browsers to surf the Internet privately without the user being worried about leaving traces. Researchers have therefore suggested that experiments in the area of private mode browsing need to be

examined further in the areas where information is held, as web browsing activities could be potential evidence in a digital forensics' investigation

III. METHODOLOGY

REVIEW OF SIMILAR REASEARCH

Since many of the devices have browser capabilities, researchers are investigating social media services, specific browser forensics, and specific social media forensic opportunities. The importance of digital forensics, particularly in the context of social media forensics, is visible not only in news articles but in research activities as well. The authors pointed out that online information can be changed by a suspect prior to an analyst capturing relevant information. Hence, they went on to make the point that a range of devices from the suspect may need to be examined during an investigation. The authors also pointed out that the acquisition of evidence form a variety of platforms presents difficulties. Specific research efforts that explicitly studied Facebook forensic issues include efforts to extract Facebook actives that include friends, news feeds, postings to walls group messages, and chats.
Additional research by Mulazzani et al. utilizes Facebook API's to extract data and cluster information without interacting with the provider. The researchers did note that this approach is easier with the user's credentials. Previous research has also investigated live memory data procurement from desktops that have interacted with Facebook. The reality is that solutions of this type require hardware access, which may or may not be realistic depending on circumstances. Other researchers have specifically examined Facebook's chat to gain an understanding of specific artifacts that are of interest for extraction and reconstruction. The researchers did note that Arabic conversations had to convert to Unicode to be retrieved in searches. This is an indication that there is the potential for missed evidence if chats occur in other languages.

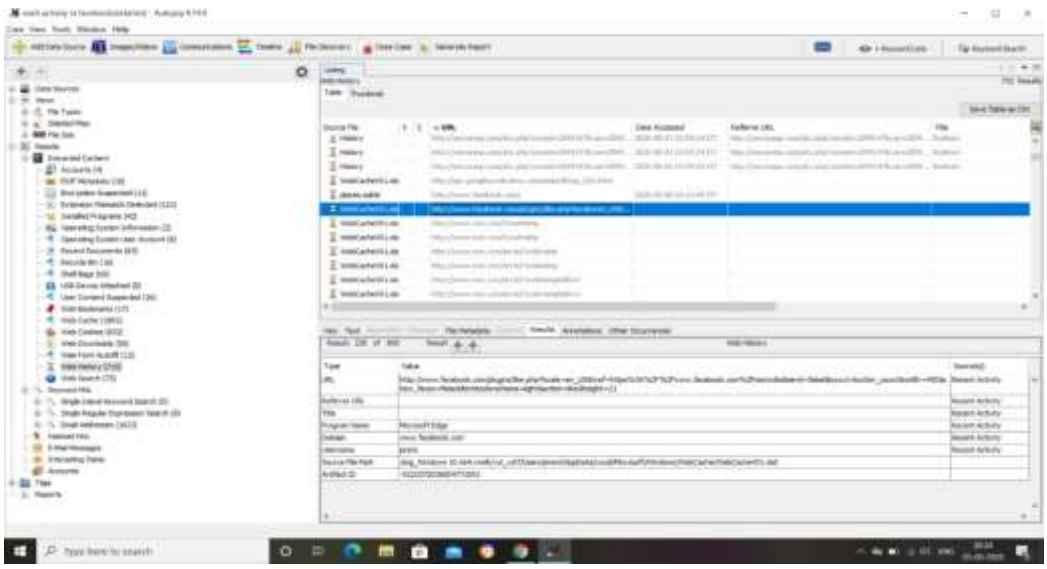
The experiment took place in three stages that included Facebook profile creation, data generation and data extraction. The evidence was determined to be discovered if there was a match between keywords found and the activities performed, as well as by the matching of the recorded date/time stamps. In the profile creation stage, three Facebook accounts were created using three separate browsers. The three accounts that were created on each browser were Fred Fox, Chris Chrome and Bob IE. The data generation stage consisted of a number of photo uploaded, comments, statuses, and created groups. The actions performed in this stage are summarized in Table 1 – Actions. These activities were recorded in a Microsoft Excel spreadsheet. To extract the data in the third stage, AUTOPSY was utilized for this procedure.

TABLE I. ACTIONS

Category	Description
Account Creation	Email or Facebook account sign-up/creation
Image Upload	Image was uploaded or posted on the website
Text Write	Action involving text that was input by the user
Text Read	An action involving text that was viewed/read by the user, but not typed by the user viewing it.
Login	User logs on to Facebook. Start of a session.
Session End/Logout	Manual user log out of Facebook

IV. RESULTS

In reference to the Firefox browser, AUTOPSY recovered actions performed. It is interesting that while six individual categories recovered 100 percent of the information that was input into the browser, seven categories defined in the experiment did not have complete recovery of the data. Regarding the high-level categories, only 32% of the text writes and 61% of the text reads were recovered. The detailed results are presented. It is interesting to observe that several residual data artifacts were recovered by accessing the "Mozilla Firefox Browse History" in the Internet/Chat Files section of AUTOPSY. Specific keywords and date/time information to confirm the information found. A sample of the information recovered from the Firefox browser history is presented.



Profile Images in Internet Explorer

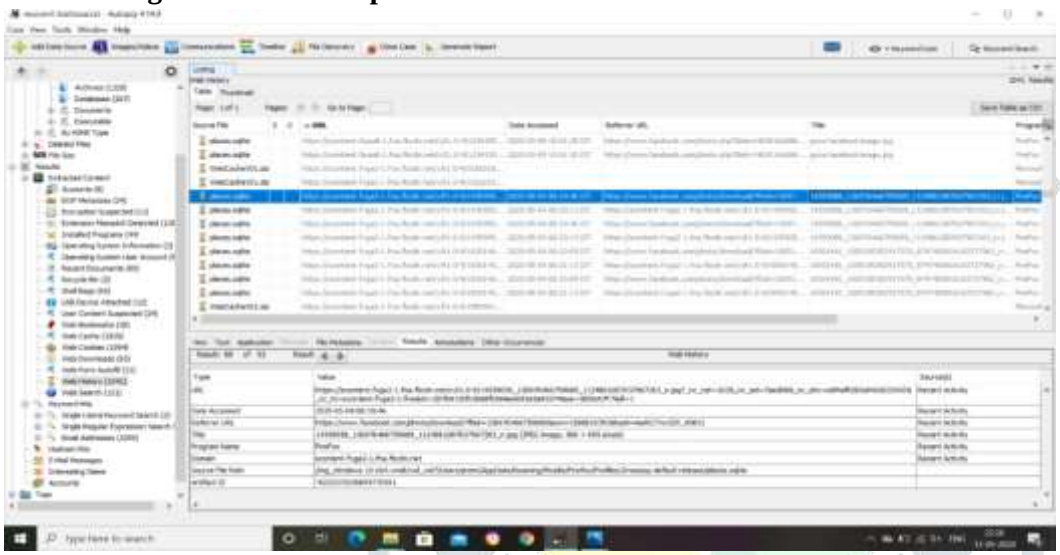
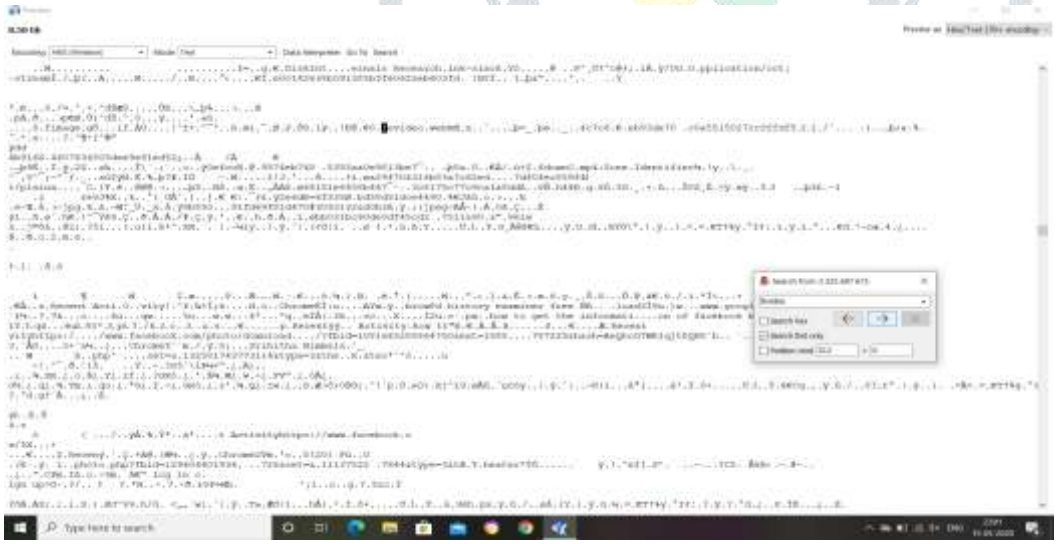
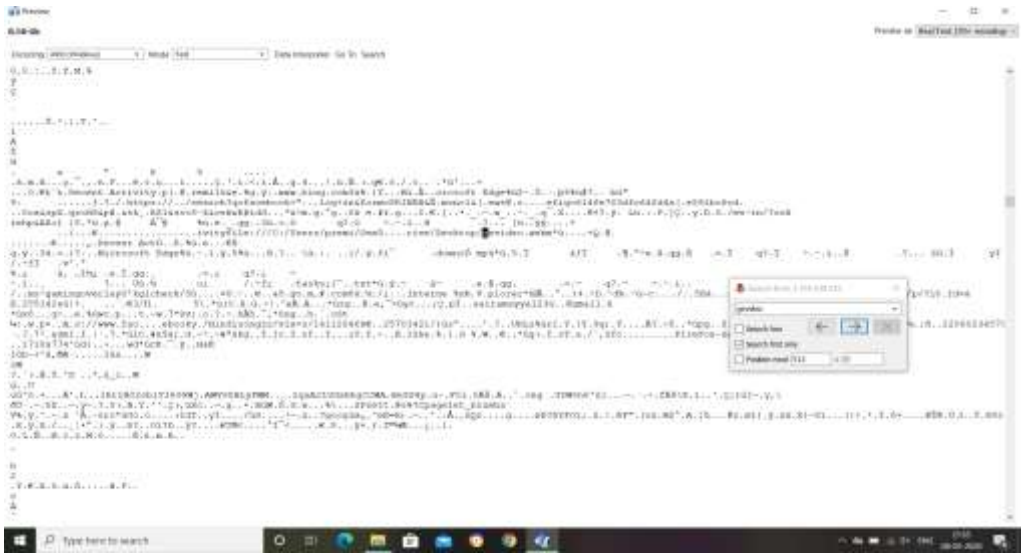


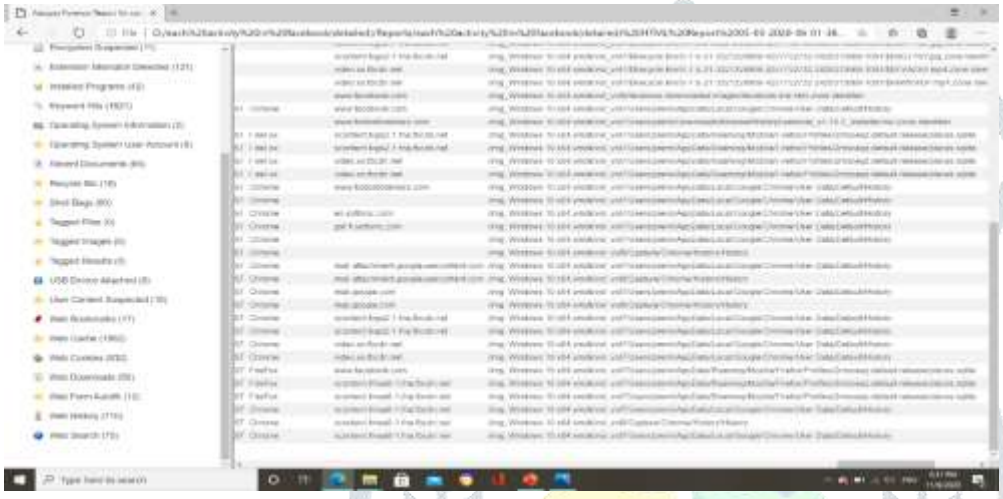
Image Download Activity in Mozilla Firefox



Video upload activity in Mozilla Firefox



Video upload activity in Google chrome



Video download activity in Google chrome and Mozilla Firefox

V. EVALUATION METRICS

DISCUSSION ON DATA ACQUISITION AND ANALYSIS:

The data acquisition was done with the help of autopsy tool. In the virtual machine in the VMware Workstation, windows 10 operating system was installed.in the windows operating system three browsers were installed namely, google chrome, internet explorer and Mozilla Firefox. In three browsers three Facebook accounts were created. In each browser and in each Facebook account, list of Facebook activities was performed as given in the paper.

For data analysis, autopsy tool was used to analyze the .vmdk file which was given as input to the autopsy tool. Analysis was done through the web history, web downloads, unallocated space and deleted files from the virtual machine disk file. The Facebook URLs with the timestamps were found in Mozilla Firefox and google chrome. Some images and videos which are downloaded from the Facebook were found in the drive unallocated space and some locations in the disk with the URLs to ensure that from which browser the particular files were downloaded. The activities done in the internet explorer were found with URLs but with no timestamps. Some of the activities with the URLs were directly found from the web history in the google chrome and the Mozilla Firefox. To examine whether any artifacts found after deleted from the recycle bin, we used “recoverit” tool to recover the data from the recycle bin. To check whether the recovered file shows the source from which it was downloaded, .vmdk file given to the autopsy. Here we found that, all data from downloaded from the Mozilla Firefox browser showing the URL’s. Data (images and videos) downloaded from the google chrome and internet explorer browsers not showing the URL’s.

The results obtained in the autopsy tool were presented below

VI. EVALUATION

Our analysis of the data gathered from the Mozilla Firefox, Google Chrome, and Internet Explorer browsers using AUTOPSY supports the idea that different browsers retain varying amounts of information about social media interactions. Findings from this study suggested that chat messages can be challenging to locate, while login information was consistently available across all three browsers. In this experiment, Google Chrome retained the most information while Mozilla Firefox saved the least amount of residual data.

This research raises the question of artifact validation when users have interacted with social media sites from different devices that potentially use different browsers. The initial results of this experiment indicated that browsers retained different residual data artifacts when interacting with social media sites. This scenario potentially impacts an investigation from an evidence perspective and an overall cost perspective. If an analyst needs to validate a user's social media actives, then they plausibly will be required to attempt to identify, locate and extract information manually. Consequently, this increases the time that they spend on an individual case.

The contribution of this research is to provide a proof-of-concept that different browsers retain various amounts of data when they interact with social media sites. Contributes to discussions about documentation and evidentiary artifacts generated through social media interactions while highlighting the importance of verifying residual data artifacts.

LIMITATIONS

The purpose of this study was to investigate the possibility of locating and extracting evidence from a local hard disk after a user has used the normal browsing feature. Although the test bench was setup and experiments were successfully conducted there were some limitations identified, which are presented in this section.

The limitations indicate that the experiments are limited to specific versions of operating systems and web browser vendors as there are many more web browsers which offer the normal browsing feature that have not been tested in this research. The operating systems used in the experiments are limited to one desktop-based operating system, an HP laptop, and a MacBook pro with the latest version release for each operating system at the time of conducting the experiments. The forensics investigation methods may differ with other operating systems such as Android and BlackBerry which are designed primarily for smartphones and tablets. In addition, the type of digital devices used may have a different way of storing information. Furthermore, there are different versions and updates of each operating system, which means that the file structure of systems could differ compared to the operating system versions used for the experimental testing. Similarly, the web browsers used for the experimental case are limited to five well-known browsers with the latest version released for each operating system. There are many different web browsers available that are not considered in this research. These include Flock, Avant, Maxton, Netscape and others. The web browsers all have different versions and updates to secure users' browsing activity.

Thirdly, there are many digital forensics tools that could be used during the digital forensics process of collecting, examining, analyzing and reporting of evidence. The chosen tools for the proposed research are selected based on their availability. The tools are capable of acquiring the evidence, examining the hard drives, and extracting and analyzing the evidence from the web browser artefacts and files. The main selected tool was Autopsy for this project, along with other open source tools used to view URL's. Other digital forensics tools were not selected and tested due to the time constraints of this particular research. It is simply not possible in limited time to test all the digital forensics tools available in this type of study.

The investigation techniques used in the proposed research are limited to the hard disk of the system. There will be more possibility for getting the more evidences from the live system by taking RAM capture. Most valuable information will be retrieved from the volatile memory.

VII. CONCLUSION

Our analysis of the data gathered from the Mozilla Firefox, Google Chrome, and Internet Explorer browsers using AUTOPSY supports the idea that different browsers retain varying amounts of information about social media interactions. Findings from this study suggested that chat messages can be challenging to locate, while login information was consistently available across all three browsers. In this experiment, Google Chrome retained the most information while Mozilla Firefox saved the least amount of residual data. This research raises the question of artefact validation when users have interacted with social media sites from different devices that potentially use different browsers. The initial results of this experiment indicated that browsers retained different residual data artefacts when

interacting with social media sites. This scenario potentially impacts an investigation from an evidence perspective and an overall cost perspective. If an analyst needs to validate a user's social media actives, then they plausibly will be required to attempt to identify, locate and extract information manually. Consequently, this increases the time that they spend on an individual case. Our research clearly shows that further data can still be recovered on host machines without the portable storage device being present. Overall, our research is a valuable resource pertaining to private and portable web browsing artefacts. Not every web browser will leave incriminating evidence but some will, depending on the situation. These residual artefacts may or may not be important to a case, but on the other hand it may be the only way to explain certain results. Computer forensic investigators must treat digital environments like a real crime scene. It is not only important to document what is found but to also note what is not there and ask why. Our research now provides an alternative way to perceive these types of findings and explain the results. We conclude that just because something is not there does not mean it never happened.

FUTURE SCOPE

There are a number of potential extensions to this research, such as the following.

Forensic taxonomy of browser apps: Future work will build on this experiment to investigate the viability of validating residual data gathered from multiple end user devices (e.g. Android, iOS and Windows Phone devices) using multiple browsers, including lightweight browsers (e.g. Dolphin, Maxton, Puffin, and UC), that have interacted with social media websites. This will allow us to present a taxonomy of forensic artifacts that can be recovered from different browser apps using different forensic tools like Encase, Sleuth Kit and Autopsy which is similar to forensic taxonomies for Android and Windows specific apps [15, 38-40]. It is envisioned that the future taxonomy will list the artifacts down the left side of the table. The first row across the top will identify the individual browsers like Firefox, Chrome, and IE. The second row will identify specific social media sites, i.e., Facebook, WhatsApp, Snapchat, etc. Individual cells will intersect the artifacts with specific social media sites in order to indicate the tool that was used and the percentage of the artifact that was recovered.

Forensic taxonomy of browser apps: Future work will build on this experiment to investigate the viability of validating residual data gathered from multiple end user devices (e.g. Android, iOS and Windows Phone devices) using multiple browsers, including lightweight browsers (e.g. Dolphin, Maxton, Puffin, and UC), that have interacted with social media websites. This will allow us to present a taxonomy of forensic artifacts that can be recovered from different browser apps using different forensic tools like Encase, Sleuth Kit and Autopsy which is similar to forensic taxonomies for Android and Windows specific apps [15, 38-40]. It is envisioned that the future taxonomy will list the artifacts down the left side of the table. The first row across the top will identify the individual browsers like Firefox, Chrome, and IE. The second row will identify specific social media sites, i.e., Facebook, WhatsApp, Snapchat, etc. Individual cells will intersect the artifacts with specific social media sites in order to indicate the tool that was used and the percentage of the artifact that was recovered

REFERENCES

1. Al Mutawa, N. I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," Digital Investigation, vol. 9, pp. S24-S33, 2012.

2. Azfar, A. Choo, K. K. R.and Liu, L. "Forensic taxonomy of Android social apps," Journal of forensic sciences, vol. 62, no. 2, pp. 435-456, 2017

3. Azfar, A. Choo, K. K. R. and Liu, L."Forensic taxonomy of android productivity apps," Multimedia Tools and Applications, vol. 76, no. 3, pp. 3313-3341, 2017.

4. Azfar, A. Choo, K. K. R. and Liu, L. "An android communication app forensic taxonomy," Journal of forensic sciences, vol. 61, no. 5, pp. 1337-1350, 2016.

5. Berman, K. W. B. Glisson, and L. M. Glisson, "Investigating the Impact of Global Positioning System (GPS) Evidence in Court Cases," in Hawaii International Conference on System Sciences (HICSS-48), Kauai, Hawaii 2015: IEEE

6. Cahyani, N .D. W. N. H. A. Rahman, W. B. Glisson, and K.-K. R. Choo, "The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Storage

7. Chu, H. C. D. J. Deng, and J. H. Park, "Live Data Mining Concerning Social Networking Forensics Based on a Facebook Session Through Aggregation of Social Data," IEEE Journal on Selected Areas in Communications, vol. 29, no. 7, pp. 1368-1376, 2011.

8. Choi, J. H. Lee, K. Park, J. Lee, C. and Lee, S. "Analysis Framework to Detect Artifacts of Portable Web Browser," Lecture Notes in Electrical Engineering, vol. 180, pp. 207-214, 2012.

9. Clutter, C. (2018, 01/29). Police investigating social media threats made toward Valley High School. Available: http://wtov9.com/news/local/police-investigating-social-media-threatsmade-toward-valley-high-school

10. Cusack, B. and Alshaifi, S. "Mining social networking sites for digital evidence," 2015.

11. Cohen. J. S. (2018, 1/28). Chicago Cop Under Investigation Again Over Social Media Posts. Available: https://www.propublica.org/article/chicago-police-officer-johncatanzara-investigation

12. Gartner. (2017, 01/22/2018). Gartner Reveals Top Predictions for IT Organizations and Users in 2018 and Beyond. Available: https://www.gartner.com/newsroom/id/3811367

13. Glisson, W. B. T. Storer, M. Campbell, A. Blyth, and G. Grispos, "Inthe-Wild Residual Data Research and Privacy," Journal of Digital Forensics, Security and Law, vol. 11, no. 1, pp. 7-36, 2016.

14. Government Technology. (2017, 01/29). Can the Police Use Facebook to Investigate Crimes? Available: http://www.govtech.com/publicsafety/can-the-police-use-facebook-to-investigate-crimes.html

15. Grigonis. H. (2018, 01/22). Desktop users could soon post to Facebook Stories in their browser. Available: https://www.digitaltrends.com/social-media/facebook-stories-ondesktop-tested/

16. Grispos, G. W. B. Glisson, and T. Storer, "Chapter 16 - Recovering residual forensic data from smartphone interactions with cloud storage providers," in The Cloud Security Ecosystem, R. K.-K. R. Choo, Ed. Boston: Syngress, 2015, pp. 347-382.

17. Grispos, G. W. B. Glisson, J. H. Pardue, and M. Dickson, "Identifying User Behavior from Residual Data in Cloud-based Synchronized Apps," Journal of Information Systems Applied Research, vol. 8, no. 2, pp. 4- 14, 2015.

18. Grispos, G. W. B. Glisson, and T. Storer, "Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services," in Hawaii International Conference on System Sciences (HICSS), 2013.

19. Grispos, G. W. B. Glisson, D. Bourrie, T. Storer, and S. Miller, "Security Incident Recognition and Reporting (SIRR): An Industrial Perspective," in Twenty-third Americas Conference on Information Systems, Boston, 2017: Americas Conference on Information Systems.

20. Hoolachan, S. and Glisson, W. B. "Organizational Handling of Digital Evidence," in The 2010 ADFSL Conference on Digital Forensics, Security and Law, St. Paul, Minnesota, USA, 2010: Association of Digital Forensics, Security and Law.

21. Jang, Y.-J and J. Kwak, J. "Digital forensics investigation methodology applicable for social network services," Multimedia Tools and Applications, vol. 74, no. 14, pp. 5029-5040, 2015.

22. Jang, Y.-J and Kwak, J. "Social network service real time data analysis process research," in Frontier and Innovation in Future Computing and Communications: Springer, 2014, pp. 643-652.

23. Mahaju, S. and Atkison, T. "Evaluation of Firefox Browser Forensics Tools," in Annual ACM Southeast Conference Featuring Multidisciplinary and Interdisciplinary Computing, 2017, pp. 5-12.

24. McMillan, J. W. B. Glisson, and M. Bromby, "Investigating the Increase in Mobile Phone Evidence in Criminal Activities," in Hawaii International Conference on System Sciences (HICSS-46), Wailea, Hawaii, 2013: IEEE

25. Mendoza, A. Kumar, A.Midcap, D.Cho, H.and Varol, C. " BrowStEx: A tool to aggregate browser storage artifacts for forensic analysis," Digital Investigation, vol. 14, pp. 63-75, 2015.

26. Mohd Najwadi, Y. and Dehghantanha, A. "Network traffic forensics on Firefox Mobile OS: Facebook, Twitter and Telegram as case studies," 2016.

27. Mulazzani, M. M. Huber, and E. Weippl, "Social network forensics: Tapping the data pool of social networks," in Eighth Annual IFIP WG, 2012, vol. 11

28. Moltisanti, M. Paratore, A. Battiato, S. and Saravo, L. "Image Manipulation on Facebook for Forensics Evidence," Cham, 2015, pp. 506-517: Springer International Publishing.
29. Mutawa, N. A. I. A. Awadhi, I. Baggili, and A. Marrington, "Forensic artifacts of Facebook's instant messaging service," in 2011 International Conference for Internet Technology and Secured Transactions, 2011, pp. 771-776.

30. N. B. Al Barghuthi and H. Said, "Social networks IM forensics: Encryption analysis," Journal of Communications, vol. 8, no. 11, pp. 708-15, 2013.

31. Norouzizadeh Dezfouli, F. A. Dehghantanha, B. Eterovic-Soric, and K.- K. R. Choo, "Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms," Australian journal of forensic sciences, vol. 48, no. 4, pp. 469-488, 2016.

32. Oh, J. Lee, S. and Lee, S. "Advanced evidence collection and analysis of web browser activity," Digital Investigation, vol. 8, pp. S62-S70, 2011/08/01/ 2011

33. Richter, F. (2018, 01/29). Facebook Inc. Dominates the Social Media Landscape. Available: https://www.statista.com/chart/5194/activeusers-of-social-networks-and-messaging-services/

34. Shafqat, N. "Forensic Investigation of User's Web Activity on Google Chrome using various Forensic Tools," International Journal of Computer Science and Network Security (IJCSNS), vol. 16, no. 9, p. 123, 2016.

35. Statista. Number of social media users worldwide from 2010 to 2021 (in billions). Available: https://www.statista.com/statistics/278414/numberof-worldwide-social-network-users/

36. Statista. Global revenue from social media from 2013 to 2019 (in billion euros). Available: https://www.statista.com/statistics/562397/worldwide-revenue-fromsocial-media/

37. Taylor, M. J. Haggerty, D. Gresty, P. Almond, and T. Berry, "Forensic investigation of social networking applications," Network Security, vol. 2014, no. 11, pp. 9-16, 2014.

38. Wong, K. Lai, A. Yeung, J. Lee, W. and Chan, P. "Facebook forensics," Valkyrie-X Security Research Group, 2011.

39. Weiss, D. and Warner, G. "Tracking Criminals on Facebook: A Case Study From A Digital Forensics REU Program," in Proceedings of the Conference on Digital Forensics, Security and Law, 2015, p. 205: Association of Digital Forensics, Security and Law.

40. Yusoff, M. Dehghantanha, A. and Mahmod, R. "Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as Case Studies."