8-2016

A comparative forensic analysis of privacy enhanced web browsers

Ryan M. Gabet
Purdue University

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Ryan M. Gabet

Entitled

A COMPARATIVE FORENSIC ANALYSIS OF PRIVACY ENHANCED WEB BROWSERS

For the degree of Master of Science

Is approved by the final examining committee:

Kathryn Seigfried-Spellar
Chair

Marcus Rogers

Raymond Hansen

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Kathryn Seigfried-Spellar

Approved by: Jeffrey Whitten 7/25/2016

Head of the Departmental Graduate Program Date

A COMPARATIVE FORENSIC ANALYSIS OF PRIVACY ENHANCED WEB BROWSERS

A Thesis

Submitted to the Faculty

of

Purdue University

by

Ryan M. Gabet

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

August 2016

Purdue University

West Lafayette, Indiana

The completion of this thesis work is in dedication to my loving and supportive family. Without their constant enouragement to set and achieve ambitious goals from a young age, this work would not be possible.

ACKNOWLEDGMENTS

I wish to gratefully acknowledge my thesis committee for their insightful comments and guidance. I also with to gratefully acknowledge my family, friends, and loving girlfriend for their constant support and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS

CFFTPM	Computer Forensics Field Triage Process Model
FTK	Forensic ToolkKit
GB	GigaByte
HDD	Hard Disk Drive
HTTPS	HyperText Transfer Protocol Secure
IM	Instant Message
KB	KiloByte
MB	MegaByte
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
OS	Operating System
URL	Uniform Resource Locator
VHD	Virtual Hard Disk
VM	Virtual Machine

GLOSSARY

Browser	Computer application that enables a user to interact with websites through the HTTP protocol (Tilborg & Jajodia, 2011, p. 1372).
Broswer Artifact	Metadata created by web browsers, often stored in database files, provides information about actions that have occured in the web browser during a session, common examples include cookies, cache, and history (McQuaid, 2014).
Browser Cache	"Folder of files or a database file where pages, images, applets, and other data are stored from your web surfing sessions (Stauffer & McElhearn, 2004, p. 344)."
Browser History	Stores information about web browser activities including visited web pages (Sheldrake, 2011, p. 143).
Cybercrime	Computer crime in which a computer serves as a target of a crime, an instrument of the crime, is incidental to a crime, or the crime is "associated with the prevalence of computers" (Reyes et al., 2007, p. 26).
Cyber Forensics	The process of extracting data and information from computers to present as digital evidence in the court of law (ISC, 2015).
File System	"The underlying structure a computer uses to organize data on a hard disk (Microsoft, 2015a)."

Internet Privacy	Issue that encompasses concerns regarding the collection of personally identifiable information as well as being electronically monitored by law enforcement, elmployers, etc (Smith, 2007, p. 58).
Metadata	Data about data, such as creation, modification, and access times of files (Lugmayr, Niiranen, & Kalli, 2004).
Operating System	"Software program that enables the computer hardware to communicate with and operate the computer software (Hope, 2016)."
Private Browsing	Web browser mode in which information about visited websites is not saved (Vermaat, Sebok, Freund, Campbell, & Frydenberg, 2015).
Virtual Machine	"A virtual machine (VM) is an operating system OS or application environment that is installed on software which imitates dedicated hardware. (Rouse, 2014)"

ABSTRACT

Gabet, Ryan M. M.S., Purdue University, August 2016. A Comparative forensic analysis of privacy enhanced web browsers. Major Professor: Kathryn C. Seigfried-Spellar.

Growing concerns regarding Internet privacy has led to the development of enhanced privacy web browsers. The intent of these web browsers is to provide better privacy for users who share a computer by not storing information about what websites are being visited as well as protecting user data from websites that employ tracking tools such as Google for advertisement purposes. As with most tools, users have found an alternative purpose for enhanced privacy browsers, some illegal in nature. This research conducted a digital forensic examination of three enhanced privacy web browsers and three commonly used web browsers in private browsing mode to identify if these browsers produced residual browsers artifacts and if so, if those artifacts provided content about the browsing session. The examination process, designed to simulate common practice of law enforcement digital forensic investigations, found that when comparing browser type by browser and tool combination, out of a possible 60 artifacts, the common web browsers produced 26 artifacts while the enhanced privacy browsers produced 25 for a difference of 2%. The tool set used also had an impact in this study, with FTK finding a total of 28 artifacts while Autopsy found 23, for a difference of 8%. The conclusion of this research found that although there was a difference in the number of artifacts produced by the two groups of browsers, the difference was not significant to support the claim that one group of browsers produced fewer browsers than the other. As this study has implications for privacy minded citizens as well as law enforcement and digital forensic practitioners concerned with browser forensics,

this study identified a need for future research with respect to internet browser privacy, including expanding this research to include more browsers and tools.

CHAPTER 1. INTRODUCTION

In todays digital age, where personal privacy and web presence struggle to converge at a reasonable common ground, increased public knowledge of possible invasions of Internet privacy has sparked widespread discussion for more secure and private web usage methods (Walters, 2015). Among the methods available to increase personal privacy while browsing was the use of specific web browsers that feature enhanced privacy features. Web browser developers have added enhancements to enable private session browsing capabilities as a means to enhance web anonymity and privacy for users. Giving users the capability to browse websites without leaving traces behind on the computer, private session browsers do not store web browser artifacts such as cookies, form data, or web page history entries (Hoffman, 2012). While this capability has provided a sense of privacy for users who work off of a shared computer such as a library, work, family, or school computer, it continues to present a problem for digital forensic investigators. In cases where private session browsing has been used for nefarious purposes, a lack of browser metadata or typically stored content potentially inhibited the data collection processes or caused issues for investigators as they tried to determine what happened and who was responsible.

1.1 Scope

The scope of this reseach identified, recovered, and compared recoverable web browser artifacts of three commonly used web browsers and three less commonly used, enhanced privacy web browsers using software both available and used by law enforcement agencies to conduct digital forensics examinations. This reserach only investigated web browsers that were compatible with the Microsoft

Windows 10 operating system, however one or more of the browsers used may be compatible with previous versions of the Microsoft Windows OS as well as Apple OS and various distributions of Linux OS. The tools within this scope of this reserach were those available to law enforcement agencies for conducting a forensics analysis of the files stored on hard disk and that have been used before to produce admissible evidence in the Court of Law. The web browser artifacts within the scope of this research were browser artifact files that are typically created by web browsers to store information about visited websites, viewed content, and sent and received digital communication.

1.2 Significance

The significance of this study not only benefited law enforcement involved in the field of Cyber Forensics, but also, society in general as a contribution to the discussion and pursuit of Internet privacy. With 269,422 formal complaints filed with the FBI's Internet Crime Complaint Center (IC3) (2014) in the year 2014, increased complaints filed compared to the previous year suggested cybercrime was on the rise. As cybercrime rates have rises and cybercriminals have become more educated in methods of circumventing law enforcement detection, this research served purposeful in identifying expected recoverable browser artifacts that have been helpful to law enforcement in digital investigations to reveal nefarious computer behavior such as content consistent with cybercrime, cyberstalking, or viewed and shared child pornography (NW3C, 2009).

In a different discussion, Internet privacy and government surveillance has sparked open discussion in regards to web browsing privacy. As more web browser developers have provided methods of private web browsing, this research was necessary to test the claims of privacy that web browser developers have made in regards to private session browsing and enhanced privacy features. In addition, to an increasingly privacy minded society, this research sought to identify whether

enhanced privacy web browsers provided a higher level of privacy compared to the anonymous browsing modes of common browsers based on recovered browser artifacts.

1.3 Research Question

From a web browser artifact forensics standpoint, do the enhanced privacy web browsers Epic, Comodo Dragon, or Dooble produce fewer browser artifacts and content than the private browsing mode of the common web browsers Chrome, Firefox, or Edge?

1.4 Assumptions

The assumptions for this study included:

- Additional artifacts may have been created by the process of downloading each web browser.
- Not every web browser action was found as content in a recovered browser artifact.
- The findings of this reserach were only representative of this test methodology including the operating system, file system, browser environment, and analysis tools, including version numbers, used in this research.
- All eleven lab machines used to process and analyze browser data were identical systems with identical software installed.
- Each Windows environment had only one user account.
- The CFFTPM forensic framework used to conduct the forensic examination in this methodology would generate admissble evidence in the court of law.

- Per the CFFTPM forensic framework, phases Planning and Triage have already occured, the Usage/User Profiles phase was skipped because only one user account exists, Chronology/Timeline was skipped because time stamps were not necessary for this research, and the study began with the Internet investigation phase.
- The system analyzed in this study was powered off when obtained, prior to imaging and conducting analysis.

1.5 Limitations

The limitations for this study included:

- Due to software licensing availability and cost of software licenses, only the commercial forensics software Access Forensic Toolkit was available for use in this methodology.
- Due to large data processing time requirement of the forensic tools used, eleven different machines running the same version of the tools were used for data collection and analysis.
- Some artifact files produced by the forensic tools used, required additional tools to be read and viewed, resulting in the contents remaining unknown.
- Each browser may have stored data differently including the location, file name, and content type stored in the form of artifacts.
- Additional browser artifacts or content may have existed within the file system in places other than the known artifact files and locations.
- Due to time contraints, only six browsers and two tools were used in the methodology of this research.
- The order in which the browser traffic was created was intentional.

- The same data processing actions were not carried out on every browser in each tool as both tools provided additional data processing actions for supported web browsers. Supported web browsers were typically Internet Explorer, Google Chrome, and Mozilla Firefox.
- The generated web traffic only contained ten different web sites and fewer email, video, and instant massaging sites for data population. Varying web sites, email service poviders, and instant messaging services may produce recoverable artifacts other than what is found in this research.
- Other tools and methods exist besides those used in this research methodology to create virtual machines and create disk images.
- Due to lack of documented research on browser artifacts files and locations for Comodo Dragon, Epic, and Dooble browser, the closest browser with documented artifact file and location documentation had to be used. In the case of Comodo Dragon and Epic, the same artifact names and locations as Chrome were used as both browsers are based off of the Chromium open source browser platform thus were expected to be similar to Chrome. Dooble browser was not based off of any one particular browser, therefore artifacts were searched for in the Dooble Browser application files, similar to Firefox, Chrome, and Microsoft Edge.
- The forensic examination was a local examination, meaning only information stored locally on the computer hard disk, or in this case, the VM disk, was examined.

1.6 Delimitations

The delimitations for this study included:

- Only browsers compatible with the Microsoft Windows OS environment, specifically Windows 10 were used in this research.

- Apple computers running the Macintosh OS or computers that used distrubutions of the Linux OS were not examined in this study as they require the use of different file systems.
- This study did not examine web browsers that used proxy servers or the TOR network to enhance privacy.
- The proxy tool built into Epic was disabled prior to the data population process.
- Due to the fact that each image contained in excess of 180,000 files or viewable items, this research methodology only looked for known documented artifact files in their expected locations.
- As a substitute for the commercial forensic analysis software EnCase due to unavailability of a software license, the open source Autopsy forensics analysis program was used as the second tool of analysis.
- This research only used Gmail and Yahoo mail to send and receive emails to generate email artifacts.
- This research only used Youtube to watch video content.
- This research only used the Google and Yahoo search engines to search the search terms.
- All browser data collection and analysis was conducted post-session, meaning the browser session was closed prior to imaging and analysis.
- FTK and Autopsy were used in their stock condition, meaning no additional plugins were installed or used for data processing.

1.7 Summary

This chapter provided the scope, significance, research question, assumptions, limitations, and delimitations of this research. The purpose of this chapter was to state the main object of this research in the form of a research question as well as provide a more detailed frame of the research to be conducted including a description of the intended outcome of of this research, what was done, what was not done, any assumptions made and possible flaws that existed in this research. For this research, the purpose was to identify if enhanced privacy web browsers produced fewer recoverable web browser artifacts than common web browsers in their respective private browsing modes. Primary confines of this research included three common web browsers and three enhanced privacy web browsers that were all compatible with Microsoft Windows 10; analyzed with two tools used by law enforcement agencies to conduct a forensic analysis of a raw disk image, including the abilitiy to access the entire file system of the forensic image to search for specifically documented artifact files in specific locations.

CHAPTER 2. REVIEW OF RELEVANT LITERATURE

This chapter provided a review of the literature relevant to Internet privacy, enhanced privacy web browsers, digital forensics tools, digital forensic frameworks, and research methodologies of similar studies.

2.1 Foundations of Digital Evidence and Cybercrime

Following the dawn of the information age, digital evidence has become an integral part of modern crime scene investigations. In high profile cases such as the BTK killer Dennis Rader, Scott Peterson, and David Leslie Fuller, digital evidence provided the necessary proof to convict each of murder among other charges (Ritter, 2006). Defined in the 2004 NIJ report, the term digital evidence is defined as "information stored or transmitted in binary form that may be relied on in court" (of Justice, 2004). Broad in nature, by this definition, all digital devices can be identified as digital evidence in an investigation. Even though the crimes committed in the above examples did not occur in cyber space, the digital evidence showing how the crimes were carried out, proved to be key evidence needed to secure a conviction. INTERPOL (2015) noted a distinction used by law enforcement to classify cybercrime into two categories, advanced cybercrime and cyber-enabled crime. By this definition, advanced cybercrime was described as sophistocated attacks that target computer hardware and software, while cyber-enabled crime described crime where technology and the Internet was used in some part of the process of committing a crime, such as crimes against children, financial crimes, and terrorism (INTERPOL, 2015). In the cases of Dennis Rader, Scott Peterson, and David Leslie Fuller, digital evidence revealed information about how each crime, in these three instances murder, was carried out. In the case of Casey Anthony

however, inaccurate tools and poor attention to detail in the investigation caused the technicians conducting the investigation to miss key evidence including key Internet search terms like "foolproof suffocation," which Anthony supposedly used to murder her two year old daughter (Goodison, Davis, & Jackson, 2015). These cases have demonstrated just how important digital evidence has become in today's criminal investigations, whether it reveals who committed the crime, where or how the crime occured, or how the suspect met the victim.

2.2 Internet Privacy and Concerns

Among the hotly contested debate surrounding the idea of Internet privacy, from a legal perspective is the concept of *right to privacy* on the internet (Bernal, 2014). In the post 9/11 era, where government surveillance has become an increasingly debated topic as a means to thwart foreign and domestic terror plots, differencing opinions among the American people as to whether government surveillance is a necessary precaution to thwart terrorism or whether it is an violation of privacy, has become a bipartisan political issue (G. Gao, 2015). In a 2015 poll conducted by the Pew Research Center, 87% of the poll participants said they were aware of government surveillance programs put in place following the September 11, 2001 attacks on the World Trade Center; of those, a reported 25% admitted to changing the way they use technology (G. Gao, 2015). Among poll respondents, 18% reported changing their use of email accounts, while 17% changed their use of search engines, and 15% changed their use of social media sites (G. Gao, 2015). While this poll only questioned changed usage patterns on computers with respect to email accounts, search engines, and social media sites, the previously mentioned statistics noted changes in technology usage, primarily with regards to the way technology and Internet accounts are used, thus supported that Internet privacy is a growing concern of society, especially with respect to government surveillance.

To further focus on how web browsers are being used to enhance user privacy against prying eyes, the researchers, Gao, Yang, Fu, Lindqvist, and Wang (2014) conducted a survey to identify the general populations understanding of private browsing. The term *private browsing* defined as a "web browser mode in which information about visited websites is not saved" (Vermaat et al., 2015). The survey created by the researchers was hosted on Amazon Mechanical Turk, surveyed 200 participants in the United States, and included multiple choice and open ended questions that were designed to identify what browsers are used the most, what participants knew about private browsing, and whether or not they felt "private browsing" was a useful tool to have (X. Gao et al., 2014). From their survey responses, the researchers found that Chrome had the most users (48.5% of the 200 participants) as well as highest percentage of users that knew about private browsing (76% knowing about private browsing) (X. Gao et al., 2014). Chrome was closely followed by Firefox, and Internet Explorer, whereas Opera and Safari had few users and even fewer with knowledge of private browsing (X. Gao et al., 2014).

Other questions that were asked in the survey include; "Why do you use InPrivate (Private, or Incognito) browsing?", "When do you use InPrivate (Private, or Incognito) browsing?"', "Are there any benefits of using private browser?", and "Are there any drawbacks of using private browsing?" (X. Gao et al., 2014). It should first be noted that when using the terms *InPrivate, Private,* and *Incognito* that the authors were refering to the same thing; the private browsing mode in each browser, differenciated for browser names sake. The answers to these questions supplied both qualitative and quantitative data for the researchers study. Of the 81 participants out of 200 who stated they used a private browsing mode, 39.5% said the reason they did so was, so their browser would not store cookies or web history entries, followed by protecting personal information at 22.2%, followed by visiting dating or pornography web sites at 11.1% (X. Gao et al., 2014). The poll to identify when people used private browsing returned fairly consistent numbers throughout the entire day with 21% in the morning before work, 28.4% using at

work, 39% at night after work, and 28.4% late at night after11pm (X. Gao et al., 2014). In their comparison of the leading benefits and drawbacks, 59.3% identified the key benefit of private browsing as no stored browsing history while 46.9% identified the key drawback of private browsing was there are no drawbacks (X. Gao et al., 2014). Although this study invloved surveys from 200 participants, when asked what people understand about private browsing, 79% were able to provide an opinion or thought with regards to the idea of private browsing while 21% replied that they "didn't know" (X. Gao et al., 2014). Of the 158 out of 200 participants who were able to provide an opinion or thought regarding private browsing, 135 knew about private browsing, but only 81 of the 135 had actually used private browsing. The outcome of this study supports that Internet privacy has become an a growing topic of discussion with some people even taking proactive steps to acheive better privacy when using the Internet.

2.3 Web Browser Artifacts

In their paper on software artifacts, authors Gupta and Mehtre (2013, p. 303) defined the term *web artifacts* as a "kind of by-products produced during installation and/or use of software products." Although their paper focused primarily on the broad term "software forensics," Gupta and Mehtre discussed in depth, the significance of forensic artifacts (2013). They began by discussing areas of interest on the HDD during forensic investigations, noting HKEY_CURRENT_USER as the registry location where programs, desktop settings, network connections, printers, and application preferences were found (Gupta & Mehtre, 2013). The primary items of interest found in this registry were program data and application settings as they will told what programs were recently executed, uninstalled, files recently saved or downloaded, and where software resided in the file system (Gupta & Mehtre, 2013). Of particular interest to the research of this thesis work is the mention of the AppData folder that can be found in newer

versions of Microsoft, as was said to contain specific artifacts such as program settings, IE cookies, toolbar settings, browsing history, tempory files created by applications, library, send to items, and templates among other items (Gupta & Mehtre, 2013). The information regarding browser artifacts in this paper provided a good starting point for understanding where and how to search for browser artifacts.

2.4 Research Methodology of Similar Studies

To identify what research has already been done to test the the claims of enhanced privacy made by browser developers, the following literature reports on methodologies to test the effectiveness of web browsers that claim to have improved privacy, while also identifying where gaps in research exist.

In his research, Noorulla conducted research to test the claims of anonymity of private Web browser modes (2014). Focused on four widely used and well-known web browsers (Internet Explorer, Firefox, Chrome, and Safari) he designed a methodology that included a two part test. The first test involved monitoring the file system for changes made as a result of operating in the private mode of each browser (Noorulla, 2014). For the second test, Noorulla conducted a memory dump of the system after finishing operating in the private browser mode of each browser (Noorulla, 2014). Since files can be written and altered in the file system, memory, or both, Noorulla's methodology was tailored to address all three scenarios to ensure that nothing was missed. In his results, Noorulla found that when looking at the changes made to the file system, only Chrome and Firefox did not write any changes to the file system, whereas Safari wrote data to a single database file called WebpageIcons.db, and Internet Explorer wrote data to the file system but then deleted it (Noorulla, 2014). Looking at the results from the second test, Noorulla found that all browsers left recoverable browser artifacts in memory (Noorulla, 2014). With respect to future research, Noorulla identifed three areas that require more research; those being the effectiveness of browser data eraser software, further

analysis of other browsers, and analysis of browsers designed for mobile devices (Noorulla, 2014).

Research by Marrington, Baggili, Ismail, and Al Kaf (2012) investigated portable web browsers from a forensic investigation perspective. In their study, they posed the research question "Do portable web browsers leave similar forensic artifacts to those left by installed web browsers?" (Marrington et al., 2012). The methodology used by the researchers to investigate the posed question involved creating three similar web browsing sessions, one in the installed version of Google Chrome, one in the portable version of Google Chrome, and one in the portable version of Google Chrome in Incognito mode (Marrington et al., 2012). Once the session data was created, analysis and comparison of the artifacts left behind on the host computer lead to the determination of which instance of Chrome left the smallest forensic footprint on the host computer. In their results, the researchers asserted that using a portable version of Chrome still left artifacts on the computer hard drive even after the USB drive containing the portable instance of Chrome had been removed, thus being able to state that portable browsers did not provide a viable solution to better browsing privacy (Marrington et al., 2012). Future research suggested by the researchers involved conducting a similar test on other popular portable web browsers such as Opera and Firefox.

In research conducted by Aggarwal, Bursztein, Jackson, and Boneh (2010), they investigated the usage patterns of private browsing modes and the level of security these browsers provide for the user. As part of their research, Aggarweal et al., provided a definition for their usage of the phrase "goals of private browsing," that being to protect users from local attackers and to protect the user from web attacks (2010). Their methodology used a technique that used ads and ad-networks to generate traffic that was used to determine if the users navigating to the ads were using a private browsing mode or not and to identify usage patterns for private browsing modes (Aggarwal et al., 2010). For this study, the four widely used web browsers (Firefox, Safari, Chrome, and Internet Explorer) were used. In their

results, the researchers found that private browsing was used mostly for browsing shopping websites and adult websites (those characterized as websites hosting pornographic or other explicit material). Additional findings provided that in terms of security, browser addons and extensions pose potential security risks such as URL whitelist/blocklist/queues, URL mapping, and timestamp storage; all of which can store unwanted browser artifacts (Aggarwal, et al., 2010). Future research identified by the researchers included more research into how to build stronger security measures to maximize user security without degrading the user experience (Aggarwal et al., 2010).

In Gritzalis' paper (2004) about Web privacy, he employed an integrated comparison framework to compare various Web anonymity enhancing security mechanisms, tools, applications, and services. In his research, Gritzalis compared GNUnets Anonymity Protocol (GAP), Freedom, Hordes, Crowds, Onion Routing, Platform for Privacy Preferences (P3P), TRUSTe, Lucent Personalized Web Assistant (LPWA), and Anonymizer (2004). While his work did not discuss the use of private browser modes, this fairly dated research provides evidence that increased awareness for Web anonymity has resulted in increased development of methods of achieving Web anonymity. The methodology used by Gritzalis for his study involved laying out in detail how each anonymity solution worked at the architectural level, then conducted a comparison of the features (2004). As this study was a comparison, their results identified the pros and cons of each anonymity solution but did not specifically say which was the best solution. Future research proposed by Gritzalis included conducting more research into identifying features that have not been implemented yet to provide better security and anonymity (Gritzalis, 2004)

In the study done by Said, Mutawa, Al Awadhi, and Guimaraes (2011), the researchers analyzed the browsers Internet Explorer, Firefox, and Chrome in private browsing mode using FTK Imager Lite, Winhex, EnCase, and cache and history viewers to locate browser artifacts as if the investigation were for a criminal case. The goal of this study was to identify whether or not artifacts from private browsing

sessions can be recovered in the case of a criminal investigation. The methodology used by the researchers involved setting up three identical workstations, each with one of the three browsers installed. In each web browser, web traffic was generated in a private browsing mode unique to each work station as to prevent cross-contamination of data. Using the tools FTK Imager Lite, Winhex, EnCase, cache, and history viewers, an image of the physical memory and hard disk was captured followed by an examination of each instance for browser artifacts. The findings of this study asserted that based on the artifacts that were recovered and the processes necessary to recover those artifacts, private browsing mode offered a level of privacy that is "sufficient for the average user" such that the average user more than likely would not be able to find traces of their web traffic. However, someone with more technical knowledge or a more advanced toolset may still be able to recover artifacts from well-known places where artifacts are stored (Said et al., 2011). The researchers concluded that of the three, Chrome does the best job at hiding artifacts or rendering them unrecoverable. While this study focused on browser history artifacts, the researchers suggested more research into this process with other artifacts such as cookies, certificates, form passwords, and flash cookies (Said et al., 2011).

A similar study by Mahendrakar, Irving, and Patel (2012) investigated artifacts stored in physical memory by private browsing modes of various popular web browsers. In their methodology, the researchers created a website that would generate the following browser artifacts: SSL certificates, form passwords, form text entries, HTML files up to 16MB in size, JPEG files ranging between 100KB and 16MB in size, and cookies (Mahendrakar et al., 2012). VMware Workstation was used to host a Windows XP SP2 machine that was used for the research, giving the researchers the ability to snapshot the machine before the test, after navigating to the page, and again after closing the browser (Mahendrakar et al., 2012). The tool Memory Parser was used to analyze the memory snapshots captured providing the data for this study. The results of this study showed that when looking at browser

memory, in Firefox, Internet Explorer, and Chrome, some artifacts existed but the content in memory had been zeroed while Safari had not zeroed any of the content in browser memory. When looking at the full memory dump for each browser, many more artifacts were recoverable in all four browsers.

The researchers Satvat, Forshaw, Hao, and Toreini (2014) attempted to identify security holes in private browsing modes of common browsers. In their study, the researchers conducted a "from all angles" assessment of private browsing mode security (Satvat et al., 2014). As with much of the already discussed research work, Forshaw et al., populated Firefox, Chrome, Internet Explorer, and Safari with known browser data then analyzed an image of the memory and hard disk to search for recoverable artifacts. Tools used for setup and analysis in this study included VMware Player, WinHex, Index.dat Analyser, SQLite browser, and SQLite manager. The researchers in this study cited Aggarwal et al, 2010 in their definition of the threat model, that of being a local attacker versus remote attacker but they further defined each category to improve the Aggarwal et al. definition (2014). Forshaw et al., found similar results to Aggarwal et al., in that a large majority of security vulnerabilities were caused by browser extensions that make it possible for attackers to gather information about the private browser session. Future work highlighted by this study acknowledged an urgent need for a more systematic approach to design, implementation, and testing of private browser features (2014).

From a different perspective, researchers Xu, Jang, Xing, Kim, and Lee (2015) adopted a problem solving ideology to their research about a program called Ucognito. Their preliminary research identified issues and inadequacies with the current major browsers' private browsing modes much like the research of Aggarwal et al.(2010) and Forshaw et al.(2014) but Xu et al.(2015) proposed a solution instead of simply identifying a problem. Contributions made by Xu et al. were the tools UVerifier and UCognito, which were proposed to help identify security weaknesses in private browsers as well as provide added security and setting functionality for common browsers (2015). UVerifier is an automated tool designed

to identify browser security flaws while UCognito was designed to provide a better private browsing experience by utilizing a filesystem sandboxing feature that, in a nutshell, makes the browser think it is interacting with the computer's actual filesystem as it stores artifacts (Xu et al., 2015). Through implementation and evaluation, the researchers reported, "When applied to Chrome or Firefox, [UCognito] stops all known privacy leaks identified by prior work and our current study" (Xu et al., 2015, p. 11).

In their 2015 paper, researchers Ruiz, Amatte, Park, and Winter (2015) explored a method to capture data that had been created in a private browser. Contrary to much of the previously reviewed literature, this research did not seek to identify issues with private browsing modes or test the anonymity of private browsers. Instead this research identified a process for collecting artifacts that would disprove the alleged privacy of browser vendors (Ruiz et al., 2015). If successful, the process would have served as a method for assessment and validation of private browser techniques (Ruiz et al., 2015). The methodology that Amatte et al. used tested the browsers Internet Explorer 10, Firefox version 24, Google Chrome version 30, and Safari version 5 on a virtual machine using a four part test. The test SFKP is an acronym for the following; S for shutdown, F for freeze, K for kill process, and P for power down. Each of these tests involved generating specific browser data then capturing an image of the virtual machine at a different state to see what happened to the artifacts and if they could be recovered. The results of this study showed that during different machine states, different artifacts were recoverable from each browser. The researchers concluded from this study that the privacy that is being guaranteed in private browsers by browser vendors is not actually being delivered, presenting a much larger problem in a society where web privacy is becoming a large demand (Ruiz et al., 2015).

Applying an industry standard tool, Ohana and Shashidhar (2013) examined private web browsers with the widely used tool Forensic Toolkit by Access Data. Unlike many of the methodologies discussed thus far, the use of FTK is the most

likely methodology, discussed in this review, to be used by law enforcement agencies to conduct web browser forensics. Access Data's Forensic Toolkit is among the industry standards for court-cited digital forensic software, recieving the 2015 SC Magazine Award for Best Computer Forensic Solution, and is used by more than 130,000 law enfocement, government, corporation, and law firm teams and agencies world wide (AccessData, 2015). As with the other methodologies discussed so far, Ohana and Shashidhar (2013) examined and analyzed the common web browsers Chrome, Internet Explorer, Firefox, and Safari in their private browsing modes to identify what artifacts could be identified, and if so, what artifacts could be recovered, and ultimately attempted to determine which browser provides the highest level of privacy. In their methodology, each browser was launched in a virtual machine then a series of documented steps were carried out to generate web browser session data (Ohana & Shashidhar, 2013). Next, the process tree for each browser was closed to ensure the browser fully shut down, the researchers performed a RAM dump using FTK Imager Lite to create an image file to analyze, then each RAM dump was then analyzed in FTK v3.2 and the results documented (Ohana & Shashidhar, 2013). Ohana and Shashidhar (2013) concluded in their findings that all of the private browsers generated recoverable artifacts, although some were easier to establish a link to the user than others. In addition, they concluded that although not always possible for forensic examiners, the best chance of recovering browser artifacts comes from looking at RAM (Ohana & Shashidhar, 2013)

2.5 Tools of Forensic Analysis

In a series of reports on the Department of Homeland Security's website, the results of NIST tool tests are published for the following categories: deleted file recovery and active file listing, digital data acquisition, forensic media preparation, graphic file carving, harware write block, mobile device acquisition, software write block, and video file carving (NIST, 2015b). For the research being done in this

thesis work, the tools tested for deleted file recovery and active file listing is of particular interest and include ILookIX v2.2.3.151, The Sleuth Kit/Autopsy v3.2.2/2.24, X-Ways Forensics v16.0 SR-4, SMART for Linux v2011-02-02, EnCase Forensic v6.18.0.59, and FTK v3.3.0.33124 (NIST, 2015b). The NIST CFTT project adds an extra layer of validation for the tools tested by focusing on repeatability and reproductability, both of which are of great importance for law enforcement agencies that my produce digital evidence in the court of law (Holt, Bossler, & Seigfried-Spellar, 2015). As stated in their book authors Holt, Bossler, and Seigfried-Spellar (2015) note that a great deal of importance should be placed upon validation of digital forensic tools, especially when the used by law enforcement. This idea is reaffirmed by Kanellis, Kiountouzis, Kolokotronis, and Martakos (2006) in their book where they discuss in great detail the importance of the validation process for digital forensic tools and the danger of using tools that have not been properly validated.

2.6 Summary

This chapter provided a review of the literature relevant to Internet privacy, methodologies of similar studies, and discussed tools that have been used in the past to conduct similar studies. These subtopics were discussed to build a legal case for the research to be conducted. As discussed in the early studies, post 9/11 politics have prompted the growth of government surveillance programs as well as sparked debate over the legality of government surveillance and the subject of Internet privacy as a whole. Where the previous studies reviewed in this chapter focused primarily on recovering browser artifacts from Chrome, Firefox, Internet Explorer, and Safari in both their normal mode and their private browsing mode. All of these studies neglected to analyze less popular web browsers with better privacy built into them by default. The research in this chapter also failed to conduct comparisons between common web browsers and less popular, enhanced privacy browsers. The

tools identified in the above reviewed literature provide various degrees of data processing, from database viewers to full access to the file system and deleted content.

CHAPTER 3. FRAMEWORK AND METHODOLOGY

The research discussed in the above reviewed liturature focused on the four most widely used desktop web browsers for the year 2015: Google Chrome (53.95%), Microsoft Internet Explorer (19.38%), Mozilla Firefox (17.58%), and Safari (5.03%) as identified by real time, global stat tracking web page *gs.statcounter.com* (2016). Where previous research methodologies above explored different methods to recover and analyze browser artifacts from the four most common browsers, little to no research has been completed to compare the improved privacy features of third party web browsers to the private browsing mode of the four most widely used web browsers. The research completed in this thesis work addressed this research gap by attempting to recover and analyze browser artifacts from the three, common to Windows web browsers: Google Chrome, Microsoft Edge, the replacement for Internet Explorer in Windows 10, and Mozilla Firefox, and did the same for three third party, enhanced privacy web browser to conduct a comparison. This comparison was designed to assess the advancement in browser privacy by comparing the analysis of the enhanced privacy browsers to the three common browsers running in private browsing mode to determine whether enhanced privacy browsers provided better privacy or if the industry standards are caught up in terms of privacy features.

3.1 Research Framework

The general framework for this research established the experimental conditions for conducting the collection of information and artifacts from enhanced privacy web browsers (i.e. Epic, Dooble, and Comodo Dragon) and private browsing modes of common web browsers (i.e. Chrome, Edge, and Firefox) that were

analyzed and compared for results. Several forensic investigation models existed to guide investigators through the investigation process including how evidence is collected, preserved, verified, examined, analyzed, and reported. For this study, the Computer Forensics Field Triage Process Model served as the forensic analysis framework and basic guide for the investigation process of Internet-based evidence. Although several models looked similar, the CFFTP model included a more detailed phase in particular to Internet-based evidence, containing three subphases: browser artifacts, e-mail artifacts, and instant message artifacts (Rogers, Goldman, Mislan, Wedge, & Debrota, 2006). Many other models did not go into detail to specifically address Internet-based evidence in the investigation phase and thus, were not as well-suited for this research methodology.

3.2 Study Design

As a case study of applied forensic process to Internet web browsers, the research conducted was both qualitative and quantitative in nature and sought to identify, recover, and view the content of web browser artifacts from prepopulated, known web browser traffic. The browser artifact files and the contents of these files provided the basis for analysis and measurement. The focus of this research design was to conduct a case study of enhanced privacy and common web browsers in private browsing mode, in which recoverable browser artifact files served as evidence to answer the research question of this study, in particular, identifying which browsers produced fewer recoverable artifacts, and as a result, provide better privacy.

To address answering the research question, this reserach methodology conducted a forensics analysis of three enhanced privacy web browsers and three common web browsers in private browsing mode, using two different forensic analysis tools for analyzing entire disk images and file systems. Prior to analyzing the browsers, each browser was populated with known browser traffic, designed to

generate ten different types of browser artifacts. Following browser data population, the browser window was closed, the VM was saved, shut down and imaged using FTK Imager. Once imaged, the image file was loaded into each tool and the data was processed. For each browser, additional reseach of published white papers and research studies provided a list of artifact file names and locations for each artifact of each browser. Then a baseline was created for each browser by searching all of the locations for the artifact files as identified in the previous research. Following creating the baselines, ten trials were conducted by processing the baseline image on ten separate machines containing the same OS and tools. Each trial was compared tothe baseline for test-restest repeatability. The ten trials served to test the tools for reliability, while using two tools served as a reliability test of this methodology. Data collection included counts of each recovered artifact file as well as categorizing each artifact into a matrix under one of three categories: *File Present with Content, File Present with No Content Present,* and *File Present Required Tools.* Two forms of data collection allowed for both quanitative and qualitative analysis. For quantitative data analysis, means for each browser, by artifact, were calculated to conduct an ANOVA to compare the means of the two groups of browsers. These findings where then used to report the findings of this study.

3.3 Hypothesis

H: The enhanced privacy browsers Epic, Comodo Dragon, or Dooble produced fewer browser artifacts than the common web browsers Chrome, Edge, or Firefox in private browsing mode, thus providing a higher degree of privacy.

3.4 Software and Software Versions

Table 3.1 contains a list of all software and version numbers used in this research.

Table 3.1:

Software and Version Numbers

Software	**Version**
Virtual Box	5.0.16
Windows 10 Enterprise 64-bit	10.0 (build 10240)
FTK Imager	3.4.0.5
FTK	5.3.3.9
Autopsy	4.0
Microsoft Edge	20.10240.16384.0
Google Chrome	50.0.2661.102m
Mozilla Firefox	45.0.2
Epic	48.0.2553.0
Comodo Dragon	45.9.12.393
Dooble	1.56
SPSS	22

3.5 Experiment Processes

This section listed in detail each process that was foregone to conduct this research methodology. In this section, more detail was provided for each process described in the study design, including VM configuration, selection of browsers, selection of tools, data population, imaging, data processing, and data collection.

3.5.1 VM Configuration

Oracle Virtual Box v.5.0.16 was used to replicate a Microsoft Windows 10 environment as it is quicker to set up than an actual Windows environment on a physical hard drive. Virtual Box was choosen in part because it is open-source software and is free for use. Unlike VM Ware, a non-free virtual environment software, Virtual Box can store the virtual instance of an operating system

environment as a virtual hard disk file, which can easily be mounted in FTK Imager as a logical drive and imaged for analysis. The use of virtual environment software provided an efficient and free method of creating multiple instances of an OS environment without needing additional hardware such as disk drives. In this methodology, one virtual machine was created with the specifications below, then cloned five times to ensure the identical environment was used. Each VM was then booted and had one of each browser installed.

VM Configuration:

- Processor: 2 Processors
- Memory: 4 GB
- Storage: 14 GB
- VM File Format: Virtual Hard Disk (VHD)
- OS: Microsoft Windows 10 Enterprise 64-bit Build 10240
- Windows Install Type: Windows Custom Install (Windows file ONLY)
- Computer Name: (1 of 6 browsers)
- Installed browser: (1 of 6 browsers)

3.5.2 Browser Selection

This section discussesed the web browsers that were used in this methodology and why they were chosen for use in this methodology.

3.5.2.1. Enhanced Privacy Web Browsers

The research methodology of this thesis work tested common web browsers as well as third party web browsers designed with privacy and anonymity in mind, to compare to the common web browsers using anonymous browsing mode. As such, the method for choosing the web browsers to be used was based upon open source research via Google search to identify three privacy enhanced browsers, based on how likely someone would be to find one of the browsers by perfoming a Google search for the key terms "private browser," "secret browser," or "anonymous browser." One stipulation, as listed in the delimitations section, was the exclusion of any browser that used the Tor network or proxy servers, as those browsers employ network-based solutions to increase privacy was not part of this research methodology.

In a TechWorld online article on the top secure web browsers of 2015, the three highest rated enhanced privacy web browsers are Epic Browser, Comodo Dragon browser, and Dooble browser (Dunn, 2015). As stated by in the article, Epic Browser, based on Chromium, achieved better privacy by striping out many of the features which populate browser artifacts (Dunn, 2015). While Epic Browser was said to route searches through a proxy server belonging to the company that developed it, Epic did not rely on proxy server, therefore is allowable for the research methodology of this thesis work (Dunn, 2015). In addition to anonymous searching, Epic browser was also said to eliminate cookies and trackers at the end of each session in addition to not collecting any user data during the session (Dunn, 2015). Comodo Dragon browser was similar as it was a Chromium-based web

browser, but functioned differently from Epic in that it includes "SecureDNS" servers which could be used to bypass ISP infrastructure as well as a "virtualised mode" which was said to isolate the browser from the host system (Dunn, 2015). The third highest rated browser according to techworld.com was Dooble browser which featured the default use of secure HTTP and included encryption methods for bookmarks, browsing preferences, and history (Dunn, 2015).

Another blog about private web browsers again, rated Epic Browser and Comodo Dragon among the top enhanced privacy web browsers (Henry, 2014). Although Dooble browser was not listed on as many blogs and pages as Epic and Comodo Dragon, it was among the few private browsers found that did not use proxy servers or the Tor network. Additionally, among the top results during the google search was the home page for Comodo Dragon and Epic Browser.

One piece of verbage of importance to note during this search is the distinction between *secure browsers* and *private browsers*. Some browsers were listed as being more secure, often stating they did not store or allow tracking cookies, had built in malware protection, blocked advertisements, and did not allow certain plug-ins such as Java and Flash, which have a long history of presenting security vulnerabilities (Zaharia, 2015). For the research being conducted in this thesis work, these browsers were not of interest as the research focused on local artifacts, not those that would make a user identifiable by a website or server. Browsers that were listed as *private browsers* included features similar to what can be seen in Internet Explorer's InPrivate browsing mode as well as similar browsers such as Chrome and Firefox, where potential artifacts such as cookies, temporary Internet files, webpage history, form data, and more is not stored or is created but deleted upon ending the browser session (Microsoft, 2015b). As the research in this thesis work sought to conduct a comparison of enhanced privacy web browsers and common web browsers in anonymous browsing mode to determine whether enhanced privacy browsers provide better privacy, *private browsers* are the types of

web browsers that were included in the research methodology as enhanced privacy browsers.

3.5.2.2. Common Web Browsers with Private Browsing Mode

This research compared enhanced privacy web browsers with common web browsers in private browsing mode as the primary objective. As such, the common web browsers with private browsing modes were selected from a monthly online poll of the most commonly used web browsers. The online statistics website w3counter.com conducted a monthly poll of browser marketshare and reported that during the entire year of 2015, the top three most used web browsers available for the Microsoft Windows OS were Google Chrome, Microsoft Internet Explorer/Edge, and Mozilla Firefox (W3Counter, 2016). Being as these three browsers accounted for approximately 60% to 70% of all browsers used, including Safari which is a browser exclusive to the Macintosh OS, they served as the three common web browsers with built in private browsing modes used in this study (W3Counter, 2016).

3.5.3 Tool Selection

Of the tools tested by NIST, EnCase and FTK were among the most well known industry standards, used widely by law enforcement agencies and in academia (Data, 2015) (Software, 2015). As these are enterprise solutions that have been widely used by industry and government agencies, they were ideal for this reserach, however only FTK was available in the Purdue University Cyber Forensics laboratory. An open source program similar to FTK and EnCase called Autopsy was used in the place of EnCase, as it was a free, but similar program to FTK and EnCase. FTK Imager was used in this methodology to create .e01 image files of each VM following the data population process. FTK Imager can produce image

files of various types including raw image files (typically ending in a .001 file extension) and EnCase image files (.e01). This methodology used the EnCase image file type because it is supported by both FTK and Autopsy. Ultimately, this research methodology looked to employ a similar test methodology for the collection of browser artifacts as in the study done by Ohana and Shashidhar (2013), who conducted a forensic analysis on private browsing modes of Internet Explorer, Chrome, Firefox, and Safari. Although the research methodology and intended research outcomes varied slightly in scope and purpose from Ohana and Shashidhar's study, by using FTK, and Autopsy in the place of EnCase, a preliminary comparison could have been made between the outcomes of Ohana and Shashidhar's research and the reserach taking place in this study with regards to common web browsers in private browsing mode. As a source of validity, upon similar results, a basis of confidence can be established with regard to the process of collecting and recovering browser artifacts from each browser. Where this research differentiated from Ohana and Shashidhar's work, and all the other research reviewed for that matter, was the future steps and end goal of comparison of the results to identify and determine if enhanced privacy web browsers provided better privacy than the common web browsers using private browsing mode.

3.5.4 Data Population

The data population process for this research included visiting web sites, creating bookmarks, submitting credentials to websites that required username and passwords, searching terms, sending emails and instant messages, and viewing videos and images for the purpose of simulating common types of web traffic. For research purposes, this data population method was designed to create browser artifacts that, in a real investigation, may have revealed context of user browser usage. For this data population process, ten websites were selected from a list of the top 500 most viewed sites in the United States as ranked in an 2015 Alexa poll.

Alexa is an Internet-based company owned by Amazon.com that provides subscription-based web analytics and digital marketing tool services (Alexa, 2016). Due to the number of websites on this list, the sites used were all selected from the top 20, and were choosen to produce specific browser artifacts data. Table 3.2 contains a list of the web sites used, browser artifact types, and which artifacts were expected to be created from each web site as a result of the data population process. The browser artifacts used in this methodology were selected as they provide a vast amount of information about the browsing habits of the user and are typically stored in the browser application folder, making them relatively easy to locate.

Table 3.2:

Artifact Relationships

Web Site Used	**History**	**Cookies**	**Bookmarks**	**Credentials**	**Searches**	**Cache**	**URLs**	**Pic/Vid**	**IM**	**Email**
Google.com	X	X	X	X	X	X	X	X		X
Facebook.com	X	X	X	X		X	X		X	
Youtube.com	X	X	X	X	X	X	X	X		
Amazon.com	X	X	X	X	X	X	X			
Wikipedia.org	X	X	X	X		X	X			
Yahoo.com	X	X	X	X	X	X	X	X		X
Twitter.com	X	X	X	X		X	X			
Instagram.com	X	X	X	X		X	X			
Imgur.com	X	X	X	X		X	X			
Ebay.com	X	X	X	X		X	X			

Note. X = Content expected to be created for the website/artifact combination.

The additional tables listed all account information and content searched for, viewed, sent, and submitted in the data population process:

Table 3.3:

Data Population Content

	Search Terms	**Email Text**	**Instant Message Text**	**Bookmark**
1	Golf	Email1	Message1	www.google.com
2	Baseball	Email2	Message2	www.facebook.com
3	Bowling	Email3	Message3	www.youtube.com
4	Tennis	Email4	Messages4	www.amazon.com
5	Football	Email5	Message5	www.wikipedia.com
6	Hockey	Email6	Message6	www.yahoo.com
7	Cycling	Email7	Messages7	www.twitter.com
8	Soccer	Email8	Message8	www.instagram.com
9	Running	Email9	Message9	www.imgur.com
10	Lacrosse	Email10	Message10	www.ebay.com

Table 3.4 lists the user credentials that were created prior to conducting data population process.

Table 3.4:

User Account Credentials

	Website	**Username**	**Password**
1	Google	thesistest0001@gmail.com	G00glePswd
2	Facebook	thesistest0001@gmail.com	F@cebookPswd
3	Youtube	thesistest0001@gmail.com	G00glePswd
4	Amazon	thesistest0001@gmail.com	Am@zonPswd
5	Wikipedia	thesistest0001	W1kiPswd
6	Yahoo	thesistest0001@yahoo.com	Y@hooPswd
7	Twitter	thesistest0001@yahoo.com	Tw1tterPswd
8	Instagram	thesistest0001	Inst@Pswd
9	Imgur	thesistest0001	1mgurPswd
10	Ebay	thesistest0001@yahoo.com	Eb@yPswd

Below is the detailed process that was completed to populate each browser with sample data. The videos, images, instant messages, and emails have no significance other than to produce uniquely identifiable browser traffic. While not imperative to this study, it should be noted that for each image and video viewed in the benchmark trial, the same images and videos were viewed in each subsequent trial.

- Launched VM
- Opened browser in private mode (for common browsers) or normal mode (for enhanced privacy browsers).
- Opened 10 tabs and navigate to each URL from Table 3.2.
- Saved each URL as a bookmark.
- Logged into each website.
- Saved credentials in browser.
- Sent 10 emails betwen Google and Yahoo email accounts.
  - All odd numbered messages were sent from Jon Doe (Google) account.
  - All even numbered messages were sent from Jane Doe (Yahoo) account.
  - **All emails were opened and read.
- Searched each search term in Youtube and played 30 seconds of each video.
- Searched 10 terms in with search engines as follows:
  - Google:
    * Golf
    * Baseball
    * Bowling

        * Tennis
        * Football
    - Yahoo:
        * Hockey
        * Cycling
        * Soccer
        * Running
        * Lacrosse

- Sent 10 instant messages in Facebook chat.
    - All odd numbered messages were sent from John Doe Facebook account.
    - All even numbered messages were sent from Jaine Doe Facebook account.
    - **Jaine Doe account is not listed in Table 3.4 but was required to receive and send instant messages from the John Doe Facebook account.
- Closed the browser window to end the browser session.
- Saved and shut down VM.

3.5.5 Data Collection and Reporting

The data collection process required additional research to identify locations within the file system where each artifact file was expected to be found. Due to each image containing over 180,000 viewable items, data collection was limited as 132 trials in total were conducted. Once the artifact files and their locations were identified, one baseline trial was run for each browser in each tool for a total of 12 baselines. Then, 10 trials were run of each browser in each tool, with only the locations searched for in the baseline being searched in the trial as well. The trials consisted of the image used for each baseline being analzyed 10 additional times by

comparing the recoverable artifacts to those found in the baseline. This design served as a test of test-retest reliability. The results of each trial were reported in a matrix that kept track of what artifact files were found for each browser. Upon collecting the data, each artifact received one of four possible classifications:

- XX = "Artifact found, content found"
- X = "Artifact found, no content found"
- X* = "Artifact found, required additional tool"
- " - " = "No artifact found"

Following data collection, counts and means were calculated for each browser, per tool and browser to compare to each other using an Anova. Additional qualitative analysis was conducted based solely on the data represented in the matrix.

3.5.5.1. Browser Artifact Research

For each browser, additional research of published white papers and similar published technical reports were examined for documentation of known locations and file names for each browser's artifacts. The findings were similar for each browser. In the case of all of the browsers examined in this methodology, the artfiact files were found in the browser's application folder tree. Once the location and name of each file was identified, the trial process occured. Below are a list of the file names and locations that were searched for browser artifact files. Images, videos, instant messages, and emails, unlike the other traffic were not stored in database files in the browser application folder and therefore were searched for by using FTK and Autopsy indexed images, videos, Internet chat, and email files.

Microsoft Edge. The locations, including file names or folder names for each artifacts are listed below in Table 3.5. It should be noted that the data from Table

3.5 is actually for the developmental pre-release version of Edge known as Project Spartan. In the current version of Edge, artifacts are stored in the WebCache database files, spartan.edb, as well as the WebCacheV01.dat file which was consistent with the pre-release version. While the exact file path differed from the table below with respect to the folders Project ID and Spartan, the general location remained the same. FTK and Autopsy were capable of locating these database files and indexing them as Internet files as well.

Table 3.5:

Artifact Locations of Edge

Artifact	**Location**
History	"/LocalAppData/Spartan/Database/WebCacheV01.dat"
Coookies	"/LocalAppData/packages/microsoft.windows.spartan_{packageID}/AC/##!001/Spartan/Cookies"
Bookmarks	"LocalAppData/packages/microsoft.windows.spartan_{packageID}/AC/Spartan/User/Default/Favorites"
Stored Credentials	"/LocalAppData/Spartan/Database/WebCacheV01.dat"
Search Terms	"/LocalAppData/Spartan/Database/WebCacheV01.dat"
Browser Cache	"/LocalAppData/packages/microsoft.windows.spartan_{packageID}/AC/#!001/Spartan/Cache"
Typed URLs	"/LocalAppData/Spartan/Database/WebCacheV01.dat"
Viewed Images/Video	Search FTK/Autopsy
Instant Messages	Search FTK/Autopsy
Email	Search FTK/Autopsy

Note. Table data source: (Gratchoff & Kroon, 2015).

Google Chrome, Epic, and Comodo Dragon. Locations for browser artifact data from the browsers Chrome, Epic, and Comodo Dragon were listed in this section. Little to no published research was found for artifact storage of Epic and Commodo Dragon. As such, artifacts in Epic and Commodo Dragon were searched for in the same locations as Chrome. The reason for this was due to the similarity of the three browsers. The similarity was the result of all three browsers being built on the open-source Chromium browser platform (Comodo, 2016) (Epic, 2016). Since each browser used the Chromium platform, they function and store data in similar places and in similar fashions. The previous statement was confirmed by setting up a test VM with Epic and Comodo Dragon installed, then the author navigated to

the same file path as Chrome but for each browser's folder in the place of Chrome. This revealed many of the same database files and folders present in Chrome.

Table 3.6:

Artifact Locations of Chrome, Epic, and Comodo Dragon

Browser	**Location**
Chrome	C:/Users/Username/AppData/Local/Google/Chrome/User Data/Default
Epic	C:/Users/Username/AppData/Local/Epic Privacy Browser/User Data/Default
Comodo Draggon	C:/Users/Username/AppData/Local/Comodo/Dragon/User Data/Default

Note. Table data source: (Akbal, Gunes, & Akbal, 2016).

Firefox. Locations for browser artifact data in Firefox was listed in this section. Similar to Chrome, Epic, and Comodo Dragon, Firefox stored its artifacts in a single folder within the user applications directory. As stated in an article on browser forensics, Firefox stored artifacts in different locations, depending on the OS, however for Microsoft Windows 7 and newer, they were stored in the location listed in Table 3.7 (McQuaid, 2014). This folder, like that of Chrome, Epic, and Comodo also contained several artifact database files.

Table 3.7:

Artifact Locations of Firefox

Browser	**Location**
Firefox	C:/Users/Username/AppData/Local/Mozilla/Profile/*.default/Cache

Note. Table data source: (McQuaid, 2014).

Dooble. Dooble browser, unlike the other five browsers in this study was not well documented or at all for that matter. Unable to find any published work or even blog postings regarding Dooble browser artifacts, the process of identifying artifacts for Dooble was reliant on the tools to index files and identify any possible

database files related to Internet usage and report them as an Internet file as done with the other browsers. In addition, becuase it was unknown if Dooble used another browser's platform in the design and development process, similar to Epic and Comodo Dragon with Chrome and Chromium, Dooble's application data was viewed for signs of artifacts. The location of Dooble's application data was listed below in Table 3.8.

Table 3.8:

Artifact Locations of Dooble

Browser	**Location**
Firefox	C:/Users/Username/AppData/Local/

3.6 Variables

For this study, the independent variables being tested were the web browsers Epic Browser, Dooble, Comodo Dragon, Google Chrome, Firefox Mozilla, and Microsoft Edge as well as the forensic analysis tools Forensic Toolkit and Autopsy. Each browser served as an individual test, therefore the dependent variable being observed and measured in each experiment was the artifacts recovered.

3.7 Summary

This chapter discussed in detail the study design, methodology, and methodological components for this research. The focus of this methodology was the process forgone to populate the browsers with data, find and identify artifact files in known locations, discern the classification of each artifact file found (See -Data Reporting- for classifications), and ultimiately conducted a qualitative and quantitatve analysis of the reserach outcome.

CHAPTER 4. RESULTS

This chapter described the results as found from the descriptive statistics for the current study, discussed in the following sections: descriptive statistics, hypothesis testing, and post hoc assessment. The section titled descriptive statistics provided a narrative of the browser artifacts recovered by each browser-tool combination in terms of both artifact type and counts recovered. The section that followed, titled hypothesis testing specifically addressed the author's hypothesis via a conducted comparison of the relationships between browser type and artifacts recovered. Finally, the post hoc analysis section compared the two tools tested in this research to address and compare the effectiveness of each tool with respect to browser artifact recovery.

4.1 Descriptive Staistics

The process of data collection artifact files were categorized into 1 of 3 groups: "Artifact Found - Content Found", "Artifact Found - No Content Found", or "Artifact Found - Requires Tool". This categorization dictated that if no artifact file is found, the result would be "No Artifact Found", however this category was not included in the result matrix. Following the 10 trials of each browser, it was noted that all ten trials produced the same artifact files for each given browser such that there was no variance between the ten trials of a browser. For further clarification, there was variance found between the number and type of recovered artifacts for each of the six browsers but no variance was found between the ten trials of a given browsers. Since there was no variance in the results of the ten trials for each browser and tool combination, an ANOVA test to compare the means of each browser and tool combination was a moot point and thus was not conducted. The lack of

Table 4.1:

Browser Artifacts Recovered by Browser and Tool

Browser Type/Browser	Tool	History	Cookies	Bookmarks	Credentials	Searches	Cache	URLs	Pic/Vid	IM	Emails
Common											
Edge	FTK	XX	XX	XX	-	-	XX	-	XX	-	-
	Autopsy	X*	XX	XX	-	-	X*	-	XX	-	-
Chrome	FTK	XX	X	XX	X	X	-	-	-	-	-
	Autopsy	X	X	XX	X	X	-	-	-	-	-
Firefox	FTK	XX	X	XX	-	-	-	-	-	-	-
	Autopsy	X*	X	XX	-	-	-	-	-	-	-
Enhanced											
Epic	FTK	X	X*	XX	XX	X	XX	-	XX	-	-
	Autopsy	X*	X*	X*	X*	-	X*	-	XX	-	-
Comodo	FTK	XX	XX	XX	X	X	XX	-	-	-	-
	Autopsy	X*	X*	XX	X*	-	-	-	-	-	-
Dooble	FTK	XX	XX	-	-	-	-	-	-	-	-
	Autopsy	-	-	-	-	-	-	-	-	-	-

Note. XX = Artifact found, content found; X = Artifact found, no content found; X* = Artifact found, required additional tool

variance among the ten trials marked test-retest reliability of the tools. As a result, analysis was conducted using the data collected and stated in the result matrix.

For this table, it is important to note that "X" represented a browser artifact file that was recovered and included those that did not contain any data from the known browser traffic or required another tool to read the artifact content. Strictly spoken in terms of recovered artifact files, looking at the two groups of web browsers, this table illustrated what kind of artifact files were recovered for each browser and tool combination. As depicted in Table 4.1, both groups of browsers produced several recoverable artifacts, with many commonly recovered artifacts like history, cookies, and bookmarks. The table also showed the difference between the tools and their ability to recover and view artifact files.

As the data in Table 4.1 illustrated, the difference between the number of artifacts recovered in the common browser group and enhanced privacy browser group differed by one at the most. Within the groups, there were browsers that produced fewer artifact files than the others, in particular Firefox and Dooble for

their respective groups. Firefox only produced three recoverable artifacts as reported by both tools while Chrome and Edge produced five artifacts as reported by both tools. Among the enhanced privacy browsers, Dooble produced two artifacts as reported by FTK and none by Autopsy while Epic produced eight as reported by FTK and seven by Autopsy; comparable to Comodo Dragon that produced six as reported by FTK and four by Autopsy. It should be noted that the number of recovered artifact files reported for each browser in the two previous statements indicated the same artifact files were found in each trial. For example, the same three artifact files were recovered in all ten trials for Firefox by each tool.

Table 4.2:

Artifact Count by Browser and Tool

		Artifacts			
Browser Type/Browser	**Tool**	**Content**	**No Content**	**Requires Tool**	**Total**
Common					
Edge	FTK	5 (50)	0 (0)	0 (0)	5 (50)
	Autopsy	3 (30)	0 (0)	2 (20)	5 (50)
Subtotal		8 (40)	0 (0)	2 (20)	10 (50)
Chrome	FTK	2 (20)	3 (30)	0 (0)	5 (50)
	Autopsy	1 (10)	4 (40)	0 (0)	5 (50)
Subtotal		3 (15)	7 (35)	0 (0)	10 (50)
Firefox	FTK	2 (20)	1 (10)	0 (0)	3 (30)
	Autopsy	1 (10)	1 (10)	1 (10)	3 (30)
Subtotal		3 (15)	2 (10)	1 (05)	6 (30)
Total		14 (23)	9 (15)	3 (05)	26 (43)
Enhanced					
Epic	FTK	4 (40)	2 (20)	1 (10)	7 (70)
	Autopsy	1 (10)	0 (0)	5 (50)	6 (60)
Subtotal		5 (50)	2 (20)	6 (60)	13 (65)
Comodo	FTK	4 (40)	2 (20)	0 (0)	6 (60)
	Autopsy	1 (10)	0 (0)	3 (30)	4 (40)
Subtotal		5 (50)	2 (20)	3 (30)	10 (50)
Dooble	FTK	2 (20)	0 (0)	0 (0)	2 (20)
	Autopsy	0 (0)	0 (0)	0 (0)	0 (0)
Subtotal		2 (10)	0 (0)	0 (0)	2 (10)
Total		12 (20)	4 (06)	9 (15)	25 (41)

Note. Values represent frequency with percentages in parentheses.

Max count for browser/tool combination was 10, max count for subtotals was 20, and max count for totals was 60.

The artifacts found were not always the same for both tools with each browser.

To further refine the raw data into a table that provided better context for the recovered artifacts, Table 4.2 listed each browser and tool however, instead of listing each artifact file, this table listed the artifact and content category as a single summed criteria. The three categories in this table describe three types of recovered artifacts. “Artifacts with Contents” described those artifacts where the artifact file was recovered by one of the tools and the tool was able to read the artifact and render metadata or content for some of the generated traffic viewable. “Artifacts without Content” described artifacts that were able to be recovered and read by the tools but did not contain any metadata or content from the generated browser traffic. “Artifact Requires Tool” described artifacts that were recovered by the tools but required an additional tool to read the metadata contents of the generated traffic. Examples of artifacts that requirde tools are some database artifacts such as ESE or SQL databases. Browsers that used these databases included Edge, Epic, Google (or Chromium variants), and Firefox, to name a few. While these may not have always required additional software to read artifact contents, in the the case of this experiment, there were at least 12 artifact files that required additional tools.

Analysis of this table showed an important difference between the two groups that was not as apparent as in Table 4.1. Based on totals alone, the enhnaced privacy browsers produced one fewer recoverable artifact in total than the common web browsers. The major differences occured in the number of recovered artifacts that did not contain content versus those recoverable artifacts that required additional tools to view content. The common browsers produced a total of nine artifacts that were viewable but did not contain content from the generated web traffic, this compared to the enhanced browsers that produced a total of four artifacts that did not contain and content from the generated web traffic. In terms of recovered artifacts that required additional tools to be viewed, the common browsers only produced three of these while the enhanced browsers produced nine. This research did not further investigate tools to view the artifacts that were not viewable in FTK or Autopsy.

4.2 Hypothesis Testing

The hypothesis posed by the author at the beginning of this experiment stated the enhanced privacy browsers would produce fewer recoverable artifacts than the common web browsers in private browsing mode. Taken into consideration the qualitative and quantitaive data in Tables 4.1 and 4.2, the two groups produced different numbers of artifacts, with the common web browsers producing one more artifact than the enhanced privacy web browsers. Table 4.1 showed that the maxium number of artifacts found, given the browser and tool combinations within the groups of common and enhanced privacy browsers was 60. Comparing frequency and percentages, the common browsers produced a total of 26 artifacts out of a possible 60, while the enhanced privacy browsers produced 25 out of a possible 60. The percentage of artifacts produced by the common browsers was 43.3% compared to the enhanced browsers at 41.6%. The difference between the frequencies and percentages was small and thus not significant, attributed to potential small sources of tool or experimental error. As such, based on the data found in Tables 4.1 and 4.2, the author failed to accept the hypothesis on the basis that although the data present showed the enhanced privacy browsers produced fewer artifacts than the common browsers, the difference was not significant.

4.3 Post Hoc Assessment

Additional analysis was conducted for the tools used in this research. In terms of tool effectiveness, Table 4.2 illustrated that FTK recovered the same number of artifacts or more than Autopsy for every browser. In addition, in cases where FTK and Autopsy recovered artifacts belonging to multiple classifications, FTK produced more viewable artifacts with content or more artifacts that at least did not require additional tools to view the content. In terms of effectiveness by browser type, both tools proved more effective at producing recoverable artifacts for the common web browsers where they combined to produce 24 viewable artifacts

compared to only 16 for the enhanced privacy browsers. Where FTK was about as equally effective for each browser type producing 13 viewable artifacts from the common web browsers and 14 for the enhanced privacy browsers, Autopsy was five times more effective on common browsers than enhanced privacy browsers, having produced 10 viewable artifacts from the common browsers it only produced two for enhnaced privacy browsers. In total, FTK produced more than double the number of viewable browser artifacts in comparison to Autopsy, with a total count of 27-12 in favor of FTK. Based on these findings, FTK was the better tool for recovering and viewing browser artifacts in the case of every browser in this study.

4.4 Summary

This chapter reported the results of the data collection and data processing procedure as outlined in the methodology of this research. Results were reported in three sections, Descriptive Statistics, Hypothesis Testing, and Post Hoc Assessment. In the section titled Descriptive Statistics, Table 4.1 reported which artifacts were recovered by each browser and tool combination and classified each artifact found as having contained browser content, contained no browser content, or required another tool to view the artifact. Table 4.2 reported the frequencies and percentages of artifacts found as well as artifacts classfied in one of the three categories in Table 4.1, both by browser and browser type. This data was compared in the section titled Hypothesis Testing to detemine that the author failed to accept the hypothesis posed for this research; that being enhanced privacy browsers produced fewer artifacts than common web browsers using private browsing mode. Finally, the Post Hoc Assessment section compared the results reported in Table 4.1 and 4.2 to report on the effectiveness of FTK and Autopsy, ultimately identifying FTK as the more effective tool.

CHAPTER 5. DISCUSSION

The question this research sought to answer was whether enhanced privacy web browsers provided better privacy than the private browsing mode of common web browsers, in particular in the case of digital forensic investigations. In the current study, there was not enough evidence to suggest that the enhanced privacy browsers did indeed outperform the common browsers.

There exist privacy-minded individuals who prefer not to leave traces of what they do on the interent on their computer. The main concern being that someone else may be able to access information about where one went to on the Internet, what they did, and potentially, who they were in communication with (G. Gao, 2015). For those who sympathize with this rhetoric, this research is relevent to identify what types or specific browsers provide the best user privacy. The opposite side of this discussion bore a distinct significance to law enforcement and technicial specialists responsibile for conducting forensic analysis to solve crime or conduct incident response. Often times, these security or forensic professionals are looking for data that an individual attempted to hide. For these individuals, having an understanding of tools and methods to obtain browser data from these types of browsers, as well as an understanding of what is expected to be found may help improve quality and accuracy of data analysis.

This study was modeled after the study conducted by Ohana and Shashidhar in which they analyzed the private browsing modes of the web browsers Chrome, Internet Explorer, Firefox, and Safari to investigate what artifacts, if any, were recoverable (2013). While their study was similar to this research, it was not the only study that investigated the effectiveness or private browsing. Studies by Noorulla (2014), Marrington et al. (2012), Said et al. (2011), Mahendrakar et al. (2012), and Ruiz et al.(2015) all investigated private session browsing for one reason

or another. In all these studies, artifacts were recovered typically either by analyzing a RAM dump or by actually analyzing the file system of a virual machine in tools like EnCase or FTK. Focusing on the E-discovery phase of the investigation, these studies sought to try to recover artifacts to see if it was possible.

This study, which had findings consistent with these previous studies, progressed these previous studies to not only see if it were possible to recover artifacts but to take it one step further by introducing three browsers that are not widely used but are said to provide better security with the goal of testing them to compare against the findings of these previous studies. While many of the studies discussed used memory dumps, this methodology yielded lots of viewable artifacts by simply conducting a file system analysis of the VM. Ultimately this study failed to compare to previous studies becuase this study was an extension of these previous studies. It was well documented in all of these studies that browser artifacts were able to be recovered. This study ventured beyond that to better understand how common web browsers in private browsing mode compared to less known browsers that were designed with better privacy in mind. What this study found was that not only did all of the browsers analyzed by the author produce recoverable artifacts, based on research completed by others, every other browser analyzed produces recoverable artifacts as well. While this scenario is favorable for investigators or law enforcement seeking to use this information for investigative purposes, as Ruiz et al. (2015) states, claims of complete privacy by web browser vendors is still not being delivered.

The toolset used in this research was selected to simulate the kind of forensic investigation that would be common practice of a law enforcment investigation of this sort. FTK and Autopsy provided complete file system analysis which is useful because in most investigations, knowledge of what data exists and where on a system is unknown prior to conducting the investigation. The studies mentioned in the previous section employed a wide variety of tools from WinHex Dump and Memory Parser to FTK and another commercial forensic software EnCase. The

issue with immediately resorting to memory dumps is that it requires machine in question be running that the time of discovery to conduct a memory dump. FTK and Autopsy on the other hand provide the capability to do "dead forensics," or forensics on a machine that has already been powered down.

For this study, any tool such as FTK, EnCase, or Autopsy that can be used to conduct a full analysis of the file system appeared to have been able to recover some of the browser artifacts files. In this particular study, FTK and Autopsy were successful in indentifying and recovering browser artifact files from common and enhanced privacy web browsers. While FTK was in many ways more effective at recovering viewable artifacts, the question still lingers; are browsers providing better privacy or are the tools used to analyze browsers not able to find certain artifacts. Based on the findings of this research and the previously reviewed studies, no browser appears to be particularly effective at the prevention of artifact recovery.

For law enforcement or investigators involved with conducting digital forensics investigations, the toolset plays a crucial role in the investigation. Based solely on the evidence of this research, two tools were used however one clearly outperformed the other. It came as no surprise that FTK outperformed Autopsy primarily based on the fact that FTK is a commercial software and is well supported by Access Data. Since EnCase could not be used in this research due to the inavailability of a software license, it is not possible to determine whether EnCase would have performed better than FTK however, in cases where a software capable of analyzing the entire file system for browser artifacts is necessary, based on this research, FTK is the most effective option.

For the privacy minded individual in search of a web browser that does not render many browser artifacts recoverable, Firefox used in private browsing mode or Dooble produced the fewest number of recoverable browser artifacts. Based primarily on the findings of this study, browsers based on the Chromium platform produced several viewable, recoverable artifacts as did Microsoft Edge. Factoring those out, Firefox and Dooble were the browsers that provided the best privacy.

Firefox, being a much more supported web browser provided a far more robust user experience, however that is not to say a better browser does not exist. Dooble ultimately produced the fewest number of recoverable browser artifacts however the browser itself was not as well supported. In the process of data population, anomolous errors proved disruptive to the user experience.

This study found that in the case of all six browsers, no artifacts were found for typed URLs, instant messages, or emails. Referring back to the data population process, there were emails sent between the Google gmail and Yahoo webmail accounts. Facebook was used to send and receive instant massages as well. These artifacts are of particular interest as they provide a great deal of information about the intent of the user. Typed URLs could be included in web history, but not all web history entries may be included in the Typed URLs list. What makes the typed URLs so useful is that they show at least in some part, that the user intended to visit a specific web page because they manually searched for it. In criminal cases, this information could reveal intentional requests for web sites with illegal content or information relevent to the case. Along with the typed URLs, the instant messages and emails provide a wealth of knowledge about the user including who they are in contact with and what is being said. Again, this information can be valuable to criminal cases as it contributes to proof of intent. While the exact reason these artifacts could not be found is unknown, potential causes could include the lack of email artifacts since email as a service, including storage, is conducted between email servers at remote locations, not the local machine itself . Therefore, if emails are only viewed but never stored by the browser, it is possible that no email artifact was created (Crocker, 2009). Additional causes as well as limitations of the tools to identify, index, and read these artifacts. Although FTK and Autopsy do have additonal processes that can be turned on during data processing to parse email and chat data, they were not used in this study.

5.1 Limitations

Limitations that placed a heavy burden upon this study were time, availability of software, and knowledge of enhanced privacy browsers. The contraint of time limited this research in scope, including number of browsers analyzed, tools used to conduct analysis, and the depth of analysis. The time required to process each trial was approximately two hours per trial, with 132 trials conducted for a total of 264 hours. As such, the entire file system could not be analyzed for artifacts. Each image file contained in excess of 180,000 viewable files or folders. As such, only the documented locations where artifacts are known to be stored were searched. Future research should expand upon the browsers tested as well as the tools used to conduct analysis.

Perhaps the most influential limitation of this study was the available documentation and research of the enhnaced privacy browsers. As stated in methodology, the three enhanced privacy browsers had vary little to no documentation or documented research, therefore the method of collecting artifact data for them was based on research of similar browsers. As a result, it was possible that additional artifacts did exist but were not found due to the tools or process followed in this study. In the case of Epic and Comodo Dragon, analysis was based on that of Chromium since they all share the Chromium platform. Dooble on the otherhand was more difficult to identify, as the web page for Dooble itself did not even contain technical informatoin. As such, Dooble was initially investigated as if it were Chrome, Firefox, or Edge to identify if it shared a similar file structure to any existing web browsers. Lack of absolute certainty as to the accuracy of what artifact files to search for and where located was cause for speculation of the accuracy of the Dooble browser results. Future research should include preliminary studies of enhanced privacy and less common web browsers to more throroughly understand and identify how and where browser artifactcs are stored.

Availability of forensic software placed an additional limitation on this study. Commerical forensic software such as EnCase and X-Ways Forensics, both

recognized and tested by NIST, as well as Magnet Forensic's Internet Evidence Finder are examples of tools that were well suited for this study (NIST, 2015a). Costs ranging from several hundred to several thousand dollars per license would have required additional funding to purchase license keys to impliment these software packages in this study. As the tools played a vital role in this research, with proper funding, future research should expand the toolset of this study to include some of the tools mentioned above.

5.2 Conclusions

The research work conducted in this study examined two groups of web browsers to investigate and identify recoverable web browser artifacts for the purpose of identifying whether enhanced privacy web browsers provide better privacy, defined by the number of recoverable artifacts as well as content, compared to common web browsers used in private browsing mode. As some error or chance of anomoly were accounted for with respect to tools and methodology, the author concluded that a difference of one artifact was not strong enough evidence to support the claim that enhanced web browsers produce fewer recoverable browser artifacts. With respect to the reserach question posed for this reserach, whether or not enhanced privacy web browsers provide better privacy was based upon whether they produced fewer recoverable browser artifacts, especially artifacts that contained content from previous browsing sessions. Based on the evidence found and analysis conducted, this study did not produce suffiencient evidence to conclude that enhanced privacy browsers do indeed provide better privacy.

In regards to the individual browsers, enough evidence was present to at least suggest individual browsers that provided better privacy than their counterparts. Among the common web browsers, Firefox produced the fewest recoverable artifacts with only 3 artifacts recoverable by both tools. Similarly for the enhanced privacy tools, Dooble performed the best, having only produced 2

recoverable artifacts in FTK and none in Autopsy. Given the choice to use one browser from group for better privacy, those two provided the best privacy. On the opposite end of the spectrum, it was identified that the browsers that were based off of Chromium, those being Chrome, Epic, and Comodo Dragon, produced five or more artifacts in all browser-tool combinations except for one where four were produced. As such, the author concluded that in general, browsers based off the Chromium platform do not provide the best privacy compared to their competitors, even when using private browsing modes.

The research conducted in this work, primarily with respect to the methodology, bares a great deal of important to both the scientific community and practitioner community. Contributions to the scientific community include recognizing a need for more research with respect to less common web browsers that claim to provide better privacy. This work also highlighted a need to test additional tools for analysis to help determine which tools are most effect or if a new tool is needed. Since this methodology was modeled in part after the process law enforcement examiners follow, future research using this methodology should help to bridge the gap between researchers and practitioners. For practitioners, this research progressed in a similar process to provide a step-by-step guide in the case that one of the browsers used in this work is encountered in a real case.

Looking beyond the research question, an evaluation of the effectiveness of the tools used in this research, found that FTK recovered more artifacts in total than Autopsy. While this difference in total number was small, a comparison of recovered artifacts that were viewable by each tool supported that FTK was a much more effective tool recovering 27 viewable artifacts compared to the 12 that Autopsy produced. The others required an additional program for the content to be viewed. This difference in performance lead the author to conclude that FTK was a much more effective tool for conducting forensic investigations of private session browsing.

Future research should expand the list of browsers and tools used to conduct the forensic analysis. With the proper funding, tools like EnCase and Internet

Evidence Finder may prove more effective than FTK at identifying and viewing web browser artifacts. This research methodology could also be applied to different operating systems. With the increasing prevelance of Macintosh computers and Linux distributions in the workplace, this would open the door to several web browsers that are not compatible with Microsoft Windows such as Linux's Iceweasel browser.

LIST OF REFERENCES

LIST OF REFERENCES

AccessData. (2015). *Accessdata's ftk named best computer forensic solution at 2015 sc awards u.s.* Retrieved 2016-1-2, from http://accessdata.com/news/press-releases/accessdatas-ftk-named-best-computer-forensic-solution-at-2015-sc-awards-u.s

Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010). An analysis of private browsing modes in modern browsers. In *Usenix security symposium* (pp. 79–94).

Akbal, E., Gunes, F., & Akbal, A. (2016). Digital forensic analysis of web browser records. *Journal of Software*.

Alexa. (2016). *Top sites in united states.* Retrieved from www.alexa.com/topsites/countries;0/US

Bernal, P. (2014). *Internet privacy rights: Rights to protect autonomy.* Cambridge United Kingdom: Cambridge Univeristy Press.

Comodo. (2016). *Dragon internet browser.* Retrieved 2016-06-12, from www.comodo.com/home/browsers-toolbars/browser.php

Crocker, D. (2009). Internet mail architecture.

Data, A. (2015). *Forensic toolkit(ftk).* Retrieved 2015-12-05, from http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

Dunn, J. (2015). *The best 7 secure browsers 2015.* Retrieved 2015-11-20, from http://www.techworld.com/security/best-7-secure-browsers-2015-3246550/

Epic. (2016). *Epic privacy browser key features.* Retrieved from www.epicbrowser.com/our-key-features.html

Gao, G. (2015). *What americans think about nsa surveillance, national security privacy.* Retrieved 2015-11-29, from http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

Gao, X., Yang, Y., Fu, H., Lindqvist, J., & Wang, Y. (2014). Private browsing: an inquiry on usability and privacy protection. In *Proceedings of the 13th workshop on privacy in the electronic society* (pp. 97–106).

Goodison, S., Davis, R., & Jackson, B. (2015). Digital evidence and the u.s. criminal justice system. *National Criminal Justice Reference Service*.

Gratchoff, J., & Kroon, G. (2015). Project spartan forensics. *Forensic Focus*.

Gritzalis, S. (2004). Enhancing web privacy and anonymity in the digital era. *Information Management & Computer Security*, *12*(3), 255–287.

Gupta, D., & Mehtre, B. (2013). *Recent trends in collection of software forensics artifacts: Issues and challenges.*

Henry, A. (2014). *The best privacy and security-focused web browsers.* Retrieved 2015-11-20, from `http://lifehacker.com/the-best-privacy-and-security-focused-web-browsers-1672758270`

Hoffman, C. (2012). *Htg explains: How private browsing works and why it doesn't offer complete privacy.* Retrieved 2015-10-03, from `http://www.howtogeek.com/117776/htg-explains-how-private-browsing-works-and-why-it-doesnt-offer-complete-privacy/`

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and digital forensics: An introduction.* New York New York: Routledge.

Hope, C. (2016). *Operating system.* Retrieved 2016-01-04, from `http://www.computerhope.com/jargon/o/os.htm`

IC3. (2014). *2014 internet crime report.* Retrieved 2015-09-23, from `http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf`

INTERPOL. (2015). *Cybercrime.* Retrieved 2015-10-4, from `http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime`

ISC. (2015). *What is cyber forensics?* Retrieved 2015-12-06, from `https://www.isc2.org/cyber-forensics.aspx`

Kanellis, P., Kiountouzis, E., Kolokotronis, N., & Martakos, D. (2006). *Digital crime and forensic science in cyberspace.* Hershey Pennsylvania: Idea Group Publishing.

Lugmayr, A., Niiranen, S., & Kalli, S. (2004). *Digital interactive tv and metadata: Future broadcast multimedia.* New York New York: Springer-Verlag New York.

Mahendrakar, A., Irving, J., & Patel, S. (2012). *Forensic analysis of private browsing mode in popular browsers.* Carnegie Mellon University, nd Web.

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).

McQuaid, J. (2014). *Forensic email analysis: browser artifacts you may find on a pc or laptop.* Retrieved 2015-12-05, from `https://www.magnetforensics.com/computer-forensics/forensic-email-analysis-browser-artifacts-you-may-find/`

Microsoft. (2015a). *Comparing ntfs and fat file systems.* Retrieved 2016-01-04, from `http://windows.microsoft.com/en-us/windows-vista/comparing-ntfs-and-fat-file-systems`

Microsoft. (2015b). *Inprivate browsing.* Retrieved 2015-12-02, from http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/in-private

NIST. (2015a). *Computer forensics tool testing handbook* (Tech. Rep.). National Institute of Standards and Tools.

NIST. (2015b). *National institute of standards and technology (nist) computer forensic tool testing (cftt) reports.* Retrieved 2015-12-05, from http://www.dhs.gov/science-and-technology/nist-cftt-reports

Noorulla, E. S. (2014). Web browser private mode forensics analysis.

NW3C. (2009). *Computer crime: Computer as an instrument of crime.* Retrieved 2015-10-02, from https://www.nw3c.org/docs/research/computer-crime-computer-as-an-instrument-of-crime.pdf?sfvrsn=6?

of Justice, N. I. (2004, April). *Forensic examination of digital evidence: A guide for law enforcement* (Tech. Rep.).

Ohana, D., & Shashidhar, N. (2013). Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions. *EURASIP Journal on Information Security*, *2013*(1), 1–13.

Reyes, A., O'Shea, K., Steele, J., Hansen, J. R., Jean, B. R., & Ralph, T. (2007). *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors.* Rockland Massachusetts: Syngress Publising, Inc.

Ritter, N. (2006). Digital evidence: How law enforcement can level the playing field with criminals. *National Institute of Justice Journal*.

Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, *1*(2), 19–38.

Rouse, M. (2014). *Virtual machine definition.* Retrieved 2016-01-03, from http://searchservervirtualization.techtarget.com/definition/virtual-machine

Ruiz, R., Amatte, F. P., Park, B., Kil Jin, & Winter, R. (2015). Overconfidence: Personal behaviors regarding privacy that allows the leakage of information in private browsing mode.

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).

Satvat, K., Forshaw, M., Hao, F., & Toreini, E. (2014). On the privacy of private browsing, a forensic approach. *Journal of Information Security and Applications*, *19*(1), 88–100.

Sheldrake, P. (2011). *The business of influence: Reframing marketing and pr for the digital age.* West Sussex United Kingdom: John Wiley Sons, Ltd.

Smith, M. (2007). *Spam and internet privacy.* New York: Nova Science Publishers, Inc.

Software, G. (2015). *Encase forensic v7.* Retrieved 2015-12-05, from https://www2.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx

StatCounter. (2016). *Top 5 desktop browsers from dec 2014 to dec 2015.* Retrieved 2016-1-4, from http://gs.statcounter.com/#desktop-browser-ww-monthly-201412-201512-bar

Stauffer, T., & McElhearn, K. (2004). *Mastering mac os x.* Alameda California: SYBEX Inc.

Tilborg, H. C. v., & Jajodia, S. (2011). *Encyclopedia of cryptology and security.* London: Springer Science+Business Media, LLC.

Vermaat, M., Sebok, S., Freund, S., Campbell, J., & Frydenberg, M. (2015). *Discovering computers enhanced.* Boston Massachusetts: Cengage Learning.

W3Counter. (2016). *Browser & platform market share.* Retrieved from www.w3counter.com/globalstats.php?year=2015&month=1

Walters, J. (2015). *Third of americans take precaution to protect web presence, pew report finds.* http://www.theguardian.com/world/2015/mar/16/americans-protect-internet-presence-pew-edward-snowden.

Xu, M., Jang, Y., Xing, X., Kim, T., & Lee, W. (2015). Ucognito: Private browsing without tears. In *Proceedings of the 22nd acm sigsac conference on computer and communications security* (pp. 438–449).

Zaharia, A. (2015). *Why are java's vulnerabilities one of the biggest security holes on your computer?* Retrieved 2015-12-02, from https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/