WHATSAPP FORENSICS: LOCATING ARTIFCATS IN WEB AND DESKTOP CLIENTS

by

Nicolás Villacís Vukadinović

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer & Information Technology

West Lafayette, Indiana

May 2019

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Kathryn C. Seigfried-Spellar, Chair

Department of Computer and Information Technology

Dr. Marcus K. Rogers

Department of Computer and Information Technology

Dr. Umit Karabiyik

Department of Computer and Information Technology

Approved by:

Dr. Eric T. Matson

Head of the Graduate Program

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Browser forensics: A subdiscipline of digital forensics concerned with the analysis of artifacts (e.g., cache, history, logs, scripts) left behind web browsers.

Digital evidence: Digital data that support or refute a hypothesis about digital events or the state of digital data.

Digital forensics: "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. (Palmer et al., 2001, p. 16)

Forensic artifact: Objects of interest in digital forensic investigations, such as files, directories, logs, and histories.

Instant messaging forensics: The application of the digital forensic science to applications that allow the instant communications between individuals.

Mobile forensics: A subset of digital forensics which is devoted to small, portable devices that use network communications (i.e., cellular, Wi-Fi) and have digital storage capabilities (Reiber, 2016).

Rooting: Scripts which allow a user to gain super privileges on an Android device (i.e., accessing the root directory). The availability or possibility of rooting a device depends on the device's model and version.

WhatsApp desktop application: The desktop WhatsApp client that can be installed by downloading an executable file from the official website, www.whatsapp.com/download, or through the Microsoft Store for Windows, or Mac App Store for Mac.

WhatsApp web client: The desktop WhatsApp client accessible through supported web browsers by navigating to https://web.whatsapp.com.

LIST OF ABBREVIATIONS

APFS	Apple File System
ANOVA	Analysis of Variance
CPU	Central Processing Unit
FTK	Forensic ToolKit
GB	Gigabyte
GPU	Graphics Processing Unit
IM	Instant Messaging
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
LNK	Link (shortcut) file
MAC	Macintosh
MB	Megabyte
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
OS	Operating System
PC	Personal Computer
PDF	Portable Document Format
QR	Quick Response
RAM	Random Access Memory
SHA1	Secure Hashing Algorithm 1
SMS	Short Message Service
TB	Terabyte
TOR	The Onion Router
WA	WhatsApp
WWW	World Wide Web

ABSTRACT

Author: Villacís Vukadinović, Nicolás. MS
Institution: Purdue University
Degree Received: May 2019
Title: WhatsApp Forensics: Locating Artifacts in Web and Desktop Clients
Committee Chair: Kathryn Seigfried-Spellar

WhatsApp is the most popular instant messaging application worldwide. Since 2016, users can send and receive messages through desktop clients, either through the WhatsApp desktop application or the web client accessible from supported web browsers. The author identified a gap in the literature in terms of WhatsApp forensics for desktop and web clients. The aim of the study was to locate forensic artifacts on WhatsApp clients. These clients included the desktop application on both Windows and Mac operating systems. Chrome and Firefox web clients were also analyzed for the Windows operating system, as well as Chrome and Safari web clients on the Mac operating system. A WhatsApp log file was identified as the main artifact providing information throughout all clients analyzed. Cached profile pictures were also found, as well as history information about visited websites and ran applications.

CHAPTER 1. INTRODUCTION

Chapter one presents the introduction to the current study. This includes the background of the WhatsApp instant messaging application, the scope, and significance outlining why WhatsApp desktop forensics is important in the digital forensics field. One main research questions was proposed, and the assumptions, limitations, and delimitations for the current study are also listed.

1.1 Background

WhatsApp is the most popular instant messaging (IM) application worldwide, with over 1.5 billion monthly active users as of July 2018 in over 180 countries (Statista, 2018). WhatsApp allows individuals to communicate with others in real time through either text, audio, or video calls. WhatsApp also allows individuals to send voice notes, photos, videos, location information, and documents of any type up to 100 MB in size, all through end-to-end encryption (WhatsApp, n.d.). WhatsApp was first released in 2009 with the intention to be an alternative for the traditional short message service (SMS; WhatsApp, 2016). As of 2016, WhatsApp stopped charging one-time and subscription fees, effectively making the application free for users around the world (WhatsApp, 2016). Over time, the capabilities of WhatsApp have increased and thus the relevance to police investigations. In January 2015, the WhatsApp web client was introduced for all major desktop browsers, and the WhatsApp desktop application for both Windows and Mac was introduced in May 2016 (WhatsApp, 2015; 2016). To use the WhatsApp web client, a user can simply navigate to https://web.whatsapp.com on any of the supported browsers on a desktop. Next, the user would scan a quick response (QR) code within the WhatsApp application on a smartphone to start sending and receiving messages. Supported web browsers include Google Chrome, Mozilla Firefox, Opera, Microsoft Edge, and Safari. For the desktop application, a user will download the client from https://www.whatsapp.com/download, install the application and scan a QR code similar to the web browser client, as seen in Figure 1. Both options are only an extension of a mobile device and only mirror what is being sent and received on the device. This means if the device is disconnected from a network then no messages can be sent or received on the desktop clients for any platform.

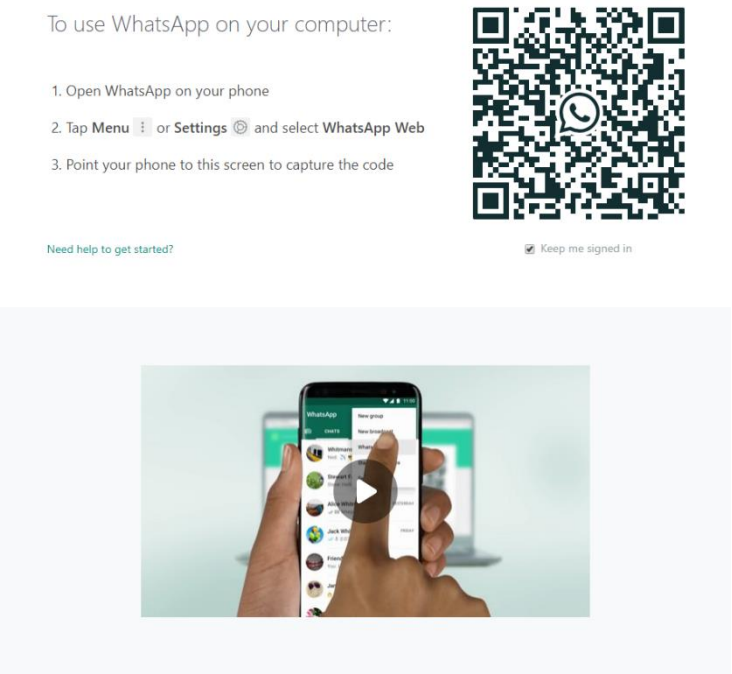

Figure 1. *Setup screen for the WhatsApp desktop and web browser clients (Web.WhatsApp.com, 2018).*

The current study had the main goal of locating forensic artifacts left behind the WhatsApp desktop application and web client for both Windows and Macintosh (Mac) operating systems (OS). It combined different areas of digital forensics, such as browser forensics, mobile forensics, and instant messaging forensics, to locate artifacts of interest on both desktop OS.

1.2 Scope

The current study was limited to the WhatsApp IM application, which can be installed on Android 4.0+, iOS 8+, and Windows Phone 8.1. For the desktop clients, research was conducted on two OS, Windows 10 and Mac OS Mojave 10.14.3 For Windows, Google Chrome and Mozilla Firefox were used for the WhatsApp web client and Google Chrome and Safari for the Mac OS WhatsApp web client. The WhatsApp desktop application on both OS was also used. These web browsers were chosen based on their popularity. For the Windows OS, the most popular browsers are Chrome, Internet Explorer, and Firefox, with 64%, 13%, and 10% of the market share, respectively (Statcounter, n.d.). Internet Explorer was not considered in

this study as the WhatsApp web client is not supported on this browser. On Mac, Chrome and Safari are the most popular browsers, with 51% and 40% of the market share, respectively (Statcounter, n.d.).

1.3 Significance

The findings of the current study will aid law enforcement in determining whether and if any forensic artifacts can be recovered from WhatsApp on a desktop environment. Examining conversations is important in digital forensic investigations since they might give an investigator important clues as to what happened or is about to happen. WhatsApp is the most popular application for communicating worldwide (Statista, 2018), and a suspect might have been using the application to communicate on their mobile device. According to Reiber (2016), every day the media reports criminal cases where a mobile device was involved, or how a criminal case was solved using evidence from a mobile device. However, sometimes acquiring data from a suspect's mobile device might not be possible due to a number of reasons, such as encryption on the device, a reset of all content and data on the device or even a physical destruction of the device. The popularity and privacy features (e.g., end-to-end encryption) WhatsApp offers can be exploited by criminals who might want to use the application. In fact, there have already been cases that have caused controversy as WhatsApp is not able to provide law enforcement with certain artifacts during a criminal investigation due to messages on its servers being encrypted. Notorious cases include the London Bridge attack, where the attacker last communicated through WhatsApp just minutes before the attack (Rayner, 2017). On another case, a judge in Brazil ordered to suspend WhatsApp services nationwide for up to 72 hours since the company was not able to provide information on an organized crime and drug-trafficking investigation (Sreeharsha, 2016).

If having a mobile device as a source of evidence is not feasible, investigators could analyze a suspect's desktop where either the WhatsApp web client or desktop application might have been used. The current study aimed at investigating whether any forensic artifacts on WhatsApp can be recovered from a desktop client. Since forensic artifacts were recovered, the study also produced a process for investigators to locate such artifacts.

1.4 Research Questions

The main goal of the proposed research was to answer the following question:

1. What artifacts can be forensically recovered when using WhatsApp on web and desktop clients?

Specifically, this question was answered with the following goals:

- To assess if the type of operating system (i.e., Windows and Mac) has an impact on what can be recovered when using the WhatsApp desktop client.
- To assess if the type of web browser used (i.e., Chrome, Firefox, Safari) has an impact on what can be recovered when using the WhatsApp web client.
- To assess if the type of forensic acquisition tool used (i.e., FTK, AXIOM, Autopsy) has an impact on what can be recovered when using the WhatsApp desktop applications and web clients.

1.5 Assumptions

The assumptions for this study included:

- An individual has used or installed either the WhatsApp web client or desktop application on either operating systems, and used these clients to send communications (i.e., IM, media, voice notes).
- The operating system for Windows 10 Version 1809 Build 17763.292 with the New Technology File System (NTFS), and Mac Mojave 10.14.3 with the Apple File System (APFS) did not change throughout the study.
- There was full access to an operating system and there was no encryption on the operating system.
- Server-side configurations of WhatsApp remained the same. In other words, the mechanism of the WhatsApp web clients and desktop applications communicating with the smartphone (i.e., the mirroring of the mobile device application) and finally to the server remained the same.
- As the web clients and the desktop application are merely mirroring a mobile device, only one WhatsApp account on a single mobile device was used to begin communications.

1.6 Limitations

The limitations for this study included:

- To use the WhatsApp application, a user needs to have a mobile phone number to authenticate and start using the application.
- The current study was restricted to using a mobile device with the WhatsApp application installed. This is due to how the WhatsApp web clients and desktop applications function, as it is merely a mirror of what is taking place on the mobile device.
- An active internet connection was required on the mobile device and desktop for the associated web and desktop WhatsApp clients to function.
- The current study was limited to analyzing WhatsApp clients on Windows 10 Version 1809 Build 17763.292 using the NTFS and Mac Mojave 10.14.3 which used the APFS. These were the latest versions and file systems at the time of research.

1.7 Delimitations

The delimitations for this study include:

- The current study will only focus on two operating systems: Windows 10 and Mac Mojave 10.14.3. All other operating systems will not be considered for analysis and comparison.
- The current study only focused on two browsers on each operating system: Chrome and Firefox for Windows, and Chrome and Safari for Mac. All other browsers for Windows and Mac were not considered for analysis and comparison.
- The mobile WhatsApp applications were installed on a Google Pixel XL and Samsung Galaxy S8, running Android version 9 and 8, respectively. Other mobile device operating systems and manufacturers were not considered.
- All software versions, including the desktop OS, web browsers, WhatsApp smartphone application, WhatsApp web, and desktop client versions remained static throughout the study. Automatic updates were disabled.
- Notifications for the web and desktop WhatsApp clients were not enabled.

- Random access memory or live forensics were not considered on either OS as it is not the primary focus during the forensic analysis. Live forensics, however, can be considered for a *post hoc* analysis or future research.
- Data carving was not performed during the forensic analysis.

1.8 Summary

Chapter one provided the background of the instant messaging application WhatsApp, the scope, and significance detailing why WhatsApp desktop forensics is important in the field. WhatsApp is a free, instant messaging application for smartphones, with the most monthly active users worldwide (Statista, 2018), compared to other instant messaging applications. WhatsApp can be used on a desktop as either a desktop application or through a web browser. The discovery of any forensic artifacts on desktop and web clients can be of utmost importance to digital forensic examiners during investigations where WhatsApp was used by a suspect. The current study included one main research question with three goals; (1) to determine the differences in recoverable artifacts between the desktop client on both OS (Windows v. Mac), (2) to determine differences in recoverable artifacts between the web clients (Chrome, Firefox, and Safari), and (3) to determine the differences in recovered artifacts with the forensic tools used (FTK, AXIOM, Autopsy). The assumptions, limitations, and delimitations for the current research study have also been listed.

CHAPTER 2. REVIEW OF RELEVANT LITERATURE

To understand the landscape of the literature and the appropriate methodology for this study, it was necessary to examine research from the following bodies of literature: Digital forensics, mobile forensics, browser forensics, instant messaging forensics, and WhatsApp forensics.

2.1 Digital forensics

Digital forensics has been described by Palmer et al. (2001) as:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (p. 16).

Digital forensics is a subdiscipline of the forensic sciences that is ever-evolving and complex as it needs to adapt to the constant changes of technologies in the market. Compared to other forensics sciences, digital forensics is relatively new. For example, toxicology forensics was established in the 1800's (Levine, 2003) and fingerprint forensics in the 1890's (Tilstone, Savage, & Clark, 2006). According to Pollitt (2010), digital forensics dates back to the 1980's with the emergence of International Business Machine's (IBM) personal computer (PC), which resulted in a rapid adoption of computers by hobbyists. Over the next nearly four decades, computers and digital forensics continued to advance. For example, Ryan and Lewis (2017) reported a steady increase on household computer and internet use in the United States from 1984 through 2015. As a result of the improvement in technologies, computers have become an integral part of court cases (Casey, 2011).

Within the digital forensics field, there are multiple digital forensic process models for investigations (Beebe & Clark, 2005; Carrier, Spafford et al., 2003; McKemmish, 1999; Mocas, 2004). A general digital forensics model was proposed by Rigby and Rogers (2007), which consists of seven different phases: (1) Preparation, (2) identification, (3) preservation, (4) collection, (5) examination, (6) analysis, and (7) presentation phase. The preparation phase involves any preparatory measures, such as education, training, and all necessary equipment, to be ready before approaching a crime scene. Identification entails recognizing every single source of digital evidence at a crime scene. Preservation ensures the identified sources of evidence are disconnected from outside communications, so no manipulation of data takes place and a chain of custody is created. The collection phase involves making an exact copy of the contents of a digital source of evidence. The examination and analysis phases are the two main phases of the investigation process as the significance of the evidence and any conclusions based on the evidence will be drown. Finally, the presentation phase will summarize findings so these can be made available in a court of law (Rigby and Rogers, 2007). Using a process model aids law enforcement, investigators, and digital forensic examiners in understanding the principles and processes involved with the field.

Digital forensics aids law enforcement in solving crimes committed with computers as a tool (e.g., cyberbullying, phishing attacks), as a target (e.g., unauthorized access to a system) or as incidental to an illegal activity (e.g., extortion, homicide) (Bossler, Holt, & Seigfried-Spellar, 2017). Artifacts, objects of interest in digital forensic investigations (e.g., files, directories, logs, histories), can be extracted from digital devices and be presented in a court of law as digital evidence (Casey, 2009). Carrier and Spafford (2004) defined digital evidence, referring to an incident, as "digital data that contain reliable information that supports or refutes a hypothesis about the incident" (p. 3). Digital evidence can aid law enforcement in showing an individual's innocence or guilt in a court of law. For example, in *Paul Ceglia v. Mark Zuckerberg*, forensic analysis of Ceglia's hard drive from 2004 showed he forged a contract which he was trying to use against Zuckerberg to claim 50% share ownership of Facebook (Ceglia v. Zuckerberg, 2012). The court ultimately dismissed Ceglia's claim and is now charged for trying to defraud Zuckerberg, although Ceglia

remains a fugitive and has fled to Ecuador (Stempel, 2018). Most cases that go to trial include digital evidence in one way or the other, according to professionals in the digital forensics field such as researchers, attorneys, and law enforcement, among others (Casey, 2011). For instance, after the death of a popular Miami art dealer, Clifford Lambert, investigators were able to see how Lambert's assets were being transferred between suspects. A text message on a suspect's device also revealed an order to kill Lambert (DigitalStrata, 2017). As technologies advances, the sources of digital evidence will also grow. For instance, court cases in recent times have seen smart watches (Boxall, 2018), and personal home assistants (McLaughlin, 2017), just to name a few examples.

2.2 Mobile forensics

Mobile forensics is a subset of digital forensics which is devoted to small, portable devices that use network communications (i.e., cellular, Wi-Fi) and have digital storage capabilities (Reiber, 2016). Examples include devices such as phones, smartphones, tablets, and smart wearables like watches. Evidence recovery should be completed using forensically approved and accepted methodologies (Jansen & Ayers, 2007).

Similar to digital forensics, mobile forensics also follows a process which includes four steps: (1) Seizure, (2) collection, (3) analysis/examination, and (4) presentation (Reiber, 2016). Similar to the digital forensics frameworks, the seizure phase ensures the identified sources of evidence are disconnected from outside communications (e.g., mobile device put into airplane mode), so no manipulation of data takes place. The collection phase involves making an exact copy of the contents of the mobile device. The analysis and examination phases will process significant forensic artifacts and draw conclusions based on the evidence found. The presentation phase will summarize findings so these can be made available in a court of law. Saxena (2009) also detail a forensic process model that should be followed with mobile devices, which includes the same steps as those proposed by Reiber (2016).

Analyzing mobile devices is different than analyzing a computer. With a mobile device, a forensic examiner must be able to communicate with the device first before any digital evidence is extracted (Reiber, 2016). Unlike computer forensics where a write

blocker can be used on a hard drive, mobile forensics manipulates data on the target device. However, forensic software tools and processes guarantee a forensically sound extraction of data which can later be presented in a court of law (Reiber, 2016).

If digital forensics is a relatively new field, mobile forensics is even more recent as the first smartphone surfaced in 2007 with the launch of Apple's first iPhone (Pothitos, 2016). The iPhone was the first smartphone geared towards the general consumer rather than a businessman, which changed the industry and paved the path for a new target market (McCarty, 2011). According to Statcounter (2018), as of August 2018, mobile devices, including smartphones and tablets, share close to 56% of the market share worldwide, dominating the market since October 2016 when mobile device internet usage first surpassed desktop internet usage. In less than a decade, mobile devices were able take a larger market share than desktop computers, a technology that has existed for close to 40 years (Ryan & Lewis, 2017). The rapid growth in mobile device use, which has surpassed desktop computers, illustrates the importance to develop mobile forensic standards and procedures for the industry.

With each year, the computer processing power, graphical processing power, memory size, power efficiency, and overall functionality of smartphones improves, opening the possibilities of more activities and processes to take place on these devices. At the same time, cybercrime is taking place on smartphones either as a target, tool, or incidental, and it continues to increase (Goel, Tyagi, & Agarwal, 2012). These devices are not limited to only cybercrime, but also civil and criminal law cases. A well-known example of a smartphone being the central point of an investigation is the San Bernardino shooter's password-protected iPhone the FBI managed to finally access after months of investigations (Zapotosky, 2016). Mobile devices, specifically smartphones, act as small computers for users and are both portable and practical due to their small size and low costs. Smartphones hold a wealth of information, including an individual's e-mails, daily calendar, social media accounts, call log, messages, browsing history, and more. Mobile device use in the United States has seen a constant increase in the last decade and the trend will be maintained for the next four year (Statista, 2017). With a wealth of information on

smartphones, coupled with the vast amount of users, mobile forensics is an important area within the digital forensic community that remains the focus of attention as it can greatly aid law enforcement.

2.3 Browser forensics

Similar to mobile forensics, browser forensics is a subdiscipline within digital forensics. A web browser is a software program that allows an individual to locate, access, and display web pages found on the world wide web (WWW; Techopedia, n.d.). Web browsers can be used on both desktop computers and mobile devices. Popular web browsers include Chrome, Mozilla Firefox, Internet Explorer (IE), Safari, and Edge (Statcounter, n.d.). Web browsers allow an individual to access the world wide web, for the search of literature, entertainment, news, education, and more. The access to vast sources of information online provides crucial artifacts which might reside on a desktop after an individual navigates the internet through a web browser. Artifacts left behind a web browser (e.g., cache, history logs, cookies) are important and can aid law enforcement in court cases after a thorough investigation. For example, in the case of "suitcase" killer Melanie McGuire, part of the evidence used by prosecutors to accuse her of murder were internet searches made by her related to deathly poisons, gun laws and murder, ten days before she murdered her husband (Nozicka, 2017).

Browser forensics poses a challenge to digital forensic examiners. For example, an investigator might come across multiple browser instances on a single desktop, which might store information in different ways (i.e., databases, logs, scripts) and leave artifacts in different locations. This is further complicated by different browser versions that might exist within a single browser (i.e., Internet Explorer 9 vs. 10), or even non-standard browsers that offer full anonymity, such as The Onion Router (Tor; Dean, n.d.).

The recommended browser forensics process model is to first identify all the browsers being used in a desktop, then locate the artifacts on default directories, which will depend on the browser model and version, and finally analyze all the artifacts (Dean, n.d.). On the

Windows OS, an examiner can determine what browsers are being used by looking at the Windows Prefetch files, located in the 'C:\Windows\Prefetch' directory (Dean, n.d.).

Past research has focused on Chrome, Firefox, and Safari for both operating systems, Windows and Mac. Existing literature has identified directories and files of interest (i.e., history, downloads, cookies, cache) where artifacts from a user's activity with the web browser are stored. Table 2.1 summarizes the paths for artifacts of interest (Akbal, Günes, & Akbal, 2016; Dean, n.d.; Rathod, 2017; Yudha, Luthfi, & Prayudi, 2017).

Table 2.1 *Web browser artifact location by browser client and OS*

Web Browser	Operating System	File/Path
Chrome	Windows Vista through 10	C:\user\{USERNAME}\AppData\Local\Google\Chrome\User Data\Default
	MacOS X	/Users/{USERNAME}/Library/Application Support/Google/Chrome/Default
Firefox	Windows Vista through 10	C:\Users\{USERNAME}\AppData\Roaming\Mozilla\Firefox\Profiles\{PROFILE}.default\places.sqlite C:\Users\{USERNAME}\AppData\Local\Mozilla\Firefox\Profiles\{PROFILE}.default\cache2\
Safari	MacOS X	/Users/{USERNAME}/Library/Safari/ /Users/{USERNAME}/Library/Caches/com.apple.Safari/

When analyzing web browser artifacts, it is important to understand the time format used throughout different files and browser versions. The goal is to get an accurate understanding of when the events took place. Table 2 summarizes the different time formats used by web browsers (Akbal et al., 2016).

Table 2.2 *Time formats used by different web browsers*

Web Browser	Time Format
Chrome	WEBKIT Time: microsecond (10-6) Since January 1, 1601 00:00:00 (UTC)
Firefox	PR Time: microsecond (10-6) Since January 1, 1970 00:00:00 (UTC)
Safari	CF Absolute Time: second Since January 1, 2001 00:00:00 (UTC)

There are several forensic tools that can analyze web browser artifacts. These are either open-source or commercial tools that will analyze the files and directories mentioned in Table 1 and parse any relevant information. Open source tools include The Sleuth Kit's Autopsy, WEFA, Nirsoft tools, browser history viewer, browser forensic tool, and McAfee's Pasco. Commercial tools include AccessData's Forensic Toolkit (FTK), Guidance Software's Encase, BlackBag's BlackLight, Magnet's AXIOM, Digital Detective's NetAnalysis, and Foxton Forensics' Browser History Examiner (Akbal et al., 2016; Dean, n.d.; Oh, Lee, & Lee, 2011).

2.4 Instant messaging forensics

Instant messaging is a form of communication that gained popularity in 1996 with the surface of the ICQ, or 'I Seek You' service (Boneva, Quinn, Kraut, Kiesler, & Shklovski, 2006). Instant messaging allows individuals to have private conversations with others through the internet in real time (Boneva, et al., 2006). Instant messaging popularity has transitioned from desktop-based applications (i.e., ICQ, Windows Live Messenger, Yahoo! Messenger) to smartphone-based applications (i.e., WhatsApp, Viber, Kik, WeChat, QQ). Instant messaging has also transitioned from only focusing on text conversations between individuals, to the exchange of media (i.e., photos, videos, documents), location, audio, and video calls/conference. Instant messaging has become so popular that even organizations, businesses, and government agencies are using this method of communication to reach individuals. Examples include WhatsApp's business chat and the Twitter accounts government officials use throughout the world. Nevertheless, conversations are critical artifacts a forensic investigator should look at when analyzing a device.

Instant messaging forensic research has been performed in the past, and it has primarily focused on popular applications on Android and iOS mobile operating systems. For example, Gao and Zhang (2013) conducted an exploratory study to look for any artifacts left behind by the third most popular IM application worldwide, WeChat, on iOS (Statista, 2018). Gao and Zhang (2013) found audio data, conversation databases, user profile information,

photos, and videos. Gao and Zhang (2013) hoped to encourage others in the field to further research on these applications, with the goal of the development of IM forensic tools that can aid law enforcement when conducting investigations.

Another IM application that has been the subject of forensic research is Kik. Kik is an application with over 300 million users as of 2016, and over 40% of its United States users being under 24 years of age (Statista, 2015, 2016). Ovens and Morison (2016) analyzed the forensic artifacts left by the Kik application on iOS. Ovens and Morison (2016) documented artifacts of interest and their directory locations, such as conversations, attachments, device states (e.g., offline, online, blocked, deleted), profile pictures, and contacts' information. Similar to Gao and Zhang (2013), the authors conclude their research with the hopes of others in the field using these discoveries to create forensics tools that will assist law enforcement in their investigations.

Sgaras, Kechadi, and Le-Khac (2015) conducted a forensic acquisition and analysis of WhatsApp, Viber, Skype, and Tango on both Android and iOS. Sgaras et al. (2015) were looking for four main sources of data, (1) traffic, (2) content, (3) user profile, and (4) contact database data. After conducting their research in controlled environments, a comparative analysis shows more information could be extracted from iOS than Android for the same applications. Stirparo (2016) investigated general iOS forensics information as well as three IM applications popular for their security features and characteristics. These included Telegram, Signal, and WhatsApp. Stirparo's (2016) research on WhatsApp corroborates Sgaras' and colleagues' (2015) findings on the application, particularly about the *ChatStorage* SQLite database that stores all the conversations, unencrypted, of the WhatsApp application on iOS.

In a recent study, Rathi, Karabiyik, Aderibigbe, and Chi (2018) published research on forensic artifacts left behind in WeChat, Telegram, Viber, and WhatsApp on Android smartphones. Rathi and colleagues (2018) looked at these popular IM applications, which encrypt a user's chat database files locally on the device, with the goal of studying and analyzing extraction methods for these databases. Rathi and colleagues (2018) were able to retrieve encrypted databases from WeChat on a rooted Android device and later decrypt

these using one of two methods presented. Rooting an Android device consists of running scripts which allow a user to gain super privileges on the device (i.e., accessing the root directory). However, this might not always be feasible depending on the device model and version. The WhatsApp message database can be retrieved from an unrooted device following a forensic process method presented by Rathi et al. (2018). The authors were not able to retrieve Viber chat databases from an unrooted Android device, however, they were able to retrieve a user's media (e.g., sent/received images and videos). Telegram proved to be the most secure application in the study as certain databases, excluding the chat database, were recovered only on a rooted device (Rathi et al., 2018).

2.5 WhatsApp forensics

The most popular IM application worldwide is WhatsApp, with one billion daily active users, 1.3 billion monthly active users, and 55 billion messages sent per day as of July 2017 (WhatsApp, 2017). As of July 2018, Statista places WhatsApp as the most popular instant messaging application worldwide with 1.5 billion monthly active users, followed by Facebook Messenger and WeChat with 1.3 billion and 1.04 billion monthly active users, respectively (Statista, 2018).

The purpose of the current study was to analyze the forensic artifacts left behind by the WhatsApp desktop client on both Windows and Mac, as well as the web WhatsApp client on both of these platforms. The literature has not extensively focused on these desktop clients. There has only been two papers published on web WhatsApp forensics, and none on the WhatsApp desktop application. Yudha et al. (2017) published a paper where they propose a model for investigating the web WhatsApp application. Yudha and colleagues (2017) did not specify which OS was used in the model. Yudha's et al. (2017) main goal was to create a forensic process model but did not explain in great detail what data, files, or databases, if any, can be recovered. Yudha and colleagues (2017) do mention they analyzed a log file created by the Chrome browser and that it saves two WhatsApp tokens, WAToken1 and WAToken2, which could potentially be used to tie a specific WhatsApp session to a user. Yudha et al. (2017) also mentioned WhatsApp web does not

create any cookie information when accessed from a Chrome browser. It can be inferred the authors were conducting their research on a Windows environment, based on a table where they explain their research methodology, although there is no reference as to what version of Windows this might be, or what WhatsApp web client version was used. Yudha and colleagues (2017) proposed a forensic process model composed of three stages: (1) Acquisition, (2) analysis, and (3) result. The acquisition stage identifies the suspected web browser on which the web WhatsApp client was accessed and the OS. Next, the analysis phase breaks into log forensics and network forensics. Log forensics investigates all the data created by the web browser in question (i.e., logs, cache, history), while network forensics investigates the traffic generated by the web WhatsApp client. Finally, the result phase gathers and compares all artifacts found on the mobile device with the information gathered from the desktop.

Due to the proposed forensic process model and the research missing crucial information (e.g., OS under investigation, version information, recovered artifacts), the current author decided not to use this process model for the study. The current author also believes there is an important gap in the field that needs to be addressed, specifically in terms of the web WhatsApp client and the desktop application running on both Windows and Mac OS, to determine whether there are recoverable forensic artifacts.

Most recently, Actoriano and Riadi (2018) published their study on the forensic investigation of WhatsApp on an Android device and for the WhatsApp web client. Actoriano and Riadi (2018) focused their research mostly on the smartphone client. The authors applied the Integrated Digital Forensics Investigation Framework (IDFIF) Version 2 model to conduct a forensic investigation of the WhatsApp application. After the application of this framework, Actoriano and Riadi (2018) found forensic artifacts previously reported by other researchers (Rathi et al., 2018; Sagras et al., 2015; Stirparo, 2016), such as the message database files and how to decrypt these files. On a desktop with Windows OS 8.1 and the Google Chrome web browser, Actoriano and Riadi (2018) found how many times a user has visited the https://web.whatsapp.com site and last visited time/date by looking at the history database file located in C:\Users\Adm\AppData\Local

\Google\Chrome\User\Data\Default. The authors also found several network capture files in Chrome's cache, however, these files provided no information as they are encrypted and the encryption key is not found within the desktop (Actoriano & Riadi, 2018).

Although no other research has been published on the web WhatsApp client or desktop application, there is literature for the WeChat desktop application. Chu, Wang, and Deng (2016) investigated the metadata of forensics artifacts of WeChat on Windows 7. Chu and colleagues (2016) set up four different scenarios for their research methodology where WeChat was used. All scenarios consisted of a random access memory (RAM) acquisition of the desktop. The first scenario was performed while the user was still logged in to the WeChat session. This yielded the most evidence, including a user's phone number, e-mail, sent and received messages, amongst others (Chut et al., 2016). The second scenario was similar, but the RAM acquisition was performed after the user had logged out of the session (Chut et al., 2016). This scenario provided the same artifacts, except for sent and received messages. The third scenario consisted of an acquisition after logging out of the WeChat client, only providing the user ID, phone number, and e-mail (Chut et al., 2016). The fourth scenario consisted of an acquisition after the desktop was rebooted, which resulted in no artifacts found (Chut et al., 2016). The current author believes a RAM acquisition is not a feasible option in most real-life scenarios due to several reasons (e.g., no password provided to unlock the suspect's desktop, limited RAM on the suspect device, device powered off, unprepared first responders), therefore the research methodology proposed by Chut et al. (2016) was not followed.

2.6 Summary

This chapter provided a review of the literature relevant to the fields of digital forensics, mobile forensics, browser forensics, instant messaging forensics, and WhatsApp forensics. The identified literature revealed a body of knowledge for different instant messaging applications, including WhatsApp forensics. For WhatsApp forensics, research has mostly concentrated on mobile devices and not the WhatsApp web client or desktop application. There are no studies on the WhatsApp desktop application and there have only been two studies published on WhatsApp web forensics. These studies have only looked at the Google Chrome browser on Windows and

have only found one relevant forensic artifact; the history file (i.e., a counter of how many times the WhatsApp website has been visited, as well as the last visit time/date). There is a gap in the field that was addressed with the current research.

The next chapter outlines the methodology for the current research, which examines the WhatsApp desktop application and four web clients on two operating systems (Windows and Mac), using three different forensic tools (FTK, AXIOM, Autopsy). In addition, the next chapter provides a flowchart for the methodology and details all specifications for virtual environments and data population.

CHAPTER 3. METHODOLOGY

Chapter three provides the methodology that was used in the research study. As demonstrated in the literature review, WhatsApp is a popular mobile application with a continuous growth in capabilities and users. With the recent addition of the web client and desktop application to WhatsApp, there is a gap in the literature. More specifically, to date, only two research studies have investigated WhatsApp in a desktop environment. It is important to further research in the field and find which artifacts, if any, are present on desktop clients when using WhatsApp. The current chapter outlines the procedures and methods of the research study.

3.1 Research Question and Hypotheses

The main goal of the proposed research was to answer the following question:

1. What artifacts can be forensically recovered when using WhatsApp on web and desktop clients?

Specifically, this question was answered with the following goals:

- To assess if the type of operating system (i.e., Windows and Mac) has an impact on what can be recovered when using the WhatsApp desktop client.
- To assess if the type of web browser used (i.e., Chrome, Firefox, Safari) has an impact on what can be recovered when using the WhatsApp web client.
- To assess if the type of forensic acquisition tool used (i.e., FTK, AXIOM, Autopsy) has an impact on what can be recovered when using WhatsApp desktop applications and web clients.

There are three hypotheses that were tested, based on each aim:

- H_1: The same number of artifacts will be recovered for the WhatsApp desktop application on both operating systems.
- H_2: The same number of artifacts will be recovered across all WhatsApp web clients.
- H_3: The same number of artifacts will be recovered when using FTK, AXIOM, and Autopsy.

3.2 Operational Definitions

A recoverable artifact is any item of interest recovered from the forensic analysis of both the WhatsApp desktop application and the web clients on each OS. Specifically, there were a total of 16 types of recoverable artifacts, which are:

- 27 text messages: 20 sent, seven received
- Three deleted messages: two sent, one received
- Five pictures: three sent, two received
- Two videos: one sent, one received
- One sent PDF file
- One photo taken with the desktop's camera
- One voice message recorded with the desktop's microphone
- An individual chat conversation
- A group chat conversation
- A sent contact's information
- Log of modification to the WhatsApp account's settings (i.e., display name, photo, about)
- Log of viewing a status
- Log of viewing a conversation's media
- Log of blocking a contact
- Log of client being used (i.e., last access date/time, how many times)
- Log of mobile device information (e.g., device make, model, IMEI, IMSI)

3.3 Research Design

3.3.1 Research Environments

To search for WhatsApp web and desktop artifacts, multiple virtual environments were set up. The best approach was to do a virtualization of the multiple operating systems, as recommended by Ali and Meghanathan (2011). Virtualization offers several advantages, such as a more efficient use of resources and less overhead investment to carry out a configuration of multiple OS environments. VMware Workstation 14 Pro, installed on a Windows host workstation, was used as the virtualization client. For Mac OS, the virtualization client VMware Fusion version 11.0.2 (10952296) was used on an iMac workstation. A total of six environments

were set up; three for Windows and three for Mac OS. For the WhatsApp account population, two accounts were set up specifically for the purpose of the research. Updates for all software, including the operating system, web browsers, and applications, were disabled once the environments were set up. Disabling updates was set so no modifications to software versions took place, potentially controlling for confounding variables. The hardware and software specifications are discussed next.

3.3.2 Hardware and Software Specifications

3.3.2.1 Windows Host Workstation

The physical host workstation for the Windows environments was a Dell OptiPlex 7060 MFF with the following specifications:

- CPU: An Intel Core i7-8700 CPU (6 cores/12MB/12T) @ 3.20 GHz up to 4.6 GHz
- RAM: Two 8GB 2666 MHz DDR4 SO-DIMM; 16 GB RAM
- Hard drive: M.2 512 GB PCIe NVMe Class 40 solid state drive
- GPU: Intel UHD Graphics 630
- OS: Windows 10 Education Version 1809, build 17763.292

3.3.2.2 Mac Host Workstation

The physical host workstation for the Mac environments was a late 2015 iMac with the following specifications:

- CPU: 3.3 GHz Intel Core i7
- RAM: Two 8GB 1867 MHz DDR3; 16 GB RAM
- Hard drive: 1 TB
- GPU: Intel Iris Pro 6200 1536 MB
- OS: Mac X 10.14.3 Mojave

3.3.2.3 Mobile Client

The mobile device used for the WhatsApp account was a Google Pixel XL 5.5” screen with 32 GB of internal storage data. This mobile device was running Android version 9 (Pie). The WhatsApp client had version 2.19.17. A separate WhatsApp account was also used to be the

other party of the conversation. This WhatsApp account ran on a Samsung Galaxy S8 with 64 GB of internal storage data, Android version 8 (Oreo), and WhatsApp version 2.19.17.

3.3.2.4 Windows Virtual Environment

There were three different virtualization environments for the Windows operating system. All virtual machines had their entire disk space, 40 GB, allocated from the beginning. All three included Windows 10 Education version 1809, build 17763.292:

- First virtualization: The only software installed, besides the default Windows 10 software, was the WhatsApp desktop application, version 0.3.1847, which can be downloaded from the official WhatsApp website or the Microsoft Store.
- Second virtualization: The only software installed, besides the default Windows software, was the Google Chrome browser, version 72.0.3626.81.
- Third virtualization: The only software installed, besides the default Windows software, was the Mozilla Firefox browser, version 65.0.

3.3.2.5 Mac Virtual Environment

There were three different virtualization environments for the Mac Mojave operating system. All virtual machines had their entire disk space, 40 GB, allocated from the beginning. All three had Mac OS 10.14.3 Mojave:

- First virtualization: The only software installed, besides the default Mac Mojave software, was the WhatsApp desktop application, version 0.3.1847, which can be downloaded from the official WhatsApp website or the Mac App Store.
- Second virtualization: The only software installed, besides the default Mac Mojave software, was the Google Chrome browser, version 72.0.3626.81.
- Third virtualization: The only software installed was the default Mac Mojave software, which included the Safari browser, version 12.0.3 (14606.4.5).

3.3.3 Population of Data

To acquire data and conduct any analysis, first a population of data had to take place. This was accomplished following recommendations from the National Institute of Standards and Technology (NIST) on mobile device data population setup. This guide outlines various types of

data that can be populated when setting up a mobile device for digital forensic tool testing purposes (NIST, 2016). Amongst their recommendations, those applicable to the current study were sending/receiving text messages in both individual and group chats and populating a contact's information with multiple fields (i.e., first, middle, and last name, phone number, address, email, date of birth, notes, and a contact picture). Media, including photos, videos, and files, were also sent and received during data population (NIST, 2016). All media files were hashed and recorded before they were sent or used. Hash logging was performed with the intention of comparing the original media files with the files sent through WhatsApp servers. Data population was accomplished by using the desktop WhatsApp clients in the different environments following a scenario. This scenario was adapted and modified from a fictitious story developed by CrimeScene.com (Crime Scene, n.d.). CrimeScene.com is a website that shares fictional crime stories that individuals can solve at their leisure. In this story, the victim received 24 harassing text messages a month before the victim was found dead. The original text messages taken from CrimeScene.com are available in Appendix A, and the modified scenario in Appendix B. This modified scenario includes a detailed timeline of when all interactions within the WhatsApp desktop clients took place. Overall, the following was accomplished:

- Creating a new group chat and individual chat.
- Sending text conversations to different chats. This was done individually to a single contact and to the same contact on a group chat.
- Sending media to different chats. Media included photos, videos, a Portable Document Format (PDF) file, and a contacts' information. A photo and a voice message were also taken with the desktop's camera and microphone.
- Modifying the WhatsApp account's settings, including display name, display photo, and about information.
- Viewing a status and conversations' media (i.e., photos and videos).
- Deleting specific messages within chats for just the sender and for both parties (can only be done up to one hour, eight minutes, and 16 seconds after the message has been sent; Sharma, 2018).
- Blocking a contact

All media items used during the population of data, found on Appendix B, were hashed. Table 3.1 shows the Message Digest 5 (MD5) and Secure Hashing Algorithm 1 (SHA1) hashes for all the media files.

Table 3.1 *Media MD5 and SHA1 hashes*

File	MD5 Hash	SHA1 Hash
Image 1	6d69863c98bc0a32c90108cbf21f6484	a854ef26d2dbe46cd3be4db8f2fb0d7cf5370374
Image 2	dfc27b64e8c8f4c3e2626603cd5f5c76	f719f77d131a3c1c43fac3c061c7521359e6abec
Image 3	cc6d3e30329e7888dd0fbcc18806fa8d	3872915fc30061de263e8d97abfefe08913af85c
Image 4	0d69b01b1a3065136dbd49cc2a03eef8	960eac7428b90dd25edd65dd3fb42437d438d695
Image 5	06ea05c10b54a9ae9f43aae636ec0b80	9b2277705a6ad741fe5496354d0a6fd257f80d6e
Image 6	537de199a944505289ef0ddd1ef74dfd	bec92798dbcf28bfd1a9caf8a325366ca0545919
Image 7	56d63e8e25b5f603c0aa1bf3747472d8	88c15fa56f57bd87216d7fa5905ecb13b6b4c5de
Image 8	79a786fb2c93f2e5dc7e0af6e6765167	6eabf820da2771dbfde46b8e5222ce299dbff244
Image 9	f51adc9a1ba060e7546ccb295761062d	57e85a7e8523e8066d5333bc2163700803d962bf
Image 10	63e9997759e80954f8ce2d92575314f4	367d4d44d1e7f96db557dea6eab16b3cfa2c77c3
Image 11	1c9dfadb507a7e0ae10094108fc56f2f	a981fadb1e8432dd9cc130cc6a26fe00a320f46f
Video 1	afebfdacf3d952af03f6855f4808d9c9	32f8087e9c952d1def99367a7f9ab7415a72c103
Video 2	cd90d521ae61ccd9f91c64e6490b4d94	00f24fa123a1f0a5af611993b6e71f027c18d205
PDF	fde93a9ad8de6ab04bdff40359145e11	001c91e37ac840ad1c627cafe0c9ab6363cff440

3.3.4 Acquisition of Data

The acquisition of data took place after the last action in Appendix B was completed, that is, closing and reopening the WhatsApp web/desktop client. Data acquisition was done in each environment before continuing with the population of data in the next environment. To acquire data for forensic analysis, first a RAM acquisition in each virtual environment was performed. For the Windows OS, FTK imager lite version 3.1.1 was used. For the Mac OS environments, no RAM captures were performed as the author did not identify reliable methods of capturing RAM on the latest Mac OS (Mojave 10.14.3) at the time of data population. After RAM was captured on the Windows environments and when the last event was performed in the Mac OS environments, a controlled shut down of the different virtual machines was performed. Once this was accomplished, the virtual machine file of each environment was imaged using FTK imager version 4.2.0.13 and the hashes were recorded. A copy of each forensic image was used for analysis with the forensic tools listed in the next section. On the mobile devices, individual and group chat backups were made for both the suspect and victim smartphones using WhatsApp's backup feature.

3.3.5 Forensic Analysis of Data

As previously mentioned in the review of the relevant literature, there are several digital forensic tools that can be used for the analysis of computers, images, and virtual environments. Popular commercial tools that were used for the analysis of the virtual machines are Access Data's FTK, and Magnet's AXIOM. FTK and AXIOM are industry-standard tools in the computer forensics field. The author decided to use these tools as they have been previously tested and identified as providing reliable results (Lawrence, 2018). Autopsy from The Sleuth Kit was also considered during the study as it is a popular open source tool freely available for the digital forensics community (SleuthKit, n.d.). These three tools were also chosen as they are currently available at Purdue University's Cyberforensics laboratory. Figure 2 shows the flow of the current study's methodology.

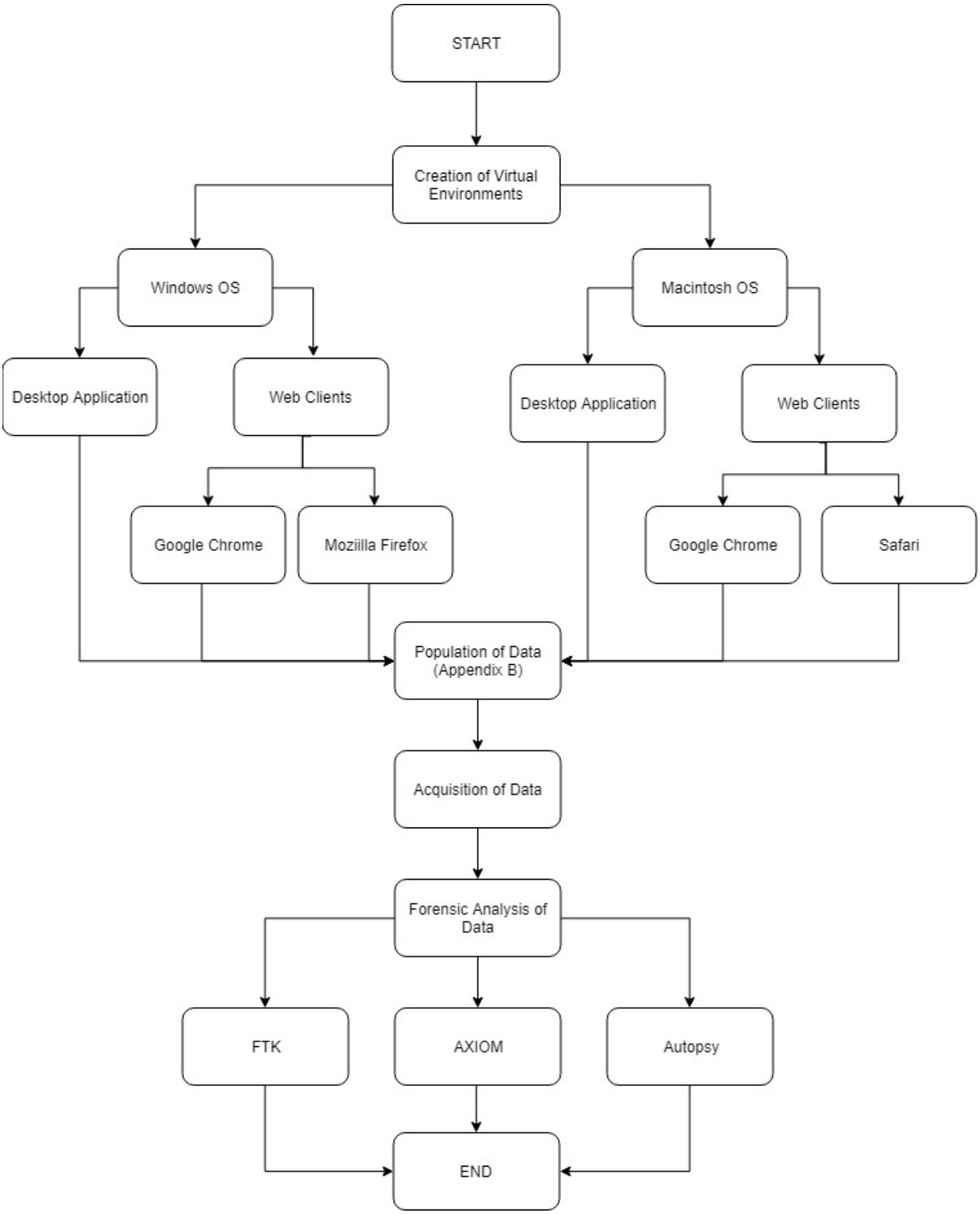

Figure 2 *Current study flowchart*

3.4 Summary

Chapter three provided an overview of the research methodology of the study. This included the research questions, hypotheses, and operational definitions. The chapter outlined the research environments, including the hardware and software specifications for all the hosts and virtual environments. A population of data took place for the WhatsApp clients on the virtual machines, as detailed in Appendix B. Forensic acquisitions were made of the virtual machines and then forensically analyzed using FTK, AXIOM, and Autopsy. Finally, a comparison of the total number of recovered artifacts on each environment was made. The next chapter details the results of the forensic analysis of the virtual machines.

CHAPTER 4. RESULTS

This chapter presents the artifacts found on each environment after conducting the forensic analysis with FTK, AXIOM, and Autopsy. There were a total of six environments; three for the Windows client and three for the Mac OS client. On both OS, the WhatsApp desktop application and Google Chrome web client were analyzed. The two other environments were the Mozilla Firefox web client for the Windows OS, and Safari for Mac OS.

4.1 Hypothesis One

The first hypothesis stated the same number of artifacts will be recovered for the WhatsApp desktop application on both operating systems. Table 4.1 presents the artifacts found with all three forensic tools across all environments on the Windows OS.

Table 4.1 *Recovered artifacts in all Windows environments*

Artifact No.	Artifact	Recovered/Total	
		Desktop WA	Chrome & Firefox
	Recovered		
1	Log of blocking a contact	1/1	1/1
2	Log of WA client being used	0/1	1/1
3	Log of mobile device information	6/6	6/6
4	Log of account's modification	3/3	3/3
5	Log of viewing status	0/2	2/2
6	Log of viewing a conversation's media	0/2	2/2
	Subtotal	10/15 (67%)	15/15 (100%)
	Partial Recovery		
7	Text messages	0/27	27/27
8	Deleted messages	0/3	2/3
9	Pictures sent	0/3	3/3
10	Video sent	0/1	1/1
11	PDFfile sent	0/1	1/1
12	Photo taken	0/1	1/1
13	Voice message recorded	0/1	1/1
14	Contact's information	0/1	1/1
15	Individual chat	1/1	1/1
16	Group chat	1/1	1/1
	Subtotal	2/40 (5%)	40/40 (100%)
	Total	12/55 (22%)	55/55 (100%)

Note. This table shows recovery status across all WhatsApp clients in the Windows OS using all three forensic tools. Partial recovery refers to artifacts for which a log or timestamp was found, yet no content was recovered. WA: WhatsApp.

There was a total of 16 types of recoverable artifacts that were defined for the purpose of the study. For most clients, six artifacts were recovered, and ten artifacts were partially recovered. Recovered and partially recovered artifacts were found on the locations outlined in Table 4.2. Partially recovered artifacts refer to those for which the content was not recovered, yet either a log or timestamp of the artifact was found. For example, there are indications the suspect read received messages, however, the contents of these messages are not shown. Partially recovered artifacts are further explained in Table 4.3. These artifacts were located in the WhatsApp log files. Timestamps found within the WhatsApp log file were compared to the chat backups made on the smartphones. The log file's timestamps were accurate as they matched with the timestamps from the backups.

Table 4.2 *Recovered artifact locations for the Windows environments*

WhatsApp Client	**WhatsApp Log File**
Desktop Application	Users\{SUSPECT}\AppData\Roaming\WhatsApp\IndexedDB\file__0.indexeddb.leveldb\{######}.log
Chrome Client	Users\{SUSPECT}\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb\{######}.log
Firefox Client	Users\{SUSPECT}\AppData\Roaming\Mozilla\Firefox\Profiles\xqimcopc.default\storage\default\https+++web.whatsapp.com\idb\{##########}wcaw.sqlite

Note. All clients described in this table refer to those located in the Windows OS.

Table 4.3 *Fully and partially recovered artifacts extracted from the WhatsApp log file*

Category	Artifact	Note
Timestamps/Actions	action,presence,[available/unavailable]	The suspect's online status.
	action,chatstate,[composing/paused/recording]	The status of the suspect's action; typing a message, stopped typing, recording an audio message. This is updated every ten seconds once the suspect starts composing a message.
	action,message,[image/video/chat/vcard/document/ptt]	Log of when the suspect sends a message. This does not specify who is recipient. Vcard is a contact's information, ptt is the push-to-talk feature (recording audio message).
	action,msgs,delete	Log of when the suspect deletes a message
	action,block,true,18125730324	Log of the suspect blocking a contact.
	action,battery,84,false	Log of the smartphone's battery level at certain time.
	action,group,create	Log of a group chat creation.
	action,set_pic,17653278892@c	Log of the suspect setting a profile picture.
	action,pushname	Log of the suspect setting a display name.
	action,status,set	Log of the suspect modifying the 'about' information.
	action,chat,read,{"fromMe":false,"remote":18125730324@c.us…}	Log of the suspect reading a message. This is known as the two blue checkmarks on WhatsApp.
	action,status,read,{"fromMe":false,"remote":"s&ð>@broadcast","id":"C259586486C33C79E0482B1F346C9D98…}"	Log of the suspect viewing a status upload.
	Media:sendToChat chat 18125730324@c.us	Log of suspect sending media to the victim through the individual chat.
	Media:sendToChat chat 17653278892-1548963594@g.us	Log of suspect sending media to the victim through the group chat.
	action,msg,relay,[chat,image,video],18125730324@c.us,17653278892@c.us	Suspect receiving a chat message, image, or video. This is known as the two green checkmarks on WhatsApp.
	action,msg,relay,image,status@broadcast,17653278892@c.us,false_status@broadcast_FCECD863D949D0AAD2DFE7260AD9DC4B,18125730324@c.us"	Suspect receiving a status update from their contact's list.
	profilePic:cache-save: profile_pic_thumb	Log of a profile picture being saved. This included the suspect's, victim's and group chat's profile pictures.
	AppUpdate:update current: 0.3.2041 latest: 0.3.2041	Log of WhatsApp client checking for updates.
Mobile Device Information	webcPhoneOsBuildNumber = PQ1A.181205.002.A1	Mobile device OS build number
	webcPhoneOsVersion = 9	Mobile device OS version
	webcPhoneAppVersion = 2.19.17	Mobile device WhatsApp application version
	webcPhoneDeviceManufacturer = Google	Mobile device manufacturer
	webcPhoneDeviceModel = marlin	Mobile device model. In this case, "marlin" is the codeword for the Google Pixel XL.
	webcPhoneCharging = false	Mobile phone charging. In this case, at the time it was not charging.
Browser User Agent	userAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36	Identifies the browser client and OS being used by the suspect.

Note. All timestamps/actions begin with a date and time (i.e., YYYY-MM-DD HH:MM:SS.MS). The time is displayed in the Pacific Time (PT) zone.

The three tools used for the forensic analysis do not currently support the APFS used on the Mac OS (i.e., FTK 7.0.0.163; AXIOM 2.9.0.12898; Autopsy 4.10.0). However, these tools were able to locate strings found on the WhatsApp log file (e.g., “action,chatstate”, “action,message,chat”). As the tools currently cannot properly read the APFS, no location is available for the WhatsApp log file across the different clients. Any search queries will locate specified data and classify it as being stored in unallocated space. Each artifact was still recovered, either partially or completely, as shown in Table 4.4. Artifact recovery was possible by using Blacklight version 2018.4, a tool that currently supports APFS. This process is further explained in the *post hoc* findings.

Table 4.4 *Recovered artifacts in all Mac OS environments*

Artifact No.	Artifact	Recovered/Total		
		Desktop WA	**Chrome WA**	**Safari WA**
	Recovered			
1	Log of blocking a contact	1/1	1/1	1/1
2	Log of WA client being used	0/1	1/1	1/1
3	Log of mobile device information	6/6	6/6	6/6
4	Log of account's modification	3/3	3/3	3/3
5	Log of viewing status	0/2	2/2	0/2
6	Log of viewing a conversation's media	0/2	2/2	0/2
	Subtotal	10/15 (67%)	15/15 (100%)	11/15 (73%)
	Partial Recovery			
7	Text messages	0/27	27/27	0/27
8	Deleted messages	0/3	2/3	2/3
9	Pictures sent	0/3	3/3	0/3
10	Video sent	0/1	1/1	0/1
11	PDFfile sent	0/1	1/1	0/1
12	Photo taken	0/1	1/1	0/1
13	Voice message recorded	0/1	1/1	0/1
14	Contact's information	0/1	1/1	0/1
15	Individual chat	1/1	1/1	1/1
16	Group chat	1/1	1/1	1/1
	Subtotal	2/40 (5%)	40/40 (100%)	4/40 (10%)
	Total	12/55 (22%)	55/55 (100%)	15/55 (27%)

Note. This table shows recovery status across all WhatsApp clients in the Mac OS using Blacklight. Partial recovery refers to artifacts for which a log or timestamp was found, yet no content was recovered. WA: WhatsApp.

Based on the results presented before on Tables 4.1 through 4.4, the first hypothesis was supported as the total number of recovered and partially recovered artifacts is the same for the WhatsApp desktop application on both Windows 10 OS and Mac OS 10.14.3.

4.2 Hypothesis Two

The second hypothesis stated the same number of artifacts will be recovered across all WhatsApp web clients. The second hypothesis was supported for the Windows web clients (i.e., Chrome and Firefox) as the same number of artifacts were recovered on the Windows 10 OS; six full recoveries and ten partial recoveries. The second hypothesis was not supported for the Mac OS 10.14.3 web clients as the number of recovered artifacts for the Safari client is less than the artifacts recovered on the Chrome client. Results show only 27% of artifacts were both partially and fully recovered for the Safari client, while all artifacts were either partially or fully recovered for the Chrome client, as seen on Table 4.4.

4.3 Hypothesis Three

The third hypothesis stated the same number of artifacts will be recovered on each WhatsApp client when using FTK, AXIOM, and Autopsy. The third hypothesis was supported as the total number of recovered and partially recovered artifacts is the same for all tools (i.e., FTK, AXIOM, Autopsy) across all WhatsApp clients on both operating systems.

4.4 *Post Hoc* Findings

Beyond the artifacts already mentioned, there were a few discoveries of artifacts which were not part of the previously defined recoverable artifacts in section 3.2. These additional artifacts include:

- The Windows registry, which shows installed programs. An installed program will have a unique installation location within the drive as well as an entry on the registry key of the machine.
- Prefetch files, which contain information regarding how many times an application was run along with its run date/time.
- Shortcut or link (LNK) files, which contain information regarding an application's last accessed date/time.
- Cached WhatsApp profile pictures, including the suspect, victim, and group chat.

- Chrome/Firefox browser history file, which contain information on the web.whatsapp.com accessed URL such as the last visited date/time, the visit count, and the number of times the URL was typed.

These artifacts' locations can be found in Table 4.5. Note that other information (e.g., databases, files, folders) might be stored within these WhatsApp directories, specifically for the WhatsApp desktop client. However, these presented no forensic significance for the current research.

Table 4.5 *Additional artifacts discovered in the Windows OS*

WhatsApp Client	Artifact and Location
Desktop Application	Installed program[1]: Users\{SUSPECT}\AppData\Local\WhatsApp Registry key[1]: Users\{SUSPECT}\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Uninstall\WhatsApp WhatsApp prefetch file[2]: Windows\Prefetch\WHATSAPP.EXE-06A9BBC4.pf WhatsApp shortcut file[3]: Users\{SUSPECT}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WhatsApp\WhatsApp.lnk Users\{SUSPECT}\AppData\Desktop\WhatsApp.lnk Cached profile pictures[4]: Users\{SUSPECT}\AppData\Roaming\WhatsApp\Cache
Chrome Client	Chrome history file[5]: Users\{SUSPECT}\AppData\Local\Google\Chrome\User Data\Default\History Chrome prefetch file[2]: Windows/Prefetch/CHROME.EXE-CCF9F3F6.pf Chrome shortcut files[3]: ProgramData/Microsoft/Windows/Start Menu/Programs/Google Chrome.lnk Users/Public/Desktop/Google Chrome.lnk Users/{SUSPECT}/AppData/Roaming/Microsoft/Internet Explorer/Quick Launch/Google Chrome.lnk Cached profile pictures[4]: Users\{SUSPECT}\AppData\Local\Google\Chrome\User Data\Default\Cache
Firefox Client	Firefox history file[5]: Users\{SUSPECT}\AppData\Roaming\Mozilla\Firefox\Profiles\xqimcopc.default\places.sqlite Firefox prefetch file[2]: Windows/Prefetch/FIREFOX.EXE-25FC0A66.pf Firefox shortcut files[3]: Users\{SUSPECT}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefox.lnk Users\{SUSPECT}\AppData\Desktop\Firefox.lnk Cached profile pictures[4]: Users\{SUSPECT}\AppData\Local\Mozilla\Firefox\Profiles\xqimcopc.default\cache2\entries

Note. All clients described on this table refer to those located in the Windows OS.

[1]: An installed program will have a unique installation location within the drive as well as an entry in the registry key of the machine.

[2]: The prefetch file will contain information regarding how many times the application was run along with its run date/time.

[3]: The shortcut files, also known as LNK file, contains information regarding the application's last accessed date/time.

[4]: Cached profile pictures recovered include the suspect, victim, and group chat.

[5]: The history file will contain information regarding the web.whatsapp.com URL such as the last visited date/time, the visit count, and the number of times the URL was typed.

A tool that supported, at the time of writing, the APFS is BlackBag Technologies' Blacklight (version 2018.4). This was used to locate the WhatsApp log file and cached profile pictures on the Mac OS environments since the three proposed tools were not able to read the APFS. These findings are shown in Table 4.6.

Table 4.6 *Recovered artifact locations for the Mac OS environments*

WhatsApp Client	WhatsApp Log File	Profile Pictures
Desktop Application	/Users/{SUSPECT}/Library/Application Support/WhatsApp/IndexedDB/file__0.indexeddb.leveldb/{#####}.log	/Users/{SUSPECT}/Library/ApplicationSupport/WhatsApp/Cache
Chrome Client	/Users/{SUSPECT}/Library/Application Support/Google/Chrome/Default/IndexedDB/https_web.whatsapp.com_0.indexeddb.leveldb/{######}.log	N/A
Safari Client	/Users/{SUSPECT}/Library/Safari/Databases/___IndexedDB/https_web.whatsapp.com_0/wawc/IndexedDB.sqlite3	/Users/{SUSPECT}/Library/Containers/com.apple.Safari/Data/Library/Caches/com.apple.Safari/WebKitCache/Version 13/Blobs /Users/{SUSPECT}/Library/Containers/com.apple.Safari/Data/Library/Caches/com.apple.Safari/WebKitCache/Version 13/Records

Note. All clients described in this table refer to those located in the Mac OS.

In April 3rd, 2017, a user reported on Forensic Focus, an online digital forensics forum, that they were able to recover chat content from a directory on the Yosemite Mac OS 10.10.13 (Forensic Focus, 2017). The post referenced the *ChatSearch* and *ChatStorage* SQLite databases, which are also found on the WhatsApp directories of mobile operating systems. However, the *post hoc* analysis conducted in the current study did not reveal these SQLite databases in the Mac OS 10.14.3 for the WhatsApp desktop client version 0.3.1847.

As previously mentioned, cached profile pictures were discovered throughout the different WhatsApp clients. The recovered profile pictures across all environments can be found on Table 4.7. None of the cached profile pictures' MD5 or SHA1 hashes matched with the hashes reported in table 3.1.

Table 4.7 *Recovered profile pictures*

	Recovered/Total		
	Suspect	**Victim**	**Group Chat**
Windows OS			
Desktop application	1/2	1/1	0/1
Chrome client	1/2	1/1	1/1
Firefox client	2/2	1/1	1/1
Mac OS			
Desktop application	1/2*	1/1	0/1
Chrome client	0/2	0/1	0/1
Safari client	1/2	1/1	1/1

Note. *: Latest profile picture was discovered.

CHAPTER 5. DISCUSSION

The purpose of this study was to determine which forensic artifacts, if at all, can be recovered when using WhatsApp on web clients and desktop applications. Specifically, this study looked at the desktop application on both Windows 10 and Mac OS Mojave 10.14.3. The web clients analyzed were the Chrome and Firefox client for the Windows OS, while Safari and Chrome were analyzed on the Mac OS.

To date, WhatsApp is the most popular instant messaging application worldwide and is available on the two major mobile operating systems, Android and iOS. WhatsApp has over 1.5 billion monthly active users in over 180 countries as of July 2018 (Statista, 2018). The findings of this research will aid investigators in locating certain artifacts, mainly timestamps and cached profile pictures, when analyzing a suspect's desktop where a WhatsApp client was used.

Results revealed several artifacts remain on all WhatsApp clients across both operating systems. These can be found within the WhatsApp log file that is automatically created when a user interacts with a client. As the extension for the file implies (i.e., .log), this is a file that records timestamps, actions, and activities that have been taking place within the WhatsApp client. However, the WhatsApp log file does not store any content. For example, when a user sends a contact's information, only the name of the contact being sent is saved on the log file and not the contact's phone number. Another example would be a timestamp of when media is sent to a contact, yet the contents of said media are not known. The discovery of the WhatsApp log file is the first of its kind in the body of literature for WhatsApp forensics, specifically web and desktop clients. However, this information should come to no surprise as WhatsApp states in its privacy policy and legal information site that it automatically collects information relating to usage, log, device, and connections to their services (WhatsApp, n.d.).

Post hoc analysis revealed other important artifacts, such as cached WhatsApp profile pictures (suspect, victim, group chat), application run count/date/time (prefetch files, link files), URL visit count/date/time (web browser history), and installed applications (Windows registry).

Out of the previously identified literature for WhatsApp clients, only two papers have been published on the web client and none on the desktop applications. In 2017, Yudha, Luthfi, and Prayudi made a reference to browsers saving log file data when they are used. This log file includes information such as the "application cache, ref, tok, file system, indexed database and

local storage" (Yudha et al., 2017). However, the authors did not make a reference to a single log file name or its location, that is created when a WhatsApp client is used on a system. The other identified literature references, based on the Chrome history file, the date/time and a count of when a user has visited the web.whatsapp.com URL (Actoriano & Riadi, 2018).

The analysis of the different OS environments revealed the main source of artifacts to be the WhatsApp log file. This file is present consistently across all web clients and desktop applications examined. It is suspected the log file is created once a user scans the QR code and starts using any WhatsApp client. Within the WhatsApp log file, three main categories of information are being recorded: (1) Timestamps of user actions, (2) mobile client device information, and (3) browser user agent information. Amongst the timestamps of user actions, events such as sending a message is recorded (i.e., text, audio, video, photo, contact), the action of deleting a message, blocking a contact, modification of the user's account information (i.e., profile picture, name, about), creating a group chat, receiving a message (i.e., text, image, video) and a few other events are recorded as shown in Table 4.3. Mobile client device information includes the smartphone's build number, OS version, WhatsApp version, battery level, and device manufacturer/model. Finally, the browser user agent reveals information about the system's OS and web client being used.

The WhatsApp log file is constantly updated as the system logs the user's new interactions with the WhatsApp client. Over time, information previously saved on this log file might be overwritten by new timestamps and actions, so it is important to note that this file might not contain a user's entire log history. It is currently not known how often or how long it will take for the client to overwrite existing log data. Future work should consider answering this question.

Even though the WhatsApp log file does not store any message or media contents, it still logs valuable timestamp information that could be useful during an investigation. For example, this valuable data could prove that a suspect sent harassing photos to a victim based on a timestamp, or perhaps that a suspect had a particular smartphone make/model running the latest OS version. Knowing the smartphone's OS version would help investigators determine which forensic acquisition techniques or tools would fit best in a particular scenario. A probable explanation as to why content information is not available or not being saved on the system could be the fact that content being sent/received to/from WhatsApp's servers is end-to-end

encrypted. WhatsApp developers might have decided not to store this information locally on a computer due to privacy concerns. It is not surprising that no content information is being stored as WhatsApp claims it does not collect the contents of communication, and not even law enforcement can have access to this type of information. In the Information for Law Enforcement authorities under Security and Privacy, WhatsApp states the following:

> A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include numbers blocking or blocked by the user, in addition to the basic subscriber records identified above (WhatsApp, n.d.).

Another plausible explanation could be that log files simply do not store this type of information, rather only lightweight timestamps or logs of different actions or activities due to storage optimization or limitations.

Within the WhatsApp log file, not all artifact types were found consistently throughout the WhatsApp clients. Compared to the web clients, the desktop applications across both operating systems provided the least number of artifacts. The Chrome clients across both operating systems and the Firefox client on Windows provided the most artifacts within the log file. Based on the current study, it is not attainable to determine why some artifact types were recovered in certain WhatsApp clients' log files while not on the others. For example, for the desktop applications on both OS, no actions initiated by the suspect were logged (e.g., sending text messages and media), while the same actions were found on the Chrome clients. A couple of explanations can be considered when trying to address why these artifacts might not have been saved on the different environments. These include the possibility that data might have been overwritten within the log file. To address this, the different WhatsApp environments should be re-populated. A larger data set or story should also be considered to capture more logged information. However, investigators should still consider the possibility that perhaps certain clients do not log the artifacts in question.

A log of deleting text messages was found for only two out of the three messages deleted. Based on the story developed for data population, two text messages sent by the suspect were deleted, and one text message sent by the victim was deleted. Out of the deleted messages by the suspect, one text message was deleted for both parties and the other was deleted for only the suspect. It is currently not attainable to determine whether the log of one of the deleted messages

belongs to the text sent by the victim. By looking at the chat backups made on the mobile client, only the deletion for both parties of the message sent by the suspect can be found. Deleting all the text messages took place within the same minute, further complicating determining which actions were logged as the chat backups made on the mobile clients did not log microseconds, unlike the WhatsApp log file found on the different environments.

Post hoc analysis revealed important additional artifacts. One of these were the cached profile pictures. Cached profile pictures were found across all WhatsApp clients, except for the Chrome client on the Mac OS. WhatsApp clients cache the profile pictures of contacts and group chats a user has been in contact with recently. This is another important artifact that could aid investigators as it would show the individuals or group chats a user has recently interacted with. Table 4.7 shows the cached profile pictures across all clients. Although no cached profile pictures were found on the Chrome client for Mac OS, this does not imply this client is not caching any profile pictures. A plausible explanation could be the tool used to analyze this client was not able to parse this data. Also, it's possible the browser in this particular research environment (i.e., Chrome web client for Mac OS) did not cache any profile pictures. Future work would address this concern by repopulating a client with data, perhaps more data than what was used in the current study, and later analyzing it to potentially discover cached profile pictures. However, investigators should also consider the possibility that this specific client might not cache profile pictures.

Results show most WhatsApp clients cached only the first image that was set as the suspect's profile picture. As seen on Appendix B, a second image was set for the suspect's profile picture. This second profile picture was only cached by the Firefox client on the Windows OS and the desktop application on the Mac OS. It is currently not attainable to determine how often these images are cached or why most clients only cached the suspect's first profile picture. Creating a larger data population story and later repopulating a client could perhaps lead to all profile pictures being cached as more time would be spent interacting with the client. An alternative explanation to consider is that perhaps the tools used to examine the environments were not able to parse or locate the profile pictures.

5.1 Limitations

One of the limitations the study faced was a short data population for the different WhatsApp client environments. Data population took around an hour on each environment to accomplish, and was limited to 27 text messages and less than ten media items. Perhaps if more data was sent through the WhatsApp clients, the WhatsApp log file might have recorded enough data where it would have needed to start purging and overwriting previous log information.

Another limitation to consider is that, although RAM was captured prior to shutting down the Windows OS environments, no RAM analysis was performed. For the Mac OS, the author did not identify any reliable methods for capturing RAM, so no RAM was acquired. Nevertheless, RAM analysis was out of the scope of the main research in this study as the author identified capturing RAM might not always be feasible in a real scenario (e.g., no password provided to unlock the suspect's desktop, limited RAM on the suspect device, device powered off, unprepared first responders).

5.2 Future research

Although the discoveries made in this study show valuable artifacts that are recorded across the different WhatsApp clients, there are still questions that remain unanswered. There is room for continuing research in the field of WhatsApp forensics, specifically with the web clients across different operating systems and the desktop applications. Future research should address discovering how often the WhatsApp log file overwrites data, and whether any previous timestamps are purged when this takes place. This would be helpful as it could give investigators an estimate of how far back in time the log file has stored information. This is something the current research was not able to determine due to a short data population, accomplished within a day on each environment.

Future work should also explore other WhatsApp web clients, such as Opera and Microsoft Edge for the Windows OS, and Mozilla Firefox and Opera for the Mac OS. As discovered in this study, all WhatsApp clients, both web and the desktop applications, record a WhatsApp log file. Future work would compare and contrast recovered artifacts within the log file on each client with what has been published in this study. This would help determine which web clients store the most information in the log file.

Analyzing RAM captures on the different WhatsApp environments is another consideration for future work. The current study did not incorporate RAM examination as part of the analysis phase, due to the reasons previously listed. Nonetheless, RAM has the potential of storing valuable information a suspect might have been transmitting through the WhatsApp clients (e.g., chat history, images, IP addresses, running applications), so future research should also focus on this.

Finally, future work should also consider repopulating data on a few of the WhatsApp client environments that did not produce as many artifacts as the other environments (i.e., cached profile pictures, timestamps for text messages and media sent). These include the WhatsApp desktop applications and Chrome clients on both Windows and Mac OS, as well as the Safari WhatsApp client on the Mac OS. Repopulating data on these environments and conducting further analysis could determine whether these artifacts are in fact present on these environments. Repopulating data could also rule out if this study's population environments simply did not produce these artifacts. It is recommended to develop a larger data population story where more messages and media is sent from the WhatsApp client. This will ensure more time will be spent interacting with the clients, potentially leading to the client saving more information on the log file and caching more profile pictures. Using other digital forensic tools, either open source or commercial, should also be considered for future work to compare data found throughout the different WhatsApp clients.

5.3 Conclusion

The analysis of the WhatsApp clients revealed the presence of several artifacts of value for digital forensics investigators. The main source of artifacts is the WhatsApp log file, present throughout all WhatsApp clients. Within this log file, different data can be found, such as timestamps of user actions, mobile client device information, and browser user agent information. The WhatsApp clients also cache the profile pictures of recent contacts, including the user's and group chats' a user has been interacting with. Furthermore, an investigator can discover the WhatsApp desktop application's run date/time/count by inspecting the prefetch files. By identifying the respective browser's history file, the web.whatsapp.com accessed URL date/time/count can also be located.

Overall, the Chrome web client on both OS and the Firefox client on the Windows OS are the clients that store the most artifacts when compared to the rest of the WhatsApp clients analyzed. The same number of artifacts were recovered within these three clients when inspecting the WhatsApp log file. The Firefox client was able to cache all profile pictures, unlike the Chrome client on both operating systems.

REFERENCES

Actoriano, B., & Riadi, I. (2018). Forensic Investigation on WhatsApp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2. *International Journal of Cyber-security and Digital Forensics (IJCSDF), 7*(4), 410-419.

Ali, I., & Meghanathan, N. (2011). Virtual machines and networks-installation, performance study, advantages and virtualization options. *International Journal of Network Security & Its Applications (IJNSA) 3*(1).

Akbal, E., Günes, F., & Akbal, A. (2016). Digital forensic analyses of web browser records. *Journal of Software* (*JSW), 11*(7), 631-637.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation, 2*(2), 147-167.

Boneva, B. S., Quinn, A., Kraut, R., Kiesler, S., & Shklovski, I. (2006). Teenage communication in the instant messaging era. *Computers, phones, and the Internet: Domesticating information technology,* 201-218.

Bossler, A., Holt, T. J., & Seigfried-Spellar, K. C. (2017*). Cybercrime and digital forensics: An introduction.* London, U.K.: Routledge.

Boxall, A. (2018, April). *Apple watch heart rate data used as evidence in Australian murder trial.* Retrieved from https://www.digitaltrends.com

Carrier, B., & Spafford, E. (2004). *Defining searches of digital crime scenes*. Under review.

Carrier, B., Spafford, E. H., et al. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1-20.

Casey, E. (2009). *Handbook of digital forensics and investigation*. London, U.K.: Academic Press.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet.* London, U.K.: Academic press.

Chu, H.-C., Wang, G.-G., & Deng, D.-J. (2016). The social networking investigation of metadata of forensic artifacts of a typical WeChat session under windows. *Security and Communication Networks, 9*(18), 5698-5709.

Crime Scene. (n.d.). *Harassing text messages*. Retrieved from https://www.crimescene.com/previous-cases-1473587462/fatal-case/casefiles-doc/2074-evidence-texts

Dean, B. (n.d.). *Best practices in browser forensics*. Retrieved from https://www.iansresearch.com/insights/reports/best-practices-in-browser-forensics

DigitalStrata. (2017, December). *Two famous cases where digital evidence was key.* Retrieved from https://www.digital-strata.com

Forensic Focus. (2017, April). *WhatsApp – desktop version*. Retrieved from https://www.forensicfocus.com/Forums/viewtopic/t=15262

Gao, F., & Zhang, Y. (2013). Analysis of WeChat on iPhone. *In 2nd International Symposium on Computer, Communication, Control, and Automation* (*3ca*) 278-281.

Goel, A., Tyagi, A., & Agarwal, A. (2012). Smartphone forensic investigation process model. *International Journal of Computer Science & Security (IJCSS), 6*(5), 322-341.

Jansen, W., & Ayers, R. (2007). Guidelines on cell phone forensics. *NIST Special Publication, 800*(101).

LaPorte, G. Paul D. Ceglia v. Mark Elliot Zuckerberg and Facebook, Inc. United States District Court Western District of New York, Civil Action No. 1: 10-cv-00569-RJA, Document 326, Case Riley Welch LaPorte & Associates Forensic Laboratories (RWL). Filed 03/26/12.

Lawrence, T., Karabiyik, U., & Shashidhar, N. (2018, March). Equipping a digital forensics lab on a budget. In *6th International Symposium on Digital Forensic and Security (ISDFS)*. Antalya, Turkey.

Levine, B. (2003). *Principles of forensic toxicology*. Washington, D.C.: AACC Press.

McCarty, B. (2011, December). *The history of smartphones*. Retrieved from https://thenextweb.com/mobile/2011/12/06/the-history-of-the-smartphone

McKemmish, R. (1999). *What is forensic computing?* Canberra: Australian Institute of Criminology.

McLaughlin, E. (2017, April). *Suspect OKs Amazon to hand over Echo recordings in murder case.* Retrieved from https://www.cnn.com

Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation, 1*(1), 61-68.

NIST. (2016, March). *Mobile device data populations setup guide, version 2.0.*

Nozicka, L. (2017, August). *Suitcase killer Melanie McGuire has yet another appeal denied*. Retrieved from https://www.nj.com

Oh, J., Lee, S., & Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. *Digital Investigation, 8*, S62-S70.

Ovens, K. M., & Morison, G. (2016). Forensic analysis of Kik messenger on iOS devices. *Digital Investigation, 17*, 40-52.

Palmer, G., et al. (2001). A road map for digital forensic research. In *First Digital Forensic Research Workshop* (pp. 27-30). *Utica, New York.*

Pollitt, M. (2010, January). A history of digital forensics. In *IFIP International Conference on Digital Forensics* (pp. 3-15). Berlin, Heidelberg. Springer.

Pothitos, A. (2016, October). *The history of the smartphone.* Retrieved from http://www.mobileindustryreview.com

Raghav, S., & Saxena, A. K. (2009, November). Mobile forensics: Guidelines and challenges in data preservation and acquisition. In *Research and Development (SCOReD) on 2009 IEEE Student Conference* (pp. 5-8). IEEE.

Rathi, K., Karabiyik, U., Aderibigbe, T., & Chi, H. (2018, March). Forensic analysis of encrypted instant messaging applications on Android. In *Digital Forensic and Security (ISDFS) on 2018 6th International Symposium* (pp. 1-6). IEEE.

Rathod, D. M. (2017). Web Browser Forensics: Google Chrome. *International Journal of Advanced Research in Computer Science*, *8*(7).

Rayner, G. (2017, March). *WhatsApp accused of giving terrorists 'a secret place to hide' as it refuses to hand over London attacker's messages.* Retrieved from http://www.telegraph.co.uk

Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. McGraw-Hill Education Group.

Rigby, S., & Rogers, M. K. (2007). The general digital forensics model. *In Annual ADFSL Conference on Digital Forensics, Security, and Law.*

Ryan, C., & Lewis, J. M. (2017). Computer and Internet use in the United States: 2015. *American Community Survey Reports*.

Sgaras, C., Kechadi, M. T., & Le-Khac, N. A. (2015). Forensics acquisition and analysis of instant messaging and VoIP applications. In *Computational forensics* (pp. 188-199). Springer, Cham.

Sharma, M. (2018). *WhatsApp sets over 13-hour windows to delete message for everyone permanently.* Retrieved from https://www.businesstoday.in

SleuthKit. (n.d.). *Open source digital forensics.* Retrieved from https://www.sleuthkit.org/

Sreeharsha, V. (2016, May). *WhatsApp blocked in Brazil as judge seeks data.* Retrieved from https://www.nytimes.com

Statcounter. (n.d.). *Browser market share worldwide - August 2018*. Retrieved from http://gs.statcounter.com/browser-market-share

Statcounter. (2018*). Desktop vs mobile vs tablet market share worldwide*. Retrieved from http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

Statista. (2015, August). *Distribution of Kik messenger users in the United States as of 2nd quarter 2015, by age*. Retrieved from https://www.statista.com

Statista. (2016). *Number of registered Kik messenger users worldwide from November 2012 to May 2016 (in millions).* Retrieved from https://www.statista.com

Statista. (2017, July). *Number of smartphone users in the United States from 2010 to 2022 (in millions).* Retrieved from https://www.statista.com

Statista. (2018, July). *Most popular mobile messaging apps worldwide as of July 2018, based on number of monthly active users (in millions).* Retrieved from https://www.statista.com

Stempel, J. (2018, August). *U.S. says Facebook fugitive Paul Ceglia arrested in Ecuador.* Retrieved from https://www.reuters.com

Stirparo, P. (2016, August). *Looking for the insider: Forensic artifacts on iOS messaging app*. Retrieved from https://isc.sans.edu

Tilstone, W. J., Savage, K. A., & Clark, L. A. (2006). *Forensic science: An encyclopedia of history, methods, and techniques*. ABC-CLIO.

Techopedia. (n.d.) *Web browser*. Retrieved from https://www.techopedia.com

Web.WhatsApp. (2018). *To use WhatsApp on your computer*. Retrieved from https://web.whatsapp.com

WhatsApp. (n.d.). *WhatsApp features*. Retrieved from https://www.whatsapp.com/features

WhatsApp. (n.d.). *WhatsApp legal info*. Retrieved from https://www.whatsapp.com/legal?eea=1#privacy-policy-information-we-collect

WhatsApp. (n.d.). *Information for law enforcement authorities*. Retrieved from https://faq.whatsapp.com/en/general/26000050/?category=5245250

WhatsApp. (2015, January). *WhatsApp web*. Retrieved from https://blog.whatsapp.com/614/WhatsApp-Web

WhatsApp. (2016). *Making WhatsApp free and more useful.* Retrieved from https://blog.whatsapp.com/615/Making-WhatsApp-free-and-more-useful

WhatsApp. (2016, February). *WhatsApp support for mobile devices*. Retrieved from https://blog.whatsapp.com/10000617/WhatsApp-support-for-mobile-devices

WhatsApp. (2016, May). *Introducing WhatsApp's desktop app*. Retrieved from https://blog.whatsapp.com/10000621/Introducing-WhatsApps-desktop-app

Yudha, F., Luth_, A., & Prayudi, Y. (2017). A proposed model for investigating on web WhatsApp application. *Advanced Science Letters, 23* (5), 4050-4054.

Zapotosky, M. (2016, March). *FBI has accessed San Bernardino shooter's phone without Apple's help.* Retrieved from https://www.washingtonpost.com

APPENDIX A. CRIMESCENE.COM HARRASSING TEXT MESSAGES

Date	Time	Acct Name	Direction	Msgs	Text Message
12/13/17	9:35 AM	662587XXXX	Received	1	You know what you did, you bitch.
12/16/17	1:01 PM	662587XXXX	Received	1	You haven't learned anything. But you will. Payback is coming.
12/19/17	6:40 PM	662587XXXX	Received	1	Too bad about your car. Maybe you should of gone straight home.
12/19/17	6:52 PM	662587XXXX	Received	2	Want me to tell you who did it?
					You don't deserve to know. As far as you know, it's just the start of the payback.
12/20/17	2:36 PM	662587XXXX	Received	1	That was an expensive lesson. Did you learn anything yet?
12/22/17	11:14 AM	662587XXXX	Received	1	How can you act like that after what you did? What would George say? What would Haley think? You think they won't find out?
12/25/17	9:48 AM	662587XXXX	Received	1	Nice holiday? You know you didn't deserve it. How do you live with yourself?
12/28/17	7:35 PM	662587XXXX	Received	1	Out drinking alone again? Don't drink and drive. Someone might call the cops.
01-02-18	8:15 AM	662587XXXX	Received	1	Who are you trying to fool? Everyone can see what a stupid, lazy bitch you are.
01-05-18	9:01 AM	662587XXXX	Received	1	Late for work today. Did you screw up again? Or are you just too lazy and stupid to be on time?
01-05-18	8:32 PM	662587XXXX	Received	3	Out with your friends again. If they knew what you did, you wouldn't have any friends.
					You should be spending time with your family while you still can.
					But maybe it's better if they start getting used to being without you.
01-06-18	7:24 PM	662587XXXX	Received	1	How dare you? You think people don't know? You think I don't know?
01-08-18	5:50 AM	662587XXXX	Received	3	Wake up, you stupid cow. Don't want to be late for work. Again.
					The coffee's brewing, but you haven't gone downstairs yet. You know you need that first cup before you can talk to anyone. George will be up soon.
					Don't ignore me. You don't want me to come in there and get you out of bed myself.
01-08-18	9:30 PM	662587XXXX	Received	3	Go ahead. Have another drink. You know you want to.
					You know how to make all this stop. Even someone as stupid as you can figure it out.
					It would be the best thing for everyone. Why should everyone else suffer because you're too stupid and selfish to do the right thing?
01-10-18	10:10 AM	662587XXXX	Received	1	You will suffer for your sins.
01-10-18	9:12 PM	662587XXXX	Received	1	Soon, very soon
01-11-18	3:25 PM	662587XXXX	Received	1	You're going to hell. And it'll still be better than you deserve.

Note: This story, titled "harassing text messages", was taken from www.crimescene.com.

APPENDIX B. SCRIPT FOR WHATSAPP DATA POPULATION

Event Number	Origin	Destination	Action
1	-	-	Set up the WhatsApp accounts for both the suspect and the victim. The suspect, with phone number 765-327-8892, will be named "Rafael" and the victim, with phone number 812-573-0324, will be named "Cynthia". Images 1 and 2 will be used as the profile pictures for the suspect and the victim, respectively. The suspect's account will register with the respective dekstop WhatsApp application. Create a contact on the suspect's phone with the following information: First name (Cynthia), last name (Staklo), phone number (812-573-0324), address (1869 Boiler Road, West Lafayette, IN 47906), email (gstaklo@mail.com), date of birth (01/01/2000), notes (SSN 789-55-7305. Two kids: George, Anne.), contact picture (image 11).
2	765-327-8892	812-573-0324	Message: You know what you did, you bitch.
3	765-327-8892	812-573-0324	Message: You haven't learned anything. But you will. Payback is coming.
4	765-327-8892	812-573-0324	Send image 3.
5	765-327-8892	812-573-0324	Message: Too bad about your car. Maybe you should of gone straight home.
6	765-327-8892	812-573-0324	Send image 4.
7	812-573-0324	765-327-8892	Message: Who is this?
8	765-327-8892	812-573-0324	Message: Want me to tell you who did it?
9	812-573-0324	765-327-8892	Message: Did you do it?
10	765-327-8892	812-573-0324	Message: You don't deserve to know. As far as you know, it's just the start of the payback.
11	812-573-0324	-	Status upload of image 5 with the following caption: "Thank you to everyone for your wishes. I am doing better now."
12	765-327-8892	812-573-0324	Suspect views victim's status and sends a message to the victim: "That was an expensive lesson. Did you learn anything yet?"
13	812-573-0324	765-327-8892	Message: The police have already been informed of your harassment. You are a primary suspect in the investigation now.
14	765-327-8892	-	Suspect modifies his profile information. Replaces profile picture with image 6, changes display name to "Anonymous", replaces the 'about' information with "We are anonymous. We do not forgive. We do not forget".
15	765-327-8892	812-573-0324	Message: How can you act like that after what you did? What would George say? What would Anne think? You think they won't find out?
16	812-573-0324	-	Status upload of image 8 with the following caption: "Enjoying the Holidays." Suspect views the status.
17	765-327-8892	812-573-0324	Message: Nice holiday? You know you didn't deserve it. How do you live with yourself?
18	765-327-8892	812-573-0324	Message: Out drinking alone again? Don't drink and drive. Someone might call the cops.
19	765-327-8892	812-573-0324	Message: Who are you trying to fool? Everyone can see what a stupid, lazy bitch you are.
20	812-573-0324	765-327-8892	Victim sends image 9 with the following message: "For your information, I already filed a police report for this harassment."
21	765-327-8892	-	Suspect views image 9. Suspect creates a group chat named "The truth", sets image 7 as the profile picture, and adds the victim to the group.
22	765-327-8892	812-573-0324	Message in group chat: Out with your friends again. If they knew what you did, you wouldn't have any friends.
23	765-327-8892	812-573-0324	Suspect sends the "Bomb Defusal Manual" PDF to the victim through the group chat.
24	765-327-8892	812-573-0324	Message in group chat: Maybe this will be helpful to you. Good luck.
25	765-327-8892	812-573-0324	Suspect sends video 1 to the victim through the group chat.
26	765-327-8892	812-573-0324	Message in group chat: Wake up, you stupid cow. Don't want to be late for work. Again.
27	765-327-8892	812-573-0324	Message in group chat: The coffee's brewing, but you haven't gone downstairs yet. You know you need that first cup before you can talk to anyone. George will be up soon.
28	765-327-8892	812-573-0324	Message: Don't ignore me. Maybe I could give George a call so you can start paying attention to me again.
29	765-327-8892	812-573-0324	Message: Look at all the information I have about you.
30	812-573-0324	765-327-8892	Message: What?
31	765-327-8892	812-573-0324	Suspect sends Cynthia's contact information to her.
32	812-573-0324	765-327-8892	The victim sends video 2 to the suspect. The suspect plays the video.
33	812-573-0324	765-327-8892	Message: This will happen to you if you continue with the harassment.
34	765-327-8892	812-573-0324	The suspect takes a photo with the desktop's camera and sends it to the victim.
35	765-327-8892	812-573-0324	The suspect records an voice message with the desktop's microphone and sends it to the victim. The voice message will be 60 seconds in length.
36	812-573-0324	765-327-8892	Message: I have had enough of you and your harassment.
37	812-573-0324	765-327-8892	Message: Expect the police soon.
38	765-327-8892	812-573-0324	Message: You think you can scare me?
39	765-327-8892	812-573-0324	Message: You will suffer for your sins.
40	765-327-8892	812-573-0324	Message: Soon, very soon.
41	765-327-8892	812-573-0324	Message: You are going to hell. And it will still be better than what you deserve.
42	765-327-8892	812-573-0324	Suspect sends image 10 to the victim.
43	765-327-8892	-	Suspect deletes message in event 41 for both parties (sender and receiver).
44	765-327-8892	-	Suspect deletes message in event 38 for the sender only.
45	765-327-8892	-	Suspect deletes message in event 37 for the receiver only.
46	765-327-8892	-	Suspect blocks the victim.
47	-	-	Close and reopen WhatsApp application/web browser.

Note: This scenario was adapted and modified from the story titled "harassing text messages", taken from www.crimescene.com.

APPENDIX C. PROPEL APPROVAL OF RESEARCH

PURDUE UNIVERSITY HUMAN RESEARCH PROTECTION PROGRAM
INSTITUTIONAL REVIEW BOARDS

To: Kathryn Seigfried-Spellar

From: Purdue University Human Research Protections Program (HRPP)

Title: WHATSAPP FORENSICS: LOCATING ARTIFCATS ON WEB CLIENTS AND THE STANDALONE DESKTOP APPLICATION

Date: 12-29-2018

Re: PROPEL Determination-Not Human Subjects Research

Through the answers you provided in response to questions in the Purdue Research Online Portal Exemption Logic (PROPEL), Purdue's HRPP has determined that the research does not qualify as Human Subjects Research under federal human subjects research regulations (e.g., 45 CFR 46).

The answers provided in PROPEL indicate that you will NOT:

- Collect data for the purpose of research intended to create generalizable knowledge. Reasons that are not considered research include purposes such as internal programmatic evaluation, quality improvement, or business analysis.
- Involve Human Subjects by collecting data from a living individual through intervention or interaction with the individual and/or identifiable private information.

What are your responsibilities now, as you move forward?

- If you have further questions about this determination, you must contact the Purdue IRB.
- You and the members of your research team acknowledge that this study is subject to review at any time by Purdue's HRPP staff, Institutional Review Board, and/or Research Quality Assurance unit. At any time, this project may be subject to monitoring by these Purdue entities to confirm the applicability of this determination. The Purdue IRB has final authority in determining if an activity is Human Subjects Research requiring IRB review.
- This determination is the Purdue HRPP assessment of regulations related only to human subjects research protections. This determination does not constitute approval from any other Purdue campus department or outside agency. The Principal Investigator and all researchers are required to affirm that the research meets all applicable local, state, and federal laws that may apply.
- Finally, if any changes occur with respect to this project, recognize that such changes could change the need for review by HRPP/IRB. Should you change the intent of the activity to involve publication, presentation, or any different application of this work, it is likely that IRB review will be required. Therefore, it is important that you again complete PROPEL to ensure that the IRB review requirements remain the same.

Should you have any questions about your rights and responsibilities regarding conducting research with people, on this project or any other, please do not hesitate to contact Purdue's HRPP at irb@purdue.edu. We are here to help!