UNIVERSITY OF NAIROBI

FACULTY OF SCIENCE AND TECHNOLOGY
DEPARTMENT OF COMPUTING AND INFORMATICS

FORENSIC ANALYSIS OF EVERNOTE DATA REMNANTS ON WINDOWS 10

KETER VINCENT
(P53/34987/2019)

SUPERVISOR

DR. ANDREW KAHONGE MWAURA

A project report submitted to the school of computing and informatics in partial fulfillment of the requirements for the degree of Master of Science in Distributed Computing Technology of the University of Nairobi.

DECLARATION

This project is my original work and to the best of my knowledge, this work has not been submitted for any other award in any university.

DATE: 06/12/2022

KETER VINCENT
(P53/34987/2019)

This project report has been submitted in partial fulfillment of the requirements of the Master of Science in Distributed Computing Technology of the University of Nairobi with my approval as the University supervisor.

DATE: 06-12-2022

DR. ANDREW MWAURA KAHONGE
DEPARTMENT OF COMPUTING AND INFORMATICS

DEDICATION

To my wife

and my son without whom this project would have

been completed much earlier.

ACKNOWLEDGEMENT

I am grateful to my supervisor Dr. Andrew Mwaura Kahonge for the direction, instruction, as well as much-needed advice during the undertaking of this project and also to the review panel led by Dr. Muchemi for their devotion and guidance throughout the different project phases. To my classmate, Mr. John Deche and Ms. Selpha Atemba thank you so much for your candid criticisms and word of support.

ABSTRACT

Cloud computing technology is rapidly growing globally and many businesses are starting to adopt cloud computing to leverage the computing power and cost of operation. Therefore, cloud-based storage services are gaining popularity among organizations and people since they provide simplicity in storing and transferring data across several geographical locations at a low cost.

However, with the difficulties in retrieving artifacts of evidential and economic value from cloud providers, cloud storage has become a target for cybercriminals for exploitation. As a result, artifacts from the client's computer might offer valuable evidence on which to build a case.

This study looked into the artifacts left by Evernote, a widely known cloud storage service, on Windows 10. The study used dead and live forensics to identify Evernote artifacts on Windows 10 for several situations such as Evernote install, file upload, file delete, and uninstall. Investigating these leftovers provides digital forensics investigators with a comprehensive grasp of the traces that are likely to persist and their evidential and business value.

The Evernote installer files, link files, browser, registry, prefetch files, and network traffic were identified as possible sources of information throughout the investigation. The traces discovered in the research can help in a criminal probe involving Evernote because they offer valuable information in trying to recreate the crime scene, and establish a chronology of occurrences, as well as knowledge of how to avoid such incidents in the future.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

Cloud computing is a model for providing ubiquitous, easy, on-demand network access to a shared pool of configurable computing (e.g., servers, networks, servers, storage, services and applications) which can be quickly provided and disconnected with minimum overhead or interaction with cloud service providers (Mell and Grance, 2011).

Cloud computing can free users from a number of responsibilities associated with computers and data storage maintenance while also lowering related expenses (Mowbray 2009). The number of cloud-based services (some of which are free) that cater to the specific demands of users is huge and expanding quickly.

Constant demand for computing power and resources, cloud computing has grown in popularity (Simou et al., 2014), ensuring flexibility, dependability, scalability, and lower prices (Pichan,2015). People and corporations are migrating away from existing on-premise information technology infrastructure towards the cloud in order to save money by choosing the less costly operational option for this kind of technology (Ghafarian, 2015).

People generally use the cloud to easily exchange and store files (Ahmed and Li, 2016). Cloud computing crime has grown and developed as a result of the rise of cloud computing platforms (Laurie Lau Y. C. ,2015), which has aided crime. Although cloud technology improves productivity, it is also vulnerable to exploitation by hackers (Biggs and Vidalis, 2009). The advent of cloud computing broadens attack vectors, allowing attackers to exploit holes on such platforms. Because of the cloud's relative isolation, accessibility, and endless processing capability, attackers may carry out such assaults with ease (Pichan et al., 2015).The Sony PlayStation Network assault made use of Amazon's Web Service (Chung et al., 2012).

Cloud storage services are a typical use of cloud computing (Ghafarian, 2015). While cloud storage services are not new, they are becoming increasingly popular (Hu et al, 2010). Cloud storage options available in the cloud marketplace include Google Drive, Evernote, Apple iCloud, etc (Castinglione et al., 2017). Evernote is one of the best-known services for cloud storage (Evernote Review, 2022).

Evernote allows users to save and manage notes, ideas, images, data, and documents from any device at any given time. It works with a variety of operating systems, such as macOS, Windows, iOS and Android. Evernote has two plans: Evernote premium and Evernote free. The free version does not have a cost implication while the premium version costs $5 per month and option of $45 per year. Basic accounts allow users to save up to 25 MB per note or upload up to 60 MB each month. It contains a function that autosaves notes as the user edits them. The upload of a note adds to the user profile, which may then be arranged. A premium account requires a monthly or yearly fee. This bundles up to 100MB of additional storage space per note, allowing 1 GB of uploads per month. You can also invite others to edit your notes and do optical character recognition. It enables searchable documents in PDF and the ability to edit and view Evernote notes without an internet connection. (Evernote, 2021)

Despite advantages of cloud storage, it is still exploited by criminals (Ahmed and Li, 2016). Terrorist actions can lead to cloud storage abuse. In the United States, 14 people were killed and 22 injured in a terrorist attack in San Bernardino in 2015. One of the main culprits of the hack, he stopped iCloud backups months before the event (Cahyani et al., 2016). Cloud storage can be used by cybercriminals to store or share illegal materials, launch botnet attacks (Ahmed et al., 2016), or steal personal information (Chung et al., 2012). Additionally, steganographic techniques can be used to covertly exchange information in such attacks (Caviglione et al. 2016).

Cloud storage raises concerns about cloud storage security and forensic investigations. Data stored in the cloud can be hacked, which is a security concern. A concern in forensics is the difficulty of conducting investigations in the cloud (Ghafarian, 2015). Cloud-based crime poses many obstacles, especially regarding encryption, obscurity, and geolocation (Taylor et al., 2011), all of which make forensic evidence collection and investigation difficult (Guo et al.,2012). Furthermore, jurisdictional issues and lack of international coordination exacerbate the problem (Guo et al, 2012). With the rise of online crime (Damshenas et al., 2012), it is important to use innovative investigative methods to address cloud security and, more broadly, cloud investigation (Guo et al. 2012).

1.1 Background of the Research

Evernote offers storage with unlimited storage, several advanced text editing features, the ability to share notes and web clips with anyone you choose, optical character recognition for reminders, images, and advanced features for organizing and searching your notes. We are proud to be a respected web clipper that offers a great option for your desktop. A version with keyboard shortcuts to speed up your work, integration with third-party applications, compatibility with many platforms, no ads, and two layers of account verification security (Karen, 2014). Windows, on the other hand, prides itself on being the world's most popular desktop operating system, with a 75% market share (Stat Counter, 2022). Growing consumer awareness of Evernote and the Windows OS has led various researchers to forensically investigate Evernote on the Windows operating system.

Analyzed Evernote data remnants (Chung et al, 2012) and their location on Windows XP, Vista, and 7 respectively. The investigation included artifacts on the hard drive. The authors found that Evernote is installed in *%UserProfile%\AppData\Local\Evernote\Databases* for Windows Vista and 7 while for Windows XP *%UserProfile%\LocalSettings\ApplicationData \Evernote\Databases*.

File [user ID]. exb and [UserID]. thumbnails are available in database folders. [UserID].exb contains data such as the title of the note, when the note was created and modified, where the user created the note, and what operating system was used to create the note. You can also identify information about attachments, such as creation time, file name and type.

There are two log files in the logs folder: AppLog_[date].txt and enclipper_[date].txt. AppLog_[Date].txt is created once a day when Evernote is started. This file contains credentials, account IDs, and application start and stop times. The enclipper_[date].txt file is created once a day, similar to AppLog_[date].txt. This file contains the time the application was started.

The Evernote database .exb files and the attachments located in *%UserProfile%\AppData\Local\Evernote\Databases* are not encrypted. The attachment. backup extension if dropped will give access to the files using any program that can open it (Walther, 2016)

1.2 Problem Statement

Cloud storage services provide consumers with storage space that they can use to store and share information. Their use is widespread due to the inclusion of various additional services such as image editing, document editing, playing music and videos, sending emails, etc. Most hosting companies offer a certain amount of free storage space, and users who need more storage space can rent more storage space (Chung et al, 2012).

Cloud-based storage may be misused cybercriminal in accordance to (Ahmed and Li, 2016), and while paired with the problems of obtaining artifacts of evidentiary value from vendors of cloud-based storage (Biggs and Vidalis, 2009), undertaking cloud forensics investigations may need extra time and effort (Taylor et al., 2011). Cloud forensic investigation, on the alternative hand, can depend on artifacts amassed from endpoint device and the cloud company (Guo et al, 2012). Client-aspect artifacts can offer potential proof where artifacts from Cloud company is problematic or hard to get; in that situation, the case may be constructed at the client-aspect artifacts (Taylor et al., 2011). Evernote is one of the famous note-taking programs amongst cloud customers and a famous cloud garage service (Chung et al, 2012) there's a projection of cloud storage growth (Cisco,2018)

21). Windows is the maximum famous computer working device withinside the world, with 75% marketplace share (Stat Counter,2022.). With Microsoft announcing its discontinuation of Windows XP in 2009, Vista in 2012, and 7 in 2020 respectively this means that they are no longer going to provide support, updates, and security patches for its line of operating systems (Microsoft, 2020). Therefore, there is a need to undertake Evernote forensics in Windows 10 which is popularly being used currently across the World. As a result, instances of misuse of Evernote operating on Windows 10 are likely, and it is vital to establish how and where digital evidence may be obtained to aid forensic study of such scenarios (Zatyko and Bay, 2011).

1.3 Research Aim

This research sought to find out the data remnants of Evernote on Windows 10 operating system. The final aim is to find out whatever data remains are left over by Evernote after it is uninstalled from the Windows 10 operating system.

1.4 Research Questions

i. What digital forensic models are employed, and how well do they fit the needs of Evernote forensics?

ii. When Evernote is installed on Windows 10, what registry and file system artifacts does it leave behind?

iii. What artifacts does Evernote leave in the Windows 10 registry and file system after uninstallation?

1.5 Objectives

i. To analyze digital forensic models and their suitability for Evernote forensic on Windows 10 Operating System.

ii. To examine any registry and file system artifacts made by Evernote when installed on Windows Operating System.

iii. To investigate Evernote artifacts left behind on Windows 10 registry and file system after uninstalling, their evidential value to forensic investigators and its implication to business.

1.6 Significance

Finding traces of Evernote artifacts on Windows 10 generates a digital forensic expert's description of the artifacts present and where they were found. Findings show links between artifact locations and the value of evidence for digital forensics examiners while exposing cybercrimes utilizing Evernote on Windows 10 operating system.

1.7 Scope

This investigation was limited to Evernote forensics on the Windows 10 operating system and focused on Evernote artifacts related to application installation, use, and uninstallation on the Windows 10 operating system. The only artifacts evaluated are those found in the registry and file system. Other Evernote artifacts of network traffic and memory can also be examined, but that was outside the scope of this study.

1.8 Limitations and Assumptions

This study made use of open-source tools. As a result, the amount of detail of the recovered artifacts may be restricted by the tools' capabilities. However, this constraint has been partly overcome by employing various tools to obtain the findings. The tools utilized are not likely to jeopardize the integrity of the artifacts established.

CHAPTER TWO

LITERATURE REVIEW

The chapter gives the analysis of the literature reviews, digital forensic approaches as well as cloud storage client application forensics. The first objective of the study was met by doing a literature review, and the third and fourth objectives were achieved by conducting an experiment and discussing the results.

A deeper grasp of the digital forensics process was achieved by examining the literature on digital forensic methodologies, an acceptable methodology for undertaking Evernote forensics in the exploratory research was selected. A careful review of cloud-based storage application forensics during assessment provided a greater understanding of the features of such investigations. Understanding digital forensics concepts was essential from the beginning since it strengthened the research.

2.1 Concepts of Digital Forensics

This concept was scientifically derived from the Digital Forensic Research Workshop (Palmer, 2001) for storing, collecting, verifying, identifying, analyzing, interpreting, documenting, and presenting digital evidence from digital sources to facilitate the reconstruction of an event that turns out to be a crime

2.1.1 Digital Forensics Classification

With cloud adoption, forensic examination may include devices on the client, server or network. The devices for computing might be turned on or off in the process of examination. As an outcome, forensic investigations may be classified based on the device's location on the network and its powered status i.e., on or off

Table 1: Types of Digital Forensics

No.	Category	Description
i.	**Server Forensics**	includes the gathering of artifacts stored on servers. Data may be hosted in various data centers across different geographical regions in highly decentralized and virtualized environments, making identification and collecting of evidence challenging (Pichan et al, 2015). With multi-

		tenancy feature of the cloud, the usual technique of seizing servers may be ineffective since it would affect a whole data center, causing harm to other users (Birk, 2011; Guo et al, 2012).
ii.	**Client Forensics**	comprises recognizing and collecting evidence-relevant items on endpoint devices such as PCs, laptops, phones and tablets (Pichan et al, 2015). On the client side, vital evidence can be uncovered, some of which may be sensitive. As a result, client forensics must be performed (Damshenas et al., 2012). Client forensics has become increasingly difficult due to the increase of client endpoints, particularly mobile endpoints (Ruan et al., 2011).
iii.	**Network Forensics**	is forensics to collect, identify, examine, correlate, analyze, and document digital evidence from multiple sources for the purpose of unearthing facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to these activities (Palmer,2001). Network forensics may also be performed in cloud platforms. The communication protocols used by virtual machines (VMs) can provide the essential information (Pichan et al, 2015). Despite their relevance as forensic artifacts, CSPs often do not offer logs of such communication (Birk, et al, 2011).
iv.	**Dead Forensics**	forensics undertaken on a powered-down system. One advantage of dead forensic is the reduced probability of data alteration. The negatives of dead forensics are data loss and the difficulty of analyzing encrypted disks (Lessing et al, 2008).
v.	**Live Forensics**	is forensics performed on a computer that is turned on.

		Before shutting down the system, real-time system data is gathered in order to ensure preservation of volatile memory, process, and network information that would otherwise be destroyed in normal dead forensic extraction (Grobler et al, 2009). The advantage of live forensics is the ability to capture volatile information and limit the data retrieved to what is relevant. On the downside, the potential for data manipulation is high and the validity and reliability of evidence is difficult to prove (Lessing et al, 2008).

2.2 Characteristics of Digital Evidence

To be admissible in court, digital evidence must meet the five qualities of evidence (Zdziarski, 2008). The following are the five characteristics: **Admissible**

Digital evidence gathering and preservation should be in such a manner that permits it to be utilized in court.

a) Authentic

A forensic examiner's ability to explain its source and the evidence itself should be importance to the case.

b) Complete

Evidence must provide the full picture when it is presented. Evidence supporting both guilt and innocence must be offered.

c) Reliable

The authenticity and integrity of the evidence must be beyond dispute. The methods employed must be reliable and well acknowledged in the industry. By employing the same strategies and practices, the opposing counsel ought to be able to produce comparable outcomes.

d) Understandable and Believable

The judges should be able to easily understand and believe the evidence. A forensic examiner must be able to communicate clearly and precisely.

2.2.1 Sources and types of Digital Evidence

A digital file from an electronic source meet criteria as digital evidence these can be email, instant messaging, text messages, documents recovered from hard drives, files and financial transactions carried out online, video files and audio files.

The following list carries potential digital evidence sources as classified by (Rowlingson, 2004);

i. Accounting packages for evidence of fraud, ERP modules for employee records and activities e.g., case of identity theft, management files and system;
ii. Servers, endpoint devices, portable devices and embedded devices;
iii. Laptops and desktops used for backup and archiving.
iv. Database transactions logs, Internet traffic, access logs, Internal network logs, printer logs, web traffic, commercial transactions and;
v. Door access records, recorded messages, CCTV phone logs, telco records, PABX data, and network records, call center logs or monitored phone calls make as other sources of digital evidence.
vi. Intrusion Detection Software, Packet sniffers, content checkers and keyboard loggers

Digital evidence can be classified into two categories;

a) Inculpatory evidence that backs up existing hypotheses, facts, and ideas. This brings the suspect closer to the crime scene.
b) Exonerating evidence contradicts previously established hypotheses, statistics, and ideas. This absolves the suspect of the offense.

All gathered data must be evaluated and classified in order to find both types of evidence (Carrier, 2003). The need for additional inference or reasoning from the evidence is another angle to consider. According to this theory, evidence can be either;

- Circumstantial evidence - needs a judge to undertake an indirect judgment, or interpretation on what occurred. or
- Direct evidence - finds a fact and doesn’t take an assumption.

A rough picture of what occurred is given by circumstantial evidence but does not provide absolute proof. Although direct evidence like victim and witness accounts have an implication on how evidence is interpreted and the chain of events recreated, digital forensic evidence is typically speculative (Lyle, 2019).

2.3 Models for Digital Forensics

Methods for investigations and digital evidence in a law court must both be proven accurate (Pichan et al, 2015). Limited prosecution has been the result of improper procedures (Kohn, Eloff, and Eloff, 2013). Digital forensics models can be used to represent both implicit and explicit processes that are necessary for a sound forensic inquiry (Grobler et al, 2009). There have been several models and frameworks for the digital forensic process established, five of them have been discussed below:

i. The Digital Forensic Analysis Cyclic Model is iterative and cyclical as stated by (Quick and Choo, 2013). The phases of the model are; start, prepare and respond, identify and collect, preserve, analyze, present, feedback, and complete.

ii. McKemmish model, which consists of identification, preservation, analysis, and presentation phases in a linear order (McKemmish, 1999).

iii. Digital Forensic Research Conference Workshop (DFRWS) came up with digital investigative model which has the following phases of *identification, preservation, collection, examination, analysis, and presentation* as stated by (Palmer, 2001).

iv. According to (Kent et al., 2006) the NIST Forensic Model has 4 phases which are; collection, examination, analysis and reporting phases

v. The Integrated Digital Forensic Process Model also known abbreviated as IDFPM, has the following steps that includes *preparation, incident, incident response, physical investigation, digital forensic investigation, and presentation*. The authors propose a standard digital forensic model, a uniform procedure, and common terms in this model (Kohn et al., 2013).

vi. Integrated Conceptual Digital Forensic Framework for Cloud Computing, has the following phases: Evidence source identification and preservation; Collection; Examination and analysis; and Reporting and Presentation (Martini and Choo, 2012).

From the above analyzed models, The McKemmish model was picked for this research and used to undertake the investigation. This digital forensic methodology typically consists of four phases, listed below. This gives confirmation that evidence gathered and analyzed is admissible in a law court (McKemmish, 1999):

a. At the identification phase, it is important to be aware of the evidence's presence, where it resides and the format is stored in. The criticality is because it aids the investigator in choosing the techniques and procedures to employ in the evidence acquisition process.
b. Preservation phase guarantees evidence is retained as near its state of originality as is practicable. The evidence shouldn't be changed but, if need be, any modifications need to be explained and supported.
c. Digital data must be extracted, processed, and interpreted as part of the analysis phase in the investigation process. This is a very important stage in the investigation process.
d. The Presentation Phase involves giving out the analyzed evidence to the court of law or the client in respect to the investigation undertaken by the forensic examiner.

2.4 Cloud Storage Forensics Analysis

2.4.1 Cloud Storage Service

Cloud storage provision elasticity and scalability in storage, which may be provided as a service through the internet (Harnik et al., 2010). Cloud storage services can be thought of as infrastructure as a service as it gives a user access to storage space as well as extra features like document and picture editing, audio and video playback, and email sending.

The cloud storage service can be accessed in a variety of ways, including installing software on a mobile device or accessing the cloud storage service using a web browser on a personal computer.

The following are some examples of companies that host cloud storage: Google Drive, Microsoft OneDrive, Adrive, SugarSync, etc. Key advantages of a cloud storage service are reliability, availability, ease of retrieval, and information sharing, which allows users to share their data with reputable third parties at any time and from any device (Seghrouchni et al ,2009).

Most users put their trust in the cloud service provider’s security mechanisms. Like any other new technology cloud storage services are exposed to attack posed by cyber criminals, these platforms have to be forensically analyzed. A classic example is the online data breach in 2011 involving abuse of Amazon Cloud Servers by hackers which brought down the Sony PlayStation Network.

2.4.2 Cloud Forensics

According to (Pichan et al, 2015) investigation of an incident in cloud computing platforms is broken into three categories: server, client, and network forensics according to. Undertaking cloud forensics can be either at the client end or the server end (Mehreen et al, 2015). Server end forensics presents several limitation or challenges such as, global positioning geographically and the jurisdiction, this makes getting access to artifacts hard. Another challenge is that, artifacts are not immediately traceable (Ahmed et al, 2016). Information that is likely to remain in Windows Operating System for instance is lost in a cloud setup when the user exit which would have kept in the virtualized environment. As an outcome, the number of artifacts which are found are minimal. Furthermore, when analyzing the flow of events, many machines may be participating in a transaction. Such challenges show the significance of client forensics in addition to server forensics.

Server-side forensics' technological and non-technical obstacles do not entirely impede (Chung et al., 2012) such investigations, as evidence of criminal action on the client's device may be revealed. As an outcome, (Ahmed et al, 2016) examiners should find the location and kind of artifact traces in the devices of cloud-based users. Client evidence (Birk and Wegener, 2011) and especially the cloud service client agent should never be overlooked in cloud environment forensic analysis.

Syncing of endpoint devices with storage in the cloud creates traces on the clients' devices (Mehreen and Aslam, 2015). Collecting out of client side, on the other hand, may not supply all of the essential data artifacts. In SaaS services, for example, clients are not usually the primary source of data. A stored version of the information which may be partial or out of date is maintained (McCulley et al, 2016). As a result, this evidence should be reinforced with evidence from network or server forensics wherever feasible. Examiners are nonetheless enthusiastic in the client 's side as evidence gathered from user devices can assist solidify the issue under inquiry. Furthermore, if acquiring information from the cloud provider is challenging, such evidence would be relevant (Taylor et al., 2011).

2.5 Windows Evernote Forensics

Evernote a note taking application, provides users with a synchronized storage service using cloud servers, where they can save and organize their notes, ideas, photos, documents, and data from any device at any time they would need. Multiple operating systems supports Evernote, including , MacOS , iOS , Windows, and Android (Evernote Review, 2022). The increased use of Evernote and windows operating system has made examiners to undertake investigations on Evernote running on windows operating systems

With Evernote, user can store an idea from any location at any time given time (Chung et al., 2012). Evernote autosaves notes each time they are edited. Users can login to their storage via Android smartphones, Windows systems, iPhones and Mac systems. Evernote usage on a Windows system results in creation of four folders in the following paths;

Table 2:Evernote Folders Location

Path	**Operating System**
%UserProfile%\LocalSettings\ApplicationData\Evernote\Evernote\Logs	Windows XP Logs
%UserProfile%\LocalSettings\ApplicationData\Evernote\Evernote \Databases	Windows XP Databases
%UserProfile%\AppData\Local\Evernote\Evernote\Logs	Windows Vista/7 logs
%UserProfile%\AppData\Local\Evernote\Evernote\Databases	Windows Vista/7 Evernote Databases

The logs and database folders are significant. It really easy to locate the contents of files because they utilize the SQLite database format and text. The files [userID].exb and [userID].exb thumbnails exist in the database folder. [userID].exb comprises of details like the title of the note, the times at which the note was created and modified, the location where the user created the note, and the type of operating system that created the note. Additionally, attached documents can be identified, through the creation time, file name and type.

The file [userID].exb.thumbnails is a combination of PNG files that take a snapshot of the note during synchronization. Extracting each .PNG file, we can know the history of note revisions.

There are two log files in the logs folder: AppLog_[Date].txt and enclipper_[Date].txt. After Evernote has been launched, AppLog_[Date].txt is created one time in a day. The file carries authentication information, the account ID, also times at which the application was launched and closed. File enclipper_[Date].txt is created one time a day, like AppLog_[Date].txt. The file comprises the time at which the application was launched.

With Microsoft announcing its discontinuation of Windows XP in 2009, Vista in 2012, and 7 in 2020 respectively this means that they are no longer going to provide support, updates, and security patches for its line of operating systems (Microsoft, 2020). Therefore, there is a need to undertake Evernote forensics in Windows 10 which is popularly being used currently globally.

2.6 Gap

The Evernote analysis on Windows XP and 7 does not give complete artifacts in the registry and other artifacts associated with Evernote usage (Chung et al., 2012). The author doesn't explain in details the registry changes that occur when Evernote is installed and when uninstalled. Also, the author does not specify the artifacts left behind when Evernote is uninstalled in windows. An experimental investigation into the artifacts produced during the; installation of Evernote, use of Evernote, and uninstallation of the Evernote client program on Windows 10 Operating System is necessary to close these gaps.

2.7 Conceptual Framework

Figure 1's conceptual framework illustrates how virtual machines were set up and the procedures used to create them. According to the studied literature, different user actions including installing Evernote, uploading files, deleting files, and uninstalling Evernote leave behind various data remains on the client PC. Both live and dead forensics were used to investigate the artifacts that were present in these instances. Virtual machines were built specifically for each circumstance and their snapshots were examined for dead forensics. Tools for analysis were installed and utilized to examine each situation for live forensics. To preserve the status of each stage of the study during live analysis, snapshots were taken. The control virtual machine served as a baseline for Evernote in both dead and live analyses.

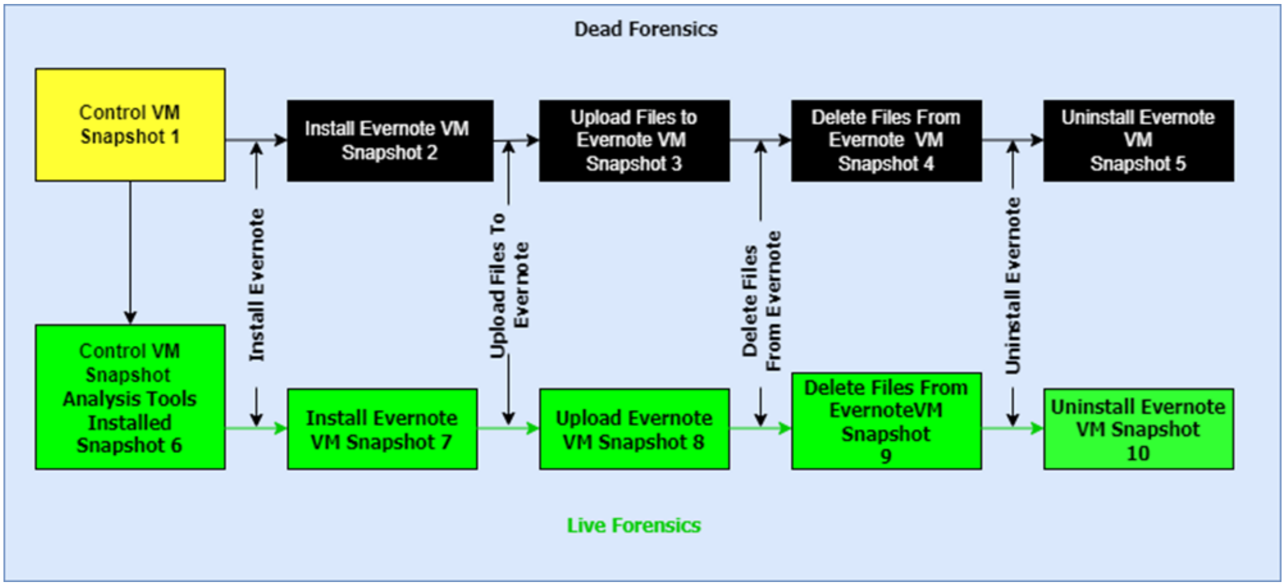

Dead Forensics
Control VM Snapshot 1
Install Evernote VM Snapshot 2
Upload Files to Evernote VM Snapshot 3
Delete Files From Evernote VM Snapshot 4
Uninstall Evernote VM Snapshot 5
Install Evernote
Upload Files To Evernote
Delete Files From Evernote
Uninstall Evernote
Control VM Snapshot Analysis Tools Installed Snapshot 6
Install Evernote VM Snapshot 7
Upload Evernote VM Snapshot 8
Delete Files From EvernoteVM Snapshot 9
Uninstall Evernote VM Snapshot 10
Live Forensics

Figure 1:Conceptual framework

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter explains the philosophical paradigm used, research design used, how data was collected and analyzed, the design limitations, and data collection and analysis methods.

3.1 Philosophy

Research philosophies influenced research questions, the interpretation of findings and project methodology.

As seen in Figure 2, well-considered assumptions create a convincing research philosophy that informs the methodology, research plan, data collecting methodologies, and analytic processes employed (Saunders et al, 2016).

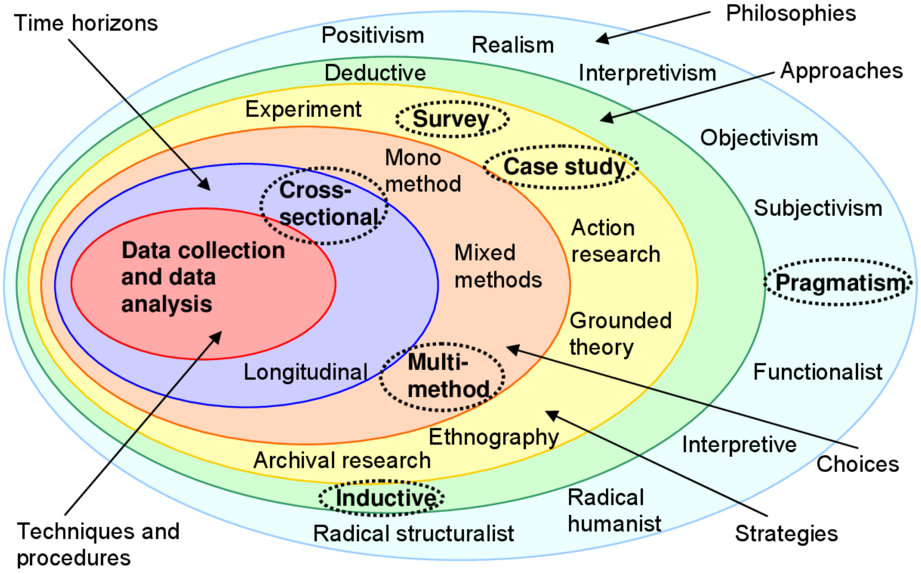


Figure 2: Research plan (Saunders et al. (2007)

3.2 Research Design

An experiment defined as a strategy in investigating effect and the cause relationships with the aim of proving or disproving a causal connection between a factor and an outcome (Oates, 2006). The experiment was carried out in a laboratory setting, with the variables to be controlled. These controls were necessary in ensuring the changes seen came as a result of installing, using, and uninstalling Evernote.

The research was exploratory with the goal of investigating Evernote artifacts left behind after uninstallation. The goal was to investigate the artifacts created during Evernote installation and then narrowing it down to the artifacts left behind after Evernote was uninstalled. As a result, an experimental research design was employed to find out such artifacts.

Experiments are normally based on hypothesis which is testable, disproved or approved based on the observed outcome (Oates, 2006). The Null hypothesis (H0) means that the independent variable does not affect dependent variable while the Alternative hypothesis (Ha) means that the independent variable affects dependent variable. For this research the two hypotheses were drawdown as follows;

- Null Hypothesis(H0) That is, Evernote doesn't leave behind any artifacts on Windows 10 Operating System after uninstalling.
- Alternative Hypothesis (Ha) to imply that after uninstalling Evernote, artifacts remain on Windows 10 Operating System.

3.3 Target Population and Sample Size

This research target population was the virtual machines created for both live forensic and dead forensic digital evidence. (Taherdoost, 2016). The sample size was 10 virtual machines snapshots for both categories; 5 virtual machine snapshots for dead and another 5 virtual machine snapshots for live forensics.

3.4 Collection of Data

Experiment data for the research came from the virtual machine snapshots configuration. The Applications listed in Table 1 below were used for the experiment.

Table 3: Applications Used in the Experiment

No.	Application	Software Version	Details
1.	Oracle VM VirtualBox	6.1 r152435	Hypervisor used to host the Virtual Machines Created.
2.	Windows 10 Pro	21H2 Build 19044.1288	The Operating System for Virtual Machines
3.	Evernote Windows Desktop Application	10.48.4	Evernote Application installed on windows 10 operating system.

4.	Access Data - FTK Imager Application	4.7.1.2	Creating Images of the VM Snapshots.
5.	Regshot	1.9.0	An open-source (LGPL) registry compare utility which allows user quickly take a snapshot of the registry and then compare it with a second one.
6.	Mirekusoft Install Monitor	2.0.300	For Applications' file and registry changes monitoring.
7.	Process_Monitor	3.9.2	Used for monitoring registry, file system, and process or thread activities.
8.	Process_Explorer	17.01	shows information about which handles and DLLs processes have opened or loaded.
9.	GlassWire	2.3	Used to monitor network connections.
10.	SQLite Database Browser	3.12.2	Used to read database (.exb) files
11.	HxD	2.5.0.0	Used to find file hex
12.	Saferoom	2.2.0	Decrypting Evernote files
13.	Recuva	1.53	To recover deleted files
14.	Autopsy	4.19.3	To analyze virtual machines images.
15.	Registry Explorer	1.6.0.0	Used to explore the registry files.

Generally acknowledged rules, standards, and processes must be followed while doing digital forensics (Mehreen and Aslam, 2015). The four steps of digital evidence as follows; identification, preservation, analysis, and presentation were used in this forensic inqury experiment (McKemmish, 1999) to ensure that the experiment followed a laid down methodology as discussed in the literature review chapter.

3.4.1 Initial Preparation

Signing up for Evernote requires an email address. Evernote.com was signed up using the email address that was generated. After signing up, an Oracle VM VirtualBox Windows 10 Pro 64-bit Virtual Machine was created as well as user account and email address was generated. To obtain the most recent features and security patches, Windows was updated and the updates paused for 7 days to avoid further changes on the registry and file system of the Control VM. This was critical for dead forensics.

Table 4:Dead Forensics Virtual Machines

Snapshot No/s	**Virtual Machines Created**	**Details**
Snapshot No.1	Control -VM	Requirements: Windows 10 Pro 64 Bit, 4GB RAM and 50 GB Hard Disk Storage.
Snapshot No. 2	Install Evernote -VM	After installing the Evernote Desktop Application.
Snapshot No. 3	Uploaded Files to Evernote-VM	After files are uploaded to Evernote Application
Snapshot No.4	Files Deleted from Evernote -VM	After files are deleted from Evernote Application
Snapshot No. 5	Evernote Uninstalled-VM	Uninstalling Evernote using the Control Panel in Windows OS

Oracle VM VirtualBox produced a VMDK file and VMEM file for every snapshot it took, which correspond to the associated virtual machine's hard drive and memory, respectively. The VMDK files were recognized as potential sources of digital evidence for the inquiry, and Access Data-FTK Imager addressed the collection of forensic images of the snapshot for use in dead forensic examination.

Snapshots of live forensics (Snapshots No.6 to No. 10) obtained from Snapshot No. 1: Control VM. Snapshot No.6: Analysis Tools Installed VM was created after installing Glasswire, Regshot, Process Explorer Mirekusoft Install Monitor, Process Monitor, SQLite Database Browser, Saferoom, and Recuva.

Table 5: Live Forensics Virtual Machines

Table 5: Live Forensics Virtual Machines

Snapshot No/s	**Virtual Machines Created**	**Details**
Snapshot No.1	Control -VM	Requirements: Windows 10 Pro 64 Bit, 4GB RAM and 50 GB Hard Disk Storage.
Snapshot No. 6	Analysis Tools Installed - VM	Install analysis tools
Snapshot No. 7	Evernote Installed – VM	After installation of Evernote
Snapshot No. 8	Files uploaded - VM	After files have been created i.e., Uploaded File.pdf and Deleted File.pdf
Snapshot No. 9	Deleted Files from Evernote -VM	After documents are deleted from the Evernote
Snapshot No. 10	Uninstall Evernote - VM	After Evernote is uninstalled using the Windows Programs and Features.

A registry, according to (Carvey, H., 2005), can be characterized as a log file since it contains data that a forensic examiner can retrieve. The accompanying key values are known as the "Lastwrite" time, which is preserved as a FILETIME and is thought to indicate the file's last modification time. When working with files, it is typically hard to determine a specific date and time of files modification; however, the Lastwrite reveals when such registry was last changed.

During Evernote installation, the analysis tools i.e Glasswire, Regshot, Process Explorer, Mirekusoft Install Monitor, and Process Monitor were used to view the network connections as well as modifications on the file system and registry. Registry snapshot was taken using Regshot prior to installing Evernote. Evernote was then installed, and the modifications were documented. Registry snapshot was taken using RegShot application after installation of Evernote and a comparison of the two-registry files was undertaken, modifications on the registry files were noted. Snapshot No.7: Evernote Installed was created as a snapshot of the VM.

To analyze changes during the file upload process, two files were submitted to the Evernote App. Network traffic and file system modifications were tracked. Snapshot No.8: Files Uploaded (to

Evernote) was created as a snapshot of the VM. A file was erased from the Evernote App to analyze changes caused by file deletion. In the process, tools for analysis were employed view network traffic and changes made in the file system. Snapshot No. 9: Files Deleted (from Evernote) was created as a snapshot of the VM.

Analysis tools were initiated during Evernote uninstallation to view network connections and changes made in the filesystem including the registry. A registry snapshot was taken before uninstalling Evernote using Regshot to document the registry status. A second snapshot obtained using Regshot, was used to compare the changes made to the registry when Evernote was uninstalled. Snapshot No.10: Evernote Uninstalled was taken and named.

Virtual machines were used over physical hard drives because they can be quickly (Mehreen et al, 2015) put-up and divergent configurations examined without reconfiguring them. Virtual machines was made up with minimal RAM and storage.

Less configurations reduces the amount of space needed for the virtual machines and forensic copies generated throughout the study period. Secondly, time is reduced for analyzing the experiment results. Finally, if meaningful data can be obtained on a small setup, equivalent artifacts are more likely to occur in larger systems (Quick and Choo, 2013).

Furthermore, Halboob et al., 2015) show that VM snapshots are useful in cloud research.

3.4.2 Digital Evidence Identification Phase

The snapshots files of the Virtual Machine Disk were located and identified as with artifacts required for dead forensic analysis. These files were important for investigating forensic artifacts in dead forensics.

3.4.3 Digital Evidence Preservation Phase

Analysis on a forensic copy is required for digital forensic inquiry (McKemmish,2008). The analysis software Access Data FTK Imager was needed to take images of the virtual machines created in order to preserve the evidence. To do this, forensic images of the Virtual Machine Har disk (VMDK) files were created using E01 extension format, the choice is because of its in-built checksum capability for confirming the integrity of the images acquired for forensic analysis.

E01 format is acknowledged in the forensic field as a standard recommended in the industry for forensic image storage (Lyons, 2016). VMDK images' integrity were validated using computation of their hashes and comparing them to those of their origin.

3.4.4 Digital Evidence Analysis Phase

Images were examined using Access Data-FTK Imager and Autopsy Application to determine Evernote data traces that remained in the registry and file system. Attempts were made to retrieve files that were deleted after the uninstallation of Evernote. GlassWire, Mirekusoft Install Monitor, Process Explorer, SQLite Database Browser, Registry Editor, Process Monitor, Regshot, Recuva, and Saferoom were all utilized for live forensic analysis.

3.4.5 Digital Evidence Reporting Phase

The findings of the experiment include Evernote changes noted while installing evernote, during usage plus data traces left behind in registry and the file system after Evernote uninstallation. This project report discusses the importance of the findings to forensic investigators.

3.5 Analysis of the Data

The data involved in the experimental study was qualitative. The artifacts such as registry entries, files system artifacts, directory structures were analyzed qualitatively. Qualitative data are often rich and holistic and with a high potential for uncovering complexity (Miles et al, 2014).

A crucial part of this investigation is the value of Evernote artifacts identified by forensic investigators. As a result, interpretations of what these meant were formed from the beginning of data collection by noticing patterns, explanations, causal processes, and assertions (Miles et al 2014).

3.6 Research Limitations

The experiment undertaken included two types of forensics live which risks data tampering and dead forensics which does not assure collection of volatile data i.e network and memory (Lessing et al, 2008). The limitation of each forensic type was complimented by performing live and dead forensics. The tools used for the experiment had limitations in capability and couldn't collect the necessary data. To remedy this, several software was put in use, and the data retrieved were utilized in establishing the entire evidence.

Forensic images of the VMs were made to address issues of VMs contamination while undertaking the experiment. These images were store away from the experiment copy and in case of a mistake while undertaking the experiment a copy would be made from the clean stored image, this was for dead forensic. Snapshots were taken for the live forensic and in case of a mistake a restore of the snapshot would be undertaken.

3.7 Research Ethics Considered

According to (Oates,2006) while conducting research ethics must be upheld to ensure no harm or risk to the participants and the researcher. This research was conducted ethically from data acquisition, data analysis and final reporting of the results.

Objectivity was attained in data collection by gathering data properly and completely while eliminating subjectivity in what was gathered. Other issues throughout this period were participants' privacy, secrecy, and anonymity (Miles et al, 2014).

While there were no human participants, the study was carried out using a fresh Evernote account and linked email address. As a result, no existing Evernote user account or client account data was impacted. It is vital to maintain impartiality undertaking analysis in order to maintain the dependability of the data gathered (Saunders, 2016). The integrity of the data was protected by reporting it accurately and completely.

CHAPTER FOUR

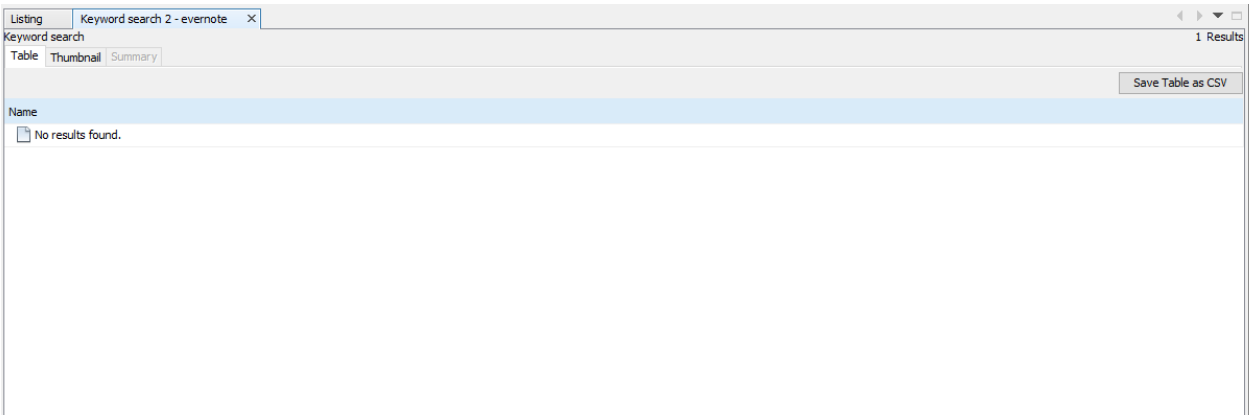
RESULTS AND DISCUSSION

The research scope was limited to the registry and the file system artifacts linked to user activities in the Evernote Forensics such as Evernote installation, uploading of files to Evernote, deletion of files from Evernote and uninstallation of Evernote from Windows 10 Operating System. The second and the third objectives are discussed in this Chapter 4 of the project report. The two objectives are as follows respectively; Objective Two: To examine any registry and file system artifacts made by Evernote on installation to Windows 10 Operating System while Objective Three: To examine Evernote artifacts left behind on Windows 10 registry and file system after uninstalling, their evidential value to forensic investigators and its implication to business.

The rest of the chapter details the artifacts connected to every user activity and the value in Evernote's forensic examination. The artifacts involved with the Evernote installation are addressed first. Thereafter, artifacts discussion about the upload and deletion of files on Evernote. Finally, artifacts left behind after uninstalling Evernote are analyzed, followed by a chapter conclusion.

4.1 Image Analysis of the Control VM

Control-VM image was analyzed and a keyword search for 'Evernote' did not return any results which confirmed that there were no data about evernote.demo2@gmail.com and Evernote files. It should be therefore noted that Evernote does not exist or no related files exist before installation of Evernote in windows 10.



Keyword search

1 Results

Name

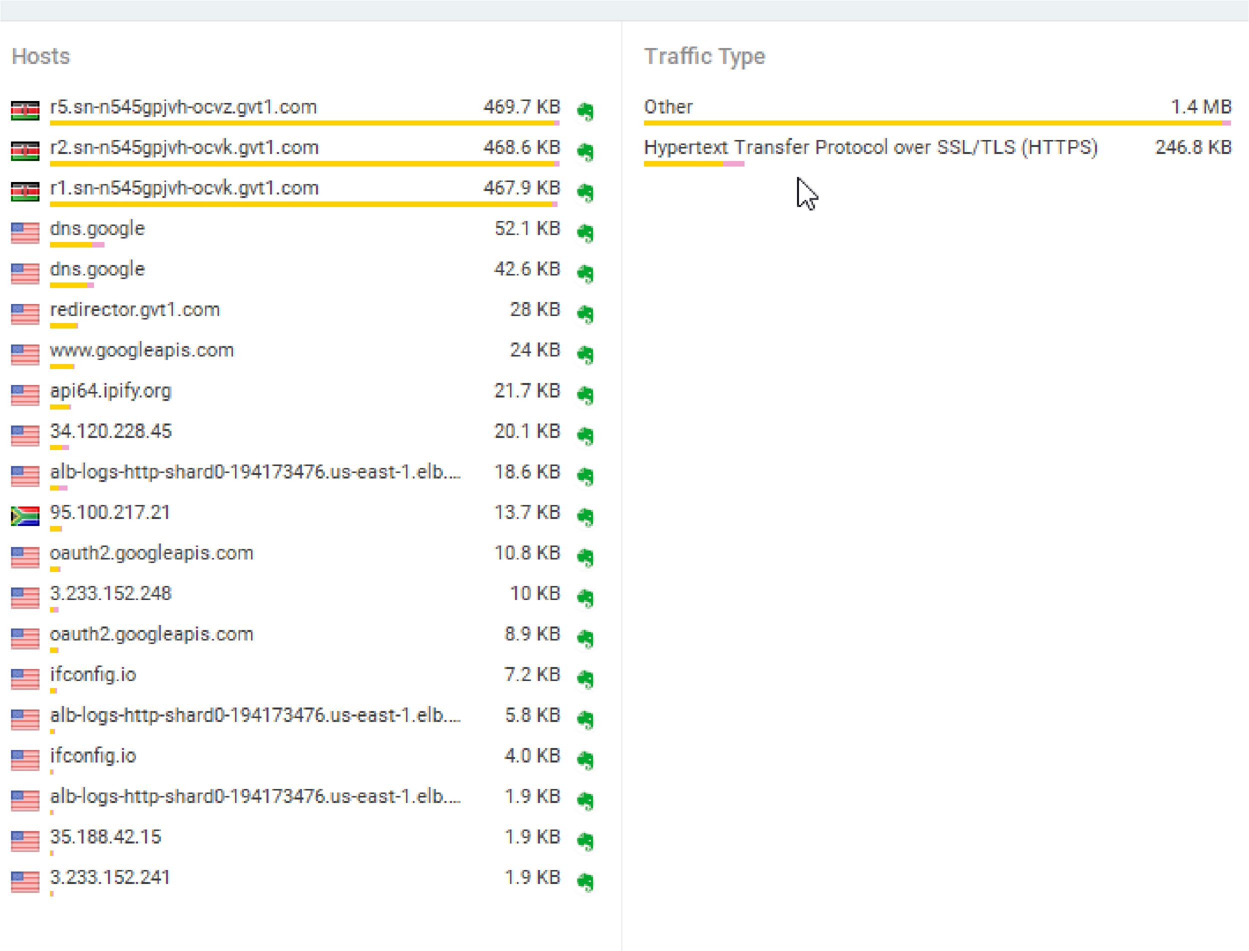
No results found.

Figure 3:Artifacts with Evernote reference in Control VM

4.2 Installation of Evernote

Evernote artifacts created while installating Evernote were identified via analysis of the Evernote Install-VM image using dead and live forensics. While installing Evernote, the program makes HTTPS calls to dns.google.com, redirector.gvt1.com, and numerous other subdomains, as seen in Figure 4.

Because HTTPS is a secure protocol (Cheng et al, 2011), it may be presumed that data is safely exchanged. The traffic is exchanged by the Evernote between the desktop application and the web server.

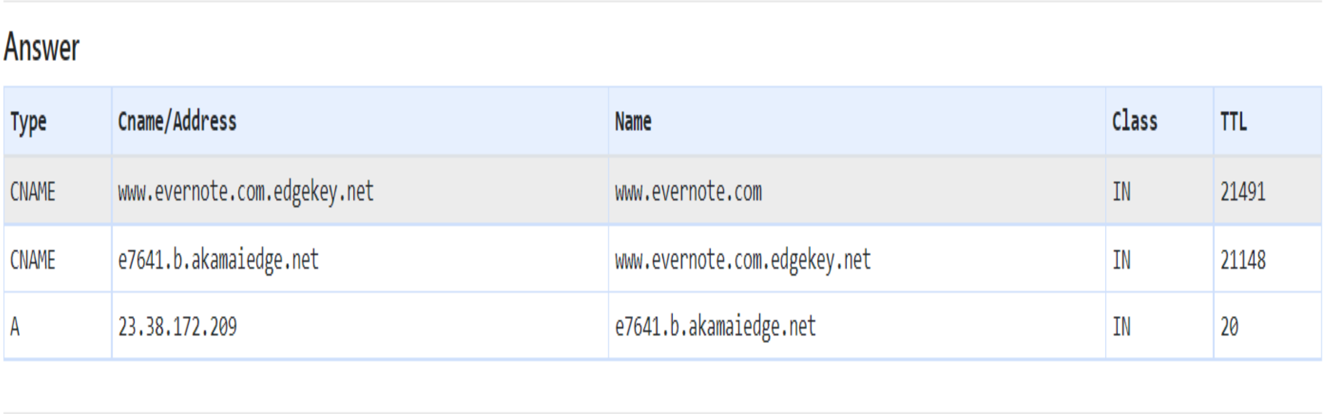


Hosts	
r5.sn-n545gpjvh-ocvz.gvt1.com	469.7 KB
r2.sn-n545gpjvh-ocvk.gvt1.com	468.6 KB
r1.sn-n545gpjvh-ocvk.gvt1.com	467.9 KB
dns.google	52.1 KB
dns.google	42.6 KB
redirector.gvt1.com	28 KB
www.googleapis.com	24 KB
api64.ipify.org	21.7 KB
34.120.228.45	20.1 KB
alb-logs-http-shard0-194173476.us-east-1.elb....	18.6 KB
95.100.217.21	13.7 KB
oauth2.googleapis.com	10.8 KB
3.233.152.248	10 KB
oauth2.googleapis.com	8.9 KB
ifconfig.io	7.2 KB
alb-logs-http-shard0-194173476.us-east-1.elb....	5.8 KB
ifconfig.io	4.0 KB
alb-logs-http-shard0-194173476.us-east-1.elb....	1.9 KB
35.188.42.15	1.9 KB
3.233.152.241	1.9 KB

Traffic Type	
Other	1.4 MB
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	246.8 KB

Figure 4:Network Activities While Installing Evernote

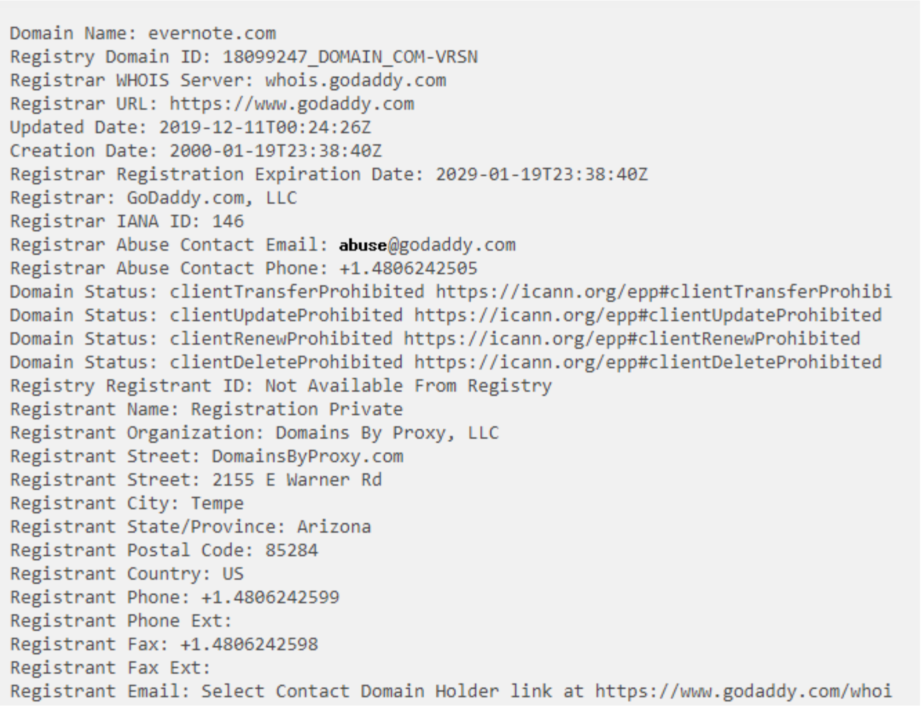
The IP address 23.38.172.209 from the DNS Lookup shows that Evernote is registered under Evernote Corporation, in Arizona USA. As a result, when obtaining evidence from the Cloud Service Provider, investigators must contact Evernote and comply with US relevant legislation because the firm is based in the US. DNS Look Up reveals www.evernote.com.edgekey.net and e7641.b.akamaiedge.net which is canonical name records used by evernote.com, i.e., *www.evernote.com.edgekey.net* redirects to *e7641.b.akamaiedge.net*, which points to IP address 23.38.172.209. The IP address appearance in the domain names and the network traffic in browsers ***might alert investigators to the presence of Evernote activity on the client system.***



Answer

Type	Cname/Address	Name	Class	TTL
CNAME	www.evernote.com.edgekey.net	www.evernote.com	IN	21491
CNAME	e7641.b.akamaiedge.net	www.evernote.com.edgekey.net	IN	21148
A	23.38.172.209	e7641.b.akamaiedge.net	IN	20

Figure 5: Domain IP Address for Evernote



```
Domain Name: evernote.com
Registry Domain ID: 18099247_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2019-12-11T00:24:26Z
Creation Date: 2000-01-19T23:38:40Z
Registrar Registration Expiration Date: 2029-01-19T23:38:40Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whoi
```

Figure 6:Domain Registration Information for Evernote

4.2.1 Artifacts Analysis of File System

4.2.1.1 Analysis of the Browser

The download activities of Evernote, including online searches for Evernote, Evernote URLs browsed, and Evernote cookies, could be observed within the browser, as illustrated.

In addition, the artifacts include the timestamps as well as accounts used to open Evernote, which can be utilized to establish a sequence of events that is capable of tying the suspect to the crime.

A search for keyword evernote.demo2@gmail.com shows trace on the location C:\Users\vketer\AppData\Local\Package\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC!\MicrosoftEdge\User\Default1\Recovery\Active\{A5B61BB7-2182-4DE1-97A2-3B0AB5B394C6}.dat linked to evernote.com account log via Google OAuth. The path of the artifact had Microsoft Edge, pointing to utilization of browser in accessing Evernote through Google OAuth.

4.2.1.2 Installation Directories

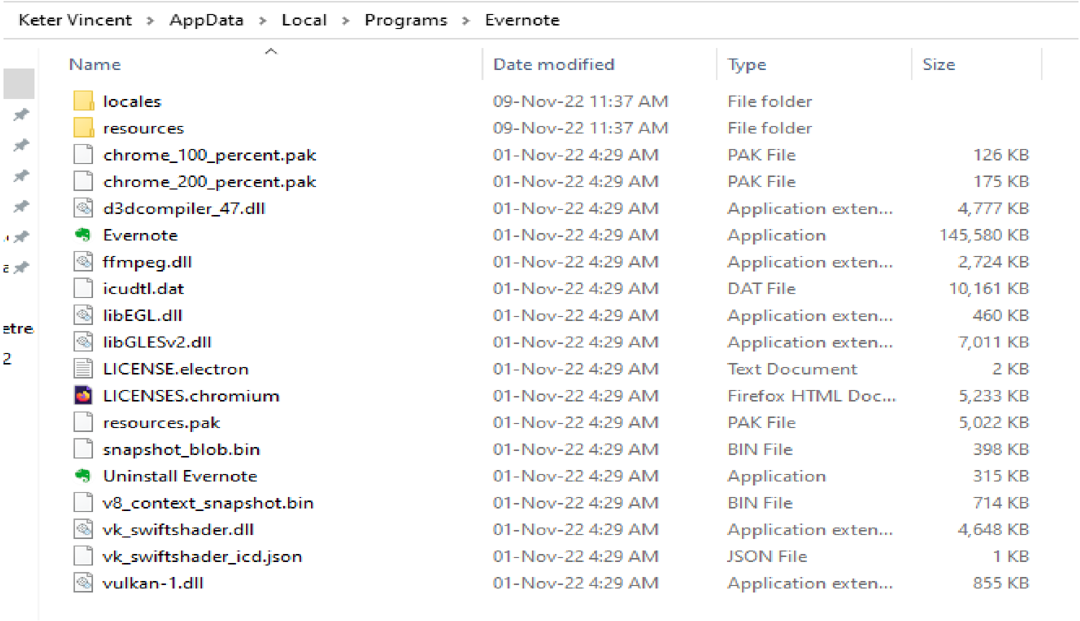
Evernote install setup could be traced in the following path C:\Users\vketer\Downloads\Evernote-10.48.4-win-ddl-ga-3760-5f4dcc5719-setup. During Evernote installation, program execution files were placed in several directories such as C:\Users\vketer\AppData\Local\Programs\Evernote and Windows directories. Evernote program folder contained files such as Evernote.exe, UninstallEvernote and several .dll relating to executing, updating, and uninstalling the Evernote application.

4.2.1.3 AppData

The AppData folder has three (3) subfolders: Local, LocalLow, and Roaming. Data and settings for Windows apps or programs are kept locally. The Local retains data exclusive to a single machine and it doesn't synchronize between computers even within domain, least trusted programs utilize LocalLow folder since its security settings is limiting. The folder for Roaming contains information which permits user in domain to move between computers (Hoffman, 2017).

Evernote had data in all three folders, namely Local, LocalLow, and Roaming. Files and directories seen in Fig.7. were present in C: Users\vketerAppData\Local\Programs\Evernote. Many .dat and

.dll , which would typically be encrypted SQLite and plaintext respectively were discovered in the folder. However, this is not necessarily the case (Picasso, 2017), since these data might as well be Base64 encoded.



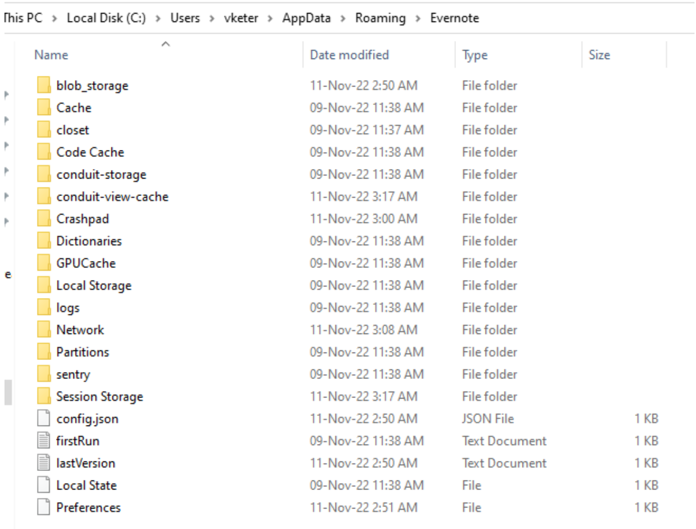
Keter Vincent > AppData > Local > Programs > Evernote

Name	Date modified	Type	Size
locales	09-Nov-22 11:37 AM	File folder	
resources	09-Nov-22 11:37 AM	File folder	
chrome_100_percent.pak	01-Nov-22 4:29 AM	PAK File	126 KB
chrome_200_percent.pak	01-Nov-22 4:29 AM	PAK File	175 KB
d3dcompiler_47.dll	01-Nov-22 4:29 AM	Application exten...	4,777 KB
Evernote	01-Nov-22 4:29 AM	Application	145,580 KB
ffmpeg.dll	01-Nov-22 4:29 AM	Application exten...	2,724 KB
icudtl.dat	01-Nov-22 4:29 AM	DAT File	10,161 KB
libEGL.dll	01-Nov-22 4:29 AM	Application exten...	460 KB
libGLESv2.dll	01-Nov-22 4:29 AM	Application exten...	7,011 KB
LICENSE.electron	01-Nov-22 4:29 AM	Text Document	2 KB
LICENSES.chromium	01-Nov-22 4:29 AM	Firefox HTML Doc...	5,233 KB
resources.pak	01-Nov-22 4:29 AM	PAK File	5,022 KB
snapshot_blob.bin	01-Nov-22 4:29 AM	BIN File	398 KB
Uninstall Evernote	01-Nov-22 4:29 AM	Application	315 KB
v8_context_snapshot.bin	01-Nov-22 4:29 AM	BIN File	714 KB
vk_swiftshader.dll	01-Nov-22 4:29 AM	Application exten...	4,648 KB
vk_swiftshader_icd.json	01-Nov-22 4:29 AM	JSON File	1 KB
vulkan-1.dll	01-Nov-22 4:29 AM	Application exten...	855 KB

Figure 7:Folders & Files - AppData\Local\Programs/Evernote

Several files utilized on the previous Evernote versions were not available. Files likes for example [userID].exb, [userID].exb thumbnails and [userID].exb, did not exist.

In C:\Users\vketer\AppData\Roaming\Evernote logs storage folder could be located as seen in Figure 8 below;



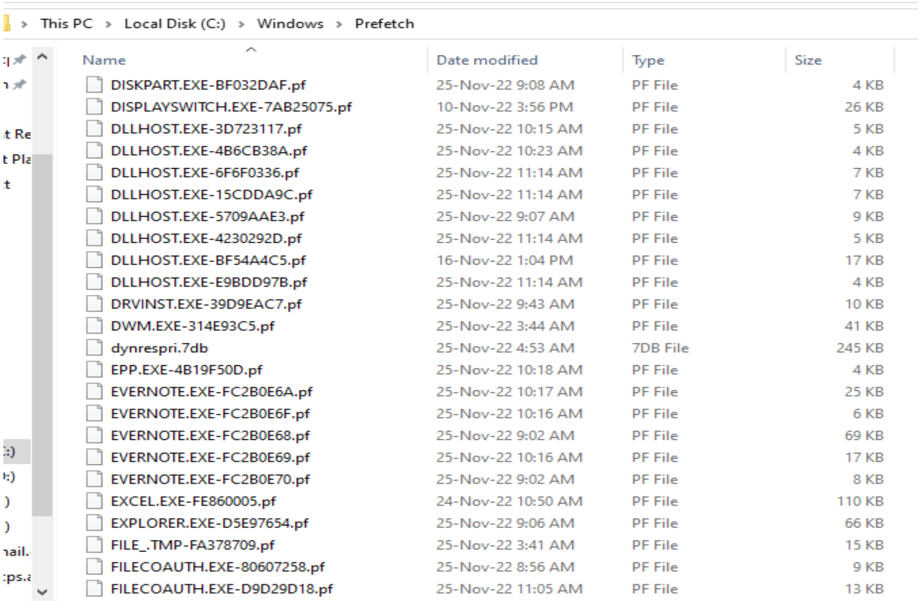
This PC > Local Disk (C:) > Users > vketer > AppData > Roaming > Evernote

Name	Date modified	Type	Size
blob_storage	11-Nov-22 2:50 AM	File folder	
Cache	09-Nov-22 11:38 AM	File folder	
closet	09-Nov-22 11:37 AM	File folder	
Code Cache	09-Nov-22 11:38 AM	File folder	
conduit-storage	09-Nov-22 11:38 AM	File folder	
conduit-view-cache	11-Nov-22 3:17 AM	File folder	
Crashpad	11-Nov-22 3:00 AM	File folder	
Dictionaries	09-Nov-22 11:38 AM	File folder	
GPUCache	09-Nov-22 11:38 AM	File folder	
Local Storage	09-Nov-22 11:38 AM	File folder	
logs	09-Nov-22 11:38 AM	File folder	
Network	11-Nov-22 3:08 AM	File folder	
Partitions	09-Nov-22 11:38 AM	File folder	
sentry	09-Nov-22 11:38 AM	File folder	
Session Storage	11-Nov-22 3:17 AM	File folder	
config.json	11-Nov-22 2:50 AM	JSON File	1 KB
firstRun	09-Nov-22 11:38 AM	Text Document	1 KB
lastVersion	11-Nov-22 2:50 AM	Text Document	1 KB
Local State	09-Nov-22 11:38 AM	File	1 KB
Preferences	11-Nov-22 2:51 AM	File	1 KB

Figure 8:Files - AppData\Roaming\Evernote

4.2.1.4 Prefetch Files

Useful information is found in prefetch files (Quick et al., 2014) that help in determining the first time launch of a program and the last time, the location the program was ran, and the files executed during that running of the application. *C:\Windows\Prefetch* contained Evernote prefetch files.



Name	Date modified	Type	Size
DISKPART.EXE-BF032DAF.pf	25-Nov-22 9:08 AM	PF File	4 KB
DISPLAYSWITCH.EXE-7AB25075.pf	10-Nov-22 3:56 PM	PF File	26 KB
DLLHOST.EXE-3D723117.pf	25-Nov-22 10:15 AM	PF File	5 KB
DLLHOST.EXE-4B6CB38A.pf	25-Nov-22 10:23 AM	PF File	4 KB
DLLHOST.EXE-6F6F0336.pf	25-Nov-22 11:14 AM	PF File	7 KB
DLLHOST.EXE-15CDDA9C.pf	25-Nov-22 11:14 AM	PF File	7 KB
DLLHOST.EXE-5709AAE3.pf	25-Nov-22 9:07 AM	PF File	9 KB
DLLHOST.EXE-4230292D.pf	25-Nov-22 11:14 AM	PF File	5 KB
DLLHOST.EXE-BF54A4C5.pf	16-Nov-22 1:04 PM	PF File	17 KB
DLLHOST.EXE-E9BDD97B.pf	25-Nov-22 11:14 AM	PF File	4 KB
DRVINST.EXE-39D9EAC7.pf	25-Nov-22 9:43 AM	PF File	10 KB
DWM.EXE-314E93C5.pf	25-Nov-22 3:44 AM	PF File	41 KB
dynrespri.7db	25-Nov-22 4:53 AM	7DB File	245 KB
EPP.EXE-4B19F50D.pf	25-Nov-22 10:18 AM	PF File	4 KB
EVERNOTE.EXE-FC2B0E6A.pf	25-Nov-22 10:17 AM	PF File	25 KB
EVERNOTE.EXE-FC2B0E6F.pf	25-Nov-22 10:16 AM	PF File	6 KB
EVERNOTE.EXE-FC2B0E68.pf	25-Nov-22 9:02 AM	PF File	69 KB
EVERNOTE.EXE-FC2B0E69.pf	25-Nov-22 10:16 AM	PF File	17 KB
EVERNOTE.EXE-FC2B0E70.pf	25-Nov-22 9:02 AM	PF File	8 KB
EXCEL.EXE-FE860005.pf	24-Nov-22 10:50 AM	PF File	110 KB
EXPLORER.EXE-D5E97654.pf	25-Nov-22 9:06 AM	PF File	66 KB
FILE_.TMP-FA378709.pf	25-Nov-22 3:41 AM	PF File	15 KB
FILECOAUTH.EXE-80607258.pf	25-Nov-22 8:56 AM	PF File	9 KB
FILECOAUTH.EXE-D9D29D18.pf	25-Nov-22 11:05 AM	PF File	13 KB

Figure 9:Evernote Prefetch Files

4.2.1.5 Link Files

Files related to Evernote found located in Desktop and in the StartMenu. The two files referenced to evernote.exe in the Program Files directory, which was used to launch the program.

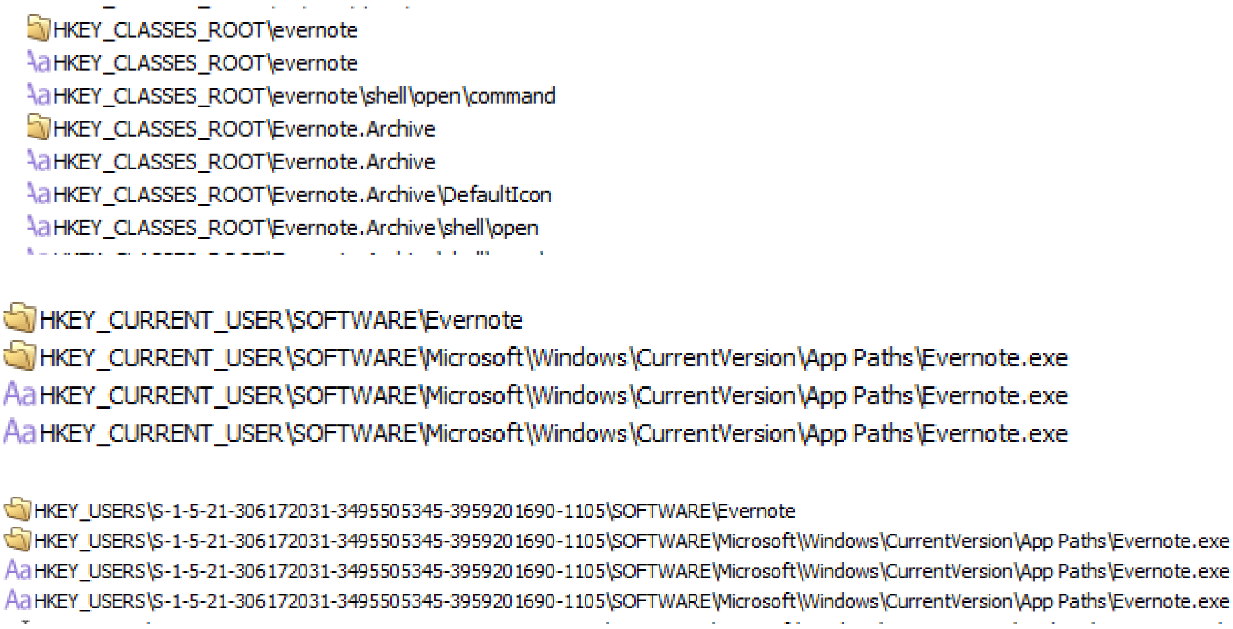
4.2.2 Registry Artifacts

Evernote version, installation path, and installation time were all stored in the registry.

Evernote artifacts were located in the registry hives, HKEY_Users, HKEY_Current_User and HKEY_Classes _Root

4.2.2.1 Directory Structure Artifacts

Evernote registry file's location and the installation path were identified, as shown in figure 10 below;



```
HKEY_CLASSES_ROOT\evernote
HKEY_CLASSES_ROOT\evernote
HKEY_CLASSES_ROOT\evernote\shell\open\command
HKEY_CLASSES_ROOT\Evernote.Archive
HKEY_CLASSES_ROOT\Evernote.Archive
HKEY_CLASSES_ROOT\Evernote.Archive\DefaultIcon
HKEY_CLASSES_ROOT\Evernote.Archive\shell\open

HKEY_CURRENT_USER\SOFTWARE\Evernote
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Evernote.exe
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Evernote.exe
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Evernote.exe

HKEY_USERS\S-1-5-21-306172031-3495505345-3959201690-1105\SOFTWARE\Evernote
HKEY_USERS\S-1-5-21-306172031-3495505345-3959201690-1105\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Evernote.exe
HKEY_USERS\S-1-5-21-306172031-3495505345-3959201690-1105\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Evernote.exe
HKEY_USERS\S-1-5-21-306172031-3495505345-3959201690-1105\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Evernote.exe
```

Figure 10:Registry Directory Structure Artifacts in EvernoteInstall-VM

4.2.2.2 Evernote Configuration Settings Artifacts

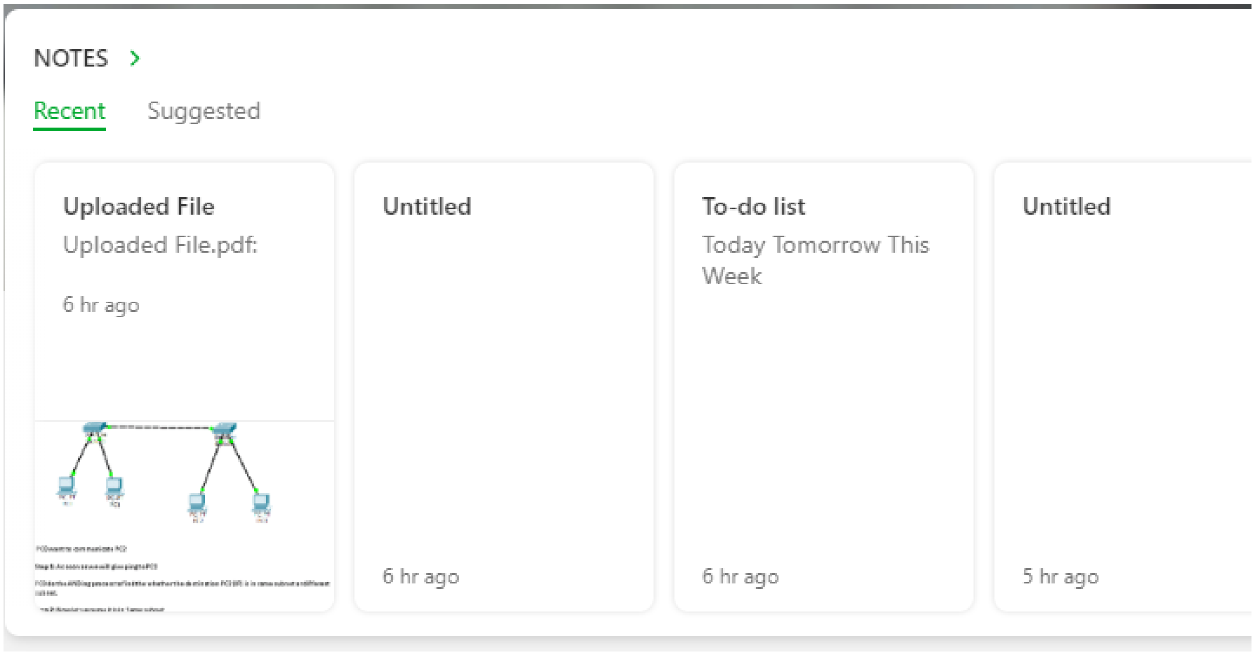
There were configuration settings discovered, such as launching Evernote on system startup and content playback.

4.2.2.3 Database Artifacts

Evernote Corporation seems to have undertaken more steps in securing the application since the database files are no longer located in the same place that other research has replicated.

4.3 File Upload on Evernote

Live forensics and the dead forensic analysis of the Upload VM image were performed to investigate artifacts produced during file Upload File.pdf posted and deleted.pdf files were uploaded to the Evernote app. Time is logged immediately the files are uploaded to Evernote web server, as seen in Figure 11 below.



NOTES >

Recent Suggested

Uploaded File
Uploaded File.pdf:
6 hr ago

Untitled
6 hr ago

To-do list
Today Tomorrow This Week
6 hr ago

Untitled
5 hr ago

Figure 11: Files Uploaded in Evernote for Live Forensics

The presence of the identical files, as well as the timestamps at which they were generated, accessed, and edited, was disclosed by analyzing the Upload-VM image. Investigators would benefit from the information in ascertaining the documents in Evernote server, which would be requested from Evernote Corporation to confirm client's side obtained documents.

Furthermore, the timestamps would aid in determining when the files were produced, edited, or accessed, as well as creating a chronology of occurrences.

4.4 File Deletion on Evernote

To discover and recover files that were deleted by a user, examination of the deleted files in Evernote -VM image was undertaken using Autopsy. The data was successfully recovered. It illustrates the feasibility of retrieving deleted Evernote files uploaded by a user from the client PC.

4.5 Uninstallation of Evernote

The final phase in the experiment evaluated the outcome of user activity in uninstalling the Evernote application using the control panel section of Windows 10. The Evernote Uninstallation-VM image was subjected to both live and dead forensic examination. Both tests revealed the traces of data remains in registry and file system of Windows 10.

4.5.1 Artifacts Analysis of the File System

4.5.1.1 Analysis of the Browser

Download activities of the Evernote, including online searches for Evernote, Evernote URLs browsed, and Evernote cookies, could still be traced within the browser. In addition, the Artifacts included timestamps and Evernote user account used to access it, which could help in piecing up chronology of occurrences which tie culprit to crime scene.

A search for keyword evernote.demo2@gmail.com found results C: Users\vketer\AppData\Local\Packages\Microsoft.MicrosoftEdge8wekyb3d8bbwe\AC\#!001\MicrosoftEdgeCacheRSU55P3Kpkg linked to the user details used in signing in to evernote account via Google OAuth.

The artifact path contains Microsoft Edge, implying that the browser was used to sign in to Evernote using Google OAuth.

4.5.1.2 Directories of Installation

The Evernote install setup could still be traced in the folder for Downloads. The was as follows directory C: Users\vketer\Downloads. Using a keyword search, the Evernote-10.48.4-win-ddl-ga-3760-5f4dcc5719-setup folder and .dll files highlighting Evernote location in the directory of Program Files. The AppData directory included log files linked to Evernote updates, which could be retrieved via Autopsy despite being reported as deleted. An 'Evernote' keyword search yielded references to an Evernote folder and other files under the AppData directory.

Other artifacts revealed were swapfile.sys,

$Extend/$UsnJrnl: $J, $LogFile, $MFT, $Recycle.Bin/S-1-5-21- 3933750032-3930657141-318433956-1001/$RPMOD0U.txt, Config.Msi/254f877.rbs, Config.Msi/254f877.rbs-slack

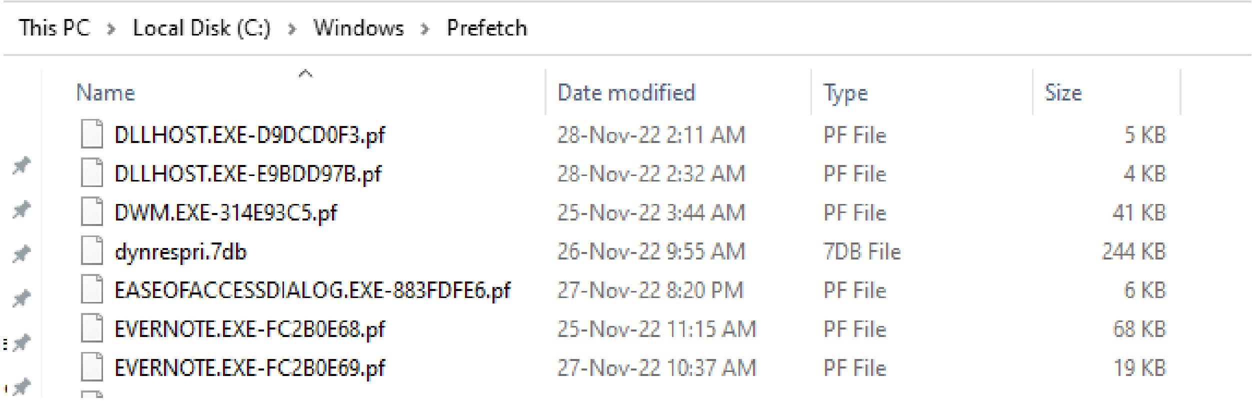
These artifacts provided information on Evernote logs, updates, link files and files in recycle bin.

4.5.1.3 AppData

Database files for the Evernote were located in C:\Users\vketer\AppData\Roaming\Evernote\Partitions\user%3A237852125\databases. Evernote folder could be located in AppData\Roaming directory of the Windows File System.

4.5.1.4 Prefetch Files

Evernote Prefetch files were found within the windows file system as shown in figure 12 below;



This PC > Local Disk (C:) > Windows > Prefetch

Name	Date modified	Type	Size
DLLHOST.EXE-D9DCD0F3.pf	28-Nov-22 2:11 AM	PF File	5 KB
DLLHOST.EXE-E9BDD97B.pf	28-Nov-22 2:32 AM	PF File	4 KB
DWM.EXE-314E93C5.pf	25-Nov-22 3:44 AM	PF File	41 KB
dynrespri.7db	26-Nov-22 9:55 AM	7DB File	244 KB
EASEOFACCESSDIALOG.EXE-883FDFE6.pf	27-Nov-22 8:20 PM	PF File	6 KB
EVERNOTE.EXE-FC2B0E68.pf	25-Nov-22 11:15 AM	PF File	68 KB
EVERNOTE.EXE-FC2B0E69.pf	27-Nov-22 10:37 AM	PF File	19 KB

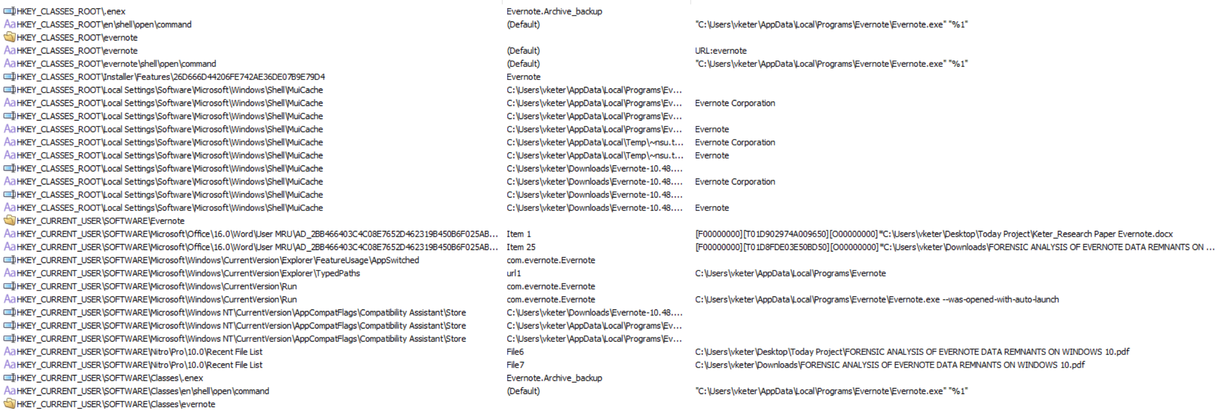
Figure 12:Evernote Prefetch Files After Uninstallation

4.5.1.5 Link Files

The word was 'evernote.lnk' searched and it yielded results such as $MFT and NTUSER.DAT. Further examination revealed they contained data on path to the Evernote Application in program files.

4.5.2 Registry Artifacts

Evernote's uninstallation left registry traces in the HKey_Classes_Root and HKey_Classes_User hives. As demonstrated in Figures 13, the registry values remaining included the ones for Evernote service, updating, and uninstalling. Evernote user values found in the registry when installing were also present.



HKEY_CLASSES_ROOT\.enex	Evernote.Archive_backup	
HKEY_CLASSES_ROOT\en\shell\open\command	(Default)	"C:\Users\vketer\AppData\Local\Programs\Evernote\Evernote.exe" "%1"
HKEY_CLASSES_ROOT\evernote		
HKEY_CLASSES_ROOT\evernote	(Default)	URL:evernote
HKEY_CLASSES_ROOT\evernote\shell\open\command	(Default)	"C:\Users\vketer\AppData\Local\Programs\Evernote\Evernote.exe" "%1"
HKEY_CLASSES_ROOT\Installer\Features\26D666D44206FE742AE36DE07B9E79D4	Evernote	
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\AppData\Local\Programs\Ev...	
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\AppData\Local\Programs\Ev...	Evernote Corporation
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\AppData\Local\Programs\Ev...	
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\AppData\Local\Programs\Ev...	Evernote
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\AppData\Local\Temp\~nsu.t...	Evernote Corporation
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\AppData\Local\Temp\~nsu.t...	Evernote
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\Downloads\Evernote-10.48....	
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\Downloads\Evernote-10.48....	Evernote Corporation
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\Downloads\Evernote-10.48....	
HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Users\vketer\Downloads\Evernote-10.48....	Evernote
HKEY_CURRENT_USER\SOFTWARE\Evernote		
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\User MRU\AD_2BB466403C4C08E7652D462319B450B6F025AB...	Item 1	[F00000000][T01D902974A009650][O00000000]*C:\Users\vketer\Desktop\Today Project\Keter_Research Paper Evernote.docx
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\User MRU\AD_2BB466403C4C08E7652D462319B450B6F025AB...	Item 25	[F00000000][T01D8FDE03E50BD50][O00000000]*C:\Users\vketer\Downloads\FORENSIC ANALYSIS OF EVERNOTE DATA REMNANTS ON ...
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched	com.evernote.Evernote	
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths	url1	C:\Users\vketer\AppData\Local\Programs\Evernote
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	com.evernote.Evernote	
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	com.evernote.Evernote	C:\Users\vketer\AppData\Local\Programs\Evernote\Evernote.exe --was-opened-with-auto-launch
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store	C:\Users\vketer\Downloads\Evernote-10.48....	
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store	C:\Users\vketer\AppData\Local\Programs\Ev...	
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store	C:\Users\vketer\AppData\Local\Programs\Ev...	
HKEY_CURRENT_USER\SOFTWARE\Nitro\Pro\10.0\Recent File List	File6	C:\Users\vketer\Desktop\Today Project\FORENSIC ANALYSIS OF EVERNOTE DATA REMNANTS ON WINDOWS 10.pdf
HKEY_CURRENT_USER\SOFTWARE\Nitro\Pro\10.0\Recent File List	File7	C:\Users\vketer\Downloads\FORENSIC ANALYSIS OF EVERNOTE DATA REMNANTS ON WINDOWS 10.pdf
HKEY_CURRENT_USER\SOFTWARE\Classes\.enex	Evernote.Archive_backup	
HKEY_CURRENT_USER\SOFTWARE\Classes\en\shell\open\command	(Default)	"C:\Users\vketer\AppData\Local\Programs\Evernote\Evernote.exe" "%1"
HKEY_CURRENT_USER\SOFTWARE\Classes\evernote		

Figure 13:Registry Artifacts in EvernoteUninstalled-VM

4.6 Conclusion

Chapter 4 of this project located artifacts resulting from the examination of the registry and the file system of Windows 10 and their importance to forensic examiners. Directory structures artifacts , Domain artefacts for Evernote, , configuration settings of Evernote, Evernote user details and browser artifacts all were examined. Files deleted manually by the user or by uninstalling Evernote might be retrieved. Evernote data remains when uninstalled from Windows 10, according to live and dead forensic research. As a result, the Null Hypothesis: Evernote Artifacts are not left behind on Windows 10 Operating System after uninstalling proposed in Chapter 3: Research Methodology was not regarded to be true and therefore not considered.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

The goal of this research was to undertake an Evernote forensic examination of the data traces in windows OS 10. This involved analyzing the registry and the file system artifacts of Evernote in Windows OS 10 to find out the finer details of the leftover data within the operating system that can be of evidential value to the forensic investigators. The objectives of the research were as follows; To analyze digital forensics models and their appropriateness for Evernote forensics, to examine any registry file system and artifacts made by Evernote when it was installed on Windows OS 10 and examine Evernote artifacts left behind on Windows OS 10 registry and file system when uninstalled, their evidential value to forensic examiners and its implication to business.

The first objective of this research examined digital forensics models and the suitability in Evernote forensics. Attaining of the goal was by conducting a literature review in Chapter 2.The following models were analyzed; Integrated Conceptual Digital Forensic Framework, IDFPM, Digital Forensic Analysis Cyclic Model, Digital Investigative Process (DIPM), , McKemmish Model and The NIST Forensic Model. Because of the standard forensic procedure of identification, preservation, analysis and presentation McKemmish Model was used in the experiment research. This model has also been employed in the majority of the earlier studies on Evernote and other cloud storage forensics.

Second objective; to examine any registry and file system artifacts made by Evernote when installed on Windows OS 10. Evernote windows forensics literature analysis was initially performed in determinining likely areas that the artifacts can be found. Following that, dead and live forensics for Evernote was undertaken on Windows 10 to identify these artifacts. Discovery was made which shows Evernote generates file system artifacts such as Evernote application files, , link-files, browser cookies, prefetch files, and the history of the browser etc. Entries pertaining to Evernote installation time, configuration settings, user keys and installation folders were discovered in the registry.

Objective number three was to look into the Evernote Artifacts that were left behind on the Windows 10 file system and registry after uninstalling, as well as their evidential and business value to forensic investigators. To determine probable sources of the Artifacts, an analysis of the literature on Evernote forensics in Windows was undertaken first, as was the second objective.

Following that, dead and live forensics analysis was performed on the Windows 10 Operating System during Evernote uninstallation. File system had Evernote traces, including prefetch files, installation files, files deleted, user-uploaded, link-files, history of browsing and cookies. Among other things, the registry contains artifacts relating to the Evernote service, updates, uninstallation, and user keys.

5.1 Recommendations: Evidential and Business Value of the Artifacts

The study brought out the evidential value of the artifacts found in the experiment to forensic investigators. Forensic investigations can use these artifacts to; discover the time of installation of Evernote in the suspect machine, find out whether Evernote was installed in the suspect computer, draw the Evernote user details such as the email address, account classification also the login account for windows used to login to Evernote, discover documents uploaded to Evernote App, recover documents deleted from the Evernote App and confirm whether the Evernote App was installed at any given time in the suspect computer. While also the artifacts can be of value to businesses, they can use them; to comprehend perpetrators of crime by tying them to the crime, discover data breach and lost information and the extent of damage and reduce the potential of experiencing costly cyberattacks in the future.

5.2 Contributions to Research and Knowledge

The experiment contributed to forensics for Evernote by providing information pertaining to artifacts associated with recent versions of Evernote, namely version 10.48.5 on Windows 10 Operating System. The following issues were highlighted in this study; artifacts made by when installing Evernote on Windows OS 10, Evernote leftovers in Windows OS 10 Operating System after uninstalling, configuration files and configuration files not in use. The study further expanded on prior research by (Chung et al, 2012) by looking at the Evernote registry artifacts left over after uninstalling.

This analysis pinpointed the location and relevance of artifacts that may be utilized to investigate Evernote-related cybercrime. Evernote subscription, account type, email address, account login details and account for windows used to login to the Evernote service were identified as artifacts that may be utilized to connect a suspect to the crime scene. Furthermore, this study revealed files erased by a culprit might be restored. The timeline of events is a crucial part of any criminal inquiry. This study supplied time-related artifacts such as file timestamps, i.e., the updated, accessed, and created times of the artifacts reported, as well as the Evernote time of installation. Timestamps of the artifacts found can be utilized in reconstructing not the crime scene and the sequence of events.

5.3 Future Research

Decrypting Evernote encrypted database files proved difficult, as mentioned in the prior section. Future studies should look towards decrypting these files because they contain vital information. Random Access Memory (RAM) and network traffic can offer relevant evidence if further research is undertaken in the two areas as they offer alternative sources of artifacts. This project focused on the file system and registry of Windows 10 Operating System.

REFERENCES

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing.*

Pearson, S., Shen, Y., & Mowbray, M. (2009, December). *A privacy manager for cloud computing. In IEEE International Conference on Cloud Computing (pp. 90-106). Springer, Berlin, Heidelberg.*

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014, June). *Cloud forensics: identifying the major issues and challenges. In International conference on advanced information systems engineering (pp. 271-284). Springer, Cham.*

Caviglione, Luca & Wendzel, Steffen & Mazurczyk, Wojciech. (2017). *The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security and Privacy Magazine. 15. 10.1109/MSP.2017.4251117.*

Laurie Lau Y. C. (2015). *Cybercrime in the cloud: Risks and responses in Hong Kong, Singapore. The Cloud Security Ecosystem, 17–35. https://doi.org/10.1016/B978-0-12-801595-7.00002-1*

Zdziarski, J. (2008). *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets. In Google Books. "O'Reilly Media, Inc." https://books.google.co.ke/books?id=R1XArTHPn9QC&lpg=PR7&ots=_iwHl6Kxqq&dq=iPhone%20Forensics%20by%20Jonathan%20Zdziarski&lr&pg=PR7#v=onepage&q=iPhone%20Forensics%20by%20Jonathan%20Zdziarski&f=false*

Rowlingson, R. (2004). *A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence Winter, 2(3). https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf*

Hine, Karen. (2014). Evernote. *Journal of the Canadian Health Libraries Association. 35. 41-43.*

Ahmed, A. A., and Li, C. X. (2016) *'Locating and Collecting Cybercrime Evidence on Cloud Storage: Review', in 2016 International Conference on Information Science and Security (ICISS), pp. 1–5. doi: 10.1109/ICISSEC.2016.7885861.*

Biggs, S. and Vidalis, S. (2009) *'Cloud Computing: The Impact on Digital Forensic Investigations', in 2009 International Conference for Internet Technology and Secured Transactions, (ICITST), pp. 1–6. DOI: 10.1109/ICITST.2009.5402561.*

Birk, D., and Wegener, C. (2011) '*Technical Issues of Forensic Investigations in Cloud Computing Environments, in 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 1–10. doi: 10.1109/SADFE.2011.17.*

Cahyani, N. D. W. et al. (2016) *'The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Apps', in Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (MobiMedia '16), pp. 199–204. Available at: http://dl.acm.org/citation.cfm?id=3021385.3021421.*

Carrier, B. (2003) *'Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers', International Journal of Digital Evidence, 1(4).*

Castiglione, L. et al. (2017) *'Covert Channels in Personal Cloud Storage Services: The Case of Dropbox', IEEE Transactions on Industrial Informatics, 13(4), pp. 1921–1931. doi:10.1109/TII.2016.2627503.*

Cisco (2018) *'Cisco Global Cloud Index: Forecast and Methodology, 2016–2021'. Available at: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf.*

Damshenas, M. et al. (2012) '*Forensics investigation challenges in cloud computing environments, in Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 190–194. DOI: 10.1109/CyberSec.2012.6246092.*

Grobler, M. and Solms, S. von (2009) *'A Best Practice Approach To Live Forensic Acquisition', in Fourth International Workshop on Digital Forensics & Incident Analysis.*

Guo, H., Jin, B., and Shang, T. (2012) *'Forensic Investigations in Cloud Environments', in 2012 International Conference on Computer Science and Information Processing (CSIP), pp. 248–251. doi: 10.1109/CSIP.2012.6308841.*

Hoffman, C. (2017) *What Is the AppData Folder in Windows? Available at: https://www.howtogeek.com/318177/what-is-the-appdata-folder-in-windows/ (Accessed: 13 May 2020).*

Hu, W., Yang, T., and Matthews, J. N. (2010) *‘The Good, the Bad and the Ugly of Consumer Cloud Storage’, SIGOPS Oper. Syst. Rev. New York, NY, USA: ACM, 44(3), pp. 110–115. D*

Kent, K. et al. (2006) ‘Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology.

Kohn, M. D., Eloff, M. M. and Eloff, J. H. P. (2013) *‘Integrated Digital Forensic Process Model’,*

Computers & Security, 38, pp. 103–115. DOI: https://doi.org/10.1016/j.cose.2013.05.001.

Lessing, M. and Solms, B. von (2008) *‘Live Forensic Acquisition as Alternative to Traditional Forensic Processes ’. Available at: https://www.imf-conference.org/imf2008/IMF2008-06_Live Forensic Acquisition as Alternative to Traditional Forensics - Marthie Lessing.pdf.*

Lyle, D. P. (2019) *Forensics for Dummies. Second Edi.*

Lyons, B. (2016) *‘Disk Image Content Model and Metadata Analysis. Harvard Library.*

Martini, B. and Choo, K.-K. R. (2012) ‘*An Integrated Conceptual Digital Forensic Framework for Cloud Computing, Digital Investigation, 9(2), pp. 71–80. DOI: https://doi.org/10.1016/j.diin.2012.07.001.*

McKemmish, R. (1999) *‘What is Forensic Computing? ’, Trends and Issues in Crime and Criminal Justice. Australia: Australian Institute of Technology, pp. 1–6. Available at: http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf.*

McKemmish, R. (2008) *‘When is Digital Evidence Forensically Sound? BT - Advances in Digital Forensics IV’, in Ray, I. and Shenoi, S. (eds). Boston, MA: Springer US, pp. 3–15.*

Mehreen, S. and Aslam, B. (2015) *‘Windows 8 Cloud Storage Analysis: EvernoteForensics’, in 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 312–317. doi: 10.1109/IBCAST.2015.7058522.*

Miles, M. B., Huberman, A. M. and Saldaña, J. (2014) *'Qualitative Data Analysis: A Methods Source Book'.*

Chung, Hyunji & Park, Jungheum & Lee, Sangjin & Kang, Cheulhoon. (2012). *Digital Forensic Investigation of Cloud Storage Services. Digital Investigation. 9. 81–95. 10.1016/j.diin.2012.05.015.*

Oates, B. J. (2006) *Researching Information Systems and Computing.*

Palmer, G. (2001) *'A Road Map for Digital Forensic Research, in The Digital Forensic Research Conference.*

Picasso, F. (2017) *'Brush up on EvernoteDBX Decryption', ZENA FORENSICS. Available at: http://blog.digital-forensics.it/2017/04/brush-up-on-dropbox-dbx-decryption.html.*

Pichan, A., Lazarescu, M. and Soh, S. T. (2015) *'Cloud Forensics: Technical Challenges, Solutions, and Comparative Analysis', Digital Investigation. Elsevier, 13, pp. 38–57. DOI: 10.1016/J.DIIN.2015.03.002.*

Quick, D. and Choo, K.-K. *Future Generation Computer Systems, R. (2013a) 'Digital Droplets: Microsoft SkyDrive Forensic Data Remnants'. North-Holland, 29(6), pp. 1378–1394. DOI: 10.1016/J.FUTURE.2013.02.001.*

Saunders, M., Lewis, P., and Thornhill, A. (2016) *Research Methods for Business Students. Simou, S. et al. (2014) 'Cloud Forensics: Identifying the Major Issues and Challenges, in Jarke,M. et al. (eds) International Conference on Advanced Information Systems Engineering. Cham: Springer International Publishing, pp. 271–284.*

Taylor, M. et al. (2011) '*Forensic Investigation of Cloud Computing Systems', Network Security*

Zatyko, K. and Bay, J. (2011) *'The Digital Forensics Cyber Exchange Principle. Available at: https://www.forensicmag.com/article/2011/12/digital-forensics-cyber-exchange-principle.*

Harnik, D., Pinkas, B., & Shulman-Peleg, A. (2010). *Side Channels in Cloud Services: Deduplication in Cloud Storage. IEEE Security & Privacy Magazine, 8(6), 40–47. https://doi.org/10.1109/msp.2010.187*

Seghrouchni, Amal & Gómez-Sanz, Jorge & Singh, Munindar. (2009). *Lecture Notes in Computer Science. 213-228. 10.1007/978-3-642-19208-1_15.*

Evernote Review 2022: *Is It the Best Note-Taking App? (n.d.). Four Minute Books. Retrieved December 5, 2022, from https://fourminutebooks.com/evernote-review/*

Cheng, Kefei & Jia, Tingqiang & Gao, Meng. (2011). *Research and Implementation of three HTTPS attacks. JNW. 6. 757-764. 10.4304/jnw.6.5.757-764.*