



Forensic Analysis of Dropbox Data Remnants on Windows 10

By

Walter Buyu

Registration No: P53/85394/2016

SCI

University of Nairobi

A Project Submitted to SCI in Partial Fulfilment of the Requirements for the
Award of the Degree of Master of Science in Distributed Computing Technology
of The University of Nairobi

Supervisor

Dr Elisha Odira Abade

July 2020

DECLARATION

I Walter Buyu, do hereby declare that this research project is entirely my own work and where there is work or contributions of other individuals, it has been duly referenced as acknowledgement.

To the best of my knowledge, similar research has not been carried out before or previously presented to any other university.

Sign: -----

Date: -----

Name: Walter Buyu

Reg. No: P53/85394/2016

School of Computing and Informatics

University of Nairobi

This project has been submitted in partial fulfilment of the requirements for the Master of Science degree in Distributed Computing Technology of the University of Nairobi with my approval as the university supervisor.

Sign: -----

Date: -----

Name: Dr Elisha O. Abade

School of Computing and Informatics

University of Nairobi.

DEDICATION

To Jilly, thank you for your unending support.

ACKNOWLEDGEMENT

I am grateful to God for the good health that I had the entire time while working on this research. I wish to thank my supervisor Dr Elisha Odira Abade, for his support during this undertaking. Thank you for providing guidance and allowing me to shape this project in my own way, thus affording me the opportunity to conduct an independent and self-directed study.

To e.KRAAL Innovation Hub, thank you for exposing me to brilliant minds from whom I learnt and gained knowledge. The exposure you have given me has opened my mind to various facets of cybersecurity. The flexible work schedule allowed me to work on this project to its conclusion. In sum, your support has contributed immensely to this research.

Lastly, I wish to thank my family and friends for encouraging me through the entire period of my studies. I am grateful to Lynne and Jan, whose happiness keeps me going; I hope this work inspires you in the future. Special thanks to my parents for encouraging me to pursue postgraduate studies and affording me the opportunities they never had. To my siblings, I am grateful for the support you accorded me during this period. And to my friends, thank you for pushing me to complete this endeavour.

ABSTRACT

Cloud storage services are popular among businesses and individuals as they offer convenience in storage and sharing of files at an affordable price. However, cloud storage is subject to abuse by cybercriminals, and coupled with the difficulty in getting artefacts of evidential value from cloud storage providers, artefacts from client computer can provide potential evidence on which a case can be based. This research investigates artefacts left behind by Dropbox, a popular cloud storage application, on Windows 10. Through live and dead forensics, the study determines Dropbox artefacts on Windows 10 for various scenarios including installation, file upload, file deletion, and uninstallation. By identifying these remnants, this work contributes to a better understanding of the artefacts that are likely to remain for digital forensics investigators. Potential information sources identified during the research include the Dropbox client software installation files, synchronisation folder, browser, link files, prefetch files, registry, and network traffic. The artefacts identified in the study can assist in criminal investigation involving Dropbox as they provide useful information in recreating the scene of crime, tying a suspect to the crime, and creating a timeline of events.

TABLE OF CONTENTS

DECLARATION	i
DEDICATION	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
1 INTRODUCTION	1
1.1 Research Background.....	2
1.2 Problem Statement	4
1.3 Research Aim	4
1.4 Research Objectives	4
1.5 Research Questions	5
1.6 Research Significance	5
1.7 Scope	5
1.8 Assumptions and Limitations.....	5
1.9 Organisation of Chapters.....	5
2 LITERATURE REVIEW	7
2.1 Digital Forensics Concepts	7
2.1.1 Types of Digital Forensics	8
2.1.2 Types of Digital Data.....	10
2.1.3 Sources of Digital Data.....	11
2.1.4 Classification of Digital Evidence	11
2.2 Rules of Digital Evidence	11
2.3 Digital Forensics Models	12
2.4 Cloud Storage Forensics.....	13
2.5 Dropbox Forensics on Windows	14

2.6	Gaps.....	16
2.7	Conceptual Architecture.....	17
3	RESEARCH METHODOLOGY.....	18
3.1	Research Philosophy	18
3.2	Research Strategy.....	19
3.3	Data Collection.....	19
3.3.1	Preparation	21
3.3.2	Identification of Digital Evidence.....	24
3.3.3	Preservation of Digital Evidence	24
3.3.4	Analysis of Digital Evidence	25
3.3.5	Reporting of Digital Evidence	25
3.4	Data Analysis	25
3.5	Limitations of Methodology.....	25
3.6	Ethical Considerations.....	26
4	RESULTS AND DISCUSSION.....	27
4.1	Control (Base) Image Analysis	27
4.2	Dropbox Installation.....	28
4.2.1	Files System Artefacts	29
4.2.2	Registry Artefacts	36
4.3	File Upload.....	38
4.4	File Deletion.....	39
4.5	Dropbox Uninstallation	41
4.5.1	File System Artefacts	41
4.5.2	Registry Artefacts	49
4.6	Conclusion.....	50

5	CONCLUSIONS AND RECOMMENDATIONS	51
5.1	Research Objectives: Summary of Findings and Conclusions	51
5.2	Contributions.....	52
5.2.1	Contributions to Research.....	52
5.2.2	Contribution to Practice	53
5.3	Limitations of the Study.....	53
5.4	Future Work	54
	REFERENCES	55

LIST OF FIGURES

Figure 1	Organisation of Chapters	6
Figure 2	Dead Forensics Image Acquisition (Lessing and Solms, 2008).....	9
Figure 3	Live Forensics Image Acquisition (Lessing and Solms, 2008).....	10
Figure 4	Conceptual Architecture	17
Figure 5	The Research Onion (Saunders, Lewis and Thornhill, 2015)	18
Figure 6	VM Snapshots for Live and Dead Forensics.....	21
Figure 7	Creation of Live Forensics Snapshots	23
Figure 8	Artefacts with Dropbox reference in Base VM.....	27
Figure 9	Dropbox Installation Network Activity.....	28
Figure 10	Dropbox Domain IP Address	29
Figure 11	Dropbox Registration Information	29
Figure 12	Dropbox Search on Microsoft Edge in Install-VM	30
Figure 13	URLs Accessed on Microsoft Edge in Install-VM.....	30
Figure 14	Dropbox Cookies in Microsoft Edge in Install-VM.....	30
Figure 15	Dropbox User Email in Install-VM.....	31
Figure 16	Dropbox Files and Folders in AppData\Local\Dropbox	32
Figure 17	Dropbox Files and Folders in AppData\Local\Dropbox\instance1	32
Figure 18	Files in AppData\Roaming\Dropbox.....	34
Figure 19	Dropbox Prefetch Files in Install-VM.....	34

Figure 20 Dropbox Link Files in Install-VM.....	35
Figure 21 Files in Dropbox Synchronisation Folder - Live Forensics.....	35
Figure 22 Files in Dropbox Synchronisation Folder in Install-VM.....	36
Figure 23 Files Uploaded in Dropbox Sync Folder - Live Forensics	39
Figure 24 Files Uploaded in Dropbox Sync Folder in Install-VM	39
Figure 25 Deleted 'delete file.txt' Found in Recycle Bin.....	40
Figure 26 Deleted 'shift delete file.txt' Found in Dropbox Sync Folder	40
Figure 27 Deleted Files Found in Dropbox Sync Folder in Deleted-VM.....	41
Figure 28 Dropbox Search on Microsoft Edge in Uninstall-VM	41
Figure 29 URLs Accessed on Microsoft Edge in Uninstall-VM.....	42
Figure 30 Dropbox Cookies in Microsoft Edge in Uninstall-VM	42
Figure 31 Dropbox User Email in Uninstall-VM	42
Figure 32 Dropbox Related Files in Program Files	43
Figure 33 Dropbox Log Files in ProgramData in Uninstall-VM.....	43
Figure 34 Dropbox Related Files in ProgramData in Uninstall-VM.....	44
Figure 35 Files Referencing Dropbox in the Root Folder in Uninstall-VM.....	44
Figure 36 Files Referencing Dropbox in System32 and NTUSER.DAT in Uninstall-VM.....	45
Figure 37 Dropbox Folder in AppData\Roaming in Uninstall-VM.....	45
Figure 38 Files Referencing Dropbox in Local\Microsoft and Local\Packages in Uninstall-VM.....	46
Figure 39 Files Referencing Dropbox in Local\Temp in Uninstall-VM	46
Figure 40 Files Referencing Dropbox in Roaming\Microsoft in Uninstall-VM	47
Figure 41 Dropbox Prefetch Files in Uninstall-VM	47
Figure 42 Dropbox Link Files in Uninstall-VM.....	48
Figure 43 Link Files to Uploaded Files in Sync Folder in Uninstall-VM	48
Figure 44 Files in Dropbox Sync Folder in Uninstall-VM.....	49
Figure 45 Dropbox Service Artefacts in Registry in Uninstall-VM.....	49
Figure 46 Dropbox Update Artefacts in Registry in Uninstall-VM	49
Figure 47 Dropbox Uninstall Artefacts in Registry in Uninstall-VM	50
Figure 48 Dropbox Update, Installer, Explorer, and Shell Artefacts in Registry in Uninstall-VM	50

LIST OF TABLES

Table 1 Software Used in Experiment	20
Table 2 Virtual Machines.....	21
Table 3 VM Images and Checksums	24
Table 4 Dropbox Database Files.....	33
Table 5 Registry Directory Structure Artefacts in Install-VM	36
Table 6 Registry Configuration Settings Artefacts in Install-VM.....	37
Table 7 Registry Time Related Artefacts in Install-VM.....	37
Table 8 Registry Encryption Artefacts in Install-VM.....	38

1 INTRODUCTION

Cloud computing can be defined as the provisioning of computing services and resources over the internet, to end-users who do not necessarily own the infrastructure supporting these services and resources. The National Institute of Science and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell and Grance, 2011).

The growing demand for computing power and resources have contributed to the growth of cloud computing (Simou *et al.*, 2014). Cloud computing is increasingly being used by both businesses and individuals (Pichan, Lazarescu and Soh, 2015) as it promises increased flexibility, high reliability, massive scalability, and decreased costs (Ghafarian, 2015). Organisations are shifting from setting up traditional in-house computing infrastructures and opting for the cloud to reduce capital expenditure by going for the cheaper option of operational expenditure for such infrastructure. Individuals mostly use the cloud to store and share files easily (Ahmed and Li, 2016).

The adoption of cloud computing has drawn the interest of cybercriminals as well to the platform (Damshenas *et al.*, 2012). While cloud computing provides efficiency within the technological space, it is equally likely to be abused by cybercriminals (Biggs and Vidalis, 2009). The uptake of cloud computing extends the attack surface to the cloud, where attackers exploit vulnerabilities on such platforms. The relative ease of anonymity, access, and unlimited computing power present in the cloud, afford attackers a convenient means of conducting their attacks (Pichan, Lazarescu and Soh, 2015). For example, Amazon's EC2 service was used in the hacking of Sony's PlayStation Network (Chung *et al.*, 2012).

A typical application of cloud computing service is cloud storage services (Ghafarian, 2015). Though not new, cloud storage services are becoming increasingly popular (Hu, Yang and Matthews, 2010). Many cloud storage applications exist in the market, including Apple iCloud, Microsoft OneDrive, Google Drive, and Dropbox (Caviglione *et al.*, 2017). Dropbox is in the tier of the popular cloud storage services (Ghafarian, 2015; Mehreen and Aslam, 2015) and is even

claimed to be the most popular among cloud users worldwide (Caviglione *et al.*, 2017). Dropbox allows users to store and share files and collaborate on projects. The service can be accessed from a PC tablet or phone using a browser or client application. Changes made on one device are automatically synced across all devices (Dropbox, 2018b). Dropbox offers two plans: Dropbox for individuals and Dropbox for business. The basic version of Dropbox offers free 2 GB storage and can be upgraded to either Dropbox Plus, Professional or Business (Dropbox, 2018a).

Despite the advantages brought by cloud storage, it is still subject to abuse by criminals (Ahmed and Li, 2016), especially where it would be difficult to get artefacts of evidential value from the cloud service provider (Biggs and Vidalis, 2009). Cloud storage services could be used in acts of terrorism. For example, in the USA, a terrorist attack in 2015 in San Bernardino led to the death of 14 people and left 22 wounded. One of the key suspects in the attack disabled iCloud backups well in advance to the incident (Cahyani *et al.*, 2016). Cybercriminals could also use cloud storage to store or share illegal files or for botnet attacks (Ahmed and Li, 2016); or to exfiltrate confidential information (Chung *et al.*, 2012). Furthermore, steganography could be employed during such attacks for covert data exchange using applications like Dropbox (Caviglione *et al.*, 2017).

Cloud storage has raised concerns about security and forensics investigation in the cloud environment. The security concern is that data stored in the cloud could be compromised. The forensics concern is that conducting a digital investigation in the cloud environment is complicated (Ghafarian, 2015). Attributing a crime committed in the cloud poses various challenges especially with encryption, anonymity and geographical location (Taylor *et al.*, 2011) which complicate the acquisition and analysis of digital evidence (Guo, Jin and Shang, 2012). This is further exacerbated by the jurisdictional challenges and lack of international collaboration (Guo, Jin and Shang, 2012). With increasing digital crime, it is necessary to address cloud security and by extension, cloud forensics (Damshenas *et al.*, 2012) using novel investigative approaches (Guo *et al.*, 2012).

1.1 Research Background

Dropbox is in the group of the most preferred cloud storage applications among cloud users worldwide (Ghafarian, 2015; Mehreen and Aslam, 2015; Caviglione *et al.*, 2017). On the other hand, Microsoft Windows OS is the most popular operating system among users globally, accounting for over 88% of the operating systems used on PCs (NetApplications, 2018). The

popularity of Dropbox and Windows OS amongst users has drawn several researchers to conduct Dropbox forensics on Windows platform.

Quick and Choo (2013) analysed Dropbox data remnants and their location on Windows 7 PC. The investigation included artefacts on the hard drive, network traffic, and memory. The authors found that Dropbox is installed in the `C:\Users\[username]\AppData\Roaming\` folder rather than `C:\Program Files\` folder. The Dropbox configuration files that were previously in plaintext had also been encrypted, and their file extensions changed from `.db` to `.dbx`. Additionally, they found that SOFTWARE and SYSTEM registry hives held the references to Dropbox files and folders. When uninstalled, only `Dropbox.exe` was deleted while other files remained including the synchronisation folder and file contents in the user home directory.

Ghafarian (2015) analysed artefacts that remain on Windows 7 client machine after each cloud activity such as creating, uploading and deleting files. The author found that more information about Dropbox folder files could be obtained such as the user id of the person who accessed the file, all the actions that were performed on the file, the date, time, etc. The network traffic analysis could reveal whether Dropbox had been used, for how long, and the activities that had been performed

Mehreen and Aslam (2015) investigated the remains of Dropbox activity on Windows 8. The authors found that Dropbox client installation directory was still the same as that of Windows 7. They also learnt that Dropbox client maintains encrypted `.dbx` files for maintaining configuration information and a history of activities. Registry analysis revealed that Dropbox maintains two encryption keys, i.e. `KS` and `KS1`. The authors conclude that artefacts present on local machines still bear invaluable information.

Amirullah, Riadi and Luthfi (2016) analysed data remnants of cloud storage applications including Dropbox on Windows 10. The analysis shows the location of application files, including log files and databases when Dropbox is installed. The authors were able to decrypt the `.dbx` files. Even after uninstallation, data remnants including Dropbox folder and the files within were still available on the host machine. The study points out that registry keys remain but do not specify the exact keys and their locations.

1.2 Problem Statement

Cloud storage is subject to abuse by cybercriminals (Ahmed and Li, 2016) and coupled with the difficulty in getting artefacts of evidential value from cloud storage providers (Biggs and Vidalis, 2009), it would take more time and effort to conduct cloud forensics investigation when solely relying on evidence from the cloud storage providers (Taylor *et al.*, 2011). However, artefacts from both the client computer and cloud service provider can be relied on for cloud forensic investigation (Guo, Jin and Shang, 2012). Artefacts from client computer can provide potential evidence even when it is challenging to obtain corroborating artefacts from CSPs, in which case, the case can be based on the artefacts from the client-side (Taylor *et al.*, 2011).

Cloud storage is expected to grow (Cisco, 2018: 21) and with Dropbox being one of the popular cloud storage applications among cloud users, it is likely to be abused by cybercriminals, for example, to covertly exchange information (Caviglione *et al.*, 2017). Windows OS, on the other hand, is the most popular among users globally, accounting for almost 90% of OS used on PCs (NetApplications, 2018). Windows 7 support is expected to end in January 2020 with that of Windows 8.1 ending in 2023 (Microsoft, 2018). Therefore, by 2020 most Windows systems are expected to run Windows 10 (Keizer, 2018). Consequently, cases of abuse of Dropbox running on Windows 10 are likely to arise, bringing the need to identify and categorize unique aspects of where and how digital evidence can be found (Zatyko and Bay, 2011) to support forensic investigation of such cases.

1.3 Research Aim

The aim of this research is to investigate Dropbox data remnants on Windows 10. The research seeks to answer the question: What data remnants are left by Dropbox on Windows 10 after uninstallation?

1.4 Research Objectives

1. Analyse digital forensics methodologies and their appropriateness for Dropbox forensics.
2. Investigate file system and registry artefacts created by Dropbox when installed on Windows 10.
3. Investigate Dropbox artefacts left on Windows 10 file system and registry after uninstallation and their significance to forensic investigators.

1.5 Research Questions

1. Which digital forensic methodologies are in use and how appropriate are they for conducting Dropbox forensics?
2. What file system and registry artefacts are created by Dropbox when installed on Windows 10?
3. What artefacts are left by Dropbox on Windows 10 file system and registry after uninstallation?

1.6 Research Significance

By determining Dropbox data remnants on Windows 10, a contribution is made to understand better the artefacts that are likely to remain, and where digital forensic examiners could find them. The output of this research provides the location and significance of artefacts of evidential value to digital forensics investigators probing cybercrimes involving Dropbox in a Windows 10 environment.

1.7 Scope

This research is restricted to Dropbox forensics on Windows 10. It focuses on the Dropbox artefacts related to the installation, use, and uninstallation of the application on Windows 10. The artefacts investigated are restricted to those found in the registry and file system. Although other Dropbox artefacts such as those in memory and network traffic could be examined, this research does not cover them.

1.8 Assumptions and Limitations

Both commercial and open source tools are used in conducting the experiment in the study. Therefore, the level of detail of artefacts retrieved may be limited by the capabilities of the tools. However, this limitation is partially addressed in some instances by using more than one tool and corroborating the results. It is assumed that the tools used do not tamper with the integrity of the artefacts retrieved.

1.9 Organisation of Chapters

This research consists of five chapters. The flow of the chapters is shown in Figure 1.

Chapter 1 introduces cloud computing, the research area in which this project is based, with an emphasis on cloud storage forensics. It further provides the objectives, scope and significance of this study.

Chapter 2 provides a review of literature on digital forensics and a critical analysis of previous work on Dropbox forensics. Gaps in literature are identified which need to be addressed through an empirical study. This chapter addresses the theoretical objectives of this study.

Chapter 3 addresses the methodology used for the empirical study. It describes the research philosophy, research strategy, data collection method, and data analysis method used in the study. It further outlines the limitations of the methods and how they are overcome. Ethical considerations when conducting the research are also addressed.

Chapter 4 provides the results from the experiment and discusses their significance to Dropbox forensics investigations. This chapter answers both the empirical and practical objectives of the study.

Chapter 5 concludes this work by providing a summary of the research, its contributions, limitations, and a suggestion of areas for future work.

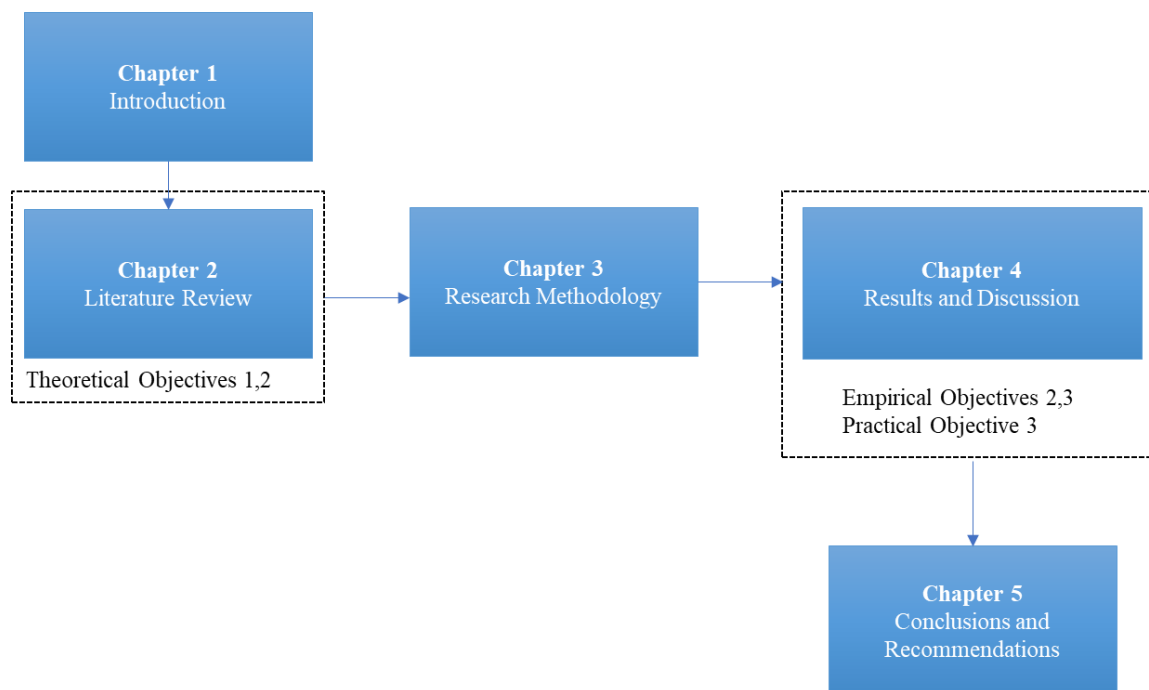


Figure 1 Organisation of Chapters

2 LITERATURE REVIEW

This literature review will analyse various digital forensic methodologies and cloud storage client application forensics. Through the literature review, the first objectives of the study will be addressed (the third and fourth objectives will be addressed through an empirical study in which an experiment will be conducted, and the results analysed).

By reviewing the literature on digital forensic methodologies, a better understanding of the digital forensics process will be gained, and an appropriate methodology for conducting Dropbox forensics in the empirical study adopted. A critical review of cloud storage client applications forensics will provide better knowledge of the peculiarities of such investigations which will be considered when conducting the experiment. From the onset, it is essential to gain an understanding of digital forensics concepts as they underpin the study.

2.1 Digital Forensics Concepts

Several definitions of digital forensics have been provided by forensic experts. McKemmish (1999) defines digital forensics as “the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable”. Lessing and Solms (2008) emphasises on the legal and computing aspects of forensics in their definition: Unlike McKemmish's perspective of forensic computing as a process, they view digital forensics as a discipline that combines law and computing in the collection and analysis of data from digital devices and networks in a way acceptable to courts.

The Digital Forensic Research Workshop (DFRWS) provides a more comprehensive definition overemphasising on the use of scientific methods for events found to be criminal or otherwise. In their definition, the methods used in the forensic process must be scientific and proven. Furthermore, the goal of the forensic investigation should be to facilitate or further the reconstruction of criminal events, or foresee undesirable actions to planned operations (Palmer, 2001).

Despite the comprehensive definition by DFRWS, there is no single conclusive definition of digital forensics. After reviewing definitions of forensic computing, Hannan (2004) concludes that “no single definition can adequately define the current meaning of Forensic Computing”. Despite the differences in definitions, all of them emphasise on the need to maintain evidentiary weight on the

forensic computing product (McKemmish, 2008). For this study, McKemmish (1999) definition of digital forensics is adopted. The definitions of digital forensics refer to digital evidence which is defined as “any information of probative value that is either stored or transmitted in a digital form” (EC-Council, 2010). The definition means that digital evidence must prove or demonstrate something.

2.1.1 Types of Digital Forensics

The shift to cloud computing means that forensic investigation could involve computing devices on the client, network or server. While conducting the investigation, the computing devices could either be in a powered on or off state. Therefore, the types of forensic investigations can be classified according to the location of the devices on the network and their powered state.

Client forensics involves the identification and collection of artefacts of evidential value from client-side devices, including laptops, PCs, and mobile devices (Pichan, Lazarescu and Soh, 2015). Vital evidence can be found on client-side, some of which may be sensitive. Therefore, it is necessary to conduct client forensics (Damshenas *et al.*, 2012). The proliferation of client endpoints, especially mobile endpoints, has made client forensics more challenging (Ruan *et al.*, 2011).

Server forensics involves the collection of artefacts available on servers. In highly decentralised and virtualised environments, data might be located in multiple data centres across different geographical locations, making identification and collection of evidence difficult (Pichan, Lazarescu and Soh, 2015). The traditional approach of seizing servers may be impractical as it would impact a whole data centre, affecting other consumers due to multi-tenancy (Birk and Wegener, 2011; Guo, Jin and Shang, 2012).

Network forensics is the capturing, recording, and analysis of network events in order to discover the source of attacks or other problem incidents (EC-Council, 2010). Network forensics can be conducted in cloud environments as well. The communication protocols between the VMs inside and outside the cloud can provide the required information (Pichan, Lazarescu and Soh, 2015). However, CSPs ordinarily do not provide logs of such communication despite their importance as part of forensic artefacts (Birk and Wegener, 2011).

Dead forensics is forensics done on a powered-off computer. The advantages of dead forensics include a minimal chance of data modification. Disadvantages include loss of volatile data and difficulty in the analysis of encrypted disks (Lessing and Solms, 2008). Figure 2 shows the process of image acquisition using dead forensics. Hardware or software write blockers are used to prevent writing to the hard disk, thus preserving the integrity of the evidence (SWGDE, 2009).

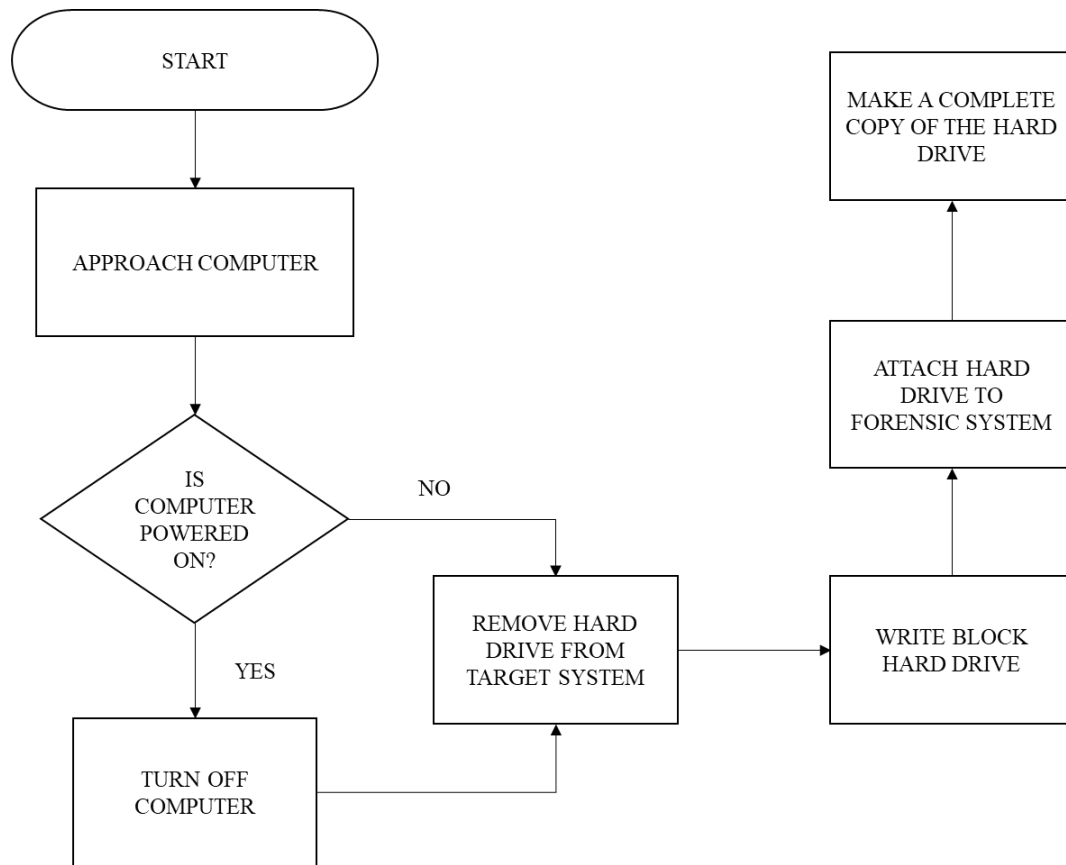


Figure 2 Dead Forensics Image Acquisition (Lessing and Solms, 2008)

Live forensics is forensics conducted on a powered-on computer. Real-time system data is obtained before shutting down the system to preserve memory, process and network information that would otherwise be lost in a traditional (dead) forensic acquisition (Grobler and Solms, 2009). The pros of live forensics include retrieval of volatile information and limitation of acquired data to only those that are relevant. On the downside, chances of data modification are high, coupled with difficulty to prove authenticity and reliability of evidence (Lessing and Solms, 2008). Figure 3 shows the process of image acquisition in live forensics in which collection and analysis is done on the live system before acquiring the image for traditional analysis.

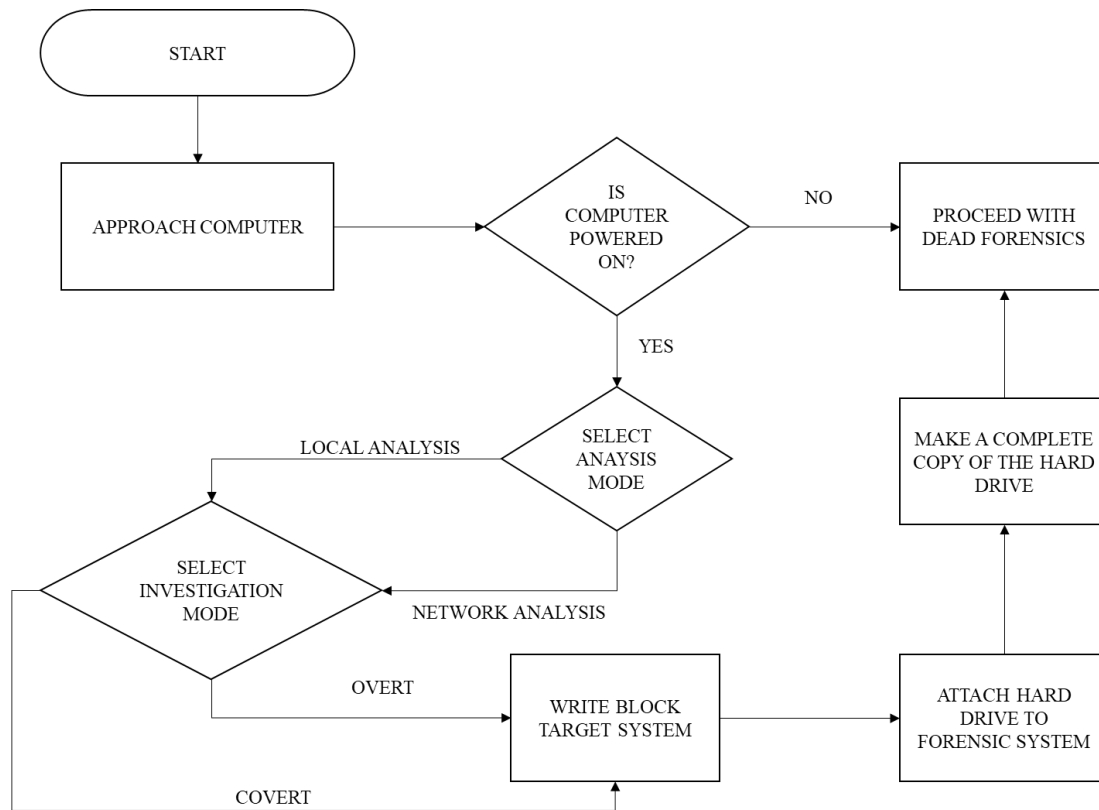


Figure 3 Live Forensics Image Acquisition (Lessing and Solms, 2008)

2.1.2 Types of Digital Data

Different types of data can be collected when conducting digital forensics. The data should be collected from the most volatile to the least volatile. The types of data that can be found are described as follows (EC-Council, 2010):

- **Volatile data** is data that is lost when a computer is turned off. Such data includes open files, process information, network information, memory data, cache data, etc.
- **Non-volatile data** persists even after shutdown and is found in secondary storage. The data includes hidden files, hidden partitions, registry settings, event logs, etc.
- **Backup data** is a copy of the system data and can be used during recovery after a disaster or system crash.
- **Residual data** is data that remains on the computer when a file is deleted.
- **Metadata** is data maintained about a file and includes the file format and how, when, who created and modified the file.

2.1.3 Sources of Digital Data

The digital data can be found from various devices (EC-Council, 2010):

- **Endpoints** including hard drive, memory, thumb drive, memory card, personal digital assistants, smart cards, scanners, printers, digital cameras, telephones, mobile phones, GPS, wearable technology, fax, etc.
- **Network devices** including routers, hubs, switches, network interface card, network cables, network connectors, etc.

2.1.4 Classification of Digital Evidence

Depending on whether the evidence implicates the suspect, evidence can be inculpatory or exculpatory. **Inculpatory evidence** supports existing data and theories. It ties the suspect to the crime. **Exculpatory evidence** contradicts existing data and theories. It exonerates the suspect from the crime. To find both evidence types, all acquired data must be analysed and identified (Carrier, 2003).

Another perspective is whether the evidence requires further reasoning or inference. From this perspective, evidence can be either direct or circumstantial. **Direct evidence** establishes a fact and requires no inference. **Circumstantial evidence**, on the other hand, requires that a judge and/or jury make an indirect judgment, or inference, about what happened. Circumstantial evidence is not absolute proof; instead, it provides a general idea of what happened. Most often, evidence identified through digital forensics is circumstantial, though direct evidence such as witness and victim statements or suspect confessions may impact the interpretation of evidence or recreation of the chain of events (Lyle, 2019).

2.2 Rules of Digital Evidence

For digital evidence to be acceptable in a court of law, it must meet the five rules of evidence (EC-Council, 2010):

1. **Admissible:** Evidence must have been preserved and gathered in such a way that it can be used in court.
2. **Authentic:** The evidence must be relevant to the case, and the forensic examiner must be able to account for the origin of the evidence.

3. **Complete:** When evidence is presented, it must tell the whole story. Both inculpatory and exculpatory evidence must be presented.
4. **Reliable:** There must be no doubt on the evidence's authenticity and veracity. The techniques used must be credible and generally accepted in the field. The opposing counsel should be able to achieve similar results using the same techniques and procedures.
5. **Understandable and Believable:** The evidence should be clearly understood and easy to believe by the judges.

2.3 Digital Forensics Models

Both the digital evidence and the process followed in conducting the investigation must prevail in a court of law (Pichan, Lazarescu and Soh, 2015). Inappropriate processes have resulted in limited prosecution (Kohn, Eloff and Eloff, 2013). A sound forensic investigation must meet both implied and explicit processes (Grobler and Solms, 2009) which are captured by digital forensics models. Various digital forensic process frameworks and models have been proposed, some of which are discussed below:

1. The McKemmish model, one of the pioneering models, is a four-step model consisting of *Identification, Preservation, Analysis and Presentation* (McKemmish, 1999).
2. The Digital Investigative Process incorporates a decision after the presentation of evidence and consists of the following steps: *Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision* (Palmer, 2001).
3. The National Institute of Science and Technology forensics guideline provides a four-step model comprising of *Collection, Examination, Analysis and Reporting* (Kent *et al.*, 2006).
4. The Integrated Conceptual Digital Forensic Framework for Cloud Computing is similar to McKemmish and NIST models in naming and purpose but differs in meaning and implementation. It consists of four steps, namely *Evidence Source Identification and Preservation; Collection; Examination and Analysis; and Reporting and Presentation phases* (Martini and Choo, 2012).
5. The Digital Forensic Analysis Cycle model is cyclic and iterative with seven steps namely *Commence (scope), Prepare and Respond, Identify and Collect, Preserve (Forensic Copy), Analyze, Present, Feedback, and Complete or Further Tasks Identified* (Quick and Choo, 2013a).

6. The Integrated Digital Forensic Process Model incorporates physical investigation conducted in concert with the digital investigation in cases where the crime is not confined to the digital space. It comprises of six steps, namely: *Preparation, Incident, Incident Response, Physical Investigation, Digital Forensic Investigation, and Presentation* phases (Kohn, Eloff and Eloff, 2013).

McKemmish model is adopted for this study. To ensure that evidence is collected and processed in a manner acceptable in a court of law, the digital forensics methodology is followed, which generally consists of four phases (McKemmish, 1999):

1. **Identification** phase is about knowing the evidence that is present, its location, and the form in which it is stored. This is important as it helps the investigator determine the technology and processes to use in the recovery of the evidence.
2. **Preservation** ensures that the evidence is kept as close as possible to its original state. There should be no alteration to the evidence, but where it is unavoidable, such changes must be accounted for and justified
3. **Analysis** involves extraction, processing and interpretation of digital data. It is regarded as the most critical step in the investigation process.
4. **Presentation** entails communication of the evidence to the client or in a court of law.

2.4 Cloud Storage Forensics

The process of investigating an incident in cloud computing platforms can broadly be grouped into three, i.e. client forensics, server forensics and network forensics (Pichan, Lazarescu and Soh, 2015). Cloud forensics may be conducted at the provider's end or the user's end (Mehreen and Aslam, 2015). Server-side forensics pose various challenges, including jurisdiction and geographical location, which make access to artefacts difficult. In some incidents, artefacts may not be easily traceable (Ahmed and Li, 2016). For example, data that would normally persist on the operating system would be stored in a virtual environment and as such, lost when the user exits the cloud environment. Consequently, artefacts left behind are limited. Additionally, different machines might also be involved in a transaction making analysis of the sequence of events difficult (Guo, Jin and Shang, 2012). In other instances, obtaining evidence from the cloud service provider (CSP) would be difficult such as the San Bernardino incident in which Apple Inc. refused

to assist the FBI in unlocking the suspect's phone (Cahyani et al., 2016). These challenges underscore the need for client-side forensics to complement server-side forensics.

The technical and non-technical challenges posed by server-side forensics does not completely hinder such investigation as traces of criminal activity could be located on the client's device (Chung et al., 2012). Therefore, it is important for investigators to know the location and type of data remnants on cloud users' devices (Ahmed and Li, 2016). While investigating cloud environments, evidence from the client system, particularly the user agent used to access the cloud service, should not be ignored (Birk and Wegener, 2011).

The synchronisation of end devices with cloud storage services leaves evidence in the clients' devices (Mehreen and Aslam, 2015). However, acquisition from the client side may not provide all the data artefacts of interest. For SaaS applications, for example, the clients might not necessarily be the original source of data. It maintains a cached version of data which may be incomplete or outdated (McCulley and Roussev, 2016). Therefore, such evidence where possible should be augmented with those from the server or network forensics. The client's end remains of interest to investigators as evidence based on artefacts obtained from client-side devices can help cement the case under investigation. Furthermore, such evidence would be significant where obtaining evidence from CSP is difficult (Taylor et al., 2011).

2.5 Dropbox Forensics on Windows

The popularity of Dropbox and Windows OS amongst users has drawn several researchers to conduct Dropbox forensics on Windows platform.

McCain (2011) investigated Dropbox data remnants on Windows XP and noted that various artefacts could be found on the system including installation directory, registry changes, network activity, database files, log files, and uninstallation data. The database files included `host.db`, `unlink.db`, `config.db`, `filecache.db`, and `sigstore.db` which were unencrypted SQLite files. Even though the remnants were identified, it is not clear the kind of data that was found and its significance in cloud storage forensics (Chung *et al.*, 2012).

Marturana *et al.*, (2012) determined that on Windows 7, browser artefacts, sync logs, and timeline of recently opened, modified, and deleted files by Dropbox, could be obtained. By performing live and dead forensics, the study concluded that Dropbox user activities could be constructed.

Similarly, on Windows 7, Epifani (2013) established that from the Dropbox registry changes, installation directory and installation version could be determined. The `host.db` file contained the sync folder name encoded using Base64. Dropbox also created link files and prefetch files which pointed to the installation and use of Dropbox.

Quick and Choo (2013) analysed Dropbox data remnants and their location on Windows 7 PC. The investigation included artefacts on the hard drive, network traffic, and memory. The authors found that Dropbox is installed in the `C:\Users\[username]\AppData\Roaming\` folder rather than `C:\Program Files\` folder. The Dropbox configuration files that were previously in plaintext had also been encrypted, and their file extensions changed from `.db` to `.dbx`. Additionally, they found that SOFTWARE and SYSTEM registry hives held the references to Dropbox files and folders. When uninstalled, only `Dropbox.exe` was deleted while other files remained including the synchronisation folder and file contents in the user home directory.

Ghafarian (2015) analysed artefacts that remain on Windows 7 client machine after each cloud activity such as creating, uploading and deleting files. The author found that more information about Dropbox folder files could be obtained such as the user id of the person who accessed the file, all the actions that were performed on the file, the date, time, etc. The network traffic analysis could reveal whether Dropbox had been used, for how long, and the activities that had been performed.

Mehreen and Aslam (2015) investigated the remains of Dropbox activity on Windows 8. The authors found that Dropbox client is installed under `C:\Users\[username]\AppData\Roaming\Dropbox\bin\Dropbox.exe`. They also learnt that Dropbox client maintains `.dbx` files in `C:\Users\[username]\AppData\Roaming\Dropbox\instance1\` for maintaining configuration information and a history of activities. The files include `host.dbx`, `config.dbx`, `filecache.dbx`, `deleted.dbx`, `notification.dbx`, `photo.dbx`, `unlink.dbx`, `sigstore.dbx`, `aggregation.dbx`. Registry analysis revealed that changes were made to `HKCU\Software\Dropbox` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer` registry keys. `HKCU\Software\Dropbox` contains the installation directory and has two folders with

different key values, i.e. ks and ks1, which are Dropbox user keys used to derive Dropbox encryption keys (Picasso, 2017). The authors conclude that artefacts found on local machines still carry much valuable information.

Malik *et al.*, (2015a) conducted Dropbox investigation on Windows 8.1. The authors noted traces of browser-related artefacts, including cookies, URLs, keywords searched, and login details such as email. Even though Dropbox still encrypted the configuration and database files, using *Magnet Forensics Dropbox Decryptor*, the files could be decrypted by providing Dropbox encryption keys from the registry, and Windows user account password. Deleted files could also be recovered as references to these files were still present in the Master File Table. When uninstalled, the Dropbox root folder was still present. In addition to the root folder, Dropbox folder in C:\Users\[username]\AppData\Roaming was intact, but the encrypted files in it had been deleted. Several registry keys were also present.

Amirullah, Riadi and Luthfi (2016) analysed data remnants of cloud storage applications including Dropbox on Windows 10. The analysis shows the location of application files, including log files and databases when Dropbox is installed. The authors were able to decrypt the .dbx files. Even after uninstallation, data remnants including Dropbox folder and the files within were still available on the host machine. The study points out that registry keys remain but does not specify the exact keys and their locations. Furthermore, in the methodology, the work does not explain how the process of identification, preservation, analysis, and presentation was met, yet it is a requirement in any digital forensic investigation (McKemmish, 1999).

2.6 Gaps

From the literature reviewed, much work is yet to be done on Dropbox forensics on Windows 10. The Dropbox analysis by Amirullah, Riadi and Luthfi (2016) on Windows 10 does not give complete artefacts created during installation. For example, they do not specify the location of the Dropbox synchronisation folder. The authors also do not comprehensively cover the data remnants left when Dropbox is uninstalled. They state that multiple registry keys are left behind but do not specify the exact keys and their significance. To address these gaps, it is imperative to conduct an empirical study to investigate the artefacts created during installation, use, and uninstallation of Dropbox client application on Windows 10.

2.7 Conceptual Architecture

The conceptual architecture in Figure 4 shows the virtual machines to be set up and the processes involved in their creation. From the literature reviewed, different user activities such as Dropbox installation, file upload, file deletion, and uninstallation, result in different data remnants on the client machine. To examine the artefacts present in these scenarios, both live and dead forensics should be carried out. For dead forensics, virtual machines are created for each situation, and their images analysed. For live forensics, analysis tools must be set up and used to analyse each scenario. Snapshots are used to save the state of each step of the investigation during live analysis. In both dead and live analysis, the base/control virtual machine provides a reference point to compare Dropbox changes introduced as it does not have the Dropbox client application installed.

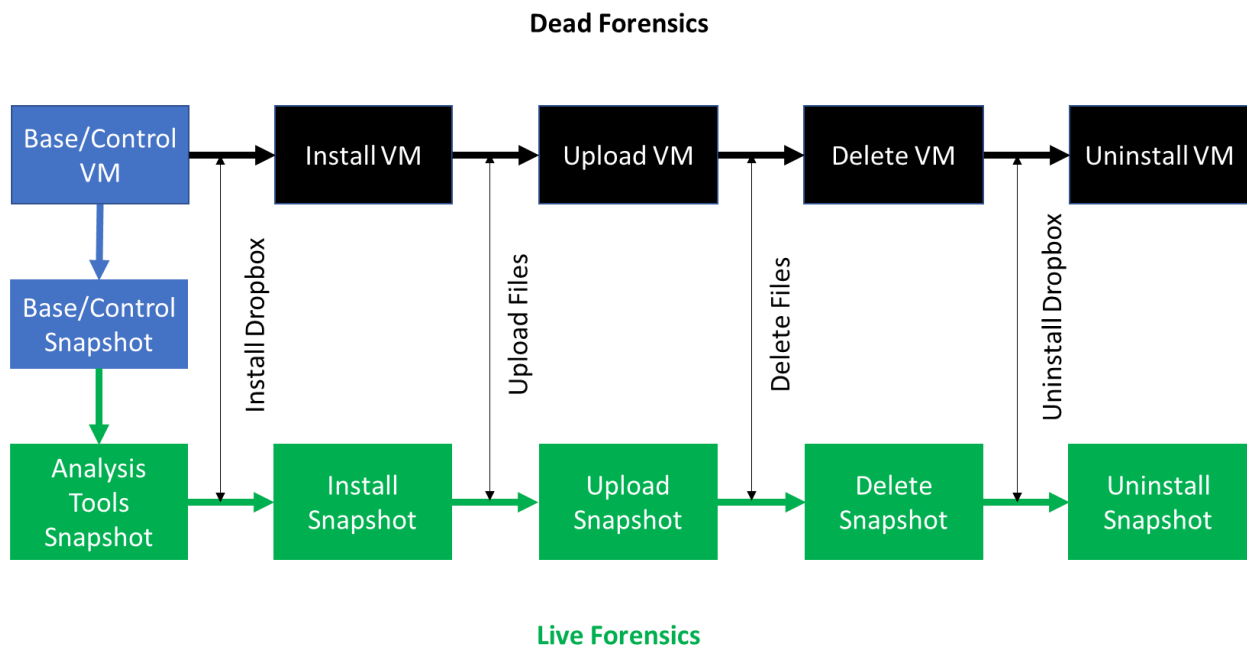


Figure 4 Conceptual Architecture

3 RESEARCH METHODOLOGY

This chapter provides details of the philosophical paradigm that will be adopted, the research strategy to be used, how data will be collected and analysed, the limitations of the strategy and methods of data collection and analysis; and ethical considerations while conducting the research.

3.1 Research Philosophy

Philosophical assumptions shape the research questions, methodology and interpretation of findings. Clearly thought-out assumptions provide a credible research philosophy which underpins the methodology adopted, the research strategy chosen, data collection techniques used, and the analysis procedures employed (Saunders, Lewis and Thornhill, 2016: 124-125) as demonstrated in Figure 5.

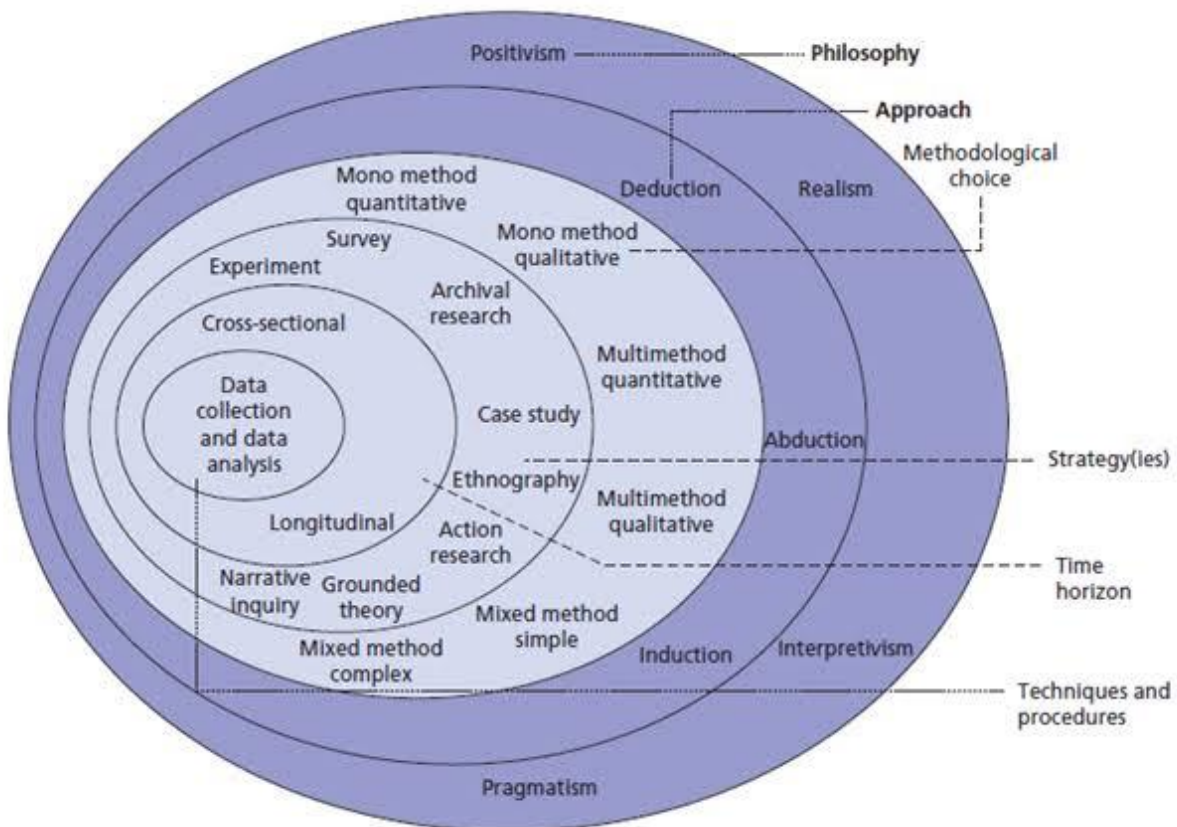


Figure 5 The Research Onion (Saunders, Lewis and Thornhill, 2015)

Positivism was adopted as the philosophical paradigm for the study. Positivism was appropriate as the study focused on observable facts (artefacts) based on scientific methods (experiment) in which the researcher was objective and independent of what was researched (Saunders, Lewis and Thornhill, 2016: 136).

3.2 Research Strategy

The research conducted was exploratory in nature as the goal was to investigate Dropbox artefacts left post uninstallation. The focus was initially broad, exploring the artefacts created during the installation of Dropbox and later narrow down to those left after Dropbox is uninstalled. As such, an experiment research strategy was used to find out these artefacts.

An experiment is a strategy that “investigates cause and effect relationships seeking to prove or disprove a causal link between a factor and an observed outcome”(Oates, 2006). A true experiment was conducted in a laboratory set-up so that all variables could be carefully controlled. Controls were necessary to guarantee that the changes observed were because of installation, use, and subsequent uninstallation of Dropbox. Consequently, control measures such as disabling Windows updates were in force amongst others.

An experiment is based on a hypothesis that is testable and can be disproved (Oates, 2006). A standard experiment has two opposing hypotheses: the **null hypothesis** and the **alternative hypothesis**. The null hypothesis predicts there will be no significant difference or relationship between the variables. The alternative hypothesis predicts there may be a significant difference or relationship between the variables (Saunders, Lewis and Thornhill, 2016). For this study, the null and alternative hypotheses were as follows:

- i. *Null Hypothesis*: Dropbox does not leave artefacts on Windows 10 after uninstallation
- ii. *Alternative Hypothesis*: Dropbox leaves artefacts on Windows 10 after uninstallation

3.3 Data Collection

The data for this study was collected from the experiment conducted. To perform the experiment, the software detailed in Table 1 were used.

Table 1 Software Used in Experiment

Software	Version	Purpose
VMWare Workstation 15 Pro	15.5.2	Creating virtual machines (VMs)
Windows 10 Pro	1903 (OS Build 18362)	The OS for the VMs
Dropbox Windows Client	91.4.548	Setting up Dropbox on Windows 10 Pro
Access Data FTK Imager	4.2.1.4	Imaging VMs
Regshot	1.9.0	Take registry snapshots and compare them
Mirekusoft Install Monitor	4.4.1020.1	Monitor file and registry changes by made by applications
Process Monitor	3.53.0.0	Monitor file system, registry and process/thread activity
Process Explorer	16.31.0.0	Monitor handles and DLLs processes have opened or loaded
GlassWire	2.1.167	Monitoring network connections
DB Browser for SQLite	3.11.2	Reading database (.db) files compatible with SQLite
HxD	2.4.0.0	Check hex of files
Decwindbx		Decrypting Dropbox dbx files
Magnet Forensics Decryptor	1.3	
EaseUS Data Recovery Wizard	13.2	Recovering deleted files
Autopsy	4.14.0	Forensic analysis of VM images

While conducting digital forensics, generally accepted rules, standards and procedures must be followed (Mehreen and Aslam, 2015). In conducting this forensic investigation, the four stages of identification, preservation, analysis and presentation of digital evidence (McKemmish, 1999) were followed.

3.3.1 Preparation

Dropbox requires an email address to sign up for the service. The email account dfimlabs@gmail.com was created and used to sign up on *dropbox.com* using the *Signup with Google* option. After signing up on the host machine, *Windows 10 Pro* 64-bit VM was created using *VMWare Workstation Pro* and a user account with the email address dfimlabs@outlook.com set up. A Windows update was then performed to the latest version to get the latest features and security fixes. Following the update, Windows update was paused for 35 days using the *Windows Update Settings* feature. This was to ensure that no further updates occur during the experiment, especially when taking snapshots for dead forensics. *Snapshot 1: Base VM* was then taken. From this snapshot, other snapshots were taken for dead and live forensic analysis, as shown in Figure 6. Snapshot 6 was taken twice because *EaseUS Data Recovery Wizard* software was installed after taking the initial snapshot with the other tools installed.

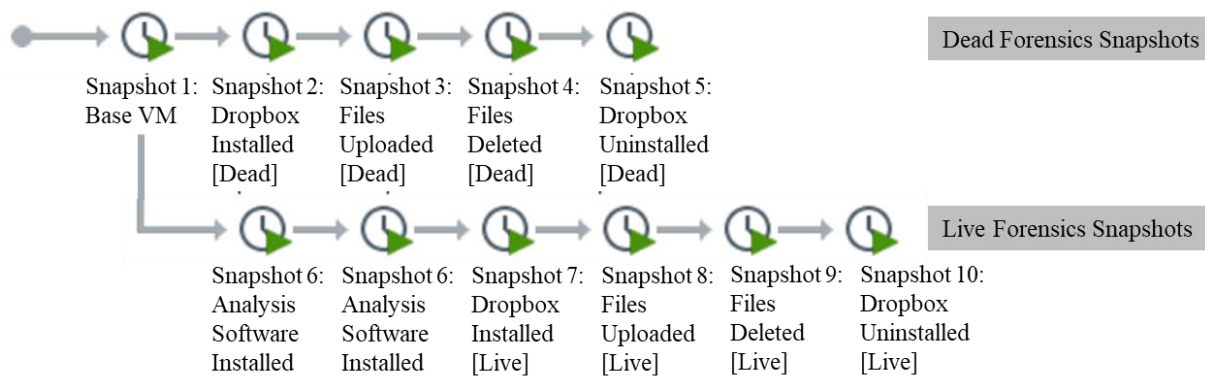


Figure 6 VM Snapshots for Live and Dead Forensics

Five VMs were derived from the snapshots for dead forensic investigation as detailed in Table 2.

Table 2 Virtual Machines for Dead Forensics

Snapshot	VM	Description
Snapshot 1	Base-VM	Windows 10 Pro 64-bit with the latest windows update. Specifications: 2GB RAM, 32GB HDD, 2vCPUs
Snapshot 2	Install-VM	Dropbox Windows Client installed
Snapshot 3	Upload-VM	Documents uploaded in the Dropbox folder
Snapshot 4	Deleted-VM	Documents deleted from the Dropbox folder
Snapshot 5	Uninstall-VM	Dropbox uninstalled using the Windows Programs and Features

The VMs were derived as follows. *Snapshot 1: Base-VM* was taken after updating Windows 10 and disabling further updates as explained earlier. This state represented the Base-VM. Dropbox was then installed, and *Snapshot 2: Dropbox Installed[Dead]* taken. This state represented the Install-VM. Three files `keep file.txt`, `delete file.txt` and `shift delete file.txt` were uploaded to the Dropbox synchronisation folder and allowed to sync with the Dropbox server. *Snapshot 3: Files Uploaded[Dead]* was then taken. This state represented Upload-VM. Two of the files `delete file.txt` and `shift delete file.txt` were then deleted using the 'Delete' button and 'Shift + Delete' buttons, respectively. *Snapshot 4: Files Deleted[Dead]* was then taken. This state represented the Deleted-VM.

In the last step, Dropbox was uninstalled, and *Snapshot 5: Dropbox Uninstalled[Dead]* taken. This state represented Uninstall-VM. For each of the snapshots taken, *VMware Workstation* created a VMDK file and VMEM file representing the hard disk and memory of the associated virtual machine respectively. The VMDK files would then be identified later as sources of digital evidence for the investigation and their forensic copies acquired for dead forensic analysis.

After taking *Snapshot 5: Dropbox Uninstalled[Dead]*, *VMWare Workstation Pro Snapshot Manager* was used to revert to *Snapshot 1: Base VM*. Live forensics snapshots (Snapshots 6-10) were derived from *Snapshot 1: Base VM* as shown in Figure 7 as follows. The analysis tools including *Regshot*, *Glasswire*, *Mirekrosoft Install Monitor*, *Process Monitor*, *Process Explorer*, *DB Browser for SQLite*, *Magnet Forensics Dropbox Decryptor* and *EaseUS Data Recovery Wizard* were installed. A snapshot of the VM was then taken and named *Snapshot 6: Analysis Tools Installed*.

The analysis tools were then run to monitor the network connection and changes to the registry and file system during Dropbox installation. These tools comprised of *Regshot*, *Glasswire*, *Mirekrosoft Install Monitor*, *Process Monitor*, and *Process Explorer*. *Regshot* was used to take a snapshot of the registry before Dropbox installation. Dropbox was subsequently installed, and the changes captured using the tools. A second snapshot of the registry was taken using *Regshot* and a comparison file generated with the registry changes made by Dropbox when installed. A snapshot of the VM was then taken and named *Snapshot 7: Dropbox Installed[Live]*.

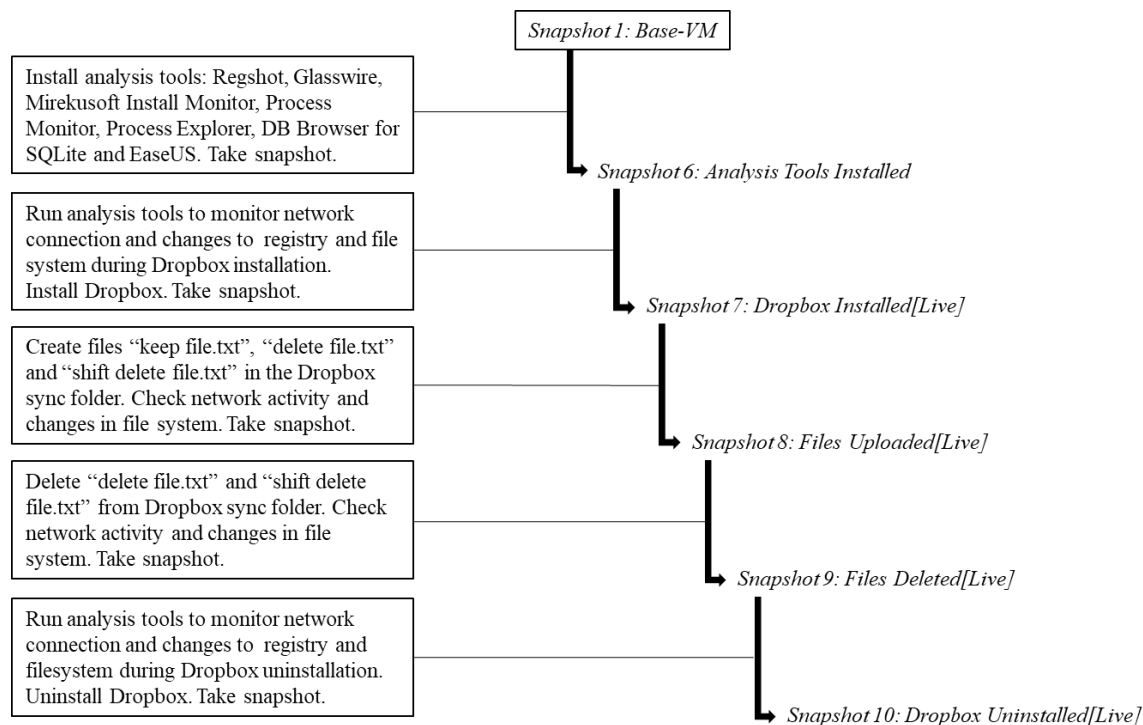


Figure 7 Creation of Live Forensics Snapshots

To investigate changes during file upload, the files *keep file.txt*, *delete file.txt* and *shift delete file.txt* were added to the Dropbox sync folder. Network activity and changes in the file system were monitored. A snapshot of the VM was then taken and named *Snapshot 8: Files Uploaded[Live]*. To investigate changes due to deletion of files, *delete file.txt*, and *shift delete file.txt* were deleted from Dropbox sync folder. The *delete file.txt* file was deleted normally by selecting the file and pressing ‘delete’ button. The *shift delete file.txt* file was deleted by selecting the file and pressing ‘shift + delete’ buttons for permanent deletion. The analysis tools were used to monitor network activity and changes in the file system in the process. A snapshot of the VM was then taken and named *Snapshot 9: Files Deleted[Live]*.

To check changes made during uninstallation, analysis tools were launched to monitor the network connection and changes to registry and filesystem during Dropbox uninstallation. *Regshot* was used to take a snapshot of the registry before uninstalling Dropbox. Subsequently, Dropbox was uninstalled, and the changes noted. A second snapshot of the registry was taken using *Regshot* and a comparison file generated with the registry changes made by Dropbox when uninstalled. A snapshot of the VM was then taken and named *Snapshot 10: Dropbox Uninstalled[Live]*. This marked the end of live forensics.

The VMs were preferred to physical hard drives as they are quick to set up and analyse different configurations without having to re-configure (Mehreen and Aslam, 2015). The VMs were set up using minimal memory and storage. The minimal configuration reduces the storage space required for the VMs and the forensic images that would be created during the experiment. Secondly, it reduces the time required to analyse the data resulting from the experiment. Lastly, if pertinent data can be located on a minimalist configuration, then it is more likely that such artefacts would exist in larger systems (Quick and Choo, 2013b). In addition, VM snapshots have been found to be efficient in cloud investigations (Rani and Geethakumari, 2015).

3.3.2 Identification of Digital Evidence

The Virtual Machine Disk (VMDK) files were identified as files which would contain the artefacts needed to conduct the analysis. The VMDK files for snapshots 1-5 were identified for dead forensic analysis.

3.3.3 Preservation of Digital Evidence

Digital forensic investigation requires that analysis is done on a forensic copy (McKemmish, 2008; ACPO, 2012). To preserve the evidence, *Access Data FTK Imager* was used to create copies of the VMs created. This was achieved by creating forensic copies of the identified VMDK files in the E01 container format. E01 format was used as it has a built-in checksum to check the integrity of images. It also provides compression, and this was important as there was a lot of free space in the VMDK files. The VMDK files were compressed from 32GB to 8GB images in the E01 format. The E01 format is also accepted in the forensic community and is recognised as an industry standard for storing forensic images (Lyons, 2016). The integrity of the VMDK copies was verified by calculating the hash of the copies and comparing them with those of their origin. Table 3 shows the VM image files created from the VMDK files and their checksums.

Table 3 VM Images and Checksums

VM Image	MD5 Checksum	SHA1 Checksum
Base-VM.E01	cf9a01165cca3038e1e202139065c94a	b8dc0264c7be89db7fb6dff1184a15b35efd1f72
Install-VM.E01	a91801722bc4b853fdf849a8a5fcbf13	7ad4253c69a2bac659edc8312a8fd6780d80b7c4
Upload-VM.E01	302f812e06c651f9e627702678e05a1b	4ca678d970cf52e32337b4c2318d704866bb94ac
Deleted-VM.E01	1b09da62a4ceb64a9164f874048fa07f	88a246040007b66191ddd1beb85fbd6185548c52
Uninstall-VM.E01	f02478805019a6ba56ebbd28d59bec08	f02699eef5f97c0022d2740acbb76171e43dad40

3.3.4 Analysis of Digital Evidence

The images created were analysed using *Autopsy* and *Access Data FTK Imager* to find out the Dropbox data remnants left in the registry and file system as suggested in previous research (Quick and Choo, 2013b; Amirullah, Riadi and Luthfi, 2016). Attempts were also made to recover files deleted during uninstallation. Similarly, several tools were used for live forensic analysis including *Mirekrosoft Install Monitor*, *GlassWire*, *EaseUS Data Recovery Wizard*, *DB Browser for SQLite*, *Registry Editor*, *Process Monitor*, *Process Explorer*, *Regshot*, and *Decwindbx*.

3.3.5 Reporting of Digital Evidence

The results obtained from the analysis phase are presented in **Chapter 4: Results and Discussion**. The results are those pertaining to changes made by Dropbox during installation and the data remnants left in the registry and file system when it is uninstalled. The significance of the findings to forensic investigators is also discussed.

3.4 Data Analysis

The data collected in the empirical study was primarily qualitative data (artefacts including registry entries, files, and directory structures) and as such, was subjected to qualitative analysis. Qualitative data tend to be rich and full (Saunders, Lewis and Thornhill, 2016) with strong potential for revealing complexity (Miles, Huberman and Saldaña, 2014). An important aspect of this study was to provide the significance of Dropbox artefacts found to forensic investigators. Therefore, from the onset of data collection, interpretation of what these meant was made by noting patterns, explanations, causal flows, and propositions (Miles, Huberman and Saldaña, 2014).

Several analysis tools were used, as shown in Table 1. In addition to the analysis tools, secondary data was used to build on the analysis of empirical data to provide additional or different knowledge, interpretations or conclusions (Saunders, Lewis and Thornhill, 2016).

3.5 Limitations of Methodology

In conducting the experiment, both live and dead forensics were carried out. Live forensics poses the danger of data modification while dead forensics does not guarantee the acquisition of volatile data such as network data (Lessing and Solms, 2008). By conducting both live and dead forensics, the shortcomings of each of were countered by the counterpart, i.e. live forensics addressed the shortcomings of dead forensics and vice-versa.

Some of the tools used for the experiment were limited in capacity and thus would not fully capture the data required. To address this, multiple complementing software was used, and the results obtained corroborated to build complete evidence.

There was the possibility of contamination of the VMs and associated images during the experiment. Consequently, copies of the VMs and images were created and stored separately from the working copy. In case of any inadvertent actions on the working copy, another copy would be made from the preserved images. For live forensics, snapshots were taken, which could be reverted to in case of undesired actions during the experiment.

3.6 Ethical Considerations

Research must be conducted in an ethical manner with no harm or risk to the researcher and the participants (Oates, 2006; Miles, Huberman and Saldaña, 2014). The empirical study was conducted in an ethical manner from data collection and analysis to reporting.

In data collection, objectivity was achieved by collecting data accurately and fully and avoiding subjectivity in what was collected. Other concerns in this phase were on the privacy, confidentiality and anonymity of participants (Miles, Huberman and Saldaña, 2014). While no human participants were involved, a new Dropbox account and associated email address were created for the purpose of conducting the study. Therefore, no pre-existing Dropbox user or user account was affected.

Objectivity during analysis is important to ensure the data collected is not misrepresented (Saunders, Lewis and Thornhill, 2016). This was realised by fully and accurately reporting on the data collected.

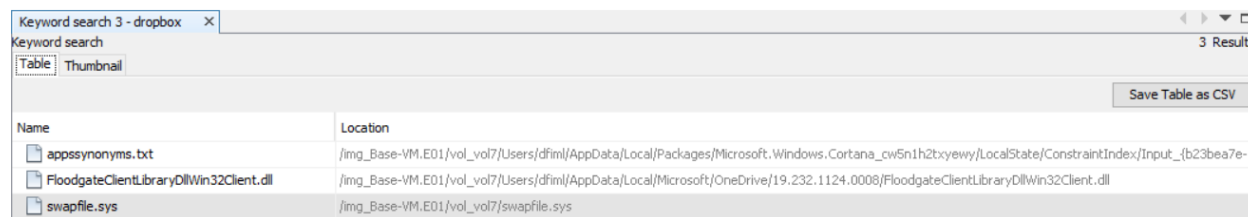
4 RESULTS AND DISCUSSION

This chapter analyses the results of the experiment described in **Chapter 3: Research Methodology**. The research concentrated on Dropbox registry and file system artefacts triggered by Dropbox user activities, including installation, file upload, file deletion, and uninstallation. Through this chapter, the second objective: *Investigate file system and registry artefacts created by Dropbox when installed on Windows 10*, and the third objective: *Investigate Dropbox artefacts left on Windows 10 file system and registry after uninstallation and their significance to forensic investigators*; are addressed.

The remainder of this chapter provides the artefacts related to each of the user activities and discusses their significance in Dropbox forensic investigations. First, artefacts related to Dropbox installation are discussed. A discourse of artefacts pertaining to upload and deletion of files on Dropbox follows. Lastly, artefacts left behind after uninstallation of Dropbox are examined, followed by a conclusion of the chapter.

4.1 Control (Base) Image Analysis

Analysis of the Base-VM image confirmed absence of data related to dfimlabs@gmail.com and Dropbox files. A keyword search for ‘dropbox’ found references in `appssynonyms.txt`, `FloodgateClientLibraryDllWin32Client.dll` and `swapfile.sys`, files which are associated with *Cortana*, *OneDrive*, and Windows swapping system respectively, as shown in Figure 8. *Cortana* can be used to search for files on Dropbox (Warren, 2015) and hence the presence of Dropbox reference in *Cortana*. Microsoft has integrated Dropbox into *Office* (Warren, 2014) and this explains the Dropbox reference in *OneDrive* as *Office* files in Dropbox can be directly edited from Windows PC and synced back to Dropbox. This suggests that *OneDrive* is used to cache the files during editing and synchronisation



Name	Location
appssynonyms.txt	/img_Base-VM.E01/vol_vol7/Users/dfim/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/LocalState/ConstraintIndex/Input_{b23bea7e-1
FloodgateClientLibraryDllWin32Client.dll	/img_Base-VM.E01/vol_vol7/Users/dfim/AppData/Local/Microsoft/OneDrive/19.232.1124.0008/FloodgateClientLibraryDllWin32Client.dll
swapfile.sys	/img_Base-VM.E01/vol_vol7/swapfile.sys

Figure 8 Artefacts with Dropbox reference in Base VM

While references to Dropbox exists in the Base-VM, it does not necessarily point to the installation and use of Dropbox (Quick *et al.*, 2014). The control VM shows that matches for Dropbox may occur even without user activity relating to Dropbox. Therefore, the search results must be understood in context.

4.2 Dropbox Installation

Artefacts created by Dropbox during installation were determined through live forensics and dead forensic analysis of Install-VM image. When installing Dropbox, the application makes calls to dropbox-dns.com, dropbox.com, and several dropbox.com subdomains over HTTPS as listed in Figure 9. HTTPS is a secure protocol (Rescorla, 2000); therefore, it can be assumed that during installation, data is securely transferred between Dropbox servers and the client machine.



Figure 9 Dropbox Installation Network Activity

A DNS lookup of dropbox.com on <https://who.is> reveals the IP address to be 162.125.6.1 registered to Dropbox Inc, in California, USA, as shown in Figures 10 and 11. The lookup also identifies dropbox-dns.com as the canonical name (CNAME) record for dropbox.com, i.e. dropbox-dns.com points to dropbox.com, which in turn points to the IP address 162.125.6.1. The presence of this IP address on the network traffic, or the domain names in the browser, would inform investigators of the presence of Dropbox activity on the client machine.

Dropbox is registered under Dropbox Inc. Therefore, when requesting for evidence from the CSP, investigators would have to contact Dropbox Inc. and comply with USA legal requirements as the company resides there.

DNS Records for dropbox.com

Hostname	Type	TTL	Priority	Content
www.dropbox.com	A	59		162.125.6.1
www.dropbox.com	AAAA	59		2620:100:601c:1::a27d:601
www.dropbox.com	CNAME	43		www.dropbox-dns.com

Figure 10 Dropbox Domain IP Address

```
Registrant Organization: Dropbox, Inc.  
Registrant State/Province: CA  
Registrant Country: US  
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/dropbox.com  
Admin Organization: Dropbox, Inc.  
Admin State/Province: CA  
Admin Country: US  
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/dropbox.com  
Tech Organization: Dropbox, Inc.  
Tech State/Province: CA  
Tech Country: US
```

Figure 11 Dropbox Registration Information

4.2.1 Files System Artefacts

4.2.1.1 Browser

Dropbox download activity can be traced within the browser, including web search for Dropbox, Dropbox URLs accessed, and Dropbox cookies as shown in Figures 12, 13 and 14. In addition to these, the artefacts contain the timestamps and accounts used to access Dropbox, information which can be used to build a timeline of events and tie the suspect to the crime.

Source File	Domain	Text	Program Name	Date Accessed	Data Source
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Install-VM.E01

Figure 12 Dropbox Search on Microsoft Edge in Install-VM

Source File	URL	Program Name	Domain	Username	Data Source
WebCacheV01.dat	https://www.dropbox.com/profile_services/open_identity_...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/profile_services/open_identity_...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/profile_services/open_identity_...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/profile_services/open_identity_...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/install	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/install	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/install	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/google/authcallback?state=AC...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/google/authcallback?state=AC...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/google/authcallback?state=AC...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01
WebCacheV01.dat	https://www.dropbox.com/google/authcallback?state=AC...	Microsoft Edge	www.dropbox.com	dfiml	Install-VM.E01

Figure 13 URLs Accessed on Microsoft Edge in Install-VM

Source File	URL	Name	Value	Program Name	Domain	Data Source
WebCacheV01.dat	dropbox.com		en	Microsoft Edge	dropbox.com	Install-VM.E01
WebCacheV01.dat	dropbox.com	t	RM8rwKqnOxTg2VCJ6w5Jk31r	Microsoft Edge	dropbox.com	Install-VM.E01
WebCacheV01.dat	dropbox.com		en	Microsoft Edge	dropbox.com	Install-VM.E01
WebCacheV01.dat	dropbox.com	t	RM8rwKqnOxTg2VCJ6w5Jk31r	Microsoft Edge	dropbox.com	Install-VM.E01
WebCacheV01.dat	dropboxstatic.com	__cfduid	d7fa6fb3038a289a326301f883b0669991582986466	Microsoft Edge	dropboxstatic.com	Install-VM.E01
WebCacheV01.dat	dropboxstatic.com	__cfduid	d7fa6fb3038a289a326301f883b0669991582986466	Microsoft Edge	dropboxstatic.com	Install-VM.E01

Figure 14 Dropbox Cookies in Microsoft Edge in Install-VM

A keyword search of dfimllabs@gmail.com returned a hit in C:\Users\dfiml\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wkyb3d8bbwe\AC\MicrosoftEdge\User\Default\Recovery\Active\{A5B61BB7-2182-4DE1-97A2-3B0AB5B394C6}.dat associated with the account log on to dropbox.com using *Google OAuth* as shown in Figure 15. The artefact path contained *Microsoft Edge*, suggesting the use of the browser to log on to *Dropbox* via *Google OAuth*.

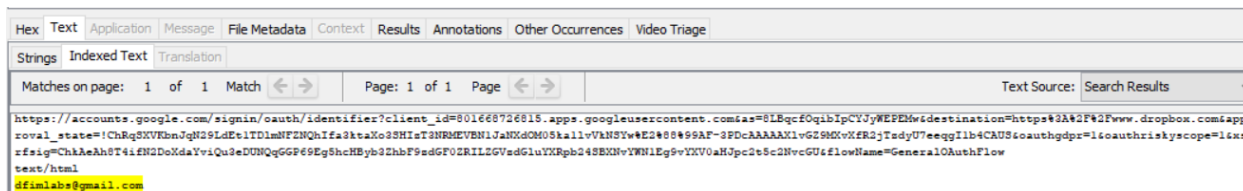


Figure 15 Dropbox User Email in Install-VM

4.2.1.2 Installation Directories

Dropbox installer was downloaded to the Downloads directory. It was found in the path `C:\Users\dfiml\Downloads\DropboxInstaller.exe`. During installation, Dropbox installed program execution files in various directories including Program Files, ProgramData, and Windows directories. `C:\Program Files (x86)\Dropbox` folder contained files related to running, updating and uninstalling Dropbox including `Dropbox.exe`, `DropboxUninstaller.exe`, `dbxsvc.exe`, `DropboxUpdate.exe`; and several `.dll` files under three folders namely Client, CrashReports and Updates. `C:\ProgramData\Dropbox` folder contained log files related to Dropbox updates. Other Dropbox related files were found in `C:\Windows\System32` and `C:\Windows\SysWOW64`.

4.2.1.3 AppData

AppData folder stores data and settings for Windows applications. The folder has three sub-folders – Local, LocalLow and Roaming. Local folder stores data specific to a single computer and it is never synced from computer to computer even when in a domain. LocalLow folder is similar to the Local folder but is for less trusted applications that run with more restricted security settings. Roaming folder contains data that would allow a user with a roaming profile in a domain to roam from computer to computer (Hoffman, 2017). It was observed that Dropbox had data in all the three folders as follows.

In `C:\Users\dfiml\AppData\Local\Dropbox`, the files and folders in Figure 16 were present. The folder contained several `.db` and `.dbx` database files which normally would be plaintext and encrypted SQLite files, respectively. However, this might not always be the case as sometimes, these files could be Base64 encoded (Picasso, 2017).

Name	Date modified	Type	Size
avatar_cache	14/03/2020 13:13	File folder	
Crashpad	14/03/2020 13:07	File folder	
CrashReports	14/03/2020 13:04	File folder	
events	27/04/2020 15:33	File folder	
instance_db	27/04/2020 15:34	File folder	
instance1	27/04/2020 17:11	File folder	
logs	14/03/2020 13:08	File folder	
machine_storage	14/03/2020 13:08	File folder	
metrics	14/03/2020 13:07	File folder	
QuitReports	27/04/2020 15:34	File folder	
Dropbox.exe	27/04/2020 15:34	Text Document	3 KB
host	27/04/2020 15:34	Data Base File	1 KB
host.dbx	14/03/2020 13:13	DBX File	1 KB
info.json	27/04/2020 15:34	JSON File	1 KB
unlink	14/03/2020 13:13	Data Base File	1 KB

Figure 16 Dropbox Files and Folders in AppData\Local\Dropbox

The instance_db folder had instance.dbx file while instance1 folder had several configuration files, as shown in Figure 17.

Name	Date modified	Type	Size
sync	27/04/2020 15:33	File folder	
aggregation.dbx	14/03/2020 13:13	DBX File	12 KB
avatarcache	14/03/2020 13:13	Data Base File	12 KB
browse_cache	27/04/2020 15:34	Data Base File	12 KB
config.dbx	27/04/2020 17:11	DBX File	52 KB
contacts_polaris	27/04/2020 15:27	Data Base File	40 KB
folder_preferences	27/04/2020 15:33	Data Base File	16 KB
home	14/03/2020 13:13	Data Base File	84 KB
icon	14/03/2020 13:13	Data Base File	28 KB
onboarding	27/04/2020 15:33	Data Base File	28 KB
photo.dbx	27/04/2020 15:33	DBX File	52 KB
preview_cache	14/03/2020 13:13	Data Base File	12 KB
unlink	14/03/2020 13:13	Data Base File	1 KB

Figure 17 Dropbox Files and Folders in AppData\Local\Dropbox\instance1

Table 4 lists the database files in the Local\Dropbox folder and their description. Using *DB Browser for SQLite*, contents in avatarcache.db, home.db, icon.db, and preview_cache could be parsed. The remaining .db and .dbx files could not be parsed as they were not in the SQLite format.

Further inspection of the files using *HxD* confirmed that those that failed to open were not in SQLite format. As noted by Picasso (2017), the `.db` and `.dbx` files are not necessary in plaintext. They may be encrypted or encoded in Base64. Attempts to decrypt the files using *Decwindbx* and *Magnet Forensics Dropbox Decryptor* were unsuccessful despite being successfully used in previous research (Malik, Shashidhar and Chen, 2015a; Amirullah, Riadi and Luthfi, 2016; Picasso, 2017). This could be attributed to changes in the encryption mechanism deployed by Dropbox, which has not been updated in these tools. From previous research, the details of some of these files were determined.

Table 4 Dropbox Database Files

File	Description
host.db and host.dbx	Includes the path for Dropbox file storage in Base64 string encoded text (Quick and Choo, 2013b)
unlink.db	A binary file
instance_db\instance.dbx	Encrypted file. Content not determined.
instance1\aggregation.dbx	Contains timestamp values, server paths, and a blocklist value and a snapshot table (Malik, Shashidhar and Chen, 2015b).
instance1\avatarcache.db	Contains account avatar information
instance1\browse_cache.db	A binary file
instance1\config.dbx	An encrypted file containing user email address, display name, host ID, Dropbox folder path, list of recently changed files, among other settings (Malik, Shashidhar and Chen, 2015a; Amirullah, Riadi and Luthfi, 2016).
instance1\contact_polaris.db	A binary file
instance1\folder_preferences.db	A binary file
instance1\home.db	Contains information related to activity feed and calendar items among other settings.
instance1\icon.db	Contains information on the icons used.
instance1\onboarding.db	A binary file
instance1\photo.dbx	Encrypted file. Content not determined.
instance1\preview_cache.db	Contains an assets table
instance1\unlink.db	A binary file
info.json	Contains info on Dropbox account type, subscription type, sync folder path, host ID

It was also noted that some of the files used in older versions of Dropbox were no longer present. For example, sigstore.dbx, filecache.dbx, deleted.dbx, notification.dbx and dropbox.db did not exist. New files absent in the older versions of Dropbox were also found, including browse_cache.db, contacts_polaris.db, folder_preferences.db, onboarding.db, avatacache.db, home.db, icon.db and preview_cache.db among others.

In C:\Users\dfiml\AppData\Roaming\Dropbox Dropbox file related to installer was found as shown in Figure 18.

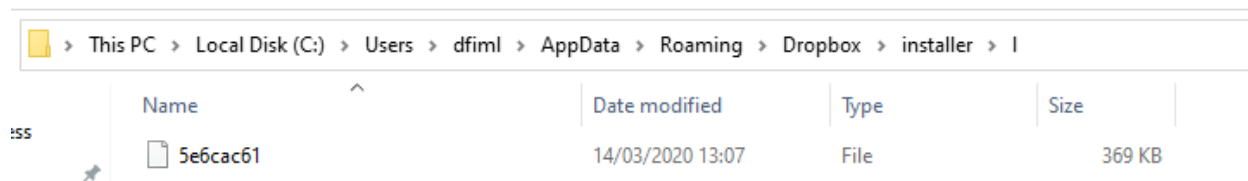


Figure 18 Files in AppData\Roaming\Dropbox

In C:\Users\dfiml\AppData\LocalLow\Microsoft\CryptnetUrlCache data related to access to dropbox.com was found in the MetaData folder.

4.2.1.4 Prefetch Files

Prefetch files provide valuable information that can be used to determine inter alia the first and last time a program was run, the location from which it was run, and the files that were executed during the run (Quick *et al.*, 2014). Dropbox prefetch files were found in C:\Windows\Prefetch, as shown in Figure 19.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
DROPBOX.EXE-41A1197E.pf				2020-02-29 17:26:59 EAT	2020-02-29 17:26:59 EAT	2020-02-29 17:26:59 EAT	2020-02-29 17:26:53 EAT	34404
DROPBOX.EXE-A0062768.pf				2020-02-29 17:25:36 EAT	2020-02-29 17:25:36 EAT	2020-02-29 17:25:36 EAT	2020-02-29 17:25:36 EAT	27722
DROPBOXCLIENT_91.4.548.EXE-944B0CE5.pf				2020-02-29 17:24:57 EAT	2020-02-29 17:24:57 EAT	2020-02-29 17:24:57 EAT	2020-02-29 17:24:57 EAT	48334
DROPBOXCRASHHANDLER.EXE-3BF847B4.pf				2020-02-29 17:29:00 EAT	2020-02-29 17:29:00 EAT	2020-02-29 17:29:00 EAT	2020-02-29 17:29:00 EAT	6613
DROPBOXINSTALLER.EXE-4DA08EFE.pf				2020-02-29 17:24:16 EAT	2020-02-29 17:24:16 EAT	2020-02-29 17:24:16 EAT	2020-02-29 17:24:16 EAT	7055
DROPBOXUPDATE.EXE-89BC44CC.pf				2020-02-29 17:24:23 EAT	2020-02-29 17:24:23 EAT	2020-02-29 17:24:23 EAT	2020-02-29 17:24:17 EAT	19616
DROPBOXUPDATE.EXE-E72FEFE1.pf				2020-02-29 17:29:10 EAT	2020-02-29 17:29:10 EAT	2020-02-29 17:29:10 EAT	2020-02-29 17:24:18 EAT	29514
DROPBOXUPDATEONDEMAND.EXE-83F9CACE.pf				2020-02-29 17:26:43 EAT	2020-02-29 17:26:43 EAT	2020-02-29 17:26:43 EAT	2020-02-29 17:26:43 EAT	3560

Figure 19 Dropbox Prefetch Files in Install-VM

4.2.1.5 Link Files

Link files related to Dropbox were found on the Desktop and Start Menu, as shown in Figure 20. Both files pointed to Dropbox.exe in Program Files used to launch the application.



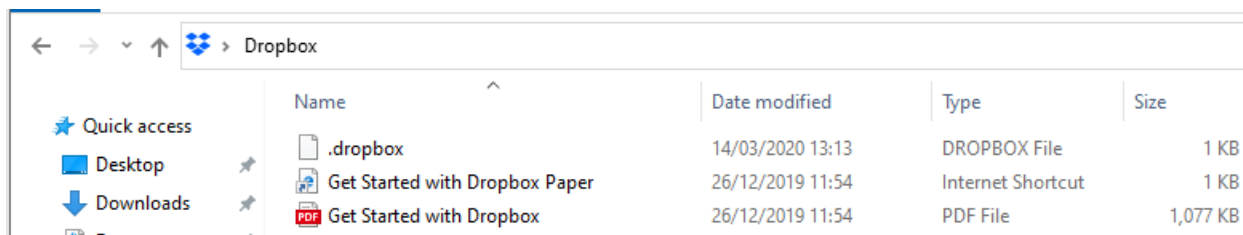
Name	Location
 Dropbox.lnk	/img_Install-VM.E01/vol_vol7/Users/dfiml/Desktop/Dropbox.lnk
 Dropbox.lnk	/img_Install-VM.E01/vol_vol7/ProgramData/Microsoft/Windows/Start Menu/Programs/Dropbox/Dropbox.lnk

Figure 20 Dropbox Link Files in Install-VM

4.2.1.6 Synchronisation Folder

Dropbox created a synchronisation folder under C:\Users\dfiml as C:\Users\dfiml\Dropbox as shown in Figures 21 and 22. Three files were present by default .dropbox, Get Started with Dropbox.pdf and Get Started with Dropbox Paper.url. Mehreen and Aslam (2015) had noted that the .dropbox extension file contained a numerical value and suggested future investigation on the artefact since no research had investigated its purpose yet.

The .dropbox file contained the string {"tag": "dropbox", "ns": 6848688752, "n": true}. The file is used by Dropbox application to track the identity of the shared folder so that in case it is moved, it is still recognised as the shared folder. Deleting the file would render the folder unrecognisable to Dropbox as the shared folder (StackExchange, 2012). Get Started with Dropbox.pdf contained information on how to start using Dropbox. Get Started with Dropbox Paper.url contained a URL to dropbox.com landing on a page with information on getting started with Dropbox.



Name	Date modified	Type	Size
.dropbox	14/03/2020 13:13	DROPBOX File	1 KB
Get Started with Dropbox Paper	26/12/2019 11:54	Internet Shortcut	1 KB
Get Started with Dropbox	26/12/2019 11:54	PDF File	1,077 KB

Figure 21 Files in Dropbox Synchronisation Folder - Live Forensics

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
.dropbox			0	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	42
.dropbox.cache				2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	56
Get Started with Dropbox Paper.url			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	240
Get Started with Dropbox Paper.url:com.dropbox.attrs			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	26
Get Started with Dropbox.pdf			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	1102331
Get Started with Dropbox.pdf:com.dropbox.attrs			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:38 EAT	26
[current folder]				2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 17:36:34 EAT	56
[parent folder]				2020-02-29 17:36:34 EAT	2020-02-29 17:36:34 EAT	2020-02-29 17:36:34 EAT	2020-01-16 19:05:50 EAT	256
desktop.ini			0	2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	176

Figure 22 Files in Dropbox Synchronisation Folder in Install-VM

4.2.2 Registry Artefacts

Registry contained artefacts relating to Dropbox version, installation directory, installation time, synchronisation folder, and encryption keys used to encrypt and decrypt the Dropbox .dbx files. The Dropbox artefacts were observed in HKEY_Local_Machine, HKEY_Classes_Root, HKEY_Current_User, and HKEY_Users registry hives.

4.2.2.1 Directory Structure Artefacts

Dropbox synchronisation and client version folders were identified, as shown in Table 5.

Table 5 Registry Directory Structure Artefacts in Install-VM

Artefact	Description
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager\Dropbox!S-1-5-21-3933750032-3930657141-318433956-1001!personal\UserSyncRoots\S-1-5-21-3933750032-3930657141-318433956-1001:"C:\Users\dfiml\Dropbox"	Dropbox synchronisation folder
HKLM\SOFTWARE\Classes\TypeLib\{527E621D-39D6-4627-8185-08F387A73307}\1.0\HELPDIR\:"C:\Program Files (x86)\Dropbox\Client\92.4.382"	Dropbox client version directory

4.2.2.2 Configuration Settings Artefacts

Configuration settings, including starting Dropbox on system startup and autoplay of content, were found, as shown in Table 6.

Table 6 Registry Configuration Settings Artefacts in Install-VM

Artefact	Description
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\Dropbox: ""C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup"	Dropbox auto-start
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\LocalServer32: ""C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /autoplay"	Auto-play content

4.2.2.3 Time-Related Artefacts

Time artefacts related to the installation of Dropbox were found in Unix hexadecimal timestamp, as shown in Table 7. They were converted to human readable time using *Unix Hex Timestamp Converter* found online at <https://www.epochconverter.com/hex>. The artefacts establish the time Dropbox was installed on the user computer.

Table 7 Registry Time Related Artefacts in Install-VM

Artefact	Time
HKLM\SOFTWARE\WOW6432Node\DropboxUpdate\Update\ClientState\{CC46080E-4C33-4981-859A-BBA2F780F31E}\InstallTime: 0x5E6CAC5E	Saturday, March 14, 2020 1:05:18 PM GMT+03:00
HKLM\SOFTWARE\WOW6432Node\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\InstallTime: 0x5E6CAC2F	Saturday, March 14, 2020 1:04:31 PM GMT+03:00

4.2.2.4 Encryption Artefacts

Two registry keys containing Dropbox users keys were found, as shown in Table 8. These keys were ks and ks1. From previous work (Picasso, 2017), ks key can be used to derive .dbx decryption key for .dbx files in AppData\Local\Dropbox\instance_db while ks1 key

can be used to derive .dbx decryption key for .dbx files in AppData\Local\Dropbox\instance1.

Table 8 Registry Encryption Artefacts in Install-VM

Artefact	Description
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\ks	User key for decrypting files in instance_db folder
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\ks1	User key for decrypting files in instance1 folder
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\ks\Client-p: 00 00 00 00 10 00 00 00 FF BE ED 0C 98 BC FF 81 EB 36 55 21 26 79 43 16 17 89 BE F7 18 80 88 41 13 A8 B5 11 12 57 93 90 00	ks user key value
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\ks1\Client-p: 00 00 00 00 10 00 00 00 D6 EF F5 A5 80 B8 87 95 44 A3 63 07 55 EE A4 6B 85 7E 32 05 BE 35 AE C1 E8 88 5E F6 4F 84 A0 1A 00	ks1 user key value

4.3 File Upload

To analyse artefacts created during file upload, live forensics was conducted alongside dead forensic analysis of the Upload-VM image. Three files keep file.txt, delete file.txt and shift delete file.txt were added to the Dropbox synchronisation folder. The files were automatically uploaded to the Dropbox server and marked green once the upload completed, as shown in Figure 23.

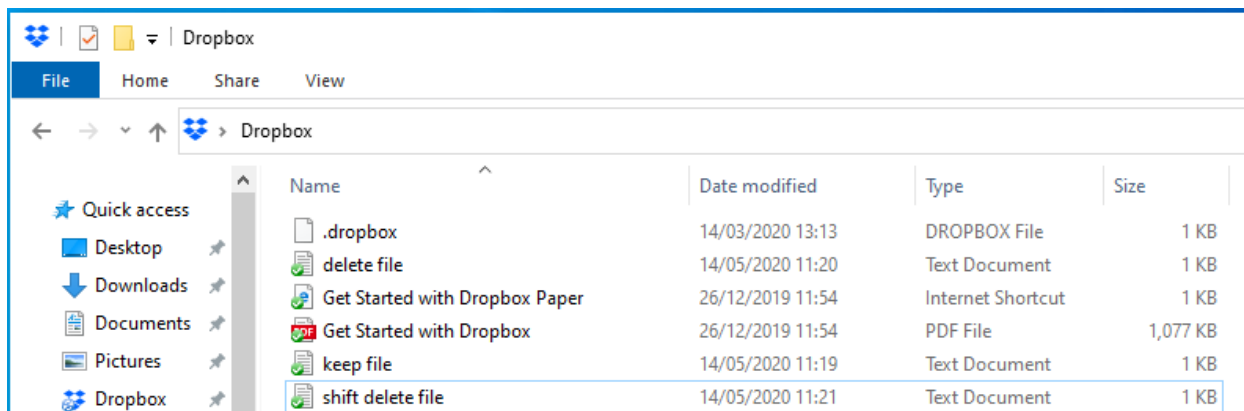


Figure 23 Files Uploaded in Dropbox Sync Folder - Live Forensics

Analysis of the Upload-VM image revealed the existence of the same files and the timestamps they were created, accessed, and modified, as shown in Figure 24.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
.dropbox				2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT
Get Started with Dropbox Paper.url				2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:47:54 EAT	2020-02-29 17:36:38 EAT
Get Started with Dropbox Paper.url:com.dropbox.attrs				2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:47:54 EAT	2020-02-29 17:36:38 EAT
Get Started with Dropbox.pdf				2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:43 EAT	2020-02-29 17:36:38 EAT
Get Started with Dropbox.pdf:com.dropbox.attrs				2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:43 EAT	2020-02-29 17:36:38 EAT
desktop.ini				2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 17:58:31 EAT	2020-02-29 17:36:42 EAT
delete file.txt				2020-02-29 17:47:59 EAT	2020-02-29 17:57:08 EAT	2020-02-29 17:56:56 EAT	2020-02-29 17:47:27 EAT
delete file.txt:com.dropbox.attrs				2020-02-29 17:47:59 EAT	2020-02-29 17:57:08 EAT	2020-02-29 17:56:56 EAT	2020-02-29 17:47:27 EAT
keep file.txt				2020-02-29 17:47:27 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17:47:50 EAT	2020-02-29 17:47:27 EAT
keep file.txt:com.dropbox.attrs				2020-02-29 17:47:27 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17:47:50 EAT	2020-02-29 17:47:27 EAT
shift delete file.txt				2020-02-29 17:57:15 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17:57:18 EAT	2020-02-29 17:57:15 EAT
shift delete file.txt:com.dropbox.attrs				2020-02-29 17:57:15 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17:57:18 EAT	2020-02-29 17:57:15 EAT

Figure 24 Files Uploaded in Dropbox Sync Folder in Install-VM

The information would be useful to investigators in determining the files uploaded to the Dropbox server, which would be requested from Dropbox Inc. to corroborate those found on the client machine. In addition, the timestamps would help determine when such files were created, modified or accessed and help in building the timeline of events of the case.

4.4 File Deletion

To analyse data remnants when a user deletes a file, live analysis was conducted alongside dead analysis on the Deleted-VM. Two files previously created in the Dropbox synchronisation folder were deleted. The `delete file.txt` was deleted by selecting the file and pressing the delete

button. The shift delete file.txt was deleted by selecting the file and pressing shift + delete keys for a 'permanent' delete.

The delete file.txt file was located in the recycle bin while shift delete file.txt wasn't. Using *EaseUS Data Recovery Wizard*, a live scan for deleted files was conducted in the Dropbox synchronisation folder, and both files were found, as shown in Figures 25 and 26.

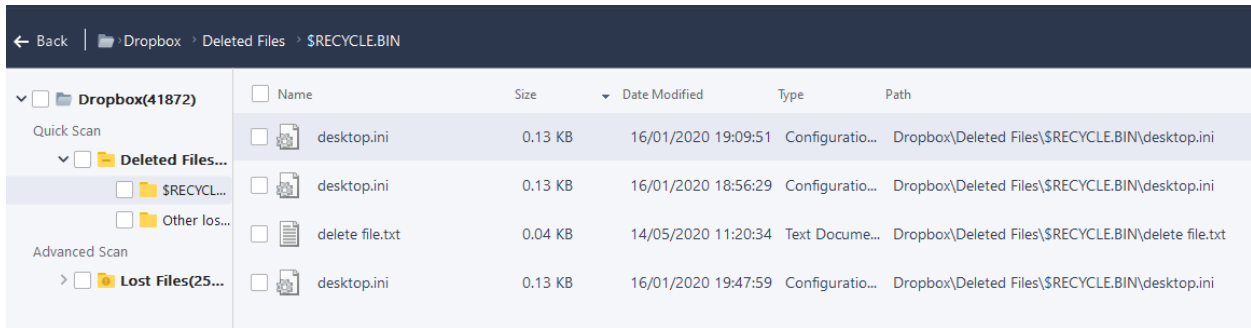


Figure 25 Deleted 'delete file.txt' Found in Recycle Bin

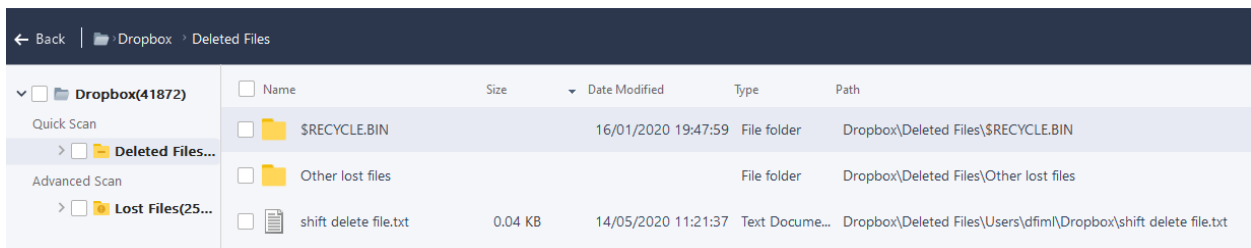


Figure 26 Deleted 'shift delete file.txt' Found in Dropbox Sync Folder

Using *Autopsy*, an analysis was done on the Deleted-VM image to locate and recover the files, as shown in Figure 27. The files were located and recovered successfully. This demonstrates that it is possible to recover Dropbox user files that have been deleted from the client machine.

/img_Deleted-VM.E01/vol_vol7/Users/dfiml/Dropbox								
Table Thumbnail Save T								
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	
.dropbox.cache				2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	
.dropbox			0	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	
Get Started with Dropbox Paper.url			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 20:36:31 EAT	2020-02-29 17:36:38 EAT	
Get Started with Dropbox Paper.url:com.dropbox.attrs			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 20:36:31 EAT	2020-02-29 17:36:38 EAT	
Get Started with Dropbox.pdf			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:43 EAT	2020-02-29 17:36:38 EAT	
Get Started with Dropbox.pdf:com.dropbox.attrs			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:43 EAT	2020-02-29 17:36:38 EAT	
desktop.ini			0	2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 20:36:31 EAT	2020-02-29 17:36:42 EAT	
delete file.txt			0	2020-02-29 20:36:59 EAT	2020-02-29 20:36:59 EAT	2020-02-29 17:57:11 EAT	2020-02-29 17:47:27 EAT	
keep file.txt			0	2020-02-29 17:47:27 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17:47:50 EAT	2020-02-29 17:47:27 EAT	
keep file.txt:com.dropbox.attrs			0	2020-02-29 17:47:27 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17:47:50 EAT	2020-02-29 17:47:27 EAT	
shift delete file.txt			0	2020-02-29 17:57:15 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17:57:18 EAT	2020-02-29 17:57:15 EAT	
shift delete file.txt:com.dropbox.attrs			0	2020-02-29 17:57:15 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17:57:18 EAT	2020-02-29 17:57:15 EAT	

Figure 27 Deleted Files Found in Dropbox Sync Folder in Deleted-VM

4.5 Dropbox Uninstallation

The last step of this research was undertaken to assess the results of a user uninstalling the Dropbox client using *Programs and Features* in *Windows 10 Control Panel*. Live forensic was conducted as well as dead forensic analysis of the Uninstall-VM image. From both analyses, the presence of data remnants was established in the file system and registry.

4.5.1 File System Artefacts

4.5.1.1 Browser

Dropbox download activity could still be traced within the browser including web search for Dropbox, Dropbox URLs accessed, and Dropbox cookies as shown in Figures 28, 29 and 30. In addition to these, the artefacts contain the timestamps and accounts used to access Dropbox, information which can be used to build a timeline of events and tie the suspect to the crime.

Source File	Domain	Text	Program Name	Date Accessed	Data Source
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Uninstall-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Uninstall-VM.E01
WebCacheV01.dat	www.bing.com	microsoft change alternate email	Microsoft Edge	0000-00-00 00:00:00	Uninstall-VM.E01
WebCacheV01.dat	www.bing.com	dropbox	Microsoft Edge	0000-00-00 00:00:00	Uninstall-VM.E01

Figure 28 Dropbox Search on Microsoft Edge in Uninstall-VM

Source File	URL	Program Name	Domain	Username	Data Source
WebCacheV01.dat	https://www.dropbox.com/profile_services/open_identity...	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/profile_services/open_identity...	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/logout	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/logout	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/login?src=logout	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/login?src=logout	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/install	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/install	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/h	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/h	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/google/authcallback?state=AC...	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/google/authcallback?state=AC...	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01
WebCacheV01.dat	https://www.dropbox.com/google/authcallback?state=ACk...	Microsoft Edge	www.dropbox.com	dfiml	Uninstall-VM.E01

Figure 29 URLs Accessed on Microsoft Edge in Uninstall-VM

Source File	URL	Name	Value	Program Name	Domain	Data Source
WebCacheV01.dat	dropbox.com	en		Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	t	EqXeNCaskhrclO0-4M08OAw7	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	_gcd_au	1.1.1445646104.1582987731	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	_fbp	fb.1.1582987731671.1564505792	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	utag_main	v_id:0170916be3660069742a04be57bc010810028079007...	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	_ga	GA1.2.1762511100.1582987737	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	_gid	GA1.2.1840745940.1582987737	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	cto_bundle	jzUs3f9ITQI4T3l5NGrUu915WpUv21a51pMZWnkZUU1Z1dT...	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	last_active_role	personal	Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	SnapABugRef		Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	SnapABugHistory		Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	SnapABugUserAlias		Microsoft Edge	dropbox.com	Uninstall-VM.E01
WebCacheV01.dat	dropbox.com	blid		Microsoft Edge	dropbox.com	Uninstall-VM.E01

Figure 30 Dropbox Cookies in Microsoft Edge in Uninstall-VM

A keyword search of dfimllabs@gmail.com returned a hit in C:\Users\dfiml\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\RSU55P3K\pkg-loadable.min-vflsg-sUD[1].js-slack associated with the account log on to dropbox.com using Google OAuth as shown in Figure 31. The artefact path contained Microsoft Edge, suggesting the use of the browser to log on to Dropbox via Google OAuth.

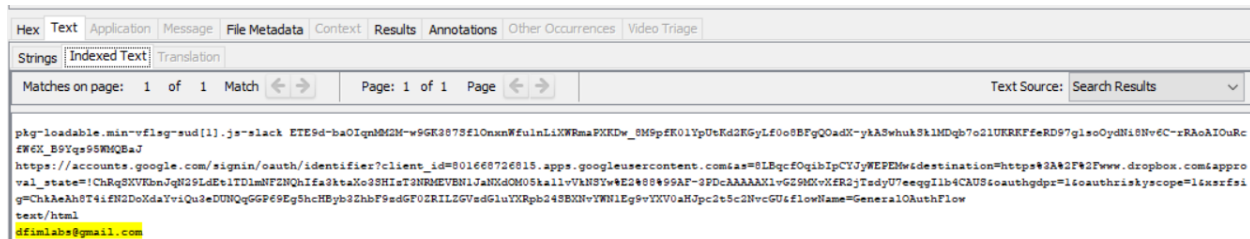


Figure 31 Dropbox User Email in Uninstall-VM

4.5.1.2 Installation Directories

Dropbox installer was still present in the Download folder. It was found in the path C:\Users\dfiml\Downloads\DropboxInstaller.exe. Dropbox folder and .dll files referencing Dropbox were found in Program Files directory using keyword search as shown in Figure 32. The ProgramData directory contained log files related to Dropbox update, which though marked as deleted could be recovered using *Autopsy* as shown in Figure 33. Keyword search of ‘Dropbox’ also returned references to a Dropbox folder and other files inside the ProgramData directory, as shown in Figure 34. The files found in ProgramData contained information related to Dropbox including search query, browser and search engine used, client version, installation directory, and application data stored in AppData.

Name	Location
Dropbox	/img_Uninstall-VM.E01/vol_vol7/Program Files (x86)/Dropbox
Newtonsoft.Json.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApps/Microsoft.Getstarted_8.2.22942.0_x64__8wekyb3d8bbwe/fmui/Newtonsoft.Json.dll
CsiImm.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApps/Microsoft.Office.OneNote_16001.12527.20128.0_x64__8wekyb3d8bbwe/CsiImm.dll
mso20imm.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApps/Microsoft.Office.OneNote_16001.12527.20128.0_x64__8wekyb3d8bbwe/mso20imm.dll
saext.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApps/Microsoft.Office.OneNote_16001.12527.20128.0_x64__8wekyb3d8bbwe/saext.dll
HxOutlookBackground.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApps/microsoft.windowscommunicationsapps_16005.12527.20152.0_x64__8wekyb3d8bbwe/HxOutlookBackground.dll
mso20imm.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApps/microsoft.windowscommunicationsapps_16005.12527.20152.0_x64__8wekyb3d8bbwe/mso20imm.dll
saext.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApps/microsoft.windowscommunicationsapps_16005.12527.20152.0_x64__8wekyb3d8bbwe/saext.dll

Figure 32 Dropbox Related Files in Program Files

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
DropboxUpdate.log-2020-02-29-16-29-00-563-3452-finished			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
DropboxUpdate.log-2020-02-29-17-29-00-551-3500-finished			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
[current folder]				2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 17:24:07 EAT	48
[parent folder]				2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 17:24:07 EAT	48
DropboxUpdate.log-2020-02-29-15-29-01-149-4852-finished			0	2020-02-29 18:29:18 EAT	2020-02-29 18:29:18 EAT	2020-02-29 18:29:18 EAT	2020-02-29 18:29:01 EAT	27390
DropboxUpdate.log-2020-02-29-18-13-47-361-5420-finished			0	2020-02-29 21:13:48 EAT	2020-02-29 21:13:48 EAT	2020-02-29 21:13:48 EAT	2020-02-29 21:13:47 EAT	26118
DropboxUpdate.log-2020-02-29-18-13-48-611-2464-finished			0	2020-02-29 21:13:48 EAT	2020-02-29 21:13:48 EAT	2020-02-29 21:13:48 EAT	2020-02-29 21:13:48 EAT	366
DropboxUpdate.log-2020-02-29-18-13-48-752-3548-finished			0	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:48 EAT	10814
DropboxUpdate.log-2020-02-29-18-13-49-252-3548-finished			0	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	366
DropboxUpdate.log-2020-02-29-18-13-49-424-3548-finished			0	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	938
DropboxUpdate.log-2020-02-29-18-13-49-486-3548-finished			0	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	2020-02-29 21:13:49 EAT	938

Figure 33 Dropbox Log Files in ProgramData in Uninstall-VM

Name	Location
Dropbox	/img_Uninstall-VM.E01/vol_vol7/ProgramData/Dropbox
Windows.edb	/img_Uninstall-VM.E01/vol_vol7/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.edb
edb.jtx	/img_Uninstall-VM.E01/vol_vol7/ProgramData/Microsoft/Search/Data/Applications/Windows/edb.jtx
edb0000B.jtx	/img_Uninstall-VM.E01/vol_vol7/ProgramData/Microsoft/Search/Data/Applications/Windows/edb0000B.jtx
MPLLog-20200116-185317.log	/img_Uninstall-VM.E01/vol_vol7/ProgramData/Microsoft/Windows Defender/Support/MPLLog-20200116-185317.log
MpWppTracing-20200229-10	/img_Uninstall-VM.E01/vol_vol7/ProgramData/Microsoft/Windows Defender/Support/MpWppTracing-20200229-102220-00000003-ffffff.bin
Dropbox	/img_Uninstall-VM.E01/vol_vol7/ProgramData/Microsoft/Windows/Start Menu/Programs/Dropbox

Figure 34 Dropbox Related Files in ProgramData in Uninstall-VM

Other artefacts returned by the keyword search included `swapfile.sys`, `$Extend/$UsnJrnl:$J`, `$LogFile`, `$MFT`, `$Recycle.Bin/S-1-5-21-3933750032-3930657141-318433956-1001/$RPMODOU.txt`, `Config.Msi/254f877.rbs`, `Config.Msi/254f877.rbs-slack` as shown in Figure 35. These artefacts contained information related to Dropbox logs, update, synchronisation folder path, deleted user files in the recycle bin, and link files.

Name	Location	Modified Time	Change Time	Access Time	Created Time
\$UsnJrnl:\$J	/img_Uninstall-VM.E01/vol_vol7/\$Extend/\$UsnJrnl:\$J	2020-01-17 05:52:55 EAT	2020-01-17 05:52:55 EAT	2020-01-17 05:52:55 EAT	2020-01-17 05:52:55 EAT
\$LogFile	/img_Uninstall-VM.E01/vol_vol7/\$LogFile	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT
\$MFT	/img_Uninstall-VM.E01/vol_vol7/\$MFT	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT
Recycle Bin Artifact	/img_Uninstall-VM.E01/vol_vol7/\$Recycle.Bin/S-1-5-21-393...	2020-02-29 17:47:59 EAT	2020-02-29 20:36:59 EAT	2020-02-29 17:57:11 EAT	2020-02-29 17:47:27 EAT
254f877.rbs	/img_Uninstall-VM.E01/vol_vol7/Config.Msi/254f877.rbs	2020-02-29 21:13:51 EAT	2020-02-29 21:13:51 EAT	2020-02-29 21:13:51 EAT	2020-02-29 21:13:51 EAT
254f877.rbs-slack	/img_Uninstall-VM.E01/vol_vol7/Config.Msi/254f877.rbs-slack	2020-02-29 21:13:51 EAT	2020-02-29 21:13:51 EAT	2020-02-29 21:13:51 EAT	2020-02-29 21:13:51 EAT

Figure 35 Files Referencing Dropbox in the Root Folder in Uninstall-VM

Other results from the keyword search referenced Dropbox in the Desktop, NTUSER.DAT, and `Windows\System32`, as shown in Figure 36. These artefacts contained information related to Dropbox installation in Program Files, Dropbox update helper, and computer user account tied to Dropbox installation.

Name	Location	Modified Time	Change Time	Access Time
desktop.ini	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/Dropbox/desktop.ini	2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 20:36:31 EAT
NTUSER.DAT	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/NTUSER.DAT	2020-02-29 10:20:49 EAT	2020-01-16 19:05:50 EAT	2020-02-29 10:22:42 EAT
ntuser.dat.LOG1	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/ntuser.dat.LOG1	2020-01-16 19:05:50 EAT	2020-01-16 19:05:50 EAT	2020-01-16 19:05:50 EAT
ntuser.dat.LOG2	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/ntuser.dat.LOG2	2020-01-16 19:05:50 EAT	2020-01-16 19:05:50 EAT	2020-01-16 19:05:50 EAT
ntuser.dat.LOG2-slack	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/ntuser.dat.LOG2-slack	2020-01-16 19:05:50 EAT	2020-01-16 19:05:50 EAT	2020-01-16 19:05:50 EAT
Installed Programs Artifact	/img_Uninstall-VM.E01/vol_vol7/Windows/System32/config/SOFTWARE	2020-02-29 10:21:44 EAT	2020-01-17 05:51:46 EAT	2020-02-29 10:21:44 EAT
Installed Programs Artifact	/img_Uninstall-VM.E01/vol_vol7/Windows/System32/config/SOFTWARE	2020-02-29 10:21:44 EAT	2020-01-17 05:51:46 EAT	2020-02-29 10:21:44 EAT

Figure 36 Files Referencing Dropbox in System32 and NTUSER.DAT in Uninstall-VM

4.5.1.3 AppData

Dropbox database files contained in C:\Users\dfiml\AppData\Local\Dropbox were not found. Dropbox folder could be traced in AppData\Roaming directory, as shown in Figure 37. The directory only had one file in the installer sub-directory.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-01-16 19:05:50 EAT	352	Allocated	Allocated
[parent folder]				2020-01-16 19:05:50 EAT	2020-01-16 19:05:50 EAT	2020-02-29 20:45:12 EAT	2020-01-16 19:05:50 EAT	344	Allocated	Allocated
Microsoft				2020-02-27 11:06:24 EAT	2020-02-27 11:06:24 EAT	2020-02-29 21:12:25 EAT	2020-01-16 19:05:50 EAT	56	Allocated	Allocated
Adobe				2020-01-16 19:09:17 EAT	2020-01-16 19:09:17 EAT	2020-01-16 19:09:17 EAT	2020-01-16 19:09:17 EAT	264	Allocated	Allocated
Dropbox				2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 17:24:56 EAT	48	Unallocated	Unallocated

Figure 37 Dropbox Folder in AppData\Roaming in Uninstall-VM

A keyword search for ‘dropbox’ established references to Dropbox in the Local\Microsoft, Local\Packages, Local\Temp and Roaming\Microsoft subdirectories. The files in Local\Microsoft and Local\Packages contained information related to Dropbox activity including browser search, download and installation, as shown in Figure 38.

Keyword search		160 Res		
Table Thumbnail		Save Table as CSV		
Name	Location	Modified Time	Change Time	Access Time
Web History Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
Web Search Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
Web Search Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
Web History Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
Web History Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
Web History Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
WebCacheV01.dat	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
Web History Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Microsoft/Windows/WebCache/WebC...	2020-02-29 19:23:20 EAT	2020-02-29 19:23:20 EAT	2020-02-29 19
auth_body_v2.min-vfInWQa[1].j	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Packages/Microsoft.MicrosofEdge_8...	2020-02-29 17:49:51 EAT	2020-02-29 17:49:51 EAT	2020-02-29 17
credentials_form.min-vf3yMi7N[1].	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Packages/Microsoft.MicrosofEdge_8...	2020-02-29 17:48:49 EAT	2020-02-29 17:48:49 EAT	2020-02-29 17
dropdown.min-vfen1yHH[1].js	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Packages/Microsoft.MicrosofEdge_8...	2020-02-29 17:49:49 EAT	2020-02-29 17:49:49 EAT	2020-02-29 17
flash_pagelet.min-vfRy75Ma[1].js	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Packages/Microsoft.MicrosofEdge_8...	2020-02-29 17:48:53 EAT	2020-02-29 17:48:53 EAT	2020-02-29 17

Figure 38 Files Referencing Dropbox in Local\Microsoft and Local\Packages in Uninstall-VM

The Local\Temp folder contained four files, as shown in Figure 39, which were analysed. DropboxExt64.32.0.dll254fb83 contained information related to time and calls to APIs, kernel, and other dlls. DropboxUpdate.exe254fab8 and goopdate.dll254fb35 contained information on Dropbox update. Au_.exe contained information on the Dropbox client and the calls for Dropbox installation and uninstallation.

Keyword search		160 Result		
Table Thumbnail		Save Table as CSV		
Name	Location	Modified Time	Change Time	Access Time
DropboxExt64.32.0.dll254fb83	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Temp/DropboxExt64.32.0.dll254fb83	2020-02-19 16:21:46 EAT	2020-02-29 21:13:52 EAT	2020-02-29 21
DropboxUpdate.exe254fab8	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Temp/DropboxUpdate.exe254fab8	2020-02-29 17:24:06 EAT	2020-02-29 21:13:51 EAT	2020-02-29 21
goopdate.dll254fb35	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Temp/goopdate.dll254fb35	2020-02-29 17:24:06 EAT	2020-02-29 21:13:51 EAT	2020-02-29 21
Au_.exe	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local/Temp/~nsu.tmp/Au_.exe	2020-02-19 16:28:54 EAT	2020-02-29 17:25:58 EAT	2020-02-29 21

Figure 39 Files Referencing Dropbox in Local\Temp in Uninstall-VM

The files in Roaming\Microsoft contained information on the path to the Dropbox synchronisation folder and the user files contained in the folder. They also had the link files to the three text files that had been uploaded to the folder, as shown in Figure 40.

Keyword search					160 Res
Table Thumbnail					Save Table as CSV
Name	Location	Modified Time	Change Time	Access Time	
5f7b5f1e01b83767.automaticDesti	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Auto...	2020-02-29 20:37:48 EAT	2020-02-29 20:37:48 EAT	2020-02-29 20	
f01b4d95cf55d32a.automaticDesti	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Auto...	2020-02-29 17:59:33 EAT	2020-02-29 17:59:33 EAT	2020-02-29 21	
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Dropb...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17	
Dropbox.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Dropb...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17	
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/delete...	2020-02-29 17:48:03 EAT	2020-02-29 17:48:03 EAT	2020-02-29 17	
delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/delete...	2020-02-29 17:48:03 EAT	2020-02-29 17:48:03 EAT	2020-02-29 17	
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/keep f...	2020-02-29 17:47:51 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17	
keep file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/keep f...	2020-02-29 17:47:51 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17	
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/shift d...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17	
shift delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/shift d...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17	

Figure 40 Files Referencing Dropbox in Roaming\Microsoft in Uninstall-VM

4.5.1.4 Prefetch Files

Prefetch files related to Dropbox client, update, installer, uninstaller, thumbnail generator and crash handler were found as shown in Figure 41.

/img_Uninstall-VM.E01/vol_vol7/Windows/Prefetch											259 Res
Table Thumbnail											Save Table as CSV
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)		
DROPBOX.EXE-41A1197E.pf				2020-02-29 21:13:23 EAT	2020-02-29 21:13:23 EAT	2020-02-29 21:13:23 EAT	2020-02-29 17:26:53 EAT	36828	Allocated		
DROPBOX.EXE-A0062768.pf				2020-02-29 17:25:36 EAT	2020-02-29 17:25:36 EAT	2020-02-29 19:31:20 EAT	2020-02-29 17:25:36 EAT	27722	Allocated		
DROPBOXCLIENT_91.4.548.EXE-944B0CE5.pf				2020-02-29 17:24:57 EAT	2020-02-29 17:24:57 EAT	2020-02-29 19:31:20 EAT	2020-02-29 17:24:57 EAT	48334	Allocated		
DROPBOXCRASHHANDLER.EXE-3BF847B4.pf				2020-02-29 17:29:00 EAT	2020-02-29 17:29:00 EAT	2020-02-29 19:31:20 EAT	2020-02-29 17:29:00 EAT	6613	Allocated		
DROPBOXINSTALLER.EXE-4DA08EFE.pf				2020-02-29 17:24:16 EAT	2020-02-29 17:24:16 EAT	2020-02-29 19:31:20 EAT	2020-02-29 17:24:16 EAT	7055	Allocated		
DROPBOXTHUMBNAILGENERATOR.EXE-7C2F3680.pf				2020-02-29 17:57:51 EAT	2020-02-29 17:57:51 EAT	2020-02-29 19:31:20 EAT	2020-02-29 17:47:35 EAT	15872	Allocated		
DROPBOXUNINSTALLER.EXE-2628D09B.pf				2020-02-29 21:13:14 EAT	2020-02-29 21:13:14 EAT	2020-02-29 21:13:14 EAT	2020-02-29 21:13:14 EAT	7126	Allocated		
DROPBOXUPDATE.EXE-89BC44CC.pf				2020-02-29 17:24:23 EAT	2020-02-29 17:24:23 EAT	2020-02-29 19:31:20 EAT	2020-02-29 17:24:17 EAT	19616	Allocated		
DROPBOXUPDATE.EXE-E72FEFE1.pf				2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 21:13:52 EAT	2020-02-29 17:24:18 EAT	17385	Allocated		
DROPBOXUPDATEONDEMAND.EXE-83F9CACE.pf				2020-02-29 17:26:43 EAT	2020-02-29 17:26:43 EAT	2020-02-29 19:31:20 EAT	2020-02-29 17:26:43 EAT	3560	Allocated		

Figure 41 Dropbox Prefetch Files in Uninstall-VM

4.5.1.5 Link Files

A keyword search for 'dropbox.lnk' returned hits in files including \$MFT and NTUSER.DAT, as shown in Figure 42. Further analysis of the files established that they contained information on the path to Dropbox synchronisation folder, the path to Dropbox.exe in Program Files, and settings used by Dropbox in playing of content.

Name	Location	Modified Time	Change Time
\$UsnJrnl:\$J	/img_Uninstall-VM.E01/vol_vol7/\$Extend/\$UsnJrnl:\$J	2020-01-17 05:52:55 EAT	2020-01-17 05:52:55 EAT
\$LogFile	/img_Uninstall-VM.E01/vol_vol7/\$LogFile	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT
\$MFT	/img_Uninstall-VM.E01/vol_vol7/\$MFT	2020-01-17 05:46:10 EAT	2020-01-17 05:46:10 EAT
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000012.db	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local...	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local...	2020-02-29 21:13:31 EAT	2020-02-29 21:13:31 EAT
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000014.db	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Local...	2020-02-29 21:13:33 EAT	2020-02-29 21:13:33 EAT
Dropbox.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT
NTUSER.DAT	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/NTUSER.DAT	2020-02-29 10:20:49 EAT	2020-01-16 19:05:50 EAT

Figure 42 Dropbox Link Files in Uninstall-VM

Link files to the three text files that had been uploaded, i.e. keep file.txt, delete file.txt and shift delete file.txt were also established as shown in Figure 43. The link files contained the full path to the corresponding text files.

Name	Location	Modified Time	Change Time	Access Time
5f7b5f1e01b83767.automaticDesti...	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Auto...	2020-02-29 20:37:48 EAT	2020-02-29 20:37:48 EAT	2020-02-29 20
f01b4d95cf55d32a.automaticDesti...	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Auto...	2020-02-29 17:59:33 EAT	2020-02-29 17:59:33 EAT	2020-02-29 21
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Dropb...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17
Dropbox.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/Dropb...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/delete...	2020-02-29 17:48:03 EAT	2020-02-29 17:48:03 EAT	2020-02-29 17
delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/delete...	2020-02-29 17:48:03 EAT	2020-02-29 17:48:03 EAT	2020-02-29 17
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/keep f...	2020-02-29 17:47:51 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17
keep file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/keep f...	2020-02-29 17:47:51 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/shift d...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17
shift delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roaming/Microsoft/Windows/Recent/shift d...	2020-02-29 17:57:48 EAT	2020-02-29 17:57:48 EAT	2020-02-29 17

Figure 43 Link Files to Uploaded Files in Sync Folder in Uninstall-VM

4.5.1.6 Synchronisation Folder

Dropbox synchronisation folder contained both files that were not deleted and those that were deleted by pressing the ‘delete’ button, as shown in Figure 44. The file that had been ‘permanently’ deleted, i.e. shift delete file.txt could not be traced after the uninstallation. However, the link file to it was present, as shown in Figure 44.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
.dropbox			0	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	42
.dropbox.cache				2020-02-29 17:36:36 EAT	2020-02-29 17:36:36 EAT	2020-02-29 21:13:24 EAT	2020-02-29 17:36:36 EAT	56
Get Started with Dropbox Paper.url			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 20:36:31 EAT	2020-02-29 17:36:38 EAT	240
Get Started with Dropbox Paper.url:com.dropbox.attrs			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 20:36:31 EAT	2020-02-29 17:36:38 EAT	26
Get Started with Dropbox.pdf			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:43 EAT	2020-02-29 17:36:38 EAT	1102331
Get Started with Dropbox.pdf:com.dropbox.attrs			0	2019-12-26 11:54:35 EAT	2020-02-29 17:36:38 EAT	2020-02-29 17:36:43 EAT	2020-02-29 17:36:38 EAT	26
[current folder]				2020-02-29 20:37:48 EAT	2020-02-29 20:37:48 EAT	2020-02-29 20:37:48 EAT	2020-02-29 17:36:34 EAT	56
[parent folder]				2020-02-29 17:36:34 EAT	2020-02-29 17:36:34 EAT	2020-02-29 21:12:25 EAT	2020-01-16 19:05:50 EAT	256
delete file.txt				2020-02-29 20:36:59 EAT	2020-02-29 20:36:59 EAT	2020-02-29 17:57:11 EAT	2020-02-29 17:47:27 EAT	0
desktop.ini			0	2020-02-29 17:36:42 EAT	2020-02-29 17:36:42 EAT	2020-02-29 20:36:31 EAT	2020-02-29 17:36:42 EAT	176
keep file.txt			0	2020-02-29 17:47:27 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17:47:50 EAT	2020-02-29 17:47:27 EAT	0
keep file.txt:com.dropbox.attrs			0	2020-02-29 17:47:27 EAT	2020-02-29 17:47:51 EAT	2020-02-29 17:47:50 EAT	2020-02-29 17:47:27 EAT	26

Figure 44 Files in Dropbox Sync Folder in Uninstall-VM

4.5.2 Registry Artefacts

Uninstallation of Dropbox left registry remnants in HKLM and HKU hives. Registry keys left include those for the Dropbox service, update, and uninstallation as shown in Figures 45, 46, 47 and 48. Dropbox user keys stored in the registry identified during installation were also present.

```

HKLM\SYSTEM\ControlSet001\Services\DbxSvc\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\ImagePath: "%SystemRoot%\system32\DbxSvc.exe"
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\ImagePath: "%SystemRoot%\system32\DbxSvc.exe"
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\DisplayName: "DbxSvc"
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\DisplayName: "DbxSvc"
HKLM\SYSTEM\ControlSet001\Services\DbxSvc>Description: "Dropbox Service"
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\RequiredPrivileges: 53 65 4C 6F 61 64 44 72 69 76
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\FailureActions: 10 0E 00 00 00 00 00 00 00 00

```

Figure 45 Dropbox Service Artefacts in Registry in Uninstall-VM

```

HKLM\SOFTWARE\Classes\AppID\DropboxUpdate.exe\AppID: "{76E258F0-DE86-4CEC-9D30-3F728A898741}"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync: "CoCreateAsync"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync\CLSID: "{A496C5D9-84FE-4E84-9D20-7481589E1C23}"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync\CurVer: "DropboxUpdate.CoCreateAsync.1.0"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync\CurVer: "DropboxUpdate.CoCreateAsync.1.0"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync.1.0: "CoCreateAsync"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync.1.0\CLSID: "{A496C5D9-84FE-4E84-9D20-7481589E1C23}"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoreClass: "Dropbox Update Core Class"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoreClass\CLSID: "{3A337332-37E4-4063-B4F3-6416846C8A33}"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoreClass\CurVer: "DropboxUpdate.CoreClass.1"

```

Figure 46 Dropbox Update Artefacts in Registry in Uninstall-VM

```

HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\UninstallString: ""C:\Program Files (x86)\Dropbox\Client\DropboxUn
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\InstallLocation: "C:\Program Files (x86)\Dropbox\Client"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\DisplayName: "Dropbox"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\UninstallPath: "C:\Program Files (x86)\Dropbox\Client\DropboxUninst
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\Publisher: "Dropbox, Inc."
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\VersionMajor: 0x00000061
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\VersionMinor: 0x00000004
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\DisplayIcon: "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe,0"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\DisplayVersion: "97.4.467"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\URLInfoAbout: "https://www.dropbox.com"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\HelpLink: "https://www.dropbox.com"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\NoModify: 0x00000001
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\NoRepair: 0x00000001

```

Figure 47 Dropbox Uninstall Artefacts in Registry in Uninstall-VM

```

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\c\52c64b7e\@C:\Program Files (x86)\Dropbox\Update\1.3.295.1\goopdate.dll,-3000: "Dropbox Update"
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\c\52c64b7e\@C:\Program Files (x86)\Dropbox\Update\1.3.295.1\goopdate.dll,-3000: "Dropbox Update"
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\InstallerRestartStormcrow: 0x00000001
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\EnableCloudDocsLauncher: 0x00000001
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\EnableCloudDocsLauncher_LaunchCount: 0x00000000
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\EnableWindowLauncher: 0x00000001
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\EnableWindowLauncher_LaunchCount: 0x00000000
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{E31EA727-12ED-4702-820C-4B6445F28E1A}\: "Dropbox"
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Microsoft\Windows\CurrentVersion\Shell_Extensions\Approved\{FB314ED9-A251-47B7-93E1-CDD82E34F8B}\: "DropboxExt"

```

Figure 48 Dropbox Update, Installer, Explorer, and Shell Artefacts in Registry in Uninstall-VM

4.6 Conclusion

This chapter identified artefacts resulting from the experiment and discussed their significance to forensic investigators. Artefacts related to Dropbox domain, browser, directory structures, configuration settings, application users, and time, were analysed. It was demonstrated that files deleted by the user manually or through uninstallation of Dropbox could be recovered. Through live and dead forensic analysis, it was determined that Dropbox leaves data remnants when uninstalled from Windows 10. On this basis, the *Null Hypothesis: Dropbox does not leave artefacts on Windows 10 after uninstallation* postulated in **Chapter 3: Research Methodology** was rejected. The next chapter concludes this study and provides areas for future work.

5 CONCLUSIONS AND RECOMMENDATIONS

The overall aim of this research was to investigate Dropbox data remnants on Windows 10, particularly in the registry and file system. The specific research objectives were:

1. Analyse digital forensics methodologies and their appropriateness for Dropbox forensics.
2. Investigate file system and registry artefacts created by Dropbox when installed on Windows 10.
3. Investigate Dropbox artefacts left on Windows 10 file system and registry after uninstallation and their significance to forensic investigators.

This chapter concludes the study by providing a summary of the findings of the research objectives, contributions of the study, its limitations, and suggestions for future work. By adopting this approach, a cyclical closure is achieved.

5.1 Research Objectives: Summary of Findings and Conclusions

The first objective was to analyse digital forensics methodologies and their appropriateness for Dropbox forensics. The objective was met through the literature review in Chapter 2. Six models were analysed:

1. McKemmish Model
2. Digital Investigative Process
3. NIST Model
4. Integrated Conceptual Digital Forensic Framework
5. Digital Forensic Analysis Cycle
6. Integrated Digital Forensic Process Model

McKemmish model was adopted for the study as it followed the general process in digital forensics of identification, preservation, analysis, and presentation. Furthermore, it had been used by most of the previous research on Dropbox forensics.

The second objective was to investigate file system and registry artefacts created by Dropbox when installed on Windows 10. To achieve this objective, a literature review on Dropbox forensics in Windows was conducted first to identify potential sources of the artefacts. Subsequently, live and dead forensic analysis of Dropbox was conducted on Windows 10 to establish these artefacts. It

was established that Dropbox created artefacts in the file system, including Dropbox client application files, prefetch files, link files, browser cookies, and browser history, among other artefacts. In the registry, entries related to Dropbox configuration settings, installation time, installation directories, and user keys were found.

The third objective was to investigate Dropbox artefacts left on Windows 10 file system and registry after uninstallation and their significance to forensic investigators. Like the second objective, a literature review on Dropbox forensics in Windows was conducted first to identify potential sources of the artefacts. Subsequently, live and dead forensics analysis was conducted during Dropbox uninstallation on Windows 10. Traces of Dropbox were established in the file system including installation files, prefetch files, link files, files uploaded by the user, files deleted by the user, browser history, and cookies. The registry contained artefacts related to Dropbox service, update, uninstallation, and user keys amongst others.

The study highlighted the significance of these artefacts to forensic investigators. From the artefacts, investigators could, among other things:

1. Establish whether Dropbox was installed in the suspect machine.
2. Get the time when Dropbox was installed.
3. Get Dropbox user information including the email account, account type, type of subscription, and Windows account used to access Dropbox.
4. Locate documents shared in the Dropbox synchronisation folder.
5. Recover documents deleted from the Dropbox synchronisation folder.
6. Establish if Dropbox had been uninstalled from the suspect machine in cases where the suspect uninstalls the application.

5.2 Contributions

This research has made contributions to the research community and practice, which are outlined in the subsequent sub-sections.

5.2.1 Contributions to Research

The study extended Dropbox forensics research by contributing knowledge on artefacts related to newer versions of Dropbox, in particular, version 91.4.548 on Windows 10. The following were brought to fore in this study:

- Artefacts created by Dropbox when installed on Windows 10
- Dropbox data remnants on Windows 10 post-uninstallation
- Configuration files no longer used by Dropbox
- New configuration files used by Dropbox
- Dropbox IP address, domain, and sub-domains

The study also extended previous work by Armirullah *et al.*, (2016) by investigating Dropbox registry artefacts left post uninstallation. Likewise, it provided further insight on `.dropbox` file found in the Dropbox synchronisation folder. Mehreen and Aslam (2015) had recommended further research on the file to identify its purpose, and this research did so.

5.2.2 Contribution to Practice

This work identified the location and significance of artefacts that can be used when investigating cybercrime involving Dropbox. Artefacts that can be used to tie a suspect to the crime were identified, including Dropbox user email, account type, account subscription, account login, and Windows account used to access the Dropbox account. Location of uploaded and shared files in the Dropbox synchronisation folder was also demonstrated. In addition, this research showed that files deleted by a suspect could be recovered.

An important aspect of any criminal investigation is recreating the timeline of events. This study provided time-related artefacts, including file timestamps (modified, accessed, and created times) of artefacts presented and Dropbox installation time. The artefacts presented together with their timestamps can be used to recreate not only the crime scene but also the sequence in which events occurred.

5.3 Limitations of the Study

This research was limited by the inability to decrypt the encrypted database files despite using decryption tools that successfully decrypted them in previous studies. This could possibly be attributed to changes in the Dropbox encryption mechanism. Another challenge was the automatic update of Dropbox application during live forensics when conducted over several days. Dropbox does not provide an option to disable the auto-update. The update modified some of the configuration files and which could bring doubt to the integrity of evidence presented. However,

dead forensics compensated for this. Nevertheless, investigators should be cognisant of this feature when conducting Dropbox live forensics.

5.4 Future Work

As highlighted in the preceding section, decrypting Dropbox encrypted database files was a challenge. Future research should explore the decryption of these files as they bear valuable information. While this work focused on Dropbox artefacts in the registry and file system, invaluable evidence can also be found in the memory and network traffic. Therefore, future studies should investigate potential artefacts from these sources.

REFERENCES

- ACPO (2012) 'ACPO Good Practice Guide for Digital Evidence'. Available at: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.
- Ahmed, A. A. and Li, C. X. (2016) 'Locating and Collecting Cybercrime Evidences on Cloud Storage: Review', in *2016 International Conference on Information Science and Security (ICISS)*, pp. 1–5. doi: 10.1109/ICISSEC.2016.7885861.
- Amirullah, A., Riadi, I. and Luthfi, A. (2016) 'Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System', *International Journal of Computer Applications*, 143(1).
- Biggs, S. and Vidalis, S. (2009) 'Cloud Computing: The Impact on Digital Dorensic 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).
- Caviglione, 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.
- Chung, H. *et al.* (2012) 'Digital Forensic Investigation of Cloud Storage Services', *Digital Investigation*. Elsevier, 9(2), pp. 81–95. doi: 10.1016/J.DIIN.2012.05.015.

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.

Dropbox (2018a) *How much does Dropbox cost?* Available at: <https://www.dropbox.com/help/billing/cost> (Accessed: 21 November 2018).

Dropbox (2018b) *What is Dropbox?* Available at: <https://www.dropbox.com/features> (Accessed: 21 November 2018).

EC-Council (2010) *Investigating Network Intrusions and Cybercrime*.

Epifani, M. (2013) ‘Cloud Storage Forensics’. Available at: https://www.sans.org/summit-archives/file/summit_archive_1493920922.pdf.

Ghafarian, A. (2015) ‘Forensics Analysis of Cloud Computing Services’, in *2015 Science and Information Conference (SAI)*, pp. 1335–1339. doi: 10.1109/SAI.2015.7237316.

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.

Hannan, M. (2004) ‘To Revisit: What is Forensic Computing?’, in *Proceedings of the Second Australian Computer, Network and Information Forensics Conference*, pp. 103–111.

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. doi:

10.1145/1842733.1842751.

Keizer, G. (2018) *Windows by the numbers: Windows 10 nears 'crossover' point with veteran Windows 7*. Available at: <https://www.itworld.com/article/3199373/windows-pcs/windows-by-the-numbers-windows-10-nears-crossover-point-with-veteran-windows-7.html?page=2#toc-1> (Accessed: 21 November 2018).

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](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.

Malik, R., Shashidhar, N. and Chen, L. (2015a) 'Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform', in *Proceedings of the International Conference on Security and Management*.

Malik, R., Shashidhar, N. and Chen, L. (2015b) 'Cloud Storage Client Application Analysis', *International Journal of Security*, 9(1).

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>.

Maturana, F., Me, G. and Tacconi, S. (2012) 'A Case Study on Digital Forensics in the Cloud', in *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 111–116.

McClain, F. (2011) *Dropbox Forensics*, *Forensic Focus*. Available at: <https://www.forensicfocus.com/articles/dropbox-forensics/> (Accessed: 20 April 2020).

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 Sheno, S. (eds). Boston, MA: Springer US, pp. 3–15.

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

Mell, P. and Grance, T. (2011) 'The NIST Definition of Cloud Computing', *NIST Special Publication 800-145*. NIST, p. 2. Available at: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

Microsoft (2018) *Windows Lifecycle Fact Sheet*. Available at: <https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet> (Accessed: 21 November 2018).

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

NetApplications (2018) *Operating System Market Share*. Available at: <https://netmarketshare.com/operating-system-market-share.aspx?options=%257B%2522filter%2522%253A%257B%2522%2524and%2522%253A%255B%257B%2522deviceType%2522%253A%257B%2522%2524in%2522%253A%255B%2522Desktop%2522Flaptop%2522%255D%257D%257D%255D%257D%252C%2522dateLabel%2522%253A%2522Trend%2522%252C%2522attributes%2522%253A%2522share%2522%252> (Accessed: 21 November 2018).

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 Dropbox DBX 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. *et al.* (2014) 'Dropbox Analysis: Data Remnants on User Machines', *Cloud Storage Forensics*. Syngress, pp. 63–93. doi: 10.1016/B978-0-12-419970-5.00004-1.
- Quick, D. and Choo, K.-K. R. (2013a) 'Digital Droplets: Microsoft SkyDrive Forensic Data Remnants', *Future Generation Computer Systems*. North-Holland, 29(6), pp. 1378–1394. doi: 10.1016/J.FUTURE.2013.02.001.
- Quick, D. and Choo, K.-K. R. (2013b) 'Dropbox Analysis: Data Remnants on User Machines', *Digital Investigation*. Elsevier, 10(1), pp. 3–18. doi: 10.1016/J.DIIN.2013.02.003.
- Rani, D. R. and Geethakumari, G. (2015) 'An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots', in *2015 International Conference on Pervasive Computing (ICPC)*, pp. 1–5. doi: 10.1109/PERVASIVE.2015.7087206.
- Rescorla, E. (2000) *HTTP Over TLS*. Available at: <https://tools.ietf.org/html/rfc2818> (Accessed: 13 May 2020).
- Ruan, K. *et al.* (2011) 'Cloud Forensics BT - Advances in Digital Forensics VII', in Peterson, G. and Sheno, S. (eds). Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 35–46.
- Saunders, M., Lewis, P. and Thornhill, A. (2015) *Research Methods for Business Students*.
- 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.
- StackExchange (2012) *.dropbox files, can they be deleted?* Available at: <https://superuser.com/questions/472616/dropbox-files-can-they-be-deleted> (Accessed: 13 May 2020).
- SWGDE (2009) 'SWGDE Best Practices for Computer Forensics Version 2.1'.
- Taylor, M. *et al.* (2011) 'Forensic Investigation of Cloud Computing Systems', *Network Security*.

Elsevier Advanced Technology, 2011(3), pp. 4–10. doi: 10.1016/S1353-4858(11)70024-1.

Warren, T. (2014) *Dropbox and Microsoft form surprise partnership for Office integration*. Available at: <https://www.theverge.com/2014/11/4/7153975/dropbox-microsoft-partnership-microsoft-office> (Accessed: 13 May 2020).

Warren, T. (2015) *Cortana for Windows 10 will search Dropbox and Google Drive on Lenovo PCs*. Available at: <https://www.theverge.com/2015/5/28/8676557/lenovo-cortana-reachit-windows-10> (Accessed: 13 May 2020).

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>.