SCHOOL OF SCIENCE, ENGINEERING AND ENVIRONMENT

CYBER FORENSICS

Forensic Investigation of Cloud Computing

Comparative Analysis Across Cloud Vendors:
DropBox, AWS, Microsoft Azure, and Evernote.

January 2022

Authors:

A Dinusha Dissanayaka	@00608177
Olorogun Oluwafunke	@00642856
Ikechukwu Donald	@00618728
Adeoye Abodunrin	@00640110

ABSTRACT

Storage and synchronization of files on Cloud services have received a positive reception from internet users, and these services provide capabilities such as storing files on the cloud, synching those files with either a computer or mobile device, and sharing these files either personal or private with the public or with a particular individual. Recently, cybercriminals or malicious individuals have targeted cloud services to carry out malicious activities such as unauthorized alteration or deletion, cyber terrorism, identity theft, sexual harassment, malware, and privacy issues. Over and above that, evidence retrieval via cloud storage systems like AWS, Evernote, DropBox, and Azure, among others, has been noted as a growing difficulty for digital forensic researchers. (Daryabar et al., 2016)

To investigate cloud storage services, traditional digital forensic procedures are insufficient. Therefore, mobile and cloud forensics must be used to perform a thorough examination (Chung et al., 2012). Hence, the result from this research work can be used to establish the facts behind digital forensics investigations for cloud storage platforms.

This research focuses on gathering evidence from Linux, Windows and Android devices /computers that accessed a cloud service. The objective is to locate and collect artefacts left by users after performing different activities, not limited to deletion/modifications of files, privilege escalation and the likes. Furthermore, this study will show what kind of data traces can be recovered, the comprehensive network analysis, file system analysis using different forensic tools on the snapshots/images, log and memory analysis. The integrity of the acquired data/artifacts (the hash) in the cloud is validated against the original data/artifacts during the research. Timestamp information is critical to the forensic investigation, hence, it's imperative to keep track of the information and to understand the conditions around the file.

We hope to improve the efficiency of cloud forensics and crime investigation by detecting data remnants on user devices and cloud infrastructure.

Keywords: Evernote, Dropbox, AWS, Microsoft Azure, Cloud Computing, Forensic Investigation

INTRODUCTION

Cloud computing has become a popular option for many Internet users and businesses in recent years. It provides consumers with significant financial benefits by offering a scalable infrastructure, low-cost pay-as-you-go services, and on-demand computation. However, the same technology also provides several risks, including criminal exploitation, which can leave a little trace and make it easy to carry out malicious acts.

Cybercriminals, for example, are using current cloud services as infrastructure to target their victims. In 2013, a Chinese gang used Dropbox to transmit malware as part of an initial stage of Distributed Denial of Service (DDoS) operations . In preparation for an initial round of DDoS operations, a Chinese gang hacked cloud file-hosting services and used Dropbox to distribute malware in 2013.

Security and privacy are ranked as the top concerns for cloud adoption. As a result, numerous businesses are wary of cloud computing. Finance and healthcare are two critical public industries that are progressively warming to the idea of putting their data and apps to the cloud. However, cloud computing is being merged with a number of methodologies to determine the general security needs for cloud adoption. Despite this, researchers are still searching for the best ways to regulate cloud computing adoption. While security has been an afterthought with emerging technologies like the cloud digital forensics. When conducting a digital investigation in the cloud, investigators confront various problems due to the distributed nature and configuration of the cloud-computing infrastructure. These difficulties are specific to cloud computing and are not found in typical digital systems. This is because cloud computing brings unique characteristics, such as on-demand self-service quick elasticity, broad resource pooling, measured service, and network access.

While security has been an afterthought with emerging technologies like cloud digital forensics, investigators confront various problems due to the distributed nature and configuration of the cloud-computing infrastructure when conducting a digital investigation in the cloud. These difficulties are specific to cloud computing and are not found in typical digital systems. This is because cloud computing brings unique characteristics, such as on-demand self-service quick elasticity, broad resource pooling, measured service, and network access. (Alqahtany et al., 2015) Furthermore, a knowledge gap and non-readily available cloud forensic tools might make it challenging to locate relevant data quickly. This can negatively impact the investigation as critical data required to substantiate the accuracy of the incident may be missed; as a result, data identification is an essential aspect of the digital investigation process.

CONTRIBUTION

This study aims to identify the remnants left on user devices when a user accesses AWS, Microsoft Azure, Evernote and DropBox.

The following questions were investigated using these platforms as a case study:

- What data remains on a computer hard disc after the platform users has used client software or accessed cloud storage through a browser, and where can data remnants be found in the Windows 10 operating system, Linux or Android OS?
- What data is visible in network traffic, and what data is stored in memory?
- What artefacts can be found on a computer hard drive and memory after a user has used the Symform client application and web application?

The findings of this study will help the forensic community to better understand the types of terrestrial artefacts that are likely to remain after using cloud infrastructure on PCs and mobile devices with different operating systems.

Cloud forensic Challenges.

In this section, challenges of cloud forensics are discussed. We illustrate our findings by examining the problems that investigators face at each level of the computer forensics process. The following are some of the significant challenges experienced by cloud forensic investigators:

Forensic data acquisition: Most crucial step in the forensic procedure is gathering digital evidence. The following are some of the challenges encountered during this stage:

- Physical Inaccessibility: In cloud forensics, the inaccessibility of digital evidence makes the evidence collection process more difficult. The techniques and processes for digital forensics presuppose that we have physical access to the machines. In cloud forensics, however, the situation is different. We do not always know the physical location of the data because it is spread across numerous hosts in multiple data centers.
- Minimal Control in Clouds and Dependence on the Cloud Service Providers (CSP): Investigators in traditional computer forensics have complete control over the evidence (e.g., a hard drive). Regrettably, data control in the cloud differs depending on the service type. As a result, customers have limited control in different layers for the three service models – IaaS, PaaS, and SaaS. As a result, we rely heavily on the CSP to gather digital evidence from the cloud computing environment. In the collection phase, this is a major bottleneck.
- Volatile Data: Without power, volatile data will be permanently lost. For example, if images of a Virtual Machine (VM) are not captured at the instance when malicious activities are suspected, we will lose all data when VM is powered off. Several research studies have focused on this subject.
- Multi-tenancy: Various virtual machines (VMs) can share the same physical infrastructure in cloud computing, allowing data from multiple clients to be co-located. Therefore, we need to show that our data was not mixed with other users. Similarly, we must protect the privacy of all other tenants while conducting the investigation, which makes obtaining digital evidence more difficult.

Decentralization of logs and Absence of Critical Information in Logs: Log information is not stored on a single centralised log server in cloud infrastructure; rather, logs are distributed among numerous servers. The log data of numerous users may be stored on the same server or dispersed across multiple servers. Logs do not have a defined format. Logs are provided in a variety of forms, originating from various tiers and service providers.

Chain of Custody: Maintaining a chain of custody in a cloud context will be difficult due to several jurisdictional laws, proprietary technologies and procedures. The chain of custody preservation all through the cloud forensic investigation process is questionable since multiple individuals may have access to the material, and we must depend on the CSP to get the evidence.

Limitations of Existing Forensics Techniques: The present forensic tools cannot handle the environment due to cloud computing's distributed and elastic nature. In the investigation, some researchers emphasized the limits of current forensic technologies. Tools and processes for investigating in a virtualized environment have yet to be established, particularly at the hypervisor level.

Crime Scene Reconstruction: Investigators will need to reconstruct the crime scene to investigate a malicious action. In addition, it assists them in comprehending how an adversary started an attack.

In a cloud setting, this is a critical issue. It will be impossible to reconstruct the crime scene if an adversary shuts down her virtual instance after a criminal action or uninstalls his malicious website.

Cross-Border Law: The issue of cloud forensics is being exacerbated by multi-jurisdictional or cross-border law. The service providers' data centers are located all around the world. However, privacy protection and information exchange regulations are not uniform over the world, and they may differ in various parts of a country. In various cloud forensic research efforts, cross-border legislation and red tape concerns arose, making the evidence collection process difficult.

Presentation: Compared to the complicated structure of cloud computing, proving evidence in front of a jury for traditional computer forensics is very simple. Jury members may have a basic understanding of computers or, at the very least, privately-held local storage. However, the practicalities of a cloud data centre, which runs thousands of virtual machines and is accessible by hundreds of users at the same time, are just too sophisticated for the jury to comprehend. (Hasan & Zawoad, 2013)

RELATED WORK

i. From a forensic standpoint, McClain discusses Dropbox client software. On the machine of a cloud end-user, he discovered some data fragments. He concluded that registry modifications, updated files, web cache and the recovery of deleted files are the most common remnants identified on Windows 7. (Focus, 2011).

ii. Chung investigated the forensic remnants of cloud storage across several operating systems. In addition, he discussed strategies for gathering and evaluating data on a number of cloud storage providers. (Chung et al., 2012)

iii. Jason describes the digital artefacts left behind when the machine accesses an Amazon Cloud Drive. File transfers to and from an Amazon Cloud Drive on a Windows 7 PC can be determined using the methods available to a forensic examiner. (Hale, 2013)

iv. Darren Quick talks about Dropbox data remnants on end-user devices. He wanted to see what data remains on a Windows 7 computer and an Apple iPhone 3G when users save, upload, and access data in the cloud using different techniques. (Quick & Choo, 2013)

v. Darren Quick talks about Evernote data leftovers on user devices. To access Evernote, he utilized a computer and an iPhone. He wanted to discover what was remaining on the client's gadgets. His research evaluated the advantages of employing a proposed framework that will guide an investigation when doing a forensic analysis of a cloud computing environment when a user accesses Evernote. (Quick & Choo, 2014).

vi. Darren Quick also discusses data remnants on user workstations as a result of using Microsoft SkyDrive. To access Microsoft SkyDrive, they utilise a PC and an iPhone. (Quick & Choo, 2013b).

vii. Shu Yun Lim describes the detection of data traces left behind from a user's Dropbox utilization on Windows 10. She and the team attempted to find data traces of cloud storage activities, notably Dropbox on the Windows10 platform, focusing on the cloud end-user. (Lim et al., 2020).

PROBLEM STATEMENT

Cloud services are increasingly being adopted as an efficient means of managing computing resources for individuals, public and the corporate clients. So, the need for digital forensics in those environments has become a necessary requirement for incident managers and the forensic professionals. There are static cloud forensic tools with the capacity to acquire evidence, and to provide facility to analyse them or use another application to do the analysis. We could not afford to purchase the licenses of those tools for this particular assignment, rather, we deployed the use of client based tools like autopsy, FTK, encase to acquire the images, then analyse them using autopsy with the other internet based tools.

Digital forensic analysis is the technique of reviewing electronic evidence for legal purposes. However, a current understanding of the location and type of data remnants left behind after an incident in cloud storage is also vital for an examiner. This has been a critical challenge to cloud forensic investigators. Therefore, adequate studies for such services should systematically assist the investigators in collecting evidence and artifacts.

FORENSIC RESEARCH METHODOLOGY

The goal of digital forensics is to investigate and reconstruct a computer or digital artefact-related event (Roussev, 2009). Forensic investigators and practitioners have created digital forensic methodologies and systems. This research utilizes a forensic approach for assessing digital evidence on cloud computing devices and mobile devices developed by the National Institute of Standards and Technology (NIST).

Figure 1 illustrates the flow of the NIST technique.

Figure 1. Demonstrates NIST technique for Forensic Investigation

3.1 Authorization and Preparation

This is the first stage of the forensic process. In this stage, before addressing digital evidence, we need to be certain that the search will not break any laws or cause liability. This will require computer security professionals to get instructions and formal consent from law enforcement entities before obtaining digital evidence related to an investigation. Unless the individual consents, a search warrant is normally necessary to access places or data that the individual considers personal or private. (Dargahi, 2021)

3.2 Identification

This process speaks to the evidence that can be acquired, where it is held, how it is stored and in which format and so on. Personal computers, mobile phones, and personal digital assistants (PDAs) are examples of electronic storage mediums where artefacts can be identified.

3.2 Collection/Preservation

The preservation stage is another name for this step. This step entails gathering, identifying, labelling, recording, and retrieving evidence in the form of hardware that will be utilised as digital evidence in a digital crime investigation. Data integrity protection mechanisms are followed during this process.

Data integrity can be preserved by separating physical evidence and creating backups in the form of clone or image files.

Procedure for collection stage is shown below:

Figure 2. Collection process

3.2 Examination

This part of an investigation include analyzing and issuing data based on demands while protecting data integrity, as well as processing digitally gathered forensic data utilising a combination of different scenarios, both automatically and manually. Figure below depicts the steps of the examination procedure..

Figure 3. Examination process

3.3 Analysis

The examination findings are analysed using procedures that have been justified technically and legally in order to gather relevant information and answer questions that serve as a source or a driver in the collecting and examination process. Figure 4 depicts the flow of the analytical

phase.

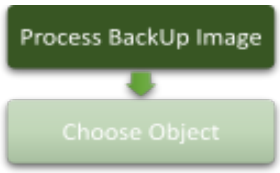


Figure 4. Analysis phase

3.4 Reporting

The ultimate outcome of an analytical procedure is a report. Written reports for documentation or spoken reports in the form of presentations are both examples of analytical reports. Figure 5 depicts the reporting procedure.

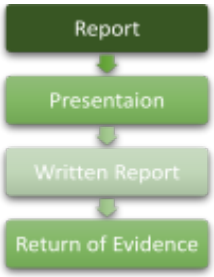


Figure 5. Reporting Process

SOFTWARE AS A SERVICE (SAAS)

1. DROPBOX

Dropbox is a file hosting facility that enables clients to store and share files and folders. This service grants 2 GB of free data storage, and additional storage space can be taken by signing up as a new user or subscribing to a paid service of up to 5000GB for £120 per year or as much space as needed for £180 per year. Dropbox can be accessed using the client software or web browser (e.g., Google Chrome, Firefox, and Microsoft Edge). Dropbox client software is available for Windows operating systems (OS), Linux, Mac OSX, Apple iOS, Android, Windows, and Blackberry phone devices.

For this study, a personal computer (PC) environment with Windows 10 OS, and Linux OS (Ubuntu) and phone devices with iOS and android installed was used to determine data remnants. It is disclosed that the use of a virtual computer with a typical installation of the OS would permit various configurations to be immediately set up and assessed, in need of getting to re-configure and copying physical hard drives, memory, or allowing external network capture. This allowed the evaluation of a variety of test PCs in several configurations to facilitate forensic analysis of the Dropbox client software and various browsers, namely Google Chrome, Microsoft Edge, and Mozilla Firefox.

In the next section, the procedures of discovering data remnants of a user logging on to Dropbox in numerous methods and initiating anti-forensics to disguise the intent of cloud storage on PC and mobile devices are instigated by engaging the suggested framework. This framework is then utilised in an iPhone (iOS) and android phone and scrutinised to identify the data remnants when using the inbuilt browser and the Dropbox client software (iOS and android). The section concludes with a summary of the consequences and suggests areas for future investigations.

Dropbox analysis

During this investigation, files were discovered that contained the information needed to complete the review. The VMDK files in each Virtual Machine (VM) folder (for the hard drive), the VMEM file (for the memory capture), and the saved network capture (PCAP) file are the files used in this situation (for the network captures). For each VM, these files were identified.

Each virtual hard disc (VMDK file) was forensically copied using AccessData FTK Imager 4.5.0.3 in the E01 container format for this study. Each memory file (VMEM) and network capture (PCAP) file was also forensically copied in the AccessData Logical Image (AD1) format, and an MD5 hash value for each original file was computed and verified [2].

HxD version 2.5.0.0, EnCase version 6.19.4, Autopsy 4.19.2, AccessData FTK Imager version 4.5.0.3 and 3.1.1, AccessData Registry Viewer 2.0.0.7, Network Miner 1.0, Wireshark 1.6.5, Magnet Software Internet Evidence Finder 5.52 and Magnet RAM Capture 1.2.0.0, and RegRipper version 3.0 were used to inspect each of the forensic copies of the VMDK, VMEM, and PCAP files. Many of these tools are widely utilised by law enforcement agencies and the private sector for digital forensic analysis. Encase and FTK Imager software have also been tested by the National Institute of Standards and Technology's Office of Law Enforcement Standards (NIST).

Dropbox Client Software

The Dropbox client software was recognised in the Upload-VMs as being installed in the 'C:Program FilesDropbox' folder on Windows 10. On the hard drive, Dropbox sample files and folders were analysed in the default Dropbox folder location ('C:Users[username]Dropbox'). Table 1 lists the filenames, locations, MD5 values, and SHA-256 values for the software and sample files computed with Autopsy 4.19.2. The hash values of the standard files and sample files may need to be recomputed when the latest version of the Dropbox Windows client software is published.

Filename	Location	MD5 Value	SHA-256 Value
Dropbox.exe	C:\Program Files\Dropbox\Dropbox.exe	1e7777eaebd9432642415dba8c1a8ff1	0d1800a88b0bf5e553c86f8a73b2930413b12b48c4a062c1e6aaa2f9df50f26f
Base Paper-Research Assignment.pdf	C:\Users\[username]\Dropbox	157cef95964ba4f9caea786d4a01167f	e6da8363dfdad8d63a6b3571684831df057f63123390f225c3418a5596fb4ac0
Get Started with Dropbox.pdf	C:\Users\[username]\Dropbox\	2a0171ddea96cbfcf6e95d935405b4d3	7d0d0a54066745c6ad7897309ac613577a2a771967beba40f3df44e783007b6d
desktop.ini	C:\Users\[username]\Dropbox\PC	978e57482914bbb6b6fda1bd812224f4	2f8041f69d2786d1473341b78213cc98d1016d0c37b75af09c711d38676a0f49

Host.db	C:\Users\[username]\AppData\Local\Dropbox	6ab03f7f81a140c912a3de226f4e7213	085edad47ff7944c3be47a28a9fa37a274f39ad0b9ff0a98666662308cbba266
Host.dbx	C:\Users\[username]\AppData\Local\Dropbox	-	-
Info.json	C:\Users\[username]\AppData\Local\Dropbox	-	-

Table 1: Dropbox Windows software files with MD5 and SHA-256 values

Heretofore, the Dropbox client software contained a filecache.db file that contained a list of synchronised filenames. The Dropbox client software utilised for this study does not have this file (version 1.3.541.1). There is, however, a Filecache.dbx file, which appears to be encrypted. The path for Dropbox file storage is stored in Base64 string encoded data in the 'host.db' file. Inside the 'host.dbx' file, the string 'QzpcVXNlcnNcRGludVxEcm9wYm94' was found. When you convert this to a Base64 string, you'll get the following: ‘C:\Users\ADDissanayaka\Dropbox’

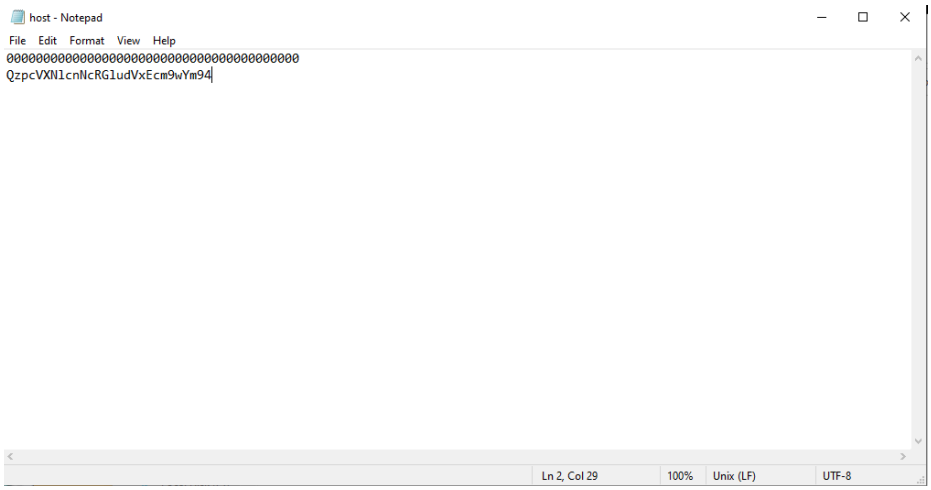


Figure 1: host.dbx file that contains the string

Dropbox account information

1. Accessing with different IPs

If someone has been using Dropbox for a prolonged and has switched PCs and smartphones multiple times during that time, they may have a huge list of associated devices, and it is extremely easy to see when they last used them. There is a Trash bin icon that allows people to delink the selected device so that no one else can access their account automatically (Figure 2). With the client software installed, complete access to an account could be obtained by clicking on the Dropbox icon in the system tray, which contains a link to the Dropbox website, without having to provide a login or password.

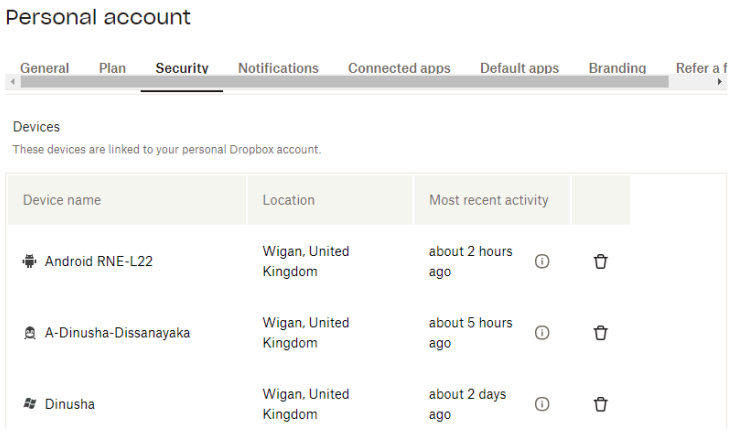


Figure 2: List of linked devices to Dropbox

Users can also see their recent web sessions, which display the browsers that are currently enrolled into their Dropbox account. This list can reassure users that no one else is logging into their accounts, and all of these sessions can be viewed under "SettingsSecurityWeb browsers." It also shows the last activity's location and time stamp [2]. There is also the option of removing a linked web browser.

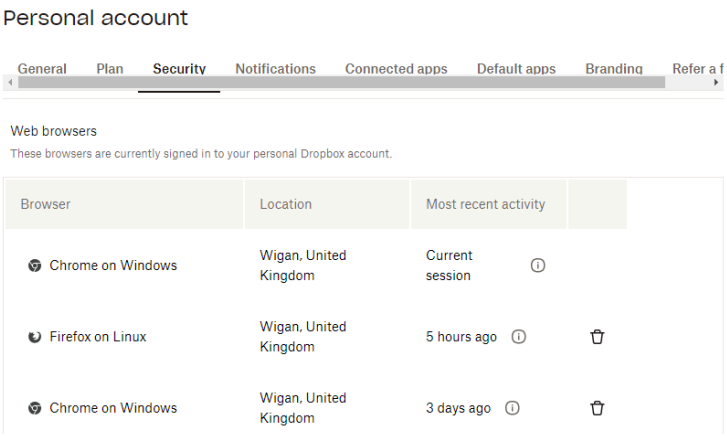


Figure 3: List of linked web browsers to Dropbox

When customers sign into Dropbox through a third-party app, Dropbox shares their private information with that app, as previously stated. Users may forget which apps they gave permission to access their Dropbox accounts over time, or they may have stopped using them altogether. Users may examine all the apps they have permitted at the bottom of Dropbox's security settings page. They can easily withdraw rights for any given app, just like they may de-list trusted devices.

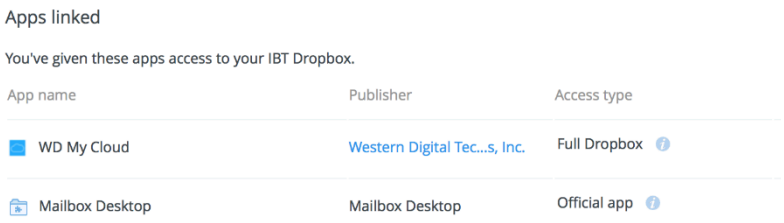


Figure 4: List of apps to Dropbox

Two-step verification (two-factor authentication), which is available on well-known online services like Gmail and Facebook today, is a powerful method for preventing unauthorised access to Dropbox accounts. This feature requests the code every time someone attempts to access the account from a new device, which must be given to the account owner's cell phone.

Under "SettingsSecurity," you can enable two-factor authentication. When you enable this option, you'll be prompted to re-enter your Dropbox password, and then the users will be asked whether you want codes sent to your phone as a text message or to an authenticator app like Google Authenticator.

After that, they will be asked to enter your phone number and will be given a test code. Dropbox then requests a backup phone number in the event that the user's primary phone is lost. Dropbox also provides a list of ten backup codes, which you should print or write down and save in a secure location.

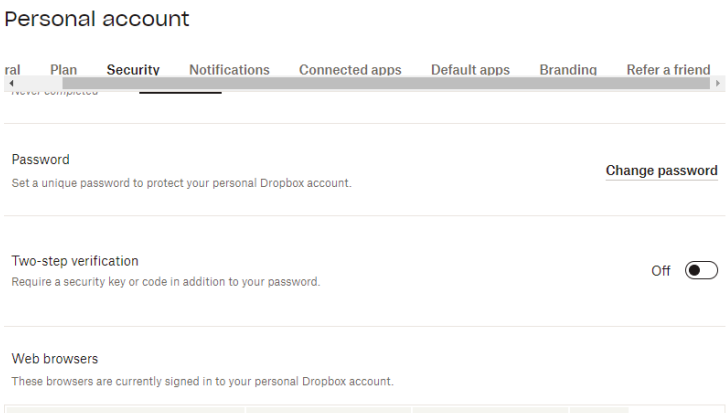


Figure 5: Dropbox two-step verification feature

2. Using a VPN

Dropbox may not be able to pinpoint users' exact whereabouts, but it can obtain a general idea of where they are. It may be able to pinpoint the user's exact location based on the IP address assigned to them (Figure 6).

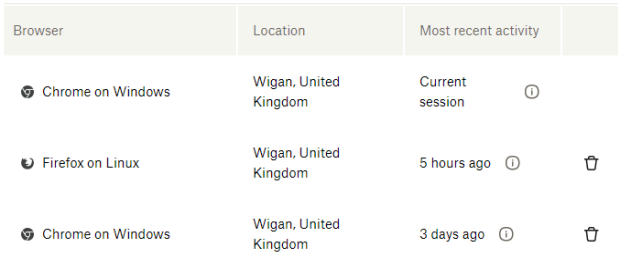


Figure 6: Location identification by Dropbox

A virtual private network (VPN) is a group of connected computers that creates an encrypted tunnel that redirects web traffic to a VPN server rather than a public server [3]. Dropbox will not be able to divulge the genuine IP address as a result of this (Figure 7).

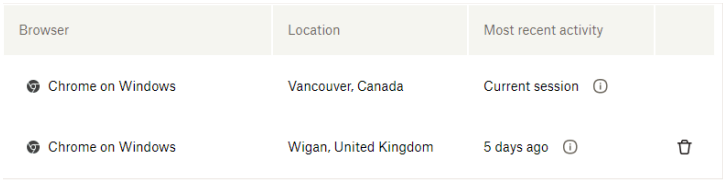


Figure 7: Location identification by Dropbox after using a VPN to browse from Canada.

3. Alteration of files

When using a web browser to access a Dropbox account, you may also see deleted files, which are available for thirty days for free accounts and indefinitely for paid ones. If the option to 'Show Deleted Files' is not chosen, a file is not visible when it is deleted; however, the last changed date is not shown. The data that have been erased from the browser can be restored or permanently destroyed. Each time a file is edited, Dropbox creates a snapshot of it, and the history of a file may be examined. A timeline of previous occurrences, such as when files were uploaded, deleted, restored, or other machines were joined to the account, may also be examined, as well as the date and time for the event (Figure 8).

Figure 8: Timeline of previous events of Dropbox

Dropbox Analysis On Computer Devices

1. Directory Listing

AccessData FTK Imager 4.5.0.3 was used to build a directory listing for all of the VM hard discs. Encase was used to examine the filenames during the evaluation. There were no references to the Dropbox files or Dropbox sample files in the directory and file listings of the control Base-VM hard discs. Before installing the software or accessing the files, it was expected that references to Dropbox were not present in the control media directory listings. [4].

- Windows 10 Education

In the other VMs, there were multiple allusions. A substantial number of filenames were exposed in the Upload-VMs, as well as in the Desktop folder, Downloads folder, and Dropbox folder; 'C:User[username]Dropbox'. In the Upload-VMs file listings, Dropbox URL references were found, but

not in the Access-VMs or Download-VMs. This URL was created as part of the Dropbox client software installation process.

- Ubuntu 21.10

It would be easier to recover deleted synced data if the trash folder in the /home/[User Profile]/.local/share/Trash/files path was not empty. Furthermore, the.TRASHINFO file in /home/[User Profile]/.local/share/Trash/info/ could include the deleted files' original file locations and deletion timestamps. A search of the /var/lib/dropbox/.mono/certs/Trust folder resulted in the discovery of a list of Dropbox certificates.

The user password can be obtained in a variety of ways, including manually searching the RAM for keywords, cracking the password list kept in the web browser, utilising a credential management like Keychain, or straight from the user. Only the directories in the /opt/ dropbox, /var/log/ dropbox, and /var/lib/ dropbox paths were removed after the uninstallation.

2. Prefetch

Windows uses prefetch files to collect information about software activities, such as how often it has run and the linked files it has accessed. Prefetch files on every VM hard drive except the control Base-VM hard drives had information about the filenames of the Dropbox executable and Dropbox sample files, according to an examination of the VM hard drives. Even after using Eraser and CCleaner to delete prefetch files like wordpad.exe.pf, notepad.exe.pf, dllhost.exe.pf, and explorer.exe.pf, there was enough information in them to reveal the existence and path of the sample Dropbox files.

3. Link files

Within the control Base-VMs, no Dropbox linked link files were detected. All Upload-VM, Download-VM, and Eraser-VM hard drives have link files corresponding to Dropbox. The filenames and folder names for the Dropbox executable and Dropbox sample files were reviewed in the link files. These were in the Users 'AppData' directory, under the 'WindowsStart' and 'WindowsRecent' folders. The Access-VM hard drives did not contain any Dropbox link files. This demonstrates that link files were not formed if files were not downloaded from Dropbox to the computer.

4. Registry

AccessData Registry Viewer version 2.0.0.7 and RegRipper version 3.0 were used to examine registry files. There were no references to Dropbox files in the control Base-VM hard discs, according to the analysis. In the Upload-VM, Access-VM, and Download-VM registry files, there were references to the Dropbox URL, Dropbox software files, folders, and Dropbox sample files. The 'RecentDocs' key in the NTUSER.dat registry file displayed a list of Dropbox files [5], and Figure 9 shows a RegRipper result.

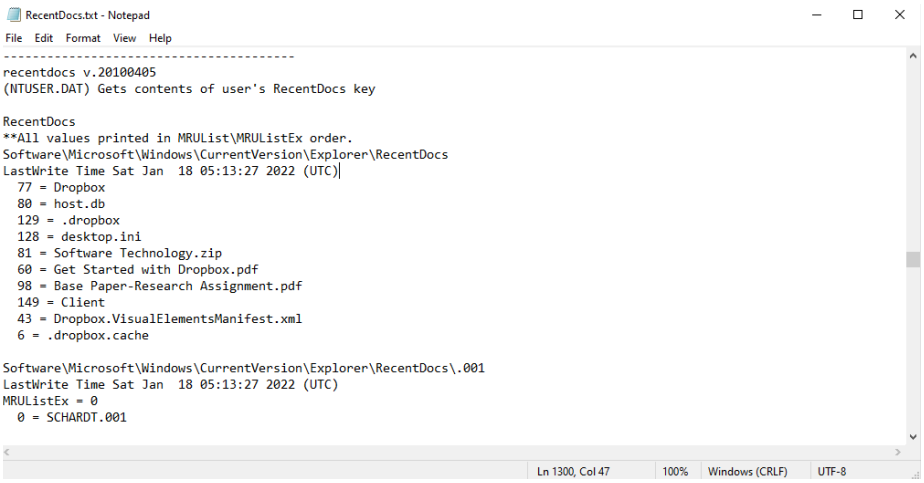


Figure 9: RegRipper output for Dropbox in NTUSER.DAT file

In any of the VMs, there was no evidence of the Dropbox login in the registry files. The NTUSER.dat registry files in the Chrome and Edge CCleaner-VMs contained deleted Dropbox information, including as filenames and URL references [6], but not in the Firefox CCleaner-VM. After the Dropbox client software was installed, file references to Dropbox software were in the SOFTWARE and SYSTEM registry hives, but not after a browser was used to log on or download data from Dropbox. After using the Dropbox client programme, references were also found in the 'UsrClass.dat' registry files, but not after using a browser to access Dropbox.

5. Thumbcache

Before installing or accessing Dropbox, an examination of the thumbnails stored in the thumbcache files in the control Base VMs revealed that no Dropbox or Enron sample picture thumbnails were present. The Upload-VM, Download-VM, and Eraser-VMs all had thumbnails for the Dropbox sample photographs, but neither the Access-VMs nor the CCleaner-VMs did. This indicates that the thumbnail cache is a potential source of Dropbox usage data, although the results may not be definitive. Dropbox can be used

in select situations when no evidence is dropped in thumbnails, such as reading files through a browser without having to download them to a computer.

6. Event Logs

- Windows 10

Once client software was installed and launched, the keyword term 'dropbox' was detected in the 'Windows Firewall.evtx' event log files. There were further references to Dropbox and Enron sample data files in the 'GroupPolicy Operational.evtx' files after Microsoft Edge was used to download data from a Dropbox online application. Despite this, EvtParser, Event Log Explorer, and the built-in Windows Event Viewer were unable to decipher the information included in these entries. After using the Google Chrome and Mozilla Firefox browsers, no parallel entries were found.

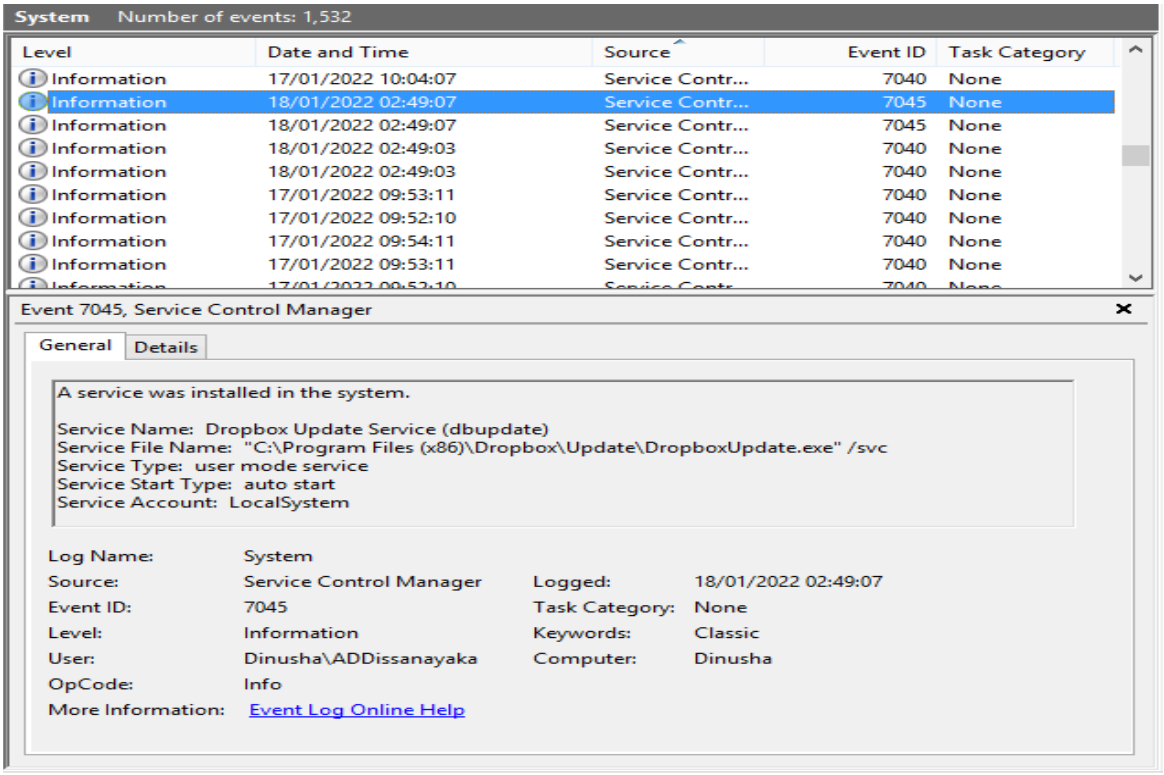
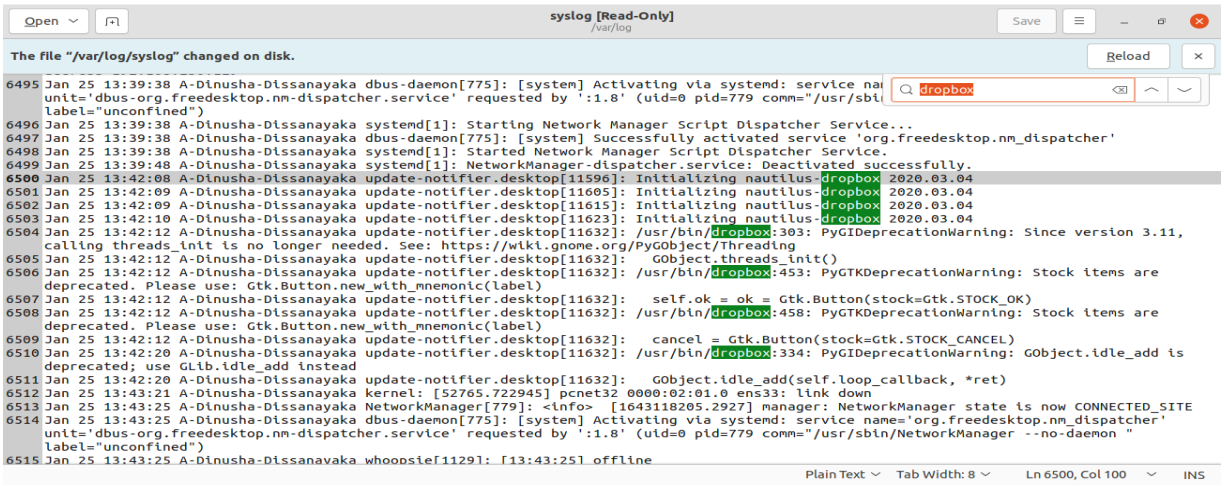


Figure 10: Windows event log entry for Dropbox installation

- Ubuntu 21.10

Almost all processes, events, and user account activity are watched in Linux inspections, therefore log files are very important [7]. A scan of the /var/log/syslog for the word 'dropbox' revealed time references for the installation of the major dropbox services (Figure 11).



Timestamp references for the installation of Dropbox in Syslog file

The /var/log/dpkg.log contained information on the dropbox.deb installer package, including the Dropbox version installed, installation status (e.g., installed, configured, and unpacked), and the matching installation time (Figure 12).

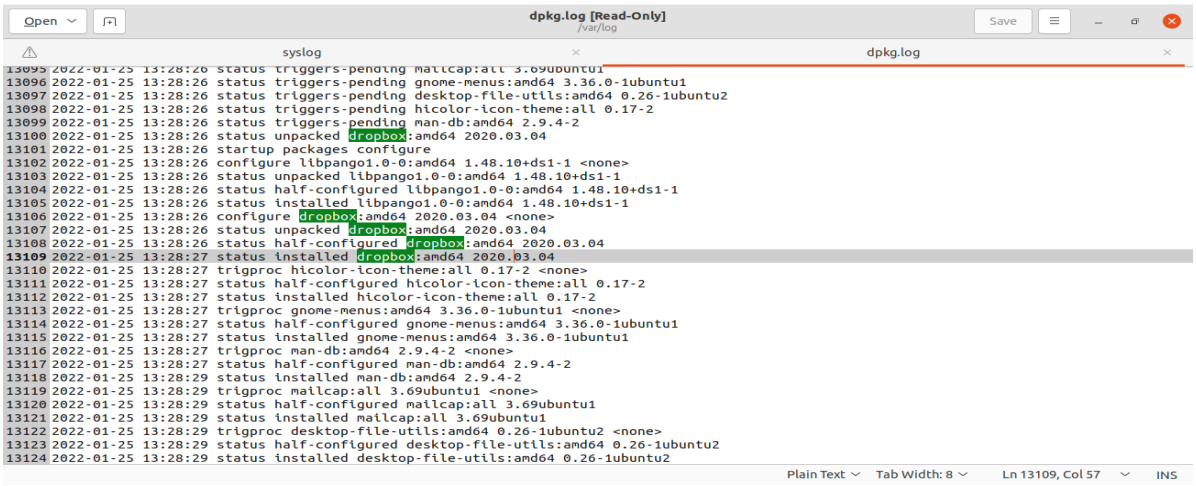


Figure 12: Dropbox version installed, installation status, and installation time in dpkg log file

The authorisation (giving superuser permission) information for the installation, the paths used throughout the installation, and the parallel installation time were all found in the /var/log/auth.log (Figure 13).

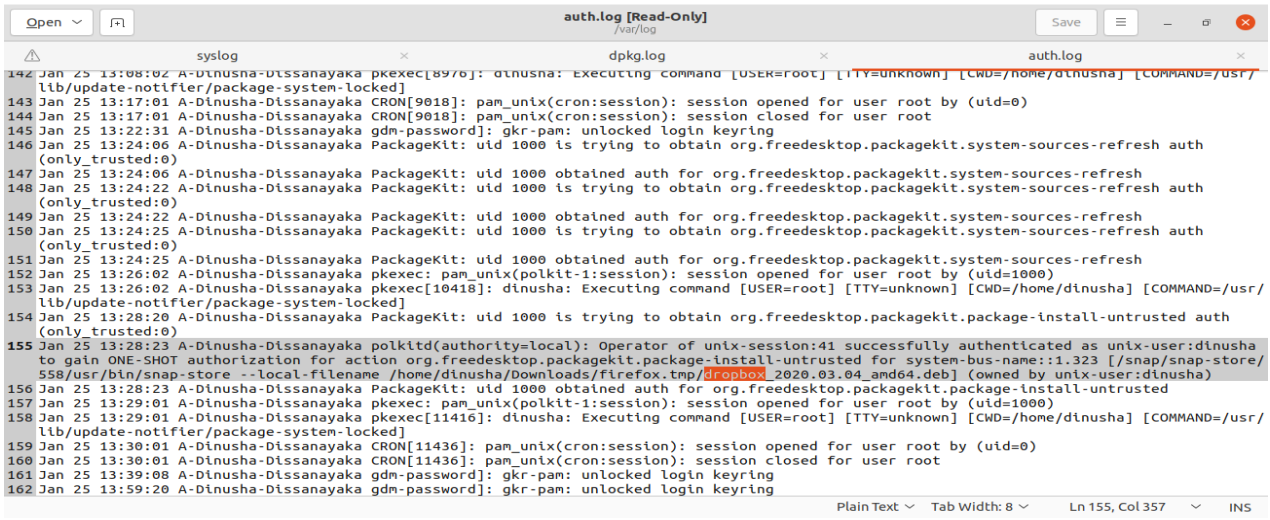


Figure 13: Details found in auth log file

7. Browser Analysis

Encase 6.19.4, Internet Evidence Finder (IEF) Standard Edition, Magnet Software, Digital Detective NetAnalysis, and SQLite Database Browser were used to examine internet browsing data. It was confirmed that the internet browsing history of the control Base-VM files contained neither Dropbox or Enron sample data. After using Mozilla Firefox and Google Chrome, the Dropbox account username was revealed, but after using Microsoft Edge, there was no trace of it. However, if the login and password were saved using Microsoft Edge, Nirsoft IE PassView was able to recover the information. The username was saved in the 'formhistory.sqlite' database in Firefox and the Autofill 'Web Data' file in Google Chrome.

After logging in to Dropbox with Microsoft Edge, Mozilla Firefox, or Google Chrome, the website data were located in Cookie files, web history, FavIcons, and the FileSlack of other files. Filenames for downloaded items, such as the Dropbox sample files, were also discovered in the browsers' online history. The presence of the aforementioned URLs in Google Chrome's percent AppData percent LocalGoogleChromeUser DataDefaultSessionsSession files, Mozilla Firefox's percent AppData percent RoamingMozillaFirefoxProfiles percent PROFILE percent.default sessionstore.js, and Microsoft Edge's percent AppData percent LocalMicrosoftWindowsWebCacheWebCacheV01.log and percent AppData percent LocalMicrosoftWindowsWebCacheWebCache (Figure 14). All references in Mozilla Firefox and Microsoft Edge VMs were wiped using all CCleaner settings, however the details remained in the Google Chrome 'FavIcon' history [8], revealing Dropbox usage.

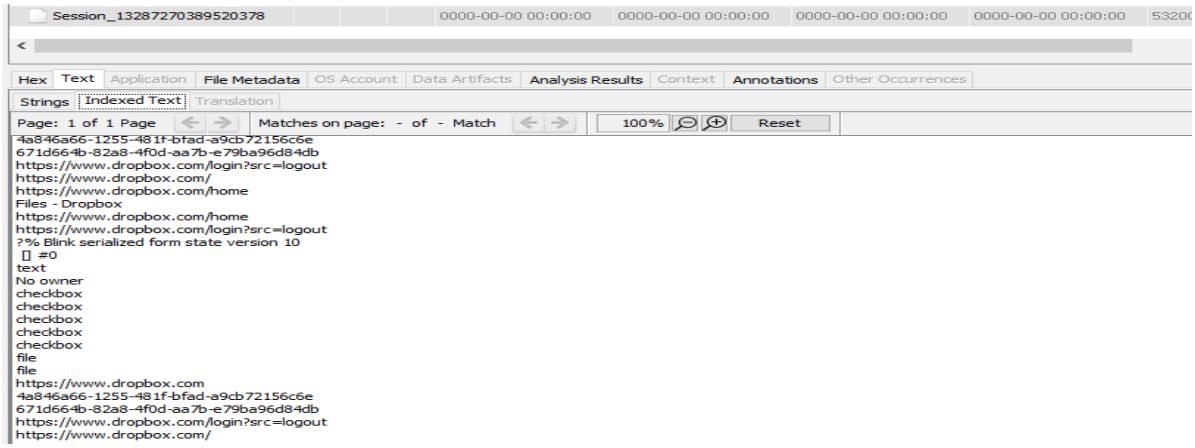


Figure 14: Google Chrome Session file

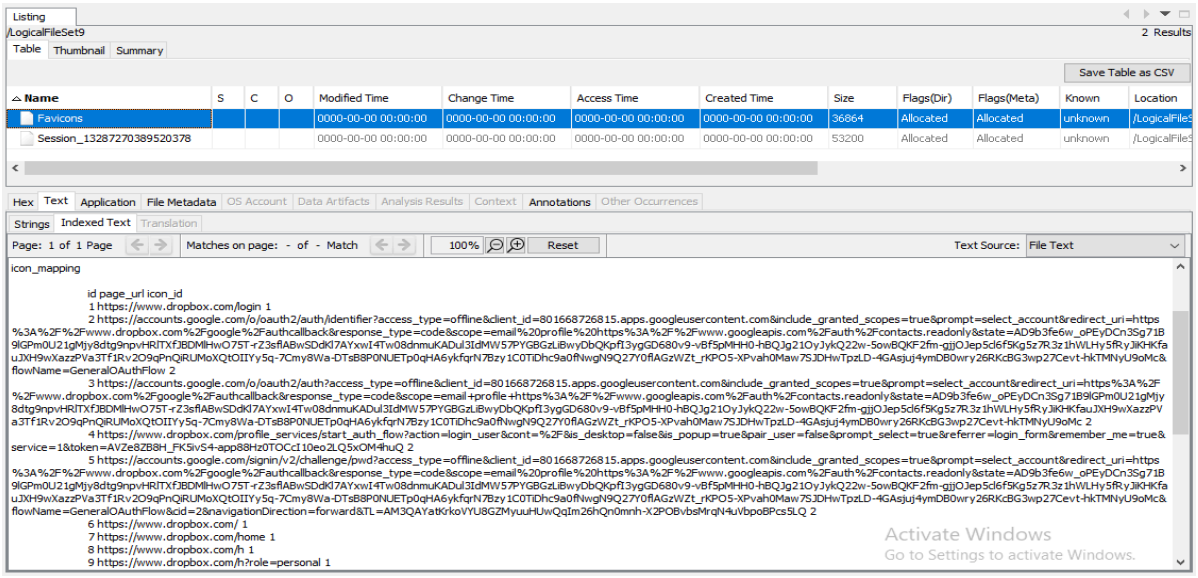


Figure 15: Google Chrome 'FavIcon' history

8. Network Analysis

Evaluation of the network traffic capture files was commenced using Network Miner and Wireshark Portable software. The network traffic was only noticed on TCP Port 443 (HTTPS) and 80 (HTTP). When logging into the Dropbox using the Client software or a web browser, a session with an IP in the range of 199.47.216.0 – 199.47.219.255 was initiated on Port 80, and then another session with an IP in the range of 199.7.48.0 – 199.7.63.255 or 199.16.80.0-199.16.95.255 on Port 80 and then on Port 443, that is

registered to VeriSign/Thawte. Certificates seemed to be certified using VeriSign/Thawte services. The next accessed IP's seemed to be in the range of 74.125.0.0 – 74.125.255.255, that are registered to Google, and seem to be part of the Google Analytics service. IP numbers assigned to AmazonAWS, the Amazon Web Services (EC2) service, were then detected. Table 2 shows a list of IP number ranges with their registered owners.

9. RAM Analysis

Encase and AccessData FTK [9] were used to evaluate the memory captures (VMEM files). In the memory captures of the Microsoft Edge and Google Chrome control Base-VM files, the term 'dropbox' was identified, but none in the Mozilla Firefox control Base-VM file. The entries were discovered with lists of other URLs in the Chrome and Microsoft Edge memory. The Dropbox username near to text; 'u'email' was found within the memory grabs when utilising the client software. This text can be used to look into and find prospective Dropbox account usernames. Encase and AccessData FTK [8] were used to evaluate the memory captures (VMEM files). In the memory captures of the Microsoft Edge and Google Chrome control Base-VM files, the term 'dropbox' was identified, but none in the Mozilla Firefox control Base-VM file. The entries were discovered with lists of other URLs in the Chrome and Microsoft Edge memory. The Dropbox username near to text; 'u'email' was found within the memory grabs when utilising the client software. This text can be used to look into and find prospective Dropbox account usernames.

Except for the control Base-VM, all VMs were examined for Dropbox and Enron filename references. In all Upload-VMs, as well as practically all Access-VMs, Download-VMs, and CCleaner-VMs, website information such as 'www.dropbox.com' was retrieved. In the Upload-VM, Access-VM, and Download-VM memory grabs, the whole text of the Enron and Dropbox example files was recovered. From the memory captures of Access-VM, Upload-VM, and Download-VM files, data sculpting was performed, resulting in the retrieval of thumbnail photographs and Dropbox sample pictures.

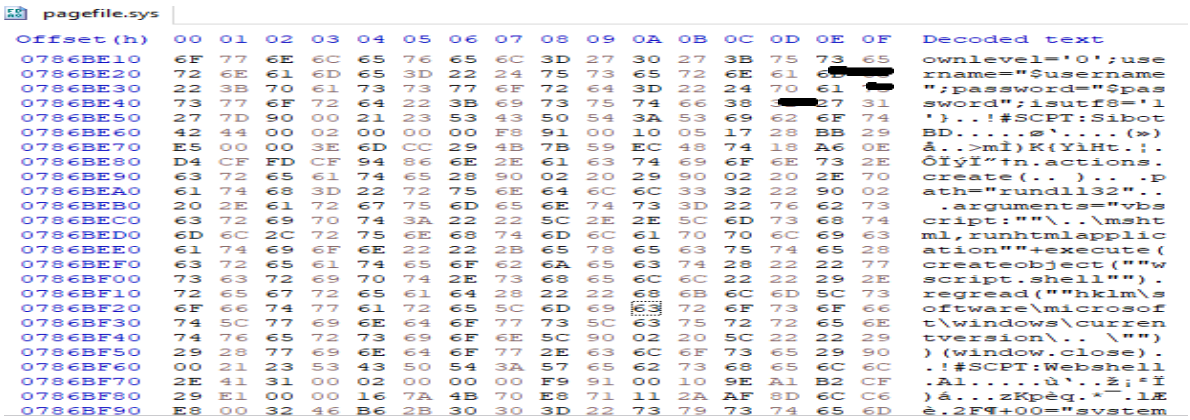


Figure 16: Remnants located within the memory space of dropboxsync.exe

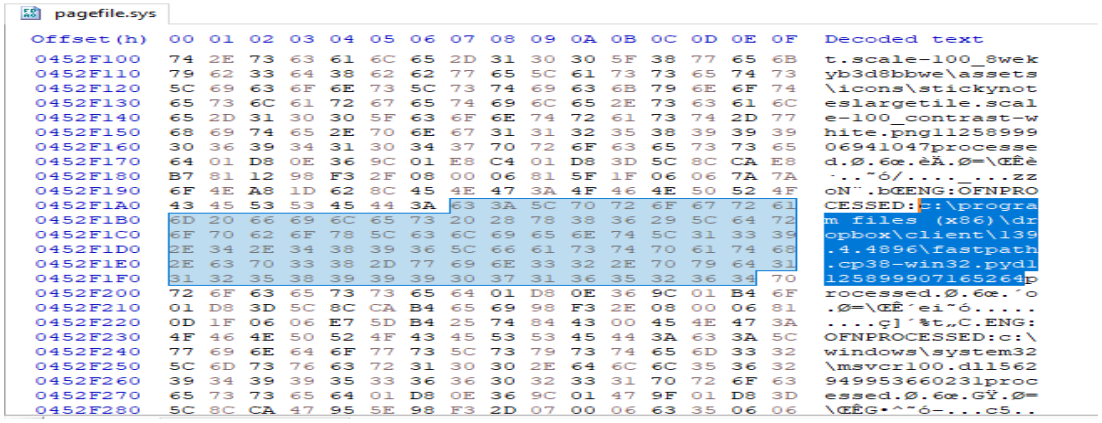


Figure 17: Data observed in the memory space of client software

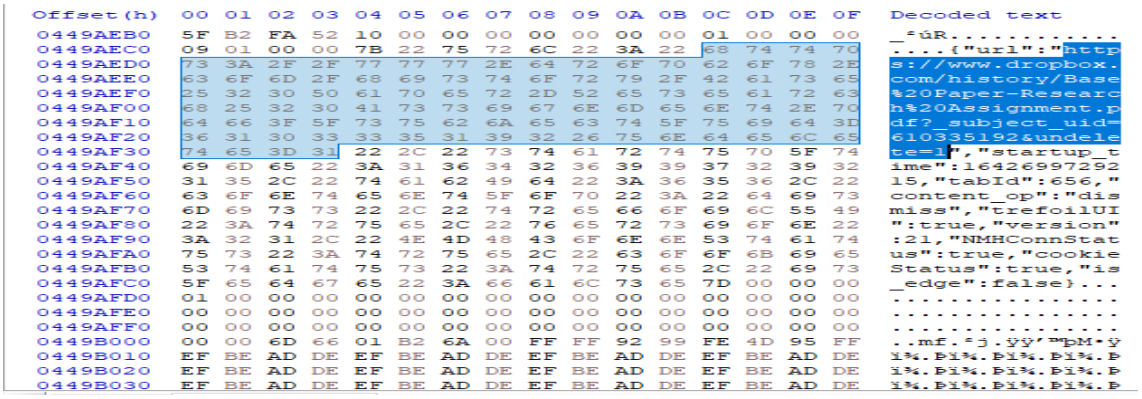


Figure 18: A file download link recovered from the RAM of Mozilla Firefox VM

Pagefile.sys file evaluation was not as conclusive as memory capture files [10]. There were no matches to Dropbox sample files or Enron data photos or thumbnails while data carving the pagefile.sys files. The Mozilla Firefox Upload-VM pagefile contained some thumbnail icons, and the Google Chrome

Access-VM pagefile contained a partial screen capture of the Dropbox website, displaying a thumbnail symbol used in the Google Chrome navigation tab. The pagefile.sys files did not contain the username or password.

Dropbox Analysis On Mobile Devices

The goal of this section of the study is to look at the data leftovers on an iPhone 3G running iOS 4.2.1 when it's used to visit Dropbox via a browser or the Dropbox iOS app.

1. **Dropbox Analysis on iOS**

The.XRY extract files and the outcome of the.XRY software, were discovered as files that would include the evidence required to conduct the evaluation. For each of the extracts, Base, Browser, and Application, these were discovered.

A copy of the.XRY extract files and the reports were made to evaluate the concepts of forensic computer analysis. Because these were logical files, the X-Ways Evidence File Container format was used (ctr). MD5 hash values were used to verify the data's forensic integrity.

Forensic tools such as X-Ways Forensic version 16.5 and Guidance Software EnCase version 6.19.4 were used to examine each of the forensic files. The contents of the Apple plist files recovered by were examined using PList Explorer v1.0. The sqlite files were examined using XRY. SQLite Database Browser 2.0.

- Control - Base-XRY

Evaluation of the control Base-XRY extract proved there was no data originally present involving to the Dropbox sample files, the Enron sample test data, or the Dropbox application. Furthermore, no references were found for the term ‘dropbox’ or the website URL (www.dropbox.com).

- Dropbox accessed via the iOS Safari Browser

The research username or account password was not discovered in the Browser-XRY extracts. Filenames for the Dropbox sample files and Enron test files were in History.plist. These details were also extracted by XRY in the Web-History.txt file (Figure 19).

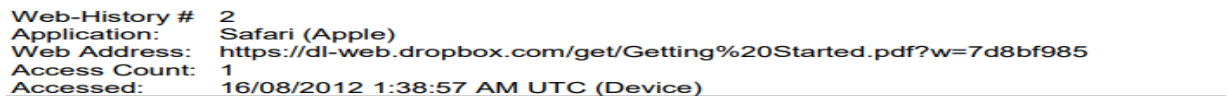

Web-History # 2
Application: Safari (Apple)
Web Address: https://dl-web.dropbox.com/get/Getting%20Started.pdf?w=7d8bf985
Access Count: 1
Accessed: 16/08/2012 1:38:57 AM UTC (Device)

Figure 19: .XRY Web-History.txt file #2

The dropbox website URL was also found in the History.plist and Web-History.txt files (Figure 20). The URL was also found in the Cookies.binarycookies file

Web-History #	14
Application:	Safari (Apple)
Web Address:	https://www.dropbox.com/m/home?path=/Dataset
Page Title:	Dropbox files
Access Count:	1
Accessed:	16/08/2012 1:22:56 AM UTC (Device)

Figure 20: .XRY Web-History.txt file #14

- Dropbox Application (App) used to access the research account

The login used to access the Dropbox account was verified using the third XRY extract. This was discovered in the files 'com.getdropbox.Dropbox.plist' and 'keychain-backup.plist', near the words '=]DBAccountInfo'. XRY does not appear to parse this information. Data in the 'iTunesstored2.sqlitedb' file also accessed Dropbox to see if the application was there. There was no text from the Enron files in any of the extracts. None of the extracts or files contained a password.

2. Dropbox Analysis on Android

On the laptop, a virtual machine was created to simulate an Android smartphone. Genymotion, a well-known Android emulator based on VirtualBox, was downloaded. After that, the Open GApps were downloaded. As a result, it will be able to download software from the Google Play Store. This mobile device emulator allows you to use a computer to run a virtual mobile device. This emulator allows users to test Android apps without needing to hold an actual device, and it also includes documentation and utilities that can help with device forensics (Figure 21).

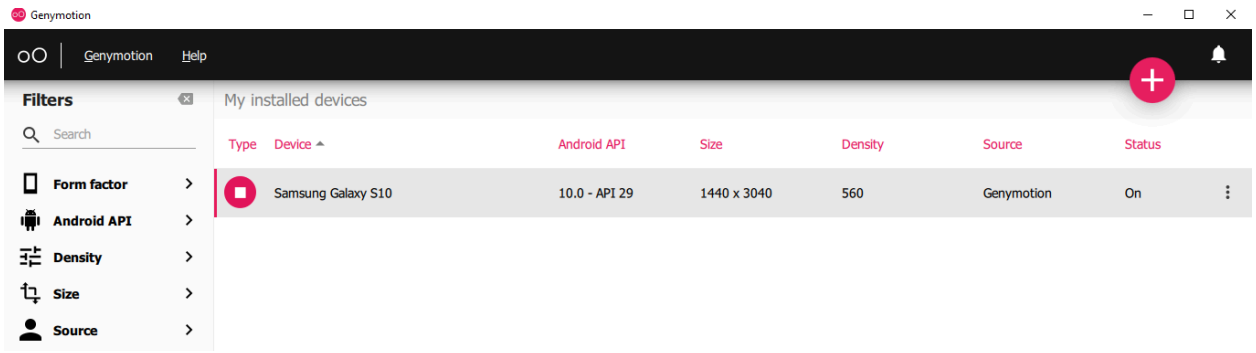


Figure 21: Samsung Galaxy S10 virtual device created in Genymotion Android Emulator

In the Genymotion software, a virtual Samsung Galaxy S10 mobile device was created using the Android 10.0 (Quince Tart) API. The Play Store was installed using the Genymotion software's Open GApps functionality. Then Dropbox was installed and synced with the research Dropbox account, resulting in Dropbox files that were similar across all operating systems. The Dropbox files and folders were viewed using the ES File Explorer software (Figure 22).

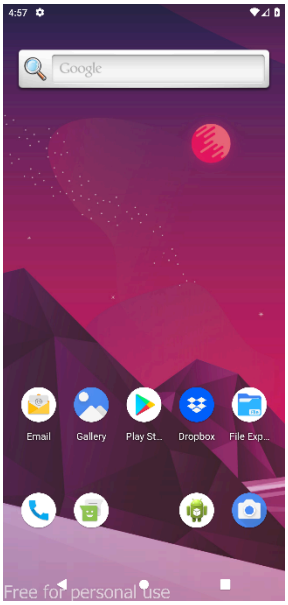


Figure 22: Virtual Android device after installation of Dropbox and ES file Explorer

The installation of the Dropbox Android app triggered the creation of /Android/data/com.dropbox.android folder which has two subfolders, namely cache, and files (Figure 23). Copies of the viewed files were found in the download folder in /Android/data/com.dropbox.android /files/downloads. No Dropbox related folder or file remained once the Android app was uninstalled

.

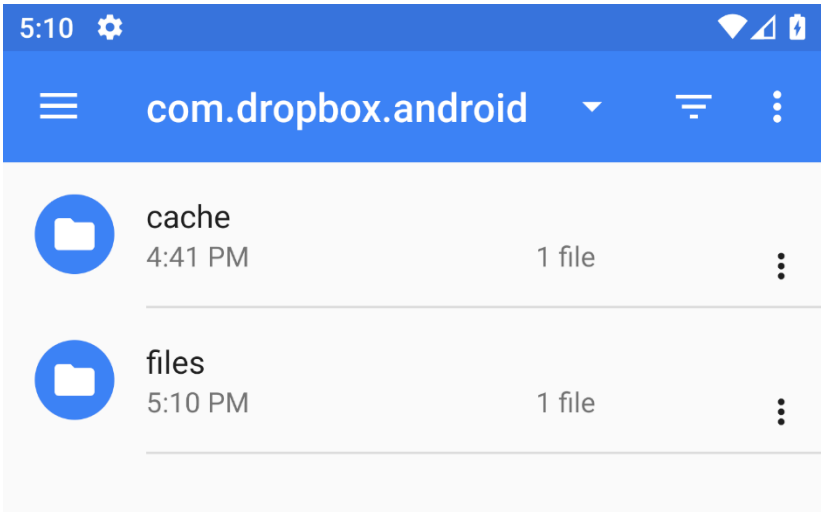


Figure 23: Two folders in the path /Android/data/com.dropbox.android

Inside the "cache" folder were two subfolders labeled "thumbs" and "tmp." The contents of the "thumbs" folder show a full list of Dropbox stored data. The folder structure was intact as it was locally on the Android emulator, demonstrating the main Dropbox file structure as well as the subfolders. No data was found in the temporary, or "tmp" folder using the path /Android/data/com.dropbox.android/cache/tmp.

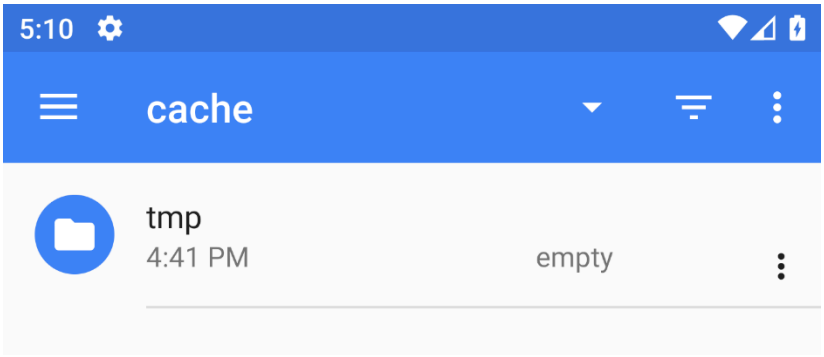


Figure 24: tmp folder in the path /Android/data/com.dropbox.android/cache

The next folder is present under the com.dropbox.android named "files," which was a subfolder of the "cache" folder, was also observed. The "files" folder had a subfolder, "scratch," with three subfolders inside that. Yet, no data was present in these folders.

Discussion and Conclusion of DropBox

A range of data remnants was discovered when a user used Dropbox to store or access data. Dropbox client software, sample data files, and the common locations were summarised in Table 3. This information facilitates an examiner to perform hash analysis and keyword searches for the file names listed and will aid to clarify if Dropbox client software has been used. From the evaluation commenced, the task of identifying whether a Dropbox account has been logged on either using Dropbox client software or a web browser can be revealed in several ways. Details investigated such as URLs in the network traffic, filename references in directory listings, filename data in prefetch and link files, browser history, RecentDocs and typed URL's in registry files, and information retrieved from memory files demonstrated the use of Dropbox, filenames, and actual dat. When the forensic investigation has concluded that a Dropbox account has possible proof of relevance to an inspection, the investigator can communicate this to relevant persons to facilitate them to respond to secure evidence in an appropriate manner. Network analysis revealed that the majority of the network traffic was encrypted, and the file information was not retrieved. Some of the network traffic was not encrypted, and thus useful to detect Dropbox access, and to discover if Dropbox client software or a browser was used to access the Dropbox. Evaluation of the RAM captures retrieved all files, filenames, the Dropbox username, etc. This implies that memory capture is crucial, and when feasible should be carried out. It was also noticed that Dropbox maintains a record of computers used to log on and synchronise with an account. These details would be advantageous to clarify whether a specific computer was synchronised to a Dropbox account. There is a timestamped history of files and computer synchronisation, and prior versions of files that are also accessible through the Dropbox account when accessed via a browser.

Control (Base-VM)	Data artifacts found
Username, Password, Software, URL, Enron KWS terms	Nil Nil Matches to 'dropbox' in 'index.dat' files, 'msjint40.dll.mui', 'pagefile.sys', unallocated clusters, and memory captures
Client Software (Upload-VM)	Data artifacts found
Username Password Software	Memory capture files near; 'u'email':' Located in RAM – search for 'free name periods' Dropbox 1.2.52.exe file located when downloaded.

URL Enron sample filenames Enron sample files KWS terms	Dropbox Software installation under '[User]\AppData\Roaming\Dropbox' Dropbox sample files and folders at location 'C:\Users\[username]\Dropbox' When software downloaded, URLs included www.dropbox.com Multiple locations, including Prefetch, Link files, $MFT, Registry. Located in Sync folder under User\Dropbox. Thumbnail pictures in Thumbcache 'dropbox' in Event Logs
Browser Access (Access-VM)	Data artifacts found
Username Password Software URL Enron sample filenames Enron sample files KWS terms	FF and GC History; 'formhistory.sqlite' and 'Autofill'. Memory capture files 'login_email' Nil Nil Multiple locations; cookie, history, icons, pagefile.sys and unallocated Sufficient to identify files accessed with references to the filenames in Registry and Browsing History Full text in RAM Multiple matches to KWS terms
Browser Download (Download-VM)	Data artifacts found
Username Password Software URL Enron sample filenames Enron sample files KWS terms	FF and GC History; 'formhistory.sqlite' and 'Autofill'. Nil Nil Multiple locations; cookie, history, icons, pagefile.sys and unallocated Sufficient to identify files accessed with references in $MFT, Link, Registry and Prefetch files Via uncompressed zip or folder name; 'Documents.zip' References in Event Logs (ME)

Eraser (Eraser-VM)	Data artefacts found
Username	FF and GC History; ‘formhistory.sqlite’ and ‘Autofill’.
Password	Nil
Software	Nil
URL	Multiple locations; cookie, history, icons, pagefile.sys and
Enron sample filenames	unallocated
Enron sample files	Sufficient to identify files accessed with references to the
KWS terms	filenames in $MFT, Link and
	Prefetch files
	Thumbnail pictures in Thumbcache
	Multiple matches to KWS terms
CCleaner (Ccleaner-VM)	Data artefacts found
Username	Nil
Password	Nil
Software	Nil
URL	Google Chrome FavIcon history
Enron sample filenames	Sufficient to identify files accessed with references to the
Enron sample files	filenames in Prefetch and Link files
KWS terms	Nil
	Multiple matches to KWS terms

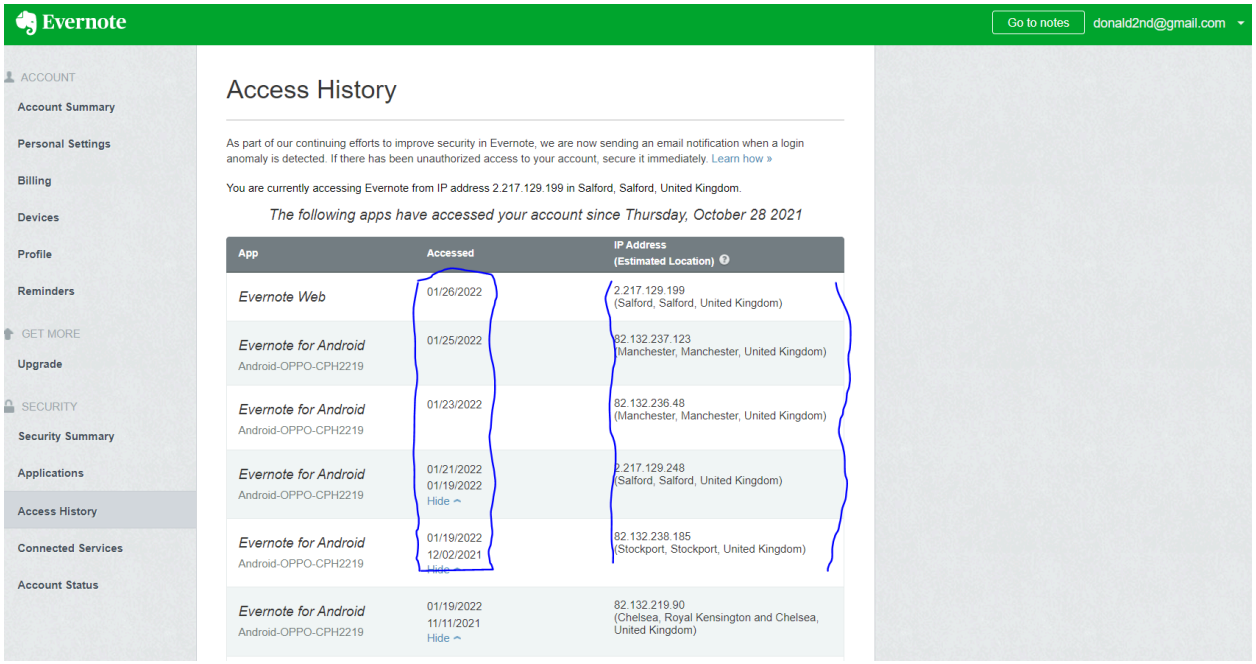
Table 3: Summary of Dropbox final outcomes in computer devices

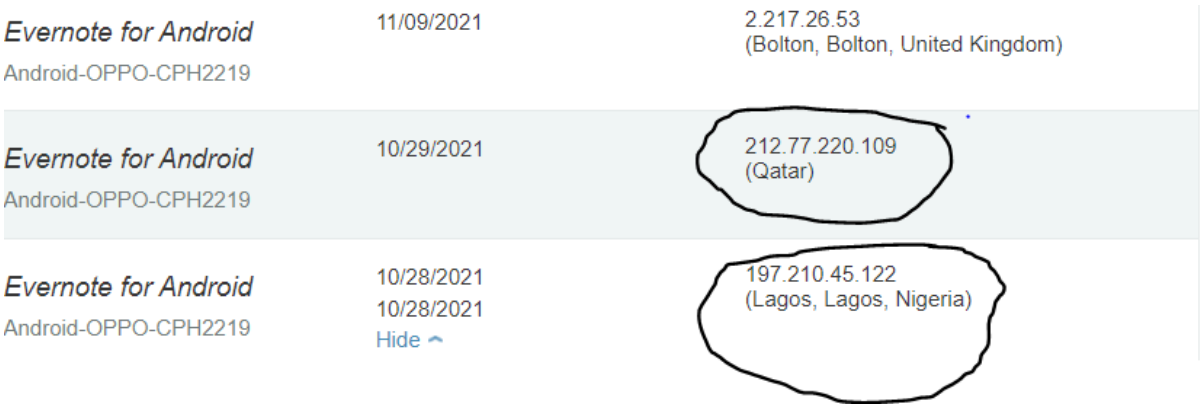
When looking for proof of Dropbox usage on iPhone and Android mobile devices, several data fragments were uncovered. Although no matches to the keyword 'dropbox' were found in the control extract, matches in consequent extracts suggested that running a search for the keyword 'dropbox' could disclose whether the Dropbox had been utilised. Records were left over in the History.plist file once the in-built browser is used to log on to Dropbox, which were also recorded in the.XRY Web-History.txt file. The extract did not reveal the login or password. The filenames for the Enron files were saved in the History.plist and.XRY Web-History.txt files. The username was discovered in the 'com.getdropbox. Dropbox.plist' file after the Dropbox was installed and logged on to the research account. Nonetheless, no text from the Dropbox or Enron sample files could be discovered on any of the mobile devices, and no password for the account could be found.

2. EVERNOTE

Evernote is cloud based software as a service solution, which works through mobile apps and websites that enable users to store information on the move. The solution is such that it enables a user to keep notes for a long time because it is not device dependent, meaning that you can retrieve your notes with or without your mobile devices . It has designs and tracking abilities for different human documentation needs, e.g a boarding pass, receipt, article you want to read, to do list, or even a simple typed note.

The solution has robust inbuilt logging abilities such that assist forensic investigations of a user. As seen in the diagram below, it has information on the IP address, location, operating system and device name of the user. The evidence is substantiated with the date stamps of the events on the storage location.





SN	Email address of the Evernote account owner	Data access Date	Name of the native environment used to access Evernote	IP address and Location of the device used to access Evernote	Device name
1	Donald2nd@gmail.com	01/26/2022	Web, Android,	2.217.129.199-Salford United Kingdom	Android Oppo-CPH 2219

PLATFORM AS A SERVICE (PAAS)

1. AZURE PLATFORM

We set up a windows 2016 server on the AZURE environment. The purpose was to carry out transactions and collect evidence from the location for analyses. In the absence of straight through forensic tools, we tried installing FTK and Autopsy on the server to enable collection of images from Windows OS and LINUX servers. The screenshot below explains the experimental setup.

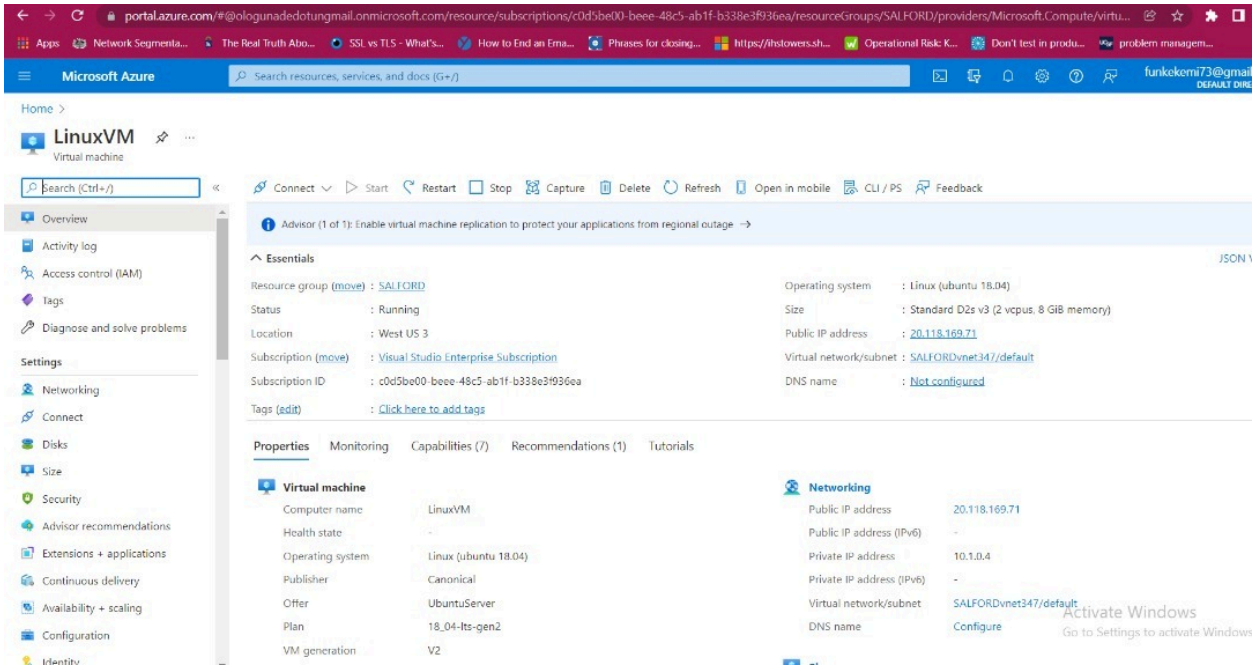


Fig.1. Screenshot of Azure Platform with UBUNTU 18.04

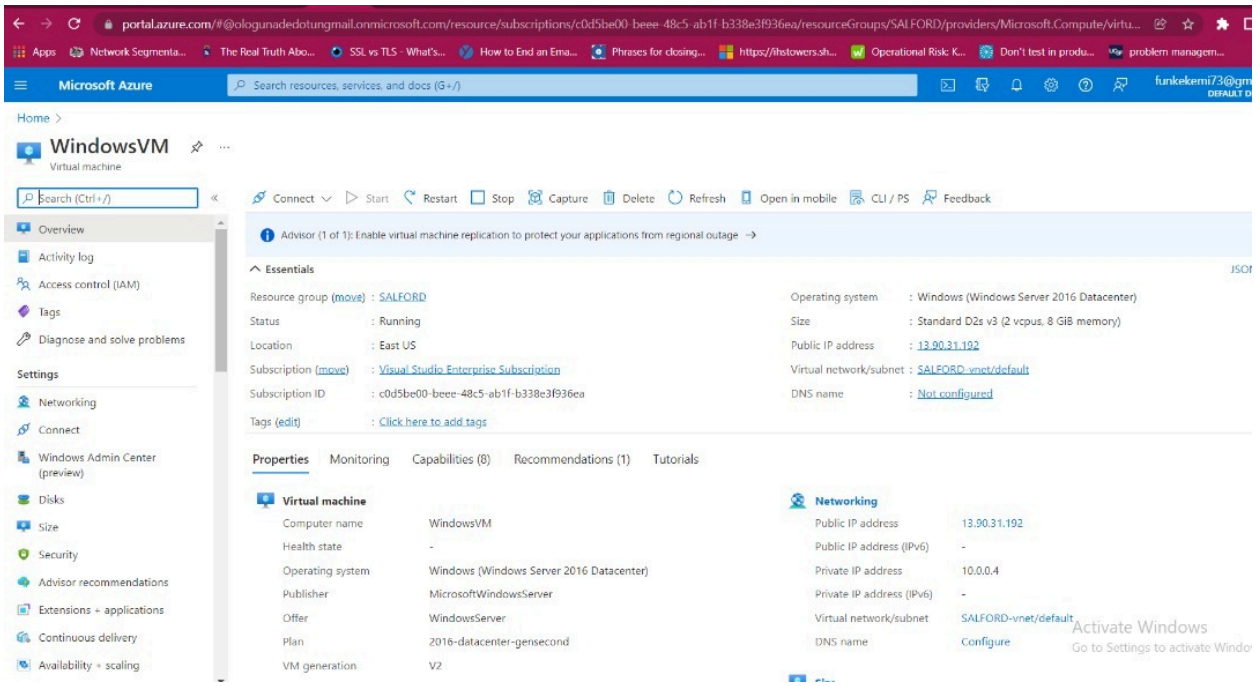


Fig.2. Screenshot of Azure Platform with Windows 2016, v2 environment.

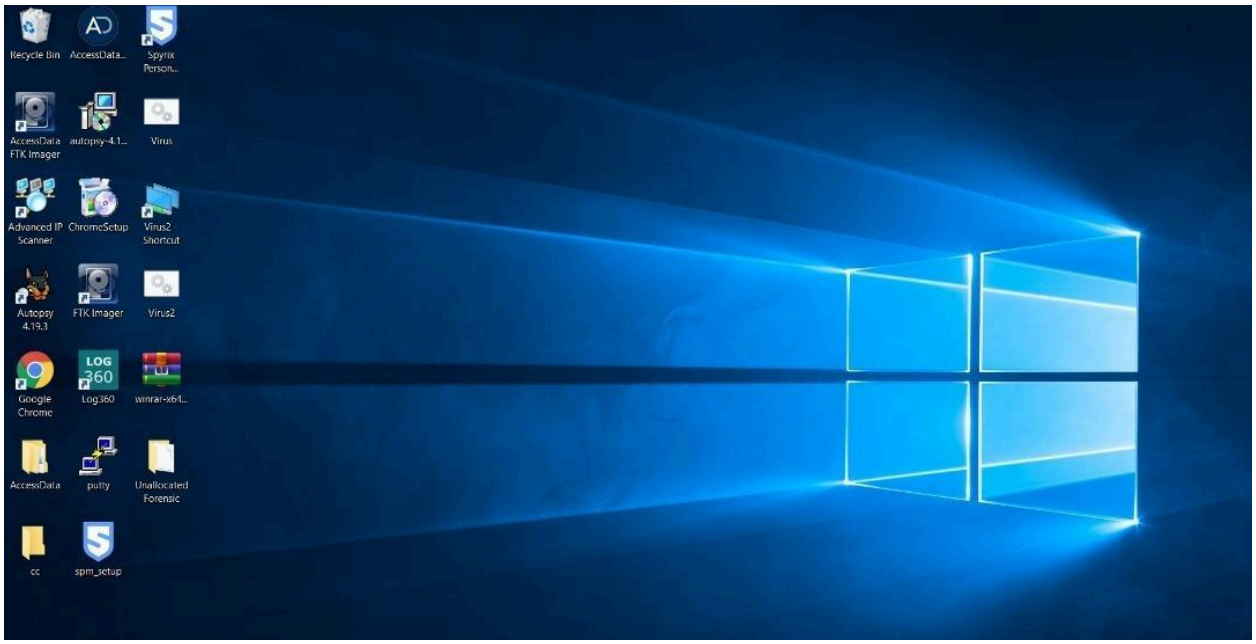


Fig.3. Screenshot of Azure Platform, showing installation of FTK and Autopsy tools, planned for image collection and analysis.

ANALYSIS

We carried out the following activities on the windows 2016 server for the purposes of the review;

- Creation of word pad file by a user
- Alteration of the file by another user
- Changing of windows registry files
- Creating of files by a user
- Visiting several Internet sites by several users.

Forensic Evidence with Autopsy

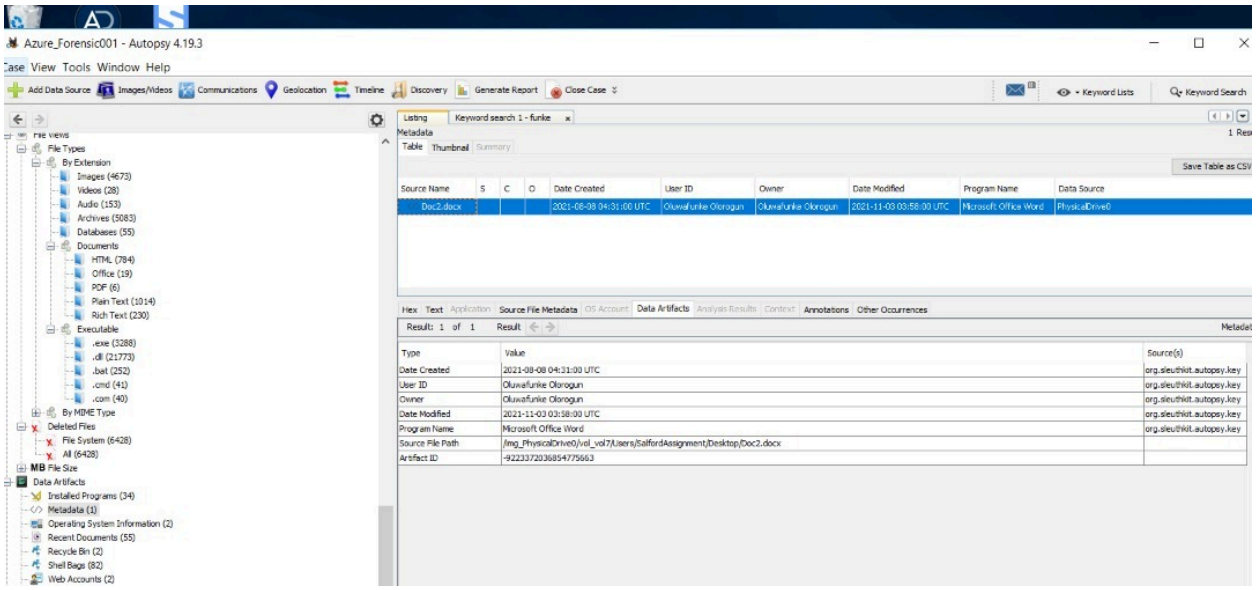


Fig.4. Showing a meta data, indicating that Funke user created a file with the meta data information of the file.

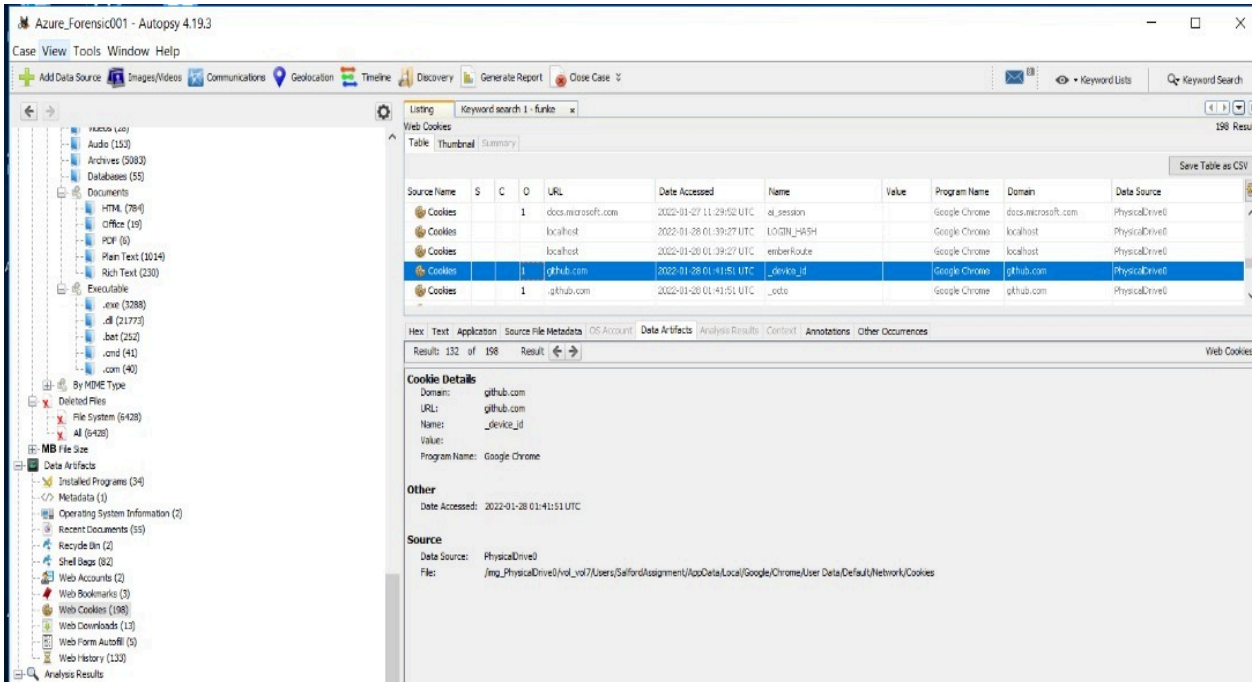


Fig.5. Showing a meta data, indicating a user with internet browsing history with metadata showing details of time, website name etc.

CRITICAL ANALYSIS

Research on cloud Digital forensics was an interesting assignment. Paths were followed to achieve results but there were frustrations due the issues related to tools that will work efficiently in the cloud environment. The experience shows that there is a difference between forensics on a local device compared to carrying forensics on the cloud infrastructures of software as a service and platform as a service.

We discovered that there were static tools that could pick evidence at the cloud locations directly through supplying the user name and password of the subscribed cloud user. Example of such a tool that could enable successful cloud forensics is called Anxiom Magnet.

In the absence of such a tool, we had to do a mix of lots. We installed FTK and Autopsy at the cloud servers for image collection and analysis. Before that, we used different users to carry out transactions on the servers so that each of the user activities will be captured in the analysed results. Limited results came our way due to the limitations of the platform owners and the nature of instability experience at the platform locations. In addition, we were able to review the log information available on windows, which could be helpful in establishing evidence in the support of tracking down actors of computer incidents.

On Saas environments like Dropbox, Evernote, and google drive, we leveraged on the tools to pick some helpful technical information. In addition, the platforms have logs that were helpful in establishing a series of incidents depending on the client's activities. Those trails were discussed in the work.

Finally, the assignment establishes that Cloud digital forensics requires a suite of tools that will image and analyse activities on those cloud environments as a whole. Breaking them into pieces as we did could bring some technical challenges that could negatively impact on success and the chains of custody requirements.

REFERENCES

Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2015). A forensic acquisition and analysis system for IaaS. *Cluster Computing*, *19*(1), 439–453. https://doi.org/10.1007/s10586-015-0509-x

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital Investigation*, *9*(2), 81–95. https://doi.org/10.1016/j.diin.2012.05.015

Daryabar, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R. (2016). Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. *Australian Journal of Forensic Sciences*, *48*(6), 615–642. https://doi.org/10.1080/00450618.2015.1110620

Focus, F. (2011, July 24). *Dropbox Forensics*. Forensic Focus. https://articles.forensicfocus.com/2011/07/24/dropbox-forensics/

Hale, J. S. (2013). Amazon Cloud Drive forensic analysis. *Digital Investigation*, *10*(3), 259–265. https://doi.org/10.1016/j.diin.2013.04.006

Hasan, R., & Zawoad, S. (2013). *Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems*.

Lim, S. Y., Johan, A., Daud, P., & Ismail, N. A. (2020). Dropbox Forensics: Forensic Analysis of a Cloud Storage Service. *International Journal of Engineering Trends and Technology*, *2231-5381*, 45–49. https://doi.org/10.14445/22315381/cati3p207

Quick, D., & Choo, K.-K. R. (2013a). Dropbox analysis: Data remnants on user machines. *Digital Investigation*, *10*(1), 3–18. https://doi.org/10.1016/j.diin.2013.02.003

Quick, D., & Choo, K.-K. R. (2013b). Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems*, *29*(6), 1378–1394. https://doi.org/10.1016/j.future.2013.02.001

Quick, D., & Choo, K.-K. R. (2014). Evernote: Forensic analysis of data remnants. *Journal of Network and Computer Applications*, *40*, 179–193. https://doi.org/10.1016/j.jnca.2013.09.016

Roussev, V. (2009). Hashing and Data Fingerprinting in Digital Forensics. *IEEE Security & Privacy Magazine*, *7*(2), 49–55. https://doi.org/10.1109/msp.2009.40

Mohammad Shariati, Ali Dehghantanha, Ben Martini and Kim-Kwang Raymond Choo, “Ubuntu One Investigation: Detecting Evidences on Client Machines,” Greater Manchester.

DAVID GILBERT, “Is Dropbox Secure? 10 Ways To Make The File Sharing Service Safer To Use,” comparitech, 23 07 2021. [Online].

K.-K. R. Choo, “Dropbox analysis: Data remnants on user machines,” in *Digital Investigation*, Australia, 2013, pp. Pages 3-18.

K. Buzdar, “What Is the NTUSER.DAT File in Windows 10?,” FAQforge. [Online].

Kumar, “What is the NTUSER.DAT File? How it Woks?,” TRICKS N TECH, 22 01 2018. [Online].

C. H. Malin, E. Casey and J. M. Aquilina, “Discovering and Extracting Malware and Associated,” in *MALWARE FORENSICS FIELD GUIDE FOR LINUX SYSTEMS: Digital Forensics Field Guides*, Syngress, 2013.

R. Malik, N. Shashidhar and L. Chen, “Analysis of Evidence in Cloud Storage Client,” USA.

N. A. Hassan and R. Hijazi, “Data Hiding Forensics,” in *Data Hiding Techniques in Windows OS*, United Kingdom, 2017, pp. Pages 207-265.

N. Trivedi, “Study on Pagefile.sys in Windows System,” *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. 16, no. 2, p. 6, 2014.

Aye Chan Ko and Wint Thida Zaw, “Digital forensic investigation of Dropbox cloud storage service,” Myanmar.

Reflection

It was a great learning experience of using the knowledge which I acquired through lectures, practical sessions, and self-studies, and how to work as a team in an effective and successful way.

We were able to successfully solve this real-world cyber investigation by utilizing the skills and knowledge of each team member while maintaining professional and effective communication. I learnt how to use forensics tools to retrieve information gather evidence and draw conclusions based on them. As we did compare a number of tools for our case study, now I have good exposure to the tools which are used in the industry.

One of the most essential things I have learnt is the importance of working as a group. After completing my master's program, eventually, I will work for some organisation in the industry, and I will be working with a team. To be successful as a team you need to be able to adapt, communicate effectively and professionally, respect others' opinions, manage time effectively and find the best way to utilize the skills and knowledge of the team members. These aspects usually do not come from theoretical lessons, by completing this assignment I have gained a firm grip on how to succeed as a team.

One of the difficulties that we have faced is selecting a suitable tool for our case study. We have tried ENCASE and MAGNET which are the best industry standards but unfortunately, they kept rejecting our requests for trial versions of the software. As a result of this, we had to find alternative tools, which we did, and it also turned out to be beneficial for us as we were exposed to a quite number of tools.

Working as a group also comes with extra challenges such as time management, agreeing on things, meeting deadlines, etc. To manage the time effectively we assigned specific tasks to each team member, and we set a time to get together to share the experience. When agreeing on things we would arrange a team meeting to discuss the pros and cons and draw a conclusion to take the decision. When we were not able to arrange a meeting, for example late in the evening, we would use online channels such as Microsoft Teams to conduct meetings.

To conclude things, I would like to mention that this was a great opportunity for me, not just to use my knowledge and skills on a practical scenario but also to work as a team in an effective and successful way to meet a deadline.