Forensic Analysis of Dropbox Data Remnants on Windows 10

Walter Buyu
University of Nairobi
University Way
Nairobi, Kenya

Elisha Odira Abade
University of Nairobi
University Way
Nairobi, Kenya

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 paper 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 client software installation files, browser, link files, prefetch files, registry, and network traffic.

General Terms

Digital Forensics, Computer Forensics, Cloud Storage Applications.

Keywords

Windows 10, Dropbox Forensics, Dropbox Analysis, Digital Forensics, Computer Forensics, Cloud Storage Applications.

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” [1]. The growing demand for computing power and resources have contributed to the growth of cloud computing [2]. Cloud computing is increasingly being used by both businesses and individuals [3] as it promises increased flexibility, high reliability, massive scalability, and decreased costs [4].

A typical application of cloud computing service is cloud storage services [4]. Though not new, cloud storage services are becoming increasingly popular [5]. Many cloud storage applications exist in the market, including Apple iCloud, Microsoft OneDrive, Google Drive, and Dropbox [6]. Dropbox is one of the popular cloud storage services [4, 7] and is even claimed to be the most popular among cloud users worldwide [6]. Dropbox allows users to store and share files and collaborate on projects. The service can be accessed from a PC, tablet or a smartphone, using a browser or client application. File changes on one device are automatically synchronised across all devices [8]. 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 [9].

The adoption of cloud computing has drawn the interest of cybercriminals [10]. 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 [3]. For example, Amazon’s EC2 cloud computing service was used in the hacking of Sony’s PlayStation Network [11]. Cloud storage services have also been used to commit other crimes, including DDoS, malware distribution, and child pornography [7].

Cloud storage is subject to abuse by cybercriminals [12] and coupled with the difficulty in getting artefacts of evidential value from cloud storage providers [13], it would take more time and effort to conduct cloud forensics investigation when solely relying on evidence from the cloud storage providers [14]. However, artefacts from both the client computer and cloud service provider can be relied on for cloud forensic investigation [15]. 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 [14].

Cloud storage is expected to grow [16], 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 [6]. Windows OS, on the other hand, is the most popular among users globally, accounting for almost 90% of OS used on PCs [17]. Windows 7 support ended in January 2020 with that of Windows 8.1 expected to end in 2023 [18]. Therefore, in the present decade, most Windows systems are expected to run Windows 10 [19]. Consequently, cases of abuse of Dropbox in Windows 10 environment are likely to arise, necessitating the need to identify and categorise unique aspects of where and how digital evidence can be found [20] to support forensic investigation of such cases.

Dropbox forensics has been conducted on several Windows platforms including Windows XP [21], Windows 7 [4, 22–24], Windows 8 [7], Windows 8.1 [25] and Windows 10 [26]. These studies have shown evidence of Dropbox data remnants in the respective Windows OS. New versions of Dropbox continue to be released, introducing new artefacts that are yet to be examined. The contribution of this paper is the identification of Dropbox version 91.4.548 data remnants in the registry and file system of a Windows 10 version 1903 machine. The Dropbox version investigated is newer than those investigated by previous researchers. The rest of the paper is organised as follows. Previous research in the area is discussed in section 2. Section 3 details the methodology adopted in this research. Section 4 provides the results and discussion. The paper is concluded in section 5.

2. RELATED WORK

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

McCain [21] 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 [11].

Marturana et al., [22] 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 [24] 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 [23] 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 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 [4] 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 [7] investigated data remnants 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 included *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" contained the installation directory and had two folders with different key values, i.e. *ks* and *ks1*, which are Dropbox user keys used to derive Dropbox encryption keys [27]. The authors conclude that artefacts found on local machines still carry much valuable information.

Malik et al., [25] 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 "AppData\Roaming" was intact, but the encrypted files in it had been deleted. Several registry keys were also present.

Amirullah et al., [26] 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 using similar software as [25]. Further analysis of memory, deleted files, and uninstallation remnants was conducted. Even after uninstallation, data remnants including Dropbox folder and the files within are still available on the host machine. The authors point out that registry keys remain but do not specify the exact keys and their locations. Furthermore, in their methodology, the authors do not explain how they went about the process of identification, preservation, analysis, and presentation during their investigation, which is required in any digital forensic investigation [28].

From the literature reviewed, much work is yet to be done on Dropbox forensics on Windows 10. The Dropbox analysis by Amirullah et al., [26] on Windows 10 does not give complete artefacts created during installation. For example, they do not specify the location of the Dropbox folder. Their study also does not comprehensively address the traces left when Dropbox is uninstalled. They state that multiple registry keys are left behind but do not specify the exact keys and their significance. This study fills these gaps and provides additional artefacts not presented in the previous studies.

3. METHODOLOGY

While conducting digital forensics, generally accepted rules, standards, and procedures must be followed [7]. In conducting this forensic investigation, the four stages of identification, preservation, analysis, and presentation of digital evidence [28] were followed.

3.1 Preparation

A variety of software was used in the experiment as tabulated in Table 1. Dropbox requires an email address to sign up for the service, and this informed the first step. The email account *dfimlabs@gmail.com* was created and used to sign up for Dropbox 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 on the PC. 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.

Table 1. Software used in the experiment

Software	Version	Purpose
VMWare Workstation 15 Pro	15.5.2	Creating virtual machines (VMs)
Windows 10 Pro 64-bit	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 and analysing 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 Magnet Forensics Dropbox Decryptor	1.3	Decrypting Dropbox dbx files
EaseUS Data Recovery Wizard	13.2	Recovering deleted files
Autopsy	4.14.0	Forensic analysis of VM images

Snapshots for creating images for dead forensics were created 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 five snapshots taken, *VMware Workstation* created a Virtual Machine Disk (VMDK) file and Virtual Memory (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 follows. The analysis tools including *Regshot, Glasswire, Mirekusoft 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, Mirekusoft 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]*.

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 clicking ‘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.

As noted, VMs were used in this experiment. The VMs were preferred to physical hard drives as they are quick to set up and analyse different configurations without having to re-configure [7]. The VMs were configured to run on minimum memory and storage space of 2GB and 32GB, respectively, as required for *Windows 10 64-bit* [29]. 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 [23]. In addition, VM snapshots have been found to be efficient in cloud investigations [30].

3.2 Identification

The VMDK files were identified as files which would contain the artefacts needed to conduct the analysis. VMDK files were identified for the five snapshots created for dead forensics (Snapshots 1-5) representing the various VMs for dead forensic analysis, as shown in Table 2.

Table 2. Snapshots with their corresponding VMs

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

3.3 Preservation

Digital forensic investigation requires that analysis be done on a forensic copy [31, 32]. 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 of the VMs 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. Even more importantly, the format is accepted in the forensic community and is recognised as an industry standard for storing forensic images [33]. The integrity of the VMDK copies was verified by calculating the hash of the copies and comparing them with those of their origin. The copies of the VM were then used in the analysis phase. The VM images created and their checksums are as shown in Table 3.

Table 3. VM images and their 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

3.4 Analysis

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 [23, 26]. Before beginning analysis, the integrity of the images was verified using in-built integrity-check modules present in both tools. The hashes produced by both *Autopsy* and *Access Data FTK Imager* matched those that had been obtained during preservation. This confirmed that the images had not been altered. Keyword searches were conducted, and files analysed. Attempts were also made to recover files deleted by the user and those deleted during uninstallation.

3.5 Presentation

The results obtained from the analysis phase are presented in the next section. The results are those pertaining to changes made by Dropbox during installation, file upload, file deletion, and uninstallation. The significance of the findings to forensic investigators is also discussed.

4. RESULTS AND DISCUSSION

4.1 Base VM

Analysis of the *Base-VM* image confirmed there was no data present relating 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. *Cortana* can be used to search for files on Dropbox [34] and hence the presence of Dropbox reference in *Cortana*. Microsoft has integrated Dropbox into *Office* [35], 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. While references to Dropbox exists in the *Base-VM*, it does not necessarily point to the installation and use of Dropbox [36]. Therefore, the *Base-VM* shows that matches for Dropbox may occur even without user activity relating to Dropbox. Consequently, any supporting evidence found must be understood in context.

4.2 Dropbox installation

Artefacts created by Dropbox during installation were determined through live forensics during the installation of Dropbox 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. HTTPS is a secure protocol [37]; therefore, it can be assumed that during installation and subsequent communications, data is securely transferred between Dropbox servers and the client machine.

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. 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.

4.2.1 File system artefacts

4.2.1.1 Browser

Dropbox download activity can be traced within the browser. These include web search for Dropbox, Dropbox URLs accessed, and Dropbox cookies. In addition to these, the artefacts contain the timestamps and computer account used to access Dropbox, information which can be used to build a timeline of events and tie the suspect to the crime. A keyword search of *dfimlabs@gmail.com* returned a hit in "C:\Users\dfiml\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\Recovery\Active\{A5B61BB7-2182-4DE1-97A2-3B0AB5B394C6}.dat". The file contains information associated with account log on to *dropbox.com* using *Google OAuth*. The artefact path contained *Microsoft Edge*, suggesting the use of the browser to log on to Dropbox via *Google OAuth*.

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".

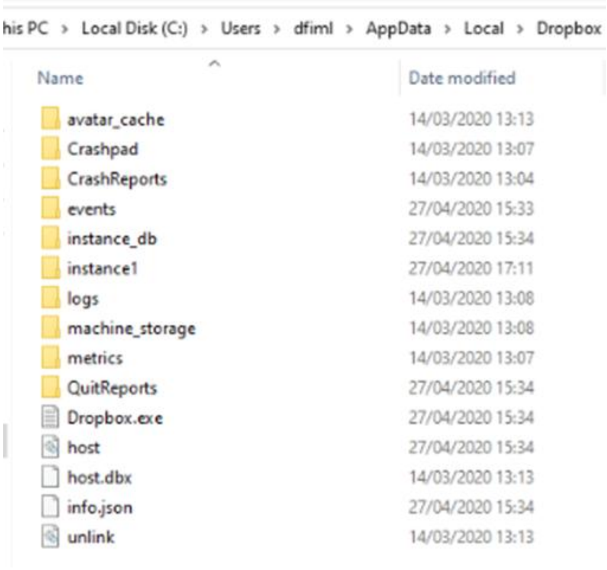
"C:\Users\<username>\AppData" folder stores data and settings for Windows applications. The folder has three sub-folders – *Local*, *LocalLow* and *Roaming*. *Local* folder stores data specific to a single computer and it is never synced from computer to computer even when in a domain. *LocalLow* folder 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 [38]. 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 Fig 1 were present. The folder contained several *.db* and *.dbx* database files which generally would be plaintext and encrypted SQLite files, respectively [21, 23]. However, this might not always be the case as sometimes, these files could be encrypted or Base64 encoded [27]. The *instance_db* folder had *instance.dbx* file while *instance1* folder had several configuration files, as shown in Fig 2. A description of these files is provided in Table 4. 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 [27], 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 [25–27]. 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.

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, avatarcache.db, home.db, icon.db* and *preview_cache.db* among others.

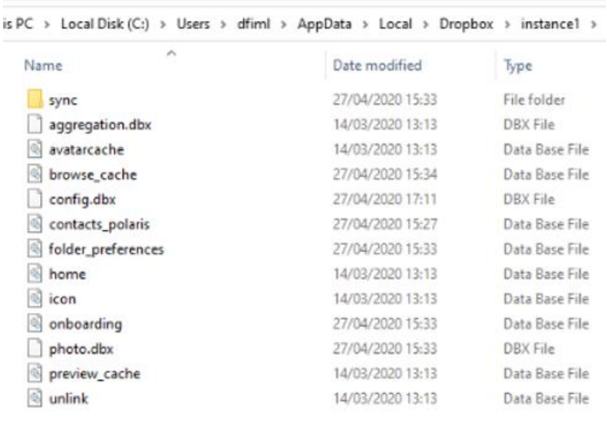
In "C:\Users\dfiml\AppData\Roaming\Dropbox" a file with an alphanumeric name was found. It had information related to Dropbox installer. In "C:\Users\dfiml\AppData\LocalLow\Microsoft\CryptnetUrlCache", data related to access to *dropbox.com* was found in the *MetaData* folder.



his PC › Local Disk (C:) › Users › dfiml › AppData › Local › Dropbox

Name	Date modified
avatar_cache	14/03/2020 13:13
Crashpad	14/03/2020 13:07
CrashReports	14/03/2020 13:04
events	27/04/2020 15:33
instance_db	27/04/2020 15:34
instance1	27/04/2020 17:11
logs	14/03/2020 13:08
machine_storage	14/03/2020 13:08
metrics	14/03/2020 13:07
QuitReports	27/04/2020 15:34
Dropbox.exe	27/04/2020 15:34
host	27/04/2020 15:34
host.dbx	14/03/2020 13:13
info.json	27/04/2020 15:34
unlink	14/03/2020 13:13

Fig 1: Files and folders in AppData\Local\Dropbox



is PC › Local Disk (C:) › Users › dfiml › AppData › Local › Dropbox › instance1 ›

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

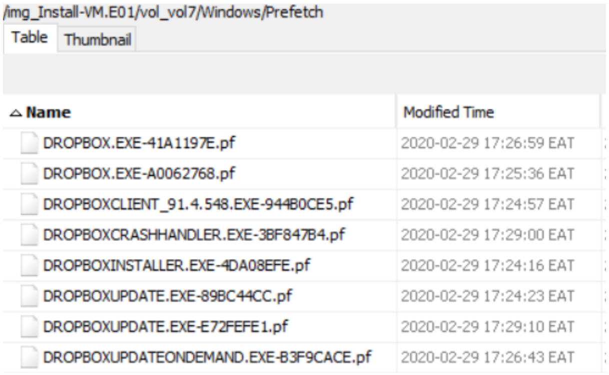
Fig 2: Files in AppData\Local\Dropbox\instance1

Table 4. Dropbox database files

File	Description
C:\Users\dfiml\AppData\Local\Dropbox \host.db and host.dbx	Includes the path for Dropbox file storage in Base64 string encoded text [23]
C:\Users\dfiml\AppData\Local\Dropbox \unlink.db	A binary file. Content not parsed.
C:\Users\dfiml\AppData\Local\instance_db\instance.dbx	Encrypted file. Content not parsed.
C:\Users\dfiml\AppData\Local\Dropbox\ instance1\aggregation.dbx	Contains timestamp values, server paths, and a blocklist value and a snapshot table [39].
C:\Users\dfiml\AppData\Local\Dropbox\ instance1\avatarcache.db	Contains account avatar information
C:\Users\dfiml\AppData\Local\Dropbox\ instance1\browse_cache.db	A binary file. Content not parsed.
C:\Users\dfiml\AppData\Local\Dropbox\ instance1\config.dbx	Contains user email address, display name, host ID, Dropbox folder path, list of recently changed files, among other settings [25, 26].
C:\Users\dfiml\AppData\Local\Dropbox \instance1\contact_polaris.db	A binary file. Content not parsed.
C:\Users\dfiml\AppData\Local\Dropbox \instance1\folder_preferences.db	A binary file. Content not parsed.
C:\Users\dfiml\AppData\Local\Dropbox \instance1\home.db	Contains information related to activity feed and calendar items among other settings.
C:\Users\dfiml\AppData\Local\Dropbox \instance1\icon.db	Contains information on the icons used.
C:\Users\dfiml\AppData\Local\Dropbox \instance1\onboarding.db	A binary file. Content not parsed.
C:\Users\dfiml\AppData\Local\Dropbox \instance1\photo.dbx	Encrypted file. Content not parsed.
C:\Users\dfiml\AppData\Local\Dropbox \instance1\preview_cache.db	Contains a url_asset_table.
C:\Users\dfiml\AppData\Local\Dropbox \instance1\unlink.db	A binary file. Content not parsed.
C:\Users\dfiml\AppData\Local\Dropbox \info.json	Contains info on Dropbox account type, subscription type, sync folder path, host ID

4.2.1.3 *Prefetch files*

Prefetch files are used by Windows to store information related to software activity, including the number of times the software has run and associated files used by the software [36]. Dropbox prefetch files were found in “C:\Windows\Prefetch” as shown in Fig 3.



Name	Modified Time
DROPBOX.EXE-41A1197E.pf	2020-02-29 17:26:59 EAT
DROPBOX.EXE-A0062768.pf	2020-02-29 17:25:36 EAT
DROPBOXCLIENT_91.4.548.EXE-944B0CE5.pf	2020-02-29 17:24:57 EAT
DROPBOXCRASHHANDLER.EXE-3BF847B4.pf	2020-02-29 17:29:00 EAT
DROPBOXINSTALLER.EXE-4DA08EFE.pf	2020-02-29 17:24:16 EAT
DROPBOXUPDATE.EXE-89BC44CC.pf	2020-02-29 17:24:23 EAT
DROPBOXUPDATE.EXE-E72FEFE1.pf	2020-02-29 17:29:10 EAT
DROPBOXUPDATEONDEMAND.EXE-B3F9CACE.pf	2020-02-29 17:26:43 EAT

Fig 3: Dropbox prefetch files

4.2.1.4 *Link files*

Link files related to Dropbox were found on the *Desktop* and *Start Menu*. Both files pointed to *Dropbox.exe* in the *Program Files* folder used to launch the application.

4.2.1.5 *Synchronisation folder*

Dropbox created a synchronisation folder under “C:\Users\dfiml” with the path “C:\Users\dfiml\Dropbox”. Three files were present by default: *.dropbox*, *Get Started with Dropbox.pdf* and *Get Started with Dropbox Paper.url*. Mehreen and Aslam [7] 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. Therefore, further investigation was conducted on the file.

The .dropbox file contains 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 [40]. *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* that directed to a page with information on getting started with Dropbox.

4.2.2 *Registry artefacts*

Registry contained artefacts relating to Dropbox version, installation directory, installation time, synchronisation folder, and user 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

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

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

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*

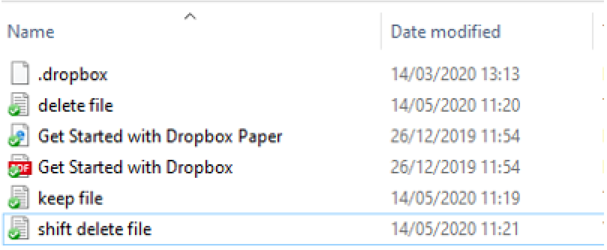
Two registry keys containing Dropbox user keys, *ks* and *ks1*, were found, as shown in Table 8. From previous work [27], these keys are protected using the *Windows* in-built *Data Protection API (DPAPI)*. The keys are stored as *DPAPI blobs*, so the *Windows* user's login password or its SHA1 hash is required to allow their decryption. The *ks* key can be used to derive the decryption key for *.dbx* files in "AppData\Local\Dropbox\instance_db". The *ks1* key can be used to derive the decryption key for *.dbx* files in "AppData\Local\Dropbox\instance1" and those found in the root folder "AppData\Local\Dropbox".

Table 8. Registry encryption artefacts

Artefact	Description
HKU\S-1-5-21-3933750032-3930657141-318433956-1001\Software\Dropbox\ks	User key for decrypting files in instance_db folder decryption key
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 forensics 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 Fig 7.



Name	Date modified
.dropbox	14/03/2020 13:13
delete file	14/05/2020 11:20
Get Started with Dropbox Paper	26/12/2019 11:54
Get Started with Dropbox	26/12/2019 11:54
keep file	14/05/2020 11:19
shift delete file	14/05/2020 11:21

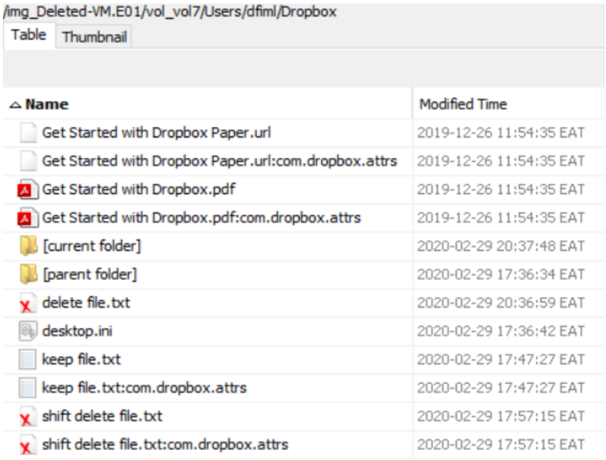
Fig 4: Files uploaded in the synchronisation folder

Analysis of the *Upload-VM* image using *Autopsy* revealed the existence of the same files and the timestamps they were created, accessed, and modified. 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. Also, the timestamps would help determine when such files were created, modified, or accessed, and build the timeline of events of the case.

4.4 File Deletion

To analyse data remnants when a user deletes a file, a 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' key. 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* was not. Using *EaseUS Data Recovery Wizard*, a live scan for deleted files was conducted in the Dropbox synchronisation folder, and both files were found. Using *Autopsy*, an analysis was done on the *Deleted-VM* image to locate and recover the files, as shown in Fig 8. The files were located and recovered successfully. This demonstrates that it may be possible to recover Dropbox user files that have been deleted from the client machine.



/img_Deleted-VM.E01/vol_vol7/Users/dfiml/Dropbox

Name	Modified Time
Get Started with Dropbox Paper.url	2019-12-26 11:54:35 EAT
Get Started with Dropbox Paper.url:com.dropbox.attrs	2019-12-26 11:54:35 EAT
Get Started with Dropbox.pdf	2019-12-26 11:54:35 EAT
Get Started with Dropbox.pdf:com.dropbox.attrs	2019-12-26 11:54:35 EAT
[current folder]	2020-02-29 20:37:48 EAT
[parent folder]	2020-02-29 17:36:34 EAT
✗ delete file.txt	2020-02-29 20:36:59 EAT
desktop.ini	2020-02-29 17:36:42 EAT
keep file.txt	2020-02-29 17:47:27 EAT
keep file.txt:com.dropbox.attrs	2020-02-29 17:47:27 EAT
✗ shift delete file.txt	2020-02-29 17:57:15 EAT
✗ shift delete file.txt:com.dropbox.attrs	2020-02-29 17:57:15 EAT

Fig 5: Deleted files found in the synchronisation folder

4.5 Dropbox Uninstallation

The last step of this research was undertaken to assess the results of a user uninstalling Dropbox client using the *Programs and Features* functionality 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.

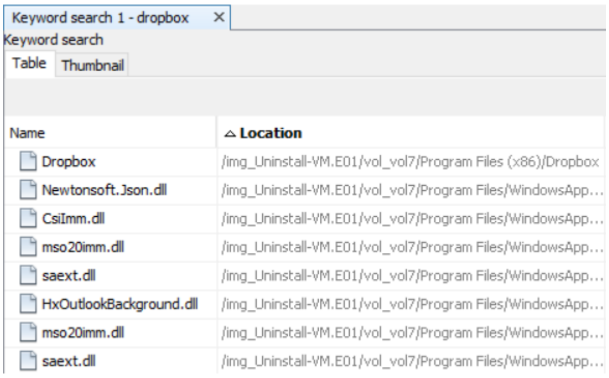
4.5.1 File system artefacts

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. In addition to these, the artefacts contained 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. A keyword search for *dfimlabs@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”. The file had information associated with the account log on to *dropbox.com* using *Google OAuth*. The artefact path contained *Microsoft Edge*, suggesting the use of the browser to log on to *Dropbox* via *Google OAuth*.

4.5.1.2 Installation directories

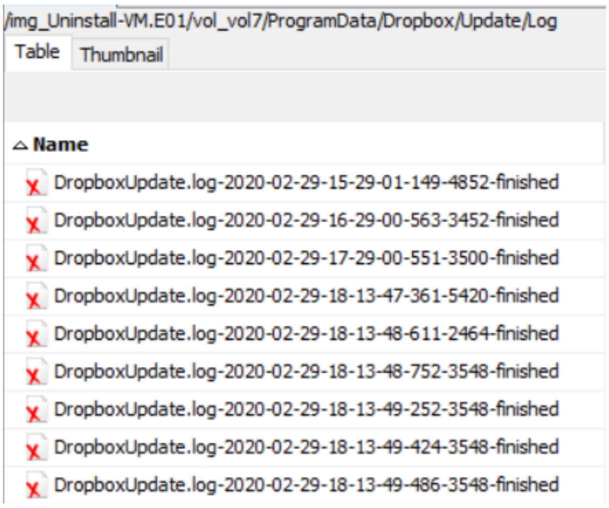
Dropbox installer was still present in the *Downloads* folder in the path “C:\Users\dfiml\Downloads\DropboxInstaller.exe”. *Dropbox* folder and *.dll* files referencing Dropbox were found in *Program Files* directory using keyword search as shown in Fig 9. The *Dropbox* file contains the path “C:\Program Files (x86)\Dropbox” which references the program installation path of the 32-bit version of the application. *Newtonsoft.Json.dll* is used for encoding JSON arguments for Dropbox API in .NET environment [41]. The remaining files contain references to Dropbox notifications.



Name	Location
Dropbox	/img_Uninstall-VM.E01/vol_vol7/Program Files (x86)/Dropbox
Newtonsoft.Json.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApp...
CsiImm.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApp...
mso20imm.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApp...
saext.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApp...
HxOutlookBackground.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApp...
mso20imm.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApp...
saext.dll	/img_Uninstall-VM.E01/vol_vol7/Program Files/WindowsApp...

Fig 6: Dropbox related files in Program Files

The *ProgramData* directory contained log files related to Dropbox update which though marked as deleted could be recovered using *Autopsy* as shown in Fig 10.

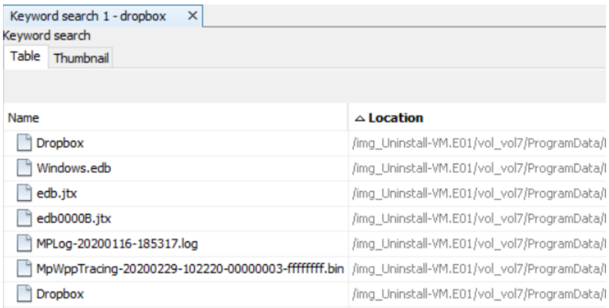


/img_Uninstall-VM.E01/vol_vol7/ProgramData/Dropbox/Update/Log

Name
✗ DropboxUpdate.log-2020-02-29-15-29-01-149-4852-finished
✗ DropboxUpdate.log-2020-02-29-16-29-00-563-3452-finished
✗ DropboxUpdate.log-2020-02-29-17-29-00-551-3500-finished
✗ DropboxUpdate.log-2020-02-29-18-13-47-361-5420-finished
✗ DropboxUpdate.log-2020-02-29-18-13-48-611-2464-finished
✗ DropboxUpdate.log-2020-02-29-18-13-48-752-3548-finished
✗ DropboxUpdate.log-2020-02-29-18-13-49-252-3548-finished
✗ DropboxUpdate.log-2020-02-29-18-13-49-424-3548-finished
✗ DropboxUpdate.log-2020-02-29-18-13-49-486-3548-finished

Fig 7: Dropbox log files in ProgramData

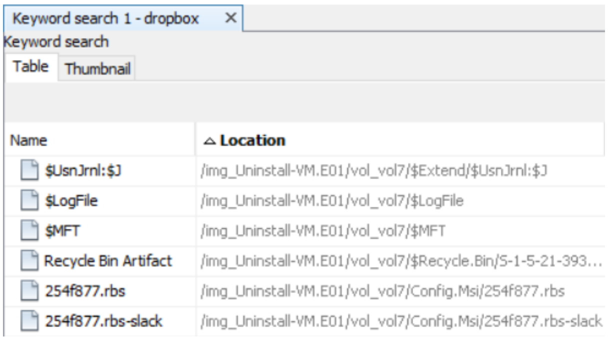
Keyword search for ‘Dropbox’ also returned references to a *Dropbox* folder and other files inside *ProgramData* directory as shown in Fig 11. The files found in *ProgramData* contained information related to Dropbox including search query, browser and search engine used, client version, installation directory, and application data stored in *AppData*.



Name	Location
Dropbox	/img_Uninstall-VM.E01/vol_vol7/ProgramData/I
Windows.edb	/img_Uninstall-VM.E01/vol_vol7/ProgramData/I
edb.jtx	/img_Uninstall-VM.E01/vol_vol7/ProgramData/I
edb0000B.jtx	/img_Uninstall-VM.E01/vol_vol7/ProgramData/I
MPLog-20200116-185317.log	/img_Uninstall-VM.E01/vol_vol7/ProgramData/I
MpWppTracing-20200229-102220-00000003-ffffffff.bin	/img_Uninstall-VM.E01/vol_vol7/ProgramData/I
Dropbox	/img_Uninstall-VM.E01/vol_vol7/ProgramData/I

Fig 8: Dropbox related files in ProgramData

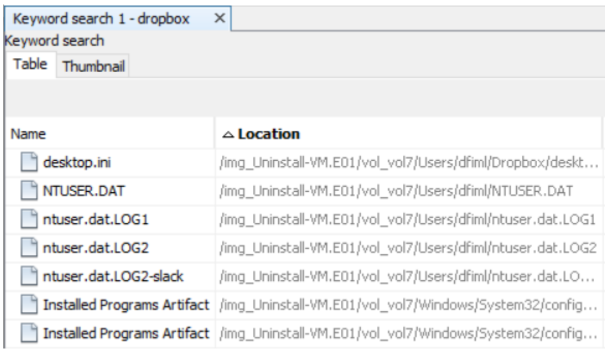
Other artefacts returned by the keyword search included *swapfile.sys*, *$Extend/$UsnJrnl:$J*, *$LogFile*, *$MFT*, *$Recycle.Bin/S-1-5-21-3933750032-3930657141-318433956-1001/$RPMOD0U.txt*, *Config.Msi/254f877.rbs*, and *Config.Msi/254f877.rbs-slack* as shown in Fig 12. These artefacts contained information related to Dropbox logs, update, synchronisation folder path, deleted user files in the recycle bin, and link files.



Name	△ Location
$UsnJrnl:$J	/img_Uninstall-VM.E01/vol_vol7/$Extend/$UsnJrnl:$J
$LogFile	/img_Uninstall-VM.E01/vol_vol7/$LogFile
$MFT	/img_Uninstall-VM.E01/vol_vol7/$MFT
Recycle Bin Artifact	/img_Uninstall-VM.E01/vol_vol7/$Recycle.Bin/S-1-5-21-393…
254f877.rbs	/img_Uninstall-VM.E01/vol_vol7/Config.Msi/254f877.rbs
254f877.rbs-slack	/img_Uninstall-VM.E01/vol_vol7/Config.Msi/254f877.rbs-slack

Fig 9: Files in the root folder referencing Dropbox

Other results from the keyword search reference Dropbox in the *Desktop*, *NTUSER.DAT*, and "HKLM\Software" as shown in Fig 13. These artefacts contained information related to Dropbox installation in *Program Files*, Dropbox update helper, and computer user account tied to the Dropbox installation.

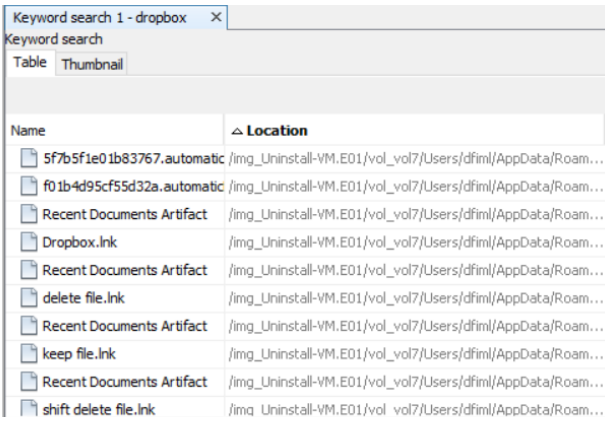


Name	△ Location
desktop.ini	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/Dropbox/deskt…
NTUSER.DAT	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/NTUSER.DAT
ntuser.dat.LOG1	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/ntuser.dat.LOG1
ntuser.dat.LOG2	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/ntuser.dat.LOG2
ntuser.dat.LOG2-slack	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/ntuser.dat.LO…
Installed Programs Artifact	/img_Uninstall-VM.E01/vol_vol7/Windows/System32/config…
Installed Programs Artifact	/img_Uninstall-VM.E01/vol_vol7/Windows/System32/config…

Fig 10: Files in System32 and NTUSER.DAT referencing Dropbox

Dropbox database files contained in "C:\Users\dfiml\AppData\Local\Dropbox" were not found. Dropbox folder could be traced in "AppData\Roaming" directory. The directory only had one file in the installer subdirectory. 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.

The "Local\Temp" folder contained four files 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. 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, and two deleted, as shown in Fig 14.

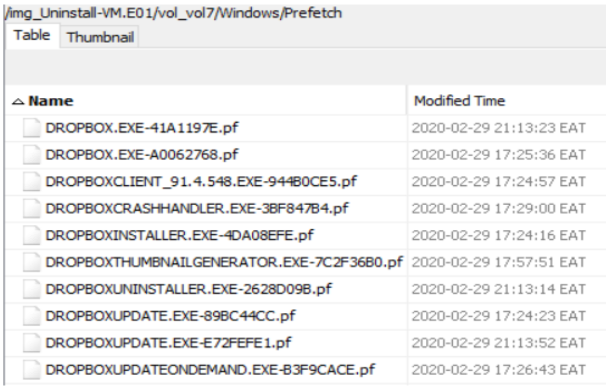


Name	△ Location
5f7b5f1e01b83767.automatic	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
f01b4d95cf55d32a.automatic	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
Dropbox.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
keep file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…
shift delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam…

Fig 11: Files in Roaming\Microsoft referencing Dropbox

4.5.1.3 *Prefetch files*

Prefetch files related to Dropbox client, update, installer, uninstaller, thumbnail generator, and crash handler were found as shown in Fig 15.

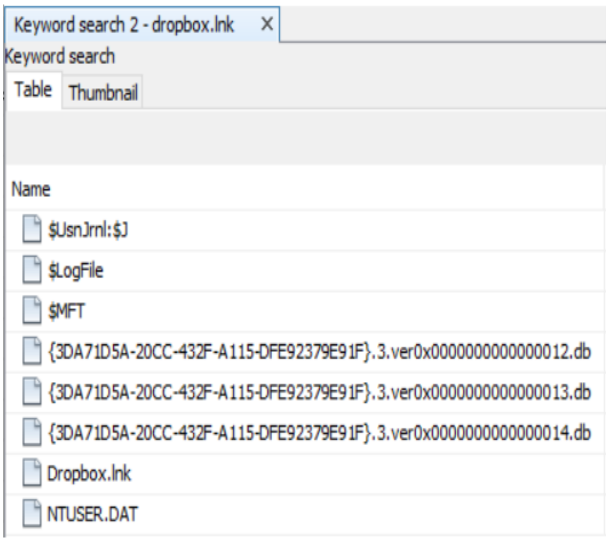

/img_Uninstall-VM.E01/vol_vol7/Windows/Prefetch

△ Name	Modified Time
DROPBOX.EXE-41A1197E.pf	2020-02-29 21:13:23 EAT
DROPBOX.EXE-A0062768.pf	2020-02-29 17:25:36 EAT
DROPBOXCLIENT_91.4.548.EXE-944B0CE5.pf	2020-02-29 17:24:57 EAT
DROPBOXCRASHHANDLER.EXE-3BF847B4.pf	2020-02-29 17:29:00 EAT
DROPBOXINSTALLER.EXE-4DA08EFE.pf	2020-02-29 17:24:16 EAT
DROPBOXTHUMBNAILGENERATOR.EXE-7C2F36B0.pf	2020-02-29 17:57:51 EAT
DROPBOXUNINSTALLER.EXE-2628D09B.pf	2020-02-29 21:13:14 EAT
DROPBOXUPDATE.EXE-89BC44CC.pf	2020-02-29 17:24:23 EAT
DROPBOXUPDATE.EXE-E72FEFE1.pf	2020-02-29 21:13:52 EAT
DROPBOXUPDATEONDEMAND.EXE-B3F9CACE.pf	2020-02-29 17:26:43 EAT

Fig 12: Dropbox prefetch files

4.5.1.4 *Link files*

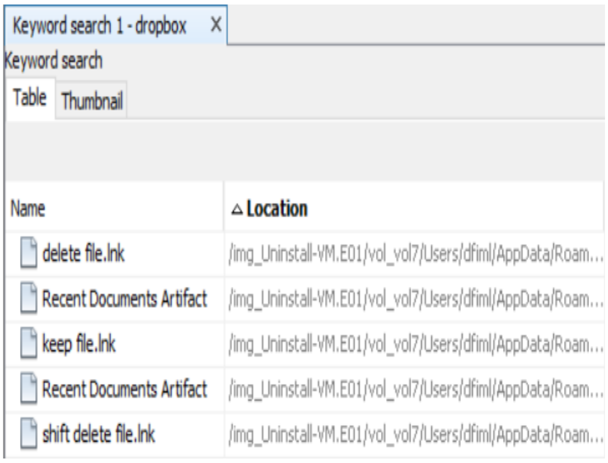
A keyword search for 'dropbox.lnk' returned hits in files including *$MFT* and *NTUSER.DAT* as shown in Fig 16. Further analysis of the files established that they contained information on the path to Dropbox synchronisation folder, the path to *Dropbox.exe* in *Program Files*, and settings used by Dropbox when playing content.



Name
$UsnJrnl:$J
$LogFile
$MFT
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000012.db
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000013.db
{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000014.db
Dropbox.lnk
NTUSER.DAT

Fig 13: Dropbox link files

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 Fig 17. The link files contained the full path to the corresponding text files.

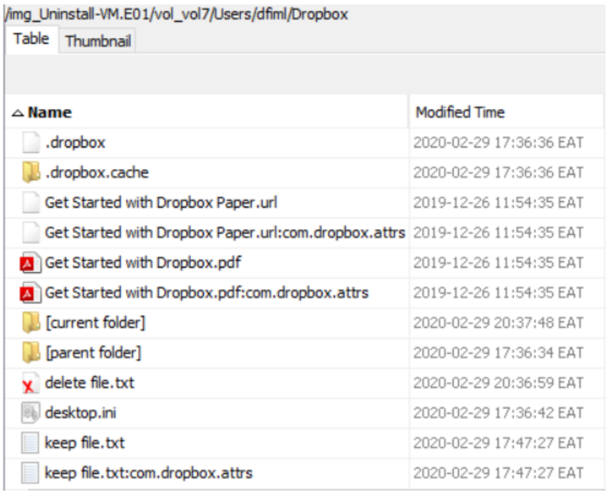


Name	Location
delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam...
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam...
keep file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam...
Recent Documents Artifact	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam...
shift delete file.lnk	/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/AppData/Roam...

Fig 14: Link files to uploaded files in Dropbox sync folder

4.5.1.5 *Synchronisation folder*

Dropbox synchronisation folder contained both files that were not deleted, and those that were deleted by pressing 'delete' button as shown in Fig 18. 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.



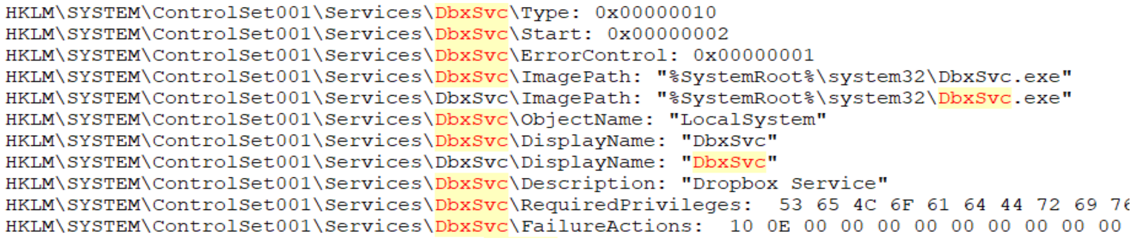
/img_Uninstall-VM.E01/vol_vol7/Users/dfiml/Dropbox

Name	Modified Time
.dropbox	2020-02-29 17:36:36 EAT
.dropbox.cache	2020-02-29 17:36:36 EAT
Get Started with Dropbox Paper.url	2019-12-26 11:54:35 EAT
Get Started with Dropbox Paper.url:com.dropbox.attrs	2019-12-26 11:54:35 EAT
Get Started with Dropbox.pdf	2019-12-26 11:54:35 EAT
Get Started with Dropbox.pdf:com.dropbox.attrs	2019-12-26 11:54:35 EAT
[current folder]	2020-02-29 20:37:48 EAT
[parent folder]	2020-02-29 17:36:34 EAT
delete file.txt	2020-02-29 20:36:59 EAT
desktop.ini	2020-02-29 17:36:42 EAT
keep file.txt	2020-02-29 17:47:27 EAT
keep file.txt:com.dropbox.attrs	2020-02-29 17:47:27 EAT

Fig 15: Files in Dropbox sync folder

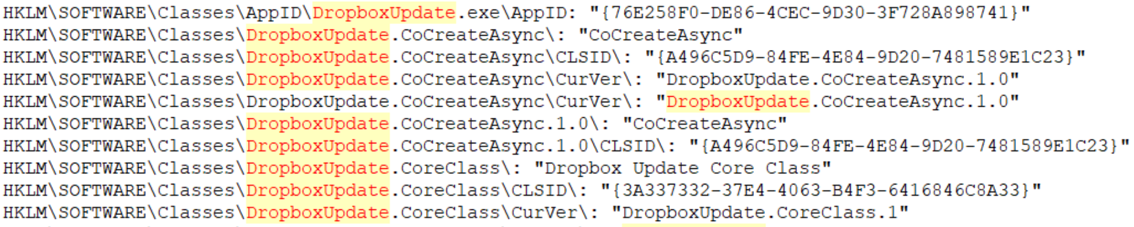
4.5.2 *Registry artefacts*

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 Fig 19-22. The keys referenced in the registry artefacts such as *DbxSvc.exe*, *DropboxUpdate*, *goopdate.dll*, and *DropboxExt*, had files in the file system related to them. For example, *DropboxUpdate* could be traced in "AppData\Local\Temp" folder as *DropboxUpdate.exe254fab8.* Dropbox user keys identified during installation were also present in the registry even after uninstallation.



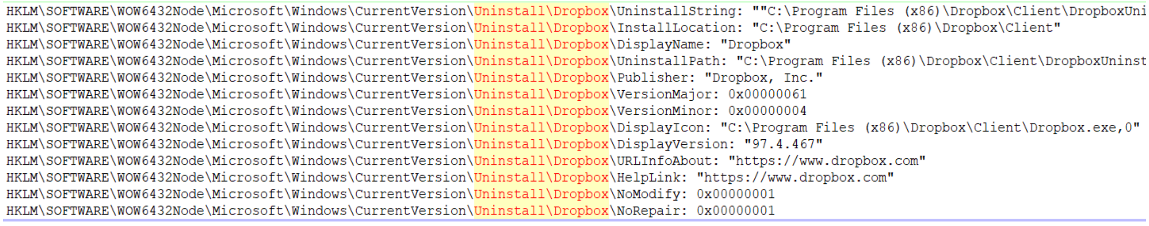
```
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\ImagePath: "%SystemRoot%\system32\DbxSvc.exe"
HKLM\SYSTEM\ControlSet001\Services\DbxSvc\ImagePath: "%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 00
```

Fig 16: Dropbox service artefacts in registry



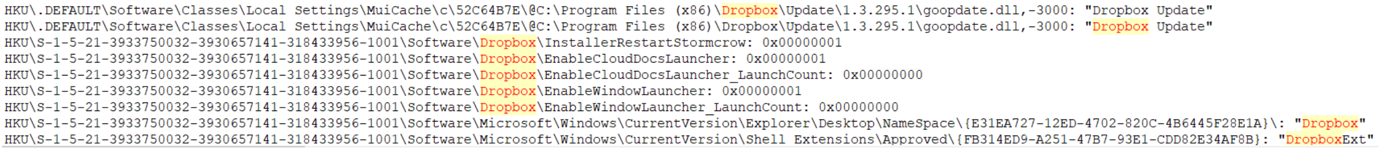
```
HKLM\SOFTWARE\Classes\AppID\DropboxUpdate.exe\AppID: "{76E258F0-DE86-4CEC-9D30-3F728A898741}"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync\: "CoCreateAsync"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync\CLSID\: "{A496C5D9-84FE-4E84-9D20-7481589E1C23}"
HKLM\SOFTWARE\Classes\DropboxUpdate.CoCreateAsync\CurVer\: "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"
```

Fig 17: Dropbox update artefacts in registry



```
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox\UninstallString: ""C:\Program Files (x86)\Dropbox\Client\DropboxUni
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
```

Fig 18: Dropbox uninstall artefacts in registry



```
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-CDD82E34AF8B}: "DropboxExt"
```

Fig 19: Dropbox update, installer, explorer, and shell artefacts in registry

5. CONCLUSION

This research has established the location of artefacts in the registry and file system that can be used to determine Dropbox user details and activities on Windows 10. Evidence of usage of Dropbox client can be found in the browser, link files, prefetch files, directory listing, registry, and network traffic. Dropbox user email address and Windows account used to access the application can be determined as well. Furthermore, files that have been uploaded by the user can be recovered, including those that may have been deleted. The work has also shown some of the new database files used by Dropbox, and the older ones that are no longer used.

This research was limited by the inability to decrypt the encrypted database files, possibly because of changes in the Dropbox encryption mechanism. Future research should explore the decryption of these files as they bear valuable information. While this work focused on artefacts in the registry and file system, invaluable evidence can be found in the memory and network traffic. Therefore, future studies should investigate potential artefacts from these sources.

6. REFERENCES

[1] Mell P, Grance T. 2011. The NIST Definition of Cloud Computing. NIST Spec Publ 800-145 :2.

[2] Simou S, Kalloniatis C, Kavakli E, Gritzalis S. 2014. Cloud Forensics: Identifying the Major Issues and Challenges. In: Jarke M, Mylopoulos J, Quix C, Rolland C, Manolopoulos Y, Mouratidis H, Horkoff J (eds) Int. Conf. Adv. Inf. Syst. Eng. Springer International Publishing, Cham, pp 271–284.

[3] Pichan A, Lazarescu M, Soh ST. 2015. Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis. Digit Investig 13:38–57.

[4] Ghafarian A. 2015. Forensiscs Analysis of Cloud Computing Services. In: 2015 Sci. Inf. Conf. pp 1335–1339.

[5] Hu W, Yang T, Matthews JN. 2010. The Good, the Bad and the Ugly of Consumer Cloud Storage. SIGOPS Oper Syst Rev 44(3):110–115.

[6] Caviglione L, Podolski M, Mazurczyk W, Ianigro M. 2017. Covert Channels in Personal Cloud Storage Services: The Case of Dropbox. IEEE Trans Ind Informatics 13(4):1921–1931.

[7] Mehreen S, Aslam B. 2015. Windows 8 Cloud Storage Analysis: Dropbox Forensics. In: 2015 12th Int. Bhurban Conf. Appl. Sci. Technol. pp 312–317.

[8] [Dropbox. 2018. What is Dropbox? Available from: https://www.dropbox.com/features, [21/11/2018].

[9] Dropbox. 2018. How much does Dropbox cost? Available from: https://www.dropbox.com/help/billing/cost, [21/11/2018].

[10] Damshenas M, Dehghantanha A, Mahmoud R, Shamsuddin S bin. 2012. Forensics investigation challenges in cloud computing environments. In: Proc. Title 2012 Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic. pp 190–194.

[11] Chung H, Park J, Lee S, Kang C. 2012. Digital Forensic Investigation of Cloud Storage Services. Digit Investig 9(2):81–95.

[12] Ahmed AA, Li CX. 2016. Locating and Collecting Cybercrime Evidences on Cloud Storage: Review. In: 2016 Int. Conf. Inf. Sci. Secur. pp 1–5.

[13] Biggs S, Vidalis S. 2009. Cloud Computing: The Impact on Digital Dorensic Investigations. In: 2009 Int. Conf. Internet Technol. Secur. Trans. pp 1–6.

[14] Taylor M, Haggerty J, Gresty D, Lamb D. 2011. Forensic Investigation of Cloud Computing Systems. Netw Secur 2011(3):4–10.

[15] Guo H, Jin B, Shang T. 2012. Forensic Investigations in Cloud Environments. In: 2012 Int. Conf. Comput. Sci. Inf. Process. pp 248–251.

[16] Cisco. 2018. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021. .

[17] NetApplications. 2018. Operating System Market Share. Available from: 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%252Flaptop%2522%255D%257D%257D%255D%257D%252C%2522dateLabel%2522%253A%2522Trend%2522%252C%2522attributes%2522%253A%2522share%2522%252, [21/11/2018].

[18] Microsoft. 2018. Windows Lifecycle Fact Sheet. Available from: https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet, [21/11/2018].

[19] Keizer G. 2018. Windows by the numbers: Windows 10 nears 'crossover' point with veteran Windows 7. Available from: 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, [21/11/2018].

[20] Zatyko K, Bay J. 2011. The Digital Forensics Cyber Exchange Principle. 2017:.

[21] McClain F. 2011. Dropbox Forensics. Forensic Focus. Available from: https://www.forensicfocus.com/articles/dropbox-forensics/, [20/04/2020].

[22] Marturana F, Me G, Tacconi S. 2012. A Case Study on Digital Forensics in the Cloud. In: 2012 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. pp 111–116.

[23] Quick D, Choo K-KR. 2013. Dropbox Analysis: Data

Remnants on User Machines. Digit Investig 10(1):3–18.

[24] Epifani M. 2013. Cloud Storage Forensics. .

[25] Malik R, Shashidhar N, Chen L. 2015. Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform. Proc. Int. Conf. Secur. Manag. .

[26] Amirullah A, Riadi I, Luthfi A. 2016. Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System. Int. J. Comput. Appl. 143:.

[27] Picasso F. 2017. Brush up on Dropbox DBX Decryption. ZENA FORENSICS 2017:.

[28] McKemmish R. 1999. What is Forensic Computing? . Trends Issues Crime Crim Justice 118:1–6.

[29] Microsoft. 2019. How to Find Windows 10 Computer Specifications & Systems Requirements. Available from: https://www.microsoft.com/en-us/windows/windows-10-specifications, [15/01/2020].

[30] Rani DR, Geethakumari G. 2015. An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots. In: 2015 Int. Conf. Pervasive Comput. pp 1–5.

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

[32] ACPO. 2012. ACPO Good Practice Guide for Digital Evidence. .

[33] Lyons B. 2016. Disk Image Content Model and Metadata Analysis. .

[34] Warren T. 2015. Cortana for Windows 10 will search Dropbox and Google Drive on Lenovo PCs. Available from:https://www.theverge.com/2015/5/28/8676557/lenovo-cortana-reachit-windows-10, [13/05/2020].

[35] Warren T. 2014. Dropbox and Microsoft form surprise partnership for Office integration. Available from: https://www.theverge.com/2014/11/4/7153975/dropbox-microsoft-partnership-microsoft-office, [13/05/2020].

[36] Quick D, Martini B, Choo K-KR, Quick D, Martini B, Choo K-KR. 2014. Dropbox Analysis: Data Remnants on User Machines. Cloud Storage Forensics :63–93.

[37] Rescorla E. 2000. HTTP Over TLS. Available from: https://tools.ietf.org/html/rfc2818, [13/05/2020].

[38] Hoffman C. 2017. What Is the AppData Folder in Windows? Available from: https://www.howtogeek.com/318177/what-is-the-appdata-folder-in-windows/, [13/05/2020].

[39] Malik R, Shashidhar N, Chen L. 2015. Cloud Storage Client Application Analysis. Int. J. Secur. 9:.

[40] StackExchange. 2012. .dropbox files, can they be deleted? Available from: https://superuser.com/questions/472616/dropbox-files-can-they-be-deleted, [13/05/2020].

[41] Dropbox. Encoding for JSON Arguments. Available from: https://www.dropbox.com/developers/reference/json-encoding, [10/07/2020].