Dropbox Forensics: Forensic Analysis of a Cloud Storage Service

Shu Yun Lim[1], Alfonso Johan[2], Paridah Daud[3], Noor Azma Ismail[4]

[1,3,4]Faculty of Business and Technology, UNITAR International University, Selangor, Malaysia
[2]ICT Services, UNITAR International University, Selangor, Malaysia

ABSTRACT

With the rising popularity of cloud storage and its ever-increasing versatility, many enterprises and individuals have jumped on the cloud bandwagon. This increased adoption of cloud storage had amplified the demand for cloud forensics, the cross-discipline between cloud computing and digital forensics. Cloud storage forensics is deemed the emerging challenge to digital forensic investigator since it allows an application on the local system to connect to the cloud storage and automate synching of files. When misused as a tool of crimes, investigators can expect to find evidence and traces of criminal activity in both local system and cloud providers. Forensic implications of Dropbox, an online cloud storage service with millions of users are the focus of this study. Dropbox client application on Windows 10 platform was examined and relevant valuable artifacts were presented.

Keywords : *cloud storage, cloud forensics, digital forensics, Dropbox.*

I. INTRODUCTION

Digital forensics on cloud application is challenging because of its dynamic and distributed nature. Standard guidelines for digital forensics may not be fully appropriate for evidence in cloud environments. Consequently, practitioners tend to perform the investigation based on their own judgement and nature of the case. Since cloud is where the evidence resides, cloud is now the digital evidence which need to be preserved and acquired. The real challenge starts on acquiring them as a forensic copy, detecting any other laptop which had previously accessed to the storage or uploaded items to the cloud.

Dropbox Forensic is the examination of Dropbox cloud storage data, related files and configuration to determine who what and why in any investigation that uses Dropbox cloud as a subject or a tool of crime. Dropbox cloud storage service, with more than 500 million users worldwide received a lot of attention in the field of digital forensics. [1] [2] and [3] examined popular cloud client apps and identified artefacts of forensic interest. These research work on Dropbox forensics were carried out and published before year 2016 on Windows 8 platform. There is a gap in technology few years later, therefore a more comprehensive forensics study on the latest Windows operating system is required.

Our study is focusing on the use of Dropbox on a Windows 10 system. Dropbox is a web-based file synchronization and sharing service. Its primary feature is the ability to sync files across systems and devices automatically. A Dropbox client is required on a system that wishes to participate in this synchronization. The client runs constantly looking for new changes locally in the designated Dropbox folder and synchronizing with cloud as required. Dropbox supports across a variety of desktop and mobile operating systems. Users can access their files and folder at any time from the desktop, mobile applications or through any application connected to Dropbox.

By determining the data remnants on client devices, we contribute to a better understanding of the types of terrestrial artifacts that are likely to remain for digital forensics practitioners and examiners. This study also discussed the challenges that forensic analyst faced during the acquisition and examination in cloud environment.

II. RELATED WORKS

A study of Dropbox Forensic by Frank McClain [4] examined registry, database files and network activities of the client application. The authors concluded that Dropbox directory in user profile and uninstall entry in registry both contain important information regarding Dropbox application in the local drive. Aside from that, the research also highlighted additional information that can be obtained from Dropbox database files and registry. To view system information of the Dropbox configurations and recent file activities, one may refer to *dropbox.cache* folder, or *filecache.dbx* database file. Additionally, Internet history should provide information verifying account synchronization. This information is essential to point Dropbox investigations towards the right direction.

On the other hand, Daryabar et. al. [1] examined popular cloud client apps and identified artefacts of forensic interest. The research presented a tool taxonomy which provides investigators with a searchable catalog of tools that can meet their technical requirements during cloud forensic investigations.

A research undertaken by Darren Q. et al. [2] to determine the data remnants on a Windows 7 computer and an Apple iPhone 3G after using Dropbox by a user. Information sources identified during the research include client software files, prefetch files, link files, network traffic capture, and memory captures.

Another comprehensive investigation conducted back in 2012 by H.J. Chung et. al. [3] on cloud storage services such as Amazon S3, Dropbox, Evernote and Google Docs. In this research work Dropbox version 1.1.35 for Window 8 was investigated. A newer research is needed to ascertain artifacts of Dropbox in Microsoft newer operating systems. Our research is here to patch the gap

III. CLOUD FORENSICS TOOLS

Dropbox Decryptor from Magnet Forensics [5] has the capability to decrypt Dropbox database files – *filecache.dbx* and *config.dbx*, which are both encrypted SQLite databases. From both of the files, one will have access to list of the files that have been synced to Dropbox, registered email address of the said Dropbox user, list of changed files, HostID, local path to the user Dropbox folder and many others.

Another tool named Internet Evidence Finder Triage [6] released by the same company, Magnet Forensic. This tool finds hundreds of digital forensic artifacts by parsing and carving data from allocated and unallocated space on computers, smartphones and tablets. In particular, this tool can help forensic examiner to find the remnants of Dropbox files and configurations and resulted them with details including file names, file sizes and more.

There is another free forensics tool called Dropbox Reader released by ATC-NY [7]. It is a set of Python scripts provide investigators with information about a Dropbox user's account and activities, such as the registration e-mail, Dropbox identifier and most recently changed files. The scripts output information from Dropbox *config.db* and *sigstore.db* and this allows investigator to acquire information about the registered Dropbox account, shared directories, and synchronized files. This tool can run on Windows, Macintosh, and Linux systems

IV. DROPBOX FORENSICS

A. Investigation Methodology

In this research work, system registry changes due to installation and uninstallation had been examined without relying on commercial cloud forensics tools stated in section III. Network activities such as connection from clients to the server for files access, update linked devices when files being added, changed or removed were also being investigated in this forensics analysis with network tools such as Wireshark, CurrPorts and LiveTcpUdpWatch. Lastly, artifacts block such as database and binaries files were parsed and examined with SQLite DB tools. SQLite file such as *config.db*, *sigstore.db* etc. contains some info about the local Dropbox installation and account. It shows account information, the email address associated with the account, and current version/build for the local application which could provide more insights to the investigators.

B. Installation and Uninstallation Changes to Registry

The installation of Dropbox in the windows will create new Dropbox folder in the directory "C:\Users\username\"., "C:\User\username\AppData\Local", and "C:\User\username\AppData\Roaming". These folders contain information regarding the data that comes along with Dropbox installations.

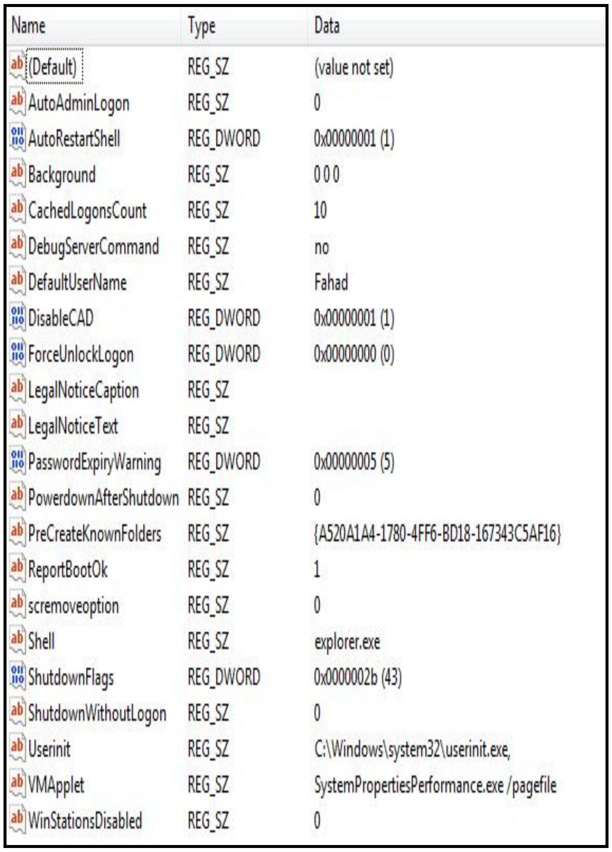
A lot of interesting changes occurred during the installation process. Several registry values were created during the installation process of the Dropbox. Registry changes took place in the following key hives:

HKLM\SOFTWARE\Policies\Microsoft\Cryptography
HKLM\System\CurrentControlSet\services\WinSock2\Parameters
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

HKLM\SOFTWARE\Policies\Microsoft\Cryptography is the cryptography registry that contains detailed description of the Microsoft Cryptography functions, interfaces, objects and other programming elements. It also deals with digital certificates, certificate services and certificate enrolment control. The changes within this key hive indicates that Dropbox is creating or setting a lot of parameters in the cryptography registry file.

It was also noted that Dropbox creates new entries in Winsock, which is a technical specification that defines how Windows network software should access network services, especially TCP/IP. Dropbox alters network connectivity structure as well as TCP/IP registries.

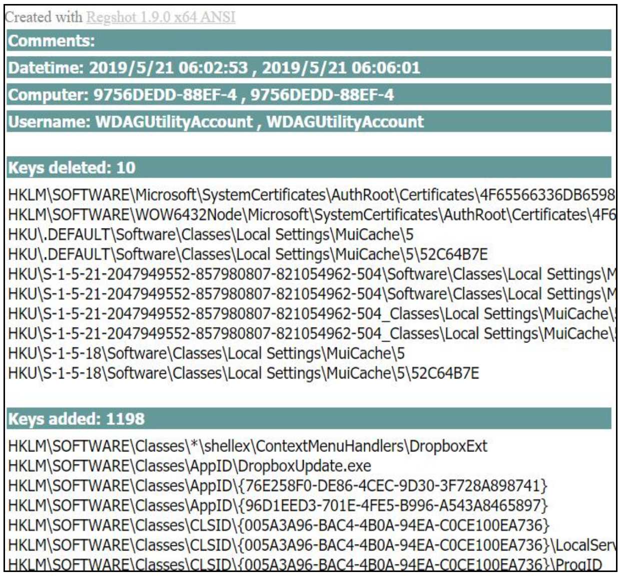
Winlogon registry is the component of Microsoft Windows operating systems that is responsible for handling secure attention sequence, loading of user profile during logon, and optionally locking the computer when a screensaver is running (requiring another authentication step). The actual procurement and verification of user credentials is left to other components. Winlogon is a common target for several threats that could modify its function and memory usage. During installation Dropbox made new entries in the WinLogon services which creates a serious threat. Fig. 1 shows some of the parameters of the WinLogon registry.



Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoAdminLogon	REG_SZ	0
AutoRestartShell	REG_DWORD	0x00000001 (1)
Background	REG_SZ	0 0 0
CachedLogonsCount	REG_SZ	10
DebugServerCommand	REG_SZ	no
DefaultUserName	REG_SZ	Fahad
DisableCAD	REG_DWORD	0x00000001 (1)
ForceUnlockLogon	REG_DWORD	0x00000000 (0)
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
PasswordExpiryWarning	REG_DWORD	0x00000005 (5)
PowerdownAfterShutdown	REG_SZ	0
PreCreateKnownFolders	REG_SZ	{A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
Shell	REG_SZ	explorer.exe
ShutdownFlags	REG_DWORD	0x0000002b (43)
ShutdownWithoutLogon	REG_SZ	0
Userinit	REG_SZ	C:\Windows\system32\userinit.exe,
VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled	REG_SZ	0

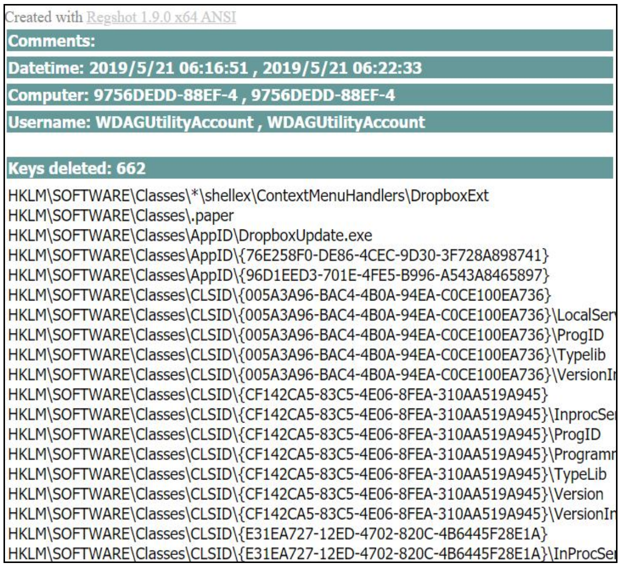
Figure 1 WinLogon registry

Very often trojans tend to manipulate *Userinit.exe* and the action of Dropbox editing registry in this particular section is pretty dangerous and suspicious. The changes in the registry before and after installation of Dropbox can be traced using RegShot [8]. Regshot is an open-source (LGPL) registry compare utility. A registry image before the installation and one after the installation were saved and compared. Based on our observation, approximately 1198 new values related to Dropbox were added to the Registry (Fig. 2). Also, a similar test was performed after the uninstallation of Dropbox. 662 keys were found to be deleted from the registry (Fig. 3).



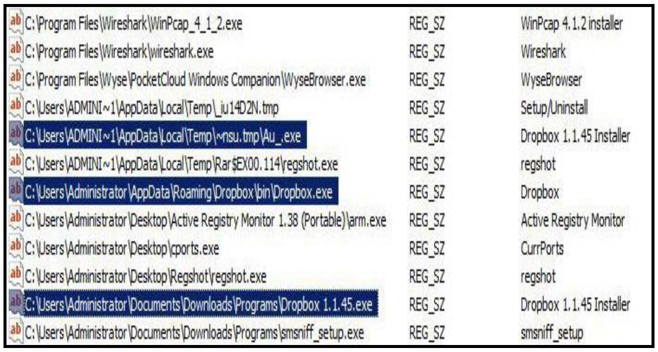
```
Created with Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2019/5/21 06:02:53 , 2019/5/21 06:06:01
Computer: 9756DEDD-88EF-4 , 9756DEDD-88EF-4
Username: WDAGUtilityAccount , WDAGUtilityAccount

Keys deleted: 10
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4F65566336DB6598
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\4F6
HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\5
HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\5\52C64B7E
HKU\S-1-5-21-2047949552-857980807-821054962-504\Software\Classes\Local Settings\M
HKU\S-1-5-21-2047949552-857980807-821054962-504\Software\Classes\Local Settings\M
HKU\S-1-5-21-2047949552-857980807-821054962-504_Classes\Local Settings\MuiCache\
HKU\S-1-5-21-2047949552-857980807-821054962-504_Classes\Local Settings\MuiCache\
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\5
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\5\52C64B7E

Keys added: 1198
HKLM\SOFTWARE\Classes\*\shellex\ContextMenuHandlers\DropboxExt
HKLM\SOFTWARE\Classes\AppID\DropboxUpdate.exe
HKLM\SOFTWARE\Classes\AppID\{76E258F0-DE86-4CEC-9D30-3F728A898741}
HKLM\SOFTWARE\Classes\AppID\{96D1EED3-701E-4FE5-B996-A543A8465897}
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\LocalServ
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\ProgID
```

Figure 2 Registry after installation



```
Created with Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2019/5/21 06:16:51 , 2019/5/21 06:22:33
Computer: 9756DEDD-88EF-4 , 9756DEDD-88EF-4
Username: WDAGUtilityAccount , WDAGUtilityAccount

Keys deleted: 662
HKLM\SOFTWARE\Classes\*\shellex\ContextMenuHandlers\DropboxExt
HKLM\SOFTWARE\Classes\.paper
HKLM\SOFTWARE\Classes\AppID\DropboxUpdate.exe
HKLM\SOFTWARE\Classes\AppID\{76E258F0-DE86-4CEC-9D30-3F728A898741}
HKLM\SOFTWARE\Classes\AppID\{96D1EED3-701E-4FE5-B996-A543A8465897}
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\LocalServ
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\ProgID
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\Typelib
HKLM\SOFTWARE\Classes\CLSID\{005A3A96-BAC4-4B0A-94EA-C0CE100EA736}\VersionIr
HKLM\SOFTWARE\Classes\CLSID\{CF142CA5-83C5-4E06-8FEA-310AA519A945}
HKLM\SOFTWARE\Classes\CLSID\{CF142CA5-83C5-4E06-8FEA-310AA519A945}\InprocSe
HKLM\SOFTWARE\Classes\CLSID\{CF142CA5-83C5-4E06-8FEA-310AA519A945}\ProgID
HKLM\SOFTWARE\Classes\CLSID\{CF142CA5-83C5-4E06-8FEA-310AA519A945}\Programr
HKLM\SOFTWARE\Classes\CLSID\{CF142CA5-83C5-4E06-8FEA-310AA519A945}\TypeLib
HKLM\SOFTWARE\Classes\CLSID\{CF142CA5-83C5-4E06-8FEA-310AA519A945}\Version
HKLM\SOFTWARE\Classes\CLSID\{CF142CA5-83C5-4E06-8FEA-310AA519A945}\VersionIr
HKLM\SOFTWARE\Classes\CLSID\{E31EA727-12ED-4702-820C-4B6445F28E1A}
HKLM\SOFTWARE\Classes\CLSID\{E31EA727-12ED-4702-820C-4B6445F28E1A}\InProcSe
```

Figure 3 Registry after uninstallation



C:\Program Files\Wireshark\WinPcap_4_1_2.exe	REG_SZ	WinPcap 4.1.2 installer
C:\Program Files\Wireshark\wireshark.exe	REG_SZ	Wireshark
C:\Program Files\Wyse\PocketCloud Windows Companion\WyseBrowser.exe	REG_SZ	WyseBrowser
C:\Users\ADMINI~1\AppData\Local\Temp_iu14D2N.tmp	REG_SZ	Setup/Uninstall
C:\Users\ADMINI~1\AppData\Local\Temp\~nsu.tmp\Au_.exe	REG_SZ	Dropbox 1.1.45 Installer
C:\Users\ADMINI~1\AppData\Local\Temp\Rar$EX00.114\regshot.exe	REG_SZ	regshot
C:\Users\Administrator\AppData\Roaming\Dropbox\bin\Dropbox.exe	REG_SZ	Dropbox
C:\Users\Administrator\Desktop\Active Registry Monitor 1.38 (Portable)\arm.exe	REG_SZ	Active Registry Monitor
C:\Users\Administrator\Desktop\cports.exe	REG_SZ	CurrPorts
C:\Users\Administrator\Desktop\Regshot\regshot.exe	REG_SZ	regshot
C:\Users\Administrator\Documents\Downloads\Programs\Dropbox 1.1.45.exe	REG_SZ	Dropbox 1.1.45 Installer
C:\Users\Administrator\Documents\Downloads\Programs\smsniff_setup.exe	REG_SZ	smsniff_setup

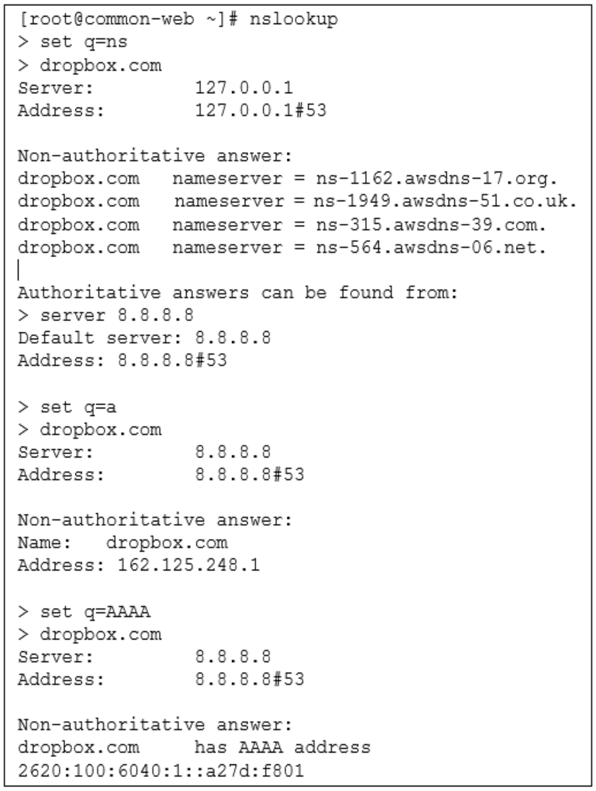
Figure 4 Remnants of Dropbox registry

Even after Dropbox client had been uninstalled, Dropbox folder remains in the system, located at *"%AppData%"*. By just looking at the registry, one can determine whether there has been an installation of Dropbox. Fig. 4 depicts the remnants of Dropbox registry after uninstallation. We can see from the second highlighted row that Dropbox.exe was previously executed on the system.

C. Network Activity

When folders and files are being synchronized, there are network activities that serve as good artefacts for investigation. Dropbox claims to keep the data encrypted, to verify that the connection that the data is transmit on HTTPS or SSL/TLS protocol, packets were captured while uploading the file to Dropbox cloud storage.

URL to Dropbox web account is a secure connection *https://www.dropbox.com/home#*. Nslookup was performed to resolve the IP address of *www.dropbox.com* and the IPs are found to be 162.125.248.1 2620:100:6040:1::a27d:f801 (Fig. 5)

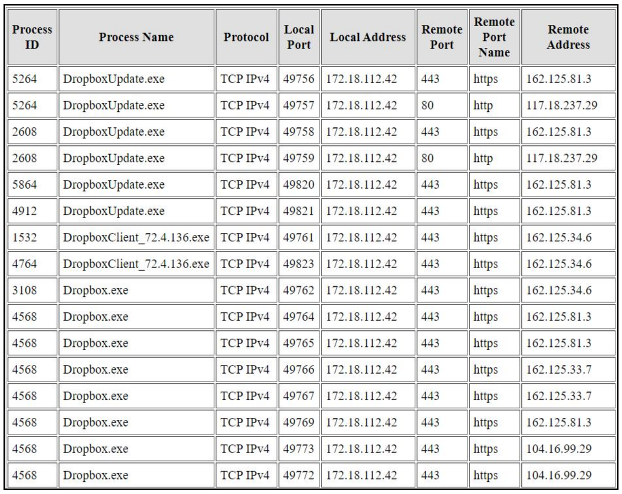


```
[root@common-web ~]# nslookup
> set q=ns
> dropbox.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
dropbox.com     nameserver = ns-1162.awsdns-17.org.
dropbox.com     nameserver = ns-1949.awsdns-51.co.uk.
dropbox.com     nameserver = ns-315.awsdns-39.com.
dropbox.com     nameserver = ns-564.awsdns-06.net.
|
Authoritative answers can be found from:
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53

> set q=a
> dropbox.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   dropbox.com
Address: 162.125.248.1

> set q=AAAA
> dropbox.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
dropbox.com     has AAAA address
2620:100:6040:1::a27d:f801
```

Figure 5 Resolving Dropbox IP address

Investigation with Wireshark reveals that the connection protocol is "TLSv1" and using TCP port 443, which represents secure https with encrypted communication. Dropbox's transmission protocol between the client software and the server is built on HTTPS. All files stored on Dropbox servers are encrypted (AES 256). The connections between the clients and the Dropbox servers are secured with SSL. Uploaded data is encrypted with AES. The AES key is user independent and only secures the data during storage while transfer security relies on SSL.

Packets captured by Wireshark and LiveTcpUdpWatch reveal a HTTP non-encrypted connection with Dropbox server and is recognized as the desktop notification.



Process ID	Process Name	Protocol	Local Port	Local Address	Remote Port	Remote Port Name	Remote Address
5264	DropboxUpdate.exe	TCP IPv4	49756	172.18.112.42	443	https	162.125.81.3
5264	DropboxUpdate.exe	TCP IPv4	49757	172.18.112.42	80	http	117.18.237.29
2608	DropboxUpdate.exe	TCP IPv4	49758	172.18.112.42	443	https	162.125.81.3
2608	DropboxUpdate.exe	TCP IPv4	49759	172.18.112.42	80	http	117.18.237.29
5864	DropboxUpdate.exe	TCP IPv4	49820	172.18.112.42	443	https	162.125.81.3
4912	DropboxUpdate.exe	TCP IPv4	49821	172.18.112.42	443	https	162.125.81.3
1532	DropboxClient_72.4.136.exe	TCP IPv4	49761	172.18.112.42	443	https	162.125.34.6
4764	DropboxClient_72.4.136.exe	TCP IPv4	49823	172.18.112.42	443	https	162.125.34.6
3108	Dropbox.exe	TCP IPv4	49762	172.18.112.42	443	https	162.125.34.6
4568	Dropbox.exe	TCP IPv4	49764	172.18.112.42	443	https	162.125.81.3
4568	Dropbox.exe	TCP IPv4	49765	172.18.112.42	443	https	162.125.81.3
4568	Dropbox.exe	TCP IPv4	49766	172.18.112.42	443	https	162.125.33.7
4568	Dropbox.exe	TCP IPv4	49767	172.18.112.42	443	https	162.125.33.7
4568	Dropbox.exe	TCP IPv4	49769	172.18.112.42	443	https	162.125.81.3
4568	Dropbox.exe	TCP IPv4	49773	172.18.112.42	443	https	104.16.99.29
4568	Dropbox.exe	TCP IPv4	49772	172.18.112.42	443	https	104.16.99.29

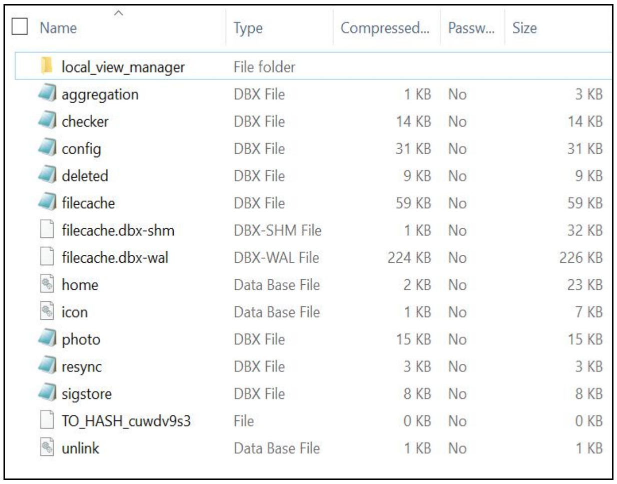
Figure 6 List of Dropbox connection in LiveTcpUdpWatch

D. Dropbox Related Files and Issues

Dropbox binaries are installed into *%AppData%\Dropbox\bin* instead of the standard *%PROGRAMFILES%.* Dropbox installation directory is not in standard Program Files *%PROGRAMFILES%*, but instead Dropbox binaries are installed into *%AppData%\Dropbox\bin* under the user profile. On Windows 10 it falls under *Users/username/AppData/Roaming/Dropbox.*

Dropbox stores information about the host locally, located at *%AppData%\Dropbox* folder. It was discovered that Dropbox client uses only the *host_id* to authenticate. *host_id* is located inside *config.db* of Dropbox folder. The file could be read using SQLite DB tool.

Using *host_id* for authentication had raised a security issue. The concern is that *config.db* file is completely portable and is not tied to the system. If someone gets access to a *config.db* file, he or she can use HEX Editor to find the path of Dropbox installation and replicate it the folder location and this will in turn resync all the files of that particular account.



Name	Type	Compressed...	Passw...	Size
local_view_manager	File folder			
aggregation	DBX File	1 KB	No	3 KB
checker	DBX File	14 KB	No	14 KB
config	DBX File	31 KB	No	31 KB
deleted	DBX File	9 KB	No	9 KB
filecache	DBX File	59 KB	No	59 KB
filecache.dbx-shm	DBX-SHM File	1 KB	No	32 KB
filecache.dbx-wal	DBX-WAL File	224 KB	No	226 KB
home	Data Base File	2 KB	No	23 KB
icon	Data Base File	1 KB	No	7 KB
photo	DBX File	15 KB	No	15 KB
resync	DBX File	3 KB	No	3 KB
sigstore	DBX File	8 KB	No	8 KB
TO_HASH_cuwdv9s3	File	0 KB	No	0 KB
unlink	Data Base File	1 KB	No	1 KB

Figure 7 Database files

V. CLOUD FORENSICS CHALLENGES

Cloud forensic is one branch of digital forensic which possess many challenges. Digital forensic analyst or examiner encounter obstacles at the stage of evidence acquisition, preservation and recovery of the evidence [9]. They need to have the ability to identify proper account held within cloud by customer and to gain access to the desired data in cloud storage. This process normally requires assistance of cloud service providers. Due to the large volume and remote access of the cloud storage, many forensic examiners find it challenging to obtain a complete image of a cloud storage in a forensically sound manner. Validation of image and identifying deleted data in the cloud attribute to a specific user is still challenging at this point of time. Besides, time synchronization of live acquisition is still unclear for cloud services. More training and knowledge sharing in the field of cloud forensics is necessary

VI. CONCLUSION

There are a lot of local artefacts from using Dropbox applications. In general, all these cloud-based services will create such artefacts that are useful to forensic examiner. All the research from this study may not be true by the time this paper is published as there will be newer updates or versions of Dropbox that might have completely different settings and configurations as the one we research on. Our research findings from this study hopefully will educate people or forensic examiner on what Dropbox forensic is and helps them understand the impact of Dropbox forensic can add to cloud forensic field.

ACKNOWLEDGEMENT

This research is supported by UNITAR Internal Research Grant IG15/42-2019.

REFERENCES

[1] Daryabar, F., et al., "*Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices*". Australian Journal of Forensic Sciences, 2016. 48(6): p. 615-642.

[2] Quick, D. and K.-K.R. Choo, "*Dropbox analysis: Data remnants on user machines*". Digit. Investig., 2013. 10(1): p. 3-18.

[3] Hyunji Chung, J.P., SangJin Lee, Chulhoon Kang, "*Digital Forensics Investigation of Cloud Storage Services*". Elservier: Digital investigation, 2012. Volume 9(Issue 2): p. 81-95.

[4] McClain, F. "*A write-up about some forensic aspects of online storage/file-synching service Dropbox™*". 2011; Available from: http://www.forensicfocus.com/dropbox-forensics.

[5] Forensics, M. Dropbox Decryptor. 2014; Available from: https://www.magnetforensics.com/resources/dropbox-decryptor/.

[6] Forensics, M. Magnet Internet Evidence Finder (IEF). 2016; Available from: https://www.teeltech.com/mobile-device-forensic-tools/magnet-forensics/magnet-internet-evidence-finder-ief/.

[7] Reading, D. New Free Forensics Tool: Dropbox Reader. 2011; Available from: https://www.darkreading.com/attacks-breaches/new-free-forensics-tool-dropbox-reader/d/d-id/1135893.

[8] SourceForge. RegShot. 2018 cited 2019; Available from: https://sourceforge.net/p/regshot/wiki/Home/.

[9] NIST, NIST Cloud Computing Forensic Science Challenges. 2014, NIST Cloud Computing Forensic Science Working Group, Information Technology Laboratory