Université Libre de Bruxelles
Ecole Royale Militaire

INFO-Y119 Forensics and reverse engineering

Cyber forensics case study (Project)

RIVAS Chin

December 2021

Contents

1 Context **4**

2 Evidence **4**

3 Hard disk image **4**
3.1 Integrity check . . . 4
3.2 Mounting Kali Linux . . . 5
3.3 Mounting Windows 10 . . . 6

4 Workstation basic informations **7**
4.1 OS version . . . 7
4.2 Computer Name . . . 7
4.3 Timezone . . . 7
4.4 Last Shutdown time . . . 7
4.5 Network information . . . 7
4.5.1 Interfaces . . . 7
4.5.2 Network list . . . 8

5 User's information **8**

6 User's files **9**
6.1 Encrypted Files . . . 9
6.2 Downloaded files . . . 9

7 User activity **10**
7.1 Recent documents . . . 10
7.2 UserAssist Key . . . 11
7.3 OpenSaved Registry Key . . . 11
7.4 Recent Documents Shortcut Files (.lnk) . . . 11
7.5 Email forensics . . . 11
7.5.1 Attilus Kerrin conversations . . . 12
7.5.2 Attacker's malicious email . . . 12
7.5.3 Ransom email . . . 12
7.6 Web browser . . . 12
7.6.1 Internet Explorer . . . 12
7.6.2 Mozilla Firefox . . . 13
7.7 NextCloud Logs . . . 13
7.8 Event Logs . . . 13
7.8.1 Microsoft-Windows-Windows Defender%4Operational.evtx . . . 14
7.8.2 Application logs . . . 14
7.8.3 Security logs . . . 15
7.8.4 System logs . . . 15

8 USB Forensics **15**

9 Memory forensics **16**

10 Timeline **17**

11 Conclusion **18**

12 Appendix **19**

A Workstation files **19**
A.1 Encrypted files . . . 19
A.2 Download folder . . . 21
A.3 LNK files . . . 22
A.4 Email files . . . 23
A.4.1 local files . . . 23
A.4.2 Attilus Kerrin conversation . . . 24
A.4.3 Attacker's malicious email . . . 25
A.4.4 ransom email . . . 26
A.5 Internet Explorer . . . 26
A.5.1 Containers . . . 26
A.5.2 Full History . . . 27
A.5.3 2021-10-19 History . . . 27
A.5.4 2021-10-20 History . . . 28
A.6 Mozilla Firefox . . . 28
A.6.1 Artefacts . . . 28
A.6.2 Downloads . . . 29
A.6.3 History . . . 29
A.7 NextCloud logs . . . 30
A.7.1 synchronization log . . . 30
A.8 Event Logs - Windows defender logs . . . 31
A.8.1 2021-10-19 . . . 31
A.8.2 2021-10-20 . . . 33
A.9 Event Logs - Application logs . . . 35
A.10 Event Logs - Security logs . . . 37
A.10.1 2021-10-19 15:23:02 to 15:25:36 . . . 37
A.10.2 2021-10-20 12:57:00 to 13:08:08 . . . 38
A.11 Event Logs - System logs . . . 38
A.11.1 2021-10-20 12:57:00 to 13:08:08 . . . 39

B Registry Forensics **39**
B.1 SAM Hive . . . 39
B.1.1 user's information . . . 39
B.2 NTUSER.DAT Hive . . . 40
B.2.1 Recent documents . . . 40
B.2.2 UserAssist Key . . . 41
B.3 SOFTWARE Hive . . . 43
B.3.1 OpenSaved Key . . . 43
B.4 SOFTWARE Hive . . . 44
B.4.1 OS version . . . 44
B.4.2 Network List . . . 45
B.5 SYSTEM Hive . . . 45
B.5.1 Computer Name . . . 45
B.5.2 timezone . . . 46
B.5.3 Network Interfaces . . . 46
B.5.4 Shutdown . . . 47
B.5.5 USB devices . . . 47

C CORSAIR USB files **48**
C.1 USB recover files . . . 48
C.2 TO_DO.txt . . . 48

D Memory Forensics **49**
D.1 Profile 49
D.2 pslist 49
D.3 psxview 50
D.4 pstree 51

1 Context

GAST (Global Agency for Ship Tracking) is an agency that provides satellite nautical navigation thanks to AIS (Automatic Identification System) receivers that are used for monitoring maritime traffic at a global scale.
A cyber incident occurred at one of GAST's affiliates that is responsible for project documentation and application research. Confidential documents were encrypted on an employee's workstation by a hacker. The attacker then sent an email to the employee demanding a ransom to decrypt the files and not make them public. The encrypted documents are of critical importance to the GAST agency and making them public will have a major financial impact.
The concerned employee worked from home due to COVID. The person had a connection to a NextCloud server, where affiliate's documents and code were stored. The user's machine was configured by the IT department and Administrator's privileges were given to the employee.
The employee provided her workstation to a technician which extracted the workstation's memory and hard drive images using FTK imager. In this document, the forensic analysis of these images will be made in order to discover how the hacker got access to the machine and encrypted the files. Once a timeline of events that lead to the incident is presented, we will determine whether the workstation user is implicated or not.

2 Evidence

I was provided with the following files to work with:

- **Hard disk image** : Win10_disk_image.zip
  - MD5 checksum: dd5a862ee9612691a5aa9e81e5fb9d00
  - SHA1 checksum: e974008b3191b1f9e64168d8b28f1c7a97fefee0
- **Memory image** :
  - **memdump.mem**
  - **pagefile.sys**

The forensic analysis will be done in a kali linux virtual machine and a Windows 10 machine.
Important note: All timestamps found during the forensic analysis were converted to the local Brussels time, this is of vital importance for the creation of the timeline of events.

3 Hard disk image

We will analyze first, the Hard disk image. We download the Win10_disk_image.zip file into the virtual machine. Once the hard disk image has been extracted, we will be using the ewf-tools package to check and mount the image:

```
$ sudo apt install ewf-tools
```

3.1 Integrity check

We check the hash of the image in order to verify that the image has not been tampered, using the **ewfinfo** command as shown in Figure 1

```
┌──(root💀kali)-[/home/kali/Desktop/win10_disk_image]
└─# ewfinfo win10_disk_image.E01
ewfinfo 20140807

Acquiry information
        Case number:            01
        Description:            Win10_hard_disk
        Examiner name:
        Evidence number:        01
        Notes:
        Acquisition date:       Wed Oct 20 14:48:51 2021
        System date:            Wed Oct 20 14:48:51 2021
        Operating system used:  Win 201x
        Software version used:  ADI3.2.0.0
        Password:               N/A

EWF information
        File format:            FTK Imager
        Sectors per chunk:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      104857600
        Media size:             50 GiB (53687091200 bytes)

Digest hash information
        MD5:                    dd5a862ee9612691a5aa9e81e5fb9d00
        SHA1:                   e974008b3191b1f9e64168d8b28f1c7a97fefee0
```

Figure 1: hash verification

3.2 Mounting Kali Linux

We present the steps to follow to successfully mount the disk image in a kali linux virtual machine:

- Make a new folder were the raw image will be mounted, at **/mnt/** . We called this folder *ewfWin10*.
- Using the command *ewfmount* to mount the raw image at **/mnt/ewfWin10**
- Verification of the raw's image partition table with the command *mmls* to check the start of the main partition and calculate the offset that will be used to mount the raw image. In this case the value is 104448 which means that the **offset will be : 53477376** (104448 * 512).
- Make a new folder were the hard drive will be mounted, at **/mnt/**. We called this folder *windows_10*.
- The raw image is then mounted at */mnt/windows_10* using the command:

```
$ mount -o loop,ro,show_sys_files,stream_interface=windows,offset=53477376
/mnt/ewfWin10/ewf1 /mnt/windows_10
```

```
┌──(root💀kali)-[/home/kali]
└─# mkdir /mnt/ewfWin10

┌──(root💀kali)-[/home/kali]
└─# ewfmount /home/kali/Desktop/win10_disk_image/win10_disk_image.E01 /mnt/ewfWin10
ewfmount 20140807


┌──(root💀kali)-[/home/kali]
└─# ls /mnt/ewfWin10
ewf1

┌──(root💀kali)-[/home/kali]
└─# mmls /mnt/ewfWin10/ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000104447   0000102400   NTFS / exFAT (0x07)
003:  000:001   0000104448   0103829949   0103725502   NTFS / exFAT (0x07)
004:  ------    0103829950   0103831551   0000001602   Unallocated
005:  000:002   0103831552   0104853503   0001021952   Unknown Type (0x27)
006:  ------    0104853504   0104857599   0000004096   Unallocated

┌──(root💀kali)-[/home/kali]
└─# mkdir /mnt/windows_10

┌──(root💀kali)-[/home/kali]
└─# mount -o loop,ro,show_sys_files,stream_interface=windows,offset=53477376 /mnt/ewfWin10/ewf1 /mnt/windows_10

┌──(root💀kali)-[/home/kali]
└─#
```

Figure 2: Hard drive mount

3.3 Mounting Windows 10

Windows 10 will also be used to do some forensic analysis. There are a couple of tools that are already integrated (event viewer) or are more "user friendly" as SysTools MBOX viewer for email forensics.
In order to mount the image in windows, we use FTK Imager 4.5. This tool has a mounting image feature that allow us to mount an image as a logical hard drive in the host computer.

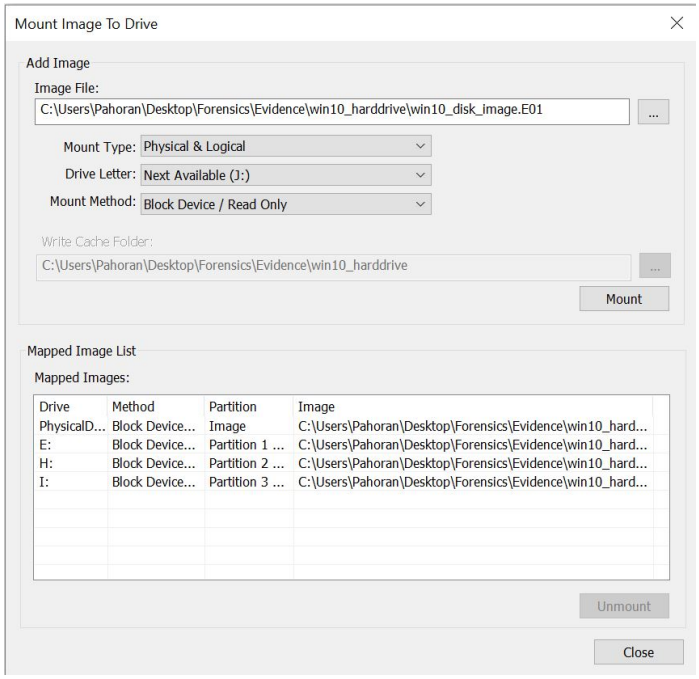


Figure 3: FTK Imager - Hard drive mount in Windows

4 Workstation basic informations

Registry forensics are useful to obtain valued information about the worktation and user's actions. We will focus in a couple of the main registry hives and they can be found at the following addresses:

- **SAM hive** - */mnt/windows_10/Windows/System32/config/SAM.*
- **SOFTWARE hive** - */mnt/windows_10/Windows/System32/config/SOFTWARE.*
- **SYSTEM hive** - */mnt/windows_10/Windows/System32/config/SYSYEM.*

To parse the information of the hives, we will be using the RegRipper 3.0 tool . This application has plugins that make the forensic analysis more handy. It is important to notice that timestamps are usually format in UTC time so we will be converting those timestamps to the current regional time.

4.1 OS version

the following command will gives us the OS information as well as the OS installation times as shown in Appendix B.4.1 :

```
$ rip.pl -r SOFTWARE -p winver
```

Operating system : Windows 10 Enterprise
Build : 19041.vb_release.191206-1406
Installation time : 2021-03-17 16:43:58

4.2 Computer Name

```
$ rip.pl -r SYSTEM -p compname
```

Computer Name : DESKTOP-M8160L5
TCP/IP Hostname : DESKTOP-M8160L5

4.3 Timezone

```
$ rip.pl -r SYSTEM -p timezone
```

StandardNAme : @tzres.dll,-302
TimeZoneKeyName : Romance Standard Time

4.4 Last Shutdown time

```
$ rip.pl -r SYSTEM -p shutdown
```

ShutdownTime : 2021-10-17 18:43:17

4.5 Network information

4.5.1 Interfaces

List of the networks interfaces on the workstations as shown in Appendix B.5.3.

```
$ rip.pl -r SYSTEM -p nic2
$ rip.pl -r SYSTEM -p networksetup2
```

Adapter : 901ee3f6-8364-4665-a31e-f868a6a10fdf
DhcpIPAddress : 192.168.1.39
DhcpSubnetMask : 255.255.255.0
DhcpServer : 192.168.1.1
DhcpNameServer : 192.168.1.1

DhcpDefaultGateway : 192.168.1.1
DhcpDomain : lan
Network Adapter : Ethernet - Intel(R) PRO/1000 MT Desktop Adapter (wired).
PermanentAddress : 8:0:27:35:e3:3a

4.5.2 Network list

List of networks to which the workstation was connected as shown in Appendix B.4.2

```
$ rip.pl -r SOFTWARE -p networklist
```

Network
Type : Wired
DefaultGatewayMAC : 52-54-00-12-35-02
Creation date : 2021-03-07 17:43:34
Last connected : 2021-10-13 09:42:08
Last write : 2021-10-13 16:42:08

Network2
Type : Wired
DefaultGatewayMAC : E0-B9-E5-DE-50-CA
Creation date : 2021-03-18 07:34:47
Last connected : 2021-10-20 15:04:54
Last write : 2021-10-20 13:04:54

Network3
Type : Wired
DefaultGatewayMAC : 00-00-5E-00-01-2A
Creation date : 2021-10-12 03:59:03
Last connected : 2021-10-12 03:59:03
Last write : 2021-10-12 10:59:03

5 User's information

From the SAM hive, we can look at the user's profiles and type of accounts as shown in Appendix B.1.1.

```
$ rip.pl -r SAM -f sam
```

Full Name : Victoria Timmers
User Name : vagrant
SID : 1001
Account creation date : 2021-03-17 16:53:21
Last login date: 2021-10-17 18:43:43
Last Password Fail date: 2021-10-10 13:26:50
Last Password reset date : 2021-03-17 16:53:21
Password reset data: 3 security questions and same answer: *batman* for all three.
Login count : 28
Groups: Administrators

As we can see, Victoria Timmers is the user of the workstation and she log in as vagrant. She has administrator rights which means that she have complete and unrestricted access to the computer.It is also worth to notice that she is using the same known name (batman) as her answer for the three reset password questions.

6 User's files

Now that we know that vagrant is the user's account, we can have a look at the files to see if there are some malicious files that could be the cause of the attack.

6.1 Encrypted Files

First, we have a look at the files that were encrypted (Appendix A.1), we can see that all files in the folder *Work* at vagrant Documents folder (*/mnt/windows_10/Users/vagrant/Documents*) were encrypted:
../Work/Code/data.json
../Work/Code/random_generator.py
../Work/Code/random_range_generator.py
../Work/Code/read_json_to_dictionary.py
../Work/Code/scripts.js
../Work/Documents/proposal_new_project.odt
../Work/Documents/review_2020.odt
../Work/Drafts/flight_organisation.pdf
../Work/Drafts/prepare_for_deployment.odt
../Work/Drafts/proposal_Rafiki_project.odt
With the command *stat* on the encrypted files as shown in Appendix A.1. we can also notice that the **encryption of the files was executed the 2021-10-20 between 14:50:04 and 14:53:54**

6.2 Downloaded files

Several executables were found at vagrant's Download folder (*/mnt/windows_10/Users/vagrant/Downloads* as shown in Appendix A.2. I checked every executable with Virus Total website and one of the executables named **cert.exe** was found to be a malware and the execution of this malicious application could have started the attack on Victoria Timmers workstation. It is really early in the investigation to prove the relation (if there is one) between this malware and the attack, however it is a good starting point.

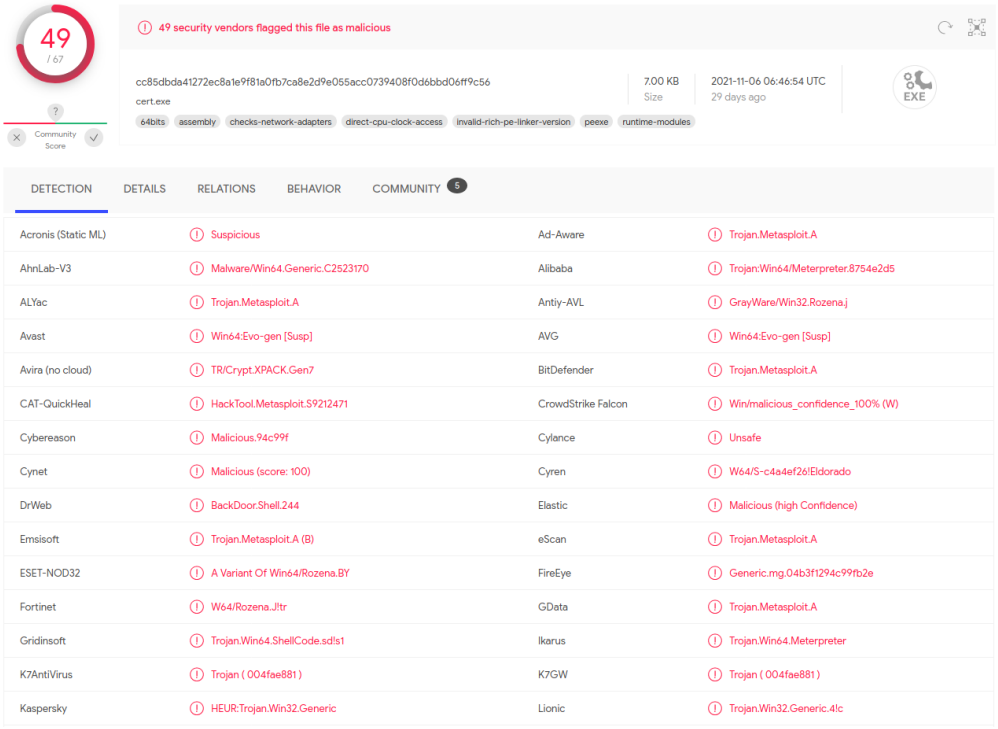


Figure 4: Virus Total analysis of cert.exe

By using the command *stat* on **cert.exe** in the terminal we have the following information about this file:
Creation date : Not specify
Last access time : 2021-10-20 13:07:56
Last modification time : 2021-10-20 13:07:13
Change time : 2021-10-20 13:07:31
The file seems to have been executed about one hour before the encryption of the files.

7 User activity

In this section we will analyze multiple files/data from the workstation hard drive, so we can verify if the user of the workstation participated in someway to the deployment of the attack. We will also verify if the malicious file *cert.exe* was the application that started the deployment of the attack.

7.1 Recent documents

The NTUSER.DAT hive provides a key with the last files/folders that were executed/open by the user. The NTUSER.DAT file is lcoated at */mnt/windows_10/Users/vagrant*. The recent documents list can be retrieved with the following command:

```
$ rip.pl -r NTUSER.DAT -p recentdocs
```

As shown in Appendix B.2.1, the file cert.exe is not shown in the list. Nevertheless, there are some files/folders in the list that could be worth to mention:
CORSAIR(E:) : seems to be a removable storage device, we will discuss more about it in the USB forensics section.
thread/ : possible thread warning
User accounts : this entry is made when an user wants to get administrator rights to execute an application.

7.2 UserAssist Key

The UserAssist registry key shows which programs were launched by the user and it is very useful for the forensic analysis. The UserAssist key can be parsed with the following command:

```
$ rip.pl -r NTUSER.DAT -p userassist
```

As we can see in the UserAssist list(Appendix B.2.2), **we can confirm that the user did actually execute cert.exe on 2021-10-20 at 13:07:31**. Now we just need to find how and when *cert.exe* was downloaded to the workstation. The UserAssist registry key provides also a list of the recent LNK files. We will merge the information of this LNK's list with the LNK files that we will analyzing later in the forensic analysis of shell items.

7.3 OpenSaved Registry Key

This key is responsible of keeping the most recent files that were opened/saved/save as via the "Common Dialog" window. The command to parse this key with RegRipper is :

```
$ rip.pl -r NTUSER.DAT -p comdlg32
```

The result list (Appendix B.3.1) shows odd results. The CIDSizeMRU list last write time is on 2021-10-20 at 12:07:26 but when looking at the OpenSavePldMRU lists, it is odd that the last write time are at most recent as 2021-10-17. It seems like the most recent entries were deleted, furthermore there is not entry of the execution of cert.exe.

7.4 Recent Documents Shortcut Files (.lnk)

LNK files are pointers to the applications launched by the user, which are created by Windows automatically. The LNK files are located in the *Recent* folder :

/mnt/windows_10/Users/vagrant.AppData/Roaming/Microsoft/Windows/Recent

LNK files can be analyzed with the *lnkinfo* command from the **liblnk package**.The creation time of a LNK file can be interpreted as the first time the pointed file was executed/open or to the creation of the file. Moreover, the modification time of a LNK file refers to the last time the pointed file was executed/open. The command *ls -la -t* can be used to show the list of LNK files found in the *Recent* folder, sorted by modification time as we can see in Appendix A.3.
From the list of LNK files, no LNK file linked to cert.exe was found and no relevant information was found. Nevertheless, if we look at the recent executed LNK files that were found in the UserAssist registry key in section 7.2, **We can observe the different executions of Mozilla thunderbird, which lead us to the next step in our forensic analysis**

7.5 Email forensics

Thanks to the list of recent LNK files found in the UseAssist registry key, we know that Mozilla Thunderbid was used by the user as email application. Emails are the main target of phishing attacks and the forensic analysis will determine if the user was the victim of one of them. the local email files are located at:

/mnt/windows_10/Users/vagrant/Appdata/Roaming/Thunderbird/Profiles

Once we select the right profile, in this case the profile folder is called *iswb7fmm.default-release*; we enter to the *imapMail* folder and we realize that a folder called *imap.gmail.com* contains 4 important files that we will be analyzing : **INBOX, All Mail, Sent Mail and Trash** as it is shown in Appendix A.4.1.
In order to have an user friendly lecture of the mails we will be using the free version of SysTools MBOX Viewer in our windows 10 workstation.
By looking at the emails exchanged with Victoria Timmers (v1c.t1m.m3r@gmail.com), we found out the following information:

7.5.1 Attilus Kerrin conversations

Attilus Kerrin (att.ker.1n@gmail.com) seems to be another employee and from the extracted email conversations (Appendix A.4.2), we can obtain the following information:

- **2020-03-10 05:58:00** - Attilus informs Victoria about the set up of her new workstation.
- **2020-03-11 05:59:00** - Attilus sends to Victoria her login information to the repository server. He ask to contact the IT department if she wants to change the password.
- **2020-10-15 16:21:26** - Attilus informs Victoria that her machine has been reinstalled after a crash.
- **2020-10-15 16:47:01** - Attilus informs Victoria that her password to the repository server has been reset and he ask her to contact him to change it.
- **2021-10-12 11:38:06** - Attilus informs Victoria that Nextcloud has been prepared so employees can safety work from home.

7.5.2 Attacker's malicious email

On **2021-10-20 at 12:03:21**, a malicious attacker send an email to Victoria from the email address: **at.k3r.1n@gmail.com** as we can observe in Appendix A.4.3. He uses the name Atilus Kerin which is similar to Attilus Kerrin in order to impersonate him. He tell victoria that the certificates for the repository servers have been updated and ask Victoria to **download the "updated certificate" from Nextcloud** at *Project/Tools/cert.exe*.
From this email we can notice that the attacker:

- Has knowledge of the repository server.
- Knows about Victoria's vacation.
- Has access to the Nextcloud server and upload the cert.exe malware.
- Knows about the relation between Attilus Kerrin and Victoria.

7.5.3 Ransom email

An email from anonymous source (noreply@anonymousemail.me) was sent to Victoria Timmers the **2021-10-20 at 16:38:51** as shown in Appendix A.4.4. The attacker says that he has encrypted the files and he is asking for 100 bitcoins, otherwise he will make the confidential files public.

7.6 Web browser

Now that cert.exe is known to be the attacker's malicious file, web browser forensic analysis could help us know when and by whom it was downloaded.

7.6.1 Internet Explorer

History, cache, download history and cookies metadata can be found in the WebCacheV*.dat file that is stored at:

/mnt/windows_10/Users/vagrant/AppData/Local/Microsoft/Windows/INetCache/.

ESEDatabaseView is the tool that we use in our windows 10 machine to open the WebCacheV01 file found in vagrant's files.
When opening the **WebCacheV01.dat** file, we encounter several tables but we focus on the **Containers table**, because that is the one that contains information about the containers tables that keep the IE history of the user. As we can see in Appendix A.5.1, the container table **number 2** contains the full history of the user. Furthermore, the container tables **number 57 and 58** keep

the user's history of 2021-10-19 and 2021-10-20 respectively.
After analyzing the container table 2 (Appendix A.5.2), It is possible to observe that it is **missing the information about the file/webpage that was modified the 2021-10-19 at 15:23**. Thankfully we can find this missing information by looking at container table 57 (Appendix A.5.3), where we can verify that this entry correspond to a windows defender threat detection.
Another interesting entry (Appendix A.5.4) to observe, is the file **TO_DO.txt** that was opened in Internet Explorer on **2021-10-20 at 12:57:40** from what it seems to be an external device. We will go more in details about this file in our USB forensics analysis in section 8.

7.6.2 Mozilla Firefox

History, Cookies, auto-complete and downloaded files are keep it by Mozilla Firefox in SQLite database files. this files can be found at:

/mnt/windows_10/Users/vagrant/AppData/Roaming/Mozilla/Firefox/Profiles/

We will focus on **places.sqlite** database (Appendix A.6.1) that's the one that contains the history and downloads information. SQLite Database Browser is the tool that we will be using to open the places.sqlite database. The Linux command to install this application is the following:

```
$ sudo apt-get install sqlitebrowser
```

With SQLite Database Browser, we can open the database places.sqlite and if we select the *moz_annos* table, we have access to the downloads list as shown in Appendix A.6.2. The dates are in Unix epoch time but it can be easily converted. From the download list we can verify that **cert.exe was downloaded using Mozilla Firefox the 2021-10-20 at 13:07:13**.
By Browsing the moz_places table (Appendix A.6.3), we can also notice that the vagrant user **log in to nextcloud using Mozilla Firefox browser at 13:06:12**

7.7 NextCloud Logs

We can have access to the local NextCloud logs on the workstation, this can be useful to verify when the malicious file cert.exe was uploaded to the server. The NextCloud logs are located at:

/mnt/windows_10/Users/vagrant/AppData/Roaming/Nextcloud

We can have a look at Nextcloud_sync.log file, this file keeps the record of all the files synchronization between the workstation and the server, as shown in Appendix A.7.1. The first time we observe the file **cert.exe** on the synchronization log, is in the failed synchronization the **2021-10-19 at 15:22:55**. We can notice that **cert.exe** and **run.exe** were uploaded to *Projects/Tools*. The synchronization did not complete successfully due to a Windows Error after detecting that both files are malware. The application tries to synchronize both files 3 more times (15:23:03, 15:23:05 and 15:23:08) without succeed.
On **2021-10-20** the synchronization of only the file **cert.exe** it is shown to fail to complete 4 times (at 12:59:23, 12:59:26, 12:59:28 and 12:59:30) due to Windows detecting it as a virus.
Finally on **2021-10-20 at 15:02:39, the synchronization of cert.exe is successfully complete** and the file is downloaded to the corresponding folder in the workstation.

7.8 Event Logs

Event logs are very useful when working on forensics, they provide a significant amount of information about applications, security, system, etc. Event logs tracks the important occurrences in the system or in a program, and it can help us to add or verify findings in the forensic analysis. These logs are located at :

/mnt/windows_10/Windows/System32/winevt/logs/

Windows 10 has a integrated tool that can be used to import and view .evtx log files. This tool is called **Event Viewer** and we will use it to review the following logs from Victoria Timmers workstation:

- **Microsoft-Windows-Windows Defender%4Operational.evtx** - Contains Windows Defender logs such as malware detection and activation/deactivation of the protection.
- **Application.evtx** - applications events logs
- **Security.evtx** - access control and security settings logs
- **System.evtx** - windows services event logs

7.8.1 Microsoft-Windows-Windows Defender%4Operational.evtx

The following information was found in the log file (Appendix A.8.1 and Appendix A.8.2) :

- **2021-10-19 at 15:23:06** - Windows Defender Antivirus has detected **cert.exe**
- **2021-10-19 at 15:23:11** - Windows Defender Antivirus has detected **run.exe**
- **2021-10-19 at 15:23:54** - Windows Defender has put cert.exe in quarantine.
- **2021-10-19 at 15:24:16** - Windows Defender has put run.exe in quarantine.
- **2021-10-19 at 15:24:44** - Windows Defender Antivirus was disabled.
- **2021-10-19 at 15:14:45** - Windows Defender SpynetReporting disabled.
- **2021-10-19 at 15:14:46** - Windows Defender SubmitSamplesConsent disabled.
- **2021-10-19 at 15:14:48** - Windows Defender TamperProtection was changed.
- **2021-10-19 at 15:14:48** - Windows Defender TamperProtectionSource was changed.
- **2021-10-20 at 12:12:11** - Windows Defender Antivirus was enabled.
- **2021-10-20 at 12:59:24** - Windows Defender Antivirus has detected **cert.exe**.
- **2021-10-20 at 12:59:49** - Windows Defender Antivirus has put **cert.exe** in quarantine.
- **2021-10-20 at 13:05:20** - Windows Defender Antivirus was disabled.

We noticed that Windows defender did actually detected and quarantine both cert.exe and run.exe. However, Windows defender was disabled just after detection on both 19th and 20th october.

7.8.2 Application logs

From the Application.evtx log file we can retrieve the following information (Appendix A.9:

- **2021-10-19 at 15:24:46** - Windows defender was put in **SNOOZED** state.
- **2021-10-20 at 12:12:06** - Windows defender was put in **ON** state.
- **2021-10-20 at 13:05:22** - Windows defender was put in **SNOOZED** state.
- **2021-10-20 at 13:10:13** - Application **mmc.exe** crashed with faulting module **KERNELBASE.dll**

This information corroborates the fact that windows defender was disabled at the times observed in Windows Defender logs.

7.8.3 Security logs

We can observe in the Security logs (Appendix A.10) that special logins were used to obtain administrator rights in order to disable windows defender both times : **2021-10-19 at 15:23:20 and 2021-10-20 at 13:05:10**.

7.8.4 System logs

We also found out that a service called **zzncmy** was installed in the system the **2021-10-20 at 13:10:50** as shown in Appendix A.11

8 USB Forensics

Sometimes important documents or files can be found in USB devices that could determine user's activities on the workstation. But first, it is important to determine if usb devices were used on the workstation. The **SYSTEM registry hive** keeps information about usb devices that are connected to the computer.
As we were hint in Section 7.1 and Section 7.6.1, we already know that a CORSAIR USB device was connected to the computer and a file called TO_DO.txt was opened from it. We can confirm this by looking at the SYSTEM hive with the following command:

```
$ rip.pl -r SYSTEM -p usbstor
```

The information about the USB device (Appendix B.5.5) are :

- **Vendor**: CORSAIR
- **Product**: Flash Voyager
- **Version**: 0.00
- **Serial number**: 7fc594859ef57c
- **Drive Letter Device**: E
- **First Install date**: 2021-10-16 at 20:35:40
- **Last Connected date** : 2021-10-20 at 12:57:29
- **Last Removal date** : 2021-10-20 at 13:01:39

After contacting the Point of Contact, the image of the CORSAIR USB was provided with its respectively hash values to verify integrity:
MD5 checksum : dfc358d06ae92af69e9dbc825018dd19
SHA1 checksum : 304c3050e39c22f977d7b64318b76ecbef4bae2e
The image was mounted in our kali linux machine doing the same steps that we follow to mount the windows 10 hard drive. The verification of the integrity of the image was also made. To analyze the USB we use the **Autopsy** Tool that is already installed in the kali virtual machine. As shown in Appendix C.1, the CORSAIR usb contains mostly pictures but thanks to the recovery function of Autopsy, it is possible to notice that one file and its zone identifier were deleted:

- **Goedkope vluchten naar Dubai op Skyscanner.html**
- **Goedkope vluchten naar Dubai op Skyscanner.html:Zone.Identifier**

Those files seems to be linked to the **flight_planning.pdf** file that was encrypted but does not prove anything related to the attack.

Another interesting file that can be found in the USB is a text file called **TO_DO.txt**, the content of this file as it can be verified in Appendix C.2 is the next text:

```
1. Buy milk
2. Buy bread
3. Go to the hardware store
4. Call Simona
5. Get the documents from El
6. ????
7. Profit!
```

We have not idea of the meaning of this text but we leave it here as part of the investigation.

9 Memory forensics

In this section we will make the forensic analysis of the memory image (**memdump.mem**) in our kali virtual machine. The Tool used to perfom the memory forensics is Volatility . The steps to install this tool in the kali linux machine are :

```
# Installing system dependecies
  $ sudo apt install -y build-essential git libdistorm3-dev yara
    libraw1394-11 libcapstone-dev capstone-tool tzdata
# Installing pip for Python2
  $ sudo apt install -y python2 python2.7-dev libpython2-dev
  $ curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
  $ sudo python2 get-pip.py
  $ sudo python2 -m pip install -U setuptools wheel
# Installing Python 2  dependencies
  $ python2 -m pip install -U distorm3 yara pycrypto pillow openpyxl
    ujson pytz ipython capstone
  $ sudo ln -s /usr/local/lib/python2.7/dist-packages/usr/lib/libyara.so
    /usr/lib/libyara.so
# Installing Volatility
  $ python2 -m pip install -U git+https://github.com/volatilityfoundation/volatility.git
```

Volatility works with profiles, so the first step is to find out what It is the right profile to use with our memory image. For this, the option flag **imageinfo** comes handy:

```
$ vol.py -f memdump.mem imageinfo
```

As shown in Appendix D.1, The suggested profile found is **Win10x64_19041**. Now that we know which profile to use in our memory image, we can check the processes list from the _EPROCESS instances that windows keeps in memory. The command used to get this list is:

```
$ vol.py -f memdump.mem --profile=Win10x64_19041 pslist
```

From the pslist (Appendix D.2), the only malicious processes that was observed were the **265 PING.EXE executions the 2021-10-20 from 13:21:06 until 13:22:32**. In order to get more information about those processes, the plugin pstree with the option -v was used as follow:

```
$ vol.py -f memdump.mem --profile=Win10x64_19041 pstree -v
```

As shown in Appendix D.4, The parent of PING.EXE is an instance of svchost.exe and after verifying both executables from the paths provided with the option -v, they seem to be legit microsoft files. This means that the malware tried to check the internet connections from the infected workstation. The verification of hidden processes can be done with the command:

```
$ vol.py -f memdump.mem --profile=Win10x64_19041 psxview
```

When trying to look for **false** values in the pslist column, just 3 processes were found. But as we can see in Appendix D.3, they do not provide any human readable name, neither a valid PID. DLLs used from those 3 processes were also not found with the volatility plugin *dllist* given the offsets of each one of them.

10 Timeline

Now that the forensic analysis is done, a timeline representation of the main events that lead to the attack is presented:

- **2021-10-17 at 18:43:17** - Workstation last shutdown.
- **2021-10-17 at 18:43:13** - vagrant account last login.
- **2021-10-19 at 15:22:55** - NextCloud Synchronization started.
- **2021-10-19 at 15:23:06** - cert.exe and run.exe are detected by Windows Defender.
- **2021-10-19 at 15:23:54** - cert.exe and run.exe are put in quarantine by Windows Defender.
- **2021-10-19 at 15:24:44** - Windows Defender Antivirus was disabled.
- **2021-10-20 at 12:03:21** - Reception of the malicious email.
- **2021-10-20 at 12:12:11** - Windows Defender Antivirus was enabled.
- **2021-10-20 at 12:57:29** - CORSAIR USB is connected to the workstation.
- **2021-10-20 at 12:57:40** - TO_DO.txt file is opened with Internet Explorer.
- **2021-10-20 at 12:59:23** - NextCloud Synchronization started.
- **2021-10-20 at 12:59:24** - cert.exe is detected by Windows Defender.
- **2021-10-20 at 12:59:49** - cert.exe is put in quarantine by Windows Defender.
- **2021-10-20 at 13:01:39** - CORSAIR USB is disconnected from the workstation.
- **2021-10-20 at 13:05:20** - Windows Defender Antivirus was disabled.
- **2021-10-20 at 13:06:12** - Victoria Timmers Nextcloud login (Firefox).
- **2021-10-20 at 13:07:13** - cert.exe is downloaded to the workstation (Firefox).
- **2021-10-20 at 13:07:31** - cert.exe is executed by vagrant user.
- **2021-10-20 at 14:50:04** - Encryption of files started.
- **2021-10-20 at 16:38:51** - Ransom email is received.

11 Conclusion

The events in the timeline help us to better understand the implication of the analyzed workstation in the incident. It is clear that the malware was uploaded to the NextCloud server but it did failed to synchronize to the workstation twice, on october 19th and 20th. Windows Defender Antivirus detected the malicious files in both times but then it was disabled by the user.
The malicious file cert.exe was then downloaded from NextCloud by the user via Mozilla Firefox. Furthermore, the user is also responsible for its execution.
From the malicious email received by Victoria Timmers, it is clear that the attacker has knowledge of Victoria work relationship with Attilus Kerrin and she/he has access to the NextCloud server of the company. It is also important to notice the content of the file **TO_DO.txt** founded in the USB does not have a direct link with the attack but it could be used in the overall investigation.

Was workstation's user implicated in the incident?

Yes, the user is responsible of download and execute the malicious file that was uploaded by the attacker.

Was she/he willfully committing sabotage?

The forensic analysis does not provide enough information to prove 100% that the workstation's user was willfully committing sabotage. However, the following information can be used to prove user negligence:

- The attacker's malicious email had various typographical errors. **Including user's name**.
- Windows Defender Antivirus was disabled by the user after detection of malicious files. **Twice, on October 19th AND October 20th**.
- **The user downloaded and executed cert.exe** after the fact that Windows Defender had detected the file as a virus.

Recommendations

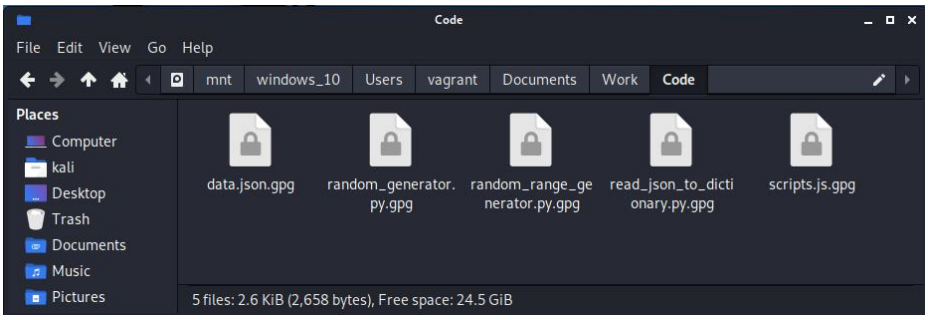
The recommendations to avoid similar incidents in the future are:

- Avoid giving administrator rights to users who don't need them to do their jobs.
- Files uploaded to the Nextcloud server need to be analyzed to avoid malicious files.
- Configuration and storage of relevant Nextcloud server logs that can be used in the forensic investigation.

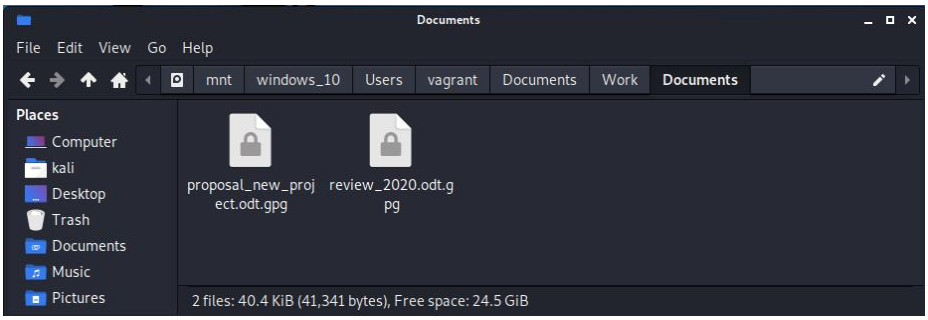
12 Appendix

A Workstation files

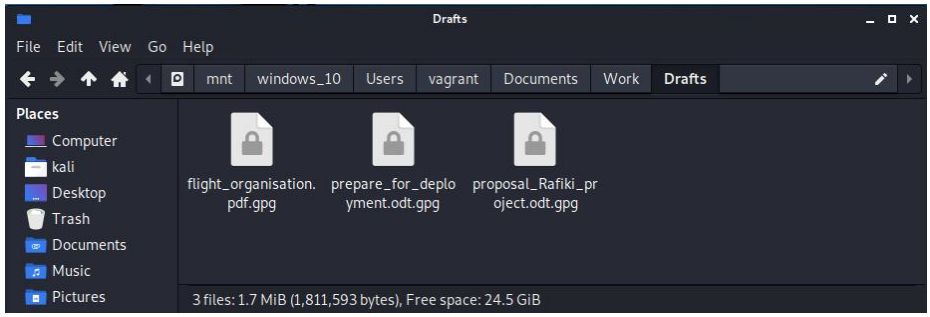
A.1 Encrypted files




```
┌──(kali㉿kali)-[/mnt/…/vagrant/Documents/Work/Code]
└─$ stat data.json.gpg random_generator.py.gpg random_range_generator.py.gpg read_json_to_dictionary.py.gpg scripts
.js.gpg
  File: data.json.gpg
  Size: 250             Blocks: 1          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 515785      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:50:04.187263900 -0400
Modify: 2021-10-20 08:50:04.187263900 -0400
Change: 2021-10-20 08:50:04.187263900 -0400
 Birth: -
  File: random_generator.py.gpg
  Size: 219             Blocks: 1          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 514393      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:50:04.102331200 -0400
Modify: 2021-10-20 08:50:04.102331200 -0400
Change: 2021-10-20 08:50:04.102331200 -0400
 Birth: -
  File: random_range_generator.py.gpg
  Size: 310             Blocks: 1          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 515792      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:50:04.445023200 -0400
Modify: 2021-10-20 08:50:04.445023200 -0400
Change: 2021-10-20 08:50:04.445023200 -0400
 Birth: -
  File: read_json_to_dictionary.py.gpg
  Size: 367             Blocks: 1          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 515788      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:50:04.274734300 -0400
Modify: 2021-10-20 08:50:04.274734300 -0400
Change: 2021-10-20 08:50:04.274734300 -0400
 Birth: -
  File: scripts.js.gpg
  Size: 1512            Blocks: 8          IO Block: 4096   regular file
Device: 700h/1792d      Inode: 515789      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:50:04.359841900 -0400
Modify: 2021-10-20 08:50:04.359841900 -0400
Change: 2021-10-20 08:50:04.359841900 -0400
 Birth: -
```

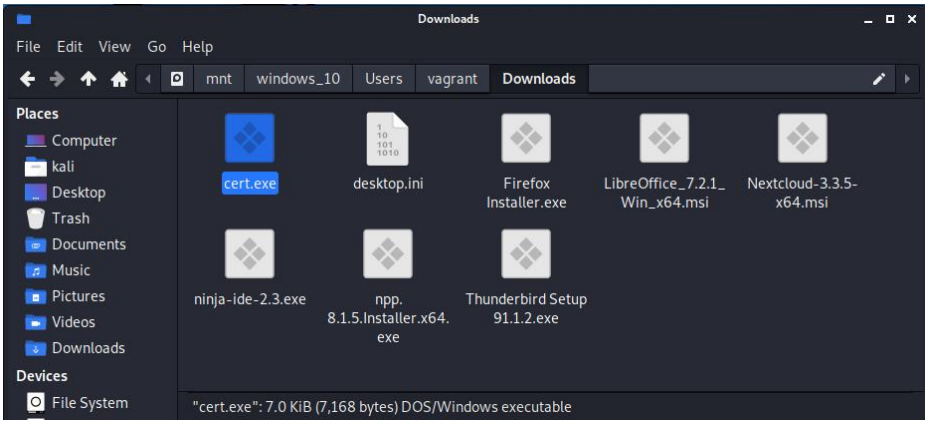


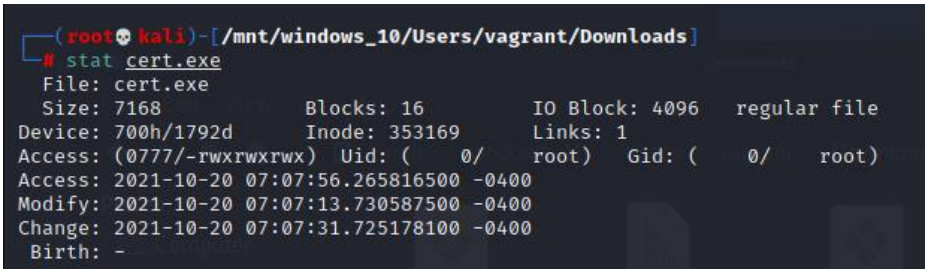
```
┌──(kali㉿kali)-[/mnt/…/vagrant/Documents/Work/Documents]
└─$ stat proposal_new_project.odt.gpg review_2020.odt.gpg
  File: proposal_new_project.odt.gpg
  Size: 24158           Blocks: 48         IO Block: 4096   regular file
Device: 700h/1792d      Inode: 516701      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:51:51.939512400 -0400
Modify: 2021-10-20 08:51:51.939512400 -0400
Change: 2021-10-20 08:51:51.939512400 -0400
 Birth: -
  File: review_2020.odt.gpg
  Size: 17183           Blocks: 40         IO Block: 4096   regular file
Device: 700h/1792d      Inode: 516702      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:51:52.035433000 -0400
Modify: 2021-10-20 08:51:52.035433000 -0400
Change: 2021-10-20 08:51:52.035433000 -0400
 Birth: -
```



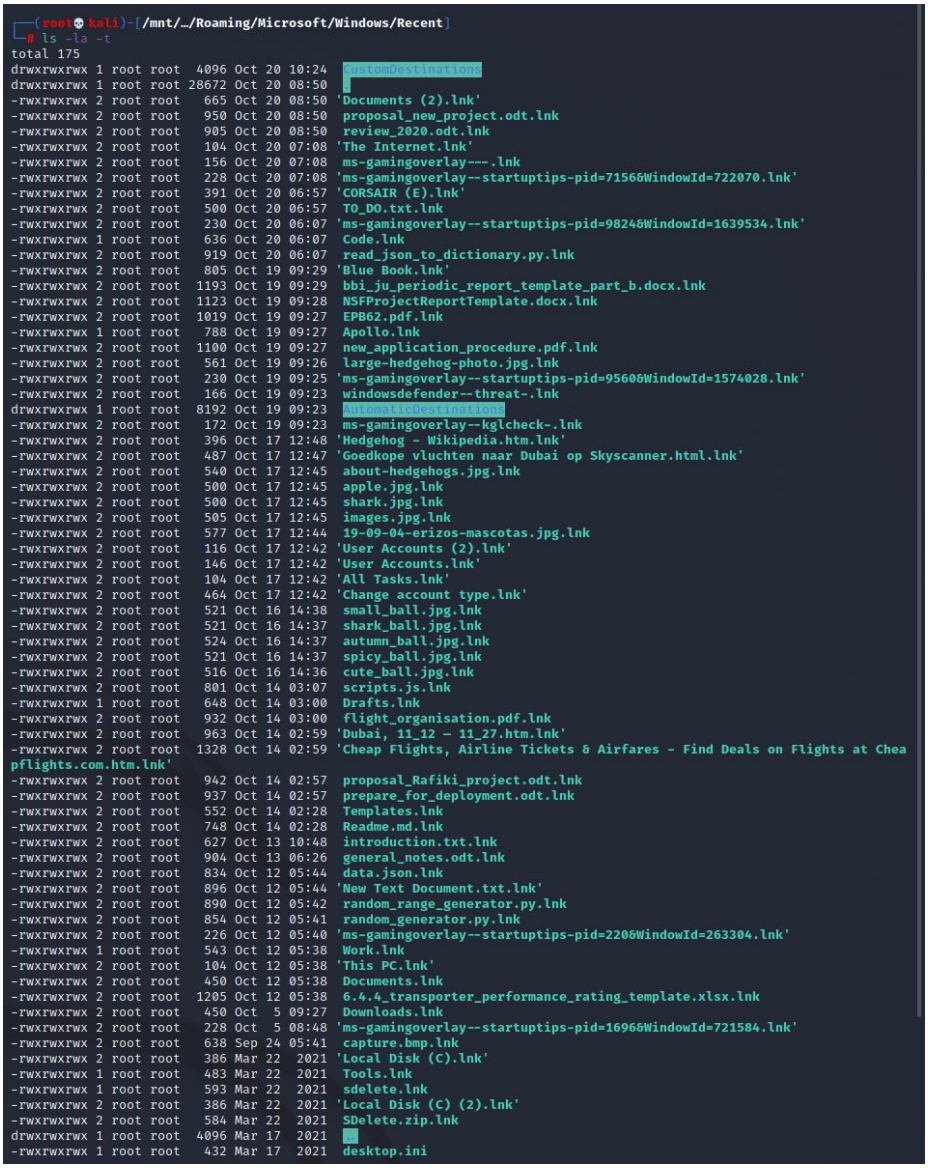

```
┌──(kali㉿kali)-[/mnt/…/vagrant/Documents/Work/Drafts]
└─$ stat flight_organisation.pdf.gpg prepare_for_deployment.odt.gpg proposal_Rafiki_project.odt.gpg
  File: flight_organisation.pdf.gpg
  Size: 1783277         Blocks: 3488       IO Block: 4096   regular file
Device: 700h/1792d      Inode: 29950       Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:53:54.702877900 -0400
Modify: 2021-10-20 08:53:54.702877900 -0400
Change: 2021-10-20 08:53:54.702877900 -0400
 Birth: -
  File: prepare_for_deployment.odt.gpg
  Size: 15815           Blocks: 32         IO Block: 4096   regular file
Device: 700h/1792d      Inode: 515413      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:53:54.905432300 -0400
Modify: 2021-10-20 08:53:54.905432300 -0400
Change: 2021-10-20 08:53:54.905432300 -0400
 Birth: -
  File: proposal_Rafiki_project.odt.gpg
  Size: 12501           Blocks: 32         IO Block: 4096   regular file
Device: 700h/1792d      Inode: 506557      Links: 2
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-10-20 08:53:54.808979300 -0400
Modify: 2021-10-20 08:53:54.808979300 -0400
Change: 2021-10-20 08:53:54.808979300 -0400
 Birth: -
```

A.2 Download folder



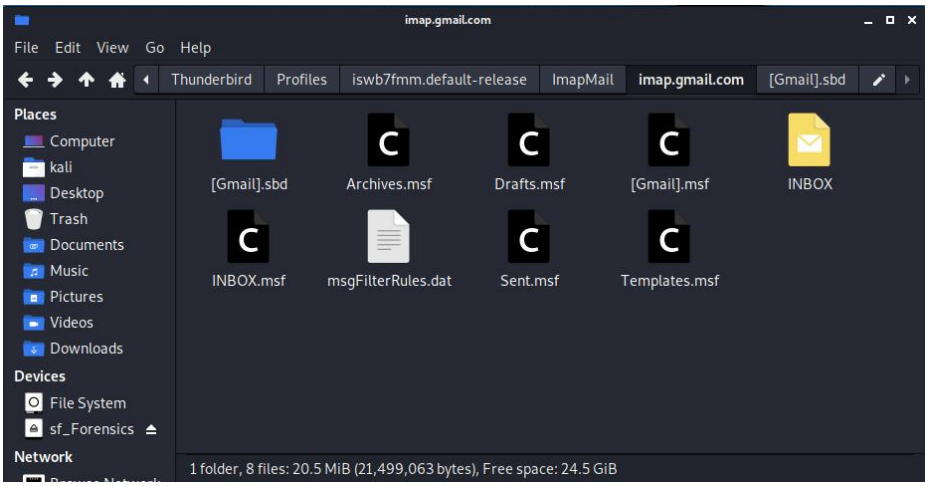


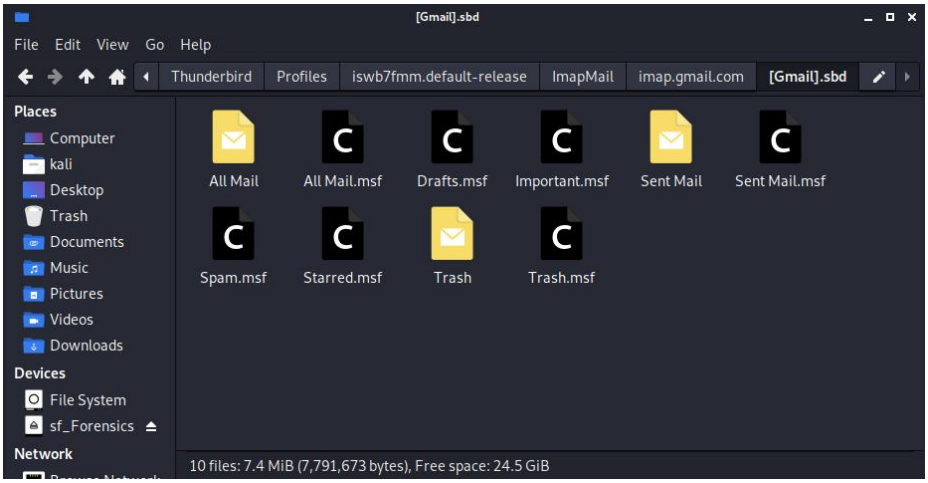
A.3 LNK files


┌──(root💀kali)-[/mnt/…/Roaming/Microsoft/Windows/Recent]
└─# ls -la -t
total 175
drwxrwxrwx 1 root root 4096 Oct 20 10:24 CustomDestinations
drwxrwxrwx 1 root root 28672 Oct 20 08:50 .
-rwxrwxrwx 2 root root   665 Oct 20 08:50 'Documents (2).lnk'
-rwxrwxrwx 2 root root   950 Oct 20 08:50 proposal_new_project.odt.lnk
-rwxrwxrwx 2 root root   905 Oct 20 08:50 review_2020.odt.lnk
-rwxrwxrwx 2 root root   104 Oct 20 07:08 'The Internet.lnk'
-rwxrwxrwx 2 root root   156 Oct 20 07:08 ms-gamingoverlay---.lnk
-rwxrwxrwx 2 root root   228 Oct 20 07:08 'ms-gamingoverlay--startuptips-pid=71568WindowId=722070.lnk'
-rwxrwxrwx 2 root root   391 Oct 20 06:57 'CORSAIR (E).lnk'
-rwxrwxrwx 2 root root   500 Oct 20 06:57 TO_DO.txt.lnk
-rwxrwxrwx 2 root root   230 Oct 20 06:07 'ms-gamingoverlay--startuptips-pid=98248WindowId=1639534.lnk'
-rwxrwxrwx 1 root root   636 Oct 20 06:07 Code.lnk
-rwxrwxrwx 2 root root   919 Oct 20 06:07 read_json_to_dictionary.py.lnk
-rwxrwxrwx 2 root root   805 Oct 19 09:29 'Blue Book.lnk'
-rwxrwxrwx 2 root root 1193 Oct 19 09:29 bbi_ju_periodic_report_template_part_b.docx.lnk
-rwxrwxrwx 2 root root 1123 Oct 19 09:28 NSFProjectReportTemplate.docx.lnk
-rwxrwxrwx 2 root root 1019 Oct 19 09:27 EPB62.pdf.lnk
-rwxrwxrwx 1 root root   788 Oct 19 09:27 Apollo.lnk
-rwxrwxrwx 2 root root 1100 Oct 19 09:27 new_application_procedure.pdf.lnk
-rwxrwxrwx 2 root root   561 Oct 19 09:26 large-hedgehog-photo.jpg.lnk
-rwxrwxrwx 2 root root   230 Oct 19 09:25 'ms-gamingoverlay--startuptips-pid=95608WindowId=1574028.lnk'
-rwxrwxrwx 2 root root   166 Oct 19 09:23 windowsdefender--threat-.lnk
drwxrwxrwx 1 root root 8192 Oct 19 09:23 AutomaticDestinations
-rwxrwxrwx 2 root root   172 Oct 19 09:23 ms-gamingoverlay--kglcheck-.lnk
-rwxrwxrwx 2 root root   396 Oct 17 12:48 'Hedgehog - Wikipedia.htm.lnk'
-rwxrwxrwx 2 root root   487 Oct 17 12:47 'Goedkope vluchten naar Dubai op Skyscanner.html.lnk'
-rwxrwxrwx 2 root root   540 Oct 17 12:45 about-hedgehogs.jpg.lnk
-rwxrwxrwx 2 root root   500 Oct 17 12:45 apple.jpg.lnk
-rwxrwxrwx 2 root root   500 Oct 17 12:45 shark.jpg.lnk
-rwxrwxrwx 2 root root   505 Oct 17 12:45 images.jpg.lnk
-rwxrwxrwx 2 root root   577 Oct 17 12:44 19-09-04-erizos-mascotas.jpg.lnk
-rwxrwxrwx 2 root root   116 Oct 17 12:42 'User Accounts (2).lnk'
-rwxrwxrwx 2 root root   146 Oct 17 12:42 'User Accounts.lnk'
-rwxrwxrwx 2 root root   104 Oct 17 12:42 'All Tasks.lnk'
-rwxrwxrwx 2 root root   464 Oct 17 12:42 'Change account type.lnk'
-rwxrwxrwx 2 root root   521 Oct 16 14:38 small_ball.jpg.lnk
-rwxrwxrwx 2 root root   521 Oct 16 14:37 shark_ball.jpg.lnk
-rwxrwxrwx 2 root root   524 Oct 16 14:37 autumn_ball.jpg.lnk
-rwxrwxrwx 2 root root   521 Oct 16 14:37 spicy_ball.jpg.lnk
-rwxrwxrwx 2 root root   516 Oct 16 14:36 cute_ball.jpg.lnk
-rwxrwxrwx 2 root root   801 Oct 14 03:07 scripts.js.lnk
-rwxrwxrwx 1 root root   648 Oct 14 03:00 Drafts.lnk
-rwxrwxrwx 2 root root   932 Oct 14 03:00 flight_organisation.pdf.lnk
-rwxrwxrwx 2 root root   963 Oct 14 02:59 'Dubai, 11_12 – 11_27.htm.lnk'
-rwxrwxrwx 2 root root 1328 Oct 14 02:59 'Cheap Flights, Airline Tickets & Airfares - Find Deals on Flights at Chea
pflights.com.htm.lnk'
-rwxrwxrwx 2 root root   942 Oct 14 02:57 proposal_Rafiki_project.odt.lnk
-rwxrwxrwx 2 root root   937 Oct 14 02:57 prepare_for_deployment.odt.lnk
-rwxrwxrwx 2 root root   552 Oct 14 02:28 Templates.lnk
-rwxrwxrwx 2 root root   748 Oct 14 02:28 Readme.md.lnk
-rwxrwxrwx 2 root root   627 Oct 13 10:48 introduction.txt.lnk
-rwxrwxrwx 2 root root   904 Oct 13 06:26 general_notes.odt.lnk
-rwxrwxrwx 2 root root   834 Oct 12 05:44 data.json.lnk
-rwxrwxrwx 2 root root   896 Oct 12 05:44 'New Text Document.txt.lnk'
-rwxrwxrwx 2 root root   890 Oct 12 05:42 random_range_generator.py.lnk
-rwxrwxrwx 2 root root   854 Oct 12 05:41 random_generator.py.lnk
-rwxrwxrwx 2 root root   226 Oct 12 05:40 'ms-gamingoverlay--startuptips-pid=2206WindowId=263304.lnk'
-rwxrwxrwx 1 root root   543 Oct 12 05:38 Work.lnk
-rwxrwxrwx 2 root root   104 Oct 12 05:38 'This PC.lnk'
-rwxrwxrwx 2 root root   450 Oct 12 05:38 Documents.lnk
-rwxrwxrwx 2 root root 1205 Oct 12 05:38 6.4.4_transporter_performance_rating_template.xlsx.lnk
-rwxrwxrwx 2 root root   450 Oct 5 09:27 Downloads.lnk
-rwxrwxrwx 2 root root   228 Oct 5 08:48 'ms-gamingoverlay--startuptips-pid=16968WindowId=721584.lnk'
-rwxrwxrwx 2 root root   638 Sep 24 05:41 capture.bmp.lnk
-rwxrwxrwx 2 root root   386 Mar 22 2021 'Local Disk (C).lnk'
-rwxrwxrwx 1 root root   483 Mar 22 2021 Tools.lnk
-rwxrwxrwx 1 root root   593 Mar 22 2021 sdelete.lnk
-rwxrwxrwx 2 root root   386 Mar 22 2021 'Local Disk (C) (2).lnk'
-rwxrwxrwx 2 root root   584 Mar 22 2021 SDelete.zip.lnk
drwxrwxrwx 1 root root 4096 Mar 17 2021 ..
-rwxrwxrwx 1 root root   432 Mar 17 2021 desktop.ini

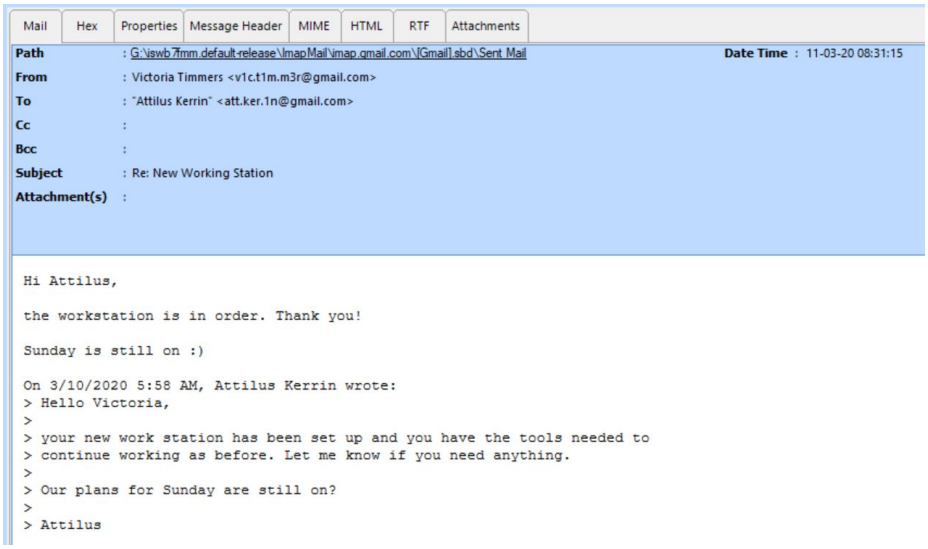
A.4 Email files

A.4.1 local files





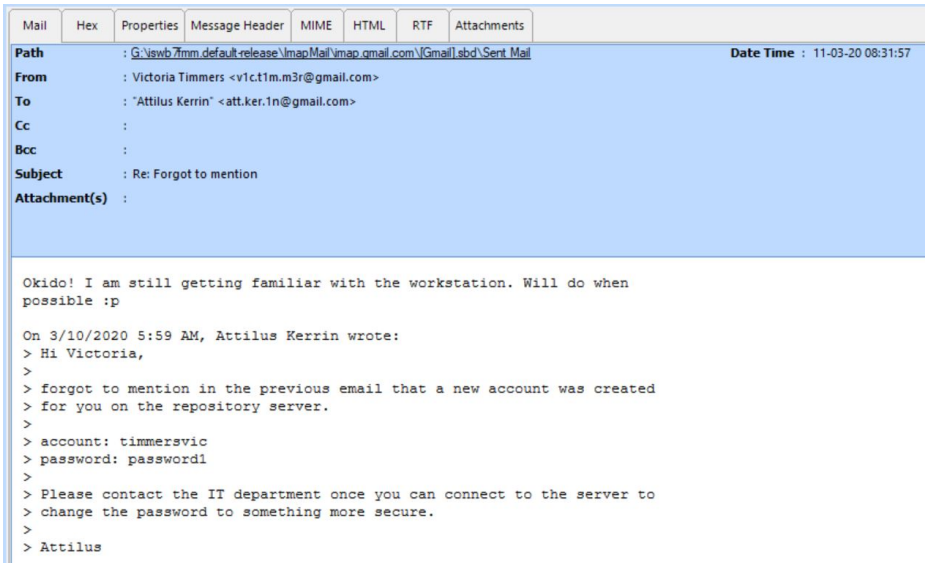
A.4.2 Attilus Kerrin conversation



Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : G:\swb7mm.default-release\ImapMail\imap.gmail.com\[Gmail].sbd\Sent Mail **Date Time** : 11-03-20 08:31:15
From : Victoria Timmers <v1c.t1m.m3r@gmail.com>
To : "Attilus Kerrin" <att.ker.1n@gmail.com>
Cc :
Bcc :
Subject : Re: New Working Station
Attachment(s) :

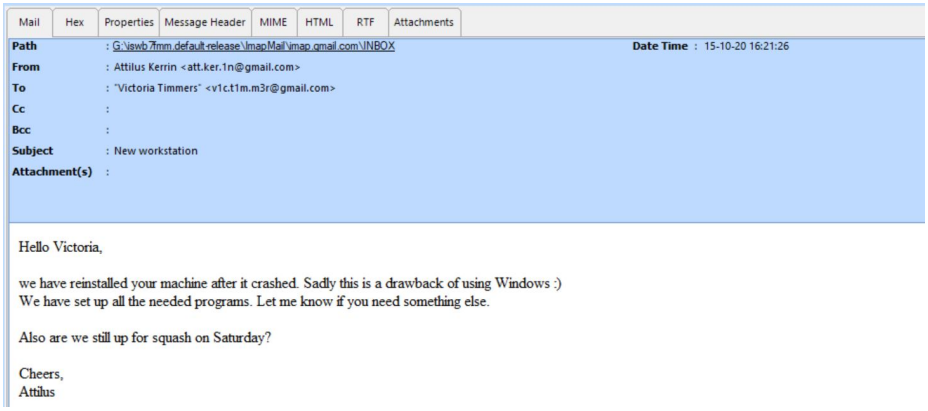
```
Hi Attilus,

the workstation is in order. Thank you!

Sunday is still on :)

On 3/10/2020 5:58 AM, Attilus Kerrin wrote:
> Hello Victoria,
>
> your new work station has been set up and you have the tools needed to
> continue working as before. Let me know if you need anything.
>
> Our plans for Sunday are still on?
>
> Attilus
```



Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : G:\swb7mm.default-release\ImapMail\imap.gmail.com\[Gmail].sbd\Sent Mail **Date Time** : 11-03-20 08:31:57
From : Victoria Timmers <v1c.t1m.m3r@gmail.com>
To : "Attilus Kerrin" <att.ker.1n@gmail.com>
Cc :
Bcc :
Subject : Re: Forgot to mention
Attachment(s) :

```
Okido! I am still getting familiar with the workstation. Will do when
possible :p

On 3/10/2020 5:59 AM, Attilus Kerrin wrote:
> Hi Victoria,
>
> forgot to mention in the previous email that a new account was created
> for you on the repository server.
>
> account: timmersvic
> password: password1
>
> Please contact the IT department once you can connect to the server to
> change the password to something more secure.
>
> Attilus
```



Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

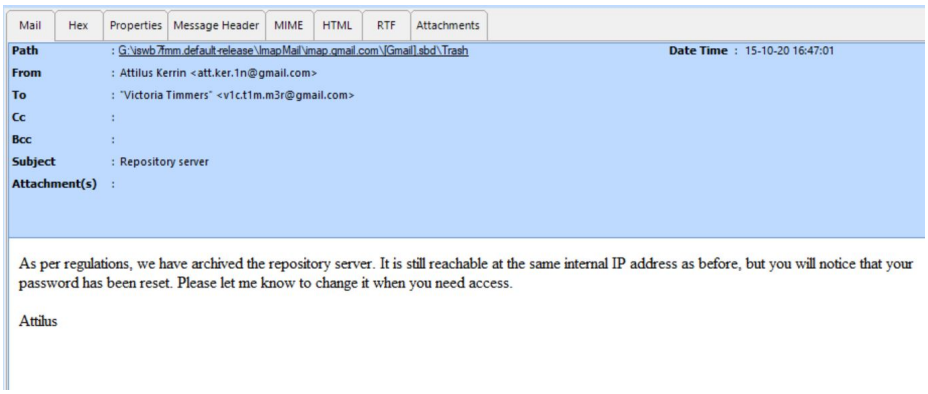
Path : G:\swb7mm.default-release\ImapMail\imap.gmail.com\INBOX **Date Time** : 15-10-20 16:21:26
From : Attilus Kerrin <att.ker.1n@gmail.com>
To : "Victoria Timmers" <v1c.t1m.m3r@gmail.com>
Cc :
Bcc :
Subject : New workstation
Attachment(s) :

Hello Victoria,

we have reinstalled your machine after it crashed. Sadly this is a drawback of using Windows :)
We have set up all the needed programs. Let me know if you need something else.

Also are we still up for squash on Saturday?

Cheers,
Attilus



Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : G:\iswb7fmm.default-release\ImapMail\imap.gmail.com\[Gmail].sbd\Trash **Date Time** : 15-10-20 16:47:01
From : Attilus Kerrin <att.ker.1n@gmail.com>
To : "Victoria Timmers" <v1c.t1m.m3r@gmail.com>
Cc :
Bcc :
Subject : Repository server
Attachment(s) :

As per regulations, we have archived the repository server. It is still reachable at the same internal IP address as before, but you will notice that your password has been reset. Please let me know to change it when you need access.

Attilus

Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : G:\iswb7fmm.default-release\ImapMail\imap.gmail.com\INBOX **Date Time** : 12-10-21 11:38:06
From : Attilus Kerrin <att.ker.1n@gmail.com>
To : "Victoria Timmers" <v1c.t1m.m3r@gmail.com>
Cc :
Bcc :
Subject : Welcome back
Attachment(s) :

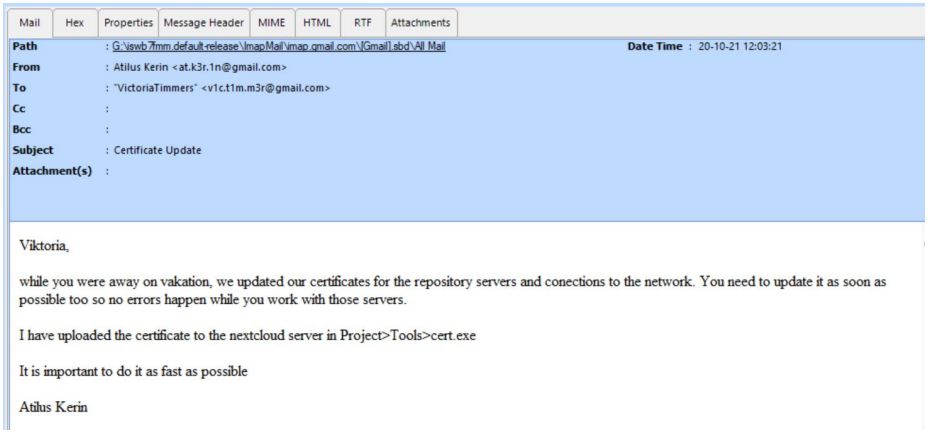
Hello Victoria,

welcome back from vacation! I hope you had a nice trip to Norway, in the meantime we were busy setting up everything to work properly during the COVID situation, so people can safely work from home.

The Nextcloud has been prepared so employees can still access all the relevant documents and so on. If you have any questions, please let me know.

Attilus

A.4.3 Attacker's malicious email



Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : G:\iswb7fmm.default-release\ImapMail\imap.gmail.com\[Gmail].sbd\All Mail **Date Time** : 20-10-21 12:03:21
From : Atilus Kerin <at.k3r.1n@gmail.com>
To : "VictoriaTimmers" <v1c.t1m.m3r@gmail.com>
Cc :
Bcc :
Subject : Certificate Update
Attachment(s) :

Viktoria,

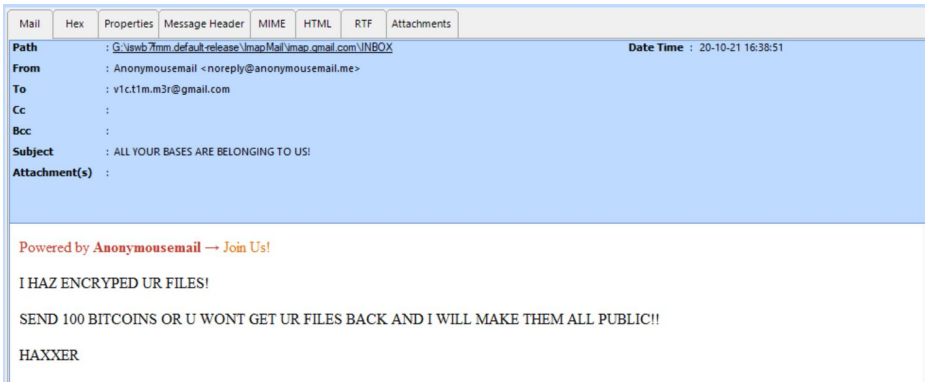
while you were away on vakation, we updated our certificates for the repository servers and conections to the network. You need to update it as soon as possible too so no errors happen while you work with those servers.

I have uploaded the certificate to the nextcloud server in Project>Tools>cert.exe

It is important to do it as fast as possible

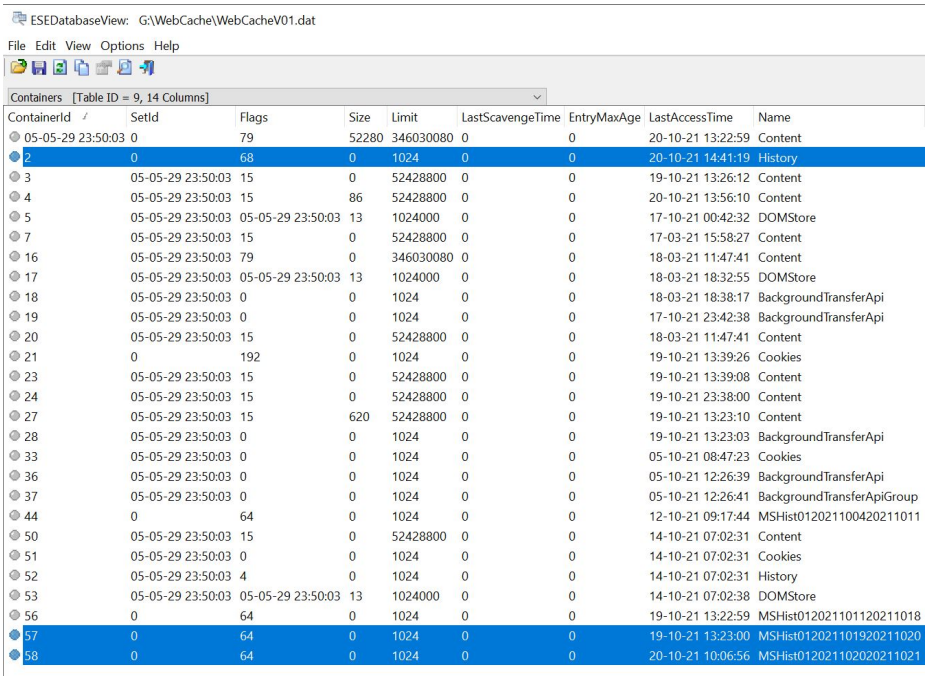
Atilus Kerin

A.4.4 ransom email



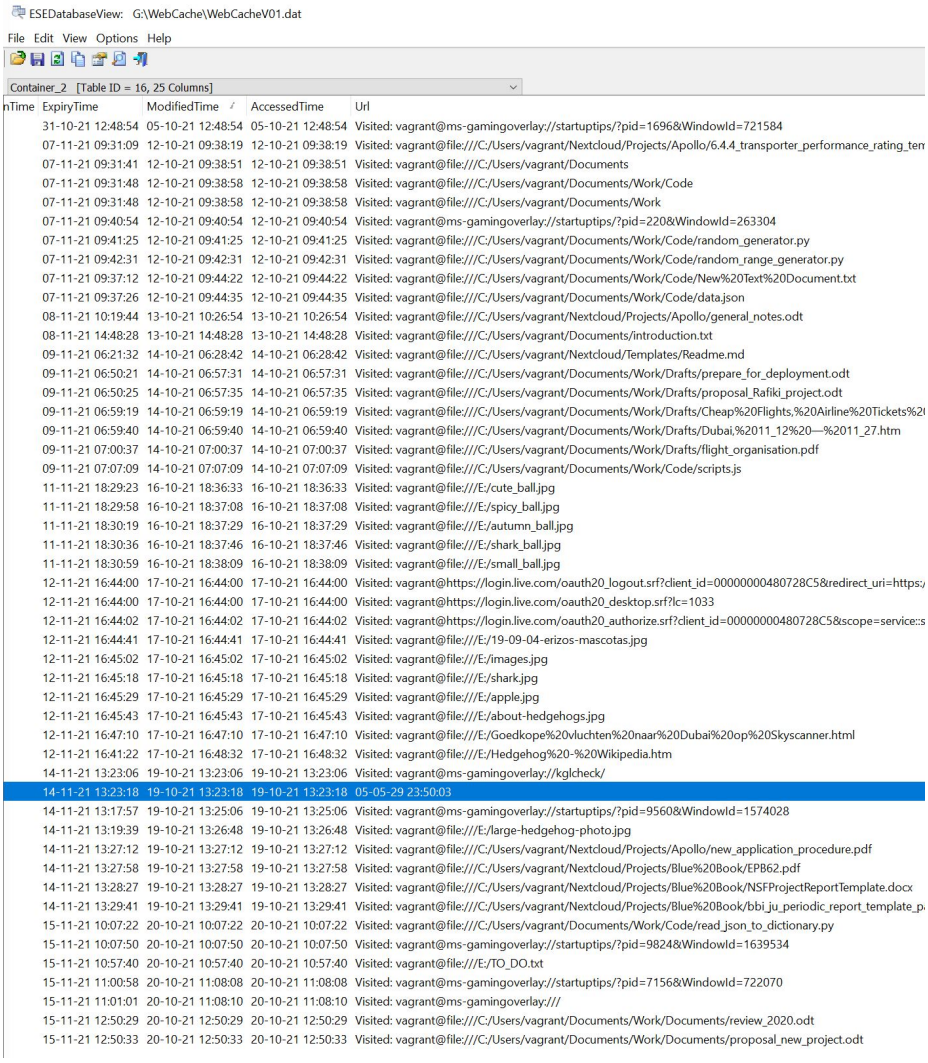
A.5 Internet Explorer

A.5.1 Containers



ContainerId	SetId	Flags	Size	Limit	LastScavengeTime	EntryMaxAge	LastAccessTime	Name
05-05-29 23:50:03	0	79	52280	346030080	0	0	20-10-21 13:22:59	Content
2	0	68	0	1024	0	0	20-10-21 14:41:19	History
3	05-05-29 23:50:03	15	0	52428800	0	0	19-10-21 13:26:12	Content
4	05-05-29 23:50:03	15	86	52428800	0	0	20-10-21 13:56:10	Content
5	05-05-29 23:50:03	05-05-29 23:50:03	13	1024000	0	0	17-10-21 00:42:32	DOMStore
7	05-05-29 23:50:03	15	0	52428800	0	0	17-03-21 15:58:27	Content
16	05-05-29 23:50:03	79	0	346030080	0	0	18-03-21 11:47:41	Content
17	05-05-29 23:50:03	05-05-29 23:50:03	13	1024000	0	0	18-03-21 18:32:55	DOMStore
18	05-05-29 23:50:03	0	0	1024	0	0	18-03-21 18:38:17	BackgroundTransferApi
19	05-05-29 23:50:03	0	0	1024	0	0	17-10-21 23:42:38	BackgroundTransferApi
20	05-05-29 23:50:03	15	0	52428800	0	0	18-03-21 11:47:41	Content
21	0	192	0	1024	0	0	19-10-21 13:39:26	Cookies
23	05-05-29 23:50:03	15	0	52428800	0	0	19-10-21 13:39:08	Content
24	05-05-29 23:50:03	15	0	52428800	0	0	19-10-21 23:38:00	Content
27	05-05-29 23:50:03	15	620	52428800	0	0	19-10-21 13:23:10	Content
28	05-05-29 23:50:03	0	0	1024	0	0	19-10-21 13:23:03	BackgroundTransferApi
33	05-05-29 23:50:03	0	0	1024	0	0	05-10-21 08:47:23	Cookies
36	05-05-29 23:50:03	0	0	1024	0	0	05-10-21 12:26:39	BackgroundTransferApi
37	05-05-29 23:50:03	0	0	1024	0	0	05-10-21 12:26:41	BackgroundTransferApiGroup
44	0	64	0	1024	0	0	12-10-21 09:17:44	MSHist012021100420211011
50	05-05-29 23:50:03	15	0	52428800	0	0	14-10-21 07:02:31	Content
51	05-05-29 23:50:03	0	0	1024	0	0	14-10-21 07:02:31	Cookies
52	05-05-29 23:50:03	4	0	1024	0	0	14-10-21 07:02:31	History
53	05-05-29 23:50:03	05-05-29 23:50:03	13	1024000	0	0	14-10-21 07:02:38	DOMStore
56	0	64	0	1024	0	0	19-10-21 13:22:59	MSHist012021101120211018
57	0	64	0	1024	0	0	19-10-21 13:23:00	MSHist012021101920211020
58	0	64	0	1024	0	0	20-10-21 10:06:56	MSHist012021102020211021

A.5.2 Full History



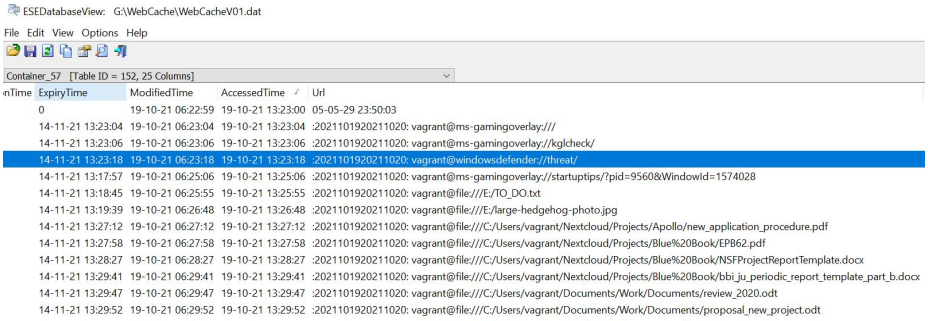
ESEDatabaseView: G:\WebCache\WebCacheV01.dat

File Edit View Options Help

Container_2 [Table ID = 16, 25 Columns]

nTime	ExpiryTime	ModifiedTime	AccessedTime	Url
	31-10-21 12:48:54	05-10-21 12:48:54	05-10-21 12:48:54	Visited: vagrant@ms-gamingoverlay://startuptips/?pid=1696&WindowId=721584
	07-11-21 09:31:09	12-10-21 09:38:19	12-10-21 09:38:19	Visited: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Apollo/6.4.4_transporter_performance_rating_ten
	07-11-21 09:31:41	12-10-21 09:38:51	12-10-21 09:38:51	Visited: vagrant@file:///C:/Users/vagrant/Documents
	07-11-21 09:31:48	12-10-21 09:38:58	12-10-21 09:38:58	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Code
	07-11-21 09:31:48	12-10-21 09:38:58	12-10-21 09:38:58	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work
	07-11-21 09:40:54	12-10-21 09:40:54	12-10-21 09:40:54	Visited: vagrant@ms-gamingoverlay://startuptips/?pid=220&WindowId=263304
	07-11-21 09:41:25	12-10-21 09:41:25	12-10-21 09:41:25	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Code/random_generator.py
	07-11-21 09:42:31	12-10-21 09:42:31	12-10-21 09:42:31	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Code/random_range_generator.py
	07-11-21 09:37:12	12-10-21 09:44:22	12-10-21 09:44:22	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Code/New%20Text%20Document.txt
	07-11-21 09:37:26	12-10-21 09:44:35	12-10-21 09:44:35	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Code/data.json
	08-11-21 10:19:44	13-10-21 10:26:54	13-10-21 10:26:54	Visited: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Apollo/general_notes.odt
	08-11-21 14:48:28	13-10-21 14:48:28	13-10-21 14:48:28	Visited: vagrant@file:///C:/Users/vagrant/Documents/introduction.txt
	09-11-21 06:21:32	14-10-21 06:28:42	14-10-21 06:28:42	Visited: vagrant@file:///C:/Users/vagrant/Nextcloud/Templates/Readme.md
	09-11-21 06:50:21	14-10-21 06:57:31	14-10-21 06:57:31	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Drafts/prepare_for_deployment.odt
	09-11-21 06:50:25	14-10-21 06:57:35	14-10-21 06:57:35	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Drafts/proposal_Rafiki_project.odt
	09-11-21 06:59:19	14-10-21 06:59:19	14-10-21 06:59:19	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Drafts/Cheap%20Flights,%20Airline%20Tickets%2
	09-11-21 06:59:40	14-10-21 06:59:40	14-10-21 06:59:40	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Drafts/Dubai,%2011_12%20—%2011_27.htm
	09-11-21 07:00:37	14-10-21 07:00:37	14-10-21 07:00:37	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Drafts/flight_organisation.pdf
	09-11-21 07:07:09	14-10-21 07:07:09	14-10-21 07:07:09	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Code/scripts.js
	11-11-21 18:29:23	16-10-21 18:36:33	16-10-21 18:36:33	Visited: vagrant@file:///E:/cute_ball.jpg
	11-11-21 18:29:58	16-10-21 18:37:08	16-10-21 18:37:08	Visited: vagrant@file:///E:/spicy_ball.jpg
	11-11-21 18:30:19	16-10-21 18:37:29	16-10-21 18:37:29	Visited: vagrant@file:///E:/autumn_ball.jpg
	11-11-21 18:30:36	16-10-21 18:37:46	16-10-21 18:37:46	Visited: vagrant@file:///E:/shark_ball.jpg
	11-11-21 18:30:59	16-10-21 18:38:09	16-10-21 18:38:09	Visited: vagrant@file:///E:/small_ball.jpg
	12-11-21 16:44:00	17-10-21 16:44:00	17-10-21 16:44:00	Visited: vagrant@https://login.live.com/oauth20_logout.srf?client_id=00000000480728C5&redirect_uri=https:/
	12-11-21 16:44:00	17-10-21 16:44:00	17-10-21 16:44:00	Visited: vagrant@https://login.live.com/oauth20_desktop.srf?lc=1033
	12-11-21 16:44:02	17-10-21 16:44:02	17-10-21 16:44:02	Visited: vagrant@https://login.live.com/oauth20_authorize.srf?client_id=00000000480728C5&scope=service::s
	12-11-21 16:44:41	17-10-21 16:44:41	17-10-21 16:44:41	Visited: vagrant@file:///E:/19-09-04-erizos-mascotas.jpg
	12-11-21 16:45:02	17-10-21 16:45:02	17-10-21 16:45:02	Visited: vagrant@file:///E:/images.jpg
	12-11-21 16:45:18	17-10-21 16:45:18	17-10-21 16:45:18	Visited: vagrant@file:///E:/shark.jpg
	12-11-21 16:45:29	17-10-21 16:45:29	17-10-21 16:45:29	Visited: vagrant@file:///E:/apple.jpg
	12-11-21 16:45:43	17-10-21 16:45:43	17-10-21 16:45:43	Visited: vagrant@file:///E:/about-hedgehogs.jpg
	12-11-21 16:47:10	17-10-21 16:47:10	17-10-21 16:47:10	Visited: vagrant@file:///E:/Goedkope%20vluchten%20naar%20Dubai%20op%20Skyscanner.html
	12-11-21 16:41:22	17-10-21 16:48:32	17-10-21 16:48:32	Visited: vagrant@file:///E:/Hedgehog%20-%20Wikipedia.htm
	14-11-21 13:23:06	19-10-21 13:23:06	19-10-21 13:23:06	Visited: vagrant@ms-gamingoverlay://kglcheck/
	14-11-21 13:23:18	19-10-21 13:23:18	19-10-21 13:23:18	05-05-29 23:50:03
	14-11-21 13:17:57	19-10-21 13:25:06	19-10-21 13:25:06	Visited: vagrant@ms-gamingoverlay://startuptips/?pid=9560&WindowId=1574028
	14-11-21 13:19:39	19-10-21 13:26:48	19-10-21 13:26:48	Visited: vagrant@file:///E:/large-hedgehog-photo.jpg
	14-11-21 13:27:12	19-10-21 13:27:12	19-10-21 13:27:12	Visited: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Apollo/new_application_procedure.pdf
	14-11-21 13:27:58	19-10-21 13:27:58	19-10-21 13:27:58	Visited: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Blue%20Book/EPB62.pdf
	14-11-21 13:28:27	19-10-21 13:28:27	19-10-21 13:28:27	Visited: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Blue%20Book/NSFProjectReportTemplate.docx
	14-11-21 13:29:41	19-10-21 13:29:41	19-10-21 13:29:41	Visited: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Blue%20Book/bbi_ju_periodic_report_template_p
	15-11-21 10:07:22	20-10-21 10:07:22	20-10-21 10:07:22	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Code/read_json_to_dictionary.py
	15-11-21 10:07:50	20-10-21 10:07:50	20-10-21 10:07:50	Visited: vagrant@ms-gamingoverlay://startuptips/?pid=9824&WindowId=1639534
	15-11-21 10:57:40	20-10-21 10:57:40	20-10-21 10:57:40	Visited: vagrant@file:///E:/TO_DO.txt
	15-11-21 11:00:58	20-10-21 11:08:08	20-10-21 11:08:08	Visited: vagrant@ms-gamingoverlay://startuptips/?pid=7156&WindowId=722070
	15-11-21 11:01:01	20-10-21 11:08:10	20-10-21 11:08:10	Visited: vagrant@ms-gamingoverlay:///
	15-11-21 12:50:29	20-10-21 12:50:29	20-10-21 12:50:29	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Documents/review_2020.odt
	15-11-21 12:50:33	20-10-21 12:50:33	20-10-21 12:50:33	Visited: vagrant@file:///C:/Users/vagrant/Documents/Work/Documents/proposal_new_project.odt

A.5.3 2021-10-19 History



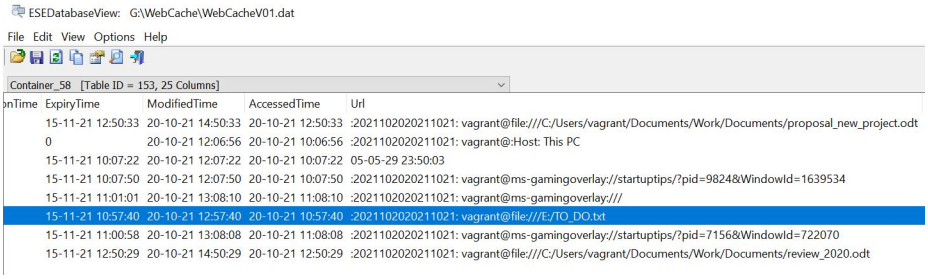
ESEDatabaseView: G:\WebCache\WebCacheV01.dat

File Edit View Options Help

Container_57 [Table ID = 152, 25 Columns]

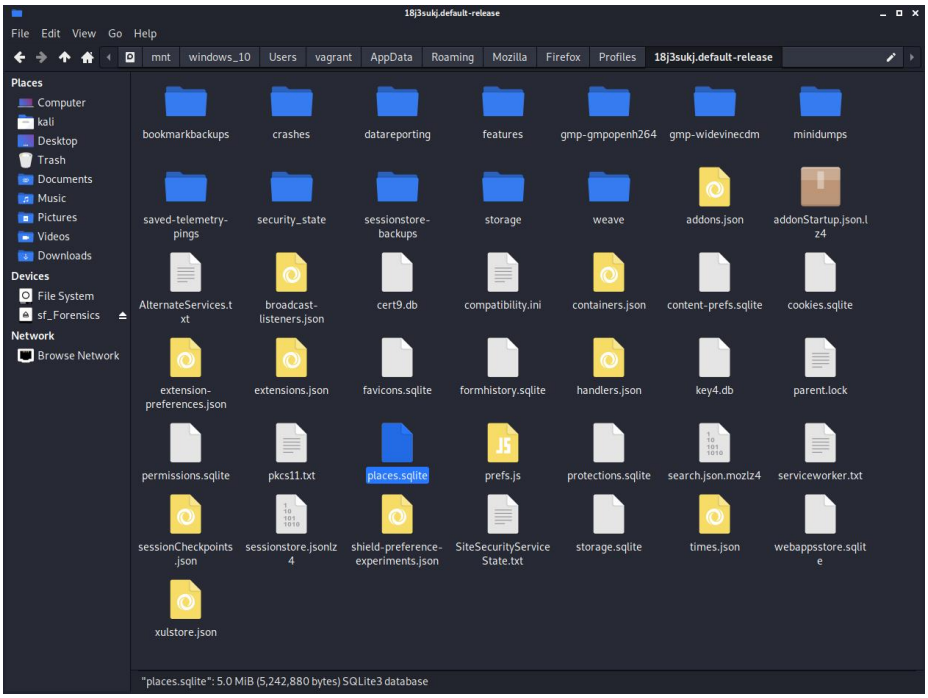
nTime	ExpiryTime	ModifiedTime	AccessedTime	Url
	0	19-10-21 06:22:59	19-10-21 13:23:00	05-05-29 23:50:03
	14-11-21 13:23:04	19-10-21 06:23:04	19-10-21 13:23:04	:20211019202110 20: vagrant@ms-gamingoverlay:///
	14-11-21 13:23:06	19-10-21 06:23:06	19-10-21 13:23:06	:20211019202110 20: vagrant@ms-gamingoverlay://kglcheck/
	14-11-21 13:23:18	19-10-21 06:23:18	19-10-21 13:23:18	:20211019202110 20: vagrant@windowsdefender://threat/
	14-11-21 13:17:57	19-10-21 06:25:06	19-10-21 13:25:06	:20211019202110 20: vagrant@ms-gamingoverlay://startuptips/?pid=9560&WindowId=1574028
	14-11-21 13:18:45	19-10-21 06:25:55	19-10-21 13:25:55	:20211019202110 20: vagrant@file:///E:/TO_DO.txt
	14-11-21 13:19:39	19-10-21 06:26:48	19-10-21 13:26:48	:20211019202110 20: vagrant@file:///E:/large-hedgehog-photo.jpg
	14-11-21 13:27:12	19-10-21 06:27:12	19-10-21 13:27:12	:20211019202110 20: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Apollo/new_application_procedure.pdf
	14-11-21 13:27:58	19-10-21 06:27:58	19-10-21 13:27:58	:20211019202110 20: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Blue%20Book/EPB62.pdf
	14-11-21 13:28:27	19-10-21 06:28:27	19-10-21 13:28:27	:20211019202110 20: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Blue%20Book/NSFProjectReportTemplate.docx
	14-11-21 13:29:41	19-10-21 06:29:41	19-10-21 13:29:41	:20211019202110 20: vagrant@file:///C:/Users/vagrant/Nextcloud/Projects/Blue%20Book/bbi_ju_periodic_report_template_part_b.docx
	14-11-21 13:29:47	19-10-21 06:29:47	19-10-21 13:29:47	:20211019202110 20: vagrant@file:///C:/Users/vagrant/Documents/Work/Documents/review_2020.odt
	14-11-21 13:29:52	19-10-21 06:29:52	19-10-21 13:29:52	:20211019202110 20: vagrant@file:///C:/Users/vagrant/Documents/Work/Documents/proposal_new_project.odt

A.5.4 2021-10-20 History

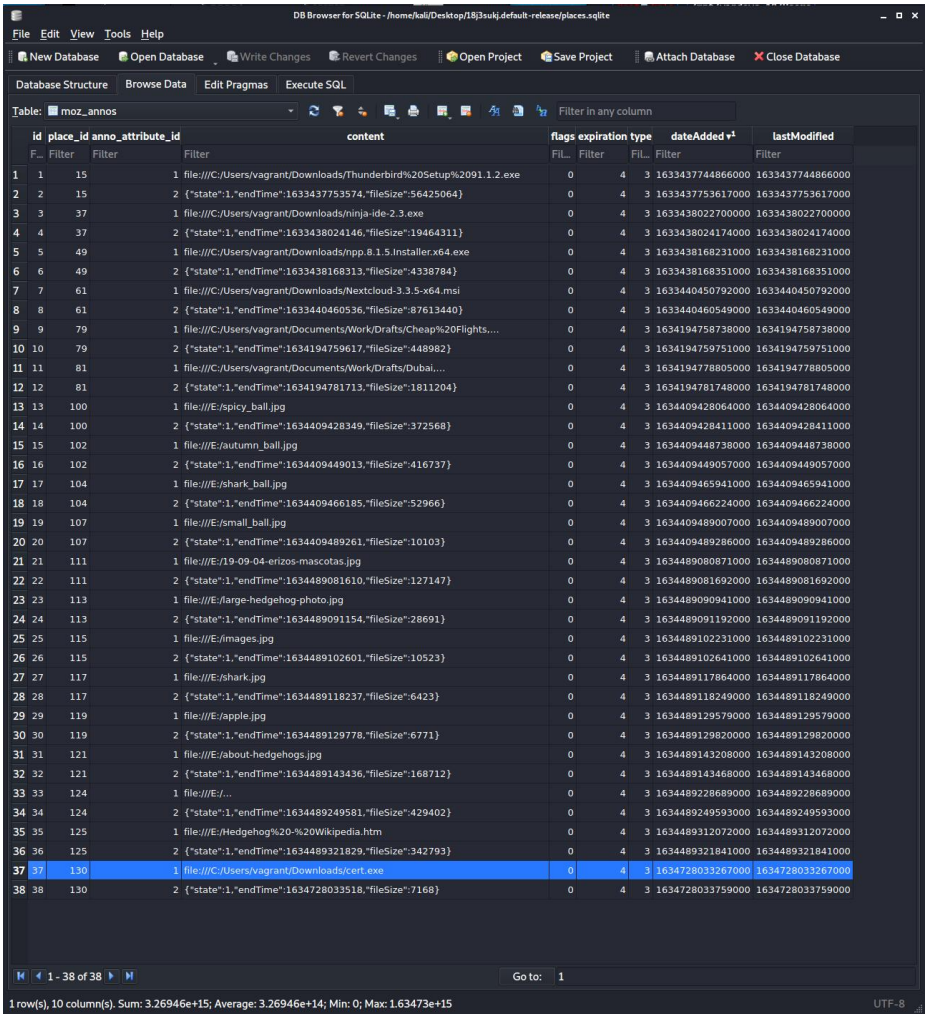


A.6 Mozilla Firefox

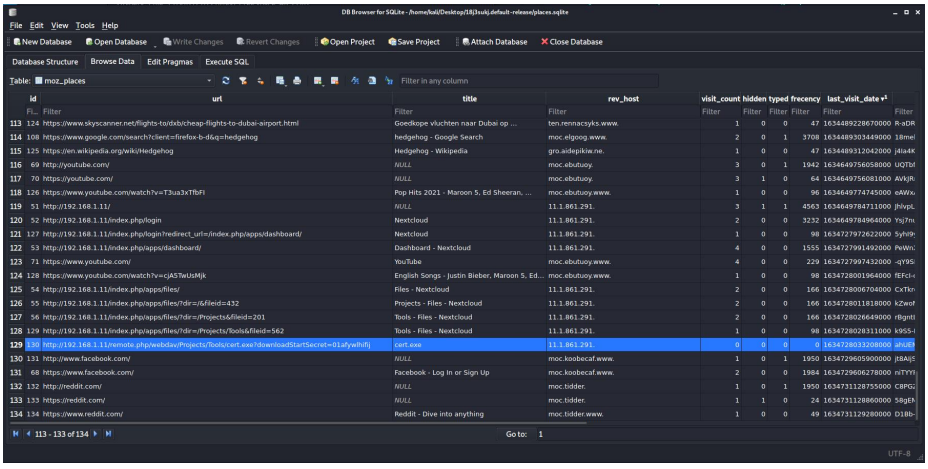
A.6.1 Artefacts



A.6.2 Downloads



A.6.3 History



A.7 NextCloud logs

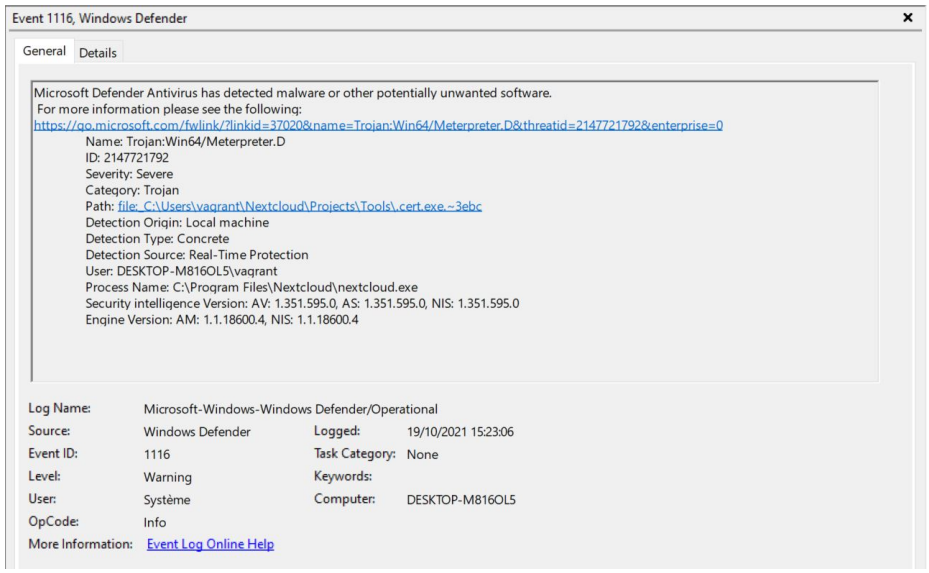
A.7.1 synchronization log

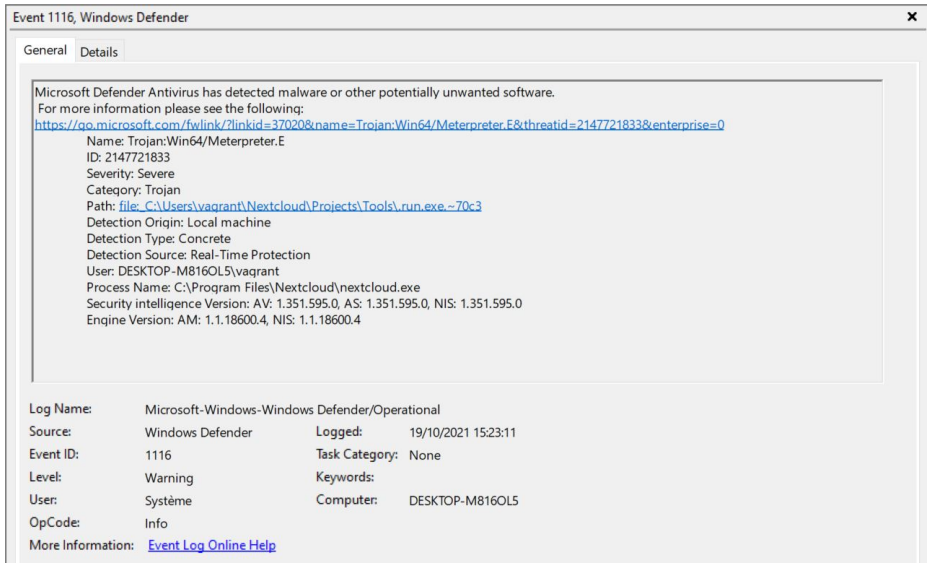
```
#=#=#=# Syncrun started 2021-10-19T13:22:55Z
#=#=#=#=# Propagation starts 2021-10-19T13:22:56Z (last step: 682 msec, total: 682 msec)
||Projects/Tools|8|2|1634641217|616ea5415cd7e|0|00000562oc2ilciw4ftj|4||0|0|0||
13:22:56||Projects/Tools/cert.exe|8|2|1634564850|abd32716fdcd898b10a1d069ae63c332|7168|00000611oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|200|0|0|903de4a8-6d2a-4b50-b08c-54bdec44c931|
13:22:56||Projects/Tools/run.exe|8|2|1634131489|ec91cd9a4d199466e4ecef4f2b47c639|7168|00000615oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|200|0|0|af984671-dc78-46c7-9877-bee18e4efd6d|
#=#=#=# Syncrun finished 2021-10-19T13:23:00Z (last step: 3667 msec, total: 4349 msec)
#=#=#=# Syncrun started 2021-10-19T13:23:03Z
#=#=#=#=# Propagation starts 2021-10-19T13:23:03Z (last step: 240 msec, total: 240 msec)
||Projects/Tools/cert.exe|8|2|1634564850|abd32716fdcd898b10a1d069ae63c332|7168|00000611oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
||Projects/Tools/run.exe|8|2|1634131489|ec91cd9a4d199466e4ecef4f2b47c639|7168|00000615oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
#=#=#=# Syncrun finished 2021-10-19T13:23:03Z (last step: 10 msec, total: 250 msec)
#=#=#=# Syncrun started 2021-10-19T13:23:05Z
#=#=#=#=# Propagation starts 2021-10-19T13:23:06Z (last step: 322 msec, total: 322 msec)
||Projects/Tools/cert.exe|8|2|1634564850|abd32716fdcd898b10a1d069ae63c332|7168|00000611oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
||Projects/Tools/run.exe|8|2|1634131489|ec91cd9a4d199466e4ecef4f2b47c639|7168|00000615oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
#=#=#=# Syncrun finished 2021-10-19T13:23:06Z (last step: 20 msec, total: 342 msec)
#=#=#=# Syncrun started 2021-10-19T13:23:08Z
#=#=#=#=# Propagation starts 2021-10-19T13:23:08Z (last step: 356 msec, total: 356 msec)
||Projects/Tools/cert.exe|8|2|1634564850|abd32716fdcd898b10a1d069ae63c332|7168|00000611oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
||Projects/Tools/run.exe|8|2|1634131489|ec91cd9a4d199466e4ecef4f2b47c639|7168|00000615oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
#=#=#=# Syncrun finished 2021-10-19T13:23:08Z (last step: 18 msec, total: 374 msec)
#=#=#=# Syncrun started 2021-10-19T13:24:30Z
#=#=#=#=# Propagation starts 2021-10-19T13:24:30Z (last step: 341 msec, total: 341 msec)
#=#=#=# Syncrun finished 2021-10-19T13:24:30Z (last step: 8 msec, total: 349 msec)
#=#=#=# Syncrun started 2021-10-19T15:24:32Z
#=#=#=#=# Propagation starts 2021-10-19T15:24:32Z (last step: 72 msec, total: 72 msec)
#=#=#=# Syncrun finished 2021-10-19T15:24:32Z (last step: 5 msec, total: 77 msec)
#=#=#=# Syncrun started 2021-10-19T17:24:32Z
#=#=#=#=# Propagation starts 2021-10-19T17:24:32Z (last step: 69 msec, total: 69 msec)
#=#=#=# Syncrun finished 2021-10-19T17:24:32Z (last step: 6 msec, total: 75 msec)
#=#=#=# Syncrun started 2021-10-19T19:24:33Z
#=#=#=#=# Propagation starts 2021-10-19T19:24:33Z (last step: 82 msec, total: 82 msec)
#=#=#=# Syncrun finished 2021-10-19T19:24:33Z (last step: 7 msec, total: 89 msec)
#=#=#=# Syncrun started 2021-10-19T21:24:33Z
#=#=#=#=# Propagation starts 2021-10-19T21:24:33Z (last step: 86 msec, total: 86 msec)
#=#=#=# Syncrun finished 2021-10-19T21:24:33Z (last step: 5 msec, total: 92 msec)
#=#=#=# Syncrun started 2021-10-19T23:24:34Z
#=#=#=#=# Propagation starts 2021-10-19T23:24:34Z (last step: 80 msec, total: 80 msec)
#=#=#=# Syncrun finished 2021-10-19T23:24:34Z (last step: 5 msec, total: 86 msec)
#=#=#=# Syncrun started 2021-10-20T01:24:34Z
#=#=#=#=# Propagation starts 2021-10-20T01:24:34Z (last step: 73 msec, total: 73 msec)
#=#=#=# Syncrun finished 2021-10-20T01:24:34Z (last step: 5 msec, total: 78 msec)
#=#=#=# Syncrun started 2021-10-20T03:24:37Z
#=#=#=#=# Propagation starts 2021-10-20T03:24:37Z (last step: 64 msec, total: 64 msec)
#=#=#=# Syncrun finished 2021-10-20T03:24:37Z (last step: 5 msec, total: 69 msec)
#=#=#=# Syncrun started 2021-10-20T05:24:41Z
#=#=#=#=# Propagation starts 2021-10-20T05:24:41Z (last step: 87 msec, total: 87 msec)
#=#=#=# Syncrun finished 2021-10-20T05:24:41Z (last step: 4 msec, total: 91 msec)
#=#=#=# Syncrun started 2021-10-20T07:24:44Z
#=#=#=#=# Propagation starts 2021-10-20T07:24:44Z (last step: 106 msec, total: 106 msec)
#=#=#=# Syncrun finished 2021-10-20T07:24:44Z (last step: 4 msec, total: 111 msec)
#=#=#=# Syncrun started 2021-10-20T09:24:47Z
#=#=#=#=# Propagation starts 2021-10-20T09:24:48Z (last step: 87 msec, total: 87 msec)
#=#=#=# Syncrun finished 2021-10-20T09:24:48Z (last step: 4 msec, total: 92 msec)
```

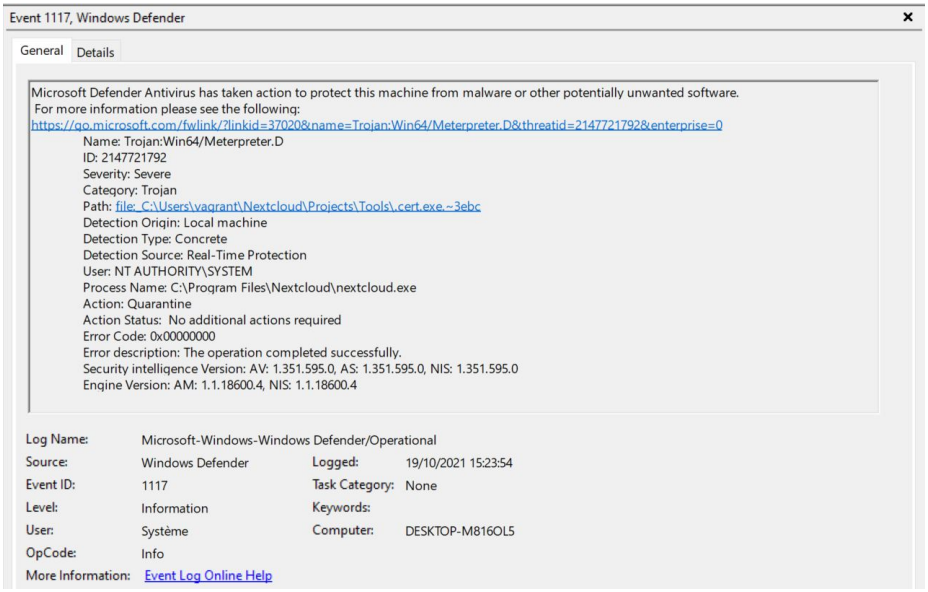
```
#=#=#=# Syncrun started 2021-10-20T10:59:23Z
#=#=#=#=# Propagation starts 2021-10-20T10:59:23Z (last step: 191 msec, total: 191 msec)
10:59:24||Projects/Tools/cert.exe|8|2|1634564850|b9484f2337f4d9b571b86d50129c0d4c|7168|00000621oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|200|0|0|d1070ff3-fe0c-4079-91ae-7dfda9fee3a4|
#=#=#=# Syncrun finished 2021-10-20T10:59:24Z (last step: 146 msec, total: 338 msec)
#=#=#=# Syncrun started 2021-10-20T10:59:26Z
#=#=#=#=# Propagation starts 2021-10-20T10:59:26Z (last step: 156 msec, total: 156 msec)
||Projects/Tools/cert.exe|8|2|1634564850|b9484f2337f4d9b571b86d50129c0d4c|7168|00000621oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
#=#=#=# Syncrun finished 2021-10-20T10:59:26Z (last step: 6 msec, total: 162 msec)
#=#=#=# Syncrun started 2021-10-20T10:59:28Z
#=#=#=#=# Propagation starts 2021-10-20T10:59:28Z (last step: 200 msec, total: 200 msec)
||Projects/Tools/cert.exe|8|2|1634564850|b9484f2337f4d9b571b86d50129c0d4c|7168|00000621oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
#=#=#=# Syncrun finished 2021-10-20T10:59:28Z (last step: 6 msec, total: 207 msec)
#=#=#=# Syncrun started 2021-10-20T10:59:30Z
#=#=#=#=# Propagation starts 2021-10-20T10:59:30Z (last step: 184 msec, total: 184 msec)
||Projects/Tools/cert.exe|8|2|1634564850|b9484f2337f4d9b571b86d50129c0d4c|7168|00000621oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|0|0|0||
#=#=#=# Syncrun finished 2021-10-20T10:59:30Z (last step: 6 msec, total: 191 msec)
#=#=#=# Syncrun started 2021-10-20T13:02:39Z
#=#=#=#=# Propagation starts 2021-10-20T13:02:40Z (last step: 1244 msec, total: 1244 msec)
13:02:40||Projects/Tools/cert.exe|8|2|1634564850|b9484f2337f4d9b571b86d50129c0d4c|7168|00000621oc2ilciw4ftj|4||200|0|0|c8e72d7f-9bfe-4f97-b9f1-fb6007eab88e|
#=#=#=# Syncrun finished 2021-10-20T13:02:40Z (last step: 431 msec, total: 1676 msec)
```

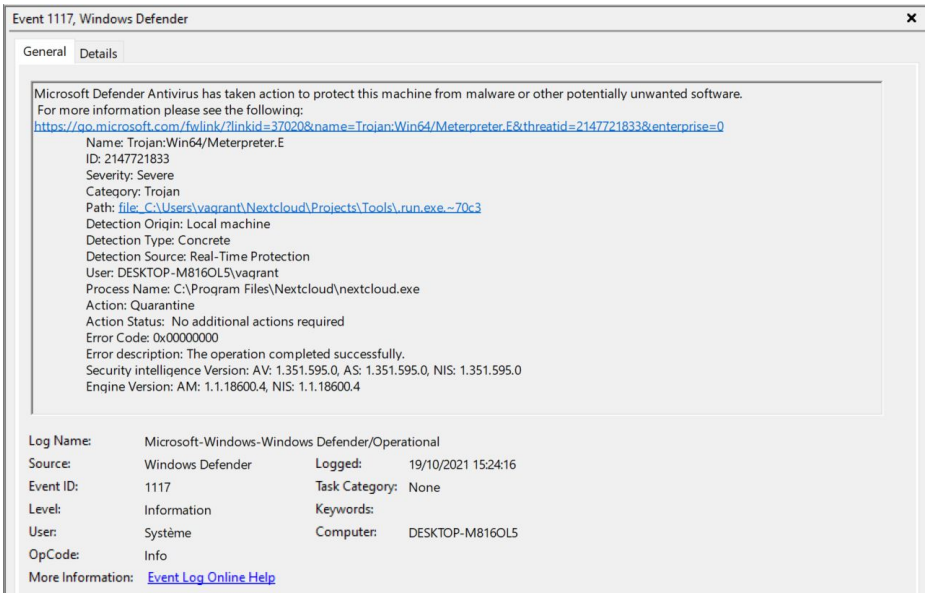
A.8 Event Logs - Windows defender logs

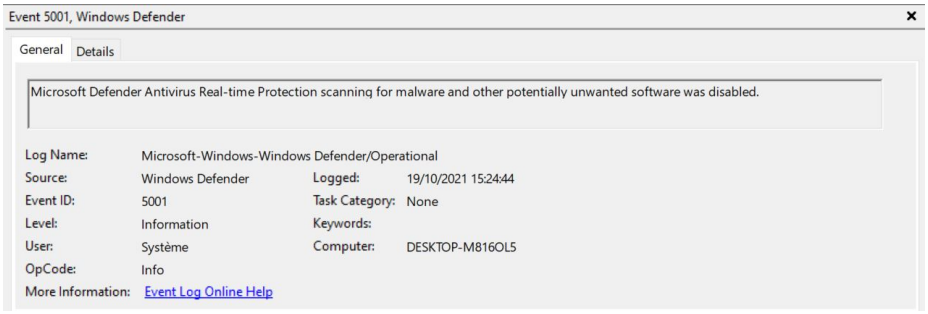
A.8.1 2021-10-19

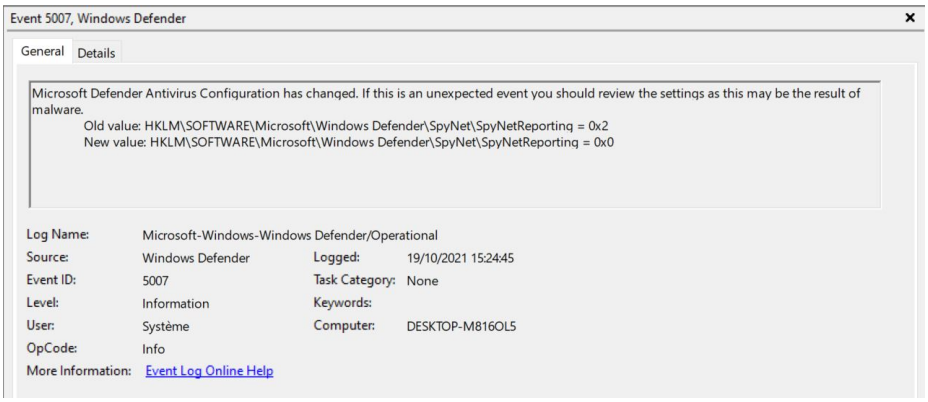


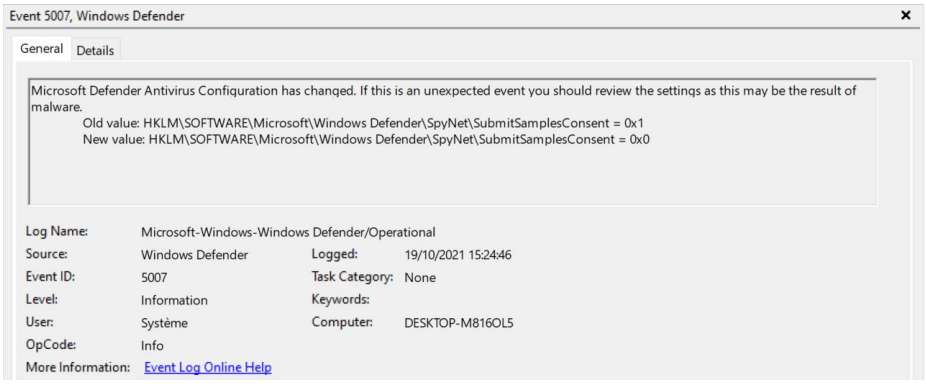


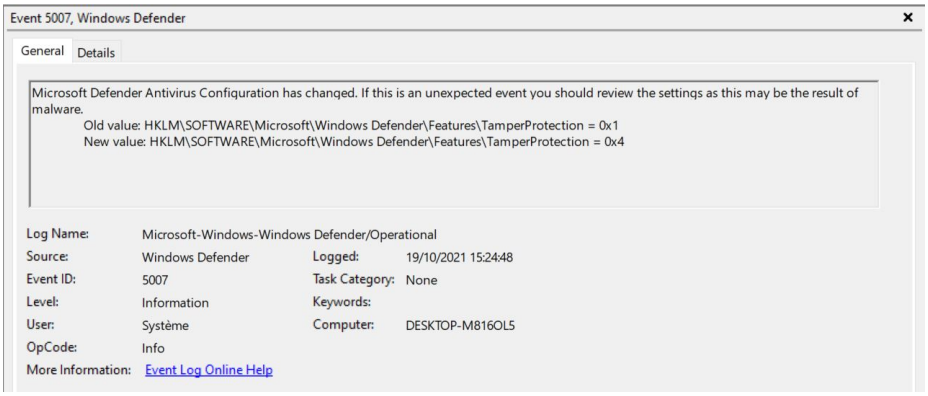

Event 1117, Windows Defender
General
Details
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.D&threatid=2147721792&enterprise=0
Name: Trojan:Win64/Meterpreter.D
ID: 2147721792
Severity: Severe
Category: Trojan
Path: file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.cert.exe.~3ebc
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
User: NT AUTHORITY\SYSTEM
Process Name: C:\Program Files\Nextcloud\nextcloud.exe
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Security intelligence Version: AV: 1.351.595.0, AS: 1.351.595.0, NIS: 1.351.595.0
Engine Version: AM: 1.1.18600.4, NIS: 1.1.18600.4
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender
Logged: 19/10/2021 15:23:54
Event ID: 1117
Task Category: None
Level: Information
Keywords:
User: Système
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help


Event 1117, Windows Defender
General
Details
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.E&threatid=2147721833&enterprise=0
Name: Trojan:Win64/Meterpreter.E
ID: 2147721833
Severity: Severe
Category: Trojan
Path: file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.run.exe.~70c3
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
User: DESKTOP-M816OL5\vagrant
Process Name: C:\Program Files\Nextcloud\nextcloud.exe
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Security intelligence Version: AV: 1.351.595.0, AS: 1.351.595.0, NIS: 1.351.595.0
Engine Version: AM: 1.1.18600.4, NIS: 1.1.18600.4
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender
Logged: 19/10/2021 15:24:16
Event ID: 1117
Task Category: None
Level: Information
Keywords:
User: Système
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help

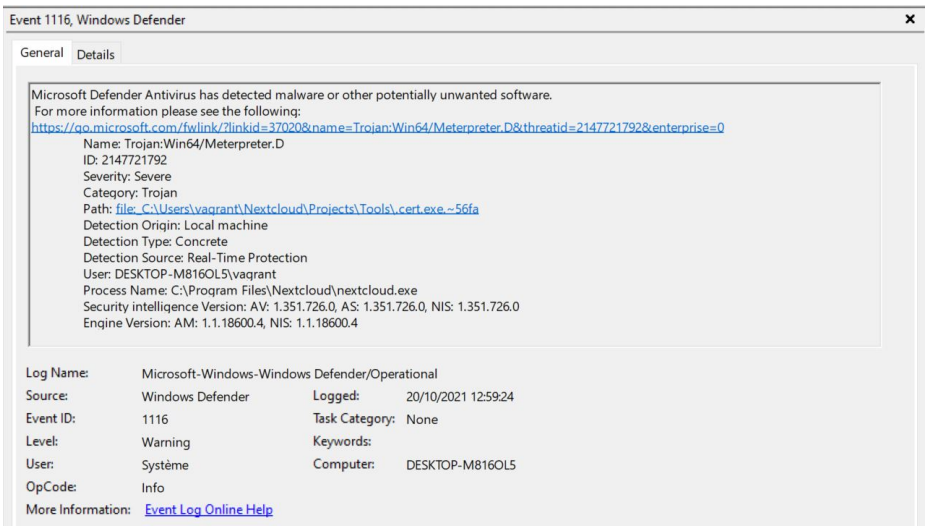

Event 5001, Windows Defender
General
Details
Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender
Logged: 19/10/2021 15:24:44
Event ID: 5001
Task Category: None
Level: Information
Keywords:
User: Système
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help

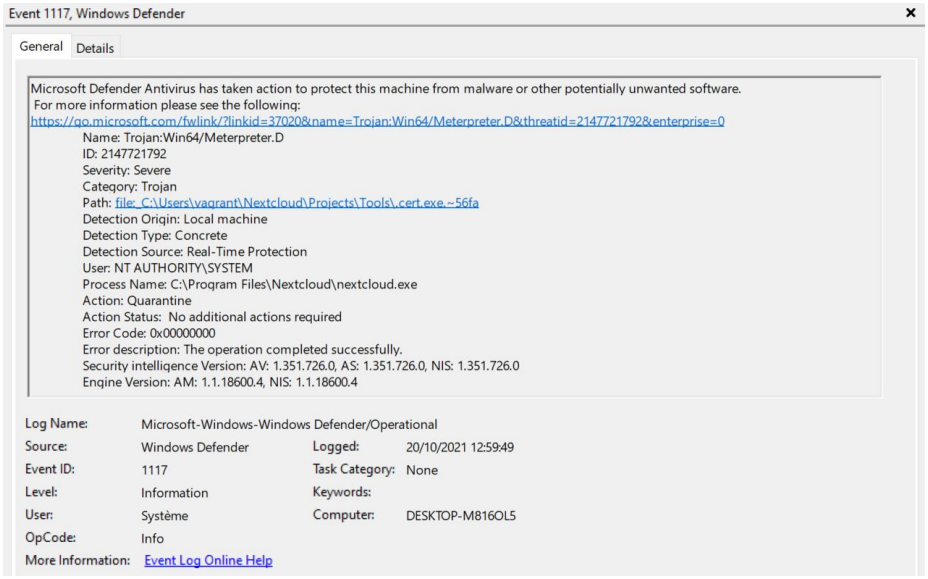


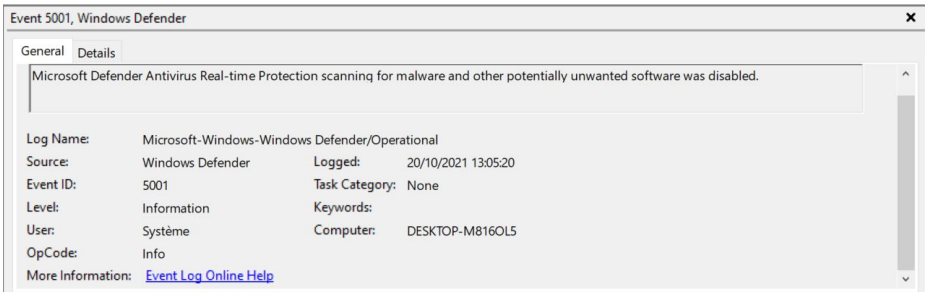


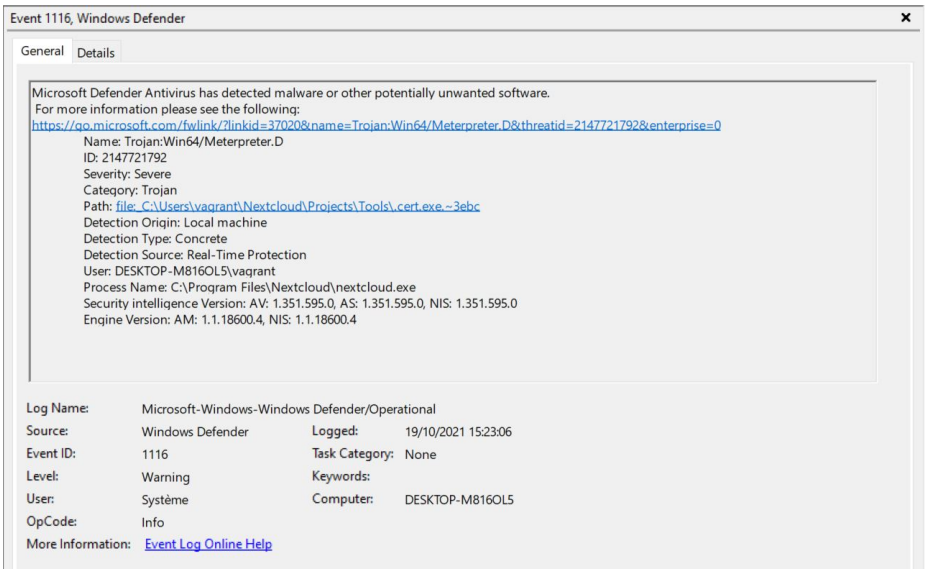


A.8.2 2021-10-20


Event 1116, Windows Defender
General
Details
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.D&threatid=2147721792&enterprise=0
Name: Trojan:Win64/Meterpreter.D
ID: 2147721792
Severity: Severe
Category: Trojan
Path: file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.cert.exe.~56fa
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
User: DESKTOP-M816OL5\vagrant
Process Name: C:\Program Files\Nextcloud\nextcloud.exe
Security intelligence Version: AV: 1.351.726.0, AS: 1.351.726.0, NIS: 1.351.726.0
Engine Version: AM: 1.1.18600.4, NIS: 1.1.18600.4
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender
Logged: 20/10/2021 12:59:24
Event ID: 1116
Task Category: None
Level: Warning
Keywords:
User: Système
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help

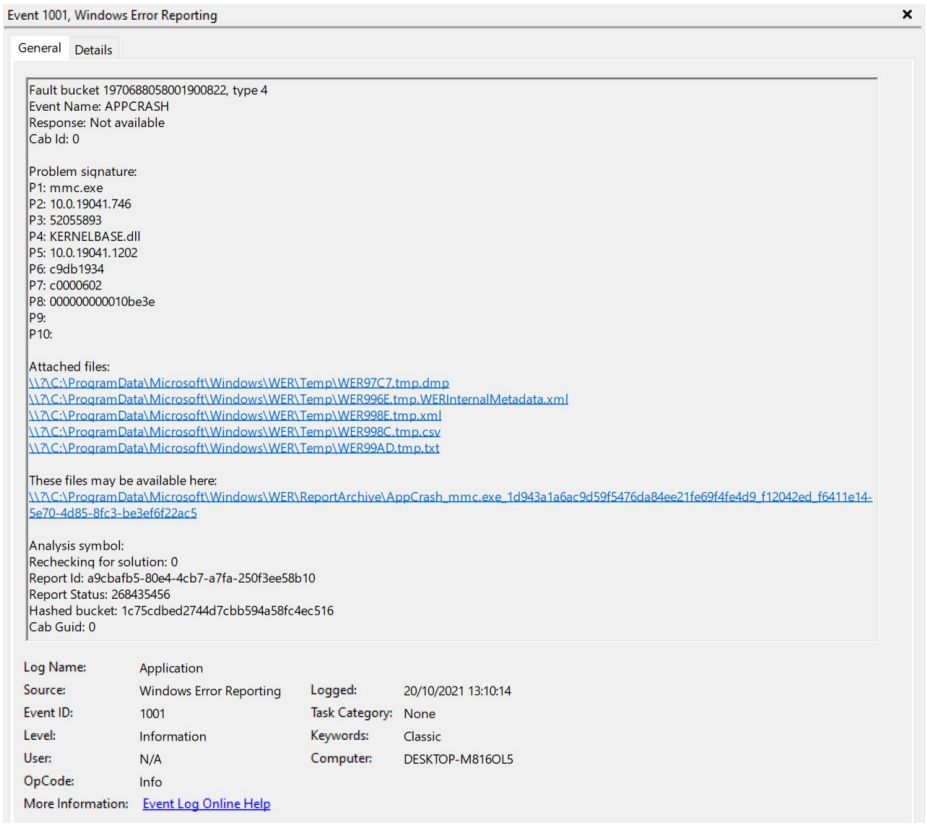

Event 1117, Windows Defender
General
Details
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.D&threatid=2147721792&enterprise=0
Name: Trojan:Win64/Meterpreter.D
ID: 2147721792
Severity: Severe
Category: Trojan
Path: file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.cert.exe.~56fa
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
User: NT AUTHORITY\SYSTEM
Process Name: C:\Program Files\Nextcloud\nextcloud.exe
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Security intelligence Version: AV: 1.351.726.0, AS: 1.351.726.0, NIS: 1.351.726.0
Engine Version: AM: 1.1.18600.4, NIS: 1.1.18600.4
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender
Logged: 20/10/2021 12:59:49
Event ID: 1117
Task Category: None
Level: Information
Keywords:
User: Système
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help


Event 5001, Windows Defender
General
Details
Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender
Logged: 20/10/2021 13:05:20
Event ID: 5001
Task Category: None
Level: Information
Keywords:
User: Système
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help



A.9 Event Logs - Application logs


Event 1000, Application Error
General
Details
Faulting application name: mmc.exe, version: 10.0.19041.746, time stamp: 0x52055893
Faulting module name: KERNELBASE.dll, version: 10.0.19041.1202, time stamp: 0xc9db1934
Exception code: 0xc0000602
Fault offset: 0x000000000010be3e
Faulting process id: 0x2294
Faulting application start time: 0x01d7c5a30d37d04e
Faulting application path: C:\Windows\system32\mmc.exe
Faulting module path: C:\Windows\System32\KERNELBASE.dll
Report Id: a9cbafb5-80e4-4cb7-a7fa-250f3ee58b10
Faulting package full name:
Faulting package-relative application ID:
Log Name: Application
Source: Application Error
Logged: 20/10/2021 13:10:13
Event ID: 1000
Task Category: Application Crashing Events
Level: Error
Keywords: Classic
User: N/A
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help


Event 1001, Windows Error Reporting
General
Details
Fault bucket 197068805800190822, type 4
Event Name: APPCRASH
Response: Not available
Cab Id: 0
Problem signature:
P1: mmc.exe
P2: 10.0.19041.746
P3: 52055893
P4: KERNELBASE.dll
P5: 10.0.19041.1202
P6: c9db1934
P7: c0000602
P8: 000000000010be3e
P9:
P10:
Attached files:
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER97C7.tmp.dmp
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER998E.tmp.xml
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER998C.tmp.csv
\\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER99AD.tmp.txt
These files may be available here:
\\?\C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_mmc.exe_1d943a1a6ac9d59f5476da84ee21fe69f4fe4d9_f12042ed_f6411e14-5e70-4d85-8fc3-be3ef6f22ac5
Analysis symbol:
Rechecking for solution: 0
Report Id: a9cbafb5-80e4-4cb7-a7fa-250f3ee58b10
Report Status: 268435456
Hashed bucket: 1c75cdbed2744d7cbb594a58fc4ec516
Cab Guid: 0
Log Name: Application
Source: Windows Error Reporting
Logged: 20/10/2021 13:10:14
Event ID: 1001
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: DESKTOP-M816OL5
OpCode: Info
More Information: Event Log Online Help

A.10 Event Logs - Security logs

A.10.1 2021-10-19 15:23:02 to 15:25:36

Security Number of events: 14 266

Level	Date and Time	Source	Even...	Task Category
Information	19/10/2021 15:25:36	Microsoft Windows security auditing.	4798	User Account Management
Information	19/10/2021 15:25:16	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:25:16	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:25:16	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:25:16	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:25:16	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:25:16	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:25:16	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:50	Microsoft Windows security auditing.	4672	Special Logon
Information	19/10/2021 15:24:50	Microsoft Windows security auditing.	4624	Logon
Information	19/10/2021 15:24:45	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:45	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:44	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:44	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:43	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:43	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:43	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:43	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:43	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:43	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:29	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:29	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:29	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:29	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:29	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:29	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:29	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:24:19	Microsoft Windows security auditing.	4798	User Account Management
Information	19/10/2021 15:23:43	Microsoft Windows security auditing.	5379	User Account Management
Information	19/10/2021 15:23:20	Microsoft Windows security auditing.	4672	Special Logon
Information	19/10/2021 15:23:20	Microsoft Windows security auditing.	4624	Logon
Information	19/10/2021 15:23:18	Microsoft Windows security auditing.	5382	User Account Management
Information	19/10/2021 15:23:18	Microsoft Windows security auditing.	5382	User Account Management
Information	19/10/2021 15:23:17	Microsoft Windows security auditing.	4672	Special Logon
Information	19/10/2021 15:23:17	Microsoft Windows security auditing.	4624	Logon
Information	19/10/2021 15:23:03	Microsoft Windows security auditing.	5381	User Account Management
Information	19/10/2021 15:23:03	Microsoft Windows security auditing.	5381	User Account Management
Information	19/10/2021 15:23:03	Microsoft Windows security auditing.	5381	User Account Management
Information	19/10/2021 15:23:02	Microsoft Windows security auditing.	5379	User Account Management

A.10.2 2021-10-20 12:57:00 to 13:08:08

Security Number of events: 14 266

Level	Date and Time	Source	Even...	Task Category
Information	20/10/2021 13:08:08	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:08:08	Microsoft Windows security auditing.	5381	User Account Management
Information	20/10/2021 13:08:08	Microsoft Windows security auditing.	5381	User Account Management
Information	20/10/2021 13:05:12	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 13:05:12	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 13:05:10	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 13:05:10	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 13:04:58	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:58	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:58	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:58	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 13:04:57	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 13:04:52	Microsoft Windows security auditing.	4616	Security State Change
Information	20/10/2021 12:59:43	Microsoft Windows security auditing.	4799	Security Group Management
Information	20/10/2021 12:59:43	Microsoft Windows security auditing.	4799	Security Group Management
Information	20/10/2021 12:59:39	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 12:59:39	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 12:58:45	Microsoft Windows security auditing.	5379	User Account Management
Information	20/10/2021 12:57:29	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 12:57:29	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 12:57:02	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 12:57:02	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 12:57:01	Microsoft Windows security auditing.	4672	Special Logon
Information	20/10/2021 12:57:01	Microsoft Windows security auditing.	4624	Logon
Information	20/10/2021 12:57:00	Microsoft Windows security auditing.	4672	Special Logon

A.11 Event Logs - System logs

Event 7045, Service Control Manager ×

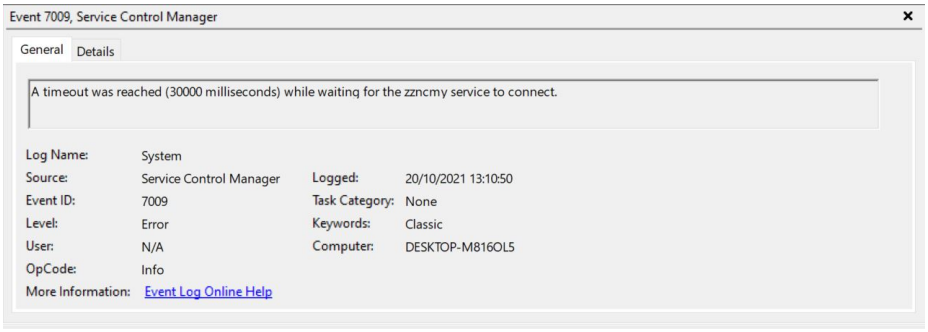
General Details

A service was installed in the system.

Service Name: zzncmy
Service File Name: cmd.exe /c echo zzncmy > \\.\pipe\zzncmy
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name:	System		
Source:	Service Control Manager	Logged:	20/10/2021 13:10:50
Event ID:	7045	Task Category:	None
Level:	Information	Keywords:	Classic
User:	S-1-5-21-26097017-1149114(	Computer:	DESKTOP-M816OL5
OpCode:	Info		
More Information:	Event Log Online Help		

A.11.1 2021-10-20 12:57:00 to 13:08:08



B Registry Forensics

B.1 SAM Hive

B.1.1 user's information

```
Username        : vagrant [1001]
Full Name       : Victoria Timmers
User Comment    :
Account Type    :
Account Created : 2021-03-17 15:53:21Z
Name            :
Password Hint   :
Reset Data        : {"version":1,"questions":[{"question":"What was your first pet's name?","answer":"batman"},{"qu
estion":"What was your childhood nickname?","answer":"batman"},{"question":"What's the first name of your oldest co
usin?","answer":"batman"}]}
Last Login Date : 2021-10-17 16:43:43Z
Pwd Reset Date  : 2021-03-17 15:53:21Z
Pwd Fail Date   : 2021-10-10 11:26:50Z
Login Count     : 28
Embedded RID    : 1001
  --> Password not required
  --> Normal user account
  --> Password does not expire
```

```
Group Name    : Administrators [2]
LastWrite     : 2021-03-17 15:53:57Z
Group Comment : Administrators have complete and unrestricted access to the computer/domain
Users :
  S-1-5-21-26097017-1149114655-3768198679-1001
  S-1-5-21-26097017-1149114655-3768198679-500
```

B.2 NTUSER.DAT Hive

B.2.1 Recent documents

```
┌──(root㉿kali)-[/mnt/windows_10/Users/vagrant]
└─# rip.pl -r NTUSER.DAT -p recentdocs
Launching recentdocs v.20200427
recentdocs v.20200427
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2021-10-20 12:50:33Z
  27 = Documents
  28 = proposal_new_project.odt
  26 = review_2020.odt
  3 = The Internet
  4 = ms-gamingoverlay:///
  64 = ?pid=71566WindowId=722070
  39 = CORSAIR (E:)
  44 = TO_DO.txt
  63 = ?pid=98246WindowId=1639534
  11 = Code
  22 = read_json_to_dictionary.py
  60 = Blue Book
  62 = bbi_ju_periodic_report_template_part_b.docx
  61 = NSFProjectReportTemplate.docx
  59 = EPB62.pdf
  18 = Apollo
  17 = new_application_procedure.pdf
  50 = large-hedgehog-photo.jpg
  58 = ?pid=95606WindowId=1574028
  57 = threat/
  5 = kglcheck/
  56 = Hedgehog - Wikipedia.htm
  55 = Goedkope vluchten naar Dubai op Skyscanner.html
  54 = about-hedgehogs.jpg
  53 = apple.jpg
  52 = shark.jpg
  51 = images.jpg
  49 = 19-09-04-erizos-mascotas.jpg
  48 = User Accounts
  47 = ::{60632754-C523-4B62-B45C-4172DA012619}
  46 = All Tasks
  45 = {63A7F0F7-6ACD-4D19-92FE-FB4BD9D35BA6}
  43 = small_ball.jpg
  42 = shark_ball.jpg
  41 = autumn_ball.jpg
  40 = spicy_ball.jpg
  38 = cute_ball.jpg
  37 = scripts.js
  32 = Drafts
  36 = flight_organisation.pdf
  35 = Dubai, 11_12 – 11_27.htm
  34 = Cheap Flights, Airline Tickets & Airfares - Find Deals on Flights at Cheapflights.com.htm
  33 = proposal_Rafiki_project.odt
  31 = prepare_for_deployment.odt
  30 = Templates
  29 = Readme.md
  13 = introduction.txt
  25 = general_notes.odt
  24 = data.json
  23 = New Text Document.txt
  21 = random_range_generator.py
  7 = random_generator.py
  20 = ?pid=2206WindowId=263304
  2 = Work
  1 = This PC
  0 = ms-gamingoverlay:///
  19 = 6.4.4_transporter_performance_rating_template.xlsx
  16 = Downloads
  15 = ?pid=16966WindowId=721584
  14 = capture.bmp
  9 = Local Disk (C:)
  8 = Tools
  12 = sdelete
  10 = C:\
  6 = SDelete.zip
```

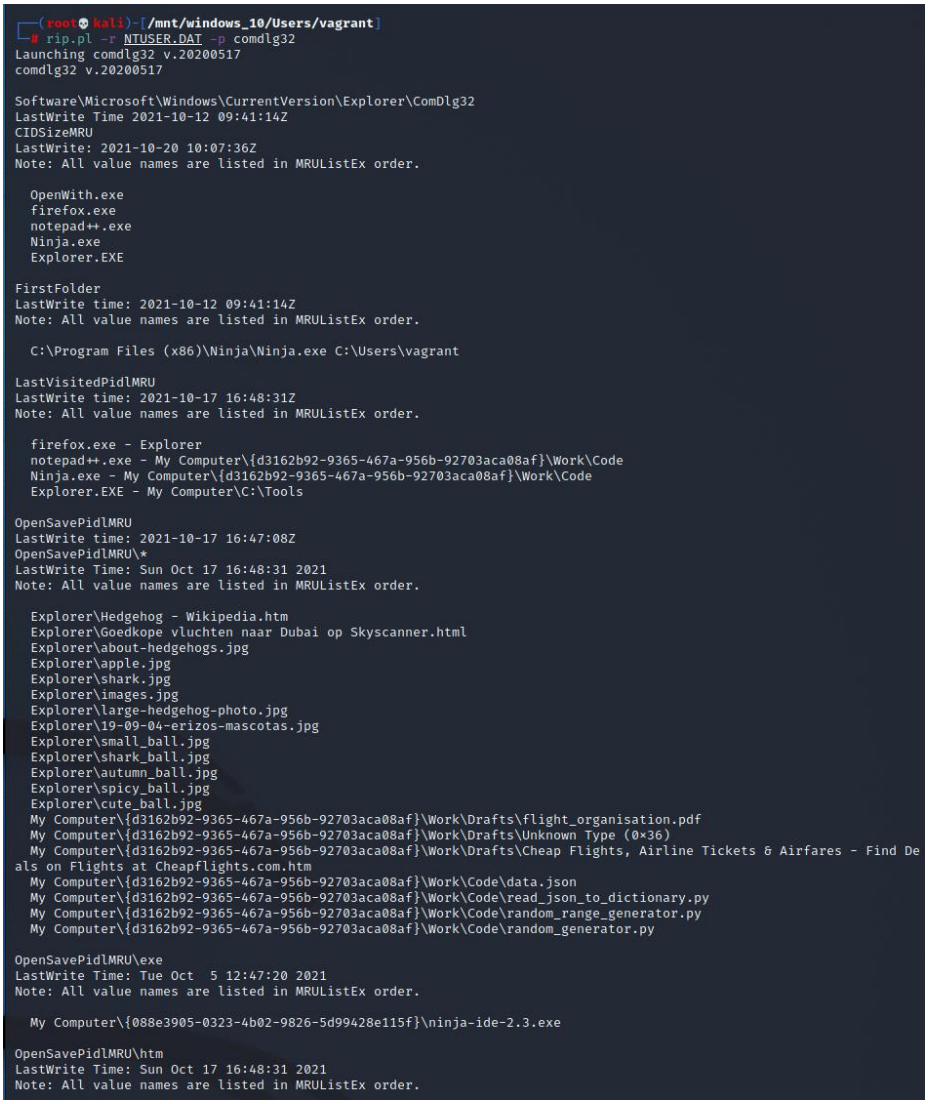
B.2.2 UserAssist Key

```
┌──(root💀kali)-[/mnt/windows_10/Users/vagrant]
└─# rip.pl -r NTUSER.DAT -p userassist
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2021-03-17 15:54:03Z

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2021-10-20 14:41:13Z
  E:\ULB_project\FTK Imager\FTK Imager.exe (1)
2021-10-20 14:23:57Z
  D78BF5DD33499EC2 (5)
2021-10-20 11:59:01Z
  TheDocumentFoundation.LibreOffice.Writer (11)
2021-10-20 11:08:09Z
  Microsoft.XboxGamingOverlay_8wekyb3d8bbwe!App (39)
2021-10-20 11:08:04Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Ninja\Ninja.exe (5)
2021-10-20 11:07:31Z
  C:\Users\vagrant\Downloads\cert.exe (1)
2021-10-20 11:07:22Z
  Microsoft.Windows.Explorer (23)
2021-10-20 10:57:40Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (11)
2021-10-19 13:35:13Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Notepad++\notepad++.exe (2)
2021-10-19 13:27:58Z
  MSEdge (16)
2021-10-19 13:26:50Z
  Microsoft.Windows.Photos_8wekyb3d8bbwe!App (2)
2021-10-19 13:23:14Z
  Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI (1)
2021-10-19 13:22:28Z
  308046B0AF4A39CB (6)
2021-10-17 16:42:39Z
  Microsoft.Windows.ControlPanel (1)
2021-10-14 07:02:09Z
  microsoft.windowscommunicationsapps_8wekyb3d8bbwe!microsoft.windowslive.mail (1)
2021-10-13 14:42:14Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (14)
2021-10-13 14:32:04Z
  C:\Users\vagrant\Desktop\license_key.bat (2)
2021-10-13 14:29:19Z
  windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel (7)
2021-10-13 10:26:12Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Nextcloud\nextcloud.exe (2)
2021-10-12 09:29:23Z
  TheDocumentFoundation.LibreOffice.Calc (1)
2021-10-05 13:28:02Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msiexec.exe (1)
2021-10-05 12:48:24Z
  C:\Users\vagrant\Downloads\ninja-ide-2.3.exe (1)
2021-09-24 09:43:34Z
  {F38BF404-1D43-42F2-9305-67DE0B28FC23}\regedit.exe (1)
2021-09-24 09:42:06Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (8)
2021-03-24 18:16:09Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\osk.exe (2)
2021-03-24 18:15:37Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\dfrgui.exe (4)
2021-03-18 13:14:03Z
  D:\VBoxWindowsAdditions.exe (1)
2021-03-17 16:04:52Z
  Microsoft.Windows.Computer (1)
2021-03-17 15:52:27Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
  Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App (13)
  Microsoft.WindowsMaps_8wekyb3d8bbwe!App (12)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (11)
  Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (9)
  Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (8)
```

```
Value names with no time stamps:
  UEME_CTLCUACount:ctor
  Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App
  Microsoft.Windows.Search_cw5n1h2txyewy!CortanaUI
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\wscript.exe
  Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy!App
  Microsoft.LockApp_cw5n1h2txyewy!WindowsDefaultLockScreen
  D:\VBoxWindowsAdditions-amd64.exe
  C:\Tools\sdelete\sdelete64.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\MusNotificationUx.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msdt.exe
  Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge
  C:\Users\vagrant\AppData\Local\Temp\7zS8A657B9E\setup-stub.exe
  C:\Users\vagrant\Downloads\Thunderbird Setup 91.1.2.exe
  C:\Users\vagrant\Downloads\npp.8.1.5.Installer.x64.exe
  Microsoft.Windows.WindowsInstaller
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\OpenWith.exe
  Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App

{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
2021-10-20 14:23:57Z
  C:\Users\Public\Desktop\Thunderbird.lnk (1)
2021-10-20 11:08:04Z
  C:\Users\vagrant\Desktop\Ninja.lnk (5)
2021-10-20 11:07:22Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\File Explorer.lnk (20)
2021-10-19 13:35:13Z
  C:\Users\Public\Desktop\Notepad++.lnk (2)
2021-10-19 13:25:10Z
  C:\Users\Public\Desktop\Mozilla Thunderbird.lnk (4)
2021-10-19 13:22:28Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Firefox.lnk (5)
2021-10-17 16:42:39Z
  {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Control Panel.lnk (1)
2021-10-14 06:29:59Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Microsoft Edge.lnk (11)
2021-10-13 10:26:12Z
  C:\Users\Public\Desktop\Nextcloud.lnk (2)
2021-10-13 10:23:36Z
  C:\Users\Public\Desktop\Firefox.lnk (1)
2021-10-13 10:23:23Z
  {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Command Prompt.lnk (10)
2021-09-24 09:43:34Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Administrative Tools\Registry Editor.lnk (1)
2021-03-24 18:16:09Z
  {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessibility\On-Screen Keyboard.lnk (2)
2021-03-24 18:15:37Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Administrative Tools\dfrgui.lnk (4)
2021-03-18 18:35:37Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Notepad.lnk (1)
2021-03-17 15:59:21Z
  C:\Users\Public\Desktop\Microsoft Edge.lnk (1)
2021-03-17 15:52:27Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (9)
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (7)

Value names with no time stamps:
  UEME_CTLCUACount:ctor

{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}
```

B.3 SOFTWARE Hive

B.3.1 OpenSaved Key



```
┌──(root💀kali)-[/mnt/windows_10/Users/vagrant]
└─# rip.pl -r NTUSER.DAT -p comdlg32
Launching comdlg32 v.20200517
comdlg32 v.20200517

Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
LastWrite Time 2021-10-12 09:41:14Z
CIDSizeMRU
LastWrite: 2021-10-20 10:07:36Z
Note: All value names are listed in MRUListEx order.

  OpenWith.exe
  firefox.exe
  notepad++.exe
  Ninja.exe
  Explorer.EXE

FirstFolder
LastWrite time: 2021-10-12 09:41:14Z
Note: All value names are listed in MRUListEx order.

  C:\Program Files (x86)\Ninja\Ninja.exe C:\Users\vagrant

LastVisitedPidlMRU
LastWrite time: 2021-10-17 16:48:31Z
Note: All value names are listed in MRUListEx order.

  firefox.exe - Explorer
  notepad++.exe - My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code
  Ninja.exe - My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code
  Explorer.EXE - My Computer\C:\Tools

OpenSavePidlMRU
LastWrite time: 2021-10-17 16:47:08Z
OpenSavePidlMRU\*
LastWrite Time: Sun Oct 17 16:48:31 2021
Note: All value names are listed in MRUListEx order.

  Explorer\Hedgehog - Wikipedia.htm
  Explorer\Goedkope vluchten naar Dubai op Skyscanner.html
  Explorer\about-hedgehogs.jpg
  Explorer\apple.jpg
  Explorer\shark.jpg
  Explorer\images.jpg
  Explorer\large-hedgehog-photo.jpg
  Explorer\19-09-04-erizos-mascotas.jpg
  Explorer\small_ball.jpg
  Explorer\shark_ball.jpg
  Explorer\autumn_ball.jpg
  Explorer\spicy_ball.jpg
  Explorer\cute_ball.jpg
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Drafts\flight_organisation.pdf
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Drafts\Unknown Type (0x36)
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Drafts\Cheap Flights, Airline Tickets & Airfares - Find De
als on Flights at Cheapflights.com.htm
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\data.json
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\read_json_to_dictionary.py
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\random_range_generator.py
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\random_generator.py

OpenSavePidlMRU\exe
LastWrite Time: Tue Oct  5 12:47:20 2021
Note: All value names are listed in MRUListEx order.

  My Computer\{088e3905-0323-4b02-9826-5d99428e115f}\ninja-ide-2.3.exe

OpenSavePidlMRU\htm
LastWrite Time: Sun Oct 17 16:48:31 2021
Note: All value names are listed in MRUListEx order.
```

```
  Explorer\Goedkope vluchten naar Dubai op Skyscanner.html

OpenSavePidlMRU\jpg
LastWrite Time: Sun Oct 17 16:45:43 2021
Note: All value names are listed in MRUListEx order.

  Explorer\about-hedgehogs.jpg
  Explorer\apple.jpg
  Explorer\shark.jpg
  Explorer\images.jpg
  Explorer\large-hedgehog-photo.jpg
  Explorer\19-09-04-erizos-mascotas.jpg
  Explorer\small_ball.jpg
  Explorer\shark_ball.jpg
  Explorer\autumn_ball.jpg
  Explorer\spicy_ball.jpg
  Explorer\cute_ball.jpg

OpenSavePidlMRU\json
LastWrite Time: Tue Oct 12 09:44:56 2021
Note: All value names are listed in MRUListEx order.

  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\data.json

OpenSavePidlMRU\pdf
LastWrite Time: Thu Oct 14 07:00:37 2021
Note: All value names are listed in MRUListEx order.

  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Drafts\flight_organisation.pdf

OpenSavePidlMRU\py
LastWrite Time: Tue Oct 12 09:44:13 2021
Note: All value names are listed in MRUListEx order.

  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\read_json_to_dictionary.py
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\random_range_generator.py
  My Computer\{d3162b92-9365-467a-956b-92703aca08af}\Work\Code\random_generator.py
```

B.4 SOFTWARE Hive

B.4.1 OS version

```
┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName             Windows 10 Enterprise
ReleaseID               2009
BuildLab                19041.vb_release.191206-1406
BuildLabEx              19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID    Enterprise
RegisteredOrganization
RegisteredOwner         vagrant
InstallDate             2021-03-17 15:43:58Z
InstallTime             2021-03-17 15:43:58Z
```

B.4.2 Network List

```
┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SOFTWARE -p networklist
Launching networklist v.20200518
Launching networklist v.20200518
(Software) Collects network info from NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
Network 3
  Key LastWrite     : 2021-10-12 08:59:03Z
  DateLastConnected: 2021-10-12 01:59:03
  DateCreated       : 2021-10-12 01:59:03
  DefaultGatewayMac: 00-00-5E-00-01-2A
  Type              : wired

Network 2
  Key LastWrite     : 2021-10-20 11:04:54Z
  DateLastConnected: 2021-10-20 13:04:54
  DateCreated       : 2021-03-18 06:34:47
  DefaultGatewayMac: E0-B9-E5-DE-50-CA
  Type              : wired

Network
  Key LastWrite     : 2021-10-13 14:42:08Z
  DateLastConnected: 2021-10-13 07:42:08
  DateCreated       : 2021-03-17 16:43:34
  DefaultGatewayMac: 52-54-00-12-35-02
  Type              : wired


Domain/IP
intra.rma.ac.be
lan
rma.ac.be
```

B.5 SYSTEM Hive

B.5.1 Computer Name

```
┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = DESKTOP-M816OL5
TCP/IP Hostname = DESKTOP-M816OL5
```

B.5.2 timezone

```
┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SYSTEM -p timezone
Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2021-10-20 10:04:49Z
  DaylightName    → @tzres.dll,-301
  StandardName    → @tzres.dll,-302
  Bias            → -60 (-1 hours)
  ActiveTimeBias  → -120 (-2 hours)
  TimeZoneKeyName→ Romance Standard Time
```

B.5.3 Network Interfaces

```
┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SYSTEM -p nic2
Launching nic2 v.20200525
nic2 v.20200525
(System) Gets NIC info from System hive

Adapter: {88b5ac91-2a3a-11eb-b696-806e6f6e6963}
LastWrite Time: 2020-11-19 07:41:09Z

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {901ee3f6-8364-4665-a31e-f868a6a10fdf}
LastWrite Time: 2021-10-20 13:49:59Z
  EnableDHCP                  1
  Domain
  NameServer
  DhcpIPAddress               192.168.1.39
  DhcpSubnetMask              255.255.255.0
  DhcpServer                  192.168.1.1
  Lease                       3600
  LeaseObtainedTime           2021-10-20 13:49:59Z
  T1                          2021-10-20 14:17:18Z
  T2                          2021-10-20 14:39:48Z
  LeaseTerminatesTime         2021-10-20 14:49:59Z
  AddressType                 0
  IsServerNapAware            0
  DhcpConnForceBroadcastFlag  0
  DhcpDomain                  lan
  DhcpNameServer              192.168.1.1
  DhcpDefaultGateway          192.168.1.1
  DhcpSubnetMaskOpt           255.255.255.0
  DhcpInterfaceOptions        üýýýýýýýÂ¨QõÿÿDESKTOP-M816OL5.lanõlanõÂ¨õÂ¨õÂ¨ÿõÿÿÿ;õ
                                                                                :õg3õ6õÂ¨5õ
  DhcpGatewayHardware         Ä¨à·åÞPÊ
  DhcpGatewayHardwareCount    1

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {f364fd2f-1d3e-426d-8358-7450d2593cd6}
LastWrite Time: 2020-11-19 07:40:57Z
  EnableDHCP                  1
  Domain
  NameServer

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.

┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SYSTEM -p networksetup2
Launching networksetup2 v.20191004
networksetup2 v.20191004
(System) Get NetworkSetup2 subkey info

Ethernet - Intel(R) PRO/1000 MT Desktop Adapter (wired)
  CurrentAddress   : 8:0:27:35:e3:3a
  PermanentAddress : 8:0:27:35:e3:3a
```

B.5.4 Shutdown

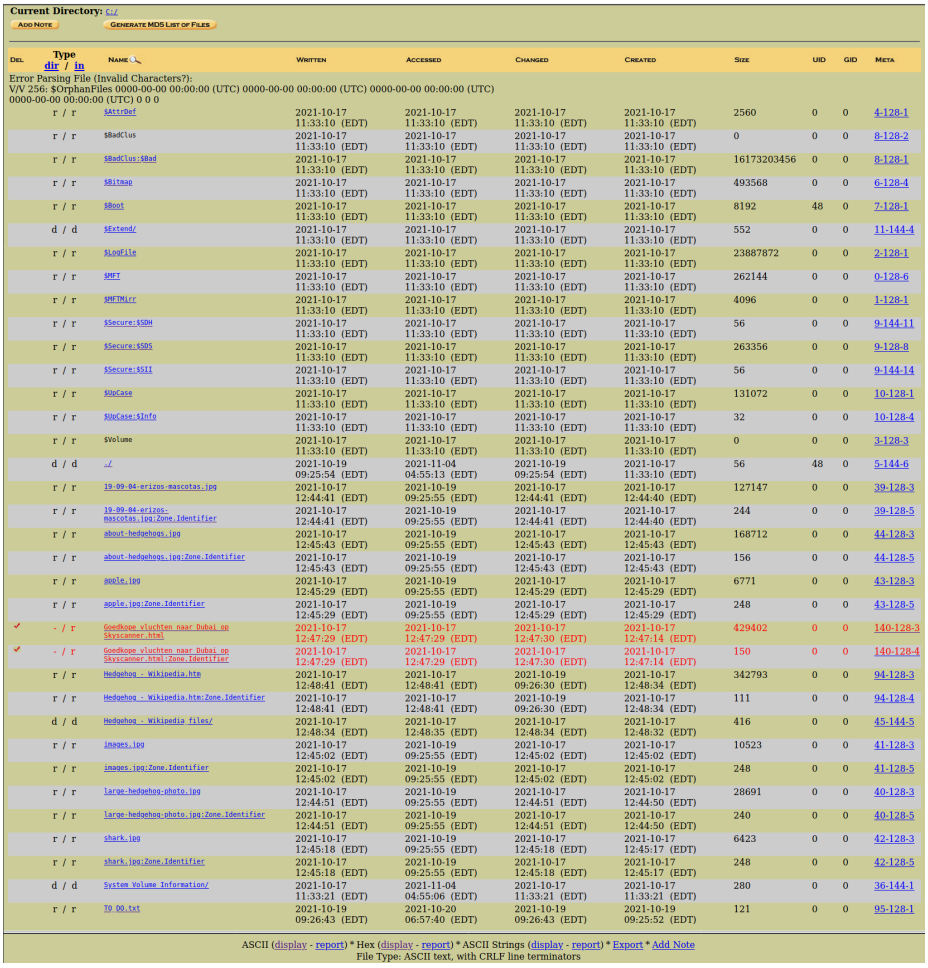
```
┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SYSTEM -p shutdown
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2021-10-17 16:43:17Z
ShutdownTime  : 2021-10-17 16:43:17Z
```

B.5.5 USB devices

```
┌──(root💀kali)-[/mnt/windows_10/Windows/System32/config]
└─# rip.pl -r SYSTEM -p usbstor
Launching usbstor v.20200515
usbstor v.20200515
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_Corsair&Prod_Flash_Voyager&Rev_0.00 [2021-10-16 18:35:40]
  S/N: 7fc594859ef57c80 [2021-10-16 18:35:40Z]
  Device Parameters LastWrite: [2021-10-16 18:35:40Z]
  Properties LastWrite       : [2021-10-16 18:35:44Z]
    FriendlyName          : Corsair Flash Voyager USB Device
    First InstallDate     : 2021-10-16 18:35:40Z
    InstallDate           : 2021-10-16 18:35:40Z
    Last Arrival          : 2021-10-20 10:57:29Z
    Last Removal          : 2021-10-20 11:01:39Z
```

C CORSAIR USB files

C.1 USB recover files



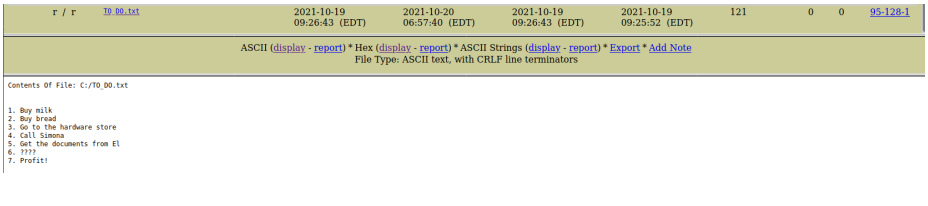
Current Directory: C:/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
Error Parsing File (Invalid Characters?): V/V 256: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0										
	r / r	$AttrDef	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2560	0	0	4-128-1
	r / r	$BadClus	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	0	0	0	8-128-2
	r / r	$BadClus:$Bad	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	16173203456	0	0	8-128-1
	r / r	$Bitmap	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	493568	0	0	6-128-4
	r / r	$Boot	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	8192	48	0	7-128-1
	d / d	$Extend/	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	552	0	0	11-144-4
	r / r	$LogFile	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	23887872	0	0	2-128-1
	r / r	$MFT	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	262144	0	0	0-128-6
	r / r	$MFTMirr	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	4096	0	0	1-128-1
	r / r	$Secure:$SDH	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	56	0	0	9-144-11
	r / r	$Secure:$SDS	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	263356	0	0	9-128-8
	r / r	$Secure:$SII	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	56	0	0	9-144-14
	r / r	$UpCase	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	131072	0	0	10-128-1
	r / r	$UpCase:$Info	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	32	0	0	10-128-4
	r / r	$Volume	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	2021-10-17 11:33:10 (EDT)	0	0	0	3-128-3
	d / d	./	2021-10-19 09:25:54 (EDT)	2021-11-04 04:55:13 (EDT)	2021-10-19 09:25:54 (EDT)	2021-10-17 11:33:10 (EDT)	56	48	0	5-144-6
	r / r	19-09-04-erizos-mascotas.jpg	2021-10-17 12:44:41 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:44:41 (EDT)	2021-10-17 12:44:40 (EDT)	127147	0	0	39-128-3
	r / r	19-09-04-erizos-mascotas.jpg:Zone.Identifier	2021-10-17 12:44:41 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:44:41 (EDT)	2021-10-17 12:44:40 (EDT)	244	0	0	39-128-5
	r / r	about-hedgehogs.jpg	2021-10-17 12:45:43 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:43 (EDT)	2021-10-17 12:45:43 (EDT)	168712	0	0	44-128-3
	r / r	about-hedgehogs.jpg:Zone.Identifier	2021-10-17 12:45:43 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:43 (EDT)	2021-10-17 12:45:43 (EDT)	156	0	0	44-128-5
	r / r	apple.jpg	2021-10-17 12:45:29 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:29 (EDT)	2021-10-17 12:45:29 (EDT)	6771	0	0	43-128-3
	r / r	apple.jpg:Zone.Identifier	2021-10-17 12:45:29 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:29 (EDT)	2021-10-17 12:45:29 (EDT)	248	0	0	43-128-5
✔	- / r	Goedkope vluchten naar Dubai op Skyscanner.html	2021-10-17 12:47:29 (EDT)	2021-10-17 12:47:29 (EDT)	2021-10-17 12:47:30 (EDT)	2021-10-17 12:47:14 (EDT)	429402	0	0	140-128-3
✔	- / r	Goedkope vluchten naar Dubai op Skyscanner.html:Zone.Identifier	2021-10-17 12:47:29 (EDT)	2021-10-17 12:47:29 (EDT)	2021-10-17 12:47:30 (EDT)	2021-10-17 12:47:14 (EDT)	150	0	0	140-128-4
	r / r	Hedgehog - Wikipedia.htm	2021-10-17 12:48:41 (EDT)	2021-10-17 12:48:41 (EDT)	2021-10-19 09:26:30 (EDT)	2021-10-17 12:48:34 (EDT)	342793	0	0	94-128-3
	r / r	Hedgehog - Wikipedia.htm:Zone.Identifier	2021-10-17 12:48:41 (EDT)	2021-10-17 12:48:41 (EDT)	2021-10-19 09:26:30 (EDT)	2021-10-17 12:48:34 (EDT)	111	0	0	94-128-4
	d / d	Hedgehog - Wikipedia files/	2021-10-17 12:48:34 (EDT)	2021-10-17 12:48:35 (EDT)	2021-10-17 12:48:34 (EDT)	2021-10-17 12:48:32 (EDT)	416	0	0	45-144-5
	r / r	images.jpg	2021-10-17 12:45:02 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:02 (EDT)	2021-10-17 12:45:02 (EDT)	10523	0	0	41-128-3
	r / r	images.jpg:Zone.Identifier	2021-10-17 12:45:02 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:02 (EDT)	2021-10-17 12:45:02 (EDT)	248	0	0	41-128-5
	r / r	large-hedgehog-photo.jpg	2021-10-17 12:44:51 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:44:51 (EDT)	2021-10-17 12:44:50 (EDT)	28691	0	0	40-128-3
	r / r	large-hedgehog-photo.jpg:Zone.Identifier	2021-10-17 12:44:51 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:44:51 (EDT)	2021-10-17 12:44:50 (EDT)	240	0	0	40-128-5
	r / r	shark.jpg	2021-10-17 12:45:18 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:18 (EDT)	2021-10-17 12:45:17 (EDT)	6423	0	0	42-128-3
	r / r	shark.jpg:Zone.Identifier	2021-10-17 12:45:18 (EDT)	2021-10-19 09:25:55 (EDT)	2021-10-17 12:45:18 (EDT)	2021-10-17 12:45:17 (EDT)	248	0	0	42-128-5
	d / d	System Volume Information/	2021-10-17 11:33:21 (EDT)	2021-11-04 04:55:06 (EDT)	2021-10-17 11:33:21 (EDT)	2021-10-17 11:33:21 (EDT)	280	0	0	36-144-1
	r / r	TO_DO.txt	2021-10-19 09:26:43 (EDT)	2021-10-20 06:57:40 (EDT)	2021-10-19 09:26:43 (EDT)	2021-10-19 09:25:52 (EDT)	121	0	0	95-128-1

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: ASCII text, with CRLF line terminators

C.2 TO_DO.txt



	r / r	TO_DO.txt	2021-10-19 09:26:43 (EDT)	2021-10-20 06:57:40 (EDT)	2021-10-19 09:26:43 (EDT)	2021-10-19 09:25:52 (EDT)	121	0	0	95-128-1

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: ASCII text, with CRLF line terminators

Contents Of File: C:/TO_DO.txt

1. Buy milk
2. Buy bread
3. Go to the hardware store
4. Call Simona
5. Get the documents from El
6. ????
7. Profit!

D Memory Forensics

D.1 Profile

```
┌──(root💀kali)-[/home/kali/Desktop/memory]
└─# vol.py -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_19041
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/memory/memdump.mem)
                      PAE type : No PAE
                           DTB : 0x1aa002L
                          KDBG : 0xf8012c000b20L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80127daf000L
             KUSER_SHARED_DATA : 0xffffff78000000000L
           Image date and time : 2021-10-20 14:45:59 UTC+0000
     Image local date and time : 2021-10-20 16:45:59 +0200
```

D.2 pslist

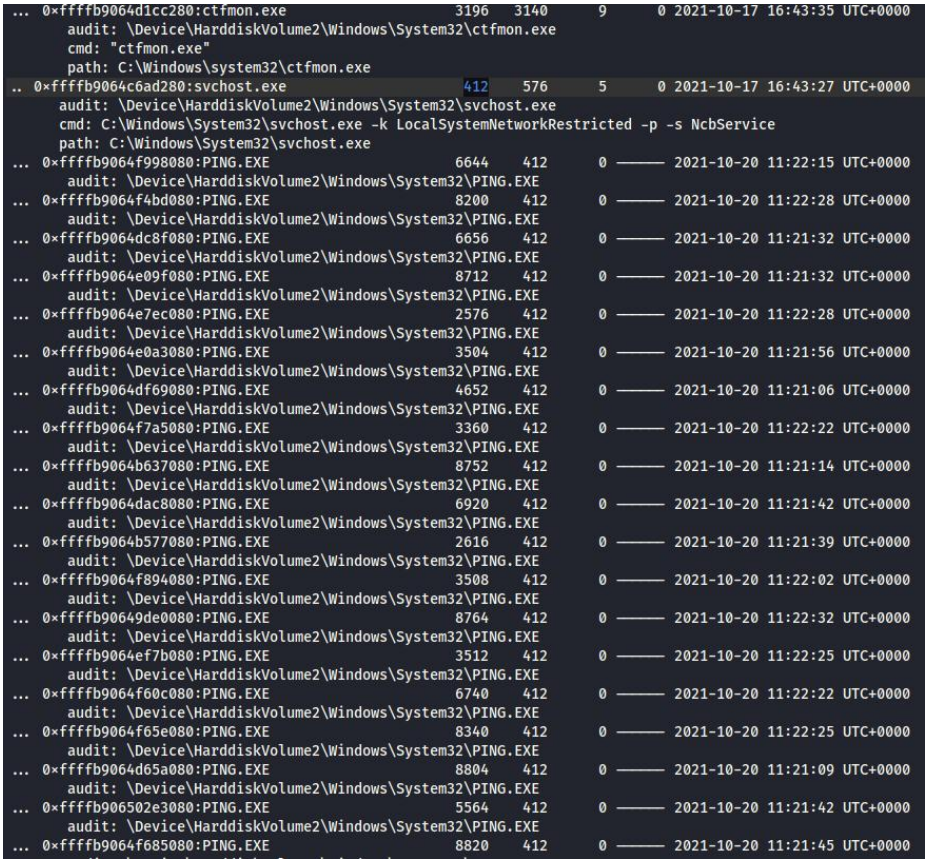
130	0xffffb9064df83080	SystemSettings	940	728	20	0	1	0	2021-10-20 10:09:19 UTC+0000	
131	0xffffb9064d6b2300	svchost.exe	5664	576	3	0	0	0	2021-10-20 11:04:55 UTC+0000	
132	0xffffb9064d709080	SecHealthUI.ex	8396	728	33	0	1	0	2021-10-20 11:05:09 UTC+0000	
133	0xffffb9064f1e7080	SecurityHealth	936	728	1	0	1	0	2021-10-20 11:05:09 UTC+0000	
134	0xffffb90649e31080	SecurityHealth	3968	728	1	0	1	0	2021-10-20 11:05:19 UTC+0000	
135	0xffffb9064b53e080	whoami.exe	6776	2548	0	————	1	0	2021-10-20 11:10:11 UTC+0000	2021-10-20 11:10:11 UTC+0000
136	0xffffb9064d7f8080	whoami.exe	5112	5644	0	————	1	0	2021-10-20 11:10:11 UTC+0000	2021-10-20 11:10:11 UTC+0000
137	0xffffb90649a4b2c0	svchost.exe	9796	576	2	0	0	0	2021-10-20 11:14:42 UTC+0000	
138	0xffffb906499c02c0	PING.EXE	252	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:06 UTC+0000
139	0xffffb9064df69080	PING.EXE	4652	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
140	0xffffb9064d2832c0	PING.EXE	4988	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
141	0xffffb90649a45080	PING.EXE	7252	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
142	0xffffb9064ce1f080	PING.EXE	5288	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
143	0xffffb9064ef91080	PING.EXE	5736	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
144	0xffffb9064e74d080	PING.EXE	6428	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
145	0xffffb9064df85080	PING.EXE	7740	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
146	0xffffb9064e5d4080	PING.EXE	8376	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
147	0xffffb90649dce080	PING.EXE	3488	412	0	————	0	0	2021-10-20 11:21:06 UTC+0000	2021-10-20 11:21:09 UTC+0000
148	0xffffb9064f7860c0	PING.EXE	7424	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:12 UTC+0000
149	0xffffb9064f679080	PING.EXE	5608	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:12 UTC+0000
150	0xffffb9064f6090c0	PING.EXE	7440	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:09 UTC+0000
151	0xffffb9064d27f080	PING.EXE	6960	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:12 UTC+0000
152	0xffffb9064d9e4080	PING.EXE	9604	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:12 UTC+0000
153	0xffffb9064b2dd080	PING.EXE	6332	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:12 UTC+0000
154	0xffffb9064f4c1080	PING.EXE	688	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:09 UTC+0000
155	0xffffb9064d9c3080	PING.EXE	7804	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:12 UTC+0000
156	0xffffb90649be4080	PING.EXE	9292	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:13 UTC+0000
157	0xffffb9064d65a080	PING.EXE	8804	412	0	————	0	0	2021-10-20 11:21:09 UTC+0000	2021-10-20 11:21:12 UTC+0000
158	0xffffb9064e05d080	PING.EXE	9808	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
159	0xffffb9064d8c7080	PING.EXE	9564	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:18 UTC+0000
160	0xffffb9064b637080	PING.EXE	8752	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
161	0xffffb9064b1f6080	PING.EXE	6328	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
162	0xffffb9064cd5f080	PING.EXE	2536	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
163	0xffffb9064dce4080	PING.EXE	5796	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
164	0xffffb9064d7ee080	PING.EXE	5764	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
165	0xffffb9064b580080	PING.EXE	7900	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
166	0xffffb9064c6a4080	PING.EXE	6964	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
167	0xffffb90649a42080	PING.EXE	10000	412	0	————	0	0	2021-10-20 11:21:14 UTC+0000	2021-10-20 11:21:17 UTC+0000
168	0xffffb9064d77e080	PING.EXE	8848	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:21 UTC+0000
169	0xffffb9064d42e080	PING.EXE	6540	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
170	0xffffb9064f548080	PING.EXE	3612	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
171	0xffffb9064f958080	PING.EXE	8968	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
172	0xffffb9064b2f0080	PING.EXE	9688	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
173	0xffffb9064d4d2080	PING.EXE	220	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
174	0xffffb9064d5de080	PING.EXE	6040	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
175	0xffffb9064d33e080	PING.EXE	6216	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:19 UTC+0000
176	0xffffb9064dab5080	PING.EXE	9836	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
177	0xffffb9064df95080	PING.EXE	9516	412	0	————	0	0	2021-10-20 11:21:19 UTC+0000	2021-10-20 11:21:22 UTC+0000
178	0xffffb9064e749080	PING.EXE	7840	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:22 UTC+0000
179	0xffffb9064cd6a080	PING.EXE	8524	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
180	0xffffb9064b5f2080	PING.EXE	3132	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
181	0xffffb9064e08c080	PING.EXE	5256	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
182	0xffffb9064df47080	PING.EXE	5436	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
183	0xffffb90649d64080	PING.EXE	1948	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
184	0xffffb9064f662080	PING.EXE	1208	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
185	0xffffb9064f603080	PING.EXE	9060	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
186	0xffffb9064b578080	PING.EXE	7140	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
187	0xffffb90649dcc080	PING.EXE	3724	412	0	————	0	0	2021-10-20 11:21:22 UTC+0000	2021-10-20 11:21:25 UTC+0000
188	0xffffb9064ce15080	PING.EXE	912	412	0	————	0	0	2021-10-20 11:21:26 UTC+0000	2021-10-20 11:21:29 UTC+0000
189	0xffffb9064b072080	PING.EXE	9224	412	0	————	0	0	2021-10-20 11:21:26 UTC+0000	2021-10-20 11:21:29 UTC+0000
190	0xffffb9064f492080	PING.EXE	9520	412	0	————	0	0	2021-10-20 11:21:26 UTC+0000	2021-10-20 11:21:28 UTC+0000

```
376 0×ffffb9064f65e080 PING.EXE              8340    412      0 ──────       0      0 2021-10-20 11:22:25 UTC+0000   2021-10-20 11:22:28 UTC+0000
377 0×ffffb9064f65c080 PING.EXE              5572    412      0 ──────       0      0 2021-10-20 11:22:25 UTC+0000   2021-10-20 11:22:28 UTC+0000
378 0×ffffb906507e3080 PING.EXE              2140    412      0 ──────       0      0 2021-10-20 11:22:28 UTC+0000   2021-10-20 11:22:31 UTC+0000
379 0×ffffb9064e7ec080 PING.EXE              2576    412      0 ──────       0      0 2021-10-20 11:22:28 UTC+0000   2021-10-20 11:22:31 UTC+0000
380 0×ffffb90649ddf080 PING.EXE              7052    412      0 ──────       0      0 2021-10-20 11:22:28 UTC+0000   2021-10-20 11:22:31 UTC+0000
381 0×ffffb90649b20080 PING.EXE              5592    412      0 ──────       0      0 2021-10-20 11:22:28 UTC+0000   2021-10-20 11:22:31 UTC+0000
382 0×ffffb9064ce65080 PING.EXE              5016    412      0 ──────       0      0 2021-10-20 11:22:28 UTC+0000   2021-10-20 11:22:31 UTC+0000
383 0×ffffb9064f4bd080 PING.EXE              8200    412      0 ──────       0      0 2021-10-20 11:22:28 UTC+0000   2021-10-20 11:22:31 UTC+0000
384 0×ffffb9064f9b9080 PING.EXE              6624    412      0 ──────       0      0 2021-10-20 11:22:29 UTC+0000   2021-10-20 11:22:31 UTC+0000
385 0×ffffb9064f9bb080 PING.EXE              6592    412      0 ──────       0      0 2021-10-20 11:22:29 UTC+0000   2021-10-20 11:22:31 UTC+0000
386 0×ffffb9064e9ec080 PING.EXE               216    412      0 ──────       0      0 2021-10-20 11:22:29 UTC+0000   2021-10-20 11:22:31 UTC+0000
387 0×ffffb9064e7ed080 PING.EXE              2392    412      0 ──────       0      0 2021-10-20 11:22:29 UTC+0000   2021-10-20 11:22:31 UTC+0000
388 0×ffffb9064ce66080 PING.EXE              7676    412      0 ──────       0      0 2021-10-20 11:22:32 UTC+0000   2021-10-20 11:22:34 UTC+0000
389 0×ffffb9064e9ee080 PING.EXE              6388    412      0 ──────       0      0 2021-10-20 11:22:32 UTC+0000   2021-10-20 11:22:35 UTC+0000
390 0×ffffb9064e7eb080 PING.EXE              1784    412      0 ──────       0      0 2021-10-20 11:22:32 UTC+0000   2021-10-20 11:22:34 UTC+0000
391 0×ffffb9064dde5080 PING.EXE              8860    412      0 ──────       0      0 2021-10-20 11:22:32 UTC+0000   2021-10-20 11:22:34 UTC+0000
392 0×ffffb90649de0080 PING.EXE              8764    412      0 ──────       0      0 2021-10-20 11:22:32 UTC+0000   2021-10-20 11:22:34 UTC+0000
393 0×ffffb9064ebe0200 PING.EXE              3676    412      0 ──────       0      0 2021-10-20 11:22:32 UTC+0000   2021-10-20 11:22:34 UTC+0000
394 0×ffffb9064f4a60c0 thunderbird.ex        7556   3448      0 ──────       1      0 2021-10-20 14:23:57 UTC+0000   2021-10-20 14:39:51 UTC+0000
395 0×ffffb9064f7bc0c0 svchost.exe           6912    576      9       0      0      0 2021-10-20 14:33:49 UTC+0000
396 0×ffffb9064d06c340 WUDFHost.exe          6108    576      7       0      0      0 2021-10-20 14:40:56 UTC+0000
397 0×ffffb9064f4f9080 smartscreen.ex        1388    728      7       0      1      0 2021-10-20 14:41:13 UTC+0000
398 0×ffffb9064b1f5340 FTK Imager.exe        4076   3448     19       0      1      1 2021-10-20 14:41:16 UTC+0000
399
```

D.3 psxview

```
 75 0×0000000011884c240 svchost.exe           1564 True   True   False    False  True  True    False
 76 0×0000000004999f080 svchost.exe           3868 True   False  True     False  True  True    False
 77 0×000000002f6552c0 svchost.exe            2300 True   True   False    False  True  True    False
 78 0×0000000075ecb080 YourPhone.exe          9504 True   True   True     False  True  True    False
 79 0×000000001eea3080 svchost.exe            1188 True   False  True     False  True  True    False
 80 0×0000000037dad340 WUDFHost.exe           6108 True   True   True     False  True  True    False
 81 0×0000000022f0c542 ??▒▒???                   0 False  False  False    False  True  False   False
 82 0×000000011cb04080 ApplicationFra         2952 True   True   True     False  True  True    False
 83 0×0000000106646080 svchost.exe            9328 True   True   True     False  True  True    False
 84 0×0000000084c88080 RuntimeBroker.         2816 True   False  True     False  True  True    False
 85 0×000000002f677240 svchost.exe            2440 True   False  False    False  True  True    False
 86 0×00000000210fd300 fontdrvhost.ex          712 True   True   False    False  True  True    False
 87 0×000000002014a080 svchost.exe            1548 True   False  True     False  True  True    False
 88 0×0000000005932b080 RuntimeBroker.        5008 True   True   False    False  True  True    False
 89 0×0000000049c3b562 ???xK?                    0 False  False  False    False  True  False   False
 90 0×00000000d60c4080 fodhelper.exe          6784 True   False  False    False  True  True    False
 91 0×000000006c9ce080 TextInputHost.         6376 True   True   True     False  True  True    False
 92 0×0000000013caf080 Microsoft.Phot         2864 True   False  True     False  True  True    False
 93 0×0000000022d45240 svchost.exe             864 True   True   True     False  True  True    False
 94 0×0000000040094080 svchost.exe            3320 True   True   True     False  True  True    False
 95 0×000000007f113080 RuntimeBroker.         7716 True   True   False    False  True  True    False
 96 0×000000001cd91080 lsass.exe               584 True   True   True     False  True  True    False
 97 0×000000002d1d6080 svchost.exe            2324 True   True   True     False  True  True    False
 98 0×0000000033233a0c0 HxOutlook.exe         4304 True   True   True     False  True  True    False
 99 0×0000000071179080 svchost.exe            2180 True   False  False    False  True  True    False
100 0×0000000015acc240 spoolsv.exe            1356 True   True   True     False  True  True    False
101 0×0000000024ca5280 svchost.exe             412 True   True   True     False  True  True    False
102 0×0000000024e5f300 svchost.exe             504 True   True   True     False  True  True    False
103 0×000000002f68c340 MsMpEng.exe           2344 True   True   True     False  True  True    False
104 0×000000006f11c080 VBoxTray.exe          4840 True   True   True     False  True  True    False
105 0×000000010f77d080 svchost.exe           3476 True   True   True     False  True  True    False
106 0×0000000400de080 explorer.exe           3448 True   False  True     False  True  True    False
107 0×0000000021001080 fontdrvhost.ex         720 True   False  True     False  True  True    False
108 0×000000010664b2c0 svchost.exe           9796 True   True   False    False  True  True    False
109 0×00000000249d1240 svchost.exe           1124 True   True   False    False  True  True    False
110 0×000000006f11b080 TrustedInstall        3632 True   False  True     False  True  True    False
111 0×000000002be05080 svchost.exe           1892 True   False  False    False  True  True    False
112 0×000000006c89d080 SecurityHealth        4572 True   False  False    False  True  True    False
113 0×0000000102b78240 svchost.exe           9840 True   False  False    False  True  True    False
114 0×000000002d8c80c0 svchost.exe           1700 True   True   False    False  True  True    False
115 0×000000008744b080 TiWorker.exe          6484 True   False  True     False  True  True    False
116 0×000000004cd23080 OneDrive.exe          5176 True   True   True     False  True  True    False
117 0×000000009c92c080 svchost.exe           7108 True   True   False    False  True  True    False
118 0×00000000d366e080 dllhost.exe           6120 True   True   True     False  True  True    False
119 0×000000011ca4f080 WinStore.App.e         708 True   True   True     False  True  True    False
120 0×0000000112574340 MoUsoCoreWorke        6936 True   False  True     False  True  True    False
121 0×000000006c99c280 SecurityHealth        2848 True   False  True     False  True  True    False
122 0×00000000693f2080 taskhostw.exe         7688 True   True   True     False  True  True    False
123 0×000000001056e9280 svchost.exe          5264 True   True   True     False  True  True    False
124 0×000000011ca8f080 RuntimeBroker.        1576 True   True   True     False  True  True    False
125 0×0000000003b0ed18                         11 False  False  False    False  False False   True
126 0×00000001054c2080 PING.EXE              10016 True   False  False    False  False True    False   2021-10-20 11:21:31 UTC+0000
127 0×000000009134f080 PING.EXE              4452 True   False  False    False  False True    False   2021-10-20 11:21:45 UTC+0000
128 0×0000000027799080 PING.EXE              8512 True   False  False    False  False True    False   2021-10-20 11:21:58 UTC+0000
129 0×00000000665f7080 PING.EXE              9604 True   True   False    False  False True    False   2021-10-20 11:21:12 UTC+0000
130 0×00000000366fa080 PING.EXE               912 True   False  False    False  False True    False   2021-10-20 11:21:29 UTC+0000
131 0×00000001047bc080 PING.EXE              8592 True   False  False    False  False True    False   2021-10-20 11:21:28 UTC+0000
132 0×00000000d0fff080 PING.EXE              3508 True   True   False    False  False True    False   2021-10-20 11:22:05 UTC+0000
133 0×0000000102bdf080 PING.EXE              7052 True   False  False    False  False True    False   2021-10-20 11:22:31 UTC+0000
134 0×0000000009140080 PING.EXE              6624 True   True   False    False  False True    False   2021-10-20 11:22:31 UTC+0000
135 0×0000000008ea1080 PING.EXE              9440 True   False  False    False  False True    False   2021-10-20 11:21:48 UTC+0000
136 0×000000011b755040 Registry                72 True   True   True     False  False False   False
137 0×000000010f6d2080 PING.EXE              10160 True   False  False    False  False True    False   2021-10-20 11:22:24 UTC+0000
```

D.4 pstree



```
... 0×ffffb9064d1cc280:ctfmon.exe                    3196   3140      9      0 2021-10-17 16:43:35 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\ctfmon.exe
      cmd: "ctfmon.exe"
      path: C:\Windows\system32\ctfmon.exe
.. 0×ffffb9064c6ad280:svchost.exe                    412    576      5      0 2021-10-17 16:43:27 UTC+0000
     audit: \Device\HarddiskVolume2\Windows\System32\svchost.exe
     cmd: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
     path: C:\Windows\System32\svchost.exe
... 0×ffffb9064f998080:PING.EXE                      6644    412      0 ------ 2021-10-20 11:22:15 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064f4bd080:PING.EXE                      8200    412      0 ------ 2021-10-20 11:22:28 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064dc8f080:PING.EXE                      6656    412      0 ------ 2021-10-20 11:21:32 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064e09f080:PING.EXE                      8712    412      0 ------ 2021-10-20 11:21:32 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064e7ec080:PING.EXE                      2576    412      0 ------ 2021-10-20 11:22:28 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064e0a3080:PING.EXE                      3504    412      0 ------ 2021-10-20 11:21:56 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064df69080:PING.EXE                      4652    412      0 ------ 2021-10-20 11:21:06 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064f7a5080:PING.EXE                      3360    412      0 ------ 2021-10-20 11:22:22 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064b637080:PING.EXE                      8752    412      0 ------ 2021-10-20 11:21:14 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064dac8080:PING.EXE                      6920    412      0 ------ 2021-10-20 11:21:42 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064b577080:PING.EXE                      2616    412      0 ------ 2021-10-20 11:21:39 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064f894080:PING.EXE                      3508    412      0 ------ 2021-10-20 11:22:02 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb90649de0080:PING.EXE                      8764    412      0 ------ 2021-10-20 11:22:32 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064ef7b080:PING.EXE                      3512    412      0 ------ 2021-10-20 11:22:25 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064f60c080:PING.EXE                      6740    412      0 ------ 2021-10-20 11:22:22 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064f65e080:PING.EXE                      8340    412      0 ------ 2021-10-20 11:22:25 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064d65a080:PING.EXE                      8804    412      0 ------ 2021-10-20 11:21:09 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb906502e3080:PING.EXE                      5564    412      0 ------ 2021-10-20 11:21:42 UTC+0000
      audit: \Device\HarddiskVolume2\Windows\System32\PING.EXE
... 0×ffffb9064f685080:PING.EXE                      8820    412      0 ------ 2021-10-20 11:21:45 UTC+0000
```