Toan c Ngo
Date:4/24/24

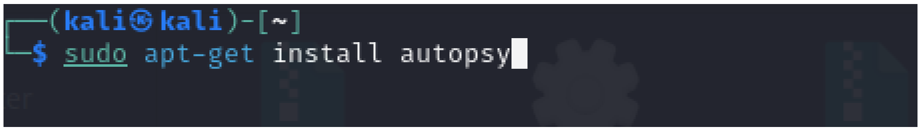
Lab 12 and 14

In this week's lab report, we will cover two chapters, one how do you set up a digital autopsy platform on a linux machine and what can it do on it, and second we will take a look at network forensics and what you can do in it. However, first we need to get a base understanding on what is autopsy and what are network forensic involving.

What is an autopsy in a normal sense ? In criminal investigation, an autopsy is an investigation technique that examines the body to determine the cause of death and to gather any other information related to what happened to the body when it was alive and related to the case. In digital forensic autopsy basically functions the same way, however with the difference being a change to examining the body to examining a file and instead of examining for the cause of death, you examine for cyber crime that has been committed using a computer and gathering all the relative information for that crime.

What is network forensic ? network forensic deals with monitors and examines the network connection, and its potential illegal connections. Network forensic also centralized around on the discovery and retrieval all the related information of a crime that happened on the network environment, and the some of the common technique that use in this field are capture, recording, and tracking packet event that occur on a network in order to establish where is the source of the attack are coming from. You can think of network forensic as tracing where the bad network is coming from before it connects to your machine.

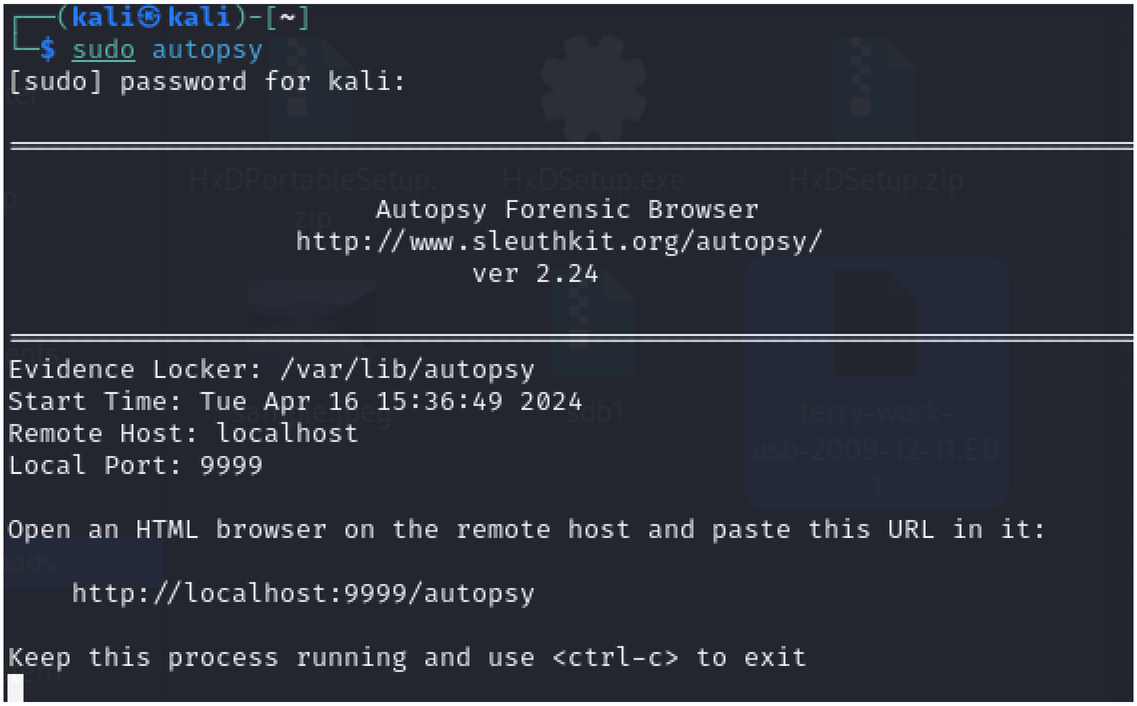
First lets see how to set up autopsy on linux



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install autopsy
```

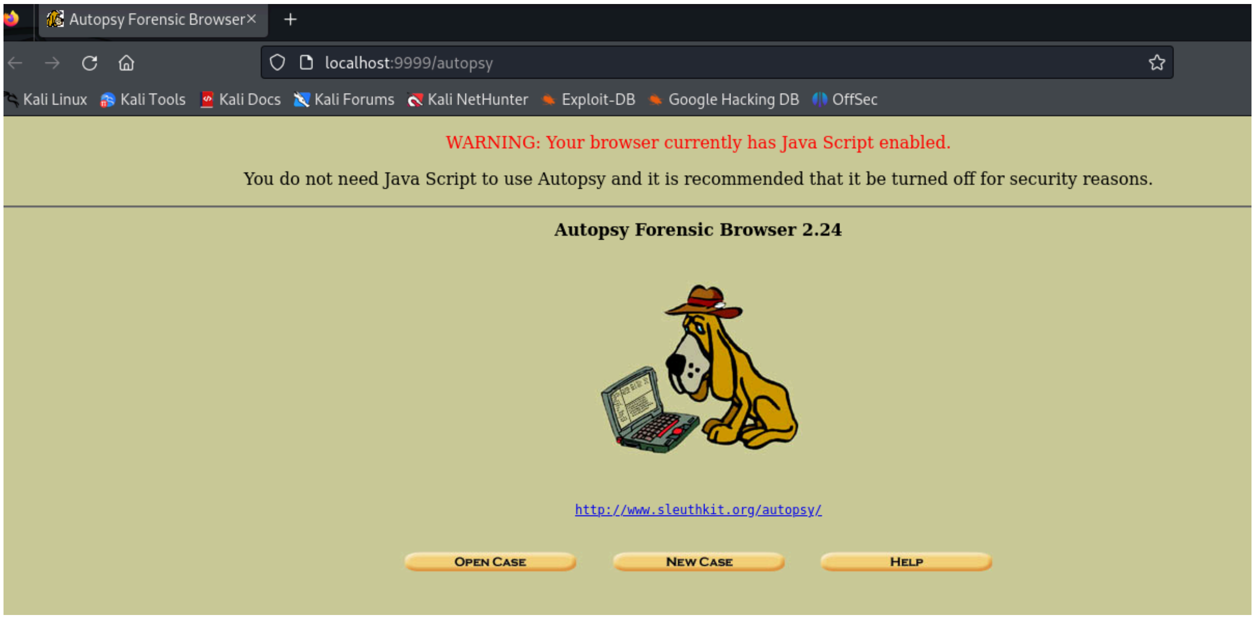
First before you can do autopsy you will have to install it first and you can do that by running the above command.

Toan c Ngo
Date:4/24/24



```
┌──(kali㉿kali)-[~]
└─$ sudo autopsy
[sudo] password for kali:

============================================================================

                       Autopsy Forensic Browser
                   http://www.sleuthkit.org/autopsy/
                              ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Tue Apr 16 15:36:49 2024
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Now lets run the autopsy by input Sudo autopsy
After it runs it should give you a http link, this is not a live link by the way, it's just a local server that is run by your machine and that is where the autopsy application at.



WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

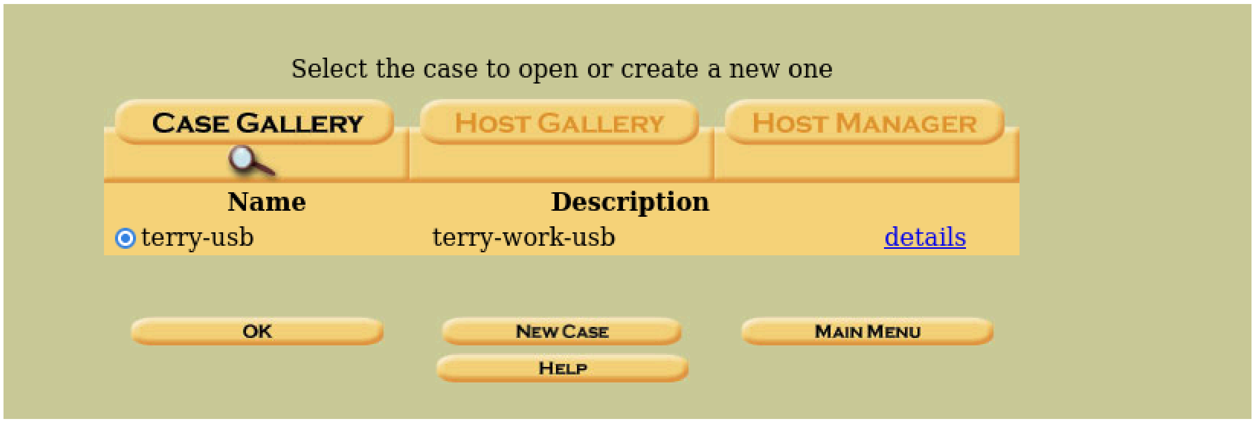
Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

Now after you click the link it should take you to this page where you can pick what you want to.
Open case- open a save autopsy case files
New case- create new case files

Toan c Ngo
Date:4/24/24

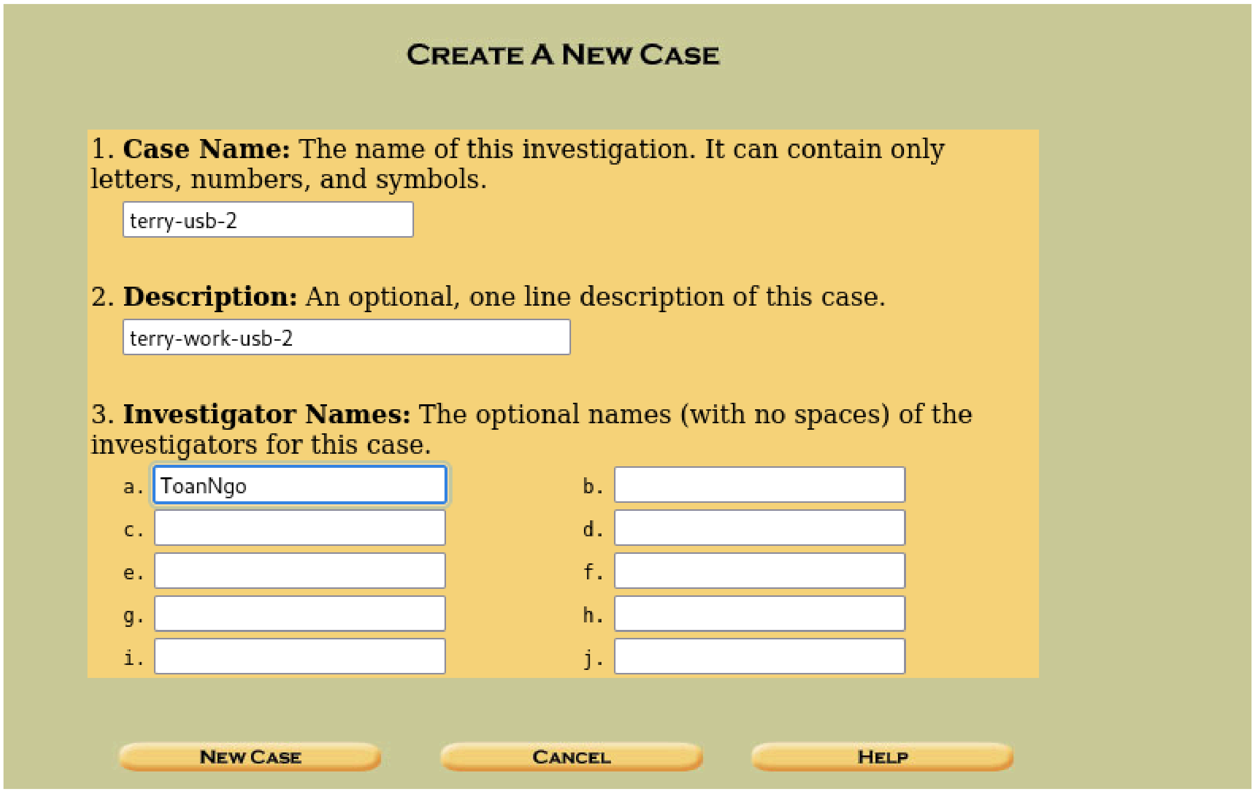
Help-its should display all the information related to what you can do in this application.
<for this lap we will make new case files for autopsy, so click on the new case >



Select the case to open or create a new one

Name	Description	
● terry-usb	terry-work-usb	details

This is what you see if you click on open a case, and because i did a case before as a test it now shows that i have a case on files but that is not important for this lap, now click on New Case to create a new one .



Create A New Case

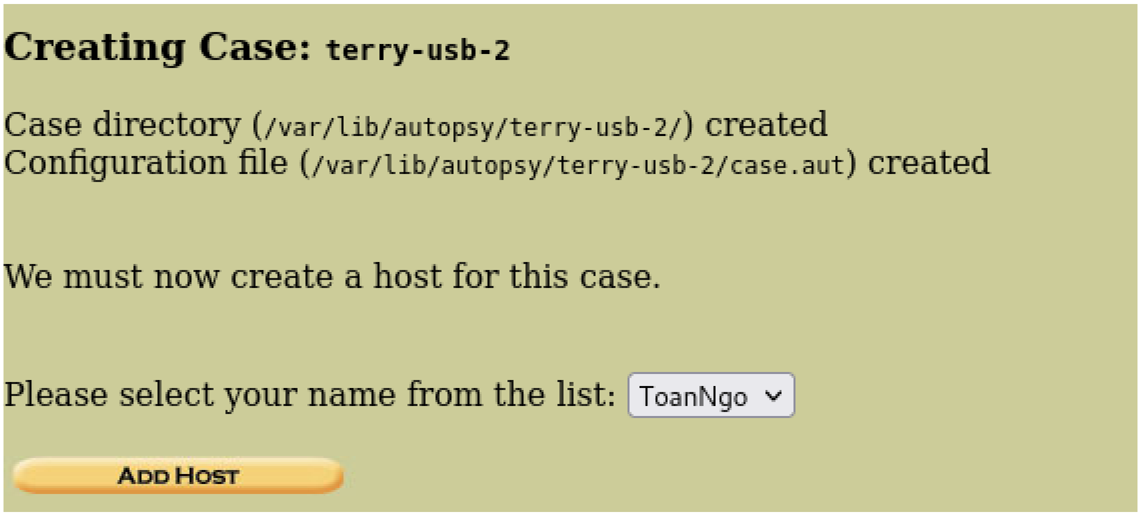
1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.
terry-usb-2

2. **Description:** An optional, one line description of this case.
terry-work-usb-2

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.
a. ToanNgo
b.
c.
d.
e.
f.
g.
h.
i.
j.

After clicking on a new case this is where you fill out all the information related to the case like what is the case name, what is the case about, and how many investigators are investigating this case.
When done click on New Case

Toan c Ngo
Date:4/24/24



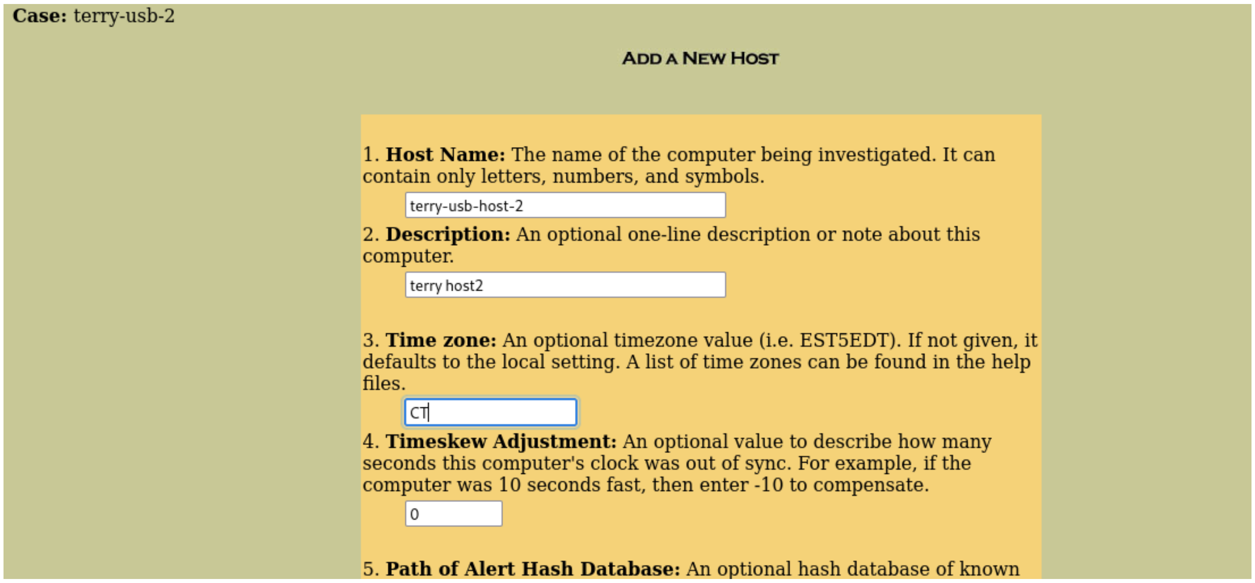
Creating Case: `terry-usb-2`

Case directory (`/var/lib/autopsy/terry-usb-2/`) created
Configuration file (`/var/lib/autopsy/terry-usb-2/case.aut`) created

We must now create a host for this case.

Please select your name from the list: ToanNgo

After you fill out all the information related to the case you can select which investigator is going to use this case.
After you done selecting the name from list click add host



Case: terry-usb-2

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
terry-usb-host-2

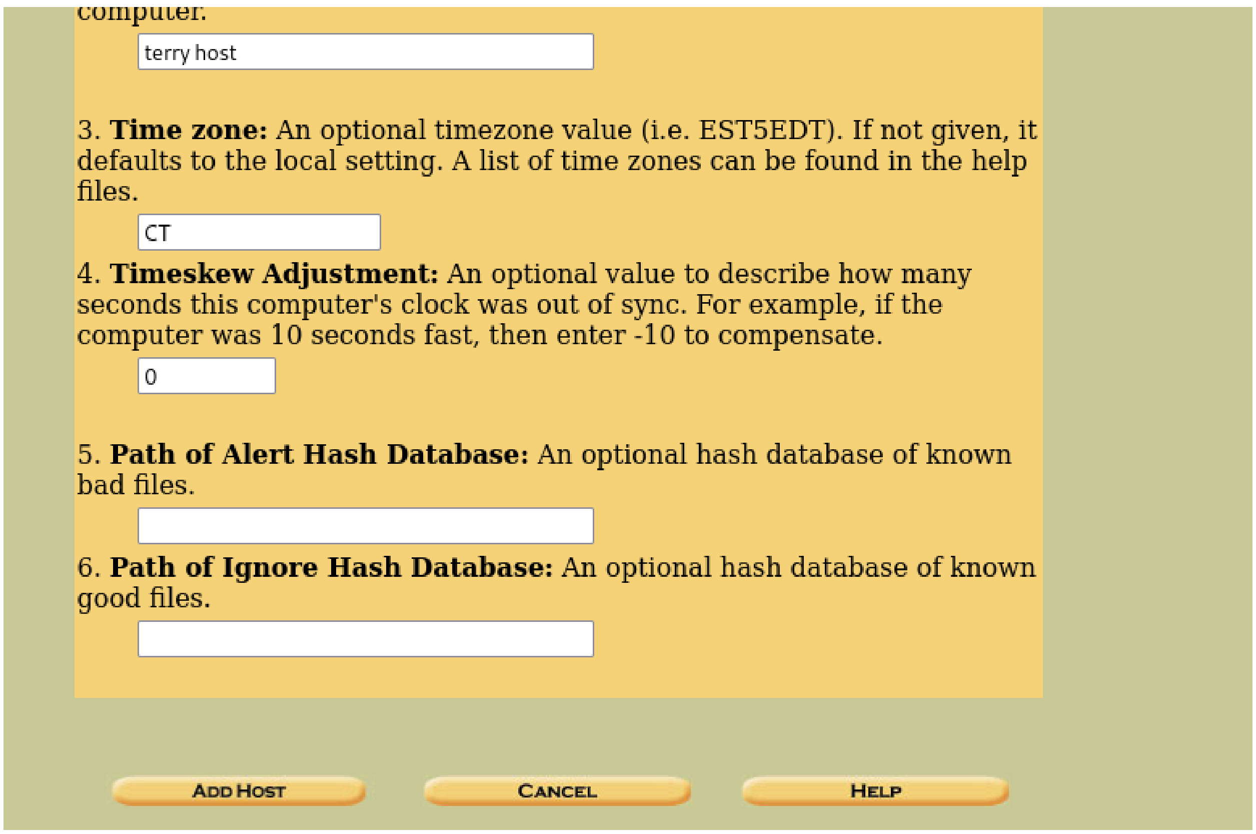
2. **Description:** An optional one-line description or note about this computer.
terry host2

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
CT

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0

5. **Path of Alert Hash Database:** An optional hash database of known

Now in this screen you will enter the information about who computers are being investigated and what is this investigation about in the description.



computer.

terry host

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

CT

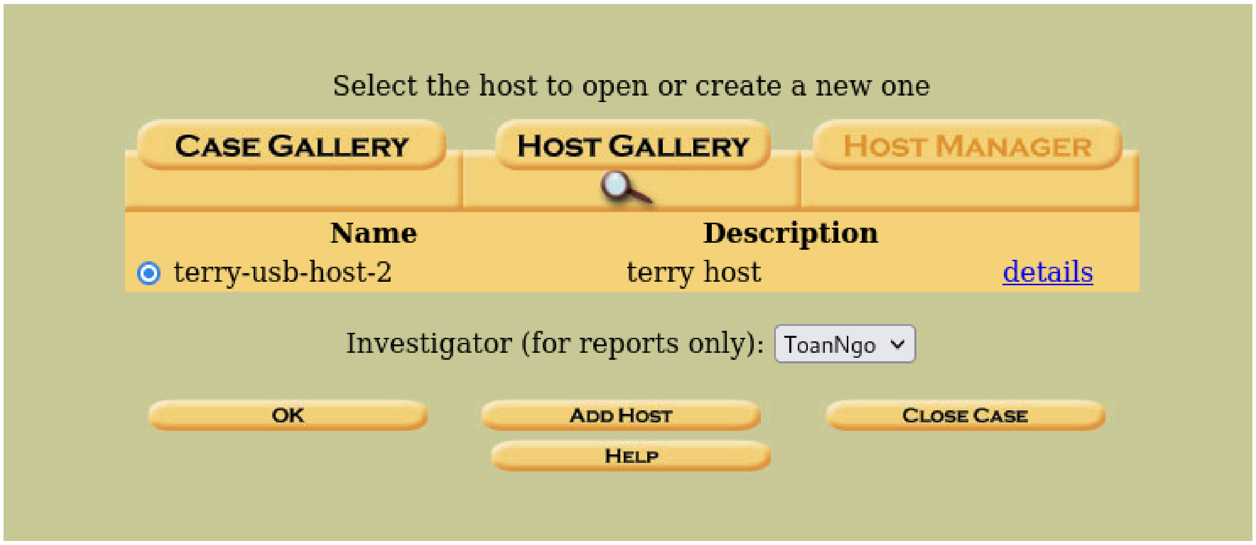
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

After you done you click on add host

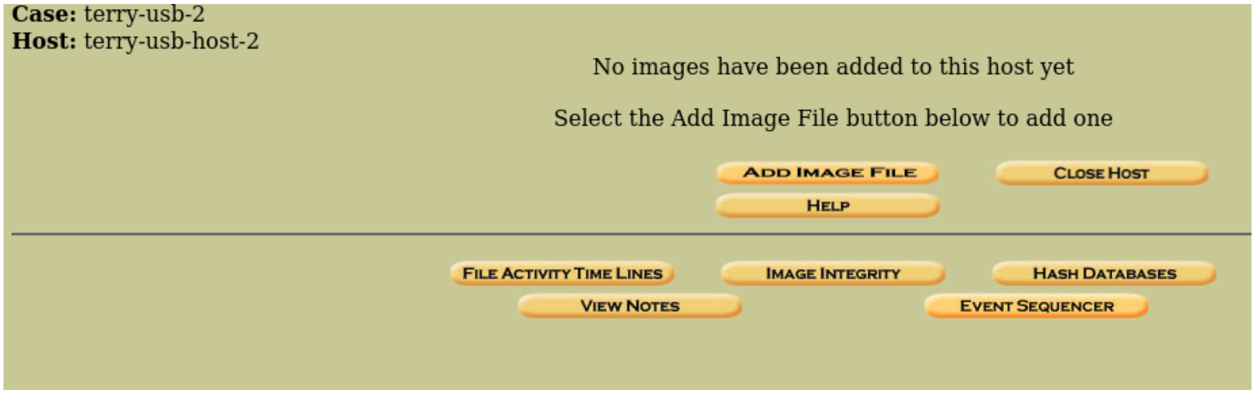


Select the host to open or create a new one

Name	Description	
● terry-usb-host-2	terry host	details

Investigator (for reports only): ToanNgo

After you did everything in the previous step it should take you to this place select the case name that you just created and click ok

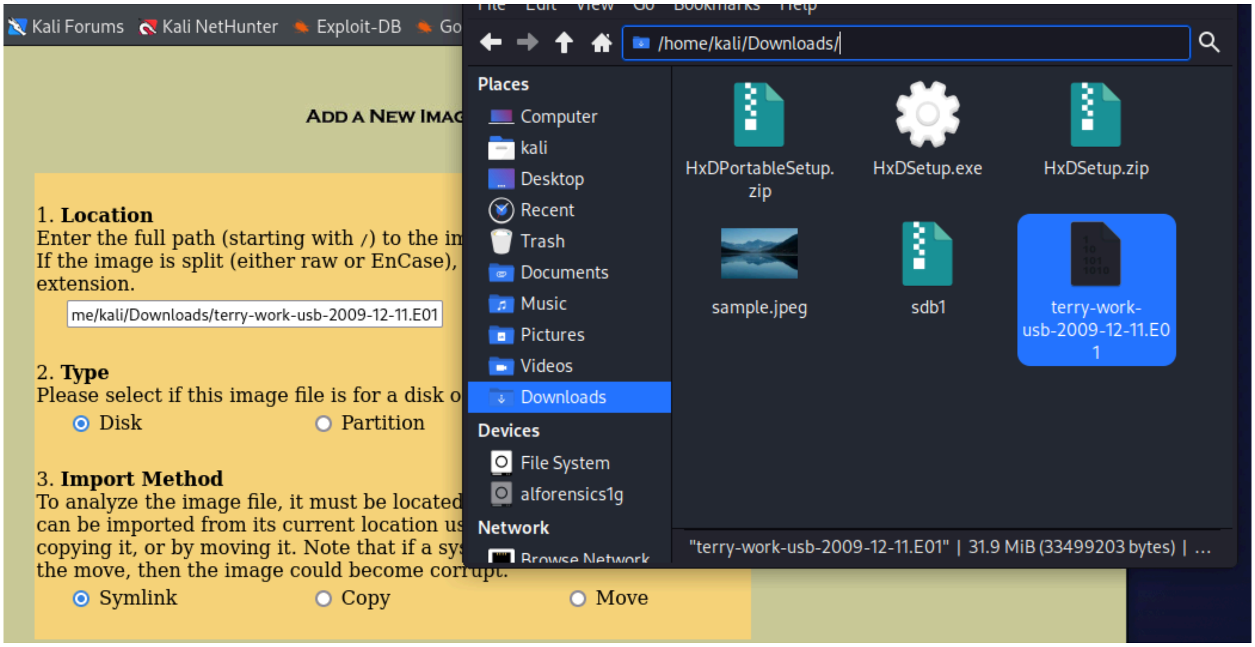


Case: terry-usb-2
Host: terry-usb-host-2

No images have been added to this host yet

Select the Add Image File button below to add one

Now after you click on the ok button it should take you to this page where you can select what you want to investigate with, for this lap we will do an image file investigation.
Go to this website:
https://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/usb/
And select: terry-work-usb-2009-12-11.E01 download it in a folders
Now that you have the file downloaded click on the <add image file>



/home/kali/Downloads/

"terry-work-usb-2009-12-11.E01" | 31.9 MiB (33499203 bytes) | ...

ADD A NEW IMAG

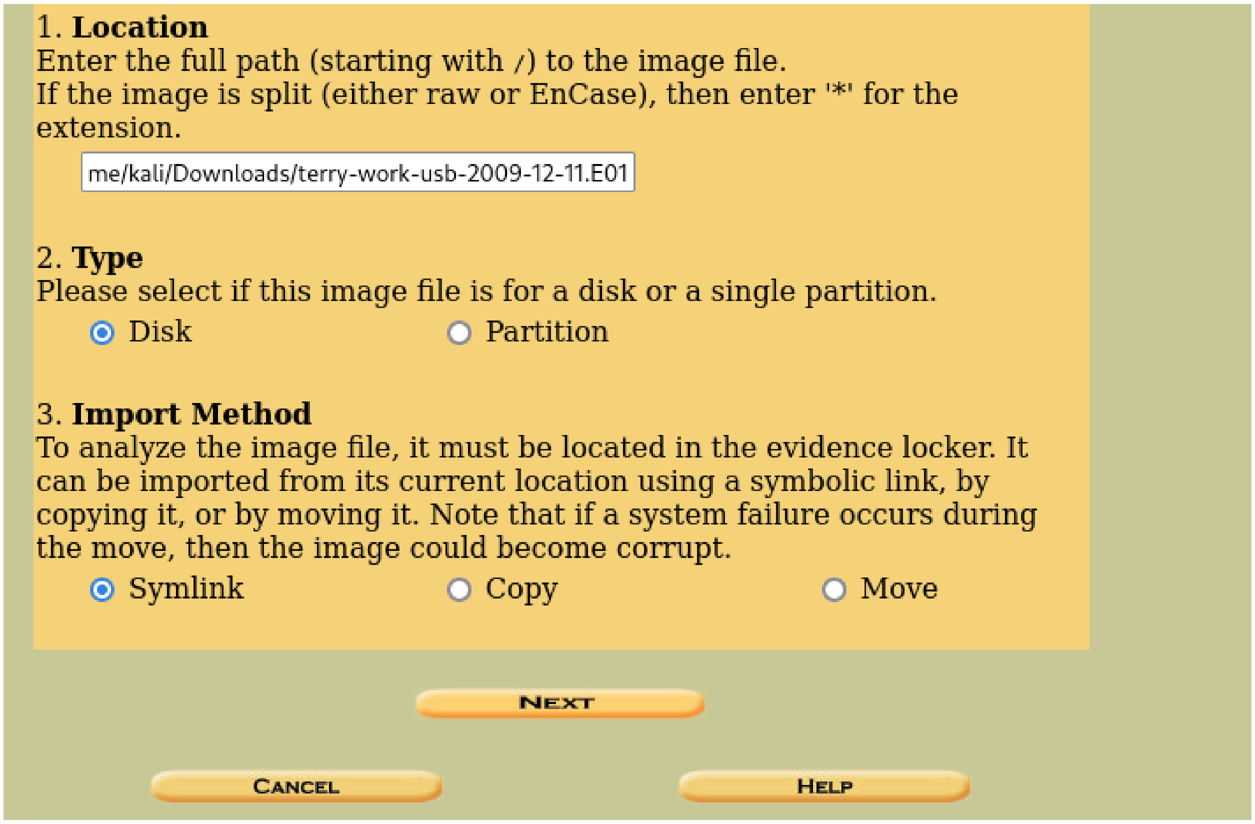
1. **Location**
Enter the full path (starting with /) to the im
If the image is split (either raw or EnCase),
extension.
me/kali/Downloads/terry-work-usb-2009-12-11.E01

2. **Type**
Please select if this image file is for a disk o
● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located
can be imported from its current location us
copying it, or by moving it. Note that if a sys
the move, then the image could become corrupt.
● Symlink ○ Copy ○ Move

If you know the file enter it on the location box, if not then you will have to go to the folder that contains the image file you downloaded from there you can get the files path that way.

Toan c Ngo
Date:4/24/24



1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

me/kali/Downloads/terry-work-usb-2009-12-11.E01

2. **Type**
Please select if this image file is for a disk or a single partition.

● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move

For type select disk because we are analyzing a disk image not a partition

For import method you select between three choices
Symlink - where you you can import the files by linking the application/folder that this conduct on to it

Copy- where you make a copy of the files and move it into the folder that you are currently working with.

Move- move this image file from its origin folder to your working folder, but be warned if a case of a system failure occurs during the transfer process then the image could become corrupted.

For this lap we will do Symlink so select it

Toan c Ngo
Date:4/24/24

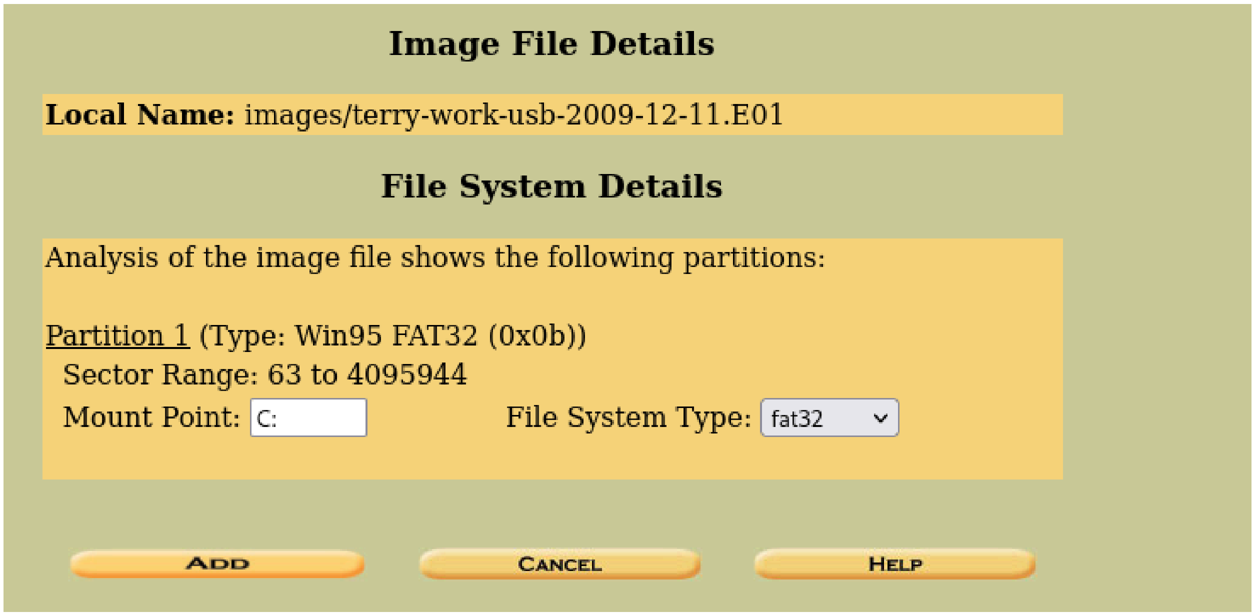


Image File Details

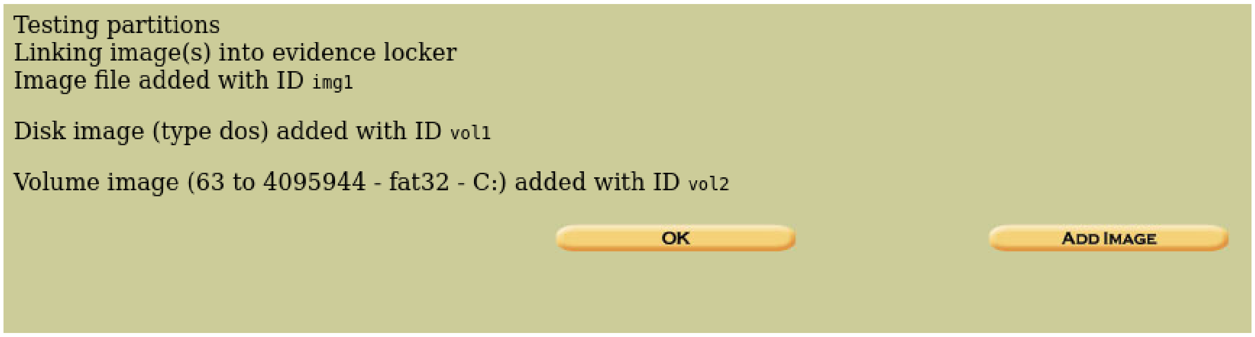
Local Name: images/terry-work-usb-2009-12-11.E01

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: Win95 FAT32 (0x0b))
Sector Range: 63 to 4095944
Mount Point: C: File System Type: fat32

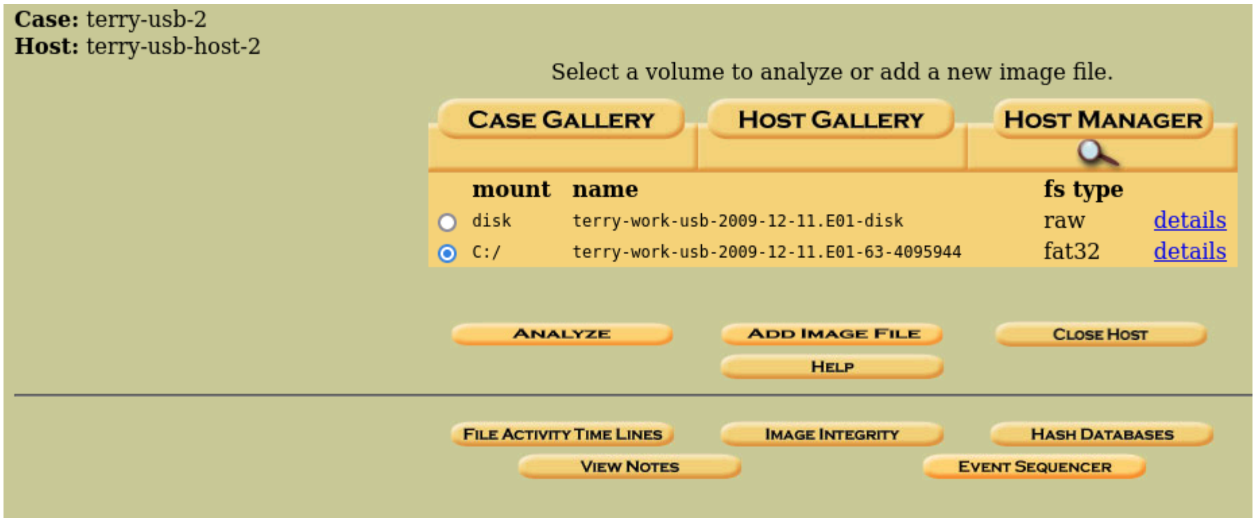
Now at this screen, put mount point to c because that where we download the files to and the system file type to Fat32 and click add



```
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Disk image (type dos) added with ID vol1

Volume image (63 to 4095944 - fat32 - C:) added with ID vol2
```

This is the review screen click ok

Toan c Ngo
Date:4/24/24

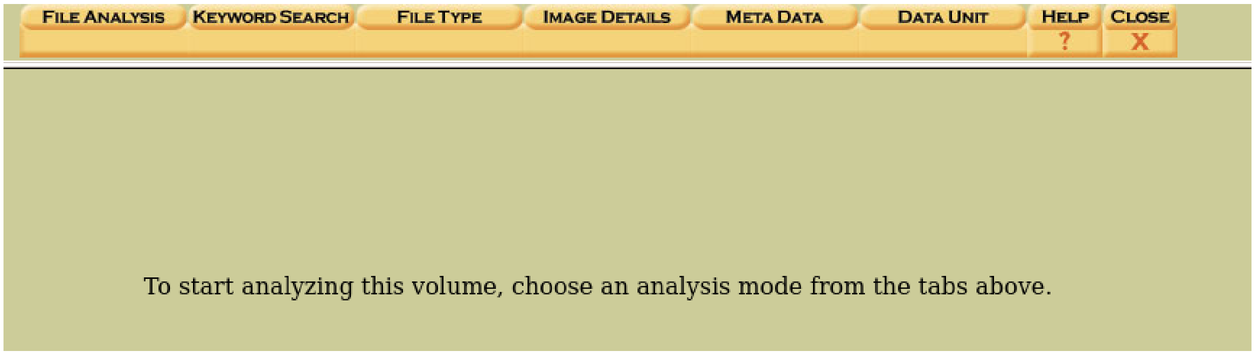


Case: terry-usb-2
Host: terry-usb-host-2

Select a volume to analyze or add a new image file.

	mount	name	fs type	
○	disk	terry-work-usb-2009-12-11.E01-disk	raw	details
●	C:/	terry-work-usb-2009-12-11.E01-63-4095944	fat32	details

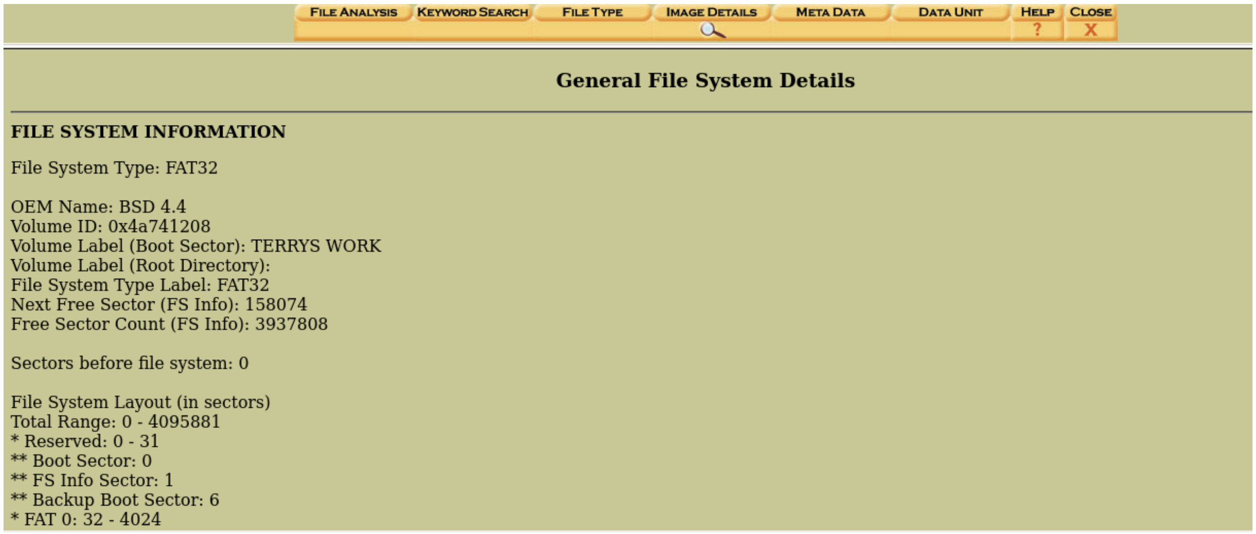
After the prev screen it should taking you to this screen right here
Select the files that we just make together and click on analyze



To start analyzing this volume, choose an analysis mode from the tabs above.

Now in this screen, there a lot of option you can choose from and all of it are for analyzing the image disk/data
For now let us click on the image detail.

Toan c Ngo
Date:4/24/24



General File System Details

FILE SYSTEM INFORMATION

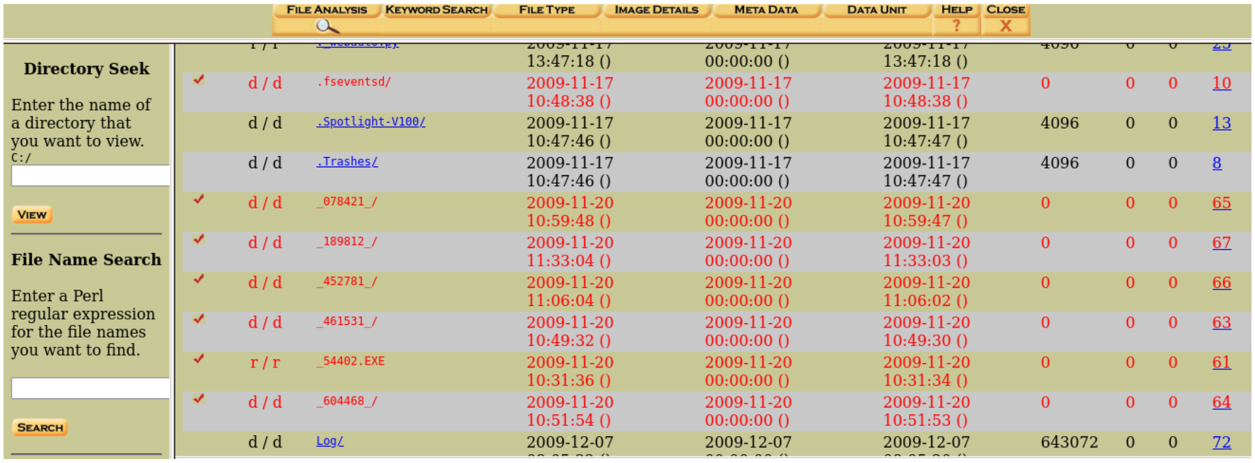
File System Type: FAT32

OEM Name: BSD 4.4
Volume ID: 0x4a741208
Volume Label (Boot Sector): TERRYS WORK
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 158074
Free Sector Count (FS Info): 3937808

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 4095881
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 4024

This should show you the detail of the image
Next let's try to analyst the image and we can do just that by clicking on file analysis



Directory Seek

Enter the name of a directory that you want to view.
C:/

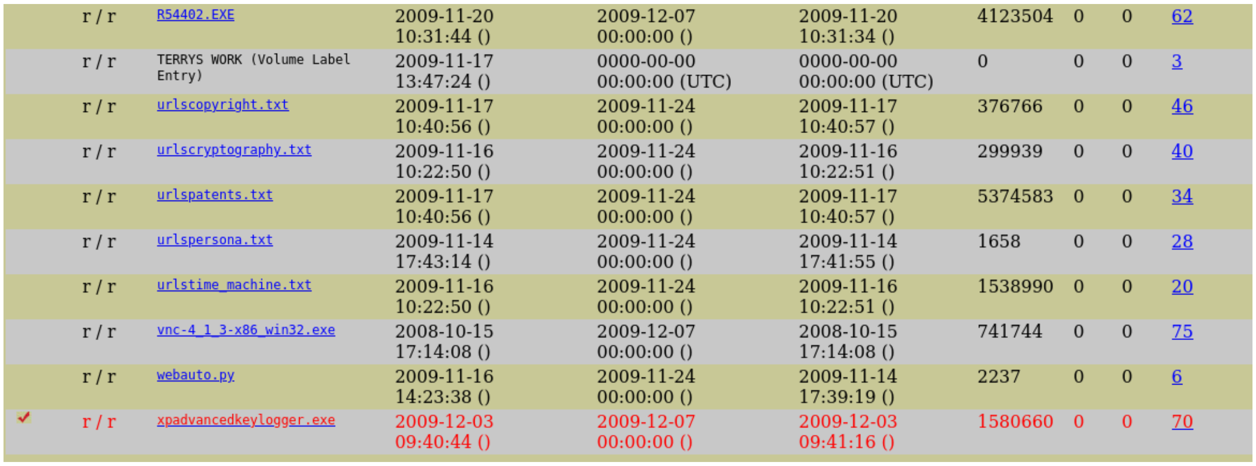
File Name Search

Enter a Perl regular expression for the file names you want to find.

			13:47:18 ()	00:00:00 ()	13:47:18 ()				
✓	d / d	.fseventsd/	2009-11-17 10:48:38 ()	2009-11-17 00:00:00 ()	2009-11-17 10:48:38 ()	0	0	0	10
	d / d	.Spotlight-V100/	2009-11-17 10:47:46 ()	2009-11-17 00:00:00 ()	2009-11-17 10:47:47 ()	4096	0	0	13
	d / d	.Trashes/	2009-11-17 10:47:46 ()	2009-11-17 00:00:00 ()	2009-11-17 10:47:47 ()	4096	0	0	8
✓	d / d	_078421_/	2009-11-20 10:59:48 ()	2009-11-20 00:00:00 ()	2009-11-20 10:59:47 ()	0	0	0	65
✓	d / d	_189812_/	2009-11-20 11:33:04 ()	2009-11-20 00:00:00 ()	2009-11-20 11:33:03 ()	0	0	0	67
✓	d / d	_452781_/	2009-11-20 11:06:04 ()	2009-11-20 00:00:00 ()	2009-11-20 11:06:02 ()	0	0	0	66
✓	d / d	_461531_/	2009-11-20 10:49:32 ()	2009-11-20 00:00:00 ()	2009-11-20 10:49:30 ()	0	0	0	63
✓	r / r	_54402.EXE	2009-11-20 10:31:36 ()	2009-11-20 00:00:00 ()	2009-11-20 10:31:34 ()	0	0	0	61
✓	d / d	_604468_/	2009-11-20 10:51:54 ()	2009-11-20 00:00:00 ()	2009-11-20 10:51:53 ()	0	0	0	64
	d / d	Log/	2009-12-07	2009-12-07	2009-12-07	643072	0	0	72

This is the files and directory on the computer that this image are capturing from and if you scroll all the way to the end you will see something interesting
Also just a note
-The red text are the files/directory has being deleted by the user of that computer
-The blue are the files that are still remain/active

Toan c Ngo
Date:4/24/24

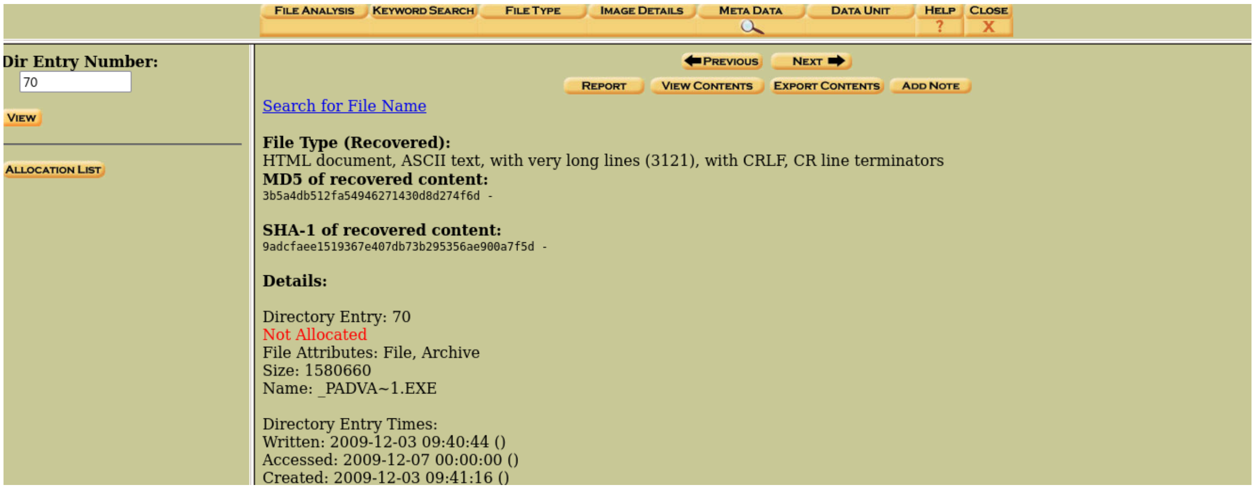


	r / r	R54402.EXE	2009-11-20 10:31:44 ()	2009-12-07 00:00:00 ()	2009-11-20 10:31:34 ()	4123504	0	0	62
	r / r	TERRYS WORK (Volume Label Entry)	2009-11-17 13:47:24 ()	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	3
	r / r	urlscopyright.txt	2009-11-17 10:40:56 ()	2009-11-24 00:00:00 ()	2009-11-17 10:40:57 ()	376766	0	0	46
	r / r	urlscryptography.txt	2009-11-16 10:22:50 ()	2009-11-24 00:00:00 ()	2009-11-16 10:22:51 ()	299939	0	0	40
	r / r	urlspatents.txt	2009-11-17 10:40:56 ()	2009-11-24 00:00:00 ()	2009-11-17 10:40:57 ()	5374583	0	0	34
	r / r	urlspersona.txt	2009-11-14 17:43:14 ()	2009-11-24 00:00:00 ()	2009-11-14 17:41:55 ()	1658	0	0	28
	r / r	urlstime_machine.txt	2009-11-16 10:22:50 ()	2009-11-24 00:00:00 ()	2009-11-16 10:22:51 ()	1538990	0	0	20
	r / r	vnc-4_1_3-x86_win32.exe	2008-10-15 17:14:08 ()	2009-12-07 00:00:00 ()	2008-10-15 17:14:08 ()	741744	0	0	75
	r / r	webauto.py	2009-11-16 14:23:38 ()	2009-11-24 00:00:00 ()	2009-11-14 17:39:19 ()	2237	0	0	6
✓	r / r	xpadvancedkeylogger.exe	2009-12-03 09:40:44 ()	2009-12-07 00:00:00 ()	2009-12-03 09:41:16 ()	1580660	0	0	70

After you did the previous step you should see this where the file name keylogger.exe has been deleted, and keyloggers are illegal so the user of this image is definitely up to something.

So what if you want to generate a report based on this image ?
Then you will go to the MetaData tab and click on the report buttons for it to generate the report, or you could also view the contents of the report, or export the content, it entirely depends on your need.

Just a note you could also use dir entry number to generate a report based on one entry only.



Dir Entry Number: 70

File Type (Recovered):
HTML document, ASCII text, with very long lines (3121), with CRLF, CR line terminators
MD5 of recovered content:
`3b5a4db512fa54946271430d8d274f6d -`

SHA-1 of recovered content:
`9adcfaee1519367e407db73b295356ae900a7f5d -`

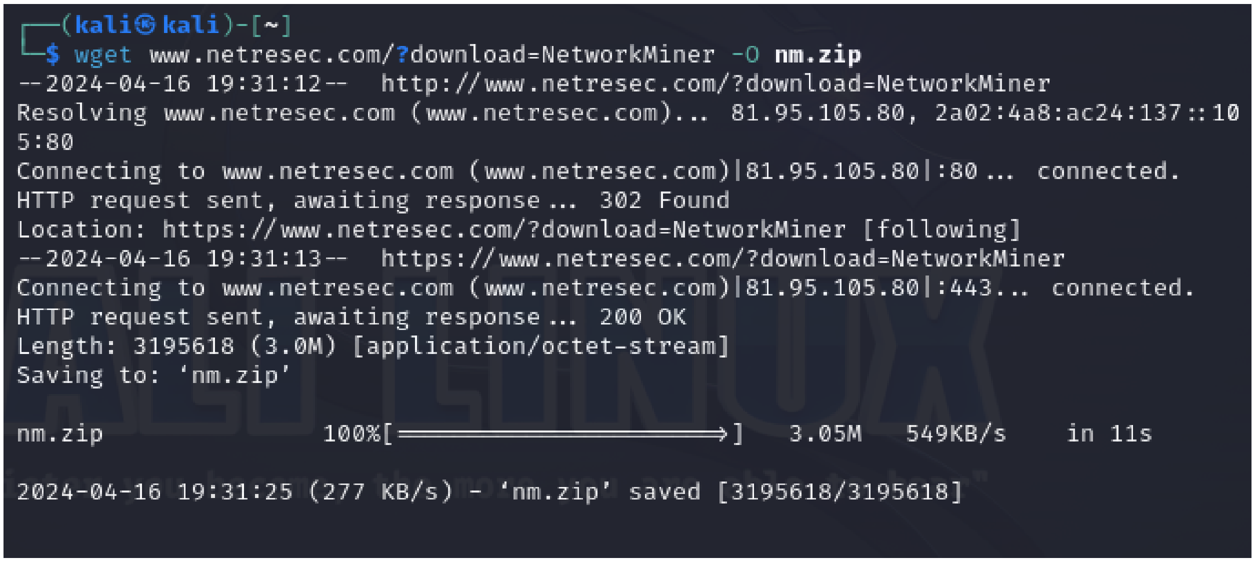
Details:

Directory Entry: 70
Not Allocated
File Attributes: File, Archive
Size: 1580660
Name: _PADVA~1.EXE

Directory Entry Times:
Written: 2009-12-03 09:40:44 ()
Accessed: 2009-12-07 00:00:00 ()
Created: 2009-12-03 09:41:16 ()

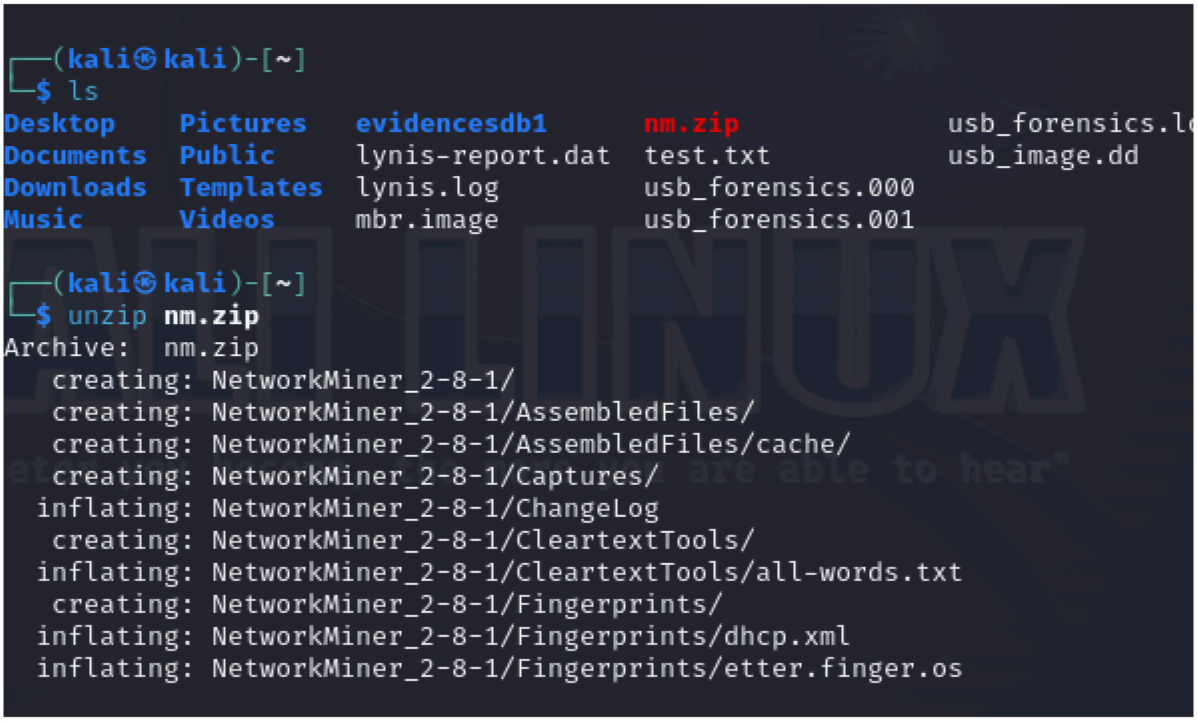
Now let's move on to the network forensic
First we need to get some files

Toan c Ngo
Date:4/24/24



```
┌──(kali㉿kali)-[~]
└─$ wget www.netresec.com/?download=NetworkMiner -O nm.zip
--2024-04-16 19:31:12--  http://www.netresec.com/?download=NetworkMiner
Resolving www.netresec.com (www.netresec.com)... 81.95.105.80, 2a02:4a8:ac24:137::10
5:80
Connecting to www.netresec.com (www.netresec.com)|81.95.105.80|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.netresec.com/?download=NetworkMiner [following]
--2024-04-16 19:31:13--  https://www.netresec.com/?download=NetworkMiner
Connecting to www.netresec.com (www.netresec.com)|81.95.105.80|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3195618 (3.0M) [application/octet-stream]
Saving to: ‘nm.zip’

nm.zip                  100%[=========================>]   3.05M   549KB/s    in 11s

2024-04-16 19:31:25 (277 KB/s) - ‘nm.zip’ saved [3195618/3195618]
```

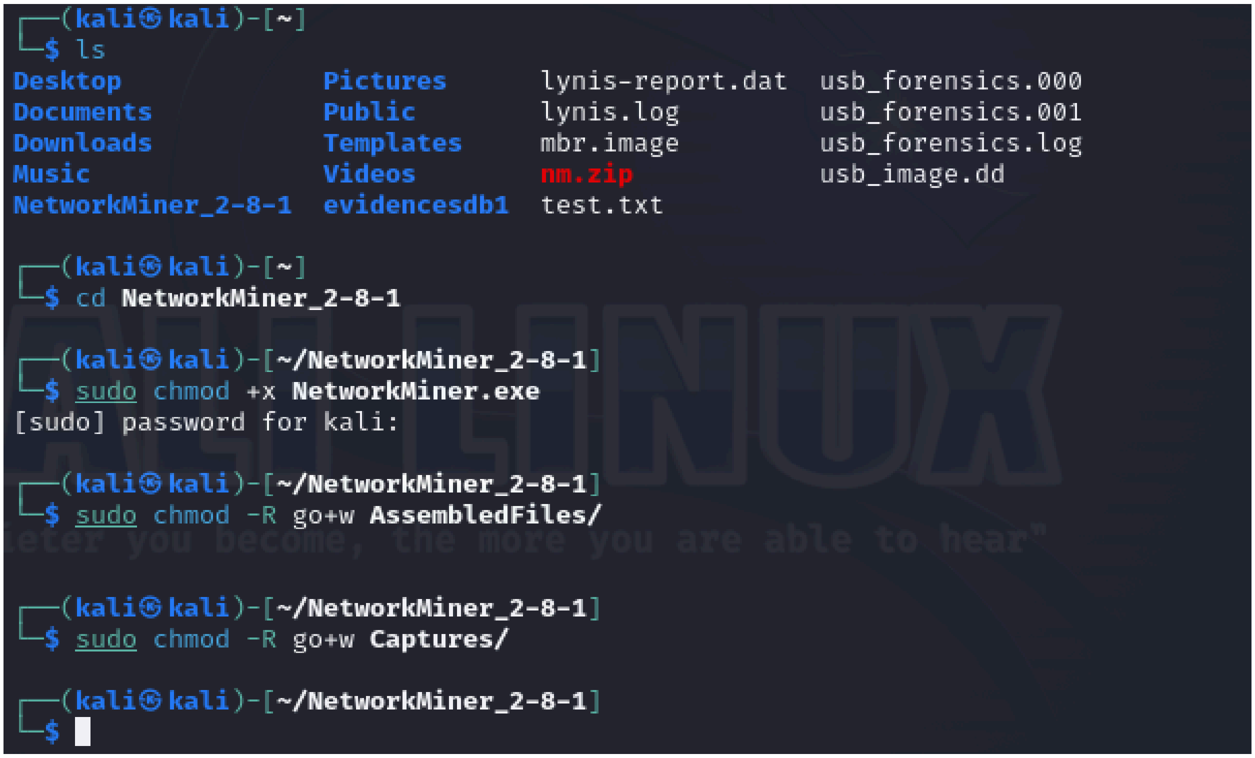
Run the above command to get the necessarily file wget-online search and download
After it finish running you should see it appear in the system when you call ls



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Pictures   evidencesdb1      nm.zip            usb_forensics.l
Documents  Public     lynis-report.dat  test.txt          usb_image.dd
Downloads  Templates  lynis.log         usb_forensics.000
Music      Videos     mbr.image         usb_forensics.001

┌──(kali㉿kali)-[~]
└─$ unzip nm.zip
Archive:  nm.zip
   creating: NetworkMiner_2-8-1/
   creating: NetworkMiner_2-8-1/AssembledFiles/
   creating: NetworkMiner_2-8-1/AssembledFiles/cache/
   creating: NetworkMiner_2-8-1/Captures/
  inflating: NetworkMiner_2-8-1/ChangeLog
   creating: NetworkMiner_2-8-1/CleartextTools/
  inflating: NetworkMiner_2-8-1/CleartextTools/all-words.txt
   creating: NetworkMiner_2-8-1/Fingerprints/
  inflating: NetworkMiner_2-8-1/Fingerprints/dhcp.xml
  inflating: NetworkMiner_2-8-1/Fingerprints/etter.finger.os
```

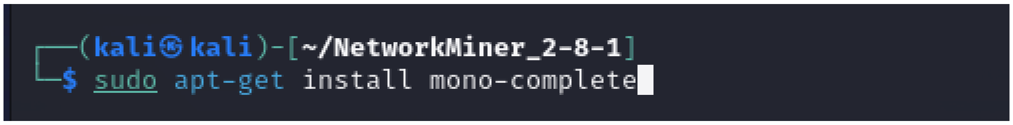
Now unzip the file by using the unzip command
After the unzip command done use ls again and you should see a directory name networkminer_2-8-1, move to that directory by “cd”

Toan c Ngo
Date:4/24/24



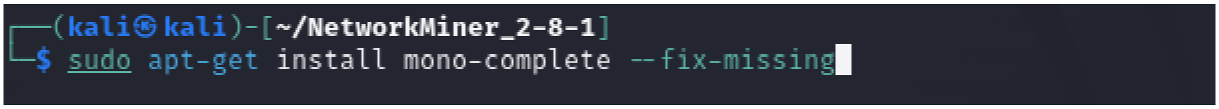
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop              Pictures      lynis-report.dat  usb_forensics.000
Documents            Public        lynis.log         usb_forensics.001
Downloads            Templates     mbr.image         usb_forensics.log
Music                Videos        nm.zip            usb_image.dd
NetworkMiner_2-8-1   evidencesdb1  test.txt

┌──(kali㉿kali)-[~]
└─$ cd NetworkMiner_2-8-1

┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo chmod +x NetworkMiner.exe
[sudo] password for kali:

┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo chmod -R go+w AssembledFiles/

┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo chmod -R go+w Captures/

┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ 
```

So what the chmod command do in this case is change the permission of the folder and here are the list of option
+w-add write permission
-go - group together files
+x - add execution permission
-R - recursion loop



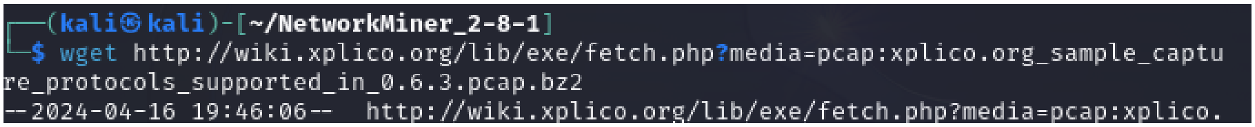
```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo apt-get install mono-complete
```

So in order for us to run the .exe file on linux we need the mono framework and you can get it by running this command



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo apt-get install mono-complete --fix-missing
```

And if you ever ran into a problem using the install command above you can try this
Sudo apt-get install mono-complete –fix-missing
after it run and its should fix the install files

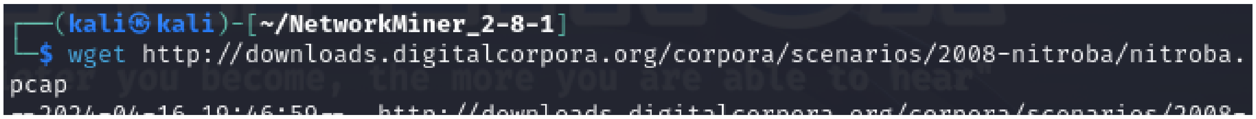


```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ wget http://wiki.xplico.org/lib/exe/fetch.php?media=pcap:xplico.org_sample_captu
re_protocols_supported_in_0.6.3.pcap.bz2
--2024-04-16 19:46:06--  http://wiki.xplico.org/lib/exe/fetch.php?media=pcap:xplico.
```

Now we need to get the pcap file so use the wget command and following this link

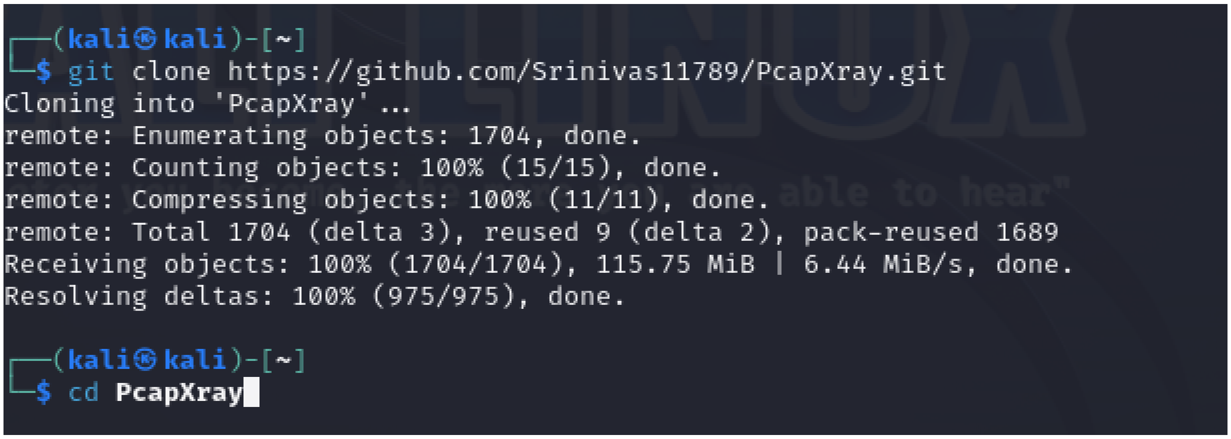
Toan c Ngo
Date:4/24/24

http://wiki.xplico.org/lib/exe/fetch.php?media=pcap:xplico.org_sample_capture_protocols_supported_in_0.6.3.pcap.bz2



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ wget http://downloads.digitalcorpora.org/corpora/scenarios/2008-nitroba/nitroba.
pcap
--2024-04-16 19:46:59--  http://downloads.digitalcorpora.org/corpora/scenarios/2008-
```

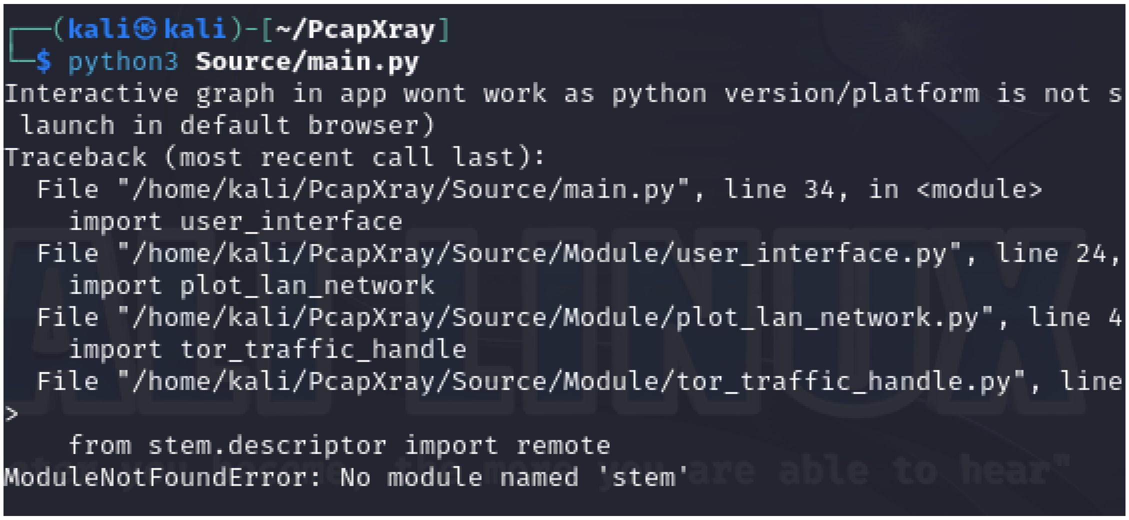
Do the same thing as the prev step but now use this link:
http://downloads.digitalcorpora.org/corpora/scenarios/2008-nitroba/nitroba.pcap



```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/Srinivas11789/PcapXray.git
Cloning into 'PcapXray'...
remote: Enumerating objects: 1704, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 1704 (delta 3), reused 9 (delta 2), pack-reused 1689
Receiving objects: 100% (1704/1704), 115.75 MiB | 6.44 MiB/s, done.
Resolving deltas: 100% (975/975), done.

┌──(kali㉿kali)-[~]
└─$ cd PcapXray
```

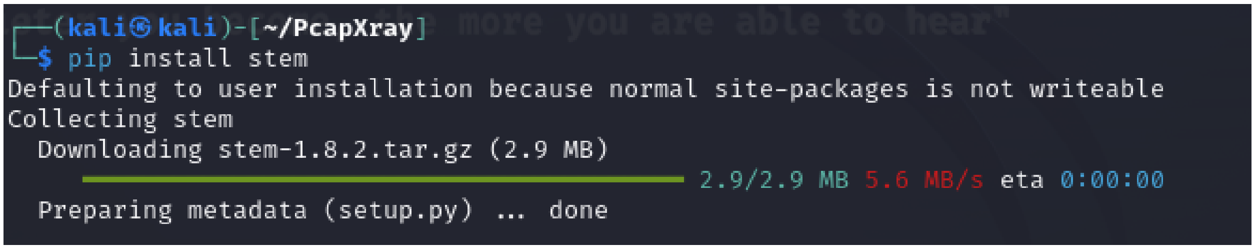
Now that we should have the files download we need to install application call pcapXray and to do that you input this command
Git clone https://github.com/Srinivas11789/PcapXray.git
After you done installing go to that directory using cd
Also you will need to have python installed as well and you can do so by running the following command.
sudo apt-get install python3-pip
Sudo apt-get install python3-tk
Sudo apt-get install graphviz
Sudo apt-get install python3-pil python3-pil.imagetk

Toan c Ngo
Date:4/24/24



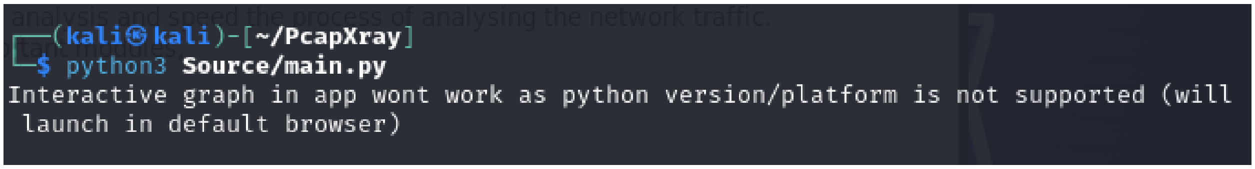
```
┌──(kali㉿kali)-[~/PcapXray]
└─$ python3 Source/main.py
Interactive graph in app wont work as python version/platform is not s
 launch in default browser)
Traceback (most recent call last):
  File "/home/kali/PcapXray/Source/main.py", line 34, in <module>
    import user_interface
  File "/home/kali/PcapXray/Source/Module/user_interface.py", line 24,
    import plot_lan_network
  File "/home/kali/PcapXray/Source/Module/plot_lan_network.py", line 4
    import tor_traffic_handle
  File "/home/kali/PcapXray/Source/Module/tor_traffic_handle.py", line
>
    from stem.descriptor import remote
ModuleNotFoundError: No module named 'stem'
```

Now if you try and run this command it will first show you an error message and in this case it's said that i have a missing module name stem, which mean that i need to install it
And i can do just that by this command: pip install stem



```
┌──(kali㉿kali)-[~/PcapXray]
└─$ pip install stem
Defaulting to user installation because normal site-packages is not writeable
Collecting stem
  Downloading stem-1.8.2.tar.gz (2.9 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.9/2.9 MB 5.6 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
```

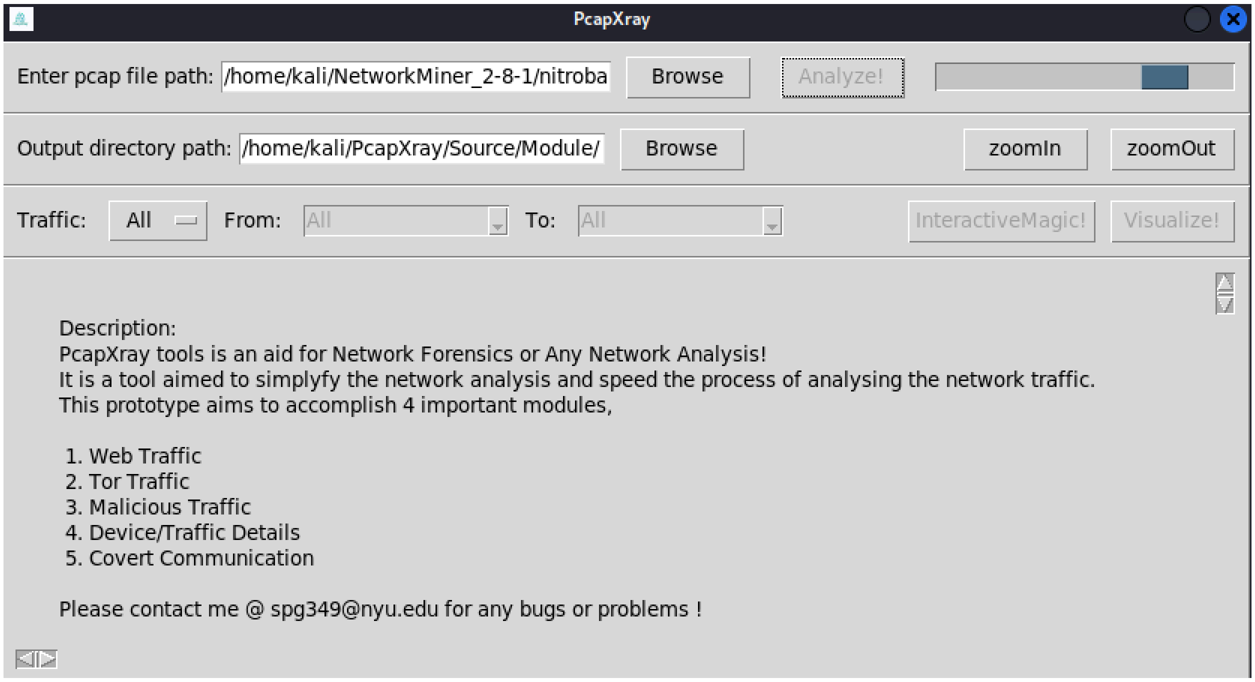
This is the command for install dependency



```
┌──(kali㉿kali)-[~/PcapXray]
└─$ python3 Source/main.py
Interactive graph in app wont work as python version/platform is not supported (will
 launch in default browser)
```

Now lets run the command again.

Toan c Ngo
Date:4/24/24



Enter pcap file path: /home/kali/NetworkMiner_2-8-1/nitroba

Output directory path: /home/kali/PcapXray/Source/Module/

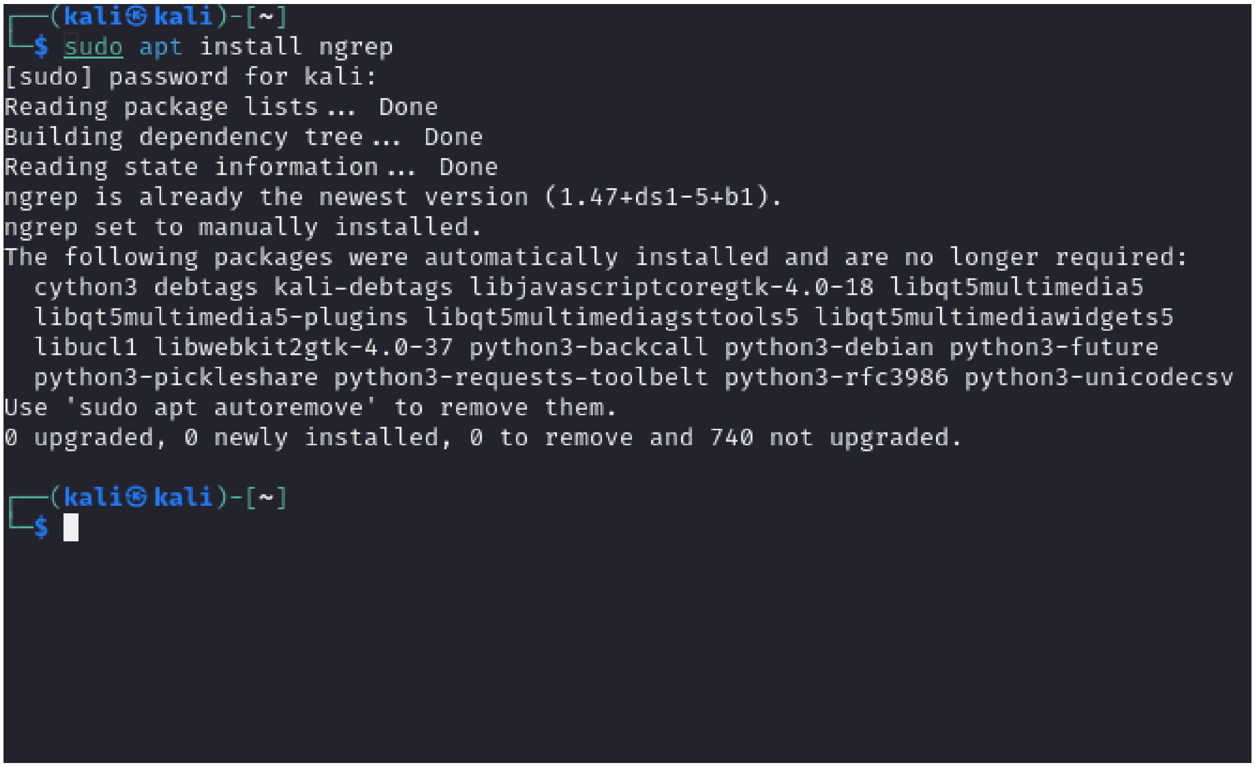
Traffic: All From: All To: All

Description:
PcapXray tools is an aid for Network Forensics or Any Network Analysis!
It is a tool aimed to simplyfy the network analysis and speed the process of analysing the network traffic.
This prototype aims to accomplish 4 important modules,

1. Web Traffic
2. Tor Traffic
3. Malicious Traffic
4. Device/Traffic Details
5. Covert Communication

Please contact me @ spg349@nyu.edu for any bugs or problems !

If the command were successfully run then this screen should popup
Here you can use this tool to trace the connection of the packet and manage the network traffic of incoming and outgoing connection to the network.



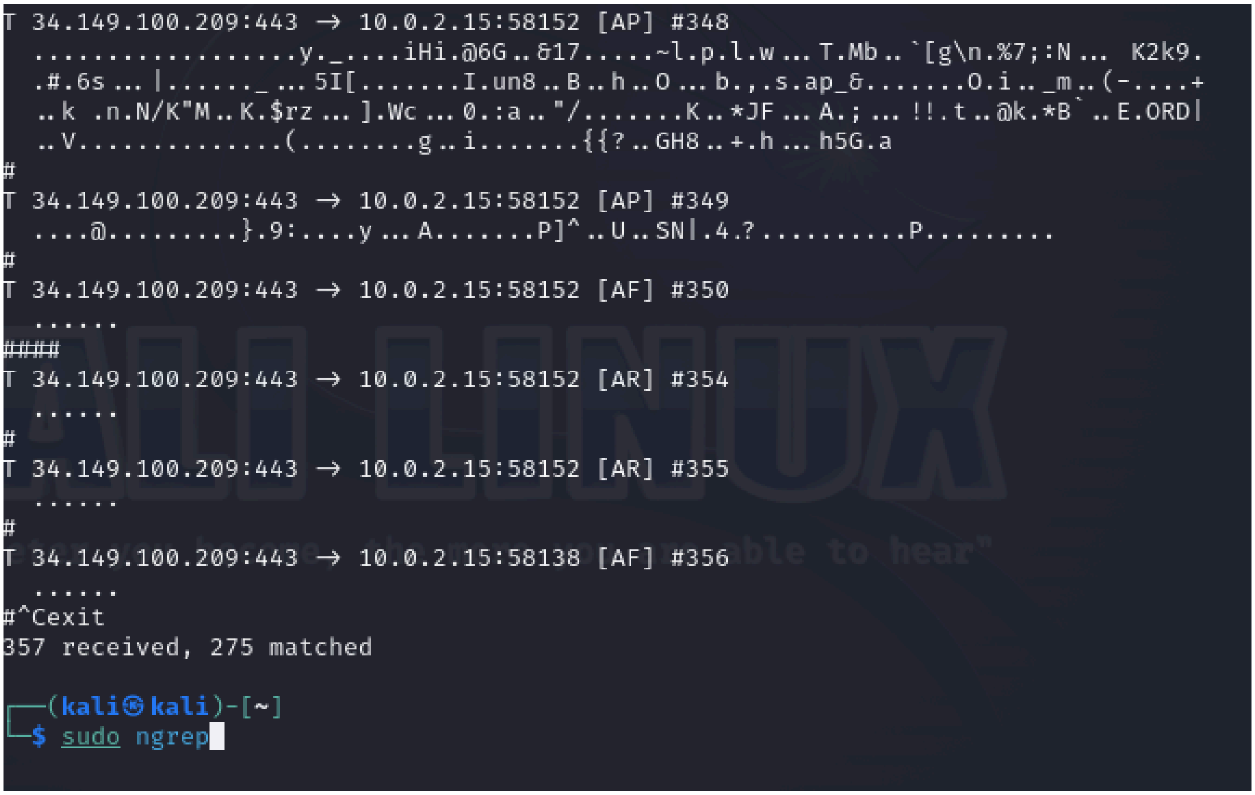
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ngrep
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ngrep is already the newest version (1.47+ds1-5+b1).
ngrep set to manually installed.
The following packages were automatically installed and are no longer required:
  cython3 debtags kali-debtags libjavascriptcoregtk-4.0-18 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5
  libucl1 libwebkit2gtk-4.0-37 python3-backcall python3-debian python3-future
  python3-pickleshare python3-requests-toolbelt python3-rfc3986 python3-unicodecsv
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 740 not upgraded.

┌──(kali㉿kali)-[~]
└─$ 
```

Now let's take a look into a forensic tool named ngrep.

Toan c Ngo
Date:4/24/24

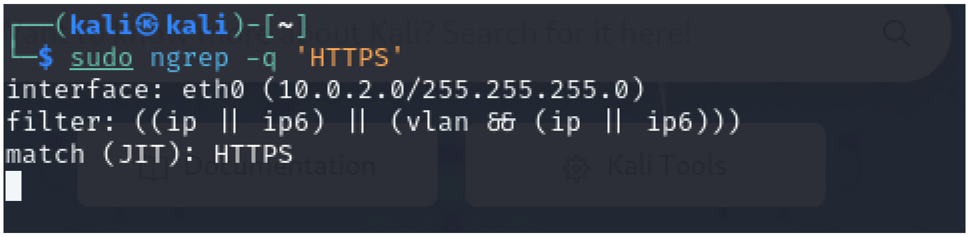
Ngrep is a grep-like tool to analyze interface traffic of pcap files and it offer some of the option as follow:
-i - case sensitive search
-q - be quiet
-v - invert the match
-(uppercase i)I - dump pcap files
-(uppercase o)O - output the result as pcap file
-num - match a specific number of packet
-bpf - Berkeley packet filters (powerful tool to filter specific packets)

Inorder to run this tool we first we need to install it.
Run this: sudo apt install ngrep



```
T 34.149.100.209:443 -> 10.0.2.15:58152 [AP] #348
  ..................y._....iHi.@6G..&17.....~l.p.l.w...T.Mb..`[g\n.%7;:N...  K2k9.
  .#.6s...|......_...5I[.......I.un8..B..h..O...b.,.s.ap_&.......O.i.._m..(-....+
  ..k .n.N/K"M..K.$rz...].Wc...0.:a.."/.......K..*JF...A.;...!!.t..@k.*B`..E.ORD|
  ..V..............(........g..i.......{{?..GH8..+.h...h5G.a
#
T 34.149.100.209:443 -> 10.0.2.15:58152 [AP] #349
  ....@.........}.9:....y...A.......P]^..U..SN|.4.?..........P.........
#
T 34.149.100.209:443 -> 10.0.2.15:58152 [AF] #350
  ......
####
T 34.149.100.209:443 -> 10.0.2.15:58152 [AR] #354
  ......
#
T 34.149.100.209:443 -> 10.0.2.15:58152 [AR] #355
  ......
#
T 34.149.100.209:443 -> 10.0.2.15:58138 [AF] #356
  ......
#^Cexit
357 received, 275 matched

┌──(kali㉿kali)-[~]
└─$ sudo ngrep
```

Now if you run sudo ngrep you will see a lot of packet because you are connecting to the internet and inorder to stop the output use ctrl + c
At this stage this packet are not really useful , so next we will apply a filter to it.

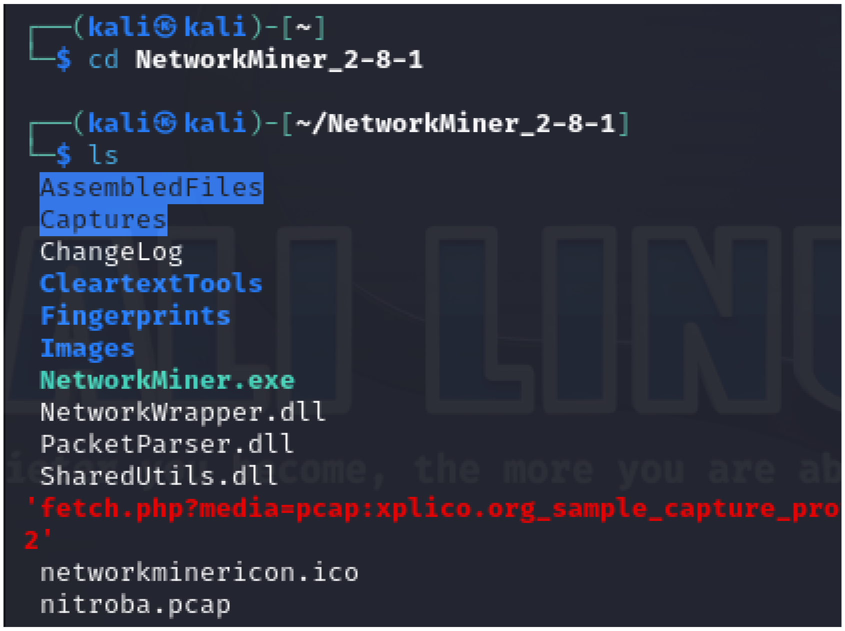


```
┌──(kali㉿kali)-[~]
└─$ sudo ngrep -q 'HTTPS'
interface: eth0 (10.0.2.0/255.255.255.0)
filter: ((ip || ip6) || (vlan && (ip || ip6)))
match (JIT): HTTPS
```

Now let's apply a filter to ngrep that only output when HTTPS are detected

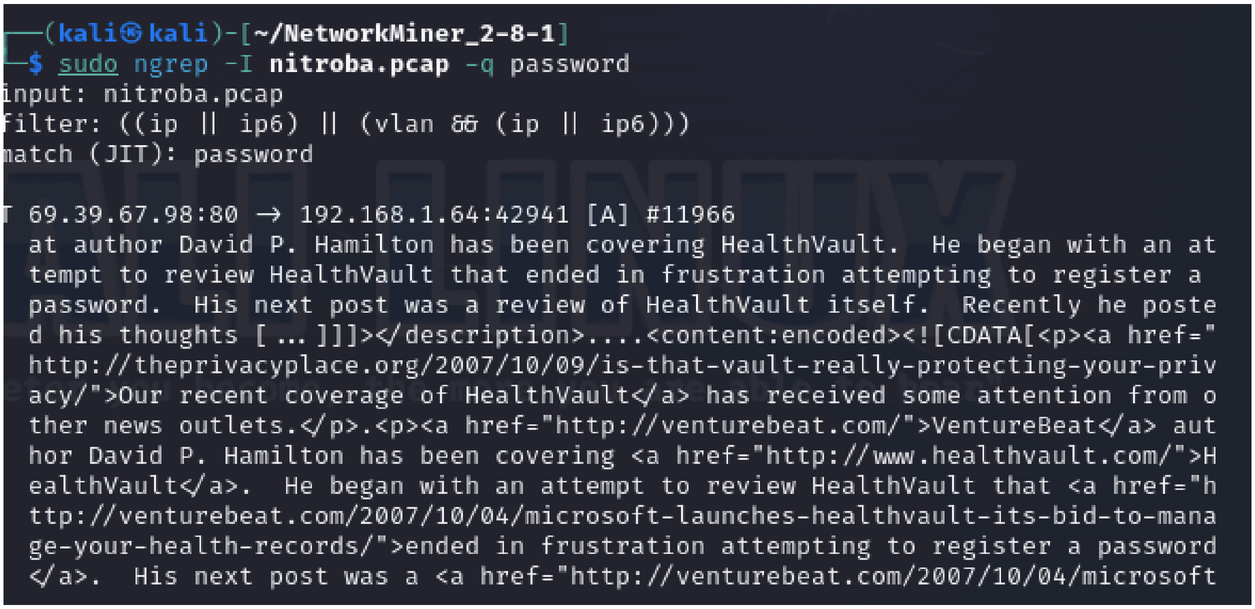
Toan c Ngo
Date:4/24/24

Now if you open a browser and go to a website the connection should be displayed here.



```
┌──(kali㉿kali)-[~]
└─$ cd NetworkMiner_2-8-1

┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ ls
 AssembledFiles
 Captures
 ChangeLog
 CleartextTools
 Fingerprints
 Images
 NetworkMiner.exe
 NetworkWrapper.dll
 PacketParser.dll
 SharedUtils.dll
'fetch.php?media=pcap:xplico.org_sample_capture_pro
2'
 networkminericon.ico
 nitroba.pcap
```

Now for the next part we gonna analyze a pcap file
First go to the directory/folders that you have download the nitroba.pcap files using the Cd

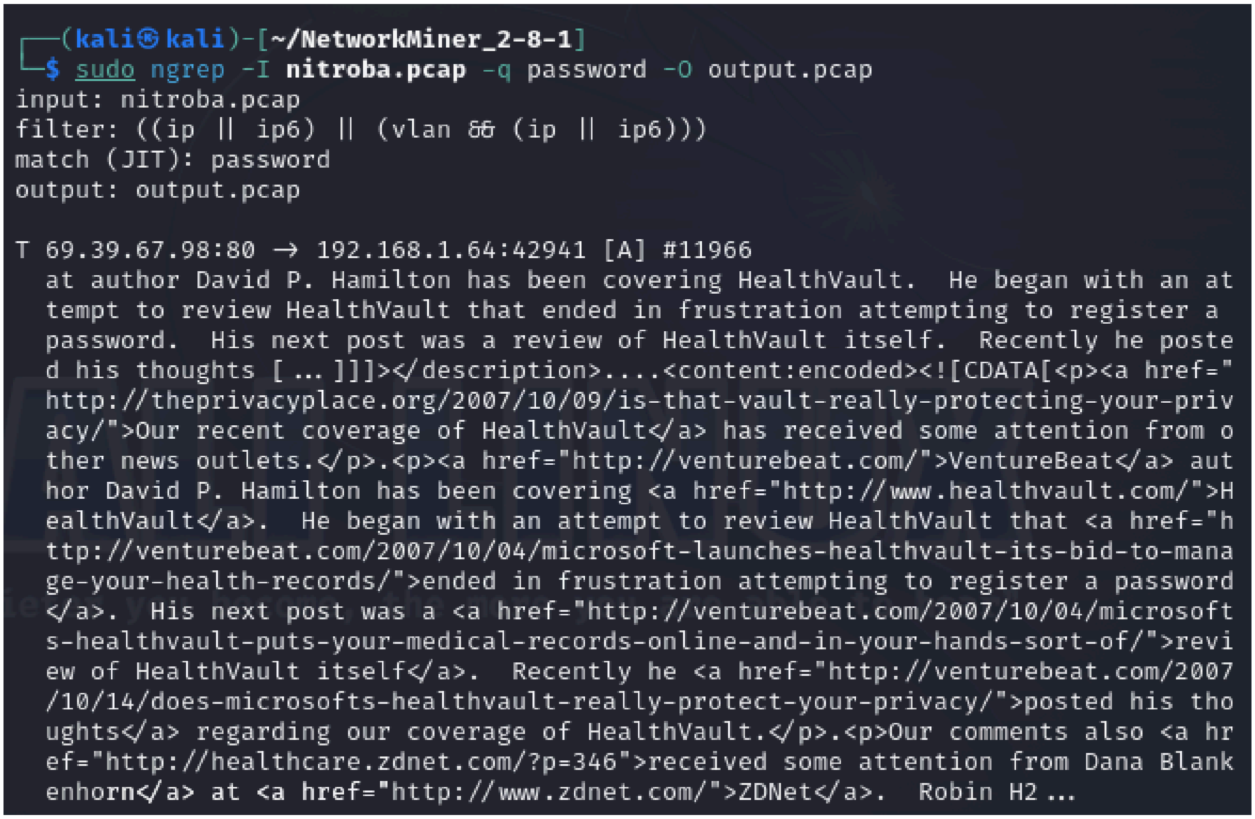


```
──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo ngrep -I nitroba.pcap -q password
input: nitroba.pcap
filter: ((ip || ip6) || (vlan && (ip || ip6)))
match (JIT): password

T 69.39.67.98:80 → 192.168.1.64:42941 [A] #11966
  at author David P. Hamilton has been covering HealthVault.  He began with an at
  tempt to review HealthVault that ended in frustration attempting to register a
  password.  His next post was a review of HealthVault itself.  Recently he poste
  d his thoughts [ ... ]]]></description>....<content:encoded><![CDATA[<p><a href="
  http://theprivacyplace.org/2007/10/09/is-that-vault-really-protecting-your-priv
  acy/">Our recent coverage of HealthVault</a> has received some attention from o
  ther news outlets.</p>.<p><a href="http://venturebeat.com/">VentureBeat</a> aut
  hor David P. Hamilton has been covering <a href="http://www.healthvault.com/">H
  ealthVault</a>.  He began with an attempt to review HealthVault that <a href="h
  ttp://venturebeat.com/2007/10/04/microsoft-launches-healthvault-its-bid-to-mana
  ge-your-health-records/">ended in frustration attempting to register a password
  </a>.  His next post was a <a href="http://venturebeat.com/2007/10/04/microsoft
```

Now that whe should be in the directory that contain the pcap file
Lets run this command:
Sudo ngrep -I nitroba.pcap -q password

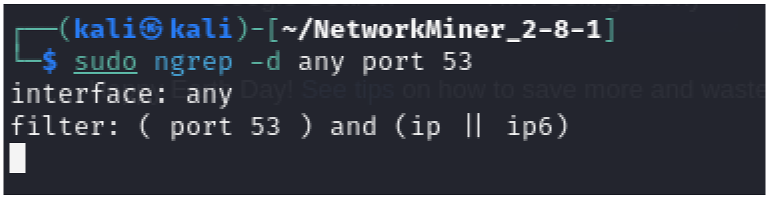
Toan c Ngo
Date:4/24/24

What we doing here is run the ngrep command in case sensitive search for the file nitroba.pcap with the search term password and with the option of -q where it excluding everything else.



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo ngrep -I nitroba.pcap -q password -O output.pcap
input: nitroba.pcap
filter: ((ip || ip6) || (vlan && (ip || ip6)))
match (JIT): password
output: output.pcap

T 69.39.67.98:80 → 192.168.1.64:42941 [A] #11966
  at author David P. Hamilton has been covering HealthVault.  He began with an at
  tempt to review HealthVault that ended in frustration attempting to register a
  password.  His next post was a review of HealthVault itself.  Recently he poste
  d his thoughts [ … ]]]></description>....<content:encoded><![CDATA[<p><a href="
  http://theprivacyplace.org/2007/10/09/is-that-vault-really-protecting-your-priv
  acy/">Our recent coverage of HealthVault</a> has received some attention from o
  ther news outlets.</p>.<p><a href="http://venturebeat.com/">VentureBeat</a> aut
  hor David P. Hamilton has been covering <a href="http://www.healthvault.com/">H
  ealthVault</a>.  He began with an attempt to review HealthVault that <a href="h
  ttp://venturebeat.com/2007/10/04/microsoft-launches-healthvault-its-bid-to-mana
  ge-your-health-records/">ended in frustration attempting to register a password
  </a>. His next post was a <a href="http://venturebeat.com/2007/10/04/microsoft
  s-healthvault-puts-your-medical-records-online-and-in-your-hands-sort-of/">revi
  ew of HealthVault itself</a>.  Recently he <a href="http://venturebeat.com/2007
  /10/14/does-microsofts-healthvault-really-protect-your-privacy/">posted his tho
  ughts</a> regarding our coverage of HealthVault.</p>.<p>Our comments also <a hr
  ef="http://healthcare.zdnet.com/?p=346">received some attention from Dana Blank
  enhorn</a> at <a href="http://www.zdnet.com/">ZDNet</a>.  Robin H2 …
```

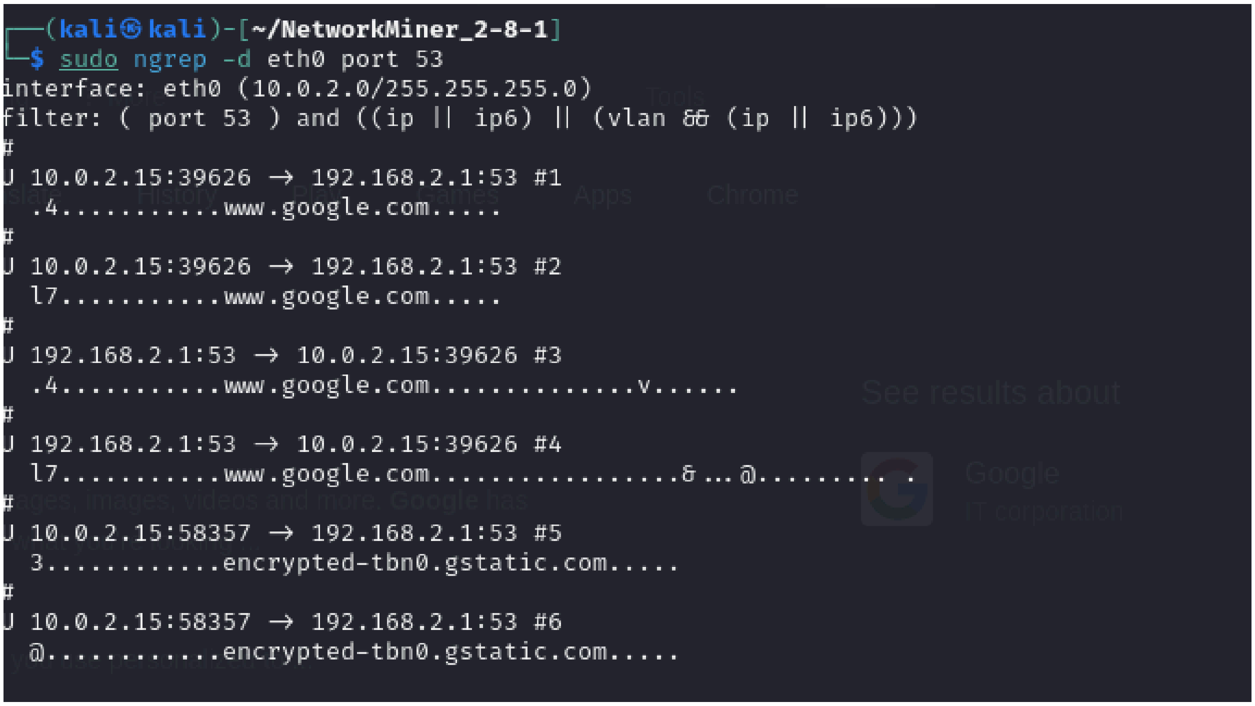
This command is working the same way as the above command but with one small different and that is the -O output.pcap this mean that ngrep searches the packet that contain the work password and output it into a file called output.pcap.



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo ngrep -d any port 53
interface: any
filter: ( port 53 ) and (ip || ip6)
█
```

You can also use ngrep to filter out the port connection as well.
This will display anything that connects to the port 53 on your local machine.

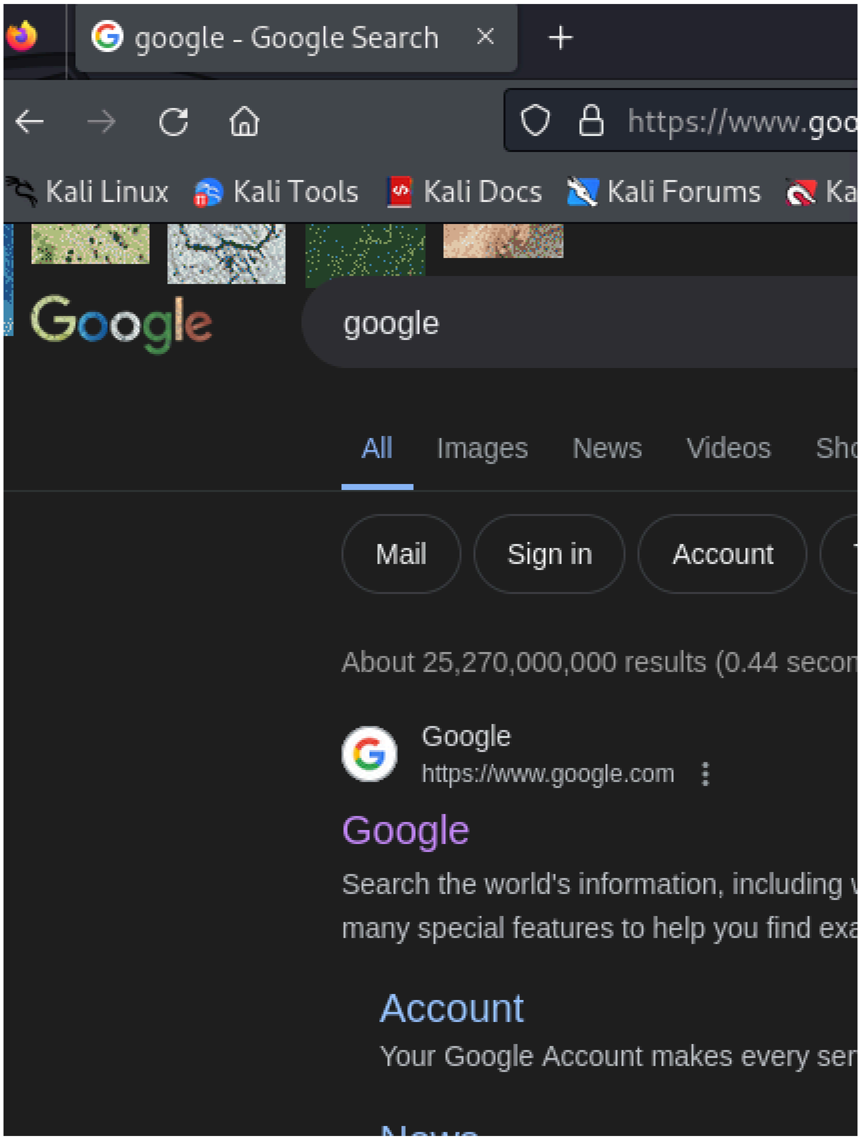
Toan c Ngo
Date:4/24/24



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo ngrep -d eth0 port 53
interface: eth0 (10.0.2.0/255.255.255.0)
filter: ( port 53 ) and ((ip || ip6) || (vlan && (ip || ip6)))
#
U 10.0.2.15:39626 -> 192.168.2.1:53 #1
  .4...........www.google.com.....
#
U 10.0.2.15:39626 -> 192.168.2.1:53 #2
  l7...........www.google.com.....
#
U 192.168.2.1:53 -> 10.0.2.15:39626 #3
  .4...........www.google.com.............v......
#
U 192.168.2.1:53 -> 10.0.2.15:39626 #4
  l7...........www.google.com................&...@......... .
#
U 10.0.2.15:58357 -> 192.168.2.1:53 #5
  3............encrypted-tbn0.gstatic.com.....
#
U 10.0.2.15:58357 -> 192.168.2.1:53 #6
  @............encrypted-tbn0.gstatic.com.....
```

Same as above but in this we want to specifically listen to port 53 with eth0
And as you can see it displays the port 53 are being used to connect to google website.

Toan c Ngo
Date:4/24/24



About 25,270,000,000 results (0.44 secon

Google
https://www.google.com

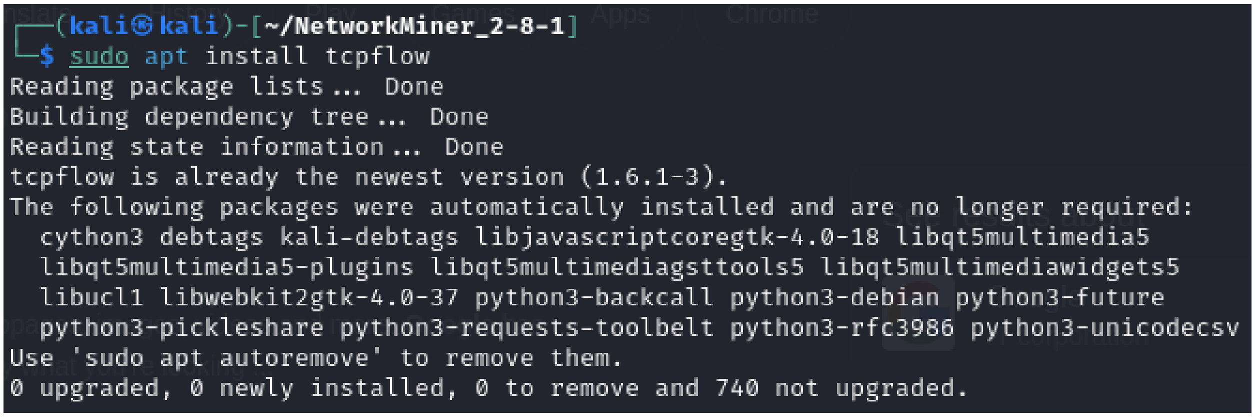
Google

Search the world's information, including v
many special features to help you find exa

Account

Your Google Account makes every ser

This is another application in the same system that I used to contact google.



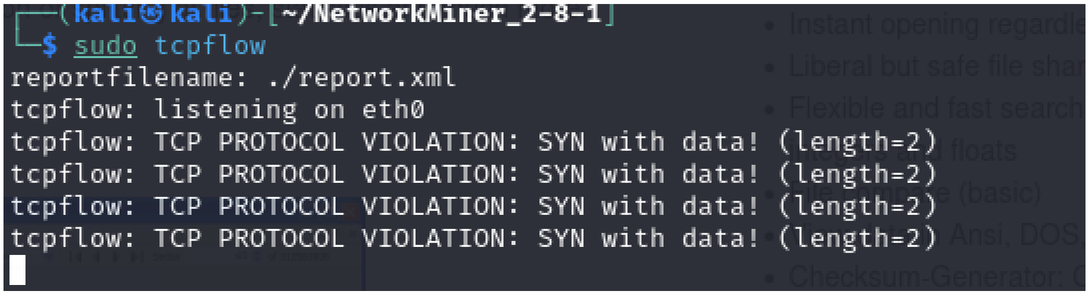
```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo apt install tcpflow
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tcpflow is already the newest version (1.6.1-3).
The following packages were automatically installed and are no longer required:
  cython3 debtags kali-debtags libjavascriptcoregtk-4.0-18 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5
  libucl1 libwebkit2gtk-4.0-37 python3-backcall python3-debian python3-future
  python3-pickleshare python3-requests-toolbelt python3-rfc3986 python3-unicodecsv
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 740 not upgraded.
```

Next we will use another tool that helps capture that data using TCP connection.
This tool is called tcpflow and is used to capture incoming and outgoing tcp packets.

Toan c Ngo
Date:4/24/24

Lets run a command that install the tools: sudo apt install tcpflow

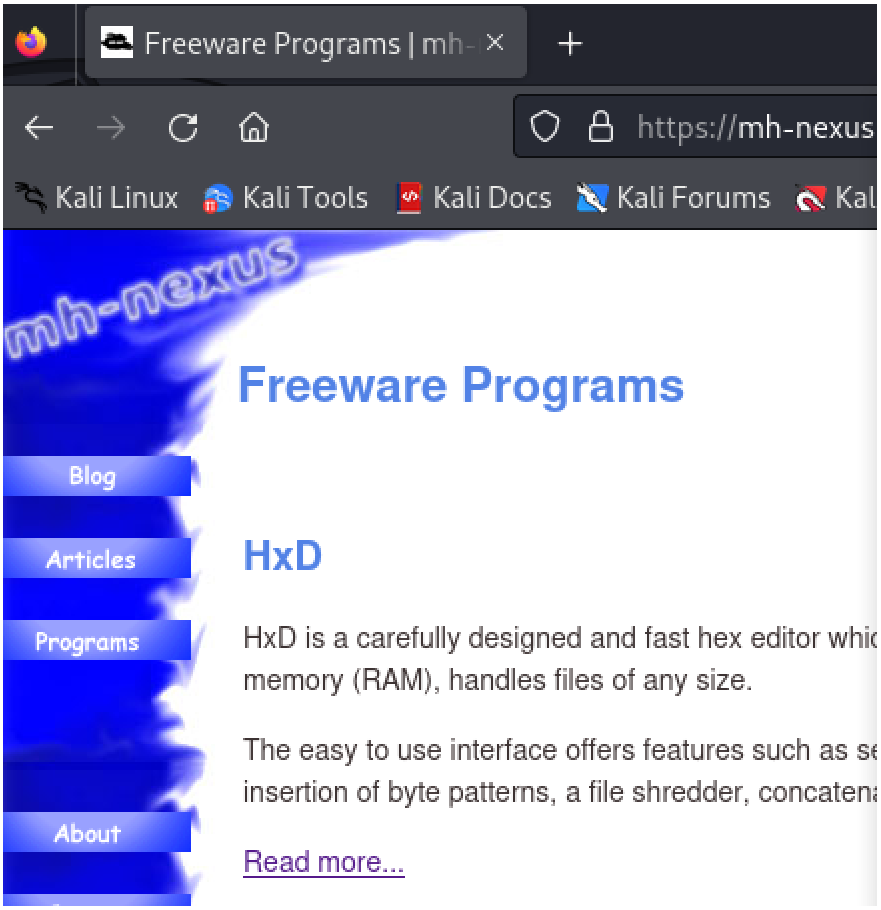
Here is the list of option of what you can do with it:
-B force binary output
-b capture no more than max_bytes bytes per flow
-c console print without storing any captured data
-C console print without the packet source and destination details being printed
-i capture traffic for a particular interface
-r read from a pcap file



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo tcpflow
reportfilename: ./report.xml
tcpflow: listening on eth0
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
```

Now lets us test out the tool by running it: sudo tcpflow
The tool will now start the packet capturing process and for each packet it will get stored in a separated files

Toan c Ngo
Date:4/24/24



Freeware Programs

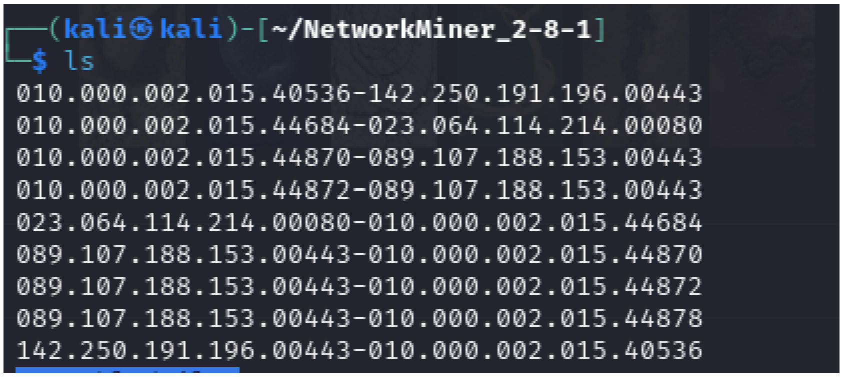
HxD

HxD is a carefully designed and fast hex editor whic
memory (RAM), handles files of any size.

The easy to use interface offers features such as se
insertion of byte patterns, a file shredder, concaten

Read more...

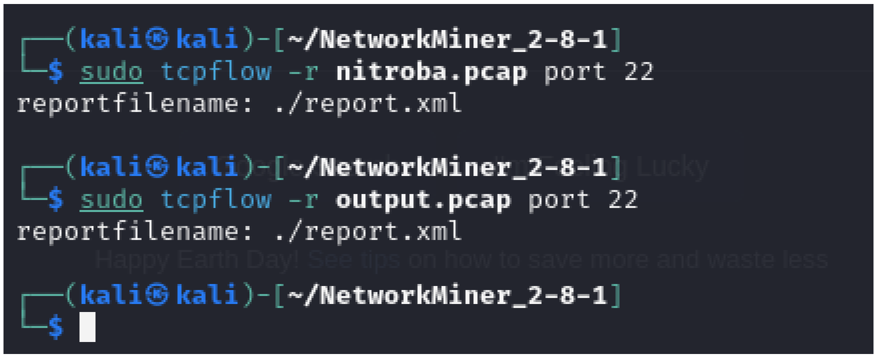
Just for demonstration I opened a website to trigger the tcp packets connection.



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ ls
010.000.002.015.40536-142.250.191.196.00443
010.000.002.015.44684-023.064.114.214.00080
010.000.002.015.44870-089.107.188.153.00443
010.000.002.015.44872-089.107.188.153.00443
023.064.114.214.00080-010.000.002.015.44684
089.107.188.153.00443-010.000.002.015.44870
089.107.188.153.00443-010.000.002.015.44872
089.107.188.153.00443-010.000.002.015.44878
142.250.191.196.00443-010.000.002.015.40536
```

Now after you run the tcpflow and open a website do ctrl+c to stop the tcpflow and look into the current directory using ls, you should see all the file that was captured using tcpflow.

Toan c Ngo
Date:4/24/24



```
┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo tcpflow -r nitroba.pcap port 22
reportfilename: ./report.xml

┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ sudo tcpflow -r output.pcap port 22
reportfilename: ./report.xml

┌──(kali㉿kali)-[~/NetworkMiner_2-8-1]
└─$ 
```

You could also use tcpflow to extract information from pcap file as well
In this case i use tcpflow to extract all the information that related to port 22 using recursion (-r)

To sum everything up, you can use the autopsy tool to extract and gather system image file information, you could also use these tools to generate a report or let other investigators work alongside you with the same file. We also took a look at some networking forensic tools one tools have a UI where you can trace and find where the connection are coming from, another one are use to analyze the traffic of the pcap files or you could also use it to listening to a live port connection of your choice, where you can generate a report based on the packet you get using the ngrep tools, and the final tool are call tcpflow which use to analyze the information that contains in the tcp connection of input and output port. For tcpflow you could use this tool to capture live tcp connection as well as extracting ssh packets from files. As a digital forensic investigator It entirely depends on your to select which tools are the most suitable for the jobs.

Toan c Ngo
Date:4/24/24

Source

Normal criminal autopsy
https://www.merriam-webster.com/dictionary/autopsy

Autopsy in digital forensic
https://www.ccslearningacademy.com/what-is-autopsy-in-cybersecurity/

Network forensic
https://onlinedegrees.sandiego.edu/network-forensics/

All others information are found in the lap12 and lap14 pdf