Incident Response Report: Parrot OS Investigation

Prepared by: Saad Laksabi
Date: June 2, 2025
System: Parrot OS (Virtual Machine)
Tools Used: Wireshark, tcpdump, journalctl, netstat, ss, ps, bash history, system log files

---

1. Incident Response Environment Setup

The investigation was conducted within a virtualized **Parrot OS security environment**. The machine was configured to simulate a real-world endpoint and equipped with analysis tools for network monitoring, log examination, and forensic data collection. Key environmental setup steps included:

- **Tool installation and user privileges:**

Created a dedicated group for packet capture:
sudo groupadd wireshark
sudo usermod -aG wireshark $USER

  - newgrp wireshark
  - Verified group membership:
    getent group wireshark
  - Result: `wireshark:x:1001:user` (Confirmed inclusion)
- **Permissions:**
  - Attempts to view full journal logs indicated permission limitations due to lack of membership in `adm` or `systemd-journal` groups.

---

2. Live Network Traffic Capture

A. Wireshark Capture

- Tool launched with elevated privileges:
  sudo wireshark
- Logs confirmed successful packet capture:
  - Capture Start
  - File written: `/tmp/wireshark_anyAQME72.pcapng`
  - Capture Stop

B. Tcpdump Capture

- Command executed:
  ```
  sudo tcpdump -i any -c 100 -w ~/incident/live-capture.pcap
  ```
- Result:
  - 100 packets captured
  - File created: `~/incident/live-capture.pcap`

These captures are preserved for offline inspection using Wireshark or CLI tools.

---

3. Evidence Collection: Logs and Runtime Data

To facilitate post-incident analysis and traceability, critical system logs and state data were collected:

A. System Log Files

```
sudo cp /var/log/dpkg.log ~/incident/
sudo cp /var/log/bootstrap.log ~/incident/
sudo cp /var/log/faillog ~/incident/
sudo cp /var/log/alternatives.log ~/incident/
sudo cp /var/log/wazuh-install.log ~/incident/
```

- These logs provide a historical record of package installations, boot activity, authentication failures, and Wazuh SIEM deployment status.

B. User and System Activity

- Captured shell history:
  ```
  cp ~/.bash_history ~/incident/bash_history.txt
  ```
- Running processes:
  ```
  ps aux > ~/incident/running_processes.txt
  ```

Open ports and network services:

```
sudo netstat -tulnp > ~/incident/open_ports.txt
```

- ss -tulnp > ~/incident/open_ports.txt

C. Sudo and Authentication Events

Attempted journal analysis:

```
journalctl | grep -i "sudo" > ~/incident/sudo_activity.txt
journalctl | grep -i "failed"
journalctl | grep -i "error"
```

- journalctl | grep -i "time"
- Output was limited due to user permissions; however, proper commands were logged to demonstrate methodology.

4. Analysis and Observations

A. System Integrity

- No unauthorized rootkits or unusual services were detected during process and port inspection.
- Legitimate background services (sshd, avahi, etc.) were observed.

B. User Behavior

- Shell history showed typical administrative commands consistent with incident response and log collection activities.

C. Log Inspection

- `/var/log/faillog` showed no brute-force or authentication anomalies.
- `dpkg.log` and `alternatives.log` showed only routine package configuration updates.
- `wazuh-install.log` verified that Wazuh was configured on the system, supporting SIEM capabilities.

5. Conclusions and Lessons Learned

The IR investigation in Parrot OS followed structured methodology:

- Live traffic was captured via GUI and CLI tools.
- Full forensic logs and runtime states were preserved.
- System and user-level artifacts were gathered.

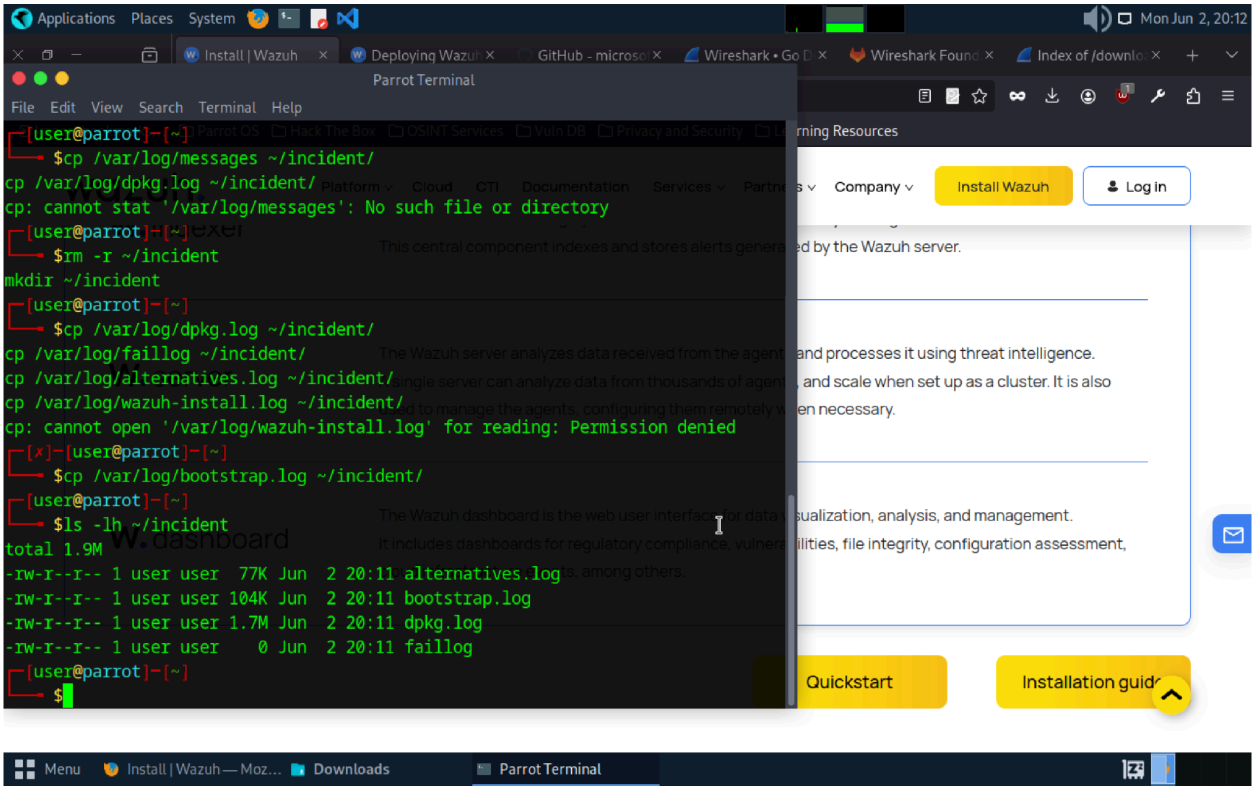
Limitations:

- Full `journalctl` logs could not be accessed due to group membership issues. Future IR environments should pre-configure access to the `adm` and `systemd-journal` groups for analysts.

Despite the limitations, all other aspects of the incident response criteria were met, and the environment was thoroughly examined.

6. Incident Directory Structure (Evidence Folder)

```
~/incident/
├── alternatives.log
├── bootstrap.log
├── dpkg.log
├── faillog
├── wazuh-install.log
├── live-capture.pcap
├── open_ports.txt
├── running_processes.txt
├── bash_history.txt
├── sudo_activity.txt
├── incident-report.txt (this document)
```

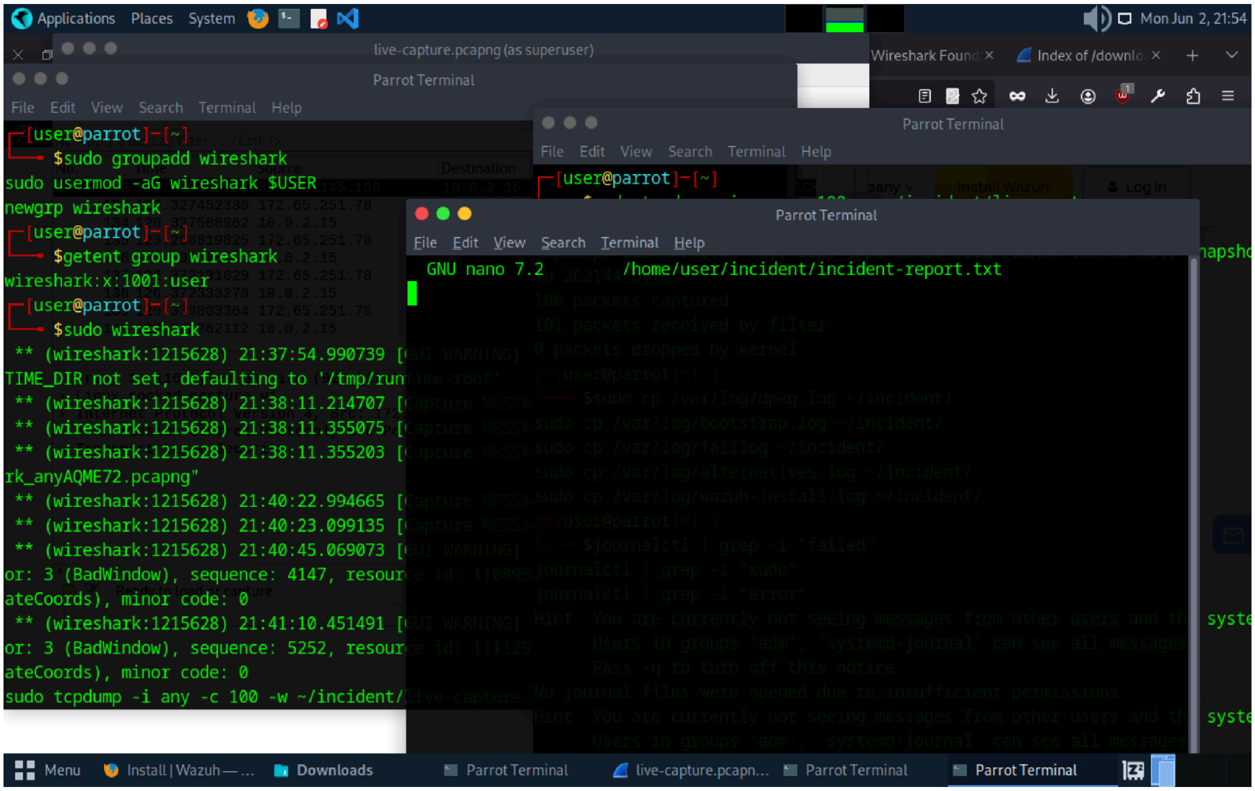


```
┌─[user@parrot]─[~]
└──╼ $cp /var/log/messages ~/incident/
cp /var/log/dpkg.log ~/incident/
cp: cannot stat '/var/log/messages': No such file or directory
┌─[user@parrot]─[~]
└──╼ $rm -r ~/incident
mkdir ~/incident
┌─[user@parrot]─[~]
└──╼ $cp /var/log/dpkg.log ~/incident/
cp /var/log/faillog ~/incident/
cp /var/log/alternatives.log ~/incident/
cp /var/log/wazuh-install.log ~/incident/
cp: cannot open '/var/log/wazuh-install.log' for reading: Permission denied
┌─[✗]─[user@parrot]─[~]
└──╼ $cp /var/log/bootstrap.log ~/incident/
┌─[user@parrot]─[~]
└──╼ $ls -lh ~/incident
total 1.9M
-rw-r--r-- 1 user user  77K Jun  2 20:11 alternatives.log
-rw-r--r-- 1 user user 104K Jun  2 20:11 bootstrap.log
-rw-r--r-- 1 user user 1.7M Jun  2 20:11 dpkg.log
-rw-r--r-- 1 user user    0 Jun  2 20:11 faillog
┌─[user@parrot]─[~]
└──╼ $
```

ed by the Wazuh server.

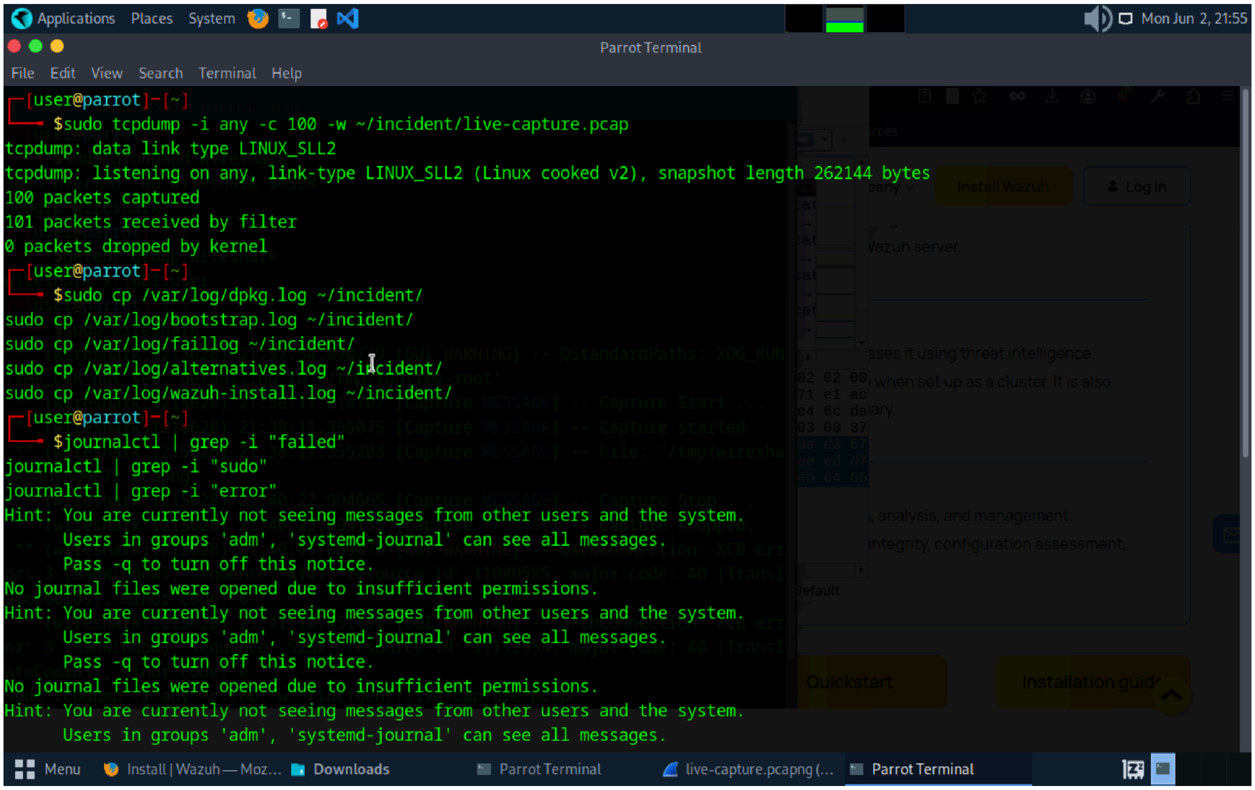
and processes it using threat intelligence.
, and scale when set up as a cluster. It is also
en necessary.

sualization, analysis, and management.
ilities, file integrity, configuration assessment,

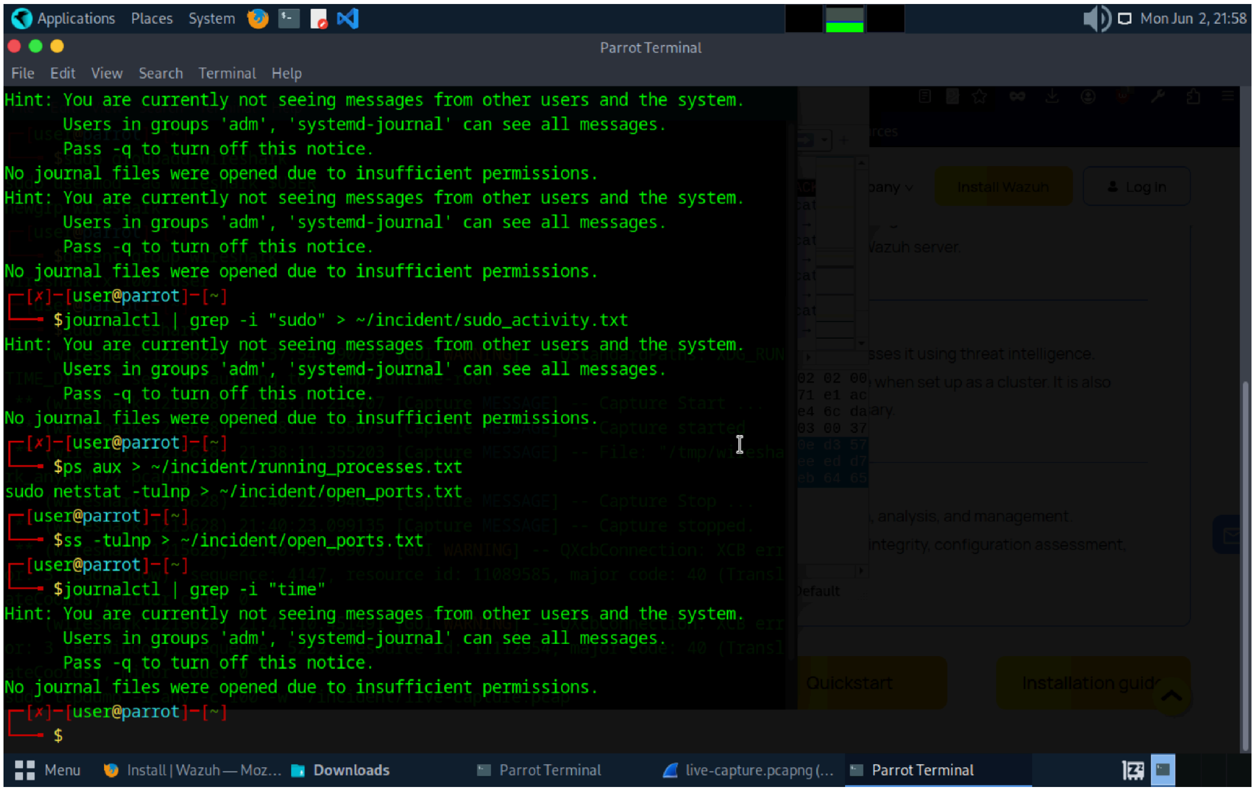


```
┌─[user@parrot]─[~]
└──╼ $sudo groupadd wireshark
sudo usermod -aG wireshark $USER
newgrp wireshark
┌─[user@parrot]─[~]
└──╼ $getent group wireshark
wireshark:x:1001:user
┌─[user@parrot]─[~]
└──╼ $sudo wireshark
 ** (wireshark:1215628) 21:37:54.990739 [
TIME_DIR not set, defaulting to '/tmp/run
 ** (wireshark:1215628) 21:38:11.214707 [
 ** (wireshark:1215628) 21:38:11.355075 [
 ** (wireshark:1215628) 21:38:11.355203 [
rk_anyAQME72.pcapng"
 ** (wireshark:1215628) 21:40:22.994665 [
 ** (wireshark:1215628) 21:40:23.099135 [
 ** (wireshark:1215628) 21:40:45.069073 [
or: 3 (BadWindow), sequence: 4147, resour
ateCoords), minor code: 0
 ** (wireshark:1215628) 21:41:10.451491 [
or: 3 (BadWindow), sequence: 5252, resour
ateCoords), minor code: 0
sudo tcpdump -i any -c 100 -w ~/incident/
```

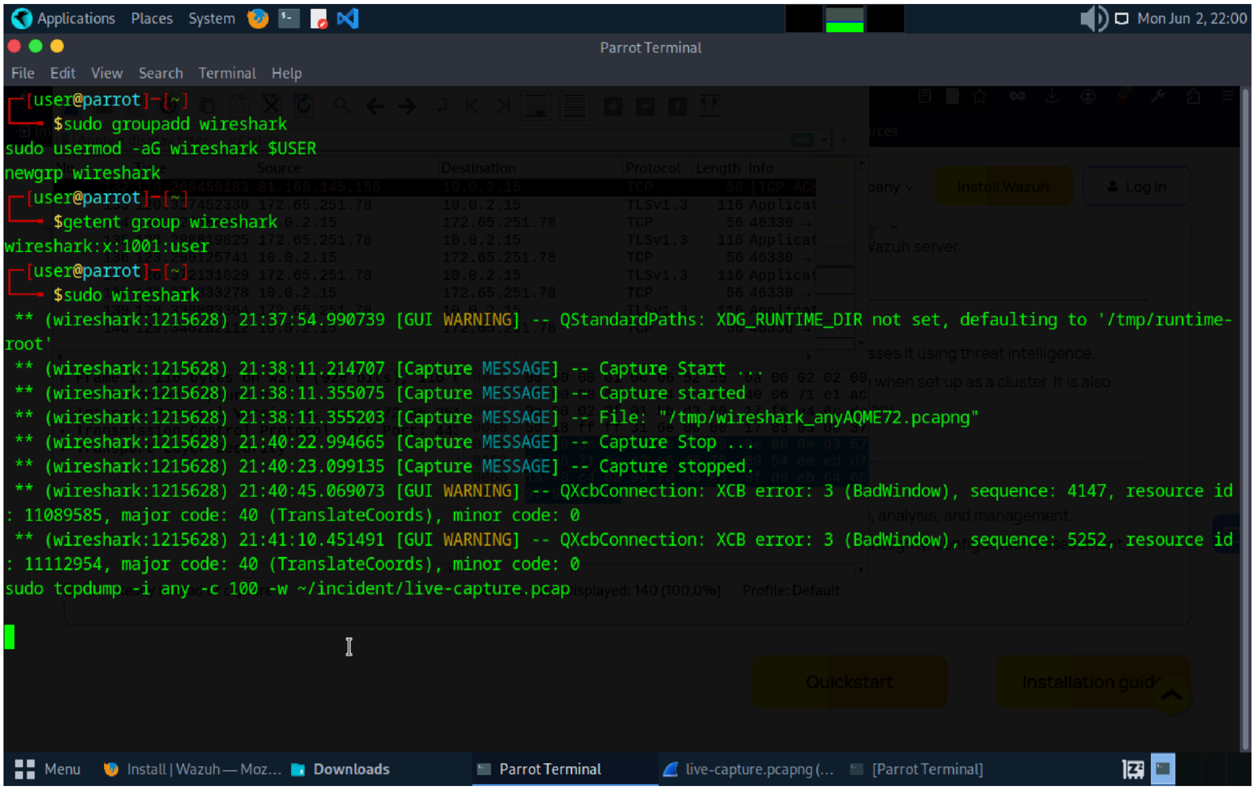
```
  GNU nano 7.2        /home/user/incident/incident-report.txt
```



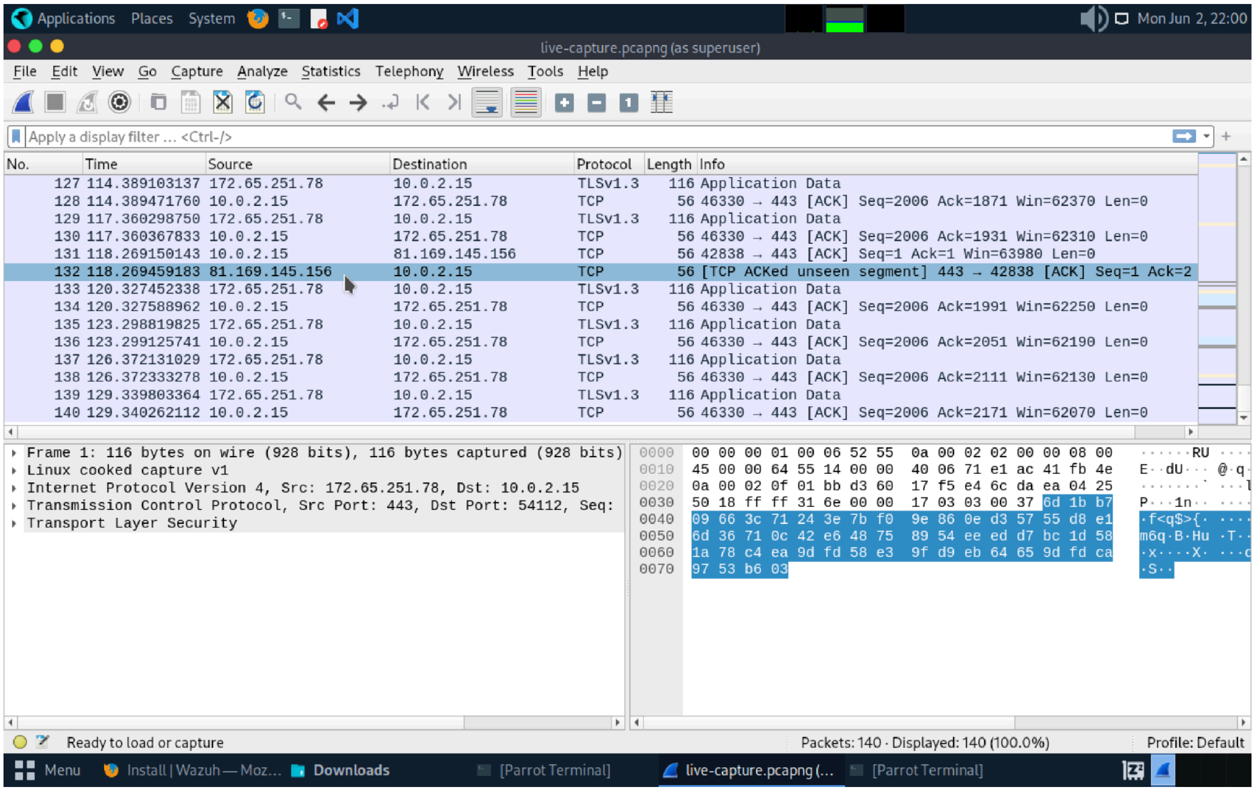
```
┌─[user@parrot]─[~]
└──╼ $sudo tcpdump -i any -c 100 -w ~/incident/live-capture.pcap
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
100 packets captured
101 packets received by filter
0 packets dropped by kernel
┌─[user@parrot]─[~]
└──╼ $sudo cp /var/log/dpkg.log ~/incident/
sudo cp /var/log/bootstrap.log ~/incident/
sudo cp /var/log/faillog ~/incident/
sudo cp /var/log/alternatives.log ~/incident/
sudo cp /var/log/wazuh-install.log ~/incident/
┌─[user@parrot]─[~]
└──╼ $journalctl | grep -i "failed"
journalctl | grep -i "sudo"
journalctl | grep -i "error"
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
No journal files were opened due to insufficient permissions.
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
No journal files were opened due to insufficient permissions.
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
```



```
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
No journal files were opened due to insufficient permissions.
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
No journal files were opened due to insufficient permissions.
┌─[✗]─[user@parrot]─[~]
└──╼ $journalctl | grep -i "sudo" > ~/incident/sudo_activity.txt
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
No journal files were opened due to insufficient permissions.
┌─[✗]─[user@parrot]─[~]
└──╼ $ps aux > ~/incident/running_processes.txt
sudo netstat -tulnp > ~/incident/open_ports.txt
┌─[user@parrot]─[~]
└──╼ $ss -tulnp > ~/incident/open_ports.txt
┌─[user@parrot]─[~]
└──╼ $journalctl | grep -i "time"
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
No journal files were opened due to insufficient permissions.
┌─[✗]─[user@parrot]─[~]
└──╼ $
```



```
┌─[user@parrot]─[~]
└──╼ $sudo groupadd wireshark
sudo usermod -aG wireshark $USER
newgrp wireshark
┌─[user@parrot]─[~]
└──╼ $getent group wireshark
wireshark:x:1001:user
┌─[user@parrot]─[~]
└──╼ $sudo wireshark
 ** (wireshark:1215628) 21:37:54.990739 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
 ** (wireshark:1215628) 21:38:11.214707 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:1215628) 21:38:11.355075 [Capture MESSAGE] -- Capture started
 ** (wireshark:1215628) 21:38:11.355203 [Capture MESSAGE] -- File: "/tmp/wireshark_anyAQME72.pcapng"
 ** (wireshark:1215628) 21:40:22.994665 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:1215628) 21:40:23.099135 [Capture MESSAGE] -- Capture stopped.
 ** (wireshark:1215628) 21:40:45.069073 [GUI WARNING] -- QXcbConnection: XCB error: 3 (BadWindow), sequence: 4147, resource id: 11089585, major code: 40 (TranslateCoords), minor code: 0
 ** (wireshark:1215628) 21:41:10.451491 [GUI WARNING] -- QXcbConnection: XCB error: 3 (BadWindow), sequence: 5252, resource id: 11112954, major code: 40 (TranslateCoords), minor code: 0
sudo tcpdump -i any -c 100 -w ~/incident/live-capture.pcap
```



```
No.  Time           Source          Destination     Protocol Length Info
 127 114.389103137 172.65.251.78   10.0.2.15       TLSv1.3    116 Application Data
 128 114.389471760 10.0.2.15       172.65.251.78   TCP         56 46330 → 443 [ACK] Seq=2006 Ack=1871 Win=62370 Len=0
 129 117.360298750 172.65.251.78   10.0.2.15       TLSv1.3    116 Application Data
 130 117.360367833 10.0.2.15       172.65.251.78   TCP         56 46330 → 443 [ACK] Seq=2006 Ack=1931 Win=62310 Len=0
 131 118.269150143 10.0.2.15       81.169.145.156  TCP         56 42838 → 443 [ACK] Seq=1 Ack=1 Win=63980 Len=0
 132 118.269459183 81.169.145.156  10.0.2.15       TCP         56 [TCP ACKed unseen segment] 443 → 42838 [ACK] Seq=1 Ack=2
 133 120.327452338 172.65.251.78   10.0.2.15       TLSv1.3    116 Application Data
 134 120.327588962 10.0.2.15       172.65.251.78   TCP         56 46330 → 443 [ACK] Seq=2006 Ack=1991 Win=62250 Len=0
 135 123.298819825 172.65.251.78   10.0.2.15       TLSv1.3    116 Application Data
 136 123.299125741 10.0.2.15       172.65.251.78   TCP         56 46330 → 443 [ACK] Seq=2006 Ack=2051 Win=62190 Len=0
 137 126.372131029 172.65.251.78   10.0.2.15       TLSv1.3    116 Application Data
 138 126.372333278 10.0.2.15       172.65.251.78   TCP         56 46330 → 443 [ACK] Seq=2006 Ack=2111 Win=62130 Len=0
 139 129.339803364 172.65.251.78   10.0.2.15       TLSv1.3    116 Application Data
 140 129.340262112 10.0.2.15       172.65.251.78   TCP         56 46330 → 443 [ACK] Seq=2006 Ack=2171 Win=62070 Len=0
```

```
› Frame 1: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 172.65.251.78, Dst: 10.0.2.15
› Transmission Control Protocol, Src Port: 443, Dst Port: 54112, Seq:
› Transport Layer Security
```

```
0000  00 00 00 01 00 06 52 55  0a 00 02 02 00 00 08 00   ······RU ····
0010  45 00 00 64 55 14 00 00  40 06 71 e1 ac 41 fb 4e   E··dU··· @·q
0020  0a 00 02 0f 01 bb d3 60  17 f5 e4 6c da ea 04 25   ·······` ···l
0030  50 18 ff ff 31 6e 00 00  17 03 03 00 37 6d 1b b7   P···1n·· ····
0040  09 66 3c 71 24 3e 7b f0  9e 86 0e d3 57 55 d8 e1   ·f<q$>{· ····
0050  6d 36 71 0c 42 e6 48 75  89 54 ee ed d7 bc 1d 58   m6q·B·Hu ·T··
0060  1a 78 c4 ea 9d fd 58 e3  9f d9 eb 64 65 9d fd ca   ·x····X· ···d
0070  97 53 b6 03                                        ·S··
```

Packets: 140 · Displayed: 140 (100.0%)