Automated Packet Capture and Analysis on Kali Linux with tcpdump & Wireshark

In this self-designed lab, I created a streamlined environment to simulate, capture, and analyze network traffic using `tcpdump`, Bash scripting, and Wireshark. I initiated traffic using `ping` and `ssh` commands, scripted automated capture sessions via `.sh` files, and saved packets into structured `.pcap` files for analysis.

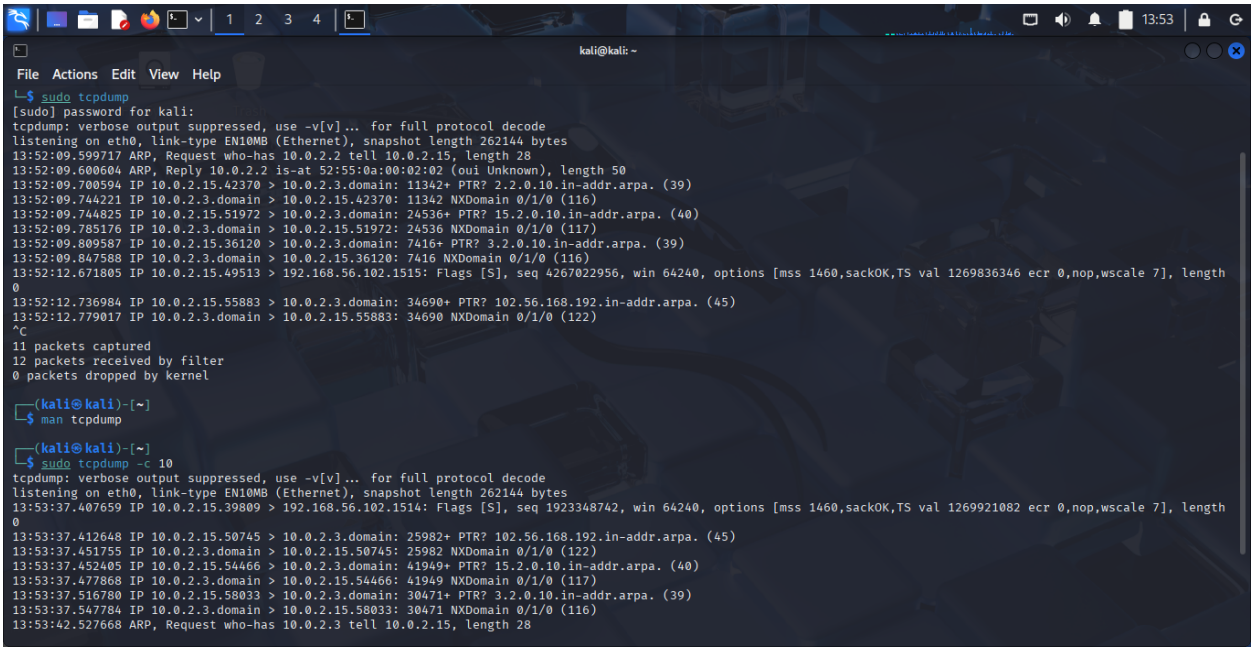
I experimented with advanced `tcpdump` flags (`-c`, `-G`, `-w`, `-nn`, `-xx`, etc.), and built timestamped logging and filtering rules to isolate flows from domains like `coursera.org`. To validate, I ran parallel sessions (e.g., `ping localhost`) while capturing on another terminal, verifying functionality across multiple use-cases.

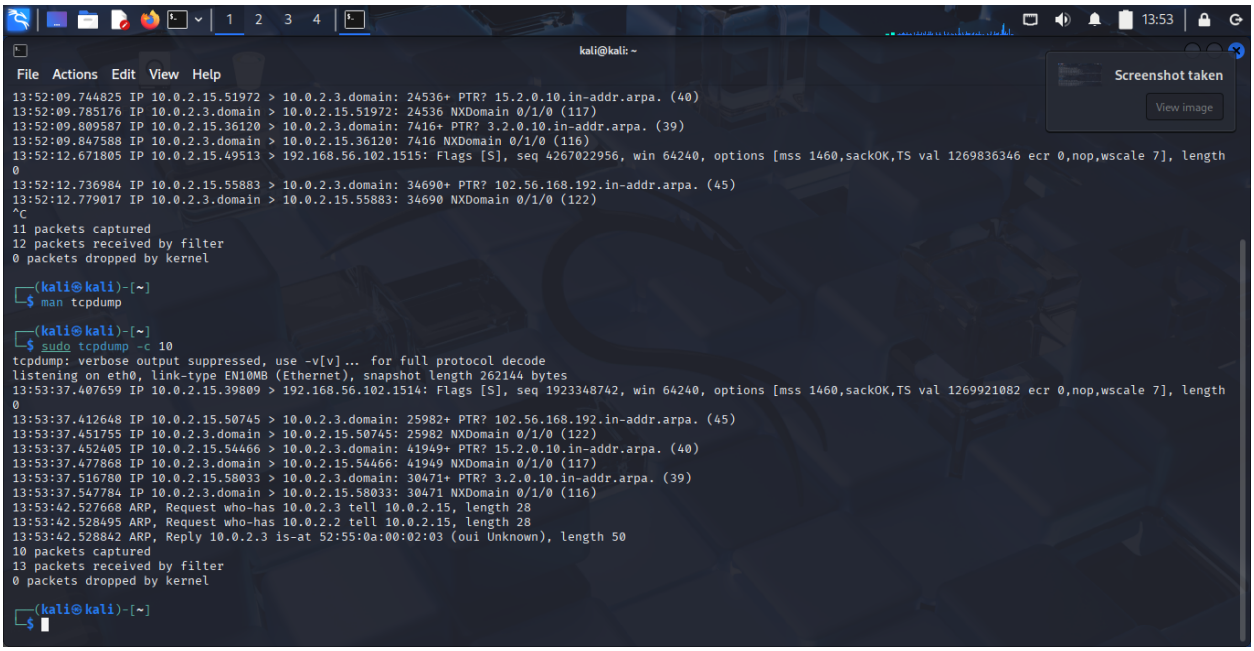
Using Wireshark, I transformed raw `.pcap` data into readable traffic views — confirming timestamps, port usage, protocol breakdowns, and packet counts. This project showcases my ability to automate repetitive CLI tasks, analyze network behavior, and communicate findings in a reproducible, scalable format.

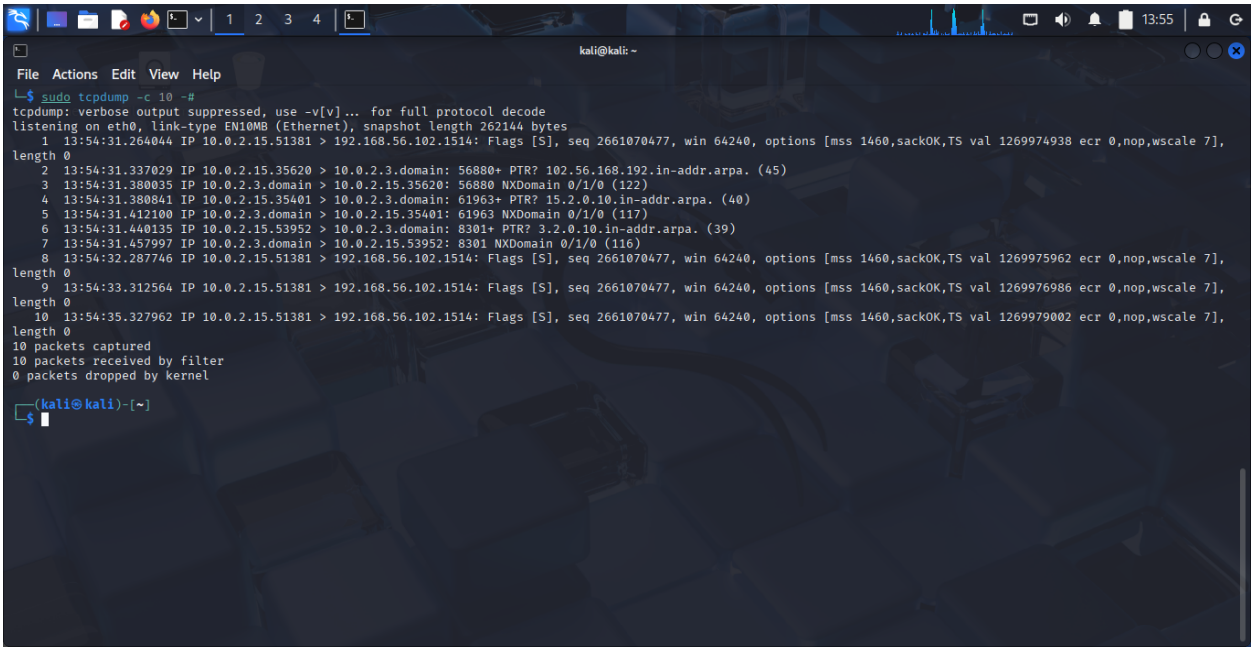
Screenshots & Demo Walkthrough

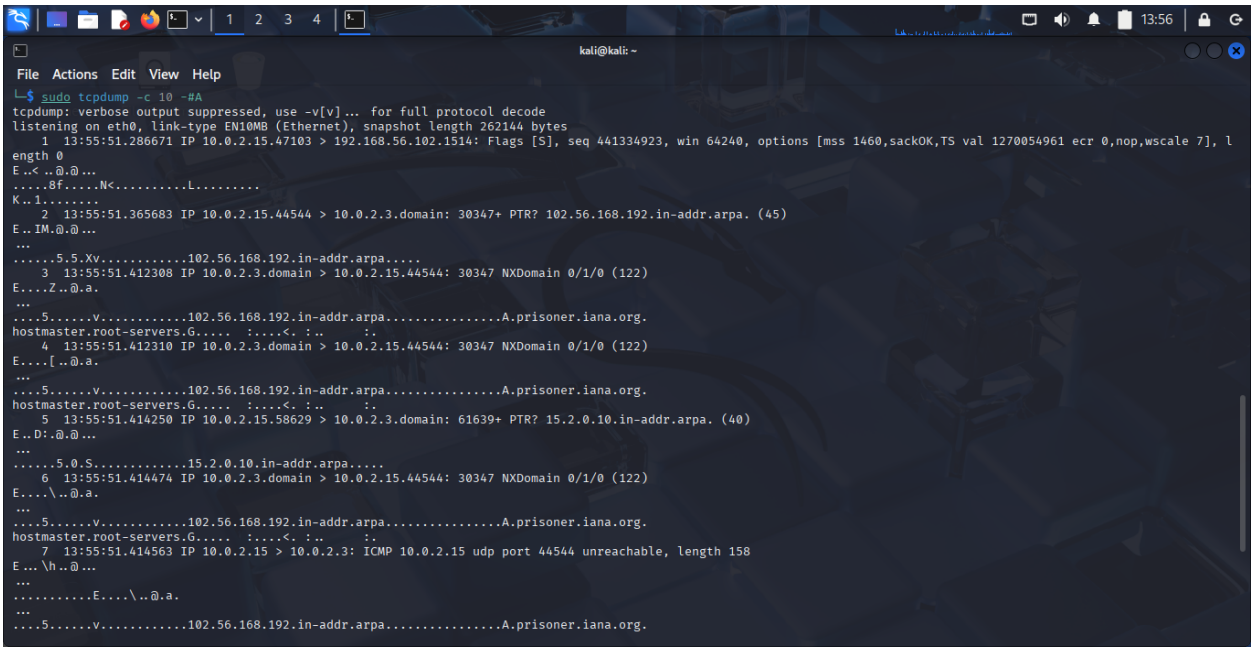
Packet Capture Kickoff (tcpdump on Kali Linux)

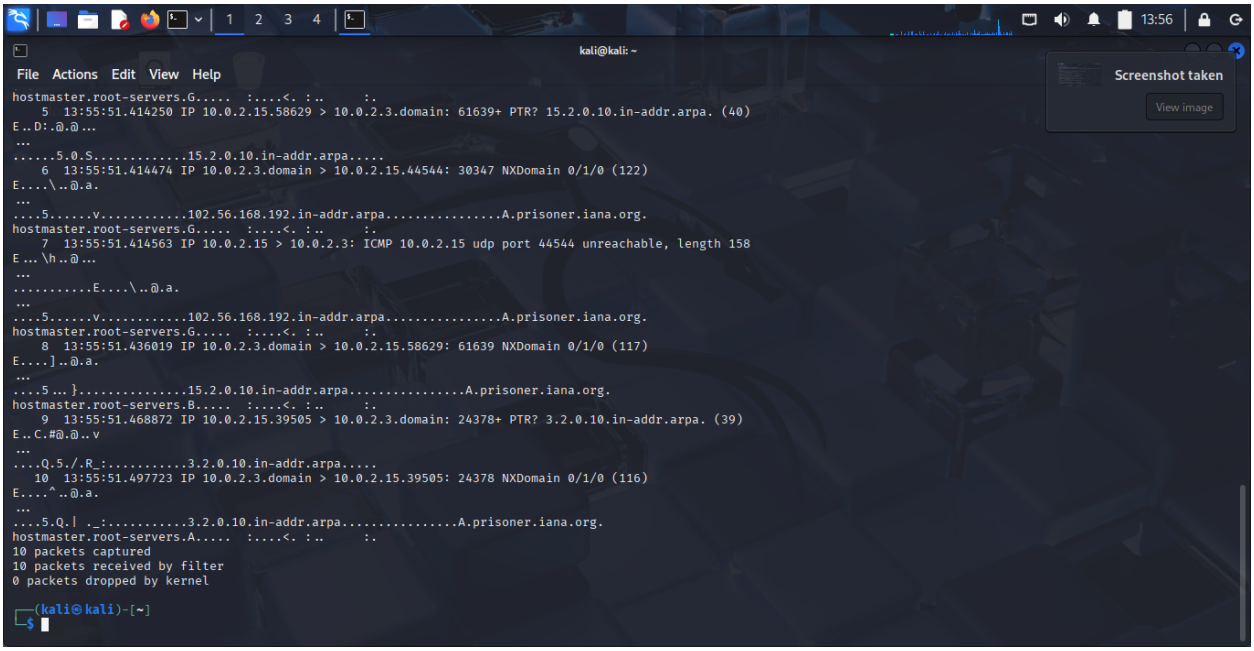
Initiated live traffic capture using `sudo tcpdump` on Kali. Reviewed syntax via `man tcpdump`, then tested with `-c 10` to capture a limited packet set. Explored advanced flags like `-A` (ASCII output), `-X` (hex + ASCII), and `-xx` (full hex dump) to inspect payloads and headers in-depth — building a strong foundation for filtered, scriptable packet analysis.

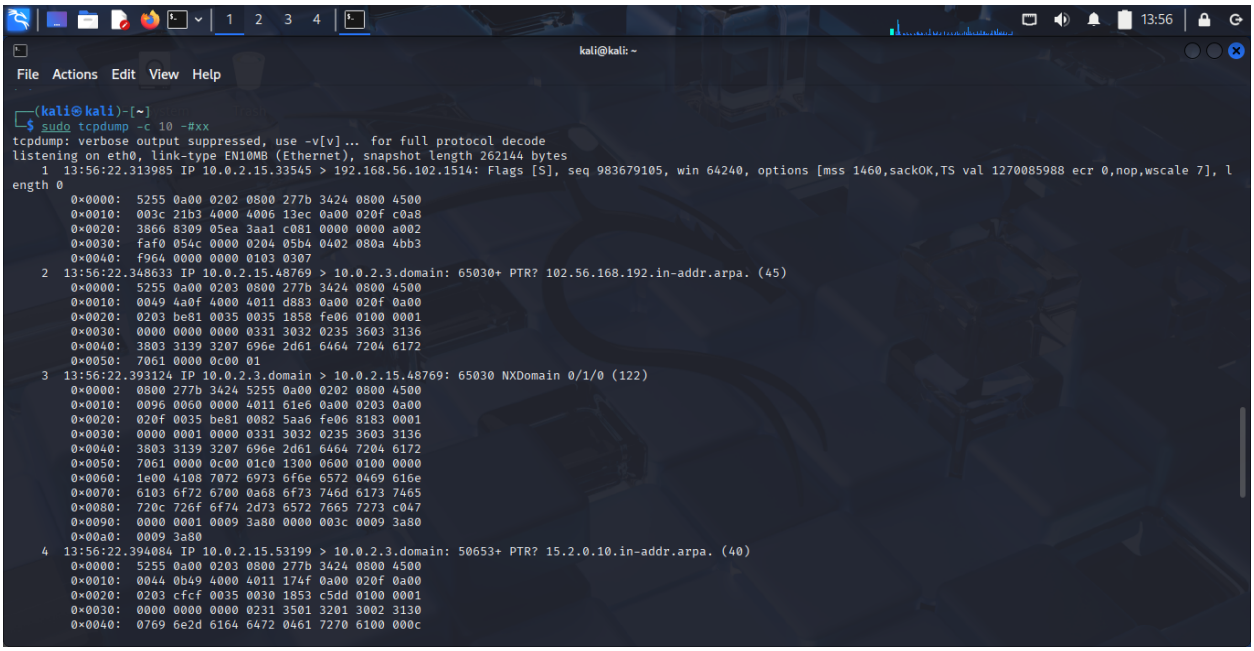


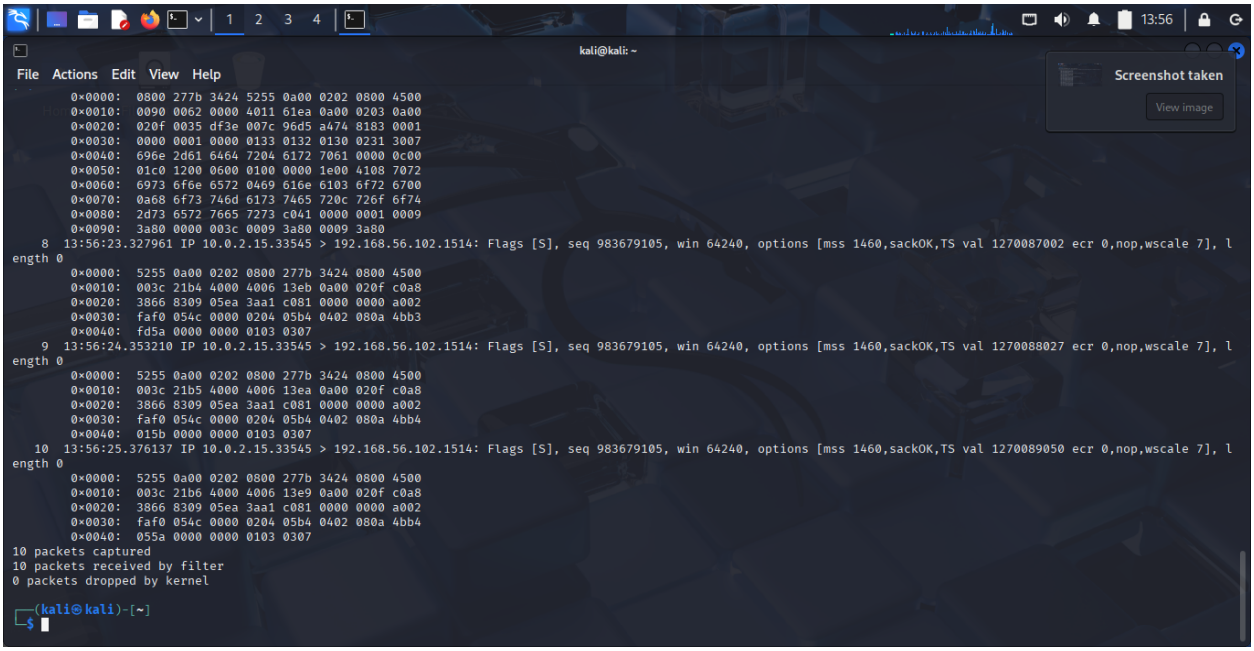

1 2 3 4
13:53
kali@kali: ~
File Actions Edit View Help
13:52:09.744825 IP 10.0.2.15.51972 > 10.0.2.3.domain: 24536+ PTR? 15.2.0.10.in-addr.arpa. (40)
13:52:09.785176 IP 10.0.2.3.domain > 10.0.2.15.51972: 24536 NXDomain 0/1/0 (117)
13:52:09.809587 IP 10.0.2.15.36120 > 10.0.2.3.domain: 7416+ PTR? 3.2.0.10.in-addr.arpa. (39)
13:52:09.847588 IP 10.0.2.3.domain > 10.0.2.15.36120: 7416 NXDomain 0/1/0 (116)
13:52:12.671805 IP 10.0.2.15.49513 > 192.168.56.102.1515: Flags [S], seq 4267022956, win 64240, options [mss 1460,sackOK,TS val 1269836346 ecr 0,nop,wscale 7], length 0
13:52:12.736984 IP 10.0.2.15.55883 > 10.0.2.3.domain: 34690+ PTR? 102.56.168.192.in-addr.arpa. (45)
13:52:12.779017 IP 10.0.2.3.domain > 10.0.2.15.55883: 34690 NXDomain 0/1/0 (122)
^C
11 packets captured
12 packets received by filter
0 packets dropped by kernel
(kali㉿kali)-[~]
$ man tcpdump
(kali㉿kali)-[~]
$ sudo tcpdump -c 10
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:53:37.407659 IP 10.0.2.15.39809 > 192.168.56.102.1514: Flags [S], seq 1923348742, win 64240, options [mss 1460,sackOK,TS val 1269921082 ecr 0,nop,wscale 7], length 0
13:53:37.412648 IP 10.0.2.15.50745 > 10.0.2.3.domain: 25982+ PTR? 102.56.168.192.in-addr.arpa. (45)
13:53:37.451755 IP 10.0.2.3.domain > 10.0.2.15.50745: 25982 NXDomain 0/1/0 (122)
13:53:37.452405 IP 10.0.2.15.54466 > 10.0.2.3.domain: 41949+ PTR? 15.2.0.10.in-addr.arpa. (40)
13:53:37.477868 IP 10.0.2.3.domain > 10.0.2.15.54466: 41949 NXDomain 0/1/0 (117)
13:53:37.516780 IP 10.0.2.15.58033 > 10.0.2.3.domain: 30471+ PTR? 3.2.0.10.in-addr.arpa. (39)
13:53:37.547784 IP 10.0.2.3.domain > 10.0.2.15.58033: 30471 NXDomain 0/1/0 (116)
13:53:42.527668 ARP, Request who-has 10.0.2.3 tell 10.0.2.15, length 28
13:53:42.528495 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
13:53:42.528842 ARP, Reply 10.0.2.3 is-at 52:55:0a:00:02:03 (oui Unknown), length 50
10 packets captured
13 packets received by filter
0 packets dropped by kernel
(kali㉿kali)-[~]
$
Screenshot taken
View image


1 2 3 4
13:55
kali@kali: ~
File Actions Edit View Help
$ sudo tcpdump -c 10 -#
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
1 13:54:31.264044 IP 10.0.2.15.51381 > 192.168.56.102.1514: Flags [S], seq 2661070477, win 64240, options [mss 1460,sackOK,TS val 1269974938 ecr 0,nop,wscale 7], length 0
2 13:54:31.337029 IP 10.0.2.15.35620 > 10.0.2.3.domain: 56880+ PTR? 102.56.168.192.in-addr.arpa. (45)
3 13:54:31.380035 IP 10.0.2.3.domain > 10.0.2.15.35620: 56880 NXDomain 0/1/0 (122)
4 13:54:31.380841 IP 10.0.2.15.35401 > 10.0.2.3.domain: 61963+ PTR? 15.2.0.10.in-addr.arpa. (40)
5 13:54:31.412100 IP 10.0.2.3.domain > 10.0.2.15.35401: 61963 NXDomain 0/1/0 (117)
6 13:54:31.440135 IP 10.0.2.15.53952 > 10.0.2.3.domain: 8301+ PTR? 3.2.0.10.in-addr.arpa. (39)
7 13:54:31.457997 IP 10.0.2.3.domain > 10.0.2.15.53952: 8301 NXDomain 0/1/0 (116)
8 13:54:32.287746 IP 10.0.2.15.51381 > 192.168.56.102.1514: Flags [S], seq 2661070477, win 64240, options [mss 1460,sackOK,TS val 1269975962 ecr 0,nop,wscale 7], length 0
9 13:54:33.312564 IP 10.0.2.15.51381 > 192.168.56.102.1514: Flags [S], seq 2661070477, win 64240, options [mss 1460,sackOK,TS val 1269976986 ecr 0,nop,wscale 7], length 0
10 13:54:35.327962 IP 10.0.2.15.51381 > 192.168.56.102.1514: Flags [S], seq 2661070477, win 64240, options [mss 1460,sackOK,TS val 1269979002 ecr 0,nop,wscale 7], length 0
10 packets captured
10 packets received by filter
0 packets dropped by kernel
(kali㉿kali)-[~]
$


1 2 3 4
13:56
kali@kali: ~
File Actions Edit View Help
└─$ sudo tcpdump -c 10 -#A
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
1 13:55:51.286671 IP 10.0.2.15.47103 > 192.168.56.102.1514: Flags [S], seq 441334923, win 64240, options [mss 1460,sackOK,TS val 1270054961 ecr 0,nop,wscale 7], l
ength 0
E..< ..@.@...
.....8f.....N<..........L.........
K..1........
2 13:55:51.365683 IP 10.0.2.15.44544 > 10.0.2.3.domain: 30347+ PTR? 102.56.168.192.in-addr.arpa. (45)
E..IM.@.@...
....
.......5.5.Xv............102.56.168.192.in-addr.arpa.....
3 13:55:51.412308 IP 10.0.2.3.domain > 10.0.2.15.44544: 30347 NXDomain 0/1/0 (122)
E....Z..@.a.
....
....5......v............102.56.168.192.in-addr.arpa...............A.prisoner.iana.org.
hostmaster.root-servers.G..... :....<. :..   :.
4 13:55:51.412310 IP 10.0.2.3.domain > 10.0.2.15.44544: 30347 NXDomain 0/1/0 (122)
E....[..@.a.
....
....5......v............102.56.168.192.in-addr.arpa...............A.prisoner.iana.org.
hostmaster.root-servers.G..... :....<. :..   :.
5 13:55:51.414250 IP 10.0.2.15.58629 > 10.0.2.3.domain: 61639+ PTR? 15.2.0.10.in-addr.arpa. (40)
E..D:.@.@...
....
......5.0.S.............15.2.0.10.in-addr.arpa.....
6 13:55:51.414474 IP 10.0.2.3.domain > 10.0.2.15.44544: 30347 NXDomain 0/1/0 (122)
E....\..@.a.
....
....5......v............102.56.168.192.in-addr.arpa...............A.prisoner.iana.org.
hostmaster.root-servers.G..... :....<. :..   :.
7 13:55:51.414563 IP 10.0.2.15 > 10.0.2.3: ICMP 10.0.2.15 udp port 44544 unreachable, length 158
E...\h..@...
....
...........E....\..@.a.
....
....5......v............102.56.168.192.in-addr.arpa...............A.prisoner.iana.org.

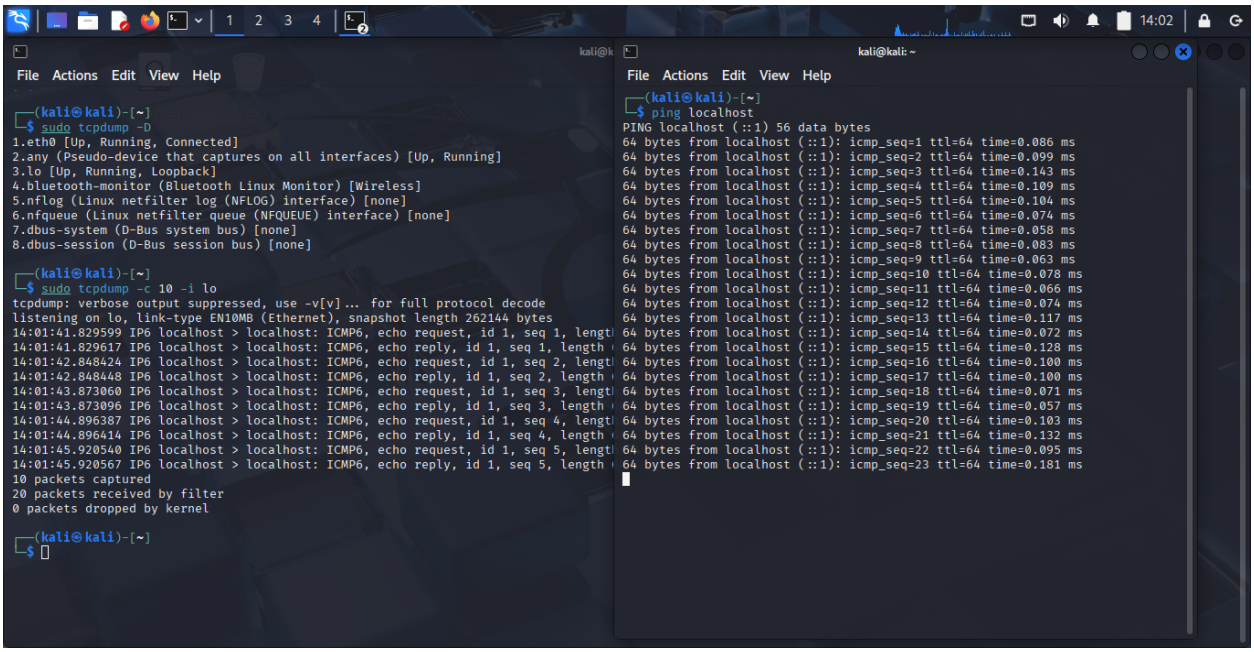

1 2 3 4
13:56
kali@kali: ~
File Actions Edit View Help
Screenshot taken
View image
hostmaster.root-servers.G..... :....<. :..   :.
5 13:55:51.414250 IP 10.0.2.15.58629 > 10.0.2.3.domain: 61639+ PTR? 15.2.0.10.in-addr.arpa. (40)
E..D:.@.@...
....
......5.0.S.............15.2.0.10.in-addr.arpa.....
6 13:55:51.414474 IP 10.0.2.3.domain > 10.0.2.15.44544: 30347 NXDomain 0/1/0 (122)
E....\..@.a.
....
....5......v............102.56.168.192.in-addr.arpa...............A.prisoner.iana.org.
hostmaster.root-servers.G..... :....<. :..   :.
7 13:55:51.414563 IP 10.0.2.15 > 10.0.2.3: ICMP 10.0.2.15 udp port 44544 unreachable, length 158
E...\h..@...
....
...........E....\..@.a.
....
....5......v............102.56.168.192.in-addr.arpa...............A.prisoner.iana.org.
hostmaster.root-servers.G..... :....<. :..   :.
8 13:55:51.436019 IP 10.0.2.3.domain > 10.0.2.15.58629: 61639 NXDomain 0/1/0 (117)
E....]..@.a.
....
....5...}..............15.2.0.10.in-addr.arpa...............A.prisoner.iana.org.
hostmaster.root-servers.B..... :....<. :..   :.
9 13:55:51.468872 IP 10.0.2.15.39505 > 10.0.2.3.domain: 24378+ PTR? 3.2.0.10.in-addr.arpa. (39)
E..C.#@.@..v
....
....Q.5./.R_:...........3.2.0.10.in-addr.arpa.....
10 13:55:51.497723 IP 10.0.2.3.domain > 10.0.2.15.39505: 24378 NXDomain 0/1/0 (116)
E....^..@.a.
....
....5.Q.| ._:...........3.2.0.10.in-addr.arpa...............A.prisoner.iana.org.
hostmaster.root-servers.A..... :....<. :..   :.
10 packets captured
10 packets received by filter
0 packets dropped by kernel
┌──(kali㉿kali)-[~]
└─$





🔷 Controlled Packet Capture & Traffic Simulation

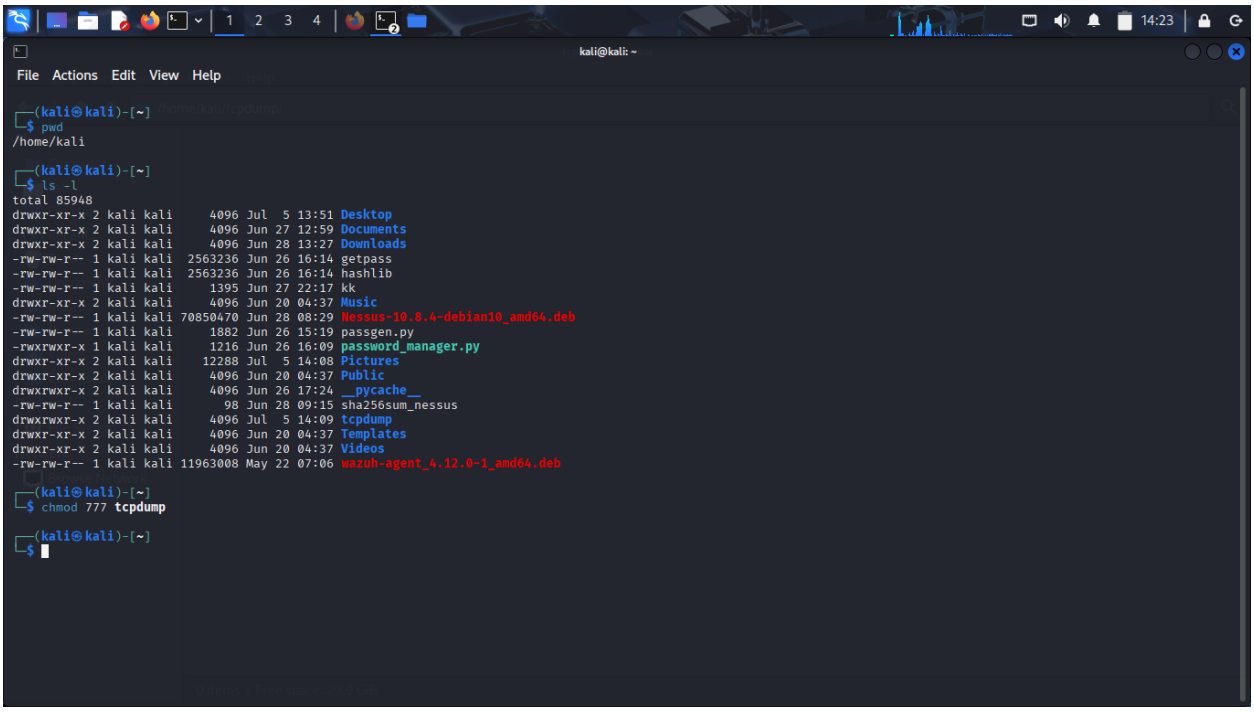
Executed `sudo tcpdump -c 10 -xxtttt` to capture and inspect packets with full hex and ASCII output, including timestamp precision. Used `sudo tcpdump -D` to identify active interfaces. Then, while running `sudo tcpdump -c 10 -i lo` to capture loopback traffic, I simulated ICMP activity by pinging `localhost` from a second terminal. This confirmed packet visibility, interface targeting, and my ability to correlate generated traffic with captured data — a critical blue team skill for verifying alerts and reproducing network events in controlled environments.

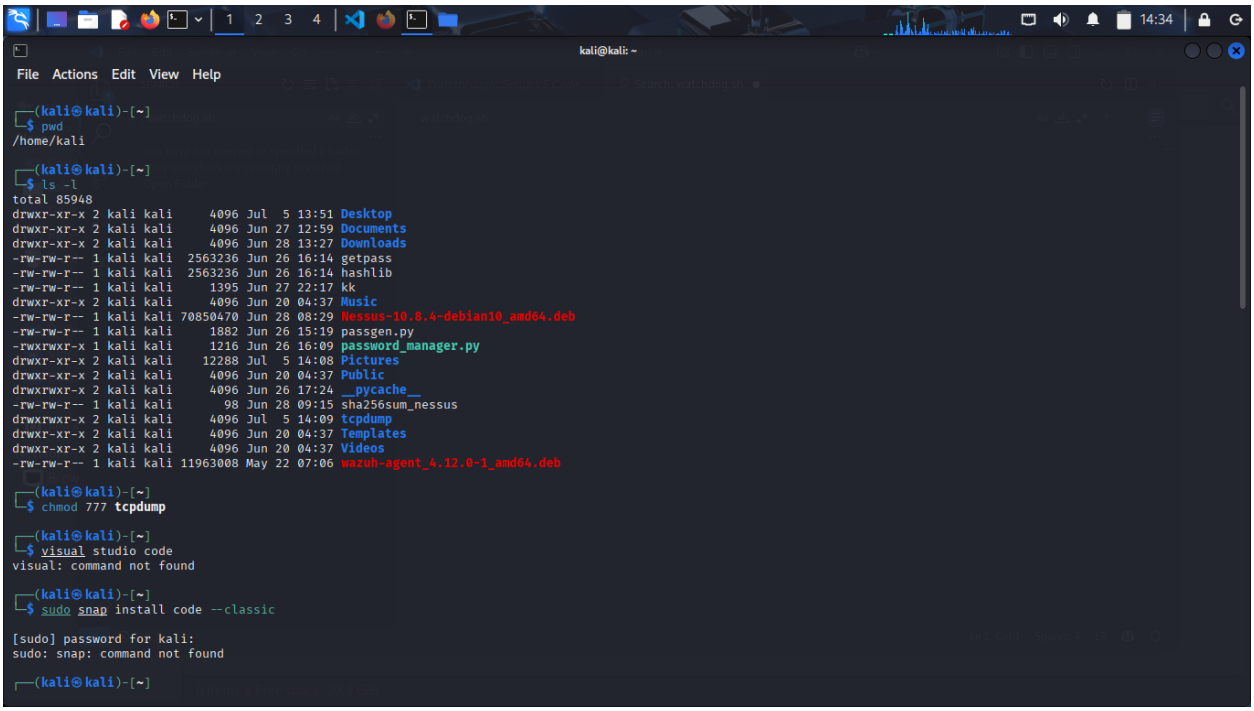


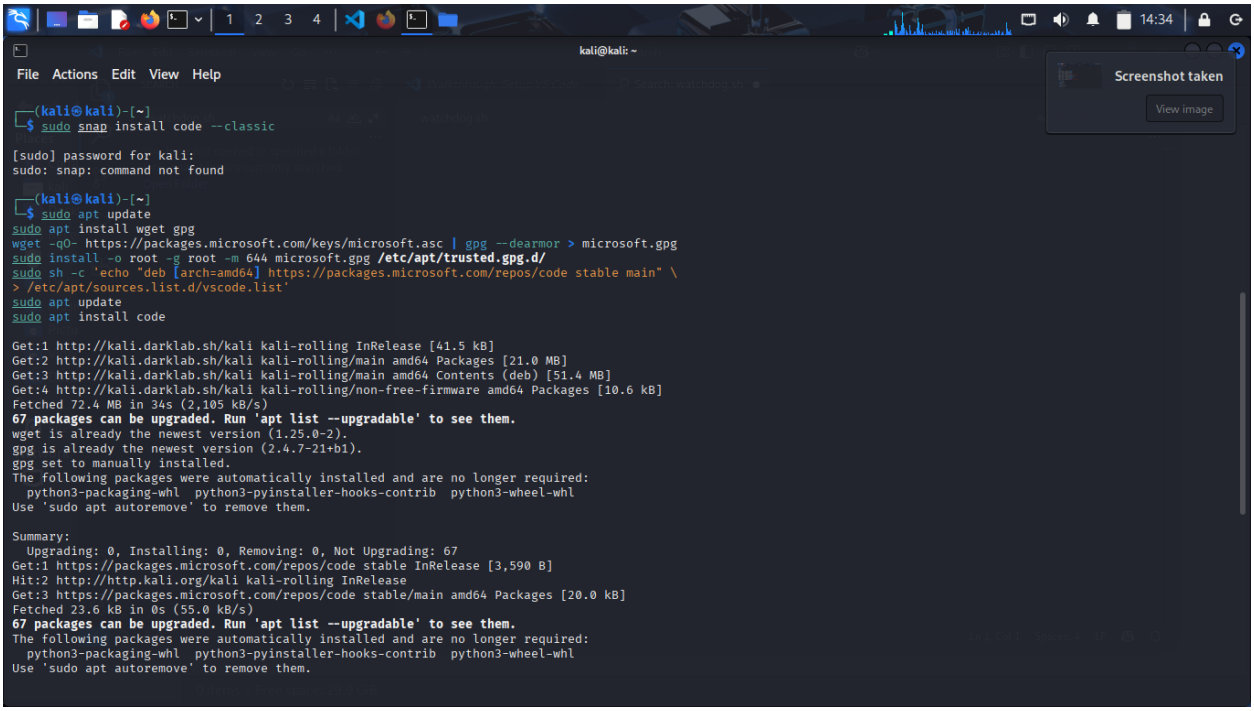
🔷 Scripted Packet Capture Automation (Bash + tcpdump)

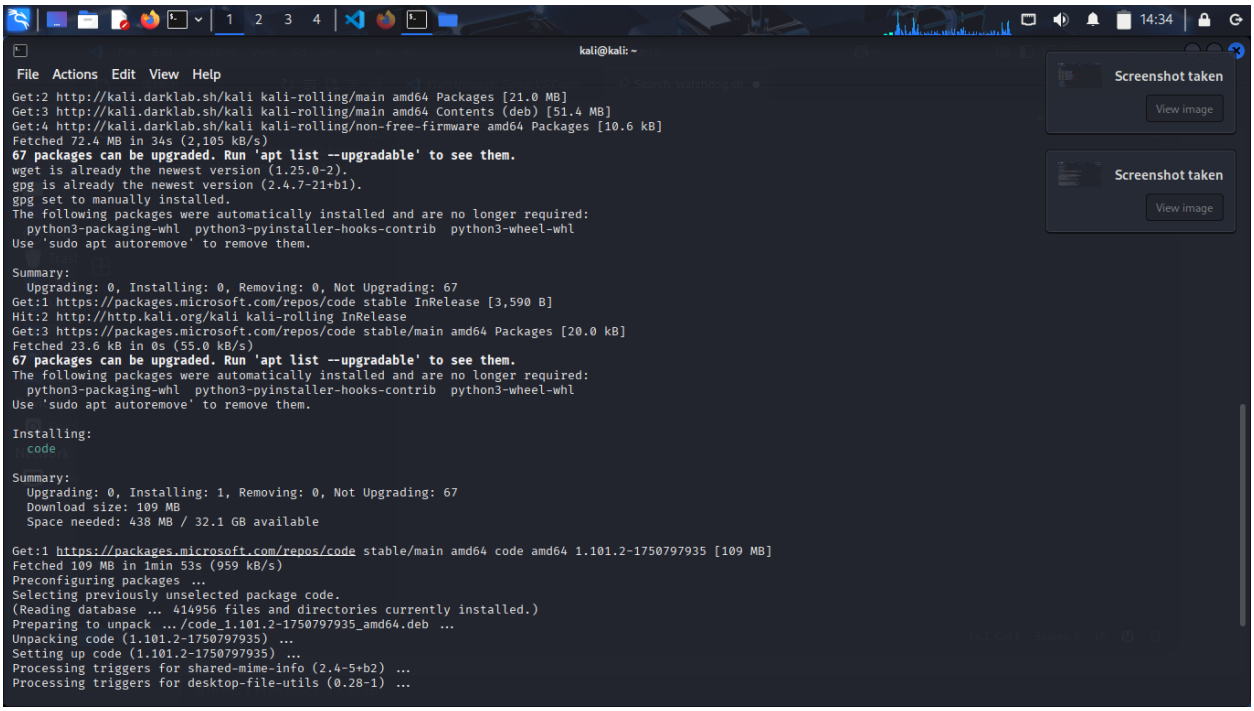
Installed Visual Studio Code on Kali Linux to streamline CLI automation. Created a Bash script (`whatsDoc.sh`) and wrote logic to execute `sudo tcpdump -c 10 -xxtttt host tcpdump`. This script captures a fixed number of packets with full hex and timestamp detail, targeting traffic related to `tcpdump`. This step marked the transition from manual testing to repeatable, automated packet inspection — a key SOC-level skill for scalable analysis and

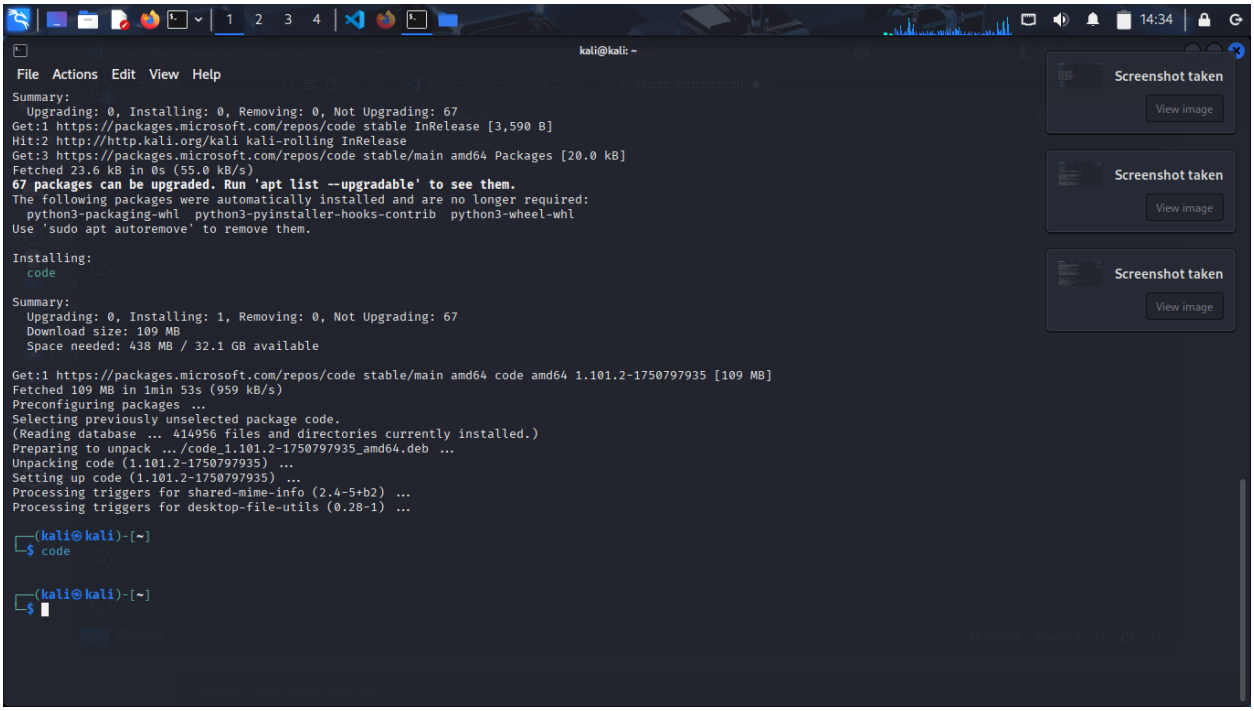
playbook development.

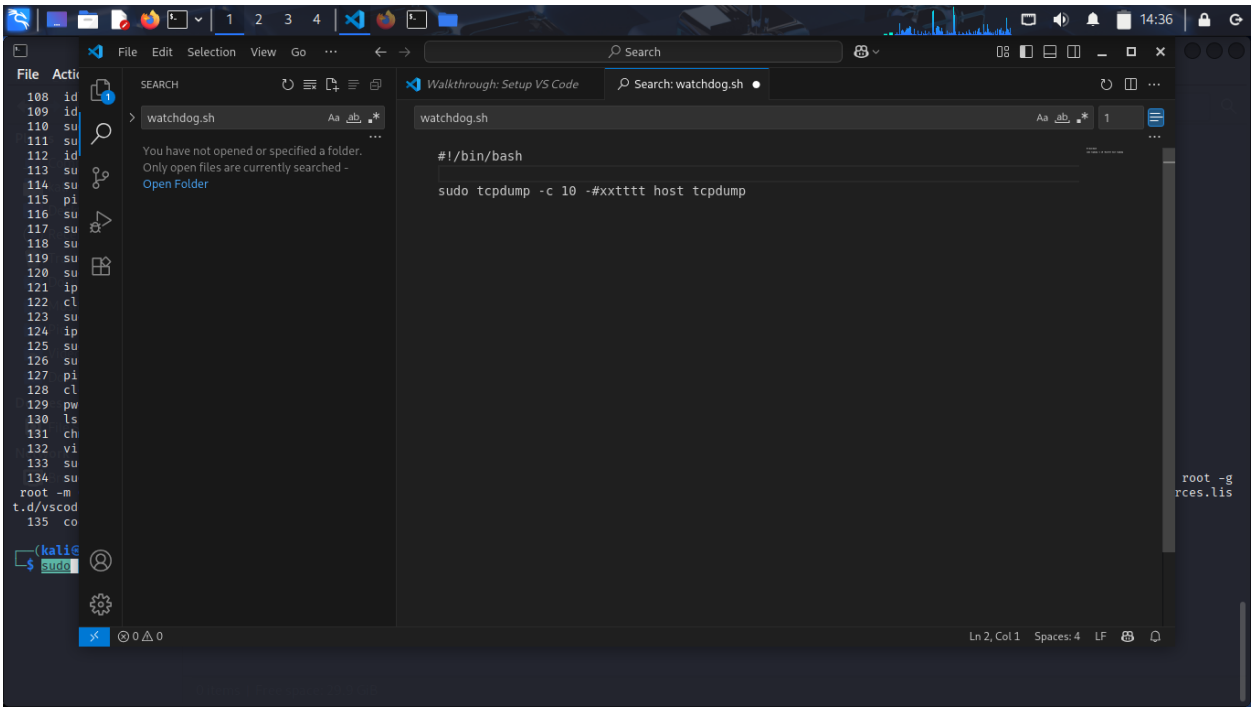



1 2 3 4
14:34
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali
┌──(kali㉿kali)-[~]
└─$ ls -l
total 85948
drwxr-xr-x 2 kali kali 4096 Jul 5 13:51 Desktop
drwxr-xr-x 2 kali kali 4096 Jun 27 12:59 Documents
drwxr-xr-x 2 kali kali 4096 Jun 28 13:27 Downloads
-rw-rw-r-- 1 kali kali 2563236 Jun 26 16:14 getpass
-rw-rw-r-- 1 kali kali 2563236 Jun 26 16:14 hashlib
-rw-rw-r-- 1 kali kali 1395 Jun 27 22:17 kk
drwxr-xr-x 2 kali kali 4096 Jun 20 04:37 Music
-rw-rw-r-- 1 kali kali 70850470 Jun 28 08:29 Nessus-10.8.4-debian10_amd64.deb
-rw-rw-r-- 1 kali kali 1882 Jun 26 15:19 passgen.py
-rwxrwxr-x 1 kali kali 1216 Jun 26 16:09 password_manager.py
drwxr-xr-x 2 kali kali 12288 Jul 5 14:08 Pictures
drwxr-xr-x 2 kali kali 4096 Jun 20 04:37 Public
drwxrwxr-x 2 kali kali 4096 Jun 26 17:24 __pycache__
-rw-rw-r-- 1 kali kali 98 Jun 28 09:15 sha256sum_nessus
drwxrwxr-x 2 kali kali 4096 Jul 5 14:09 tcpdump
drwxr-xr-x 2 kali kali 4096 Jun 20 04:37 Templates
drwxr-xr-x 2 kali kali 4096 Jun 20 04:37 Videos
-rw-rw-r-- 1 kali kali 11963008 May 22 07:06 wazuh-agent_4.12.0-1_amd64.deb
┌──(kali㉿kali)-[~]
└─$ chmod 777 tcpdump
┌──(kali㉿kali)-[~]
└─$ visual studio code
visual: command not found
┌──(kali㉿kali)-[~]
└─$ sudo snap install code --classic
[sudo] password for kali:
sudo: snap: command not found
┌──(kali㉿kali)-[~]


1 2 3 4
14:34
kali@kali: ~
File Actions Edit View Help
Screenshot taken
View image
┌──(kali㉿kali)-[~]
└─$ sudo snap install code --classic
[sudo] password for kali:
sudo: snap: command not found
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install wget gpg
wget -qO- https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor > microsoft.gpg
sudo install -o root -g root -m 644 microsoft.gpg /etc/apt/trusted.gpg.d/
sudo sh -c 'echo "deb [arch=amd64] https://packages.microsoft.com/repos/code stable main" \
> /etc/apt/sources.list.d/vscode.list'
sudo apt update
sudo apt install code
Get:1 http://kali.darklab.sh/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.darklab.sh/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.darklab.sh/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]
Get:4 http://kali.darklab.sh/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Fetched 72.4 MB in 34s (2,105 kB/s)
67 packages can be upgraded. Run 'apt list --upgradable' to see them.
wget is already the newest version (1.25.0-2).
gpg is already the newest version (2.4.7-21+b1).
gpg set to manually installed.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 67
Get:1 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Get:3 https://packages.microsoft.com/repos/code stable/main amd64 Packages [20.0 kB]
Fetched 23.6 kB in 0s (55.0 kB/s)
67 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

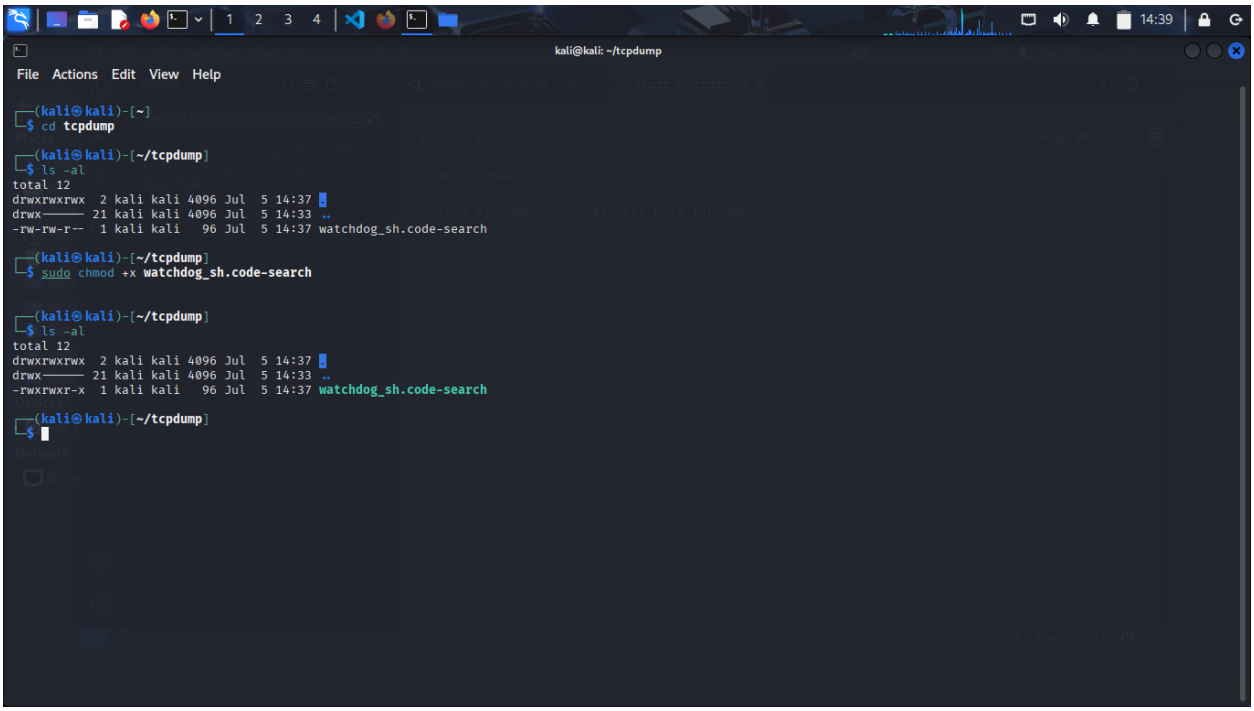

1 2 3 4
14:34
kali@kali: ~
File Actions Edit View Help
Get:2 http://kali.darklab.sh/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.darklab.sh/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]
Get:4 http://kali.darklab.sh/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Fetched 72.4 MB in 34s (2,105 kB/s)
67 packages can be upgraded. Run 'apt list --upgradable' to see them.
wget is already the newest version (1.25.0-2).
gpg is already the newest version (2.4.7-21+b1).
gpg set to manually installed.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 67
Get:1 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Get:3 https://packages.microsoft.com/repos/code stable/main amd64 Packages [20.0 kB]
Fetched 23.6 kB in 0s (55.0 kB/s)
67 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
Installing:
code
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 67
Download size: 109 MB
Space needed: 438 MB / 32.1 GB available
Get:1 https://packages.microsoft.com/repos/code stable/main amd64 code amd64 1.101.2-1750797935 [109 MB]
Fetched 109 MB in 1min 53s (959 kB/s)
Preconfiguring packages ...
Selecting previously unselected package code.
(Reading database ... 414956 files and directories currently installed.)
Preparing to unpack .../code_1.101.2-1750797935_amd64.deb ...
Unpacking code (1.101.2-1750797935) ...
Setting up code (1.101.2-1750797935) ...
Processing triggers for shared-mime-info (2.4-5+b2) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Screenshot taken
View image
Screenshot taken
View image

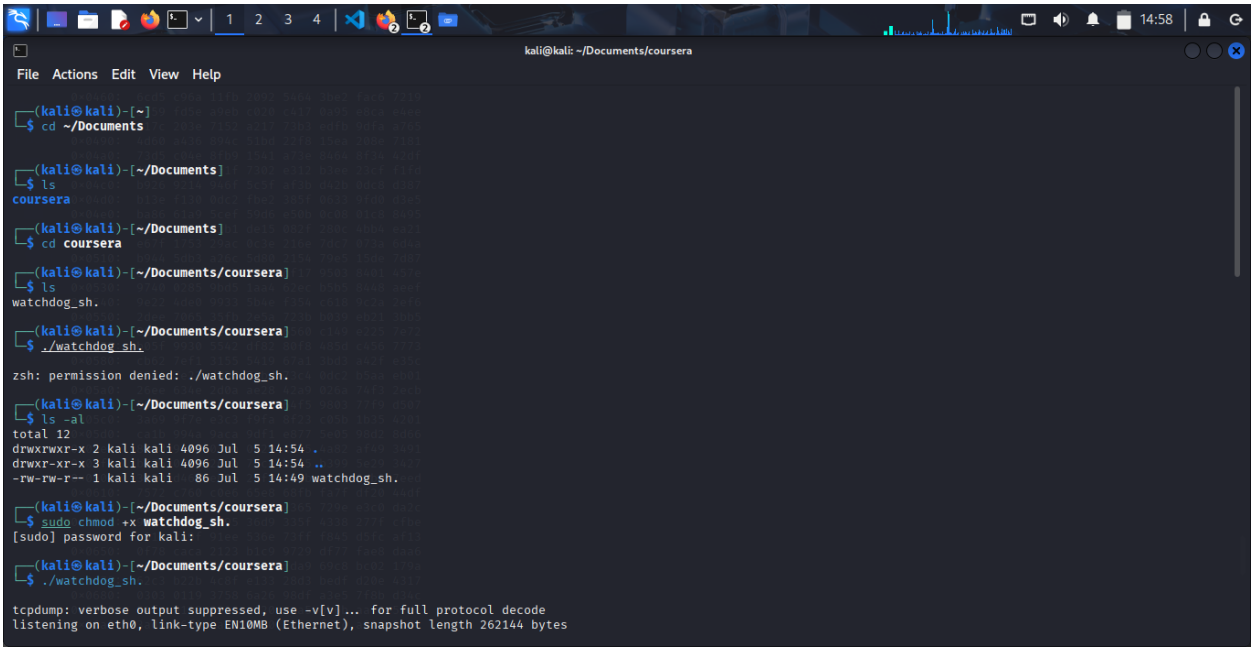

1 2 3 4
14:34
kali@kali: ~
File Actions Edit View Help
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 67
Get:1 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Get:3 https://packages.microsoft.com/repos/code stable/main amd64 Packages [20.0 kB]
Fetched 23.6 kB in 0s (55.0 kB/s)
67 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
Installing:
code
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 67
Download size: 109 MB
Space needed: 438 MB / 32.1 GB available
Get:1 https://packages.microsoft.com/repos/code stable/main amd64 code amd64 1.101.2-1750797935 [109 MB]
Fetched 109 MB in 1min 53s (959 kB/s)
Preconfiguring packages ...
Selecting previously unselected package code.
(Reading database ... 414956 files and directories currently installed.)
Preparing to unpack .../code_1.101.2-1750797935_amd64.deb ...
Unpacking code (1.101.2-1750797935) ...
Setting up code (1.101.2-1750797935) ...
Processing triggers for shared-mime-info (2.4-5+b2) ...
Processing triggers for desktop-file-utils (0.28-1) ...
┌──(kali㉿kali)-[~]
└─$ code
┌──(kali㉿kali)-[~]
└─$
Screenshot taken
View image
Screenshot taken
View image
Screenshot taken
View image

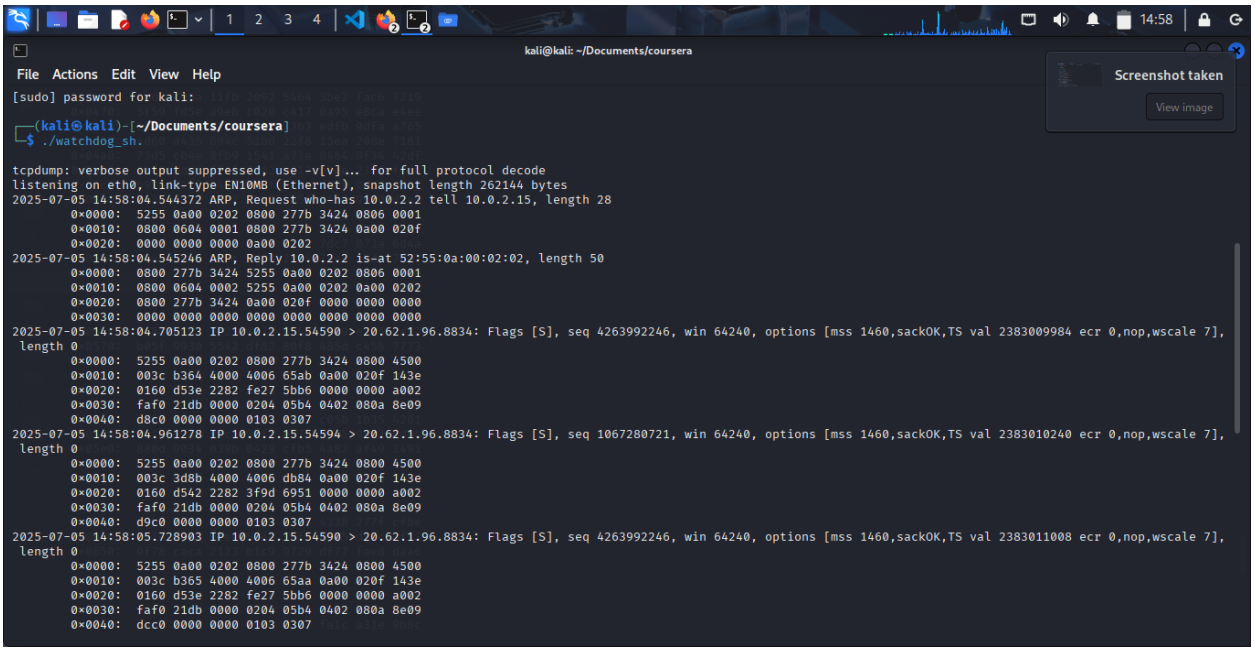


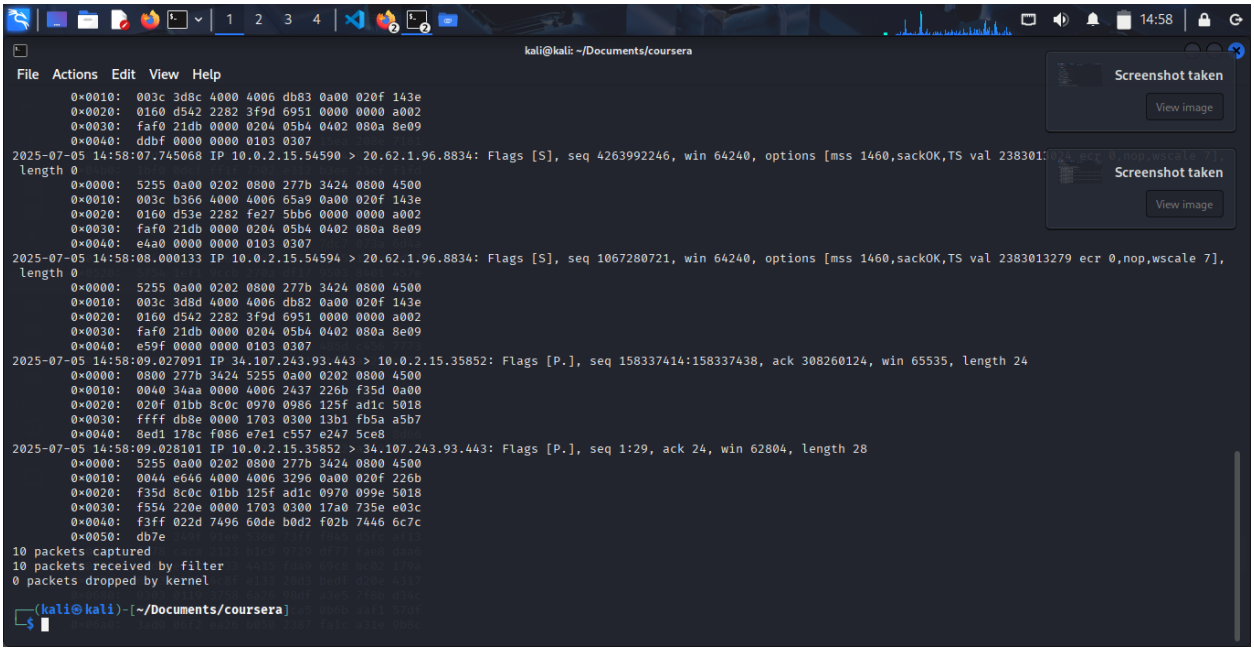
. 🔷 **Executing the Capture Script & Validating Output**

Navigated to the project directory via terminal, verified file permissions, and applied executable rights to my custom Bash script (`watchdog_sh`). Upon execution, the script ran `tcpdump` with pre-set flags and successfully captured 10 packets, including traffic from `coursera.org`. Output confirmed timestamp accuracy and filter effectiveness — demonstrating end-to-end control from script deployment to real-world traffic visibility.


14:39
kali@kali: ~/tcpdump
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd tcpdump
┌──(kali㉿kali)-[~/tcpdump]
└─$ ls -al
total 12
drwxrwxrwx 2 kali kali 4096 Jul 5 14:37 .
drwx------ 21 kali kali 4096 Jul 5 14:33 ..
-rw-rw-r-- 1 kali kali   96 Jul 5 14:37 watchdog_sh.code-search
┌──(kali㉿kali)-[~/tcpdump]
└─$ sudo chmod +x watchdog_sh.code-search
┌──(kali㉿kali)-[~/tcpdump]
└─$ ls -al
total 12
drwxrwxrwx 2 kali kali 4096 Jul 5 14:37 .
drwx------ 21 kali kali 4096 Jul 5 14:33 ..
-rwxrwxr-x 1 kali kali   96 Jul 5 14:37 watchdog_sh.code-search
┌──(kali㉿kali)-[~/tcpdump]
└─$

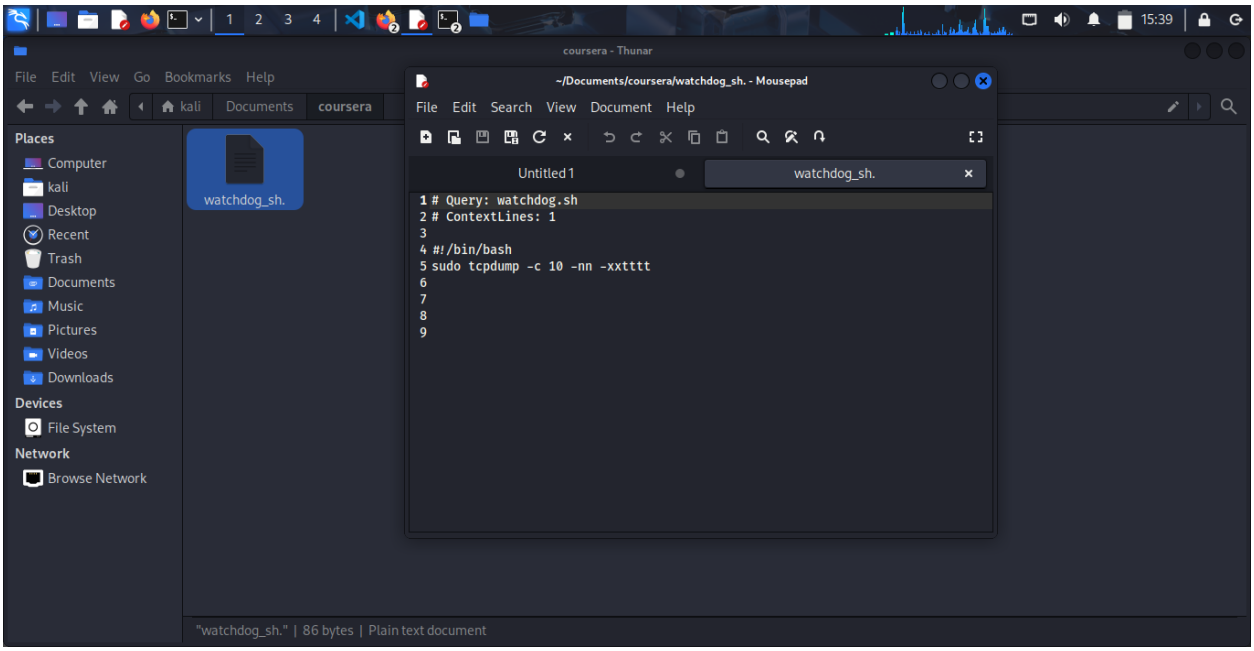

14:58
kali@kali: ~/Documents/coursera
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd ~/Documents
┌──(kali㉿kali)-[~/Documents]
└─$ ls
coursera
┌──(kali㉿kali)-[~/Documents]
└─$ cd coursera
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ls
watchdog_sh.
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ./watchdog_sh.
zsh: permission denied: ./watchdog_sh.
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ls -al
total 12
drwxrwxr-x 2 kali kali 4096 Jul 5 14:54 .
drwxr-xr-x 3 kali kali 4096 Jul 5 14:54 ..
-rw-rw-r-- 1 kali kali   86 Jul 5 14:49 watchdog_sh.
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ sudo chmod +x watchdog_sh.
[sudo] password for kali:
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ./watchdog_sh.
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

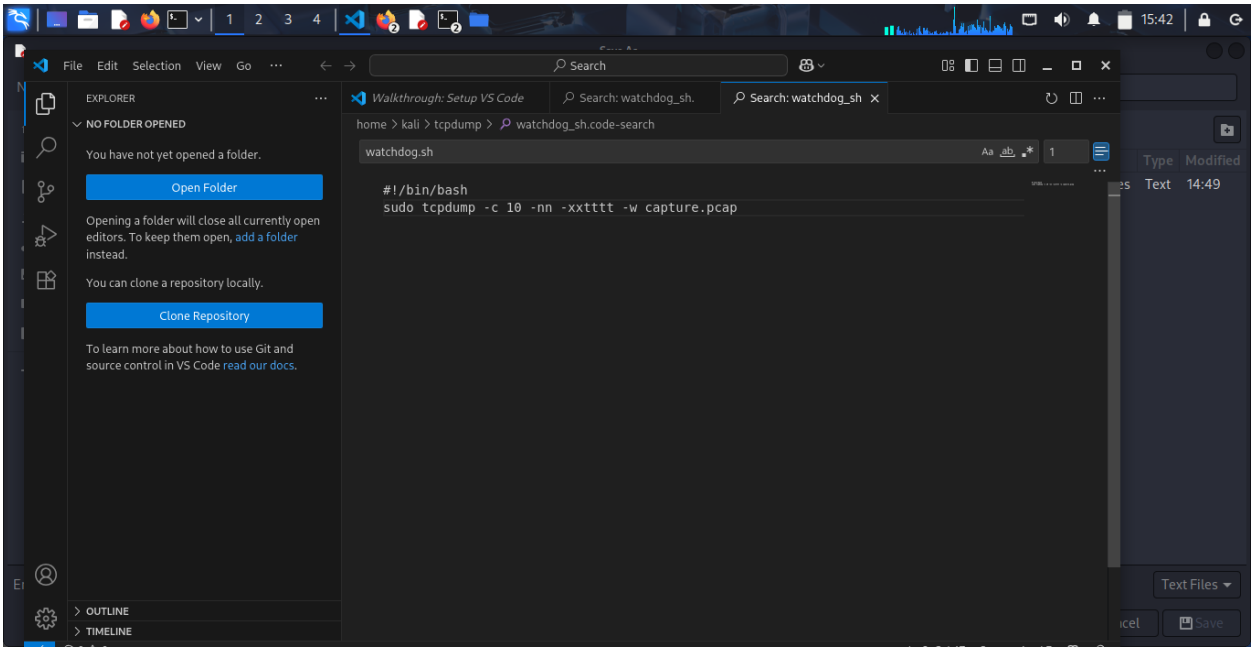


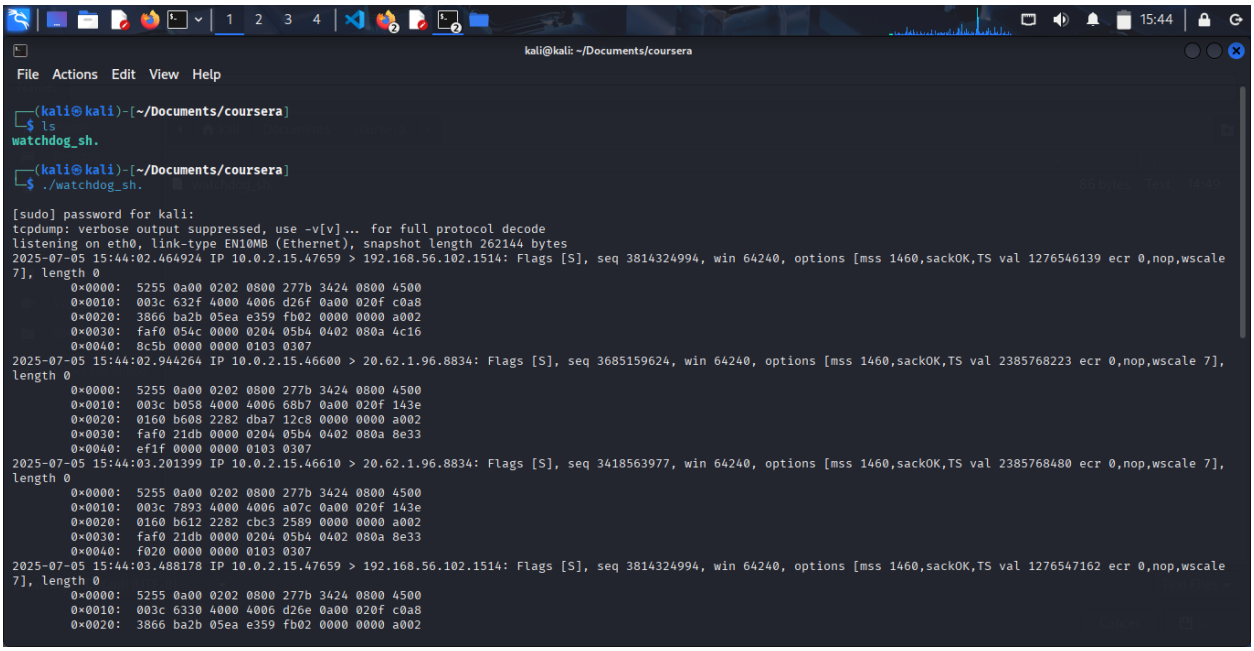


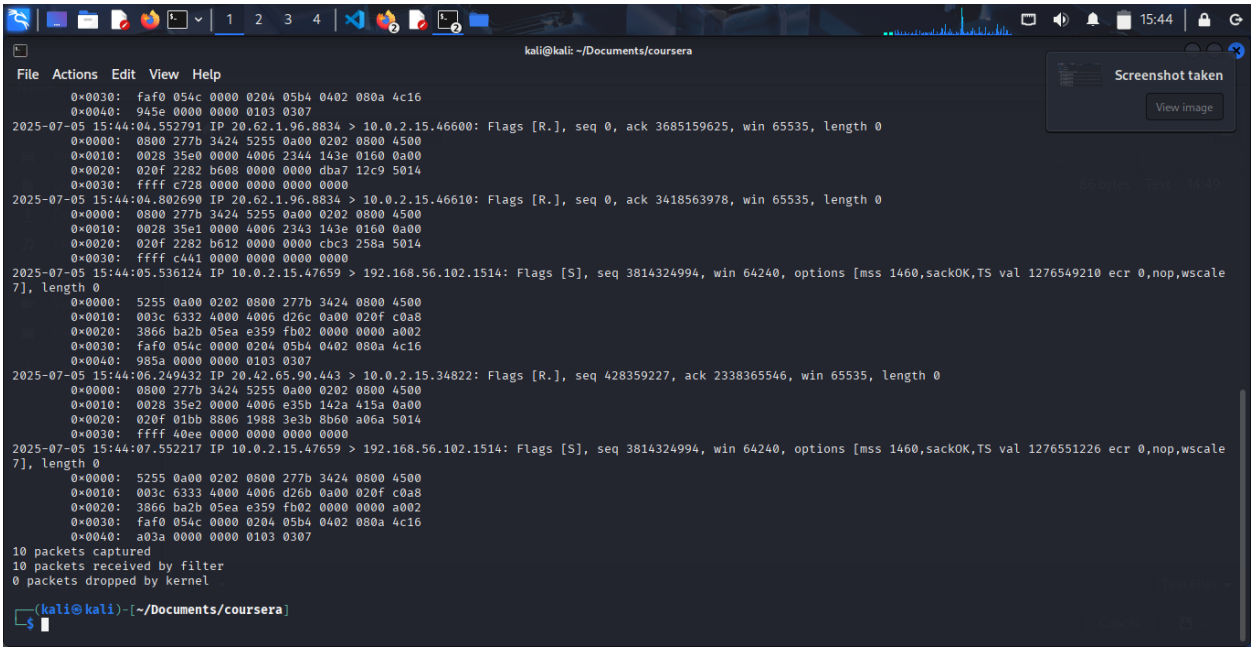
🔷 Advanced Packet Capture & Analysis Workflow

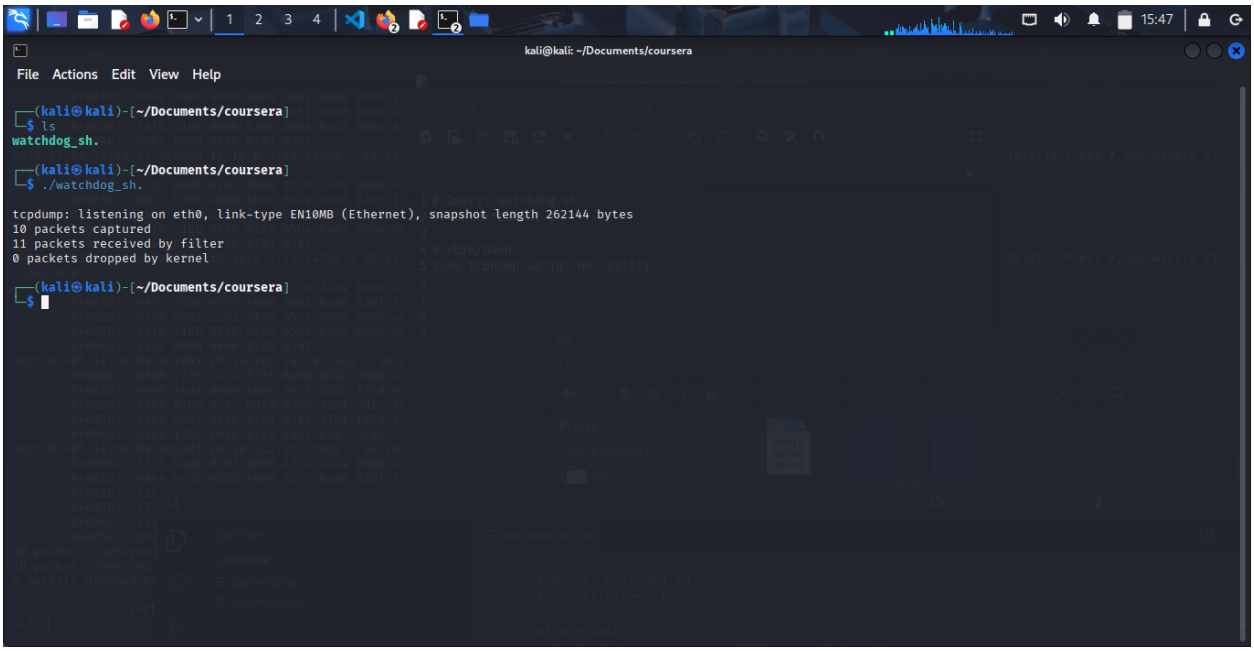
Refined my Bash script in VS Code to include flags for no name resolution (`-nn`), detailed hex and ASCII output (`-xx`), precise timestamps (`-tttt`), and saving captures to `capture.pcap`. Executed the script to collect 10 packets, then used `tcpdump -r` with enhanced flags to review the `.pcap` file in the terminal, adding packet numbering for clarity. Finally, imported the capture into Wireshark for comprehensive, human-readable analysis — including timestamps, ports, protocols, and traffic flow. This end-to-end process demonstrated my ability to automate captures, interpret raw data, and leverage industry-standard tools for forensic investigation.

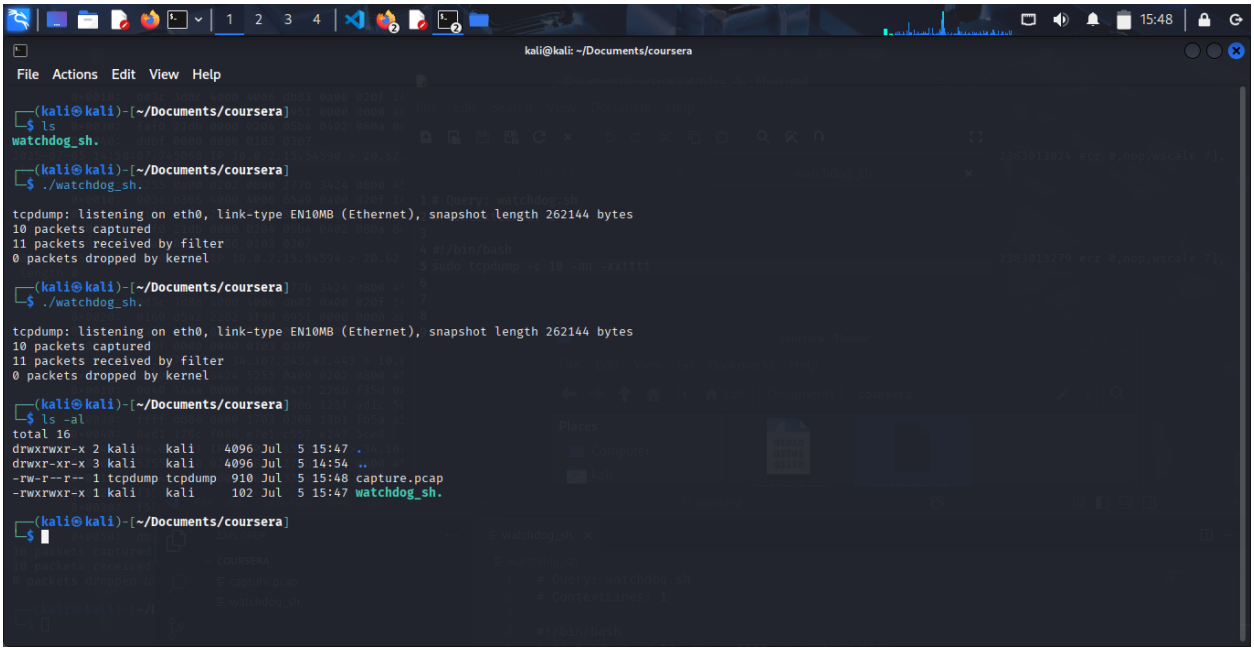

15:39
coursera - Thunar
File Edit View Go Bookmarks Help
kali Documents coursera
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
watchdog_sh.
~/Documents/coursera/watchdog_sh. - Mousepad
File Edit Search View Document Help
Untitled 1
watchdog_sh.
1 # Query: watchdog.sh
2 # ContextLines: 1
3
4 #!/bin/bash
5 sudo tcpdump -c 10 -nn -xxtttt
6
7
8
9
"watchdog_sh." | 86 bytes | Plain text document

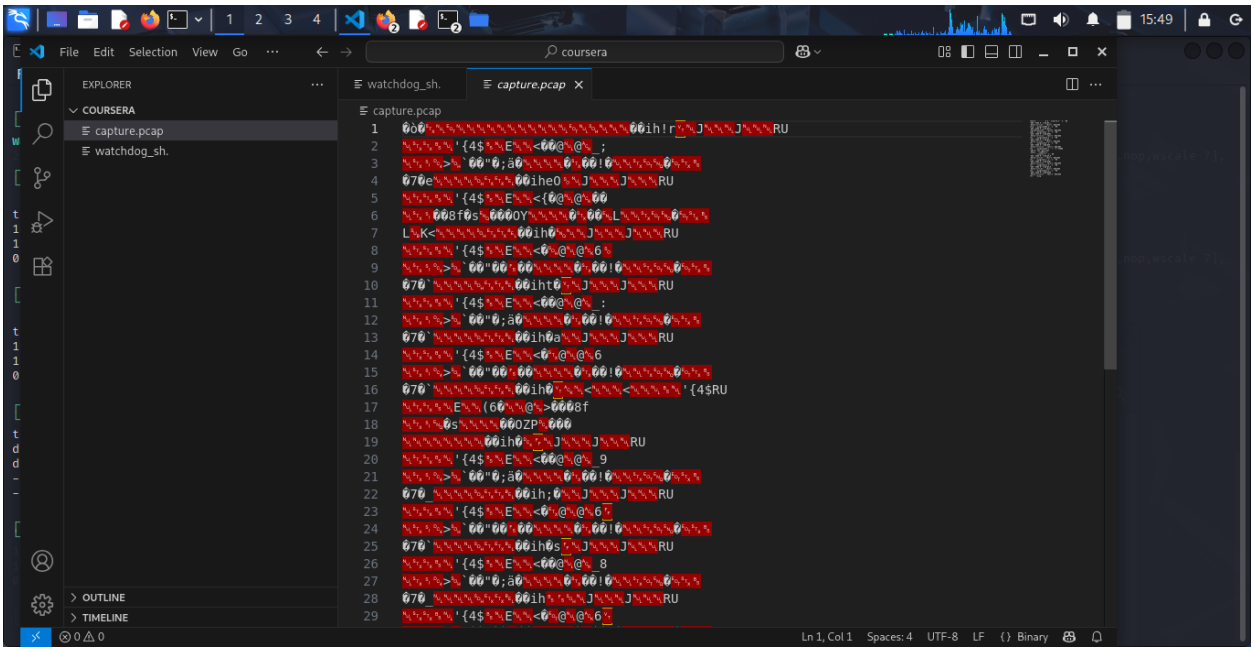

15:42
File Edit Selection View Go
Search
EXPLORER
NO FOLDER OPENED
You have not yet opened a folder.
Open Folder
Opening a folder will close all currently open editors. To keep them open, add a folder instead.
You can clone a repository locally.
Clone Repository
To learn more about how to use Git and source control in VS Code read our docs.
OUTLINE
TIMELINE
Walkthrough: Setup VS Code
Search: watchdog_sh.
Search: watchdog_sh
home > kali > tcpdump > watchdog_sh.code-search
watchdog.sh
#!/bin/bash
sudo tcpdump -c 10 -nn -xxtttt -w capture.pcap
Type Modified
Text 14:49
Text Files
Save

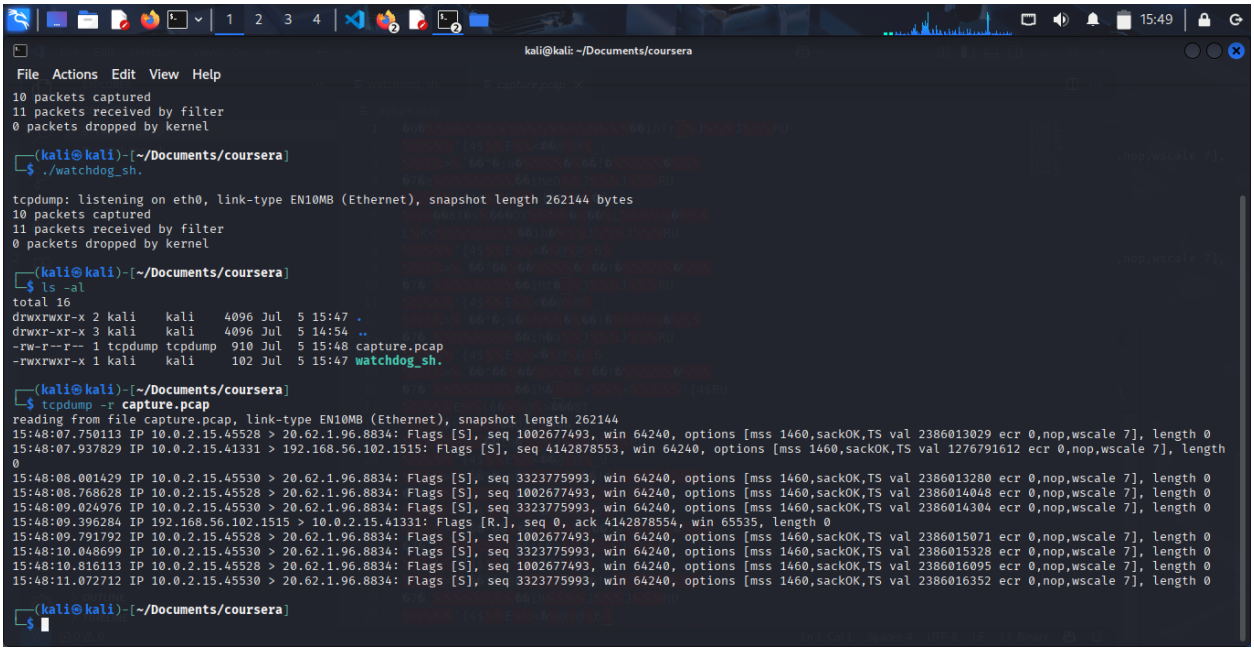

15:44
kali@kali: ~/Documents/coursera
File Actions Edit View Help
(kali㉿kali)-[~/Documents/coursera]
$ ls
watchdog_sh.
(kali㉿kali)-[~/Documents/coursera]
$ ./watchdog_sh.
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
2025-07-05 15:44:02.464924 IP 10.0.2.15.47659 > 192.168.56.102.1514: Flags [S], seq 3814324994, win 64240, options [mss 1460,sackOK,TS val 1276546139 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c 632f 4000 4006 d26f 0a00 020f c0a8
0×0020: 3866 ba2b 05ea e359 fb02 0000 0000 a002
0×0030: faf0 054c 0000 0204 05b4 0402 080a 4c16
0×0040: 8c5b 0000 0000 0103 0307
2025-07-05 15:44:02.944264 IP 10.0.2.15.46600 > 20.62.1.96.8834: Flags [S], seq 3685159624, win 64240, options [mss 1460,sackOK,TS val 2385768223 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c b058 4000 4006 68b7 0a00 020f 143e
0×0020: 0160 b608 2282 dba7 12c8 0000 0000 a002
0×0030: faf0 21db 0000 0204 05b4 0402 080a 8e33
0×0040: ef1f 0000 0000 0103 0307
2025-07-05 15:44:03.201399 IP 10.0.2.15.46610 > 20.62.1.96.8834: Flags [S], seq 3418563977, win 64240, options [mss 1460,sackOK,TS val 2385768480 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c 7893 4000 4006 a07c 0a00 020f 143e
0×0020: 0160 b612 2282 cbc3 2589 0000 0000 a002
0×0030: faf0 21db 0000 0204 05b4 0402 080a 8e33
0×0040: f020 0000 0000 0103 0307
2025-07-05 15:44:03.488178 IP 10.0.2.15.47659 > 192.168.56.102.1514: Flags [S], seq 3814324994, win 64240, options [mss 1460,sackOK,TS val 1276547162 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c 6330 4000 4006 d26e 0a00 020f c0a8
0×0020: 3866 ba2b 05ea e359 fb02 0000 0000 a002

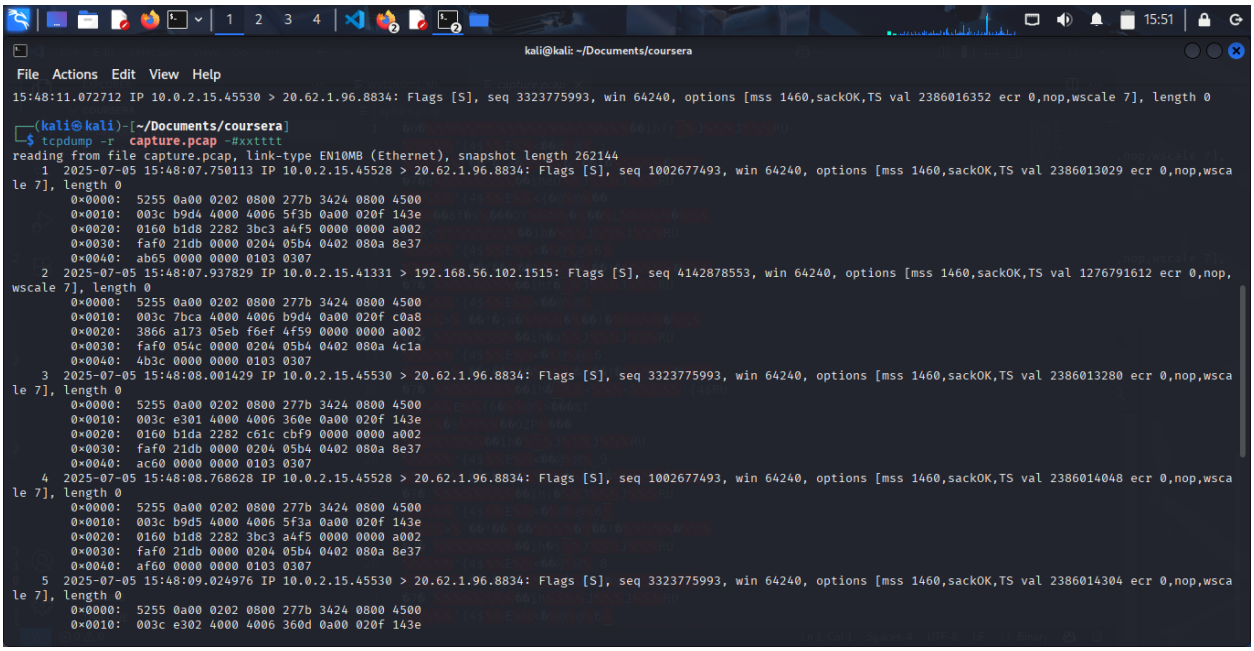

15:44
kali@kali: ~/Documents/coursera
File Actions Edit View Help
Screenshot taken
View image
0×0030: faf0 054c 0000 0204 05b4 0402 080a 4c16
0×0040: 945e 0000 0000 0103 0307
2025-07-05 15:44:04.552791 IP 20.62.1.96.8834 > 10.0.2.15.46600: Flags [R.], seq 0, ack 3685159625, win 65535, length 0
0×0000: 0800 277b 3424 5255 0a00 0202 0800 4500
0×0010: 0028 35e0 0000 4006 2344 143e 0160 0a00
0×0020: 020f 2282 b608 0000 0000 dba7 12c9 5014
0×0030: ffff c728 0000 0000 0000 0000
2025-07-05 15:44:04.802690 IP 20.62.1.96.8834 > 10.0.2.15.46610: Flags [R.], seq 0, ack 3418563978, win 65535, length 0
0×0000: 0800 277b 3424 5255 0a00 0202 0800 4500
0×0010: 0028 35e1 0000 4006 2343 143e 0160 0a00
0×0020: 020f 2282 b612 0000 0000 cbc3 258a 5014
0×0030: ffff c441 0000 0000 0000 0000
2025-07-05 15:44:05.536124 IP 10.0.2.15.47659 > 192.168.56.102.1514: Flags [S], seq 3814324994, win 64240, options [mss 1460,sackOK,TS val 1276549210 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c 6332 4000 4006 d26c 0a00 020f c0a8
0×0020: 3866 ba2b 05ea e359 fb02 0000 0000 a002
0×0030: faf0 054c 0000 0204 05b4 0402 080a 4c16
0×0040: 985a 0000 0000 0103 0307
2025-07-05 15:44:06.249432 IP 20.42.65.90.443 > 10.0.2.15.34822: Flags [R.], seq 428359227, ack 2338365546, win 65535, length 0
0×0000: 0800 277b 3424 5255 0a00 0202 0800 4500
0×0010: 0028 35e2 0000 4006 e35b 142a 415a 0a00
0×0020: 020f 01bb 8806 1988 3e3b 8b60 a06a 5014
0×0030: ffff 40ee 0000 0000 0000 0000
2025-07-05 15:44:07.552217 IP 10.0.2.15.47659 > 192.168.56.102.1514: Flags [S], seq 3814324994, win 64240, options [mss 1460,sackOK,TS val 1276551226 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c 6333 4000 4006 d26b 0a00 020f c0a8
0×0020: 3866 ba2b 05ea e359 fb02 0000 0000 a002
0×0030: faf0 054c 0000 0204 05b4 0402 080a 4c16
0×0040: a03a 0000 0000 0103 0307
10 packets captured
10 packets received by filter
0 packets dropped by kernel
(kali㉿kali)-[~/Documents/coursera]
$

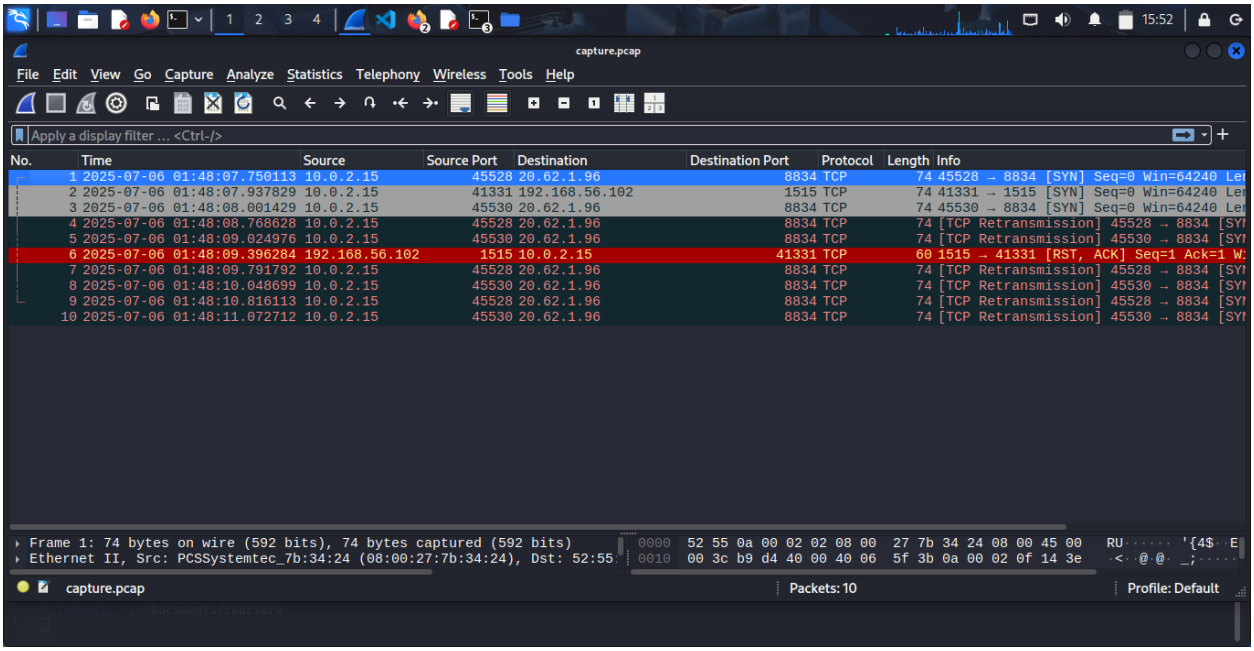

15:47
kali@kali: ~/Documents/coursera
File Actions Edit View Help
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ls
watchdog_sh.
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ./watchdog_sh.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
11 packets received by filter
0 packets dropped by kernel
┌──(kali㉿kali)-[~/Documents/coursera]
└─$

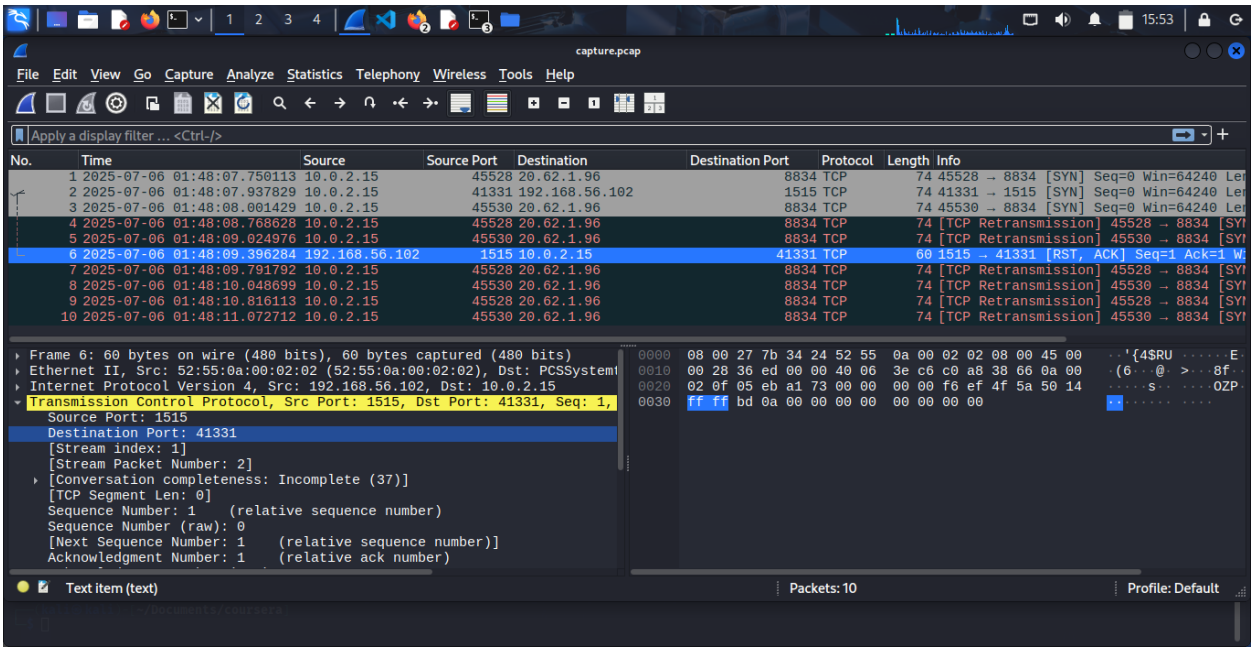

15:48
kali@kali: ~/Documents/coursera
File Actions Edit View Help
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ls
watchdog_sh.
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ./watchdog_sh.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
11 packets received by filter
0 packets dropped by kernel
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ./watchdog_sh.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
11 packets received by filter
0 packets dropped by kernel
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ ls -al
total 16
drwxrwxr-x 2 kali kali 4096 Jul 5 15:47 .
drwxr-xr-x 3 kali kali 4096 Jul 5 14:54 ..
-rw-r--r-- 1 tcpdump tcpdump 910 Jul 5 15:48 capture.pcap
-rwxrwxr-x 1 kali kali 102 Jul 5 15:47 watchdog_sh.
┌──(kali㉿kali)-[~/Documents/coursera]
└─$


File Edit Selection View Go
coursera
EXPLORER
COURSERA
capture.pcap
watchdog_sh.
OUTLINE
TIMELINE
Ln 1, Col 1 Spaces: 4 UTF-8 LF Binary


kali@kali: ~/Documents/coursera
File Actions Edit View Help
10 packets captured
11 packets received by filter
0 packets dropped by kernel
(kali㉿kali)-[~/Documents/coursera]
$ ./watchdog_sh.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
11 packets received by filter
0 packets dropped by kernel
(kali㉿kali)-[~/Documents/coursera]
$ ls -al
total 16
drwxrwxr-x 2 kali kali 4096 Jul 5 15:47 .
drwxr-xr-x 3 kali kali 4096 Jul 5 14:54 ..
-rw-r--r-- 1 tcpdump tcpdump 910 Jul 5 15:48 capture.pcap
-rwxrwxr-x 1 kali kali 102 Jul 5 15:47 watchdog_sh.
(kali㉿kali)-[~/Documents/coursera]
$ tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
15:48:07.750113 IP 10.0.2.15.45528 > 20.62.1.96.8834: Flags [S], seq 1002677493, win 64240, options [mss 1460,sackOK,TS val 2386013029 ecr 0,nop,wscale 7], length 0
15:48:07.937829 IP 10.0.2.15.41331 > 192.168.56.102.1515: Flags [S], seq 4142878553, win 64240, options [mss 1460,sackOK,TS val 1276791612 ecr 0,nop,wscale 7], length 0
15:48:08.001429 IP 10.0.2.15.45530 > 20.62.1.96.8834: Flags [S], seq 3323775993, win 64240, options [mss 1460,sackOK,TS val 2386013280 ecr 0,nop,wscale 7], length 0
15:48:08.768628 IP 10.0.2.15.45528 > 20.62.1.96.8834: Flags [S], seq 1002677493, win 64240, options [mss 1460,sackOK,TS val 2386014048 ecr 0,nop,wscale 7], length 0
15:48:09.024976 IP 10.0.2.15.45530 > 20.62.1.96.8834: Flags [S], seq 3323775993, win 64240, options [mss 1460,sackOK,TS val 2386014304 ecr 0,nop,wscale 7], length 0
15:48:09.396284 IP 192.168.56.102.1515 > 10.0.2.15.41331: Flags [R.], seq 0, ack 4142878554, win 65535, length 0
15:48:09.791792 IP 10.0.2.15.45528 > 20.62.1.96.8834: Flags [S], seq 1002677493, win 64240, options [mss 1460,sackOK,TS val 2386015071 ecr 0,nop,wscale 7], length 0
15:48:10.048699 IP 10.0.2.15.45530 > 20.62.1.96.8834: Flags [S], seq 3323775993, win 64240, options [mss 1460,sackOK,TS val 2386015328 ecr 0,nop,wscale 7], length 0
15:48:10.816113 IP 10.0.2.15.45528 > 20.62.1.96.8834: Flags [S], seq 1002677493, win 64240, options [mss 1460,sackOK,TS val 2386016095 ecr 0,nop,wscale 7], length 0
15:48:11.072712 IP 10.0.2.15.45530 > 20.62.1.96.8834: Flags [S], seq 3323775993, win 64240, options [mss 1460,sackOK,TS val 2386016352 ecr 0,nop,wscale 7], length 0
(kali㉿kali)-[~/Documents/coursera]
$

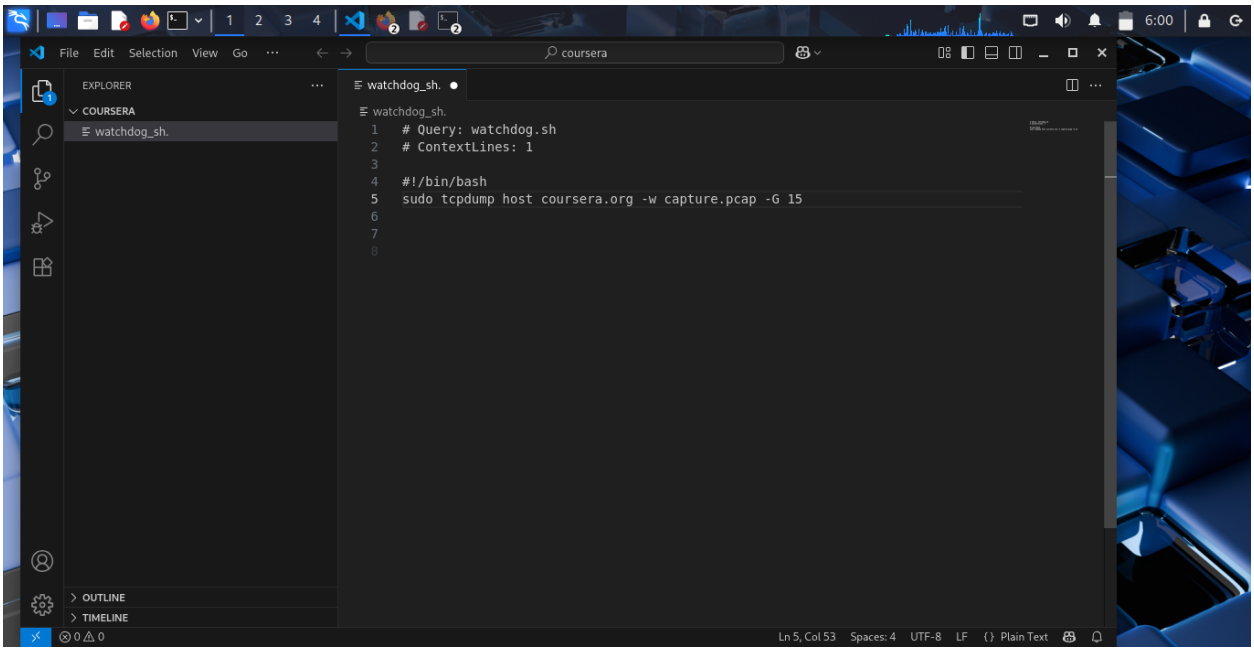

15:51
kali@kali: ~/Documents/coursera
File Actions Edit View Help
15:48:11.072712 IP 10.0.2.15.45530 > 20.62.1.96.8834: Flags [S], seq 3323775993, win 64240, options [mss 1460,sackOK,TS val 2386016352 ecr 0,nop,wscale 7], length 0
┌──(kali㉿kali)-[~/Documents/coursera]
└─$ tcpdump -r capture.pcap -#xxtttt
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
1 2025-07-05 15:48:07.750113 IP 10.0.2.15.45528 > 20.62.1.96.8834: Flags [S], seq 1002677493, win 64240, options [mss 1460,sackOK,TS val 2386013029 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c b9d4 4000 4006 5f3b 0a00 020f 143e
0×0020: 0160 b1d8 2282 3bc3 a4f5 0000 0000 a002
0×0030: faf0 21db 0000 0204 05b4 0402 080a 8e37
0×0040: ab65 0000 0000 0103 0307
2 2025-07-05 15:48:07.937829 IP 10.0.2.15.41331 > 192.168.56.102.1515: Flags [S], seq 4142878553, win 64240, options [mss 1460,sackOK,TS val 1276791612 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c 7bca 4000 4006 b9d4 0a00 020f c0a8
0×0020: 3866 a173 05eb f6ef 4f59 0000 0000 a002
0×0030: faf0 054c 0000 0204 05b4 0402 080a 4c1a
0×0040: 4b3c 0000 0000 0103 0307
3 2025-07-05 15:48:08.001429 IP 10.0.2.15.45530 > 20.62.1.96.8834: Flags [S], seq 3323775993, win 64240, options [mss 1460,sackOK,TS val 2386013280 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c e301 4000 4006 360e 0a00 020f 143e
0×0020: 0160 b1da 2282 c61c cbf9 0000 0000 a002
0×0030: faf0 21db 0000 0204 05b4 0402 080a 8e37
0×0040: ac60 0000 0000 0103 0307
4 2025-07-05 15:48:08.768628 IP 10.0.2.15.45528 > 20.62.1.96.8834: Flags [S], seq 1002677493, win 64240, options [mss 1460,sackOK,TS val 2386014048 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c b9d5 4000 4006 5f3a 0a00 020f 143e
0×0020: 0160 b1d8 2282 3bc3 a4f5 0000 0000 a002
0×0030: faf0 21db 0000 0204 05b4 0402 080a 8e37
0×0040: af60 0000 0000 0103 0307
5 2025-07-05 15:48:09.024976 IP 10.0.2.15.45530 > 20.62.1.96.8834: Flags [S], seq 3323775993, win 64240, options [mss 1460,sackOK,TS val 2386014304 ecr 0,nop,wscale 7], length 0
0×0000: 5255 0a00 0202 0800 277b 3424 0800 4500
0×0010: 003c e302 4000 4006 360d 0a00 020f 143e

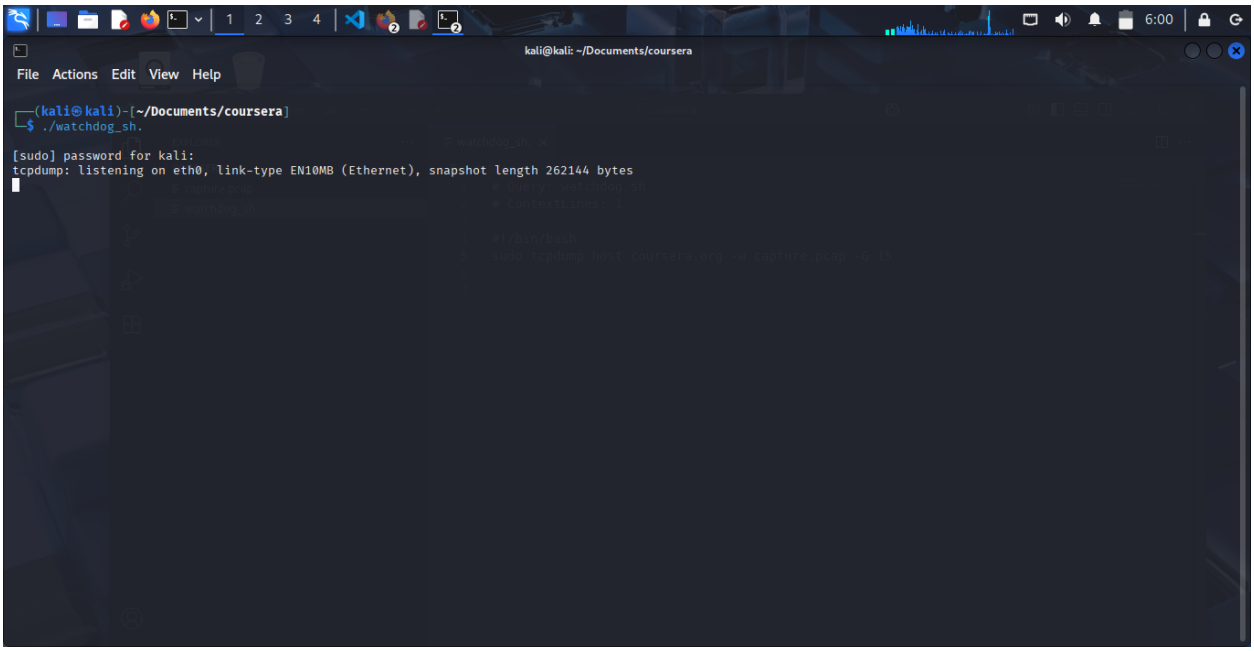

15:52
capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Source Port Destination Destination Port Protocol Length Info
1 2025-07-06 01:48:07.750113 10.0.2.15 45528 20.62.1.96 8834 TCP 74 45528 → 8834 [SYN] Seq=0 Win=64240 Le
2 2025-07-06 01:48:07.937829 10.0.2.15 41331 192.168.56.102 1515 TCP 74 41331 → 1515 [SYN] Seq=0 Win=64240 Le
3 2025-07-06 01:48:08.001429 10.0.2.15 45530 20.62.1.96 8834 TCP 74 45530 → 8834 [SYN] Seq=0 Win=64240 Le
4 2025-07-06 01:48:08.768628 10.0.2.15 45528 20.62.1.96 8834 TCP 74 [TCP Retransmission] 45528 → 8834 [SY
5 2025-07-06 01:48:09.024976 10.0.2.15 45530 20.62.1.96 8834 TCP 74 [TCP Retransmission] 45530 → 8834 [SY
6 2025-07-06 01:48:09.396284 192.168.56.102 1515 10.0.2.15 41331 TCP 60 1515 → 41331 [RST, ACK] Seq=1 Ack=1 W
7 2025-07-06 01:48:09.791792 10.0.2.15 45528 20.62.1.96 8834 TCP 74 [TCP Retransmission] 45528 → 8834 [SY
8 2025-07-06 01:48:10.048699 10.0.2.15 45530 20.62.1.96 8834 TCP 74 [TCP Retransmission] 45530 → 8834 [SY
9 2025-07-06 01:48:10.816113 10.0.2.15 45528 20.62.1.96 8834 TCP 74 [TCP Retransmission] 45528 → 8834 [SY
10 2025-07-06 01:48:11.072712 10.0.2.15 45530 20.62.1.96 8834 TCP 74 [TCP Retransmission] 45530 → 8834 [SY
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PCSSystemtec_7b:34:24 (08:00:27:7b:34:24), Dst: 52:55
0000 52 55 0a 00 02 02 08 00 27 7b 34 24 08 00 45 00
0010 00 3c b9 d4 40 00 40 06 5f 3b 0a 00 02 0f 14 3e
capture.pcap
Packets: 10
Profile: Default

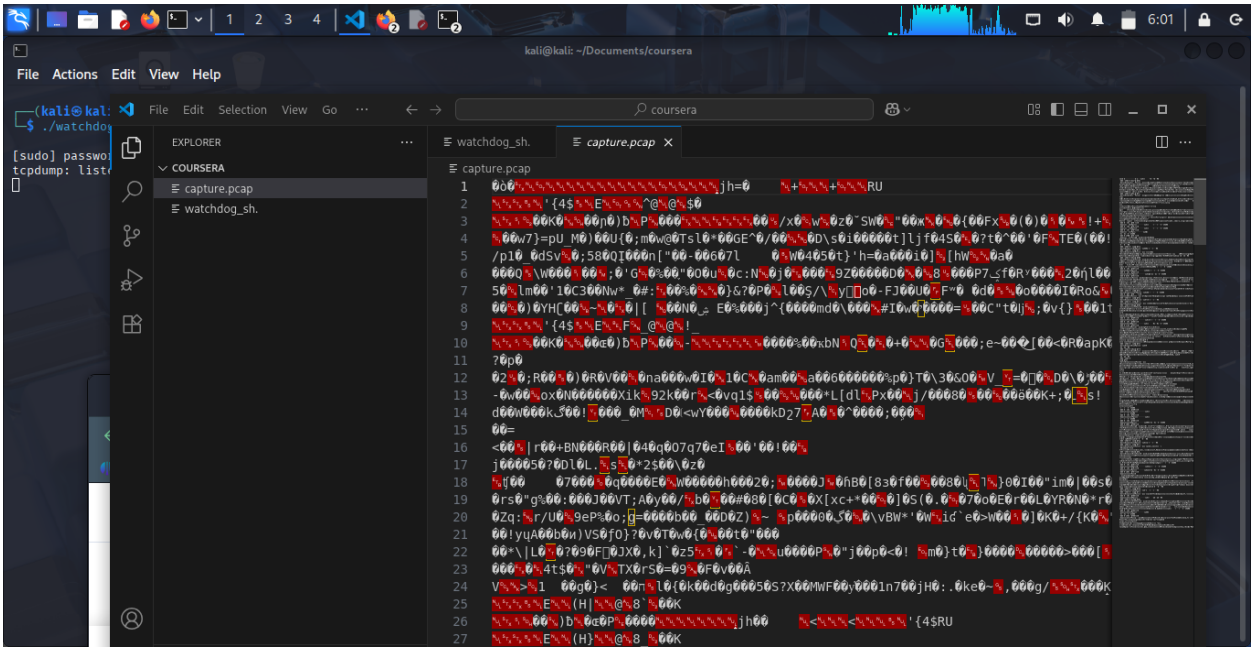


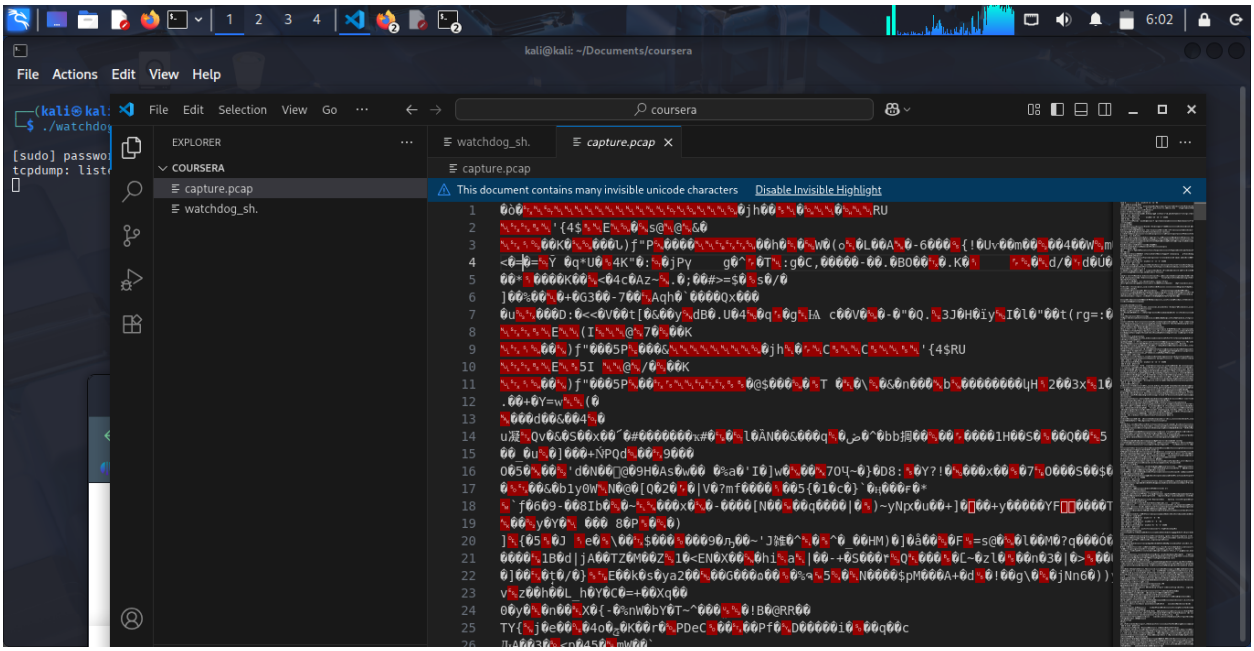
🔷 Dynamic Packet Capture with Time-Based Rotation

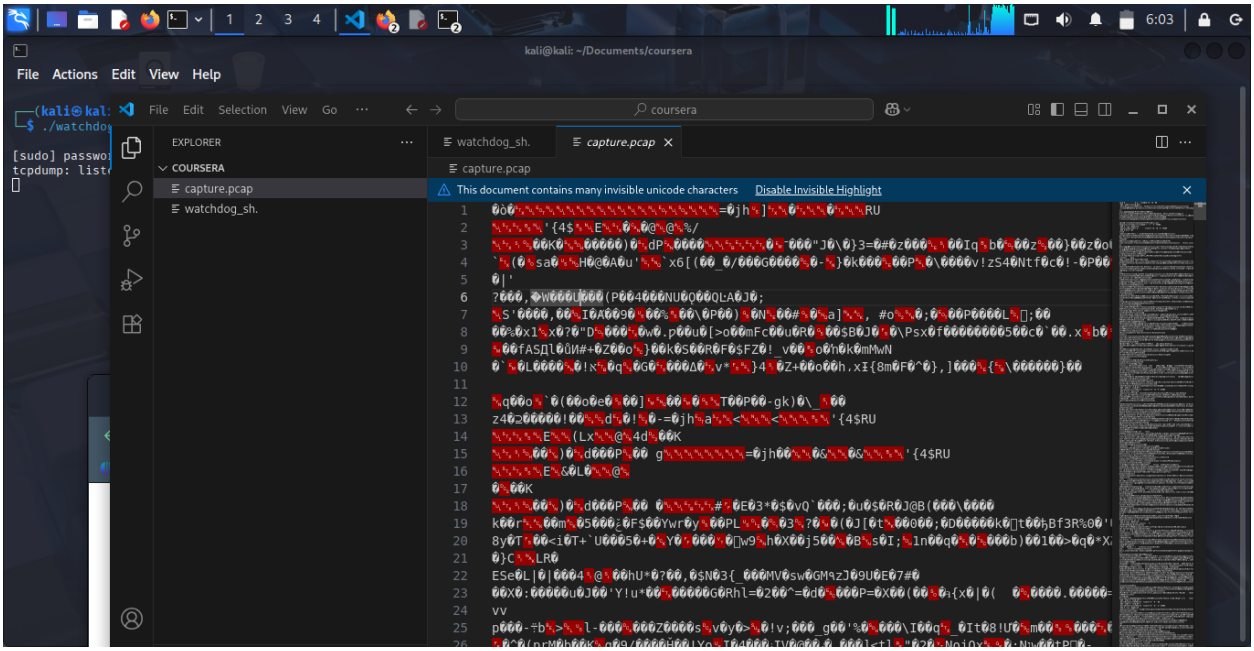
Enhanced my capture script in VS Code to target traffic from `coursera.org`, using `sudo tcpdump host coursera.org -w capture.pcap -G 15` to segment captures every 15 seconds. Executed and verified capture files in the terminal and VS Code, then optimized storage by deleting redundant `.pcap` files. Next, implemented extended rotation with `-G 600` to save captures in a timestamped directory (`$HOME/Documents/coursera-capture.pcap`), demonstrating scalable data management and advanced control over continuous network monitoring.

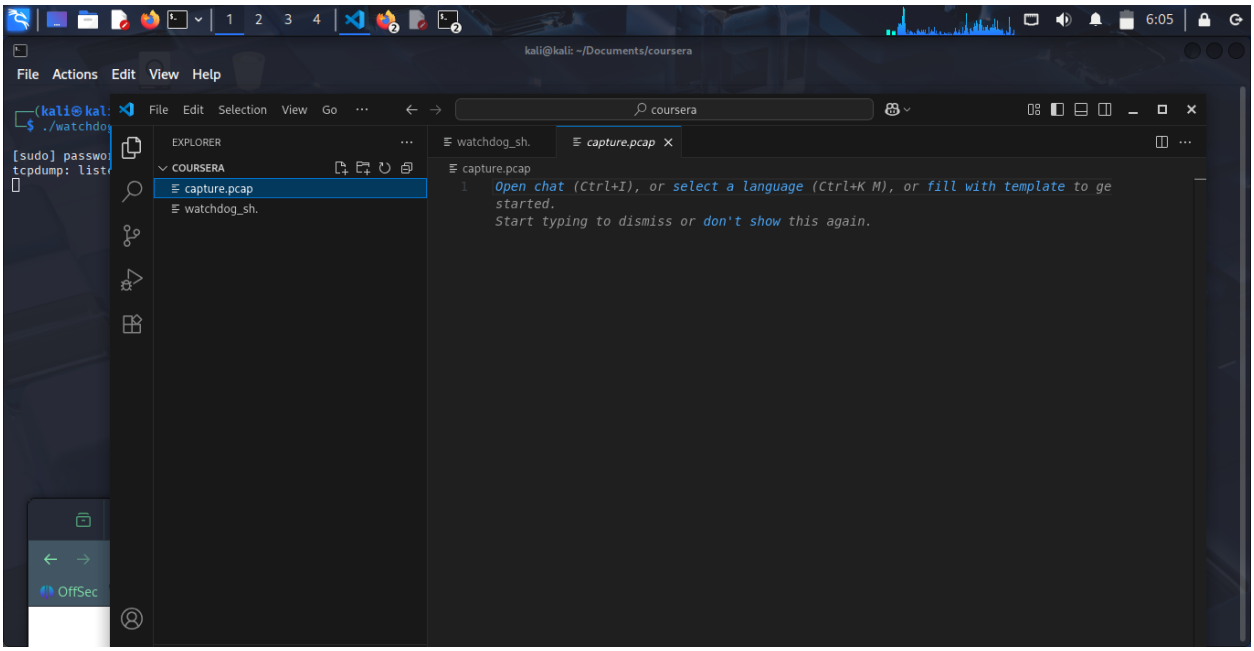


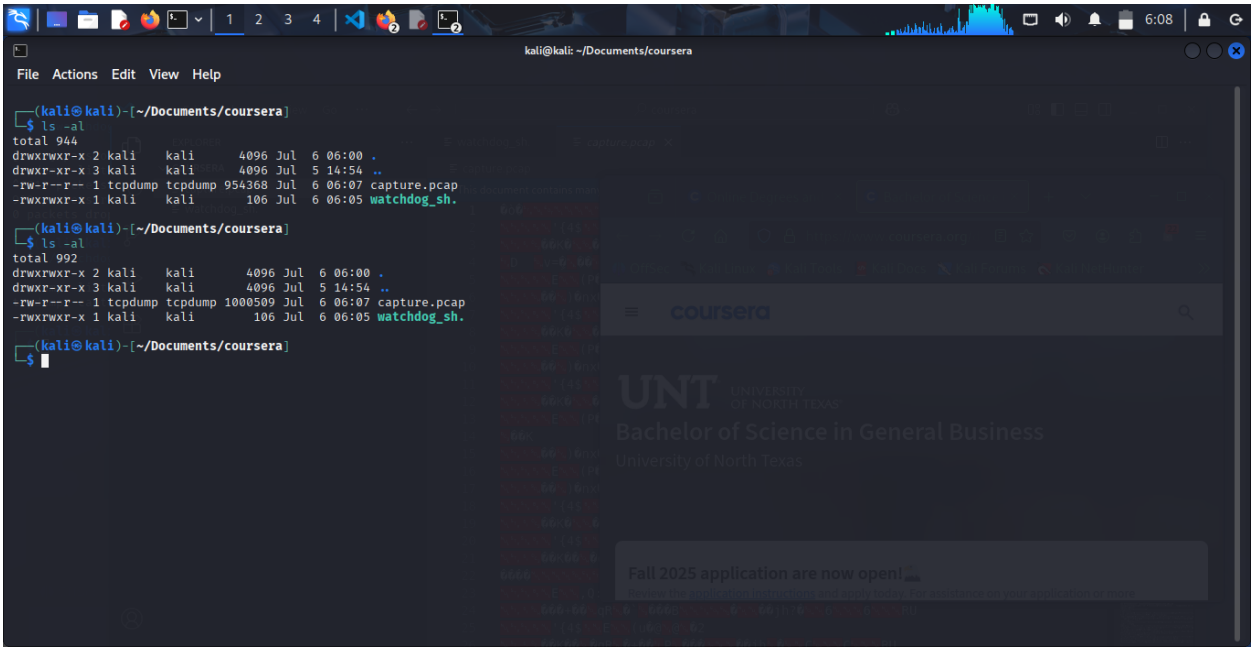

kali@kali: ~/Documents/coursera
File Actions Edit View Help
(kali㉿kali)-[~/Documents/coursera]
$ ./watchdog_sh.
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

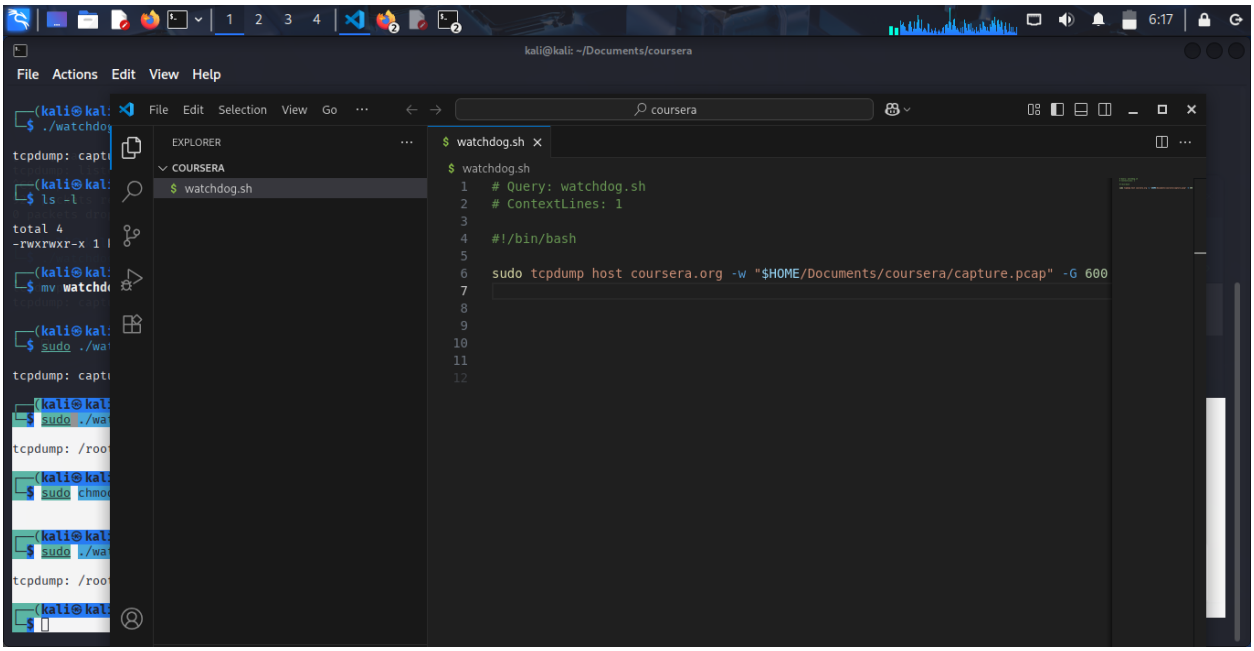

kali@kali: ~/Documents/coursera
File Actions Edit View Help
File Edit Selection View Go
coursera
EXPLORER
COURSERA
capture.pcap
watchdog_sh.
watchdog_sh.
capture.pcap
capture.pcap


6:02
kali@kali: ~/Documents/coursera
File Actions Edit View Help
File Edit Selection View Go
coursera
EXPLORER
COURSERA
capture.pcap
watchdog_sh.
watchdog_sh.
capture.pcap
capture.pcap
This document contains many invisible unicode characters
Disable Invisible Highlight


6:03
kali@kali: ~/Documents/coursera
File Actions Edit View Help
File Edit Selection View Go
coursera
EXPLORER
COURSERA
capture.pcap
watchdog_sh.
watchdog_sh.
capture.pcap
capture.pcap
This document contains many invisible unicode characters
Disable Invisible Highlight

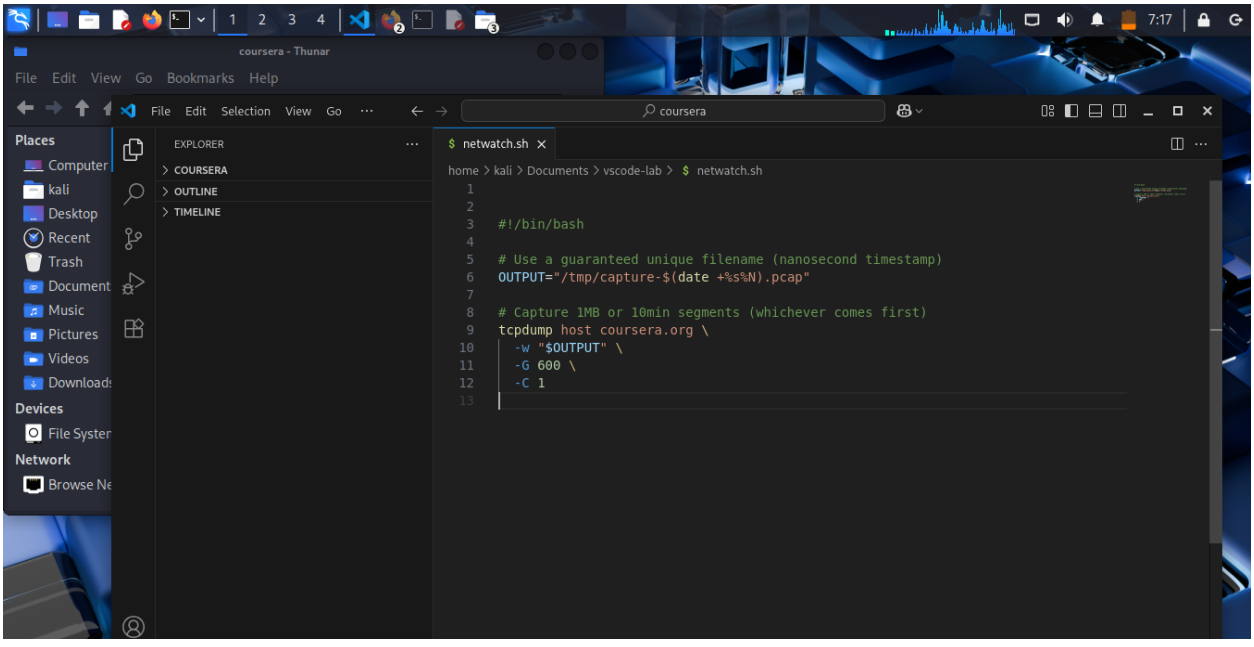

6:05
kali@kali: ~/Documents/coursera
File Actions Edit View Help
File Edit Selection View Go
coursera
EXPLORER
COURSERA
capture.pcap
watchdog_sh.
watchdog_sh.
capture.pcap
capture.pcap
Open chat (Ctrl+I), or select a language (Ctrl+K M), or fill with template to ge
started.
Start typing to dismiss or don't show this again.
OffSec

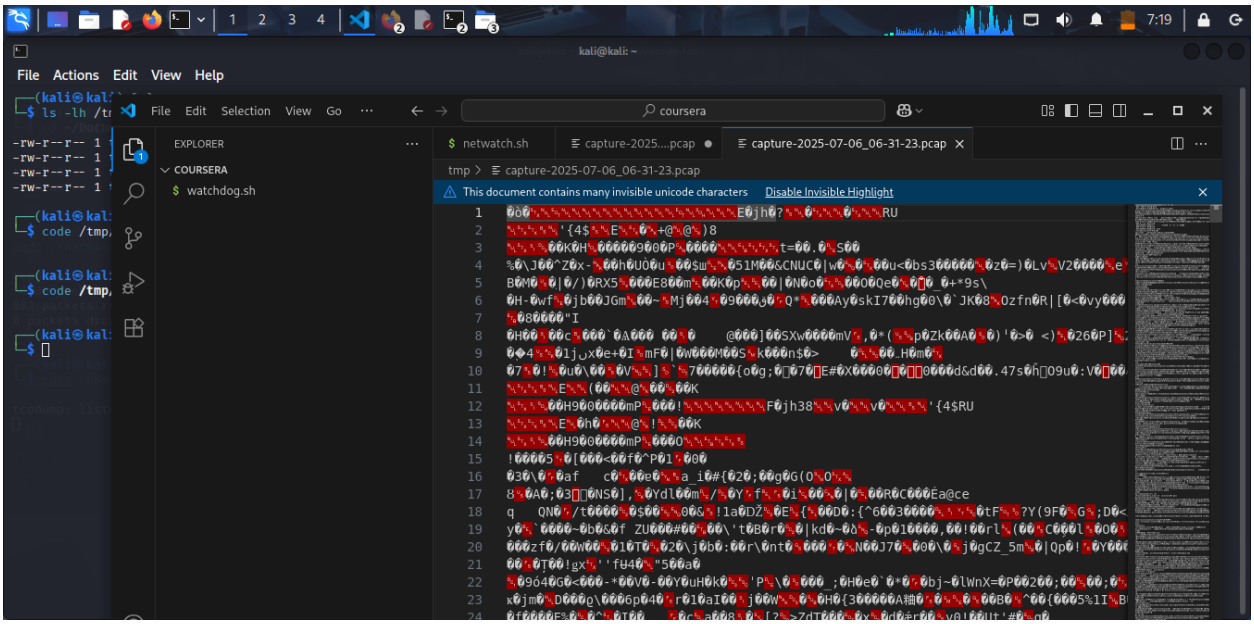

6:08
kali@kali: ~/Documents/coursera
File Actions Edit View Help
(kali㉿kali)-[~/Documents/coursera]
$ ls -al
total 944
drwxrwxr-x 2 kali kali 4096 Jul 6 06:00 .
drwxr-xr-x 3 kali kali 4096 Jul 5 14:54 ..
-rw-r--r-- 1 tcpdump tcpdump 954368 Jul 6 06:07 capture.pcap
-rwxrwxr-x 1 kali kali 106 Jul 6 06:05 watchdog_sh.
(kali㉿kali)-[~/Documents/coursera]
$ ls -al
total 992
drwxrwxr-x 2 kali kali 4096 Jul 6 06:00 .
drwxr-xr-x 3 kali kali 4096 Jul 5 14:54 ..
-rw-r--r-- 1 tcpdump tcpdump 1000509 Jul 6 06:07 capture.pcap
-rwxrwxr-x 1 kali kali 106 Jul 6 06:05 watchdog_sh.
(kali㉿kali)-[~/Documents/coursera]
$
coursera
UNT
Bachelor of Science in General Business
University of North Texas
Fall 2025 application are now open!

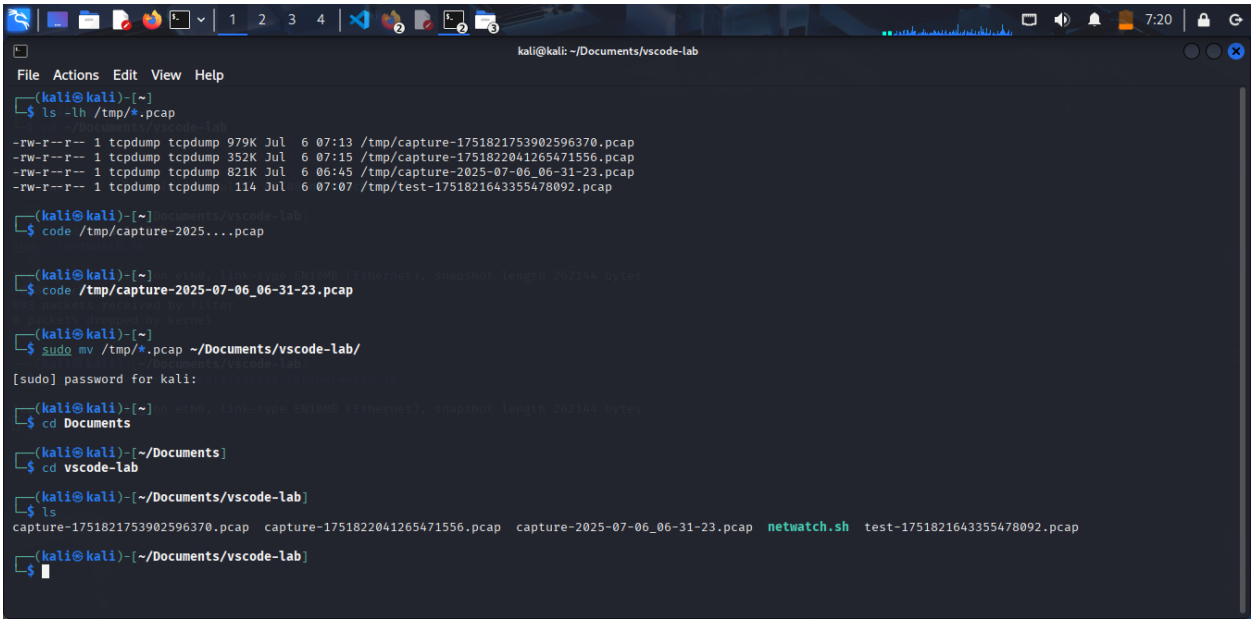


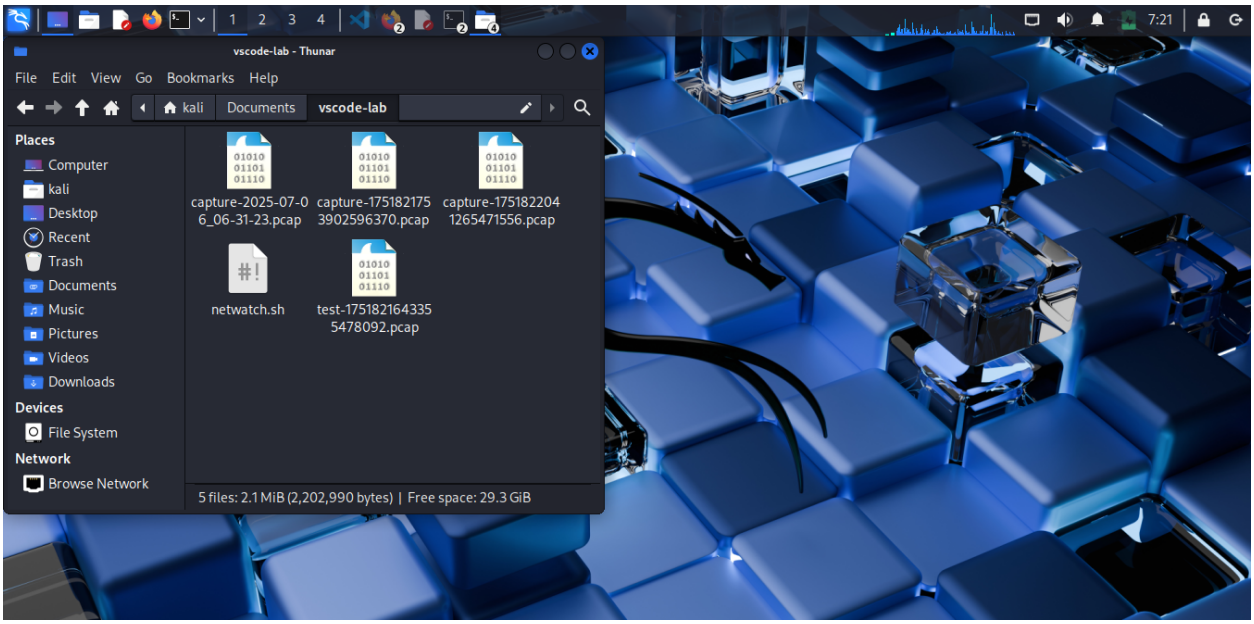
Customizing Capture Output and Automation

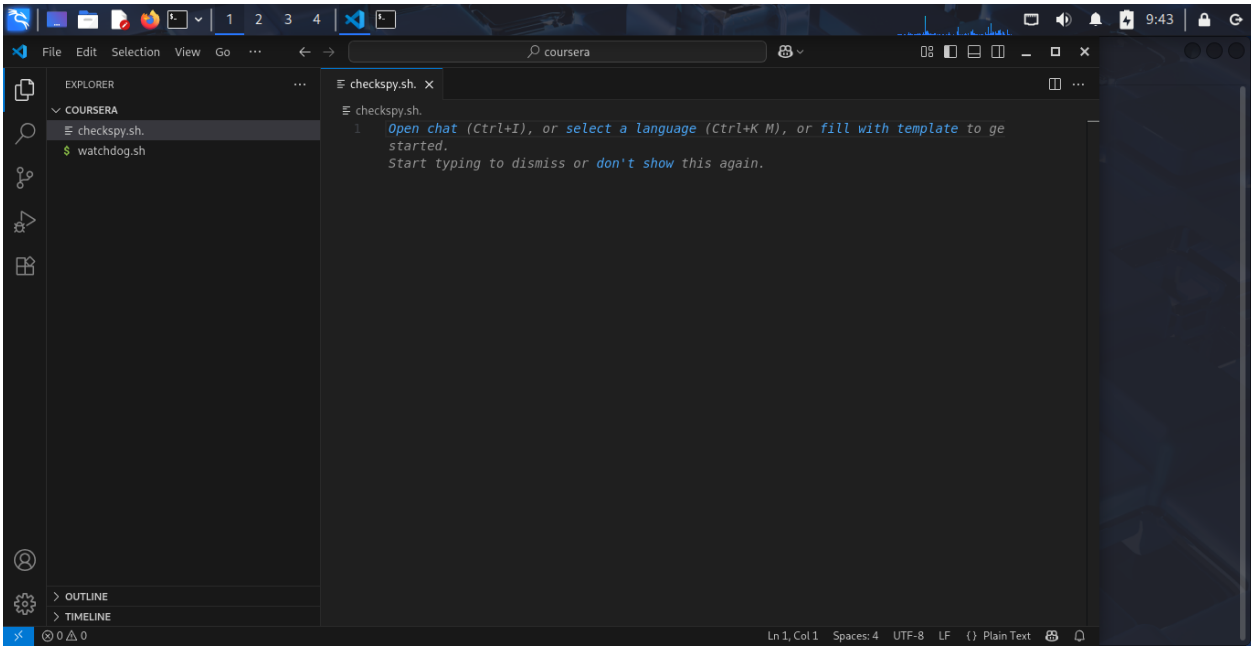
Created a new script in VS Code to dynamically generate output filenames using variables (e.g., `output=$HOME/kali/documents/vscode-lab-capture-$(date).pcap`). Employed `tcpdump` with targeted host filtering (`coursera.org`), time-based file rotation (`-G 600`), and packet count limits (`-c 1`) to capture precise, manageable packet samples. This approach highlights my ability to automate network captures with flexible, parameterized scripting—key for scalable SOC data collection and incident analysis.

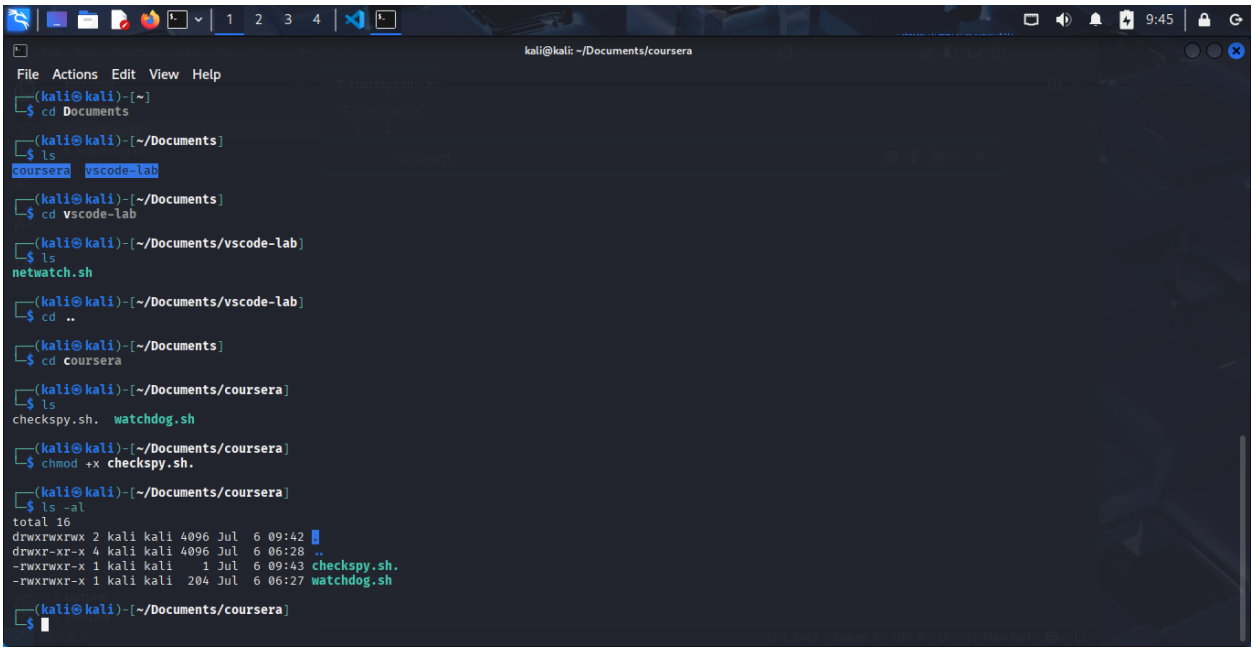


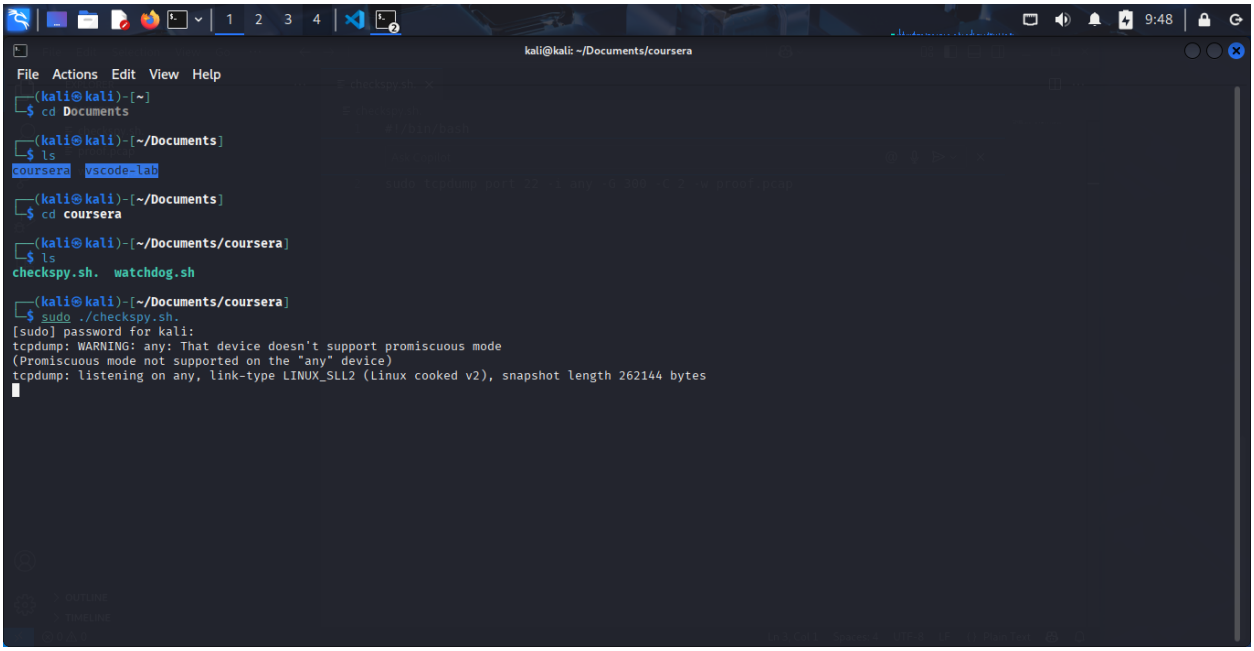

kali@kali: ~
File Actions Edit View Help
File Edit Selection View Go
coursera
EXPLORER
COURSERA
watchdog.sh
netwatch.sh
capture-2025....pcap
capture-2025-07-06_06-31-23.pcap
tmp > capture-2025-07-06_06-31-23.pcap
This document contains many invisible unicode characters
Disable Invisible Highlight


kali@kali: ~/Documents/vscode-lab
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls -lh /tmp/*.pcap
-rw-r--r-- 1 tcpdump tcpdump 979K Jul 6 07:13 /tmp/capture-1751821753902596370.pcap
-rw-r--r-- 1 tcpdump tcpdump 352K Jul 6 07:15 /tmp/capture-1751822041265471556.pcap
-rw-r--r-- 1 tcpdump tcpdump 821K Jul 6 06:45 /tmp/capture-2025-07-06_06-31-23.pcap
-rw-r--r-- 1 tcpdump tcpdump 114 Jul 6 07:07 /tmp/test-1751821643355478092.pcap
$ code /tmp/capture-2025....pcap
$ code /tmp/capture-2025-07-06_06-31-23.pcap
$ sudo mv /tmp/*.pcap ~/Documents/vscode-lab/
[sudo] password for kali:
$ cd Documents
$ cd vscode-lab
$ ls
capture-1751821753902596370.pcap capture-1751822041265471556.pcap capture-2025-07-06_06-31-23.pcap netwatch.sh test-1751821643355478092.pcap


vscode-lab - Thunar
File Edit View Go Bookmarks Help
kali Documents vscode-lab
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
capture-2025-07-06_06-31-23.pcap
capture-1751821753902596370.pcap
capture-1751822041265471556.pcap
netwatch.sh
test-1751821643355478092.pcap
5 files: 2.1 MiB (2,202,990 bytes) | Free space: 29.3 GiB

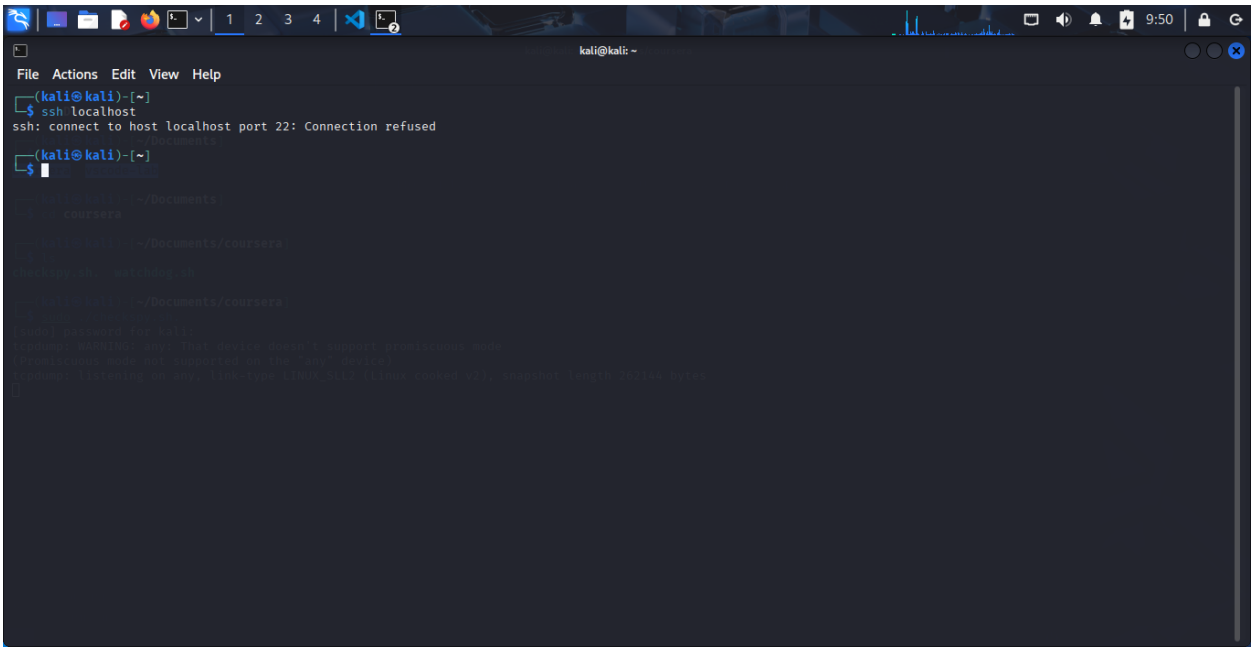

File Edit Selection View Go
coursera
EXPLORER
COURSERA
checkspy.sh.
watchdog.sh
checkspy.sh.
Open chat (Ctrl+I), or select a language (Ctrl+K M), or fill with template to ge started.
Start typing to dismiss or don't show this again.
OUTLINE
TIMELINE
Ln 1, Col 1 Spaces: 4 UTF-8 LF Plain Text

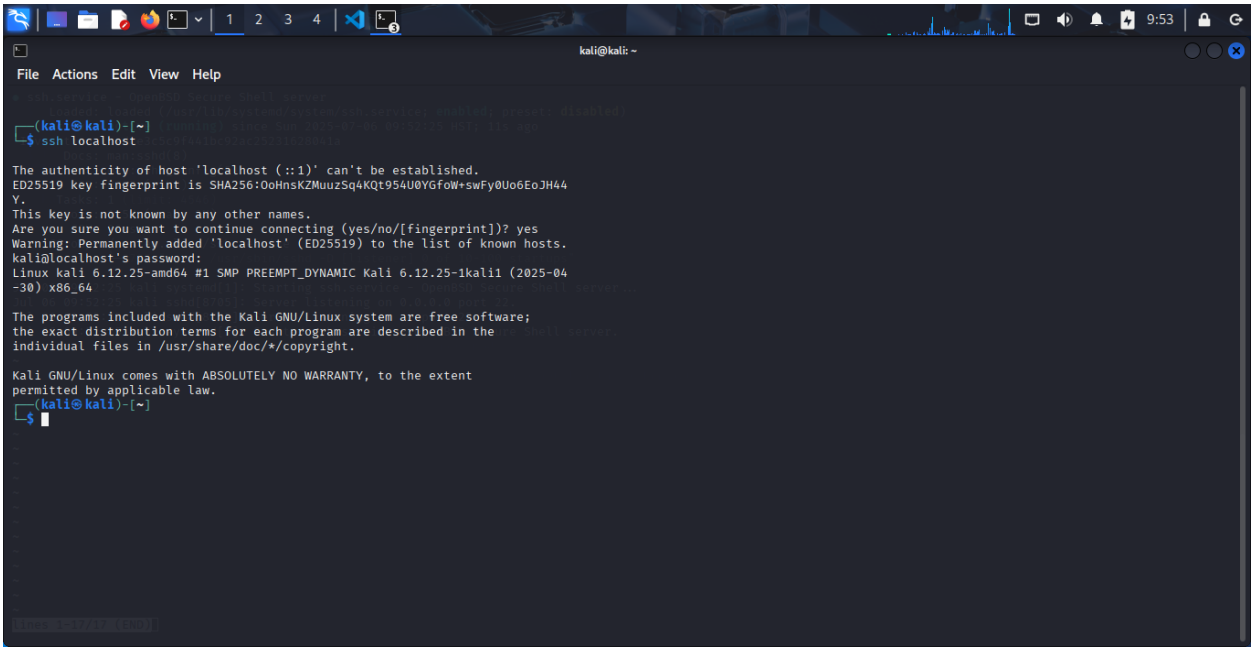


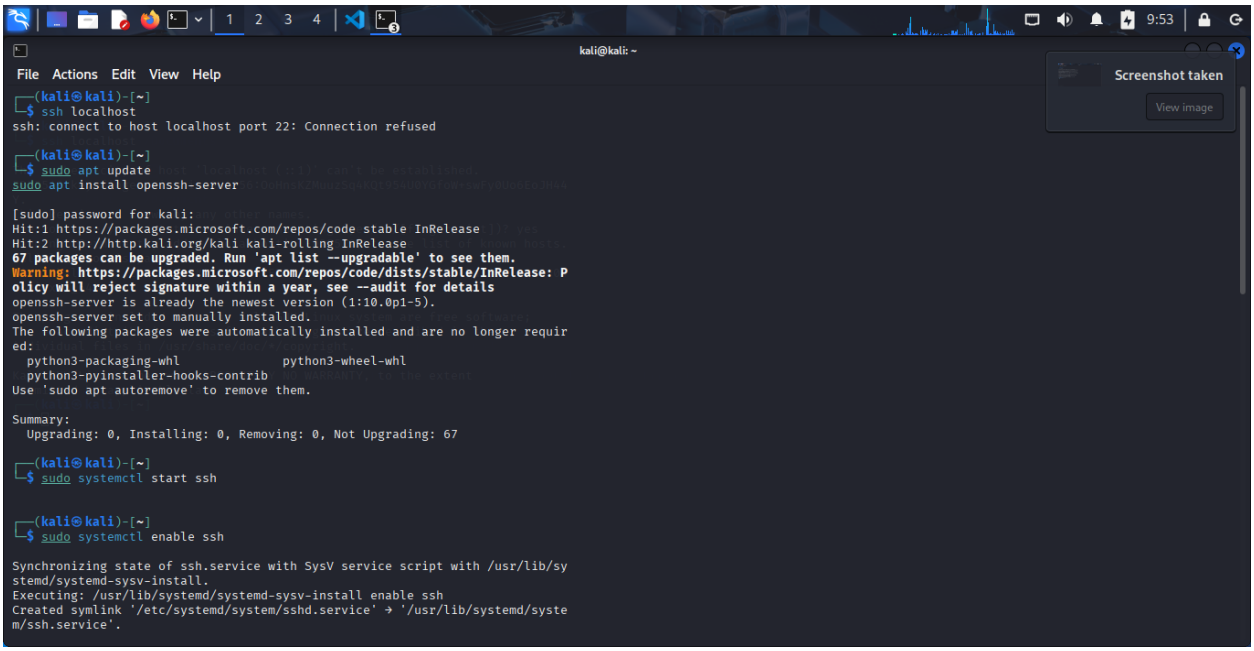


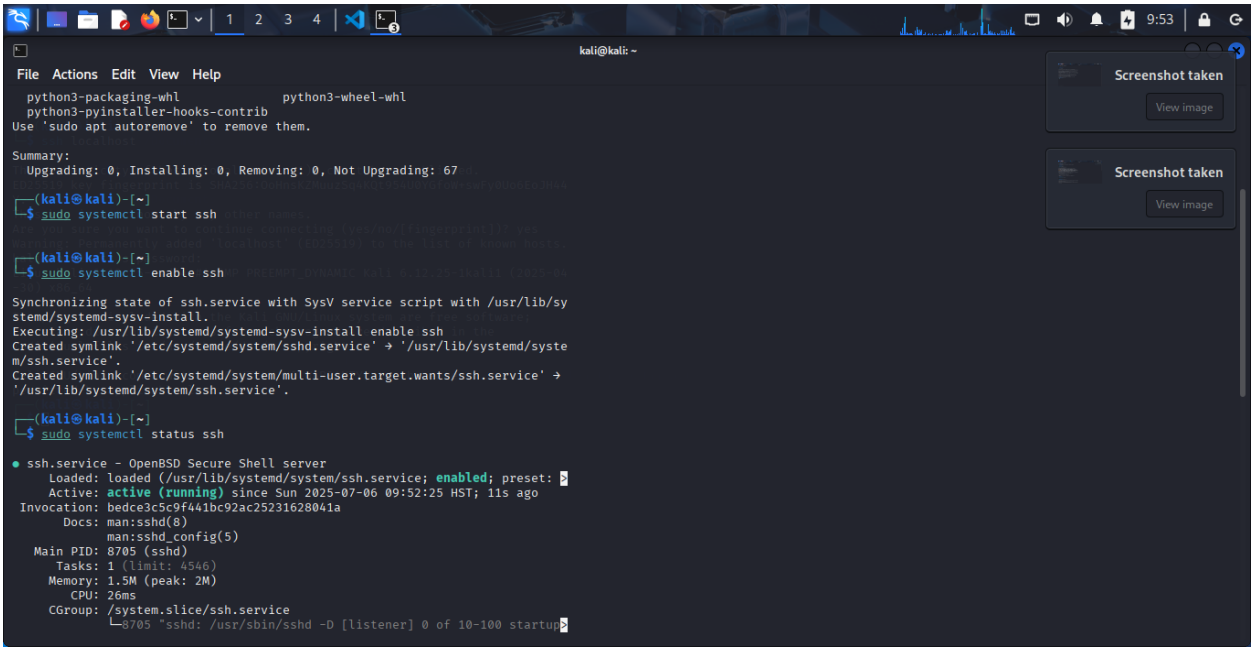
Setting Up and Capturing SSH Traffic Locally

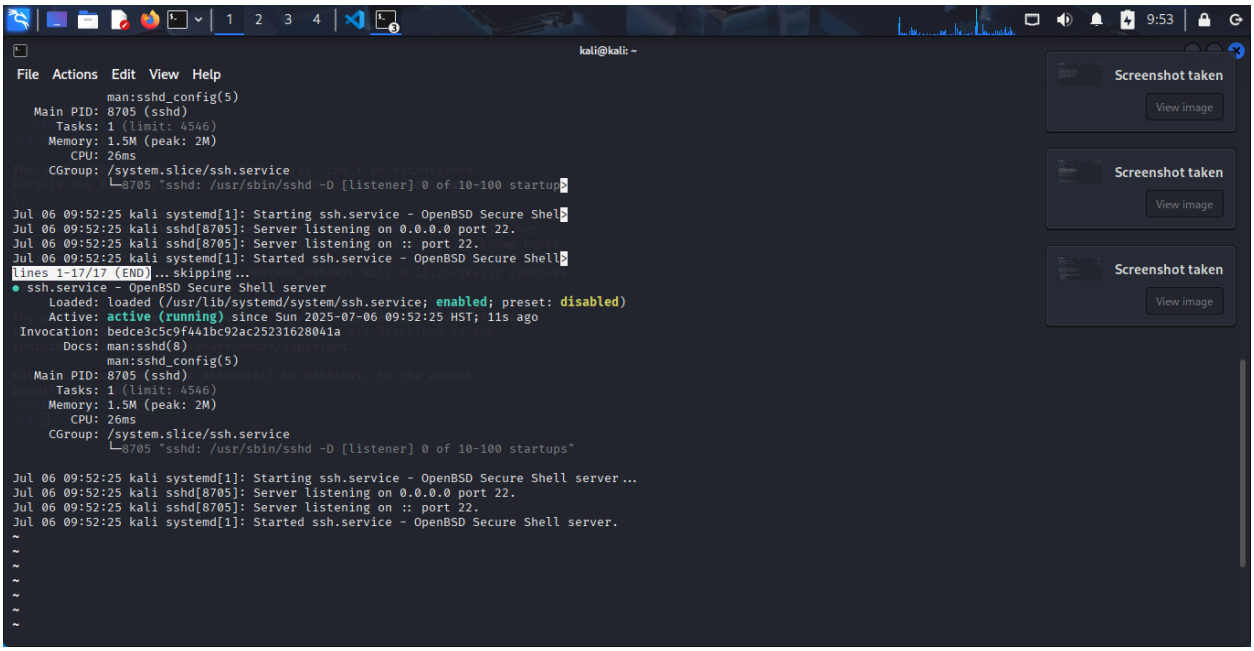
Configured and started the OpenSSH server on Kali Linux using `sudo systemctl start ssh` and `enable ssh` to enable SSH service. Established an SSH connection to `localhost` to generate encrypted traffic. Simultaneously, ran packet captures which produced a `.pcap` file (`proof.pcap`). Imported this capture into Wireshark, where I analyzed the encrypted SSH packets, validating my ability to generate, capture, and inspect secure traffic flows within a controlled environment—a critical skill for SOC analysts handling encrypted threat data.

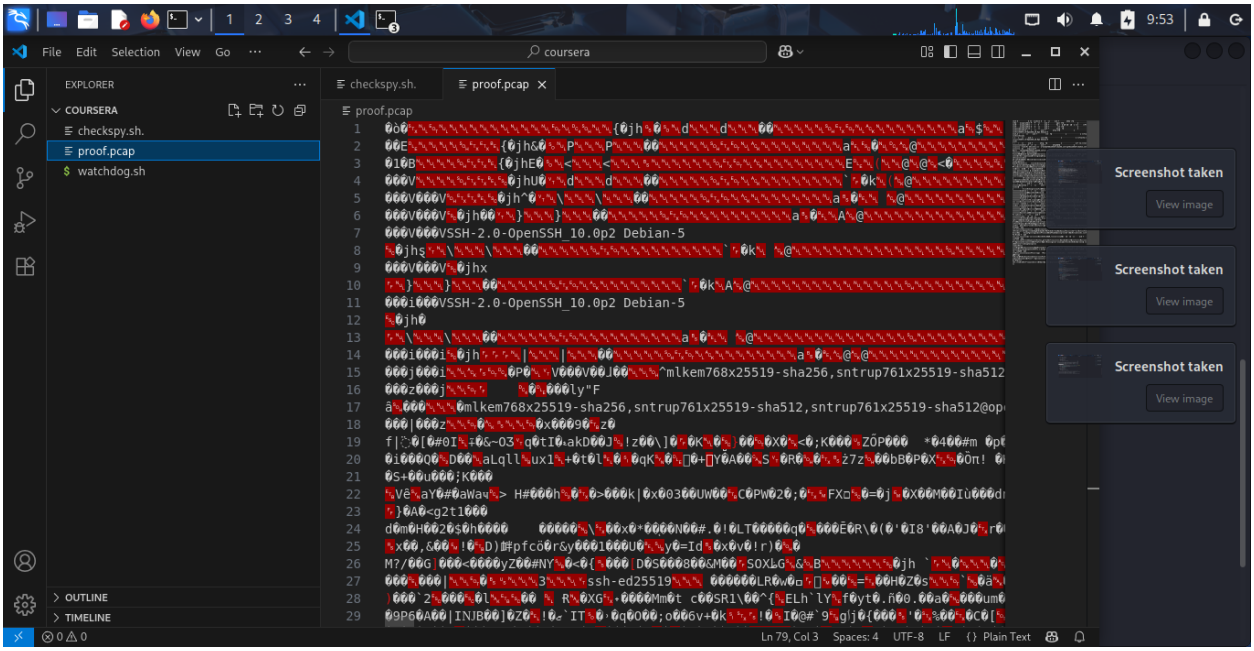

1 2 3 4
9:50
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ssh localhost
ssh: connect to host localhost port 22: Connection refused
┌──(kali㉿kali)-[~]
└─$

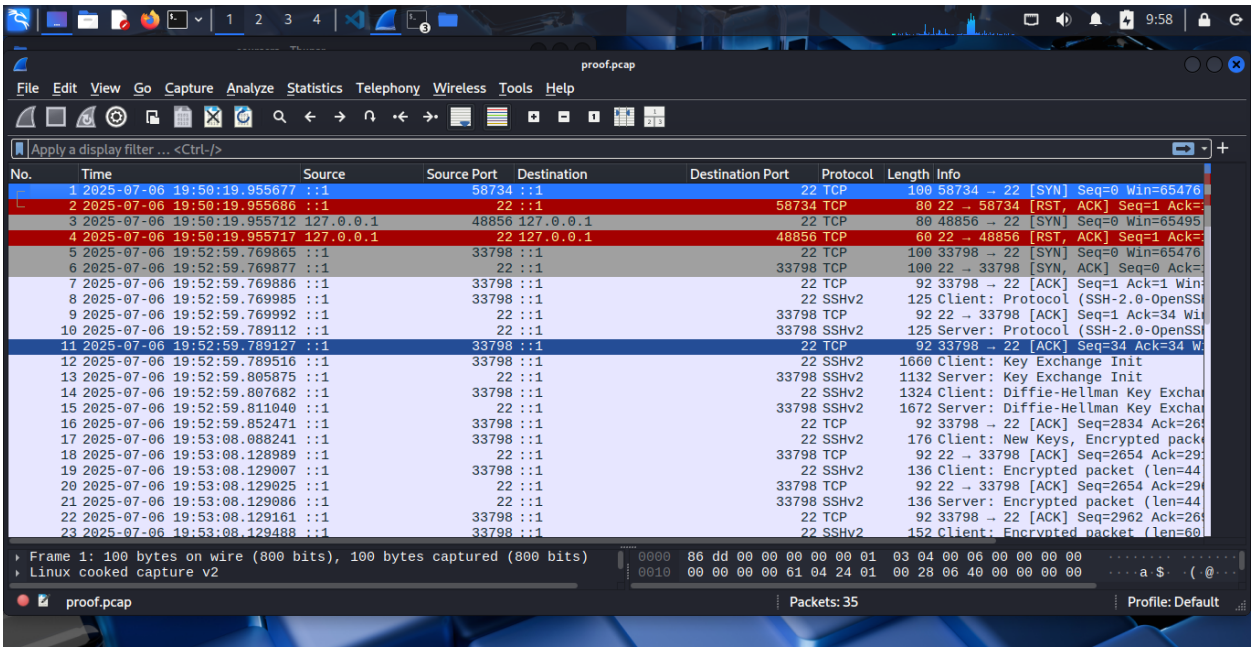

1 2 3 4
9:53
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:OoHnsKZMuuzSq4KQt954U0YGfoW+swFy0Uo6EoJH44
Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
kali@localhost's password:
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04
-30) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌──(kali㉿kali)-[~]
└─$


1 2 3 4
9:53
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ssh localhost
ssh: connect to host localhost port 22: Connection refused
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install openssh-server
[sudo] password for kali:
Hit:1 https://packages.microsoft.com/repos/code stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
67 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: https://packages.microsoft.com/repos/code/dists/stable/InRelease: P
olicy will reject signature within a year, see --audit for details
openssh-server is already the newest version (1:10.0p1-5).
openssh-server set to manually installed.
The following packages were automatically installed and are no longer requir
ed:
python3-packaging-whl python3-wheel-whl
python3-pyinstaller-hooks-contrib
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 67
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start ssh
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/sy
stemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/syste
m/ssh.service'.
Screenshot taken
View image


1 2 3 4
9:53
kali@kali: ~
File Actions Edit View Help
python3-packaging-whl python3-wheel-whl
python3-pyinstaller-hooks-contrib
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 67
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start ssh
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/sy
stemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/syste
m/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' →
'/usr/lib/systemd/system/ssh.service'.
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset:
Active: active (running) since Sun 2025-07-06 09:52:25 HST; 11s ago
Invocation: bedce3c5c9f441bc92ac25231628041a
Docs: man:sshd(8)
man:sshd_config(5)
Main PID: 8705 (sshd)
Tasks: 1 (limit: 4546)
Memory: 1.5M (peak: 2M)
CPU: 26ms
CGroup: /system.slice/ssh.service
└─8705 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup
Screenshot taken
View image
Screenshot taken
View image


kali@kali: ~
File Actions Edit View Help
man:sshd_config(5)
Main PID: 8705 (sshd)
Tasks: 1 (limit: 4546)
Memory: 1.5M (peak: 2M)
CPU: 26ms
CGroup: /system.slice/ssh.service
└─8705 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup
Jul 06 09:52:25 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shel
Jul 06 09:52:25 kali sshd[8705]: Server listening on 0.0.0.0 port 22.
Jul 06 09:52:25 kali sshd[8705]: Server listening on :: port 22.
Jul 06 09:52:25 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell
lines 1-17/17 (END) ...skipping...
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
Active: active (running) since Sun 2025-07-06 09:52:25 HST; 11s ago
Invocation: bedce3c5c9f441bc92ac25231628041a
Docs: man:sshd(8)
man:sshd_config(5)
Main PID: 8705 (sshd)
Tasks: 1 (limit: 4546)
Memory: 1.5M (peak: 2M)
CPU: 26ms
CGroup: /system.slice/ssh.service
└─8705 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Jul 06 09:52:25 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jul 06 09:52:25 kali sshd[8705]: Server listening on 0.0.0.0 port 22.
Jul 06 09:52:25 kali sshd[8705]: Server listening on :: port 22.
Jul 06 09:52:25 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Screenshot taken
View image
Screenshot taken
View image
Screenshot taken
View image


File Edit Selection View Go
coursera
EXPLORER
COURSERA
checkspy.sh
proof.pcap
watchdog.sh
checkspy.sh
proof.pcap
OUTLINE
TIMELINE
Ln 79, Col 3 Spaces: 4 UTF-8 LF {} Plain Text
Screenshot taken
View image
Screenshot taken
View image
Screenshot taken
View image
Screenshot taken
View image



Conclusion

This project demonstrates my comprehensive ability to design, automate, and analyze network traffic capture workflows using industry-standard tools like `tcpdump`, Bash scripting, and Wireshark. By simulating real-world traffic and employing advanced capture techniques, I developed a scalable process for generating, filtering, and inspecting `.pcap` data that mirrors core SOC operational practices.

Beyond technical execution, I showed disciplined validation, precise control of network interfaces, and adaptability in data management—skills essential for effective threat detection and incident response. This hands-on experience deepens my proficiency in packet-level forensics and underscores my readiness to contribute immediately to blue team environments and SOC analyst roles, where automation, accuracy, and actionable insight are paramount.

Moving forward, I aim to integrate this workflow with SIEM tools and threat intelligence platforms to further enhance detection capabilities and build robust, real-time security monitoring pipelines—strengthening my ability to protect organizations from evolving threats.