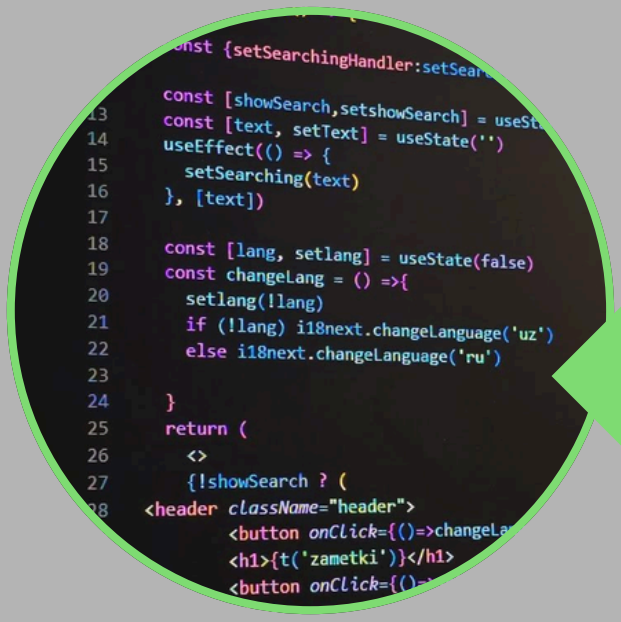
Uneeq interns

2025/
2026

Network-traffic analysis report

Traffic Capture and Protocol Analysis Using Wireshark and Command-Line Tools



Prepared by

Fareeda HossamEldin

LinkedIn Profile:

www.linkedin.com/in/fareeda-hossameldin-4154a2353

Uneeq interns

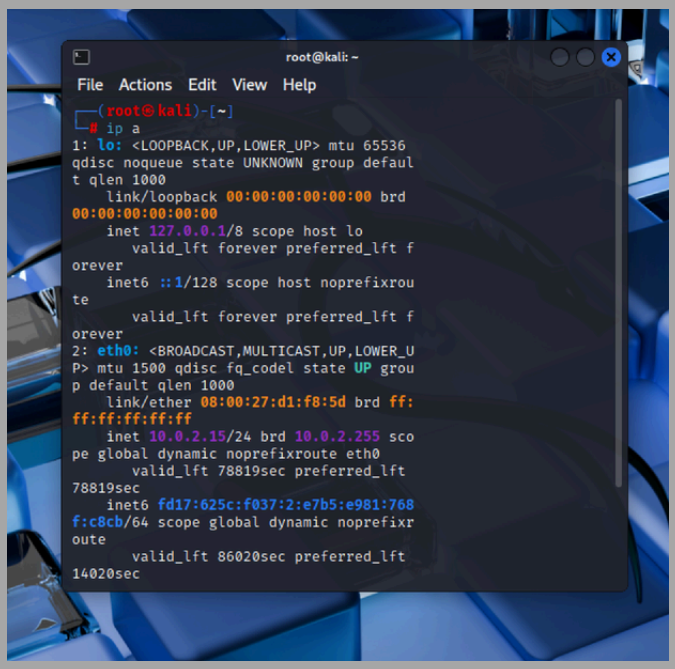
Project Summary

This project involved capturing and analyzing network traffic to study connectivity, protocol behavior, and communication patterns, providing insights into network performance and troubleshooting

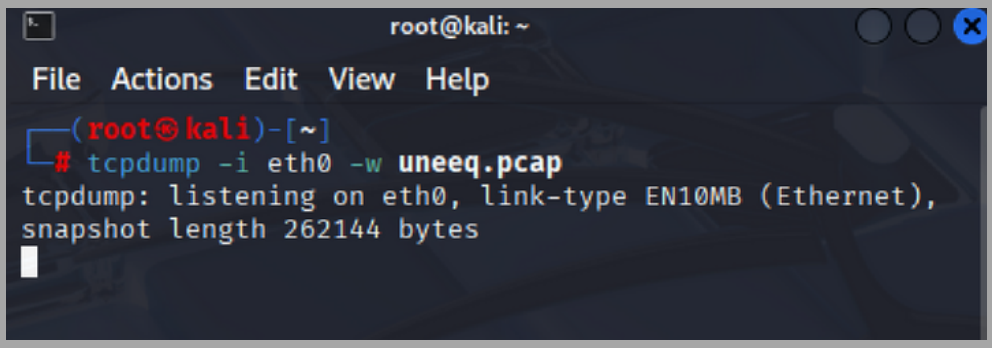
Project Objectives:

- Capture and analyze network traffic.
- Check connectivity and detect issues.
- Study protocol behavior and functions.

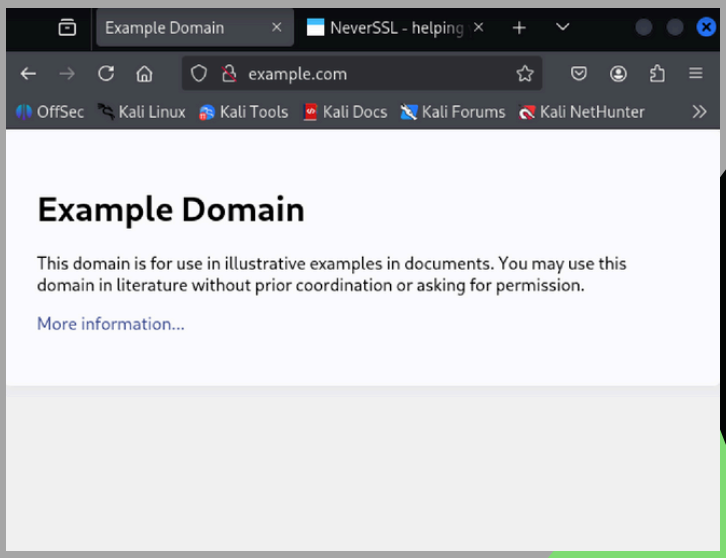
Checking for active interface using ip a:



Starting TCPdump capture:



Generating Traffic:



Preform DNS lookup using “dig”:

```
┌──(root㉿kali)-[~]
└─# dig badsite.example

; <<>> DiG 9.20.9-1-Debian <<>> badsite.example
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43679
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: d4348068cbbae54caa43a00f689a067600c2ddb37274112 (good)
;; QUESTION SECTION:
;badsite.example.               IN      A

;; AUTHORITY SECTION:
example.                8003    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2025081101 1800 900 604800 86400

;; Query time: 16 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Mon Aug 11 11:03:06 EDT 2025
;; MSG SIZE  rcvd: 147
```

```
┌──(root㉿kali)-[~]
└─# dig freebitcoin.win

; <<>> DiG 9.20.9-1-Debian <<>> freebitcoin.win
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40831
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 60c1ab6690b1a166732131e4689a066ed8c74999edc14fd (good)
;; QUESTION SECTION:
;freebitcoin.win.               IN      A

;; ANSWER SECTION:
freebitcoin.win.        300     IN      A       104.21.32.203
freebitcoin.win.        300     IN      A       172.67.187.117

;; Query time: 60 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Mon Aug 11 11:03:21 EDT 2025
;; MSG SIZE  rcvd: 104
```

send icmp requests:

```
┌──(root㉿kali)-[~]
└─# ping -c 20 198.51.100.5
PING 198.51.100.5 (198.51.100.5) 56(84) bytes of data.

--- 198.51.100.5 ping statistics ---
20 packets transmitted, 0 received, 100% packet loss, time 19445ms
```

root@kali: ~

File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# ping -c 20 203.0.113.10
PING 203.0.113.10 (203.0.113.10) 56(84) bytes of data.

--- 203.0.113.10 ping statistics ---
20 packets transmitted, 0 received, 100% packet loss, time 19433ms
```

TCP Port Connectivity Test with Netcat:

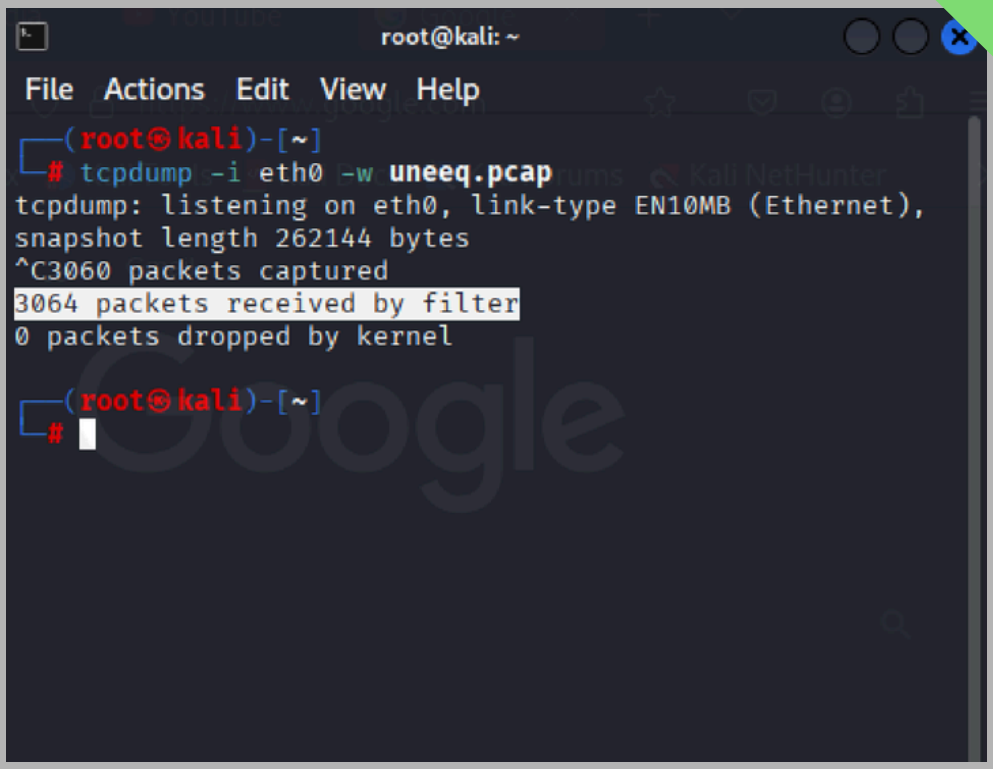
root@kali: ~

File Actions Edit View Help

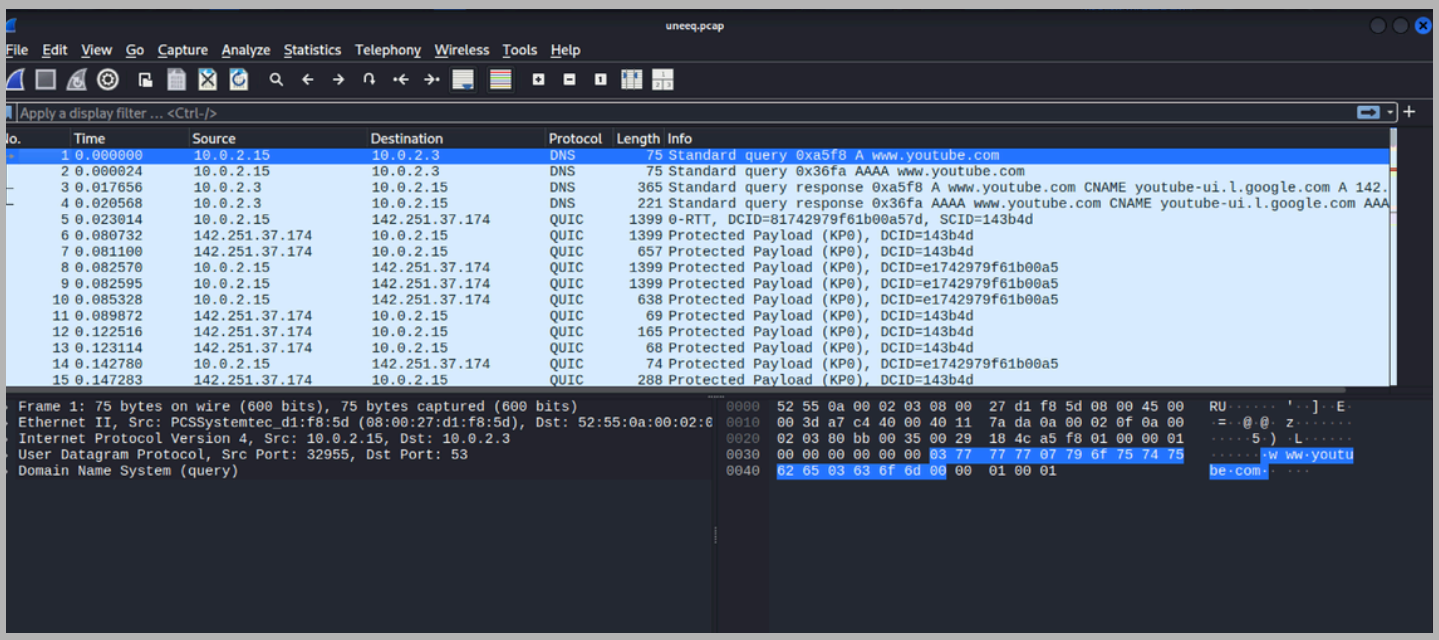
```
┌──(root㉿kali)-[~]
└─# nc scanme.nmap.org 8080
scanme.nmap.org [45.33.32.156] 8080 (http-alt) : Connection refused

┌──(root㉿kali)-[~]
└─#
```

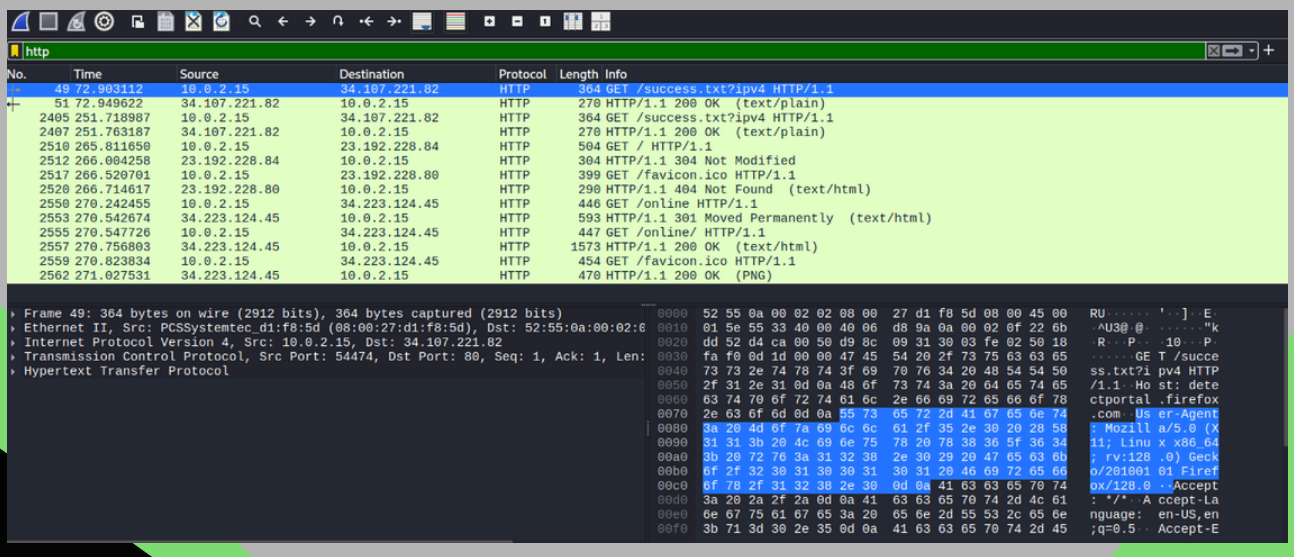
Stop TCPdump:



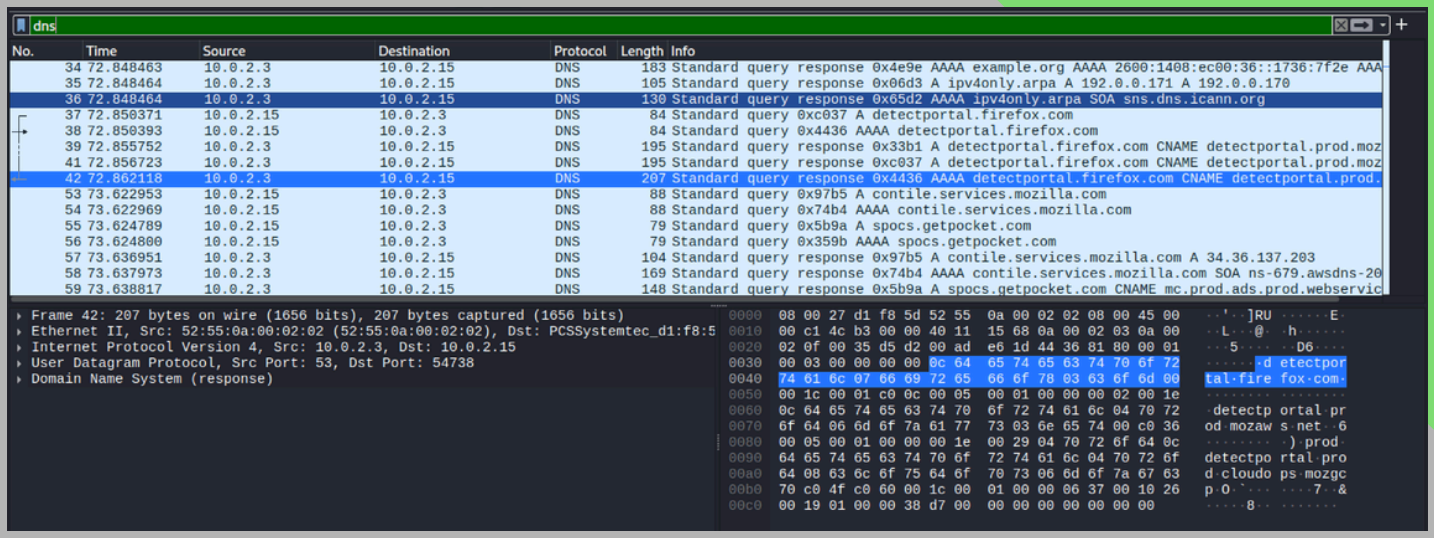
Open “uneeq.pcap” file on Wireshark:



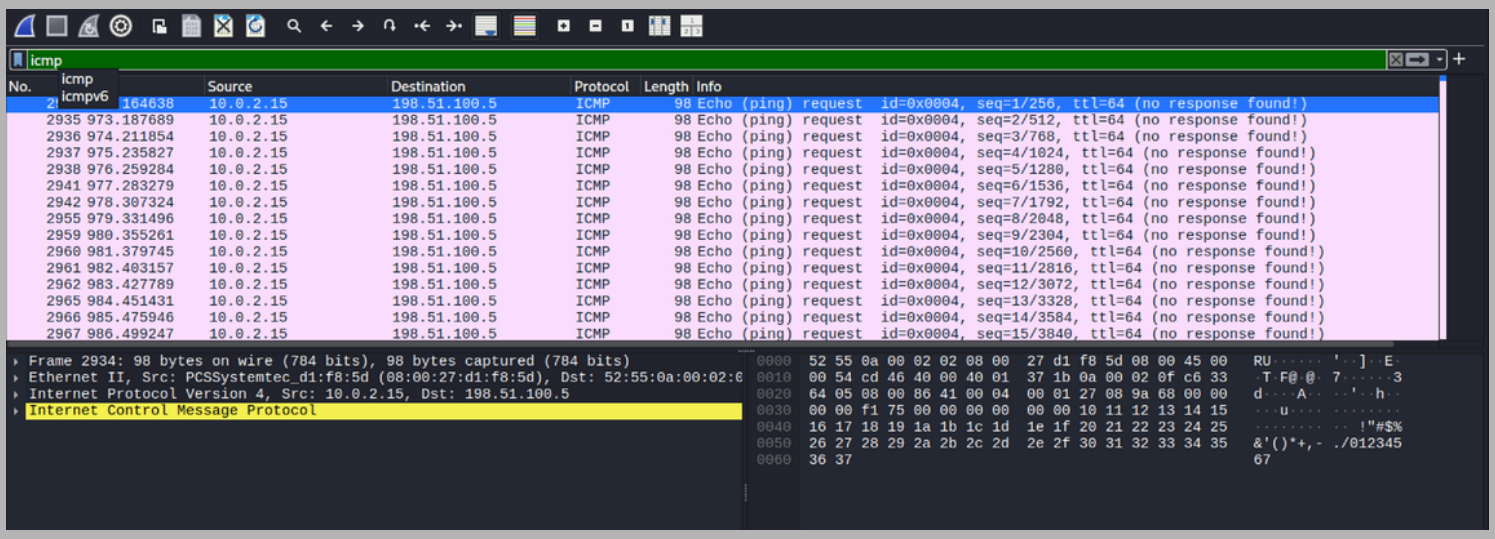
Applying “http” Fiter: Captured HTTP requests and headers such as Host, User-Agent, etc



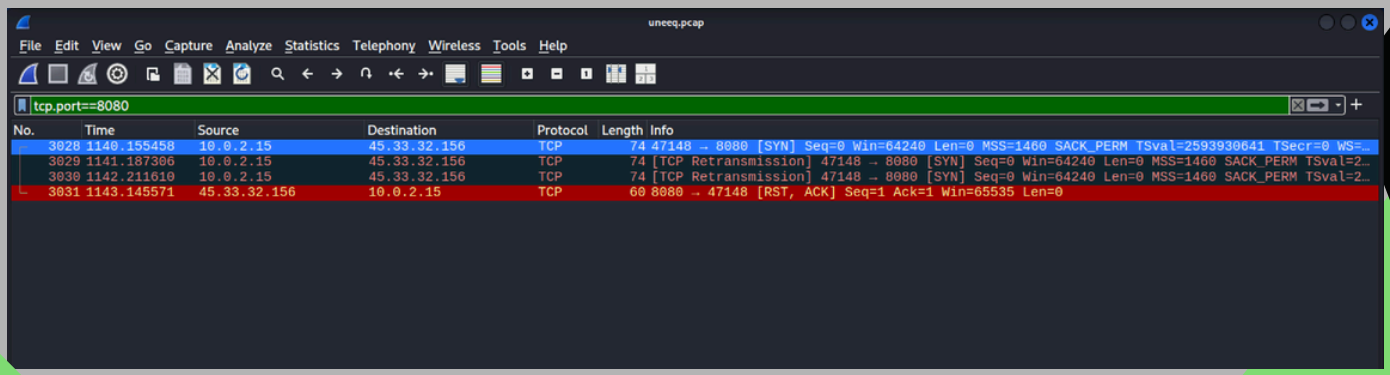
Applying “dns” filter: Observed DNS requests and replies to analyze domain name resolution.



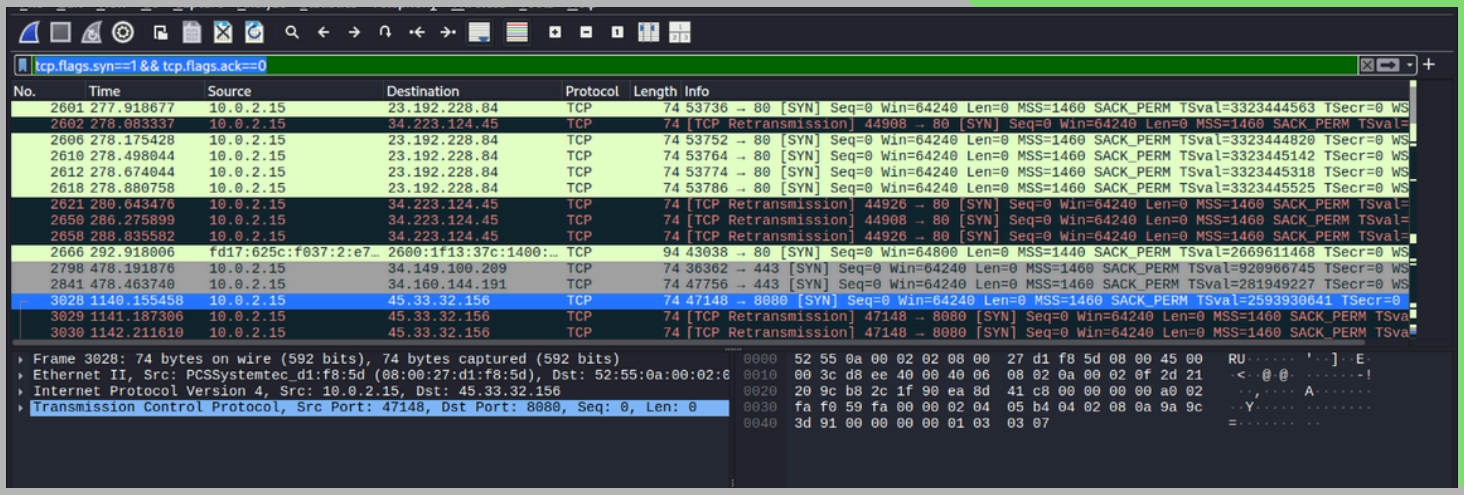
Apply “icmp” filter: to show echo requests (ping) sent to test reachability and echo replies received as responses.



Applying “tcp.port==8080” Fiter:

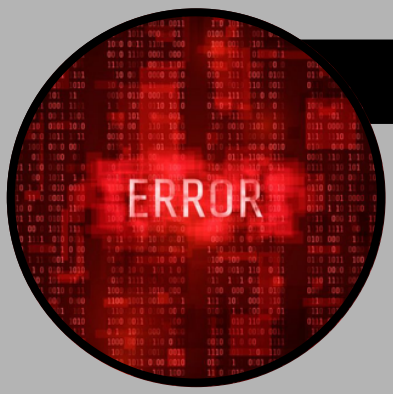


Applying “tcp.flags.syn==1 && tcp.flags.ack==0" filter:



Uneeq interns

Suspicious activity and recommendations



Suspicious activity

- Unusual TCP SYN Traffic: Multiple SYN packets to port 8080 from unknown IPs, possible scan/probe.
- Suspicious HTTP Requests: Hostnames not linked to expected traffic , potential phishing/malware.
- Repeated ICMP Requests: Excessive pings from one external IP , possible reconnaissance.

Recommendations

- Block Unused Ports: Filter unsolicited SYN packets on non-essential ports.
- DNS Filtering: Block resolution of suspicious domains.
- Restrict ICMP: Allow only from trusted IPs.
- Monitor Regularly: Run periodic tcpdump/Wireshark captures.
- Update IDS Rules: Keep detection signatures current.

Conclusion

- The analysis successfully identified normal and potentially malicious traffic patterns using Linux commands and Wireshark filters. Detected anomalies, such as unusual SYN packets, suspicious HTTP requests, and repeated ICMP pings, highlight the need for proactive security measures. Implementing the recommended controls will enhance network protection and reduce exposure to threats.