

# Network-traffic analysis report

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



```
const [setSearchingHandler:setSearchin
13 const [showSearch, setShowSearch] = useState(false)
14 const [text, setText] = useState('')
15 useEffect(() => {
16   setSearching(text)
17 }, [text])
18
19 const [lang, setLang] = useState(false)
20 const changeLang = () =>{
21   setLang(!lang)
22   if (!lang) i18next.changeLanguage('uz')
23   else i18next.changeLanguage('ru')
24 }
25 return (
26   <>
27   {!showSearch ? (
28     <header className="header">
29       <button onClick={()=>changeLang}>
```

Prepared by  
Fareeda HossamEldin



LinkedIn Profile:

[www.linkedin.com/in/fareeda-hossameldin-4154a2353](https://www.linkedin.com/in/fareeda-hossameldin-4154a2353)

# 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.

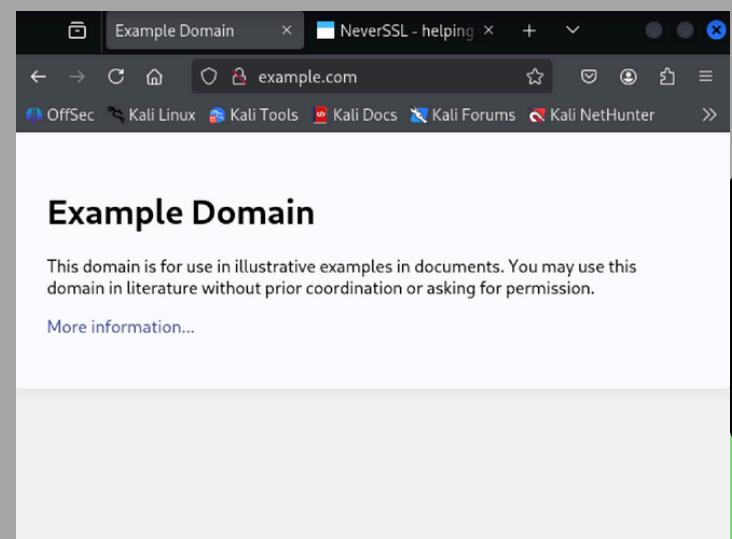
## Checking for active interface using ip a:

```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536
qdisc noqueue state UNKNOWN group default
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qlen 1000
        link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute
            valid_lft 78819sec preferred_lft 78819sec
            inet6 fd17:625c:f037:2:e7b5:e981:768f:c8cb/64 scope global dynamic noprefixroute
                valid_lft 86020sec preferred_lft 14020sec
```

## Starting TCPdump capture:

```
root@kali:~# tcpdump -i eth0 -w uneeq.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

## 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: NOERROR, id: 43679
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: d4348068ccbbae54caa43a00f689a06
; QUESTION SECTION:
; badsite.example.
; AUTHORITY SECTION:
; A 8003rev IN S
A a.root-servers.net. ns1.root-servers.net. 2025081101 1800 900 604800 8
400
; 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: 60c1ab6690b1a166732131e4689a06
; QUESTION SECTION:
; freebitcoin.win.
; 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

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

#
```

## Stop TCPdump:

```
root@kali:~#
# tcpdump -i eth0 -w uneeq.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet),
snapshot length 262144 bytes
^C3060 packets captured
3064 packets received by filter
0 packets dropped by kernel
#
```

## Open “uneeq.pcap” file on Wireshark:

The screenshot shows the Wireshark interface with the file "uneeq.pcap" loaded. The packet list pane displays 15 captured DNS requests from 10.0.2.15 to 10.0.2.3. The details pane shows the DNS query structure, and the bytes pane shows the raw hex and ASCII data for one of the requests.

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

The screenshot shows the Wireshark interface with an applied "http" filter. The packet list pane shows several HTTP requests, including GET /success.txt and /favicon.ico. The details pane shows the request headers and the response content, and the bytes pane shows the raw hex and ASCII data for one of the requests.

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

dns

No.	Time	Source	Destination	Protocol	Length	Info
34	72.848463	10.0.2.3	10.0.2.15	DNS	183	Standard query response 0x4e9e AAAA example.org AAAA 2600:1408:ec00:36::1736:7f2e AAA
35	72.848464	10.0.2.3	10.0.2.15	DNS	105	Standard query response 0x06d3 A ipv4only.arpa A 192.0.0.171 A 192.0.0.170
36	72.848464	10.0.2.3	10.0.2.15	DNS	130	Standard query response 0x05d2 AAAA ipv4only.arpa SOA sns.dns.icann.org
37	72.850371	10.0.2.15	10.0.2.3	DNS	84	Standard query 0xc037 A detectportal.firefox.com
38	72.850393	10.0.2.15	10.0.2.3	DNS	84	Standard query 0x443e AAAA detectportal.firefox.com
39	72.856752	10.0.2.3	10.0.2.15	DNS	195	Standard query response 0x33b1 A detectportal.firefox.com CNAME detectportal.prod.moz
41	72.856723	10.0.2.3	10.0.2.15	DNS	195	Standard query response 0xc037 A detectportal.firefox.com CNAME detectportal.prod.moz
42	72.862118	10.0.2.3	10.0.2.15	DNS	207	Standard query response 0x4436 AAAA detectportal.firefox.com CNAME detectportal.prod.
53	73.622953	10.0.2.15	10.0.2.3	DNS	88	Standard query 0x97b5 A contile.services.mozilla.com
54	73.622969	10.0.2.15	10.0.2.3	DNS	88	Standard query 0x74b4 AAAA contile.services.mozilla.com
55	73.624789	10.0.2.15	10.0.2.3	DNS	79	Standard query 0xb5b9 A spocs.getpocket.com
56	73.624800	10.0.2.15	10.0.2.3	DNS	79	Standard query 0x359b AAAA spocs.getpocket.com
57	73.636951	10.0.2.3	10.0.2.15	DNS	104	Standard query response 0x97b5 A contile.services.mozilla.com A 34.36.137.203
58	73.637973	10.0.2.3	10.0.2.15	DNS	168	Standard query response 0x74b4 AAAA contile.services.mozilla.com SOA ns-679.awsdns-26
59	73.638817	10.0.2.3	10.0.2.15	DNS	148	Standard query response 0xb5b9 A spocs.getpocket.com CNAME mdc.prod.ads.prod.webservic

```

Frame 42: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits)
Ethernet II, Src: PCSSystemtec_d1:f8:s5 (52:55:0a:00:02:02), Dst: PCSSystemtec_d1:f8:s5 (52:55:0a:00:02:02)
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 54738
Domain Name System (response)

0000 08 00 27 d1 f8 5d 52 55 0a 00 02 02 08 00 45 00 ... ]RU ..... E.
0010 00 c1 4c b3 00 00 40 11 15 68 00 00 02 03 00 00 ..L..@.h.....
0020 02 0f 00 35 d5 d2 00 ad e6 1d 44 36 81 80 00 01 ... 5 ... .D6...
0030 00 03 00 00 00 00 0c 64 05 74 65 63 74 70 6f 72 ..... fd detectpor
0040 74 61 6c 07 66 69 72 65 56 6f 78 03 63 6f 6d 00 tal.fire fox.com.
0050 00 1c 00 01 c0 0c 00 05 00 01 00 00 00 02 00 1e
0060 0c 64 65 74 65 63 74 70 6f 72 74 61 6c 04 70 72 detectp ortal.pr
0070 0f 64 66 6d 0f 7a 61 77 73 03 66 65 74 00 c0 36 od mozaw s.net -6
0080 00 05 00 01 00 00 00 01 e0 00 29 04 70 72 6f 64 0c ..... ) prod.
0090 64 65 74 65 63 74 70 6f 72 74 61 6c 04 70 72 6f detectpo ral pro
00a0 00 08 63 6c 0f 75 64 6f 70 73 06 6d 0f 7a 67 63 d cloudo ps mozgc
00b0 70 c0 4f c0 00 00 01 00 00 00 37 00 10 26 p 0... .7 &
00c0 00 19 01 00 00 38 d7 00 00 00 00 00 00 00 00 00 ..8 .....
```

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

icmp

No.	icmpv6	Source	Destination	Protocol	Length	Info
21	164638	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=1/256, ttl=64 (no response found!)
2935	973.187689	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=2/512, ttl=64 (no response found!)
2936	974.211854	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=3/768, ttl=64 (no response found!)
2937	975.235827	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024, ttl=64 (no response found!)
2938	976.259284	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=5/1280, ttl=64 (no response found!)
2941	977.283279	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=6/1536, ttl=64 (no response found!)
2942	978.307324	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=7/1792, ttl=64 (no response found!)
2955	979.331496	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=8/2048, ttl=64 (no response found!)
2959	980.355261	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=9/2304, ttl=64 (no response found!)
2960	981.379745	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=10/2560, ttl=64 (no response found!)
2961	982.403157	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=11/2816, ttl=64 (no response found!)
2962	983.427789	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=12/3072, ttl=64 (no response found!)
2965	984.451431	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=13/3328, ttl=64 (no response found!)
2966	985.475946	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=14/3584, ttl=64 (no response found!)
2967	986.499247	10.0.2.15	198.51.100.5	ICMP	98	Echo (ping) request id=0x0004, seq=15/3840, ttl=64 (no response found!)

```

Frame 2934: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: PCSSystemtec_d1:f8:s5 (52:55:0a:00:02:02), Dst: 52:55:0a:00:02:02
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 198.51.100.5
Internet Control Message Protocol
0000 52 55 0a 00 02 02 08 00 27 d1 f8 5d 08 00 45 00 RU...[.]E.
0010 00 54 cd 46 40 00 40 01 37 1b 0a 00 02 0f c6 33 T.F@.0.7..3
0020 04 05 08 00 86 41 00 04 00 01 27 08 9a 68 00 00 d...A...h...
0030 00 00 f1 75 00 00 00 00 00 00 00 10 11 12 13 14 15 ..u..
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ...!#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67

Frame 2934: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: PCSSystemtec_d1:f8:s5 (52:55:0a:00:02:02), Dst: 52:55:0a:00:02:02
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 198.51.100.5
Internet Control Message Protocol
0000 52 55 0a 00 02 02 08 00 27 d1 f8 5d 08 00 45 00 RU...[.]E.
0010 00 54 cd 46 40 00 40 01 37 1b 0a 00 02 0f c6 33 T.F@.0.7..3
0020 04 05 08 00 86 41 00 04 00 01 27 08 9a 68 00 00 d...A...h...
0030 00 00 f1 75 00 00 00 00 00 00 00 10 11 12 13 14 15 ..u..
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ...!#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67
```

## Applying “tcp.port==8080” Filter:

tcp.port==8080

No.	Time	Source	Destination	Protocol	Length	Info
3628	1140.155458	10.0.2.15	45.33.32.156	TCP	74	47148 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=2593930641 TSecr=0 WS=...
3629	1141.187306	10.0.2.15	45.33.32.156	TCP	74	[TCP Retransmission] 47148 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=2...
3630	1142.211610	10.0.2.15	45.33.32.156	TCP	74	[TCP Retransmission] 47148 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=2...
3631	1143.145571	45.33.32.156	10.0.2.15	TCP	60	8080 → 47148 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0

Applying "tcp.flags.syn==1 && tcp.flags.ack==0"

filter:

No.	Time	Source	Destination	Protocol	Length	Info
2601	277.918677	10.0.2.15	23.192.228.84	TCP	74	53736 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3323444563 TSecr=0 WS
2602	278.083337	10.0.2.15	34.223.124.45	TCP	74	[TCP Retransmission] 44908 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=
2606	278.175428	10.0.2.15	23.192.228.84	TCP	74	53752 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3323444620 TSecr=0 WS
2610	278.498044	10.0.2.15	23.192.228.84	TCP	74	53764 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3323445142 TSecr=0 WS
2612	278.674044	10.0.2.15	23.192.228.84	TCP	74	53774 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3323445318 TSecr=0 WS
2618	278.880758	10.0.2.15	23.192.228.84	TCP	74	53786 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=3323445525 TSecr=0 WS
2621	280.643476	10.0.2.15	34.223.124.45	TCP	74	[TCP Retransmission] 44926 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=
2658	286.275899	10.0.2.15	34.223.124.45	TCP	74	[TCP Retransmission] 44908 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=
2658	288.835582	10.0.2.15	34.223.124.45	TCP	74	[TCP Retransmission] 44926 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=
2666	292.918066	fd17:625c:f037:2:e7... 2600:1f13:37c:1400:...	TCP	94	43638 - 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TStamp=2669611468 TSecr=0 WS	
2798	478.191876	10.0.2.15	34.149.100.209	TCP	74	36362 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=920966745 TSecr=0 WS
2841	478.463740	10.0.2.15	34.160.144.191	TCP	74	47756 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=281949227 TSecr=0 WS
3028	1146.155458	10.0.2.15	45.33.32.156	TCP	74	47148 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=2593936641 TSecr=0
3029	1141.187306	10.0.2.15	45.33.32.156	TCP	74	[TCP Retransmission] 47148 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=
3030	1142.211610	10.0.2.15	45.33.32.156	TCP	74	[TCP Retransmission] 47148 - 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=

> Frame 3028: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)  
> Ethernet II, Src: PCSsystemtec\_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:55:0a:00:02:06  
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 45.33.32.156  
> Transmission Control Protocol, Src Port: 47148, Dst Port: 8080, Seq: 0, Len: 0

0000 52 55 0a 00 02 02 08 00 27 d1 f8 5d 08 00 45 00 RU . . . . E  
0010 00 3c d8 ee 40 00 40 06 08 02 0a 00 02 0f 2d 21 < . . . !  
0020 20 9c b8 2c 1f 90 ea 8d 41 c8 00 00 00 00 a0 02 . , . A  
0030 fa f8 59 fa 00 00 02 04 05 b4 04 02 08 0a 9a 9c . Y  
0040 3d 91 00 00 00 00 01 03 03 07 = . . .

## 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.

