Name: Temidayo, Oluwarantimi Blessing

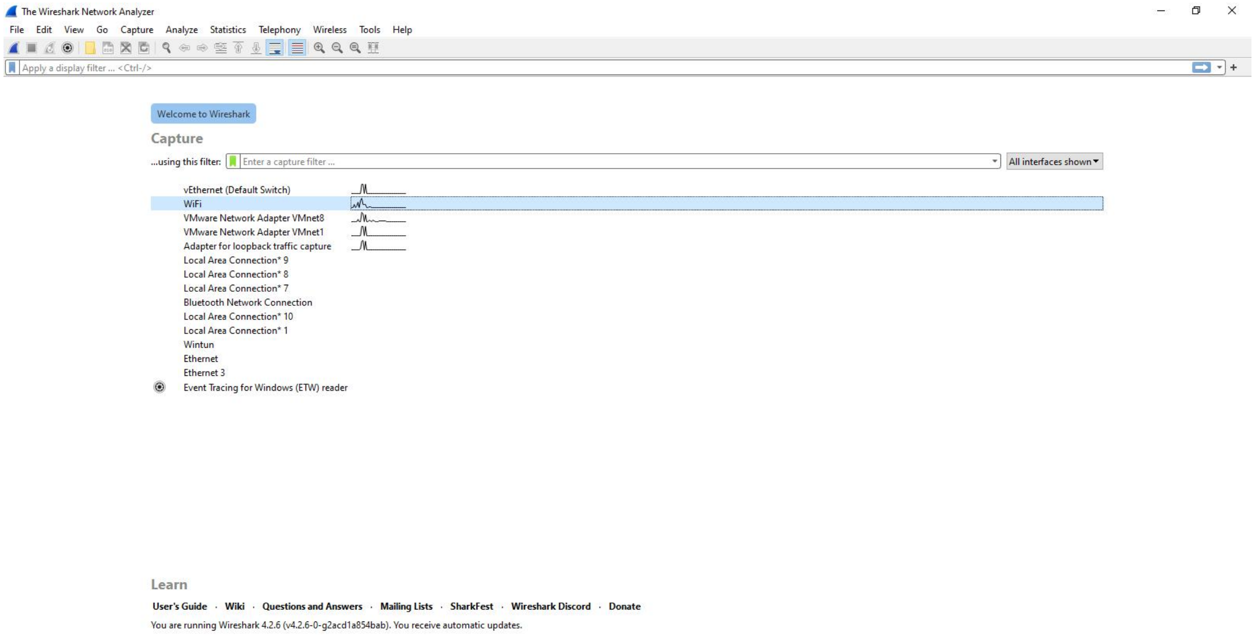
Student ID: IDEAS/24/51291

Week 2: Exploitation, Web Application Testing, and Advanced Networking

INT302: Kali Linux Tools and System Security – Lab 7: Practical Use Cases for Wireshark in Real-World

Exercise 1: Describe the overall network traffic during the incident. Are there any noticeable spikes or anomalies? What potential indicators of compromise did you identify?

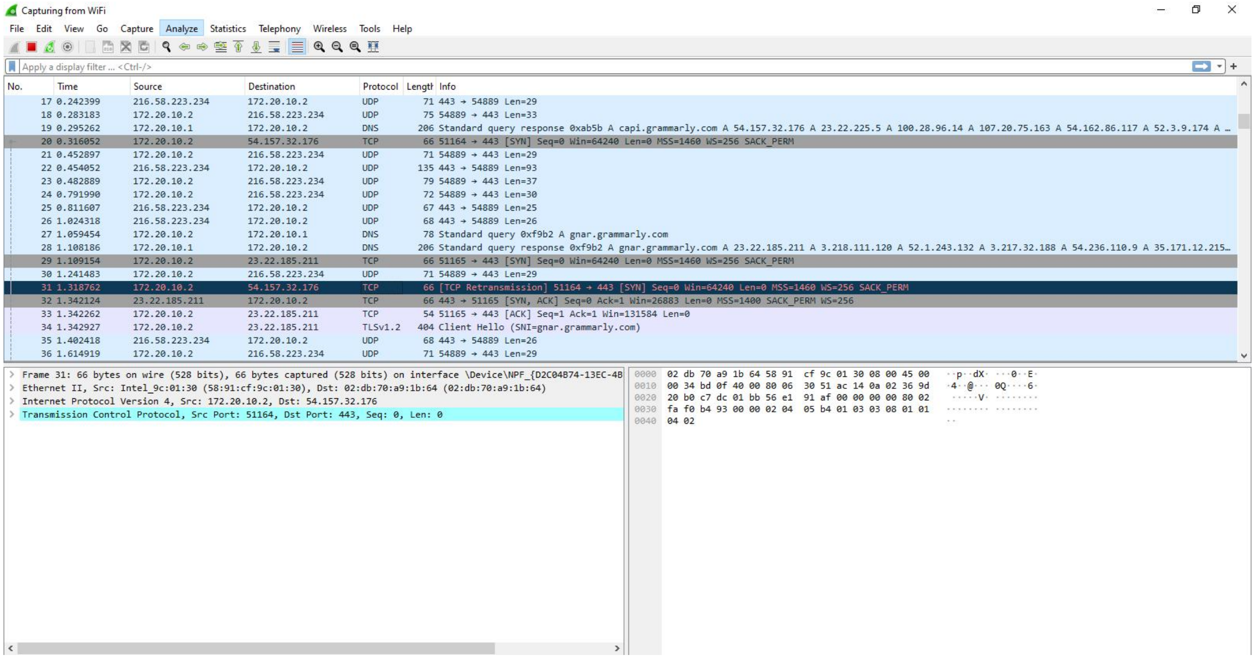
Using Wireshark helps to easily capture packets and network traffic. My analysis is stated below:


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

vEthernet (Default Switch)
WiFi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Adapter for loopback traffic capture
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 1
Wintun
Ethernet
Ethernet 3
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.2.6 (v4.2.6-0-g2acd1a854bab). You receive automatic updates.

In the above diagram, we can see that different interfaces can be captured. I chose to capture the one WiFi interface. The wave means it is actively capturing traffic.

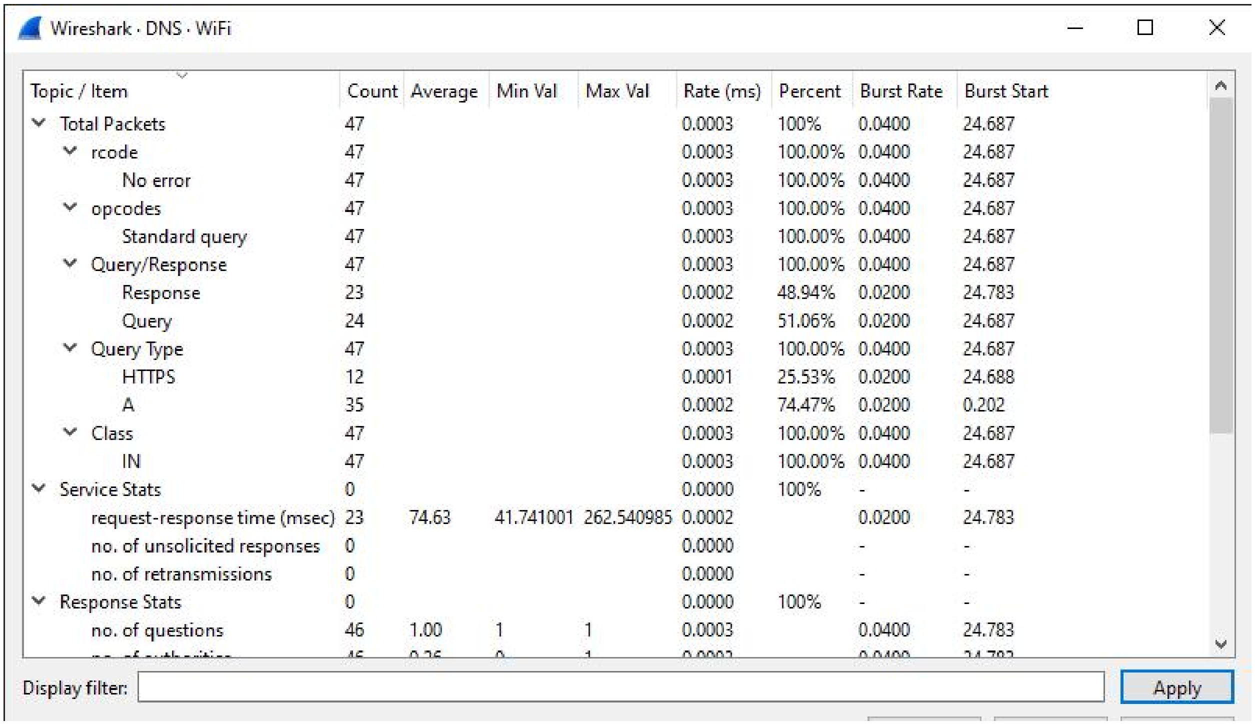

Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time      Source          Destination     Protocol Length Info
    17 0.242399  216.58.223.234  172.20.10.2     UDP       71 443 → 54889 Len=29
    18 0.283183  172.20.10.2     216.58.223.234  UDP       75 54889 → 443 Len=33
    19 0.295262  172.20.10.1     172.20.10.2     DNS      206 Standard query response 0xab5b A capi.grammarly.com A 54.157.32.176 A 23.22.225.5 A 100.28.96.14 A 107.20.75.163 A 54.162.86.117 A 52.3.9.174 A …
    20 0.316052  172.20.10.2     54.157.32.176   TCP       66 51164 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    21 0.452897  172.20.10.2     216.58.223.234  UDP       71 54889 → 443 Len=29
    22 0.454052  216.58.223.234  172.20.10.2     UDP      135 443 → 54889 Len=93
    23 0.482889  172.20.10.2     216.58.223.234  UDP       79 54889 → 443 Len=37
    24 0.791990  172.20.10.2     216.58.223.234  UDP       72 54889 → 443 Len=30
    25 0.811607  216.58.223.234  172.20.10.2     UDP       67 443 → 54889 Len=25
    26 1.024318  216.58.223.234  172.20.10.2     UDP       68 443 → 54889 Len=26
    27 1.059454  172.20.10.2     172.20.10.1     DNS       78 Standard query 0xf9b2 A gnar.grammarly.com
    28 1.108186  172.20.10.1     172.20.10.2     DNS      206 Standard query response 0xf9b2 A gnar.grammarly.com A 23.22.185.211 A 3.218.111.120 A 52.1.243.132 A 3.217.32.188 A 54.236.110.9 A 35.171.12.215…
    29 1.109154  172.20.10.2     23.22.185.211   TCP       66 51165 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    30 1.241483  172.20.10.2     216.58.223.234  UDP       71 54889 → 443 Len=29
    31 1.318762  172.20.10.2     54.157.32.176   TCP       66 [TCP Retransmission] 51164 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    32 1.342124  23.22.185.211   172.20.10.2     TCP       66 443 → 51165 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1400 SACK_PERM WS=256
    33 1.342262  172.20.10.2     23.22.185.211   TCP       54 51165 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
    34 1.342927  172.20.10.2     23.22.185.211   TLSv1.2  404 Client Hello (SNI=gnar.grammarly.com)
    35 1.402418  216.58.223.234  172.20.10.2     UDP       68 443 → 54889 Len=26
    36 1.614919  172.20.10.2     216.58.223.234  UDP       71 54889 → 443 Len=29
```

```
> Frame 31: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D2C04B74-13EC-4B
> Ethernet II, Src: Intel_9c:01:30 (58:91:cf:9c:01:30), Dst: 02:db:70:a9:1b:64 (02:db:70:a9:1b:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 54.157.32.176
> Transmission Control Protocol, Src Port: 51164, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  02 db 70 a9 1b 64 58 91  cf 9c 01 30 08 00 45 00   ··p··dX· ···0··E·
0010  00 34 bd 0f 40 00 80 06  30 51 ac 14 0a 02 36 9d   ·4··@··· 0Q····6·
0020  20 b0 c7 dc 01 bb 56 e1  91 af 00 00 00 00 80 02    ·····V· ········
0030  fa f0 b4 93 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Diagram of different packets being captured. The red indicator can mean an **error** or **issues** with the packet. Often this is used to indicate **error messages**, failed connections, or other abnormal network conditions.

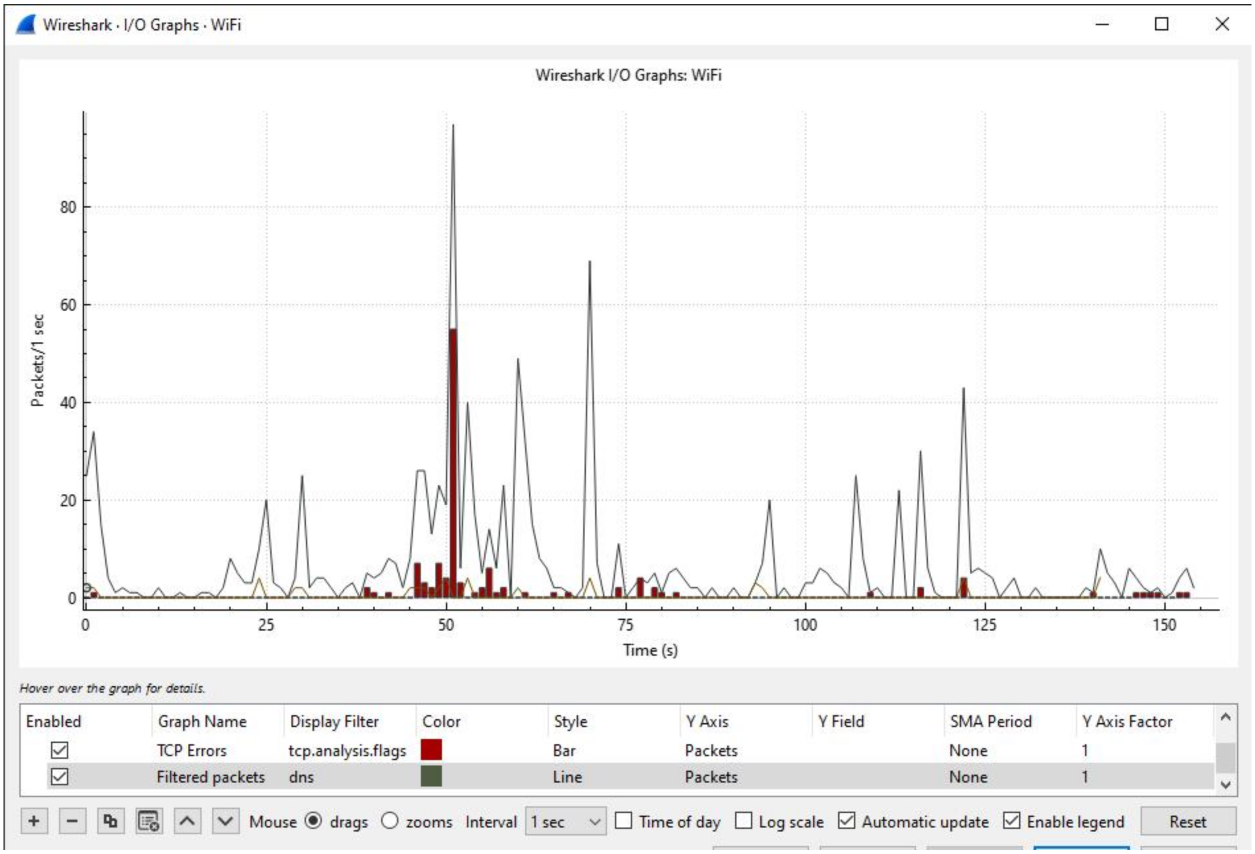


Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	47				0.0003	100%	0.0400	24.687
rcode	47				0.0003	100.00%	0.0400	24.687
No error	47				0.0003	100.00%	0.0400	24.687
opcodes	47				0.0003	100.00%	0.0400	24.687
Standard query	47				0.0003	100.00%	0.0400	24.687
Query/Response	47				0.0003	100.00%	0.0400	24.687
Response	23				0.0002	48.94%	0.0200	24.783
Query	24				0.0002	51.06%	0.0200	24.687
Query Type	47				0.0003	100.00%	0.0400	24.687
HTTPS	12				0.0001	25.53%	0.0200	24.688
A	35				0.0002	74.47%	0.0200	0.202
Class	47				0.0003	100.00%	0.0400	24.687
IN	47				0.0003	100.00%	0.0400	24.687
Service Stats	0				0.0000	100%	-	-
request-response time (msec)	23	74.63	41.741001	262.540985	0.0002		0.0200	24.783
no. of unsolicited responses	0				0.0000		-	-
no. of retransmissions	0				0.0000		-	-
Response Stats	0				0.0000	100%	-	-
no. of questions	46	1.00	1	1	0.0003		0.0400	24.783
no. of authorities	46	0.26	0	1	0.0003		0.0400	24.783

A DNS rate of **0.0003 to 0.0001 pps** is **very low,** in my case, this is due to working in a small environment with minimal DNS usage.

In other cases, it may be due to Long Periods Between Captures, Short Sampling Window, Low DNS traffic, and Limited Network Activity.

A time to be concerned is if you're expecting DNS traffic and its rate is unusually low.

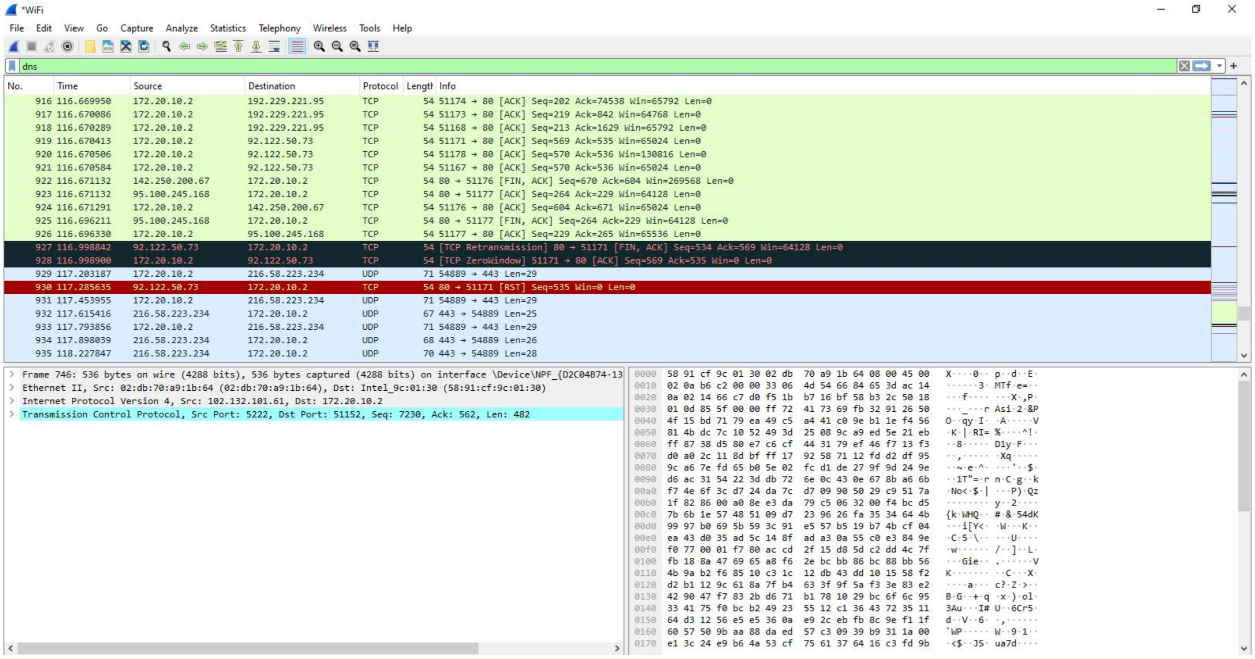


Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None	1
☑	Filtered packets	dns	🟩	Line	Packets		None	1

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ☑ Automatic update ☑ Enable legend

The diagram above shows how the packets evolve over time. The **green** is for normal traffic, and the **red** is for abnormal spikes. Abnormal spikes may mean a burst of network activity (e.g., a file transfer, large web requests, or DDoS attacks), potential network problems such as congestion or a pattern of **sustained high traffic**, which might be normal during business hours, or an event like a system update.

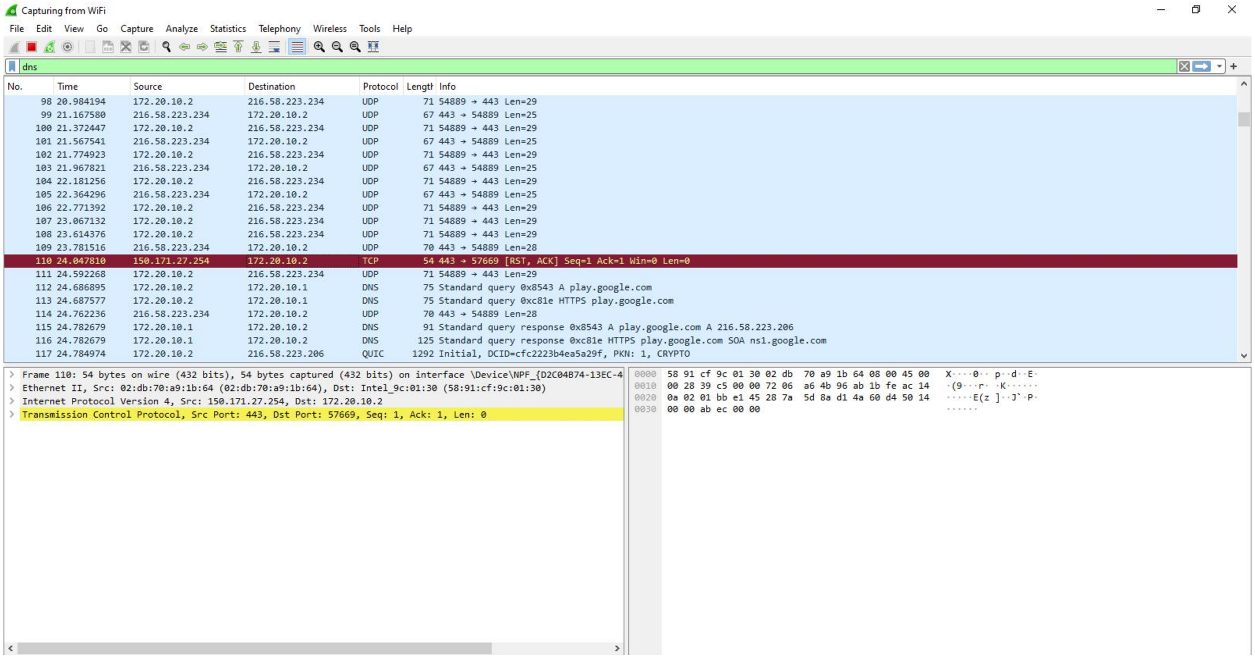

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.     Time        Source          Destination     Protocol Length Info
    916 116.669950  172.20.10.2     192.229.221.95  TCP      54 51174 → 80 [ACK] Seq=202 Ack=74538 Win=65792 Len=0
    917 116.670086  172.20.10.2     192.229.221.95  TCP      54 51173 → 80 [ACK] Seq=219 Ack=842 Win=64768 Len=0
    918 116.670289  172.20.10.2     192.229.221.95  TCP      54 51168 → 80 [ACK] Seq=213 Ack=1629 Win=65792 Len=0
    919 116.670413  172.20.10.2     92.122.50.73    TCP      54 51171 → 80 [ACK] Seq=569 Ack=535 Win=65024 Len=0
    920 116.670506  172.20.10.2     92.122.50.73    TCP      54 51178 → 80 [ACK] Seq=570 Ack=536 Win=130816 Len=0
    921 116.670584  172.20.10.2     92.122.50.73    TCP      54 51167 → 80 [ACK] Seq=570 Ack=536 Win=65024 Len=0
    922 116.671132  142.250.200.67  172.20.10.2     TCP      54 80 → 51176 [FIN, ACK] Seq=670 Ack=604 Win=269568 Len=0
    923 116.671132  95.100.245.168  172.20.10.2     TCP      54 80 → 51177 [ACK] Seq=264 Ack=229 Win=64128 Len=0
    924 116.671291  172.20.10.2     142.250.200.67  TCP      54 51176 → 80 [ACK] Seq=604 Ack=671 Win=65024 Len=0
    925 116.696211  95.100.245.168  172.20.10.2     TCP      54 80 → 51177 [FIN, ACK] Seq=264 Ack=229 Win=64128 Len=0
    926 116.696330  172.20.10.2     95.100.245.168  TCP      54 51177 → 80 [ACK] Seq=229 Ack=265 Win=65536 Len=0
    927 116.998842  92.122.50.73    172.20.10.2     TCP      54 [TCP Retransmission] 80 → 51171 [FIN, ACK] Seq=534 Ack=569 Win=64128 Len=0
    928 116.998900  172.20.10.2     92.122.50.73    TCP      54 [TCP ZeroWindow] 51171 → 80 [ACK] Seq=569 Ack=535 Win=0 Len=0
    929 117.203187  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    930 117.285635  92.122.50.73    172.20.10.2     TCP      54 80 → 51171 [RST] Seq=535 Win=0 Len=0
    931 117.453955  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    932 117.615416  216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
    933 117.793856  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    934 117.898039  216.58.223.234  172.20.10.2     UDP      68 443 → 54889 Len=26
    935 118.227847  216.58.223.234  172.20.10.2     UDP      70 443 → 54889 Len=28
```

```
> Frame 746: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{D2C04B74-13
> Ethernet II, Src: 02:db:70:a9:1b:64 (02:db:70:a9:1b:64), Dst: Intel_9c:01:30 (58:91:cf:9c:01:30)
> Internet Protocol Version 4, Src: 102.132.101.61, Dst: 172.20.10.2
> Transmission Control Protocol, Src Port: 5222, Dst Port: 51152, Seq: 7230, Ack: 562, Len: 482
```

```
0000  58 91 cf 9c 01 30 02 db  70 a9 1b 64 08 00 45 00   X····0·· p··d··E·
0010  02 0a b6 c2 00 00 33 06  4d 54 66 84 65 3d ac 14   ······3· MTf·e=··
0020  0a 02 14 66 c7 d0 f5 1b  b7 16 bf 58 b3 2c 50 18   ···f···· ···X·,P·
0030  01 0d 85 5f 00 00 ff 72  41 73 69 fb 32 91 26 50   ···_···r Asi·2·&P
0040  4f 15 bd 71 79 ea 49 c5  a4 41 c0 9e b1 1e f4 56   O··qy·I· ·A·····V
0050  81 4b dc 7c 10 52 49 3d  25 08 9c a9 ed 5e 21 eb   ·K·|·RI= %····^!·
0060  ff 87 38 d5 80 e7 c6 cf  44 31 79 ef 46 f7 13 f3   ··8····· D1y·F···
0070  d0 a0 2c 11 8d bf ff 17  92 58 71 12 fd d2 df 95   ··,····· ·Xq·····
0080  9c a6 7e fd 65 b0 5e 02  fc d1 de 27 9f 9d 24 9e   ··~·e·^· ···'··$·
0090  d6 ac 31 54 22 3d db 72  6e 0c 43 0e 67 8b a6 6b   ··1T"=·r n·C·g··k
00a0  f7 4e 6f 3c d7 24 da 7c  d7 09 90 50 29 c9 51 7a   ·No<·$·| ···P)·Qz
00b0  1f 82 86 00 a0 8e e3 da  79 c5 06 32 00 f4 bc d5   ········ y··2····
00c0  7b 6b 1e 57 48 51 09 d7  23 96 26 fa 35 34 64 4b   {k·WHQ·· #·&·54dK
00d0  99 97 b0 69 5b 59 3c 91  e5 57 b5 19 b7 4b cf 04   ···i[Y<· ·W···K··
00e0  ea 43 d0 35 ad 5c 14 8f  ad a3 0a 55 c0 e3 84 9e   ·C·5·\·· ···U····
00f0  f0 77 00 01 f7 80 ac cd  2f 15 d8 5d c2 dd 4c 7f   ·w······ /··]··L·
0100  fb 18 8a 47 69 65 a8 f6  2e bc bb 86 bc 88 bb 56   ···Gie·· .······V
0110  4b 9a b2 f6 85 10 c3 1c  12 db 43 dd 10 15 58 f2   K······· ··C···X·
0120  d2 b1 12 9c 61 8a 7f b4  63 3f 9f 5a f3 3e 83 e2   ····a··· c?·Z·>··
0130  42 90 47 f7 83 2b d6 71  b1 78 10 29 bc 6f 6c 95   B·G··+·q ·x·)·ol·
0140  33 41 75 f0 bc b2 49 23  55 12 c1 36 43 72 35 11   3Au···I# U··6Cr5·
0150  64 d3 12 56 e5 e5 36 0a  e9 2c eb fb 8c 9e f1 1f   d··V··6· ·,······
0160  60 57 50 9b aa 88 da ed  57 c3 09 39 b9 31 1a 00   `WP····· W··9·1··
0170  e1 3c 24 e9 b6 4a 53 cf  75 61 37 64 16 c3 fd 9b   ·<$··JS· ua7d····
```

In the diagram above, different colours are displayed. The **green colour** indicates normal successful packets, the **black** indicates a warning, unusual traffic, or retransmissions, the **red** indicates error or failure packets, and the **light blue** indicates normal, ongoing TCP conversation packets.


Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

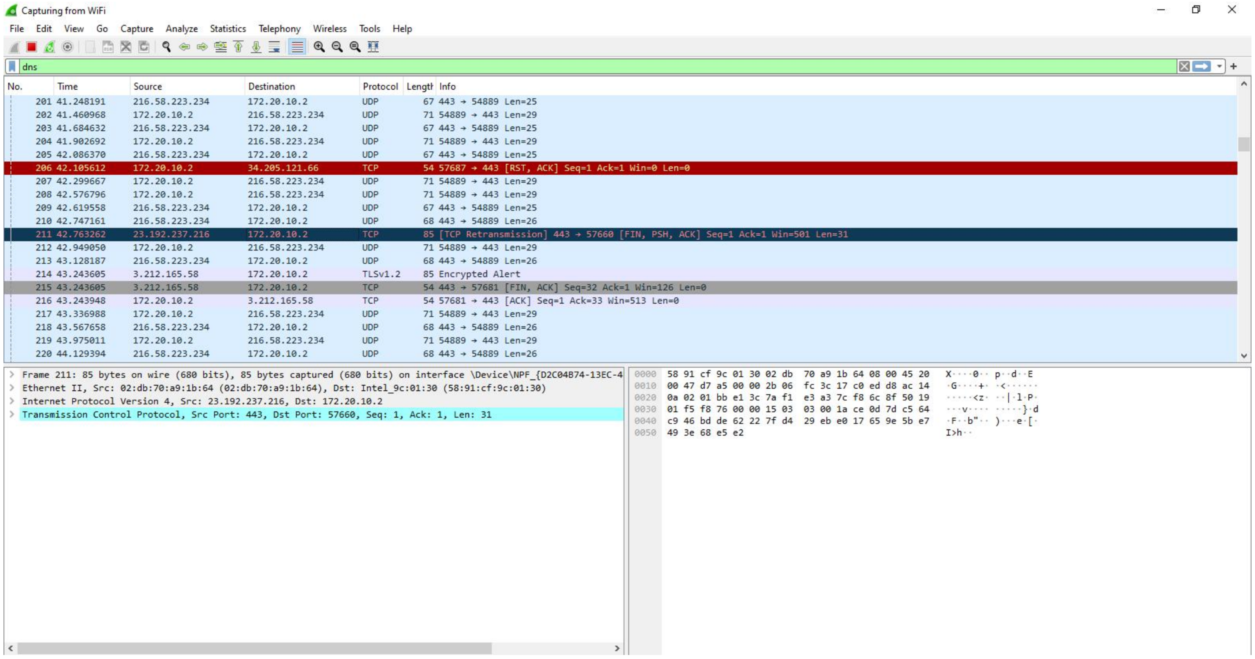
```
No.     Time        Source          Destination     Protocol Length Info
     98 20.984194   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
     99 21.167580   216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
    100 21.372447   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    101 21.567541   216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
    102 21.774923   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    103 21.967821   216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
    104 22.181256   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    105 22.364296   216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
    106 22.771392   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    107 23.067132   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    108 23.614376   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    109 23.781516   216.58.223.234  172.20.10.2     UDP      70 443 → 54889 Len=28
    110 24.047810   150.171.27.254  172.20.10.2     TCP      54 443 → 57669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    111 24.592268   172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
    112 24.686895   172.20.10.2     172.20.10.1     DNS      75 Standard query 0x8543 A play.google.com
    113 24.687577   172.20.10.2     172.20.10.1     DNS      75 Standard query 0xc81e HTTPS play.google.com
    114 24.762236   216.58.223.234  172.20.10.2     UDP      70 443 → 54889 Len=28
    115 24.782679   172.20.10.1     172.20.10.2     DNS      91 Standard query response 0x8543 A play.google.com A 216.58.223.206
    116 24.782679   172.20.10.1     172.20.10.2     DNS     125 Standard query response 0xc81e HTTPS play.google.com SOA ns1.google.com
    117 24.784974   172.20.10.2     216.58.223.206  QUIC   1292 Initial, DCID=cfc2223b4ea5a29f, PKN: 1, CRYPTO
```

```
> Frame 110: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{D2C04B74-13EC-4
> Ethernet II, Src: 02:db:70:a9:1b:64 (02:db:70:a9:1b:64), Dst: Intel_9c:01:30 (58:91:cf:9c:01:30)
> Internet Protocol Version 4, Src: 150.171.27.254, Dst: 172.20.10.2
> Transmission Control Protocol, Src Port: 443, Dst Port: 57669, Seq: 1, Ack: 1, Len: 0
```

```
0000  58 91 cf 9c 01 30 02 db  70 a9 1b 64 08 00 45 00   X····0·· p··d··E·
0010  00 28 39 c5 00 00 72 06  a6 4b 96 ab 1b fe ac 14   ·(9···r· ·K······
0020  0a 02 01 bb e1 45 28 7a  5d 8a d1 4a 60 d4 50 14   ·····E(z ]··J`·P·
0030  00 00 ab ec 00 00                                  ······
```

The information on the yellow colour: Src port **443** is the well-known port for **HTTPS (Hypertext Transfer Protocol Secure)**. **Seq 1** means this is the first packet in the sequence of data transmitted between the two devices. The **ACK 1** number is used to confirm the successful receipt of data. **Len 0** indicates that the packet carries no data but is likely being used for ACK.

Exercise 2: Identify a specific packet that raises suspicion. Provide details about the packet, including source and destination IPs, ports, and protocol. What makes this packet suspicious?



```
No.   Time       Source          Destination     Protocol Length Info
  201 41.248191  216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
  202 41.460968  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
  203 41.684632  216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
  204 41.902692  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
  205 42.086370  216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
  206 42.105612  172.20.10.2     34.205.121.66   TCP      54 57687 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  207 42.299667  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
  208 42.576796  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
  209 42.619558  216.58.223.234  172.20.10.2     UDP      67 443 → 54889 Len=25
  210 42.747161  216.58.223.234  172.20.10.2     UDP      68 443 → 54889 Len=26
  211 42.763262  23.192.237.216  172.20.10.2     TCP      85 [TCP Retransmission] 443 → 57660 [FIN, PSH, ACK] Seq=1 Ack=1 Win=501 Len=31
  212 42.949050  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
  213 43.128187  216.58.223.234  172.20.10.2     UDP      68 443 → 54889 Len=26
  214 43.243605  3.212.165.58    172.20.10.2     TLSv1.2  85 Encrypted Alert
  215 43.243605  3.212.165.58    172.20.10.2     TCP      54 443 → 57681 [FIN, ACK] Seq=32 Ack=1 Win=126 Len=0
  216 43.243948  172.20.10.2     3.212.165.58    TCP      54 57681 → 443 [ACK] Seq=1 Ack=33 Win=513 Len=0
  217 43.336988  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
  218 43.567658  216.58.223.234  172.20.10.2     UDP      68 443 → 54889 Len=26
  219 43.975011  172.20.10.2     216.58.223.234  UDP      71 54889 → 443 Len=29
  220 44.129394  216.58.223.234  172.20.10.2     UDP      68 443 → 54889 Len=26

> Frame 211: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{D2C04B74-13EC-4
> Ethernet II, Src: 02:db:70:a9:1b:64 (02:db:70:a9:1b:64), Dst: Intel_9c:01:30 (58:91:cf:9c:01:30)
> Internet Protocol Version 4, Src: 23.192.237.216, Dst: 172.20.10.2
> Transmission Control Protocol, Src Port: 443, Dst Port: 57660, Seq: 1, Ack: 1, Len: 31

0000  58 91 cf 9c 01 30 02 db  70 a9 1b 64 08 00 45 20   X····0·· p··d··E
0010  00 47 d7 a5 00 00 2b 06  fc 3c 17 c0 ed d8 ac 14   ·G····+· ·<······
0020  0a 02 01 bb e1 3c 7a f1  e3 a3 7c f8 6c 8f 50 19   ·····<z· ··|·l·P·
0030  01 f5 f8 76 00 00 15 03  03 00 1a ce 0d 7d c5 64   ···v···· ·····}·d
0040  c9 46 bd de 62 22 7f d4  29 eb e0 17 65 9e 5b e7   ·F··b"·· )···e·[·
0050  49 3e 68 e5 e2                                     I>h··
```

The packet shows no suspicious activity per se but for study purpose, I'll explain a few activity that may occur.

- **Source Port (src)**: 443 (HTTPS)
- **Destination Port (dst)**: 57660 (a high, ephemeral port)
- **Sequence Number (Seq)**: 1
- **Acknowledgment Number (Ack)**: 1
- **Length (len)**: 31 bytes of data

What Can Be Inferred From This Packet?

Let's break it down based on the information you provided:

1. **Source Port: 443 (HTTPS)**: Port 443 is commonly used for **HTTPS** traffic (secure web traffic). This means typically a secure website or API.

   If this is coming from an internal server, it's usually fine as it's a standard web protocol. However, if it's coming from an unfamiliar or external server, it could be suspicious.

2. **Destination Port: 57660**: Port 57660 is a **high-numbered ephemeral port** (often used for dynamic or temporary connections).

   This suggests that the packet is part of an **outbound** connection, where the internal system is acting as the client and is establishing a connection to an external service or server. The high port number suggests it's dynamically allocated by the operating system for a client-side connection.

   If this connection is going to an unknown or suspicious IP address, it could indicate **malicious activity**, like a botnet command-and-control (C2) server, or **data exfiltration** using unusual ports.

3. **Sequence Number: 1** and **Acknowledgment Number: 1**: The **sequence number** and **acknowledgment number** are both set to 1, which is typical for the **initial handshake** of a TCP connection.

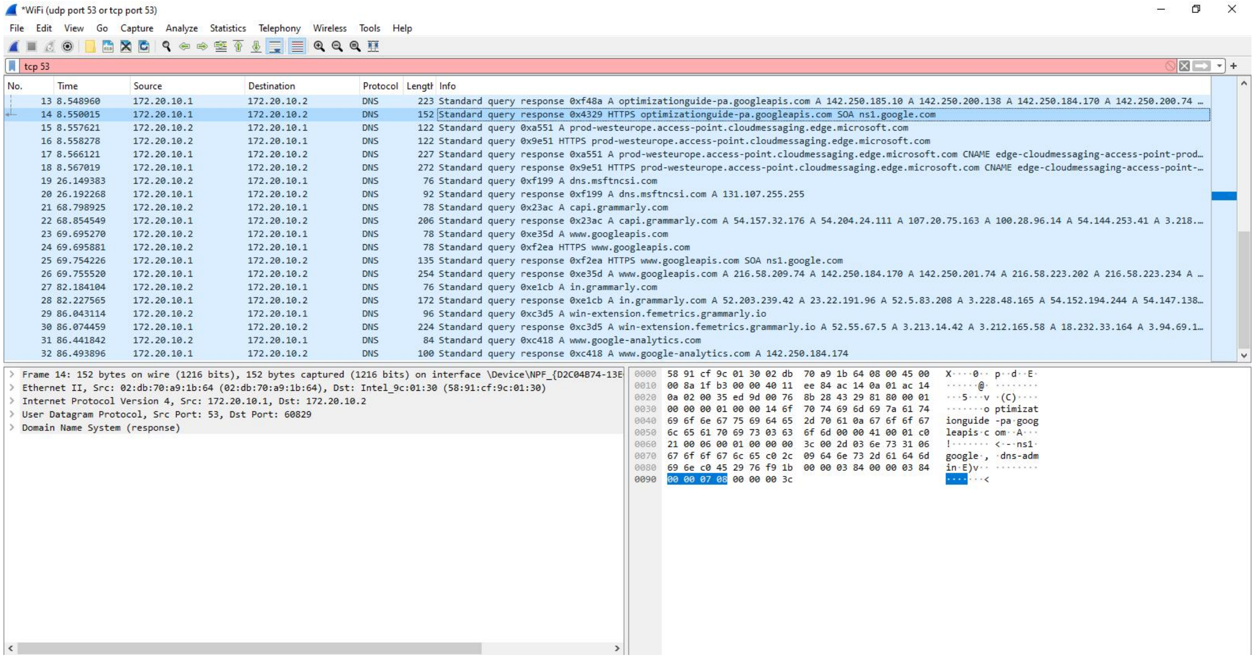
4. **Length: 31 bytes**: The packet length of 31 bytes is relatively small but might still carry meaningful data. For example, if it's part of an HTTP request (even over HTTPS), it could be a **malicious payload** or command being passed along the network.

Potential Suspicious Indicators:

1. **Unusual Communication Pattern**: Combination of port 443 (HTTPS) with a high-numbered ephemeral port (57660) might suggest that this is an application trying to disguise or obfuscate its traffic (for example, **malware** using HTTPS to hide its communication or **data exfiltration** using web protocols).

2. **Encrypted Traffic**: Since this is using **HTTPS (port 443)**, the traffic would be **encrypted**. This packet is from a known, trusted server, so there's nothing inherently suspicious here. However, if the source IP is unfamiliar, or if this is occurring with large volumes of traffic, this could point to **malicious tunneling** or **command-and-control communication**.

Exercise 3: Implement a capture filter to monitor DNS traffic. Analyze the captured packets and summarize any findings related to unusual queries or connections.



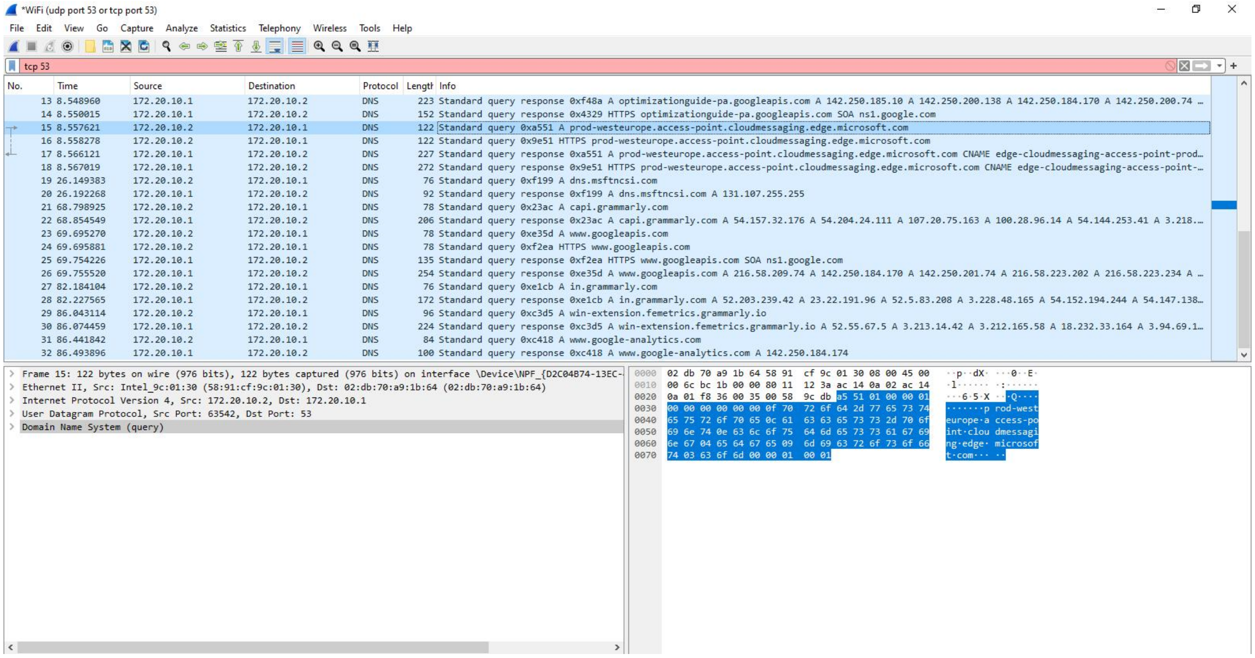
*WiFi (udp port 53 or tcp port 53)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp 53
```

```
No.  Time       Source       Destination  Protocol Length Info
  13 8.548960   172.20.10.1  172.20.10.2  DNS      223 Standard query response 0xf48a A optimizationguide-pa.googleapis.com A 142.250.185.10 A 142.250.200.138 A 142.250.184.170 A 142.250.200.74 …
  14 8.550015   172.20.10.1  172.20.10.2  DNS      152 Standard query response 0x4329 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
  15 8.557621   172.20.10.2  172.20.10.1  DNS      122 Standard query 0xa551 A prod-westeurope.access-point.cloudmessaging.edge.microsoft.com
  16 8.558278   172.20.10.2  172.20.10.1  DNS      122 Standard query 0x9e51 HTTPS prod-westeurope.access-point.cloudmessaging.edge.microsoft.com
  17 8.566121   172.20.10.1  172.20.10.2  DNS      227 Standard query response 0xa551 A prod-westeurope.access-point.cloudmessaging.edge.microsoft.com CNAME edge-cloudmessaging-access-point-prod…
  18 8.567019   172.20.10.1  172.20.10.2  DNS      272 Standard query response 0x9e51 HTTPS prod-westeurope.access-point.cloudmessaging.edge.microsoft.com CNAME edge-cloudmessaging-access-point-…
  19 26.149383  172.20.10.2  172.20.10.1  DNS       76 Standard query 0xf199 A dns.msftncsi.com
  20 26.192268  172.20.10.1  172.20.10.2  DNS       92 Standard query response 0xf199 A dns.msftncsi.com A 131.107.255.255
  21 68.798925  172.20.10.2  172.20.10.1  DNS       78 Standard query 0x23ac A capi.grammarly.com
  22 68.854549  172.20.10.1  172.20.10.2  DNS      206 Standard query response 0x23ac A capi.grammarly.com A 54.157.32.176 A 54.204.24.111 A 107.20.75.163 A 100.28.96.14 A 54.144.253.41 A 3.218.…
  23 69.695270  172.20.10.2  172.20.10.1  DNS       78 Standard query 0xe35d A www.googleapis.com
  24 69.695881  172.20.10.2  172.20.10.1  DNS       78 Standard query 0xf2ea HTTPS www.googleapis.com
  25 69.754226  172.20.10.1  172.20.10.2  DNS      135 Standard query response 0xf2ea HTTPS www.googleapis.com SOA ns1.google.com
  26 69.755520  172.20.10.1  172.20.10.2  DNS      254 Standard query response 0xe35d A www.googleapis.com A 216.58.209.74 A 142.250.184.170 A 142.250.201.74 A 216.58.223.202 A 216.58.223.234 A …
  27 82.184104  172.20.10.2  172.20.10.1  DNS       76 Standard query 0xe1cb A in.grammarly.com
  28 82.227565  172.20.10.1  172.20.10.2  DNS      172 Standard query response 0xe1cb A in.grammarly.com A 52.203.239.42 A 23.22.191.96 A 52.5.83.208 A 3.228.48.165 A 54.152.194.244 A 54.147.138…
  29 86.043114  172.20.10.2  172.20.10.1  DNS       96 Standard query 0xc3d5 A win-extension.femetrics.grammarly.io
  30 86.074459  172.20.10.1  172.20.10.2  DNS      224 Standard query response 0xc3d5 A win-extension.femetrics.grammarly.io A 52.55.67.5 A 3.213.14.42 A 3.212.165.58 A 18.232.33.164 A 3.94.69.1…
  31 86.441842  172.20.10.2  172.20.10.1  DNS       84 Standard query 0xc418 A www.google-analytics.com
  32 86.493896  172.20.10.1  172.20.10.2  DNS      100 Standard query response 0xc418 A www.google-analytics.com A 142.250.184.174
```

```
> Frame 14: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface \Device\NPF_{D2C04B74-13E
> Ethernet II, Src: 02:db:70:a9:1b:64 (02:db:70:a9:1b:64), Dst: Intel_9c:01:30 (58:91:cf:9c:01:30)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2
> User Datagram Protocol, Src Port: 53, Dst Port: 60829
> Domain Name System (response)
```

```
0000  58 91 cf 9c 01 30 02 db  70 a9 1b 64 08 00 45 00   X····0·· p··d··E·
0010  00 8a 1f b3 00 00 40 11  ee 84 ac 14 0a 01 ac 14   ······@· ········
0020  0a 02 00 35 ed 9d 00 76  8b 28 43 29 81 80 00 01   ···5···v ·(C)····
0030  00 00 00 01 00 00 14 6f  70 74 69 6d 69 7a 61 74   ·······o ptimizat
0040  69 6f 6e 67 75 69 64 65  2d 70 61 0a 67 6f 6f 67   ionguide -pa·goog
0050  6c 65 61 70 69 73 03 63  6f 6d 00 00 41 00 01 c0   leapis·c om··A···
0060  21 00 06 00 01 00 00 00  3c 00 2d 03 6e 73 31 06   !······· <·-·ns1·
0070  67 6f 6f 67 6c 65 c0 2c  09 64 6e 73 2d 61 64 6d   google·, ·dns-adm
0080  69 6e c0 45 29 76 f9 1b  00 00 03 84 00 00 03 84   in·E)v·· ········
0090  00 00 07 08 00 00 00 3c                            ·······<
```



*WiFi (udp port 53 or tcp port 53)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp 53
```

```
No.  Time       Source       Destination  Protocol Length Info
  13 8.548960   172.20.10.1  172.20.10.2  DNS      223 Standard query response 0xf48a A optimizationguide-pa.googleapis.com A 142.250.185.10 A 142.250.200.138 A 142.250.184.170 A 142.250.200.74 …
  14 8.550015   172.20.10.1  172.20.10.2  DNS      152 Standard query response 0x4329 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
  15 8.557621   172.20.10.2  172.20.10.1  DNS      122 Standard query 0xa551 A prod-westeurope.access-point.cloudmessaging.edge.microsoft.com
  16 8.558278   172.20.10.2  172.20.10.1  DNS      122 Standard query 0x9e51 HTTPS prod-westeurope.access-point.cloudmessaging.edge.microsoft.com
  17 8.566121   172.20.10.1  172.20.10.2  DNS      227 Standard query response 0xa551 A prod-westeurope.access-point.cloudmessaging.edge.microsoft.com CNAME edge-cloudmessaging-access-point-prod…
  18 8.567019   172.20.10.1  172.20.10.2  DNS      272 Standard query response 0x9e51 HTTPS prod-westeurope.access-point.cloudmessaging.edge.microsoft.com CNAME edge-cloudmessaging-access-point-…
  19 26.149383  172.20.10.2  172.20.10.1  DNS       76 Standard query 0xf199 A dns.msftncsi.com
  20 26.192268  172.20.10.1  172.20.10.2  DNS       92 Standard query response 0xf199 A dns.msftncsi.com A 131.107.255.255
  21 68.798925  172.20.10.2  172.20.10.1  DNS       78 Standard query 0x23ac A capi.grammarly.com
  22 68.854549  172.20.10.1  172.20.10.2  DNS      206 Standard query response 0x23ac A capi.grammarly.com A 54.157.32.176 A 54.204.24.111 A 107.20.75.163 A 100.28.96.14 A 54.144.253.41 A 3.218.…
  23 69.695270  172.20.10.2  172.20.10.1  DNS       78 Standard query 0xe35d A www.googleapis.com
  24 69.695881  172.20.10.2  172.20.10.1  DNS       78 Standard query 0xf2ea HTTPS www.googleapis.com
  25 69.754226  172.20.10.1  172.20.10.2  DNS      135 Standard query response 0xf2ea HTTPS www.googleapis.com SOA ns1.google.com
  26 69.755520  172.20.10.1  172.20.10.2  DNS      254 Standard query response 0xe35d A www.googleapis.com A 216.58.209.74 A 142.250.184.170 A 142.250.201.74 A 216.58.223.202 A 216.58.223.234 A …
  27 82.184104  172.20.10.2  172.20.10.1  DNS       76 Standard query 0xe1cb A in.grammarly.com
  28 82.227565  172.20.10.1  172.20.10.2  DNS      172 Standard query response 0xe1cb A in.grammarly.com A 52.203.239.42 A 23.22.191.96 A 52.5.83.208 A 3.228.48.165 A 54.152.194.244 A 54.147.138…
  29 86.043114  172.20.10.2  172.20.10.1  DNS       96 Standard query 0xc3d5 A win-extension.femetrics.grammarly.io
  30 86.074459  172.20.10.1  172.20.10.2  DNS      224 Standard query response 0xc3d5 A win-extension.femetrics.grammarly.io A 52.55.67.5 A 3.213.14.42 A 3.212.165.58 A 18.232.33.164 A 3.94.69.1…
  31 86.441842  172.20.10.2  172.20.10.1  DNS       84 Standard query 0xc418 A www.google-analytics.com
  32 86.493896  172.20.10.1  172.20.10.2  DNS      100 Standard query response 0xc418 A www.google-analytics.com A 142.250.184.174
```

```
> Frame 15: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF_{D2C04B74-13EC-
> Ethernet II, Src: Intel_9c:01:30 (58:91:cf:9c:01:30), Dst: 02:db:70:a9:1b:64 (02:db:70:a9:1b:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 63542, Dst Port: 53
> Domain Name System (query)
```

```
0000  02 db 70 a9 1b 64 58 91  cf 9c 01 30 08 00 45 00   ··p··dX· ···0··E·
0010  00 6c bc 1b 00 00 80 11  12 3a ac 14 0a 02 ac 14   ·l······ ·:······
0020  0a 01 f8 36 00 35 00 58  9c db a5 51 01 00 00 01   ···6·5·X ···Q····
0030  00 00 00 00 00 00 0f 70  72 6f 64 2d 77 65 73 74   ·······p rod-west
0040  65 75 72 6f 70 65 0c 61  63 63 65 73 73 2d 70 6f   europe·a ccess-po
0050  69 6e 74 0e 63 6c 6f 75  64 6d 65 73 73 61 67 69   int·clou dmessagi
0060  6e 67 04 65 64 67 65 09  6d 69 63 72 6f 73 6f 66   ng·edge· microsof
0070  74 03 63 6f 6d 00 00 01  00 01                     t·com··· ··
```

After analysing the above packets, both the query and response it is concluded that there is no unusual queries or connections. Though,

If you see DNS queries to unknown external servers, it could be indicative of a compromise or an attempt to contact a command and control (C&C) server, and Large numbers of DNS queries from a single internal host indicate potential malware.

Exercise 4: Identify any DNS packets that may indicate a connection to a suspicious or malicious domain. Provide details about the domain queried and any associated IP addresses.

No domain was queried. The answer to this is same as exercise 3.

Exercise 5: Document any anomalous traffic patterns you discovered. What does this suggest about potential malicious activity?

No anomalous traffic was discovered. Though potential malicious activity may include:

Suspicious DNS queries: Queries to unusual or unexpected domain names, or an unusually high volume of DNS queries from a particular host.

DNS tunneling: Malicious activity where attackers encode data in DNS queries to exfiltrate information.

Unusual traffic patterns: Uncommon or unexpected DNS port usage, unusual DNS server IP addresses, etc.

Exercise 6: Prepare an incident report based on your analysis. Include any relevant packet captures, screenshots, and detailed explanations of the findings.

Incident Report: Network Traffic Analysis

Objective

The goal of this report is to summarize the findings of a proactive network traffic analysis using Wireshark. Specifically, the focus was on monitoring DNS traffic, identifying potential indicators of compromise (IoC), and detecting any unusual or suspicious activities on the network.

1. Overview of Network Traffic During the Incident

The network traffic was captured using Wireshark on a Wi-Fi interface, and several key observations were made based on packet captures.

Traffic Observations

DNS Traffic: The DNS traffic rate was observed to be 0.0003 to 0.0002 in some and 0.0003 to 0.0001 packets per second (pps), which is relatively low. This low rate was expected, considering the small environment with minimal DNS usage.

Potential Causes for Low Traffic:

- Long periods between captures.
- Short sampling windows.
- Low DNS traffic due to limited network activity.

Concern: The DNS traffic rate was low, but since no major DNS activity was expected in the environment, this wasn’t immediately a concern. However, in a larger network where DNS traffic is expected to be more frequent, an unusually low rate could be a red flag.

General Traffic Patterns:

Normal Traffic: Represented by **green packets**; most packets seemed to be part of standard TCP conversations and HTTPS connections (port 443).

Anomalies: **Red spikes** were observed, which typically indicate:

- A burst of network activity, possibly due to file transfers, large web requests, or Distributed Denial of Service (DDoS) attacks.
- Network congestion or a pattern of sustained high traffic, possibly due to business operations or system updates.

Red flags: **Error packets (red)**, indicating failed connections or abnormal network conditions. These should be reviewed for any recurring patterns that could point to issues such as network misconfigurations or attack attempts.

Potential Indicators of Compromise:

While no immediate signs of compromise were detected, abnormal spikes in network traffic or error packets (as seen in the red indicators) could warrant further investigation. Additionally, patterns such as high-frequency DNS queries or unusual traffic (especially to external DNS servers) should be monitored for potential malware or exfiltration attempts.

2. Suspicious Packet Analysis:

For this exercise, I identified a suspicious packet for analysis. Here's a breakdown:

Packet Breakdown:

- Source Port (src): 443 (HTTPS)

-Destination Port (dst): 57660 (High ephemeral port)

-Sequence Number (Seq): 1

-Acknowledgment Number (Ack): 1

-Length (len): 31 bytes of data

Inferences from the Packet:

-Source Port (443 - HTTPS): Port 443 is typically used for encrypted HTTPS traffic. If this packet is coming from a trusted internal server, it would be considered normal. However, if the source is unfamiliar or external, it could be suspicious, as it may indicate unauthorized communication.

-Destination Port (57660 - Ephemeral Port): Port 57660 is a high, dynamic port commonly used for client-side communication. The use of this port could indicate a legitimate outbound connection from an internal client to an external server. However, if the destination IP is unknown or suspicious, this could signal:

-Data exfiltration or command-and-control (C&C) communication using HTTPS to disguise the traffic.

- Sequence and Acknowledgment Numbers (Seq: 1, Ack: 1): These numbers are typical during the initial TCP handshake, which is normal for establishing connections.

-Packet Length (31 bytes): While the packet length is small, it still carries data. If this packet is part of a larger, sustained communication session, it could indicate a pattern of potential C&C communication or other malicious activity.

Suspicious Indicators:

-Unusual Destination Port: The combination of port 443 and a high-numbered ephemeral port suggests the potential for:

-Malware traffic disguised as legitimate HTTPS traffic.

-Data exfiltration over encrypted channels.

-Encrypted Traffic: Since this packet uses HTTPS, it is encrypted, making it difficult to analyze the content directly. If this traffic is coming from an unfamiliar source or involves large volumes of data, it could be a red flag.

Conclusion

The packet itself is not inherently suspicious, but the context (i.e., if it originates from an unknown source or involves unknown destination IPs) could warrant further investigation for potential malicious activity.

3. DNS Traffic Monitoring:

For Exercise 3, I implemented a Wireshark capture filter to monitor DNS traffic, using the following filter to capture UDP and TCP traffic on port 53 (DNS):

Capture Filter: tcp 53

Analysis of Captured DNS Packets:

Findings: After analyzing the DNS query and response packets, no unusual queries or connections were found.

- All observed DNS queries appeared to be legitimate and related to standard domain resolution.

- Responses included valid DNS A-records for known domains, with no evidence of malicious domains or unusual patterns of behavior.

Key Observations:

-No DNS tunneling: No large TXT record responses or unusual data patterns were observed.

-No Suspicious Domains: All queries resolved to common, known domains with no evidence of external command-and-control (C&C) or malware-related domains.

4. Malicious Domain Detection (Exercise 4):

During the packet analysis for DNS queries, no suspicious or malicious domain names were identified. All DNS queries were either internal or directed to reputable external DNS servers. Therefore, no indicators of a connection to malicious domains were found.

5. Anomalous Traffic Patterns (Exercise 5):

No significant anomalous traffic patterns were identified during the packet capture. However, based on general network traffic behavior, potential signs of malicious activity could include:

-Suspicious DNS Queries: Large numbers of DNS queries originating from a single host or requests to unknown external servers could indicate a **compromised host** or **C&C server communication**.

-DNS Tunneling: Malicious activity where data is exfiltrated through DNS requests (e.g., unusually large TXT records) could also be a red flag.

-Unusual Traffic Patterns: If DNS traffic uses unexpected ports or involves unusual destination IPs, it could suggest that an attacker is trying to bypass network monitoring.

Incident Report Summary:

-Normal Traffic: Most packets observed in the capture were part of typical network operations (e.g., HTTPS traffic on port 443).

-Suspicious Packet: A packet with source port 443 (HTTPS) and destination port 57660 raised suspicion due to the high-numbered ephemeral port, which might indicate obfuscation or malicious activity if the destination IP was unfamiliar.

-DNS Traffic: No anomalies were detected in DNS queries. All DNS traffic appeared to be legitimate, with no unusual domains or queries observed.

Potential Indicators of Malicious Activity:

- Unusual or high-frequency DNS queries.

- Unfamiliar or suspicious external IP addresses.

- Uncommon port usage (especially for DNS).

- Large TXT records, which could indicate DNS tunneling.

Recommendations:

1. Monitor Network Traffic: Continue to monitor DNS and HTTPS traffic for any unusual patterns or spikes.

2. Investigate Suspicious Outbound Connections: Further investigate any outgoing traffic to unfamiliar external IPs, especially involving high ephemeral ports.

3. Network Security Policies: Consider implementing stricter DNS filtering or blocking of non-standard DNS traffic to prevent exfiltration attempts or C&C communication.

```
sudo update-alternatives --config java
```

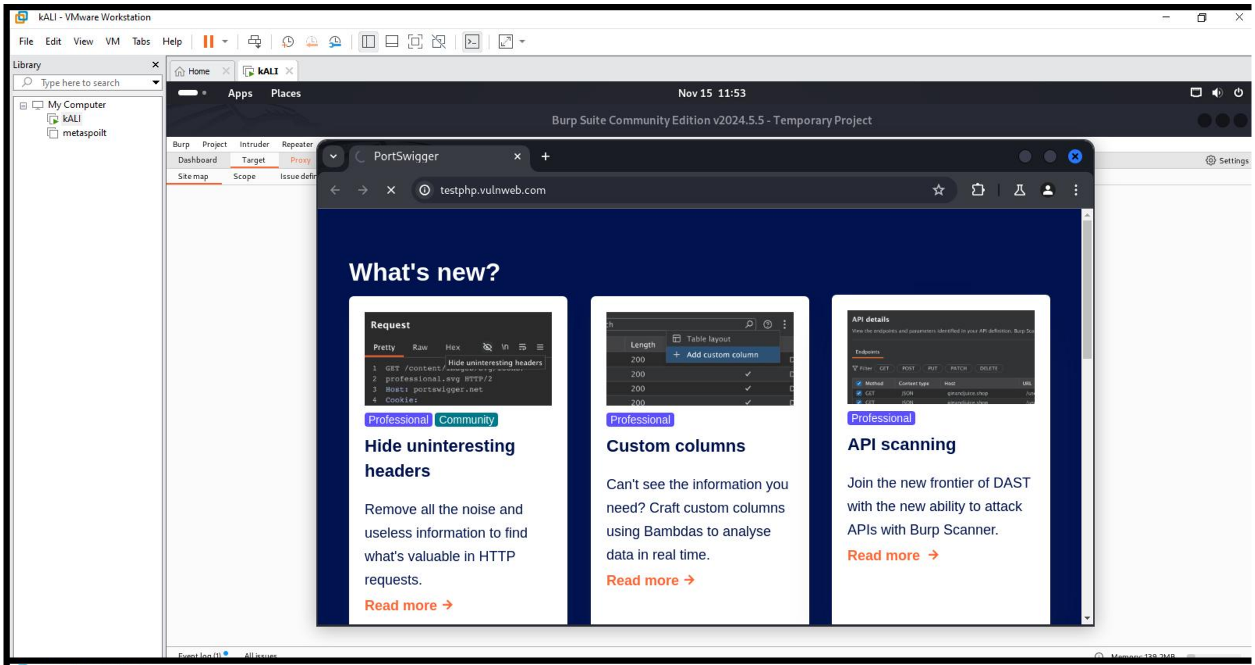
```
curl https://raw.githubusercontent.com/xiv3r/Burpsuite-Professional/main/install.sh |sudo bash
```

INT302: Kali Linux Tools and System Security – Lab 8: Web Application Security Testing with Burp Suite and OWASP ZAP

Exercise 1:

• Document the HTTP request and response headers for the home page of the target application.

What information do you find in these headers?



What's new?

```
1  GET /content/images/svg/icons/
2  professional.svg HTTP/2
3  Host: portswigger.net
4  Cookie:
```

Professional Community

Hide uninteresting headers

Remove all the noise and useless information to find what's valuable in HTTP requests.

Read more →

Professional

Custom columns

Can't see the information you need? Craft custom columns using Bambdas to analyse data in real time.

Read more →

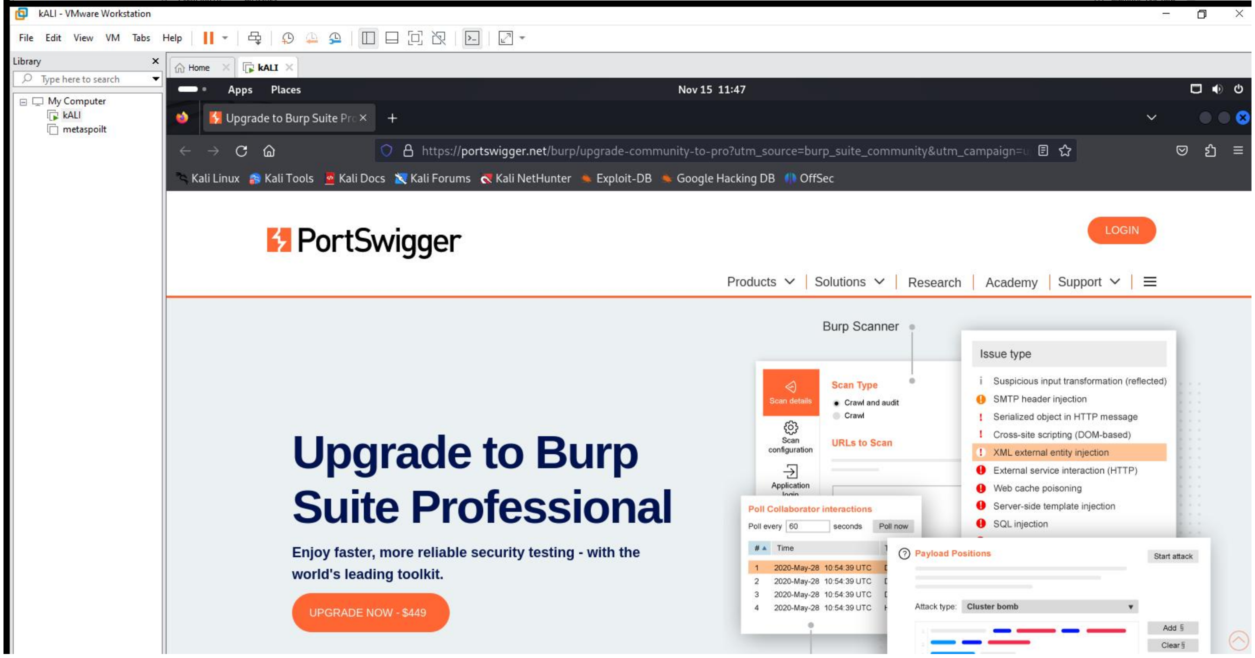
API details
Endpoints
Filter GET POST PUT PATCH DELETE
Method Content type Host URL

Professional

API scanning

Join the new frontier of DAST with the new ability to attack APIs with Burp Scanner.

Read more →

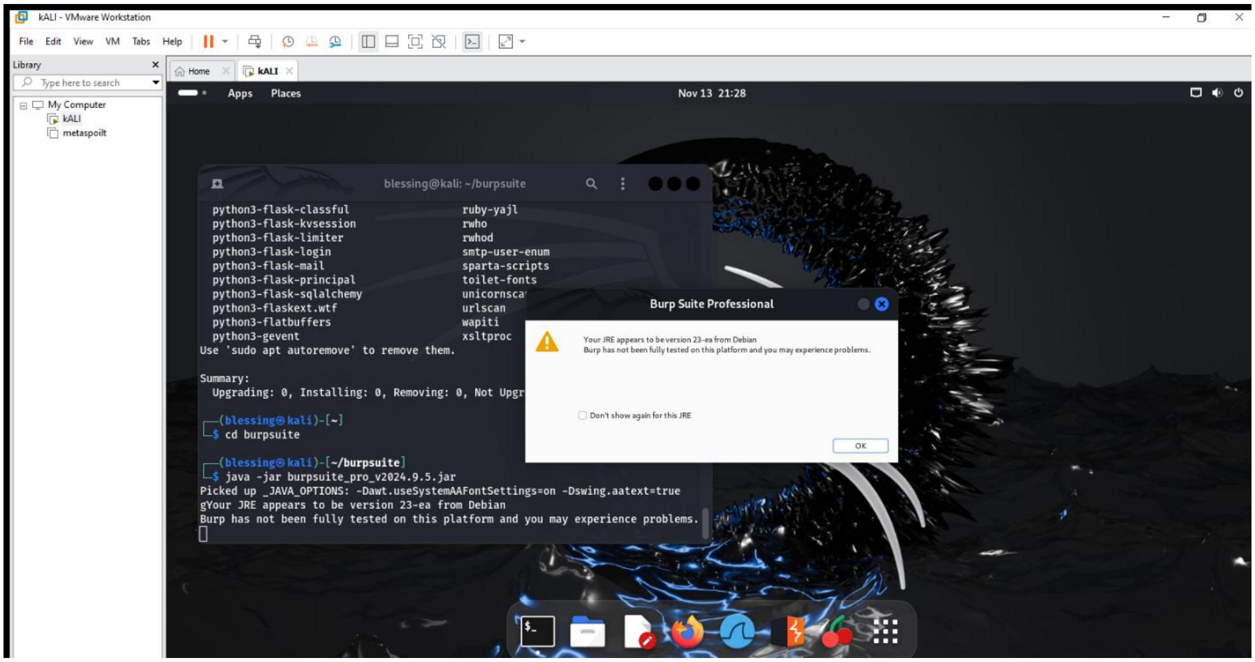

kALI - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kALI
metaspoilt
Home
kALI
Apps Places
Nov 15 11:47
Upgrade to Burp Suite Pr
https://portswigger.net/burp/upgrade-community-to-pro?utm_source=burp_suite_community&utm_campaign=
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
PortSwigger
LOGIN
Products Solutions Research Academy Support

Upgrade to Burp Suite Professional

Enjoy faster, more reliable security testing - with the world's leading toolkit.

UPGRADE NOW - $449

Burp Scanner
Scan details
Scan configuration
Application login
Scan Type
Crawl and audit
Crawl
URLs to Scan
Issue type
Suspicious input transformation (reflected)
SMTP header injection
Serialized object in HTTP message
Cross-site scripting (DOM-based)
XML external entity injection
External service interaction (HTTP)
Web cache poisoning
Server-side template injection
SQL injection
Poll Collaborator interactions
Poll every 60 seconds Poll now
# Time
1 2020-May-28 10:54:39 UTC
2 2020-May-28 10:54:39 UTC
3 2020-May-28 10:54:39 UTC
4 2020-May-28 10:54:39 UTC
Payload Positions
Start attack
Attack type: Cluster bomb
Add §
Clear §



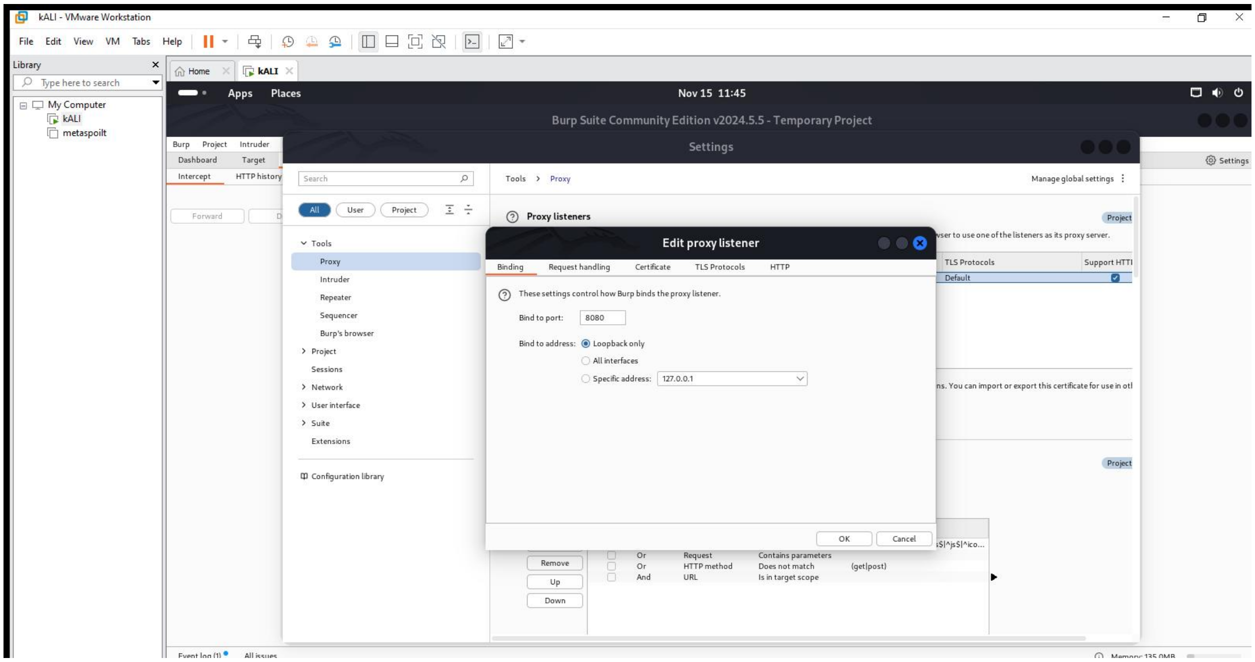
```
  python3-flask-classful              ruby-yajl
  python3-flask-kvsession             rwho
  python3-flask-limiter               rwhod
  python3-flask-login                 smtp-user-enum
  python3-flask-mail                  sparta-scripts
  python3-flask-principal             toilet-fonts
  python3-flask-sqlalchemy            unicornsca
  python3-flaskext.wtf                urlscan
  python3-flatbuffers                 wapiti
  python3-gevent                      xsltproc
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgr

┌──(blessing㉿kali)-[~]
└─$ cd burpsuite

┌──(blessing㉿kali)-[~/burpsuite]
└─$ java -jar burpsuite_pro_v2024.9.5.jar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
gYour JRE appears to be version 23-ea from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

Burp Suite Professional

Your JRE appears to be version 23-ea from Debian
Burp has not been fully tested on this platform and you may experience problems.

□ Don't show again for this JRE

OK



Proxy listeners

...ser to use one of the listeners as its proxy server.

TLS Protocols	Support HTT
Default	☑

...ns. You can import or export this certificate for use in ot...

Edit proxy listener

Binding | Request handling | Certificate | TLS Protocols | HTTP

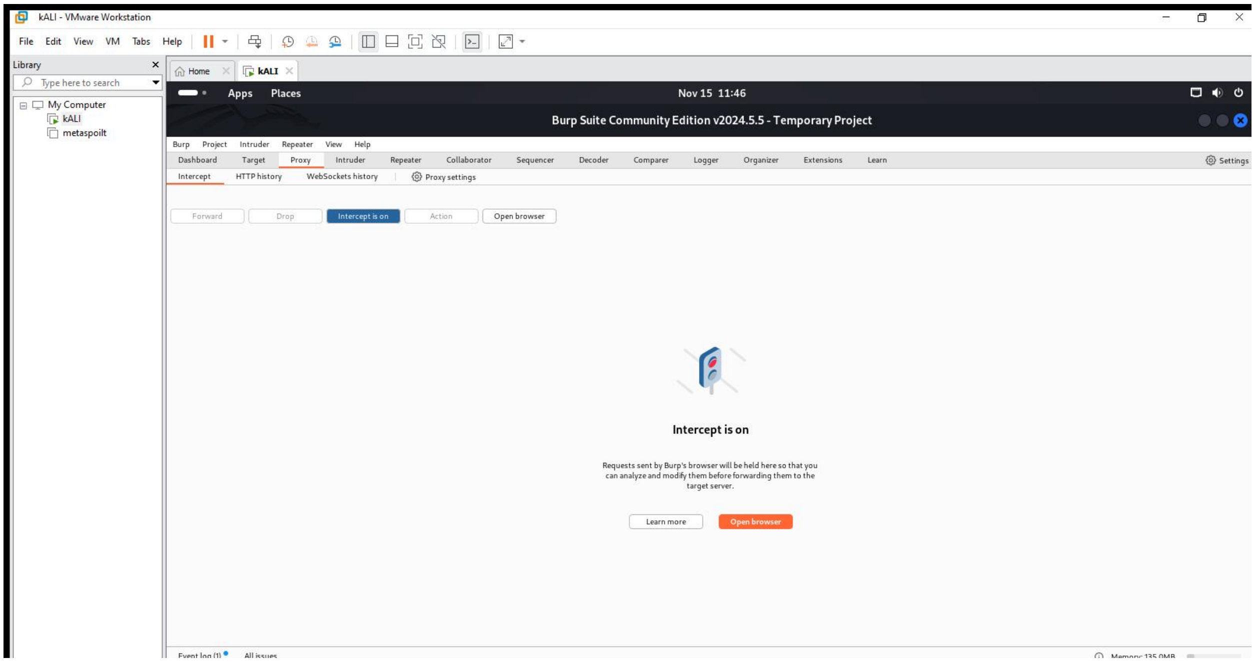
These settings control how Burp binds the proxy listener.

Bind to port: 8080

Bind to address: ● Loopback only
○ All interfaces
○ Specific address: 127.0.0.1

OK Cancel

				...s$\|^js$|^ico...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

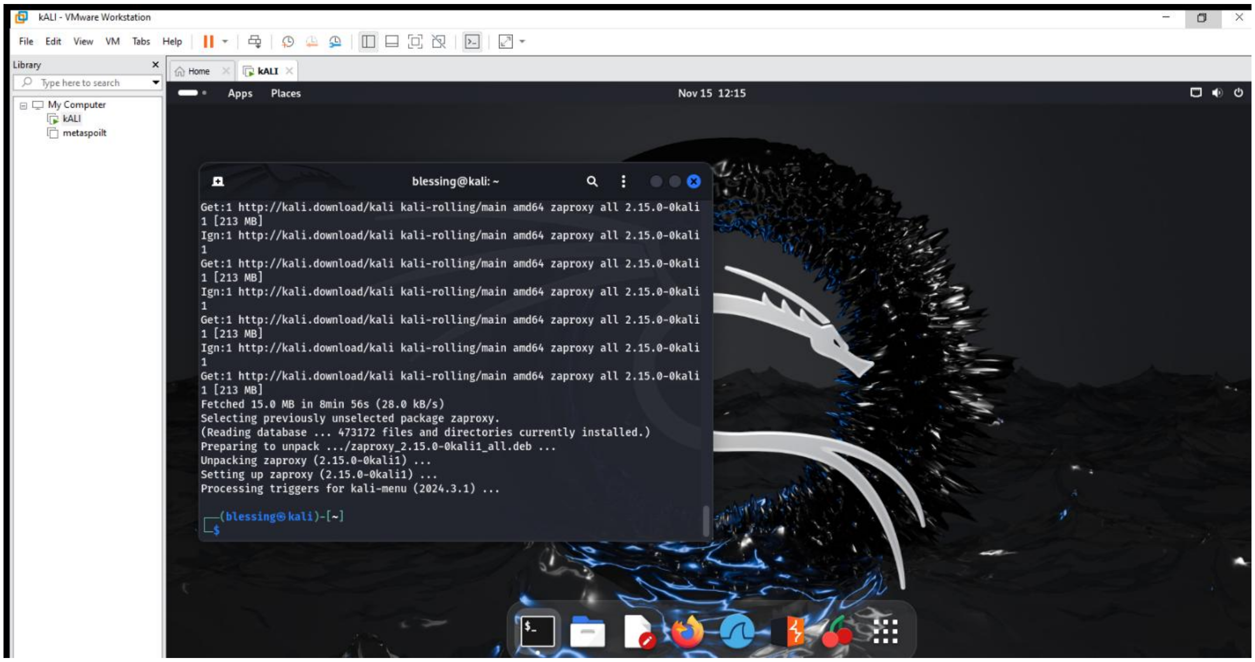

kALI - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kALI
metaspoilt
Home
kALI
Apps Places
Nov 15 11:46
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Learn more
Open browser

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

1.Launch OWASP ZAP:

- Start OWASP ZAP from your Kali Linux environment



```
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali
1 [213 MB]
Ign:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali
1
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali
1 [213 MB]
Ign:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali
1
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali
1 [213 MB]
Ign:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali
1
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.15.0-0kali
1 [213 MB]
Fetched 15.0 MB in 8min 56s (28.0 kB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 473172 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.15.0-0kali1_all.deb ...
Unpacking zaproxy (2.15.0-0kali1) ...
Setting up zaproxy (2.15.0-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...

┌──(blessing㉿kali)-[~]
└─$
```

INT302: Kali Linux Tools and System Security – Lab 9: Information Gathering with Recon-ng and Shodan

Exercise 1:

• List the modules that can be used for domain reconnaissance. What are some key modules you might consider?

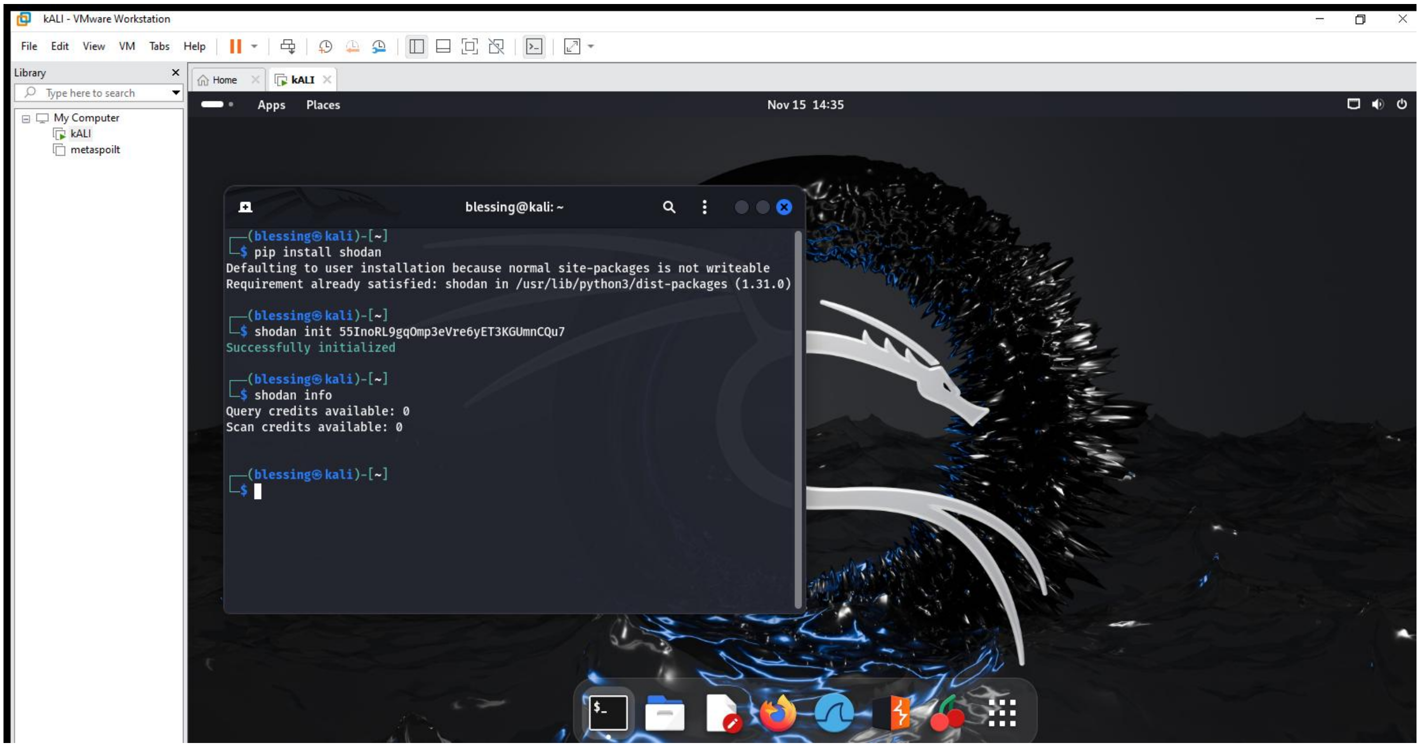
The modules are sub-domain discovery, DNS information, WHOIS data, and vulnerability scanning.

For **domain reconnaissance**, the most critical modules are those related to subdomain discovery, DNS resolution, WHOIS data, and vulnerability scanning. Some of the key modules include bing_domain_web, google_site_web, resolve_dns, and whois_record. These modules will help you gather a comprehensive set of data about your target domain, including subdomains, IP addresses, DNS records, and registration information, which are essential for a thorough reconnaissance phase.

Exercise 4:

• Verify that your API key is working by running:

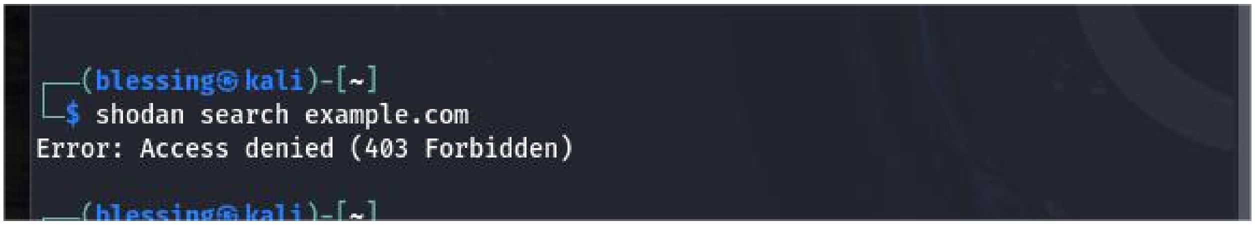
• Shodan info



```
┌──(blessing㉿kali)-[~]
└─$ pip install shodan
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: shodan in /usr/lib/python3/dist-packages (1.31.0)

┌──(blessing㉿kali)-[~]
└─$ shodan init 55InoRL9gqOmp3eVre6yET3KGUmnCQu7
Successfully initialized

┌──(blessing㉿kali)-[~]
└─$ shodan info
Query credits available: 0
Scan credits available: 0


┌──(blessing㉿kali)-[~]
└─$ 
```

Exercise 5:

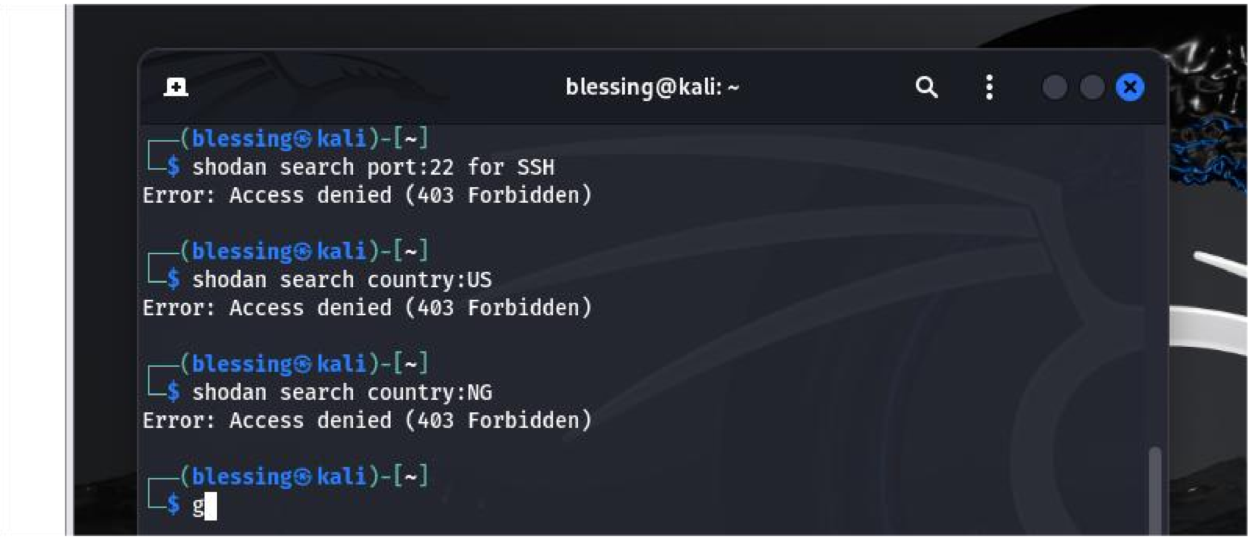
• What devices were discovered related to the target domain? Provide a brief description of the findings.



```
┌──(blessing㉿kali)-[~]
└─$ shodan search example.com
Error: Access denied (403 Forbidden)

┌──(blessing㉿kali)-[~]
```

Exercise 6:

• Perform an advanced search using two different filters. Document the results and discuss what types of devices you found.



```
┌──(blessing㉿kali)-[~]
└─$ shodan search port:22 for SSH
Error: Access denied (403 Forbidden)

┌──(blessing㉿kali)-[~]
└─$ shodan search country:US
Error: Access denied (403 Forbidden)

┌──(blessing㉿kali)-[~]
└─$ shodan search country:NG
Error: Access denied (403 Forbidden)

┌──(blessing㉿kali)-[~]
└─$ g
```