Capture and Analyze Network Traffic Using Wireshark

Name: Jerin Cherian
Date: 11/08/2025
Tool Used: Wireshark (Windows)
PCAP File: task5_capture.pcap

1. Objective

To capture live network traffic, identify at least three different protocols, and analyze their purpose.

2. Steps Performed

1. Opened Wireshark and selected the active network interface **Wi-Fi**.
2. Started live packet capture.
3. Generated network traffic by:
    - Browsing websites (*testphp.vulnweb.com, openai.com*)
    - Running *ping google.com -4 -n 5*
    - Running *nslookup openai.com*
4. Stopped the capture after ~1 minute.
5. Filtered packets using http, dns, and icmp.
6. Identified and analyzed the captured protocols.
7. Saved capture as task5_capture.pcap.

3. Protocols Identified

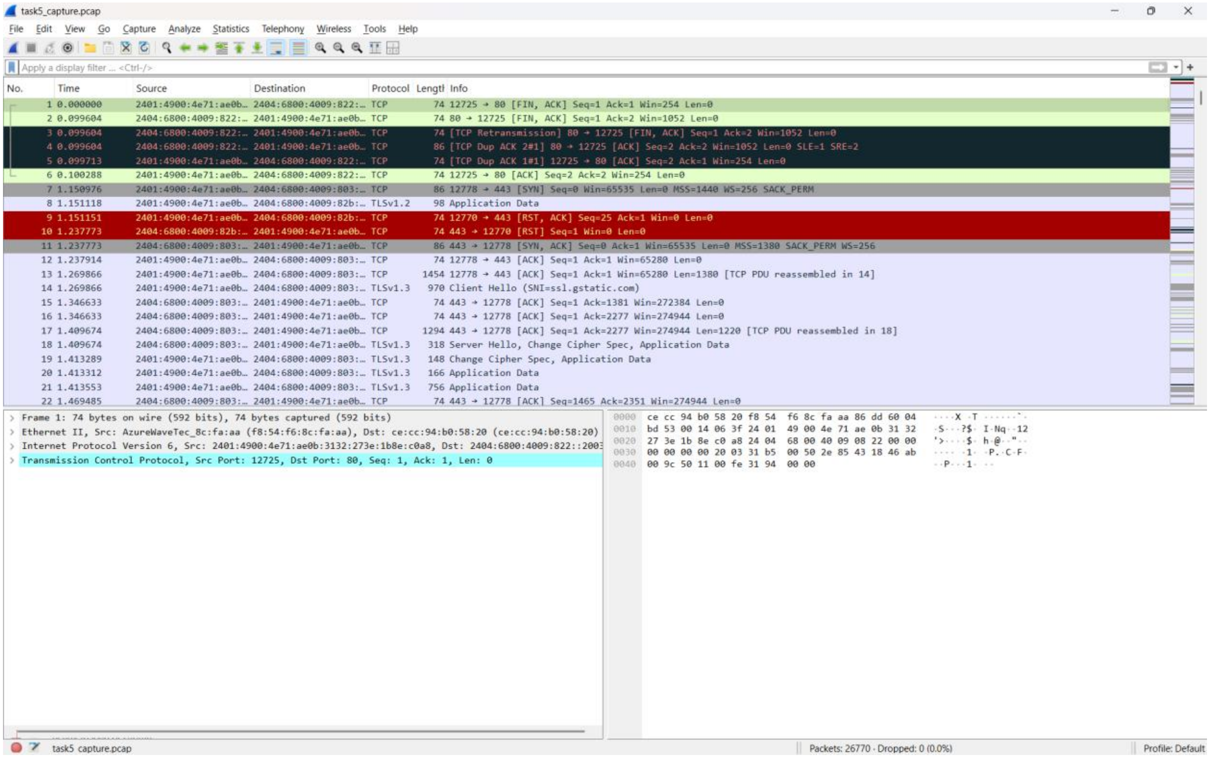
Protocol	Purpose	Example from Capture
HTTP	Web communication between client & server	GET request to *http://testphp.vulnweb.com/login.php*
DNS	Domain name resolution	Query for *openai.com* with IP returned
ICMP	Network connectivity testing	Echo request & reply from *google.com*

4. Findings Summary

Captured live traffic and identified **HTTP**, **DNS**, and **ICMP** protocols. HTTP showed web requests and responses, DNS resolved hostnames to IPs, and ICMP confirmed network connectivity through ping replies.

5. Evidence (Screenshots)

Screenshot 1: Wireshark capturing



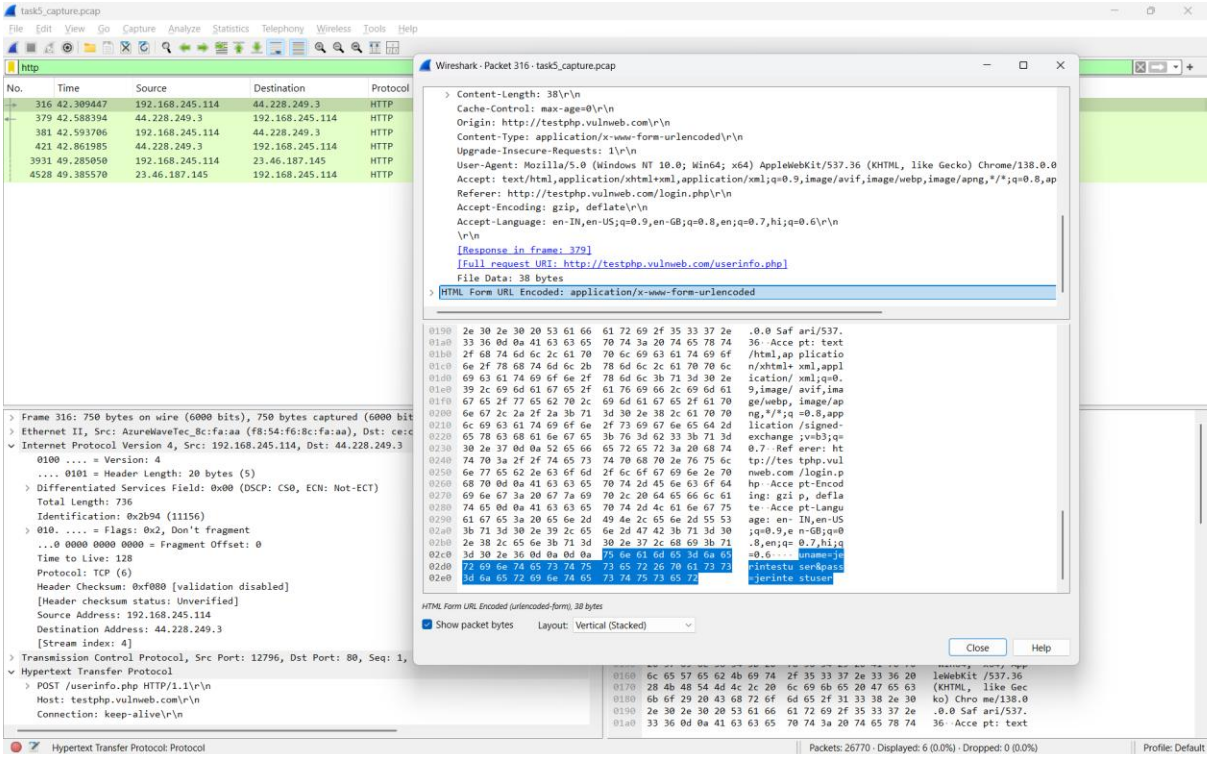
```
No.  Time      Source                Destination           Protocol Lengtl Info
  1 0.000000  2401:4900:4e71:ae0b… 2404:6800:4009:822:… TCP        74 12725 → 80 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0
  2 0.099604  2404:6800:4009:822:… 2401:4900:4e71:ae0b… TCP        74 80 → 12725 [FIN, ACK] Seq=1 Ack=2 Win=1052 Len=0
  3 0.099604  2404:6800:4009:822:… 2401:4900:4e71:ae0b… TCP        74 [TCP Retransmission] 80 → 12725 [FIN, ACK] Seq=1 Ack=2 Win=1052 Len=0
  4 0.099604  2404:6800:4009:822:… 2401:4900:4e71:ae0b… TCP        86 [TCP Dup ACK 2#1] 80 → 12725 [ACK] Seq=2 Ack=2 Win=1052 Len=0 SLE=1 SRE=2
  5 0.099713  2401:4900:4e71:ae0b… 2404:6800:4009:822:… TCP        74 [TCP Dup ACK 1#1] 12725 → 80 [ACK] Seq=2 Ack=1 Win=254 Len=0
  6 0.100288  2401:4900:4e71:ae0b… 2404:6800:4009:822:… TCP        74 12725 → 80 [ACK] Seq=2 Ack=2 Win=254 Len=0
  7 1.150976  2401:4900:4e71:ae0b… 2404:6800:4009:803:… TCP        86 12778 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
  8 1.151118  2401:4900:4e71:ae0b… 2404:6800:4009:82b:… TLSv1.2    98 Application Data
  9 1.151151  2401:4900:4e71:ae0b… 2404:6800:4009:82b:… TCP        74 12770 → 443 [RST, ACK] Seq=25 Ack=1 Win=0 Len=0
 10 1.237773  2404:6800:4009:82b:… 2401:4900:4e71:ae0b… TCP        74 443 → 12770 [RST] Seq=1 Win=0 Len=0
 11 1.237773  2404:6800:4009:803:… 2401:4900:4e71:ae0b… TCP        86 443 → 12778 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM WS=256
 12 1.237914  2401:4900:4e71:ae0b… 2404:6800:4009:803:… TCP        74 12778 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 13 1.269866  2401:4900:4e71:ae0b… 2404:6800:4009:803:… TCP      1454 12778 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1380 [TCP PDU reassembled in 14]
 14 1.269866  2401:4900:4e71:ae0b… 2404:6800:4009:803:… TLSv1.3   970 Client Hello (SNI=ssl.gstatic.com)
 15 1.346633  2404:6800:4009:803:… 2401:4900:4e71:ae0b… TCP        74 443 → 12778 [ACK] Seq=1 Ack=1381 Win=272384 Len=0
 16 1.346633  2404:6800:4009:803:… 2401:4900:4e71:ae0b… TCP        74 443 → 12778 [ACK] Seq=1 Ack=2277 Win=274944 Len=0
 17 1.409674  2404:6800:4009:803:… 2401:4900:4e71:ae0b… TCP      1294 443 → 12778 [ACK] Seq=1 Ack=2277 Win=274944 Len=1220 [TCP PDU reassembled in 18]
 18 1.409674  2404:6800:4009:803:… 2401:4900:4e71:ae0b… TLSv1.3   318 Server Hello, Change Cipher Spec, Application Data
 19 1.413289  2401:4900:4e71:ae0b… 2404:6800:4009:803:… TLSv1.3   148 Change Cipher Spec, Application Data
 20 1.413312  2401:4900:4e71:ae0b… 2404:6800:4009:803:… TLSv1.3   166 Application Data
 21 1.413553  2401:4900:4e71:ae0b… 2404:6800:4009:803:… TLSv1.3   756 Application Data
 22 1.469485  2404:6800:4009:803:… 2401:4900:4e71:ae0b… TCP        74 443 → 12778 [ACK] Seq=1465 Ack=2351 Win=274944 Len=0
```

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: AzureWaveTec_8c:fa:aa (f8:54:f6:8c:fa:aa), Dst: ce:cc:94:b0:58:20 (ce:cc:94:b0:58:20)
> Internet Protocol Version 6, Src: 2401:4900:4e71:ae0b:3132:273e:1b8e:c0a8, Dst: 2404:6800:4009:822::2003
> Transmission Control Protocol, Src Port: 12725, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  ce cc 94 b0 58 20 f8 54  f6 8c fa aa 86 dd 60 04   ····X ·T ······`·
0010  bd 53 00 14 06 3f 24 01  49 00 4e 71 ae 0b 31 32   ·S···?$· I·Nq··12
0020  27 3e 1b 8e c0 a8 24 04  68 00 40 09 08 22 00 00   '>····$· h·@··"··
0030  00 00 00 00 20 03 31 b5  00 50 2e 85 43 18 46 ab   ···· ·1· ·P.·C·F·
0040  00 9c 50 11 00 fe 31 94  00 00                     ··P···1· ··
```

task5 capture.pcap | Packets: 26770 · Dropped: 0 (0.0%) | Profile: Default

Screenshot 2: HTTP filtered packets


task5_capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 316 · task5_capture.pcap
Show packet bytes
Layout: Vertical (Stacked)
Close
Help
Profile: Default

Filter: http

No.	Time	Source	Destination	Protocol
316	42.309447	192.168.245.114	44.228.249.3	HTTP
379	42.588394	44.228.249.3	192.168.245.114	HTTP
381	42.593706	192.168.245.114	44.228.249.3	HTTP
421	42.861985	44.228.249.3	192.168.245.114	HTTP
3931	49.285050	192.168.245.114	23.46.187.145	HTTP
4528	49.385570	23.46.187.145	192.168.245.114	HTTP

```
> Frame 316: 750 bytes on wire (6000 bits), 750 bytes captured (6000 bit
> Ethernet II, Src: AzureWaveTec_8c:fa:aa (f8:54:f6:8c:fa:aa), Dst: ce:c
v Internet Protocol Version 4, Src: 192.168.245.114, Dst: 44.228.249.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 736
    Identification: 0x2b94 (11156)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xf080 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.245.114
    Destination Address: 44.228.249.3
    [Stream index: 4]
> Transmission Control Protocol, Src Port: 12796, Dst Port: 80, Seq: 1,
v Hypertext Transfer Protocol
  > POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
```

```
0160  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36
0170  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0180  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 33 38 2e 30   ko) Chro me/138.0
0190  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
01a0  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36··Acce pt: text
```

Wireshark · Packet 316 · task5_capture.pcap

```
  > Content-Length: 38\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-IN,en-US;q=0.9,en-GB;q=0.8,en;q=0.7,hi;q=0.6\r\n
    \r\n
    [Response in frame: 379]
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    File Data: 38 bytes
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0190  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
01a0  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36··Acce pt: text
01b0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
01c0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
01d0  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
01e0  39 2c 69 6d 61 67 65 2f  61 76 69 66 2c 69 6d 61   9,image/ avif,ima
01f0  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
0200  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
0210  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
0220  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
0230  30 2e 37 0d 0a 52 65 66  65 72 65 72 3a 20 68 74   0.7··Ref erer: ht
0240  74 70 3a 2f 2f 74 65 73  74 70 68 70 2e 76 75 6c   tp://tes tphp.vul
0250  6e 77 65 62 2e 63 6f 6d  2f 6c 6f 67 69 6e 2e 70   nweb.com /login.p
0260  68 70 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   hp··Acce pt-Encod
0270  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0280  74 65 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   te··Acce pt-Langu
0290  61 67 65 3a 20 65 6e 2d  49 4e 2c 65 6e 2d 55 53   age: en- IN,en-US
02a0  3b 71 3d 30 2e 39 2c 65  6e 2d 47 42 3b 71 3d 30   ;q=0.9,e n-GB;q=0
02b0  2e 38 2c 65 6e 3b 71 3d  30 2e 37 2c 68 69 3b 71   .8,en;q= 0.7,hi;q
02c0  3d 30 2e 36 0d 0a 0d 0a  75 6e 61 6d 65 3d 6a 65   =0.6···· uname=je
02d0  72 69 6e 74 65 73 74 75  73 65 72 26 70 61 73 73   rintestu ser&pass
02e0  3d 6a 65 72 69 6e 74 65  73 74 75 73 65 72         =jerinte stuser
```

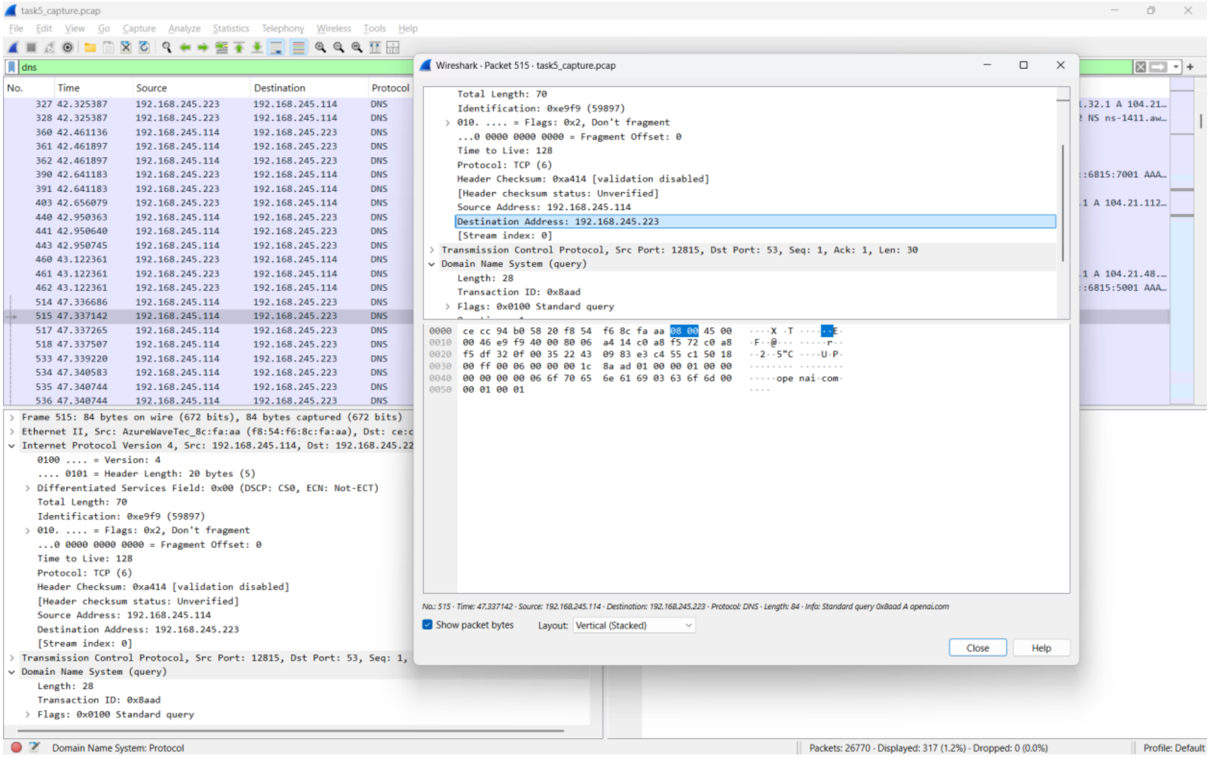
HTML Form URL Encoded (urlencoded-form), 38 bytes

☑ Show packet bytes   Layout: Vertical (Stacked)

Hypertext Transfer Protocol: Protocol

Packets: 26770 · Displayed: 6 (0.0%) · Dropped: 0 (0.0%)

Screenshot 3: DNS filtered packets


task5_capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 515 · task5_capture.pcap
Show packet bytes
Layout: Vertical (Stacked)
Close
Help
Profile: Default

Filter: dns

No.	Time	Source	Destination	Protocol	
327	42.325387	192.168.245.223	192.168.245.114	DNS	1.32.1 A 104.21…
328	42.325387	192.168.245.223	192.168.245.114	DNS	2 NS ns-1411.aw…
360	42.461136	192.168.245.114	192.168.245.223	DNS	
361	42.461897	192.168.245.114	192.168.245.223	DNS	
362	42.461897	192.168.245.114	192.168.245.223	DNS	
390	42.641183	192.168.245.223	192.168.245.114	DNS	::6815:7001 AAA…
391	42.641183	192.168.245.223	192.168.245.114	DNS	
403	42.656079	192.168.245.223	192.168.245.114	DNS	.1 A 104.21.112…
440	42.950363	192.168.245.114	192.168.245.223	DNS	
441	42.950640	192.168.245.114	192.168.245.223	DNS	
443	42.950745	192.168.245.114	192.168.245.223	DNS	
460	43.122361	192.168.245.223	192.168.245.114	DNS	.1 A 104.21.48.…
461	43.122361	192.168.245.223	192.168.245.114	DNS	::6815:5001 AAA…
462	43.122361	192.168.245.223	192.168.245.114	DNS	
514	47.336686	192.168.245.114	192.168.245.223	DNS	
515	47.337142	192.168.245.114	192.168.245.223	DNS	
517	47.337265	192.168.245.114	192.168.245.223	DNS	
518	47.337507	192.168.245.114	192.168.245.223	DNS	
533	47.339220	192.168.245.114	192.168.245.223	DNS	
534	47.340583	192.168.245.114	192.168.245.223	DNS	
535	47.340744	192.168.245.114	192.168.245.223	DNS	
536	47.340744	192.168.245.114	192.168.245.223	DNS	

```
> Frame 515: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: AzureWaveTec_8c:fa:aa (f8:54:f6:8c:fa:aa), Dst: ce:c
v Internet Protocol Version 4, Src: 192.168.245.114, Dst: 192.168.245.22
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 70
    Identification: 0xe9f9 (59897)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xa414 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.245.114
    Destination Address: 192.168.245.223
    [Stream index: 0]
> Transmission Control Protocol, Src Port: 12815, Dst Port: 53, Seq: 1,
v Domain Name System (query)
    Length: 28
    Transaction ID: 0x8aad
  > Flags: 0x0100 Standard query
```

Wireshark · Packet 515 · task5_capture.pcap

```
    Total Length: 70
    Identification: 0xe9f9 (59897)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xa414 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.245.114
    Destination Address: 192.168.245.223
    [Stream index: 0]
> Transmission Control Protocol, Src Port: 12815, Dst Port: 53, Seq: 1, Ack: 1, Len: 30
v Domain Name System (query)
    Length: 28
    Transaction ID: 0x8aad
  > Flags: 0x0100 Standard query
```

```
0000  ce cc 94 b0 58 20 f8 54  f6 8c fa aa 08 00 45 00   ····X ·T ······E·
0010  00 46 e9 f9 40 00 80 06  a4 14 c0 a8 f5 72 c0 a8   ·F··@··· ·····r··
0020  f5 df 32 0f 00 35 22 43  09 83 e3 c4 55 c1 50 18   ··2··5"C ····U·P·
0030  00 ff 00 06 00 00 00 1c  8a ad 01 00 00 01 00 00   ········ ········
0040  00 00 00 00 06 6f 70 65  6e 61 69 03 63 6f 6d 00   ·····ope nai·com·
0050  00 01 00 01                                        ····
```

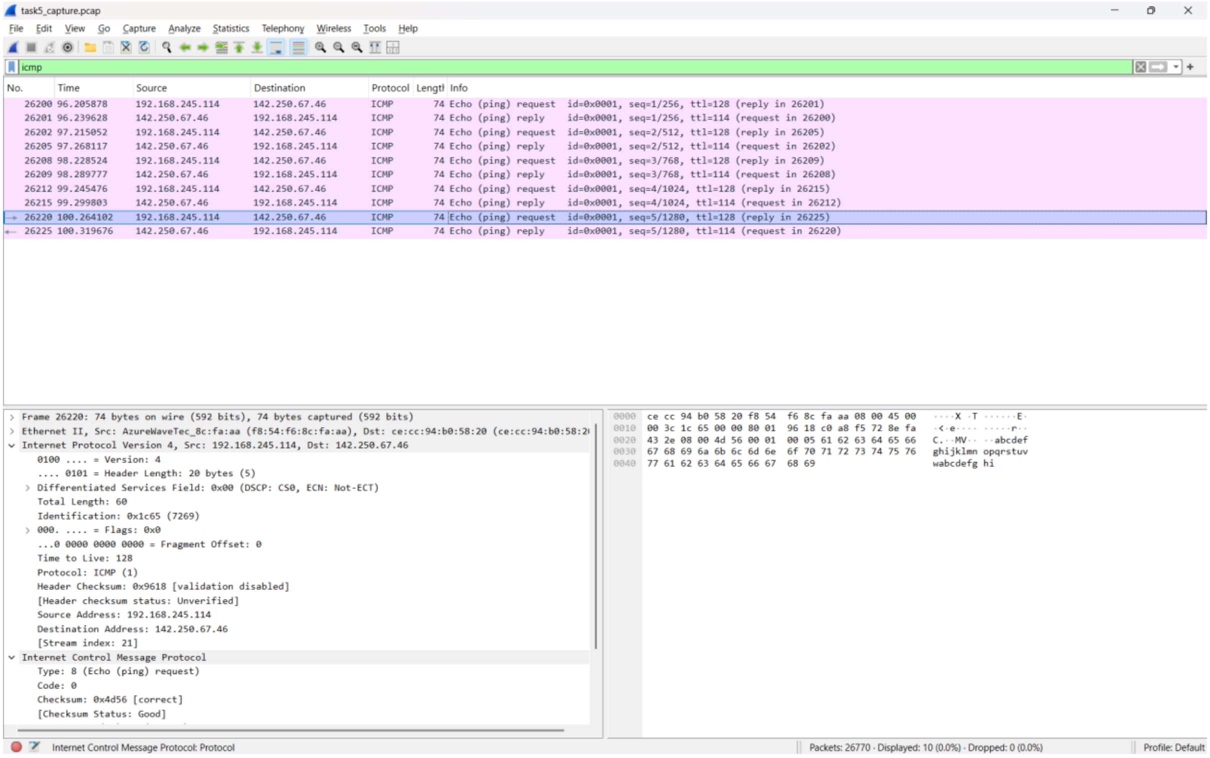
No.: 515 · Time: 47.337142 · Source: 192.168.245.114 · Destination: 192.168.245.223 · Protocol: DNS · Length: 84 · Info: Standard query 0x8aad A openai.com

☑ Show packet bytes   Layout: Vertical (Stacked)

Domain Name System: Protocol

Packets: 26770 · Displayed: 317 (1.2%) · Dropped: 0 (0.0%)

Screenshot 4: ICMP filtered packets


task5_capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
26200	96.205878	192.168.245.114	142.250.67.46	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 26201)
26201	96.239628	142.250.67.46	192.168.245.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=114 (request in 26200)
26202	97.215052	192.168.245.114	142.250.67.46	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 26205)
26205	97.268117	142.250.67.46	192.168.245.114	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=114 (request in 26202)
26208	98.228524	192.168.245.114	142.250.67.46	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 26209)
26209	98.289777	142.250.67.46	192.168.245.114	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=114 (request in 26208)
26212	99.245476	192.168.245.114	142.250.67.46	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 26215)
26215	99.299803	142.250.67.46	192.168.245.114	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=114 (request in 26212)
26220	100.264102	192.168.245.114	142.250.67.46	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 26225)
26225	100.319676	142.250.67.46	192.168.245.114	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=114 (request in 26220)

```
> Frame 26220: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: AzureWaveTec_8c:fa:aa (f8:54:f6:8c:fa:aa), Dst: ce:cc:94:b0:58:20 (ce:cc:94:b0:58:2
v Internet Protocol Version 4, Src: 192.168.245.114, Dst: 142.250.67.46
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x1c65 (7269)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x9618 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.245.114
    Destination Address: 142.250.67.46
    [Stream index: 21]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d56 [correct]
    [Checksum Status: Good]
```

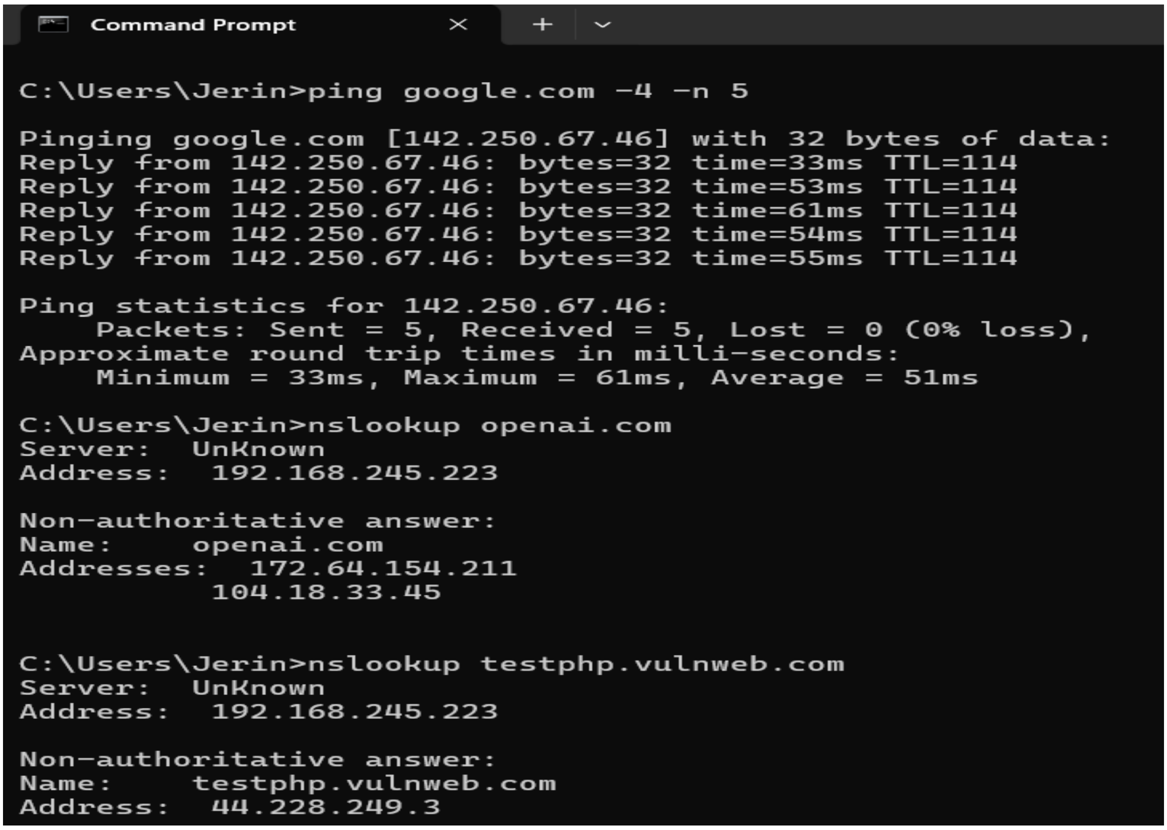
```
0000  ce cc 94 b0 58 20 f8 54  f6 8c fa aa 08 00 45 00   ····X ·T ······E·
0010  00 3c 1c 65 00 00 80 01  96 18 c0 a8 f5 72 8e fa   ·<·e···· ·····r··
0020  43 2e 08 00 4d 56 00 01  00 05 61 62 63 64 65 66   C.··MV·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol

Packets: 26770 · Displayed: 10 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

Screenshot 5: Setting ping and nslookup



```
C:\Users\Jerin>ping google.com -4 -n 5

Pinging google.com [142.250.67.46] with 32 bytes of data:
Reply from 142.250.67.46: bytes=32 time=33ms TTL=114
Reply from 142.250.67.46: bytes=32 time=53ms TTL=114
Reply from 142.250.67.46: bytes=32 time=61ms TTL=114
Reply from 142.250.67.46: bytes=32 time=54ms TTL=114
Reply from 142.250.67.46: bytes=32 time=55ms TTL=114

Ping statistics for 142.250.67.46:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 61ms, Average = 51ms

C:\Users\Jerin>nslookup openai.com
Server:  UnKnown
Address:  192.168.245.223

Non-authoritative answer:
Name:    openai.com
Addresses:  172.64.154.211
          104.18.33.45


C:\Users\Jerin>nslookup testphp.vulnweb.com
Server:  UnKnown
Address:  192.168.245.223

Non-authoritative answer:
Name:    testphp.vulnweb.com
Address:  44.228.249.3
```