ujar tech
solutions

UJAR TECH SOLUTION

Name: Rithik varma

Intern ID: UTS1103

TASK 6

Capturing Network Traffic Using Wireshark:

Using ***Wireshark*** *to capture and analyze* ***live network traffic*** *on a local machine. Apply protocol filters to study different types of traffic (HTTP, DNS, TCP, UDP, ICMP) and observe packet structures. This demonstrates how cybersecurity professionals investigate* ***real-time communication*** *and detect anomalies.*

Practical Description

Problem:- *To monitor and analyze live network traffic using Wireshark, understand packet structures, protocols, and identify potential security patterns or issues in the captured data.*

***Key Concepts of Network**:-*

Network → *A group of two or more devices connected together to share resources (data, files, internet, etc.).*

- ***Types of Networks:***
  - *LAN (Local Area Network) – small area (home, office).*
  - *WAN (Wide Area Network) – large area (internet).*
  - *MAN (Metropolitan Area Network) – city-wide networks.*

Protocol → *in networking is a set of **rules and standards** that define how data is transmitted, received, and understood between devices on a network.*

- ***Types of Protocolss:***

- ***HTTP*** *→ Web communication (uses TCP).*
- ***DNS*** *→ Resolves names to IP addresses.*
- ***TCP*** *→ Reliable, ordered communication (web, email, file transfers).*
- ***UDP*** *→ Fast, lightweight, used for streaming and gaming.*
- ***ICMP*** *→ Used for testing and error reporting (ping, traceroute).*

***Real-World Examples**:*

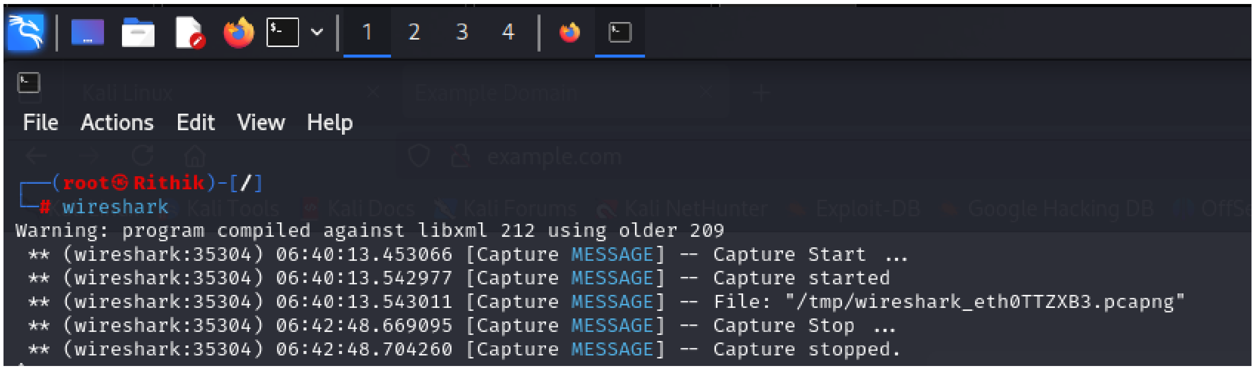
1. ***Banking Application*** *– Detecting if sensitive login credentials are transmitted in plaintext.*

2. ***Corporate Network*** *– Monitoring for suspicious ICMP floods that could signal a DoS attack.*
3. ***Healthcare System*** *– Ensuring medical records are encrypted during transmission to maintain confidentiality.*

Objective:
To gain hands-on experience in ***capturing and analyzing network packets****, understand how different protocols function, and identify patterns that could indicate* ***security risks****.*

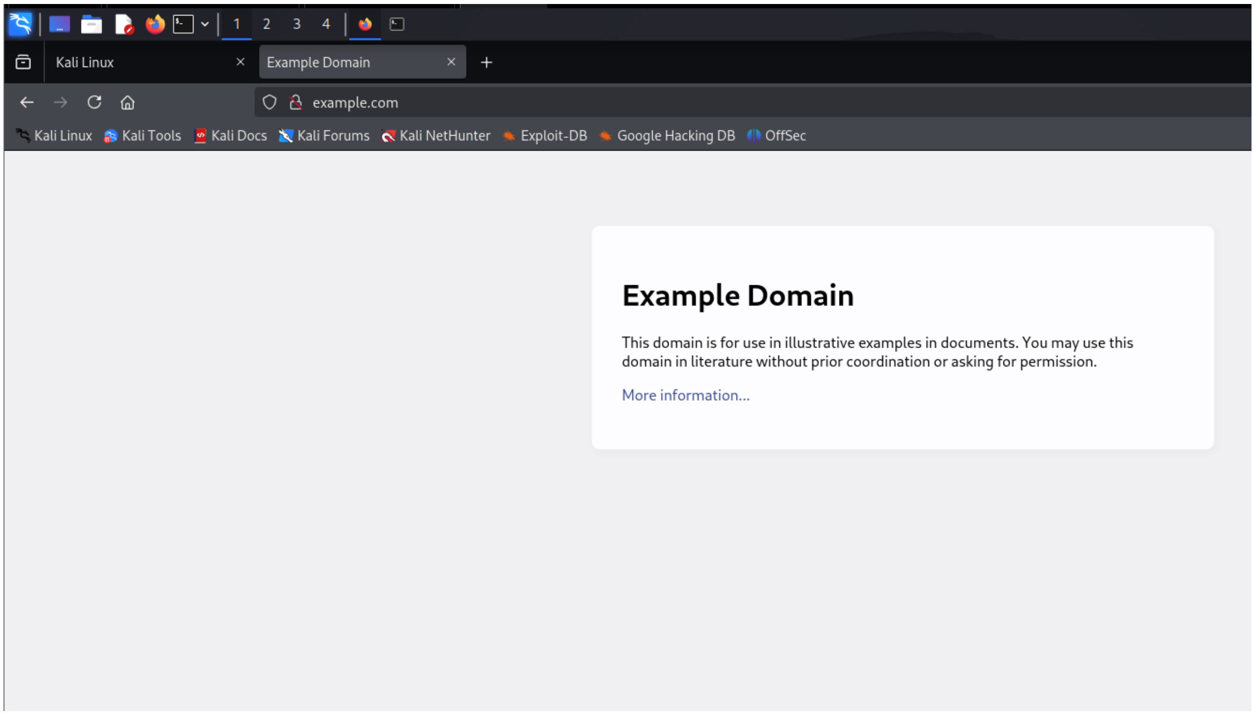
Practical of packet capture Using Kali Linux:

- *Running wireshark in root terminal.*



```
┌──(root㉿Rithik)-[/]
└─# wireshark
Warning: program compiled against libxml 212 using older 209
 ** (wireshark:35304) 06:40:13.453066 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:35304) 06:40:13.542977 [Capture MESSAGE] -- Capture started
 ** (wireshark:35304) 06:40:13.543011 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0TTZXB3.pcapng"
 ** (wireshark:35304) 06:42:48.669095 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:35304) 06:42:48.704260 [Capture MESSAGE] -- Capture stopped.
```

- *Visit websites (e.g., http://example.com)*

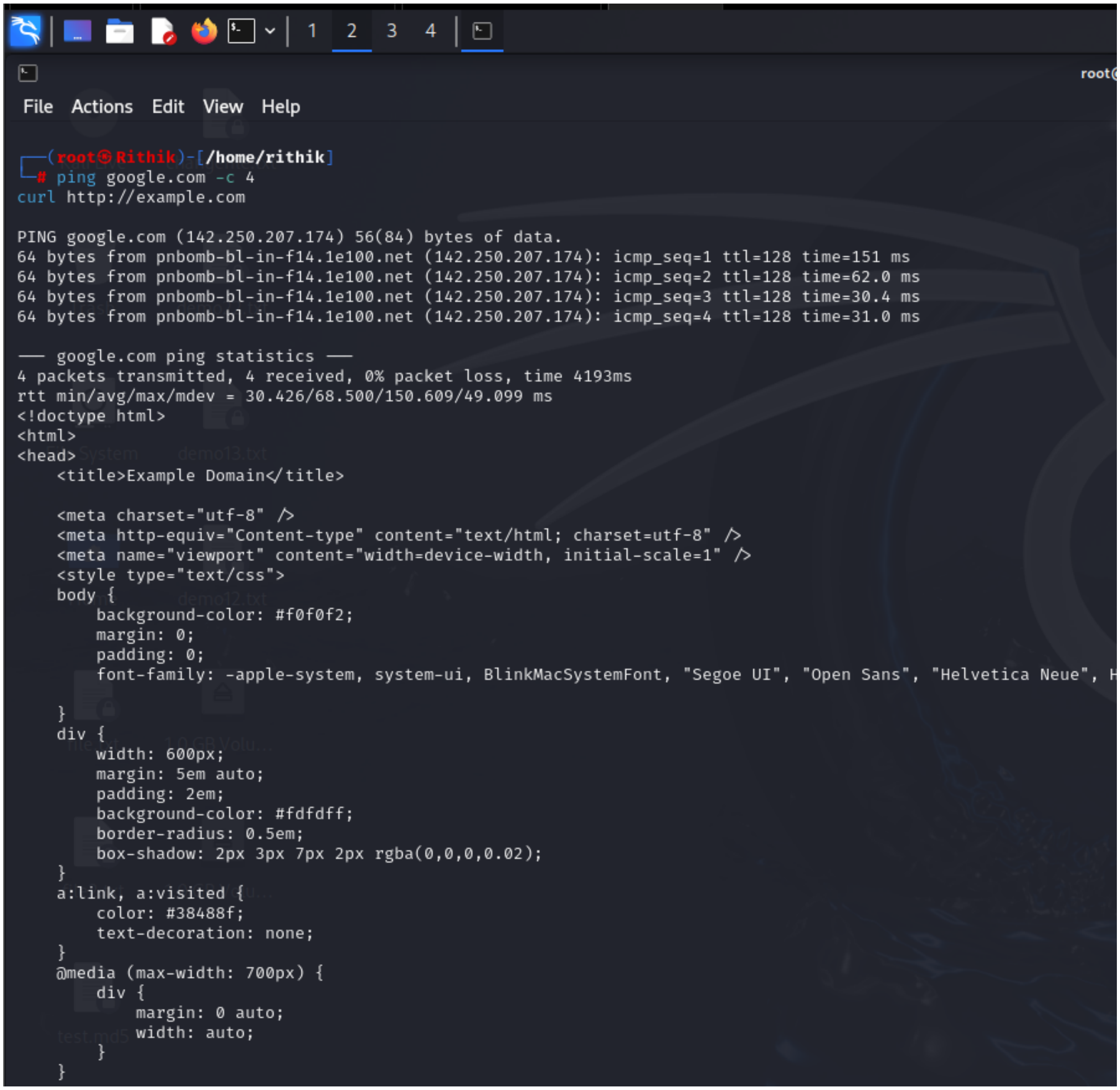


Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

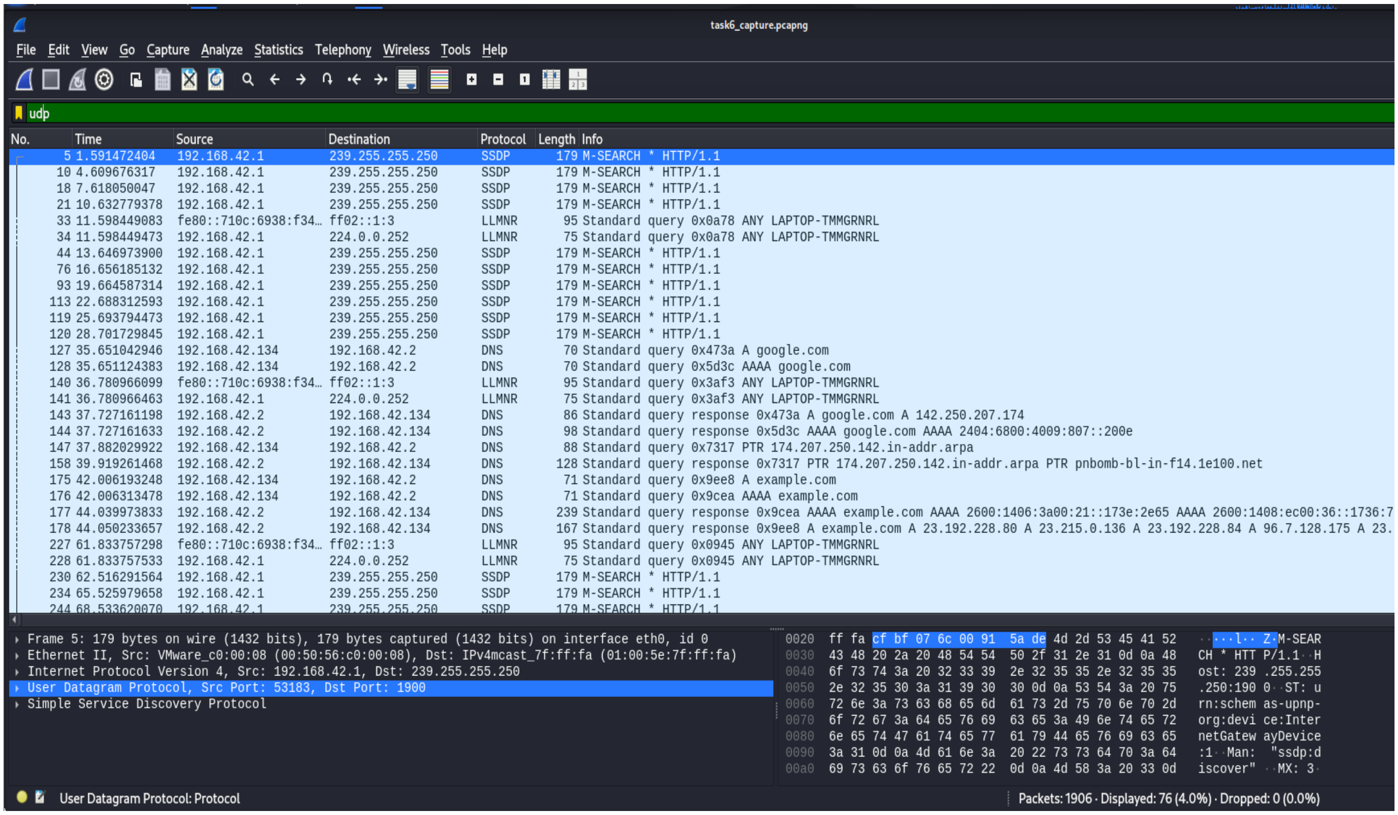
More information...

- *Use ping google.com or download a file to generate traffic.*



```
┌──(root㉿Rithik)-[/home/rithik]
└─# ping google.com -c 4
curl http://example.com

PING google.com (142.250.207.174) 56(84) bytes of data.
64 bytes from pnbomb-bl-in-f14.1e100.net (142.250.207.174): icmp_seq=1 ttl=128 time=151 ms
64 bytes from pnbomb-bl-in-f14.1e100.net (142.250.207.174): icmp_seq=2 ttl=128 time=62.0 ms
64 bytes from pnbomb-bl-in-f14.1e100.net (142.250.207.174): icmp_seq=3 ttl=128 time=30.4 ms
64 bytes from pnbomb-bl-in-f14.1e100.net (142.250.207.174): icmp_seq=4 ttl=128 time=31.0 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4193ms
rtt min/avg/max/mdev = 30.426/68.500/150.609/49.099 ms
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", H

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
```

Applied (UDP) filtered on wireshark



udp

```
No.   Time         Source                 Destination      Protocol  Length Info
    5 1.591472404  192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
   10 4.609676317  192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
   18 7.618050047  192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
   21 10.632779378 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
   33 11.598449083 fe80::710c:6938:f34…   ff02::1:3        LLMNR       95 Standard query 0x0a78 ANY LAPTOP-TMMGRNRL
   34 11.598449473 192.168.42.1           224.0.0.252      LLMNR       75 Standard query 0x0a78 ANY LAPTOP-TMMGRNRL
   44 13.646973900 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
   76 16.656185132 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
   93 19.664587314 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
  113 22.688312593 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
  119 25.693794473 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
  120 28.701729845 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
  127 35.651042946 192.168.42.134         192.168.42.2     DNS         70 Standard query 0x473a A google.com
  128 35.651124383 192.168.42.134         192.168.42.2     DNS         70 Standard query 0x5d3c AAAA google.com
  140 36.780966099 fe80::710c:6938:f34…   ff02::1:3        LLMNR       95 Standard query 0x3af3 ANY LAPTOP-TMMGRNRL
  141 36.780966463 192.168.42.1           224.0.0.252      LLMNR       75 Standard query 0x3af3 ANY LAPTOP-TMMGRNRL
  143 37.727161198 192.168.42.2           192.168.42.134   DNS         86 Standard query response 0x473a A google.com A 142.250.207.174
  144 37.727161633 192.168.42.2           192.168.42.134   DNS         98 Standard query response 0x5d3c AAAA google.com AAAA 2404:6800:4009:807::200e
  147 37.882029922 192.168.42.134         192.168.42.2     DNS         88 Standard query 0x7317 PTR 174.207.250.142.in-addr.arpa
  158 39.919261468 192.168.42.2           192.168.42.134   DNS        128 Standard query response 0x7317 PTR 174.207.250.142.in-addr.arpa PTR pnbomb-bl-in-f14.1e100.net
  175 42.006193248 192.168.42.134         192.168.42.2     DNS         71 Standard query 0x9ee8 A example.com
  176 42.006313478 192.168.42.134         192.168.42.2     DNS         71 Standard query 0x9cea AAAA example.com
  177 44.039973833 192.168.42.2           192.168.42.134   DNS        239 Standard query response 0x9cea AAAA example.com AAAA 2600:1406:3a00:21::173e:2e65 AAAA 2600:1408:ec00:36::1736:7
  178 44.050233657 192.168.42.2           192.168.42.134   DNS        167 Standard query response 0x9ee8 A example.com A 23.192.228.80 A 23.215.0.136 A 23.192.228.84 A 96.7.128.175 A 23.
  227 61.833757298 fe80::710c:6938:f34…   ff02::1:3        LLMNR       95 Standard query 0x0945 ANY LAPTOP-TMMGRNRL
  228 61.833757533 192.168.42.1           224.0.0.252      LLMNR       75 Standard query 0x0945 ANY LAPTOP-TMMGRNRL
  230 62.516291564 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
  234 65.525979658 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
  244 68.533620070 192.168.42.1           239.255.255.250  SSDP       179 M-SEARCH * HTTP/1.1
```

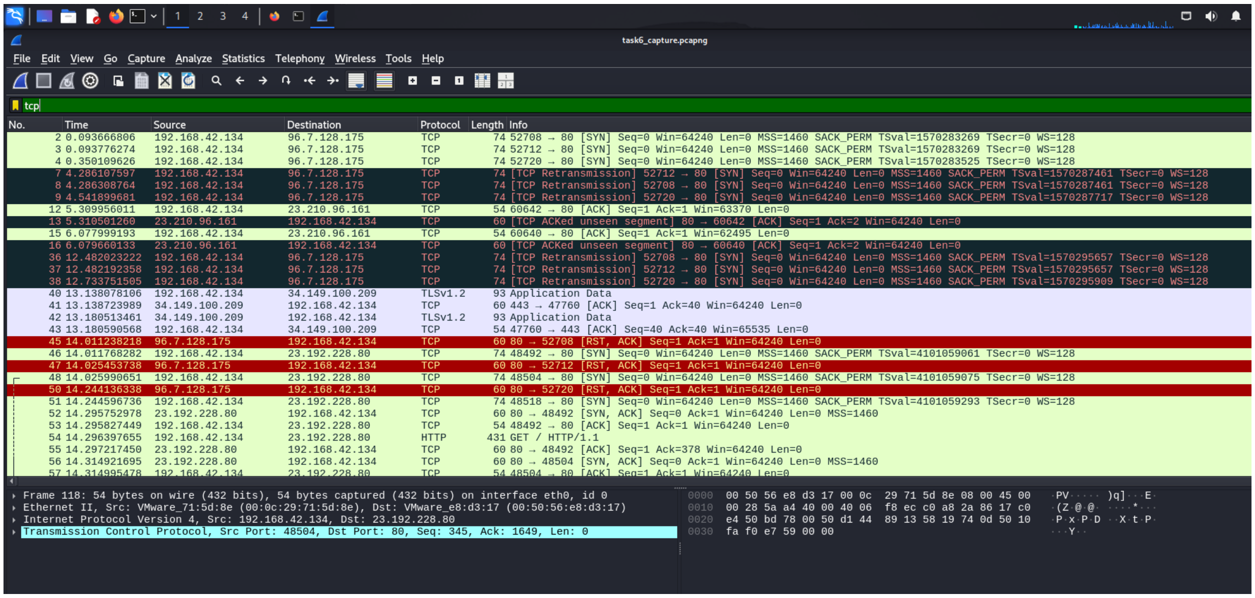
```
› Frame 5: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
› Internet Protocol Version 4, Src: 192.168.42.1, Dst: 239.255.255.250
› User Datagram Protocol, Src Port: 53183, Dst Port: 1900
› Simple Service Discovery Protocol
```

```
0020  ff fa cf bf 07 6c 00 91  5a de 4d 2d 53 45 41 52   ·····l·· Z·M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  6f 73 74 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   ost: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 53 54 3a 20 75   .250:190 0··ST: u
0060  72 6e 3a 73 63 68 65 6d  61 73 2d 75 70 6e 70 2d   rn:schem as-upnp-
0070  6f 72 67 3a 64 65 76 69  63 65 3a 49 6e 74 65 72   org:devi ce:Inter
0080  6e 65 74 47 61 74 65 77  61 79 44 65 76 69 63 65   netGatew ayDevice
0090  3a 31 0d 0a 4d 61 6e 3a  20 22 73 73 64 70 3a 64   :1··Man:  "ssdp:d
00a0  69 73 63 6f 76 65 72 22  0d 0a 4d 58 3a 20 33 0d   iscover" ··MX: 3·
```

User Datagram Protocol: Protocol

Packets: 1906 · Displayed: 76 (4.0%) · Dropped: 0 (0.0%)

- *Applied (TCP) filtered on wireshark*


1
2
3
4
task6_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

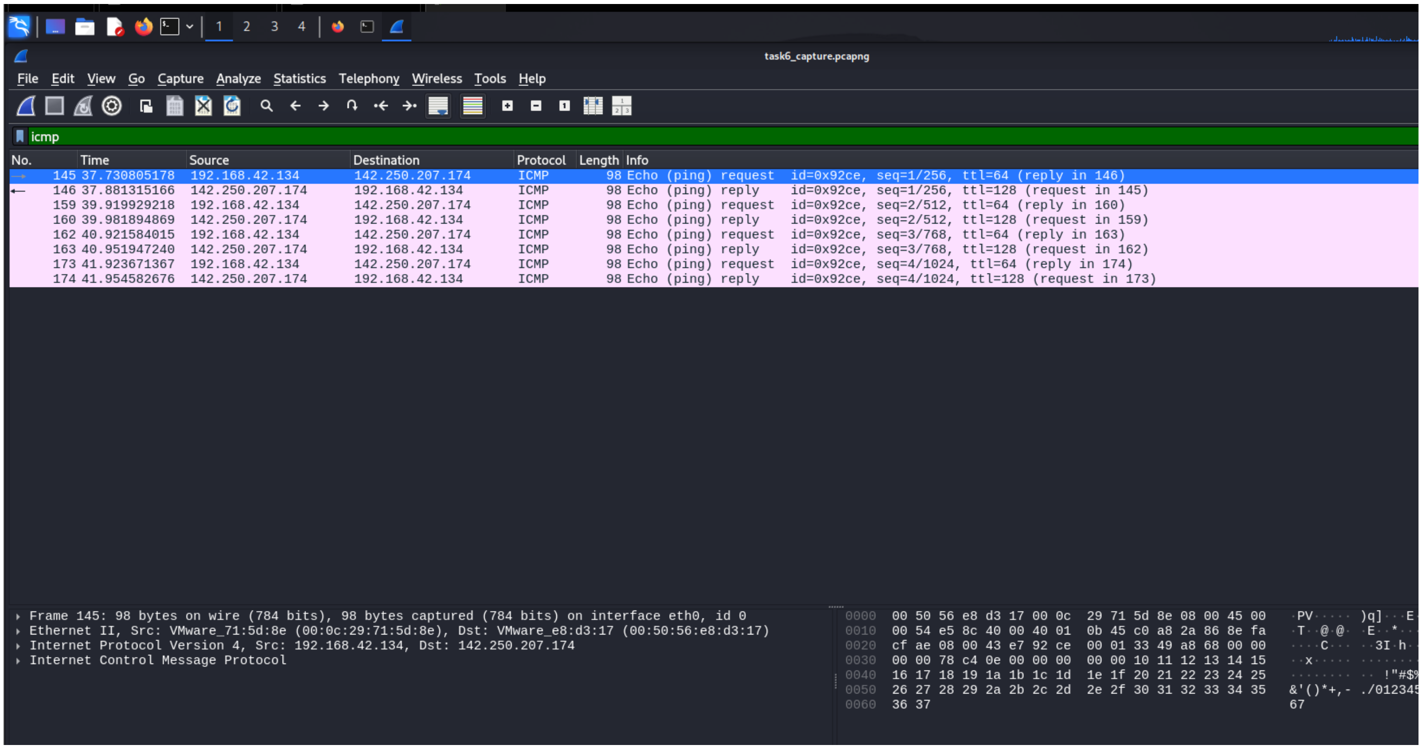
```
tcp
```

```
No.   Time          Source           Destination      Protocol  Length Info
    2 0.093666806   192.168.42.134   96.7.128.175     TCP        74 52708 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570283269 TSecr=0 WS=128
    3 0.093776274   192.168.42.134   96.7.128.175     TCP        74 52712 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570283269 TSecr=0 WS=128
    4 0.350109626   192.168.42.134   96.7.128.175     TCP        74 52720 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570283525 TSecr=0 WS=128
    7 4.286107597   192.168.42.134   96.7.128.175     TCP        74 [TCP Retransmission] 52712 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570287461 TSecr=0 WS=128
    8 4.286308764   192.168.42.134   96.7.128.175     TCP        74 [TCP Retransmission] 52708 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570287461 TSecr=0 WS=128
    9 4.541899681   192.168.42.134   96.7.128.175     TCP        74 [TCP Retransmission] 52720 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570287717 TSecr=0 WS=128
   12 5.309956011   192.168.42.134   23.210.96.161    TCP        54 60642 → 80 [ACK] Seq=1 Ack=1 Win=63370 Len=0
   13 5.310501260   23.210.96.161    192.168.42.134   TCP        60 [TCP ACKed unseen segment] 80 → 60642 [ACK] Seq=1 Ack=2 Win=64240 Len=0
   15 6.077999193   192.168.42.134   23.210.96.161    TCP        54 60640 → 80 [ACK] Seq=1 Ack=1 Win=62495 Len=0
   16 6.079660133   23.210.96.161    192.168.42.134   TCP        60 [TCP ACKed unseen segment] 80 → 60640 [ACK] Seq=1 Ack=2 Win=64240 Len=0
   36 12.482023222  192.168.42.134   96.7.128.175     TCP        74 [TCP Retransmission] 52708 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570295657 TSecr=0 WS=128
   37 12.482192358  192.168.42.134   96.7.128.175     TCP        74 [TCP Retransmission] 52712 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570295657 TSecr=0 WS=128
   38 12.733751505  192.168.42.134   96.7.128.175     TCP        74 [TCP Retransmission] 52720 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1570295909 TSecr=0 WS=128
   40 13.138078106  192.168.42.134   34.149.100.209   TLSv1.2    93 Application Data
   41 13.138723989  34.149.100.209   192.168.42.134   TCP        60 443 → 47760 [ACK] Seq=1 Ack=40 Win=64240 Len=0
   42 13.180513461  34.149.100.209   192.168.42.134   TLSv1.2    93 Application Data
   43 13.180590568  192.168.42.134   34.149.100.209   TCP        54 47760 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
   45 14.011238218  96.7.128.175     192.168.42.134   TCP        60 80 → 52708 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   46 14.011768282  192.168.42.134   23.192.228.80    TCP        74 48492 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101059061 TSecr=0 WS=128
   47 14.025453738  96.7.128.175     192.168.42.134   TCP        60 80 → 52712 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   48 14.025990651  192.168.42.134   23.192.228.80    TCP        74 48504 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101059075 TSecr=0 WS=128
   50 14.244136338  96.7.128.175     192.168.42.134   TCP        60 80 → 52720 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
   51 14.244596736  192.168.42.134   23.192.228.80    TCP        74 48518 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101059293 TSecr=0 WS=128
   52 14.295752978  23.192.228.80    192.168.42.134   TCP        60 80 → 48492 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   53 14.295827449  192.168.42.134   23.192.228.80    TCP        54 48492 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   54 14.296397655  192.168.42.134   23.192.228.80    HTTP      431 GET / HTTP/1.1
   55 14.297217450  23.192.228.80    192.168.42.134   TCP        60 80 → 48492 [ACK] Seq=1 Ack=378 Win=64240 Len=0
   56 14.314921695  23.192.228.80    192.168.42.134   TCP        60 80 → 48504 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   57 14.314995478  192.168.42.134   23.192.228.80    TCP        54 48504 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
```

```
› Frame 118: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_71:5d:8e (00:0c:29:71:5d:8e), Dst: VMware_e8:d3:17 (00:50:56:e8:d3:17)
› Internet Protocol Version 4, Src: 192.168.42.134, Dst: 23.192.228.80
› Transmission Control Protocol, Src Port: 48504, Dst Port: 80, Seq: 345, Ack: 1649, Len: 0
```

```
0000  00 50 56 e8 d3 17 00 0c  29 71 5d 8e 08 00 45 00   ·PV·····  )q]···E·
0010  00 28 5a a4 40 00 40 06  f8 ec c0 a8 2a 86 17 c0   ·(Z·@·@·  ····*···
0020  e4 50 bd 78 00 50 d1 44  89 13 58 19 74 0d 50 10   ·P·x·P·D  ··X·t·P·
0030  fa f0 e7 59 00 00                                  ···Y··
```

- *Applied (ICMP) filtered on wireshark*


1
2
3
4
task6_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

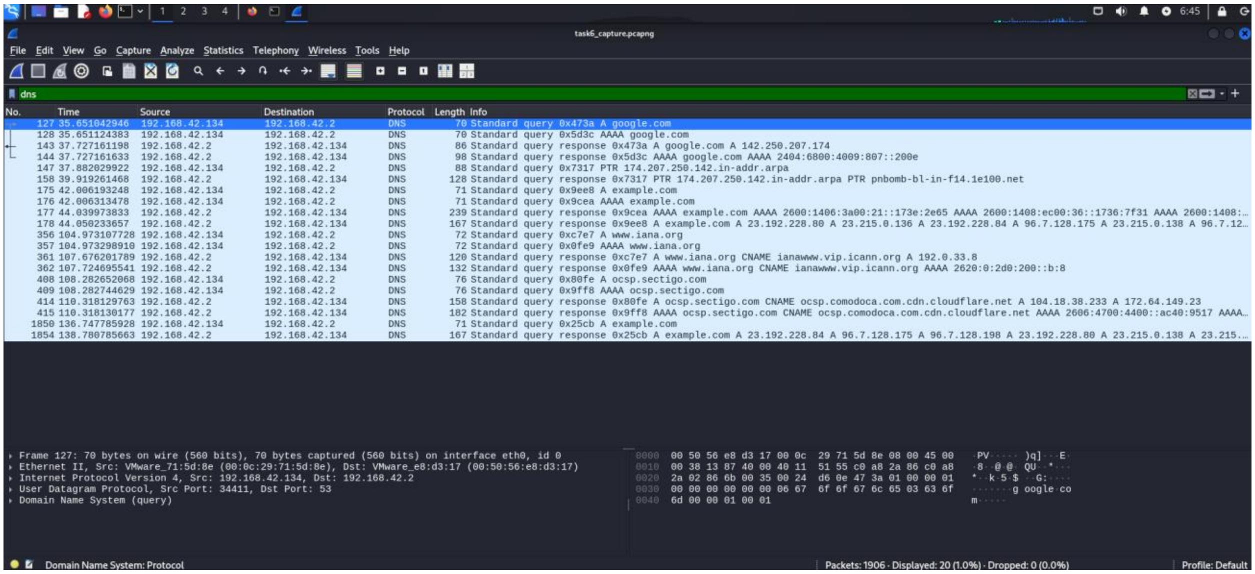
```
icmp
```

```
No.   Time          Source           Destination      Protocol  Length Info
→  145 37.730805178  192.168.42.134   142.250.207.174  ICMP      98 Echo (ping) request  id=0x92ce, seq=1/256, ttl=64 (reply in 146)
←  146 37.881315166  142.250.207.174  192.168.42.134   ICMP      98 Echo (ping) reply    id=0x92ce, seq=1/256, ttl=128 (request in 145)
   159 39.919929218  192.168.42.134   142.250.207.174  ICMP      98 Echo (ping) request  id=0x92ce, seq=2/512, ttl=64 (reply in 160)
   160 39.981894869  142.250.207.174  192.168.42.134   ICMP      98 Echo (ping) reply    id=0x92ce, seq=2/512, ttl=128 (request in 159)
   162 40.921584015  192.168.42.134   142.250.207.174  ICMP      98 Echo (ping) request  id=0x92ce, seq=3/768, ttl=64 (reply in 163)
   163 40.951947240  142.250.207.174  192.168.42.134   ICMP      98 Echo (ping) reply    id=0x92ce, seq=3/768, ttl=128 (request in 162)
   173 41.923671367  192.168.42.134   142.250.207.174  ICMP      98 Echo (ping) request  id=0x92ce, seq=4/1024, ttl=64 (reply in 174)
   174 41.954582676  142.250.207.174  192.168.42.134   ICMP      98 Echo (ping) reply    id=0x92ce, seq=4/1024, ttl=128 (request in 173)
```

```
› Frame 145: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_71:5d:8e (00:0c:29:71:5d:8e), Dst: VMware_e8:d3:17 (00:50:56:e8:d3:17)
› Internet Protocol Version 4, Src: 192.168.42.134, Dst: 142.250.207.174
› Internet Control Message Protocol
```

```
0000  00 50 56 e8 d3 17 00 0c  29 71 5d 8e 08 00 45 00   ·PV·····  )q]···E
0010  00 54 e5 8c 40 00 40 01  0b 45 c0 a8 2a 86 8e fa   ·T··@·@·  ·E··*···
0020  cf ae 08 00 43 e7 92 ce  00 01 33 49 a8 68 00 00   ····C···  ··3I·h··
0030  00 00 78 c4 0e 00 00 00  00 00 10 11 12 13 14 15   ··x·····  ········
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
```

- *Applied (DNS) filtered on wireshark*


task6_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

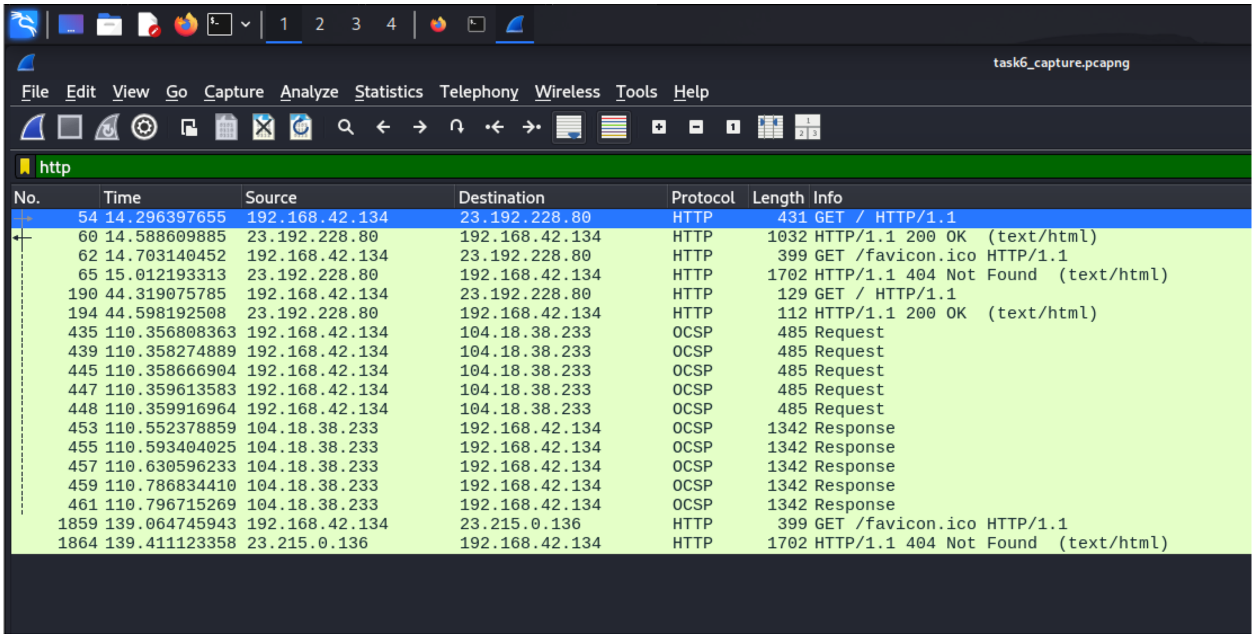
```
No.   Time          Source          Destination     Protocol Length Info
  127 35.651042946  192.168.42.134  192.168.42.2    DNS        70 Standard query 0x473a A google.com
  128 35.651124383  192.168.42.134  192.168.42.2    DNS        70 Standard query 0x5d3c AAAA google.com
  143 37.727161198  192.168.42.2    192.168.42.134  DNS        86 Standard query response 0x473a A google.com A 142.250.207.174
  144 37.727161633  192.168.42.2    192.168.42.134  DNS        98 Standard query response 0x5d3c AAAA google.com AAAA 2404:6800:4009:807::200e
  147 37.882029922  192.168.42.134  192.168.42.2    DNS        88 Standard query 0x7317 PTR 174.207.250.142.in-addr.arpa
  158 39.919261468  192.168.42.2    192.168.42.134  DNS       128 Standard query response 0x7317 PTR 174.207.250.142.in-addr.arpa PTR pnbomb-bl-in-f14.1e100.net
  175 42.006193248  192.168.42.134  192.168.42.2    DNS        71 Standard query 0x9ee8 A example.com
  176 42.006313478  192.168.42.134  192.168.42.2    DNS        71 Standard query 0x9cea AAAA example.com
  177 44.039973833  192.168.42.2    192.168.42.134  DNS       239 Standard query response 0x9cea AAAA example.com AAAA 2600:1406:3a00:21::173e:2e65 AAAA 2600:1408:ec00:36::1736:7f31 AAAA 2600:1408:…
  178 44.050233657  192.168.42.2    192.168.42.134  DNS       167 Standard query response 0x9ee8 A example.com A 23.192.228.80 A 23.215.0.136 A 23.192.228.84 A 96.7.128.175 A 23.215.0.138 A 96.7.12…
  356 104.973107728 192.168.42.134  192.168.42.2    DNS        72 Standard query 0xc7e7 A www.iana.org
  357 104.973298910 192.168.42.134  192.168.42.2    DNS        72 Standard query 0x0fe9 AAAA www.iana.org
  361 107.676201789 192.168.42.2    192.168.42.134  DNS       120 Standard query response 0xc7e7 A www.iana.org CNAME ianawww.vip.icann.org A 192.0.33.8
  362 107.724695541 192.168.42.2    192.168.42.134  DNS       132 Standard query response 0x0fe9 AAAA www.iana.org CNAME ianawww.vip.icann.org AAAA 2620:0:2d0:200::b:8
  408 108.282652068 192.168.42.134  192.168.42.2    DNS        76 Standard query 0x80fe A ocsp.sectigo.com
  409 108.282744629 192.168.42.134  192.168.42.2    DNS        76 Standard query 0x9ff8 AAAA ocsp.sectigo.com
  414 110.318129763 192.168.42.2    192.168.42.134  DNS       158 Standard query response 0x80fe A ocsp.sectigo.com CNAME ocsp.comodoca.com.cdn.cloudflare.net A 104.18.38.233 A 172.64.149.23
  415 110.318130177 192.168.42.2    192.168.42.134  DNS       182 Standard query response 0x9ff8 AAAA ocsp.sectigo.com CNAME ocsp.comodoca.com.cdn.cloudflare.net AAAA 2606:4700:4400::ac40:9517 AAAA…
 1850 136.747785928 192.168.42.134  192.168.42.2    DNS        71 Standard query 0x25cb A example.com
 1854 138.780785663 192.168.42.2    192.168.42.134  DNS       167 Standard query response 0x25cb A example.com A 23.192.228.84 A 96.7.128.175 A 96.7.128.198 A 23.192.228.80 A 23.215.0.138 A 23.215.…
```

```
› Frame 127: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_71:5d:8e (00:0c:29:71:5d:8e), Dst: VMware_e8:d3:17 (00:50:56:e8:d3:17)
› Internet Protocol Version 4, Src: 192.168.42.134, Dst: 192.168.42.2
› User Datagram Protocol, Src Port: 34411, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 50 56 e8 d3 17 00 0c  29 71 5d 8e 08 00 45 00   ·PV·····)q]···E·
0010  00 38 13 87 40 00 40 11  51 55 c0 a8 2a 86 c0 a8   ·8··@·@·QU··*···
0020  2a 02 86 6b 00 35 00 24  d6 0e 47 3a 01 00 00 01   *··k·5·$··G:····
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040  6d 00 00 01 00 01                                  m·····
```

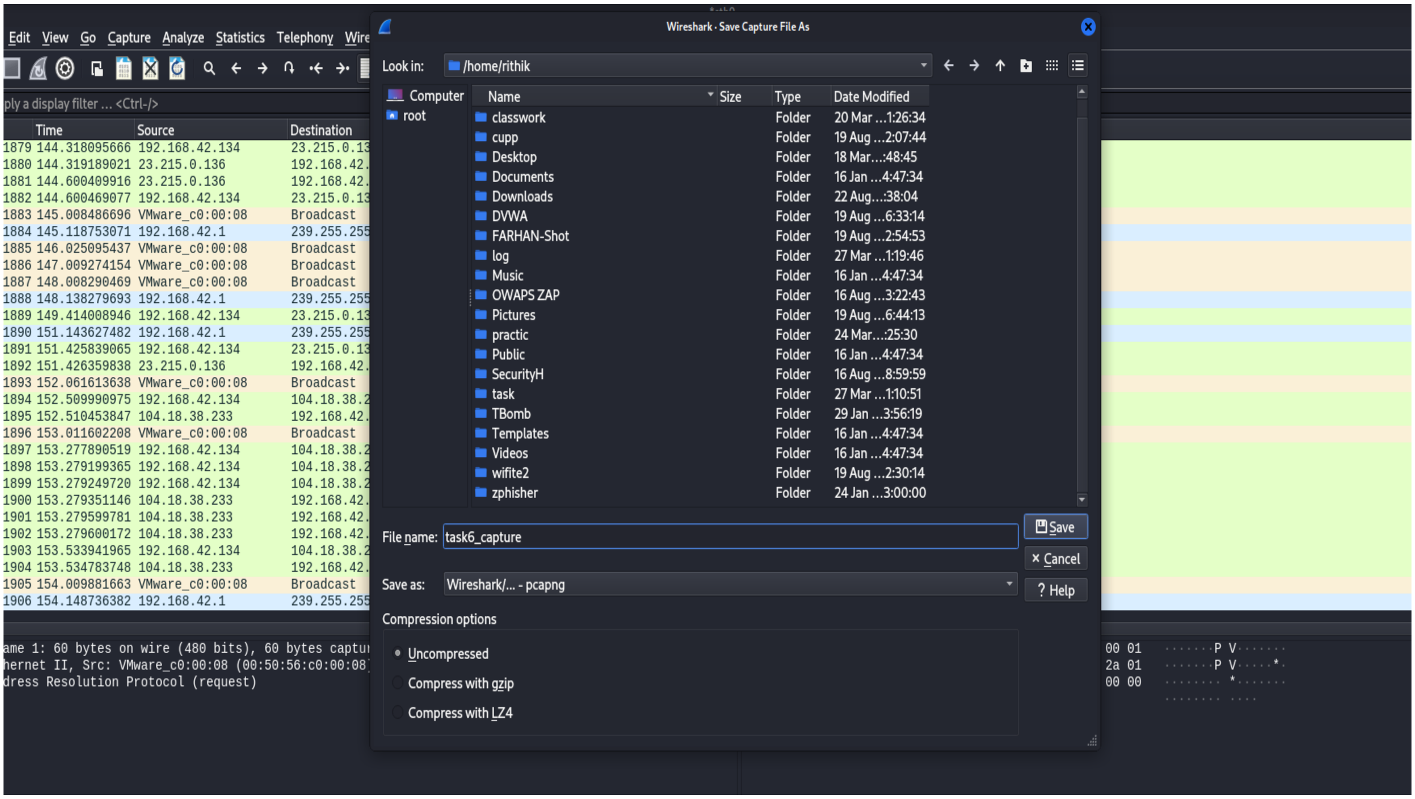
Domain Name System: Protocol | Packets: 1906 · Displayed: 20 (1.0%) · Dropped: 0 (0.0%) | Profile: Default

- *Applied (HTTP) filtered on wireshark*


task6_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time          Source          Destination     Protocol Length Info
   54 14.296397655  192.168.42.134  23.192.228.80   HTTP      431 GET / HTTP/1.1
   60 14.588609885  23.192.228.80   192.168.42.134  HTTP     1032 HTTP/1.1 200 OK  (text/html)
   62 14.703140452  192.168.42.134  23.192.228.80   HTTP      399 GET /favicon.ico HTTP/1.1
   65 15.012193313  23.192.228.80   192.168.42.134  HTTP     1702 HTTP/1.1 404 Not Found  (text/html)
  190 44.319075785  192.168.42.134  23.192.228.80   HTTP      129 GET / HTTP/1.1
  194 44.598192508  23.192.228.80   192.168.42.134  HTTP      112 HTTP/1.1 200 OK  (text/html)
  435 110.356808363 192.168.42.134  104.18.38.233   OCSP      485 Request
  439 110.358274889 192.168.42.134  104.18.38.233   OCSP      485 Request
  445 110.358666904 192.168.42.134  104.18.38.233   OCSP      485 Request
  447 110.359613583 192.168.42.134  104.18.38.233   OCSP      485 Request
  448 110.359916964 192.168.42.134  104.18.38.233   OCSP      485 Request
  453 110.552378859 104.18.38.233   192.168.42.134  OCSP     1342 Response
  455 110.593404025 104.18.38.233   192.168.42.134  OCSP     1342 Response
  457 110.630596233 104.18.38.233   192.168.42.134  OCSP     1342 Response
  459 110.786834410 104.18.38.233   192.168.42.134  OCSP     1342 Response
  461 110.796715269 104.18.38.233   192.168.42.134  OCSP     1342 Response
 1859 139.064745943 192.168.42.134  23.215.0.136    HTTP      399 GET /favicon.ico HTTP/1.1
 1864 139.411123358 23.215.0.136    192.168.42.134  HTTP     1702 HTTP/1.1 404 Not Found  (text/html)
```

- *Capture the packet on wireshark of name(task6_capture).*



```
ply a display filter … <Ctrl-/>
     Time          Source             Destination
1879 144.318095666 192.168.42.134     23.215.0.13
1880 144.319189021 23.215.0.136       192.168.42.
1881 144.600409916 23.215.0.136       192.168.42.
1882 144.600469077 192.168.42.134     23.215.0.13
1883 145.008486696 VMware_c0:00:08    Broadcast
1884 145.118753071 192.168.42.1       239.255.255
1885 146.025095437 VMware_c0:00:08    Broadcast
1886 147.009274154 VMware_c0:00:08    Broadcast
1887 148.008290469 VMware_c0:00:08    Broadcast
1888 148.138279693 192.168.42.1       239.255.255
1889 149.414008946 192.168.42.134     23.215.0.13
1890 151.143627482 192.168.42.1       239.255.255
1891 151.425839065 192.168.42.134     23.215.0.13
1892 151.426359838 23.215.0.136       192.168.42.
1893 152.061613638 VMware_c0:00:08    Broadcast
1894 152.509990975 192.168.42.134     104.18.38.2
1895 152.510453847 104.18.38.233      192.168.42.
1896 153.011602208 VMware_c0:00:08    Broadcast
1897 153.277890519 192.168.42.134     104.18.38.2
1898 153.279199365 192.168.42.134     104.18.38.2
1899 153.279249720 192.168.42.134     104.18.38.2
1900 153.279351146 104.18.38.233      192.168.42.
1901 153.279599781 104.18.38.233      192.168.42.
1902 153.279600172 104.18.38.233      192.168.42.
1903 153.533941965 192.168.42.134     104.18.38.2
1904 153.534783748 104.18.38.233      192.168.42.
1905 154.009881663 VMware_c0:00:08    Broadcast
1906 154.148736382 192.168.42.1       239.255.255

ame 1: 60 bytes on wire (480 bits), 60 bytes captur
hernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08)
dress Resolution Protocol (request)

00 01   ......P V.......
2a 01   ......P V.....*.
00 00   ........ *.......
        ........ ....
```

Wireshark · Save Capture File As

Look in: /home/rithik

Computer
root

Name	Size	Type	Date Modified
classwork		Folder	20 Mar …1:26:34
cupp		Folder	19 Aug …2:07:44
Desktop		Folder	18 Mar…:48:45
Documents		Folder	16 Jan …4:47:34
Downloads		Folder	22 Aug…:38:04
DVWA		Folder	19 Aug …6:33:14
FARHAN-Shot		Folder	19 Aug …2:54:53
log		Folder	27 Mar …1:19:46
Music		Folder	16 Jan …4:47:34
OWAPS ZAP		Folder	16 Aug …3:22:43
Pictures		Folder	19 Aug …6:44:13
practic		Folder	24 Mar…:25:30
Public		Folder	16 Jan …4:47:34
SecurityH		Folder	16 Aug …8:59:59
task		Folder	27 Mar …1:10:51
TBomb		Folder	29 Jan …3:56:19
Templates		Folder	16 Jan …4:47:34
Videos		Folder	16 Jan …4:47:34
wifite2		Folder	19 Aug …2:30:14
zphisher		Folder	24 Jan …3:00:00

File name: task6_capture

Save as: Wireshark/… - pcapng

Compression options

● Uncompressed
○ Compress with gzip
○ Compress with LZ4

Results :-

Protocol	***Observation***	***Security Insight***
HTTP	*Requests to example.com showed GET and response packets.*	*HTTP is unencrypted → sensitive data could be exposed.*
DNS	*Queries for google.com resolved to multiple IPs.*	*DNS traffic is visible; could be spoofed if not secured (DNSSEC recommended).*
TCP	*3-way handshake observed when connecting to websites.*	*Helps confirm secure session establishment.*
UDP	*Found DNS responses over UDP port 53.*	*Lightweight but lacks reliability or encryption.*
ICMP	*Echo requests/replies from ping google.com.*	*Can be abused in DoS attacks.*

Conclusion:-

*Capturing traffic with **Wireshark** provided insights into how different protocols operate on a network. The exercise highlighted that:*

- ***Confidentiality** can be compromised if unencrypted protocols like HTTP are used.*
- ***Integrity** may be at risk if attackers manipulate DNS or TCP streams.*
- ***Availability** can be threatened by ICMP floods or TCP SYN attacks.*

*This hands-on task demonstrates why monitoring traffic is essential for maintaining the **CIA Triad** and securing real-world systems.*