# Task 5

Capture and Analyze Network Traffic Using Wireshark

I perform this task use some basic command.

There are:-

1.http

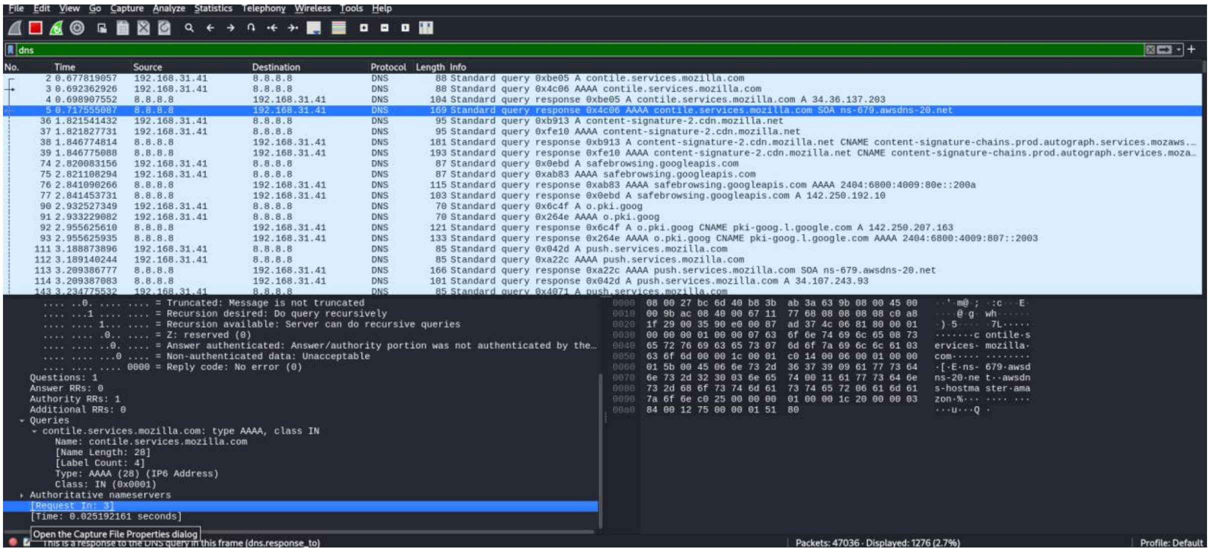
2. udp

3. tcp

4. dns

5.icmp

6.ssl/tls


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

```
No.   Time        Source          Destination     Protocol Length Info
    2 0.677819057 192.168.31.41   8.8.8.8         DNS       88 Standard query 0xbe05 A contile.services.mozilla.com
    3 0.692362926 192.168.31.41   8.8.8.8         DNS       88 Standard query 0x4c06 AAAA contile.services.mozilla.com
    4 0.698907552 8.8.8.8         192.168.31.41   DNS      104 Standard query response 0xbe05 A contile.services.mozilla.com A 34.36.137.203
    5 0.717555087 8.8.8.8         192.168.31.41   DNS      169 Standard query response 0x4c06 AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net
   36 1.821541432 192.168.31.41   8.8.8.8         DNS       95 Standard query 0xb913 A content-signature-2.cdn.mozilla.net
   37 1.821827731 192.168.31.41   8.8.8.8         DNS       95 Standard query 0xfe10 AAAA content-signature-2.cdn.mozilla.net
   38 1.846774814 8.8.8.8         192.168.31.41   DNS      181 Standard query response 0xb913 A content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.services.mozaws.…
   39 1.846775088 8.8.8.8         192.168.31.41   DNS      193 Standard query response 0xfe10 AAAA content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.services.moza…
   74 2.820083156 192.168.31.41   8.8.8.8         DNS       87 Standard query 0x0ebd A safebrowsing.googleapis.com
   75 2.821108294 192.168.31.41   8.8.8.8         DNS       87 Standard query 0xab83 AAAA safebrowsing.googleapis.com
   76 2.841090266 8.8.8.8         192.168.31.41   DNS      115 Standard query response 0xab83 AAAA safebrowsing.googleapis.com AAAA 2404:6800:4009:80e::200a
   77 2.841453731 8.8.8.8         192.168.31.41   DNS      103 Standard query response 0x0ebd A safebrowsing.googleapis.com A 142.250.192.10
   90 2.932527349 192.168.31.41   8.8.8.8         DNS       70 Standard query 0x6c4f A o.pki.goog
   91 2.933229082 192.168.31.41   8.8.8.8         DNS       70 Standard query 0x264e AAAA o.pki.goog
   92 2.955625610 8.8.8.8         192.168.31.41   DNS      121 Standard query response 0x6c4f A o.pki.goog CNAME pki-goog.l.google.com A 142.250.207.163
   93 2.955625935 8.8.8.8         192.168.31.41   DNS      133 Standard query response 0x264e AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4009:807::2003
  111 3.188873896 192.168.31.41   8.8.8.8         DNS       85 Standard query 0x042d A push.services.mozilla.com
  112 3.189140244 192.168.31.41   8.8.8.8         DNS       85 Standard query 0xa22c AAAA push.services.mozilla.com
  113 3.209386777 8.8.8.8         192.168.31.41   DNS      166 Standard query response 0xa22c AAAA push.services.mozilla.com SOA ns-679.awsdns-20.net
  114 3.209387083 8.8.8.8         192.168.31.41   DNS      101 Standard query response 0x042d A push.services.mozilla.com A 34.107.243.93
  143 3.234775532 192.168.31.41   8.8.8.8         DNS       85 Standard query 0x4071 A push.services.mozilla.com
```

```
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the…
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  ▾ Queries
    ▾ contile.services.mozilla.com: type AAAA, class IN
        Name: contile.services.mozilla.com
        [Name Length: 28]
        [Label Count: 4]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  ▸ Authoritative nameservers
    [Request In: 3]
    [Time: 0.025192161 seconds]
```

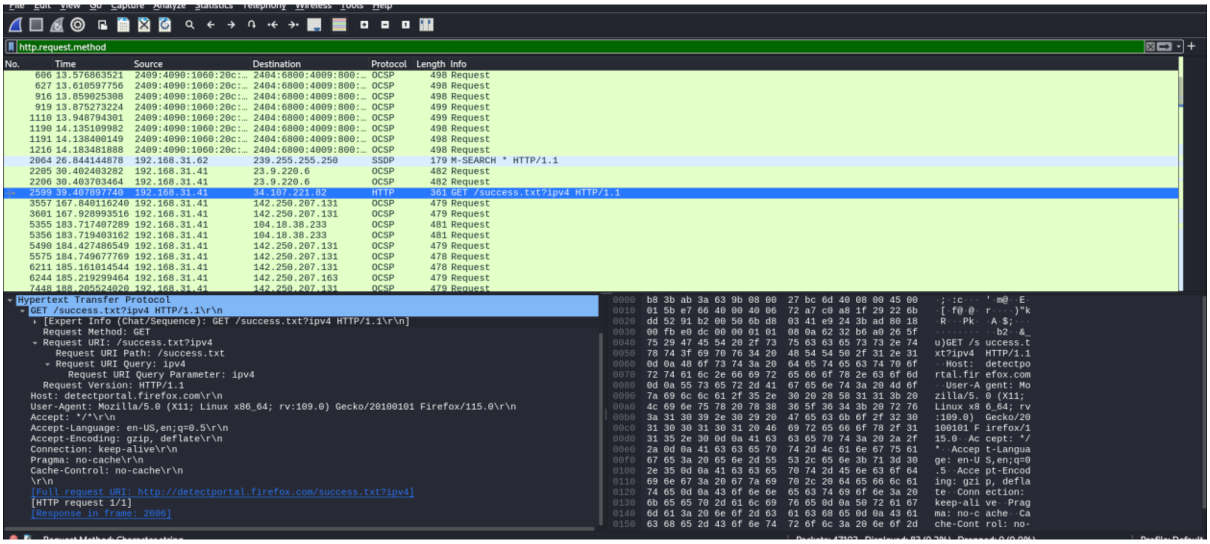
```
0000  08 00 27 bc 6d 40 b8 3b  ab 3a 63 9b 08 00 45 00   ··'·m@·; ·:c···E·
0010  00 9b ac 08 40 00 67 11  77 68 08 08 08 08 c0 a8   ····@·g· wh······
0020  1f 29 00 35 90 e0 00 87  ad 37 4c 06 81 80 00 01   ·)·5···· ·7L·····
0030  00 00 00 01 00 00 07 63  6f 6e 74 69 6c 65 08 73   ·······c ontile·s
0040  65 72 76 69 63 65 73 07  6d 6f 7a 69 6c 6c 61 03   ervices· mozilla·
0050  63 6f 6d 00 00 1c 00 01  c0 14 00 06 00 01 00 00   com····· ········
0060  01 5b 00 45 06 6e 73 2d  36 37 39 09 61 77 73 64   ·[·E·ns- 679·awsd
0070  6e 73 2d 32 30 03 6e 65  74 00 11 61 77 73 64 6e   ns-20·ne t··awsdn
0080  73 2d 68 6f 73 74 6d 61  73 74 65 72 06 61 6d 61   s-hostma ster·ama
0090  7a 6f 6e c0 25 00 00 00  01 00 00 1c 20 00 00 03   zon·%··· ···· ···
00a0  84 00 12 75 00 00 01 51  80                        ···u···Q ·
```

Open the Capture File Properties dialog

This is a response to the DNS query in this frame (dns.response_to)

Packets: 47036 · Displayed: 1276 (2.7%)

Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method

```
No.   Time          Source               Destination          Protocol Length Info
  606 13.576863521  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     498 Request
  627 13.610597756  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     498 Request
  916 13.859025308  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     498 Request
  919 13.875273224  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     499 Request
 1110 13.948794301  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     499 Request
 1190 14.135109982  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     498 Request
 1191 14.138400149  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     498 Request
 1216 14.183481888  2409:4090:1060:20c:… 2404:6800:4009:800:… OCSP     498 Request
 2064 26.844144878  192.168.31.62        239.255.255.250      SSDP     179 M-SEARCH * HTTP/1.1
 2205 30.402403282  192.168.31.41        23.9.220.6           OCSP     482 Request
 2206 30.403703464  192.168.31.41        23.9.220.6           OCSP     482 Request
 2599 39.407897740  192.168.31.41        34.107.221.82        HTTP     361 GET /success.txt?ipv4 HTTP/1.1
 3557 167.840116240 192.168.31.41        142.250.207.131      OCSP     479 Request
 3601 167.928993516 192.168.31.41        142.250.207.131      OCSP     479 Request
 5355 183.717407289 192.168.31.41        104.18.38.233        OCSP     481 Request
 5356 183.719403162 192.168.31.41        104.18.38.233        OCSP     481 Request
 5490 184.427486549 192.168.31.41        142.250.207.131      OCSP     479 Request
 5575 184.749677769 192.168.31.41        142.250.207.131      OCSP     478 Request
 6211 185.161014544 192.168.31.41        142.250.207.131      OCSP     478 Request
 6244 185.219299464 192.168.31.41        142.250.207.163      OCSP     479 Request
 7448 188.205524020 192.168.31.41        142.250.207.131      OCSP     479 Request
```

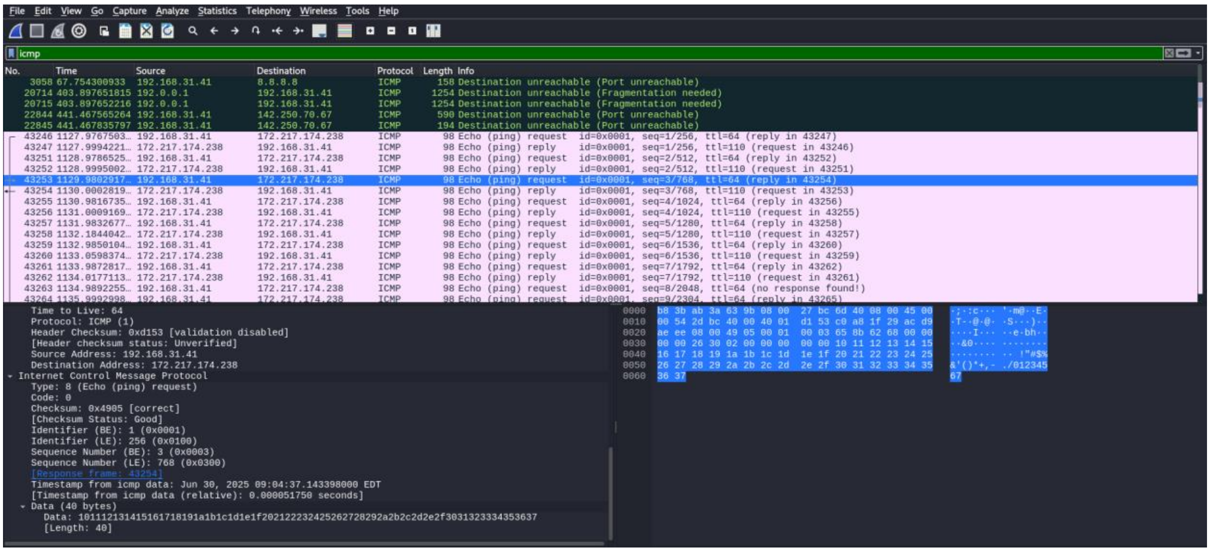
```
▾ Hypertext Transfer Protocol
  ▾ GET /success.txt?ipv4 HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /success.txt?ipv4 HTTP/1.1\r\n]
      Request Method: GET
    ▾ Request URI: /success.txt?ipv4
        Request URI Path: /success.txt
      ▾ Request URI Query: ipv4
          Request URI Query Parameter: ipv4
      Request Version: HTTP/1.1
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://detectportal.firefox.com/success.txt?ipv4]
    [HTTP request 1/1]
    [Response in frame: 2606]
```

```
0000  b8 3b ab 3a 63 9b 08 00  27 bc 6d 40 08 00 45 00   ·;·:c··· '·m@··E·
0010  01 5b e7 66 40 00 40 06  72 a7 c0 a8 1f 29 22 6b   ·[·f@·@· r····)"k
0020  dd 52 91 b2 00 50 6b d8  03 41 e9 24 3b ad 80 18   ·R···Pk· ·A·$;···
0030  00 fb e0 dc 00 00 01 01  08 0a 62 32 b6 a0 26 5f   ········ ··b2··&_
0040  75 29 47 45 54 20 2f 73  75 63 63 65 73 73 2e 74   u)GET /s uccess.t
0050  78 74 3f 69 70 76 34 20  48 54 54 50 2f 31 2e 31   xt?ipv4  HTTP/1.1
0060  0d 0a 48 6f 73 74 3a 20  64 65 74 65 63 74 70 6f   ··Host:  detectpo
0070  72 74 61 6c 2e 66 69 72  65 66 6f 78 2e 63 6f 6d   rtal.fir efox.com
0080  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0090  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3b 20   zilla/5. 0 (X11;
00a0  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
00b0  3a 31 30 39 2e 30 29 20  47 65 63 6b 6f 2f 32 30   :109.0)  Gecko/20
00c0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 31   100101 F irefox/1
00d0  31 35 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   15.0··Ac cept: */
00e0  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *··Accep t-Langua
00f0  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0100  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod
0110  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0120  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   te··Conn ection:
0130  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 50 72 61 67   keep-ali ve··Prag
0140  6d 61 3a 20 6e 6f 2d 63  61 63 68 65 0d 0a 43 61   ma: no-c ache··Ca
0150  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6e 6f 2d   che-Cont rol: no-
```

Request Method: Character string

Packets: 47103 · Displayed: 83 (0.2%) · Dropped: 0 (0.0%)

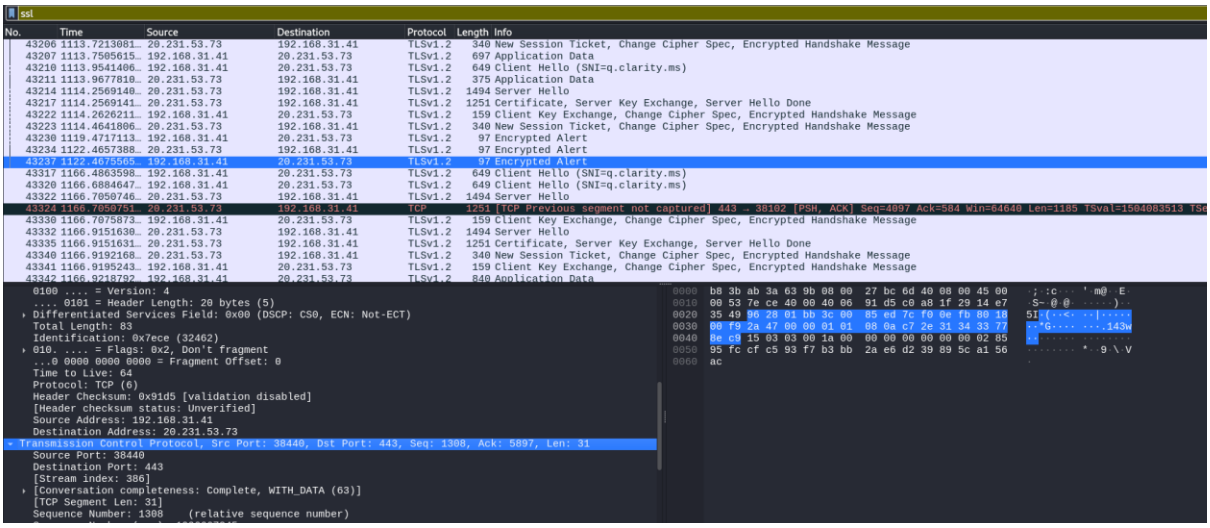
Profile: Default



```
No.       Time           Source            Destination       Protocol  Length Info
    3058 67.754300933   192.168.31.41     8.8.8.8           ICMP       158 Destination unreachable (Port unreachable)
   20714 403.897651815  192.0.0.1         192.168.31.41     ICMP      1254 Destination unreachable (Fragmentation needed)
   20715 403.897652216  192.0.0.1         192.168.31.41     ICMP      1254 Destination unreachable (Fragmentation needed)
   22844 441.467565264  192.168.31.41     142.250.70.67     ICMP       590 Destination unreachable (Port unreachable)
   22845 441.467835797  192.168.31.41     142.250.70.67     ICMP       194 Destination unreachable (Port unreachable)
   43246 1127.9767503…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (reply in 43247)
   43247 1127.9994221…  172.217.174.238   192.168.31.41     ICMP        98 Echo (ping) reply    id=0x0001, seq=1/256, ttl=110 (request in 43246)
   43251 1128.9786525…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (reply in 43252)
   43252 1128.9995002…  172.217.174.238   192.168.31.41     ICMP        98 Echo (ping) reply    id=0x0001, seq=2/512, ttl=110 (request in 43251)
   43253 1129.9802917…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (reply in 43254)
   43254 1130.0002819…  172.217.174.238   192.168.31.41     ICMP        98 Echo (ping) reply    id=0x0001, seq=3/768, ttl=110 (request in 43253)
   43255 1130.9816735…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (reply in 43256)
   43256 1131.0009169…  172.217.174.238   192.168.31.41     ICMP        98 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=110 (request in 43255)
   43257 1131.9832677…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (reply in 43258)
   43258 1132.1844042…  172.217.174.238   192.168.31.41     ICMP        98 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=110 (request in 43257)
   43259 1132.9850104…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (reply in 43260)
   43260 1133.0598374…  172.217.174.238   192.168.31.41     ICMP        98 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=110 (request in 43259)
   43261 1133.9872817…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=7/1792, ttl=64 (reply in 43262)
   43262 1134.0177113…  172.217.174.238   192.168.31.41     ICMP        98 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=110 (request in 43261)
   43263 1134.9892255…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=8/2048, ttl=64 (no response found!)
   43264 1135.9992998…  192.168.31.41     172.217.174.238   ICMP        98 Echo (ping) request  id=0x0001, seq=9/2304, ttl=64 (reply in 43265)
```

```
      Time to Live: 64
      Protocol: ICMP (1)
      Header Checksum: 0xd153 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.31.41
      Destination Address: 172.217.174.238
  ▾ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x4905 [correct]
      [Checksum Status: Good]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 3 (0x0003)
      Sequence Number (LE): 768 (0x0300)
      [Response frame: 43254]
      Timestamp from icmp data: Jun 30, 2025 09:04:37.143398000 EDT
      [Timestamp from icmp data (relative): 0.000051750 seconds]
    ▾ Data (40 bytes)
        Data: 101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
        [Length: 40]
```

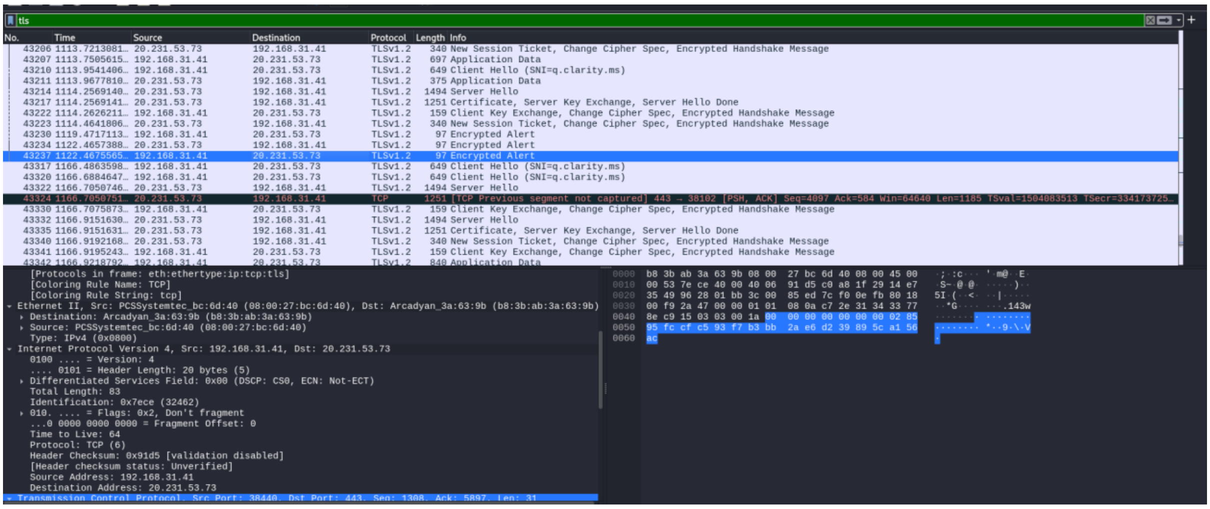
```
0000  b8 3b ab 3a 63 9b 08 00  27 bc 6d 40 08 00 45 00   ·;·:c··· '·m@··E·
0010  00 54 2d bc 40 00 40 01  d1 53 c0 a8 1f 29 ac d9   ·T-·@·@· ·S···)··
0020  ae ee 08 00 49 05 00 01  00 03 65 8b 62 68 00 00   ····I··· ··e·bh··
0030  00 00 26 30 02 00 00 00  00 00 10 11 12 13 14 15   ··&0···· ········
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
```



```
No.       Time           Source            Destination       Protocol  Length Info
   43206 1113.7213081…  20.231.53.73      192.168.31.41     TLSv1.2    340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   43207 1113.7505615…  192.168.31.41     20.231.53.73      TLSv1.2    697 Application Data
   43210 1113.9541406…  192.168.31.41     20.231.53.73      TLSv1.2    649 Client Hello (SNI=q.clarity.ms)
   43211 1113.9677810…  20.231.53.73      192.168.31.41     TLSv1.2    375 Application Data
   43214 1114.2569140…  20.231.53.73      192.168.31.41     TLSv1.2   1494 Server Hello
   43217 1114.2569141…  20.231.53.73      192.168.31.41     TLSv1.2   1251 Certificate, Server Key Exchange, Server Hello Done
   43222 1114.2626211…  192.168.31.41     20.231.53.73      TLSv1.2    159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   43223 1114.4641806…  20.231.53.73      192.168.31.41     TLSv1.2    340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   43230 1119.4717113…  192.168.31.41     20.231.53.73      TLSv1.2     97 Encrypted Alert
   43234 1122.4657388…  20.231.53.73      192.168.31.41     TLSv1.2     97 Encrypted Alert
   43237 1122.4675565…  192.168.31.41     20.231.53.73      TLSv1.2     97 Encrypted Alert
   43317 1166.4863598…  192.168.31.41     20.231.53.73      TLSv1.2    649 Client Hello (SNI=q.clarity.ms)
   43320 1166.6884647…  192.168.31.41     20.231.53.73      TLSv1.2    649 Client Hello (SNI=q.clarity.ms)
   43322 1166.7050746…  20.231.53.73      192.168.31.41     TLSv1.2   1494 Server Hello
   43324 1166.7050751…  20.231.53.73      192.168.31.41     TCP       1251 [TCP Previous segment not captured] 443 → 38102 [PSH, ACK] Seq=4097 Ack=584 Win=64640 Len=1185 TSval=1504083513 TSe
   43330 1166.7075873…  192.168.31.41     20.231.53.73      TLSv1.2    159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   43332 1166.9151630…  20.231.53.73      192.168.31.41     TLSv1.2   1494 Server Hello
   43335 1166.9151631…  20.231.53.73      192.168.31.41     TLSv1.2   1251 Certificate, Server Key Exchange, Server Hello Done
   43340 1166.9192168…  20.231.53.73      192.168.31.41     TLSv1.2    340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
   43341 1166.9195243…  192.168.31.41     20.231.53.73      TLSv1.2    159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   43342 1166.9218792…  192.168.31.41     20.231.53.73      TLSv1.2    840 Application Data
```

```
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 83
      Identification: 0x7ece (32462)
    ▸ 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0x91d5 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.31.41
      Destination Address: 20.231.53.73
  ▾ Transmission Control Protocol, Src Port: 38440, Dst Port: 443, Seq: 1308, Ack: 5897, Len: 31
      Source Port: 38440
      Destination Port: 443
      [Stream index: 386]
    ▸ [Conversation completeness: Complete, WITH_DATA (63)]
      [TCP Segment Len: 31]
      Sequence Number: 1308    (relative sequence number)
```

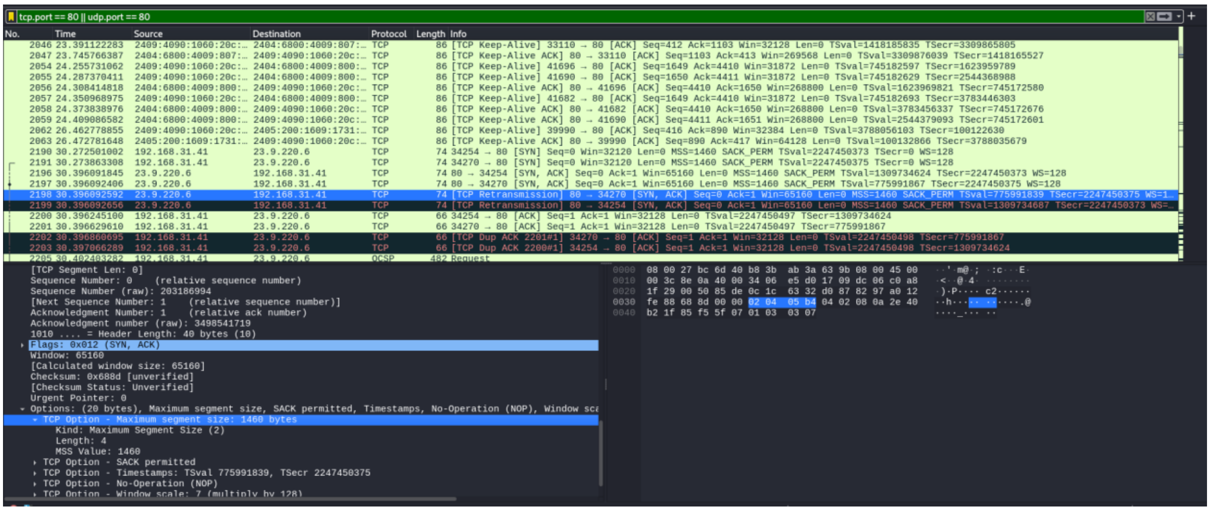
```
0000  b8 3b ab 3a 63 9b 08 00  27 bc 6d 40 08 00 45 00   ·;·:c··· '·m@··E·
0010  00 53 7e ce 40 00 40 06  91 d5 c0 a8 1f 29 14 e7   ·S~·@·@· ·····)··
0020  35 49 96 28 01 bb 3c 00  85 ed 7c f0 0e fb 80 18   5I·(··<· ··|·····
0030  00 f9 2a 47 00 00 01 01  08 0a c7 2e 31 34 33 77   ··*G···· ····.143w
0040  8e c9 15 03 03 00 1a 00  00 00 00 00 00 00 02 85   ········ ········
0050  95 fc cf c5 93 f7 b3 bb  2a e6 d2 39 89 5c a1 56   ········ *··9·\·V
0060  ac                                                 ·
```



```
tls
No.   Time            Source          Destination     Protocol Length Info
43206 1113.7213081…   20.231.53.73    192.168.31.41   TLSv1.2   340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
43207 1113.7505615…   192.168.31.41   20.231.53.73    TLSv1.2   697 Application Data
43210 1113.9541406…   192.168.31.41   20.231.53.73    TLSv1.2   649 Client Hello (SNI=q.clarity.ms)
43211 1113.9677810…   20.231.53.73    192.168.31.41   TLSv1.2   375 Application Data
43214 1114.2569140…   20.231.53.73    192.168.31.41   TLSv1.2  1494 Server Hello
43217 1114.2569141…   20.231.53.73    192.168.31.41   TLSv1.2  1251 Certificate, Server Key Exchange, Server Hello Done
43222 1114.2626211…   192.168.31.41   20.231.53.73    TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
43223 1114.4641806…   20.231.53.73    192.168.31.41   TLSv1.2   340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
43230 1119.4717113…   192.168.31.41   20.231.53.73    TLSv1.2    97 Encrypted Alert
43234 1122.4657388…   20.231.53.73    192.168.31.41   TLSv1.2    97 Encrypted Alert
43237 1122.4675565…   192.168.31.41   20.231.53.73    TLSv1.2    97 Encrypted Alert
43317 1166.4863598…   192.168.31.41   20.231.53.73    TLSv1.2   649 Client Hello (SNI=q.clarity.ms)
43320 1166.6884647…   192.168.31.41   20.231.53.73    TLSv1.2   649 Client Hello (SNI=q.clarity.ms)
43322 1166.7050746…   20.231.53.73    192.168.31.41   TLSv1.2  1494 Server Hello
43324 1166.7050751…   20.231.53.73    192.168.31.41   TCP      1251 [TCP Previous segment not captured] 443 → 38102 [PSH, ACK] Seq=4097 Ack=584 Win=64640 Len=1185 TSval=1504083513 TSecr=334173725…
43330 1166.7075873…   192.168.31.41   20.231.53.73    TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
43332 1166.9151630…   20.231.53.73    192.168.31.41   TLSv1.2  1494 Server Hello
43335 1166.9151631…   20.231.53.73    192.168.31.41   TLSv1.2  1251 Certificate, Server Key Exchange, Server Hello Done
43340 1166.9192168…   20.231.53.73    192.168.31.41   TLSv1.2   340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
43341 1166.9195243…   192.168.31.41   20.231.53.73    TLSv1.2   159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
43342 1166.9218792…   192.168.31.41   20.231.53.73    TLSv1.2   840 Application Data
```

```
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
▾ Ethernet II, Src: PCSSystemtec_bc:6d:40 (08:00:27:bc:6d:40), Dst: Arcadyan_3a:63:9b (b8:3b:ab:3a:63:9b)
  ▸ Destination: Arcadyan_3a:63:9b (b8:3b:ab:3a:63:9b)
  ▸ Source: PCSSystemtec_bc:6d:40 (08:00:27:bc:6d:40)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.31.41, Dst: 20.231.53.73
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 83
    Identification: 0x7ece (32462)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x91d5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.31.41
    Destination Address: 20.231.53.73
▾ Transmission Control Protocol, Src Port: 38440, Dst Port: 443, Seq: 1308, Ack: 5897, Len: 31
```

```
0000  b8 3b ab 3a 63 9b 08 00  27 bc 6d 40 08 00 45 00   ·;·:c···  '·m@··E·
0010  00 53 7e ce 40 00 40 06  91 d5 c0 a8 1f 29 14 e7   ·S~·@·@·  ·····)··
0020  35 49 96 28 01 bb 3c 00  85 ed 7c f0 0e fb 80 18   5I·(··<·  ··|·····
0030  00 f9 2a 47 00 00 01 01  08 0a c7 2e 31 34 33 77   ··*G····  ····.143w
0040  8e c9 15 03 03 00 1a 00  00 00 00 00 00 00 02 85   ········  ········
0050  95 fc cf c5 93 f7 b3 bb  2a e6 d2 39 89 5c a1 56   ········  *··9·\·V
0060  ac                                                 ·
```



```
tcp.port == 80 || udp.port == 80
No.  Time          Source               Destination          Protocol Length Info
2046 23.391122283  2409:4090:1060:20c:… 2404:6800:4009:807:… TCP    86 [TCP Keep-Alive] 33110 → 80 [ACK] Seq=412 Ack=1103 Win=32128 Len=0 TSval=1418185835 TSecr=3309865805
2047 23.745766387  2404:6800:4009:807:… 2409:4090:1060:20c:… TCP    86 [TCP Keep-Alive ACK] 80 → 33110 [ACK] Seq=1103 Ack=413 Win=269568 Len=0 TSval=3309876039 TSecr=1418165527
2054 24.255731062  2409:4090:1060:20c:… 2404:6800:4009:800:… TCP    86 [TCP Keep-Alive] 41696 → 80 [ACK] Seq=1649 Ack=4410 Win=31872 Len=0 TSval=745182597 TSecr=1623959789
2055 24.287370411  2409:4090:1060:20c:… 2404:6800:4009:800:… TCP    86 [TCP Keep-Alive] 41690 → 80 [ACK] Seq=1650 Ack=4411 Win=31872 Len=0 TSval=745182629 TSecr=2544368988
2056 24.308414818  2404:6800:4009:800:… 2409:4090:1060:20c:… TCP    86 [TCP Keep-Alive ACK] 80 → 41696 [ACK] Seq=4410 Ack=1650 Win=268800 Len=0 TSval=1623969821 TSecr=745172580
2057 24.350968975  2409:4090:1060:20c:… 2404:6800:4009:800:… TCP    86 [TCP Keep-Alive] 41682 → 80 [ACK] Seq=1649 Ack=4410 Win=31872 Len=0 TSval=745182693 TSecr=3783446303
2058 24.373838976  2404:6800:4009:800:… 2409:4090:1060:20c:… TCP    86 [TCP Keep-Alive ACK] 80 → 41682 [ACK] Seq=4410 Ack=1650 Win=268800 Len=0 TSval=3783456337 TSecr=745172676
2059 24.409086582  2404:6800:4009:800:… 2409:4090:1060:20c:… TCP    86 [TCP Keep-Alive ACK] 80 → 41690 [ACK] Seq=4411 Ack=1651 Win=268800 Len=0 TSval=2544379093 TSecr=745172601
2062 26.462778855  2409:4090:1060:20c:… 2405:200:1609:1731:… TCP    86 [TCP Keep-Alive] 39990 → 80 [ACK] Seq=416 Ack=890 Win=32384 Len=0 TSval=3788056103 TSecr=100122630
2063 26.472781648  2405:200:1609:1731:… 2409:4090:1060:20c:… TCP    86 [TCP Keep-Alive ACK] 80 → 39990 [ACK] Seq=890 Ack=417 Win=64128 Len=0 TSval=100132866 TSecr=3788035679
2190 30.272501002  192.168.31.41        23.9.220.6           TCP    74 34254 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2247450373 TSecr=0 WS=128
2191 30.273863308  192.168.31.41        23.9.220.6           TCP    74 34270 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2247450375 TSecr=0 WS=128
2196 30.396091845  23.9.220.6           192.168.31.41        TCP    74 80 → 34254 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1309734624 TSecr=2247450373 WS=128
2197 30.396092406  23.9.220.6           192.168.31.41        TCP    74 80 → 34270 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=775991867 TSecr=2247450375 WS=128
2198 30.396092592  23.9.220.6           192.168.31.41        TCP    74 [TCP Retransmission] 80 → 34270 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=775991839 TSecr=2247450375 WS=1…
2199 30.396092656  23.9.220.6           192.168.31.41        TCP    74 [TCP Retransmission] 80 → 34254 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1309734687 TSecr=2247450373 WS=…
2200 30.396245100  192.168.31.41        23.9.220.6           TCP    66 34254 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2247450497 TSecr=1309734624
2201 30.396629610  192.168.31.41        23.9.220.6           TCP    66 34270 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2247450497 TSecr=775991867
2202 30.396860695  192.168.31.41        23.9.220.6           TCP    66 [TCP Dup ACK 2201#1] 34270 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2247450498 TSecr=775991867
2203 30.397066289  192.168.31.41        23.9.220.6           TCP    66 [TCP Dup ACK 2200#1] 34254 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2247450498 TSecr=1309734624
2205 30.402403282  192.168.31.41        23.9.220.6           OCSP  482 Request
```

```
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 203186994
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3498541719
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x012 (SYN, ACK)
    Window: 65160
    [Calculated window size: 65160]
    Checksum: 0x688d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window sca
    ▾ TCP Option - Maximum segment size: 1460 bytes
        Kind: Maximum Segment Size (2)
        Length: 4
        MSS Value: 1460
    ▸ TCP Option - SACK permitted
    ▸ TCP Option - Timestamps: TSval 775991839, TSecr 2247450375
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - Window scale: 7 (multiply by 128)
```

```
0000  08 00 27 bc 6d 40 b8 3b  ab 3a 63 9b 08 00 45 00   ··'·m@·;  ·:c···E·
0010  00 3c 8e 0a 40 00 34 06  e5 d0 17 09 dc 06 c0 a8   ·<··@·4·  ········
0020  1f 29 00 50 85 de 0c 1c  63 32 d0 87 82 97 a0 12   ·)·P····  c2······
0030  fe 88 68 8d 00 00 02 04  05 b4 04 02 08 0a 2e 40   ··h·····  ······.@
0040  b2 1f 85 f5 5f 07 01 03  03 07                     ····_···  ··
```

Conclusion:- In this task  I use the Wireshark in the kali Linux and capturing the  network traffic and perform the some basics commands.