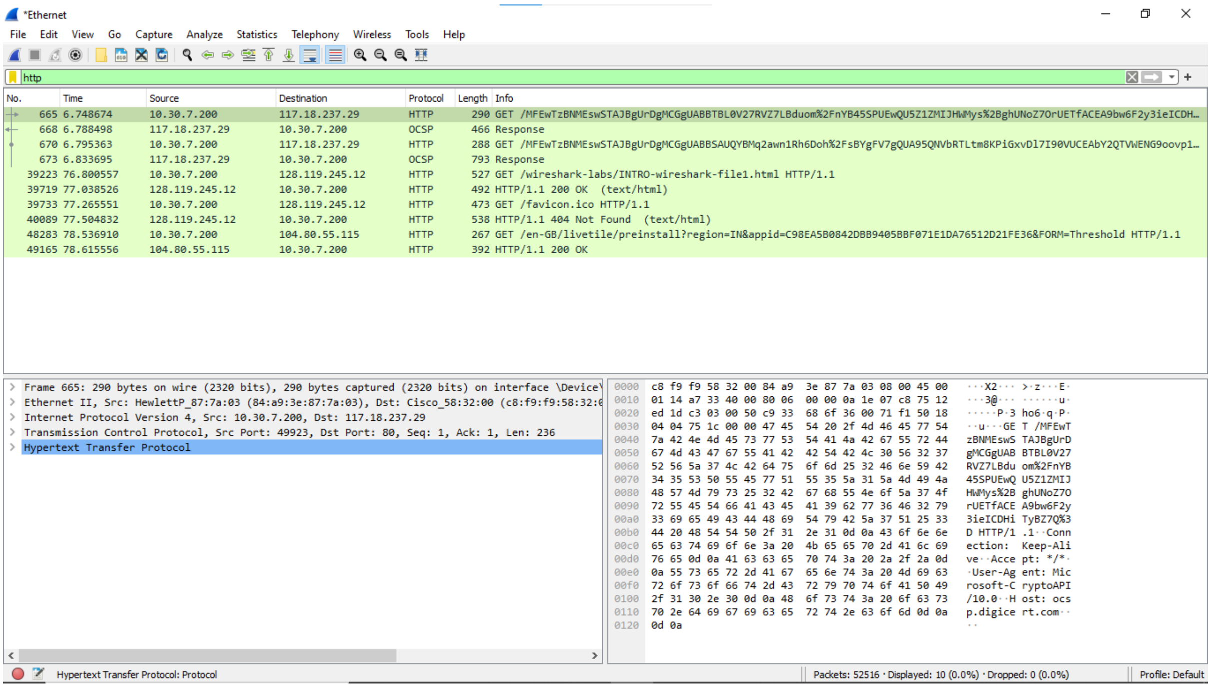
NAME: JANAKAR PATEL
ROLL NO: 20BIT061

Experiment 1:

Aim: To Study about wire-shark and packet tracer tools.

Task 1: To study and understand wireshark tools through hands-on.

Question 1: HTTP:


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

http

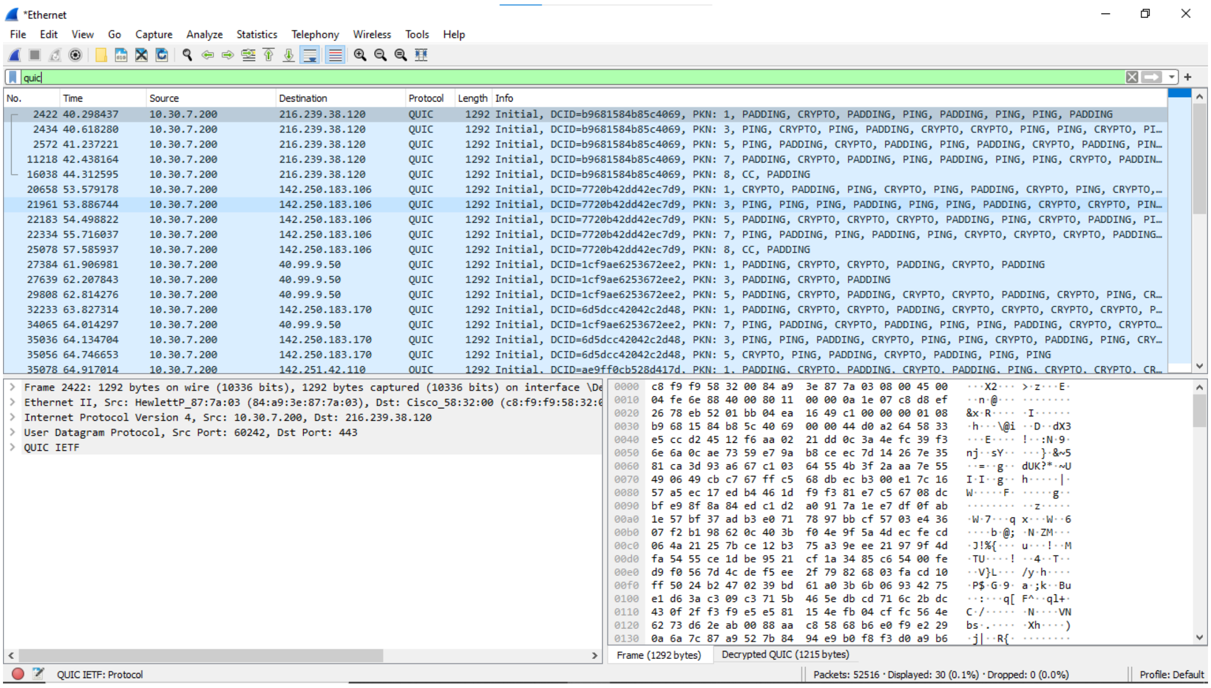
```
No.     Time       Source          Destination     Protocol Length Info
  665 6.748674   10.30.7.200     117.18.237.29   HTTP     290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA9bw6F2y3ieICDH…
  668 6.788498   117.18.237.29   10.30.7.200     OCSP     466 Response
  670 6.795363   10.30.7.200     117.18.237.29   HTTP     288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAbY2QTVWENG9oovp1…
  673 6.833695   117.18.237.29   10.30.7.200     OCSP     793 Response
39223 76.800557  10.30.7.200     128.119.245.12  HTTP     527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
39719 77.038526  128.119.245.12  10.30.7.200     HTTP     492 HTTP/1.1 200 OK  (text/html)
39733 77.265551  10.30.7.200     128.119.245.12  HTTP     473 GET /favicon.ico HTTP/1.1
40089 77.504832  128.119.245.12  10.30.7.200     HTTP     538 HTTP/1.1 404 Not Found  (text/html)
48283 78.536910  10.30.7.200     104.80.55.115   HTTP     267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
49165 78.615556  104.80.55.115   10.30.7.200     HTTP     392 HTTP/1.1 200 OK
```

```
> Frame 665: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface \Device\
> Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:(
> Internet Protocol Version 4, Src: 10.30.7.200, Dst: 117.18.237.29
> Transmission Control Protocol, Src Port: 49923, Dst Port: 80, Seq: 1, Ack: 1, Len: 236
> Hypertext Transfer Protocol
```

```
0000  c8 f9 f9 58 32 00 84 a9  3e 87 7a 03 08 00 45 00   ···X2··· >·z···E·
0010  01 14 a7 33 40 00 80 06  00 00 0a 1e 07 c8 75 12   ···3@··· ······u·
0020  ed 1d c3 03 00 50 c9 33  68 6f 36 00 71 f1 50 18   ·····P·3 ho6·q·P·
0030  04 04 75 1c 00 00 47 45  54 20 2f 4d 46 45 77 54   ··u···GE T /MFEwT
0040  7a 42 4e 4d 45 73 77 53  54 41 4a 42 67 55 72 44   zBNMEswS TAJBgUrD
0050  67 4d 43 47 67 55 41 42  42 54 42 4c 30 56 32 37   gMCGgUAB BTBL0V27
0060  52 56 5a 37 4c 42 64 75  6f 6d 25 32 46 6e 59 42   RVZ7LBdu om%2FnYB
0070  34 35 53 50 55 45 77 51  55 35 5a 31 5a 4d 49 4a   45SPUEwQ U5Z1ZMIJ
0080  48 57 4d 79 73 25 32 42  67 68 55 4e 6f 5a 37 4f   HWMys%2B ghUNoZ7O
0090  72 55 45 54 66 41 43 45  41 39 62 77 36 46 32 79   rUETfACE A9bw6F2y
00a0  33 69 65 49 43 44 48 69  54 79 42 5a 37 51 25 33   3ieICDHi TyBZ7Q%3
00b0  44 20 48 54 54 50 2f 31  2e 31 0d 0a 43 6f 6e 6e   D HTTP/1 .1··Conn
00c0  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
00d0  76 65 0d 0a 41 63 63 65  70 74 3a 20 2a 2f 2a 0d   ve··Acce pt: */*·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 69 63   ·User-Ag ent: Mic
00f0  72 6f 73 6f 66 74 2d 43  72 79 70 74 6f 41 50 49   rosoft-C ryptoAPI
0100  2f 31 30 2e 30 0d 0a 48  6f 73 74 3a 20 6f 63 73   /10.0··H ost: ocs
0110  70 2e 64 69 67 69 63 65  72 74 2e 63 6f 6d 0d 0a   p.digice rt.com··
0120  0d 0a                                              ··
```

Hypertext Transfer Protocol: Protocol | Packets: 52516 · Displayed: 10 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

QUIC:


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

quic

```
No.     Time       Source          Destination     Protocol Length Info
 2422 40.298437  10.30.7.200     216.239.38.120  QUIC     1292 Initial, DCID=b9681584b85c4069, PKN: 1, PADDING, CRYPTO, PADDING, PING, PADDING, PING, PING, PADDING
 2434 40.618280  10.30.7.200     216.239.38.120  QUIC     1292 Initial, DCID=b9681584b85c4069, PKN: 3, PING, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, PING, PING, CRYPTO, PI…
 2572 41.237221  10.30.7.200     216.239.38.120  QUIC     1292 Initial, DCID=b9681584b85c4069, PKN: 5, PING, PADDING, CRYPTO, PADDING, PING, PADDING, CRYPTO, PADDING, PIN…
11218 42.438164  10.30.7.200     216.239.38.120  QUIC     1292 Initial, DCID=b9681584b85c4069, PKN: 7, PADDING, CRYPTO, PADDING, PING, PADDING, PING, PING, CRYPTO, PADDIN…
16038 44.312595  10.30.7.200     216.239.38.120  QUIC     1292 Initial, DCID=b9681584b85c4069, PKN: 8, CC, PADDING
20658 53.579178  10.30.7.200     142.250.183.106 QUIC     1292 Initial, DCID=7720b42dd42ec7d9, PKN: 1, CRYPTO, PADDING, PING, CRYPTO, PING, PADDING, CRYPTO, PING, CRYPTO,…
21961 53.886744  10.30.7.200     142.250.183.106 QUIC     1292 Initial, DCID=7720b42dd42ec7d9, PKN: 3, PING, PING, PING, PADDING, PING, PING, PADDING, CRYPTO, CRYPTO, PIN…
22183 54.498822  10.30.7.200     142.250.183.106 QUIC     1292 Initial, DCID=7720b42dd42ec7d9, PKN: 5, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PADDING, PI…
22334 55.716037  10.30.7.200     142.250.183.106 QUIC     1292 Initial, DCID=7720b42dd42ec7d9, PKN: 7, PING, PADDING, PING, PADDING, PING, CRYPTO, CRYPTO, CRYPTO, PADDING…
25078 57.585937  10.30.7.200     142.250.183.106 QUIC     1292 Initial, DCID=7720b42dd42ec7d9, PKN: 8, CC, PADDING
27384 61.906981  10.30.7.200     40.99.9.50      QUIC     1292 Initial, DCID=1cf9ae6253672ee2, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, PADDING
27639 62.207843  10.30.7.200     40.99.9.50      QUIC     1292 Initial, DCID=1cf9ae6253672ee2, PKN: 3, PADDING, CRYPTO, PADDING
29808 62.814276  10.30.7.200     40.99.9.50      QUIC     1292 Initial, DCID=1cf9ae6253672ee2, PKN: 5, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CR…
32233 63.827314  10.30.7.200     142.250.183.170 QUIC     1292 Initial, DCID=6d5dcc42042c2d48, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, P…
34065 64.014297  10.30.7.200     40.99.9.50      QUIC     1292 Initial, DCID=1cf9ae6253672ee2, PKN: 7, PING, PADDING, CRYPTO, PADDING, PING, PING, PADDING, CRYPTO, CRYPTO…
35036 64.134704  10.30.7.200     142.250.183.170 QUIC     1292 Initial, DCID=6d5dcc42042c2d48, PKN: 3, PING, PING, PADDING, CRYPTO, PING, PING, CRYPTO, PADDING, PING, CRY…
35056 64.746653  10.30.7.200     142.250.183.170 QUIC     1292 Initial, DCID=6d5dcc42042c2d48, PKN: 5, CRYPTO, PING, PADDING, CRYPTO, PADDING, PING, PING
35078 64.917014  10.30.7.200     142.251.42.110  QUIC     1292 Initial, DCID=ae9ff0cb528d417d, PKN: 1, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, PING, CRYPTO, CRYPTO, CR…
```

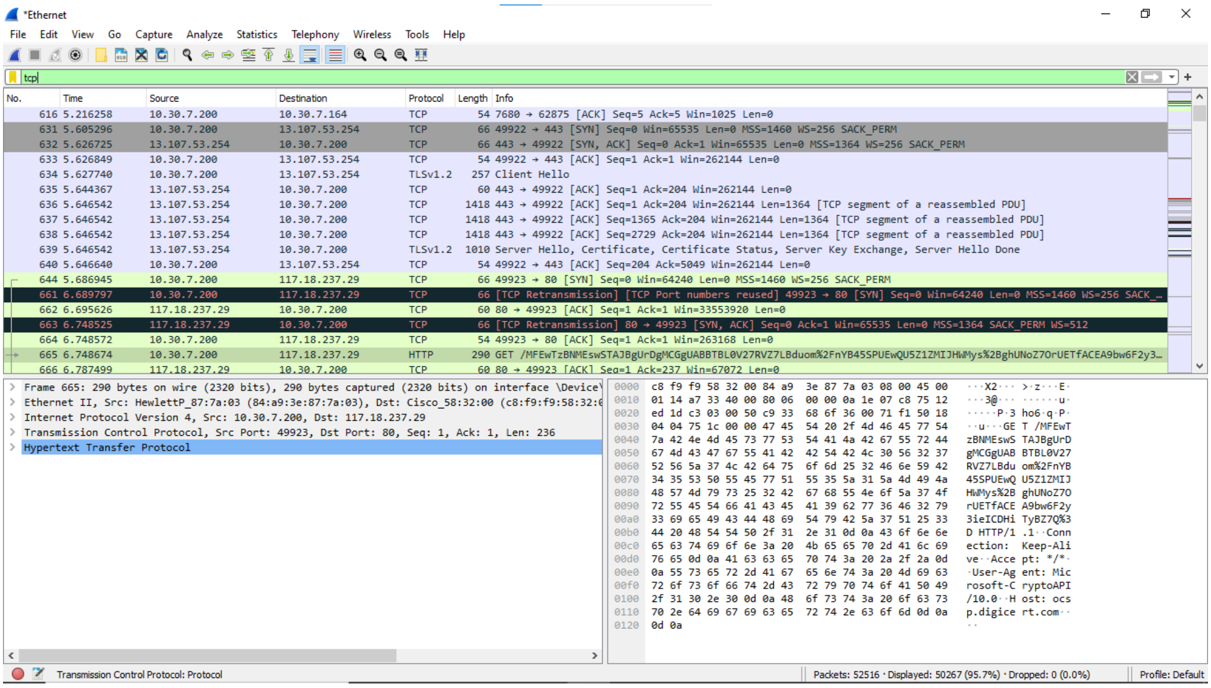
```
> Frame 2422: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \De
> Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:(
> Internet Protocol Version 4, Src: 10.30.7.200, Dst: 216.239.38.120
> User Datagram Protocol, Src Port: 60242, Dst Port: 443
> QUIC IETF
```

```
0000  c8 f9 f9 58 32 00 84 a9  3e 87 7a 03 08 00 45 00   ···X2··· >·z···E·
0010  04 fe 6e 88 40 00 80 11  00 00 0a 1e 07 c8 d8 ef   ··n·@··· ········
0020  26 78 eb 52 01 bb 04 ea  16 49 c1 00 00 00 01 08   &x·R···· ·I······
0030  b9 68 15 84 b8 5c 40 69  00 00 44 d0 a2 64 58 33   ·h···\@i ··D··dX3
0040  e5 cc d2 45 12 f6 aa 02  21 dd 0c 3a 4e fc 39 f3   ···E···· !··:N·9·
0050  6e 6a 0c ae 73 59 e7 9a  b8 ce ec 7d 14 26 7e 35   nj··sY·· ···}·&~5
0060  81 ca 3d 93 a6 67 c1 03  64 55 4b 3f 2a aa 7e 55   ··=··g·· dUK?*·~U
0070  49 06 49 cb c7 67 ff c5  68 db ec b3 00 e1 7c 16   I·I··g·· h·····|·
0080  57 a5 ec 17 ed b4 46 1d  f9 f3 81 e7 c5 67 08 dc   W·····F· ·····g··
0090  bf e9 8f 8a 84 ed c1 d2  a0 91 7a 1e e7 df 0f ab   ········ ··z·····
00a0  1e 57 bf 37 ad b3 e0 71  78 97 bb cf 57 03 e4 36   ·W·7···q x···W··6
00b0  07 f2 b1 98 62 0c 40 3b  f0 4e 9f 5a 4d ec fe cd   ····b·@; ·N·ZM···
00c0  06 4a 21 25 7b ce 12 b3  75 a3 9e ee 21 97 9f 4d   ·J!%{··· u···!··M
00d0  fa 54 55 ce 1d be 95 21  cf 1a 34 85 c6 54 00 fe   ·TU····! ··4··T··
00e0  d9 f0 56 7d 4c de f5 ee  2f 79 82 68 03 fa cd 10   ··V}L··· /y·h····
00f0  ff 50 24 b2 47 02 39 bd  61 a0 3b 6b 06 93 42 75   ·P$·G·9· a·;k··Bu
0100  e1 d6 3a c3 09 c3 71 5b  46 5e db cd 71 6c 2b dc   ··:···q[ F^··ql+·
0110  43 0f 2f f3 f9 e5 e5 81  15 4e fb 04 cf fc 56 4e   C·/····· ·N····VN
0120  62 73 d6 2e ab 00 88 aa  c8 58 68 b6 e0 f9 e2 29   bs·.···· ·Xh····)
0130  0a 6a 7c 87 a9 52 7b 84  94 e9 b0 f8 f3 d0 a9 b6   ·j|··R{· ········
```

Frame (1292 bytes) | Decrypted QUIC (1215 bytes)

QUIC IETF: Protocol | Packets: 52516 · Displayed: 30 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

TCP:


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

tcp

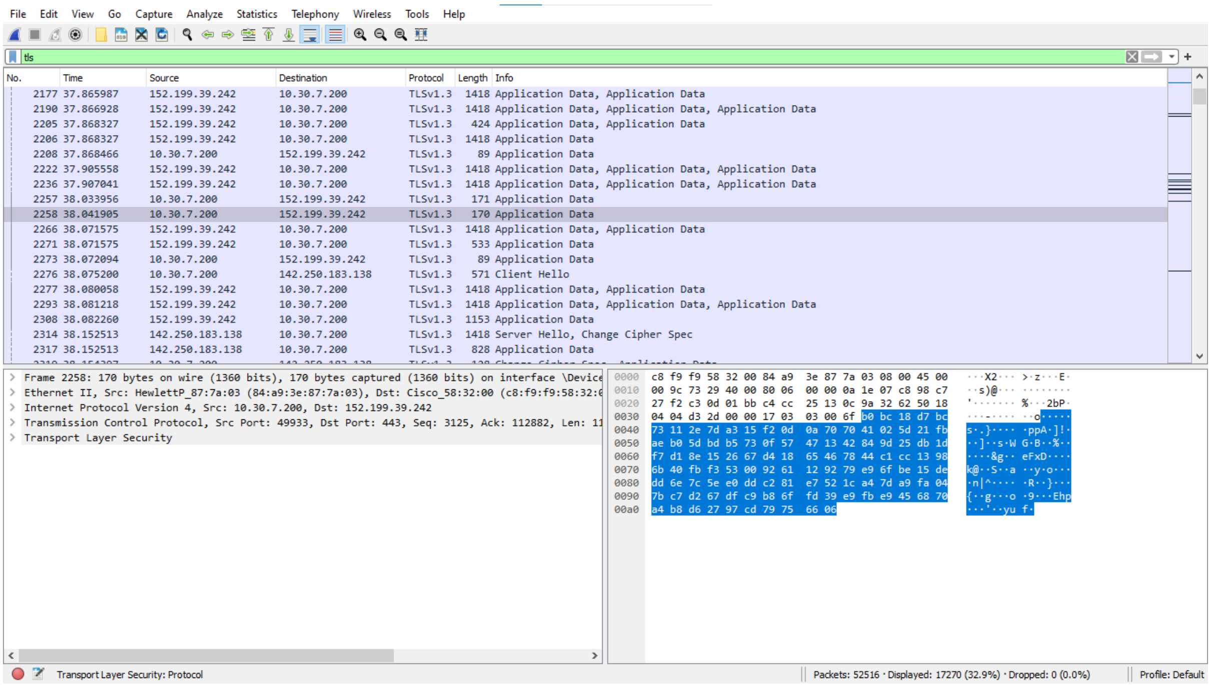
```
No.   Time       Source          Destination     Protocol Length Info
  616 5.216258   10.30.7.200     10.30.7.164     TCP        54 7680 → 62875 [ACK] Seq=5 Ack=5 Win=1025 Len=0
  631 5.605296   10.30.7.200     13.107.53.254   TCP        66 49922 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  632 5.626725   13.107.53.254   10.30.7.200     TCP        66 443 → 49922 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1364 WS=256 SACK_PERM
  633 5.626849   10.30.7.200     13.107.53.254   TCP        54 49922 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  634 5.627740   10.30.7.200     13.107.53.254   TLSv1.2   257 Client Hello
  635 5.644367   13.107.53.254   10.30.7.200     TCP        60 443 → 49922 [ACK] Seq=1 Ack=204 Win=262144 Len=0
  636 5.646542   13.107.53.254   10.30.7.200     TCP      1418 443 → 49922 [ACK] Seq=1 Ack=204 Win=262144 Len=1364 [TCP segment of a reassembled PDU]
  637 5.646542   13.107.53.254   10.30.7.200     TCP      1418 443 → 49922 [ACK] Seq=1365 Ack=204 Win=262144 Len=1364 [TCP segment of a reassembled PDU]
  638 5.646542   13.107.53.254   10.30.7.200     TCP      1418 443 → 49922 [ACK] Seq=2729 Ack=204 Win=262144 Len=1364 [TCP segment of a reassembled PDU]
  639 5.646542   13.107.53.254   10.30.7.200     TLSv1.2  1010 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
  640 5.646640   10.30.7.200     13.107.53.254   TCP        54 49922 → 443 [ACK] Seq=204 Ack=5049 Win=262144 Len=0
  644 5.686945   10.30.7.200     117.18.237.29   TCP        66 49923 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  661 6.689797   10.30.7.200     117.18.237.29   TCP        66 [TCP Retransmission] [TCP Port numbers reused] 49923 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
  662 6.695626   117.18.237.29   10.30.7.200     TCP        60 80 → 49923 [ACK] Seq=1 Ack=1 Win=33553920 Len=0
  663 6.748525   117.18.237.29   10.30.7.200     TCP        66 [TCP Retransmission] 80 → 49923 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1364 SACK_PERM WS=512
  664 6.748572   10.30.7.200     117.18.237.29   TCP        54 49923 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
  665 6.748674   10.30.7.200     117.18.237.29   HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA9bw6F2y3…
  666 6.787499   117.18.237.29   10.30.7.200     TCP        60 80 → 49923 [ACK] Seq=1 Ack=237 Win=67072 Len=0
```

```
> Frame 665: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface \Device\
> Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:0
> Internet Protocol Version 4, Src: 10.30.7.200, Dst: 117.18.237.29
> Transmission Control Protocol, Src Port: 49923, Dst Port: 80, Seq: 1, Ack: 1, Len: 236
> Hypertext Transfer Protocol
```

```
0000  c8 f9 f9 58 32 00 84 a9  3e 87 7a 03 08 00 45 00   ···X2··· >·z···E·
0010  01 14 a7 33 40 00 80 06  00 00 0a 1e 07 c8 75 12   ···3@··· ······u·
0020  ed 1d c3 03 00 50 c9 33  68 6f 36 00 71 f1 50 18   ·····P·3 ho6·q·P·
0030  04 04 75 1c 00 00 47 45  54 20 2f 4d 46 45 77 54   ··u···GE T /MFEwT
0040  7a 42 4e 4d 45 73 77 53  54 41 4a 42 67 55 72 44   zBNMEswS TAJBgUrD
0050  67 4d 43 47 67 55 41 42  42 54 42 4c 30 56 32 37   gMCGgUAB BTBL0V27
0060  52 56 5a 37 4c 42 64 75  6f 6d 25 32 46 6e 59 42   RVZ7LBdu om%2FnYB
0070  34 35 53 50 55 45 77 51  55 35 5a 31 5a 4d 49 4a   45SPUEwQ U5Z1ZMIJ
0080  48 57 4d 79 73 25 32 42  67 68 55 4e 6f 5a 37 4f   HWMys%2B ghUNoZ7O
0090  72 55 45 54 66 41 43 45  41 39 62 77 36 46 32 79   rUETfACE A9bw6F2y
00a0  33 69 65 49 43 44 48 69  54 79 42 5a 37 51 25 33   3ieICDHi TyBZ7Q%3
00b0  44 20 48 54 54 50 2f 31  2e 31 0d 0a 43 6f 6e 6e   D HTTP/1 .1··Conn
00c0  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
00d0  76 65 0d 0a 41 63 63 65  70 74 3a 20 2a 2f 2a 0d   ve··Acce pt: */*·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 69 63   ·User-Ag ent: Mic
00f0  72 6f 73 6f 66 74 2d 43  72 79 70 74 6f 41 50 49   rosoft-C ryptoAPI
0100  2f 31 30 2e 30 0d 0a 48  6f 73 74 3a 20 6f 63 73   /10.0··H ost: ocs
0110  70 2e 64 69 67 69 63 65  72 74 2e 63 6f 6d 0d 0a   p.digice rt.com··
0120  0d 0a                                              ··
```

Transmission Control Protocol: Protocol | Packets: 52516 · Displayed: 50267 (95.7%) · Dropped: 0 (0.0%) | Profile: Default

TLS:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

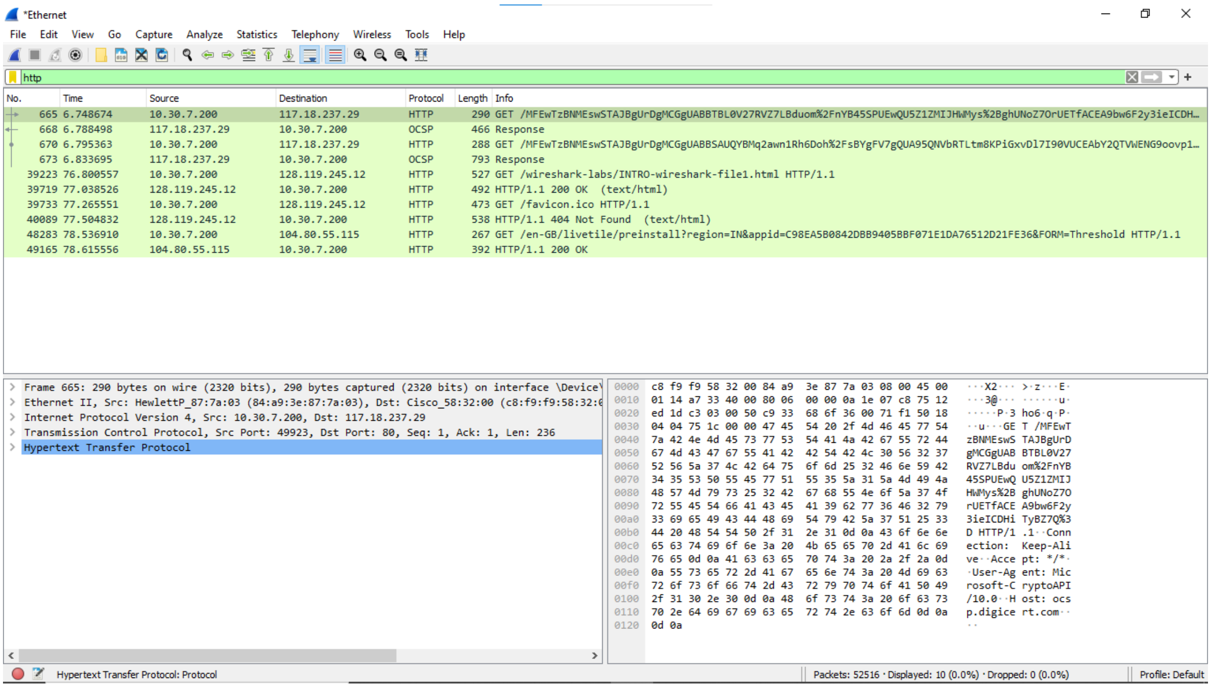
```
No.   Time        Source           Destination      Protocol Length Info
 2177 37.865987   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data, Application Data
 2190 37.866928   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data, Application Data, Application Data
 2205 37.868327   152.199.39.242   10.30.7.200      TLSv1.3   424 Application Data, Application Data
 2206 37.868327   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data
 2208 37.868466   10.30.7.200      152.199.39.242   TLSv1.3    89 Application Data
 2222 37.905558   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data, Application Data, Application Data
 2236 37.907041   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data, Application Data, Application Data
 2257 38.033956   10.30.7.200      152.199.39.242   TLSv1.3   171 Application Data
 2258 38.041905   10.30.7.200      152.199.39.242   TLSv1.3   170 Application Data
 2266 38.071575   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data, Application Data
 2271 38.071575   152.199.39.242   10.30.7.200      TLSv1.3   533 Application Data
 2273 38.072094   10.30.7.200      152.199.39.242   TLSv1.3    89 Application Data
 2276 38.075200   10.30.7.200      142.250.183.138  TLSv1.3   571 Client Hello
 2277 38.080058   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data, Application Data
 2293 38.081218   152.199.39.242   10.30.7.200      TLSv1.3  1418 Application Data, Application Data, Application Data
 2308 38.082260   152.199.39.242   10.30.7.200      TLSv1.3  1153 Application Data
 2314 38.152513   142.250.183.138  10.30.7.200      TLSv1.3  1418 Server Hello, Change Cipher Spec
 2317 38.152513   142.250.183.138  10.30.7.200      TLSv1.3   828 Application Data
```

```
> Frame 2258: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface \Device
> Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:0
> Internet Protocol Version 4, Src: 10.30.7.200, Dst: 152.199.39.242
> Transmission Control Protocol, Src Port: 49933, Dst Port: 443, Seq: 3125, Ack: 112882, Len: 11
> Transport Layer Security
```

```
0000  c8 f9 f9 58 32 00 84 a9  3e 87 7a 03 08 00 45 00   ···X2··· >·z···E·
0010  00 9c 73 29 40 00 80 06  00 00 0a 1e 07 c8 98 c7   ··s)@··· ········
0020  27 f2 c3 0d 01 bb c4 cc  25 13 0c 9a 32 62 50 18   '······· %···2bP·
0030  04 04 d3 2d 00 00 17 03  03 00 6f b0 bc 18 d7 bc   ···-···· ··o·····
0040  73 11 2e 7d a3 15 f2 0d  0a 70 70 41 02 5d 21 fb   s·.}···· ·ppA·]!·
0050  ae b0 5d bd b5 73 0f 57  47 13 42 84 9d 25 db 1d   ··]··s·W G·B··%··
0060  f7 d1 8e 15 26 67 d4 18  65 46 78 44 c1 cc 13 98   ····&g·· eFxD····
0070  6b 40 fb f3 53 00 92 61  12 92 79 e9 6f be 15 de   k@··S··a ··y·o···
0080  dd 6e 7c 5e e0 dd c2 81  e7 52 1c a4 7d a9 fa 04   ·n|^···· ·R··}···
0090  7b c7 d2 67 df c9 b8 6f  fd 39 e9 fb e9 45 68 70   {··g···o ·9···Ehp
00a0  a4 b8 d6 27 97 cd 79 75  66 06                     ···'··yu f·
```

Transport Layer Security: Protocol | Packets: 52516 · Displayed: 17270 (32.9%) · Dropped: 0 (0.0%) | Profile: Default

DNS:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

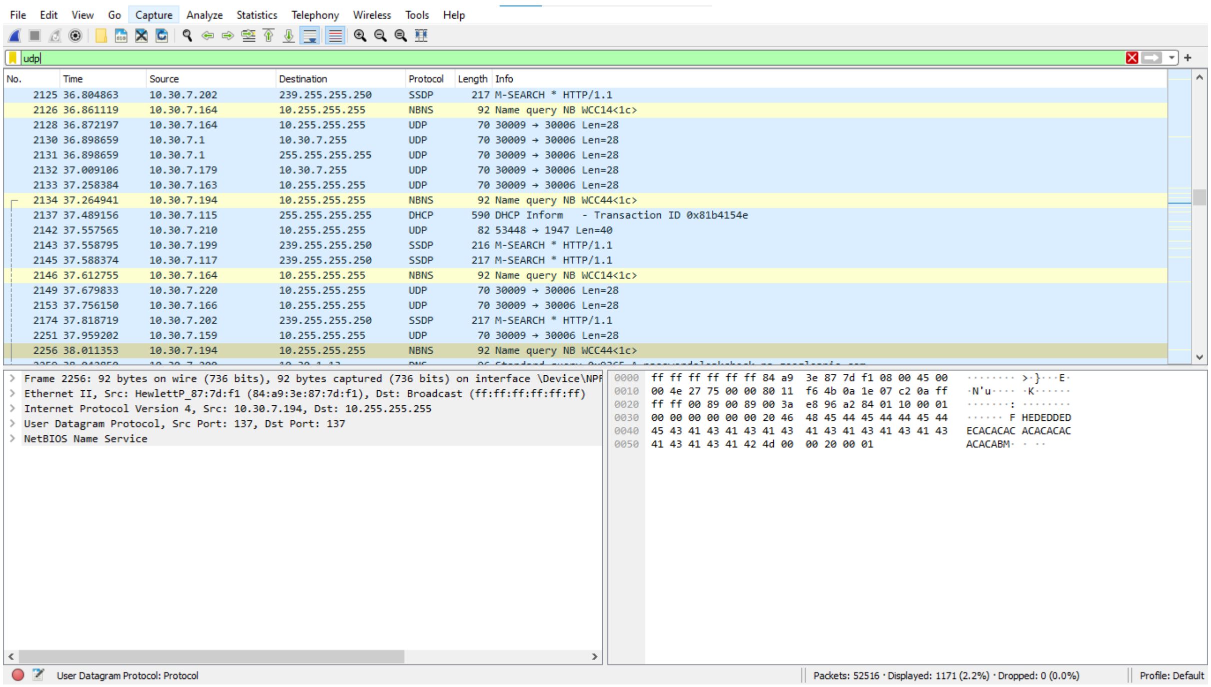
```
No.   Time       Source          Destination     Protocol Length Info
  665 6.748674   10.30.7.200     117.18.237.29   HTTP     290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA9bw6F2y3ieICDH…
  668 6.788498   117.18.237.29   10.30.7.200     OCSP     466 Response
  670 6.795363   10.30.7.200     117.18.237.29   HTTP     288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAbY2QTVWENG9oovp1…
  673 6.833695   117.18.237.29   10.30.7.200     OCSP     793 Response
39223 76.800557  10.30.7.200     128.119.245.12  HTTP     527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
39719 77.038526  128.119.245.12  10.30.7.200     HTTP     492 HTTP/1.1 200 OK  (text/html)
39733 77.265551  10.30.7.200     128.119.245.12  HTTP     473 GET /favicon.ico HTTP/1.1
40089 77.504832  128.119.245.12  10.30.7.200     HTTP     538 HTTP/1.1 404 Not Found  (text/html)
48283 78.536910  10.30.7.200     104.80.55.115   HTTP     267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
49165 78.615556  104.80.55.115   10.30.7.200     HTTP     392 HTTP/1.1 200 OK
```

```
> Frame 665: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface \Device\
> Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:0
> Internet Protocol Version 4, Src: 10.30.7.200, Dst: 117.18.237.29
> Transmission Control Protocol, Src Port: 49923, Dst Port: 80, Seq: 1, Ack: 1, Len: 236
> Hypertext Transfer Protocol
```

```
0000  c8 f9 f9 58 32 00 84 a9  3e 87 7a 03 08 00 45 00   ···X2··· >·z···E·
0010  01 14 a7 33 40 00 80 06  00 00 0a 1e 07 c8 75 12   ···3@··· ······u·
0020  ed 1d c3 03 00 50 c9 33  68 6f 36 00 71 f1 50 18   ·····P·3 ho6·q·P·
0030  04 04 75 1c 00 00 47 45  54 20 2f 4d 46 45 77 54   ··u···GE T /MFEwT
0040  7a 42 4e 4d 45 73 77 53  54 41 4a 42 67 55 72 44   zBNMEswS TAJBgUrD
0050  67 4d 43 47 67 55 41 42  42 54 42 4c 30 56 32 37   gMCGgUAB BTBL0V27
0060  52 56 5a 37 4c 42 64 75  6f 6d 25 32 46 6e 59 42   RVZ7LBdu om%2FnYB
0070  34 35 53 50 55 45 77 51  55 35 5a 31 5a 4d 49 4a   45SPUEwQ U5Z1ZMIJ
0080  48 57 4d 79 73 25 32 42  67 68 55 4e 6f 5a 37 4f   HWMys%2B ghUNoZ7O
0090  72 55 45 54 66 41 43 45  41 39 62 77 36 46 32 79   rUETfACE A9bw6F2y
00a0  33 69 65 49 43 44 48 69  54 79 42 5a 37 51 25 33   3ieICDHi TyBZ7Q%3
00b0  44 20 48 54 54 50 2f 31  2e 31 0d 0a 43 6f 6e 6e   D HTTP/1 .1··Conn
00c0  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
00d0  76 65 0d 0a 41 63 63 65  70 74 3a 20 2a 2f 2a 0d   ve··Acce pt: */*·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 69 63   ·User-Ag ent: Mic
00f0  72 6f 73 6f 66 74 2d 43  72 79 70 74 6f 41 50 49   rosoft-C ryptoAPI
0100  2f 31 30 2e 30 0d 0a 48  6f 73 74 3a 20 6f 63 73   /10.0··H ost: ocs
0110  70 2e 64 69 67 69 63 65  72 74 2e 63 6f 6d 0d 0a   p.digice rt.com··
0120  0d 0a                                              ··
```

Hypertext Transfer Protocol: Protocol | Packets: 52516 · Displayed: 10 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

UDP:


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

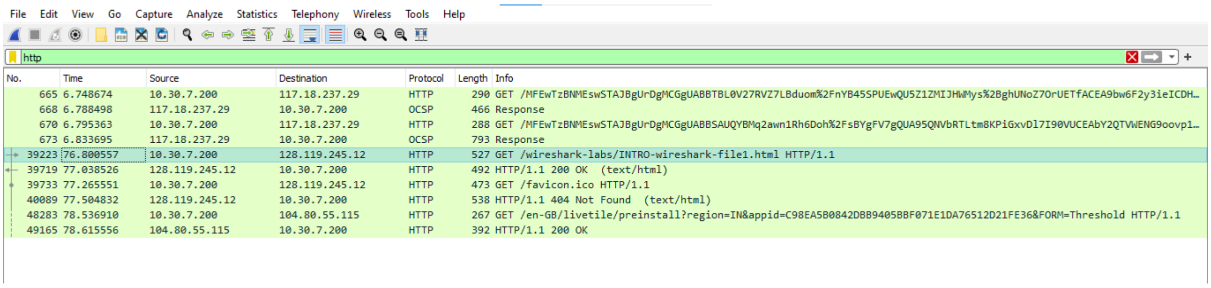
```
No.   Time       Source          Destination      Protocol Length Info
 2125 36.804863  10.30.7.202     239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
 2126 36.861119  10.30.7.164     10.255.255.255   NBNS      92 Name query NB WCC14<1c>
 2128 36.872197  10.30.7.164     10.255.255.255   UDP       70 30009 → 30006 Len=28
 2130 36.898659  10.30.7.1       10.30.7.255      UDP       70 30009 → 30006 Len=28
 2131 36.898659  10.30.7.1       255.255.255.255  UDP       70 30009 → 30006 Len=28
 2132 37.009106  10.30.7.179     10.30.7.255      UDP       70 30009 → 30006 Len=28
 2133 37.258384  10.30.7.163     10.255.255.255   UDP       70 30009 → 30006 Len=28
 2134 37.264941  10.30.7.194     10.255.255.255   NBNS      92 Name query NB WCC44<1c>
 2137 37.489156  10.30.7.115     255.255.255.255  DHCP     590 DHCP Inform   - Transaction ID 0x81b4154e
 2142 37.557565  10.30.7.210     10.255.255.255   UDP       82 53448 → 1947 Len=40
 2143 37.558795  10.30.7.199     239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
 2145 37.588374  10.30.7.117     239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
 2146 37.612755  10.30.7.164     10.255.255.255   NBNS      92 Name query NB WCC14<1c>
 2149 37.679833  10.30.7.220     10.255.255.255   UDP       70 30009 → 30006 Len=28
 2153 37.756150  10.30.7.166     10.255.255.255   UDP       70 30009 → 30006 Len=28
 2174 37.818719  10.30.7.202     239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
 2251 37.959202  10.30.7.159     10.255.255.255   UDP       70 30009 → 30006 Len=28
 2256 38.011353  10.30.7.194     10.255.255.255   NBNS      92 Name query NB WCC44<1c>
```

```
> Frame 2256: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF
> Ethernet II, Src: HewlettP_87:7d:f1 (84:a9:3e:87:7d:f1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.30.7.194, Dst: 10.255.255.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff 84 a9  3e 87 7d f1 08 00 45 00   ········ >·}···E·
0010  00 4e 27 75 00 00 80 11  f6 4b 0a 1e 07 c2 0a ff   ·N'u···· ·K······
0020  ff ff 00 89 00 89 00 3a  e8 96 a2 84 01 10 00 01   ·······: ········
0030  00 00 00 00 00 00 20 46  48 45 44 45 44 44 45 44   ······ F HEDEDDED
0040  45 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ECACACAC ACACACAC
0050  41 43 41 43 41 42 4d 00  00 20 00 01               ACACABM· · ··
```

User Datagram Protocol: Protocol | Packets: 52516 · Displayed: 1171 (2.2%) · Dropped: 0 (0.0%) | Profile: Default

Question 2:

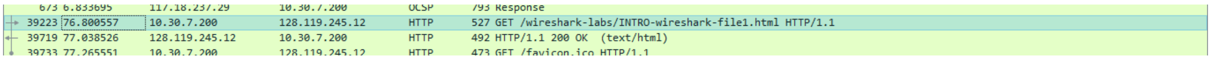


```
http

No.    Time       Source          Destination     Protocol Length Info
  665 6.748674   10.30.7.200     117.18.237.29   HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA9bw6F2y3ieICDH…
  668 6.788498   117.18.237.29   10.30.7.200     OCSP      466 Response
  670 6.795363   10.30.7.200     117.18.237.29   HTTP      288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAbY2QTVWENG9oovp1…
  673 6.833695   117.18.237.29   10.30.7.200     OCSP      793 Response
39223 76.800557  10.30.7.200     128.119.245.12  HTTP      527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
39719 77.038526  128.119.245.12  10.30.7.200     HTTP      492 HTTP/1.1 200 OK  (text/html)
39733 77.265551  10.30.7.200     128.119.245.12  HTTP      473 GET /favicon.ico HTTP/1.1
40089 77.504832  128.119.245.12  10.30.7.200     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
48283 78.536910  10.30.7.200     104.80.55.115   HTTP      267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
49165 78.615556  104.80.55.115   10.30.7.200     HTTP      392 HTTP/1.1 200 OK
```

Response Time: 77.038526-76.800557 = 0.237969 sec

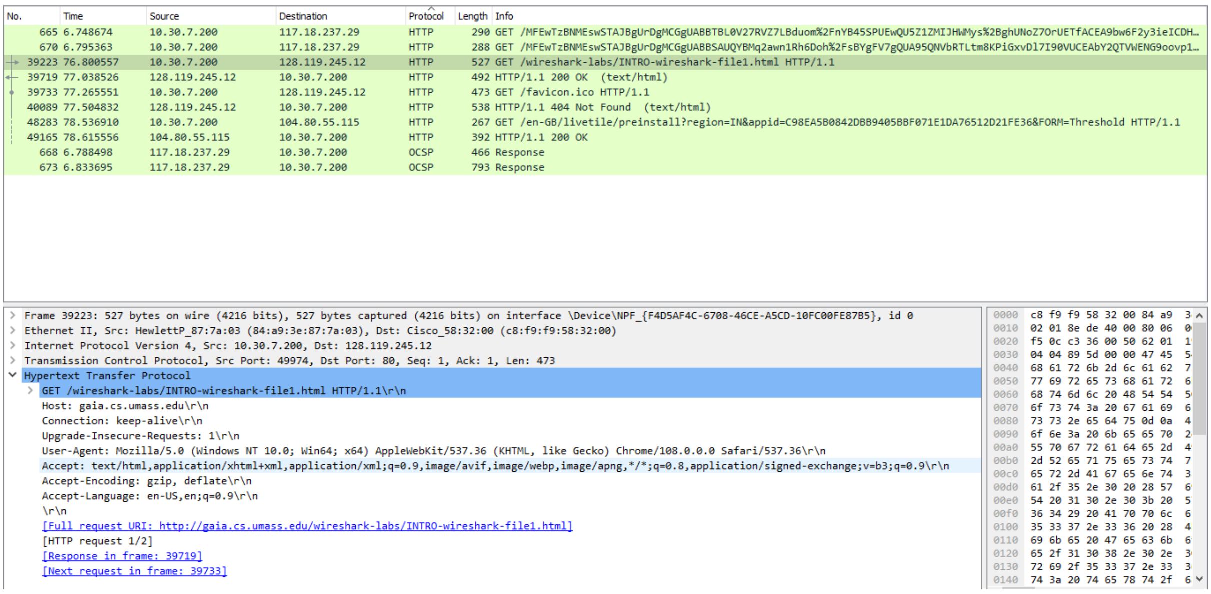
Question 3:



```
  673 6.833695   117.18.237.29   10.30.7.200     OCSP      793 Response
39223 76.800557  10.30.7.200     128.119.245.12  HTTP      527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
39719 77.038526  128.119.245.12  10.30.7.200     HTTP      492 HTTP/1.1 200 OK  (text/html)
39733 77.265551  10.30.7.200     128.119.245.12  HTTP      473 GET /favicon.ico HTTP/1.1
```

Here destination is the address of link and source is the address of our device.
10.30.7.200
128.119.245.12

Question 4:

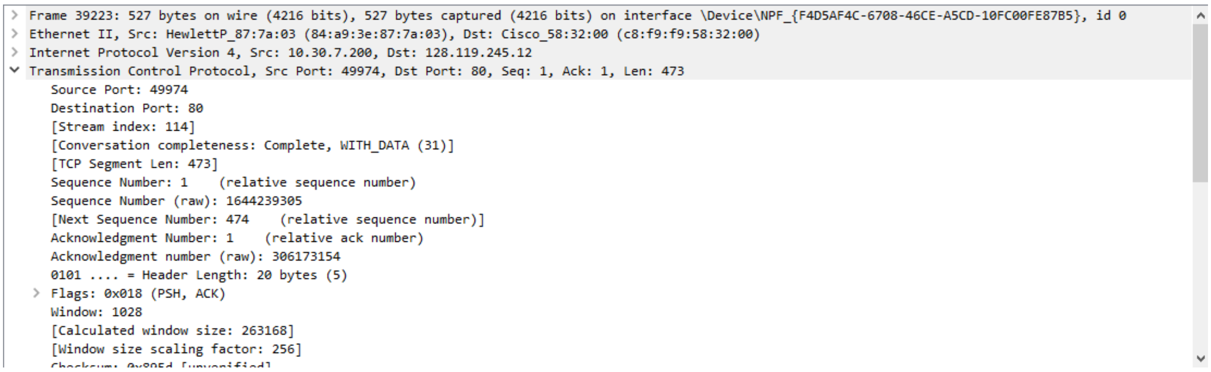


```
No.    Time       Source          Destination     Protocol Length Info
  665 6.748674   10.30.7.200     117.18.237.29   HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA9bw6F2y3ieICDH…
  670 6.795363   10.30.7.200     117.18.237.29   HTTP      288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAbY2QTVWENG9oovp1…
39223 76.800557  10.30.7.200     128.119.245.12  HTTP      527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
39719 77.038526  128.119.245.12  10.30.7.200     HTTP      492 HTTP/1.1 200 OK  (text/html)
39733 77.265551  10.30.7.200     128.119.245.12  HTTP      473 GET /favicon.ico HTTP/1.1
40089 77.504832  128.119.245.12  10.30.7.200     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
48283 78.536910  10.30.7.200     104.80.55.115   HTTP      267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
49165 78.615556  104.80.55.115   10.30.7.200     HTTP      392 HTTP/1.1 200 OK
  668 6.788498   117.18.237.29   10.30.7.200     OCSP      466 Response
  673 6.833695   117.18.237.29   10.30.7.200     OCSP      793 Response
```

```
> Frame 39223: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{F4D5AF4C-6708-46CE-A5CD-10FC00FE87B5}, id 0
> Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
> Internet Protocol Version 4, Src: 10.30.7.200, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49974, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\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/108.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 39719]
    [Next request in frame: 39733]
```

```
0000  c8 f9 f9 58 32 00 84 a9  3
0010  02 01 8e de 40 00 80 06  0
0020  f5 0c c3 36 00 50 62 01  1
0030  04 04 89 5d 00 00 47 45  5
0040  68 61 72 6b 2d 6c 61 62  7
0050  77 69 72 65 73 68 61 72  6
0060  68 74 6d 6c 20 48 54 54  5
0070  6f 73 74 3a 20 67 61 69  6
0080  73 73 2e 65 64 75 0d 0a  4
0090  6f 6e 3a 20 6b 65 65 70  2
00a0  55 70 67 72 61 64 65 2d  4
00b0  2d 52 65 71 75 65 73 74  7
00c0  65 72 2d 41 67 65 6e 74  3
00d0  61 2f 35 2e 30 20 28 57  6
00e0  54 20 31 30 2e 30 3b 20  5
00f0  36 34 29 20 41 70 70 6c  6
0100  35 33 37 2e 33 36 20 28  4
0110  69 6b 65 20 47 65 63 6b  6
0120  65 2f 31 30 38 2e 30 2e  3
0130  72 69 2f 35 33 37 2e 33  3
0140  74 3a 20 74 65 78 74 2f  6
```

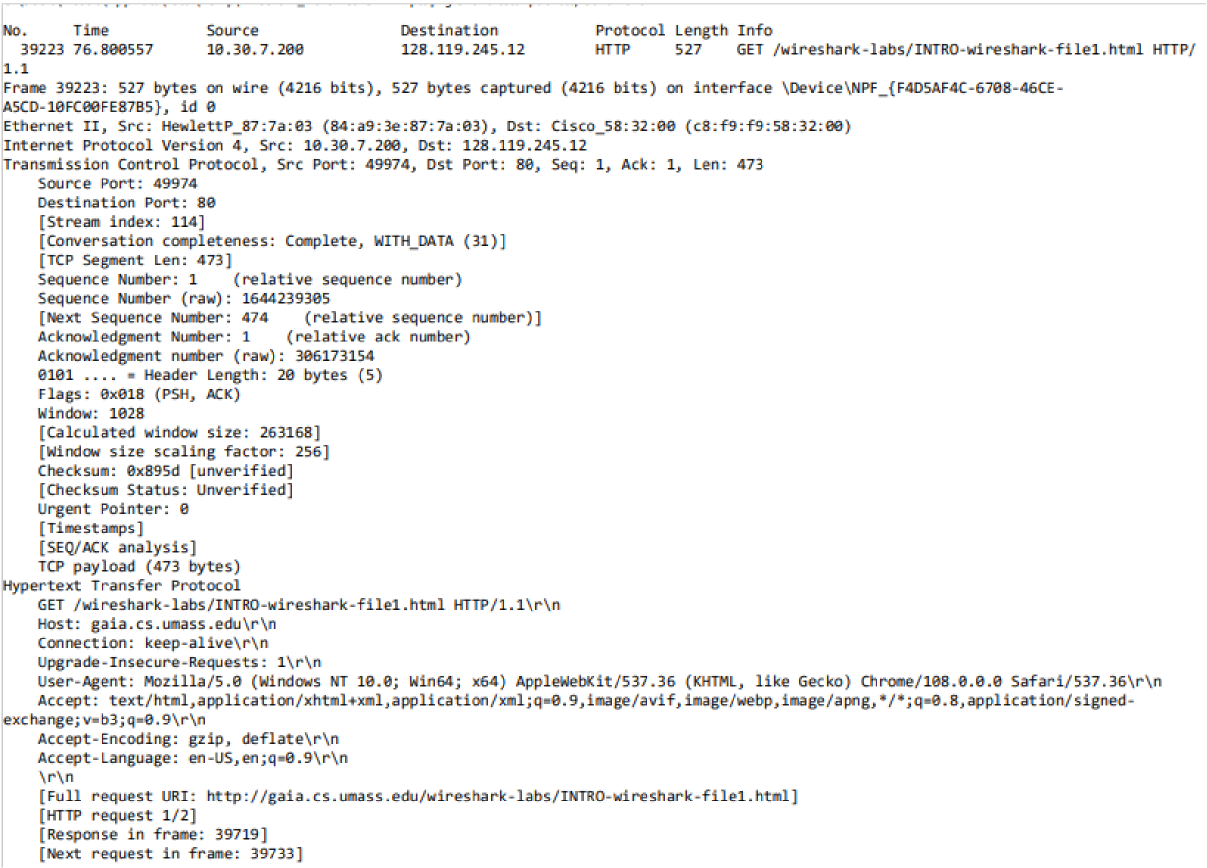
Question 5:



```
> Frame 39223: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{F4D5AF4C-6708-46CE-A5CD-10FC00FE87B5}, id 0
> Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
> Internet Protocol Version 4, Src: 10.30.7.200, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 49974, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
    Source Port: 49974
    Destination Port: 80
    [Stream index: 114]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 473]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1644239305
    [Next Sequence Number: 474    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 306173154
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1028
    [Calculated window size: 263168]
    [Window size scaling factor: 256]
    Checksum: 0x895d [unverified]
```

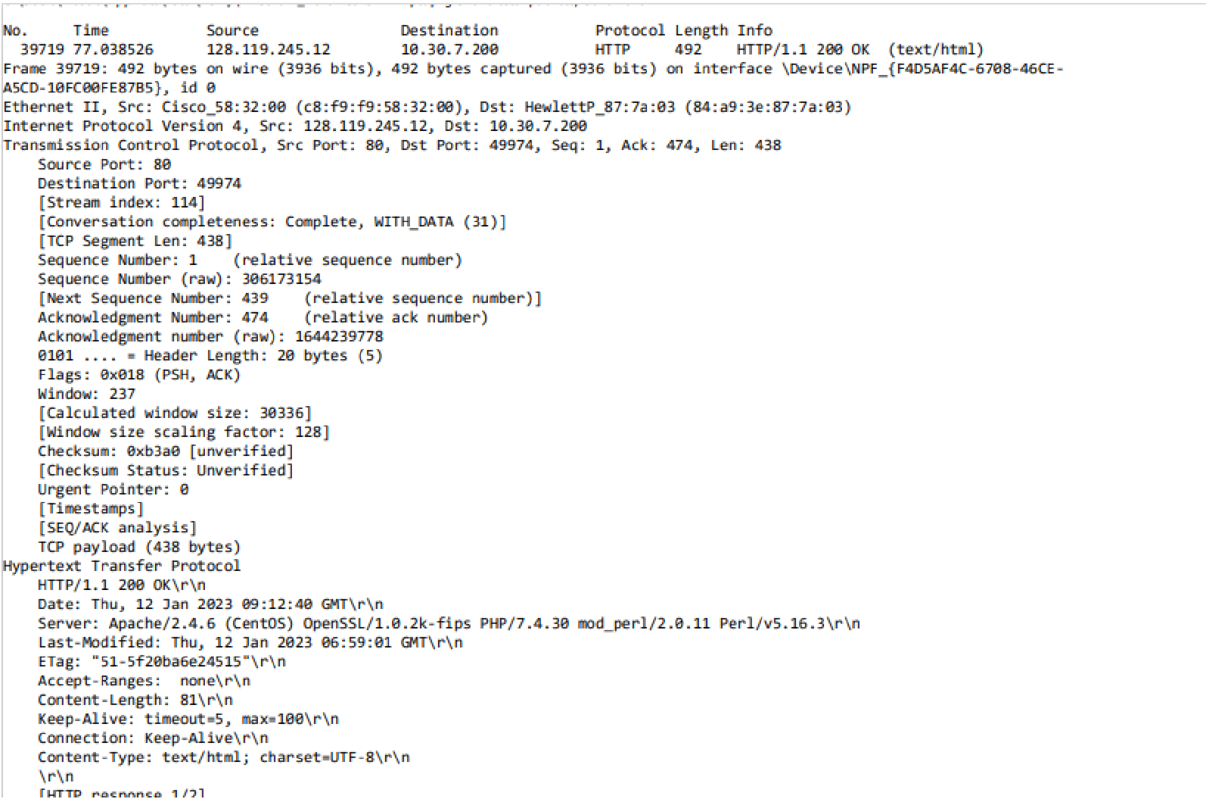
Question 6:

GET:



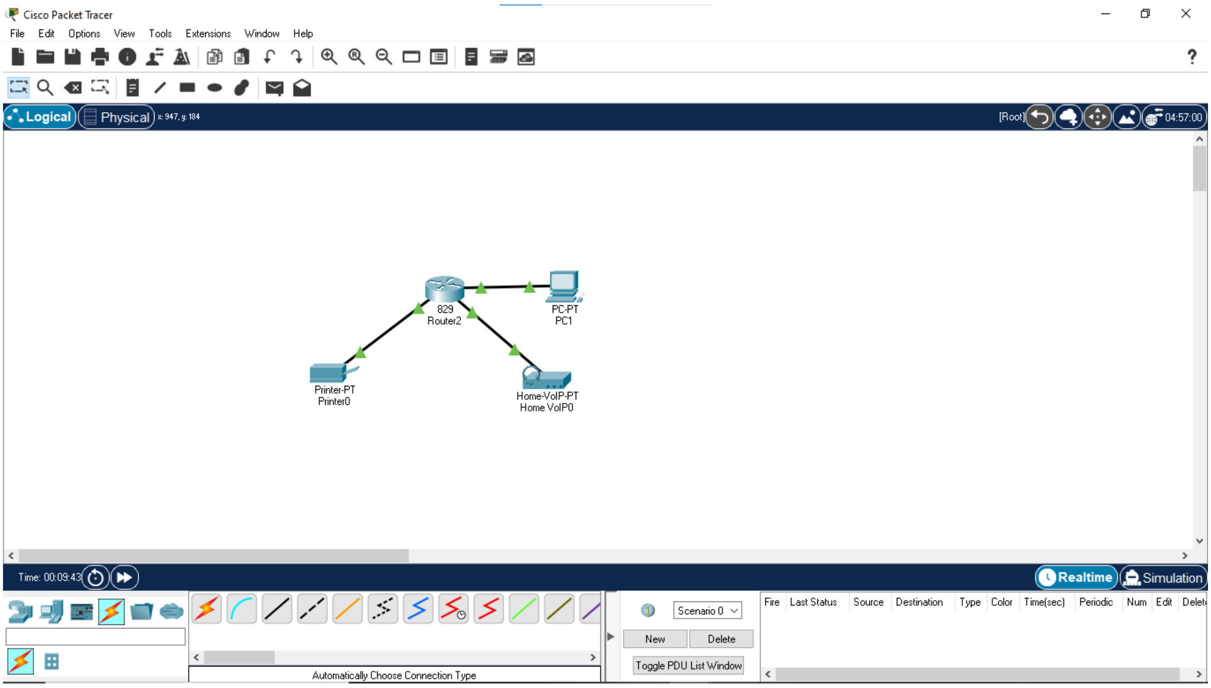
```
No.     Time           Source                Destination           Protocol Length Info
  39223 76.800557      10.30.7.200           128.119.245.12        HTTP     527    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 39223: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{F4D5AF4C-6708-46CE-
A5CD-10FC00FE87B5}, id 0
Ethernet II, Src: HewlettP_87:7a:03 (84:a9:3e:87:7a:03), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
Internet Protocol Version 4, Src: 10.30.7.200, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49974, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
    Source Port: 49974
    Destination Port: 80
    [Stream index: 114]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 473]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1644239305
    [Next Sequence Number: 474    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 306173154
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 1028
    [Calculated window size: 263168]
    [Window size scaling factor: 256]
    Checksum: 0x895d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (473 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\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/108.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 39719]
    [Next request in frame: 39733]
```

OK:



```
No.     Time           Source                Destination           Protocol Length Info
  39719 77.038526      128.119.245.12        10.30.7.200           HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 39719: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{F4D5AF4C-6708-46CE-
A5CD-10FC00FE87B5}, id 0
Ethernet II, Src: Cisco_58:32:00 (c8:f9:f9:58:32:00), Dst: HewlettP_87:7a:03 (84:a9:3e:87:7a:03)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.30.7.200
Transmission Control Protocol, Src Port: 80, Dst Port: 49974, Seq: 1, Ack: 474, Len: 438
    Source Port: 80
    Destination Port: 49974
    [Stream index: 114]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 306173154
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 474    (relative ack number)
    Acknowledgment number (raw): 1644239778
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xb3a0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 12 Jan 2023 09:12:40 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 12 Jan 2023 06:59:01 GMT\r\n
    ETag: "51-5f20ba6e24515"\r\n
    Accept-Ranges:  none\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
```

Task 2:



Here we connect one 829 router to three devices, the devices are printer, Personal computer and one home network. The network successfully configured.