Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security and Management Lab

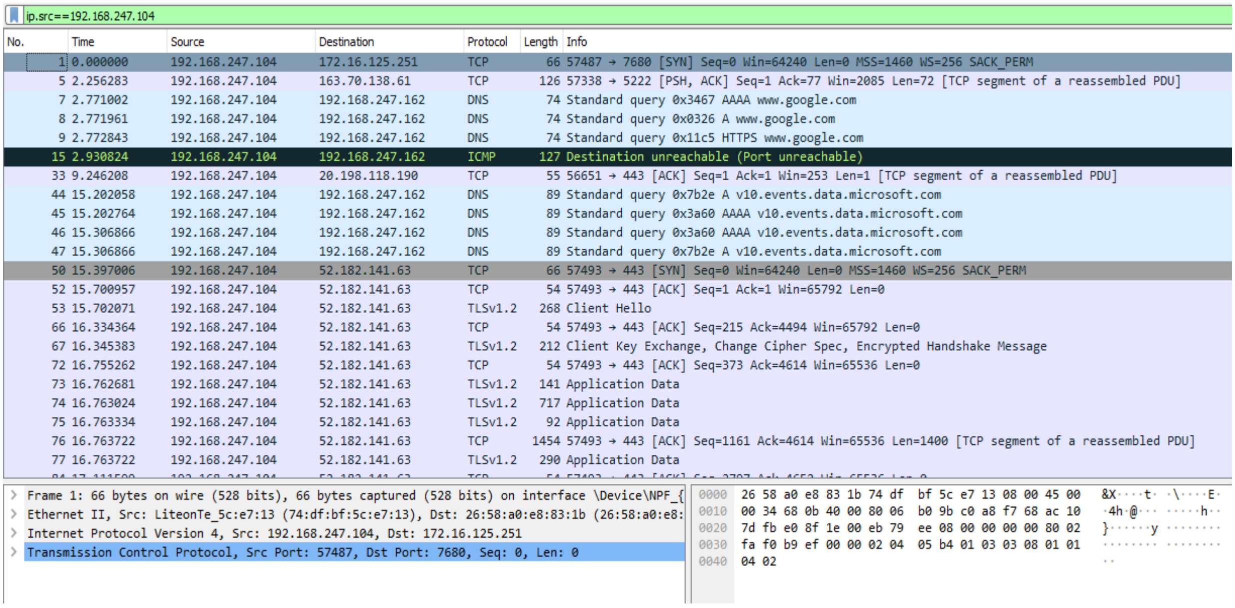
Using various filters in Wireshark

REG NO	21BCT0402
STUDENT NAME	Madasamy S
COURSE CODE	BCSE354E
SLOT & SEMESTER	L7+L8 ,Winter Semester 2023-24
COURSE NAME	Information Security Management Lab
FACULTY NAME	Chandru Vignesh C

1. Filter by source address

This will only show traffic where the source IP address is

ip.src==192.168.247.104

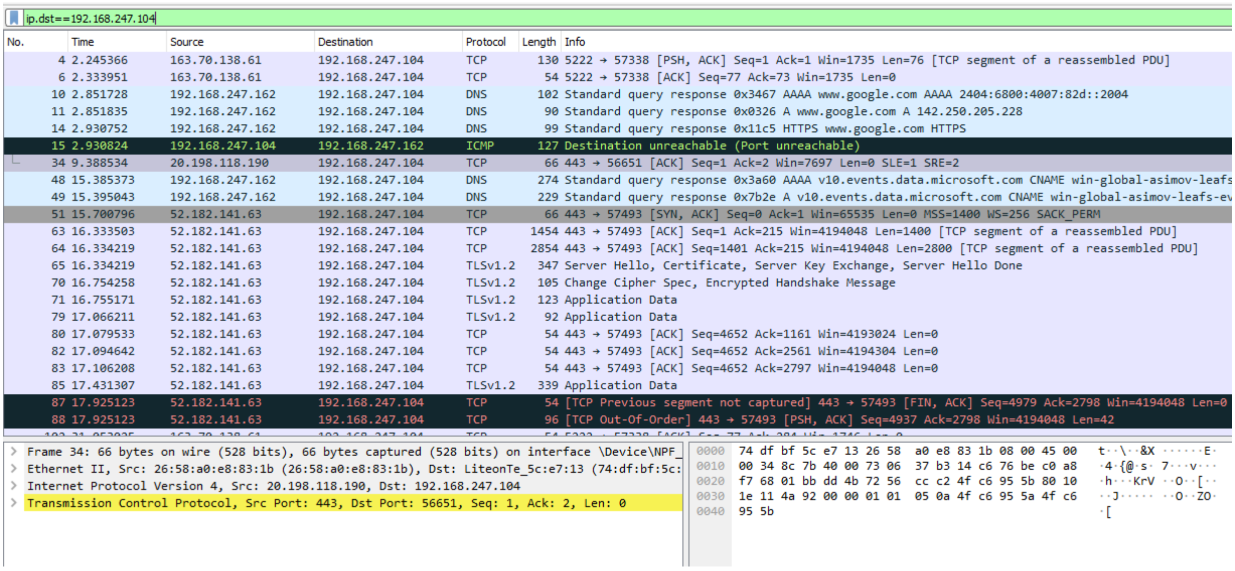


```
ip.src==192.168.247.104

No.  Time        Source            Destination       Protocol  Length Info
   1 0.000000    192.168.247.104   172.16.125.251    TCP         66 57487 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   5 2.256283    192.168.247.104   163.70.138.61     TCP        126 57338 → 5222 [PSH, ACK] Seq=1 Ack=77 Win=2085 Len=72 [TCP segment of a reassembled PDU]
   7 2.771002    192.168.247.104   192.168.247.162   DNS         74 Standard query 0x3467 AAAA www.google.com
   8 2.771961    192.168.247.104   192.168.247.162   DNS         74 Standard query 0x0326 A www.google.com
   9 2.772843    192.168.247.104   192.168.247.162   DNS         74 Standard query 0x11c5 HTTPS www.google.com
  15 2.930824    192.168.247.104   192.168.247.162   ICMP       127 Destination unreachable (Port unreachable)
  33 9.246208    192.168.247.104   20.198.118.190    TCP         55 56651 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
  44 15.202058   192.168.247.104   192.168.247.162   DNS         89 Standard query 0x7b2e A v10.events.data.microsoft.com
  45 15.202764   192.168.247.104   192.168.247.162   DNS         89 Standard query 0x3a60 AAAA v10.events.data.microsoft.com
  46 15.306866   192.168.247.104   192.168.247.162   DNS         89 Standard query 0x3a60 AAAA v10.events.data.microsoft.com
  47 15.306866   192.168.247.104   192.168.247.162   DNS         89 Standard query 0x7b2e A v10.events.data.microsoft.com
  50 15.397006   192.168.247.104   52.182.141.63     TCP         66 57493 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  52 15.700957   192.168.247.104   52.182.141.63     TCP         54 57493 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
  53 15.702071   192.168.247.104   52.182.141.63     TLSv1.2    268 Client Hello
  66 16.334364   192.168.247.104   52.182.141.63     TCP         54 57493 → 443 [ACK] Seq=215 Ack=4494 Win=65792 Len=0
  67 16.345383   192.168.247.104   52.182.141.63     TLSv1.2    212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  72 16.755262   192.168.247.104   52.182.141.63     TCP         54 57493 → 443 [ACK] Seq=373 Ack=4614 Win=65536 Len=0
  73 16.762681   192.168.247.104   52.182.141.63     TLSv1.2    141 Application Data
  74 16.763024   192.168.247.104   52.182.141.63     TLSv1.2    717 Application Data
  75 16.763334   192.168.247.104   52.182.141.63     TLSv1.2     92 Application Data
  76 16.763722   192.168.247.104   52.182.141.63     TCP       1454 57493 → 443 [ACK] Seq=1161 Ack=4614 Win=65536 Len=1400 [TCP segment of a reassembled PDU]
  77 16.763722   192.168.247.104   52.182.141.63     TLSv1.2    290 Application Data

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{
> Ethernet II, Src: LiteonTe_5c:e7:13 (74:df:bf:5c:e7:13), Dst: 26:58:a0:e8:83:1b (26:58:a0:e8:
> Internet Protocol Version 4, Src: 192.168.247.104, Dst: 172.16.125.251
> Transmission Control Protocol, Src Port: 57487, Dst Port: 7680, Seq: 0, Len: 0

0000  26 58 a0 e8 83 1b 74 df  bf 5c e7 13 08 00 45 00   &X····t· ·\····E·
0010  00 34 68 0b 40 00 80 06  b0 9b c0 a8 f7 68 ac 10   ·4h·@··· ·····h··
0020  7d fb e0 8f 1e 00 eb 79  ee 08 00 00 00 00 80 02   }······y ········
0030  fa f0 b9 ef 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

2. Filter by destination address

Displays only traffic for the matching destination IP.

ip.dst==192.168.247.104

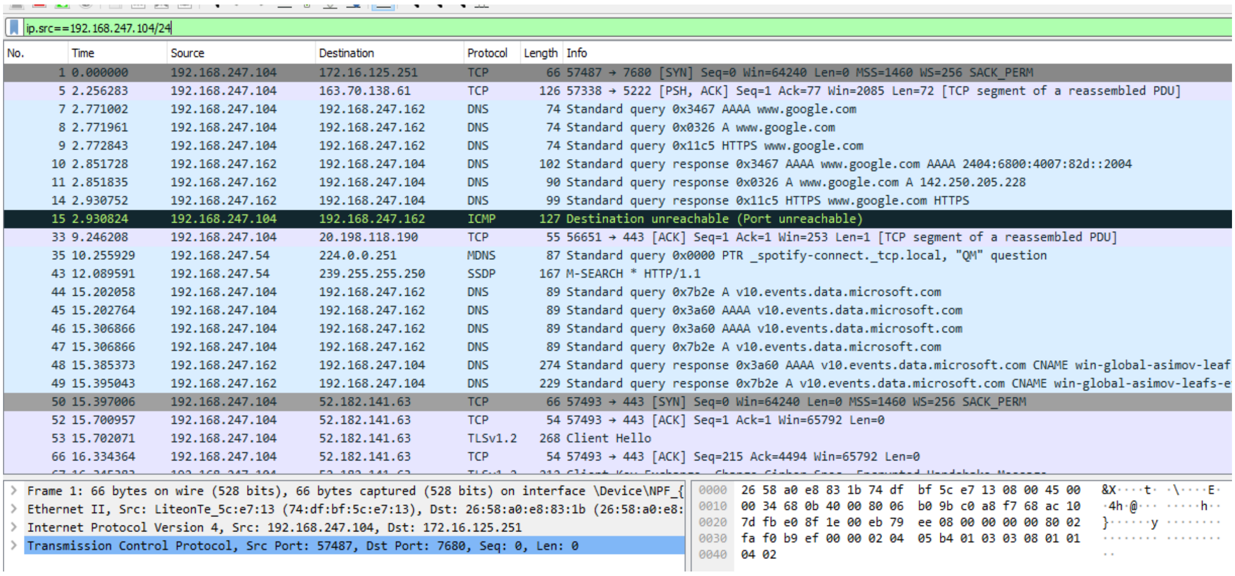


```
ip.dst==192.168.247.104

No.  Time        Source            Destination       Protocol  Length Info
   4 2.245366    163.70.138.61     192.168.247.104   TCP        130 5222 → 57338 [PSH, ACK] Seq=1 Ack=1 Win=1735 Len=76 [TCP segment of a reassembled PDU]
   6 2.333951    163.70.138.61     192.168.247.104   TCP         54 5222 → 57338 [ACK] Seq=77 Ack=73 Win=1735 Len=0
  10 2.851728    192.168.247.162   192.168.247.104   DNS        102 Standard query response 0x3467 AAAA www.google.com AAAA 2404:6800:4007:82d::2004
  11 2.851835    192.168.247.162   192.168.247.104   DNS         90 Standard query response 0x0326 A www.google.com A 142.250.205.228
  14 2.930752    192.168.247.162   192.168.247.104   DNS         99 Standard query response 0x11c5 HTTPS www.google.com HTTPS
  15 2.930824    192.168.247.104   192.168.247.162   ICMP       127 Destination unreachable (Port unreachable)
  34 9.388534    20.198.118.190    192.168.247.104   TCP         66 443 → 56651 [ACK] Seq=1 Ack=2 Win=7697 Len=0 SLE=1 SRE=2
  48 15.385373   192.168.247.162   192.168.247.104   DNS        274 Standard query response 0x3a60 AAAA v10.events.data.microsoft.com CNAME win-global-asimov-leafs
  49 15.395043   192.168.247.162   192.168.247.104   DNS        229 Standard query response 0x7b2e A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-ev
  51 15.700796   52.182.141.63     192.168.247.104   TCP         66 443 → 57493 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
  63 16.333503   52.182.141.63     192.168.247.104   TCP       1454 443 → 57493 [ACK] Seq=1 Ack=215 Win=4194048 Len=1400 [TCP segment of a reassembled PDU]
  64 16.334219   52.182.141.63     192.168.247.104   TCP       2854 443 → 57493 [ACK] Seq=1401 Ack=215 Win=4194048 Len=2800 [TCP segment of a reassembled PDU]
  65 16.334219   52.182.141.63     192.168.247.104   TLSv1.2    347 Server Hello, Certificate, Server Key Exchange, Server Hello Done
  70 16.754258   52.182.141.63     192.168.247.104   TLSv1.2    105 Change Cipher Spec, Encrypted Handshake Message
  71 16.755171   52.182.141.63     192.168.247.104   TLSv1.2    123 Application Data
  79 17.066211   52.182.141.63     192.168.247.104   TLSv1.2     92 Application Data
  80 17.079533   52.182.141.63     192.168.247.104   TCP         54 443 → 57493 [ACK] Seq=4652 Ack=1161 Win=4193024 Len=0
  82 17.094642   52.182.141.63     192.168.247.104   TCP         54 443 → 57493 [ACK] Seq=4652 Ack=2561 Win=4194304 Len=0
  83 17.106208   52.182.141.63     192.168.247.104   TCP         54 443 → 57493 [ACK] Seq=4652 Ack=2797 Win=4194048 Len=0
  85 17.431307   52.182.141.63     192.168.247.104   TLSv1.2    339 Application Data
  87 17.925123   52.182.141.63     192.168.247.104   TCP         54 [TCP Previous segment not captured] 443 → 57493 [FIN, ACK] Seq=4979 Ack=2798 Win=4194048 Len=0
  88 17.925123   52.182.141.63     192.168.247.104   TCP         96 [TCP Out-Of-Order] 443 → 57493 [PSH, ACK] Seq=4937 Ack=2798 Win=4194048 Len=42

> Frame 34: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_
> Ethernet II, Src: 26:58:a0:e8:83:1b (26:58:a0:e8:83:1b), Dst: LiteonTe_5c:e7:13 (74:df:bf:5c:
> Internet Protocol Version 4, Src: 20.198.118.190, Dst: 192.168.247.104
> Transmission Control Protocol, Src Port: 443, Dst Port: 56651, Seq: 1, Ack: 2, Len: 0

0000  74 df bf 5c e7 13 26 58  a0 e8 83 1b 08 00 45 00   t··\··&X ······E·
0010  00 34 8c 7b 40 00 73 06  37 b3 14 c6 76 be c0 a8   ·4·{@·s· 7···v···
0020  f7 68 01 bb dd 4b 72 56  cc c2 4f c6 95 5b 80 10   ·h···KrV ··O··[··
0030  1e 11 4a 92 00 00 01 01  05 0a 4f c6 95 5a 4f c6   ··J····· ··O··ZO·
0040  95 5b                                              ·[
```

3. Filter by IP subnet

Displays all traffic for the entered subnet, this will match on source or destination. Use CIDR format for subnet display filter.

ip.src==192.168.247.104/24



```
ip.src==192.168.247.104/24

No.   Time          Source            Destination       Protocol  Length  Info
    1 0.000000      192.168.247.104   172.16.125.251    TCP         66 57487 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    5 2.256283      192.168.247.104   163.70.138.61     TCP        126 57338 → 5222 [PSH, ACK] Seq=1 Ack=77 Win=2085 Len=72 [TCP segment of a reassembled PDU]
    7 2.771002      192.168.247.104   192.168.247.162   DNS         74 Standard query 0x3467 AAAA www.google.com
    8 2.771961      192.168.247.104   192.168.247.162   DNS         74 Standard query 0x0326 A www.google.com
    9 2.772843      192.168.247.104   192.168.247.162   DNS         74 Standard query 0x11c5 HTTPS www.google.com
   10 2.851728      192.168.247.162   192.168.247.104   DNS        102 Standard query response 0x3467 AAAA www.google.com AAAA 2404:6800:4007:82d::2004
   11 2.851835      192.168.247.162   192.168.247.104   DNS         90 Standard query response 0x0326 A www.google.com A 142.250.205.228
   14 2.930752      192.168.247.162   192.168.247.104   DNS         99 Standard query response 0x11c5 HTTPS www.google.com HTTPS
   15 2.930824      192.168.247.104   192.168.247.162   ICMP       127 Destination unreachable (Port unreachable)
   33 9.246208      192.168.247.104   20.198.118.190    TCP         55 56651 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
   35 10.255929     192.168.247.54    224.0.0.251       MDNS        87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
   43 12.089591     192.168.247.54    239.255.255.250   SSDP       167 M-SEARCH * HTTP/1.1
   44 15.202058     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x7b2e A v10.events.data.microsoft.com
   45 15.202764     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x3a60 AAAA v10.events.data.microsoft.com
   46 15.306866     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x3a60 AAAA v10.events.data.microsoft.com
   47 15.306866     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x7b2e A v10.events.data.microsoft.com
   48 15.385373     192.168.247.162   192.168.247.104   DNS        274 Standard query response 0x3a60 AAAA v10.events.data.microsoft.com CNAME win-global-asimov-leaf
   49 15.395043     192.168.247.162   192.168.247.104   DNS        229 Standard query response 0x7b2e A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-e
   50 15.397006     192.168.247.104   52.182.141.63     TCP         66 57493 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   52 15.700957     192.168.247.104   52.182.141.63     TCP         54 57493 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
   53 15.702071     192.168.247.104   52.182.141.63     TLSv1.2    268 Client Hello
   66 16.334364     192.168.247.104   52.182.141.63     TCP         54 57493 → 443 [ACK] Seq=215 Ack=4494 Win=65792 Len=0
```

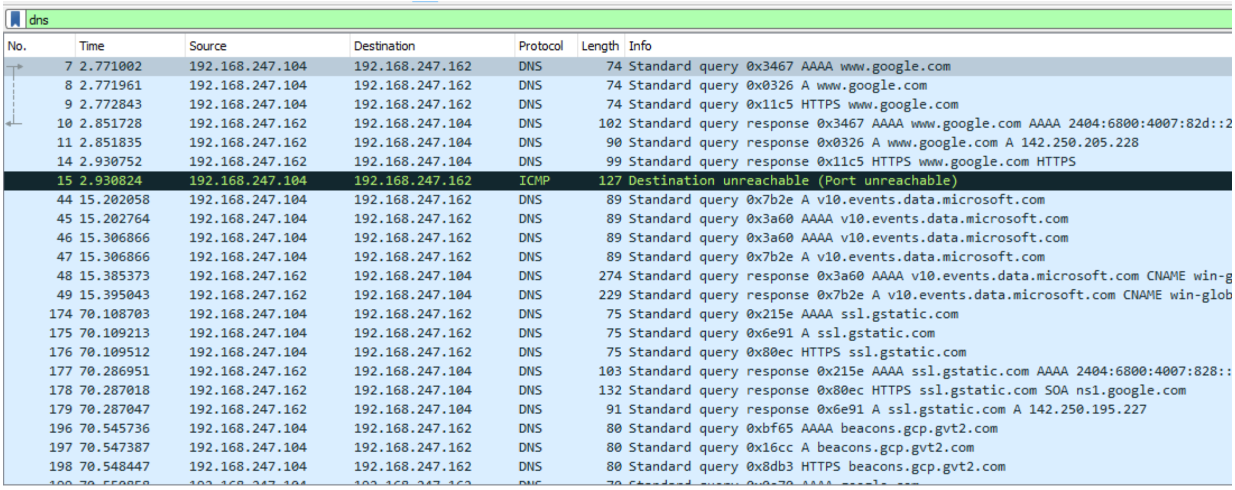
```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{
> Ethernet II, Src: LiteonTe_5c:e7:13 (74:df:bf:5c:e7:13), Dst: 26:58:a0:e8:83:1b (26:58:a0:e8:
> Internet Protocol Version 4, Src: 192.168.247.104, Dst: 172.16.125.251
> Transmission Control Protocol, Src Port: 57487, Dst Port: 7680, Seq: 0, Len: 0
```

```
0000  26 58 a0 e8 83 1b 74 df  bf 5c e7 13 08 00 45 00   &X····t· ·\····E·
0010  00 34 68 0b 40 00 80 06  b0 9b c0 a8 f7 68 ac 10   ·4h·@··· ·····h··
0020  7d fb e0 8f 1e 00 eb 79  ee 08 00 00 00 00 80 02   }······y ········
0030  fa f0 b9 ef 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

4. Filter traffic based on protocol

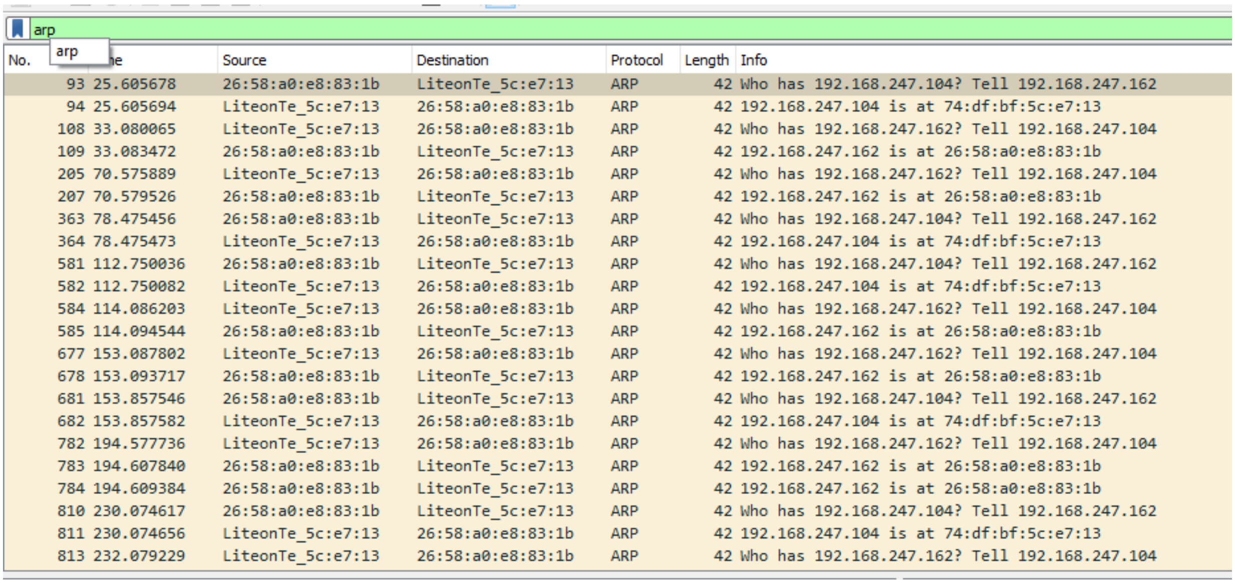
To filter for a specific protocol just type in the name of the protocol. For example to display all DNS traffic just type DNS in the filter box.

dns



```
dns

No.   Time          Source            Destination       Protocol  Length  Info
    7 2.771002      192.168.247.104   192.168.247.162   DNS         74 Standard query 0x3467 AAAA www.google.com
    8 2.771961      192.168.247.104   192.168.247.162   DNS         74 Standard query 0x0326 A www.google.com
    9 2.772843      192.168.247.104   192.168.247.162   DNS         74 Standard query 0x11c5 HTTPS www.google.com
   10 2.851728      192.168.247.162   192.168.247.104   DNS        102 Standard query response 0x3467 AAAA www.google.com AAAA 2404:6800:4007:82d::2
   11 2.851835      192.168.247.162   192.168.247.104   DNS         90 Standard query response 0x0326 A www.google.com A 142.250.205.228
   14 2.930752      192.168.247.162   192.168.247.104   DNS         99 Standard query response 0x11c5 HTTPS www.google.com HTTPS
   15 2.930824      192.168.247.104   192.168.247.162   ICMP       127 Destination unreachable (Port unreachable)
   44 15.202058     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x7b2e A v10.events.data.microsoft.com
   45 15.202764     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x3a60 AAAA v10.events.data.microsoft.com
   46 15.306866     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x3a60 AAAA v10.events.data.microsoft.com
   47 15.306866     192.168.247.104   192.168.247.162   DNS         89 Standard query 0x7b2e A v10.events.data.microsoft.com
   48 15.385373     192.168.247.162   192.168.247.104   DNS        274 Standard query response 0x3a60 AAAA v10.events.data.microsoft.com CNAME win-g
   49 15.395043     192.168.247.162   192.168.247.104   DNS        229 Standard query response 0x7b2e A v10.events.data.microsoft.com CNAME win-glob
  174 70.108703     192.168.247.104   192.168.247.162   DNS         75 Standard query 0x215e AAAA ssl.gstatic.com
  175 70.109213     192.168.247.104   192.168.247.162   DNS         75 Standard query 0x6e91 A ssl.gstatic.com
  176 70.109512     192.168.247.104   192.168.247.162   DNS         75 Standard query 0x80ec HTTPS ssl.gstatic.com
  177 70.286951     192.168.247.162   192.168.247.104   DNS        103 Standard query response 0x215e AAAA ssl.gstatic.com AAAA 2404:6800:4007:828::
  178 70.287018     192.168.247.162   192.168.247.104   DNS        132 Standard query response 0x80ec HTTPS ssl.gstatic.com SOA ns1.google.com
  179 70.287047     192.168.247.162   192.168.247.104   DNS         91 Standard query response 0x6e91 A ssl.gstatic.com A 142.250.195.227
  196 70.545736     192.168.247.104   192.168.247.162   DNS         80 Standard query 0xbf65 AAAA beacons.gcp.gvt2.com
  197 70.547387     192.168.247.104   192.168.247.162   DNS         80 Standard query 0x16cc A beacons.gcp.gvt2.com
  198 70.548447     192.168.247.104   192.168.247.162   DNS         80 Standard query 0x8db3 HTTPS beacons.gcp.gvt2.com
```

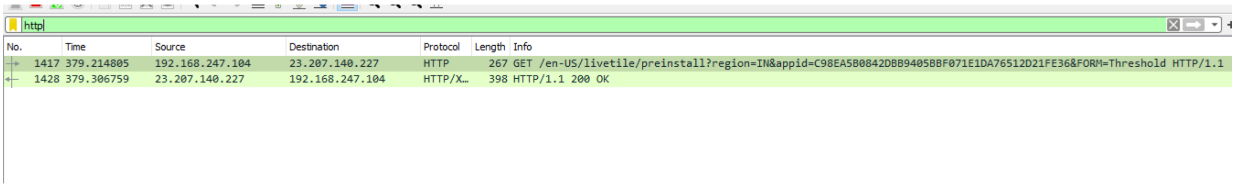
arp



arp

```
No.  arp e          Source              Destination         Protocol  Length  Info
     93 25.605678   26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 Who has 192.168.247.104? Tell 192.168.247.162
     94 25.605694   LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 192.168.247.104 is at 74:df:bf:5c:e7:13
    108 33.080065   LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
    109 33.083472   26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
    205 70.575889   LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
    207 70.579526   26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
    363 78.475456   26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 Who has 192.168.247.104? Tell 192.168.247.162
    364 78.475473   LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 192.168.247.104 is at 74:df:bf:5c:e7:13
    581 112.750036  26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 Who has 192.168.247.104? Tell 192.168.247.162
    582 112.750082  LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 192.168.247.104 is at 74:df:bf:5c:e7:13
    584 114.086203  LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
    585 114.094544  26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
    677 153.087802  LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
    678 153.093717  26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
    681 153.857546  26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 Who has 192.168.247.104? Tell 192.168.247.162
    682 153.857582  LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 192.168.247.104 is at 74:df:bf:5c:e7:13
    782 194.577736  LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
    783 194.607840  26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
    784 194.609384  26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
    810 230.074617  26:58:a0:e8:83:1b   LiteonTe_5c:e7:13   ARP        42 Who has 192.168.247.104? Tell 192.168.247.162
    811 230.074656  LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 192.168.247.104 is at 74:df:bf:5c:e7:13
    813 232.079229  LiteonTe_5c:e7:13   26:58:a0:e8:83:1b   ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
```

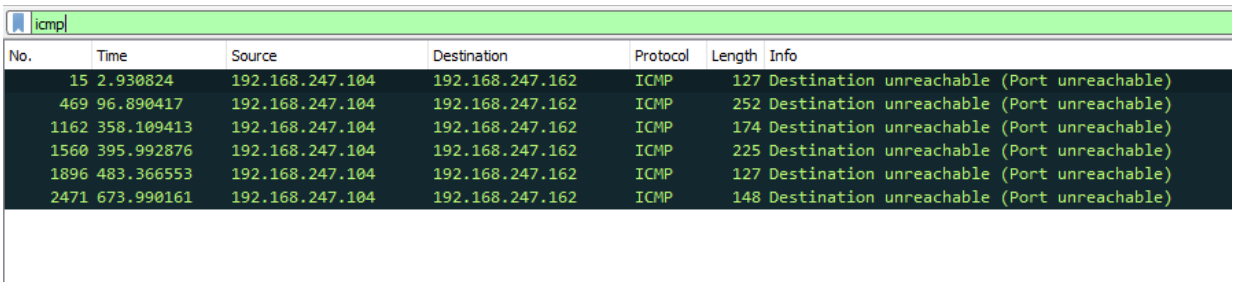
http



http

```
No.   Time         Source            Destination       Protocol  Length Info
 1417 379.214805   192.168.247.104   23.207.140.227    HTTP       267 GET /en-US/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
 1428 379.306759   23.207.140.227    192.168.247.104   HTTP/X…    398 HTTP/1.1 200 OK
```

icmp



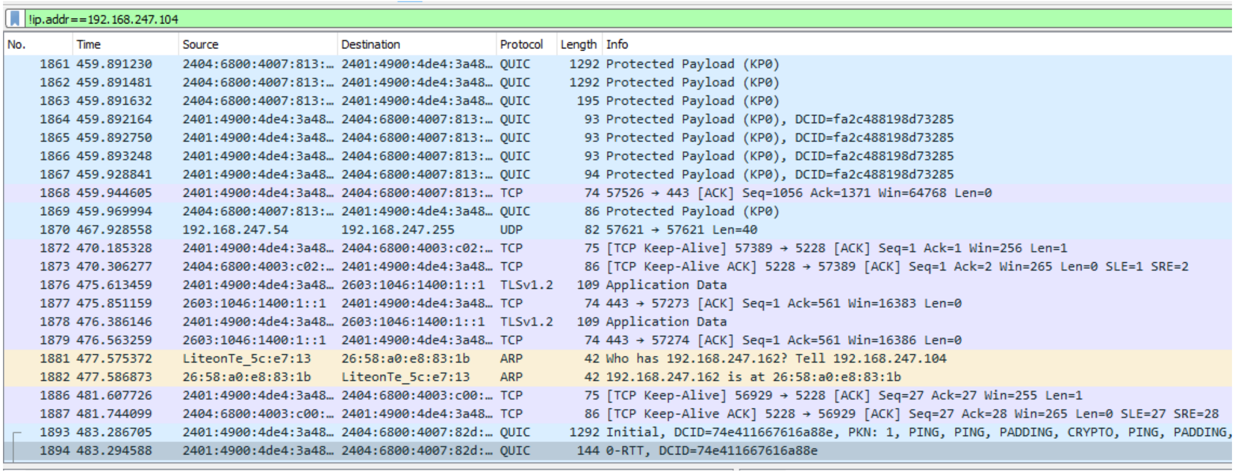
icmp

```
No.    Time         Source            Destination       Protocol  Length Info
    15 2.930824     192.168.247.104   192.168.247.162   ICMP       127 Destination unreachable (Port unreachable)
   469 96.890417    192.168.247.104   192.168.247.162   ICMP       252 Destination unreachable (Port unreachable)
  1162 358.109413   192.168.247.104   192.168.247.162   ICMP       174 Destination unreachable (Port unreachable)
  1560 395.992876   192.168.247.104   192.168.247.162   ICMP       225 Destination unreachable (Port unreachable)
  1896 483.366553   192.168.247.104   192.168.247.162   ICMP       127 Destination unreachable (Port unreachable)
  2471 673.990161   192.168.247.104   192.168.247.162   ICMP       148 Destination unreachable (Port unreachable)
```

5. Exclude IP address

If you want to filter out an IP address so it’s not displayed use this filter.

!ip.addr==192.168.247.104

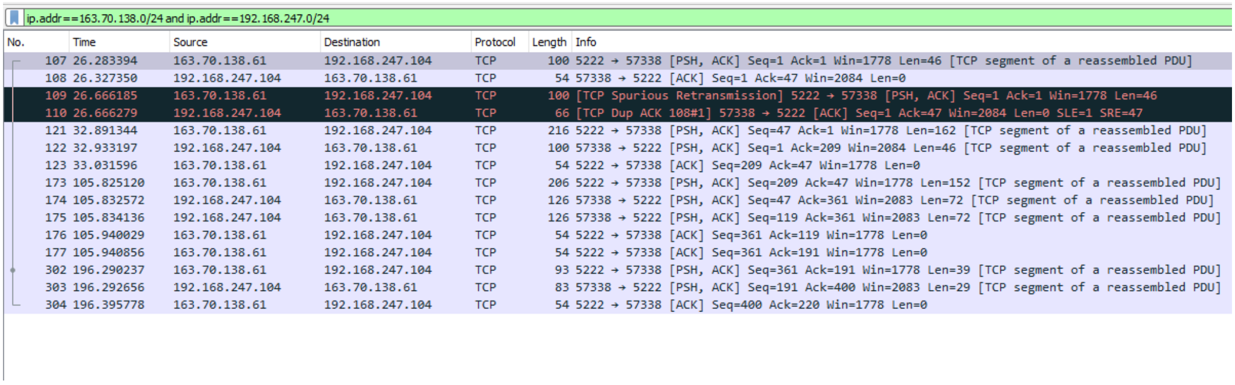


```
!ip.addr==192.168.247.104
No.   Time        Source                  Destination             Protocol Length Info
 1861 459.891230  2404:6800:4007:813:…   2401:4900:4de4:3a48…    QUIC     1292 Protected Payload (KP0)
 1862 459.891481  2404:6800:4007:813:…   2401:4900:4de4:3a48…    QUIC     1292 Protected Payload (KP0)
 1863 459.891632  2404:6800:4007:813:…   2401:4900:4de4:3a48…    QUIC      195 Protected Payload (KP0)
 1864 459.892164  2401:4900:4de4:3a48…   2404:6800:4007:813:…    QUIC       93 Protected Payload (KP0), DCID=fa2c488198d73285
 1865 459.892750  2401:4900:4de4:3a48…   2404:6800:4007:813:…    QUIC       93 Protected Payload (KP0), DCID=fa2c488198d73285
 1866 459.893248  2401:4900:4de4:3a48…   2404:6800:4007:813:…    QUIC       93 Protected Payload (KP0), DCID=fa2c488198d73285
 1867 459.928841  2401:4900:4de4:3a48…   2404:6800:4007:813:…    QUIC       94 Protected Payload (KP0), DCID=fa2c488198d73285
 1868 459.944605  2401:4900:4de4:3a48…   2404:6800:4007:813:…    TCP        74 57526 → 443 [ACK] Seq=1056 Ack=1371 Win=64768 Len=0
 1869 459.969994  2404:6800:4007:813:…   2401:4900:4de4:3a48…    QUIC       86 Protected Payload (KP0)
 1870 467.928558  192.168.247.54          192.168.247.255         UDP        82 57621 → 57621 Len=40
 1872 470.185328  2401:4900:4de4:3a48…   2404:6800:4003:c02:…    TCP        75 [TCP Keep-Alive] 57389 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
 1873 470.306277  2404:6800:4003:c02:…   2401:4900:4de4:3a48…    TCP        86 [TCP Keep-Alive ACK] 5228 → 57389 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
 1876 475.613459  2401:4900:4de4:3a48…   2603:1046:1400:1::1     TLSv1.2   109 Application Data
 1877 475.851159  2603:1046:1400:1::1     2401:4900:4de4:3a48…    TCP        74 443 → 57273 [ACK] Seq=1 Ack=561 Win=16383 Len=0
 1878 476.386146  2401:4900:4de4:3a48…   2603:1046:1400:1::1     TLSv1.2   109 Application Data
 1879 476.563259  2603:1046:1400:1::1     2401:4900:4de4:3a48…    TCP        74 443 → 57274 [ACK] Seq=1 Ack=561 Win=16386 Len=0
 1881 477.575372  LiteonTe_5c:e7:13       26:58:a0:e8:83:1b       ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
 1882 477.586873  26:58:a0:e8:83:1b       LiteonTe_5c:e7:13       ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
 1886 481.607726  2401:4900:4de4:3a48…   2404:6800:4003:c00:…    TCP        75 [TCP Keep-Alive] 56929 → 5228 [ACK] Seq=27 Ack=27 Win=255 Len=1
 1887 481.744099  2404:6800:4003:c00:…   2401:4900:4de4:3a48…    TCP        86 [TCP Keep-Alive ACK] 5228 → 56929 [ACK] Seq=27 Ack=28 Win=265 Len=0 SLE=27 SRE=28
 1893 483.286705  2401:4900:4de4:3a48…   2404:6800:4007:82d:…    QUIC     1292 Initial, DCID=74e411667616a88e, PKN: 1, PING, PING, PADDING, CRYPTO, PING, PADDING,
 1894 483.294588  2401:4900:4de4:3a48…   2404:6800:4007:82d:…    QUIC      144 0-RTT, DCID=74e411667616a88e
```

6. Show traffic between two workstations or subnet

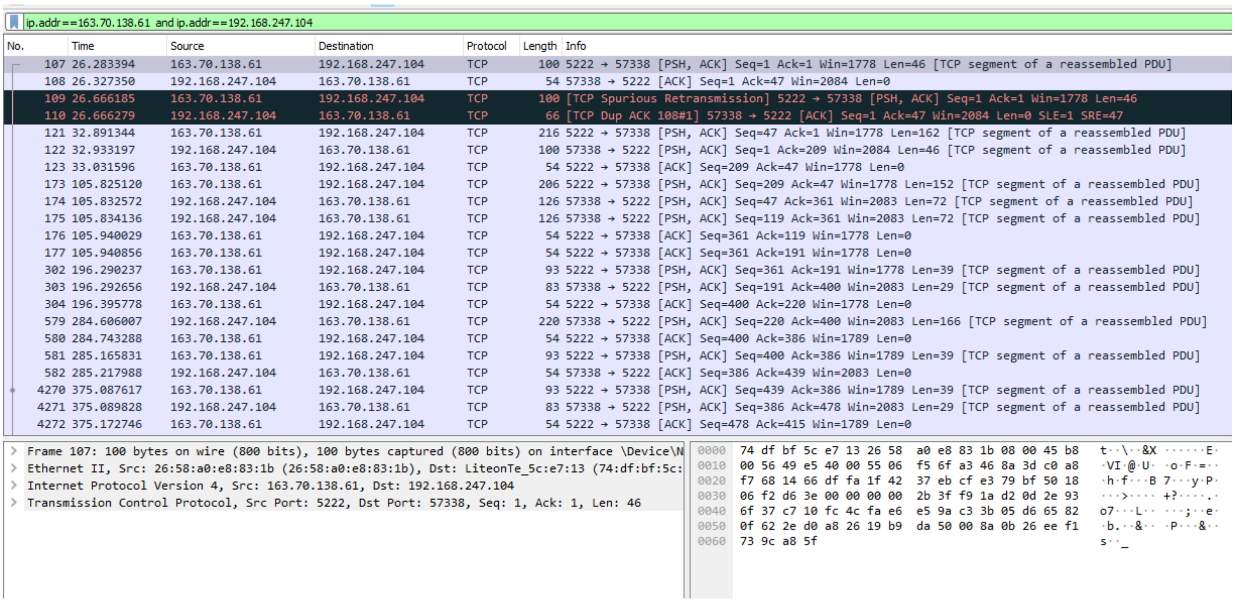
This first one will show only traffic between the twosubnets.

ip.addr==163.70.138.0/24 and ip.addr==192.168.247.0/24



```
ip.addr==163.70.138.0/24 and ip.addr==192.168.247.0/24
No.  Time        Source            Destination       Protocol Length Info
 107 26.283394   163.70.138.61     192.168.247.104   TCP       100 5222 → 57338 [PSH, ACK] Seq=1 Ack=1 Win=1778 Len=46 [TCP segment of a reassembled PDU]
 108 26.327350   192.168.247.104   163.70.138.61     TCP        54 57338 → 5222 [ACK] Seq=1 Ack=47 Win=2084 Len=0
 109 26.666185   163.70.138.61     192.168.247.104   TCP       100 [TCP Spurious Retransmission] 5222 → 57338 [PSH, ACK] Seq=1 Ack=1 Win=1778 Len=46
 110 26.666279   192.168.247.104   163.70.138.61     TCP        66 [TCP Dup ACK 108#1] 57338 → 5222 [ACK] Seq=1 Ack=47 Win=2084 Len=0 SLE=1 SRE=47
 121 32.891344   163.70.138.61     192.168.247.104   TCP       216 5222 → 57338 [PSH, ACK] Seq=47 Ack=1 Win=1778 Len=162 [TCP segment of a reassembled PDU]
 122 32.933197   192.168.247.104   163.70.138.61     TCP       100 57338 → 5222 [PSH, ACK] Seq=1 Ack=209 Win=2084 Len=46 [TCP segment of a reassembled PDU]
 123 33.031596   163.70.138.61     192.168.247.104   TCP        54 5222 → 57338 [ACK] Seq=209 Ack=47 Win=1778 Len=0
 173 105.825120  163.70.138.61     192.168.247.104   TCP       206 5222 → 57338 [PSH, ACK] Seq=209 Ack=47 Win=1778 Len=152 [TCP segment of a reassembled PDU]
 174 105.832572  192.168.247.104   163.70.138.61     TCP       126 57338 → 5222 [PSH, ACK] Seq=47 Ack=361 Win=2083 Len=72 [TCP segment of a reassembled PDU]
 175 105.834136  192.168.247.104   163.70.138.61     TCP       126 57338 → 5222 [PSH, ACK] Seq=119 Ack=361 Win=2083 Len=72 [TCP segment of a reassembled PDU]
 176 105.940029  163.70.138.61     192.168.247.104   TCP        54 5222 → 57338 [ACK] Seq=361 Ack=119 Win=1778 Len=0
 177 105.940856  163.70.138.61     192.168.247.104   TCP        54 5222 → 57338 [ACK] Seq=361 Ack=191 Win=1778 Len=0
 302 196.290237  163.70.138.61     192.168.247.104   TCP        93 5222 → 57338 [PSH, ACK] Seq=361 Ack=191 Win=1778 Len=39 [TCP segment of a reassembled PDU]
 303 196.292656  192.168.247.104   163.70.138.61     TCP        83 57338 → 5222 [PSH, ACK] Seq=191 Ack=400 Win=2083 Len=29 [TCP segment of a reassembled PDU]
 304 196.395778  163.70.138.61     192.168.247.104   TCP        54 5222 → 57338 [ACK] Seq=400 Ack=220 Win=1778 Len=0
```

This will show only traffic between the two specific IP address ip.addr==163.70.138.61 and ip.addr==192.168.247.104



```
ip.addr==163.70.138.61 and ip.addr==192.168.247.104
```

```
No.   Time        Source           Destination      Protocol Length Info
  107 26.283394   163.70.138.61    192.168.247.104  TCP      100 5222 → 57338 [PSH, ACK] Seq=1 Ack=1 Win=1778 Len=46 [TCP segment of a reassembled PDU]
  108 26.327350   192.168.247.104  163.70.138.61    TCP       54 57338 → 5222 [ACK] Seq=1 Ack=47 Win=2084 Len=0
  109 26.666185   163.70.138.61    192.168.247.104  TCP      100 [TCP Spurious Retransmission] 5222 → 57338 [PSH, ACK] Seq=1 Ack=1 Win=1778 Len=46
  110 26.666279   192.168.247.104  163.70.138.61    TCP       66 [TCP Dup ACK 108#1] 57338 → 5222 [ACK] Seq=1 Ack=47 Win=2084 Len=0 SLE=1 SRE=47
  121 32.891344   163.70.138.61    192.168.247.104  TCP      216 5222 → 57338 [PSH, ACK] Seq=47 Ack=1 Win=1778 Len=162 [TCP segment of a reassembled PDU]
  122 32.933197   192.168.247.104  163.70.138.61    TCP      100 57338 → 5222 [PSH, ACK] Seq=1 Ack=209 Win=2084 Len=46 [TCP segment of a reassembled PDU]
  123 33.031596   163.70.138.61    192.168.247.104  TCP       54 5222 → 57338 [ACK] Seq=209 Ack=47 Win=1778 Len=0
  173 105.825120  163.70.138.61    192.168.247.104  TCP      206 5222 → 57338 [PSH, ACK] Seq=209 Ack=47 Win=1778 Len=152 [TCP segment of a reassembled PDU]
  174 105.832572  192.168.247.104  163.70.138.61    TCP      126 57338 → 5222 [PSH, ACK] Seq=47 Ack=361 Win=2083 Len=72 [TCP segment of a reassembled PDU]
  175 105.834136  192.168.247.104  163.70.138.61    TCP      126 57338 → 5222 [PSH, ACK] Seq=119 Ack=361 Win=2083 Len=72 [TCP segment of a reassembled PDU]
  176 105.940029  163.70.138.61    192.168.247.104  TCP       54 5222 → 57338 [ACK] Seq=361 Ack=119 Win=1778 Len=0
  177 105.940856  163.70.138.61    192.168.247.104  TCP       54 5222 → 57338 [ACK] Seq=361 Ack=191 Win=1778 Len=0
  302 196.290237  163.70.138.61    192.168.247.104  TCP       93 5222 → 57338 [PSH, ACK] Seq=361 Ack=191 Win=1778 Len=39 [TCP segment of a reassembled PDU]
  303 196.292656  192.168.247.104  163.70.138.61    TCP       83 57338 → 5222 [PSH, ACK] Seq=191 Ack=400 Win=2083 Len=29 [TCP segment of a reassembled PDU]
  304 196.395778  163.70.138.61    192.168.247.104  TCP       54 5222 → 57338 [ACK] Seq=400 Ack=220 Win=1778 Len=0
  579 284.606007  192.168.247.104  163.70.138.61    TCP      220 57338 → 5222 [PSH, ACK] Seq=220 Ack=400 Win=2083 Len=166 [TCP segment of a reassembled PDU]
  580 284.743288  163.70.138.61    192.168.247.104  TCP       54 5222 → 57338 [ACK] Seq=400 Ack=386 Win=1789 Len=0
  581 285.165831  163.70.138.61    192.168.247.104  TCP       93 5222 → 57338 [PSH, ACK] Seq=400 Ack=386 Win=1789 Len=39 [TCP segment of a reassembled PDU]
  582 285.217988  192.168.247.104  163.70.138.61    TCP       54 57338 → 5222 [ACK] Seq=386 Ack=439 Win=2083 Len=0
 4270 375.087617  163.70.138.61    192.168.247.104  TCP       93 5222 → 57338 [PSH, ACK] Seq=439 Ack=386 Win=1789 Len=39 [TCP segment of a reassembled PDU]
 4271 375.089828  192.168.247.104  163.70.138.61    TCP       83 57338 → 5222 [PSH, ACK] Seq=386 Ack=478 Win=2083 Len=29 [TCP segment of a reassembled PDU]
 4272 375.172746  163.70.138.61    192.168.247.104  TCP       54 5222 → 57338 [ACK] Seq=478 Ack=415 Win=1789 Len=0
```

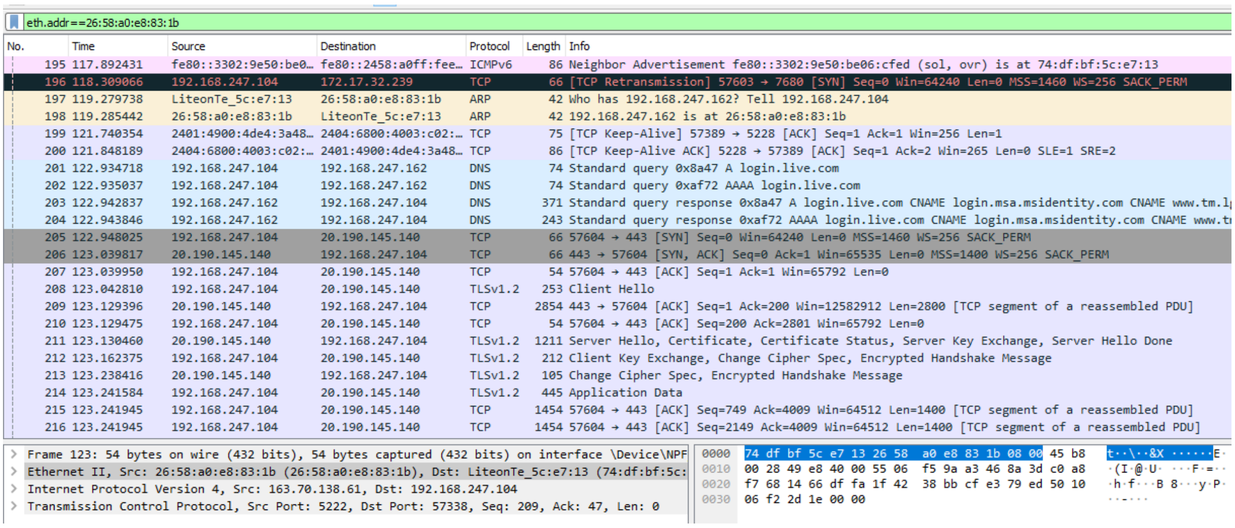
```
> Frame 107: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\N
> Ethernet II, Src: 26:58:a0:e8:83:1b (26:58:a0:e8:83:1b), Dst: LiteonTe_5c:e7:13 (74:df:bf:5c:
> Internet Protocol Version 4, Src: 163.70.138.61, Dst: 192.168.247.104
> Transmission Control Protocol, Src Port: 5222, Dst Port: 57338, Seq: 1, Ack: 1, Len: 46
```

```
0000  74 df bf 5c e7 13 26 58  a0 e8 83 1b 08 00 45 b8   t··\··&X ······E·
0010  00 56 49 e5 40 00 55 06  f5 6f a3 46 8a 3d c0 a8   ·VI·@·U· ·o·F·=··
0020  f7 68 14 66 df fa 1f 42  37 eb cf e3 79 bf 50 18   ·h·f···B 7···y·P·
0030  06 f2 d6 3e 00 00 00 00  2b 3f f9 1a d2 0d 2e 93   ···>···· +?····.·
0040  6f 37 c7 10 fc 4c fa e6  e5 9a c3 3b 05 d6 65 82   o7···L·· ···;··e·
0050  0f 62 2e d0 a8 26 19 b9  da 50 00 8a 0b 26 ee f1   ·b.··&·· ·P···&··
0060  73 9c a8 5f                                        s··_
```

7. Filter by MAC address

If you only want to see traffic for a specific MAC address use this filter

eth.addr==26:58:a0:e8:83:1b



```
eth.addr==26:58:a0:e8:83:1b
```

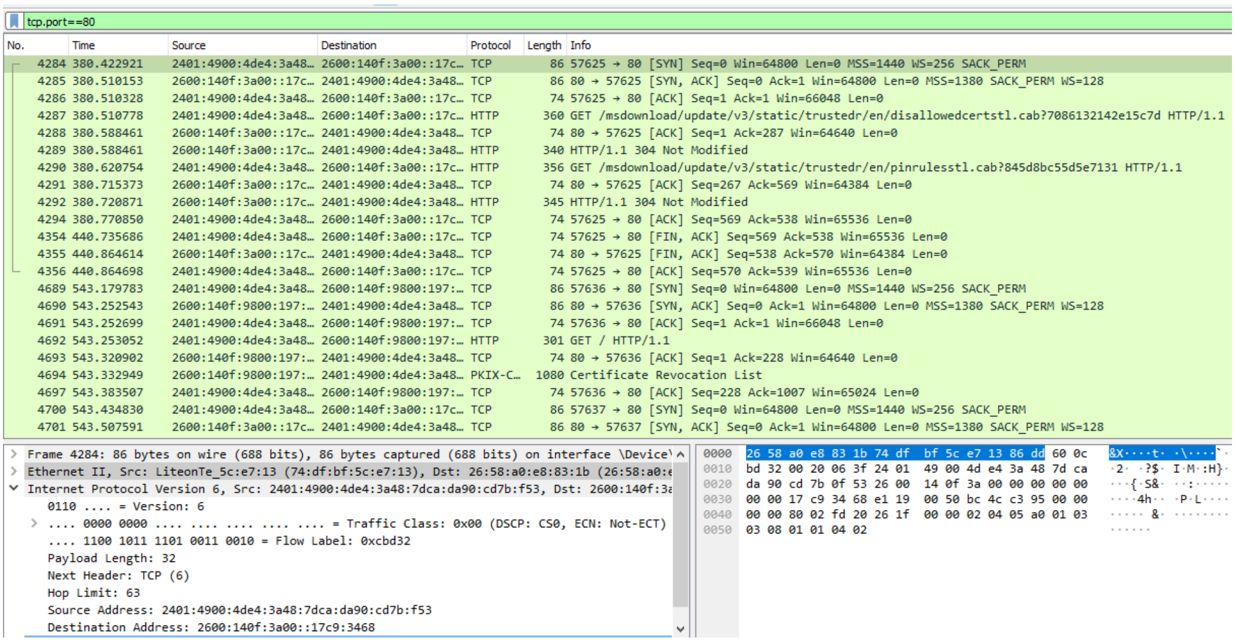
```
No.   Time        Source                   Destination              Protocol Length Info
  195 117.892431  fe80::3302:9e50:be0…     fe80::2458:a0ff:fee…     ICMPv6     86 Neighbor Advertisement fe80::3302:9e50:be06:cfed (sol, ovr) is at 74:df:bf:5c:e7:13
  196 118.309066  192.168.247.104          172.17.32.239            TCP        66 [TCP Retransmission] 57603 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  197 119.279738  LiteonTe_5c:e7:13        26:58:a0:e8:83:1b        ARP        42 Who has 192.168.247.162? Tell 192.168.247.104
  198 119.285442  26:58:a0:e8:83:1b        LiteonTe_5c:e7:13        ARP        42 192.168.247.162 is at 26:58:a0:e8:83:1b
  199 121.740354  2401:4900:4de4:3a48…     2404:6800:4003:c02:…     TCP        75 [TCP Keep-Alive] 57389 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
  200 121.848189  2404:6800:4003:c02:…     2401:4900:4de4:3a48…     TCP        86 [TCP Keep-Alive ACK] 5228 → 57389 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
  201 122.934718  192.168.247.104          192.168.247.162          DNS        74 Standard query 0x8a47 A login.live.com
  202 122.935037  192.168.247.104          192.168.247.162          DNS        74 Standard query 0xaf72 AAAA login.live.com
  203 122.942837  192.168.247.162          192.168.247.104          DNS       371 Standard query response 0x8a47 A login.live.com CNAME login.msa.msidentity.com CNAME www.tm.l
  204 122.943846  192.168.247.162          192.168.247.104          DNS       243 Standard query response 0xaf72 AAAA login.live.com CNAME login.msa.msidentity.com CNAME www.t
  205 122.948025  192.168.247.104          20.190.145.140           TCP        66 57604 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  206 123.039817  20.190.145.140           192.168.247.104          TCP        66 443 → 57604 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
  207 123.039950  192.168.247.104          20.190.145.140           TCP        54 57604 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
  208 123.042810  192.168.247.104          20.190.145.140           TLSv1.2   253 Client Hello
  209 123.129396  20.190.145.140           192.168.247.104          TCP      2854 443 → 57604 [ACK] Seq=1 Ack=200 Win=12582912 Len=2800 [TCP segment of a reassembled PDU]
  210 123.129475  192.168.247.104          20.190.145.140           TCP        54 57604 → 443 [ACK] Seq=200 Ack=2801 Win=65792 Len=0
  211 123.130460  20.190.145.140           192.168.247.104          TLSv1.2  1211 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
  212 123.162375  192.168.247.104          20.190.145.140           TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  213 123.238416  20.190.145.140           192.168.247.104          TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  214 123.241584  192.168.247.104          20.190.145.140           TLSv1.2   445 Application Data
  215 123.241945  192.168.247.104          20.190.145.140           TCP      1454 57604 → 443 [ACK] Seq=749 Ack=4009 Win=64512 Len=1400 [TCP segment of a reassembled PDU]
  216 123.241945  192.168.247.104          20.190.145.140           TCP      1454 57604 → 443 [ACK] Seq=2149 Ack=4009 Win=64512 Len=1400 [TCP segment of a reassembled PDU]
```

```
> Frame 123: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF
> Ethernet II, Src: 26:58:a0:e8:83:1b (26:58:a0:e8:83:1b), Dst: LiteonTe_5c:e7:13 (74:df:bf:5c:
> Internet Protocol Version 4, Src: 163.70.138.61, Dst: 192.168.247.104
> Transmission Control Protocol, Src Port: 5222, Dst Port: 57338, Seq: 209, Ack: 47, Len: 0
```

```
0000  74 df bf 5c e7 13 26 58  a0 e8 83 1b 08 00 45 b8   t··\··&X ······E·
0010  00 28 49 e8 40 00 55 06  f5 9a a3 46 8a 3d c0 a8   ·(I·@·U· ···F·=··
0020  f7 68 14 66 df fa 1f 42  38 bb cf e3 79 ed 50 10   ·h·f···B 8···y·P·
0030  06 f2 2d 1e 00 00                                  ··-···
```

8. Filter on TCP port

tcp.port==80



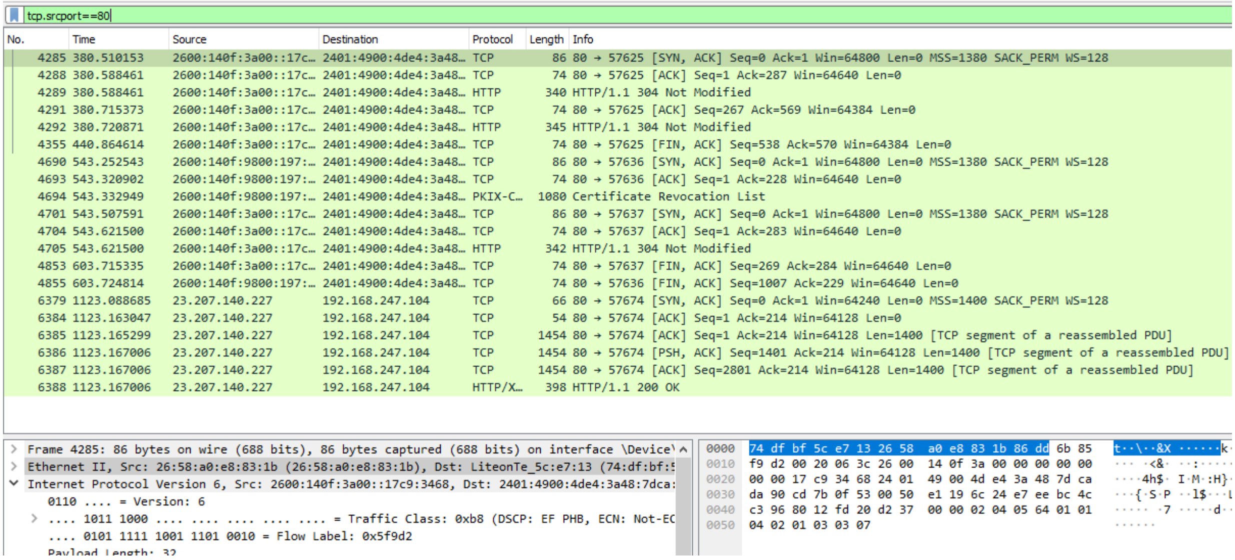
```
tcp.port==80

No.     Time        Source                 Destination            Protocol  Length Info
   4284 380.422921  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   TCP         86 57625 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
   4285 380.510153  2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         86 80 → 57625 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1380 SACK_PERM WS=128
   4286 380.510328  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   TCP         74 57625 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
   4287 380.510778  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   HTTP       360 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?7086132142e15c7d HTTP/1.1
   4288 380.588461  2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57625 [ACK] Seq=1 Ack=287 Win=64640 Len=0
   4289 380.588461  2600:140f:3a00::17c…   2401:4900:4de4:3a48…   HTTP       340 HTTP/1.1 304 Not Modified
   4290 380.620754  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   HTTP       356 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?845d8bc55d5e7131 HTTP/1.1
   4291 380.715373  2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57625 [ACK] Seq=267 Ack=569 Win=64384 Len=0
   4292 380.720871  2600:140f:3a00::17c…   2401:4900:4de4:3a48…   HTTP       345 HTTP/1.1 304 Not Modified
   4294 380.770850  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   TCP         74 57625 → 80 [ACK] Seq=569 Ack=538 Win=65536 Len=0
   4354 440.735686  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   TCP         74 57625 → 80 [FIN, ACK] Seq=569 Ack=538 Win=65536 Len=0
   4355 440.864614  2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57625 [FIN, ACK] Seq=538 Ack=570 Win=64384 Len=0
   4356 440.864698  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   TCP         74 57625 → 80 [ACK] Seq=570 Ack=539 Win=65536 Len=0
   4689 543.179783  2401:4900:4de4:3a48…   2600:140f:9800:197:…   TCP         86 57636 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
   4690 543.252543  2600:140f:9800:197:…   2401:4900:4de4:3a48…   TCP         86 80 → 57636 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1380 SACK_PERM WS=128
   4691 543.252699  2401:4900:4de4:3a48…   2600:140f:9800:197:…   TCP         74 57636 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
   4692 543.253052  2401:4900:4de4:3a48…   2600:140f:9800:197:…   HTTP       301 GET / HTTP/1.1
   4693 543.320902  2600:140f:9800:197:…   2401:4900:4de4:3a48…   TCP         74 80 → 57636 [ACK] Seq=1 Ack=228 Win=64640 Len=0
   4694 543.332949  2600:140f:9800:197:…   2401:4900:4de4:3a48…   PKIX-C…   1080 Certificate Revocation List
   4697 543.383507  2401:4900:4de4:3a48…   2600:140f:9800:197:…   TCP         74 57636 → 80 [ACK] Seq=228 Ack=1007 Win=65024 Len=0
   4700 543.434830  2401:4900:4de4:3a48…   2600:140f:3a00::17c…   TCP         86 57637 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
   4701 543.507591  2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         86 80 → 57637 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1380 SACK_PERM WS=128
```

```
> Frame 4284: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\
> Ethernet II, Src: LiteonTe_5c:e7:13 (74:df:bf:5c:e7:13), Dst: 26:58:a0:e8:83:1b (26:58:a0:e
v Internet Protocol Version 6, Src: 2401:4900:4de4:3a48:7dca:da90:cd7b:f53, Dst: 2600:140f:3a
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1100 1011 1101 0011 0010 = Flow Label: 0xcbd32
    Payload Length: 32
    Next Header: TCP (6)
    Hop Limit: 63
    Source Address: 2401:4900:4de4:3a48:7dca:da90:cd7b:f53
    Destination Address: 2600:140f:3a00::17c9:3468
```

```
0000  26 58 a0 e8 83 1b 74 df  bf 5c e7 13 86 dd 60 0c   &X····t· ·\····`·
0010  bd 32 00 20 06 3f 24 01  49 00 4d e4 3a 48 7d ca   ·2· ·?$· I·M·:H}·
0020  da 90 cd 7b 0f 53 26 00  14 0f 3a 00 00 00 00 00   ···{·S&· ··:·····
0030  00 00 17 c9 34 68 e1 19  00 50 bc 4c c3 95 00 00   ····4h·· ·P·L····
0040  00 00 80 02 fd 20 26 1f  00 00 02 04 05 a0 01 03   ····· &· ········
0050  03 08 01 01 04 02                                  ······
```

Filter on TCP port source

tcp.srcport==80



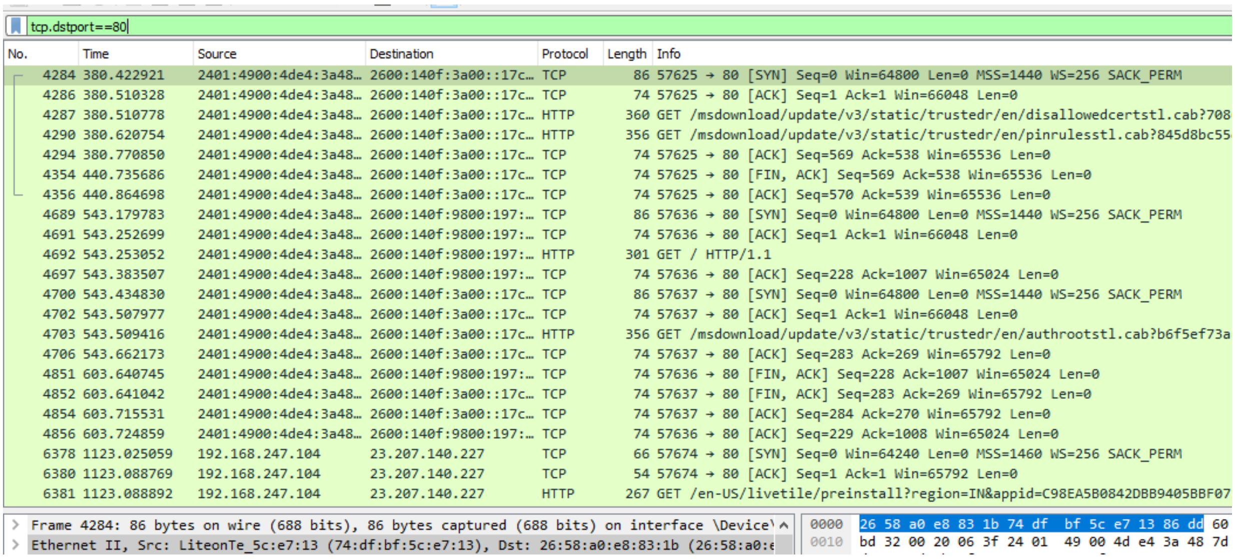
```
tcp.srcport==80

No.     Time         Source                 Destination            Protocol  Length Info
   4285 380.510153   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         86 80 → 57625 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1380 SACK_PERM WS=128
   4288 380.588461   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57625 [ACK] Seq=1 Ack=287 Win=64640 Len=0
   4289 380.588461   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   HTTP       340 HTTP/1.1 304 Not Modified
   4291 380.715373   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57625 [ACK] Seq=267 Ack=569 Win=64384 Len=0
   4292 380.720871   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   HTTP       345 HTTP/1.1 304 Not Modified
   4355 440.864614   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57625 [FIN, ACK] Seq=538 Ack=570 Win=64384 Len=0
   4690 543.252543   2600:140f:9800:197:…   2401:4900:4de4:3a48…   TCP         86 80 → 57636 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1380 SACK_PERM WS=128
   4693 543.320902   2600:140f:9800:197:…   2401:4900:4de4:3a48…   TCP         74 80 → 57636 [ACK] Seq=1 Ack=228 Win=64640 Len=0
   4694 543.332949   2600:140f:9800:197:…   2401:4900:4de4:3a48…   PKIX-C…   1080 Certificate Revocation List
   4701 543.507591   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         86 80 → 57637 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1380 SACK_PERM WS=128
   4704 543.621500   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57637 [ACK] Seq=1 Ack=283 Win=64640 Len=0
   4705 543.621500   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   HTTP       342 HTTP/1.1 304 Not Modified
   4853 603.715335   2600:140f:3a00::17c…   2401:4900:4de4:3a48…   TCP         74 80 → 57637 [FIN, ACK] Seq=269 Ack=284 Win=64640 Len=0
   4855 603.724814   2600:140f:9800:197:…   2401:4900:4de4:3a48…   TCP         74 80 → 57636 [FIN, ACK] Seq=1007 Ack=229 Win=64640 Len=0
   6379 1123.088685  23.207.140.227         192.168.247.104        TCP         66 80 → 57674 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=128
   6384 1123.163047  23.207.140.227         192.168.247.104        TCP         54 80 → 57674 [ACK] Seq=1 Ack=214 Win=64128 Len=0
   6385 1123.165299  23.207.140.227         192.168.247.104        TCP       1454 80 → 57674 [ACK] Seq=1 Ack=214 Win=64128 Len=1400 [TCP segment of a reassembled PDU]
   6386 1123.167006  23.207.140.227         192.168.247.104        TCP       1454 80 → 57674 [PSH, ACK] Seq=1401 Ack=214 Win=64128 Len=1400 [TCP segment of a reassembled PDU]
   6387 1123.167006  23.207.140.227         192.168.247.104        TCP       1454 80 → 57674 [ACK] Seq=2801 Ack=214 Win=64128 Len=1400 [TCP segment of a reassembled PDU]
   6388 1123.167006  23.207.140.227         192.168.247.104        HTTP/X…    398 HTTP/1.1 200 OK
```

```
> Frame 4285: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\
> Ethernet II, Src: 26:58:a0:e8:83:1b (26:58:a0:e8:83:1b), Dst: LiteonTe_5c:e7:13 (74:df:bf:5
v Internet Protocol Version 6, Src: 2600:140f:3a00::17c9:3468, Dst: 2401:4900:4de4:3a48:7dca:
    0110 .... = Version: 6
  > .... 1011 1000 .... .... .... .... .... = Traffic Class: 0xb8 (DSCP: EF PHB, ECN: Not-EC
    .... 0101 1111 1001 1101 0010 = Flow Label: 0x5f9d2
    Payload Length: 32
```

```
0000  74 df bf 5c e7 13 26 58  a0 e8 83 1b 86 dd 6b 85   t··\··&X ······k·
0010  f9 d2 00 20 06 3c 26 00  14 0f 3a 00 00 00 00 00   ··· ·<&· ··:·····
0020  00 00 17 c9 34 68 24 01  49 00 4d e4 3a 48 7d ca   ····4h$· I·M·:H}·
0030  da 90 cd 7b 0f 53 00 50  e1 19 6c 24 e7 ee bc 4c   ···{·S·P ··l$···L
0040  c3 96 80 12 fd 20 d2 37  00 00 02 04 05 64 01 01   ····· ·7 ·····d··
0050  04 02 01 03 03 07                                  ······
```

or destination port

tcp.dstport==80



tcp.dstport==80

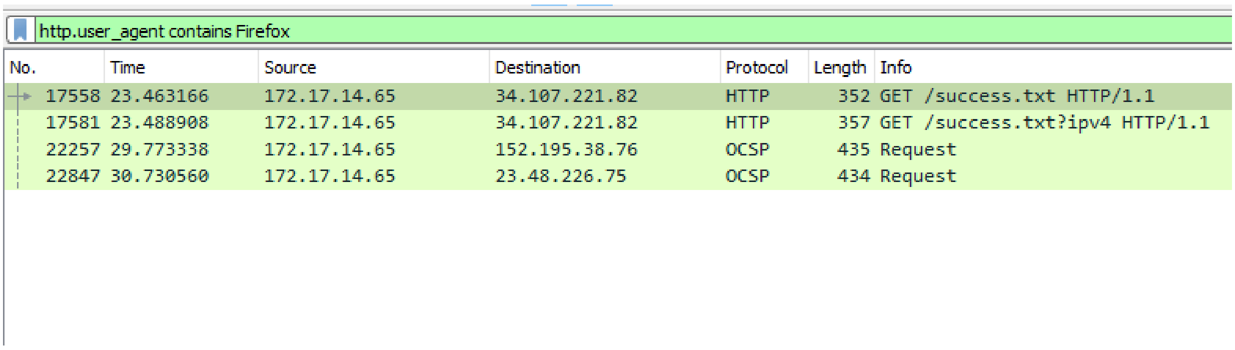
No.	Time	Source	Destination	Protocol	Length	Info
4284	380.422921	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	86	57625 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
4286	380.510328	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57625 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4287	380.510778	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	HTTP	360	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?708
4290	380.620754	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	HTTP	356	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?845d8bc55
4294	380.770850	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57625 → 80 [ACK] Seq=569 Ack=538 Win=65536 Len=0
4354	440.735686	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57625 → 80 [FIN, ACK] Seq=569 Ack=538 Win=65536 Len=0
4356	440.864698	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57625 → 80 [ACK] Seq=570 Ack=539 Win=65536 Len=0
4689	543.179783	2401:4900:4de4:3a48…	2600:140f:9800:197:…	TCP	86	57636 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
4691	543.252699	2401:4900:4de4:3a48…	2600:140f:9800:197:…	TCP	74	57636 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4692	543.253052	2401:4900:4de4:3a48…	2600:140f:9800:197:…	HTTP	301	GET / HTTP/1.1
4697	543.383507	2401:4900:4de4:3a48…	2600:140f:9800:197:…	TCP	74	57636 → 80 [ACK] Seq=228 Ack=1007 Win=65024 Len=0
4700	543.434830	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	86	57637 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
4702	543.507977	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57637 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4703	543.509416	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	HTTP	356	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?b6f5ef73a
4706	543.662173	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57637 → 80 [ACK] Seq=283 Ack=269 Win=65792 Len=0
4851	603.640745	2401:4900:4de4:3a48…	2600:140f:9800:197:…	TCP	74	57636 → 80 [FIN, ACK] Seq=228 Ack=1007 Win=65024 Len=0
4852	603.641042	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57637 → 80 [FIN, ACK] Seq=283 Ack=269 Win=65792 Len=0
4854	603.715531	2401:4900:4de4:3a48…	2600:140f:3a00::17c…	TCP	74	57637 → 80 [ACK] Seq=284 Ack=270 Win=65792 Len=0
4856	603.724859	2401:4900:4de4:3a48…	2600:140f:9800:197:…	TCP	74	57636 → 80 [ACK] Seq=229 Ack=1008 Win=65024 Len=0
6378	1123.025059	192.168.247.104	23.207.140.227	TCP	66	57674 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6380	1123.088769	192.168.247.104	23.207.140.227	TCP	54	57674 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
6381	1123.088892	192.168.247.104	23.207.140.227	HTTP	267	GET /en-US/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF07

```
> Frame 4284: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\
> Ethernet II, Src: LiteonTe_5c:e7:13 (74:df:bf:5c:e7:13), Dst: 26:58:a0:e8:83:1b (26:58:a0:e

0000  26 58 a0 e8 83 1b 74 df  bf 5c e7 13 86 dd 60
0010  bd 32 00 20 06 3f 24 01  49 00 4d e4 3a 48 7d
```

9. Find user agents

Its a good idea to understand what user agents are being used on your network, malicious traffic can often use unusual agent strings. To search for a user agent use this filter

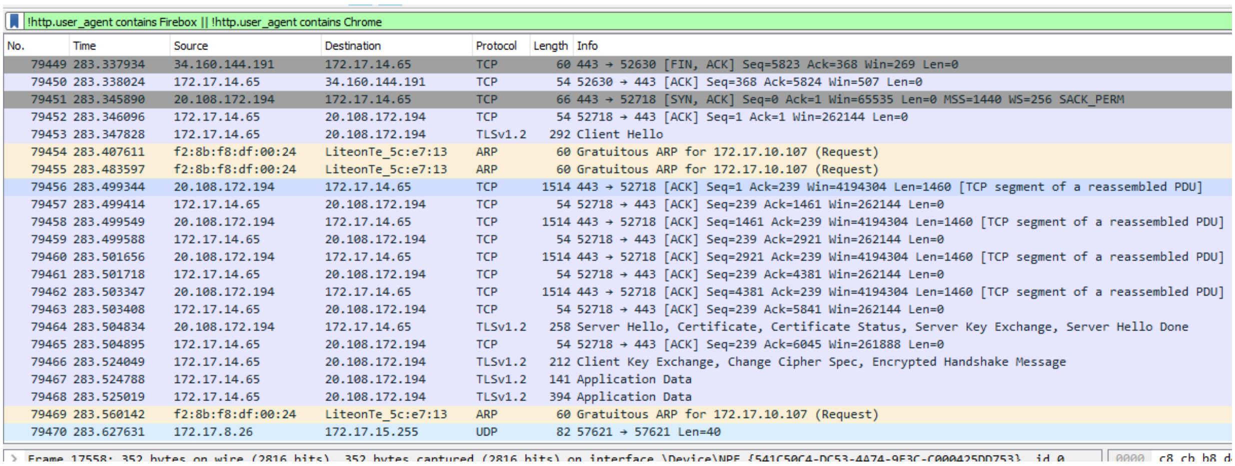
http.user_agent contains Firefox



http.user_agent contains Firefox

No.	Time	Source	Destination	Protocol	Length	Info
17558	23.463166	172.17.14.65	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
17581	23.488908	172.17.14.65	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
22257	29.773338	172.17.14.65	152.195.38.76	OCSP	435	Request
22847	30.730560	172.17.14.65	23.48.226.75	OCSP	434	Request

!http.user_agent contains Firefox || !http.user_agent contains Chrome

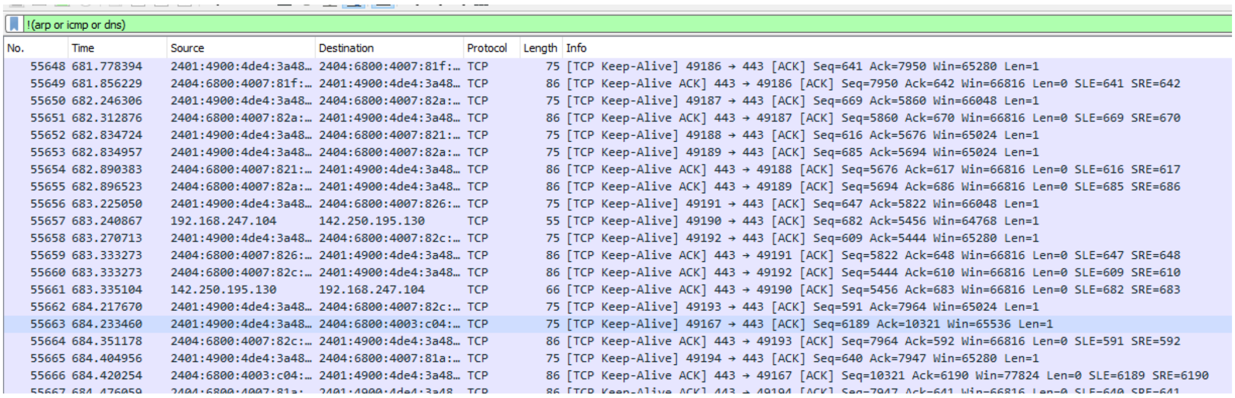


```
!http.user_agent contains Firebox || !http.user_agent contains Chrome

No.   Time        Source             Destination        Protocol Length Info
79449 283.337934  34.160.144.191     172.17.14.65       TCP        60 443 → 52630 [FIN, ACK] Seq=5823 Ack=368 Win=269 Len=0
79450 283.338024  172.17.14.65       34.160.144.191     TCP        54 52630 → 443 [ACK] Seq=368 Ack=5824 Win=507 Len=0
79451 283.345890  20.108.172.194     172.17.14.65       TCP        66 443 → 52718 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
79452 283.346096  172.17.14.65       20.108.172.194     TCP        54 52718 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
79453 283.347828  172.17.14.65       20.108.172.194     TLSv1.2   292 Client Hello
79454 283.407611  f2:8b:f8:df:00:24  LiteonTe_5c:e7:13  ARP        60 Gratuitous ARP for 172.17.10.107 (Request)
79455 283.483597  f2:8b:f8:df:00:24  LiteonTe_5c:e7:13  ARP        60 Gratuitous ARP for 172.17.10.107 (Request)
79456 283.499344  20.108.172.194     172.17.14.65       TCP      1514 443 → 52718 [ACK] Seq=1 Ack=239 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
79457 283.499414  172.17.14.65       20.108.172.194     TCP        54 52718 → 443 [ACK] Seq=239 Ack=1461 Win=262144 Len=0
79458 283.499549  20.108.172.194     172.17.14.65       TCP      1514 443 → 52718 [ACK] Seq=1461 Ack=239 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
79459 283.499588  172.17.14.65       20.108.172.194     TCP        54 52718 → 443 [ACK] Seq=239 Ack=2921 Win=262144 Len=0
79460 283.501656  20.108.172.194     172.17.14.65       TCP      1514 443 → 52718 [ACK] Seq=2921 Ack=239 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
79461 283.501718  172.17.14.65       20.108.172.194     TCP        54 52718 → 443 [ACK] Seq=239 Ack=4381 Win=262144 Len=0
79462 283.503347  20.108.172.194     172.17.14.65       TCP      1514 443 → 52718 [ACK] Seq=4381 Ack=239 Win=4194304 Len=1460 [TCP segment of a reassembled PDU]
79463 283.503408  172.17.14.65       20.108.172.194     TCP        54 52718 → 443 [ACK] Seq=239 Ack=5841 Win=262144 Len=0
79464 283.504834  20.108.172.194     172.17.14.65       TLSv1.2   258 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
79465 283.504895  172.17.14.65       20.108.172.194     TCP        54 52718 → 443 [ACK] Seq=239 Ack=6045 Win=261888 Len=0
79466 283.524049  172.17.14.65       20.108.172.194     TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
79467 283.524788  172.17.14.65       20.108.172.194     TLSv1.2   141 Application Data
79468 283.525019  172.17.14.65       20.108.172.194     TLSv1.2   394 Application Data
79469 283.560142  f2:8b:f8:df:00:24  LiteonTe_5c:e7:13  ARP        60 Gratuitous ARP for 172.17.10.107 (Request)
79470 283.627631  172.17.8.26        172.17.15.255      UDP        82 57621 → 57621 Len=40

> Frame 17558: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface \Device\NPF_{541C50C4-DC53-4474-9E3C-C000425DD753}, id 0    0000  c8 cb b8 d
```

10. Filter background network noise

There are several protocols that can be very noisy, it sometimes helps to filter this out so you can focus on other traffic. This will filter out arp, icmp and DNS traffic.

!(arp or icmp or dns)

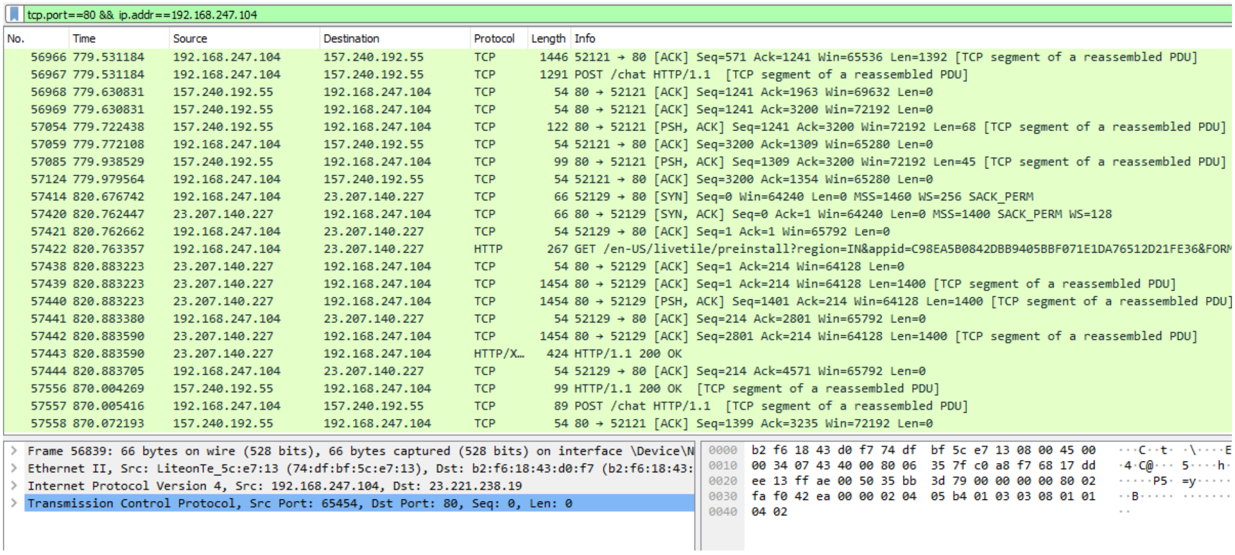


```
!(arp or icmp or dns)

No.   Time        Source                Destination           Protocol Length Info
55648 681.778394  2401:4900:4de4:3a48…  2404:6800:4007:81f:…  TCP      75 [TCP Keep-Alive] 49186 → 443 [ACK] Seq=641 Ack=7950 Win=65280 Len=1
55649 681.856229  2404:6800:4007:81f:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49186 [ACK] Seq=7950 Ack=642 Win=66816 Len=0 SLE=641 SRE=642
55650 682.246306  2401:4900:4de4:3a48…  2404:6800:4007:82a:…  TCP      75 [TCP Keep-Alive] 49187 → 443 [ACK] Seq=669 Ack=5860 Win=66048 Len=1
55651 682.312876  2404:6800:4007:82a:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49187 [ACK] Seq=5860 Ack=670 Win=66816 Len=0 SLE=669 SRE=670
55652 682.834724  2401:4900:4de4:3a48…  2404:6800:4007:821:…  TCP      75 [TCP Keep-Alive] 49188 → 443 [ACK] Seq=616 Ack=5676 Win=65024 Len=1
55653 682.834957  2401:4900:4de4:3a48…  2404:6800:4007:82a:…  TCP      75 [TCP Keep-Alive] 49189 → 443 [ACK] Seq=685 Ack=5694 Win=65024 Len=1
55654 682.890383  2404:6800:4007:821:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49188 [ACK] Seq=5676 Ack=617 Win=66816 Len=0 SLE=616 SRE=617
55655 682.896523  2404:6800:4007:82a:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49189 [ACK] Seq=5694 Ack=686 Win=66816 Len=0 SLE=685 SRE=686
55656 683.225050  2401:4900:4de4:3a48…  2404:6800:4007:826:…  TCP      75 [TCP Keep-Alive] 49191 → 443 [ACK] Seq=647 Ack=5822 Win=66048 Len=1
55657 683.240867  192.168.247.104       142.250.195.130       TCP      55 [TCP Keep-Alive] 49190 → 443 [ACK] Seq=682 Ack=5456 Win=64768 Len=1
55658 683.270713  2401:4900:4de4:3a48…  2404:6800:4007:82c:…  TCP      75 [TCP Keep-Alive] 49192 → 443 [ACK] Seq=609 Ack=5444 Win=65280 Len=1
55659 683.333273  2404:6800:4007:826:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49191 [ACK] Seq=5822 Ack=648 Win=66816 Len=0 SLE=647 SRE=648
55660 683.333273  2404:6800:4007:82c:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49192 [ACK] Seq=5444 Ack=610 Win=66816 Len=0 SLE=609 SRE=610
55661 683.335104  142.250.195.130       192.168.247.104       TCP      66 [TCP Keep-Alive ACK] 443 → 49190 [ACK] Seq=5456 Ack=683 Win=66816 Len=0 SLE=682 SRE=683
55662 684.217670  2401:4900:4de4:3a48…  2404:6800:4007:82c:…  TCP      75 [TCP Keep-Alive] 49193 → 443 [ACK] Seq=591 Ack=7964 Win=65024 Len=1
55663 684.233460  2401:4900:4de4:3a48…  2404:6800:4003:c04:…  TCP      75 [TCP Keep-Alive] 49167 → 443 [ACK] Seq=6189 Ack=10321 Win=65536 Len=1
55664 684.351178  2404:6800:4007:82c:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49193 [ACK] Seq=7964 Ack=592 Win=66816 Len=0 SLE=591 SRE=592
55665 684.404956  2401:4900:4de4:3a48…  2404:6800:4007:81a:…  TCP      75 [TCP Keep-Alive] 49194 → 443 [ACK] Seq=640 Ack=7947 Win=65280 Len=1
55666 684.420254  2404:6800:4003:c04:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49167 [ACK] Seq=10321 Ack=6190 Win=77824 Len=0 SLE=6189 SRE=6190
55667 684.476059  2404:6800:4007:81a:…  2401:4900:4de4:3a48…  TCP      86 [TCP Keep-Alive ACK] 443 → 49194 [ACK] Seq=7947 Ack=641 Win=66816 Len=0 SLE=640 SRE=641
```

11. Filter on port and IP Address

If you want to see traffic from a certain IP on a specific port use this filter

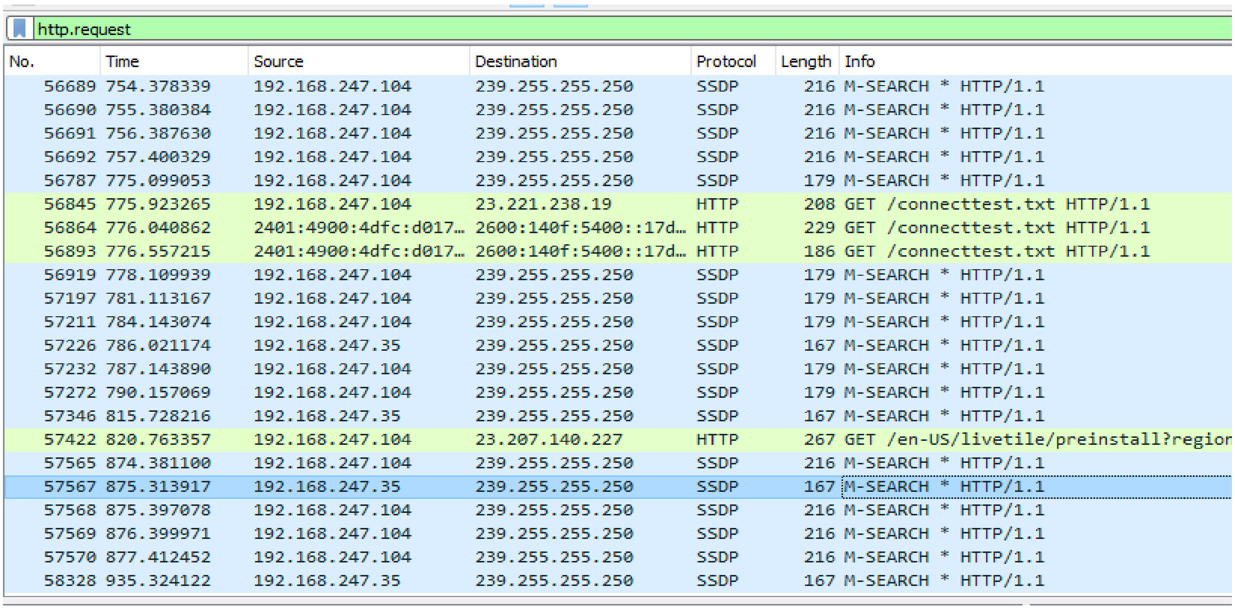
tcp.port==80 && ip.addr==192.168.247.104



```
tcp.port==80 && ip.addr==192.168.247.104

No.   Time        Source           Destination      Protocol Length Info
56966 779.531184  192.168.247.104  157.240.192.55   TCP      1446 52121 → 80 [ACK] Seq=571 Ack=1241 Win=65536 Len=1392 [TCP segment of a reassembled PDU]
56967 779.531184  192.168.247.104  157.240.192.55   TCP      1291 POST /chat HTTP/1.1  [TCP segment of a reassembled PDU]
56968 779.630831  157.240.192.55   192.168.247.104  TCP        54 80 → 52121 [ACK] Seq=1241 Ack=1963 Win=69632 Len=0
56969 779.630831  157.240.192.55   192.168.247.104  TCP        54 80 → 52121 [ACK] Seq=1241 Ack=3200 Win=72192 Len=0
57054 779.722438  157.240.192.55   192.168.247.104  TCP       122 80 → 52121 [PSH, ACK] Seq=1241 Ack=3200 Win=72192 Len=68 [TCP segment of a reassembled PDU]
57059 779.772108  192.168.247.104  157.240.192.55   TCP        54 52121 → 80 [ACK] Seq=3200 Ack=1309 Win=65280 Len=0
57085 779.938529  157.240.192.55   192.168.247.104  TCP        99 80 → 52121 [PSH, ACK] Seq=1309 Ack=3200 Win=72192 Len=45 [TCP segment of a reassembled PDU]
57124 779.979564  192.168.247.104  157.240.192.55   TCP        54 52121 → 80 [ACK] Seq=3200 Ack=1354 Win=65280 Len=0
57414 820.676742  192.168.247.104  23.207.140.227   TCP        66 52129 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
57420 820.762447  23.207.140.227   192.168.247.104  TCP        66 80 → 52129 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=128
57421 820.762662  192.168.247.104  23.207.140.227   TCP        54 52129 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
57422 820.763357  192.168.247.104  23.207.140.227   HTTP      267 GET /en-US/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM
57438 820.883223  23.207.140.227   192.168.247.104  TCP        54 80 → 52129 [ACK] Seq=1 Ack=214 Win=64128 Len=0
57439 820.883223  23.207.140.227   192.168.247.104  TCP      1454 80 → 52129 [ACK] Seq=1 Ack=214 Win=64128 Len=1400 [TCP segment of a reassembled PDU]
57440 820.883223  23.207.140.227   192.168.247.104  TCP      1454 80 → 52129 [PSH, ACK] Seq=1401 Ack=214 Win=64128 Len=1400 [TCP segment of a reassembled PDU]
57441 820.883380  192.168.247.104  23.207.140.227   TCP        54 52129 → 80 [ACK] Seq=214 Ack=2801 Win=65792 Len=0
57442 820.883590  23.207.140.227   192.168.247.104  TCP      1454 80 → 52129 [ACK] Seq=2801 Ack=214 Win=64128 Len=1400 [TCP segment of a reassembled PDU]
57443 820.883590  23.207.140.227   192.168.247.104  HTTP/X…   424 HTTP/1.1 200 OK
57444 820.883705  192.168.247.104  23.207.140.227   TCP        54 52129 → 80 [ACK] Seq=214 Ack=4571 Win=65792 Len=0
57556 870.004269  157.240.192.55   192.168.247.104  TCP        99 HTTP/1.1 200 OK  [TCP segment of a reassembled PDU]
57557 870.005416  192.168.247.104  157.240.192.55   TCP        89 POST /chat HTTP/1.1  [TCP segment of a reassembled PDU]
57558 870.072193  157.240.192.55   192.168.247.104  TCP        54 80 → 52121 [ACK] Seq=1399 Ack=3235 Win=72192 Len=0

> Frame 56839: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\N
> Ethernet II, Src: LiteonTe_5c:e7:13 (74:df:bf:5c:e7:13), Dst: b2:f6:18:43:d0:f7 (b2:f6:18:43:
> Internet Protocol Version 4, Src: 192.168.247.104, Dst: 23.221.238.19
> Transmission Control Protocol, Src Port: 65454, Dst Port: 80, Seq: 0, Len: 0

0000  b2 f6 18 43 d0 f7 74 df  bf 5c e7 13 08 00 45 00   ···C··t· ·\····E
0010  00 34 07 43 40 00 80 06  35 7f c0 a8 f7 68 17 dd   ·4·C@··· 5····h·
0020  ee 13 ff ae 00 50 35 bb  3d 79 00 00 00 00 80 02   ·····P5· =y······
0030  fa f0 42 ea 00 00 02 04  05 b4 01 03 03 08 01 01   ··B····· ·······
0040  04 02                                              ··
```

12. Filter for all http get requests

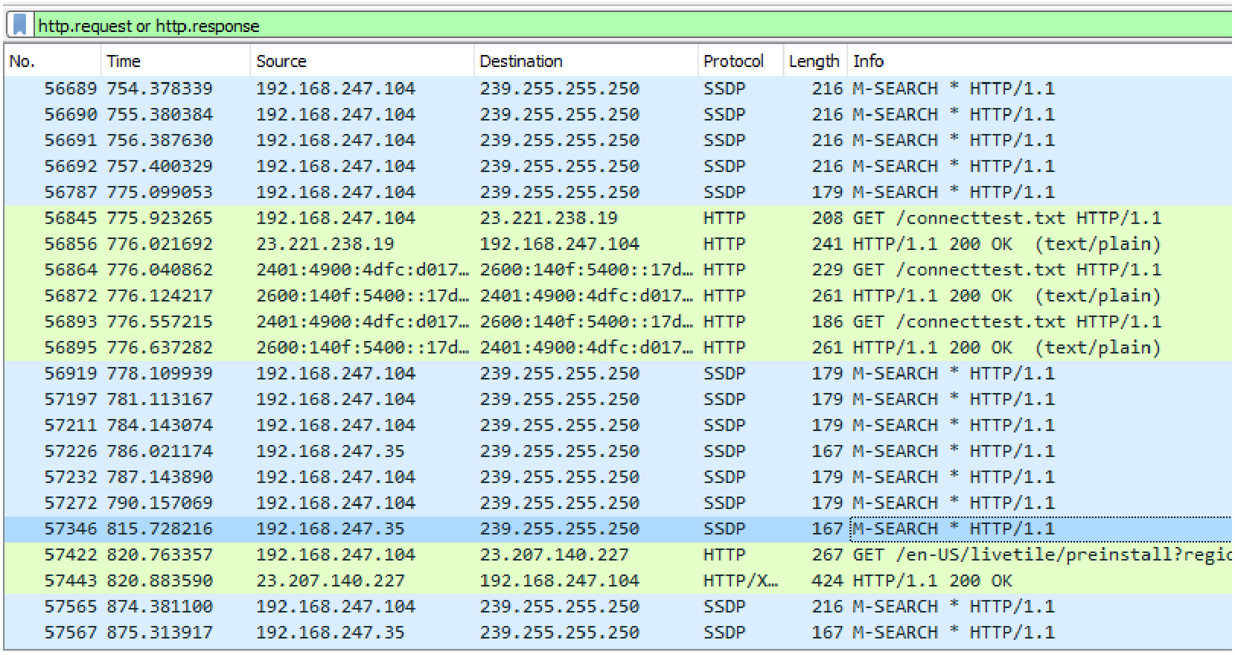
http.request



```
http.request

No.   Time        Source              Destination         Protocol Length Info
56689 754.378339  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
56690 755.380384  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
56691 756.387630  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
56692 757.400329  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
56787 775.099053  192.168.247.104     239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
56845 775.923265  192.168.247.104     23.221.238.19       HTTP      208 GET /connecttest.txt HTTP/1.1
56864 776.040862  2401:4900:4dfc:d017… 2600:140f:5400::17d… HTTP    229 GET /connecttest.txt HTTP/1.1
56893 776.557215  2401:4900:4dfc:d017… 2600:140f:5400::17d… HTTP    186 GET /connecttest.txt HTTP/1.1
56919 778.109939  192.168.247.104     239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
57197 781.113167  192.168.247.104     239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
57211 784.143074  192.168.247.104     239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
57226 786.021174  192.168.247.35      239.255.255.250     SSDP      167 M-SEARCH * HTTP/1.1
57232 787.143890  192.168.247.104     239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
57272 790.157069  192.168.247.104     239.255.255.250     SSDP      179 M-SEARCH * HTTP/1.1
57346 815.728216  192.168.247.35      239.255.255.250     SSDP      167 M-SEARCH * HTTP/1.1
57422 820.763357  192.168.247.104     23.207.140.227      HTTP      267 GET /en-US/livetile/preinstall?regior
57565 874.381100  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
57567 875.313917  192.168.247.35      239.255.255.250     SSDP      167 M-SEARCH * HTTP/1.1
57568 875.397078  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
57569 876.399971  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
57570 877.412452  192.168.247.104     239.255.255.250     SSDP      216 M-SEARCH * HTTP/1.1
58328 935.324122  192.168.247.35      239.255.255.250     SSDP      167 M-SEARCH * HTTP/1.1
```

13. Filter for http get and responses

http.request or http.response



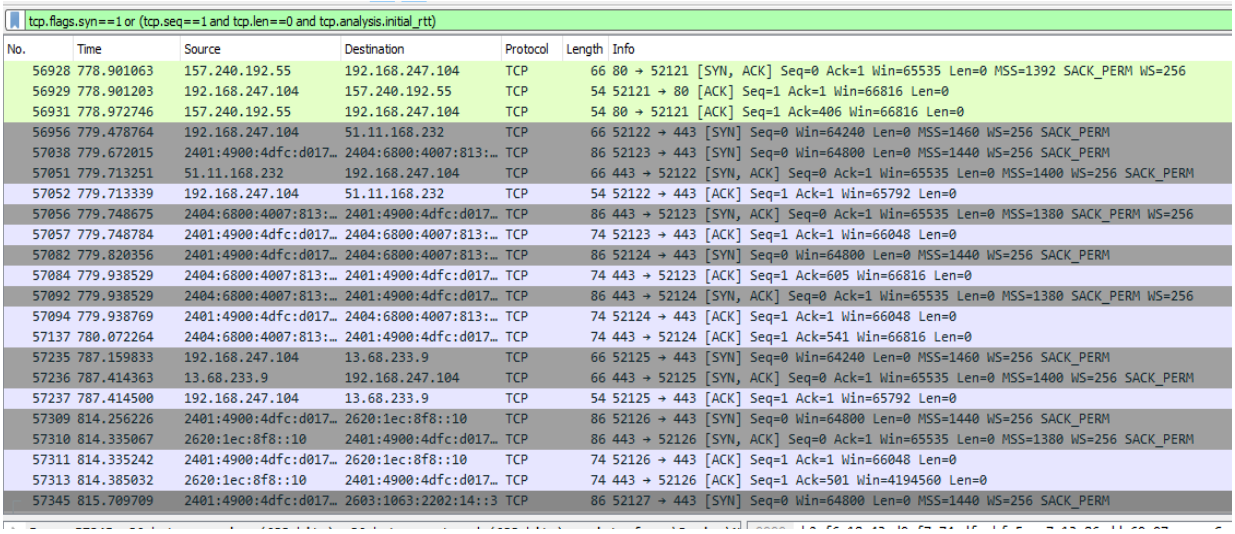
http.request or http.response

No.	Time	Source	Destination	Protocol	Length	Info
56689	754.378339	192.168.247.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
56690	755.380384	192.168.247.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
56691	756.387630	192.168.247.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
56692	757.400329	192.168.247.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
56787	775.099053	192.168.247.104	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
56845	775.923265	192.168.247.104	23.221.238.19	HTTP	208	GET /connecttest.txt HTTP/1.1
56856	776.021692	23.221.238.19	192.168.247.104	HTTP	241	HTTP/1.1 200 OK (text/plain)
56864	776.040862	2401:4900:4dfc:d017…	2600:140f:5400::17d…	HTTP	229	GET /connecttest.txt HTTP/1.1
56872	776.124217	2600:140f:5400::17d…	2401:4900:4dfc:d017…	HTTP	261	HTTP/1.1 200 OK (text/plain)
56893	776.557215	2401:4900:4dfc:d017…	2600:140f:5400::17d…	HTTP	186	GET /connecttest.txt HTTP/1.1
56895	776.637282	2600:140f:5400::17d…	2401:4900:4dfc:d017…	HTTP	261	HTTP/1.1 200 OK (text/plain)
56919	778.109939	192.168.247.104	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
57197	781.113167	192.168.247.104	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
57211	784.143074	192.168.247.104	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
57226	786.021174	192.168.247.35	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
57232	787.143890	192.168.247.104	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
57272	790.157069	192.168.247.104	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
57346	815.728216	192.168.247.35	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
57422	820.763357	192.168.247.104	23.207.140.227	HTTP	267	GET /en-US/livetile/preinstall?regic
57443	820.883590	23.207.140.227	192.168.247.104	HTTP/X…	424	HTTP/1.1 200 OK
57565	874.381100	192.168.247.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
57567	875.313917	192.168.247.35	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

14. Filter on three way handshake

The three way handshake is often used to calculate the network round trip time. This filter will display all the SYN, SYN ACK and SYN packets that should match the three way handshake.

tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0 and tcp.analysis.initial_rtt)



tcp.flags.syn==1 or (tcp.seq==1 and tcp.len==0 and tcp.analysis.initial_rtt)

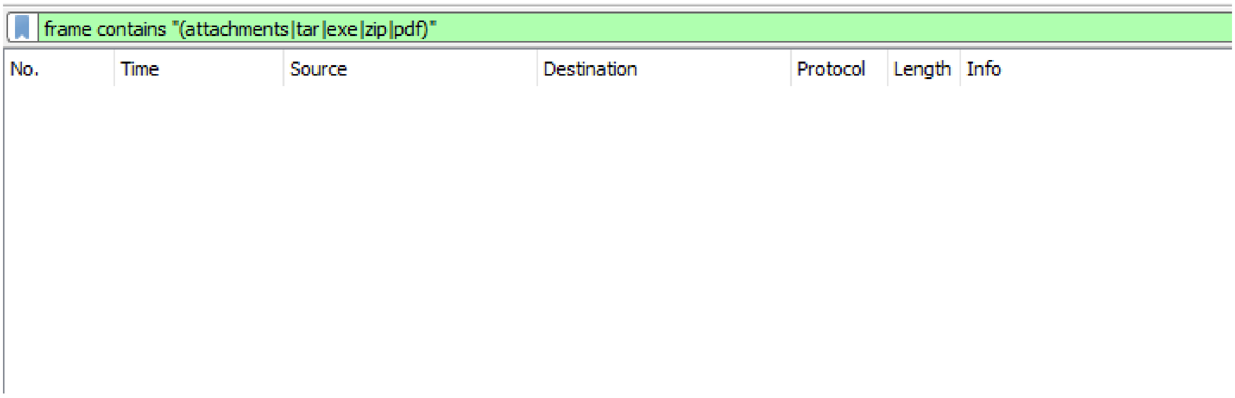
No.	Time	Source	Destination	Protocol	Length	Info
56928	778.901063	157.240.192.55	192.168.247.104	TCP	66	80 → 52121 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM WS=256
56929	778.901203	192.168.247.104	157.240.192.55	TCP	54	52121 → 80 [ACK] Seq=1 Ack=1 Win=66816 Len=0
56931	778.972746	157.240.192.55	192.168.247.104	TCP	54	80 → 52121 [ACK] Seq=1 Ack=406 Win=66816 Len=0
56956	779.478764	192.168.247.104	51.11.168.232	TCP	66	52122 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
57038	779.672015	2401:4900:4dfc:d017…	2404:6800:4007:813:…	TCP	86	52123 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
57051	779.713251	51.11.168.232	192.168.247.104	TCP	66	443 → 52122 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
57052	779.713339	192.168.247.104	51.11.168.232	TCP	54	52122 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
57056	779.748675	2404:6800:4007:813:…	2401:4900:4dfc:d017…	TCP	86	443 → 52123 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM WS=256
57057	779.748784	2401:4900:4dfc:d017…	2404:6800:4007:813:…	TCP	74	52123 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
57082	779.820356	2401:4900:4dfc:d017…	2404:6800:4007:813:…	TCP	86	52124 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
57084	779.938529	2404:6800:4007:813:…	2401:4900:4dfc:d017…	TCP	74	443 → 52123 [ACK] Seq=1 Ack=605 Win=66816 Len=0
57092	779.938529	2404:6800:4007:813:…	2401:4900:4dfc:d017…	TCP	86	443 → 52124 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM WS=256
57094	779.938769	2401:4900:4dfc:d017…	2404:6800:4007:813:…	TCP	74	52124 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
57137	780.072264	2404:6800:4007:813:…	2401:4900:4dfc:d017…	TCP	74	443 → 52124 [ACK] Seq=1 Ack=541 Win=66816 Len=0
57235	787.159833	192.168.247.104	13.68.233.9	TCP	66	52125 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
57236	787.414363	13.68.233.9	192.168.247.104	TCP	66	443 → 52125 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
57237	787.414500	192.168.247.104	13.68.233.9	TCP	54	52125 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
57309	814.256226	2401:4900:4dfc:d017…	2620:1ec:8f8::10	TCP	86	52126 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
57310	814.335067	2620:1ec:8f8::10	2401:4900:4dfc:d017…	TCP	86	443 → 52126 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
57311	814.335242	2401:4900:4dfc:d017…	2620:1ec:8f8::10	TCP	74	52126 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
57313	814.385032	2620:1ec:8f8::10	2401:4900:4dfc:d017…	TCP	74	443 → 52126 [ACK] Seq=1 Ack=501 Win=4194560 Len=0
57345	815.709709	2401:4900:4dfc:d017…	2603:1063:2202:14::3	TCP	86	52127 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM

15. Find executable or other file types

Need to see if users are download .exe or other file types use this filter

frame contains "(attachment|tar|exe|zip|pdf)"

Just add in any other file extension you want to filter for.

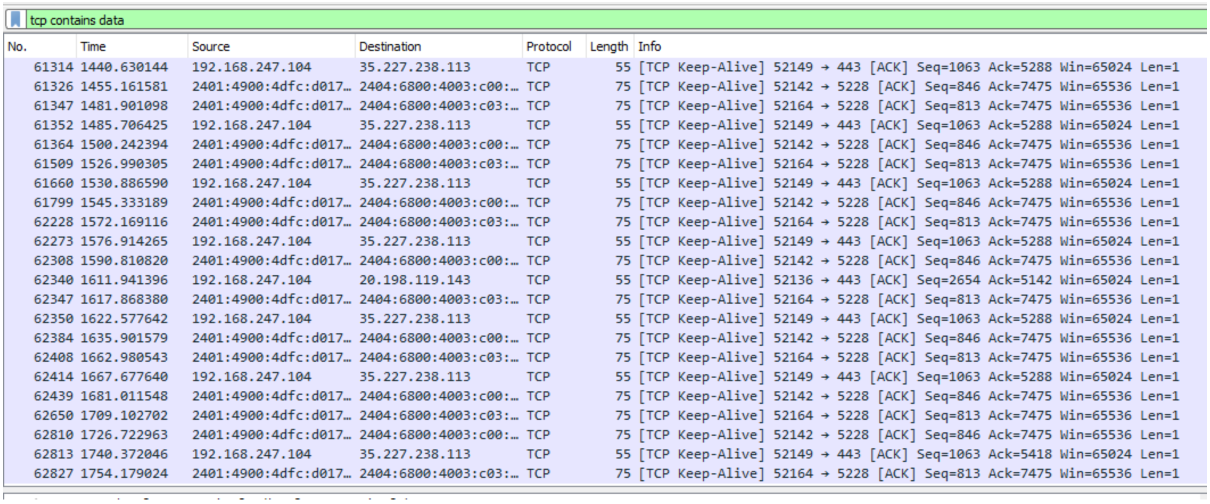


frame contains "(attachments|tar|exe|zip|pdf)"

No.	Time	Source	Destination	Protocol	Length	Info

16. Search traffic based on a keyword

tcp contains data



tcp contains data

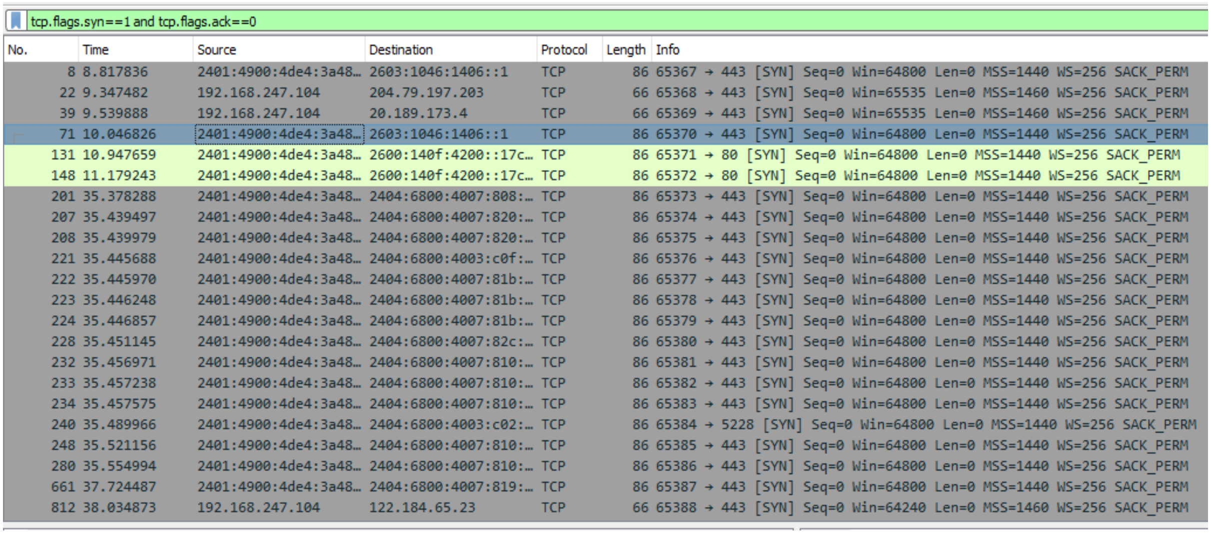
No.	Time	Source	Destination	Protocol	Length	Info
61314	1440.630144	192.168.247.104	35.227.238.113	TCP	55	[TCP Keep-Alive] 52149 → 443 [ACK] Seq=1063 Ack=5288 Win=65024 Len=1
61326	1455.161581	2401:4900:4dfc:d017…	2404:6800:4003:c00:…	TCP	75	[TCP Keep-Alive] 52142 → 5228 [ACK] Seq=846 Ack=7475 Win=65536 Len=1
61347	1481.901098	2401:4900:4dfc:d017…	2404:6800:4003:c03:…	TCP	75	[TCP Keep-Alive] 52164 → 5228 [ACK] Seq=813 Ack=7475 Win=65536 Len=1
61352	1485.706425	192.168.247.104	35.227.238.113	TCP	55	[TCP Keep-Alive] 52149 → 443 [ACK] Seq=1063 Ack=5288 Win=65024 Len=1
61364	1500.242394	2401:4900:4dfc:d017…	2404:6800:4003:c00:…	TCP	75	[TCP Keep-Alive] 52142 → 5228 [ACK] Seq=846 Ack=7475 Win=65536 Len=1
61509	1526.990305	2401:4900:4dfc:d017…	2404:6800:4003:c03:…	TCP	75	[TCP Keep-Alive] 52164 → 5228 [ACK] Seq=813 Ack=7475 Win=65536 Len=1
61660	1530.886590	192.168.247.104	35.227.238.113	TCP	55	[TCP Keep-Alive] 52149 → 443 [ACK] Seq=1063 Ack=5288 Win=65024 Len=1
61799	1545.333189	2401:4900:4dfc:d017…	2404:6800:4003:c00:…	TCP	75	[TCP Keep-Alive] 52142 → 5228 [ACK] Seq=846 Ack=7475 Win=65536 Len=1
62228	1572.169116	2401:4900:4dfc:d017…	2404:6800:4003:c03:…	TCP	75	[TCP Keep-Alive] 52164 → 5228 [ACK] Seq=813 Ack=7475 Win=65536 Len=1
62273	1576.914265	192.168.247.104	35.227.238.113	TCP	55	[TCP Keep-Alive] 52149 → 443 [ACK] Seq=1063 Ack=5288 Win=65024 Len=1
62308	1590.810820	2401:4900:4dfc:d017…	2404:6800:4003:c00:…	TCP	75	[TCP Keep-Alive] 52142 → 5228 [ACK] Seq=846 Ack=7475 Win=65536 Len=1
62340	1611.941396	192.168.247.104	20.198.119.143	TCP	55	[TCP Keep-Alive] 52136 → 443 [ACK] Seq=2654 Ack=5142 Win=65024 Len=1
62347	1617.868380	2401:4900:4dfc:d017…	2404:6800:4003:c03:…	TCP	75	[TCP Keep-Alive] 52164 → 5228 [ACK] Seq=813 Ack=7475 Win=65536 Len=1
62350	1622.577642	192.168.247.104	35.227.238.113	TCP	55	[TCP Keep-Alive] 52149 → 443 [ACK] Seq=1063 Ack=5288 Win=65024 Len=1
62384	1635.901579	2401:4900:4dfc:d017…	2404:6800:4003:c00:…	TCP	75	[TCP Keep-Alive] 52142 → 5228 [ACK] Seq=846 Ack=7475 Win=65536 Len=1
62408	1662.980543	2401:4900:4dfc:d017…	2404:6800:4003:c03:…	TCP	75	[TCP Keep-Alive] 52164 → 5228 [ACK] Seq=813 Ack=7475 Win=65536 Len=1
62414	1667.677640	192.168.247.104	35.227.238.113	TCP	55	[TCP Keep-Alive] 52149 → 443 [ACK] Seq=1063 Ack=5288 Win=65024 Len=1
62439	1681.011548	2401:4900:4dfc:d017…	2404:6800:4003:c00:…	TCP	75	[TCP Keep-Alive] 52142 → 5228 [ACK] Seq=846 Ack=7475 Win=65536 Len=1
62650	1709.102702	2401:4900:4dfc:d017…	2404:6800:4003:c03:…	TCP	75	[TCP Keep-Alive] 52164 → 5228 [ACK] Seq=813 Ack=7475 Win=65536 Len=1
62810	1726.722963	2401:4900:4dfc:d017…	2404:6800:4003:c00:…	TCP	75	[TCP Keep-Alive] 52142 → 5228 [ACK] Seq=846 Ack=7475 Win=65536 Len=1
62813	1740.372046	192.168.247.104	35.227.238.113	TCP	55	[TCP Keep-Alive] 52149 → 443 [ACK] Seq=1063 Ack=5418 Win=65024 Len=1
62827	1754.179024	2401:4900:4dfc:d017…	2404:6800:4003:c03:…	TCP	75	[TCP Keep-Alive] 52164 → 5228 [ACK] Seq=813 Ack=7475 Win=65536 Len=1

17. Detecting SYN Floods (Possible DDoS attacks)

DDos attacks can be done in a variety of ways, a large number of TCP connections is one of them.

To look for a large number of tcp connection attempts use this

filter tcp.flags.syn == 1 and tcp.flags.ack == 0

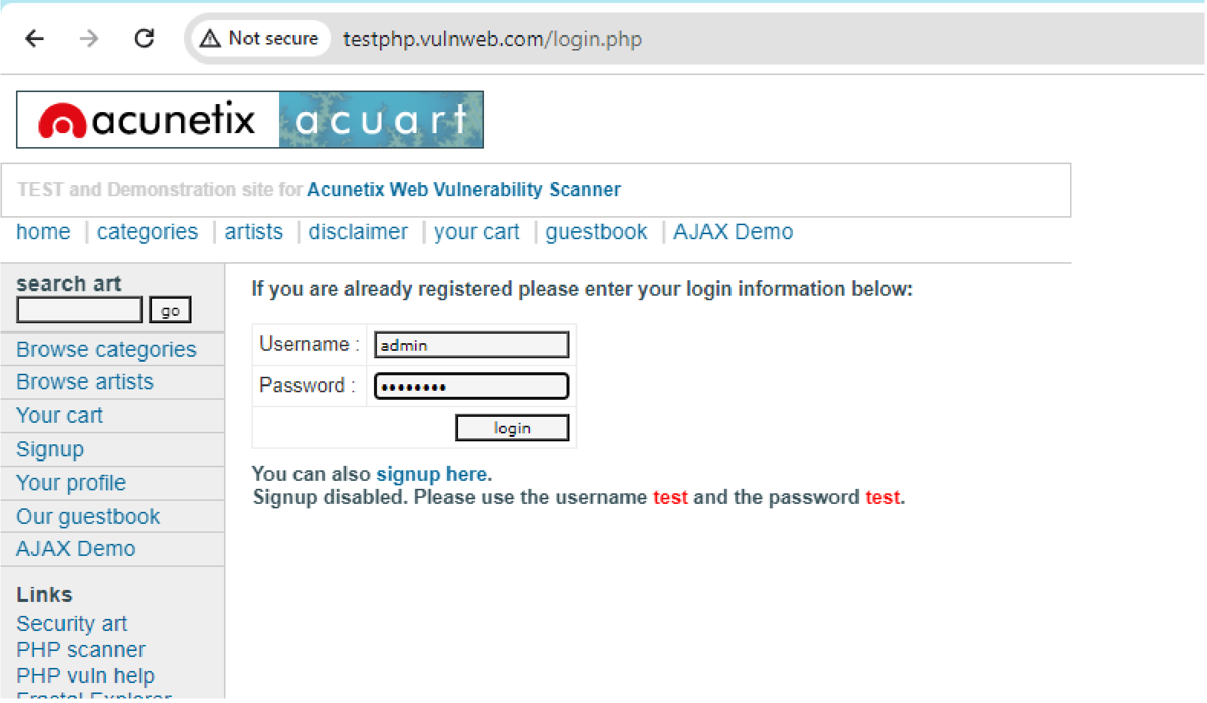


tcp.flags.syn==1 and tcp.flags.ack==0

No.	Time	Source	Destination	Protocol	Length	Info
8	8.817836	2401:4900:4de4:3a48…	2603:1046:1406::1	TCP	86	65367 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
22	9.347482	192.168.247.104	204.79.197.203	TCP	66	65368 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
39	9.539888	192.168.247.104	20.189.173.4	TCP	66	65369 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
71	10.046826	2401:4900:4de4:3a48…	2603:1046:1406::1	TCP	86	65370 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
131	10.947659	2401:4900:4de4:3a48…	2600:140f:4200::17c…	TCP	86	65371 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
148	11.179243	2401:4900:4de4:3a48…	2600:140f:4200::17c…	TCP	86	65372 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
201	35.378288	2401:4900:4de4:3a48…	2404:6800:4007:808:…	TCP	86	65373 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
207	35.439497	2401:4900:4de4:3a48…	2404:6800:4007:820:…	TCP	86	65374 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
208	35.439979	2401:4900:4de4:3a48…	2404:6800:4007:820:…	TCP	86	65375 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
221	35.445688	2401:4900:4de4:3a48…	2404:6800:4003:c0f:…	TCP	86	65376 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
222	35.445970	2401:4900:4de4:3a48…	2404:6800:4007:81b:…	TCP	86	65377 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
223	35.446248	2401:4900:4de4:3a48…	2404:6800:4007:81b:…	TCP	86	65378 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
224	35.446857	2401:4900:4de4:3a48…	2404:6800:4007:81b:…	TCP	86	65379 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
228	35.451145	2401:4900:4de4:3a48…	2404:6800:4007:82c:…	TCP	86	65380 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
232	35.456971	2401:4900:4de4:3a48…	2404:6800:4007:810:…	TCP	86	65381 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
233	35.457238	2401:4900:4de4:3a48…	2404:6800:4007:810:…	TCP	86	65382 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
234	35.457575	2401:4900:4de4:3a48…	2404:6800:4007:810:…	TCP	86	65383 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
240	35.489966	2401:4900:4de4:3a48…	2404:6800:4003:c02:…	TCP	86	65384 → 5228 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
248	35.521156	2401:4900:4de4:3a48…	2404:6800:4007:810:…	TCP	86	65385 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
280	35.554994	2401:4900:4de4:3a48…	2404:6800:4007:810:…	TCP	86	65386 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
661	37.724487	2401:4900:4de4:3a48…	2404:6800:4007:819:…	TCP	86	65387 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
812	38.034873	192.168.247.104	122.184.65.23	TCP	66	65388 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Capturing password in Wireshark:

http website:



⚠ Not secure testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP scanner

PHP vuln help

If you are already registered please enter your login information below:

Username : admin

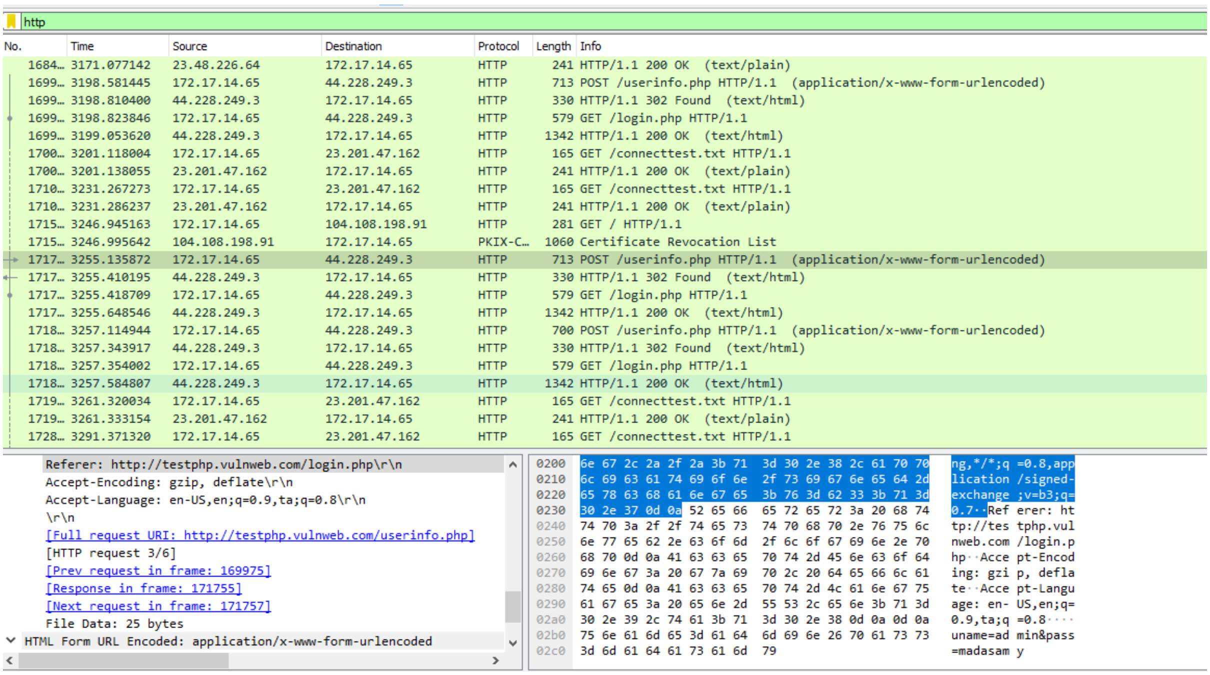
Password : ••••••••

login

You can also signup here.

Signup disabled. Please use the username test and the password test.

Capturing http packets:

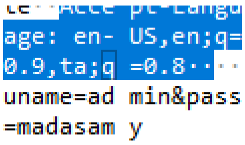


```
http

No.      Time         Source          Destination     Protocol  Length Info
1684…  3171.077142   23.48.226.64    172.17.14.65    HTTP       241 HTTP/1.1 200 OK  (text/plain)
1699…  3198.581445   172.17.14.65    44.228.249.3    HTTP       713 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
1699…  3198.810400   44.228.249.3    172.17.14.65    HTTP       330 HTTP/1.1 302 Found  (text/html)
1699…  3198.823846   172.17.14.65    44.228.249.3    HTTP       579 GET /login.php HTTP/1.1
1699…  3199.053620   44.228.249.3    172.17.14.65    HTTP      1342 HTTP/1.1 200 OK  (text/html)
1700…  3201.118004   172.17.14.65    23.201.47.162   HTTP       165 GET /connecttest.txt HTTP/1.1
1700…  3201.138055   23.201.47.162   172.17.14.65    HTTP       241 HTTP/1.1 200 OK  (text/plain)
1710…  3231.267273   172.17.14.65    23.201.47.162   HTTP       165 GET /connecttest.txt HTTP/1.1
1710…  3231.286237   23.201.47.162   172.17.14.65    HTTP       241 HTTP/1.1 200 OK  (text/plain)
1715…  3246.945163   172.17.14.65    104.108.198.91  HTTP       281 GET / HTTP/1.1
1715…  3246.995642   104.108.198.91  172.17.14.65    PKIX-C…   1060 Certificate Revocation List
1717…  3255.135872   172.17.14.65    44.228.249.3    HTTP       713 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
1717…  3255.410195   44.228.249.3    172.17.14.65    HTTP       330 HTTP/1.1 302 Found  (text/html)
1717…  3255.418709   172.17.14.65    44.228.249.3    HTTP       579 GET /login.php HTTP/1.1
1717…  3255.648546   44.228.249.3    172.17.14.65    HTTP      1342 HTTP/1.1 200 OK  (text/html)
1718…  3257.114944   172.17.14.65    44.228.249.3    HTTP       700 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
1718…  3257.343917   44.228.249.3    172.17.14.65    HTTP       330 HTTP/1.1 302 Found  (text/html)
1718…  3257.354002   172.17.14.65    44.228.249.3    HTTP       579 GET /login.php HTTP/1.1
1718…  3257.584807   44.228.249.3    172.17.14.65    HTTP      1342 HTTP/1.1 200 OK  (text/html)
1719…  3261.320034   172.17.14.65    23.201.47.162   HTTP       165 GET /connecttest.txt HTTP/1.1
1719…  3261.333154   23.201.47.162   172.17.14.65    HTTP       241 HTTP/1.1 200 OK  (text/plain)
1728…  3291.371320   172.17.14.65    23.201.47.162   HTTP       165 GET /connecttest.txt HTTP/1.1
```

```
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ta;q=0.8\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 3/6]
    [Prev request in frame: 169975]
    [Response in frame: 171755]
    [Next request in frame: 171757]
    File Data: 25 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
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  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
02a0  30 2e 39 2c 74 61 3b 71  3d 30 2e 38 0d 0a 0d 0a   0.9,ta;q =0.8····
02b0  75 6e 61 6d 65 3d 61 64  6d 69 6e 26 70 61 73 73   uname=ad min&pass
02c0  3d 6d 61 64 61 73 61 6d  79                        =madasam y
```

Username and password information:



```
te··Acce pt-Langu
age: en- US,en;q=
0.9,ta;q =0.8····
uname=ad min&pass
=madasam y
```