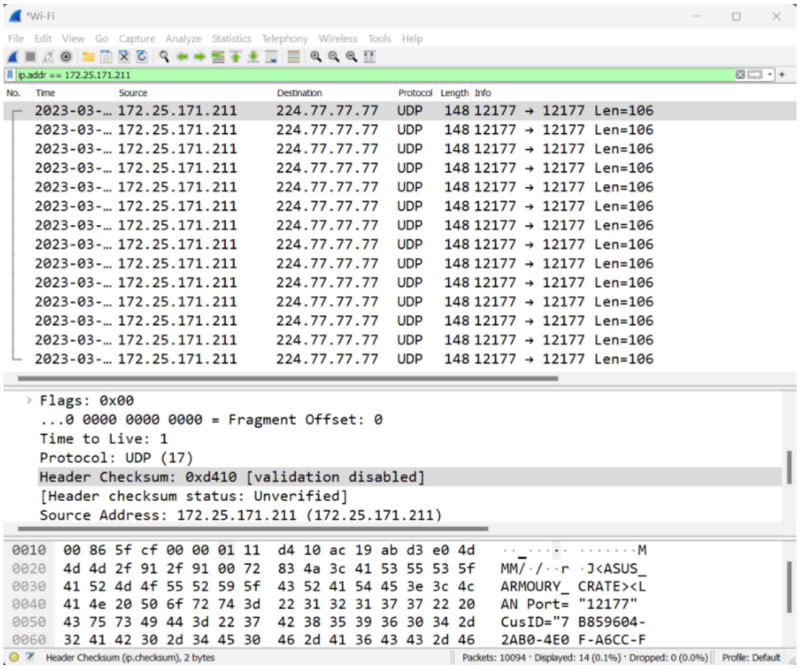
Wireshark

1. ip.addr == x.x.x.x
   Sets a filter for any packet that has x.x.x.x as the source or destination IP address. This is very useful if, let's say, you want to analyze specific traffic. Applying this filter helps you analyze outgoing traffic to see which one matches the IP or source you're looking for.



ip.addr == 172.25.171.211

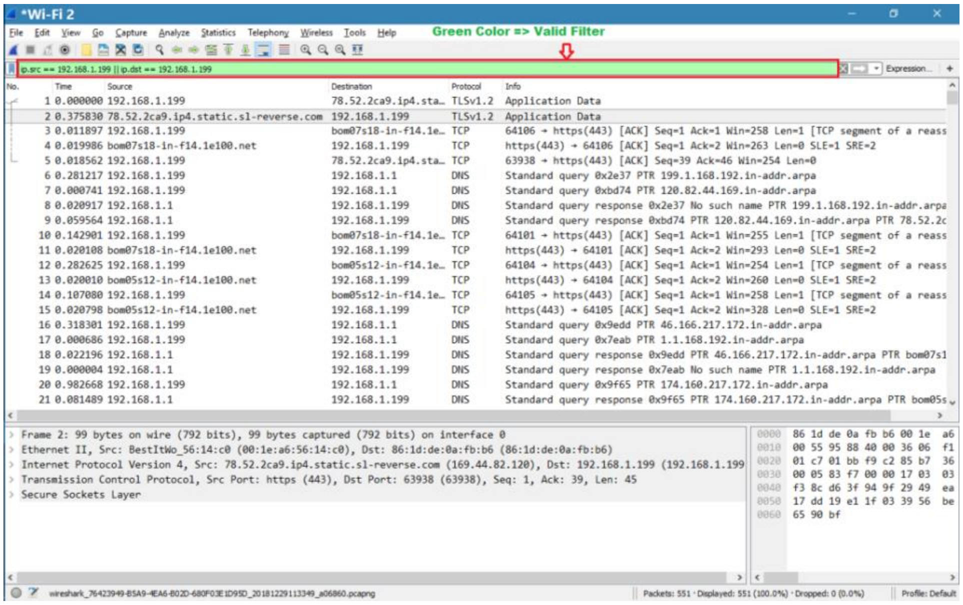
```
No.  Time          Source            Destination    Protocol Length Info
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
     2023-03-…     172.25.171.211    224.77.77.77   UDP      148 12177 → 12177 Len=106
```

```
 › Flags: 0x00
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 1
   Protocol: UDP (17)
   Header Checksum: 0xd410 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 172.25.171.211 (172.25.171.211)
```

```
0010  00 86 5f cf 00 00 01 11  d4 10 ac 19 ab d3 e0 4d   ··_·····  ·······M
0020  4d 4d 2f 91 2f 91 00 72  83 4a 3c 41 53 55 53 5f   MM/·/··r  ·J<ASUS_
0030  41 52 4d 4f 55 52 59 5f  43 52 41 54 45 3e 3c 4c   ARMOURY_  CRATE><L
0040  41 4e 20 50 6f 72 74 3d  22 31 32 31 37 37 22 20   AN Port=  "12177"
0050  43 75 73 49 44 3d 22 37  42 38 35 39 36 30 34 2d   CusID="7  B859604-
0060  32 41 42 30 2d 34 45 30  46 2d 41 36 43 43 2d 46   2AB0-4E0  F-A6CC-F
```

Header Checksum (ip.checksum), 2 bytes | Packets: 10094 · Displayed: 14 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

2. ip.addr == x.x.x.x && ip.addr == x.x.x.x
   Sets a conversation filter between two specific IP addresses. This one helps you check the data between two specific hosts or networks. It helps you when you are looking for specific data, so you don't have to go through others that don't interest you.



ip.src == 192.168.1.199 || ip.dst == 192.168.1.199

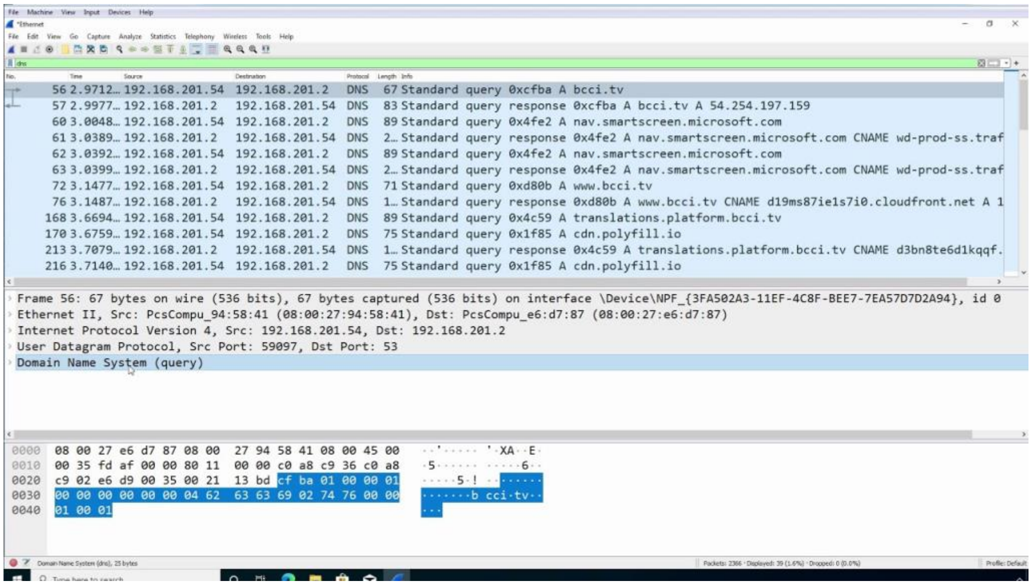
```
No.   Time     Source                               Destination          Protocol  Info
    1 0.000000 192.168.1.199                        78.52.2ca9.ip4.sta…  TLSv1.2   Application Data
    2 0.375830 78.52.2ca9.ip4.static.sl-reverse.com 192.168.1.199        TLSv1.2   Application Data
    3 0.011897 192.168.1.199                        bom07s18-in-f14.1e…  TCP       64106 → https(443) [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reass
    4 0.019986 bom07s18-in-f14.1e100.net            192.168.1.199        TCP       https(443) → 64106 [ACK] Seq=1 Ack=2 Win=263 Len=0 SLE=1 SRE=2
    5 0.018562 192.168.1.199                        78.52.2ca9.ip4.sta…  TCP       63938 → https(443) [ACK] Seq=39 Ack=46 Win=254 Len=0
    6 0.281217 192.168.1.199                        192.168.1.1          DNS       Standard query 0x2e37 PTR 199.1.168.192.in-addr.arpa
    7 0.000741 192.168.1.199                        192.168.1.1          DNS       Standard query 0xbd74 PTR 120.82.44.169.in-addr.arpa
    8 0.020917 192.168.1.1                          192.168.1.199        DNS       Standard query response 0x2e37 No such name PTR 199.1.168.192.in-addr.arpa
    9 0.059564 192.168.1.1                          192.168.1.199        DNS       Standard query response 0xbd74 PTR 120.82.44.169.in-addr.arpa PTR 78.52.2c
   10 0.142901 192.168.1.199                        bom07s18-in-f14.1e…  TCP       64101 → https(443) [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reass
   11 0.020108 bom07s18-in-f14.1e100.net            192.168.1.199        TCP       https(443) → 64101 [ACK] Seq=1 Ack=2 Win=293 Len=0 SLE=1 SRE=2
   12 0.282625 192.168.1.199                        bom05s12-in-f14.1e…  TCP       64104 → https(443) [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reass
   13 0.020010 bom05s12-in-f14.1e100.net            192.168.1.199        TCP       https(443) → 64104 [ACK] Seq=1 Ack=2 Win=260 Len=0 SLE=1 SRE=2
   14 0.107080 192.168.1.199                        bom05s12-in-f14.1e…  TCP       64105 → https(443) [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reass
   15 0.020798 bom05s12-in-f14.1e100.net            192.168.1.199        TCP       https(443) → 64105 [ACK] Seq=1 Ack=2 Win=328 Len=0 SLE=1 SRE=2
   16 0.318301 192.168.1.199                        192.168.1.1          DNS       Standard query 0x9edd PTR 46.166.217.172.in-addr.arpa
   17 0.000686 192.168.1.199                        192.168.1.1          DNS       Standard query 0x7eab PTR 1.1.168.192.in-addr.arpa
   18 0.022196 192.168.1.1                          192.168.1.199        DNS       Standard query response 0x9edd PTR 46.166.217.172.in-addr.arpa PTR bom07s1
   19 0.000004 192.168.1.1                          192.168.1.199        DNS       Standard query response 0x7eab No such name PTR 1.1.168.192.in-addr.arpa
   20 0.982668 192.168.1.199                        192.168.1.1          DNS       Standard query 0x9f65 PTR 174.160.217.172.in-addr.arpa
   21 0.081489 192.168.1.1                          192.168.1.199        DNS       Standard query response 0x9f65 PTR 174.160.217.172.in-addr.arpa PTR bom05s
```

```
› Frame 2: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0
› Ethernet II, Src: BestItWo_56:14:c0 (00:1e:a6:56:14:c0), Dst: 86:1d:de:0a:fb:b6 (86:1d:de:0a:fb:b6)
› Internet Protocol Version 4, Src: 78.52.2ca9.ip4.static.sl-reverse.com (169.44.82.120), Dst: 192.168.1.199 (192.168.1.199
› Transmission Control Protocol, Src Port: https (443), Dst Port: 63938 (63938), Seq: 1, Ack: 39, Len: 45
› Secure Sockets Layer
```

```
0000  86 1d de 0a fb b6 00 1e  a6
0010  00 55 95 88 40 00 36 06  f1
0020  01 c7 01 bb f9 c2 85 b7  36
0030  00 05 83 f7 00 00 17 03  03
0040  f3 8c d6 3f 94 9f 29 49  ea
0050  17 dd 19 e1 1f 03 39 56  be
0060  65 90 bf
```

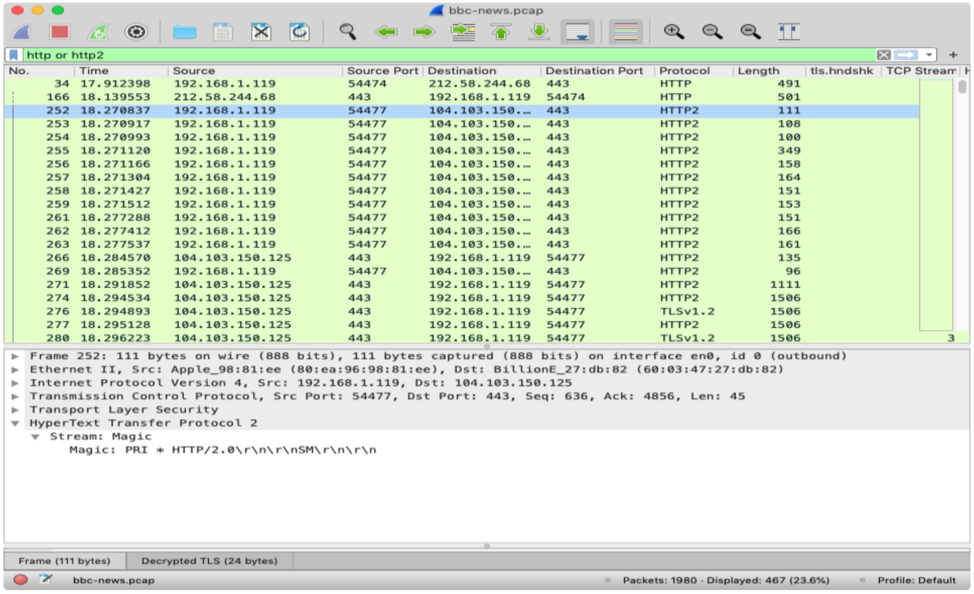
wireshark_76423949-B5A9-4EA6-B02D-680F03E1D95D_20181229113349_a06860.pcapng | Packets: 551 · Displayed: 551 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

3. http and dns
   Sets a filter to display all http and dns protocols. It lets you narrow down to the exact protocol you need.



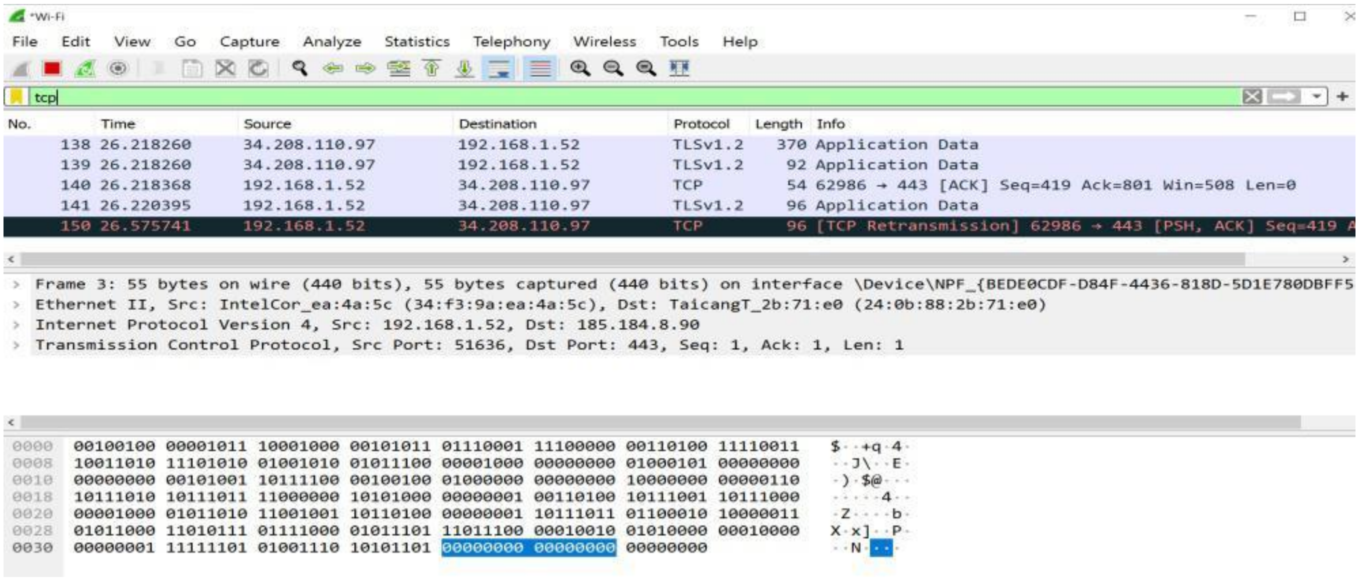
```
dns
No.  Time       Source           Destination      Protocol Length Info
  56 2.9712… 192.168.201.54 192.168.201.2  DNS  67 Standard query 0xcfba A bcci.tv
  57 2.9977… 192.168.201.2  192.168.201.54 DNS  83 Standard query response 0xcfba A bcci.tv A 54.254.197.159
  60 3.0048… 192.168.201.54 192.168.201.2  DNS  89 Standard query 0x4fe2 A nav.smartscreen.microsoft.com
  61 3.0389… 192.168.201.2  192.168.201.54 DNS  2… Standard query response 0x4fe2 A nav.smartscreen.microsoft.com CNAME wd-prod-ss.traf
  62 3.0392… 192.168.201.54 192.168.201.2  DNS  89 Standard query 0x4fe2 A nav.smartscreen.microsoft.com
  63 3.0399… 192.168.201.2  192.168.201.54 DNS  2… Standard query response 0x4fe2 A nav.smartscreen.microsoft.com CNAME wd-prod-ss.traf
  72 3.1477… 192.168.201.54 192.168.201.2  DNS  71 Standard query 0xd80b A www.bcci.tv
  76 3.1487… 192.168.201.2  192.168.201.54 DNS  1… Standard query response 0xd80b A www.bcci.tv CNAME d19ms87ie1s7i0.cloudfront.net A 1
 168 3.6694… 192.168.201.54 192.168.201.2  DNS  89 Standard query 0x4c59 A translations.platform.bcci.tv
 170 3.6759… 192.168.201.54 192.168.201.2  DNS  75 Standard query 0x1f85 A cdn.polyfill.io
 213 3.7079… 192.168.201.2  192.168.201.54 DNS  1… Standard query response 0x4c59 A translations.platform.bcci.tv CNAME d3bn8te6d1kqqf.
 216 3.7140… 192.168.201.54 192.168.201.2  DNS  75 Standard query 0x1f85 A cdn.polyfill.io

Frame 56: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{3FA502A3-11EF-4C8F-BEE7-7EA57D7D2A94}, id 0
Ethernet II, Src: PcsCompu_94:58:41 (08:00:27:94:58:41), Dst: PcsCompu_e6:d7:87 (08:00:27:e6:d7:87)
Internet Protocol Version 4, Src: 192.168.201.54, Dst: 192.168.201.2
User Datagram Protocol, Src Port: 59097, Dst Port: 53
Domain Name System (query)

0000  08 00 27 e6 d7 87 08 00  27 94 58 41 08 00 45 00   ··'·····'·XA··E·
0010  00 35 fd af 00 00 80 11  00 00 c0 a8 c9 36 c0 a8   ·5···········6··
0020  c9 02 e6 d9 00 35 00 21  13 bd cf ba 01 00 00 01   ·····5·!········
0030  00 00 00 00 00 00 04 62  63 63 69 02 74 76 00 00   ·······b cci·tv··
0040  01 00 01                                           ···

Domain Name System (dns), 25 bytes          Packets: 2366 · Displayed: 39 (1.6%) · Dropped: 0 (0.0%)          Profile: Default
```

File Machine View Input Devices Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search



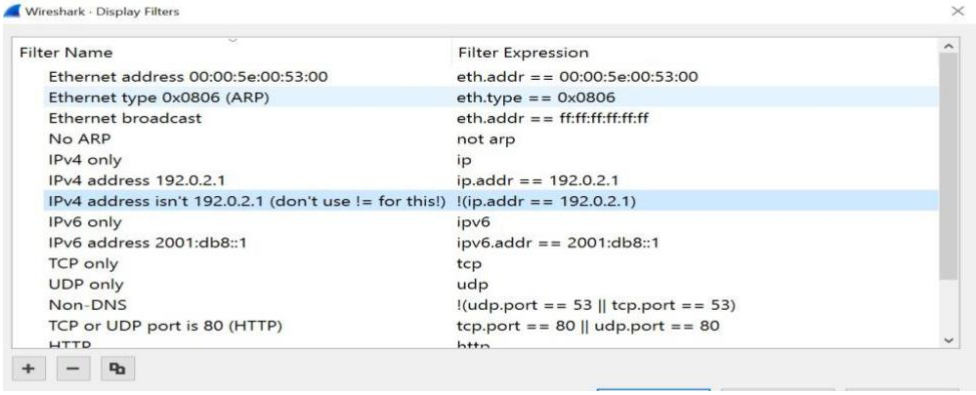
```
http or http2
No.   Time       Source          Source Port Destination      Destination Port Protocol Length tls.hndshk TCP Stream
   34 17.912398  192.168.1.119   54474       212.58.244.68    443              HTTP      491
  166 18.139553  212.58.244.68   443         192.168.1.119    54474            HTTP      501
  252 18.270837  192.168.1.119   54477       104.103.150.…    443              HTTP2     111
  253 18.270917  192.168.1.119   54477       104.103.150.…    443              HTTP2     108
  254 18.270993  192.168.1.119   54477       104.103.150.…    443              HTTP2     100
  255 18.271120  192.168.1.119   54477       104.103.150.…    443              HTTP2     349
  256 18.271166  192.168.1.119   54477       104.103.150.…    443              HTTP2     158
  257 18.271304  192.168.1.119   54477       104.103.150.…    443              HTTP2     164
  258 18.271427  192.168.1.119   54477       104.103.150.…    443              HTTP2     151
  259 18.271512  192.168.1.119   54477       104.103.150.…    443              HTTP2     153
  261 18.277288  192.168.1.119   54477       104.103.150.…    443              HTTP2     151
  262 18.277412  192.168.1.119   54477       104.103.150.…    443              HTTP2     166
  263 18.277537  192.168.1.119   54477       104.103.150.…    443              HTTP2     161
  266 18.284570  104.103.150.125 443         192.168.1.119    54477            HTTP2     135
  269 18.285352  192.168.1.119   54477       104.103.150.…    443              HTTP2      96
  271 18.291852  104.103.150.125 443         192.168.1.119    54477            HTTP2    1111
  274 18.294534  104.103.150.125 443         192.168.1.119    54477            HTTP2    1506
  276 18.294893  104.103.150.125 443         192.168.1.119    54477            TLSv1.2  1506
  277 18.295128  104.103.150.125 443         192.168.1.119    54477            HTTP2    1506
  280 18.296223  104.103.150.125 443         192.168.1.119    54477            TLSv1.2  1506              3

▶ Frame 252: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface en0, id 0 (outbound)
▶ Ethernet II, Src: Apple_98:81:ee (80:ea:96:98:81:ee), Dst: BillionE_27:db:82 (60:03:47:27:db:82)
▶ Internet Protocol Version 4, Src: 192.168.1.119, Dst: 104.103.150.125
▶ Transmission Control Protocol, Src Port: 54477, Dst Port: 443, Seq: 636, Ack: 4856, Len: 45
▶ Transport Layer Security
▼ HyperText Transfer Protocol 2
  ▼ Stream: Magic
      Magic: PRI * HTTP/2.0\r\n\r\nSM\r\n\r\n

Frame (111 bytes)   Decrypted TLS (24 bytes)
bbc-news.pcap          Packets: 1980 · Displayed: 467 (23.6%)          Profile: Default
```

4. tcp.port==xxx
   Sets filters for any TCP packet with a specific source or destination port. Sometimes is just useful and less time consuming to look only at the traffic that goes into or out of a specific port.

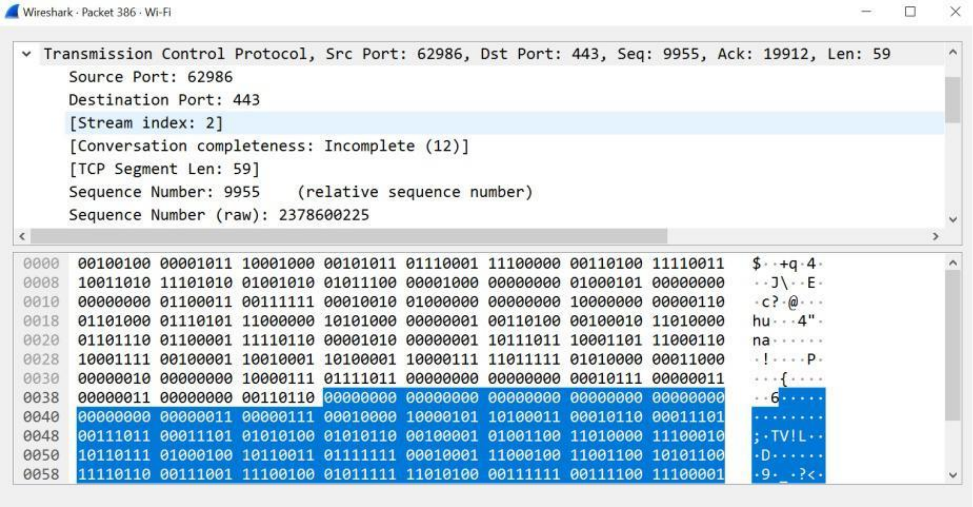


```
tcp
No.   Time       Source         Destination    Protocol Length Info
  138 26.218260  34.208.110.97  192.168.1.52   TLSv1.2   370 Application Data
  139 26.218260  34.208.110.97  192.168.1.52   TLSv1.2    92 Application Data
  140 26.218368  192.168.1.52   34.208.110.97  TCP        54 62986 → 443 [ACK] Seq=419 Ack=801 Win=508 Len=0
  141 26.220395  192.168.1.52   34.208.110.97  TLSv1.2    96 Application Data
  150 26.575741  192.168.1.52   34.208.110.97  TCP        96 [TCP Retransmission] 62986 → 443 [PSH, ACK] Seq=419 A

> Frame 3: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{BEDE0CDF-D84F-4436-818D-5D1E780DBFF5
> Ethernet II, Src: IntelCor_ea:4a:5c (34:f3:9a:ea:4a:5c), Dst: TaicangT_2b:71:e0 (24:0b:88:2b:71:e0)
> Internet Protocol Version 4, Src: 192.168.1.52, Dst: 185.184.8.90
> Transmission Control Protocol, Src Port: 51636, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000  00100100 00001011 10001000 00101011 01110001 11100000 00110100 11110011   $··+q·4·
0008  10011010 11101010 01001010 01011100 00001000 00000000 01000101 00000000   ··J\··E·
0010  00000000 00101001 10111100 00100100 01000000 00000000 10000000 00000110   ·)·$@···
0018  10111010 10111011 11000000 10101000 00000001 00110100 10111001 10111000   ·····4··
0020  00001000 01011010 11001001 10110100 00000001 10111011 01100010 10000011   ·Z····b·
0028  01011000 11010111 01111000 01011101 11011100 00010010 01010000 00010000   X·x]··P·
0030  00000001 11111101 01001110 10101101 00000000 00000000 00000000            ··N····
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



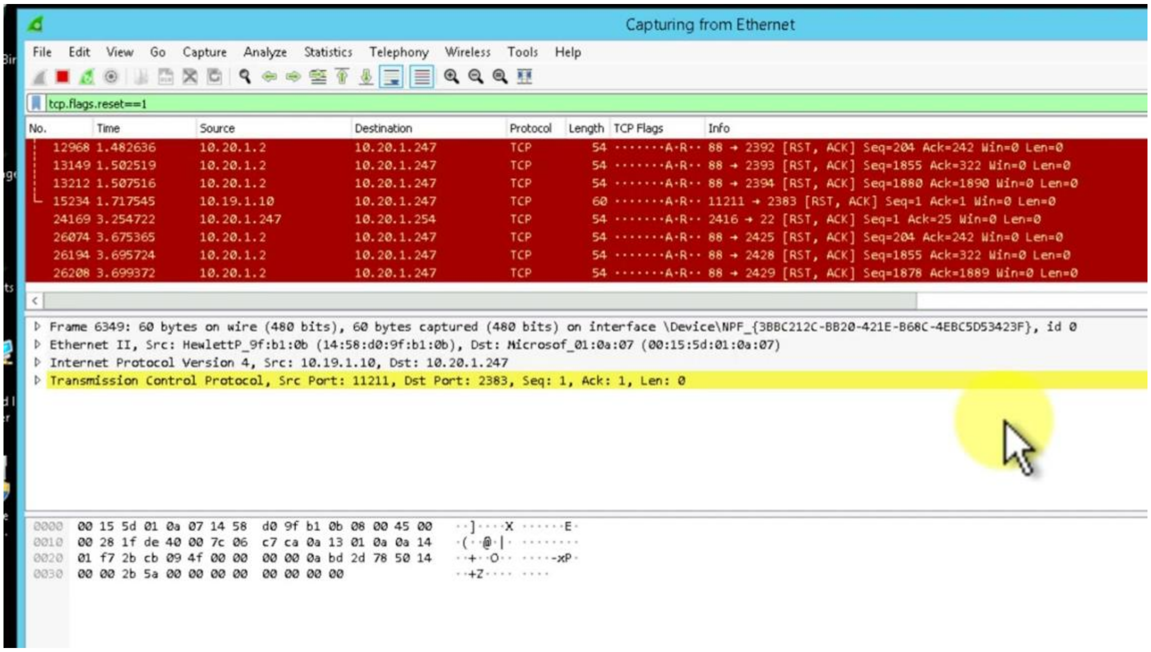
Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http



```
⌄ Transmission Control Protocol, Src Port: 62986, Dst Port: 443, Seq: 9955, Ack: 19912, Len: 59
    Source Port: 62986
    Destination Port: 443
    [Stream index: 2]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 59]
    Sequence Number: 9955    (relative sequence number)
    Sequence Number (raw): 2378600225
```

```
0000  00100100 00001011 10001000 00101011 01110001 11100000 00110100 11110011   $··+q·4·
0008  10011010 11101010 01001010 01011100 00001000 00000000 01000101 00000000   ··J\··E·
0010  00000000 01100011 00111111 00010010 01000000 00000000 10000000 00000110   ·c?·@···
0018  01101000 01110101 11000000 10101000 00000001 00110100 00100010 11010000   hu···4"·
0020  01101110 01100001 11110110 00001010 00000001 10111011 10001101 11000110   na······
0028  10001111 00100001 10010001 10100001 10000111 11011111 01010000 00011000   ·!····P·
0030  00000010 00000000 10000111 01111011 00000000 00000000 00010111 00000011   ···{····
0038  00000011 00000000 00110110 00000000 00000000 00000000 00000000 00000000   ··6·····
0040  00000000 00000011 00000111 00010000 10000101 10100011 00010110 00011101   ········
0048  00111011 00011101 01010100 01010110 00100001 01001100 11010000 11100010   ;·TV!L··
0050  10110111 01000100 10110011 01111111 00010001 11000100 11001100 10101100   ·D······
0058  11110110 00111001 11100100 01011111 11010100 00111111 00111100 11100001   ·9·_·?<·
```

5. tcp.flags.reset==1
   Sets filters to display all TCP resets. All packets have a TCP, if this is set to 1, it tells the receiving computer that it should at once stop using that connection. So, this filter is a powerful one, being that a TCP reset kills a TCP connection immediately.



tcp.flags.reset==1

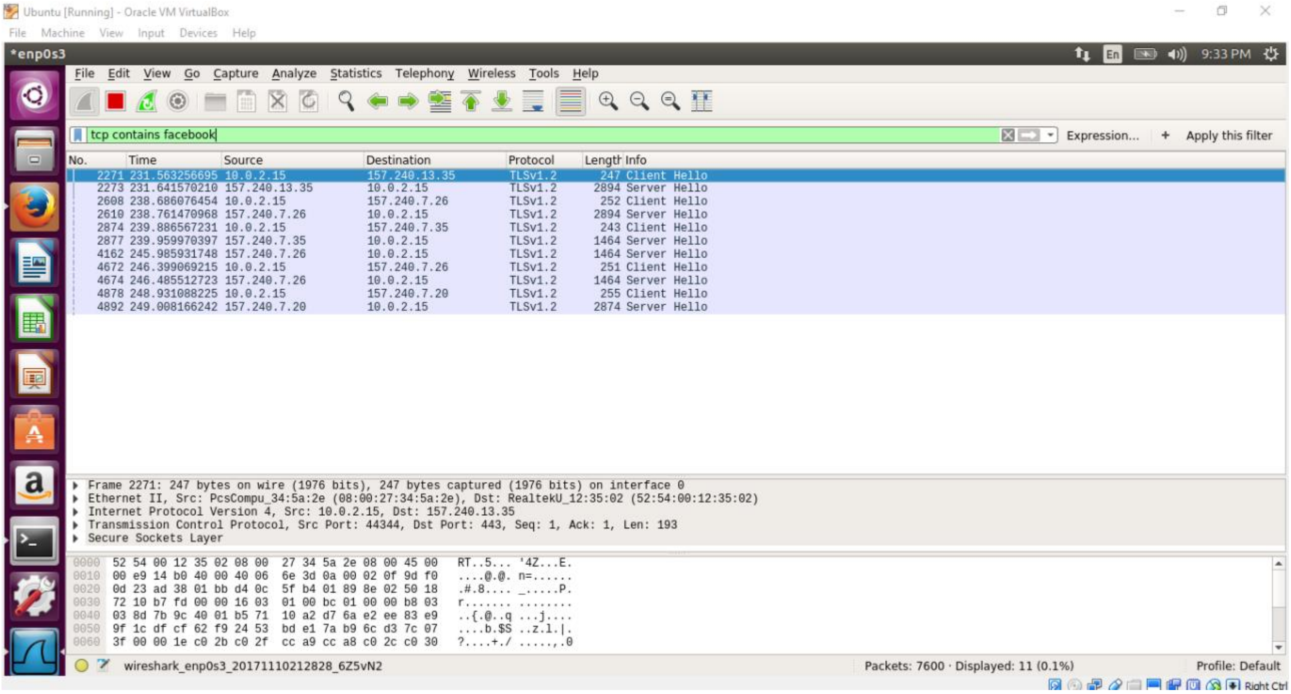
```
No.    Time      Source        Destination   Protocol Length TCP Flags   Info
 12968 1.482636  10.20.1.2     10.20.1.247   TCP      54 ·······A·R·· 88 → 2392 [RST, ACK] Seq=204 Ack=242 Win=0 Len=0
 13149 1.502519  10.20.1.2     10.20.1.247   TCP      54 ·······A·R·· 88 → 2393 [RST, ACK] Seq=1855 Ack=322 Win=0 Len=0
 13212 1.507516  10.20.1.2     10.20.1.247   TCP      54 ·······A·R·· 88 → 2394 [RST, ACK] Seq=1880 Ack=1890 Win=0 Len=0
 15234 1.717545  10.19.1.10    10.20.1.247   TCP      60 ·······A·R·· 11211 → 2383 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 24169 3.254722  10.20.1.247   10.20.1.254   TCP      54 ·······A·R·· 2416 → 22 [RST, ACK] Seq=1 Ack=25 Win=0 Len=0
 26074 3.675365  10.20.1.2     10.20.1.247   TCP      54 ·······A·R·· 88 → 2425 [RST, ACK] Seq=204 Ack=242 Win=0 Len=0
 26194 3.695724  10.20.1.2     10.20.1.247   TCP      54 ·······A·R·· 88 → 2428 [RST, ACK] Seq=1855 Ack=322 Win=0 Len=0
 26208 3.699372  10.20.1.2     10.20.1.247   TCP      54 ·······A·R·· 88 → 2429 [RST, ACK] Seq=1878 Ack=1889 Win=0 Len=0
```

```
▷ Frame 6349: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3BBC212C-BB20-421E-B68C-4EBC5D53423F}, id 0
▷ Ethernet II, Src: HewlettP_9f:b1:0b (14:58:d0:9f:b1:0b), Dst: Microsof_01:0a:07 (00:15:5d:01:0a:07)
▷ Internet Protocol Version 4, Src: 10.19.1.10, Dst: 10.20.1.247
▷ Transmission Control Protocol, Src Port: 11211, Dst Port: 2383, Seq: 1, Ack: 1, Len: 0
```

```
0000  00 15 5d 01 0a 07 14 58  d0 9f b1 0b 08 00 45 00   ··]····X ······E·
0010  00 28 1f de 40 00 7c 06  c7 ca 0a 13 01 0a 0a 14   ·(··@·|· ········
0020  01 f7 2b cb 09 4f 00 00  00 00 0a bd 2d 78 50 14   ··+··O·· ····-xP·
0030  00 00 2b 5a 00 00 00 00  00 00 00 00               ··+Z···· ····
```

6. tcp contains xxx

It's a filter that displays all TCP packets that contain a certain term (instead of xxx, use what term you're looking for). For example, if you are looking for a specific term appearing in the packet, this filter is what you need.


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
9:33 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+ Apply this filter

tcp contains facebook

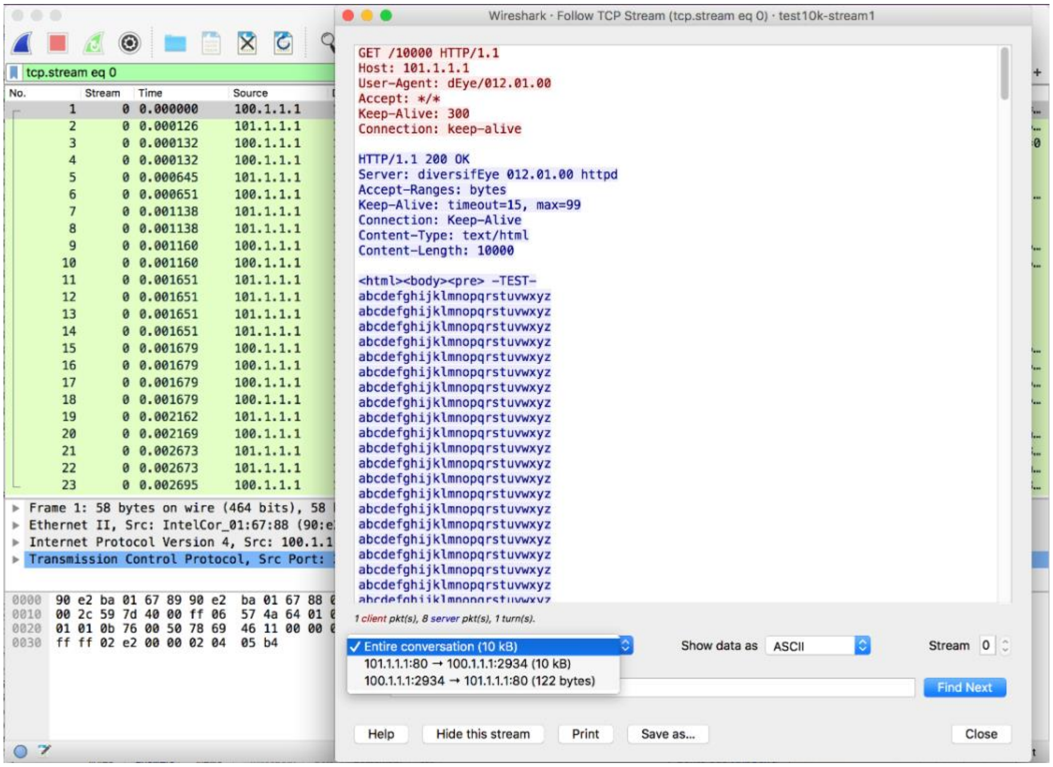
```
No.  Time           Source          Destination     Protocol  Length Info
2271 231.563256695 10.0.2.15       157.240.13.35   TLSv1.2    247 Client Hello
2273 231.641570210 157.240.13.35   10.0.2.15       TLSv1.2   2894 Server Hello
2608 238.686076454 10.0.2.15       157.240.7.26    TLSv1.2    252 Client Hello
2610 238.761470968 157.240.7.26    10.0.2.15       TLSv1.2   2894 Server Hello
2874 239.886567231 10.0.2.15       157.240.7.35    TLSv1.2    243 Client Hello
2877 239.959970397 157.240.7.35    10.0.2.15       TLSv1.2   1464 Server Hello
4162 245.985931748 157.240.7.26    10.0.2.15       TLSv1.2   1464 Server Hello
4672 246.399069215 10.0.2.15       157.240.7.26    TLSv1.2    251 Client Hello
4674 246.485512723 157.240.7.26    10.0.2.15       TLSv1.2   1464 Server Hello
4878 248.931088225 10.0.2.15       157.240.7.20    TLSv1.2    255 Client Hello
4892 249.008166242 157.240.7.20    10.0.2.15       TLSv1.2   2874 Server Hello
```

```
▸ Frame 2271: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_34:5a:2e (08:00:27:34:5a:2e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.13.35
▸ Transmission Control Protocol, Src Port: 44344, Dst Port: 443, Seq: 1, Ack: 1, Len: 193
▸ Secure Sockets Layer
```

```
0000  52 54 00 12 35 02 08 00  27 34 5a 2e 08 00 45 00   RT..5... '4Z...E.
0010  00 e9 14 b0 40 00 40 06  6e 3d 0a 00 02 0f 9d f0   ....@.@. n=......
0020  0d 23 ad 38 01 bb d4 0c  5f b4 01 89 8e 02 50 18   .#.8.... _.....P.
0030  72 10 b7 fd 00 00 16 03  01 00 bc 01 00 00 b8 03   r....... ........
0040  03 8d 7b 9c 40 01 b5 71  10 a2 d7 6a e2 ee 83 e9   ..{.@..q ...j....
0050  9f 1c df cf 62 f9 24 53  bd e1 7a b9 6c d3 7c 07   ....b.$S ..z.l.|.
0060  3f 00 00 1e c0 2b c0 2f  cc a9 cc a8 c0 2c c0 30   ?....+./ .....,.0
```

wireshark_enp0s3_20171110212828_6Z5vN2 | Packets: 7600 · Displayed: 11 (0.1%) | Profile: Default

7. tcp.stream eq X
Follows a tcp stream.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · test10k-stream1

tcp.stream eq 0

```
No.  Stream Time      Source
  1      0 0.000000  100.1.1.1
  2      0 0.000126  101.1.1.1
  3      0 0.000132  100.1.1.1
  4      0 0.000132  100.1.1.1
  5      0 0.000645  101.1.1.1
  6      0 0.000651  100.1.1.1
  7      0 0.001138  101.1.1.1
  8      0 0.001138  101.1.1.1
  9      0 0.001160  100.1.1.1
 10      0 0.001160  100.1.1.1
 11      0 0.001651  101.1.1.1
 12      0 0.001651  101.1.1.1
 13      0 0.001651  101.1.1.1
 14      0 0.001651  101.1.1.1
 15      0 0.001679  100.1.1.1
 16      0 0.001679  100.1.1.1
 17      0 0.001679  100.1.1.1
 18      0 0.001679  100.1.1.1
 19      0 0.002162  101.1.1.1
 20      0 0.002169  100.1.1.1
 21      0 0.002673  101.1.1.1
 22      0 0.002673  101.1.1.1
 23      0 0.002695  100.1.1.1
```

```
▸ Frame 1: 58 bytes on wire (464 bits), 58
▸ Ethernet II, Src: IntelCor_01:67:88 (90:e
▸ Internet Protocol Version 4, Src: 100.1.1
▸ Transmission Control Protocol, Src Port:
```

```
0000  90 e2 ba 01 67 89 90 e2  ba 01 67 88
0010  00 2c 59 7d 40 00 ff 06  57 4a 64 01
0020  01 01 0b 76 00 50 78 69  46 11 00 00
0030  ff ff 02 e2 00 00 02 04  05 b4
```

```
GET /10000 HTTP/1.1
Host: 101.1.1.1
User-Agent: dEye/012.01.00
Accept: */*
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 200 OK
Server: diversifEye 012.01.00 httpd
Accept-Ranges: bytes
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 10000

<html><body><pre> -TEST-
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyz
```

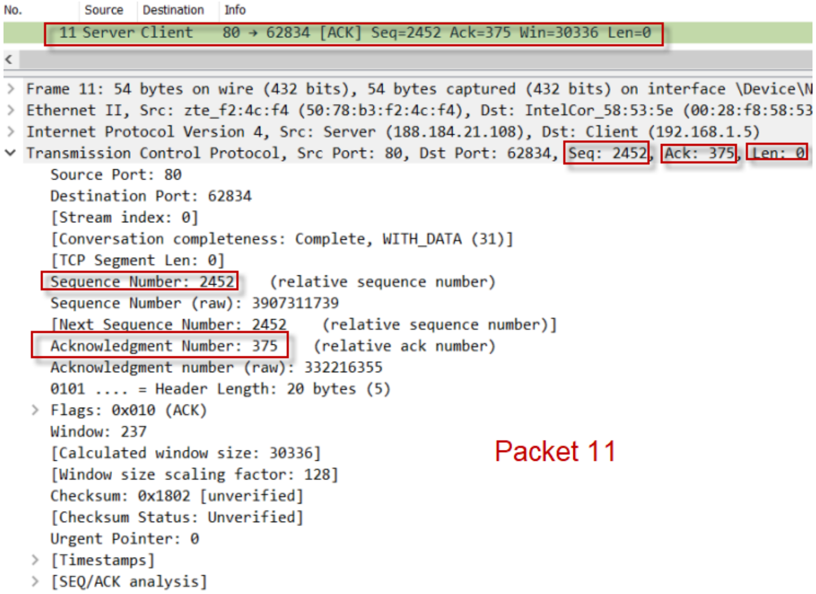
1 client pkt(s), 8 server pkt(s), 1 turn(s).

✓ Entire conversation (10 kB)
101.1.1.1:80 → 100.1.1.1:2934 (10 kB)
100.1.1.1:2934 → 101.1.1.1:80 (122 bytes)

Show data as ASCII

Stream 0

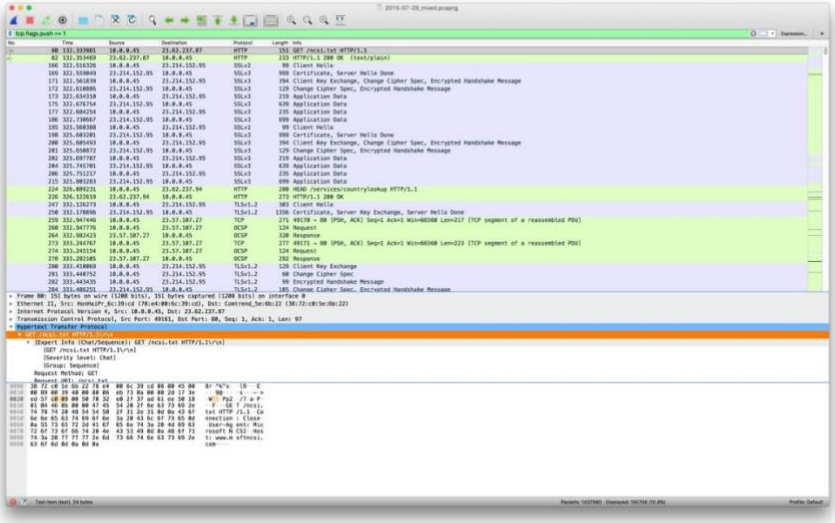
8. tcp.seq == x
Filters by sequence number.



```
No.    Source  Destination  Info
  11 Server Client    80 → 62834 [ACK] Seq=2452 Ack=375 Win=30336 Len=0

> Frame 11: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\N
> Ethernet II, Src: zte_f2:4c:f4 (50:78:b3:f2:4c:f4), Dst: IntelCor_58:53:5e (00:28:f8:58:53
> Internet Protocol Version 4, Src: Server (188.184.21.108), Dst: Client (192.168.1.5)
v Transmission Control Protocol, Src Port: 80, Dst Port: 62834, Seq: 2452, Ack: 375, Len: 0
    Source Port: 80
    Destination Port: 62834
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 2452    (relative sequence number)
    Sequence Number (raw): 3907311739
    [Next Sequence Number: 2452    (relative sequence number)]
    Acknowledgment Number: 375    (relative ack number)
    Acknowledgment number (raw): 332216355
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x1802 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

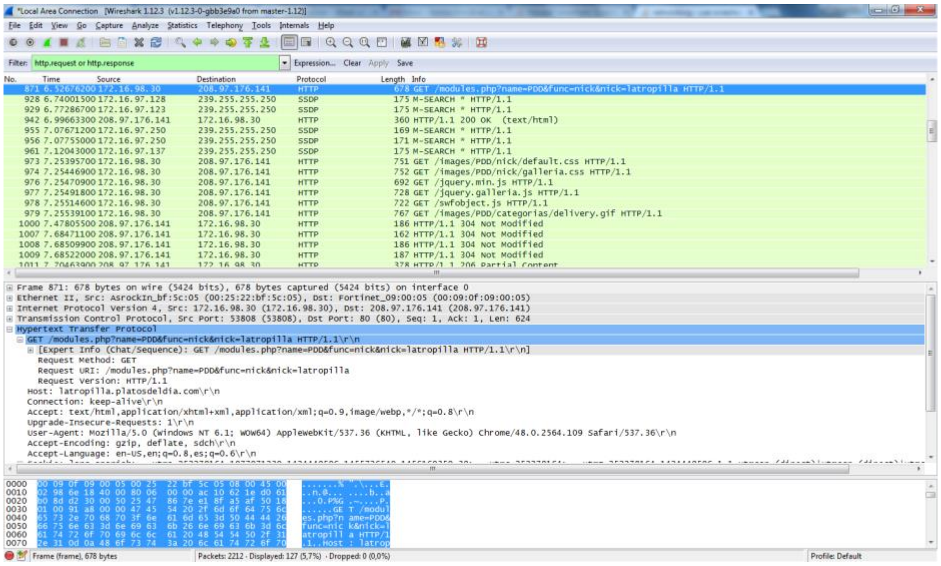
Packet 11

9. tcp.flags.push == 1
   Important for troubleshooting, this filter detects push events.



```
tcp.flags.push == 1
No.  Time         Source          Destination     Protocol  Length  Info
 80 132.333981   10.0.0.45       23.62.237.87    HTTP      151 GET /ncsi.txt HTTP/1.1
 82 132.353469   23.62.237.87    10.0.0.45       HTTP      233 HTTP/1.1 200 OK  (text/plain)
166 322.516326   10.0.0.45       23.214.152.95   SSLv2      99 Client Hello
169 322.559049   23.214.152.95   10.0.0.45       SSLv3     999 Certificate, Server Hello Done
171 322.561839   10.0.0.45       23.214.152.95   SSLv3     394 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
172 322.610086   23.214.152.95   10.0.0.45       SSLv3     129 Change Cipher Spec, Encrypted Handshake Message
173 322.634310   10.0.0.45       23.214.152.95   SSLv3     219 Application Data
175 322.676754   23.214.152.95   10.0.0.45       SSLv3     639 Application Data
177 322.684254   10.0.0.45       23.214.152.95   SSLv3     235 Application Data
186 322.730667   23.214.152.95   10.0.0.45       SSLv3     699 Application Data
195 325.560308   10.0.0.45       23.214.152.95   SSLv2      99 Client Hello
198 325.603201   23.214.152.95   10.0.0.45       SSLv3     999 Certificate, Server Hello Done
200 325.605493   10.0.0.45       23.214.152.95   SSLv3     394 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
201 325.650872   23.214.152.95   10.0.0.45       SSLv3     129 Change Cipher Spec, Encrypted Handshake Message
202 325.697707   10.0.0.45       23.214.152.95   SSLv3     219 Application Data
204 325.745701   23.214.152.95   10.0.0.45       SSLv3     639 Application Data
206 325.751217   10.0.0.45       23.214.152.95   SSLv3     235 Application Data
215 325.803283   23.214.152.95   10.0.0.45       SSLv3     699 Application Data
224 326.089231   10.0.0.45       23.62.237.94    HTTP      200 HEAD /services/countrylookup HTTP/1.1
226 326.122619   23.62.237.94    10.0.0.45       HTTP      273 HTTP/1.1 200 OK
247 332.126273   10.0.0.45       23.214.152.95   TLSv1.2   303 Client Hello
250 332.170096   23.214.152.95   10.0.0.45       TLSv1.2  1356 Certificate, Server Key Exchange, Server Hello Done
259 332.947440   10.0.0.45       23.57.107.27    TCP       271 49170 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66560 Len=217 [TCP segment of a reassembled PDU]
260 332.947776   10.0.0.45       23.57.107.27    OCSP      124 Request
264 332.982423   23.57.107.27    10.0.0.45       OCSP      320 Response
273 333.244767   10.0.0.45       23.57.107.27    TCP       277 49171 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66560 Len=223 [TCP segment of a reassembled PDU]
274 333.245154   10.0.0.45       23.57.107.27    OCSP      124 Request
278 333.282105   23.57.107.27    10.0.0.45       OCSP      292 Response
280 333.410069   10.0.0.45       23.214.152.95   TLSv1.2   129 Client Key Exchange
281 333.440752   10.0.0.45       23.214.152.95   TLSv1.2    60 Change Cipher Spec
282 333.443435   10.0.0.45       23.214.152.95   TLSv1.2    99 Encrypted Handshake Message
284 333.486251   23.214.152.95   10.0.0.45       TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message

> Frame 80: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
> Ethernet II, Src: HonHaiPr_6c:39:cd (78:e4:00:6c:39:cd), Dst: Comtrend_5e:6b:22 (38:72:c0:5e:6b:22)
> Internet Protocol Version 4, Src: 10.0.0.45, Dst: 23.62.237.87
> Transmission Control Protocol, Src Port: 49161, Dst Port: 80, Seq: 1, Ack: 1, Len: 97
v Hypertext Transfer Protocol
  v GET /ncsi.txt HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /ncsi.txt HTTP/1.1\r\n]
        [GET /ncsi.txt HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /ncsi.txt
```

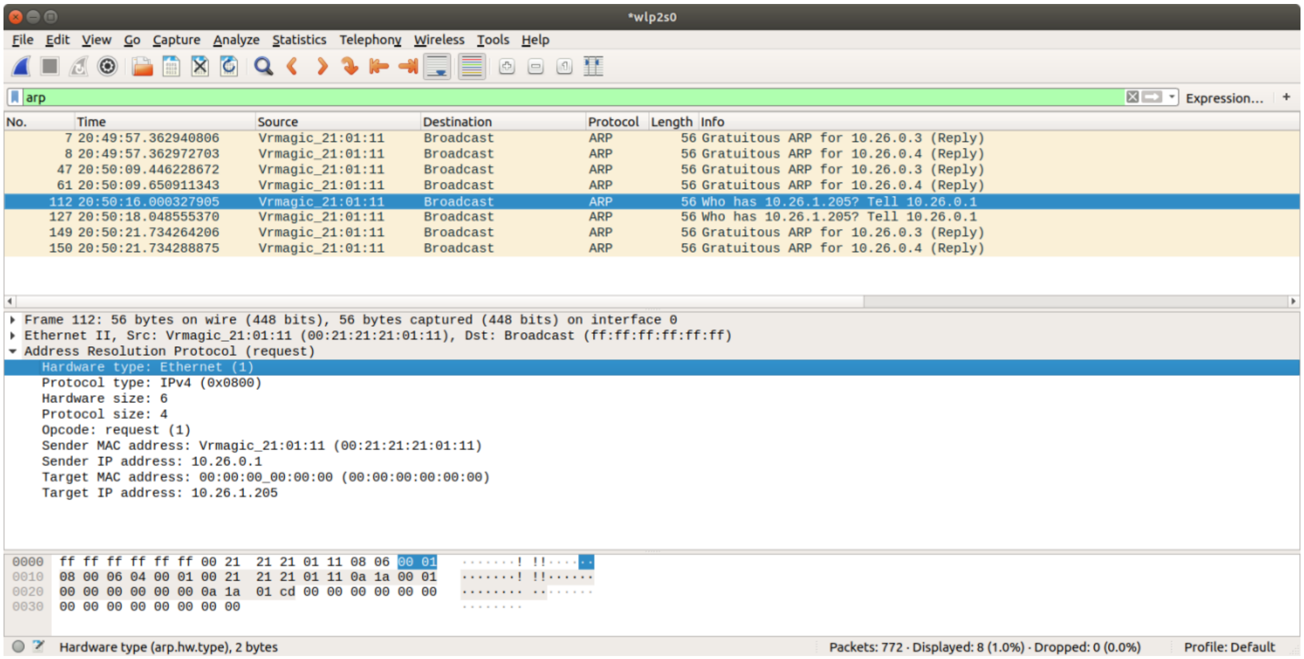
10. http.request
    This one filters all HTTP GET and POST requests. It can show the most accessed webpages.



*Local Area Connection [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
Filter: http.request or http.response
No.   Time        Source          Destination      Protocol  Length Info
  871 6.52676200 172.16.98.30    208.97.176.141   HTTP      678 GET /modules.php?name=PDD&func=nick&nick=latropilla HTTP/1.1
  928 6.74001500 172.16.97.128   239.255.255.250  SSDP      175 M-SEARCH * HTTP/1.1
  929 6.77286700 172.16.97.123   239.255.255.250  SSDP      175 M-SEARCH * HTTP/1.1
  942 6.99663300 208.97.176.141  172.16.98.30     HTTP      360 HTTP/1.1 200 OK  (text/html)
  955 7.07671200 172.16.97.250   239.255.255.250  SSDP      169 M-SEARCH * HTTP/1.1
  956 7.07755000 172.16.97.250   239.255.255.250  SSDP      171 M-SEARCH * HTTP/1.1
  961 7.12043000 172.16.97.137   239.255.255.250  SSDP      175 M-SEARCH * HTTP/1.1
  973 7.25395700 172.16.98.30    208.97.176.141   HTTP      751 GET /images/PDD/nick/default.css HTTP/1.1
  974 7.25446900 172.16.98.30    208.97.176.141   HTTP      752 GET /images/PDD/nick/galleria.css HTTP/1.1
  976 7.25470900 172.16.98.30    208.97.176.141   HTTP      692 GET /jquery.min.js HTTP/1.1
  977 7.25491800 172.16.98.30    208.97.176.141   HTTP      728 GET /jquery.galleria.js HTTP/1.1
  978 7.25514600 172.16.98.30    208.97.176.141   HTTP      722 GET /swfobject.js HTTP/1.1
  979 7.25539100 172.16.98.30    208.97.176.141   HTTP      767 GET /images/PDD/categorias/delivery.gif HTTP/1.1
 1000 7.47805500 208.97.176.141  172.16.98.30     HTTP      186 HTTP/1.1 304 Not Modified
 1007 7.68471100 208.97.176.141  172.16.98.30     HTTP      162 HTTP/1.1 304 Not Modified
 1008 7.68509900 208.97.176.141  172.16.98.30     HTTP      186 HTTP/1.1 304 Not Modified
 1009 7.68522000 208.97.176.141  172.16.98.30     HTTP      187 HTTP/1.1 304 Not Modified
 1011 7.70463900 208.97.176.141  172.16.98.30     HTTP      378 HTTP/1.1 206 Partial Content

⊞ Frame 871: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface 0
⊞ Ethernet II, Src: AsrockIn_bf:5c:05 (00:25:22:bf:5c:05), Dst: Fortinet_09:00:05 (00:09:0f:09:00:05)
⊞ Internet Protocol Version 4, Src: 172.16.98.30 (172.16.98.30), Dst: 208.97.176.141 (208.97.176.141)
⊞ Transmission Control Protocol, Src Port: 53808 (53808), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 624
⊟ Hypertext Transfer Protocol
  ⊟ GET /modules.php?name=PDD&func=nick&nick=latropilla HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /modules.php?name=PDD&func=nick&nick=latropilla HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /modules.php?name=PDD&func=nick&nick=latropilla
      Request Version: HTTP/1.1
    Host: latropilla.platosdeldia.com\r\n
    Connection: keep-alive\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8,es;q=0.6\r\n

0000  00 09 0f 09 00 05 00 25  22 bf 5c 05 08 00 45 00   .......% ".\...E.
0010  02 98 6e 18 40 00 80 06  00 00 ac 10 62 1e d0 61   ..n.@... ....b..a
0020  b0 8d d2 30 00 50 25 47  86 7e e1 8f a5 af 50 18   ...0.P%G .~....P.
0030  01 00 91 a8 00 00 47 45  54 20 2f 6d 6f 64 75 6c   ......GE T /modul
0040  65 73 2e 70 68 70 3f 6e  61 6d 65 3d 50 44 44 26   es.php?n ame=PDD&
0050  66 75 6e 63 3d 6e 69 63  6b 26 6e 69 63 6b 3d 6c   func=nic k&nick=l
0060  61 74 72 6f 70 69 6c 6c  61 20 48 54 54 50 2f 31   atropill a HTTP/1
0070  2e 31 0d 0a 48 6f 73 74  3a 20 6c 61 74 72 6f 70   .1..Host : latrop

Frame (frame), 678 bytes    Packets: 2212 · Displayed: 127 (5,7%) · Dropped: 0 (0,0%)    Profile: Default
```

11. !(arp or icmp or dns)
    Designed to filter out certain types of protocols, it masks out arp, icmp, dns, or other protocols you think are not useful. This will allow you to focus of what traffic interests you.


*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

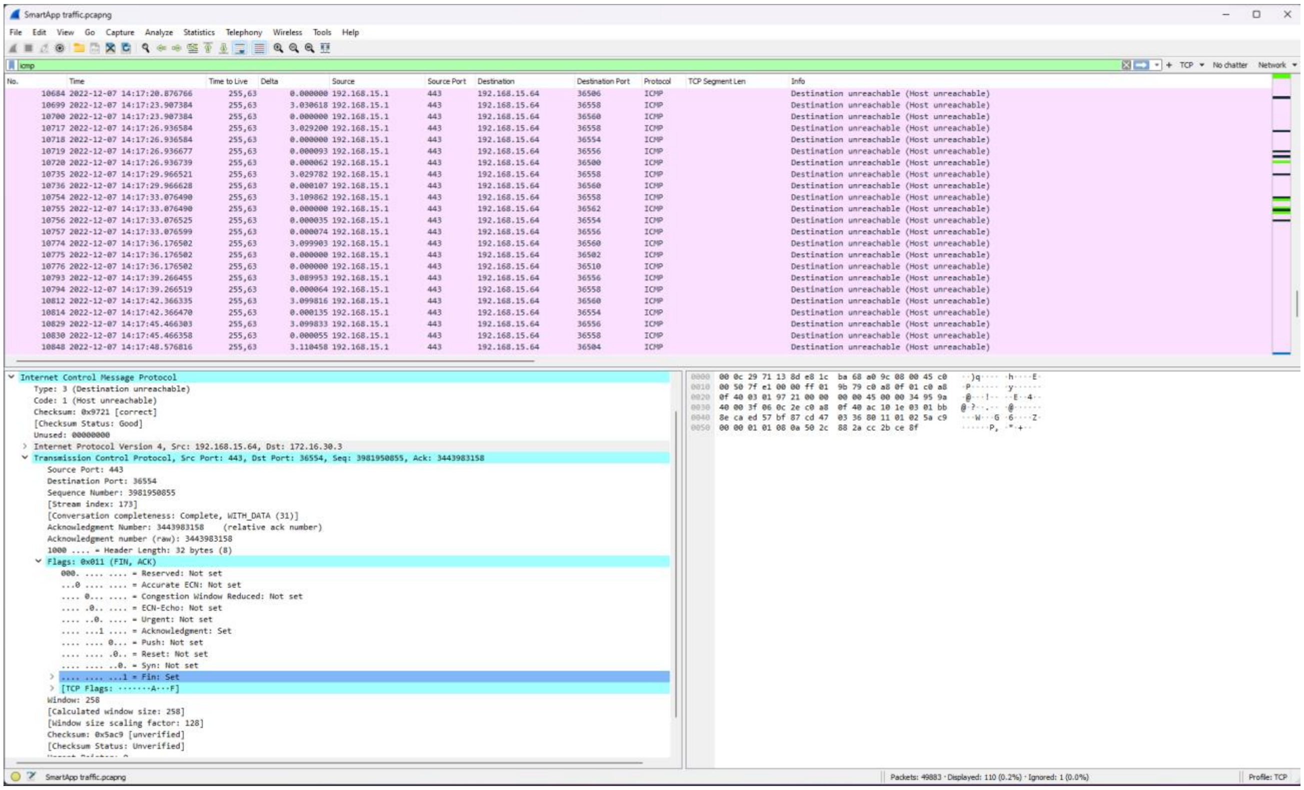
arp

```
No.     Time                Source             Destination   Protocol Length Info
      7 20:49:57.362940806  Vrmagic_21:01:11   Broadcast     ARP        56 Gratuitous ARP for 10.26.0.3 (Reply)
      8 20:49:57.362972703  Vrmagic_21:01:11   Broadcast     ARP        56 Gratuitous ARP for 10.26.0.4 (Reply)
     47 20:50:09.446228672  Vrmagic_21:01:11   Broadcast     ARP        56 Gratuitous ARP for 10.26.0.3 (Reply)
     61 20:50:09.650911343  Vrmagic_21:01:11   Broadcast     ARP        56 Gratuitous ARP for 10.26.0.4 (Reply)
    112 20:50:16.000327905  Vrmagic_21:01:11   Broadcast     ARP        56 Who has 10.26.1.205? Tell 10.26.0.1
    127 20:50:18.048555370  Vrmagic_21:01:11   Broadcast     ARP        56 Who has 10.26.1.205? Tell 10.26.0.1
    149 20:50:21.734264206  Vrmagic_21:01:11   Broadcast     ARP        56 Gratuitous ARP for 10.26.0.3 (Reply)
    150 20:50:21.734288875  Vrmagic_21:01:11   Broadcast     ARP        56 Gratuitous ARP for 10.26.0.4 (Reply)
```

```
▸ Frame 112: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▸ Ethernet II, Src: Vrmagic_21:01:11 (00:21:21:21:01:11), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Vrmagic_21:01:11 (00:21:21:21:01:11)
    Sender IP address: 10.26.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.26.1.205
```

```
0000  ff ff ff ff ff ff 00 21  21 21 01 11 08 06 00 01   ·······! !!······
0010  08 00 06 04 00 01 00 21  21 21 01 11 0a 1a 00 01   ·······! !!······
0020  00 00 00 00 00 00 0a 1a  01 cd 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00                            ········
```

Hardware type (arp.hw.type), 2 bytes   Packets: 772 · Displayed: 8 (1.0%) · Dropped: 0 (0.0%)   Profile: Default


SmartApp traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
+ TCP ▾ No chatter Network ▾

icmp

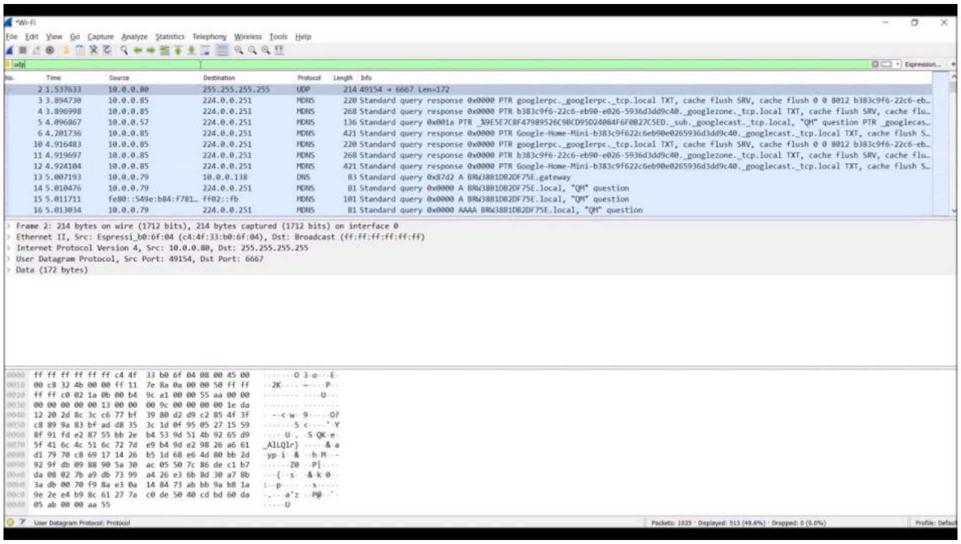
```
No.   Time                        Time to Live Delta    Source        Source Port Destination   Destination Port Protocol TCP Segment Len Info
10684 2022-12-07 14:17:20.876766  255,63       0.000000 192.168.15.1  443         192.168.15.64 36506            ICMP                     Destination unreachable (Host unreachable)
10699 2022-12-07 14:17:23.907384  255,63       3.030618 192.168.15.1  443         192.168.15.64 36558            ICMP                     Destination unreachable (Host unreachable)
10700 2022-12-07 14:17:23.907384  255,63       0.000000 192.168.15.1  443         192.168.15.64 36560            ICMP                     Destination unreachable (Host unreachable)
10717 2022-12-07 14:17:26.936584  255,63       3.029200 192.168.15.1  443         192.168.15.64 36558            ICMP                     Destination unreachable (Host unreachable)
10718 2022-12-07 14:17:26.936584  255,63       0.000000 192.168.15.1  443         192.168.15.64 36554            ICMP                     Destination unreachable (Host unreachable)
10719 2022-12-07 14:17:26.936677  255,63       0.000093 192.168.15.1  443         192.168.15.64 36556            ICMP                     Destination unreachable (Host unreachable)
10720 2022-12-07 14:17:26.936739  255,63       0.000062 192.168.15.1  443         192.168.15.64 36500            ICMP                     Destination unreachable (Host unreachable)
10735 2022-12-07 14:17:29.966521  255,63       3.029782 192.168.15.1  443         192.168.15.64 36558            ICMP                     Destination unreachable (Host unreachable)
10736 2022-12-07 14:17:29.966628  255,63       0.000107 192.168.15.1  443         192.168.15.64 36560            ICMP                     Destination unreachable (Host unreachable)
10754 2022-12-07 14:17:33.076490  255,63       3.109862 192.168.15.1  443         192.168.15.64 36558            ICMP                     Destination unreachable (Host unreachable)
10755 2022-12-07 14:17:33.076490  255,63       0.000000 192.168.15.1  443         192.168.15.64 36562            ICMP                     Destination unreachable (Host unreachable)
10756 2022-12-07 14:17:33.076525  255,63       0.000035 192.168.15.1  443         192.168.15.64 36554            ICMP                     Destination unreachable (Host unreachable)
10757 2022-12-07 14:17:33.076599  255,63       0.000074 192.168.15.1  443         192.168.15.64 36556            ICMP                     Destination unreachable (Host unreachable)
10774 2022-12-07 14:17:36.176502  255,63       3.099903 192.168.15.1  443         192.168.15.64 36560            ICMP                     Destination unreachable (Host unreachable)
10775 2022-12-07 14:17:36.176502  255,63       0.000000 192.168.15.1  443         192.168.15.64 36502            ICMP                     Destination unreachable (Host unreachable)
10776 2022-12-07 14:17:36.176502  255,63       0.000000 192.168.15.1  443         192.168.15.64 36510            ICMP                     Destination unreachable (Host unreachable)
10793 2022-12-07 14:17:39.266455  255,63       3.089953 192.168.15.1  443         192.168.15.64 36556            ICMP                     Destination unreachable (Host unreachable)
10794 2022-12-07 14:17:39.266519  255,63       0.000064 192.168.15.1  443         192.168.15.64 36558            ICMP                     Destination unreachable (Host unreachable)
10812 2022-12-07 14:17:42.366335  255,63       3.099816 192.168.15.1  443         192.168.15.64 36560            ICMP                     Destination unreachable (Host unreachable)
10814 2022-12-07 14:17:42.366470  255,63       0.000135 192.168.15.1  443         192.168.15.64 36554            ICMP                     Destination unreachable (Host unreachable)
10829 2022-12-07 14:17:45.466303  255,63       3.099833 192.168.15.1  443         192.168.15.64 36556            ICMP                     Destination unreachable (Host unreachable)
10830 2022-12-07 14:17:45.466358  255,63       0.000055 192.168.15.1  443         192.168.15.64 36558            ICMP                     Destination unreachable (Host unreachable)
10848 2022-12-07 14:17:48.576816  255,63       3.110458 192.168.15.1  443         192.168.15.64 36504            ICMP                     Destination unreachable (Host unreachable)
```

```
˅ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 1 (Host unreachable)
    Checksum: 0x9721 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 192.168.15.64, Dst: 172.16.30.3
  ˅ Transmission Control Protocol, Src Port: 443, Dst Port: 36554, Seq: 3981950855, Ack: 3443983158
      Source Port: 443
      Destination Port: 36554
      Sequence Number: 3981950855
      [Stream index: 173]
      [Conversation completeness: Complete, WITH_DATA (31)]
      Acknowledgment Number: 3443983158    (relative ack number)
      Acknowledgment number (raw): 3443983158
      1000 .... = Header Length: 32 bytes (8)
    ˅ Flags: 0x011 (FIN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
      > .... .... ...1 = Fin: Set
      > [TCP Flags: ·······A···F]
      Window: 258
      [Calculated window size: 258]
      [Window size scaling factor: 128]
      Checksum: 0x5ac9 [unverified]
      [Checksum Status: Unverified]
```

```
0000  00 0c 29 71 13 8d e8 1c  ba 68 a0 9c 08 00 45 c0   ··)q···· ·h····E·
0010  00 50 7f e1 00 00 ff 01  9b 79 c0 a8 0f 01 c0 a8   ·P······ ·y······
0020  0f 40 03 01 97 21 00 00  00 00 45 00 00 34 95 9a   ·@···!·· ··E··4··
0030  40 00 3f 06 0c 2e c0 a8  0f 40 ac 10 1e 03 01 bb   @·?··.·· ·@······
0040  8e ca ed 57 bf 87 cd 47  03 36 80 11 01 02 5a c9   ···W···G ·6····Z·
0050  00 00 01 01 08 0a 50 2c  88 2a cc 2b ce 8f         ······P, ·*·+··
```

SmartApp traffic.pcapng   Packets: 49883 · Displayed: 110 (0.2%) · Ignored: 1 (0.0%)   Profile: TCP

12. udp contains xx:xx:xx
    It sets a filter for certain HEX values at any offset.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

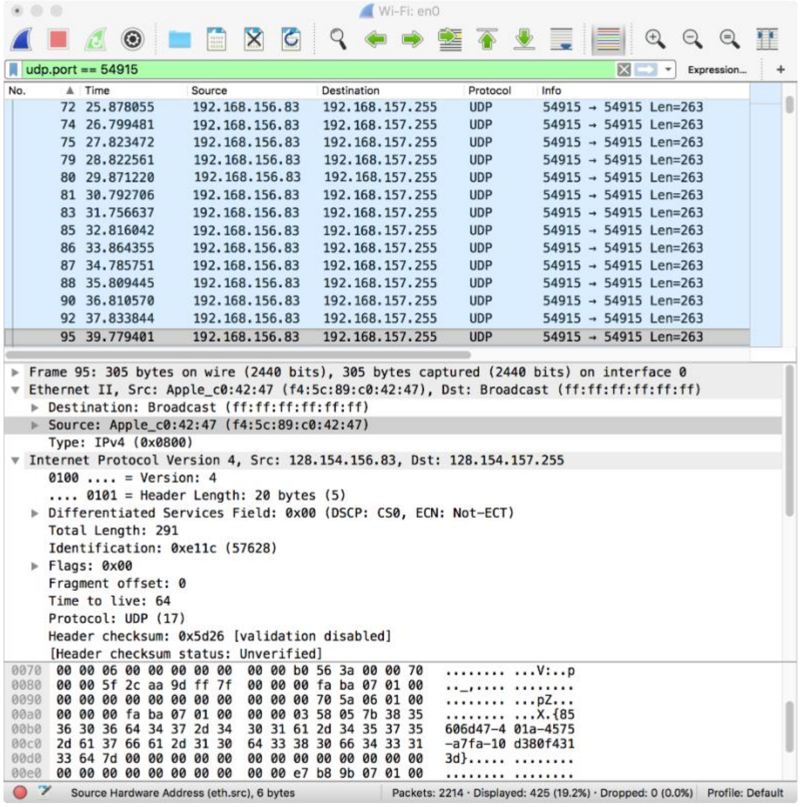
```
udp
```

```
No.   Time        Source                  Destination      Protocol  Length Info
    2 1.537633    10.0.0.80               255.255.255.255  UDP       214 49154 → 6667 Len=172
    3 3.894730    10.0.0.85               224.0.0.251      MDNS      220 Standard query response 0x0000 PTR googlerpc._googlerpc._tcp.local TXT, cache flush SRV, cache flush 0 0 8012 b383c9f6-22c6-eb…
    4 3.896998    10.0.0.85               224.0.0.251      MDNS      268 Standard query response 0x0000 PTR b383c9f6-22c6-eb90-e026-5936d3dd9c40._googlezone._tcp.local TXT, cache flush SRV, cache flu…
    5 4.096867    10.0.0.57               224.0.0.251      MDNS      136 Standard query 0x001a PTR _%9E5E7C8F47989526C9BCD95D24084F6F0827C5ED._sub._googlecast._tcp.local, "QM" question PTR _googlecas…
    6 4.201736    10.0.0.85               224.0.0.251      MDNS      421 Standard query response 0x0000 PTR Google-Home-Mini-b383c9f622c6eb90e0265936d3dd9c40._googlecast._tcp.local TXT, cache flush S…
   10 4.916483    10.0.0.85               224.0.0.251      MDNS      220 Standard query response 0x0000 PTR googlerpc._googlerpc._tcp.local TXT, cache flush SRV, cache flush 0 0 8012 b383c9f6-22c6-eb…
   11 4.919697    10.0.0.85               224.0.0.251      MDNS      268 Standard query response 0x0000 PTR b383c9f6-22c6-eb90-e026-5936d3dd9c40._googlezone._tcp.local TXT, cache flush SRV, cache flu…
   12 4.924104    10.0.0.85               224.0.0.251      MDNS      421 Standard query response 0x0000 PTR Google-Home-Mini-b383c9f622c6eb90e0265936d3dd9c40._googlecast._tcp.local TXT, cache flush S…
   13 5.007193    10.0.0.79               10.0.0.138       DNS        83 Standard query 0x87d2 A BRW38B1DB2DF75E.gateway
   14 5.010476    10.0.0.79               224.0.0.251      MDNS       81 Standard query 0x0000 A BRW38B1DB2DF75E.local, "QM" question
   15 5.011711    fe80::549e:b84:f781…    ff02::fb         MDNS      101 Standard query 0x0000 A BRW38B1DB2DF75E.local, "QM" question
   16 5.013034    10.0.0.79               224.0.0.251      MDNS       81 Standard query 0x0000 AAAA BRW38B1DB2DF75E.local, "QM" question
```

```
> Frame 2: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
> Ethernet II, Src: Espressi_b0:6f:04 (c4:4f:33:b0:6f:04), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.0.0.80, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 49154, Dst Port: 6667
> Data (172 bytes)
```

```
0000  ff ff ff ff ff ff c4 4f  33 b0 6f 04 08 00 45 00   ·······O 3·o···E·
0010  00 c8 32 4b 00 00 ff 11  7e 8a 0a 00 00 50 ff ff   ··2K···· ~····P··
0020  ff ff c0 02 1a 0b 00 b4  9c a1 00 00 55 aa 00 00   ········ ····U···
0030  00 00 00 00 00 13 00 00  00 9c 00 00 00 00 1e da   ········ ········
0040  12 20 2d 8c 3c c6 77 bf  39 80 d2 d9 c2 85 4f 3f   · -·<·w· 9·····O?
0050  c8 89 9a 83 bf ad d8 35  3c 1d 0f 95 05 27 15 59   ·······5 <····'·Y
0060  8f 91 fd e2 87 55 bb 2e  b4 53 9d 51 4b 92 65 d9   ·····U·. ·S·QK·e·
0070  5f 41 6c 4c 51 6c 72 7d  e9 b4 9d e2 98 26 a6 61   _AlLQlr} ·····&·a
0080  d1 79 70 c8 69 17 14 26  b5 1d 68 e6 4d 80 bb 2d   ·yp·i··& ··h·M··-
0090  92 9f db 09 88 90 5a 30  ac 05 50 7c 86 de c1 b7   ······Z0 ··P|····
00a0  da 08 02 7b a9 db 73 99  a4 26 e3 6b 8d 30 a7 8b   ···{··s· ·&·k·0··
00b0  3a db 00 70 f9 8a e3 0a  14 84 73 ab bb 9a b8 1a   :··p···· ··s·····
00c0  9e 2e e4 b9 8c 61 27 7a  c0 de 50 40 cd bd 60 da   ·.···a'z ··P@··`·
00d0  05 ab 00 00 aa 55                                  ·····U
```

User Datagram Protocol: Protocol | Packets: 1035 · Displayed: 513 (49.6%) · Dropped: 0 (0.0%) | Profile: Default



```
udp.port == 54915
```

```
No.  Time        Source           Destination      Protocol  Info
 72  25.878055   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 74  26.799481   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 75  27.823472   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 79  28.822561   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 80  29.871220   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 81  30.792706   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 83  31.756637   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 85  32.816042   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 86  33.864355   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 87  34.785751   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 88  35.809445   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 90  36.810570   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 92  37.833844   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
 95  39.779401   192.168.156.83   192.168.157.255  UDP       54915 → 54915 Len=263
```

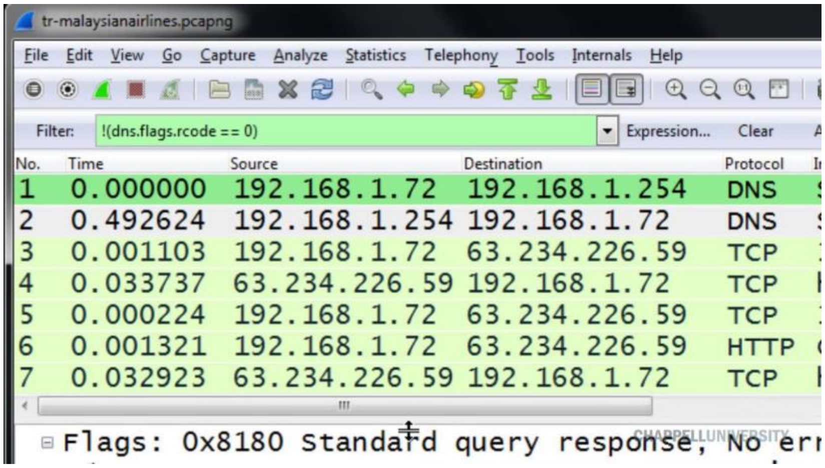
```
▶ Frame 95: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0
▼ Ethernet II, Src: Apple_c0:42:47 (f4:5c:89:c0:42:47), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Apple_c0:42:47 (f4:5c:89:c0:42:47)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 128.154.156.83, Dst: 128.154.157.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 291
    Identification: 0xe11c (57628)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x5d26 [validation disabled]
    [Header checksum status: Unverified]
```

```
0070  00 00 06 00 00 00 00 00  00 00 b0 56 3a 00 00 70   ........ ...V:..p
0080  00 00 5f 2c aa 9d ff 7f  00 00 00 fa ba 07 01 00   .._,.... ........
0090  00 00 00 00 00 00 00 00  00 00 00 70 5a 06 01 00   ........ ...pZ...
00a0  00 00 00 fa ba 07 01 00  00 00 03 58 05 7b 38 35   ........ ...X.{85
00b0  36 30 36 64 34 37 2d 34  30 31 61 2d 34 35 37 35   606d47-4 01a-4575
00c0  2d 61 37 66 61 2d 31 30  64 33 38 30 66 34 33 31   -a7fa-10 d380f431
00d0  33 64 7d 00 00 00 00 00  00 00 00 00 00 00 00 00   3d}..... ........
00e0  00 00 00 00 00 00 00 00  00 00 e7 b8 9b 07 01 00   ........ ........
```

Source Hardware Address (eth.src), 6 bytes | Packets: 2214 · Displayed: 425 (19.2%) · Dropped: 0 (0.0%) | Profile: Default

13. dns.flags.rcode != 0

    Indicates which dns requests couldn't be correctly resolved.

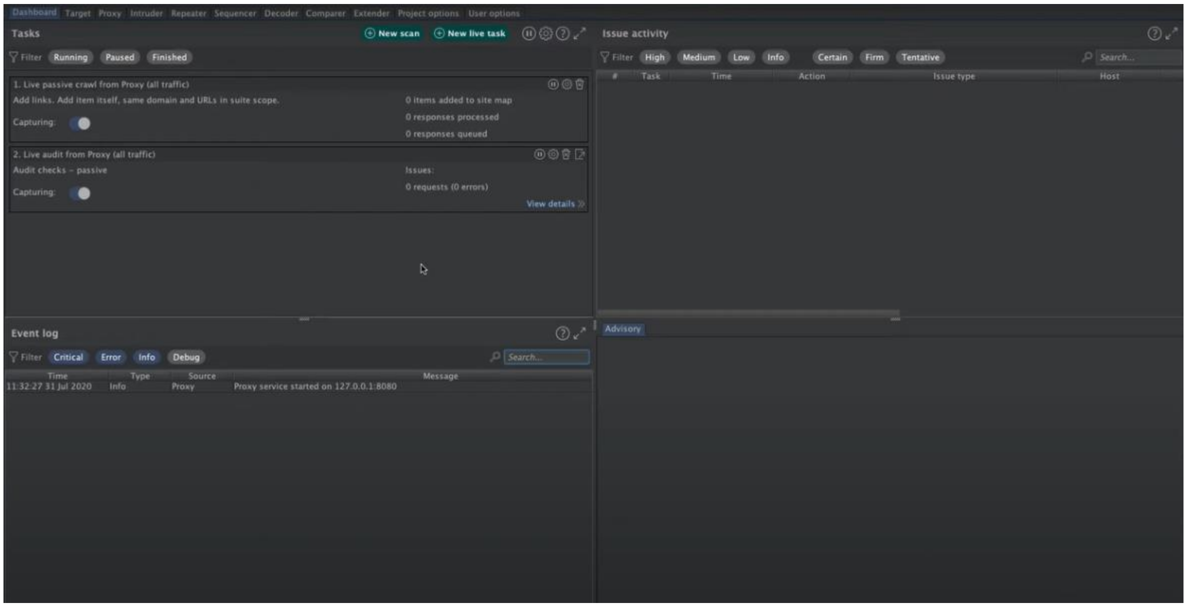

tr-malaysianairlines.pcapng
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression...
Clear

```
Filter: !(dns.flags.rcode == 0)
```

```
No. Time      Source         Destination    Protocol
1   0.000000  192.168.1.72   192.168.1.254  DNS
2   0.492624  192.168.1.254  192.168.1.72   DNS
3   0.001103  192.168.1.72   63.234.226.59  TCP
4   0.033737  63.234.226.59  192.168.1.72   TCP
5   0.000224  192.168.1.72   63.234.226.59  TCP
6   0.001321  192.168.1.72   63.234.226.59  HTTP
7   0.032923  63.234.226.59  192.168.1.72   TCP
```

```
⊟ Flags: 0x8180 Standard query response, No err
```

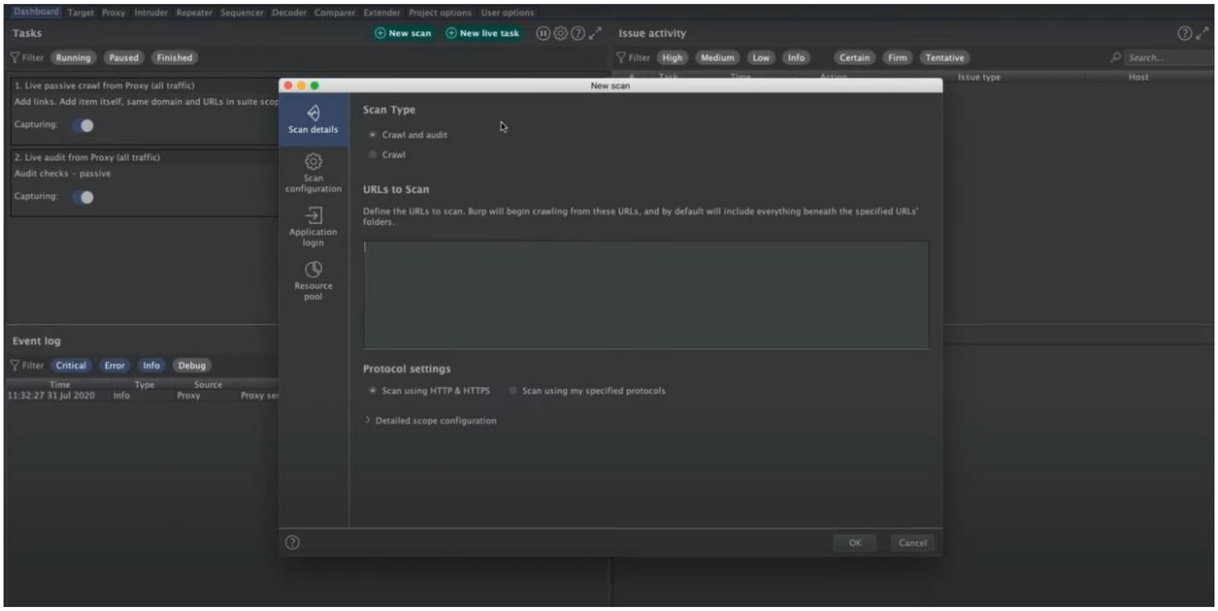
Burp Suite



1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
0 items added to site map
0 responses processed
0 responses queued

2. Live audit from Proxy (all traffic)
Audit checks – passive
Capturing:
Issues:
0 requests (0 errors)

```
Time                  Type   Source   Message
11:32:27 31 Jul 2020  Info   Proxy    Proxy service started on 127.0.0.1:8080
```



Scan Type

● Crawl and audit
○ Crawl

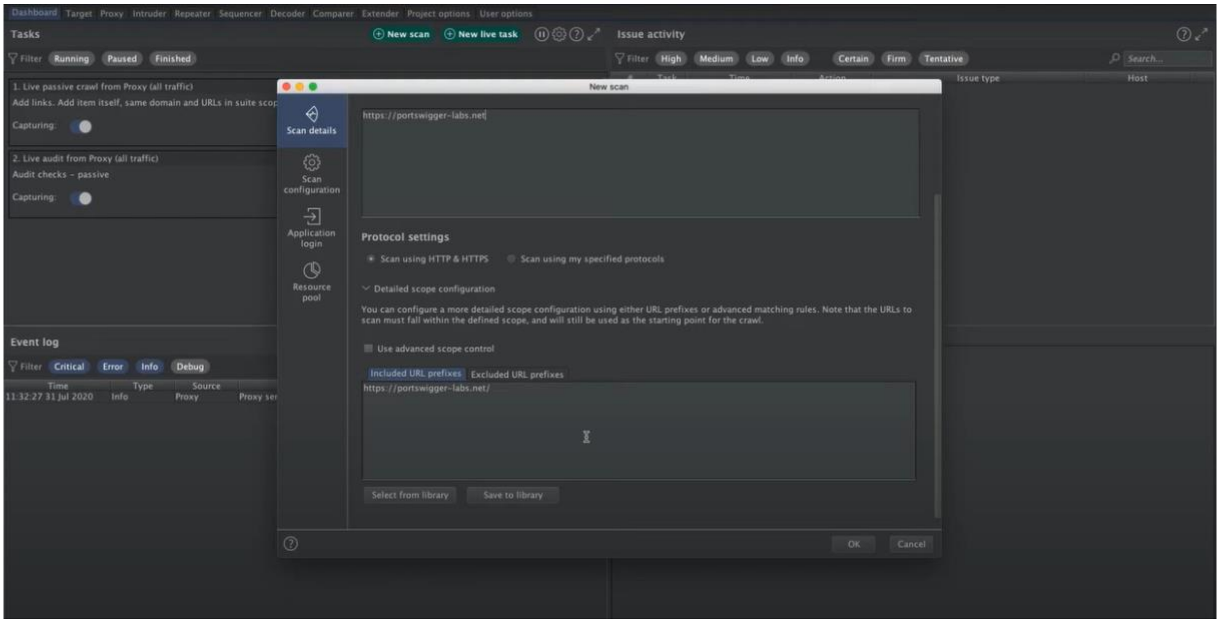
URLs to Scan

Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs' folders.

Protocol settings

● Scan using HTTP & HTTPS ○ Scan using my specified protocols

› Detailed scope configuration



https://portswigger-labs.net

Protocol settings

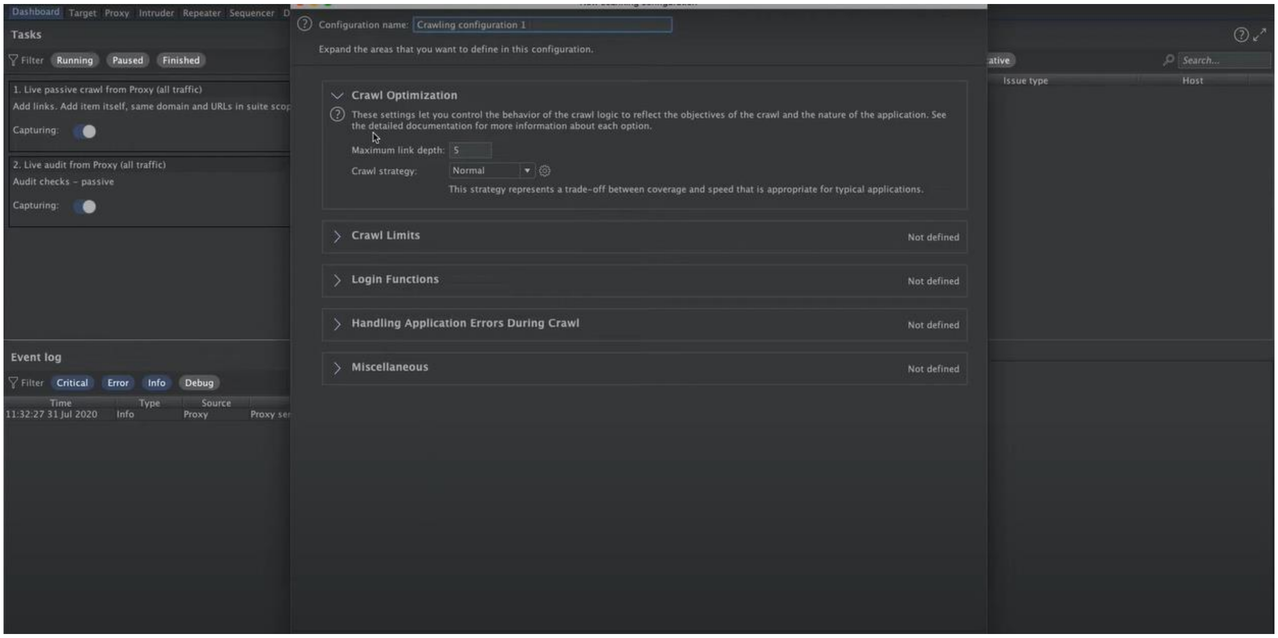
● Scan using HTTP & HTTPS ○ Scan using my specified protocols

⌄ Detailed scope configuration

You can configure a more detailed scope configuration using either URL prefixes or advanced matching rules. Note that the URLs to scan must fall within the defined scope, and will still be used as the starting point for the crawl.

□ Use advanced scope control

https://portswigger-labs.net/



1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scop
Capturing:

2. Live audit from Proxy (all traffic)
Audit checks – passive
Capturing:

Time	Type	Source	
11:32:27 31 Jul 2020	Info	Proxy	Proxy ser

Configuration name: Crawling configuration 1

Expand the areas that you want to define in this configuration.

Crawl Optimization

These settings let you control the behavior of the crawl logic to reflect the objectives of the crawl and the nature of the application. See the detailed documentation for more information about each option.

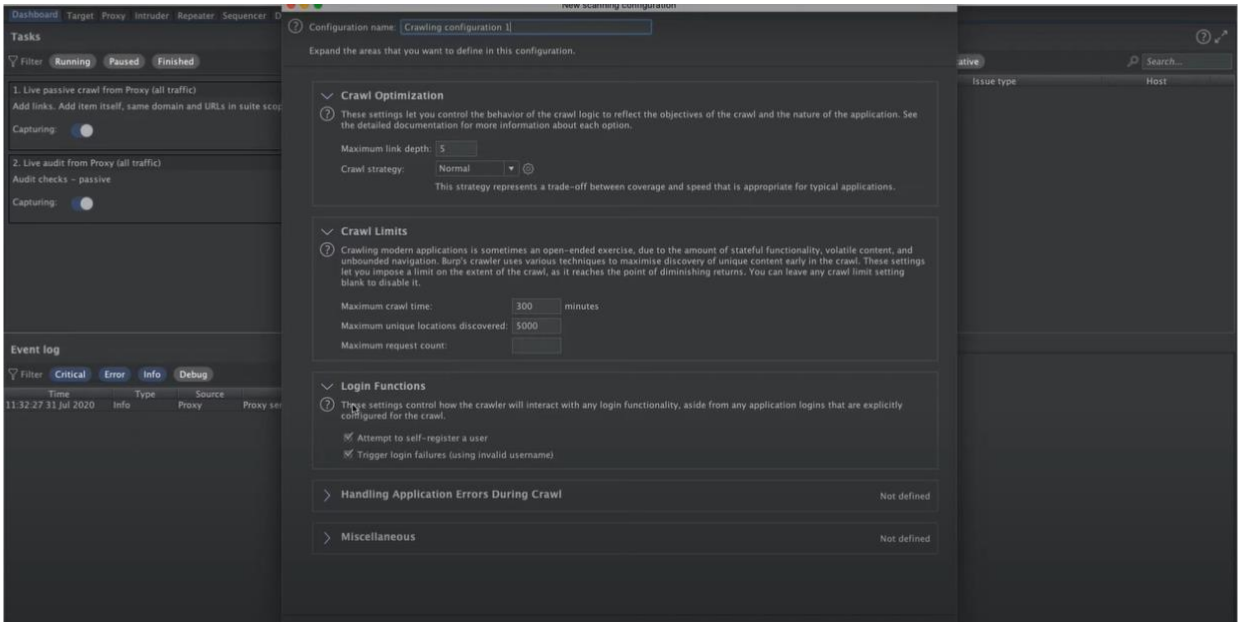
Maximum link depth: 5
Crawl strategy: Normal
This strategy represents a trade-off between coverage and speed that is appropriate for typical applications.

Crawl Limits Not defined

Login Functions Not defined

Handling Application Errors During Crawl Not defined

Miscellaneous Not defined



1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scop
Capturing:

2. Live audit from Proxy (all traffic)
Audit checks – passive
Capturing:

Time	Type	Source	
11:32:27 31 Jul 2020	Info	Proxy	Proxy ser

Configuration name: Crawling configuration 1

Expand the areas that you want to define in this configuration.

Crawl Optimization

These settings let you control the behavior of the crawl logic to reflect the objectives of the crawl and the nature of the application. See the detailed documentation for more information about each option.

Maximum link depth: 5
Crawl strategy: Normal
This strategy represents a trade-off between coverage and speed that is appropriate for typical applications.

Crawl Limits

Crawling modern applications is sometimes an open-ended exercise, due to the amount of stateful functionality, volatile content, and unbounded navigation. Burp's crawler uses various techniques to maximise discovery of unique content early in the crawl. These settings let you impose a limit on the extent of the crawl, as it reaches the point of diminishing returns. You can leave any crawl limit setting blank to disable it.

Maximum crawl time: 300 minutes
Maximum unique locations discovered: 5000
Maximum request count:

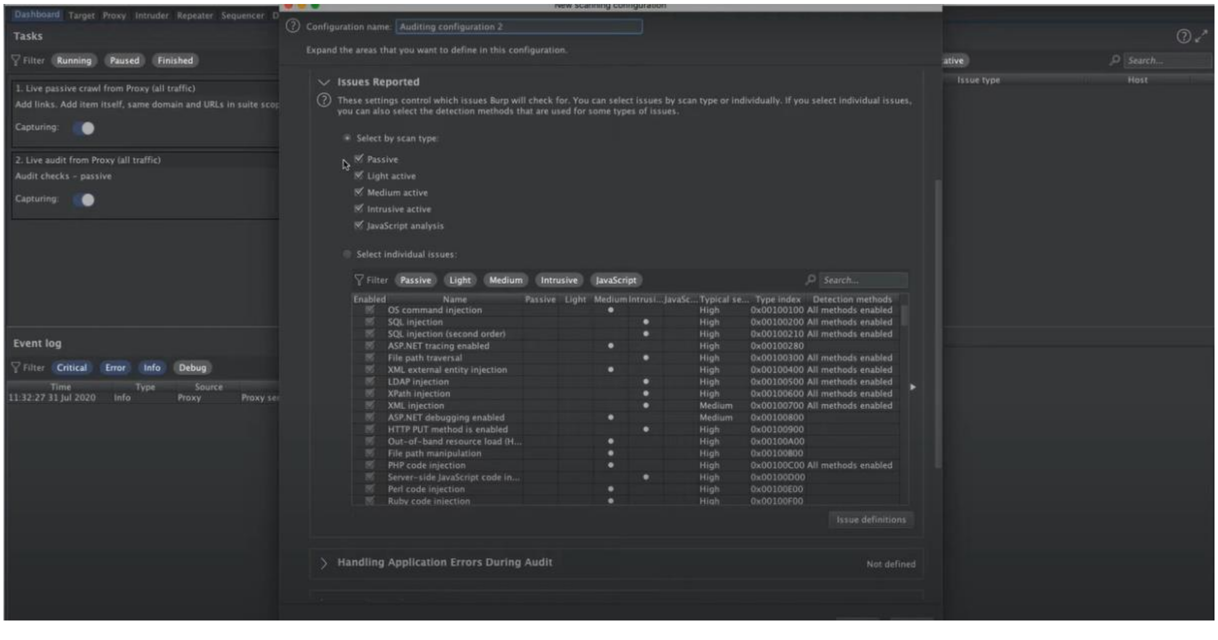
Login Functions

These settings control how the crawler will interact with any login functionality, aside from any application logins that are explicitly configured for the crawl.

☑ Attempt to self-register a user
☑ Trigger login failures (using invalid username)

Handling Application Errors During Crawl Not defined

Miscellaneous Not defined



1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scop
Capturing:

2. Live audit from Proxy (all traffic)
Audit checks – passive
Capturing:

Time	Type	Source	
11:32:27 31 Jul 2020	Info	Proxy	Proxy ser

Configuration name: Auditing configuration 2

Expand the areas that you want to define in this configuration.

Issues Reported

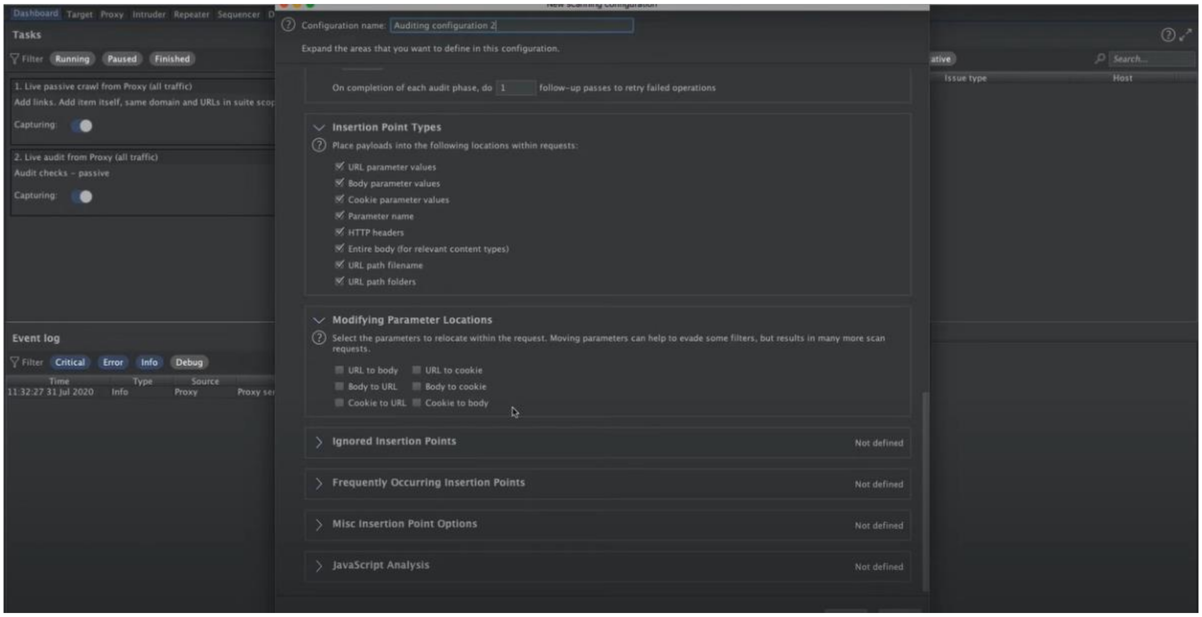
These settings control which issues Burp will check for. You can select issues by scan type or individually. If you select individual issues, you can also select the detection methods that are used for some types of issues.

● Select by scan type:
☑ Passive
☑ Light active
☑ Medium active
☑ Intrusive active
☑ JavaScript analysis

○ Select individual issues:

Enabled	Name	Passive	Light	Medium	Intrusi...	JavaSc...	Typical se...	Type index	Detection methods
☑	OS command injection			●			High	0x00100100	All methods enabled
☑	SQL injection				●		High	0x00100200	All methods enabled
☑	SQL injection (second order)				●		High	0x00100210	All methods enabled
☑	ASP.NET tracing enabled			●			High	0x00100280	
☑	File path traversal				●		High	0x00100300	All methods enabled
☑	XML external entity injection			●			High	0x00100400	All methods enabled
☑	LDAP injection				●		High	0x00100500	All methods enabled
☑	XPath injection				●		High	0x00100600	All methods enabled
☑	XML injection				●		Medium	0x00100700	All methods enabled
☑	ASP.NET debugging enabled			●			Medium	0x00100800	
☑	HTTP PUT method is enabled				●		High	0x00100900	
☑	Out-of-band resource load (H...			●			High	0x00100A00	
☑	File path manipulation			●			High	0x00100B00	
☑	PHP code injection			●			High	0x00100C00	All methods enabled
☑	Server-side JavaScript code in...				●		High	0x00100D00	
☑	Perl code injection			●			High	0x00100E00	
☑	Ruby code injection			●			High	0x00100F00	

Handling Application Errors During Audit Not defined



1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scop
Capturing:

2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:

Time	Type	Source	
11:32:27 31 Jul 2020	Info	Proxy	Proxy se

Configuration name: Auditing configuration 2

Expand the areas that you want to define in this configuration.

On completion of each audit phase, do 1 follow-up passes to retry failed operations

Insertion Point Types

Place payloads into the following locations within requests:

- ☑ URL parameter values
- ☑ Body parameter values
- ☑ Cookie parameter values
- ☑ Parameter name
- ☑ HTTP headers
- ☑ Entire body (for relevant content types)
- ☑ URL path filename
- ☑ URL path folders

Modifying Parameter Locations

Select the parameters to relocate within the request. Moving parameters can help to evade some filters, but results in many more scan requests.

□ URL to body □ URL to cookie
□ Body to URL □ Body to cookie
□ Cookie to URL □ Cookie to body

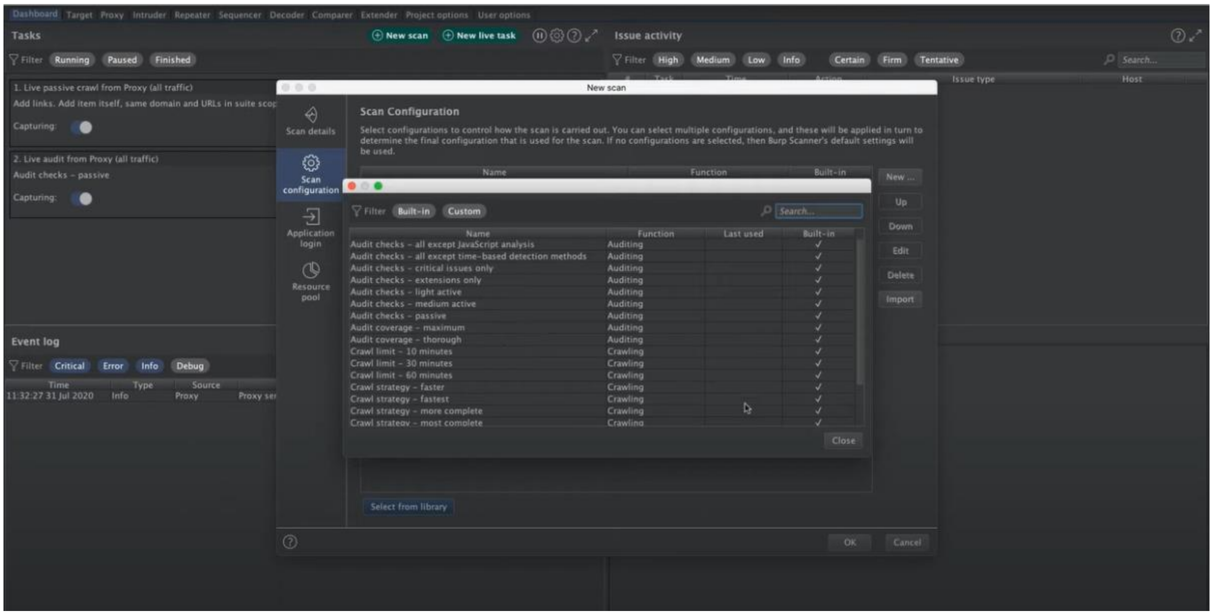
Ignored Insertion Points Not defined

Frequently Occurring Insertion Points Not defined

Misc Insertion Point Options Not defined

JavaScript Analysis Not defined

Scanning and Time checking:-

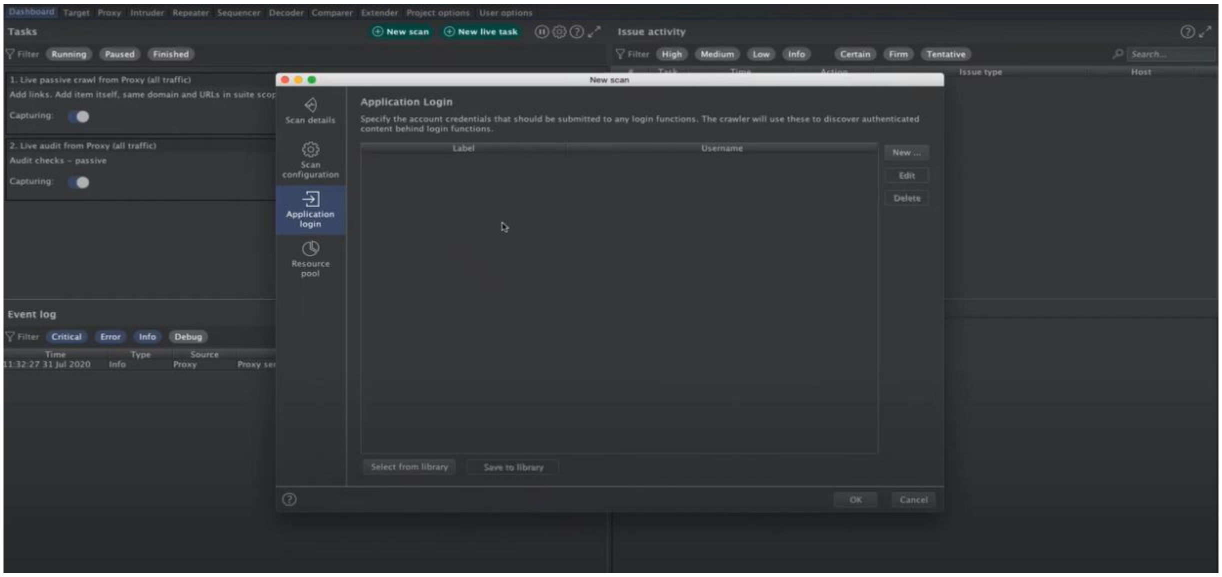


New scan

Scan Configuration

Select configurations to control how the scan is carried out. You can select multiple configurations, and these will be applied in turn to determine the final configuration that is used for the scan. If no configurations are selected, then Burp Scanner's default settings will be used.

Name	Function	Last used	Built-in
Audit checks - all except JavaScript analysis	Auditing		✓
Audit checks - all except time-based detection methods	Auditing		✓
Audit checks - critical issues only	Auditing		✓
Audit checks - extensions only	Auditing		✓
Audit checks - light active	Auditing		✓
Audit checks - medium active	Auditing		✓
Audit checks - passive	Auditing		✓
Audit coverage - maximum	Auditing		✓
Audit coverage - thorough	Auditing		✓
Crawl limit - 10 minutes	Crawling		✓
Crawl limit - 30 minutes	Crawling		✓
Crawl limit - 60 minutes	Crawling		✓
Crawl strategy - faster	Crawling		✓
Crawl strategy - fastest	Crawling		✓
Crawl strategy - more complete	Crawling		✓
Crawl strategy - most complete	Crawling		✓

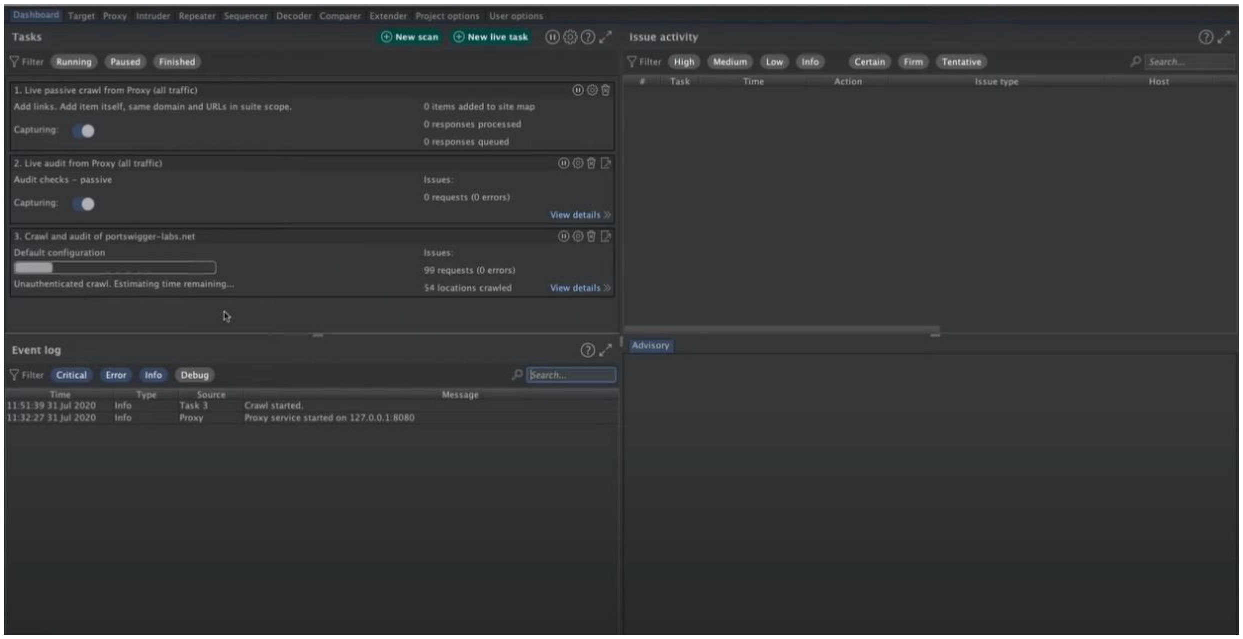


New scan

Application Login

Specify the account credentials that should be submitted to any login functions. The crawler will use these to discover authenticated content behind login functions.

Label	Username



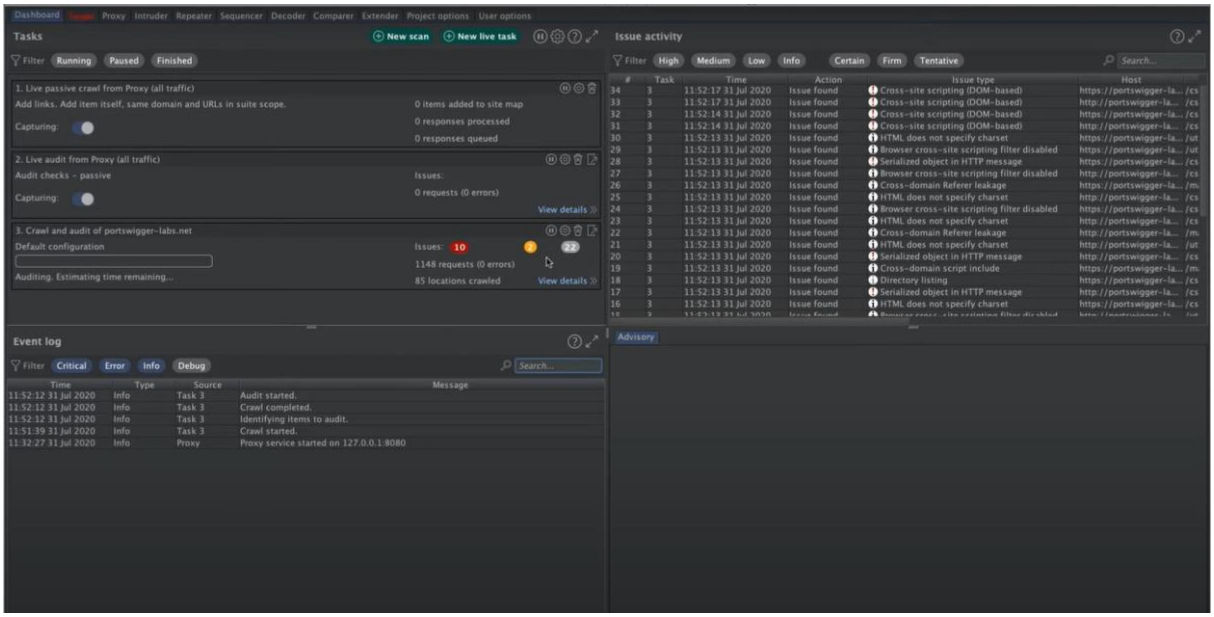
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
0 items added to site map
0 responses processed
0 responses queued

2. Live audit from Proxy (all traffic)
Audit checks – passive
Capturing:
Issues:
0 requests (0 errors)
View details »

3. Crawl and audit of portswigger-labs.net
Default configuration
Unauthenticated crawl. Estimating time remaining...
Issues:
99 requests (0 errors)
54 locations crawled
View details »

#	Task	Time	Action	Issue type	Host

```
Time                  Type   Source   Message
11:51:39 31 Jul 2020  Info   Task 3   Crawl started.
11:32:27 31 Jul 2020  Info   Proxy    Proxy service started on 127.0.0.1:8080
```



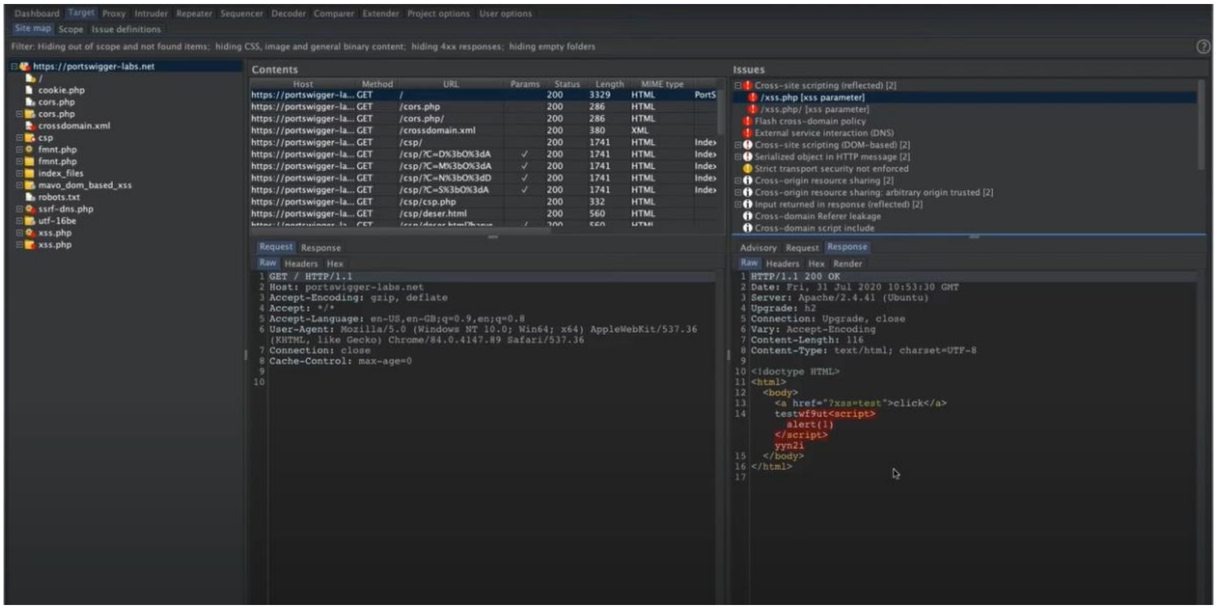
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
0 items added to site map
0 responses processed
0 responses queued

2. Live audit from Proxy (all traffic)
Audit checks – passive
Capturing:
Issues:
0 requests (0 errors)
View details »

3. Crawl and audit of portswigger-labs.net
Default configuration
Auditing. Estimating time remaining...
Issues: 10 2 22
1148 requests (0 errors)
85 locations crawled
View details »

#	Task	Time	Action	Issue type	Host
34	3	11:52:17 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	https://portswigger-la... /cs
33	3	11:52:17 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	http://portswigger-la... /cs
32	3	11:52:14 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	https://portswigger-la... /cs
31	3	11:52:14 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	http://portswigger-la... /cs
30	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	https://portswigger-la... /ut
29	3	11:52:13 31 Jul 2020	Issue found	Browser cross-site scripting filter disabled	https://portswigger-la... /ut
28	3	11:52:13 31 Jul 2020	Issue found	Serialized object in HTTP message	https://portswigger-la... /cs
27	3	11:52:13 31 Jul 2020	Issue found	Browser cross-site scripting filter disabled	http://portswigger-la... /cs
26	3	11:52:13 31 Jul 2020	Issue found	Cross-domain Referer leakage	https://portswigger-la... /m
25	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	http://portswigger-la... /cs
24	3	11:52:13 31 Jul 2020	Issue found	Browser cross-site scripting filter disabled	https://portswigger-la... /cs
23	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	http://portswigger-la... /cs
22	3	11:52:13 31 Jul 2020	Issue found	Cross-domain Referer leakage	http://portswigger-la... /m
21	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	http://portswigger-la... /ut
20	3	11:52:13 31 Jul 2020	Issue found	Serialized object in HTTP message	http://portswigger-la... /cs
19	3	11:52:13 31 Jul 2020	Issue found	Cross-domain script include	https://portswigger-la... /m
18	3	11:52:13 31 Jul 2020	Issue found	Directory listing	https://portswigger-la... /cs
17	3	11:52:13 31 Jul 2020	Issue found	Serialized object in HTTP message	http://portswigger-la... /cs
16	3	11:52:13 31 Jul 2020	Issue found	HTML does not specify charset	https://portswigger-la... /cs

```
Time                  Type   Source   Message
11:52:12 31 Jul 2020  Info   Task 3   Audit started.
11:52:12 31 Jul 2020  Info   Task 3   Crawl completed.
11:52:12 31 Jul 2020  Info   Task 3   Identifying items to audit.
11:51:39 31 Jul 2020  Info   Task 3   Crawl started.
11:32:27 31 Jul 2020  Info   Proxy    Proxy service started on 127.0.0.1:8080
```



Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

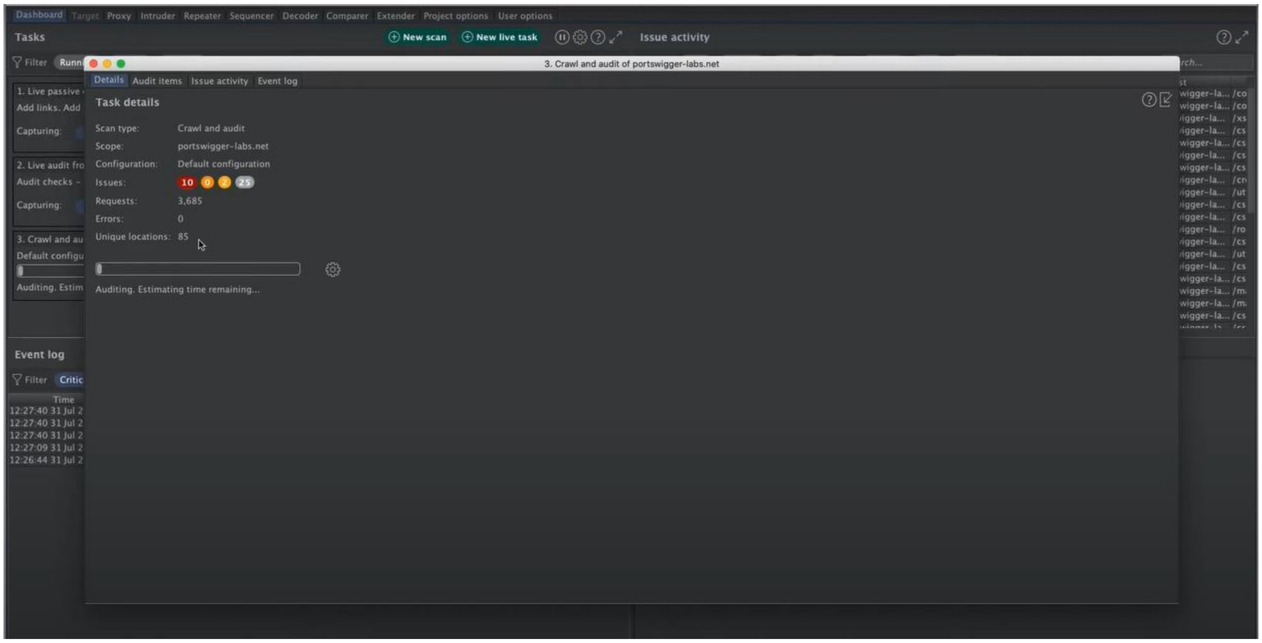
- https://portswigger-labs.net
  - /
  - cookie.php
  - cors.php
  - cors.php
  - crossdomain.xml
  - csp
  - fmnt.php
  - fmnt.php
  - index_files
  - mavo_dom_based_xss
  - robots.txt
  - ssrf-dns.php
  - utf-16be
  - xss.php
  - xss.php

Host	Method	URL	Params	Status	Length	MIME type	
https://portswigger-la...	GET	/		200	3329	HTML	PortS
https://portswigger-la...	GET	/cors.php		200	286	HTML	
https://portswigger-la...	GET	/cors.php/		200	286	HTML	
https://portswigger-la...	GET	/crossdomain.xml		200	380	XML	
https://portswigger-la...	GET	/csp/		200	1741	HTML	Inde›
https://portswigger-la...	GET	/csp/?C=D%3bO%3dA	✓	200	1741	HTML	Inde›
https://portswigger-la...	GET	/csp/?C=M%3bO%3dA	✓	200	1741	HTML	Inde›
https://portswigger-la...	GET	/csp/?C=N%3bO%3dD	✓	200	1741	HTML	Inde›
https://portswigger-la...	GET	/csp/?C=S%3bO%3dA	✓	200	1741	HTML	Inde›
https://portswigger-la...	GET	/csp/csp.php		200	332	HTML	
https://portswigger-la...	GET	/csp/deser.html		200	560	HTML	

- Cross-site scripting (reflected) [2]
  - /xss.php [xss parameter]
  - /xss.php/ [xss parameter]
- Flash cross-domain policy
- External service interaction (DNS)
- Cross-site scripting (DOM-based) [2]
- Serialized object in HTTP message [2]
- Strict transport security not enforced
- Cross-origin resource sharing [2]
- Cross-origin resource sharing: arbitrary origin trusted [2]
- Input returned in response (reflected) [2]
- Cross-domain Referer leakage
- Cross-domain script include

```
GET / HTTP/1.1
Host: portswigger-labs.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
Connection: close
Cache-Control: max-age=0


```

```
HTTP/1.1 200 OK
Date: Fri, 31 Jul 2020 10:53:30 GMT
Server: Apache/2.4.41 (Ubuntu)
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Length: 116
Content-Type: text/html; charset=UTF-8

<!doctype HTML>
<html>
  <body>
    <a href="?xss=test">click</a>
    testwf9ut<script>
      alert(1)
    </script>
    yyn2i
  </body>
</html>

```

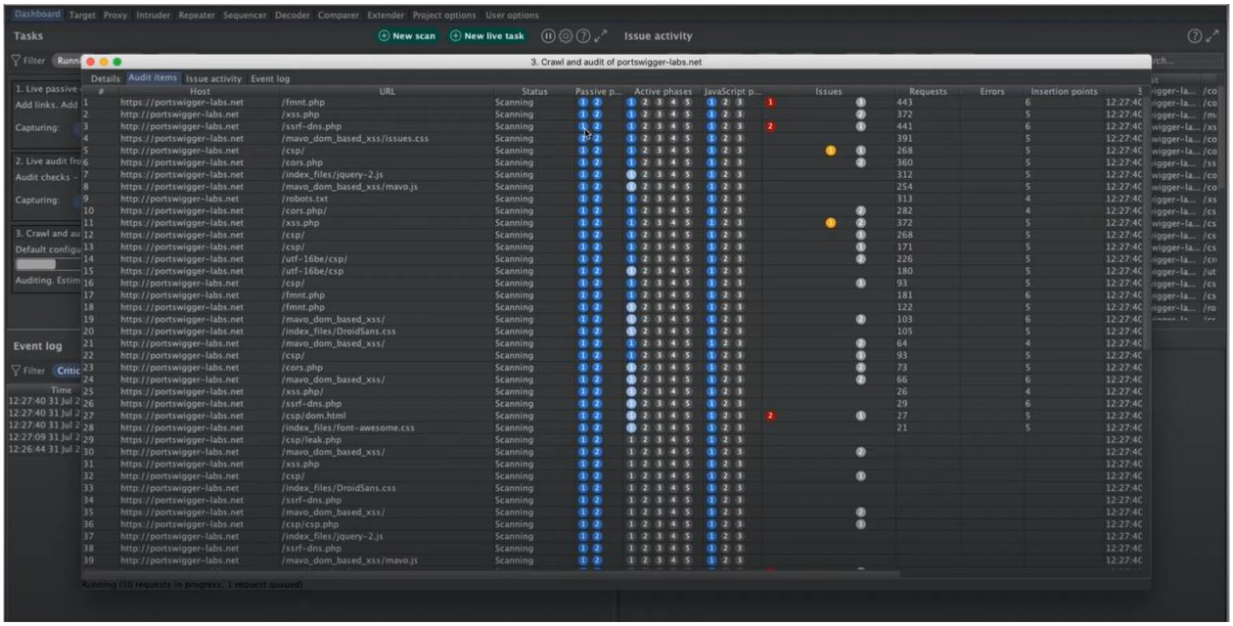


3. Crawl and audit of portswigger-labs.net

Task details

Scan type: Crawl and audit
Scope: portswigger-labs.net
Configuration: Default configuration
Issues: 10 0 2 25
Requests: 3,685
Errors: 0
Unique locations: 85

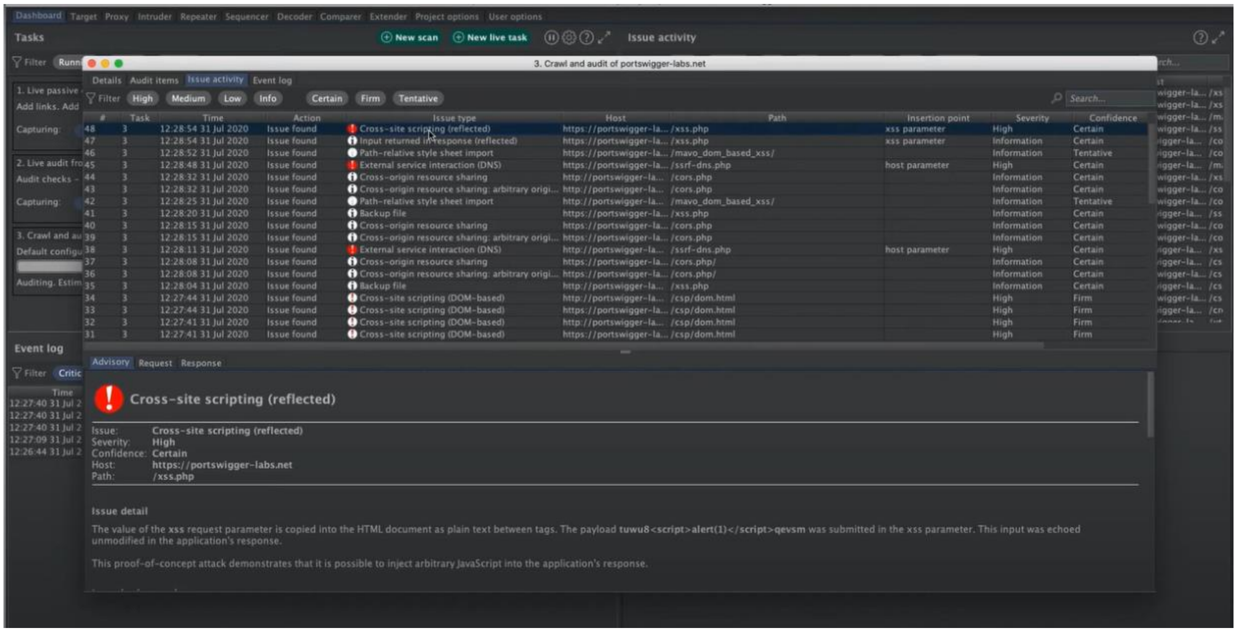
Auditing. Estimating time remaining...



3. Crawl and audit of portswigger-labs.net

#	Host	URL	Status	Passive p...	Active phases	JavaScript p...	Issues	Requests	Errors	Insertion points	S
1	https://portswigger-labs.net	/fmnt.php	Scanning	1 2	1 2 3 4 5	1 2 3	1 1	443		6	12:27:4C
2	http://portswigger-labs.net	/xss.php	Scanning	1 2	1 2 3 4 5	1 2 3	2	372		5	12:27:4C
3	http://portswigger-labs.net	/ssrf-dns.php	Scanning	1 2	1 2 3 4 5	1 2 3	2 1	441		6	12:27:4C
4	https://portswigger-labs.net	/mavo_dom_based_xss/issues.css	Scanning	1 2	1 2 3 4 5	1 2 3		391		5	12:27:4C
5	http://portswigger-labs.net	/csp/	Scanning	1 2	1 2 3 4 5	1 2 3	1 1	268		5	12:27:4C
6	https://portswigger-labs.net	/cors.php	Scanning	1 2	1 2 3 4 5	1 2 3	2	360		5	12:27:4C
7	https://portswigger-labs.net	/index_files/jquery-2.js	Scanning	1 2	1 2 3 4 5	1 2 3		312		5	12:27:4C
8	https://portswigger-labs.net	/mavo_dom_based_xss/mavo.js	Scanning	1 2	1 2 3 4 5	1 2 3		254		5	12:27:4C
9	http://portswigger-labs.net	/robots.txt	Scanning	1 2	1 2 3 4 5	1 2 3		313		4	12:27:4C
10	https://portswigger-labs.net	/cors.php/	Scanning	1 2	1 2 3 4 5	1 2 3	2	282		4	12:27:4C
11	https://portswigger-labs.net	/xss.php	Scanning	1 2	1 2 3 4 5	1 2 3	1 2	372		5	12:27:4C
12	https://portswigger-labs.net	/csp/	Scanning	1 2	1 2 3 4 5	1 2 3	1	268		5	12:27:4C
13	https://portswigger-labs.net	/csp/	Scanning	1 2	1 2 3 4 5	1 2 3	1	171		5	12:27:4C
14	https://portswigger-labs.net	/utf-16be/csp/	Scanning	1 2	1 2 3 4 5	1 2 3	2	226		5	12:27:4C
15	https://portswigger-labs.net	/utf-16be/csp	Scanning	1 2	1 2 3 4 5	1 2 3		180		5	12:27:4C
16	http://portswigger-labs.net	/csp/	Scanning	1 2	1 2 3 4 5	1 2 3	1	93		5	12:27:4C
17	http://portswigger-labs.net	/fmnt.php	Scanning	1 2	1 2 3 4 5	1 2 3		181		6	12:27:4C
18	https://portswigger-labs.net	/fmnt.php	Scanning	1 2	1 2 3 4 5	1 2 3		122		5	12:27:4C
19	https://portswigger-labs.net	/mavo_dom_based_xss/	Scanning	1 2	1 2 3 4 5	1 2 3	2	103		6	12:27:4C
20	https://portswigger-labs.net	/index_files/DroidSans.css	Scanning	1 2	1 2 3 4 5	1 2 3		105		5	12:27:4C
21	http://portswigger-labs.net	/mavo_dom_based_xss/	Scanning	1 2	1 2 3 4 5	1 2 3	2	64		4	12:27:4C
22	http://portswigger-labs.net	/csp/	Scanning	1 2	1 2 3 4 5	1 2 3	1	93		5	12:27:4C
23	http://portswigger-labs.net	/cors.php	Scanning	1 2	1 2 3 4 5	1 2 3	2	73		5	12:27:4C
24	http://portswigger-labs.net	/mavo_dom_based_xss/	Scanning	1 2	1 2 3 4 5	1 2 3	2	66		6	12:27:4C
25	https://portswigger-labs.net	/xss.php/	Scanning	1 2	1 2 3 4 5	1 2 3		26		4	12:27:4C
26	https://portswigger-labs.net	/ssrf-dns.php	Scanning	1 2	1 2 3 4 5	1 2 3		29		6	12:27:4C
27	https://portswigger-labs.net	/csp/dom.html	Scanning	1 2	1 2 3 4 5	1 2 3	2 1	27		5	12:27:4C
28	https://portswigger-labs.net	/index_files/font-awesome.css	Scanning	1 2	1 2 3 4 5	1 2 3		21		5	12:27:4C
29	https://portswigger-labs.net	/csp/leak.php	Scanning	1 2	1 2 3 4 5	1 2 3					12:27:4C
30	http://portswigger-labs.net	/mavo_dom_based_xss/	Scanning	1 2	1 2 3 4 5	1 2 3	2				12:27:4C
31	https://portswigger-labs.net	/xss.php	Scanning	1 2	1 2 3 4 5	1 2 3					12:27:4C
32	http://portswigger-labs.net	/csp/	Scanning	1 2	1 2 3 4 5	1 2 3	1				12:27:4C
33	http://portswigger-labs.net	/index_files/DroidSans.css	Scanning	1 2	1 2 3 4 5	1 2 3					12:27:4C
34	https://portswigger-labs.net	/ssrf-dns.php	Scanning	1 2	1 2 3 4 5	1 2 3					12:27:4C
35	https://portswigger-labs.net	/mavo_dom_based_xss/	Scanning	1 2	1 2 3 4 5	1 2 3	2				12:27:4C
36	https://portswigger-labs.net	/csp/csp.php	Scanning	1 2	1 2 3 4 5	1 2 3	1				12:27:4C
37	http://portswigger-labs.net	/index_files/jquery-2.js	Scanning	1 2	1 2 3 4 5	1 2 3					12:27:4C
38	http://portswigger-labs.net	/ssrf-dns.php	Scanning	1 2	1 2 3 4 5	1 2 3					12:27:4C
39	http://portswigger-labs.net	/mavo_dom_based_xss/mavo.js	Scanning	1 2	1 2 3 4 5	1 2 3					12:27:4C

Running (10 requests in progress, 1 request queued)



3. Crawl and audit of portswigger-labs.net

#	Task	Time	Action	Issue type	Host	Path	Insertion point	Severity	Confidence
48	3	12:28:54 31 Jul 2020	Issue found	Cross-site scripting (reflected)	https://portswigger-la...	/xss.php	xss parameter	High	Certain
47	3	12:28:54 31 Jul 2020	Issue found	Input returned in response (reflected)	https://portswigger-la...	/xss.php	xss parameter	Information	Certain
46	3	12:28:52 31 Jul 2020	Issue found	Path-relative style sheet import	https://portswigger-la...	/mavo_dom_based_xss/		Information	Tentative
45	3	12:28:48 31 Jul 2020	Issue found	External service interaction (DNS)	https://portswigger-la...	/ssrf-dns.php	host parameter	High	Certain
44	3	12:28:32 31 Jul 2020	Issue found	Cross-origin resource sharing	http://portswigger-la...	/cors.php		Information	Certain
43	3	12:28:32 31 Jul 2020	Issue found	Cross-origin resource sharing: arbitrary origi...	http://portswigger-la...	/cors.php		Information	Certain
42	3	12:28:25 31 Jul 2020	Issue found	Path-relative style sheet import	http://portswigger-la...	/mavo_dom_based_xss/		Information	Tentative
41	3	12:28:20 31 Jul 2020	Issue found	Backup file	https://portswigger-la...	/xss.php		Information	Certain
40	3	12:28:15 31 Jul 2020	Issue found	Cross-origin resource sharing	https://portswigger-la...	/cors.php		Information	Certain
39	3	12:28:15 31 Jul 2020	Issue found	Cross-origin resource sharing: arbitrary origi...	https://portswigger-la...	/cors.php		Information	Certain
38	3	12:28:11 31 Jul 2020	Issue found	External service interaction (DNS)	http://portswigger-la...	/ssrf-dns.php	host parameter	High	Certain
37	3	12:28:08 31 Jul 2020	Issue found	Cross-origin resource sharing	https://portswigger-la...	/cors.php/		Information	Certain
36	3	12:28:08 31 Jul 2020	Issue found	Cross-origin resource sharing: arbitrary origi...	https://portswigger-la...	/cors.php/		Information	Certain
35	3	12:28:04 31 Jul 2020	Issue found	Backup file	http://portswigger-la...	/xss.php		Information	Certain
34	3	12:27:44 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	http://portswigger-la...	/csp/dom.html		High	Firm
33	3	12:27:44 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	https://portswigger-la...	/csp/dom.html		High	Firm
32	3	12:27:41 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	http://portswigger-la...	/csp/dom.html		High	Firm
31	3	12:27:41 31 Jul 2020	Issue found	Cross-site scripting (DOM-based)	https://portswigger-la...	/csp/dom.html		High	Firm

Cross-site scripting (reflected)

Issue: Cross-site scripting (reflected)
Severity: High
Confidence: Certain
Host: https://portswigger-labs.net
Path: /xss.php

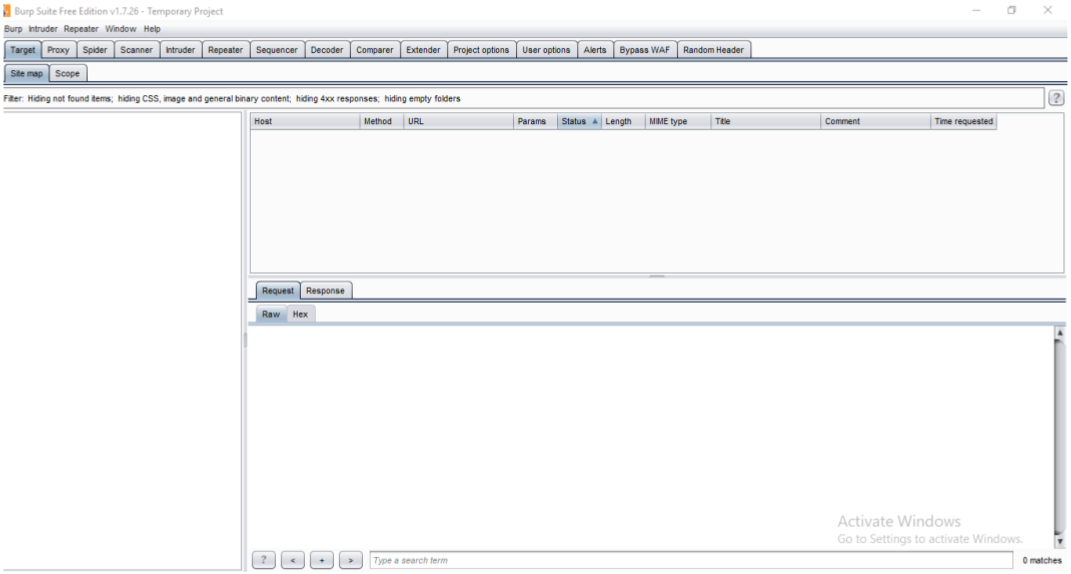
Issue detail

The value of the xss request parameter is copied into the HTML document as plain text between tags. The payload **tuwu8<script>alert(1)</script>qevsm** was submitted in the xss parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Burp Suite Tools

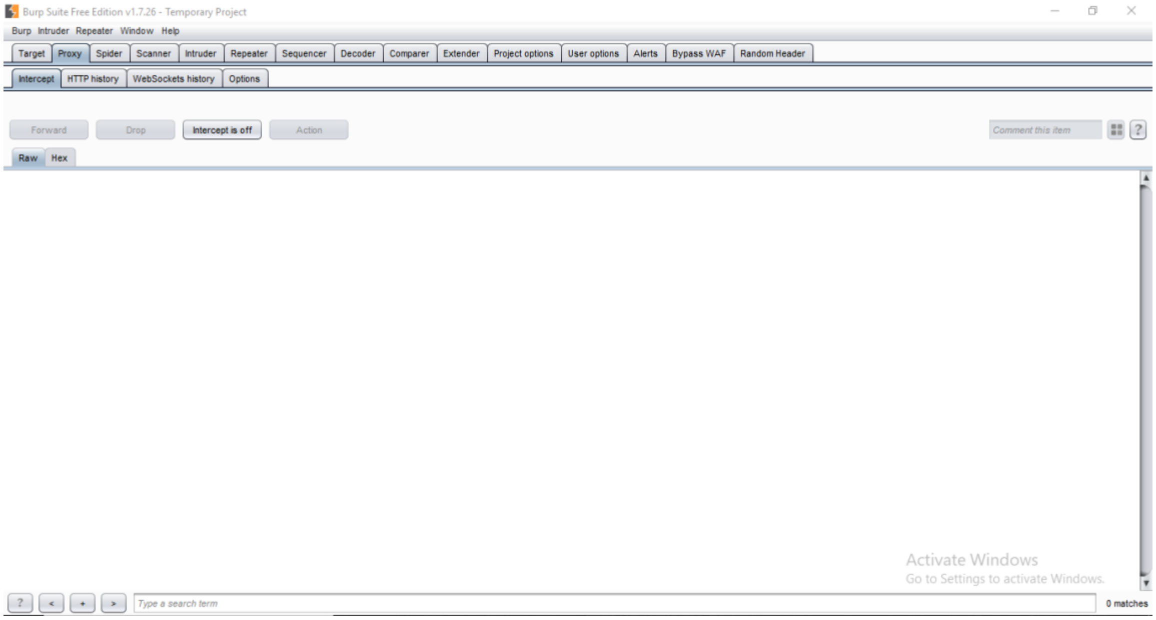
1. Spider:


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Site map Scope
Host Method URL Params Status Length MIME type Title Comment Time requested
Request Response
Raw Hex
Activate Windows
Go to Settings to activate Windows.
? < + >
Type a search term
0 matches

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

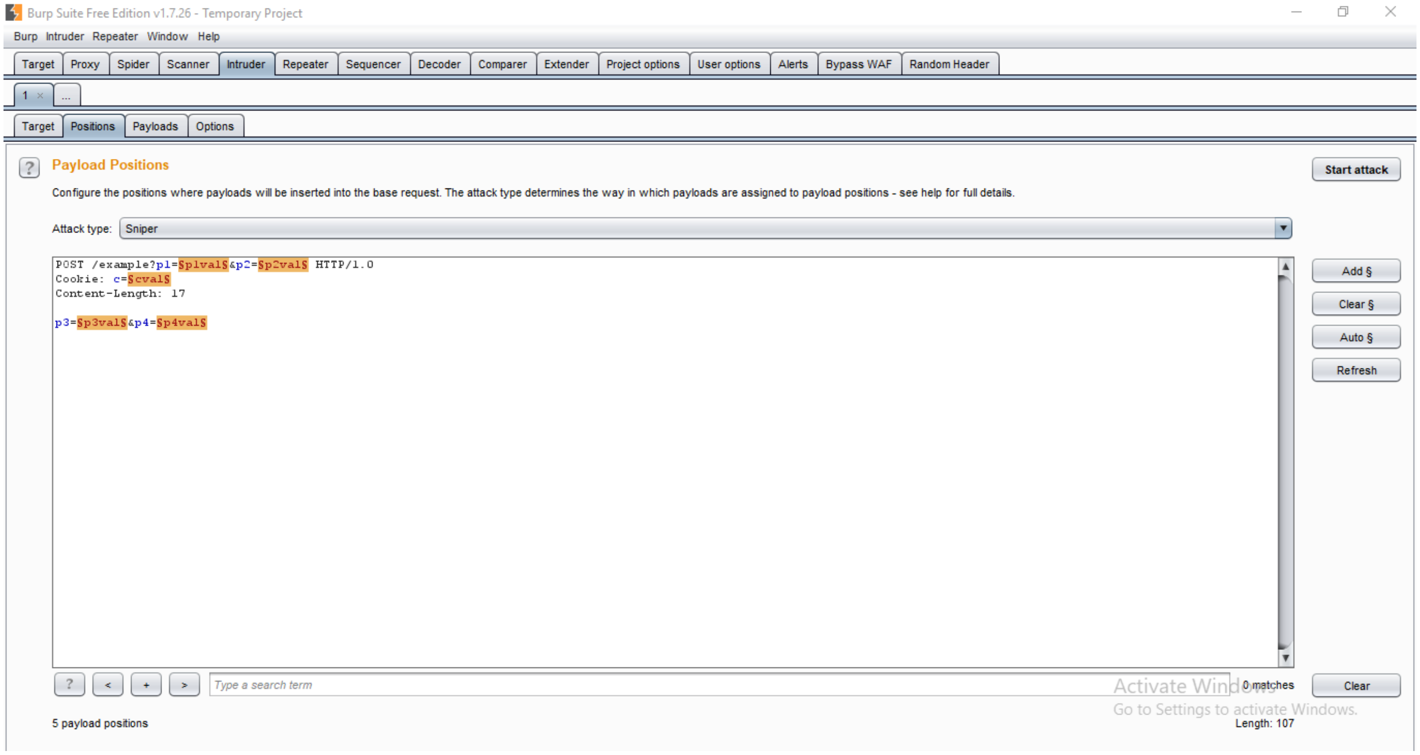
It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

2. Proxy:


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action
Comment this item
Raw Hex
Activate Windows
Go to Settings to activate Windows.
? < + >
Type a search term
0 matches

BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

3. Intruder:


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
1 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
Activate Windows
Go to Settings to activate Windows.

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /example?p1=§p1val§&p2=§p2val§ HTTP/1.0
Cookie: c=§cval§
Content-Length: 17

p3=§p3val§&p4=§p4val§
```

5 payload positions

Length: 107

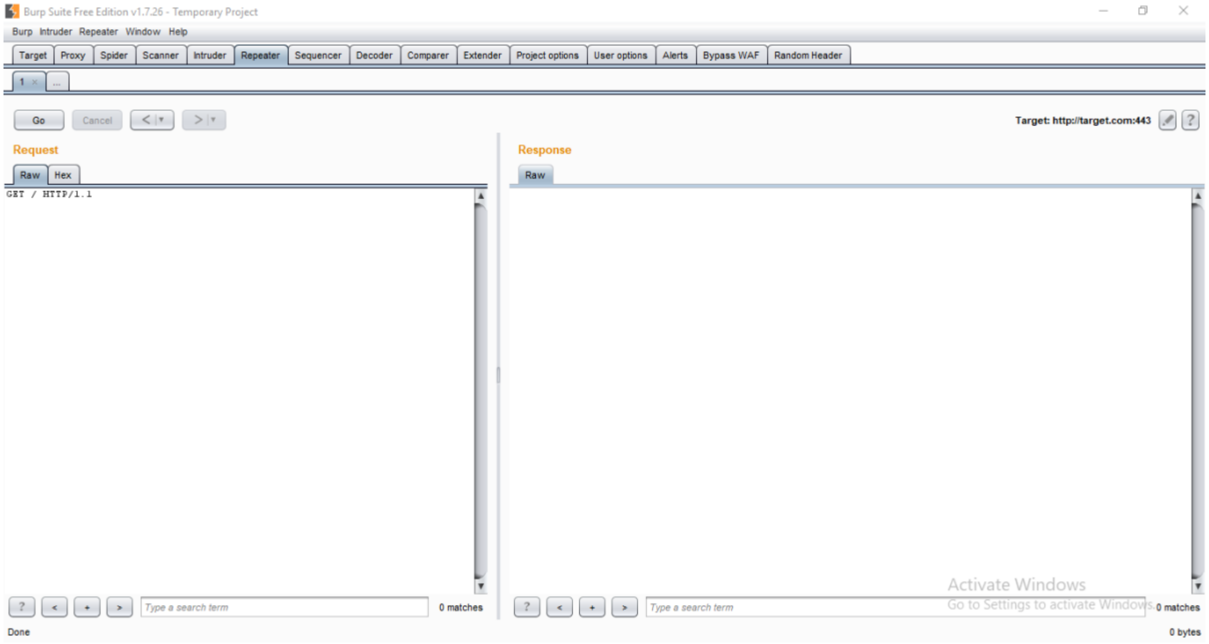
It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.

4. Repeater:

Repeater lets a user send requests repeatedly with manual modifications. It is used for:

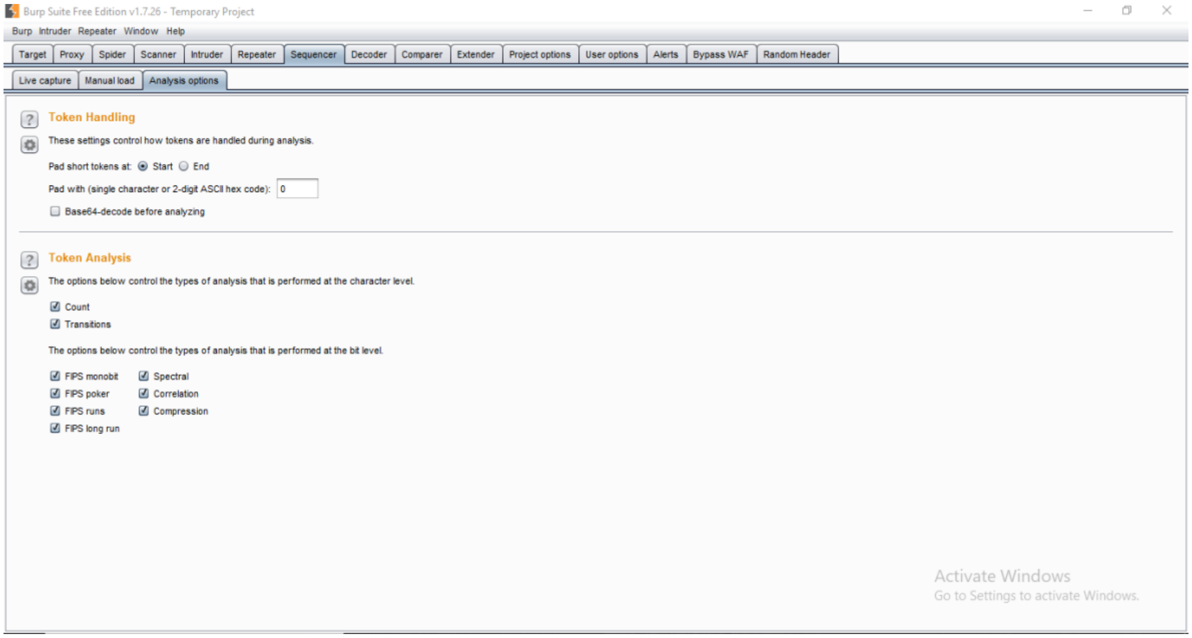
- Verifying whether the user-supplied values are being verified.
- If user-supplied values are being verified, how well is it being done?
- What values is the server expecting in an input parameter/request header?
- How does the server handle unexpected values?
- Is input sanitation being applied by the server?
- How well the server sanitizes the user-supplied inputs?
- What is the sanitation style being used by the server?
- Among all the cookies present, which one is the actual session cookie.
- How is CSRF protection being implemented and if there is a way to bypass it?


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
1 ×
...
Go
Cancel
Request
Raw
Hex
Response
Raw
Type a search term
0 matches
Done
0 bytes
Activate Windows
Go to Settings to activate Windows.

Target: http://target.com:443

```
GET / HTTP/1.1
```

5. Sequencer:


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Live capture
Manual load
Analysis options
Activate Windows
Go to Settings to activate Windows.

Token Handling

These settings control how tokens are handled during analysis.

Pad short tokens at: ● Start ○ End

Pad with (single character or 2-digit ASCII hex code): 0

☐ Base64-decode before analyzing

Token Analysis

The options below control the types of analysis that is performed at the character level.

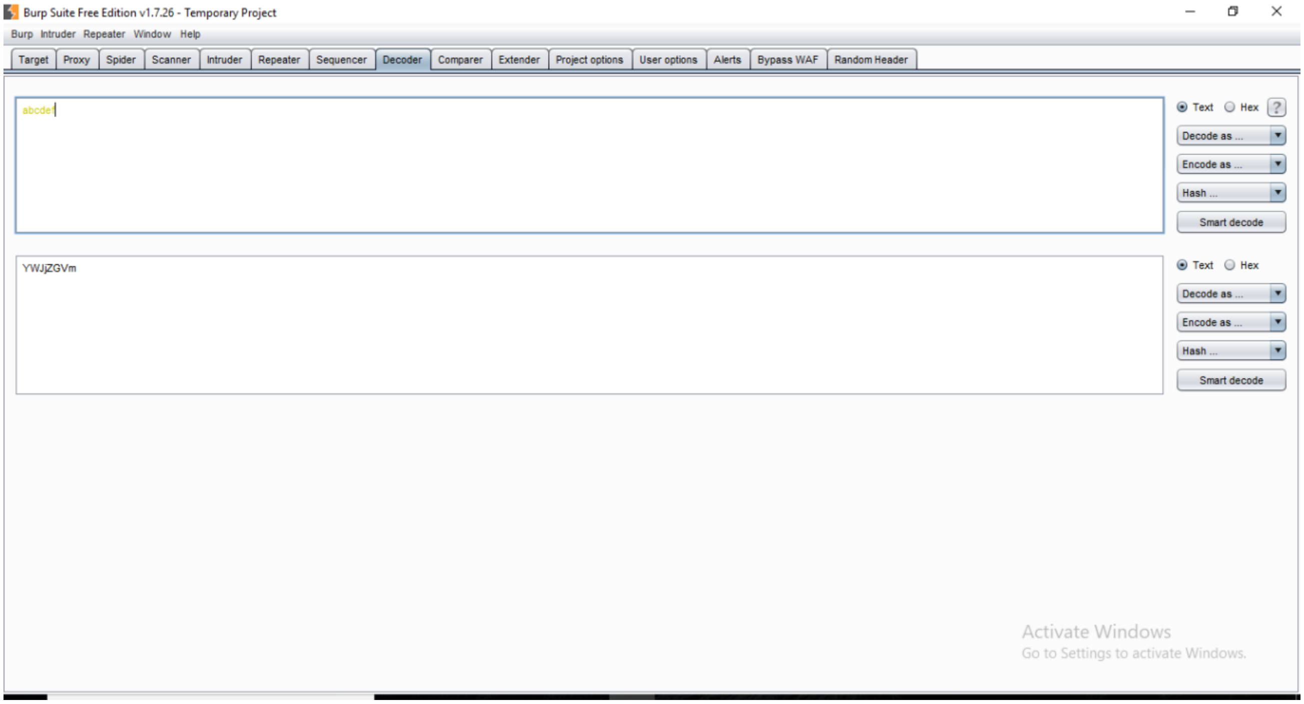
☑ Count
☑ Transitions

The options below control the types of analysis that is performed at the bit level.

☑ FIPS monobit
☑ FIPS poker
☑ FIPS runs
☑ FIPS long run
☑ Spectral
☑ Correlation
☑ Compression

The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bit-wise and character-wise. An entropy analyzer tests this hypothesis for being true. It works like this: initially, it is assumed that the tokens are random. Then the tokens are tested on certain parameters for certain characteristics. A term significance level is defined as a minimum value of probability that the token will exhibit for a characteristic, such that if the token has a characteristics probability below significance level, the hypothesis that the token is random will be rejected. This tool can be used to find out the weak tokens and enumerate their construction.

6. Decoder:


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
Activate Windows
Go to Settings to activate Windows.

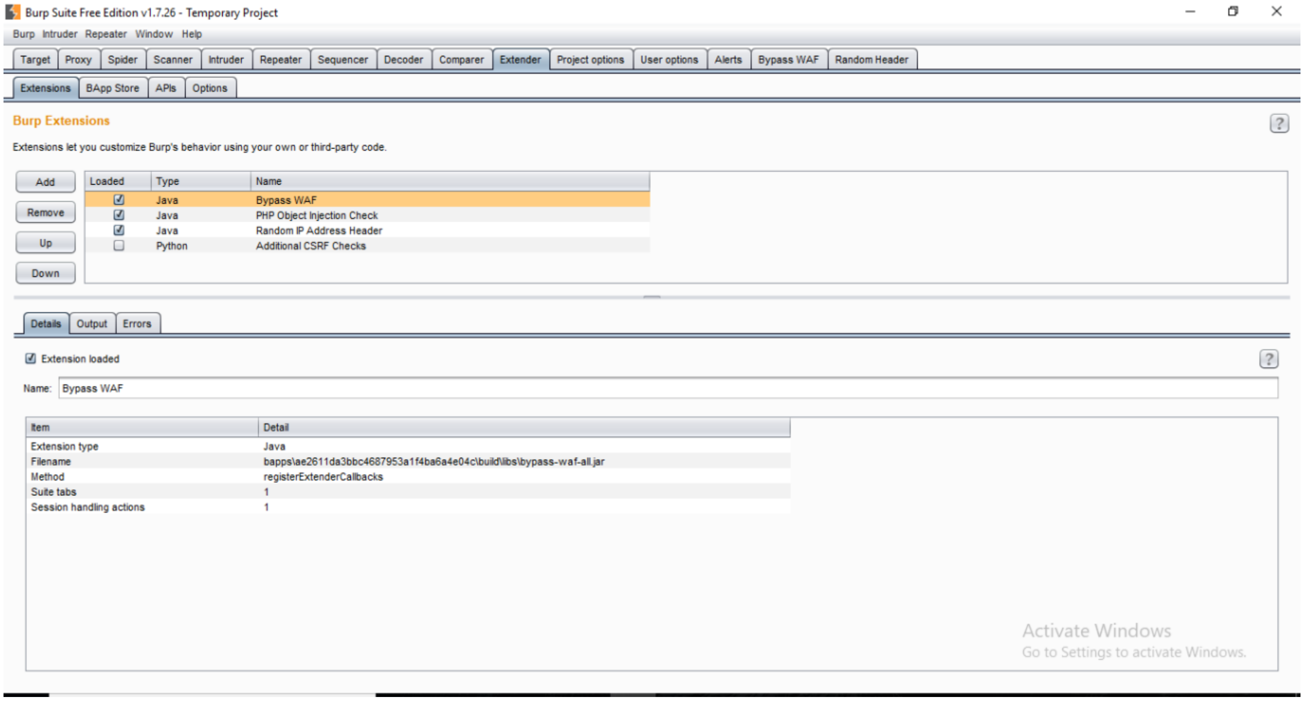
abcdef

YWJjZGVm

Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.

7. Extender:

BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called BApps. These work just like browser extensions. These can be viewed, modified, installed, and uninstalled in the Extender window. Some of them are supported on the community version, but some require the paid professional version.


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Extensions BApp Store APIs Options
Add
Remove
Up
Down
Details Output Errors
Activate Windows
Go to Settings to activate Windows.

Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

Loaded	Type	Name
☑	Java	Bypass WAF
☑	Java	PHP Object Injection Check
☑	Java	Random IP Address Header
□	Python	Additional CSRF Checks

☑ Extension loaded

Name: Bypass WAF

Item	Detail
Extension type	Java
Filename	bapps\ae2611da3bbc4687953a1f4ba6a4e04c\build\libs\bypass-waf-all.jar
Method	registerExtenderCallbacks
Suite tabs	1
Session handling actions	1