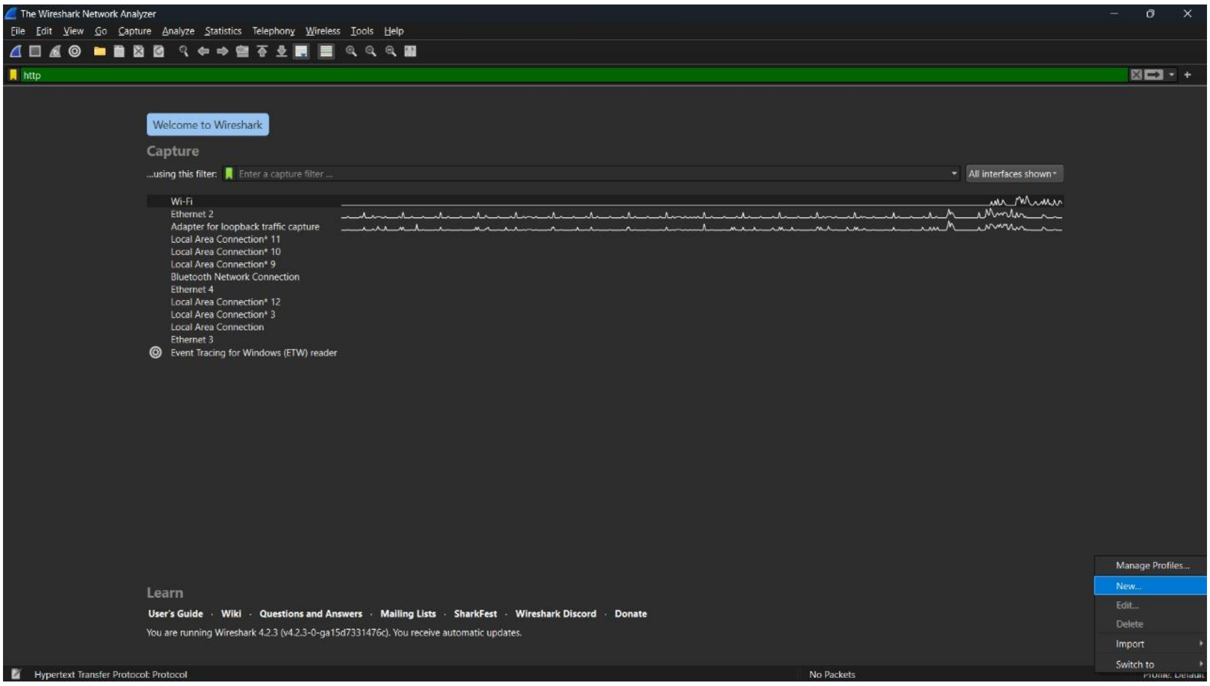
COMPUTER NETWORK LAB

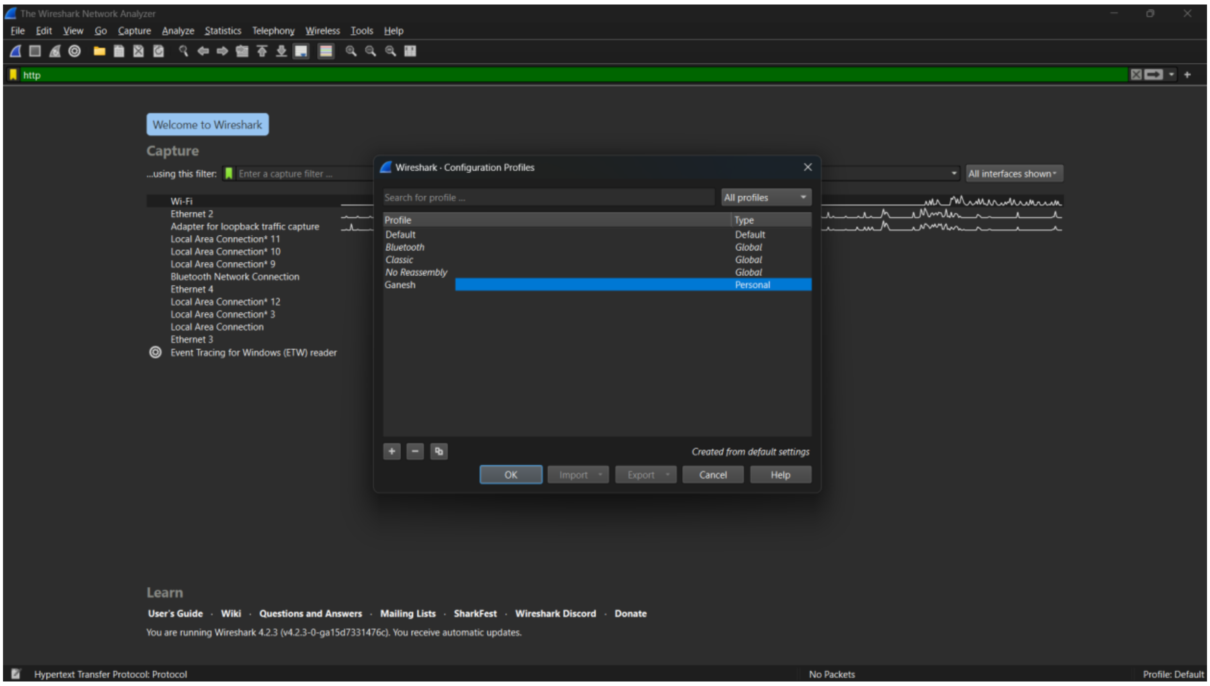
Sai Ganesh Eswaraprasad
HU22CSEN0100287

Creating Profiles


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Manage Profiles...
New...
Edit...
Delete
Import
Switch to
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Hypertext Transfer Protocol: Protocol
No Packets
Profile: Default

Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 11
Local Area Connection* 10
Local Area Connection* 9
Bluetooth Network Connection
Ethernet 4
Local Area Connection* 12
Local Area Connection* 3
Local Area Connection
Ethernet 3
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wireshark · Configuration Profiles
Search for profile ...
All profiles
+ − ⧉
OK
Import
Export
Cancel
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Hypertext Transfer Protocol: Protocol
No Packets
Profile: Default

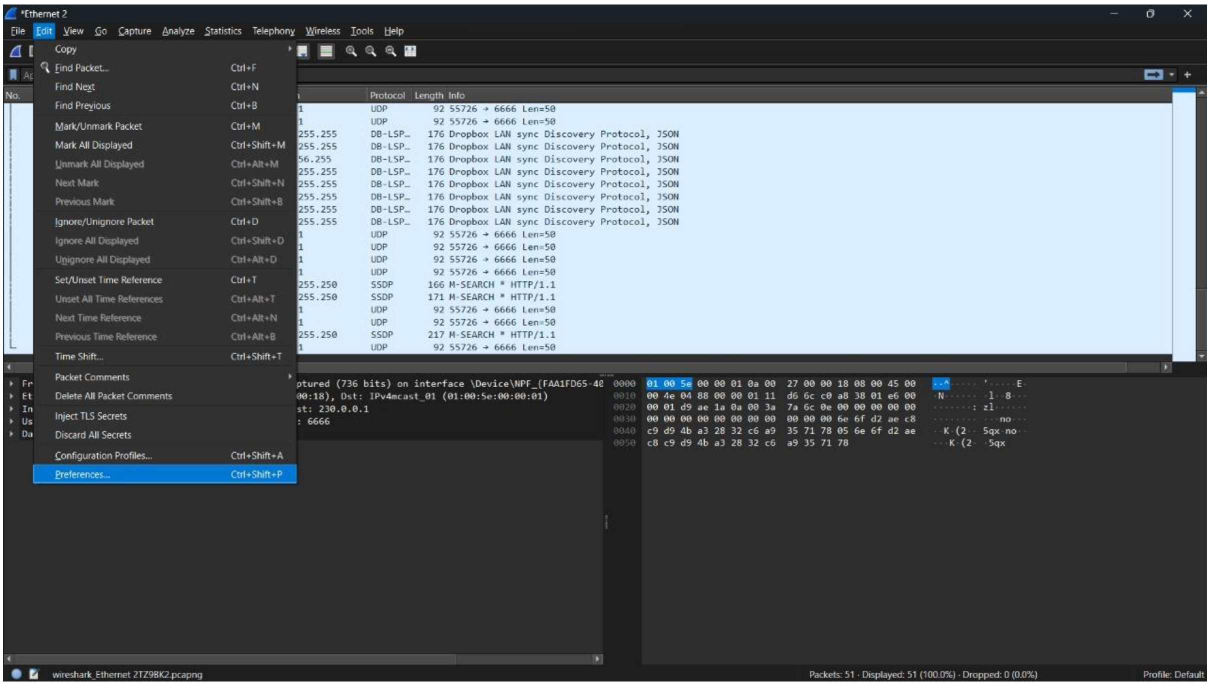
Profile	Type
Default	Default
Bluetooth	*Global*
Classic	*Global*
No Reassembly	*Global*
Ganesh	Personal

Created from default settings

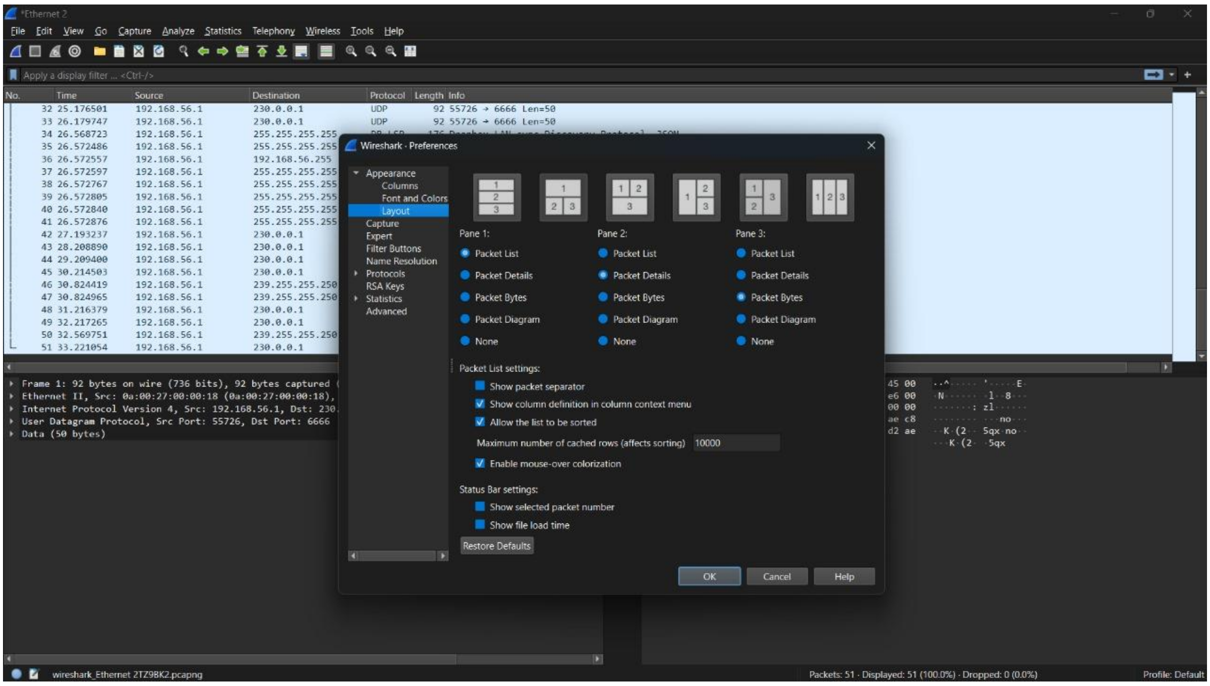
Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 11
Local Area Connection* 10
Local Area Connection* 9
Bluetooth Network Connection
Ethernet 4
Local Area Connection* 12
Local Area Connection* 3
Local Area Connection
Ethernet 3
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.

Changing Layout


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comments
Delete All Packet Comments
Inject TLS Secrets
Discard All Secrets
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
wireshark_Ethernet 2TZ9BK2.pcapng
Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

```
Protocol Length Info
UDP        92 55726 → 6666 Len=50
UDP        92 55726 → 6666 Len=50
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
DB-LSP…   176 Dropbox LAN sync Discovery Protocol, JSON
UDP        92 55726 → 6666 Len=50
UDP        92 55726 → 6666 Len=50
UDP        92 55726 → 6666 Len=50
UDP        92 55726 → 6666 Len=50
SSDP      166 M-SEARCH * HTTP/1.1
SSDP      171 M-SEARCH * HTTP/1.1
UDP        92 55726 → 6666 Len=50
UDP        92 55726 → 6666 Len=50
SSDP      217 M-SEARCH * HTTP/1.1
UDP        92 55726 → 6666 Len=50
```


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Restore Defaults
OK
Cancel
Help
wireshark_Ethernet 2TZ9BK2.pcapng
Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

```
No.  Time       Source        Destination
32 25.176501  192.168.56.1  230.0.0.1        UDP   92 55726 → 6666 Len=50
33 26.179747  192.168.56.1  230.0.0.1        UDP   92 55726 → 6666 Len=50
34 26.568723  192.168.56.1  255.255.255.255
35 26.572486  192.168.56.1  255.255.255.255
36 26.572557  192.168.56.1  192.168.56.255
37 26.572597  192.168.56.1  255.255.255.255
38 26.572767  192.168.56.1  255.255.255.255
39 26.572805  192.168.56.1  255.255.255.255
40 26.572840  192.168.56.1  255.255.255.255
41 26.572876  192.168.56.1  255.255.255.255
42 27.193237  192.168.56.1  230.0.0.1
43 28.208890  192.168.56.1  230.0.0.1
44 29.209400  192.168.56.1  230.0.0.1
45 30.214503  192.168.56.1  230.0.0.1
46 30.824419  192.168.56.1  239.255.255.250
47 30.824965  192.168.56.1  239.255.255.250
48 31.216379  192.168.56.1  230.0.0.1
49 32.217265  192.168.56.1  230.0.0.1
50 32.569751  192.168.56.1  239.255.255.250
51 33.221054  192.168.56.1  230.0.0.1
```

```
Frame 1: 92 bytes on wire (736 bits), 92 bytes captured
Ethernet II, Src: 0a:00:27:00:00:18 (0a:00:27:00:00:18),
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 230.
User Datagram Protocol, Src Port: 55726, Dst Port: 6666
Data (50 bytes)
```

Pane 1: ● Packet List ○ Packet Details ○ Packet Bytes ○ Packet Diagram ○ None

Pane 2: ○ Packet List ● Packet Details ○ Packet Bytes ○ Packet Diagram ○ None

Pane 3: ○ Packet List ○ Packet Details ● Packet Bytes ○ Packet Diagram ○ None

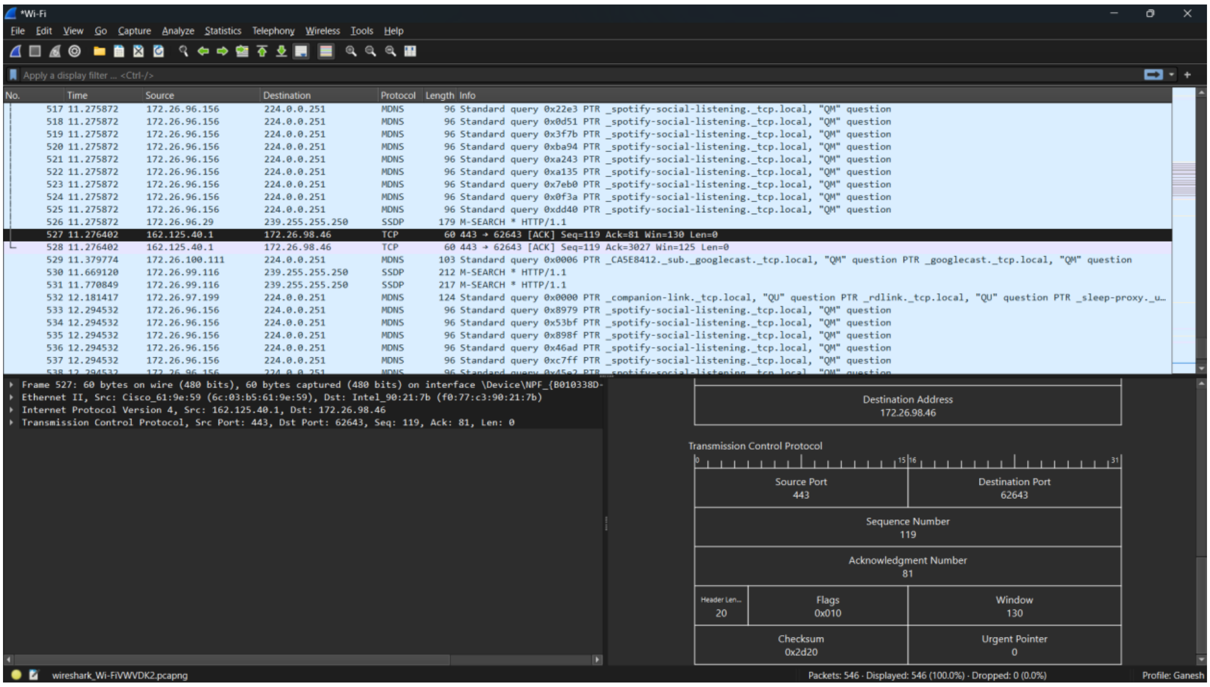
Packet List settings:

- □ Show packet separator
- ☑ Show column definition in column context menu
- ☑ Allow the list to be sorted
- Maximum number of cached rows (affects sorting) 10000
- ☑ Enable mouse-over colorization

Status Bar settings:

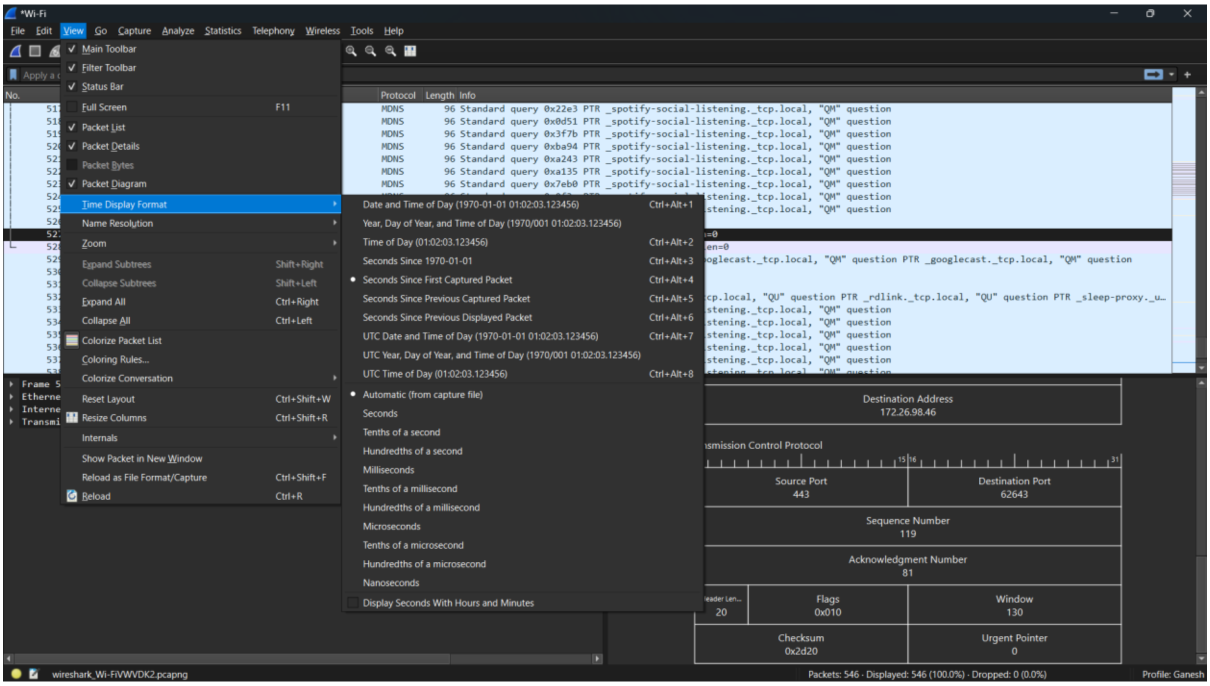
- □ Show selected packet number
- □ Show file load time

Displaying Nos in packet diagram

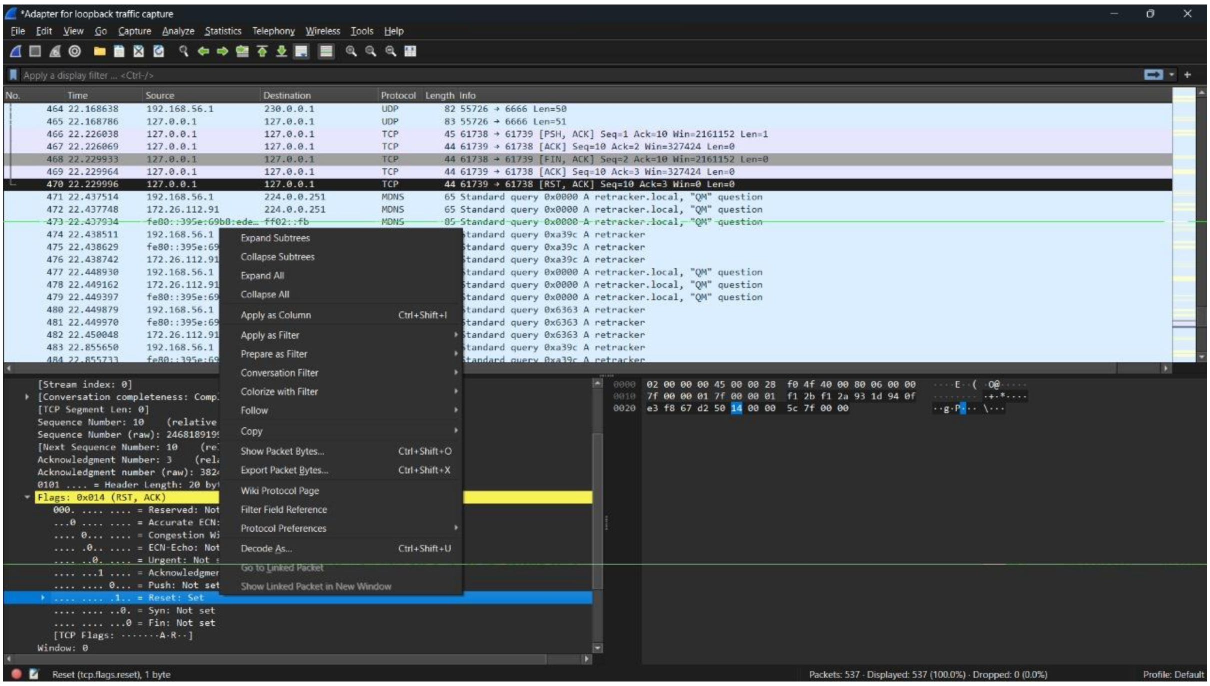

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Destination Address
172.26.98.46
Transmission Control Protocol
0
15
16
31
Source Port
443
Destination Port
62643
Sequence Number
119
Acknowledgment Number
81
Header Len...
20
Flags
0x010
Window
130
Checksum
0x2d20
Urgent Pointer
0
wireshark_Wi-FiVWVDK2.pcapng
Packets: 546 · Displayed: 546 (100.0%) · Dropped: 0 (0.0%)
Profile: Ganesh

```
No.    Time        Source          Destination      Protocol Length Info
   517 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x22e3 PTR _spotify-social-listening._tcp.local, "QM" question
   518 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x0d51 PTR _spotify-social-listening._tcp.local, "QM" question
   519 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x3f7b PTR _spotify-social-listening._tcp.local, "QM" question
   520 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0xba94 PTR _spotify-social-listening._tcp.local, "QM" question
   521 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0xa243 PTR _spotify-social-listening._tcp.local, "QM" question
   522 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0xa135 PTR _spotify-social-listening._tcp.local, "QM" question
   523 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x7eb0 PTR _spotify-social-listening._tcp.local, "QM" question
   524 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x0f3a PTR _spotify-social-listening._tcp.local, "QM" question
   525 11.275872   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0xdd40 PTR _spotify-social-listening._tcp.local, "QM" question
   526 11.275872   172.26.96.29    239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
   527 11.276402   162.125.40.1    172.26.98.46     TCP        60 443 → 62643 [ACK] Seq=119 Ack=81 Win=130 Len=0
   528 11.276402   162.125.40.1    172.26.98.46     TCP        60 443 → 62643 [ACK] Seq=119 Ack=3027 Win=125 Len=0
   529 11.379774   172.26.100.111  224.0.0.251      MDNS      103 Standard query 0x0006 PTR _CA5E8412._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
   530 11.669120   172.26.99.116   239.255.255.250  SSDP      212 M-SEARCH * HTTP/1.1
   531 11.770849   172.26.99.116   239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
   532 12.181417   172.26.97.199   224.0.0.251      MDNS      124 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _sleep-proxy._u…
   533 12.294532   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x8979 PTR _spotify-social-listening._tcp.local, "QM" question
   534 12.294532   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x53bf PTR _spotify-social-listening._tcp.local, "QM" question
   535 12.294532   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x898f PTR _spotify-social-listening._tcp.local, "QM" question
   536 12.294532   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0x46ad PTR _spotify-social-listening._tcp.local, "QM" question
   537 12.294532   172.26.96.156   224.0.0.251      MDNS       96 Standard query 0xc7ff PTR _spotify-social-listening._tcp.local, "QM" question

▸ Frame 527: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{B010338D-
▸ Ethernet II, Src: Cisco_61:9e:59 (6c:03:b5:61:9e:59), Dst: Intel_90:21:7b (f0:77:c3:90:21:7b)
▸ Internet Protocol Version 4, Src: 162.125.40.1, Dst: 172.26.98.46
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 62643, Seq: 119, Ack: 81, Len: 0
```

Changing Time Display Format


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
✓ Main Toolbar
✓ Filter Toolbar
✓ Status Bar
Full Screen F11
✓ Packet List
✓ Packet Details
Packet Bytes
✓ Packet Diagram
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
● Seconds Since First Captured Packet Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
● Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Tenths of a millisecond
Hundredths of a millisecond
Microseconds
Tenths of a microsecond
Hundredths of a microsecond
Nanoseconds
Display Seconds With Hours and Minutes
Destination Address
172.26.98.46
Source Port
443
Destination Port
62643
Sequence Number
119
Acknowledgment Number
81
20
Flags
0x010
Window
130
Checksum
0x2d20
Urgent Pointer
0
wireshark_Wi-FiVWVDK2.pcapng
Packets: 546 · Displayed: 546 (100.0%) · Dropped: 0 (0.0%)
Profile: Ganesh

Applying Filters



*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes… Ctrl+Shift+O
Export Packet Bytes… Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As… Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window

```
No.   Time       Source           Destination   Protocol Length Info
464 22.168638   192.168.56.1     230.0.0.1      UDP    82 55726 → 6666 Len=50
465 22.168786   127.0.0.1        127.0.0.1      UDP    83 55726 → 6666 Len=51
466 22.226038   127.0.0.1        127.0.0.1      TCP    45 61738 → 61739 [PSH, ACK] Seq=1 Ack=10 Win=2161152 Len=1
467 22.226069   127.0.0.1        127.0.0.1      TCP    44 61739 → 61738 [ACK] Seq=10 Ack=2 Win=327424 Len=0
468 22.229933   127.0.0.1        127.0.0.1      TCP    44 61738 → 61739 [FIN, ACK] Seq=2 Ack=10 Win=2161152 Len=0
469 22.229964   127.0.0.1        127.0.0.1      TCP    44 61739 → 61738 [ACK] Seq=10 Ack=3 Win=327424 Len=0
470 22.229996   127.0.0.1        127.0.0.1      TCP    44 61739 → 61738 [RST, ACK] Seq=10 Ack=3 Win=0 Len=0
471 22.437514   192.168.56.1     224.0.0.251    MDNS   65 Standard query 0x0000 A retracker.local, "QM" question
472 22.437748   172.26.112.91    224.0.0.251    MDNS   65 Standard query 0x0000 A retracker.local, "QM" question
473 22.437934   fe80::395e:69b8:ede… ff02::fb   MDNS   85 Standard query 0x0000 A retracker.local, "QM" question
474 22.438511   192.168.56.1                       Standard query 0xa39c A retracker
475 22.438629   fe80::395e:69                      Standard query 0xa39c A retracker
476 22.438742   172.26.112.91                      Standard query 0xa39c A retracker
477 22.448930   192.168.56.1                       Standard query 0x0000 A retracker.local, "QM" question
478 22.449162   172.26.112.91                      Standard query 0x0000 A retracker.local, "QM" question
479 22.449397   fe80::395e:69                      Standard query 0x0000 A retracker.local, "QM" question
480 22.449879   192.168.56.1                       Standard query 0x6363 A retracker
481 22.449970   fe80::395e:69                      Standard query 0x6363 A retracker
482 22.450048   172.26.112.91                      Standard query 0x6363 A retracker
483 22.855650   192.168.56.1                       Standard query 0xa39c A retracker
484 22.855733   fe80::395e:69                      Standard query 0xa39c A retracker
```

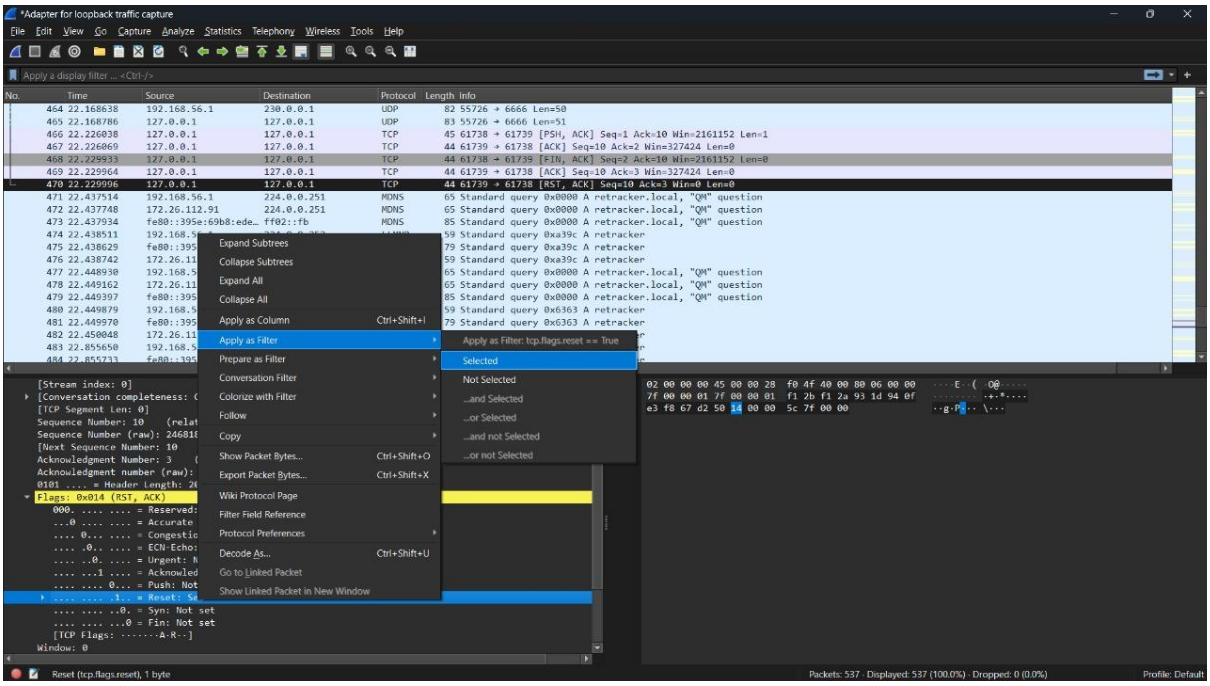
```
    [Stream index: 0]
  ▸ [Conversation completeness: Comp
    [TCP Segment Len: 0]
    Sequence Number: 10    (relative
    Sequence Number (raw): 246818919
    [Next Sequence Number: 10    (re
    Acknowledgment Number: 3    (rel
    Acknowledgment number (raw): 382
    0101 .... = Header Length: 20 by
  ▾ Flags: 0x014 (RST, ACK)
      000. .... .... = Reserved: Not
      ...0 .... .... = Accurate ECN:
      .... 0... .... = Congestion Wi
      .... .0.. .... = ECN-Echo: Not
      .... ..0. .... = Urgent: Not s
      .... ...1 .... = Acknowledgmen
      .... .... 0... = Push: Not set
    ▸ .... .... .1.. = Reset: Set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A·R··]
    Window: 0
```

```
0000  02 00 00 00 45 00 00 28  f0 4f 40 00 80 06 00 00   ····E··( ·O@·····
0010  7f 00 00 01 7f 00 00 01  f1 2b f1 2a 93 1d 94 0f   ········ ·+·*····
0020  e3 f8 67 d2 50 14 00 00  5c 7f 00 00               ··g·P··· \···
```

Reset (tcp.flags.reset), 1 byte

Packets: 537 · Displayed: 537 (100.0%) · Dropped: 0 (0.0%)

Profile: Default



```
No.   Time       Source           Destination   Protocol Length Info
464 22.168638   192.168.56.1     230.0.0.1      UDP    82 55726 → 6666 Len=50
465 22.168786   127.0.0.1        127.0.0.1      UDP    83 55726 → 6666 Len=51
466 22.226038   127.0.0.1        127.0.0.1      TCP    45 61738 → 61739 [PSH, ACK] Seq=1 Ack=10 Win=2161152 Len=1
467 22.226069   127.0.0.1        127.0.0.1      TCP    44 61739 → 61738 [ACK] Seq=10 Ack=2 Win=327424 Len=0
468 22.229933   127.0.0.1        127.0.0.1      TCP    44 61738 → 61739 [FIN, ACK] Seq=2 Ack=10 Win=2161152 Len=0
469 22.229964   127.0.0.1        127.0.0.1      TCP    44 61739 → 61738 [ACK] Seq=10 Ack=3 Win=327424 Len=0
470 22.229996   127.0.0.1        127.0.0.1      TCP    44 61739 → 61738 [RST, ACK] Seq=10 Ack=3 Win=0 Len=0
471 22.437514   192.168.56.1     224.0.0.251    MDNS   65 Standard query 0x0000 A retracker.local, "QM" question
472 22.437748   172.26.112.91    224.0.0.251    MDNS   65 Standard query 0x0000 A retracker.local, "QM" question
473 22.437934   fe80::395e:69b8:ede… ff02::fb   MDNS   85 Standard query 0x0000 A retracker.local, "QM" question
474 22.438511   192.168.5                          59 Standard query 0xa39c A retracker
475 22.438629   fe80::395                          79 Standard query 0xa39c A retracker
476 22.438742   172.26.11                          59 Standard query 0xa39c A retracker
477 22.448930   192.168.5                          65 Standard query 0x0000 A retracker.local, "QM" question
478 22.449162   172.26.11                          65 Standard query 0x0000 A retracker.local, "QM" question
479 22.449397   fe80::395                          85 Standard query 0x0000 A retracker.local, "QM" question
480 22.449879   192.168.5                          59 Standard query 0x6363 A retracker
481 22.449970   fe80::395                          79 Standard query 0x6363 A retracker
482 22.450048   172.26.11
483 22.855650   192.168.5
484 22.855733   fe80::395
```

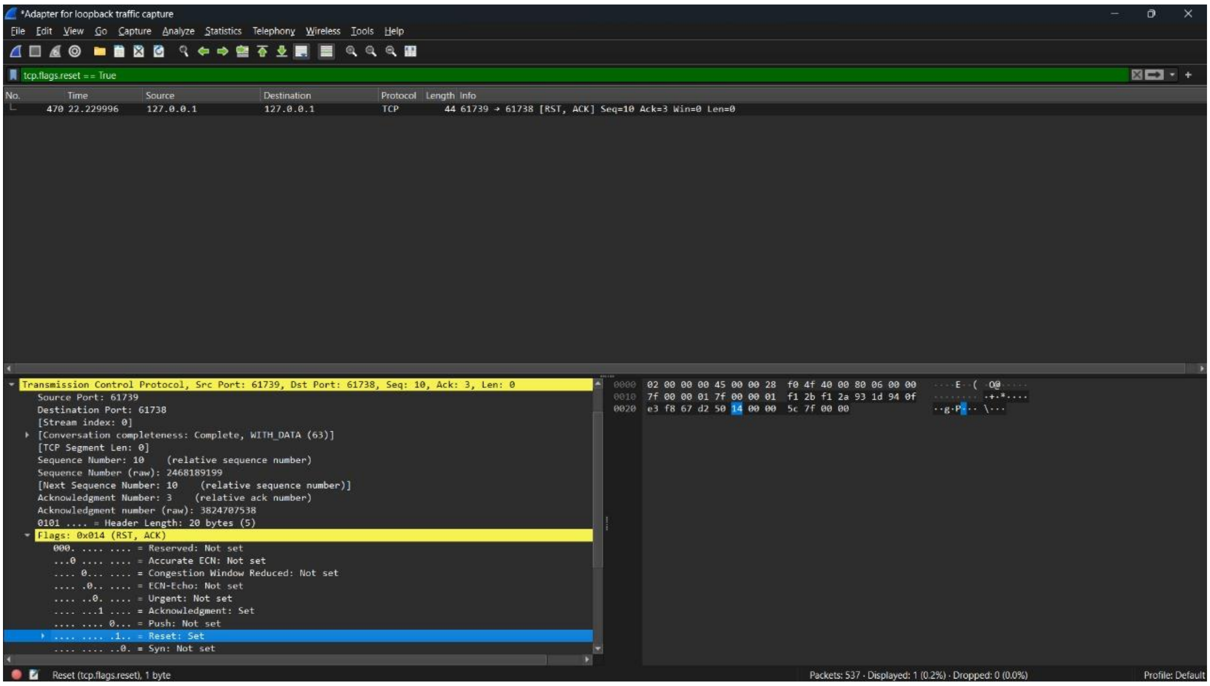
```
    [Stream index: 0]
  ▸ [Conversation completeness: C
    [TCP Segment Len: 0]
    Sequence Number: 10    (relat
    Sequence Number (raw): 246818
    [Next Sequence Number: 10
    Acknowledgment Number: 3    (
    Acknowledgment number (raw):
    0101 .... = Header Length: 20
  ▾ Flags: 0x014 (RST, ACK)
      000. .... .... = Reserved:
      ...0 .... .... = Accurate
      .... 0... .... = Congestio
      .... .0.. .... = ECN-Echo:
      .... ..0. .... = Urgent: N
      .... ...1 .... = Acknowled
      .... .... 0... = Push: Not
    ▸ .... .... .1.. = Reset: Se
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A·R··]
    Window: 0
```

```
02 00 00 00 45 00 00 28  f0 4f 40 00 80 06 00 00   ····E··( ·O@·····
7f 00 00 01 7f 00 00 01  f1 2b f1 2a 93 1d 94 0f   ········ ·+·*····
e3 f8 67 d2 50 14 00 00  5c 7f 00 00               ··g·P··· \···
```

Reset (tcp.flags.reset), 1 byte

Packets: 537 · Displayed: 537 (100.0%) · Dropped: 0 (0.0%)

Profile: Default


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.reset == True

```
No.       Time         Source          Destination     Protocol  Length  Info
    470 22.229996      127.0.0.1       127.0.0.1       TCP         44 61739 → 61738 [RST, ACK] Seq=10 Ack=3 Win=0 Len=0
```

```
Transmission Control Protocol, Src Port: 61739, Dst Port: 61738, Seq: 10, Ack: 3, Len: 0
    Source Port: 61739
    Destination Port: 61738
    [Stream index: 0]
  ▸ [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 10    (relative sequence number)
    Sequence Number (raw): 2468189199
    [Next Sequence Number: 10    (relative sequence number)]
    Acknowledgment Number: 3    (relative ack number)
    Acknowledgment number (raw): 3824707538
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x014 (RST, 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
      ▸ .... .... .1.. = Reset: Set
        .... .... ..0. = Syn: Not set
```

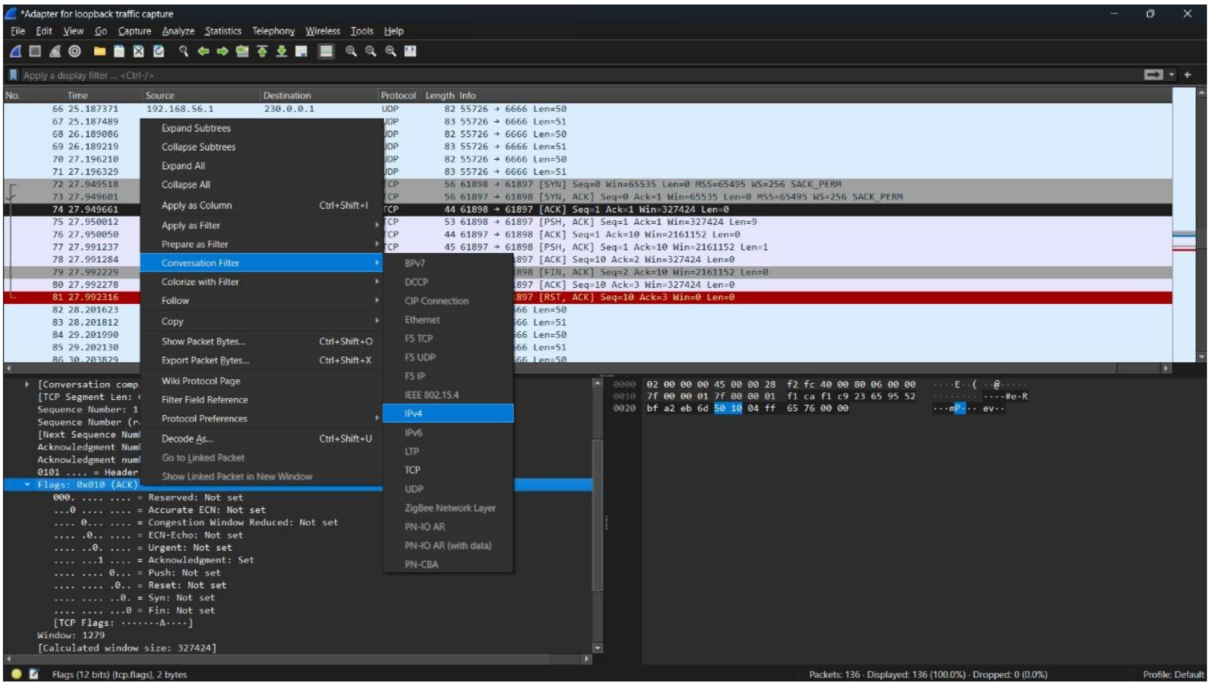
```
0000  02 00 00 00 45 00 00 28  f0 4f 40 00 80 06 00 00   ····E··( ·O@·····
0010  7f 00 00 01 7f 00 00 01  f1 2b f1 2a 93 1d 94 0f   ········ ·+·*····
0020  e3 f8 67 d2 50 14 00 00  5c 7f 00 00               ··g·P··· \···
```

Reset (tcp.flags.reset), 1 byte

Packets: 537 · Displayed: 1 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

Conversation FIlter



```
No.       Time         Source          Destination     Protocol  Length  Info
     66 25.187371      192.168.56.1    230.0.0.1       UDP         82 55726 → 6666 Len=50
     67 25.187489                                      UDP         83 55726 → 6666 Len=51
     68 26.189086                                      UDP         82 55726 → 6666 Len=50
     69 26.189219                                      UDP         83 55726 → 6666 Len=51
     70 27.196210                                      UDP         82 55726 → 6666 Len=50
     71 27.196329                                      UDP         83 55726 → 6666 Len=51
     72 27.949518                                      TCP         56 61898 → 61897 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
     73 27.949601                                      TCP         56 61897 → 61898 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
     74 27.949661                                      TCP         44 61898 → 61897 [ACK] Seq=1 Ack=1 Win=327424 Len=0
     75 27.950012                                      TCP         53 61898 → 61897 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=9
     76 27.950050                                      TCP         44 61897 → 61898 [ACK] Seq=1 Ack=10 Win=2161152 Len=0
     77 27.991237                                      TCP         45 61897 → 61898 [PSH, ACK] Seq=1 Ack=10 Win=2161152 Len=1
     78 27.991284                                                       1897 [ACK] Seq=10 Ack=2 Win=327424 Len=0
     79 27.992229                                                       1898 [FIN, ACK] Seq=2 Ack=10 Win=2161152 Len=0
     80 27.992278                                                       1897 [ACK] Seq=10 Ack=3 Win=327424 Len=0
     81 27.992316                                                       1897 [RST, ACK] Seq=10 Ack=3 Win=0 Len=0
     82 28.201623                                                       66 Len=50
     83 28.201812                                                       66 Len=51
     84 29.201990                                                       66 Len=50
     85 29.202130                                                       66 Len=51
     86 30.203829                                                       66 Len=50
```

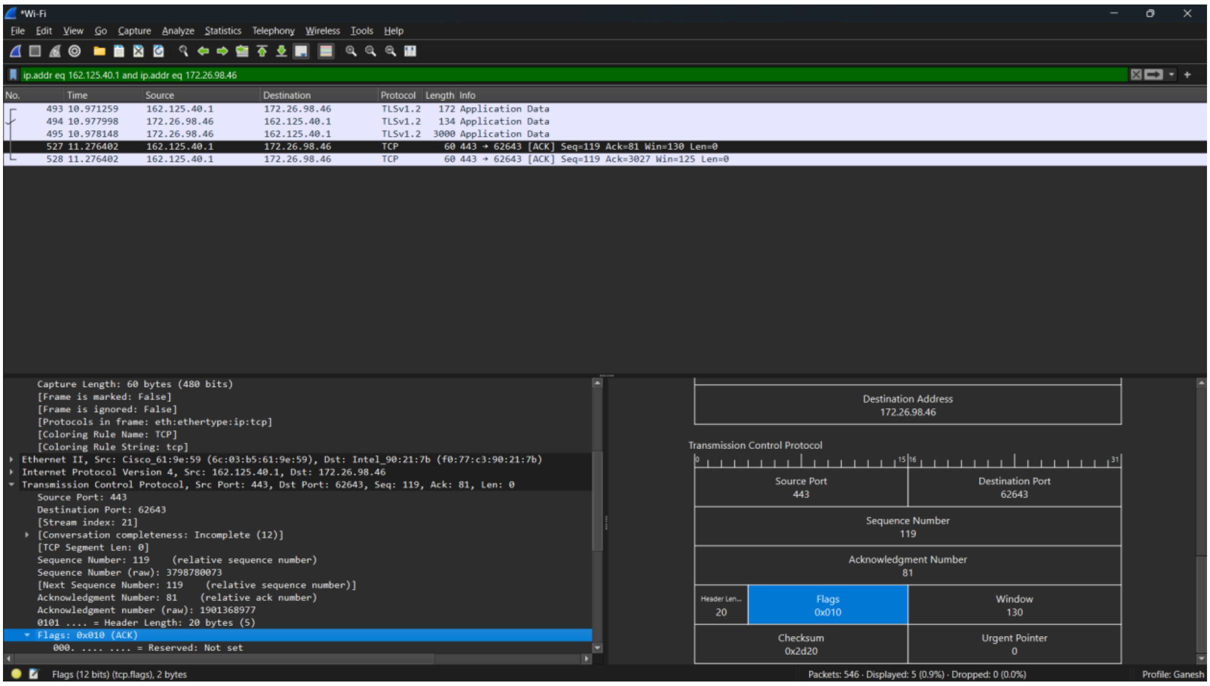
```
  ▸ [Conversation comp
    [TCP Segment Len:
    Sequence Number: 1
    Sequence Number (r
    [Next Sequence Num
    Acknowledgment Num
    Acknowledgment num
    0101 .... = Header
  ▾ Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 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
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A····]
    Window: 1279
    [Calculated window size: 327424]
```

```
0000  02 00 00 00 45 00 00 28  f2 fc 40 00 80 06 00 00   ····E··( ··@·····
0010  7f 00 00 01 7f 00 00 01  f1 ca f1 c9 23 65 95 52   ········ ····#e·R
0020  bf a2 eb 6d 50 10 04 ff  65 76 00 00               ···mP··· ev··
```

Flags (12 bits) (tcp.flags), 2 bytes

Packets: 136 · Displayed: 136 (100.0%) · Dropped: 0 (0.0%)

Profile: Default



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

ip.addr eq 162.125.40.1 and ip.addr eq 172.26.98.46

```
No.     Time       Source          Destination     Protocol Length Info
    493 10.971259  162.125.40.1    172.26.98.46    TLSv1.2   172 Application Data
    494 10.977998  172.26.98.46    162.125.40.1    TLSv1.2   134 Application Data
    495 10.978148  172.26.98.46    162.125.40.1    TLSv1.2  3000 Application Data
    527 11.276402  162.125.40.1    172.26.98.46    TCP        60 443 → 62643 [ACK] Seq=119 Ack=81 Win=130 Len=0
    528 11.276402  162.125.40.1    172.26.98.46    TCP        60 443 → 62643 [ACK] Seq=119 Ack=3027 Win=125 Len=0
```

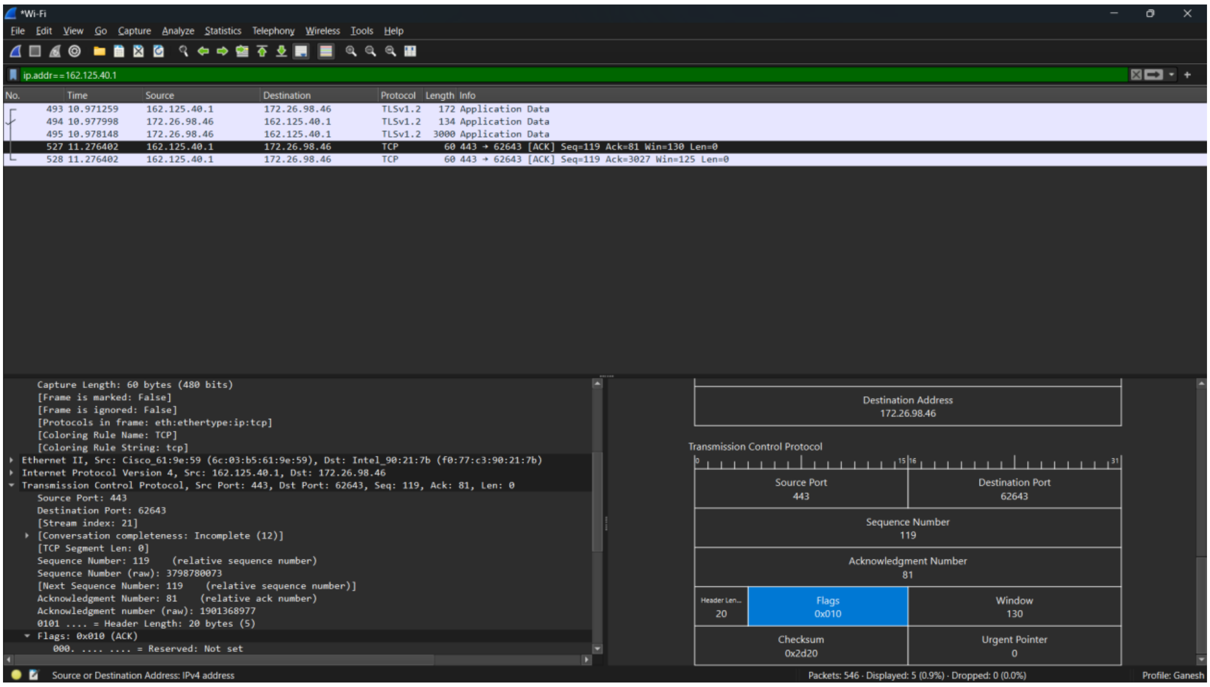
```
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
› Ethernet II, Src: Cisco_61:9e:59 (6c:03:b5:61:9e:59), Dst: Intel_90:21:7b (f0:77:c3:90:21:7b)
› Internet Protocol Version 4, Src: 162.125.40.1, Dst: 172.26.98.46
⌄ Transmission Control Protocol, Src Port: 443, Dst Port: 62643, Seq: 119, Ack: 81, Len: 0
    Source Port: 443
    Destination Port: 62643
    [Stream index: 21]
  › [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 119    (relative sequence number)
    Sequence Number (raw): 3798780073
    [Next Sequence Number: 119    (relative sequence number)]
    Acknowledgment Number: 81    (relative ack number)
    Acknowledgment number (raw): 1901368977
    0101 .... = Header Length: 20 bytes (5)
  ⌄ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
```

Flags (12 bits) (tcp.flags), 2 bytes

Packets: 546 · Displayed: 5 (0.9%) · Dropped: 0 (0.0%)

Profile: Ganesh

Searching IP address



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

ip.addr==162.125.40.1

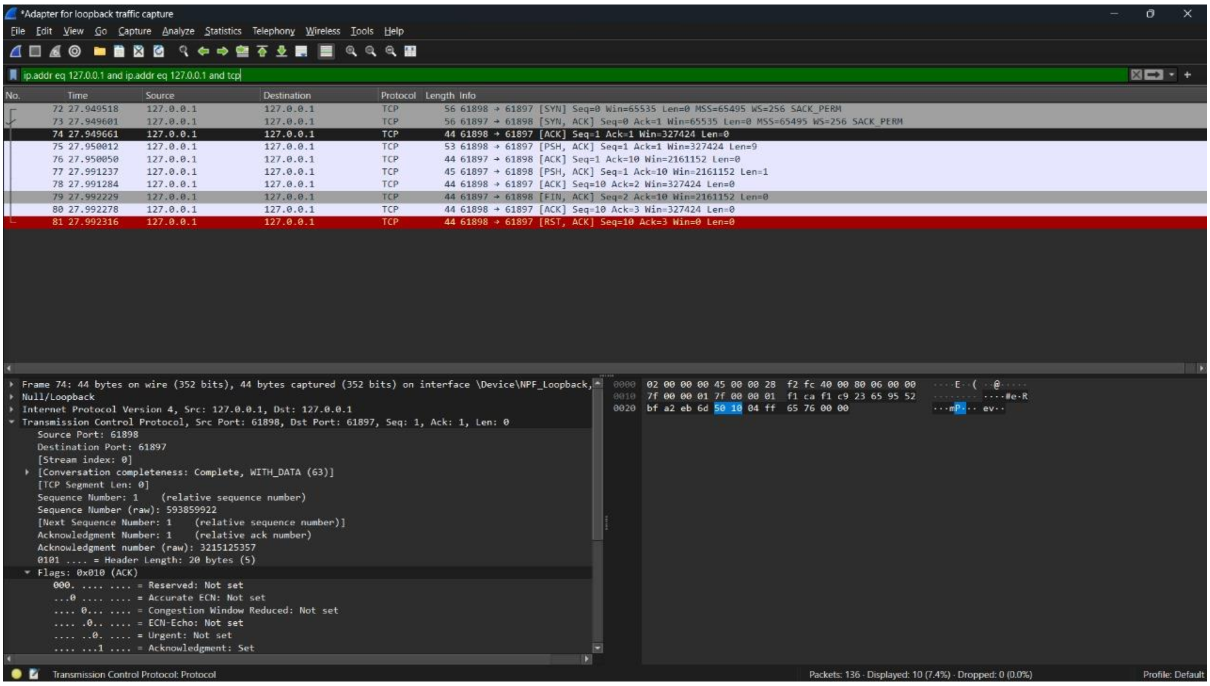
```
No.     Time       Source          Destination     Protocol Length Info
    493 10.971259  162.125.40.1    172.26.98.46    TLSv1.2   172 Application Data
    494 10.977998  172.26.98.46    162.125.40.1    TLSv1.2   134 Application Data
    495 10.978148  172.26.98.46    162.125.40.1    TLSv1.2  3000 Application Data
    527 11.276402  162.125.40.1    172.26.98.46    TCP        60 443 → 62643 [ACK] Seq=119 Ack=81 Win=130 Len=0
    528 11.276402  162.125.40.1    172.26.98.46    TCP        60 443 → 62643 [ACK] Seq=119 Ack=3027 Win=125 Len=0
```

```
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
› Ethernet II, Src: Cisco_61:9e:59 (6c:03:b5:61:9e:59), Dst: Intel_90:21:7b (f0:77:c3:90:21:7b)
› Internet Protocol Version 4, Src: 162.125.40.1, Dst: 172.26.98.46
⌄ Transmission Control Protocol, Src Port: 443, Dst Port: 62643, Seq: 119, Ack: 81, Len: 0
    Source Port: 443
    Destination Port: 62643
    [Stream index: 21]
  › [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 119    (relative sequence number)
    Sequence Number (raw): 3798780073
    [Next Sequence Number: 119    (relative sequence number)]
    Acknowledgment Number: 81    (relative ack number)
    Acknowledgment number (raw): 1901368977
    0101 .... = Header Length: 20 bytes (5)
  ⌄ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
```

Source or Destination Address: IPv4 address

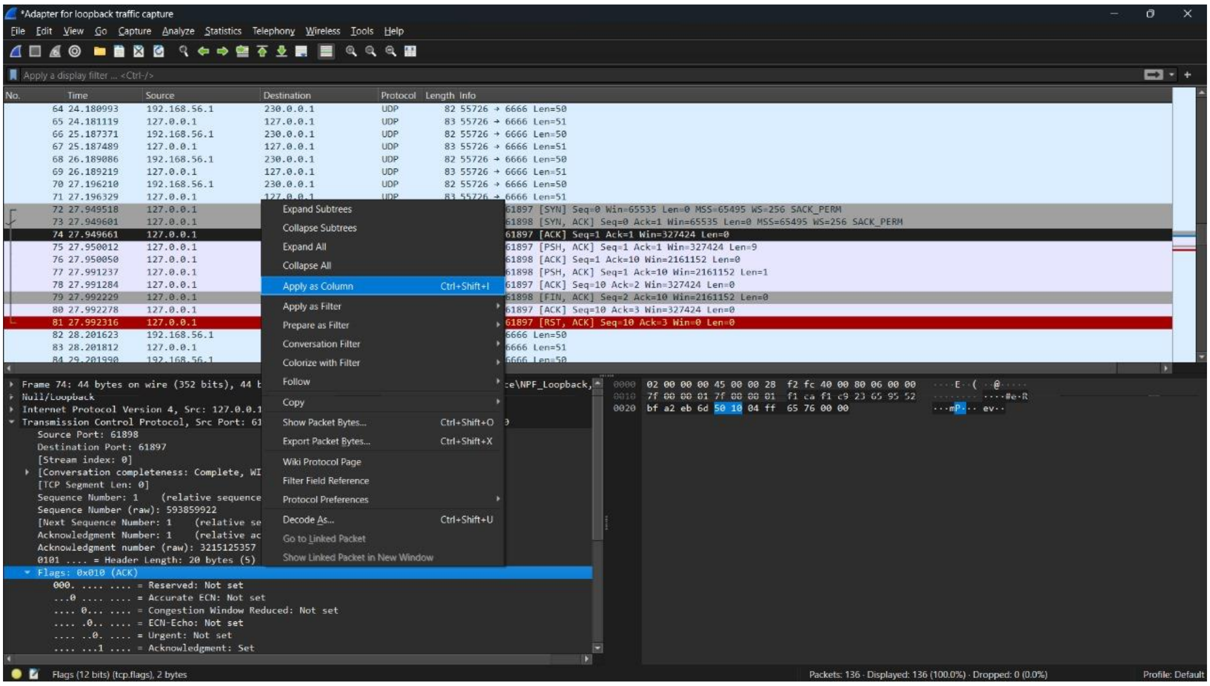
Packets: 546 · Displayed: 5 (0.9%) · Dropped: 0 (0.0%)

Profile: Ganesh

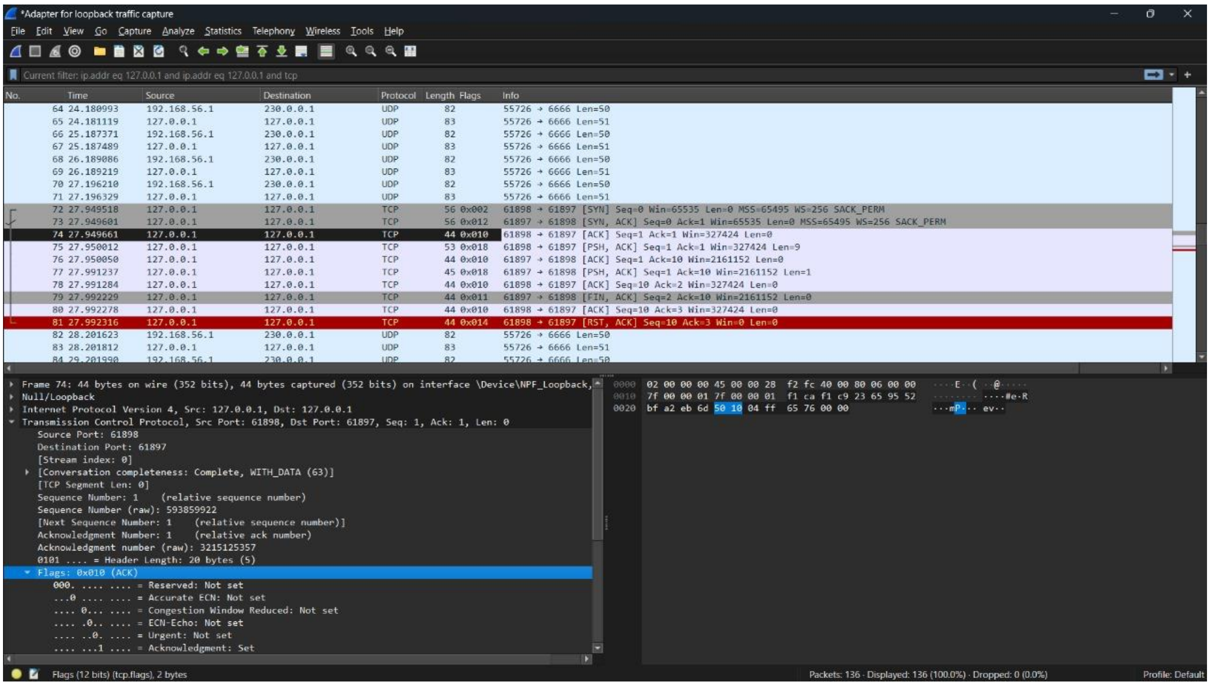

*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr eq 127.0.0.1 and ip.addr eq 127.0.0.1 and tcp

No.   Time        Source      Destination  Protocol Length Info
   72 27.949518   127.0.0.1   127.0.0.1    TCP      56 61898 → 61897 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   73 27.949601   127.0.0.1   127.0.0.1    TCP      56 61897 → 61898 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   74 27.949661   127.0.0.1   127.0.0.1    TCP      44 61898 → 61897 [ACK] Seq=1 Ack=1 Win=327424 Len=0
   75 27.950012   127.0.0.1   127.0.0.1    TCP      53 61898 → 61897 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=9
   76 27.950050   127.0.0.1   127.0.0.1    TCP      44 61897 → 61898 [ACK] Seq=1 Ack=10 Win=2161152 Len=0
   77 27.991237   127.0.0.1   127.0.0.1    TCP      45 61897 → 61898 [PSH, ACK] Seq=1 Ack=10 Win=2161152 Len=1
   78 27.991284   127.0.0.1   127.0.0.1    TCP      44 61898 → 61897 [ACK] Seq=10 Ack=2 Win=327424 Len=0
   79 27.992229   127.0.0.1   127.0.0.1    TCP      44 61897 → 61898 [FIN, ACK] Seq=2 Ack=10 Win=2161152 Len=0
   80 27.992278   127.0.0.1   127.0.0.1    TCP      44 61898 → 61897 [ACK] Seq=10 Ack=3 Win=327424 Len=0
   81 27.992316   127.0.0.1   127.0.0.1    TCP      44 61898 → 61897 [RST, ACK] Seq=10 Ack=3 Win=0 Len=0

> Frame 74: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_Loopback,
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
v Transmission Control Protocol, Src Port: 61898, Dst Port: 61897, Seq: 1, Ack: 1, Len: 0
    Source Port: 61898
    Destination Port: 61897
    [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 593859922
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3215125357
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (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

0000  02 00 00 00 45 00 00 28  f2 fc 40 00 80 06 00 00   ····E··( ··@·····
0010  7f 00 00 01 7f 00 00 01  f1 ca f1 c9 23 65 95 52   ········ ····#e·R
0020  bf a2 eb 6d 50 10 04 ff  65 76 00 00               ···mP··· ev··

Transmission Control Protocol: Protocol
Packets: 136 · Displayed: 10 (7.4%) · Dropped: 0 (0.0%)    Profile: Default
```

Applying Column


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window

```
No.   Time        Source        Destination  Protocol Length Info
   64 24.180993   192.168.56.1  230.0.0.1    UDP      82 55726 → 6666 Len=50
   65 24.181119   127.0.0.1     127.0.0.1    UDP      83 55726 → 6666 Len=51
   66 25.187371   192.168.56.1  230.0.0.1    UDP      82 55726 → 6666 Len=50
   67 25.187489   127.0.0.1     127.0.0.1    UDP      83 55726 → 6666 Len=51
   68 26.189086   192.168.56.1  230.0.0.1    UDP      82 55726 → 6666 Len=50
   69 26.189219   127.0.0.1     127.0.0.1    UDP      83 55726 → 6666 Len=51
   70 27.196210   192.168.56.1  230.0.0.1    UDP      82 55726 → 6666 Len=50
   71 27.196329   127.0.0.1     127.0.0.1    UDP      83 55726 → 6666 Len=51
   72 27.949518   127.0.0.1                            61897 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   73 27.949601   127.0.0.1                            61898 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   74 27.949661   127.0.0.1                            61897 [ACK] Seq=1 Ack=1 Win=327424 Len=0
   75 27.950012   127.0.0.1                            61897 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=9
   76 27.950050   127.0.0.1                            61898 [ACK] Seq=1 Ack=10 Win=2161152 Len=0
   77 27.991237   127.0.0.1                            61898 [PSH, ACK] Seq=1 Ack=10 Win=2161152 Len=1
   78 27.991284   127.0.0.1                            61897 [ACK] Seq=10 Ack=2 Win=327424 Len=0
   79 27.992229   127.0.0.1                            61898 [FIN, ACK] Seq=2 Ack=10 Win=2161152 Len=0
   80 27.992278   127.0.0.1                            61897 [ACK] Seq=10 Ack=3 Win=327424 Len=0
   81 27.992316   127.0.0.1                            61897 [RST, ACK] Seq=10 Ack=3 Win=0 Len=0
   82 28.201623   192.168.56.1                         6666 Len=50
   83 28.201812   127.0.0.1                            6666 Len=51
   84 29.201990   192.168.56.1                         6666 Len=50

> Frame 74: 44 bytes on wire (352 bits), 44 b                   ce\NPF_Loopback,
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1
v Transmission Control Protocol, Src Port: 61                   0
    Source Port: 61898
    Destination Port: 61897
    [Stream index: 0]
  > [Conversation completeness: Complete, WI
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence
    Sequence Number (raw): 593859922
    [Next Sequence Number: 1    (relative se
    Acknowledgment Number: 1    (relative ac
    Acknowledgment number (raw): 3215125357
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (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

0000  02 00 00 00 45 00 00 28  f2 fc 40 00 80 06 00 00   ····E··( ··@·····
0010  7f 00 00 01 7f 00 00 01  f1 ca f1 c9 23 65 95 52   ········ ····#e·R
0020  bf a2 eb 6d 50 10 04 ff  65 76 00 00               ···mP··· ev··

Flags (12 bits) (tcp.flags), 2 bytes
Packets: 136 · Displayed: 136 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: ip.addr eq 127.0.0.1 and ip.addr eq 127.0.0.1 and tcp

```
No.   Time       Source         Destination   Protocol Length Flags  Info
   64 24.180993  192.168.56.1   230.0.0.1     UDP      82           55726 → 6666 Len=50
   65 24.181119  127.0.0.1      127.0.0.1     UDP      83           55726 → 6666 Len=51
   66 25.187371  192.168.56.1   230.0.0.1     UDP      82           55726 → 6666 Len=50
   67 25.187489  127.0.0.1      127.0.0.1     UDP      83           55726 → 6666 Len=51
   68 26.189086  192.168.56.1   230.0.0.1     UDP      82           55726 → 6666 Len=50
   69 26.189219  127.0.0.1      127.0.0.1     UDP      83           55726 → 6666 Len=51
   70 27.196210  192.168.56.1   230.0.0.1     UDP      82           55726 → 6666 Len=50
   71 27.196329  127.0.0.1      127.0.0.1     UDP      83           55726 → 6666 Len=51
   72 27.949518  127.0.0.1      127.0.0.1     TCP      56 0x002     61898 → 61897 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   73 27.949601  127.0.0.1      127.0.0.1     TCP      56 0x012     61897 → 61898 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
   74 27.949661  127.0.0.1      127.0.0.1     TCP      44 0x010     61898 → 61897 [ACK] Seq=1 Ack=1 Win=327424 Len=0
   75 27.950012  127.0.0.1      127.0.0.1     TCP      53 0x018     61898 → 61897 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=9
   76 27.950050  127.0.0.1      127.0.0.1     TCP      44 0x010     61897 → 61898 [ACK] Seq=1 Ack=10 Win=2161152 Len=0
   77 27.991237  127.0.0.1      127.0.0.1     TCP      45 0x018     61897 → 61898 [PSH, ACK] Seq=1 Ack=10 Win=2161152 Len=1
   78 27.991284  127.0.0.1      127.0.0.1     TCP      44 0x010     61898 → 61897 [ACK] Seq=10 Ack=2 Win=327424 Len=0
   79 27.992229  127.0.0.1      127.0.0.1     TCP      44 0x011     61897 → 61898 [FIN, ACK] Seq=2 Ack=10 Win=2161152 Len=0
   80 27.992278  127.0.0.1      127.0.0.1     TCP      44 0x010     61898 → 61897 [ACK] Seq=10 Ack=3 Win=327424 Len=0
   81 27.992316  127.0.0.1      127.0.0.1     TCP      44 0x014     61898 → 61897 [RST, ACK] Seq=10 Ack=3 Win=0 Len=0
   82 28.201623  192.168.56.1   230.0.0.1     UDP      82           55726 → 6666 Len=50
   83 28.201812  127.0.0.1      127.0.0.1     UDP      83           55726 → 6666 Len=51
   84 29.201990  192.168.56.1   230.0.0.1     UDP      82           55726 → 6666 Len=50
```

```
Frame 74: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_Loopback,
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 61898, Dst Port: 61897, Seq: 1, Ack: 1, Len: 0
    Source Port: 61898
    Destination Port: 61897
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 593859922
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3215125357
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (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
```

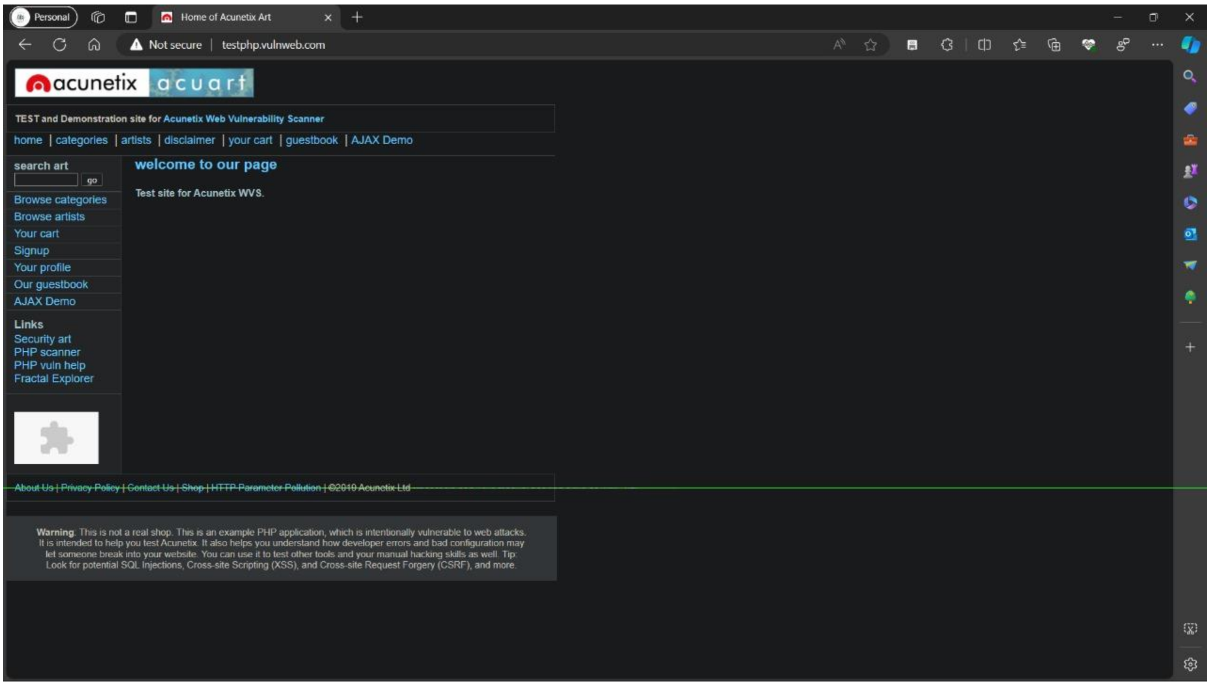
```
0000  02 00 00 00 45 00 00 28  f2 fc 40 00 80 06 00 00   ····E··( ··@·····
0010  7f 00 00 01 7f 00 00 01  f1 ca f1 c9 23 65 95 52   ········ ····#e·R
0020  bf a2 eb 6d 50 10 04 ff  65 76 00 00               ···mP··· ev··
```

Flags (12 bits) (tcp.flags), 2 bytes

Packets: 136 · Displayed: 136 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Capturing HTTP

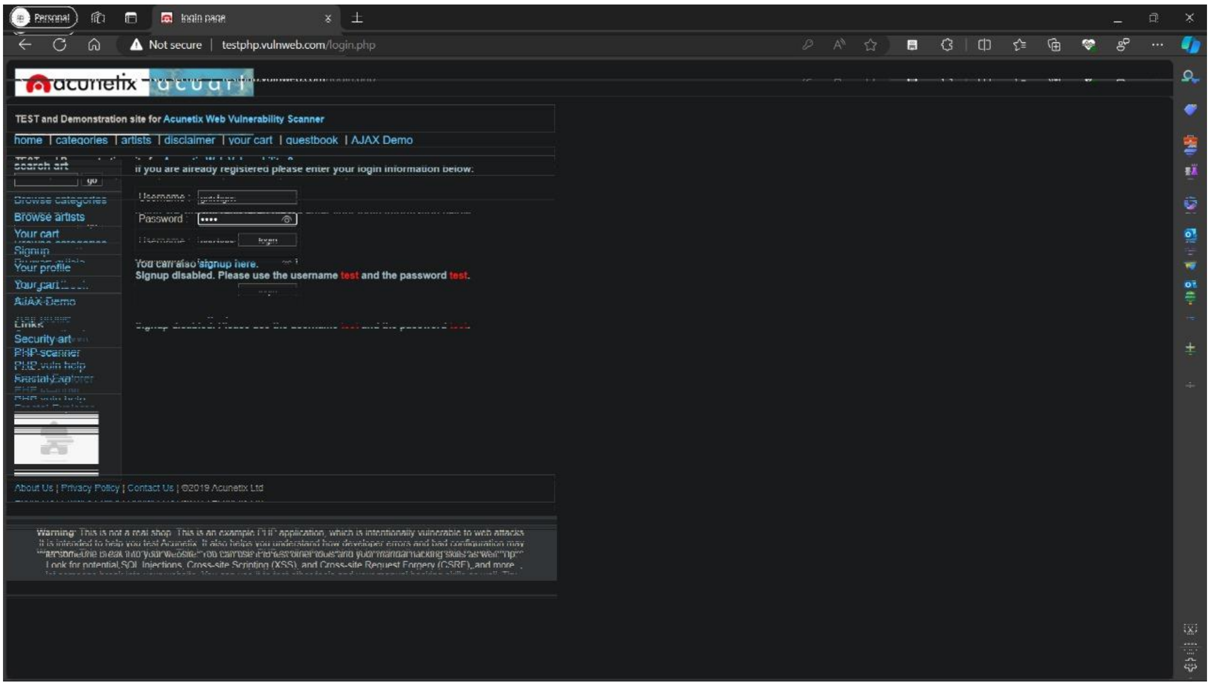


TEST and Demonstration site for Acunetix Web Vulnerability Scanner

welcome to our page

Test site for Acunetix WVS.

Warning. This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

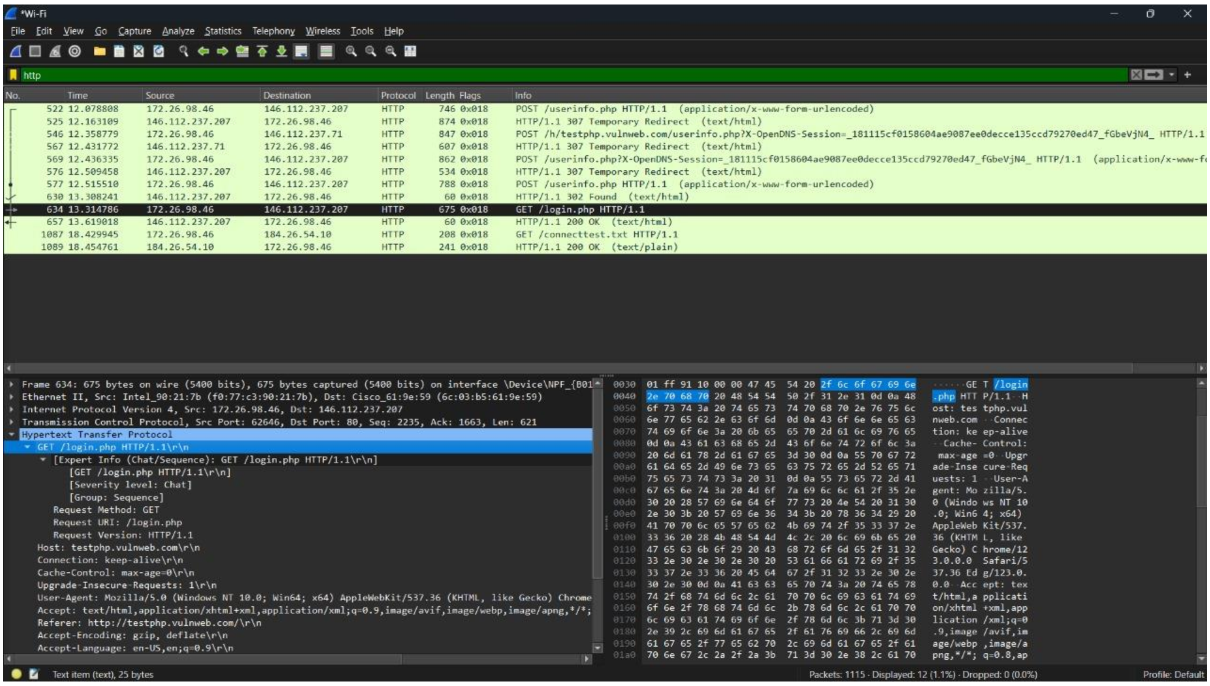
If you are already registered please enter your login information below:

Username :

Password : ••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.


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

```
http
```

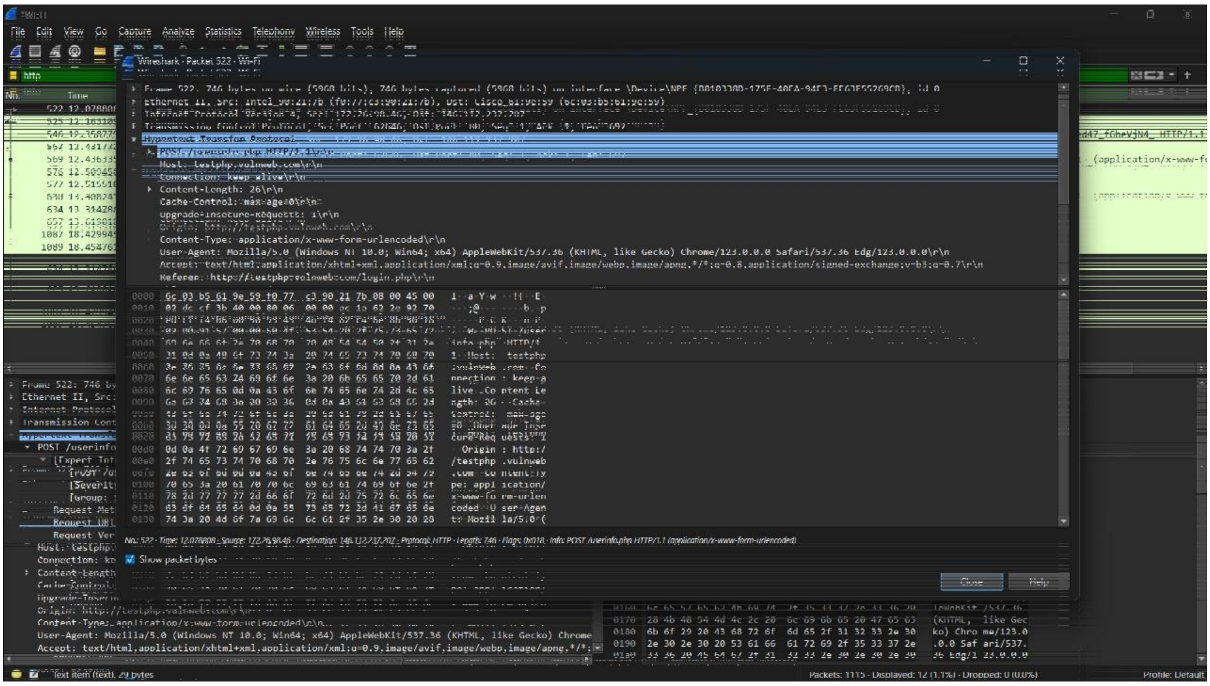
```
No.    Time       Source           Destination      Protocol Length Flags  Info
 522 12.078808  172.26.98.46     146.112.237.207  HTTP      746 0x018  POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 525 12.163109  146.112.237.207  172.26.98.46     HTTP      874 0x018  HTTP/1.1 307 Temporary Redirect  (text/html)
 546 12.358779  172.26.98.46     146.112.237.71   HTTP      847 0x018  POST /h/testphp.vulnweb.com/userinfo.php?X-OpenDNS-Session=_181115cf0158604ae9087ee0decce135ccd79270ed47_fGbeVjN4_ HTTP/1.1
 567 12.431772  146.112.237.71   172.26.98.46     HTTP      607 0x018  HTTP/1.1 307 Temporary Redirect  (text/html)
 569 12.436335  172.26.98.46     146.112.237.207  HTTP      862 0x018  POST /userinfo.php?X-OpenDNS-Session=_181115cf0158604ae9087ee0decce135ccd79270ed47_fGbeVjN4_ HTTP/1.1  (application/x-www-f
 576 12.509458  146.112.237.207  172.26.98.46     HTTP      534 0x018  HTTP/1.1 307 Temporary Redirect  (text/html)
 577 12.515510  172.26.98.46     146.112.237.207  HTTP      788 0x018  POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 630 13.308241  146.112.237.207  172.26.98.46     HTTP       60 0x018  HTTP/1.1 302 Found  (text/html)
 634 13.314786  172.26.98.46     146.112.237.207  HTTP      675 0x018  GET /login.php HTTP/1.1
 657 13.619018  146.112.237.207  172.26.98.46     HTTP       60 0x018  HTTP/1.1 200 OK  (text/html)
1087 18.429945  172.26.98.46     184.26.54.10     HTTP      208 0x018  GET /connecttest.txt HTTP/1.1
1089 18.454761  184.26.54.10     172.26.98.46     HTTP      241 0x018  HTTP/1.1 200 OK  (text/plain)
```

```
Frame 634: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits) on interface \Device\NPF_{B01
Ethernet II, Src: Intel_90:21:7b (f0:77:c3:90:21:7b), Dst: Cisco_61:9e:59 (6c:03:b5:61:9e:59)
Internet Protocol Version 4, Src: 172.26.98.46, Dst: 146.112.237.207
Transmission Control Protocol, Src Port: 62646, Dst Port: 80, Seq: 2235, Ack: 1663, Len: 621
Hypertext Transfer Protocol
  GET /login.php HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /login.php HTTP/1.1\r\n]
      [GET /login.php HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /login.php
    Request Version: HTTP/1.1
  Host: testphp.vulnweb.com\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
  Referer: http://testphp.vulnweb.com/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
```

```
0030  01 ff 91 10 00 00 47 45  54 20 2f 6c 6f 67 69 6e   ······GE T /login
0040  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0050  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0060  6e 77 65 62 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nweb.com ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 43 61 63 68 65 2d  43 6f 6e 74 72 6f 6c 3a   ··Cache- Control:
0090  20 6d 61 78 2d 61 67 65  3d 30 0d 0a 55 70 67 72    max-age =0··Upgr
00a0  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
00b0  75 65 73 74 73 3a 20 31  0d 0a 55 73 65 72 2d 41   uests: 1 ··User-A
00c0  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00d0  30 20 28 57 69 6e 64 6f  77 73 20 4e 54 20 31 30   0 (Windo ws NT 10
00e0  2e 30 3b 20 57 69 6e 36  34 3b 20 78 36 34 29 20   .0; Win6 4; x64) 
00f0  41 70 70 6c 65 57 65 62  4b 69 74 2f 35 33 37 2e   AppleWeb Kit/537.
0100  33 36 20 28 4b 48 54 4d  4c 2c 20 6c 69 6b 65 20   36 (KHTM L, like 
0110  47 65 63 6b 6f 29 20 43  68 72 6f 6d 65 2f 31 32   Gecko) C hrome/12
0120  33 2e 30 2e 30 2e 30 20  53 61 66 61 72 69 2f 35   3.0.0.0  Safari/5
0130  33 37 2e 33 36 20 45 64  67 2f 31 32 33 2e 30 2e   37.36 Ed g/123.0.
0140  30 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   0.0··Acc ept: tex
0150  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
0160  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
0170  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
0180  2e 39 2c 69 6d 61 67 65  2f 61 76 69 66 2c 69 6d   .9,image /avif,im
0190  61 67 65 2f 77 65 62 70  2c 69 6d 61 67 65 2f 61   age/webp ,image/a
01a0  70 6e 67 2c 2a 2f 2a 3b  71 3d 30 2e 38 2c 61 70   png,*/*; q=0.8,ap
```

Text item (text), 25 bytes

Packets: 1115 · Displayed: 12 (1.1%) · Dropped: 0 (0.0%)


Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 522 · Wi-Fi
Show packet bytes
Close
Help

```
Frame 522: 746 bytes on wire (5968 bits), 746 bytes captured (5968 bits) on interface \Device\NPF_{D010130D-175E-40FA-94F3-EEG3E55269CD}, id 0
Ethernet II, Src: Intel_90:21:7b (f0:77:c3:90:21:7b), Dst: Cisco_61:9e:59 (6c:03:b5:61:9e:59)
Internet Protocol Version 4, Src: 172.26.98.46, Dst: 146.112.237.207
Transmission Control Protocol, Src Port: 62646, Dst Port: 80, Seq: 1, Ack: 1, Len: 692
Hypertext Transfer Protocol
  POST /userinfo.php HTTP/1.1\r\n
  Host: testphp.vulnweb.com\r\n
  Connection: keep-alive\r\n
  Content-Length: 26\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Origin: http://testphp.vulnweb.com\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  Referer: http://testphp.vulnweb.com/login.php\r\n
```

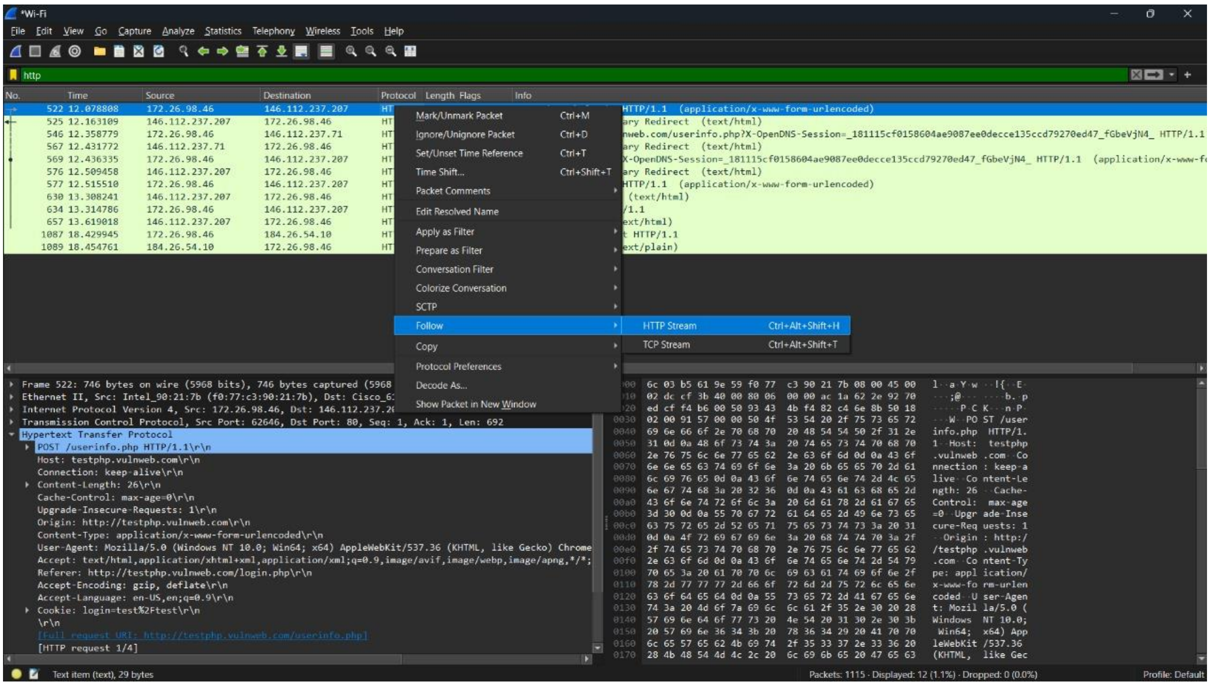
```
0000  6c 03 b5 61 9e 59 f0 77  c3 90 21 7b 08 00 45 00   l·a·Y·w ··!{··E·
0010  02 dc cf 3b 40 00 80 06  00 00 ac 1a 62 2e 92 70   ···;@··· ····b.·p
[illegible]
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 36  0d 0a 43 61 63 68 65 2d   ngth: 36 ··Cache-
```

No.: 522 · Time: 12.078808 · Source: 172.26.98.46 · Destination: 146.112.237.207 · Protocol: HTTP · Length: 746 · Flags: 0x010 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Text item (text), 29 bytes

Packets: 1115 · Displayed: 12 (1.1%) · Dropped: 0 (0.0%)

Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
HTTP Stream Ctrl+Alt+Shift+H
TCP Stream Ctrl+Alt+Shift+T

```
No.     Time         Source           Destination      Protocol  Length  Flags  Info
   522 12.078808    172.26.98.46     146.112.237.207  HT   HTTP/1.1  (application/x-www-form-urlencoded)
   525 12.163109    146.112.237.207  172.26.98.46     HT   ary Redirect  (text/html)
   546 12.358779    172.26.98.46     146.112.237.71   HT   nweb.com/userinfo.php?X-OpenDNS-Session=_181115cf0158604ae9087ee0decce135ccd79270ed47_fGbeVjN4_ HTTP/1.1
   567 12.431772    146.112.237.71   172.26.98.46     HT   ary Redirect  (text/html)
   569 12.436335    172.26.98.46     146.112.237.207  HT   X-OpenDNS-Session=_181115cf0158604ae9087ee0decce135ccd79270ed47_fGbeVjN4_ HTTP/1.1  (application/x-www-f
   576 12.509458    146.112.237.207  172.26.98.46     HT   ary Redirect  (text/html)
   577 12.515510    172.26.98.46     146.112.237.207  HT   HTTP/1.1  (application/x-www-form-urlencoded)
   630 13.308241    146.112.237.207  172.26.98.46     HT    (text/html)
   634 13.314786    172.26.98.46     146.112.237.207  HT   /1.1
   657 13.619018    146.112.237.207  172.26.98.46     HT   ext/html)
  1087 18.429945    172.26.98.46     184.26.54.10     HT   t HTTP/1.1
  1089 18.454761    184.26.54.10     172.26.98.46     HT   ext/plain)
```

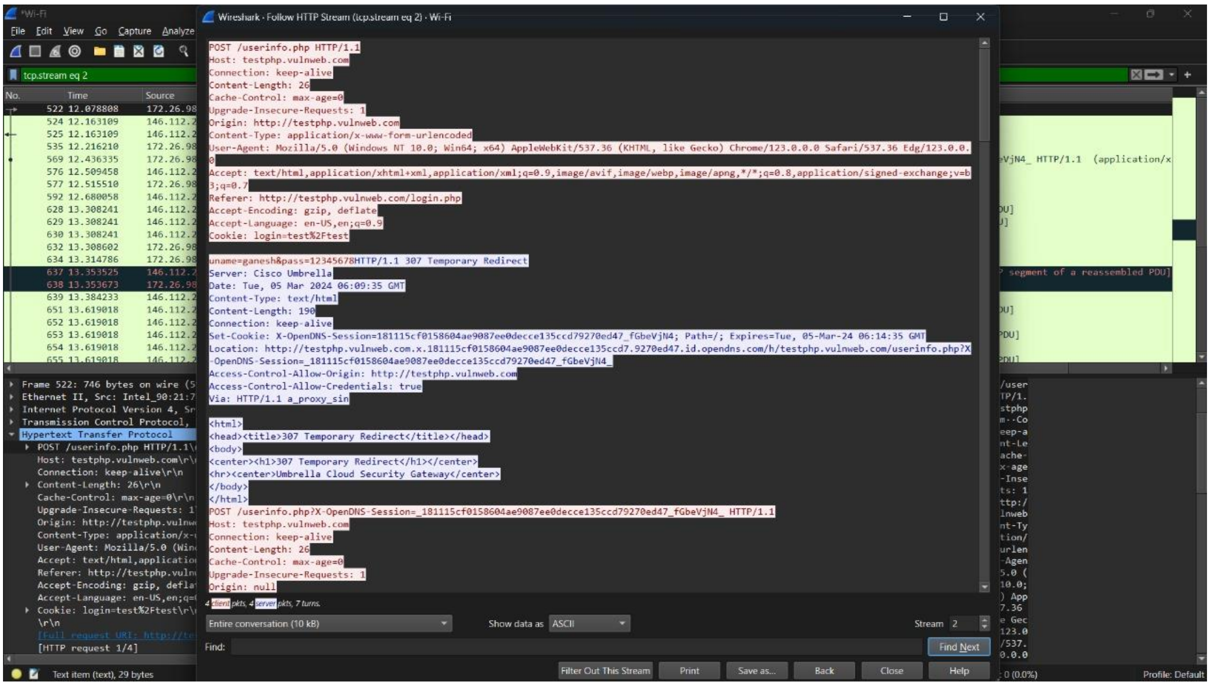
```
Frame 522: 746 bytes on wire (5968 bits), 746 bytes captured (5968
Ethernet II, Src: Intel_90:21:7b (f0:77:c3:90:21:7b), Dst: Cisco_61
Internet Protocol Version 4, Src: 172.26.98.46, Dst: 146.112.237.20
Transmission Control Protocol, Src Port: 62646, Dst Port: 80, Seq: 1, Ack: 1, Len: 692
Hypertext Transfer Protocol
  POST /userinfo.php HTTP/1.1\r\n
  Host: testphp.vulnweb.com\r\n
  Connection: keep-alive\r\n
  Content-Length: 26\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Origin: http://testphp.vulnweb.com\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
  Referer: http://testphp.vulnweb.com/login.php\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  Cookie: login=test%2Ftest\r\n
  \r\n
  [Full request URI: http://testphp.vulnweb.com/userinfo.php]
  [HTTP request 1/4]
```

```
0000  6c 03 b5 61 9e 59 f0 77  c3 90 21 7b 08 00 45 00   l·a·Y·w ··!{··E·
0010  02 dc cf 3b 40 00 80 06  00 00 ac 1a 62 2e 92 70   ···;@··· ····b.·p
0020  ed cf f4 b6 00 50 93 43  4b f4 82 c4 6e 8b 50 18   ·····P·C K···n·P·
0030  02 00 91 57 00 00 50 4f  53 54 20 2f 75 73 65 72   ···W··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 36  0d 0a 43 61 63 68 65 2d   ngth: 26 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ··Origin : http:/
00e0  2f 74 65 73 74 70 68 70  2e 76 75 6c 6e 77 65 62   /testphp .vulnweb
00f0  2e 63 6f 6d 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   .com··Co ntent-Ty
0100  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: appl ication/
0110  78 2d 77 77 77 2d 66 6f  72 6d 2d 75 72 6c 65 6e   x-www-fo rm-urlen
0120  63 6f 64 65 64 0d 0a 55  73 65 72 2d 41 67 65 6e   coded··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0150  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0160  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36
0170  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
```

Text item (text), 29 bytes

Packets: 1115 · Displayed: 12 (1.1%) · Dropped: 0 (0.0%)

Profile: Default

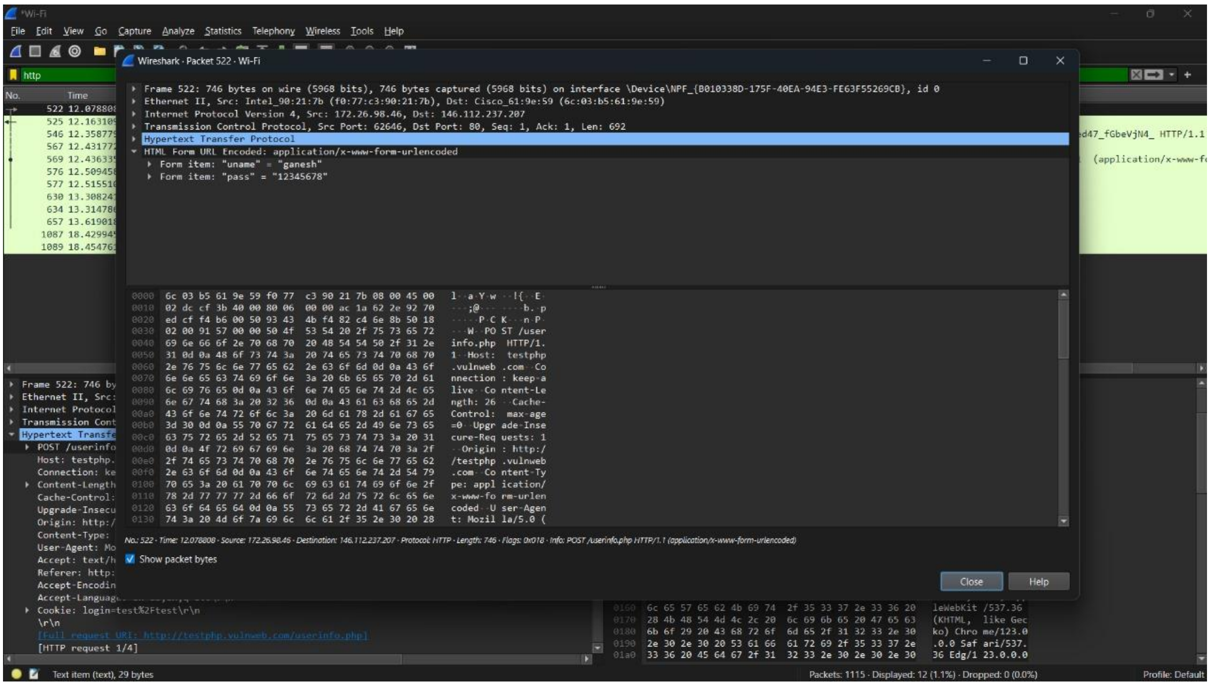


```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 26
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.
0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: login=test%2Ftest

uname=ganesh&pass=12345678HTTP/1.1 307 Temporary Redirect
Server: Cisco Umbrella
Date: Tue, 05 Mar 2024 06:09:35 GMT
Content-Type: text/html
Content-Length: 190
Connection: keep-alive
Set-Cookie: X-OpenDNS-Session=181115cf0158604ae9087ee0decce135ccd79270ed47_fGbeVjN4; Path=/; Expires=Tue, 05-Mar-24 06:14:35 GMT
Location: http://testphp.vulnweb.com.x.181115cf0158604ae9087ee0decce135ccd7.9270ed47.id.opendns.com/h/testphp.vulnweb.com/userinfo.php?X
-OpenDNS-Session=_181115cf0158604ae9087ee0decce135ccd79270ed47_fGbeVjN4_
Access-Control-Allow-Origin: http://testphp.vulnweb.com
Access-Control-Allow-Credentials: true
Via: HTTP/1.1 a_proxy_sin

<html>
<head><title>307 Temporary Redirect</title></head>
<body>
<center><h1>307 Temporary Redirect</h1></center>
<hr><center>Umbrella Cloud Security Gateway</center>
</body>
</html>
POST /userinfo.php?X-OpenDNS-Session=_181115cf0158604ae9087ee0decce135ccd79270ed47_fGbeVjN4_ HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 26
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
```

4 client pkts, 4 server pkts, 7 turns.

Entire conversation (10 kB) Show data as ASCII Stream 2

Find:



```
▸ Frame 522: 746 bytes on wire (5968 bits), 746 bytes captured (5968 bits) on interface \Device\NPF_{B010338D-175F-40EA-94E3-FE63F55269CB}, id 0
▸ Ethernet II, Src: Intel_90:21:7b (f0:77:c3:90:21:7b), Dst: Cisco_61:9e:59 (6c:03:b5:61:9e:59)
▸ Internet Protocol Version 4, Src: 172.26.98.46, Dst: 146.112.237.207
▸ Transmission Control Protocol, Src Port: 62646, Dst Port: 80, Seq: 1, Ack: 1, Len: 692
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "uname" = "ganesh"
  ▸ Form item: "pass" = "12345678"
```

```
0000  6c 03 b5 61 9e 59 f0 77  c3 90 21 7b 08 00 45 00   l··a·Y·w ··!{··E·
0010  02 dc cf 3b 40 00 80 06  00 00 ac 1a 62 2e 92 70   ···;@··· ····b.·p
0020  ed cf f4 b6 00 50 93 43  4b f4 82 c4 6e 8b 50 18   ·····P·C K···n·P·
0030  02 00 91 57 00 00 50 4f  53 54 20 2f 75 73 65 72   ···W··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 36  0d 0a 43 61 63 68 65 2d   ngth: 26 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ··Origin : http:/
00e0  2f 74 65 73 74 70 68 70  2e 76 75 6c 6e 77 65 62   /testphp .vulnweb
00f0  2e 63 6f 6d 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   .com··Co ntent-Ty
0100  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: appl ication/
0110  78 2d 77 77 77 2d 66 6f  72 6d 2d 75 72 6c 65 6e   x-www-fo rm-urlen
0120  63 6f 64 65 64 0d 0a 55  73 65 72 2d 41 67 65 6e   coded··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
```

No.: 522 · Time: 12.078808 · Source: 172.26.98.46 · Destination: 146.112.237.207 · Protocol: HTTP · Length: 746 · Flags: 0x018 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

☑ Show packet bytes

Packets: 1115 · Displayed: 12 (1.1%) · Dropped: 0 (0.0%)