Date: July 26, 2024
DRN: ECPPT0002
Prepared By: Siddique Reza Khan

Comprehensive Overview and Fundamental Usage of Wireshark

Introduction

Wireshark is a powerful network traffic analyzer used for detecting and troubleshooting network problems, identifying security anomalies, and investigating protocol details. This tool allows analysts to capture and interactively browse the traffic running on a computer network. Below is a detailed guide on its usage, interface, and functionalities.

Use Cases

1. **Detecting and Troubleshooting Network Issues:**
   - Identifying network load failure points.
   - Detecting congestion and other network inefficiencies.
2. **Security Anomaly Detection:**
   - Identifying rogue hosts.
   - Spotting abnormal port usage.
   - Analyzing suspicious traffic patterns.
3. **Protocol Analysis and Learning:**
   - Investigating protocol response codes.
   - Examining payload data.

Note: Wireshark is not an Intrusion Detection System (IDS) and does not modify packets; it only reads them. Analysts must use their expertise to discover and investigate anomalies.

Wireshark GUI Overview

Wireshark's graphical user interface (GUI) is designed for ease of use, with multiple sections for comprehensive traffic analysis:

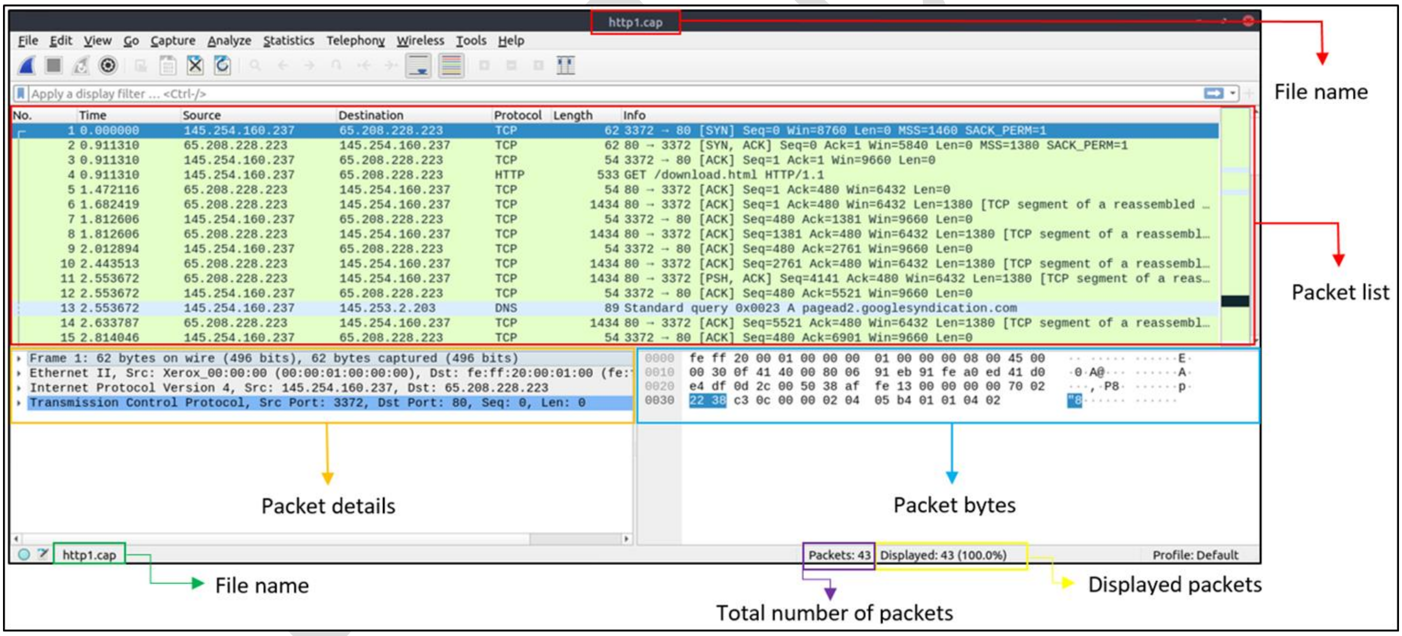
1. **Toolbar:**
   - Contains menus and shortcuts for packet sniffing, processing, filtering, sorting, summarizing, exporting, and merging.
2. **Display Filter Bar:**
   - The main section for querying and filtering network data.
3. **Recent Files:**
   - A list of recently investigated files for quick access.

4. **Capture Filter and Interfaces:**
   - Lists capture filters and available network interfaces (e.g., lo, eth0, ens33).
5. **Status Bar:**
   - Displays tool status, active profile, and numeric packet information.

Loading PCAP Files

To analyze packets, you can load PCAP files into Wireshark through the "File" menu, by dragging and dropping, or by double-clicking the file. The loaded file will display detailed packet information, split into three panes:

1. **Packet List Pane:**
   - Summarizes each packet (source, destination, protocol, and info).
   - Selecting a packet displays its details in the other panes.
2. **Packet Details Pane:**
   - Breaks down the selected packet's protocol details.
3. **Packet Bytes Pane:**
   - Displays the selected packet in hexadecimal and ASCII formats, highlighting fields based on the details pane selection.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	145.254.160.237	65.208.228.223	TCP	62	3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
2	0.911310	65.208.228.223	145.254.160.237	TCP	62	80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
3	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
5	1.472116	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled …
7	1.812606	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8	1.812606	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
9	2.012894	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10	2.443513	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
11	2.553672	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segment of a reas…
12	2.553672	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13	2.553672	145.254.160.237	145.253.2.203	DNS	89	Standard query 0x0023 A pagead2.googlesyndication.com
14	2.633787	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
15	2.814046	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0

```
› Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
› Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:
› Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
› Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   ·· ······ ······E·
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   ·0·A@··· ······A·
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ···,·P8· ······p·
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8······ ······
```

Colouring Packets

Wireshark uses packet coloring to help analysts quickly identify anomalies and protocols.

- **Temporary Rules:**
  - Available only during the current session.
- **Permanent Rules:**

  - Saved under the profile for future sessions.

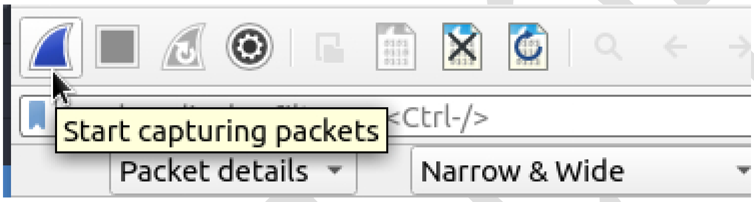
To create or manage coloring rules, use the right-click menu or navigate to "View --> Coloring Rules."

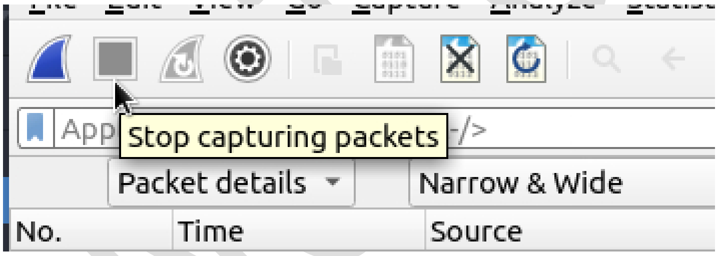
Traffic Sniffing

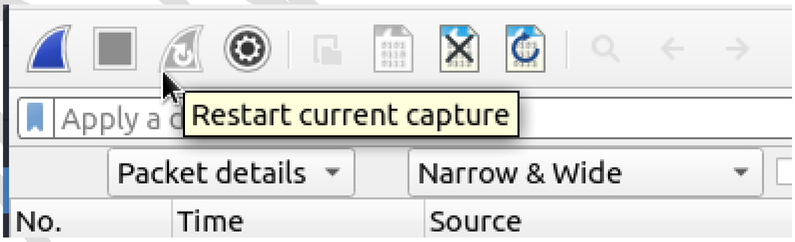
Wireshark can start and stop traffic capture using toolbar buttons:

- **Blue Shark Button:** Starts sniffing.
- **Red Button:** Stops sniffing.
- **Green Button:** Restarts sniffing.

The status bar will show the active interface and the number of collected packets.







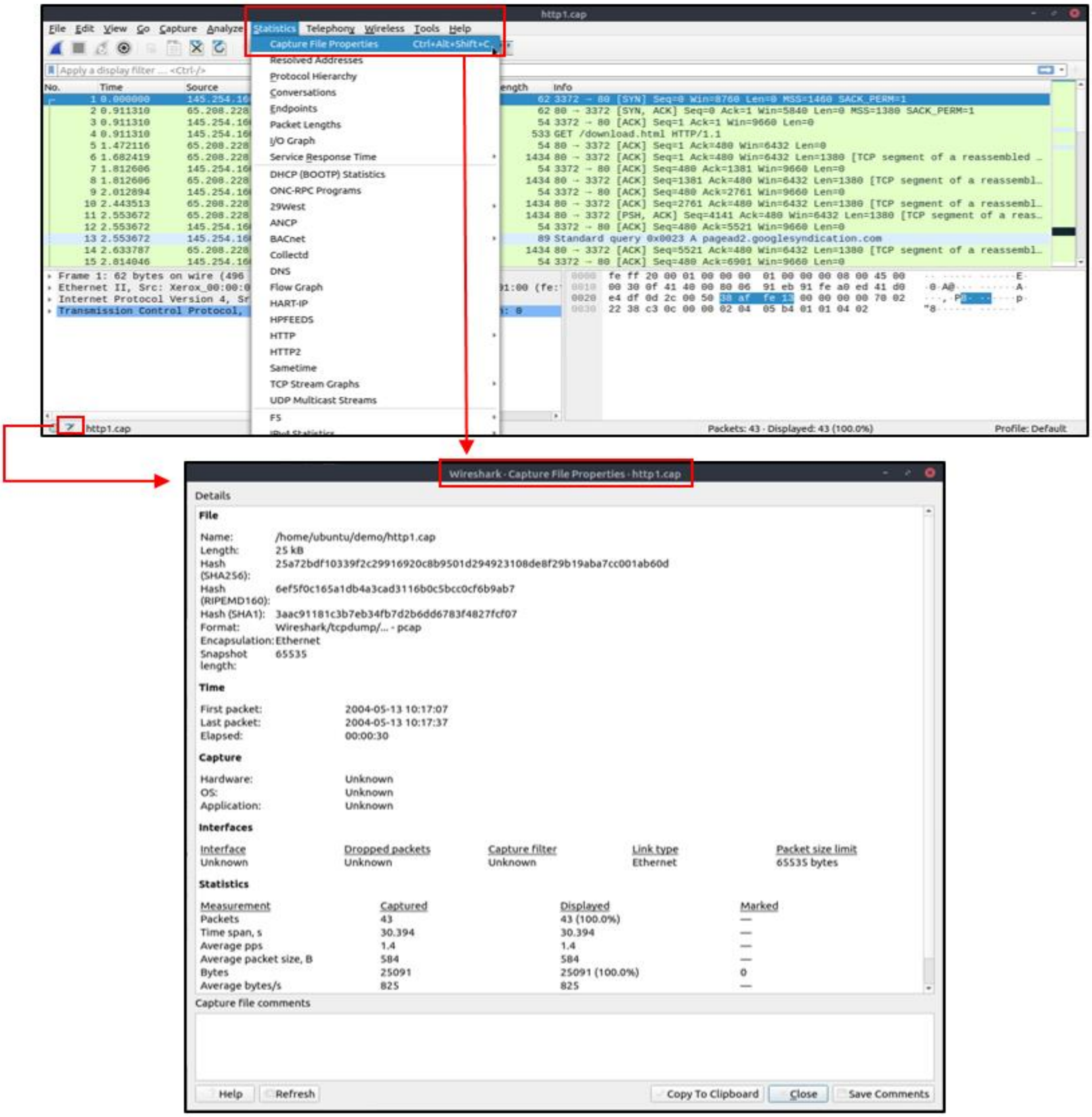
Merging PCAP Files

Wireshark allows merging two PCAP files into one via "File --> Merge." This function is useful for consolidating data from multiple captures.

Viewing File Details

To view detailed information about a capture file (such as hash, capture time, comments, interface, and statistics):

- Navigate to "Statistics --> Capture File Properties."
- Click the "PCAP icon" at the bottom left of the window.



```
No.  Time        Source        ength  Info
  1 0.000000   145.254.16       62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
  2 0.911310   65.208.228       62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
  3 0.911310   145.254.16       54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
  4 0.911310   145.254.16      533 GET /download.html HTTP/1.1
  5 1.472116   65.208.228       54 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
  6 1.682419   65.208.228     1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled …
  7 1.812606   145.254.16       54 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
  8 1.812606   65.208.228     1434 80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
  9 2.012894   145.254.16       54 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
 10 2.443513   65.208.228     1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
 11 2.553672   65.208.228     1434 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segment of a reas…
 12 2.553672   145.254.16       54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
 13 2.553672   145.254.16       89 Standard query 0x0023 A pagead2.googlesyndication.com
 14 2.633787   65.208.228     1434 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
 15 2.814046   145.254.16       54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0

› Frame 1: 62 bytes on wire (496
› Ethernet II, Src: Xerox_00:00:0        01:00 (fe:
› Internet Protocol Version 4, Sr
› Transmission Control Protocol,         : 0

0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   ··············E·
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   ·0·A@·········A·
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ···,·P8·······p·
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8············
```

Wireshark · Capture File Properties · http1.cap

Details

File

Name: /home/ubuntu/demo/http1.cap
Length: 25 kB
Hash (SHA256): 25a72bdf10339f2c29916920c8b9501d294923108de8f29b19aba7cc001ab60d
Hash (RIPEMD160): 6ef5f0c165a1db4a3cad3116b0c5bcc0cf6b9ab7
Hash (SHA1): 3aac91181c3b7eb34fb7d2b6dd6783f4827fcf07
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Snapshot length: 65535

Time

First packet: 2004-05-13 10:17:07
Last packet: 2004-05-13 10:17:37
Elapsed: 00:00:30

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	43	43 (100.0%)	—
Time span, s	30.394	30.394	—
Average pps	1.4	1.4	—
Average packet size, B	584	584	—
Bytes	25091	25091 (100.0%)	0
Average bytes/s	825	825	—

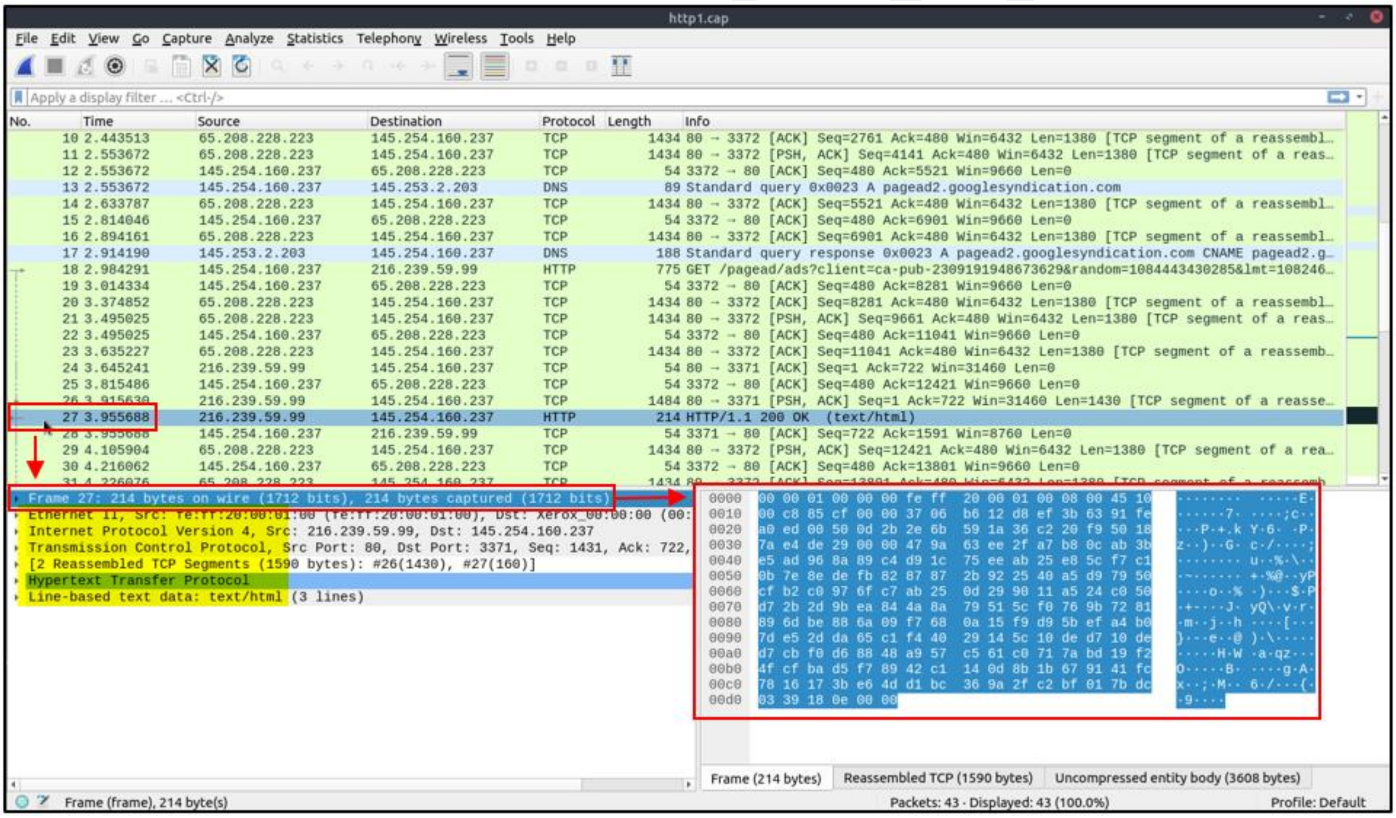
Capture file comments

Packet Dissection

Packet dissection, also known as protocol dissection, involves investigating packet details by decoding available protocols and fields. Wireshark supports a wide range of protocols for dissection and allows users to write custom dissection scripts.

Packets in Wireshark are broken down according to the OSI model, typically consisting of 5 to 7 layers:

1. **Frame (Layer 1):** Shows frame/packet details specific to the Physical layer.
2. **Source [MAC] (Layer 2):** Displays source and destination MAC addresses from the Data Link layer.
3. **Source [IP] (Layer 3):** Shows source and destination IPv4 addresses from the Network layer.
4. **Protocol (Layer 4):** Details protocol used (UDP/TCP), source, and destination ports from the Transport layer.
5. **Protocol Errors:** Continuation of Layer 4 showing specific TCP segments needing reassembly.
6. **Application Protocol (Layer 5):** Details specific to the protocol used, such as HTTP, FTP, SMB, from the Application layer.
7. **Application Data:** Extension of Layer 5 showing application-specific data.


http1.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
   10 2.443513   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
   11 2.553672   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segment of a reas…
   12 2.553672   145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
   13 2.553672   145.254.160.237  145.253.2.203    DNS        89 Standard query 0x0023 A pagead2.googlesyndication.com
   14 2.633787   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
   15 2.814046   145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
   16 2.894161   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
   17 2.914190   145.253.2.203    145.254.160.237  DNS       188 Standard query response 0x0023 A pagead2.googlesyndication.com CNAME pagead2.g…
   18 2.984291   145.254.160.237  216.239.59.99    HTTP      775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=108246…
   19 3.014334   145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
   20 3.374852   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
   21 3.495025   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [PSH, ACK] Seq=9661 Ack=480 Win=6432 Len=1380 [TCP segment of a reas…
   22 3.495025   145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 Len=0
   23 3.635227   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=11041 Ack=480 Win=6432 Len=1380 [TCP segment of a reassemb…
   24 3.645241   216.239.59.99    145.254.160.237  TCP        54 80 → 3371 [ACK] Seq=1 Ack=722 Win=31460 Len=0
   25 3.815486   145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=12421 Win=9660 Len=0
   26 3.915630   216.239.59.99    145.254.160.237  TCP      1484 80 → 3371 [PSH, ACK] Seq=1 Ack=722 Win=31460 Len=1430 [TCP segment of a reasse…
   27 3.955688   216.239.59.99    145.254.160.237  HTTP      214 HTTP/1.1 200 OK  (text/html)
   28 3.955688   145.254.160.237  216.239.59.99    TCP        54 3371 → 80 [ACK] Seq=722 Ack=1591 Win=8760 Len=0
   29 4.105904   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [PSH, ACK] Seq=12421 Ack=480 Win=6432 Len=1380 [TCP segment of a rea…
   30 4.216062   145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=13801 Win=9660 Len=0
   31 4.226076   65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=13801 Ack=480 Win=6432 Len=1380 [TCP segment of a reassemb…
```

```
▸ Frame 27: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
▸ Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:
▸ Internet Protocol Version 4, Src: 216.239.59.99, Dst: 145.254.160.237
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 3371, Seq: 1431, Ack: 722,
▸ [2 Reassembled TCP Segments (1590 bytes): #26(1430), #27(160)]
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (3 lines)
```

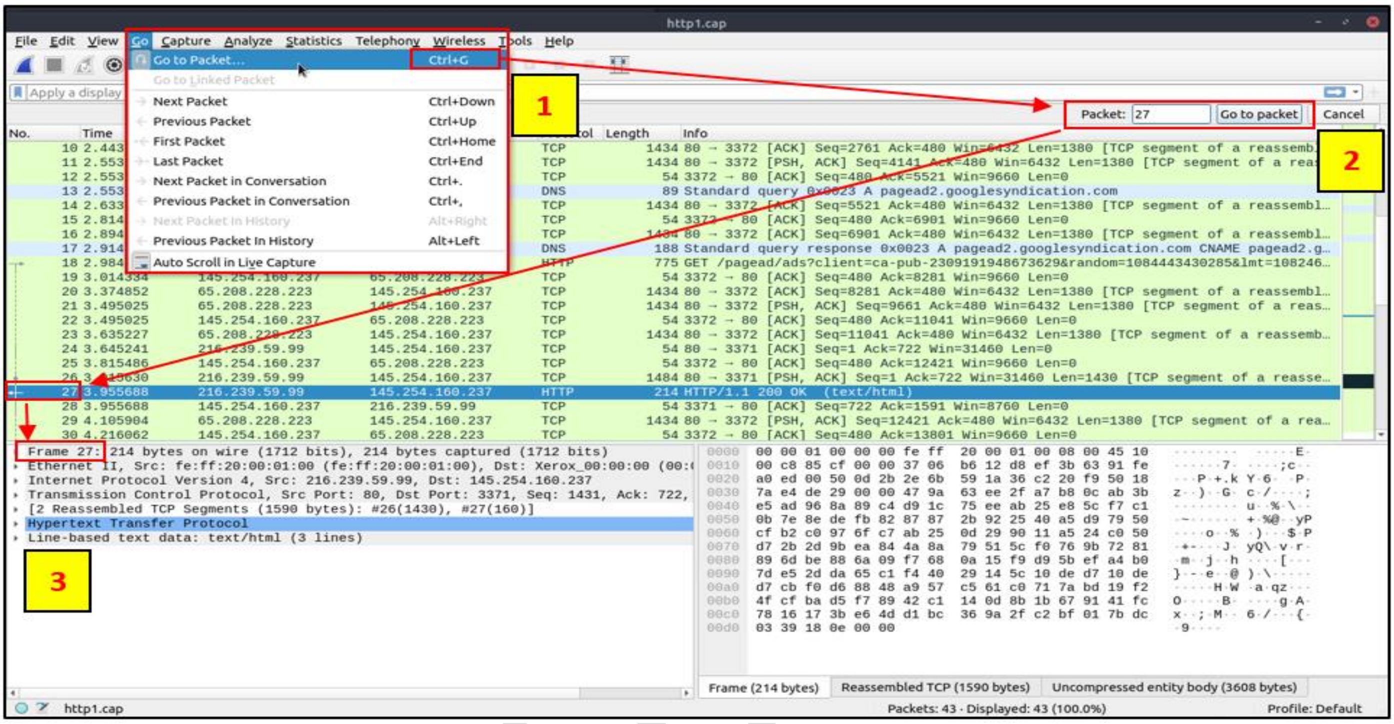
```
0000  00 00 01 00 00 00 fe ff  20 00 01 00 08 00 45 10   ········ ······E·
0010  00 c8 85 cf 00 00 37 06  b6 12 d8 ef 3b 63 91 fe   ······7· ····;c··
0020  a0 ed 00 50 0d 2b 2e 6b  59 1a 36 c2 20 f9 50 18   ···P·+.k Y·6· ·P·
0030  7a e4 de 29 00 00 47 9a  63 ee 2f a7 b8 0c ab 3b   z··)··G· c·/····;
0040  e5 ad 96 8a 89 c4 d9 1c  75 ee ab 25 e8 5c f7 c1   ········ u··%·\··
0050  0b 7e 8e de fb 82 87 87  2b 92 25 40 a5 d9 79 50   ·~······ +·%@··yP
0060  cf b2 c0 97 6f c7 ab 25  0d 29 90 11 a5 24 c0 50   ····o··% ·)···$·P
0070  d7 2b 2d 9b ea 84 4a 8a  79 51 5c f0 76 9b 72 81   ·+-···J· yQ\·v·r·
0080  89 6d be 88 6a 09 f7 68  0a 15 f9 d9 5b ef a4 b0   ·m··j··h ····[···
0090  7d e5 2d da 65 c1 f4 40  29 14 5c 10 de d7 10 de   }·-·e··@ )·\·····
00a0  d7 cb f0 d6 88 48 a9 57  c5 61 c0 71 7a bd 19 f2   ·····H·W ·a·qz···
00b0  4f cf ba d5 f7 89 42 c1  14 0d 8b 1b 67 91 41 fc   O·····B· ····g·A·
00c0  78 16 17 3b e6 4d d1 bc  36 9a 2f c2 bf 01 7b dc   x··;·M·· 6·/···{·
00d0  03 39 18 0e 00 00                                  ·9····
```

Frame (214 bytes)
Reassembled TCP (1590 bytes)
Uncompressed entity body (3608 bytes)
Frame (frame), 214 byte(s)
Packets: 43 · Displayed: 43 (100.0%)
Profile: Default

Packet Navigation

Wireshark offers several features to facilitate the navigation and analysis of packets in large captures:

1. **Packet Numbers:**
   - Each packet is assigned a unique number for easy reference and navigation.
2. **Go to Packet:**
   - Navigate between packets using the "Go" menu or toolbar.

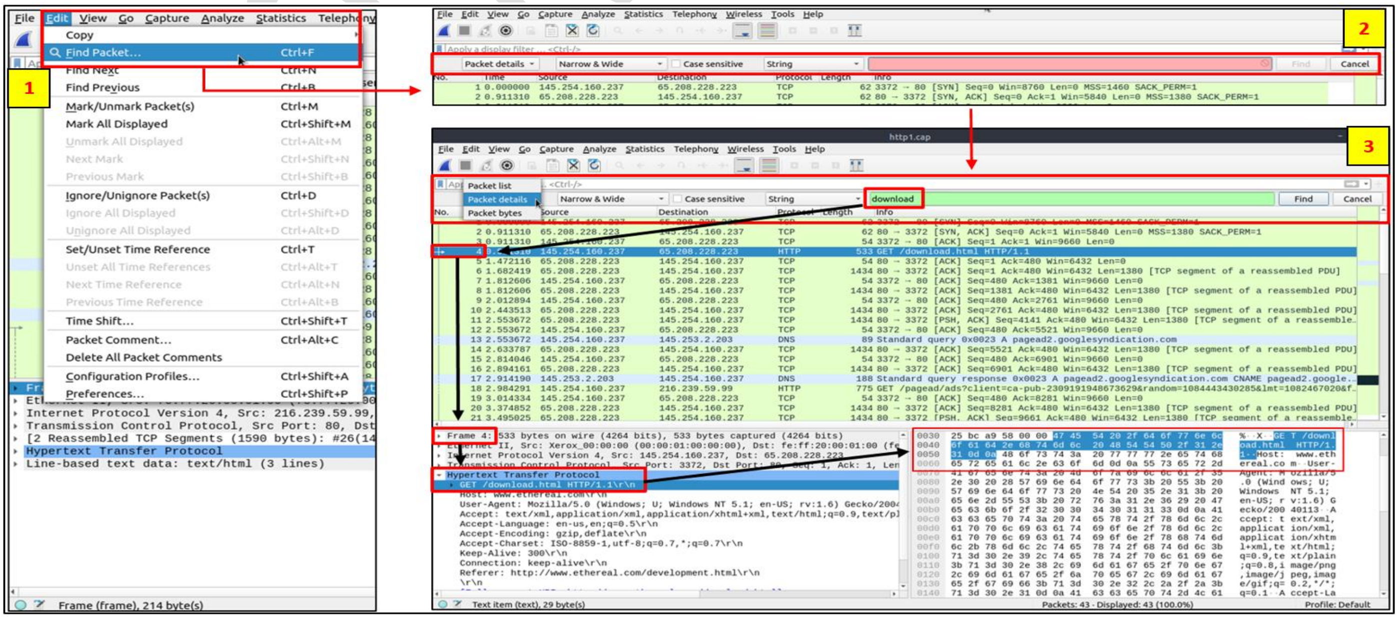

http1.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Go to Packet... Ctrl+G
Go to Linked Packet
Next Packet Ctrl+Down
Previous Packet Ctrl+Up
First Packet Ctrl+Home
Last Packet Ctrl+End
Next Packet in Conversation Ctrl+.
Previous Packet in Conversation Ctrl+,
Next Packet In History Alt+Right
Previous Packet In History Alt+Left
Auto Scroll in Live Capture
Apply a display
Packet: 27
Go to packet
Cancel
1
2
3
Frame (214 bytes)
Reassembled TCP (1590 bytes)
Uncompressed entity body (3608 bytes)
http1.cap
Packets: 43 · Displayed: 43 (100.0%)
Profile: Default

```
No.  Time                                                     Protocol Length Info
  10 2.443                                                    TCP     1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment of a reassemb…
  11 2.553                                                    TCP     1434 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segment of a rea…
  12 2.553                                                    TCP       54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
  13 2.553                                                    DNS       89 Standard query 0x0023 A pagead2.googlesyndication.com
  14 2.633                                                    TCP     1434 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
  15 2.814                                                    TCP       54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
  16 2.894                                                    TCP     1434 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
  17 2.914                                                    DNS      188 Standard query response 0x0023 A pagead2.googlesyndication.com CNAME pagead2.g…
  18 2.984                                                    HTTP     775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=108246…
  19 3.014334  145.254.160.237  65.208.228.223                TCP       54 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
  20 3.374852  65.208.228.223   145.254.160.237               TCP     1434 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembl…
  21 3.495025  65.208.228.223   145.254.160.237               TCP     1434 80 → 3372 [PSH, ACK] Seq=9661 Ack=480 Win=6432 Len=1380 [TCP segment of a reas…
  22 3.495025  145.254.160.237  65.208.228.223                TCP       54 3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 Len=0
  23 3.635227  65.208.228.223   145.254.160.237               TCP     1434 80 → 3372 [ACK] Seq=11041 Ack=480 Win=6432 Len=1380 [TCP segment of a reassemb…
  24 3.645241  216.239.59.99    145.254.160.237               TCP       54 80 → 3371 [ACK] Seq=1 Ack=722 Win=31460 Len=0
  25 3.815486  145.254.160.237  65.208.228.223                TCP       54 3372 → 80 [ACK] Seq=480 Ack=12421 Win=9660 Len=0
  26 3.815630  216.239.59.99    145.254.160.237               TCP     1484 80 → 3371 [PSH, ACK] Seq=1 Ack=722 Win=31460 Len=1430 [TCP segment of a reasse…
  27 3.955688  216.239.59.99    145.254.160.237               HTTP     214 HTTP/1.1 200 OK  (text/html)
  28 3.955688  145.254.160.237  216.239.59.99                 TCP       54 3371 → 80 [ACK] Seq=722 Ack=1591 Win=8760 Len=0
  29 4.105904  65.208.228.223   145.254.160.237               TCP     1434 80 → 3372 [PSH, ACK] Seq=12421 Ack=480 Win=6432 Len=1380 [TCP segment of a rea…
  30 4.216062  145.254.160.237  65.208.228.223                TCP       54 3372 → 80 [ACK] Seq=480 Ack=13801 Win=9660 Len=0
```

```
  Frame 27: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
▸ Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:0
▸ Internet Protocol Version 4, Src: 216.239.59.99, Dst: 145.254.160.237
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 3371, Seq: 1431, Ack: 722,
▸ [2 Reassembled TCP Segments (1590 bytes): #26(1430), #27(160)]
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (3 lines)
```

```
0000  00 00 01 00 00 00 fe ff  20 00 01 00 08 00 45 10   ········ ······E·
0010  00 c8 85 cf 00 00 37 06  b6 12 d8 ef 3b 63 91 fe   ······7· ····;c··
0020  a0 ed 00 50 0d 2b 2e 6b  59 1a 36 c2 20 f9 50 18   ···P·+.k Y·6· ·P·
0030  7a e4 de 29 00 00 47 9a  63 ee 2f a7 b8 0c ab 3b   z··)··G· c·/····;
0040  e5 ad 96 8a 89 c4 d9 1c  75 ee ab 25 e8 5c f7 c1   ········ u··%·\··
0050  0b 7e 8e de fb 82 87 87  2b 92 25 40 a5 d9 79 50   ·~······ +·%@··yP
0060  cf b2 c0 97 6f c7 ab 25  0d 29 90 11 a5 24 c0 50   ····o··% ·)···$·P
0070  d7 2b 2d 9b ea 84 4a 8a  79 51 5c f0 76 9b 72 81   ·+-···J· yQ\·v·r·
0080  89 6d be 88 6a 09 f7 68  0a 15 f9 d9 5b ef a4 b0   ·m··j··h ····[···
0090  7d e5 2d da 65 c1 f4 40  29 14 5c 10 de d7 10 de   }·-·e··@ )·\·····
00a0  d7 cb f0 d6 88 48 a9 57  c5 61 c0 71 7a bd 19 f2   ·····H·W ·a·qz···
00b0  4f cf ba d5 f7 89 42 c1  14 0d 8b 1b 67 91 41 fc   O·····B· ····g·A·
00c0  78 16 17 3b e6 4d d1 bc  36 9a 2f c2 bf 01 7b dc   x··;·M·· 6·/···{·
00d0  03 39 18 0e 00 00                                  ·9····
```

3. **Find Packets:**
   - Search for packets based on content using the "Edit --> Find Packet" menu.
   - Supports various input types (Display filter, Hex, String, Regex) and search fields (packet list, packet details, packet bytes).

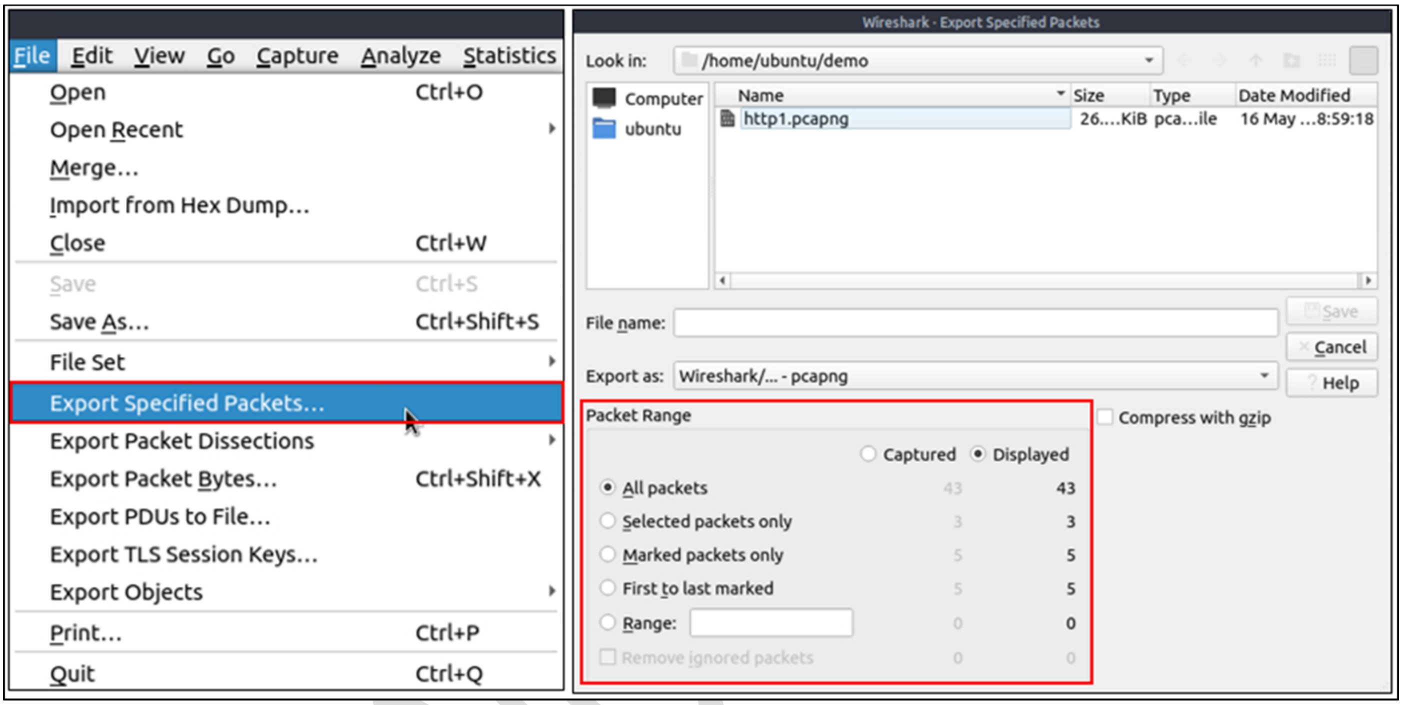

File Edit View Go Capture Analyze Statistics Telephony
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet(s) Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet(s) Ctrl+D
Ignore 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 Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
1
2
3
Packet details
Narrow & Wide
Case sensitive
String
Find
Cancel
Packet list
Packet details
Packet bytes
download
http1.cap
Frame (frame), 214 byte(s)
Text item (text), 29 byte(s)
Packets: 43 · Displayed: 43 (100.0%)
Profile: Default

```
▸ Internet Protocol Version 4, Src: 216.239.59.99,
▸ Transmission Control Protocol, Src Port: 80, Dst
▸ [2 Reassembled TCP Segments (1590 bytes): #26(14
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (3 lines)
```

```
11 2.553672  65.208.228.223   145.254.160.237  TCP   1434 80 → 3372 [P
12 2.553672  145.254.160.237  65.208.228.223   TCP     54 3372 → 80 [A
13 2.553672  145.254.160.237  145.253.2.203    DNS     89 Standard que
14 2.633787  65.208.228.223   145.254.160.237  TCP   1434 80 → 3372 [A
15 2.814046  145.254.160.237  65.208.228.223   TCP     54 3372 → 80 [A
16 2.894161  65.208.228.223   145.254.160.237  TCP   1434 80 → 3372 [A
17 2.914190  145.253.2.203    145.254.160.237  DNS    188 Standard que
18 2.984291  145.254.160.237  216.239.59.99    HTTP   775 GET /pagead/
19 3.014334  145.254.160.237  65.208.228.223   TCP     54 3372 → 80 [A
20 3.374852  65.208.228.223   145.254.160.237  TCP   1434 80 → 3372 [A
21 3.495025  65.208.228.223   145.254.160.237  TCP   1434 80 → 3372 [P
```

```
▸ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe
▸ Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
▸ Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len
▾ Hypertext Transfer Protocol
  ▸ GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/2004
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/pl
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
```

4. **Mark Packets:**
   - Mark packets for further investigation using the "Edit" or right-click menu.
   - Marked packets are highlighted in black.
5. **Packet Comments:**
   - Add comments to packets for additional context and future reference.
6. **Export Packets:**
   - Export specific packets from the capture file for deeper analysis or sharing.



Look in: /home/ubuntu/demo

Name	Size	Type	Date Modified
http1.pcapng	26....KiB	pca...ile	16 May ...8:59:18

File name:

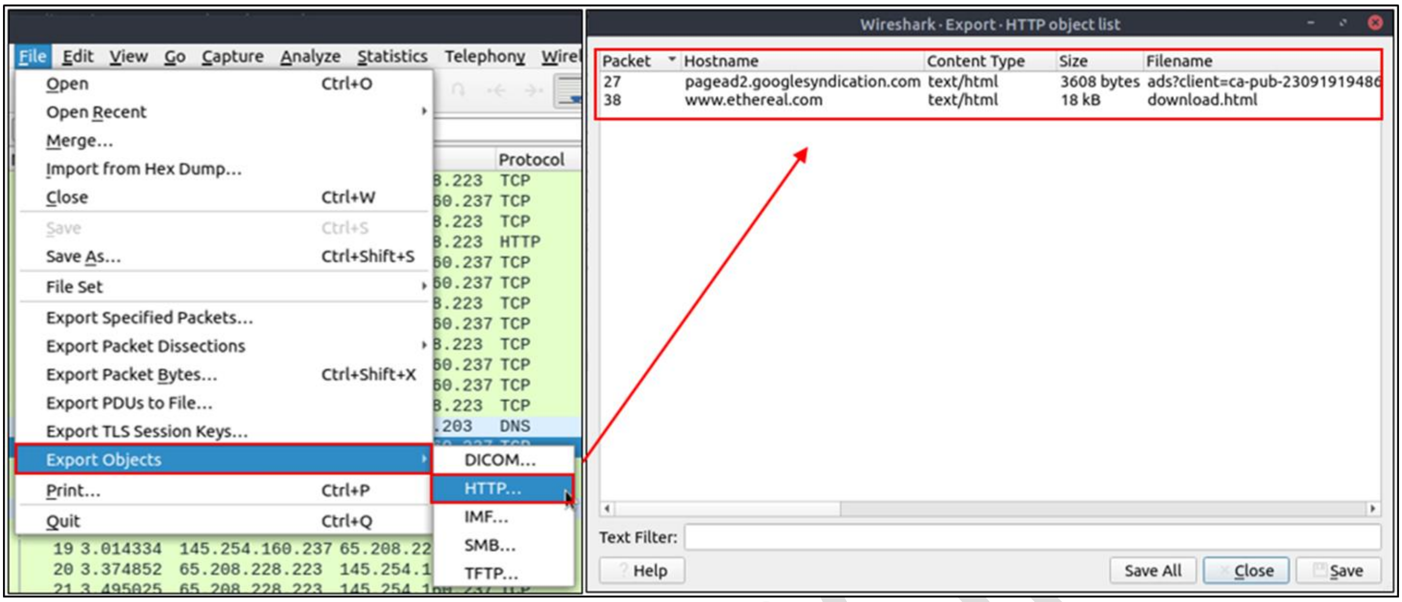
Export as: Wireshark/... - pcapng

□ Compress with gzip

Packet Range

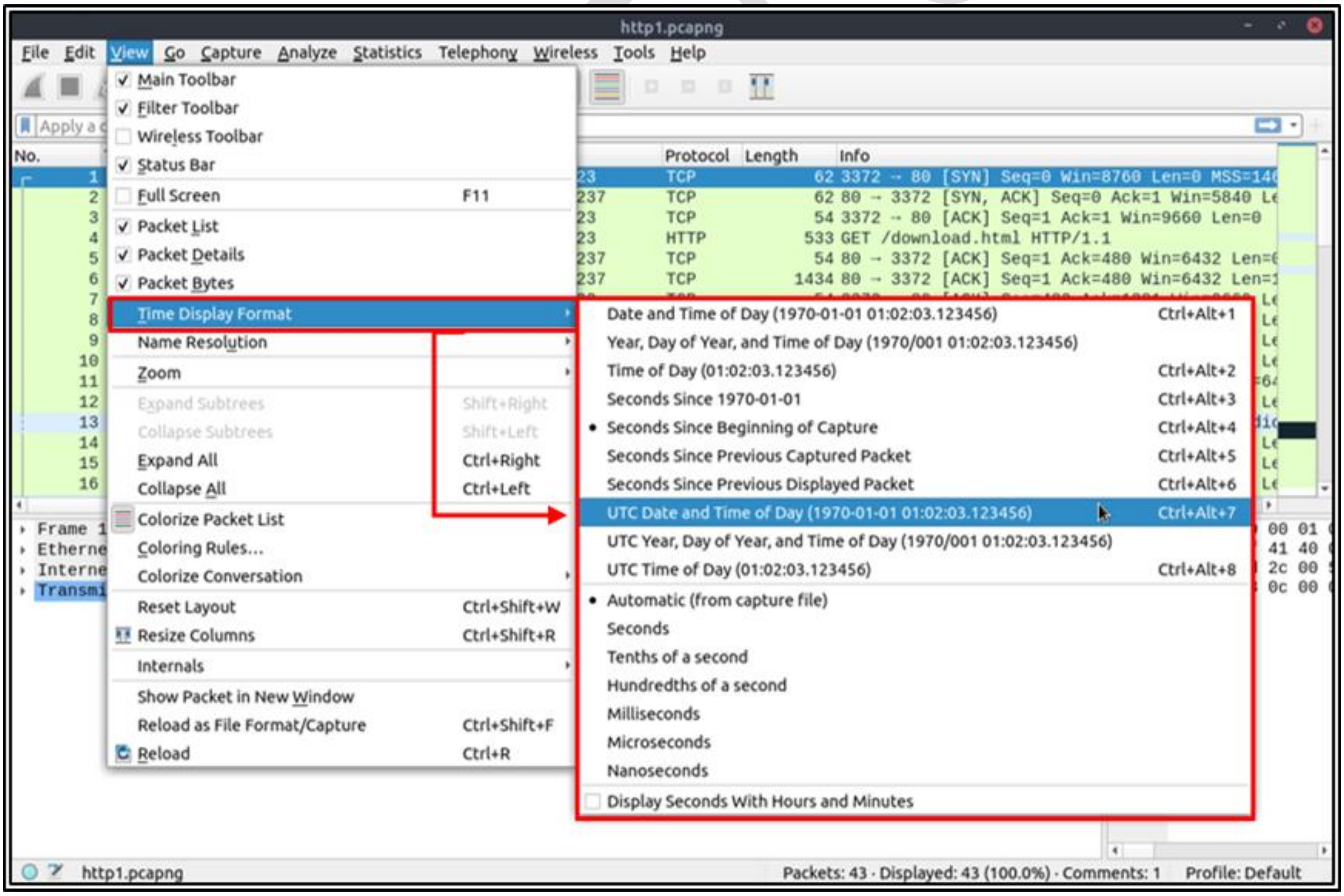
	○ Captured	● Displayed
● All packets	43	43
○ Selected packets only	3	3
○ Marked packets only	5	5
○ First to last marked	5	5
○ Range:	0	0
□ Remove ignored packets	0	0

7. **Export Objects:**
   - Extract files transferred over the network from specific protocol streams (DICOM, HTTP, IMF, SMB, TFTP).

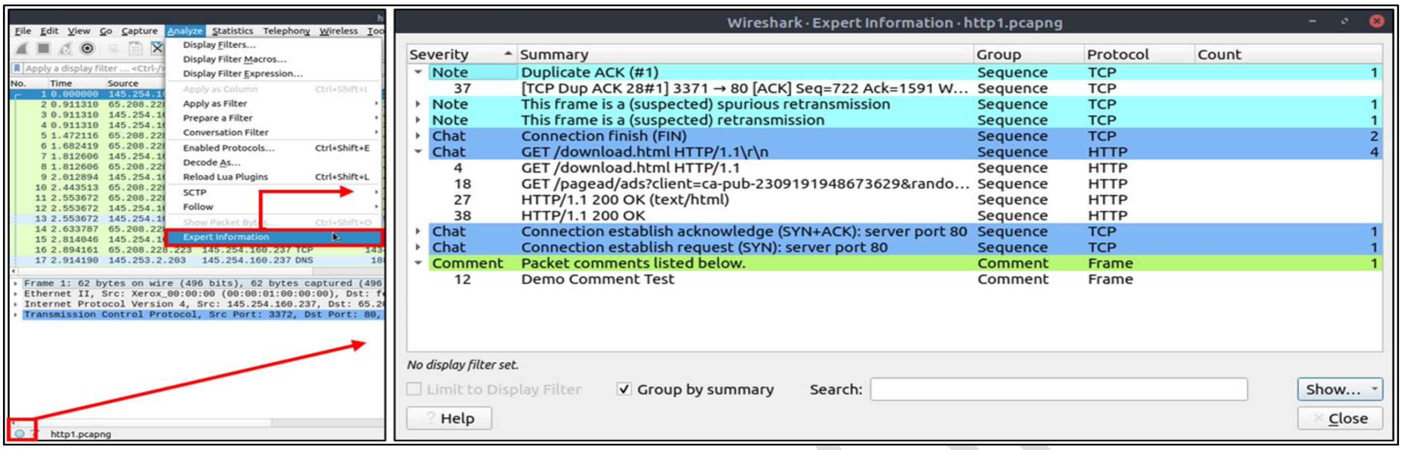


Packet	Hostname	Content Type	Size	Filename
27	pagead2.googlesyndication.com	text/html	3608 bytes	ads?client=ca-pub-23091919486
38	www.ethereal.com	text/html	18 kB	download.html

8. **Time Display Format:**
   - Change the time display format for better analysis, commonly using UTC.


http1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
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 Beginning of Capture 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
Microseconds
Nanoseconds
Display Seconds With Hours and Minutes
No. Protocol Length Info
62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=14
62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Le
54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
533 GET /download.html HTTP/1.1
54 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=
1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=
Frame
Etherne
Interne
Transmi
http1.pcapng
Packets: 43 · Displayed: 43 (100.0%) · Comments: 1
Profile: Default

9. **Expert Info:**
   - Wireshark provides expert information on protocol states to help identify potential issues.
   - Categories include Chat (Blue), Note (Cyan), Warn (Yellow), and Error (Red).


File Edit View Go Capture Analyze Statistics Telephony Wireless Too
Display Filters…
Display Filter Macros…
Display Filter Expression…
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols… Ctrl+Shift+E
Decode As…
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes… Ctrl+Shift+O
Expert Information
http1.pcapng
Wireshark · Expert Information · http1.pcapng

Severity	Summary	Group	Protocol	Count
Note	Duplicate ACK (#1)	Sequence	TCP	1
37	[TCP Dup ACK 28#1] 3371 → 80 [ACK] Seq=722 Ack=1591 W…	Sequence	TCP	
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1
Note	This frame is a (suspected) retransmission	Sequence	TCP	1
Chat	Connection finish (FIN)	Sequence	TCP	2
Chat	GET /download.html HTTP/1.1\r\n	Sequence	HTTP	4
4	GET /download.html HTTP/1.1	Sequence	HTTP	
18	GET /pagead/ads?client=ca-pub-2309191948673629&rando…	Sequence	HTTP	
27	HTTP/1.1 200 OK (text/html)	Sequence	HTTP	
38	HTTP/1.1 200 OK	Sequence	HTTP	
Chat	Connection establish acknowledge (SYN+ACK): server port 80	Sequence	TCP	1
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	1
Comment	Packet comments listed below.	Comment	Frame	1
12	Demo Comment Test	Comment	Frame	

No display filter set.

☐ Limit to Display Filter ☑ Group by summary Search:

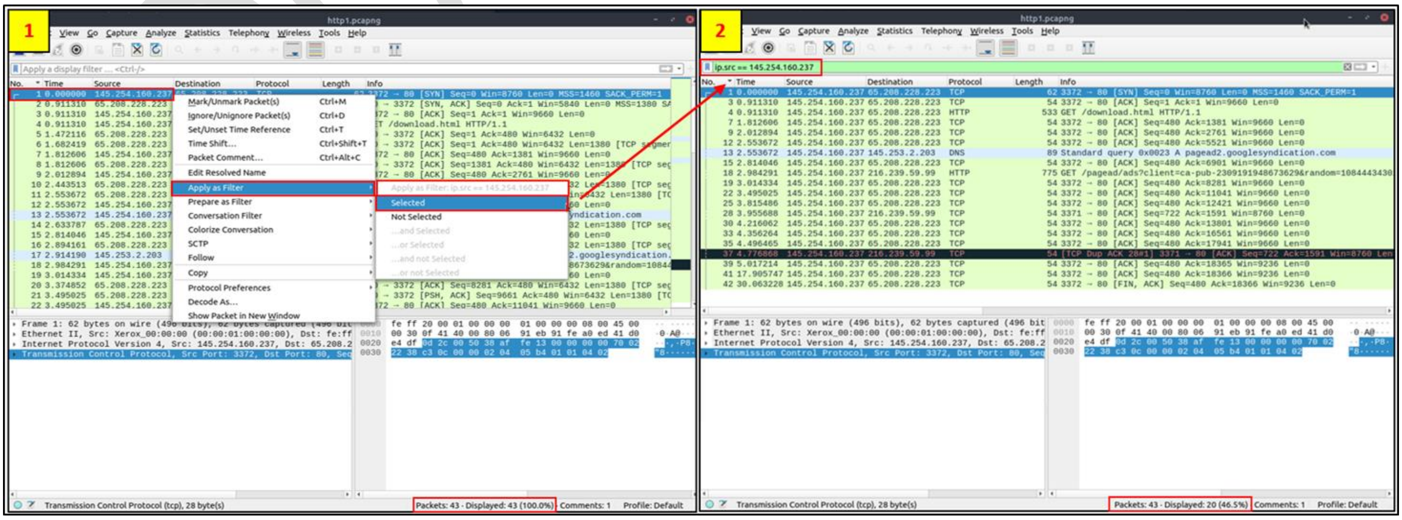
Packet Filtering

Wireshark has a powerful filter engine that helps analysts narrow down the traffic and focus on the event of interest. There are two types of filtering approaches: capture filters and display filters.

1. **Capture Filters:**
   - Used during packet capture to only collect packets that meet specific criteria.
2. **Display Filters:**
   - Applied after packet capture to view specific packets that meet certain criteria.

Apply as Filter

- Click on a field and use the "right-click menu" or "Analyse --> Apply as Filter" to filter specific values. Wireshark will generate and apply the required filter query, displaying only the selected packets.


1
http1.pcapng
View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
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
Apply as Filter: ip.src == 145.254.160.237
Selected
Not Selected
…and Selected
…or Selected
…and not Selected
…or not Selected
2

Transmission Control Protocol (tcp), 28 byte(s) Packets: 43 · Displayed: 43 (100.0%) Comments: 1 Profile: Default

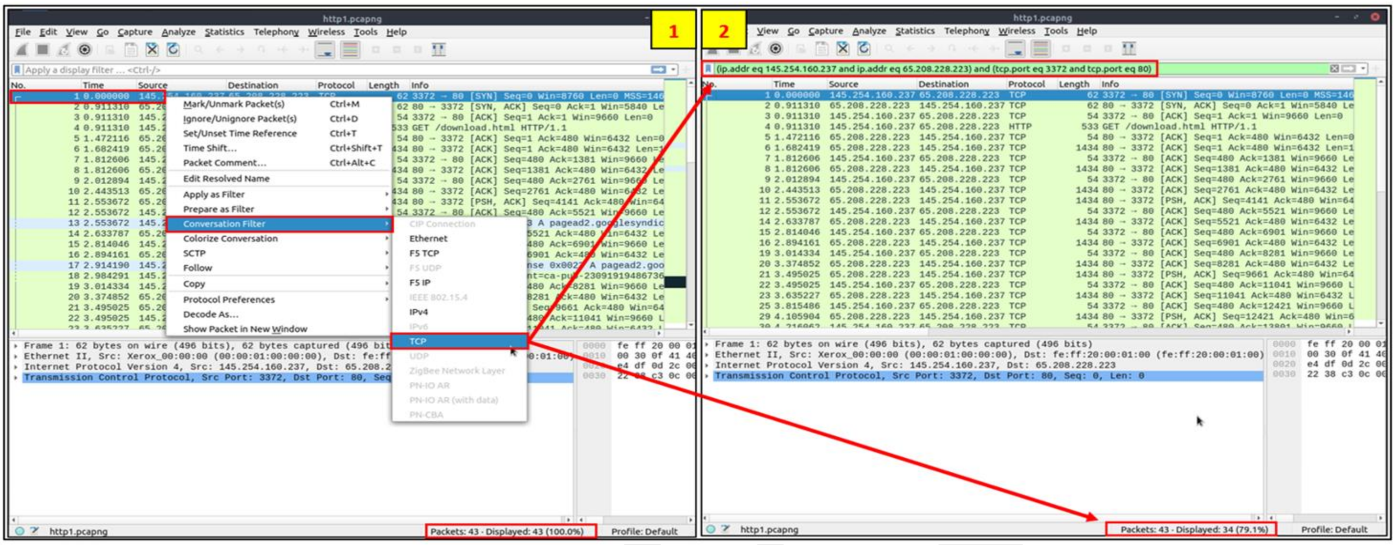
ip.src == 145.254.160.237

```
No. Time       Source          Destination     Protocol  Length Info
  1 0.000000   145.254.160.237 65.208.228.223  TCP       62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
  3 0.911310   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
  4 0.911310   145.254.160.237 65.208.228.223  HTTP     533 GET /download.html HTTP/1.1
  7 1.812606   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
  9 2.012894   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
 12 2.553672   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
 13 2.553672   145.254.160.237 145.253.2.203   DNS       89 Standard query 0x0023 A pagead2.googlesyndication.com
 15 2.814046   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
 18 2.984291   145.254.160.237 216.239.59.99   HTTP     775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430
 19 3.014334   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
 22 3.495025   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 Len=0
 25 3.815486   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=12421 Win=9660 Len=0
 28 3.955688   145.254.160.237 216.239.59.99   TCP       54 3371 → 80 [ACK] Seq=722 Ack=1591 Win=8760 Len=0
 30 4.216062   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=13801 Win=9660 Len=0
 33 4.356264   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=16561 Win=9660 Len=0
 35 4.496465   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=17941 Win=9660 Len=0
 37 4.776868   145.254.160.237 216.239.59.99   TCP       54 [TCP Dup ACK 28#1] 3371 → 80 [ACK] Seq=722 Ack=1591 Win=8760 Len
 39 5.017214   145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=18365 Win=9236 Len=0
 41 17.905747  145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [ACK] Seq=480 Ack=18366 Win=9236 Len=0
 42 30.063228  145.254.160.237 65.208.228.223  TCP       54 3372 → 80 [FIN, ACK] Seq=480 Ack=18366 Win=9236 Len=0

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bit
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.2
Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq

0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02
```

Transmission Control Protocol (tcp), 28 byte(s) Packets: 43 · Displayed: 20 (46.5%) Comments: 1 Profile: Default

Conversation Filter

- Use the "Conversation Filter" to view all packets linked by IP addresses and port numbers. This helps in analyzing specific conversations.



```
(ip.addr eq 145.254.160.237 and ip.addr eq 65.208.228.223) and (tcp.port eq 3372 and tcp.port eq 80)
```

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  145.254.160.237 65.208.228.223  TCP        62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=146
   2 0.911310  65.208.228.223  145.254.160.237 TCP        62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Le
   3 0.911310  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
   4 0.911310  145.254.160.237 65.208.228.223  HTTP      533 GET /download.html HTTP/1.1
   5 1.472116  65.208.228.223  145.254.160.237 TCP        54 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
   6 1.682419  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1
   7 1.812606  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Le
   8 1.812606  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Le
   9 2.012894  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Le
  10 2.443513  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Le
  11 2.553672  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=64
  12 2.553672  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Le
  14 2.633787  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Le
  15 2.814046  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Le
  16 2.894161  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Le
  19 3.014334  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Le
  20 3.374852  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Le
  21 3.495025  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [PSH, ACK] Seq=9661 Ack=480 Win=64
  22 3.495025  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 L
  23 3.635227  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [ACK] Seq=11041 Ack=480 Win=6432 L
  25 3.815486  145.254.160.237 65.208.228.223  TCP        54 3372 → 80 [ACK] Seq=480 Ack=12421 Win=9660 L
  29 4.105904  65.208.228.223  145.254.160.237 TCP      1434 80 → 3372 [PSH, ACK] Seq=12421 Ack=480 Win=6

▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▸ Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
▸ Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 0, Len: 0
```

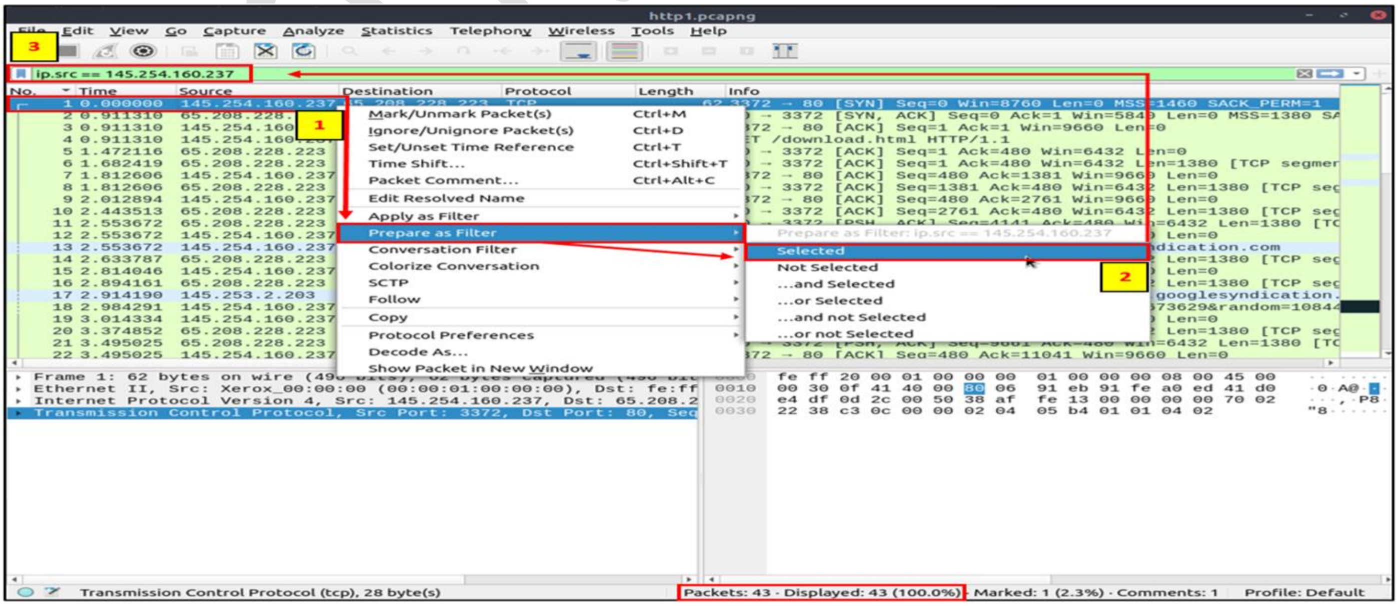
```
http1.pcapng    Packets: 43 · Displayed: 43 (100.0%)    Profile: Default
http1.pcapng    Packets: 43 · Displayed: 34 (79.1%)    Profile: Default
```

Colourise Conversation

- Highlights linked packets without reducing the number of viewed packets, using the "right-click menu" or "View --> Colourise Conversation" menu.

Prepare as Filter

- Similar to "Apply as Filter" but adds the query to the pane without applying it immediately, waiting for the execution command or further filtering options.

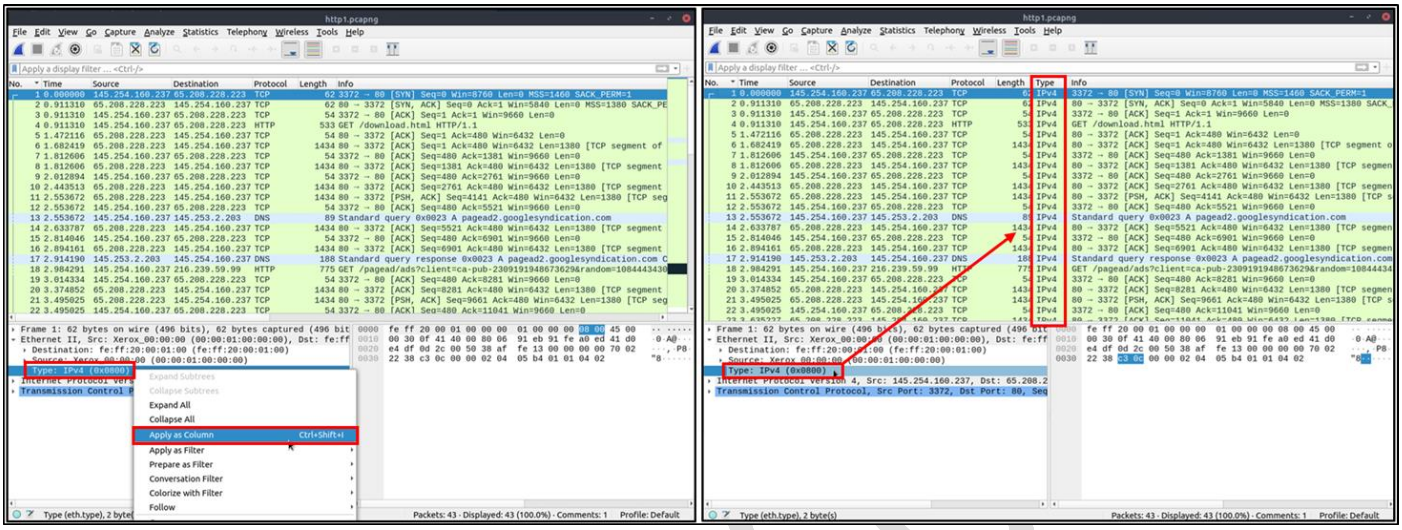

3
1
2
http1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Prepare as Filter: ip.src == 145.254.160.237
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Profile: Default

```
ip.src == 145.254.160.237
```

```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff
▸ Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.2
▸ Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq

0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   ·0·A@·
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ···,·P8·
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8······

Transmission Control Protocol (tcp), 28 byte(s)    Packets: 43 · Displayed: 43 (100.0%) · Marked: 1 (2.3%) · Comments: 1    Profile: Default
```

Apply as Column

- Adds specific values/fields as columns in the packet list pane for easier examination across packets.

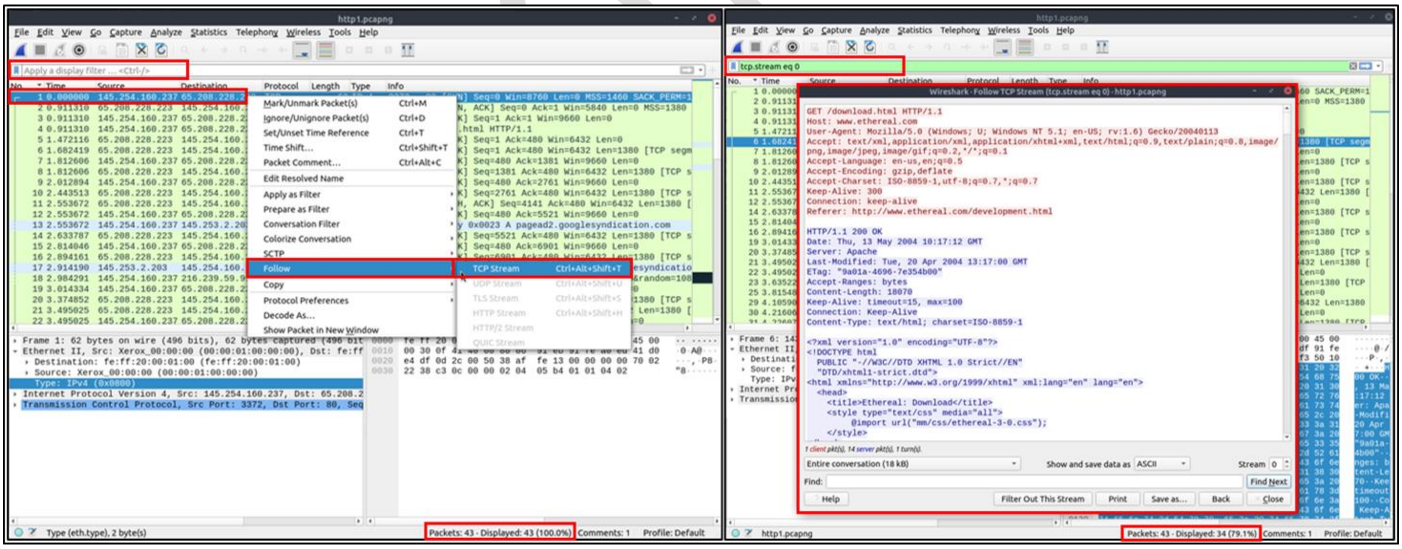


```
http1.pcapng
No.  Time     Source          Destination     Protocol Length Info
 1 0.000000 145.254.160.237 65.208.228.223  TCP      62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
 2 0.911310 65.208.228.223  145.254.160.237 TCP      62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PE
 3 0.911310 145.254.160.237 65.208.228.223  TCP      54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
 4 0.911310 145.254.160.237 65.208.228.223  HTTP    533 GET /download.html HTTP/1.1
 5 1.472116 65.208.228.223  145.254.160.237 TCP      54 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
 6 1.682419 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of
 7 1.812606 145.254.160.237 65.208.228.223  TCP      54 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
 8 1.812606 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment
 9 2.012894 145.254.160.237 65.208.228.223  TCP      54 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10 2.443513 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment
11 2.553672 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP seg
12 2.553672 145.254.160.237 65.208.228.223  TCP      54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13 2.553672 145.254.160.237 145.253.2.203   DNS      89 Standard query 0x0023 A pagead2.googlesyndication.com
14 2.633787 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment
15 2.814046 145.254.160.237 65.208.228.223  TCP      54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
16 2.894161 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP segment
17 2.914190 145.253.2.203   145.254.160.237 DNS     188 Standard query response 0x0023 A pagead2.googlesyndication.com C
18 2.984291 145.254.160.237 216.239.59.99   HTTP    775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430
19 3.014334 145.254.160.237 65.208.228.223  TCP      54 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
20 3.374852 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP segment
21 3.495025 65.208.228.223  145.254.160.237 TCP    1434 80 → 3372 [PSH, ACK] Seq=9661 Ack=480 Win=6432 Len=1380 [TCP seg
22 3.495025 145.254.160.237 65.208.228.223  TCP      54 3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 Len=0

› Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bit
˅ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff
  › Destination: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
  › Source: Xerox_00:00:00 (00:00:01:00:00:00)
    Type: IPv4 (0x0800)
› Internet Protocol Vers
› Transmission Control P

0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02

Type (eth.type), 2 byte(s)    Packets: 43 · Displayed: 43 (100.0%) · Comments: 1    Profile: Default
```

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
Type

Follow Stream

- Reconstructs streams to view raw traffic at the application level, useful for seeing unencrypted data such as usernames and passwords.



Apply a display filter ... <Ctrl-/>
Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
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
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
tcp.stream eq 0

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · http1.pcapng

GET /download.html HTTP/1.1
Host: www.ethereal.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/
png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.ethereal.com/development.html

HTTP/1.1 200 OK
Date: Thu, 13 May 2004 10:17:12 GMT
Server: Apache
Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT
ETag: "9a01a-4696-7e354b00"
Accept-Ranges: bytes
Content-Length: 18070
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
  <head>
    <title>Ethereal: Download</title>
    <style type="text/css" media="all">
        @import url("mm/css/ethereal-3-0.css");
    </style>

1 client pkt(s), 14 server pkt(s), 1 turn(s).
Entire conversation (18 kB)    Show and save data as ASCII    Stream 0

Packets: 43 · Displayed: 43 (100.0%)    Comments: 1    Profile: Default
Packets: 43 · Displayed: 34 (79.1%)    Comments: 1    Profile: Default
```

Conclusion

Wireshark is an essential tool for network analysts and cybersecurity professionals. Its ability to capture and analyze network traffic in detail makes it invaluable for troubleshooting, security investigations, and learning protocol intricacies. Familiarity with its interface and functions is crucial for effective use.

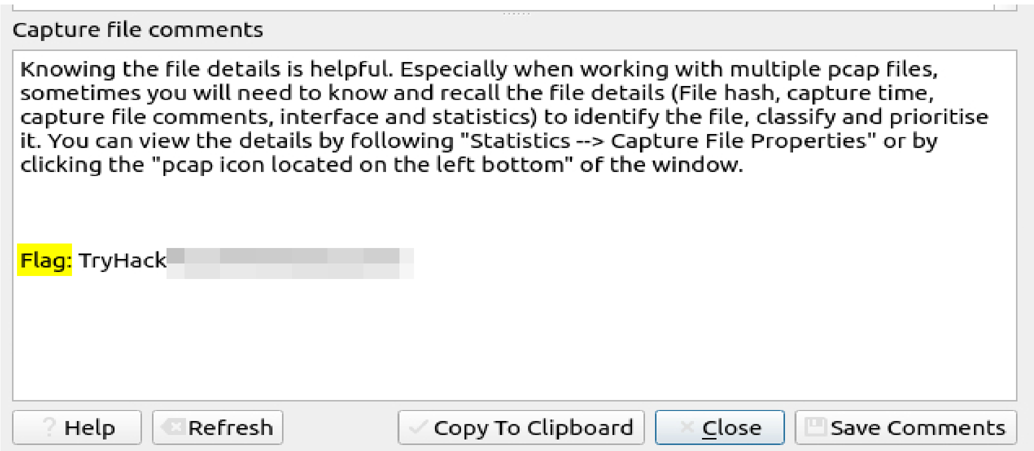
References

- Wireshark: The Basics: Link
- TryHackMe | Wireshark: The Basics Writeup Link

Appendix

Use the "Exercise.pcapng" file to answer the questions.

Read the **"capture file comments"**. What is the flag?

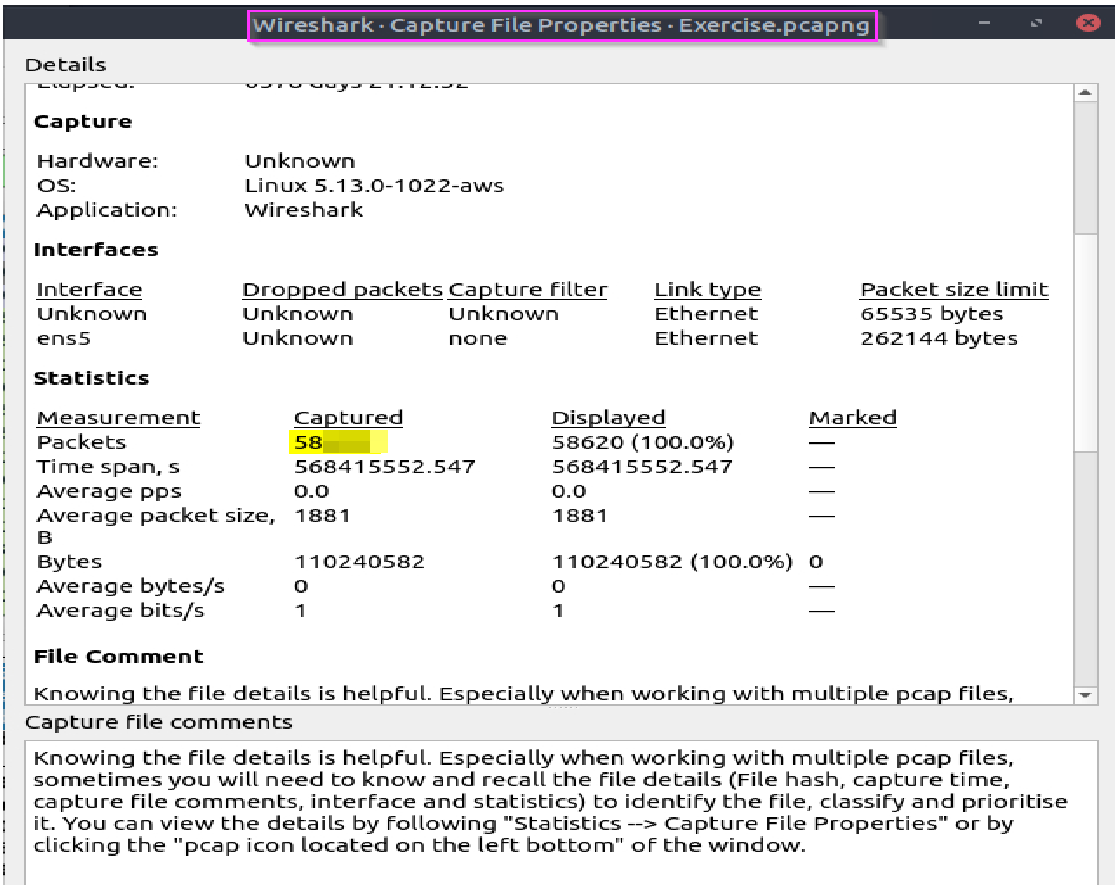


Capture file comments

Knowing the file details is helpful. Especially when working with multiple pcap files, sometimes you will need to know and recall the file details (File hash, capture time, capture file comments, interface and statistics) to identify the file, classify and prioritise it. You can view the details by following "Statistics --> Capture File Properties" or by clicking the "pcap icon located on the left bottom" of the window.

Flag: TryHack[redacted]

What is the total number of packets?



Details

Capture

Hardware: Unknown
OS: Linux 5.13.0-1022-aws
Application: Wireshark

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes
ens5	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	58[redacted]	58620 (100.0%)	—
Time span, s	568415552.547	568415552.547	—
Average pps	0.0	0.0	—
Average packet size, B	1881	1881	—
Bytes	110240582	110240582 (100.0%)	0
Average bytes/s	0	0	—
Average bits/s	1	1	—

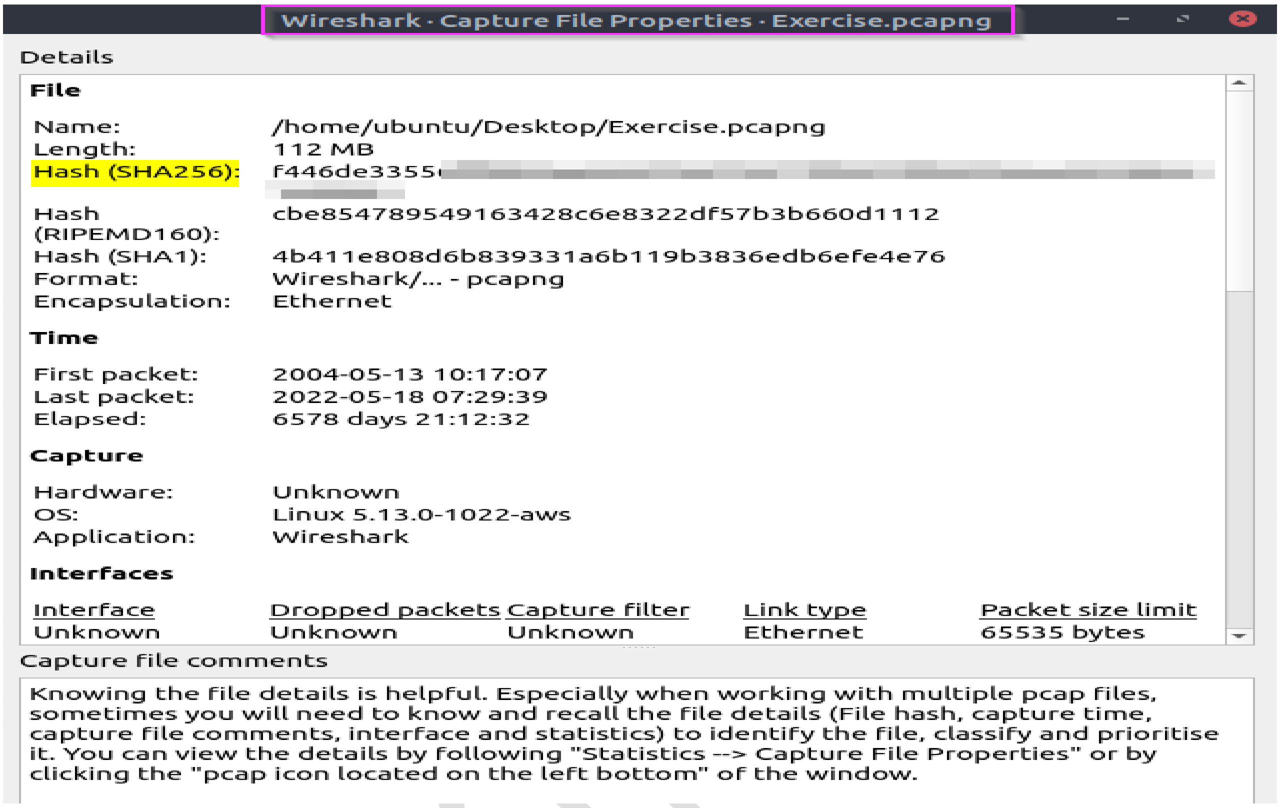
File Comment

Knowing the file details is helpful. Especially when working with multiple pcap files,

Capture file comments

Knowing the file details is helpful. Especially when working with multiple pcap files, sometimes you will need to know and recall the file details (File hash, capture time, capture file comments, interface and statistics) to identify the file, classify and prioritise it. You can view the details by following "Statistics --> Capture File Properties" or by clicking the "pcap icon located on the left bottom" of the window.

What is the **SHA256 hash** value of the capture file?



Wireshark · Capture File Properties · Exercise.pcapng

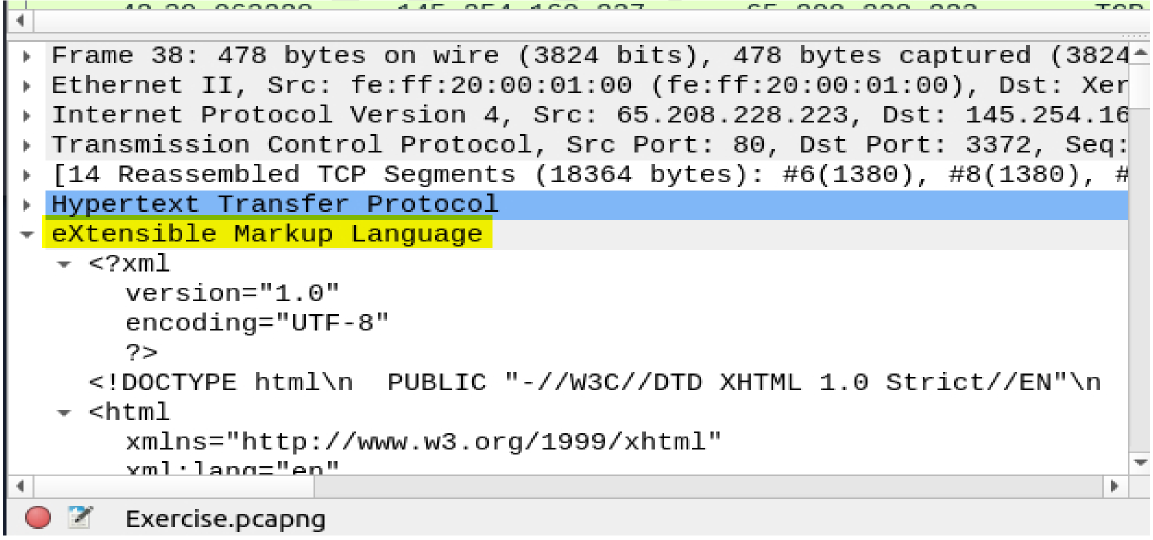
Details

```
File

Name:             /home/ubuntu/Desktop/Exercise.pcapng
Length:           112 MB
Hash (SHA256):    f446de3355[redacted]
Hash
(RIPEMD160):      cbe854789549163428c6e8322df57b3b660d1112
Hash (SHA1):      4b411e808d6b839331a6b119b3836edb6efe4e76
Format:           Wireshark/... - pcapng
Encapsulation:    Ethernet

Time

First packet:     2004-05-13 10:17:07
Last packet:      2022-05-18 07:29:39
Elapsed:          6578 days 21:12:32

Capture

Hardware:         Unknown
OS:               Linux 5.13.0-1022-aws
Application:      Wireshark

Interfaces

Interface   Dropped packets Capture filter   Link type   Packet size limit
Unknown     Unknown         Unknown          Ethernet    65535 bytes
```

Capture file comments

Knowing the file details is helpful. Especially when working with multiple pcap files, sometimes you will need to know and recall the file details (File hash, capture time, capture file comments, interface and statistics) to identify the file, classify and prioritise it. You can view the details by following "Statistics --> Capture File Properties" or by clicking the "pcap icon located on the left bottom" of the window.

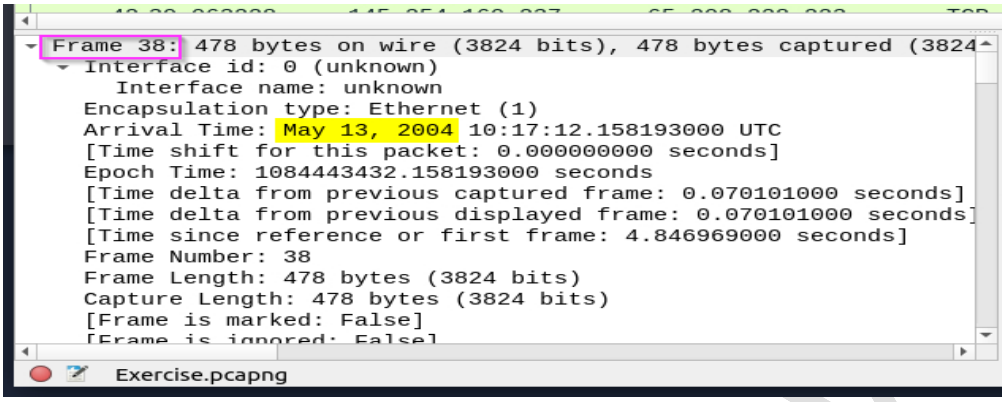
View packet number 38. Which markup language is used under the HTTP protocol?



```
▸ Frame 38: 478 bytes on wire (3824 bits), 478 bytes captured (3824
▸ Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xer
▸ Internet Protocol Version 4, Src: 65.208.228.223, Dst: 145.254.16
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 3372, Seq:
▸ [14 Reassembled TCP Segments (18364 bytes): #6(1380), #8(1380), #
▸ Hypertext Transfer Protocol
▾ eXtensible Markup Language
  ▾ <?xml
      version="1.0"
      encoding="UTF-8"
      ?>
    <!DOCTYPE html\n  PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"\n
  ▾ <html
      xmlns="http://www.w3.org/1999/xhtml"
      xml:lang="en"
```

Exercise.pcapng

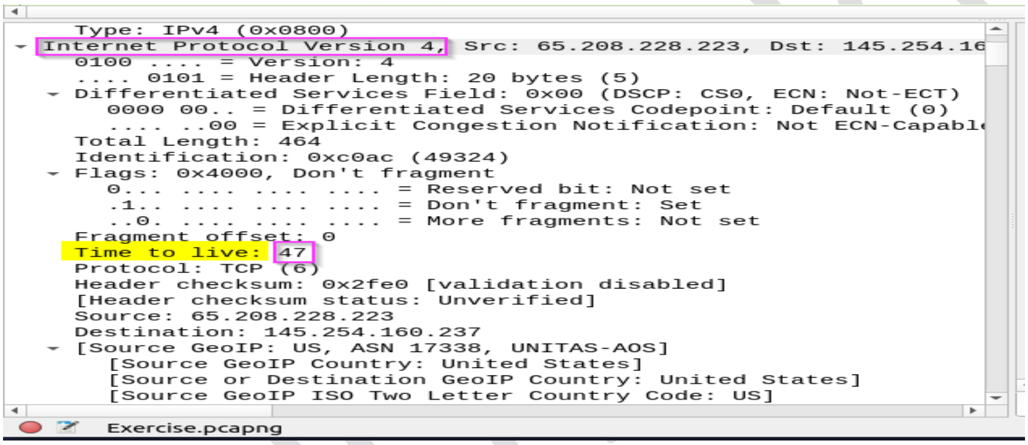
What is the arrival date of the packet? (Answer format: Month/Day/Year)



```
▾ Frame 38: 478 bytes on wire (3824 bits), 478 bytes captured (3824
  ▾ Interface id: 0 (unknown)
      Interface name: unknown
    Encapsulation type: Ethernet (1)
    Arrival Time: May 13, 2004 10:17:12.158193000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1084443432.158193000 seconds
    [Time delta from previous captured frame: 0.070101000 seconds]
    [Time delta from previous displayed frame: 0.070101000 seconds]
    [Time since reference or first frame: 4.846969000 seconds]
    Frame Number: 38
    Frame Length: 478 bytes (3824 bits)
    Capture Length: 478 bytes (3824 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

Exercise.pcapng

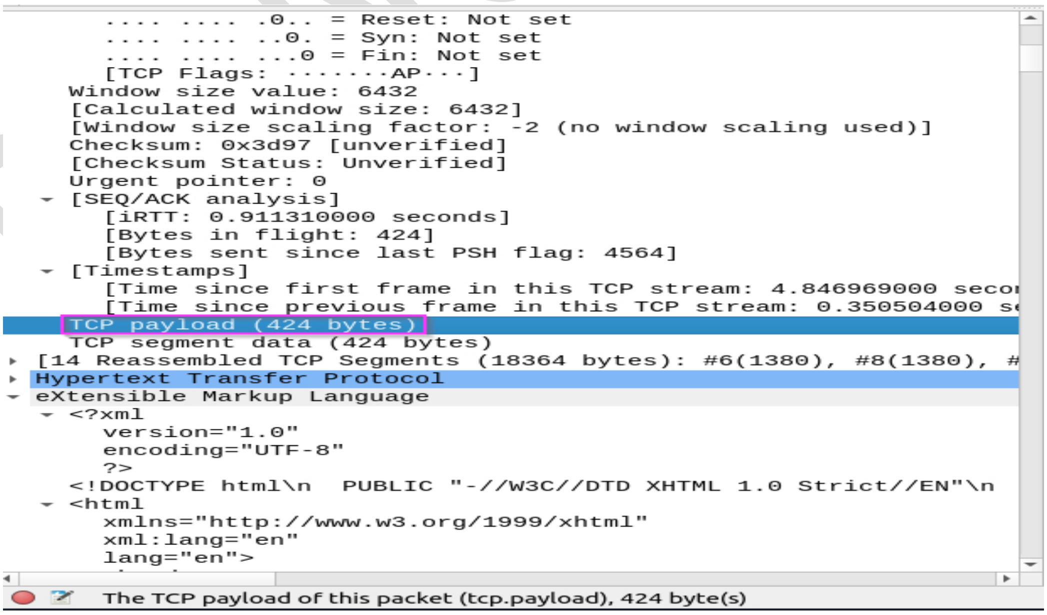
What is the TTL value?



```
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 65.208.228.223, Dst: 145.254.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable
    Total Length: 464
    Identification: 0xc0ac (49324)
  ▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 47
    Protocol: TCP (6)
    Header checksum: 0x2fe0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 65.208.228.223
    Destination: 145.254.160.237
  ▾ [Source GeoIP: US, ASN 17338, UNITAS-AOS]
      [Source GeoIP Country: United States]
      [Source or Destination GeoIP Country: United States]
      [Source GeoIP ISO Two Letter Country Code: US]
```

Exercise.pcapng

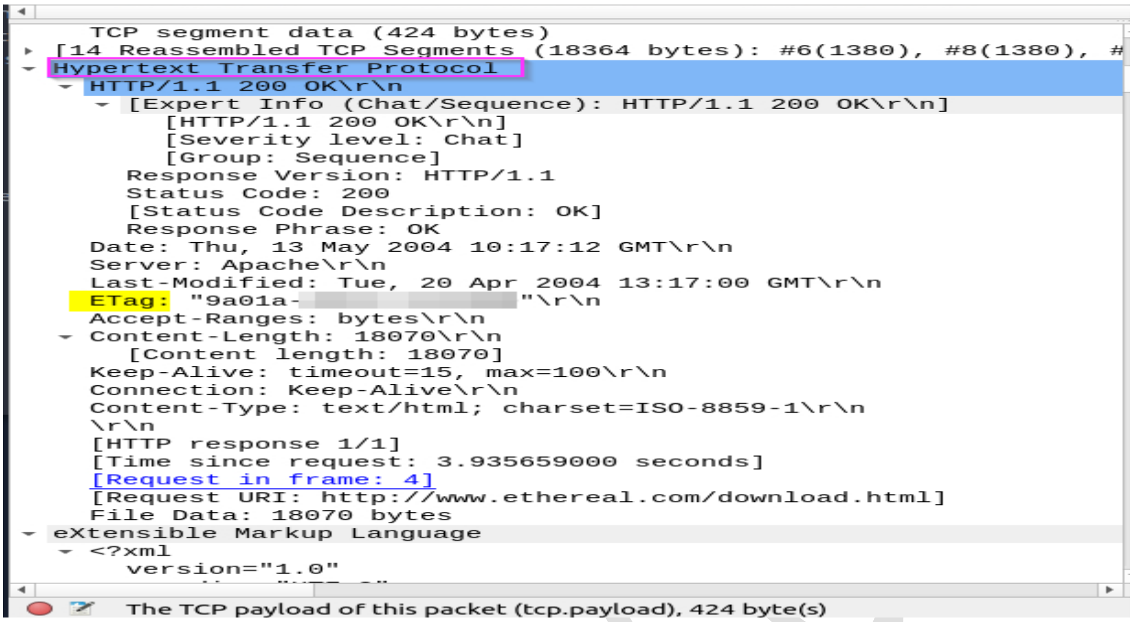
What is the TCP payload size?



```
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window size value: 6432
    [Calculated window size: 6432]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x3d97 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▾ [SEQ/ACK analysis]
      [iRTT: 0.911310000 seconds]
      [Bytes in flight: 424]
      [Bytes sent since last PSH flag: 4564]
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 4.846969000 secor
      [Time since previous frame in this TCP stream: 0.350504000 se
    TCP payload (424 bytes)
    TCP segment data (424 bytes)
▸ [14 Reassembled TCP Segments (18364 bytes): #6(1380), #8(1380), #
▸ Hypertext Transfer Protocol
▾ eXtensible Markup Language
  ▾ <?xml
      version="1.0"
      encoding="UTF-8"
      ?>
    <!DOCTYPE html\n  PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"\n
  ▾ <html
      xmlns="http://www.w3.org/1999/xhtml"
      xml:lang="en"
      lang="en">
```

The TCP payload of this packet (tcp.payload), 424 byte(s)

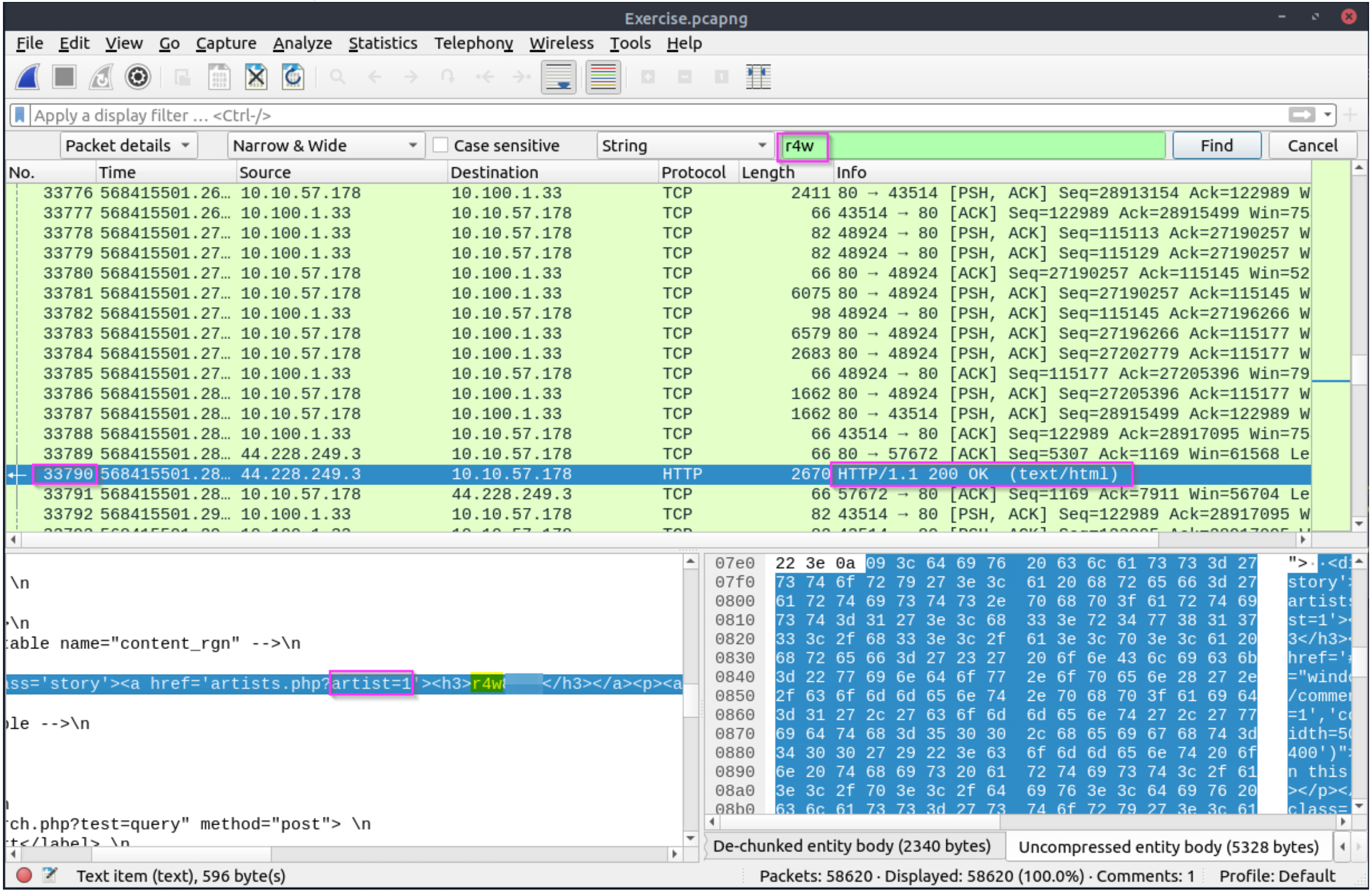
What is the e-tag value?



```
    TCP segment data (424 bytes)
  ▸ [14 Reassembled TCP Segments (18364 bytes): #6(1380), #8(1380), #
  ▾ Hypertext Transfer Protocol
    ▾ HTTP/1.1 200 OK\r\n
      ▾ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
           [HTTP/1.1 200 OK\r\n]
           [Severity level: Chat]
           [Group: Sequence]
         Response Version: HTTP/1.1
         Status Code: 200
         [Status Code Description: OK]
         Response Phrase: OK
      Date: Thu, 13 May 2004 10:17:12 GMT\r\n
      Server: Apache\r\n
      Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT\r\n
      ETag: "9a01a-[redacted]"\r\n
      Accept-Ranges: bytes\r\n
    ▾ Content-Length: 18070\r\n
         [Content length: 18070]
      Keep-Alive: timeout=15, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=ISO-8859-1\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 3.935659000 seconds]
      [Request in frame: 4]
      [Request URI: http://www.ethereal.com/download.html]
      File Data: 18070 bytes
  ▾ eXtensible Markup Language
    ▾ <?xml
         version="1.0"
```

The TCP payload of this packet (tcp.payload), 424 byte(s)

Search the **"r4w" string** in packet details. What is the name of artist 1?



Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Find
Cancel

Packet details | Narrow & Wide | □ Case sensitive | String | r4w

```
No.    Time              Source          Destination     Protocol Length Info
 33776 568415501.26… 10.10.57.178    10.100.1.33     TCP        2411 80 → 43514 [PSH, ACK] Seq=28913154 Ack=122989 W
 33777 568415501.26… 10.100.1.33     10.10.57.178    TCP          66 43514 → 80 [ACK] Seq=122989 Ack=28915499 Win=75
 33778 568415501.27… 10.100.1.33     10.10.57.178    TCP          82 48924 → 80 [PSH, ACK] Seq=115113 Ack=27190257 W
 33779 568415501.27… 10.100.1.33     10.10.57.178    TCP          82 48924 → 80 [PSH, ACK] Seq=115129 Ack=27190257 W
 33780 568415501.27… 10.10.57.178    10.100.1.33     TCP          66 80 → 48924 [ACK] Seq=27190257 Ack=115145 Win=52
 33781 568415501.27… 10.10.57.178    10.100.1.33     TCP        6075 80 → 48924 [PSH, ACK] Seq=27190257 Ack=115145 W
 33782 568415501.27… 10.100.1.33     10.10.57.178    TCP          98 48924 → 80 [PSH, ACK] Seq=115145 Ack=27196266 W
 33783 568415501.27… 10.10.57.178    10.100.1.33     TCP        6579 80 → 48924 [PSH, ACK] Seq=27196266 Ack=115177 W
 33784 568415501.27… 10.10.57.178    10.100.1.33     TCP        2683 80 → 48924 [PSH, ACK] Seq=27202779 Ack=115177 W
 33785 568415501.27… 10.100.1.33     10.10.57.178    TCP          66 48924 → 80 [ACK] Seq=115177 Ack=27205396 Win=79
 33786 568415501.28… 10.10.57.178    10.100.1.33     TCP        1662 80 → 48924 [PSH, ACK] Seq=27205396 Ack=115177 W
 33787 568415501.28… 10.10.57.178    10.100.1.33     TCP        1662 80 → 43514 [PSH, ACK] Seq=28915499 Ack=122989 W
 33788 568415501.28… 10.100.1.33     10.10.57.178    TCP          66 43514 → 80 [ACK] Seq=122989 Ack=28917095 Win=75
 33789 568415501.28… 44.228.249.3    10.10.57.178    TCP          66 80 → 57672 [ACK] Seq=5307 Ack=1169 Win=61568 Le
 33790 568415501.28… 44.228.249.3    10.10.57.178    HTTP       2670 HTTP/1.1 200 OK  (text/html)
 33791 568415501.28… 10.10.57.178    44.228.249.3    TCP          66 57672 → 80 [ACK] Seq=1169 Ack=7911 Win=56704 Le
 33792 568415501.29… 10.100.1.33     10.10.57.178    TCP          82 43514 → 80 [PSH, ACK] Seq=122989 Ack=28917095 W
```

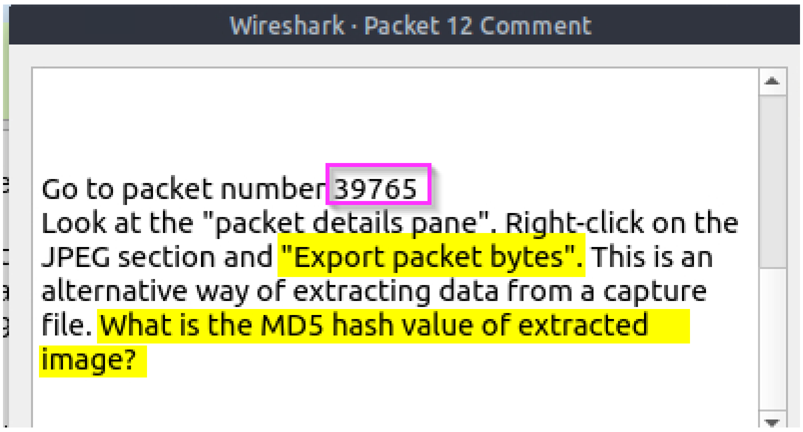
```
\n

\n
able name="content_rgn" -->\n

ss='story'><a href='artists.php?artist=1'><h3>r4w[redacted]</h3></a><p><a

le -->\n


ch.php?test=query" method="post"> \n
t</label> \n
```

```
07e0  22 3e 0a 09 3c 64 69 76  20 63 6c 61 73 73 3d 27   ">··<di
07f0  73 74 6f 72 79 27 3e 3c  61 20 68 72 65 66 3d 27   story'>
0800  61 72 74 69 73 74 73 2e  70 68 70 3f 61 72 74 69   artists
0810  73 74 3d 31 27 3e 3c 68  33 3e 72 34 77 38 31 37   st=1'>
0820  33 3c 2f 68 33 3e 3c 2f  61 3e 3c 70 3e 3c 61 20   3</h3>
0830  68 72 65 66 3d 27 23 27  20 6f 6e 43 6c 69 63 6b   href='
0840  3d 22 77 69 6e 64 6f 77  2e 6f 70 65 6e 28 27 2e   ="wind
0850  2f 63 6f 6d 6d 65 6e 74  2e 70 68 70 3f 61 69 64   /commer
0860  3d 31 27 2c 27 63 6f 6d  6d 65 6e 74 27 2c 27 77   =1','c
0870  69 64 74 68 3d 35 30 30  2c 68 65 69 67 68 74 3d   idth=5
0880  34 30 30 27 29 22 3e 63  6f 6d 6d 65 6e 74 20 6f   400')"
0890  6e 20 74 68 69 73 20 61  72 74 69 73 74 3c 2f 61   n this
08a0  3e 3c 2f 70 3e 3c 2f 64  69 76 3e 3c 64 69 76 20   ></p><
08b0  63 6c 61 73 73 3d 27 73  74 6f 72 79 27 3e 3c 61   class=
```

De-chunked entity body (2340 bytes) | Uncompressed entity body (5328 bytes)

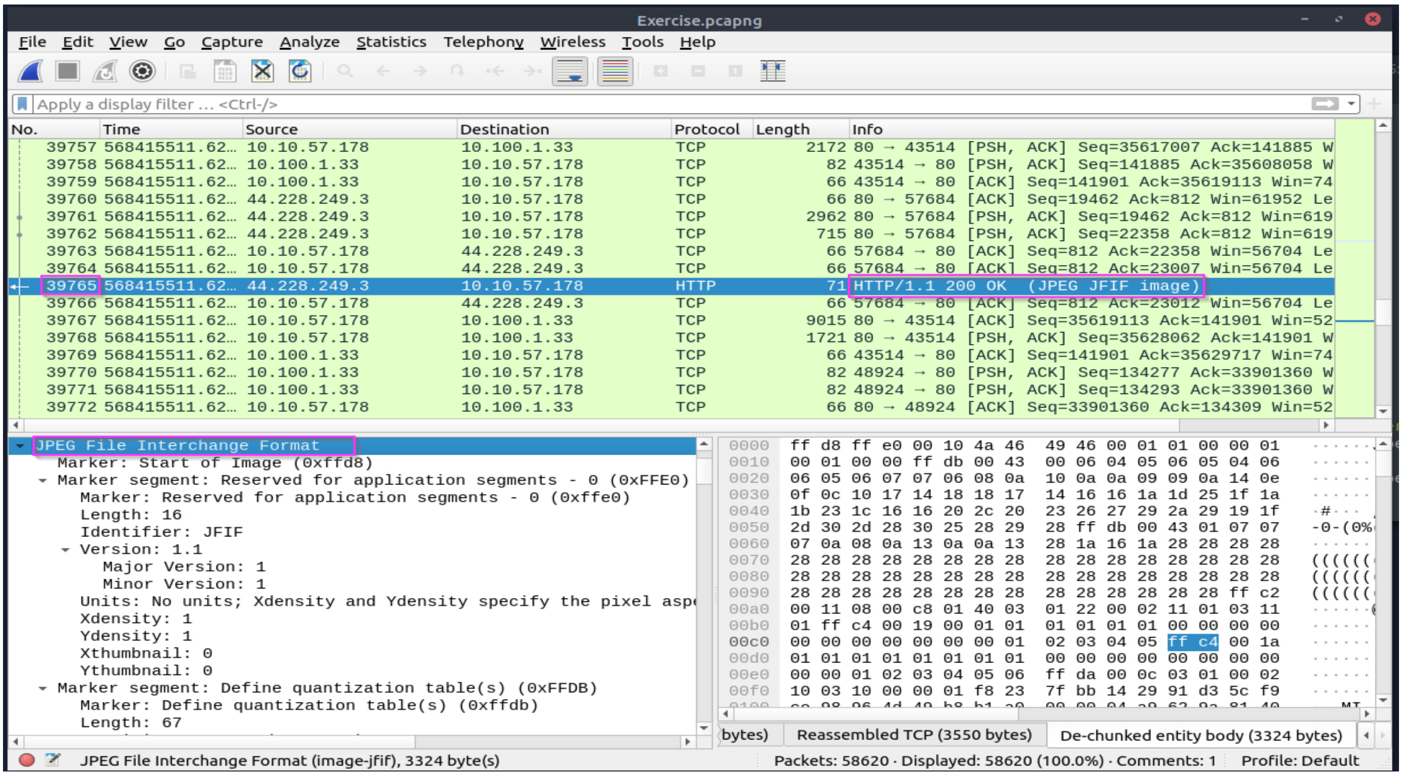
Text item (text), 596 byte(s) | Packets: 58620 · Displayed: 58620 (100.0%) · Comments: 1 | Profile: Default

Go to packet 12 and read the comments. What is the answer?



Wireshark · Packet 12 Comment

Go to packet number 39765
Look at the "packet details pane". Right-click on the JPEG section and "Export packet bytes". This is an alternative way of extracting data from a capture file. What is the MD5 hash value of extracted image?



Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time             Source         Destination    Protocol Length Info
 39757 568415511.62… 10.10.57.178   10.100.1.33    TCP      2172 80 → 43514 [PSH, ACK] Seq=35617007 Ack=141885 W
 39758 568415511.62… 10.100.1.33    10.10.57.178   TCP        82 43514 → 80 [PSH, ACK] Seq=141885 Ack=35608058 W
 39759 568415511.62… 10.100.1.33    10.10.57.178   TCP        66 43514 → 80 [ACK] Seq=141901 Ack=35619113 Win=74
 39760 568415511.62… 44.228.249.3   10.10.57.178   TCP        66 80 → 57684 [ACK] Seq=19462 Ack=812 Win=61952 Le
 39761 568415511.62… 44.228.249.3   10.10.57.178   TCP      2962 80 → 57684 [PSH, ACK] Seq=19462 Ack=812 Win=619
 39762 568415511.62… 44.228.249.3   10.10.57.178   TCP       715 80 → 57684 [PSH, ACK] Seq=22358 Ack=812 Win=619
 39763 568415511.62… 10.10.57.178   44.228.249.3   TCP        66 57684 → 80 [ACK] Seq=812 Ack=22358 Win=56704 Le
 39764 568415511.62… 10.10.57.178   44.228.249.3   TCP        66 57684 → 80 [ACK] Seq=812 Ack=23007 Win=56704 Le
 39765 568415511.62… 44.228.249.3   10.10.57.178   HTTP       71 HTTP/1.1 200 OK  (JPEG JFIF image)
 39766 568415511.62… 10.10.57.178   44.228.249.3   TCP        66 57684 → 80 [ACK] Seq=812 Ack=23012 Win=56704 Le
 39767 568415511.62… 10.10.57.178   10.100.1.33    TCP      9015 80 → 43514 [ACK] Seq=35619113 Ack=141901 Win=52
 39768 568415511.62… 10.10.57.178   10.100.1.33    TCP      1721 80 → 43514 [PSH, ACK] Seq=35628062 Ack=141901 W
 39769 568415511.62… 10.100.1.33    10.10.57.178   TCP        66 43514 → 80 [ACK] Seq=141901 Ack=35629717 Win=74
 39770 568415511.62… 10.100.1.33    10.10.57.178   TCP        82 48924 → 80 [PSH, ACK] Seq=134277 Ack=33901360 W
 39771 568415511.62… 10.100.1.33    10.10.57.178   TCP        82 48924 → 80 [PSH, ACK] Seq=134293 Ack=33901360 W
 39772 568415511.62… 10.10.57.178   10.100.1.33    TCP        66 80 → 48924 [ACK] Seq=33901360 Ack=134309 Win=52
```

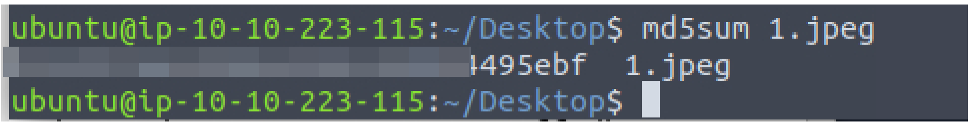
```
▾ JPEG File Interchange Format
    Marker: Start of Image (0xffd8)
  ▾ Marker segment: Reserved for application segments - 0 (0xFFE0)
      Marker: Reserved for application segments - 0 (0xffe0)
      Length: 16
      Identifier: JFIF
    ▾ Version: 1.1
        Major Version: 1
        Minor Version: 1
      Units: No units; Xdensity and Ydensity specify the pixel aspe
      Xdensity: 1
      Ydensity: 1
      Xthumbnail: 0
      Ythumbnail: 0
  ▾ Marker segment: Define quantization table(s) (0xFFDB)
      Marker: Define quantization table(s) (0xffdb)
      Length: 67
```

```
0000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 00 00 01
0010  00 01 00 00 ff db 00 43  00 06 04 05 06 05 04 06
0020  06 05 06 07 07 06 08 0a  10 0a 0a 09 09 0a 14 0e
0030  0f 0c 10 17 14 18 18 17  14 16 16 1a 1d 25 1f 1a
0040  1b 23 1c 16 16 20 2c 20  23 26 27 29 2a 29 19 1f   ·#···
0050  2d 30 2d 28 30 25 28 29  28 ff db 00 43 01 07 07   -0-(0%
0060  07 0a 08 0a 13 0a 0a 13  28 1a 16 1a 28 28 28 28
0070  28 28 28 28 28 28 28 28  28 28 28 28 28 28 28 28   ((((((
0080  28 28 28 28 28 28 28 28  28 28 28 28 28 28 28 28   ((((((
0090  28 28 28 28 28 28 28 28  28 28 28 28 28 28 ff c2   ((((((
00a0  00 11 08 00 c8 01 40 03  01 22 00 02 11 01 03 11
00b0  01 ff c4 00 19 00 01 01  01 01 01 01 00 00 00 00
00c0  00 00 00 00 00 00 00 01  02 03 04 05 ff c4 00 1a
00d0  01 01 01 01 01 01 01 01  00 00 00 00 00 00 00 00
00e0  00 00 01 02 03 04 05 06  ff da 00 0c 03 01 00 02
00f0  10 03 10 00 00 01 f8 23  7f bb 14 29 91 d3 5c f9
```

bytes) | Reassembled TCP (3550 bytes) | De-chunked entity body (3324 bytes)

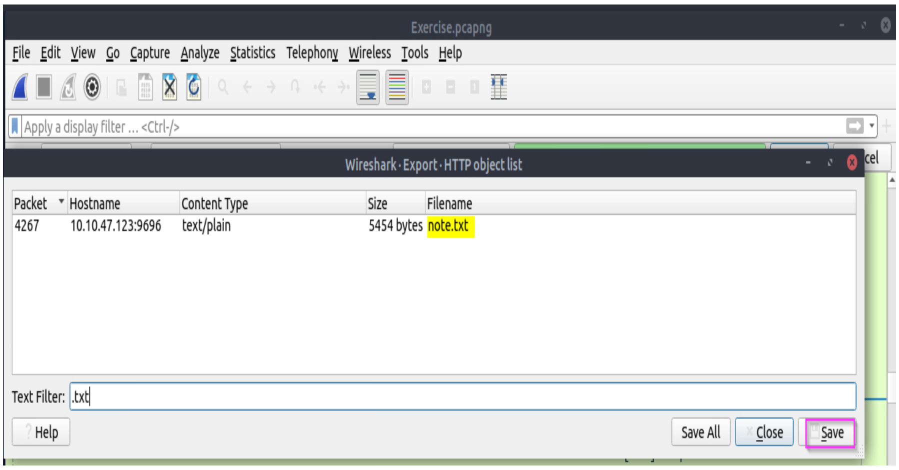
JPEG File Interchange Format (image-jfif), 3324 byte(s)

Packets: 58620 · Displayed: 58620 (100.0%) · Comments: 1   Profile: Default



```
ubuntu@ip-10-10-223-115:~/Desktop$ md5sum 1.jpeg
[redacted]495ebf  1.jpeg
ubuntu@ip-10-10-223-115:~/Desktop$ 
```

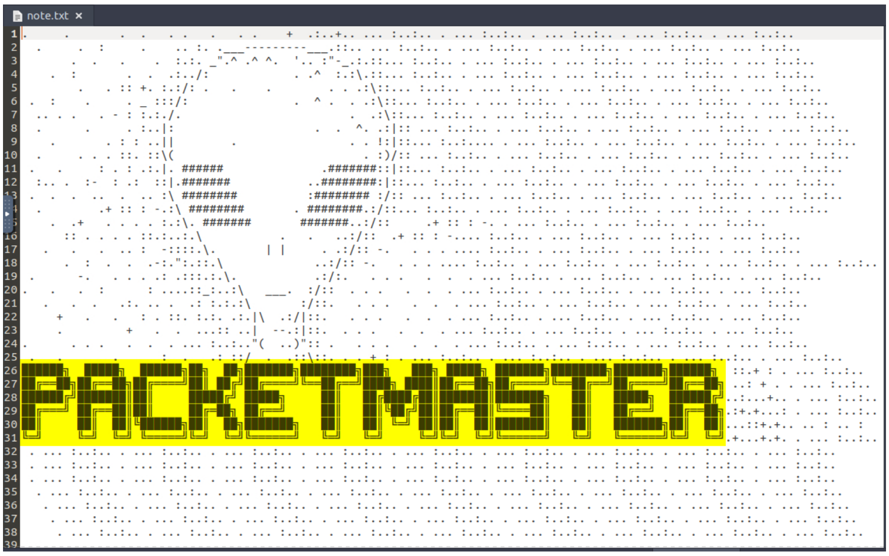
There is a **".txt"** file inside the capture file. Find the file and read it; what is the alien's name?



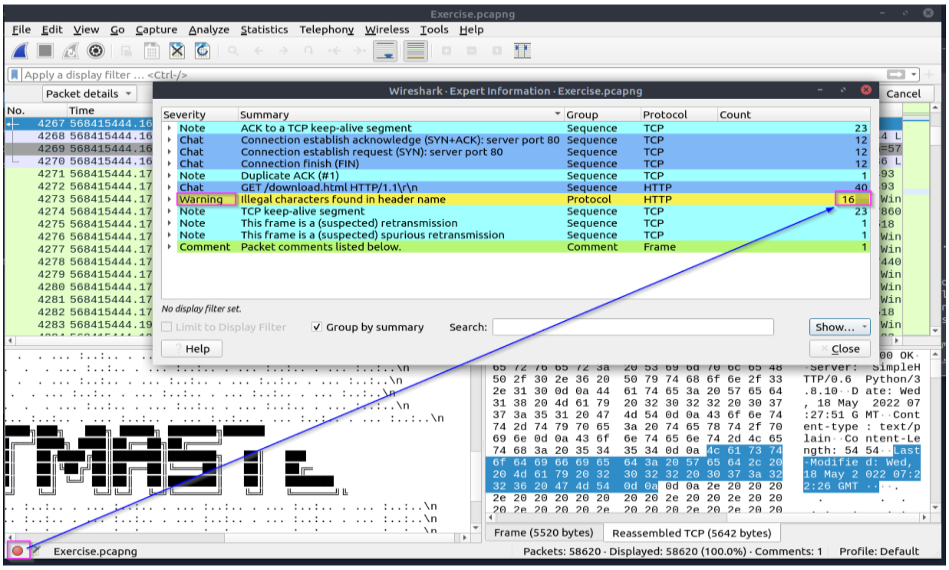
Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
4267	10.10.47.123:9696	text/plain	5454 bytes	note.txt

Text Filter: .txt



Look at the expert info section. What is the number of warnings?



Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Packet details
Wireshark · Expert Information · Exercise.pcapng

Severity	Summary	Group	Protocol	Count
Note	ACK to a TCP keep-alive segment	Sequence	TCP	23
Chat	Connection establish acknowledge (SYN+ACK): server port 80	Sequence	TCP	12
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	12
Chat	Connection finish (FIN)	Sequence	TCP	12
Note	Duplicate ACK (#1)	Sequence	TCP	1
Chat	GET /download.html HTTP/1.1\r\n	Sequence	HTTP	40
Warning	Illegal characters found in header name	Protocol	HTTP	16
Note	TCP keep-alive segment	Sequence	TCP	23
Note	This frame is a (suspected) retransmission	Sequence	TCP	1
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1
Comment	Packet comments listed below.	Comment	Frame	1

No display filter set.

□ Limit to Display Filter ☑ Group by summary Search:

Packets: 58620 · Displayed: 58620 (100.0%) · Comments: 1 Profile: Default