WIRESHARK

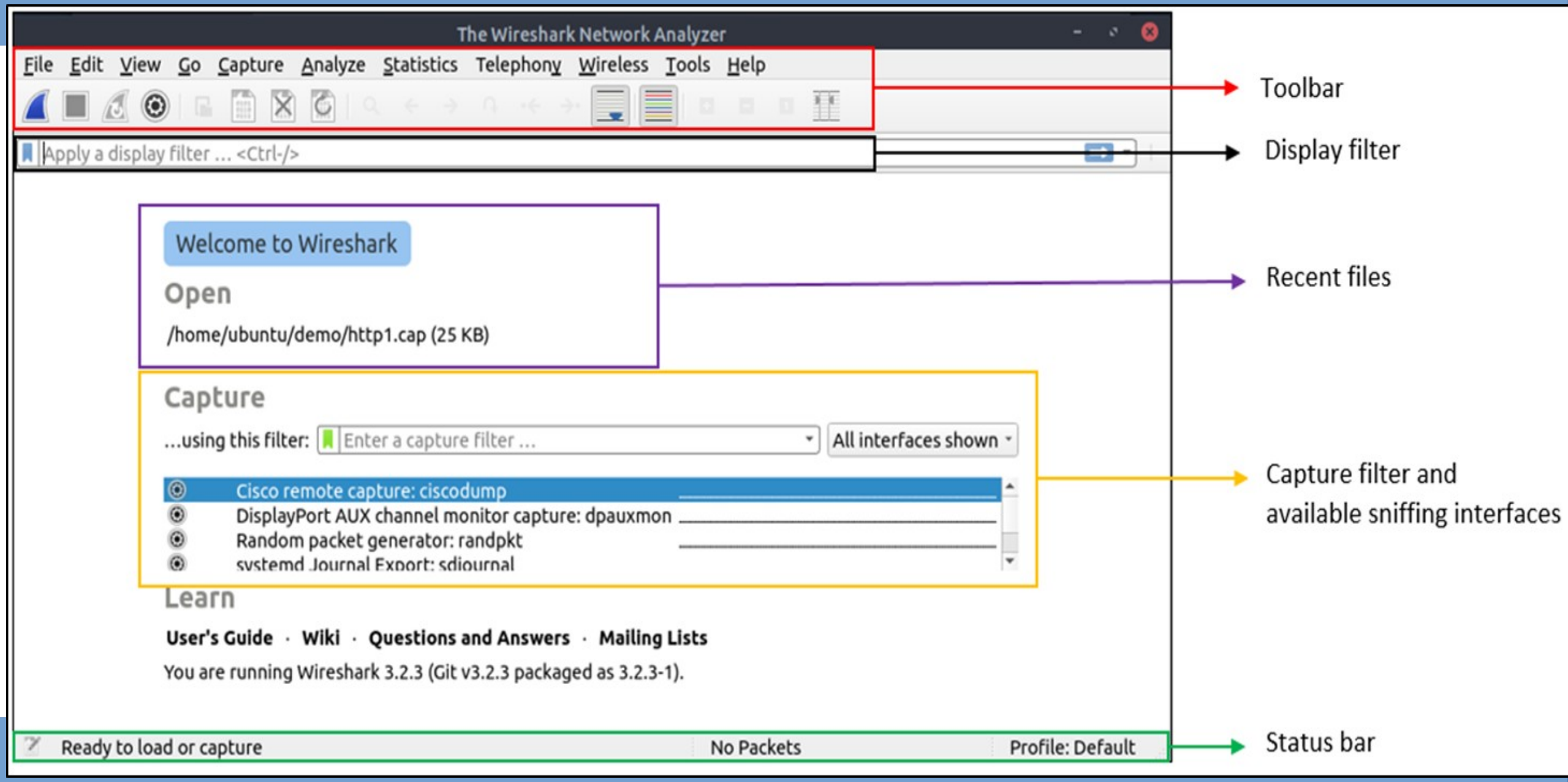
Qu’est-ce que c’est?

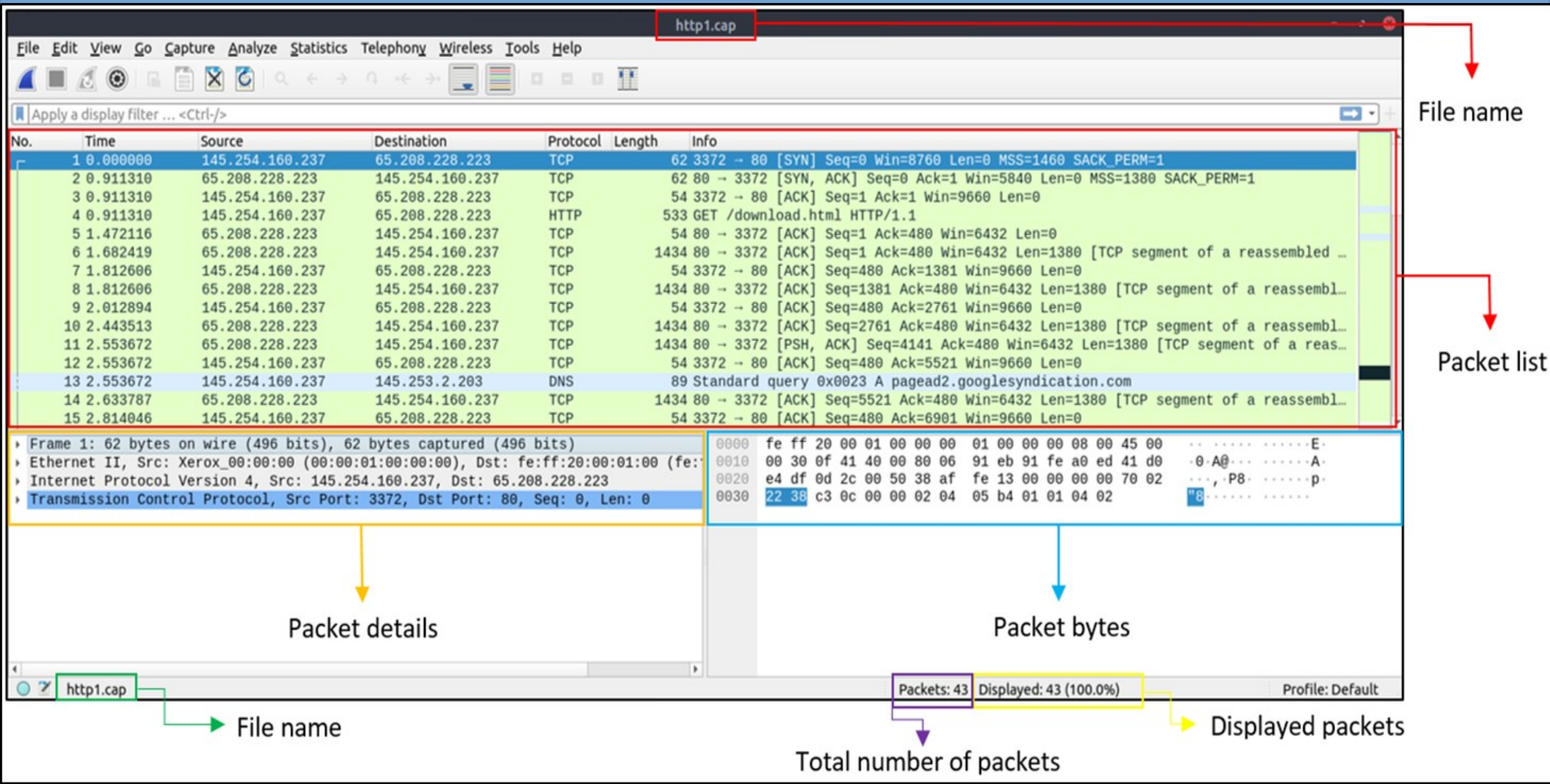
- logiciel open source d’analyse des protocoles réseaux (Gérald Combes, **1998**);
- un outil de capture et d’analyse de paquets (Windows, Linux, macOs);
- peut capturer trafic Ethernet, Bluetooth, sans fil (IEEE.**802.11**), Token Ring, Frame Relay et plus encore;
- utilisé par:
  - des agences gouvernementales,
  - des entreprises,
  - des organisations à but non lucratif,
  - des établissements pédagogiques (problèmes réseau et formations);

Red Team: **Network Sniffing**
(utiliser l'interface réseau d'un système pour surveiller ou capturer des informations transmises par une connexion câblée ou sans fil)

Blue Team: Analyse de traffic réseau

Présentation de l’interface


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
/home/ubuntu/demo/http1.cap (25 KB)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).
Ready to load or capture
No Packets
Profile: Default
Toolbar
Display filter
Recent files
Capture filter and
available sniffing interfaces
Status bar


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
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
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
http1.cap
Packets: 43
Displayed: 43 (100.0%)
Profile: Default
File name
Packet list
Packet details
Packet bytes
File name
Total number of packets
Displayed packets

- **Volet “Liste des paquets”:**

Résumé de chaque paquet (adresses source et destination, protocole et informations sur le paquet). Vous pouvez cliquer sur la liste pour choisir un paquet pour une investigation plus approfondie. Une fois que vous avez sélectionné un paquet, les détails apparaissent dans les autres panneaux.

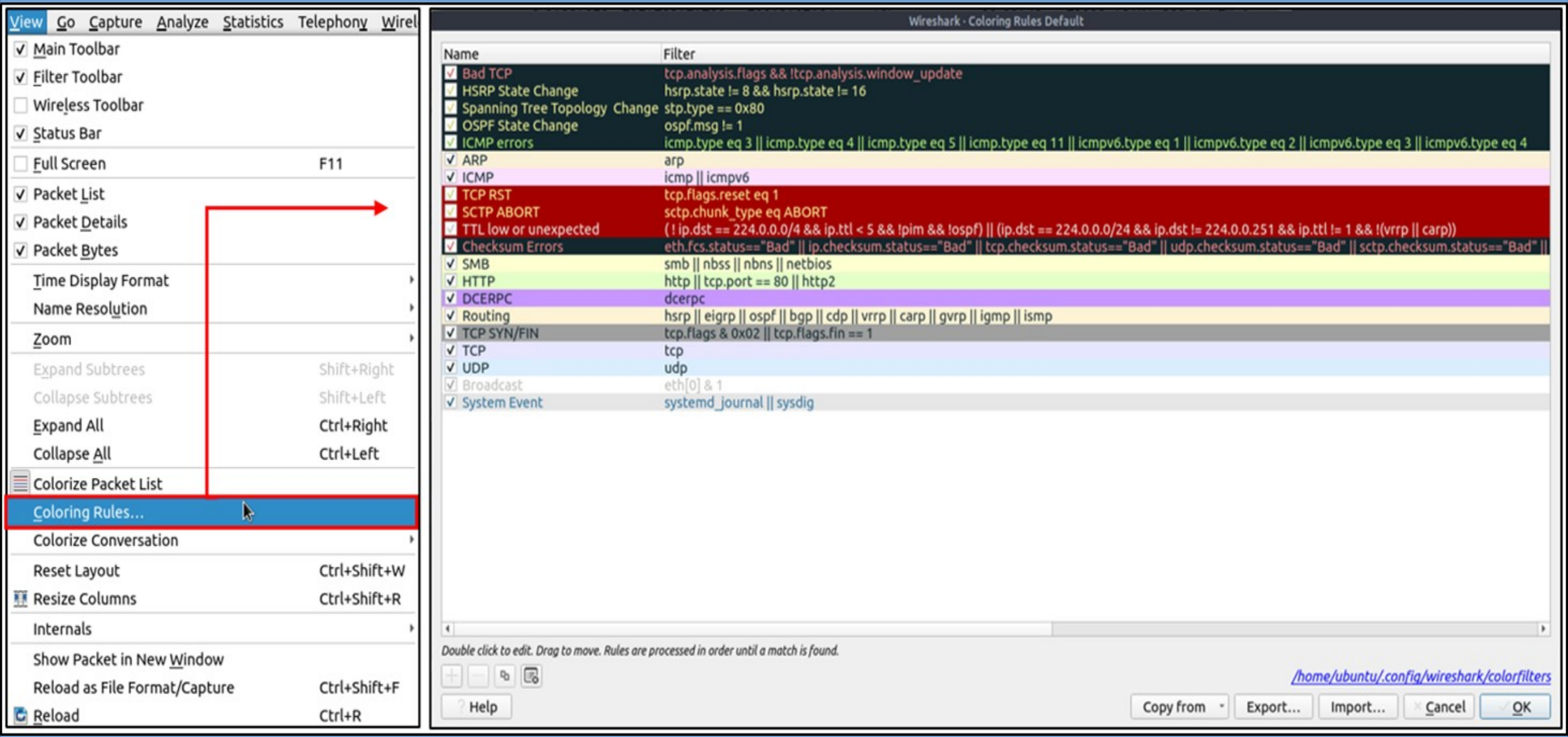
- **Panneau “Détails du paquet”:**

Détails liés au protocole du paquet sélectionné.

- **Volet “Octets du paquet”:**

Permet d’avoir un aperçu du paquet au format hexadécimal. Cela reprend l’ensemble des infos du détail d’un paquet, avec l’écriture hexadécimale à gauche et la correspondance à droite au niveau de la donnée applicative, à condition que la donnée ne soit pas chiffrée.

Coloration des paquets


View
Go
Capture
Analyze
Statistics
Telephony
Wirel
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
Wireshark · Coloring Rules Default
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" ||
SMB
smb || nbss || nbns || netbios
HTTP
http || tcp.port == 80 || http2
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
System Event
systemd_journal || sysdig
Double click to edit. Drag to move. Rules are processed in order until a match is found.
/home/ubuntu/.config/wireshark/colorfilters
Help
Copy from
Export...
Import...
Cancel
OK

- un paquet qui apparaîtra en jaune pâle sera un paquet qui matchera avec le filtre "ARP" (protocole) ;

- Les paquets apparaissant en rouge avec une écriture blanche concernent en revanche des problèmes de TTL ;

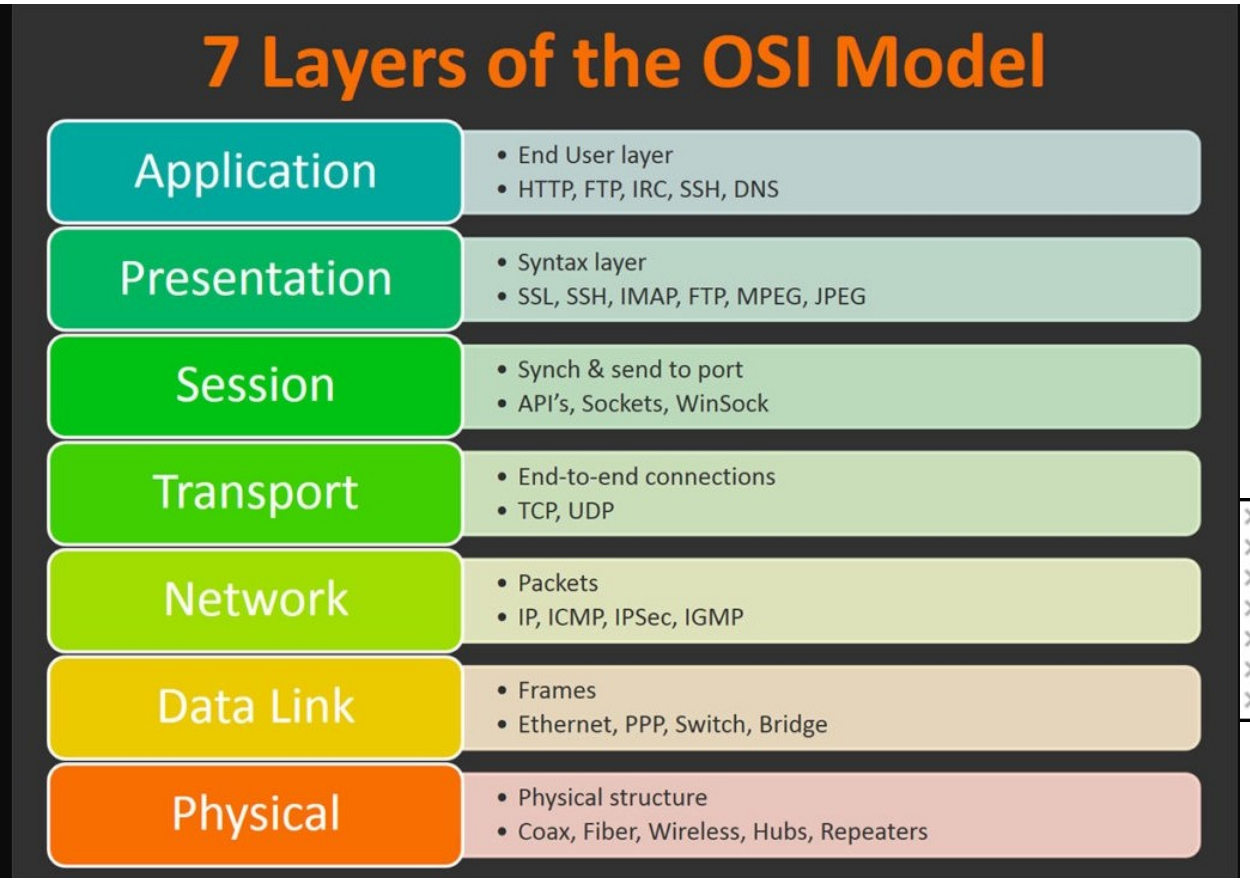
- les paquets rouges avec une écriture jaune les TCP avec le flag RST à 1 ou les SCTP ABORT, etc.

cliquez sur Affichage> Règles de coloration (View > Coloring Rules). Vous pouvez également y personnaliser et modifier les règles de coloration si vous le souhaitez.

Détail des paquets

- Vous pouvez cliquer sur un paquet dans le panneau de la liste des paquets pour ouvrir ses détails (un double-clic ouvrira les détails dans une nouvelle fenêtre).

- Les paquets sont composés de **5** à **7** couches basées sur le modèle OSI.

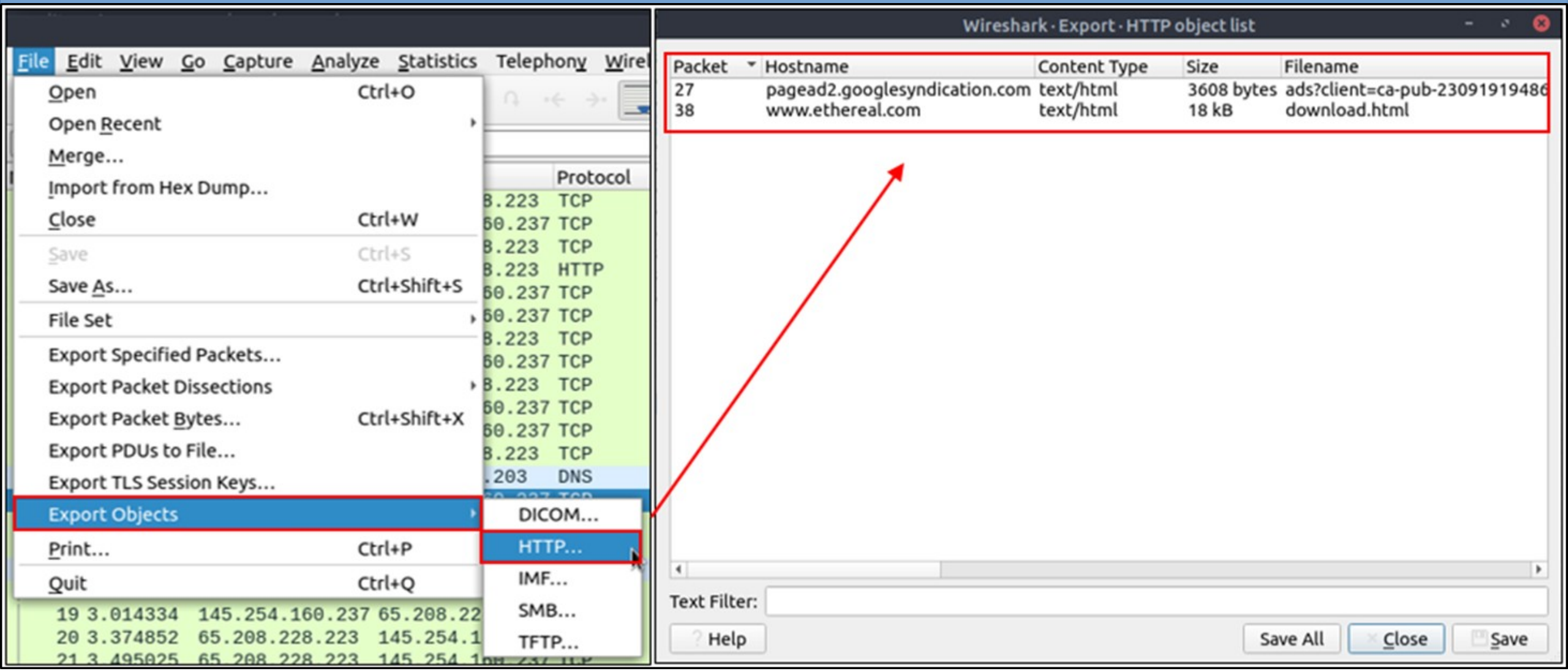



```
> Frame 27: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
> Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:00:01:00:00:00)
> Internet Protocol Version 4, Src: 216.239.59.99, Dst: 145.254.160.237
> Transmission Control Protocol, Src Port: 80, Dst Port: 3371, Seq: 778787098, Ack: 918692089, Len: 160
> [2 Reassembled TCP Segments (1590 bytes): #26(1430), #27(160)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (3 lines)
```

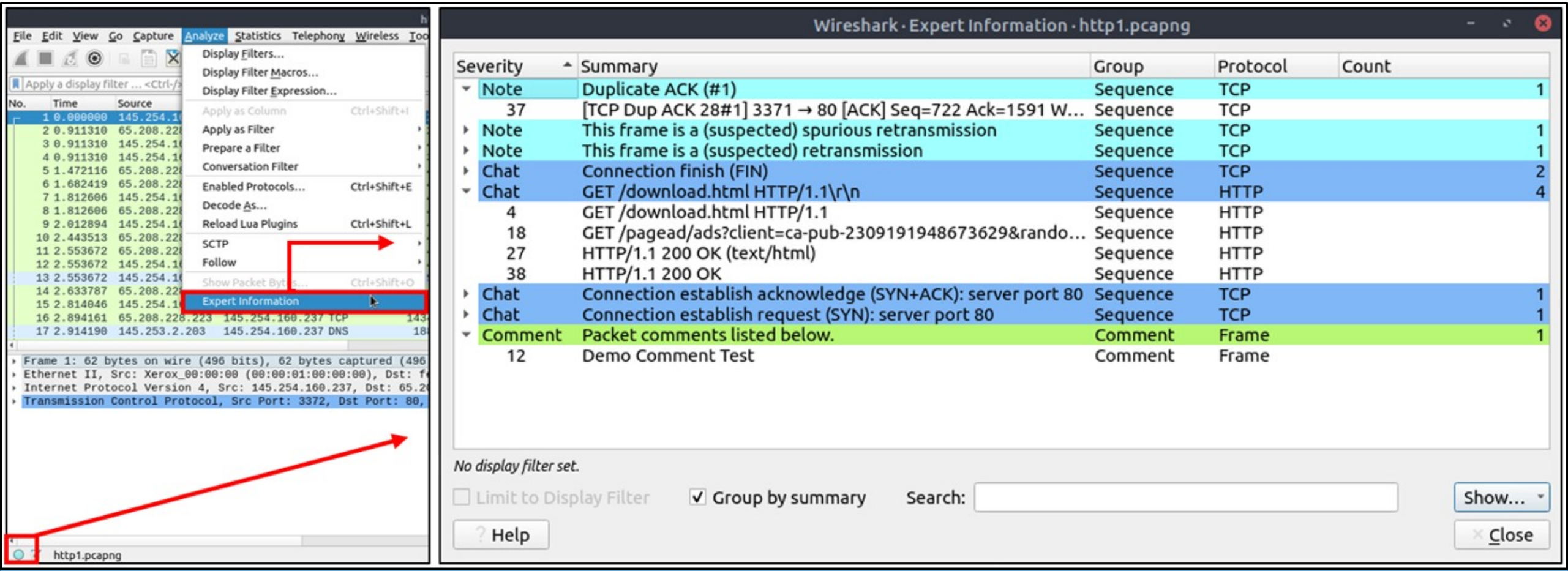
Exporter des objets

- Wireshark peut extraire les fichiers transférés par les échanges.

- L'exportation d'objets est disponible uniquement pour les flux de protocoles sélectionnés (DICOM, HTTP, IMF, SMB et TFTP).


File Edit View Go Capture Analyze Statistics Telephony Wirel
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Protocol
TCP
HTTP
DNS
19 3.014334 145.254.160.237 65.208.22
20 3.374852 65.208.228.223 145.254.1
Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
27 pagead2.googlesyndication.com text/html 3608 bytes ads?client=ca-pub-2309191948
38 www.ethereal.com text/html 18 kB download.html
Text Filter:
Help
Save All
Close
Save

Section « infos d’expert »


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
Apply a display filter ... <Ctrl-/>
No. Time Source
1 0.000000 145.254.1
2 0.911310 65.208.22
3 0.911310 145.254.1
4 0.911310 145.254.1
5 1.472116 65.208.22
6 1.682419 65.208.22
7 1.812606 145.254.1
8 1.812606 65.208.22
9 2.012894 145.254.1
10 2.443513 65.208.22
11 2.553672 65.208.22
12 2.553672 145.254.1
13 2.553672 145.254.1
14 2.633787 65.208.22
15 2.814046 145.254.1
16 2.894161 65.208.228.223 145.254.160.237 TCP
17 2.914190 145.253.2.203 145.254.160.237 DNS
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: f
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.2
Transmission Control Protocol, Src Port: 3372, Dst Port: 80,
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:
Show...
Help
Close

- **Chat: Informations sur le flux de travail habituel, par exemple, un paquet TCP avec le drapeau SYN activé.**
- **Note: Événements notables, par exemple, une application a renvoyé un code d'erreur commun tel que HTTP 404.**
- **Avertissement: Avertissements, par exemple, une application a renvoyé un code d'erreur inhabituel comme un problème de connexion.**
- **Erreur: Problèmes graves, tels que des paquets mal formés.**

Filtrage des paquets

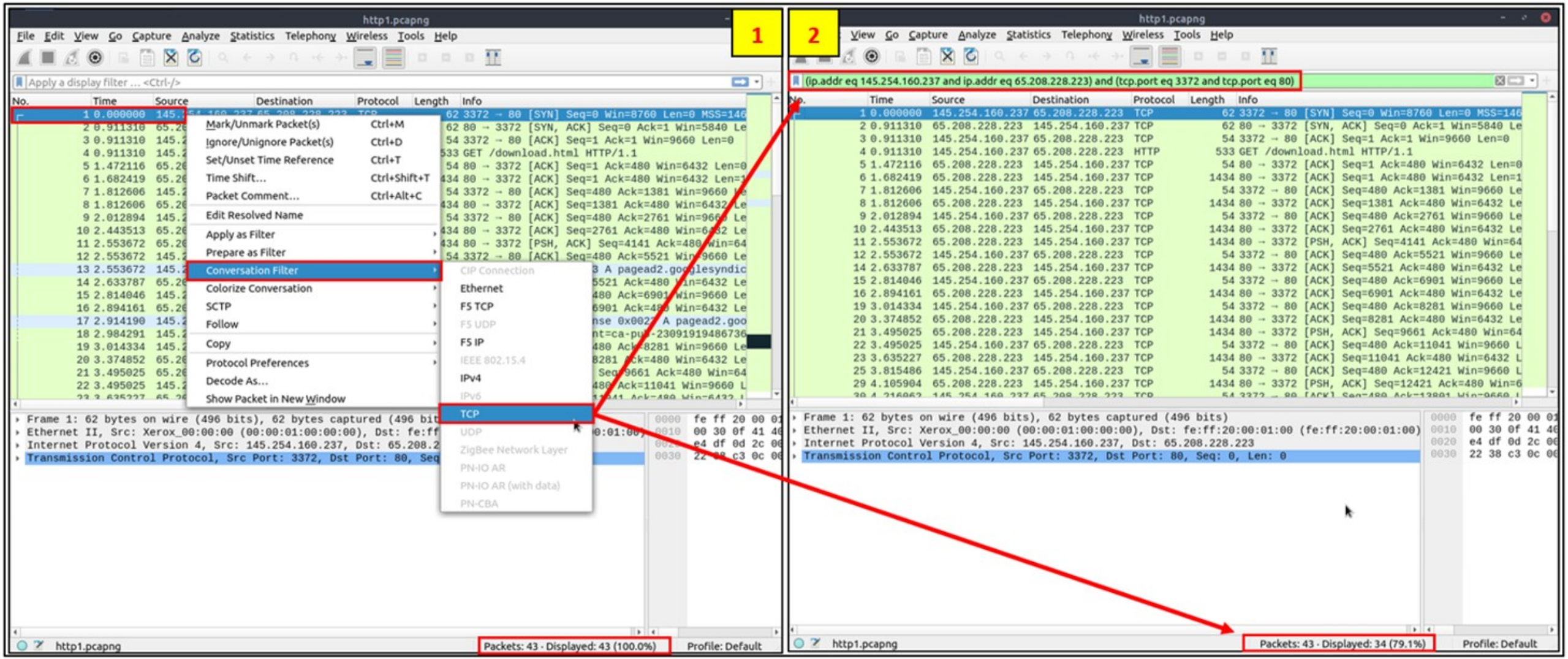
- puissant moteur de filtrage qui aide les analystes à réduire le trafic et à se concentrer sur l'événement qui les intéresse;

- Deux façons différentes de filtrer le trafic et de supprimer le bruit du fichier de capture:
  - utiliser le menu de clic droit
  - les requêtes.

1. Filtre de conversation

- Par ex: ne voir que les adresses IP et les numéros de port (en cachant le reste des paquets).

- *Vous pouvez utiliser le menu "clic droit" ou le menu **"Analyse --> Filtre de conversation"** pour filtrer les conversations.*


http1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
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
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
13 2.553672 145.254.160.237 65.208.228.223 TCP 3 A pagead2.googlesyndic
14 2.633787 65.208.228.223 145.254.160.237 TCP 5521 Ack=480 Win=6432 Le
15 2.814046 145.254.160.237 65.208.228.223 TCP 480 Ack=6901 Win=9660 Le
16 2.894161 65.208.228.223 145.254.160.237 TCP 6901 Ack=480 Win=6432 Le
17 2.914190 145.254.160.237 65.208.228.223 TCP nse 0x0023 A pagead2.goo
18 2.984291 145.254.160.237 65.208.228.223 TCP nt=ca-pub-2309191948673
19 3.014334 145.254.160.237 65.208.228.223 TCP 480 Ack=8281 Win=9660 Le
20 3.374852 65.208.228.223 145.254.160.237 TCP 8281 Ack=480 Win=6432 Le
21 3.495025 65.208.228.223 145.254.160.237 TCP Seq=9661 Ack=480 Win=64
22 3.495025 145.254.160.237 65.208.228.223 TCP 480 Ack=11041 Win=9660 L
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
CIP Connection
Ethernet
F5 TCP
F5 UDP
F5 IP
IEEE 802.15.4
IPv4
IPv6
TCP
UDP
ZigBee Network Layer
PN-IO AR
PN-IO AR (with data)
PN-CBA
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
0010 00 30 0f 41 40
0020 e4 df 0d 2c 00
0030 22 38 c3 0c 00
http1.pcapng
Packets: 43 · Displayed: 43 (100.0%)
Profile: Default
1
2
http1.pcapng
View Go Capture Analyze Statistics Telephony Wireless Tools Help
(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=1460
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
0000 fe ff 20 00 01
0010 00 30 0f 41 40
0020 e4 df 0d 2c 00
0030 22 38 c3 0c 00
http1.pcapng
Packets: 43 · Displayed: 34 (79.1%)
Profile: Default

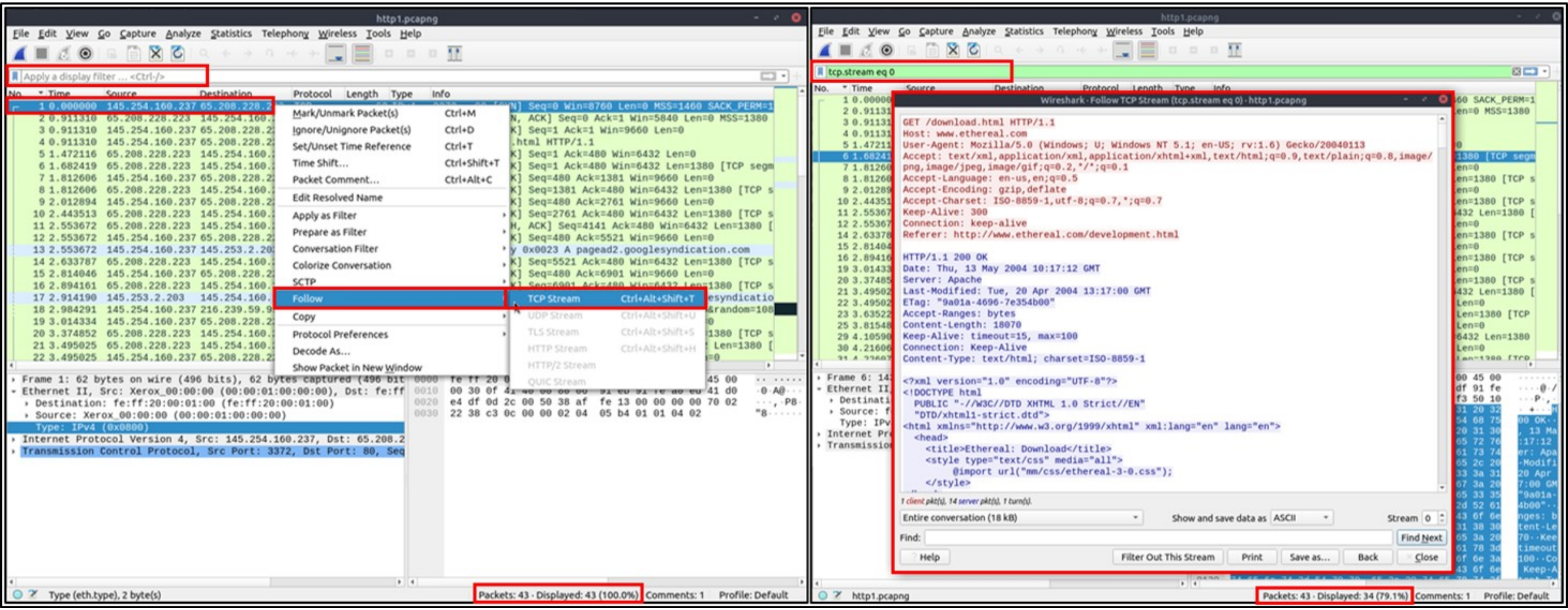
2. Suivre le flux

- pour reconstruire les flux et de visualiser le trafic brut tel qu'il se présente au niveau de l'application;

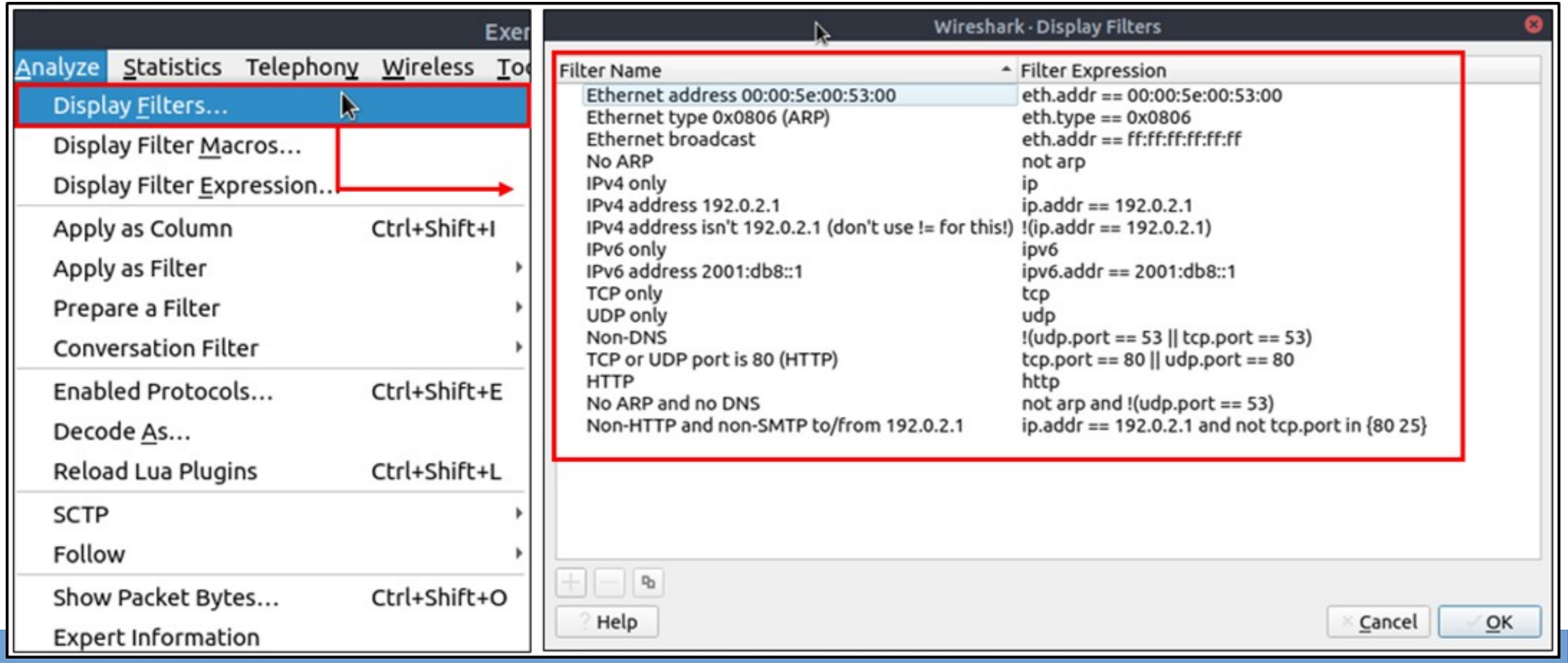
- recréer les données au niveau de l'application et à comprendre l'événement qui nous intéresse (visualiser données non cryptées pour certains protocoles: noms d'utilisateur, mots de passe, etc...);

- *Vous pouvez utiliser le menu "clic droit" ou le menu "Analyse --> Suivre le flux TCP/UDP/HTTP" pour suivre les flux de trafic;*

- les paquets provenant du serveur sont surlignés en bleu, et ceux provenant du client en rouge.


http1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Type Info
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
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 Version 4, Src: 145.254.160.237, Dst: 65.208.2
Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq
Type (eth.type), 2 byte(s)
Packets: 43 · Displayed: 43 (100.0%)
Comments: 1
Profile: Default
http1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
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
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close
http1.pcapng
Packets: 43 · Displayed: 34 (79.1%)
Comments: 1
Profile: Default

Syntaxe des filtres


Analyze
Statistics
Telephony
Wireless
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
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00 eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP) eth.type == 0x0806
Ethernet broadcast eth.addr == ff:ff:ff:ff:ff:ff
No ARP not arp
IPv4 only ip
IPv4 address 192.0.2.1 ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!) !(ip.addr == 192.0.2.1)
IPv6 only ipv6
IPv6 address 2001:db8::1 ipv6.addr == 2001:db8::1
TCP only tcp
UDP only udp
Non-DNS !(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP) tcp.port == 80 || udp.port == 80
HTTP http
No ARP and no DNS not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1 ip.addr == 192.0.2.1 and not tcp.port in {80 25}
Help
Cancel
OK

Opérateurs de comparaison

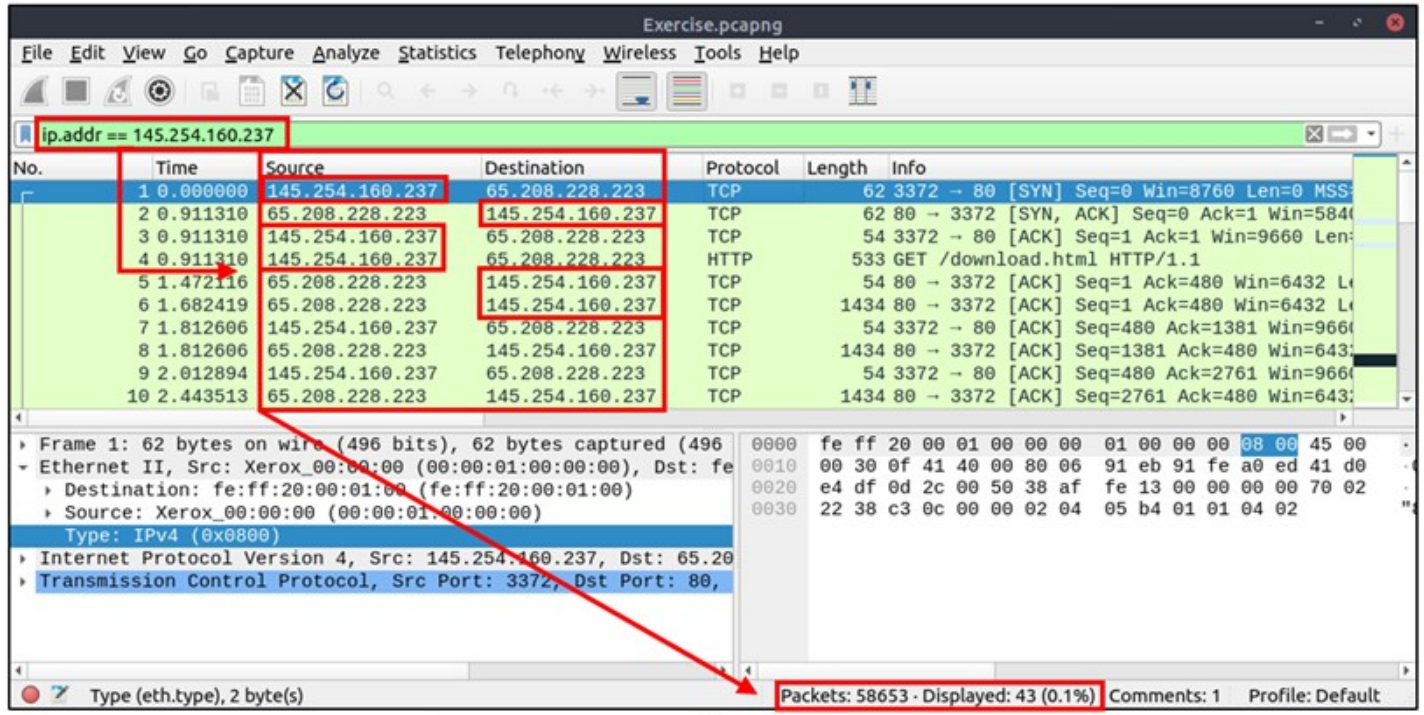
English	C-Like	Description	Example
eq	==	Equal	`ip.src == 10.10.10.100`
ne	!=	Not equal	`ip.src != 10.10.10.100`
gt	>	Greater than	`ip.ttl > 250`
lt	<	Less Than	`ip.ttl < 10`
ge	>=	Greater than or equal to	`ip.ttl >= 0xFA`
le	<=	Less than or equal to	`ip.ttl <= 0xA`

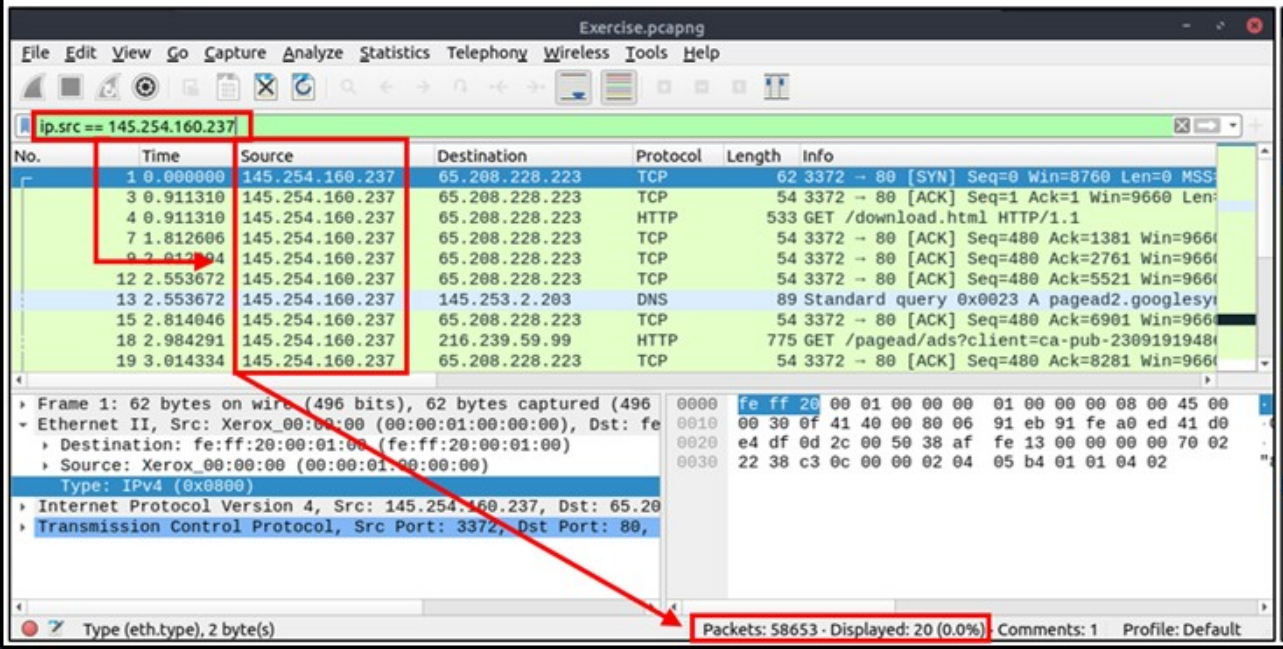
Opérateurs logiques

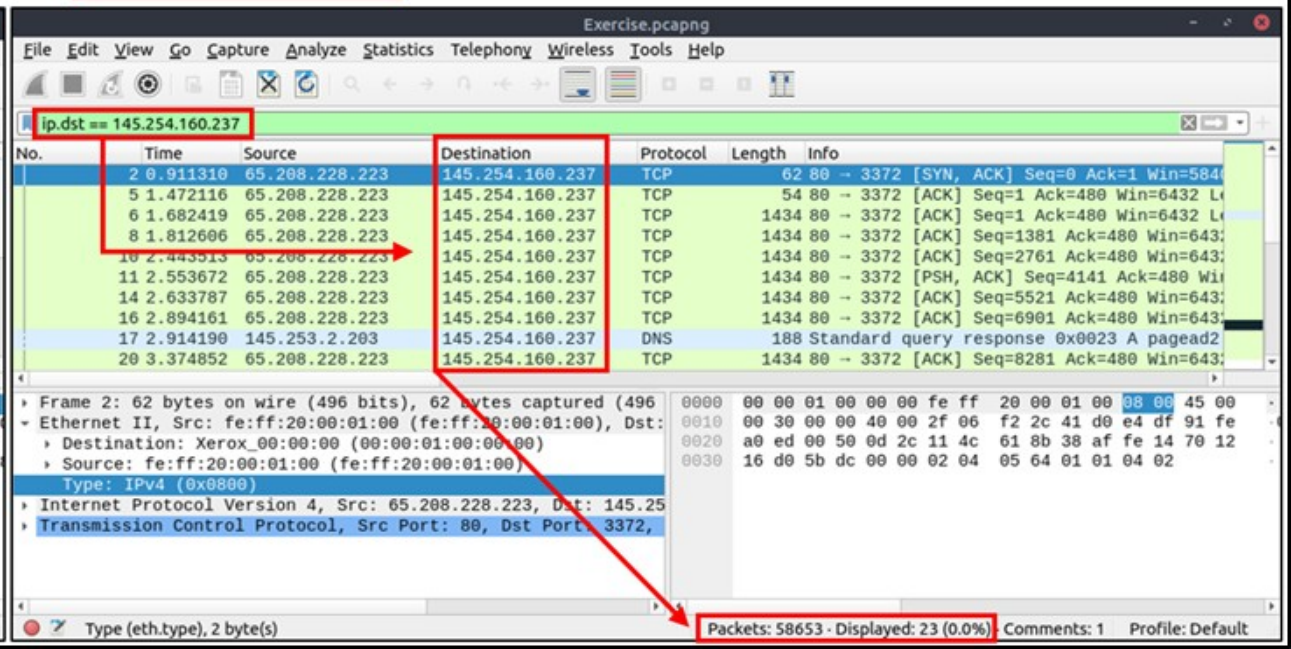
English	C-Like	Description	Example
and	&&	Logical AND	`(ip.src == 10.10.10.100) AND (ip.src == 10.10.10.111)`
or	||	Logical OR	`(ip.src == 10.10.10.100) OR (ip.src == 10.10.10.111)`
not	!	Logical NOT	`!(ip.src == 10.10.10.222)` **Note:** Usage of `!=value` is deprecated; using it could provide inconsistent results. Using the `!(value)` style is suggested for more consistent results.

Exemples de filtres selon différents protocoles:

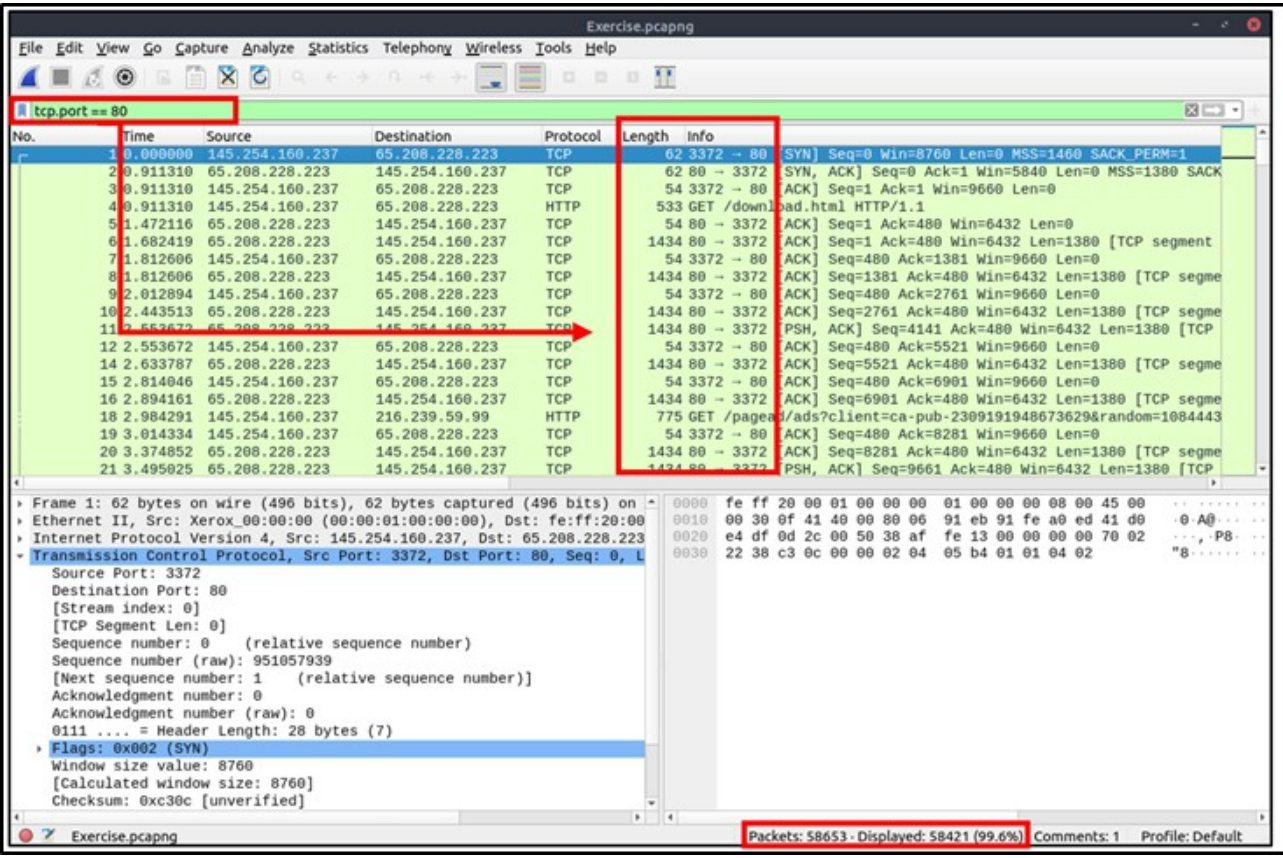
Filter	Description
`ip`	Show all IP packets.
`ip.addr == 10.10.10.111`	Show all packets containing IP address 10.10.10.111.
`ip.addr == 10.10.10.0/24`	Show all packets containing IP addresses from 10.10.10.0/24 subnet.
`ip.src == 10.10.10.111`	Show all packets originated from 10.10.10.111
`ip.dst == 10.10.10.111`	Show all packets sent to 10.10.10.111
ip.addr vs ip.src/ip.dst	**Note:** The ip.addr filters the traffic without considering the packet direction. The ip.src/ip.dst filters the packet depending on the packet direction.

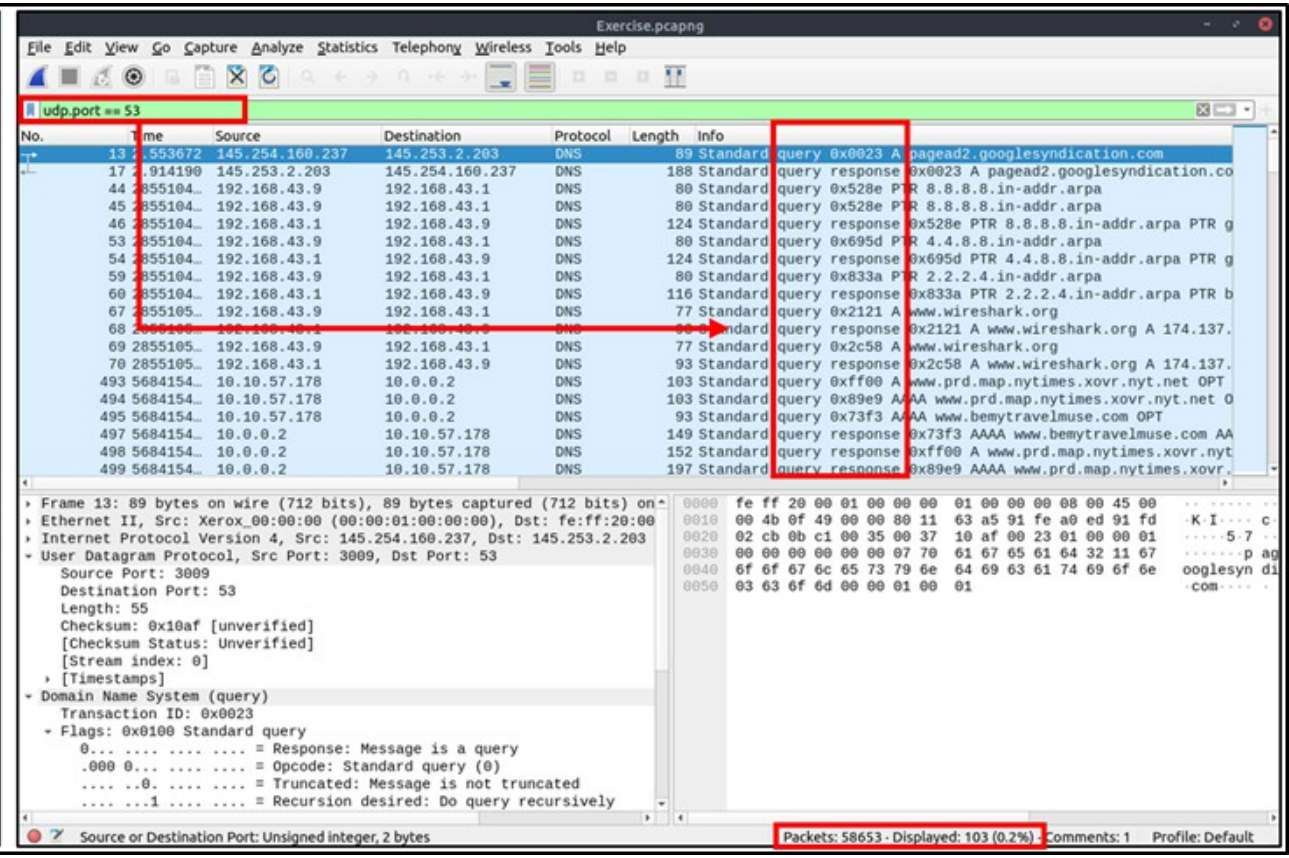

Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 145.254.160.237
No. Time Source Destination Protocol Length Info
1 0.000000 145.254.160.237 65.208.228.223 TCP 62 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS
2 0.911310 65.208.228.223 145.254.160.237 TCP 62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=584
3 0.911310 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len
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 L
6 1.682419 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 L
7 1.812606 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=1381 Win=966
8 1.812606 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=1381 Ack=480 Win=643
9 2.012894 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=2761 Win=966
10 2.443513 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=643
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe
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 Version 4, Src: 145.254.160.237, Dst: 65.20
Transmission Control Protocol, Src Port: 3372, Dst Port: 80,
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: 58653 · Displayed: 43 (0.1%)
Comments: 1
Profile: Default


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
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
3 0.911310 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len
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=966
12 2.553672 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=966
13 2.553672 145.254.160.237 145.253.2.203 DNS 89 Standard query 0x0023 A pagead2.googlesy
15 2.814046 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=6901 Win=966
18 2.984291 145.254.160.237 216.239.59.99 HTTP 775 GET /pagead/ads?client=ca-pub-2309191948
19 3.014334 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=8281 Win=966
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe
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 Version 4, Src: 145.254.160.237, Dst: 65.20
Transmission Control Protocol, Src Port: 3372, Dst Port: 80,
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: 58653 · Displayed: 20 (0.0%)
Comments: 1
Profile: Default

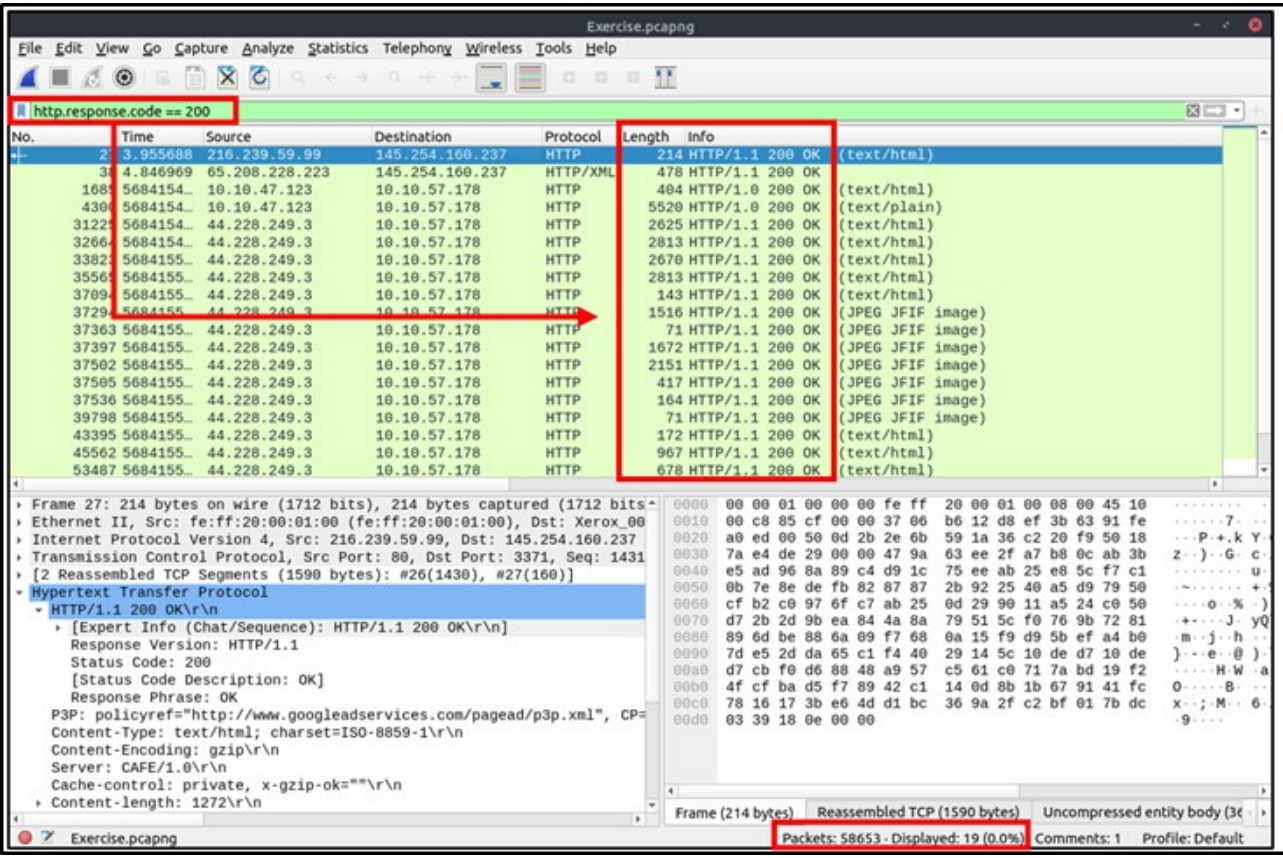

Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 145.254.160.237
No. Time Source Destination Protocol Length Info
2 0.911310 65.208.228.223 145.254.160.237 TCP 62 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=584
5 1.472116 65.208.228.223 145.254.160.237 TCP 54 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 L
6 1.682419 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 L
8 1.812606 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=1381 Ack=480 Win=643
10 2.443513 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=2761 Ack=480 Win=643
11 2.553672 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Wi
14 2.633787 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=5521 Ack=480 Win=643
16 2.894161 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=6901 Ack=480 Win=643
17 2.914190 145.253.2.203 145.254.160.237 DNS 188 Standard query response 0x0023 A pagead2
20 3.374852 65.208.228.223 145.254.160.237 TCP 1434 80 → 3372 [ACK] Seq=8281 Ack=480 Win=643
Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496
Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst:
Destination: Xerox_00:00:00 (00:00:01:00:00:00)
Source: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 65.208.228.223, Dst: 145.25
Transmission Control Protocol, Src Port: 80, Dst Port: 3372,
0000 00 00 01 00 00 00 fe ff 20 00 01 00 08 00 45 00
0010 00 30 00 00 40 00 2f 06 f2 2c 41 d0 e4 df 91 fe
0020 a0 ed 00 50 0d 2c 11 4c 61 8b 38 af fe 14 70 12
0030 16 d0 5b dc 00 00 02 04 05 64 01 01 04 02
Type (eth.type), 2 byte(s)
Packets: 58653 · Displayed: 23 (0.0%)
Comments: 1
Profile: Default

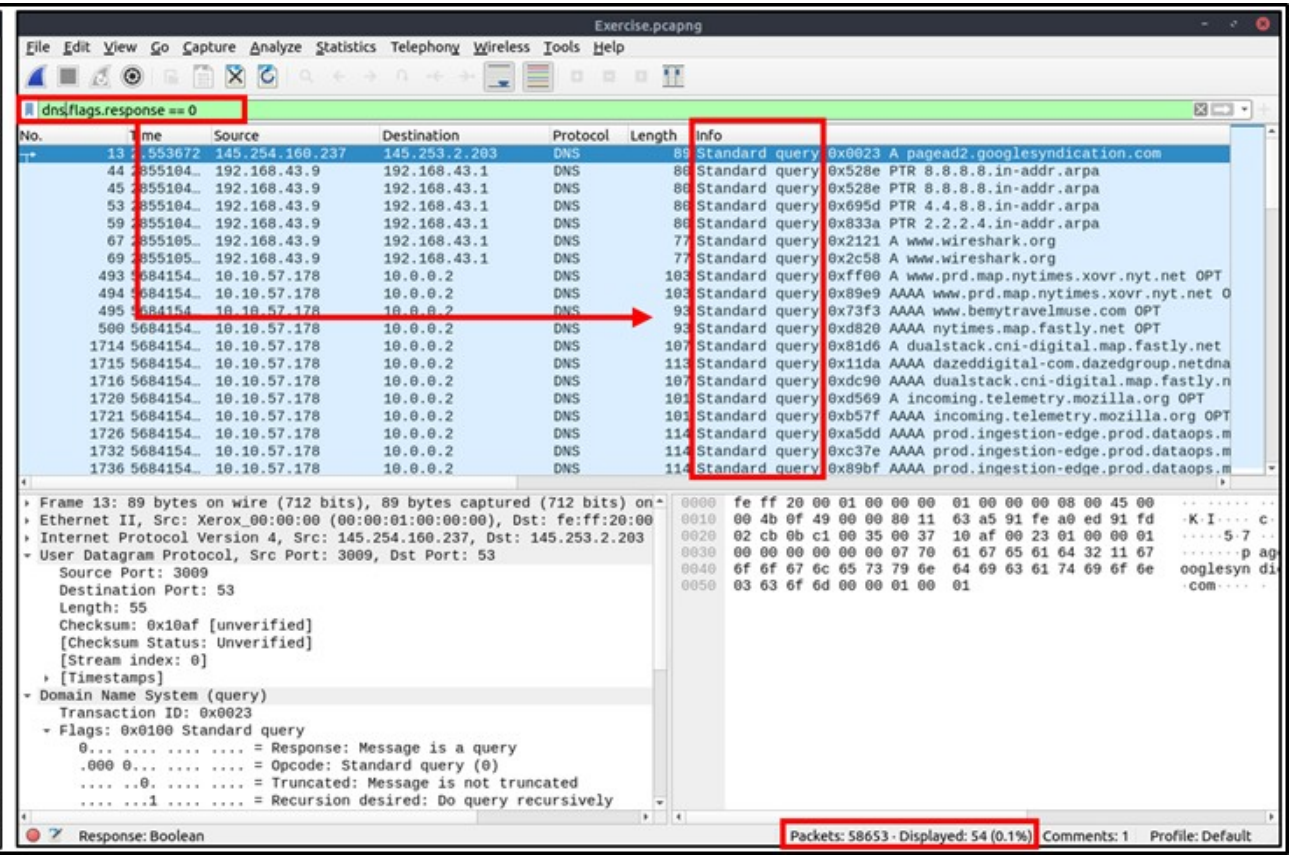
Filter	Description	Filter	Expression
`tcp.port == 80`	Show all TCP packets with port 80	`udp.port == 53`	Show all UDP packets with port 53
`tcp.srcport == 1234`	Show all TCP packets originating from port 1234	`udp.srcport == 1234`	Show all UDP packets originating from port 1234
`tcp.dstport == 80`	Show all TCP packets sent to port 80	`udp.dstport == 5353`	Show all UDP packets sent to port 5353


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 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=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
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
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 segme
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 segme
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
12 2.553672 145.254.160.237 65.208.228.223 TCP 54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
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 segme
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 segme
18 2.984291 145.254.160.237 216.239.59.99 HTTP 775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443
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 segme
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
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00
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, L
Source Port: 3372
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 951057939
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
0111 .... = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
Window size value: 8760
[Calculated window size: 8760]
Checksum: 0xc30c [unverified]
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
Exercise.pcapng
Packets: 58653 · Displayed: 58421 (99.6%)
Comments: 1
Profile: Default


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port == 53
No. Time Source Destination Protocol Length Info
13 2.553672 145.254.160.237 145.253.2.203 DNS 89 Standard query 0x0023 A pagead2.googlesyndication.com
17 2.914190 145.253.2.203 145.254.160.237 DNS 188 Standard query response 0x0023 A pagead2.googlesyndication.co
44 2855104… 192.168.43.9 192.168.43.1 DNS 80 Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
45 2855104… 192.168.43.9 192.168.43.1 DNS 80 Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
46 2855104… 192.168.43.1 192.168.43.9 DNS 124 Standard query response 0x528e PTR 8.8.8.8.in-addr.arpa PTR g
53 2855104… 192.168.43.9 192.168.43.1 DNS 80 Standard query 0x695d PTR 4.4.8.8.in-addr.arpa
54 2855104… 192.168.43.1 192.168.43.9 DNS 124 Standard query response 0x695d PTR 4.4.8.8.in-addr.arpa PTR g
59 2855104… 192.168.43.9 192.168.43.1 DNS 80 Standard query 0x833a PTR 2.2.2.4.in-addr.arpa
60 2855104… 192.168.43.1 192.168.43.9 DNS 116 Standard query response 0x833a PTR 2.2.2.4.in-addr.arpa PTR b
67 2855105… 192.168.43.9 192.168.43.1 DNS 77 Standard query 0x2121 A www.wireshark.org
68 2855105… 192.168.43.1 192.168.43.9 DNS 93 Standard query response 0x2121 A www.wireshark.org A 174.137.
69 2855105… 192.168.43.9 192.168.43.1 DNS 77 Standard query 0x2c58 A www.wireshark.org
70 2855105… 192.168.43.1 192.168.43.9 DNS 93 Standard query response 0x2c58 A www.wireshark.org A 174.137.
493 5684154… 10.10.57.178 10.0.0.2 DNS 103 Standard query 0xff00 A www.prd.map.nytimes.xovr.nyt.net OPT
494 5684154… 10.10.57.178 10.0.0.2 DNS 103 Standard query 0x89e9 AAAA www.prd.map.nytimes.xovr.nyt.net O
495 5684154… 10.10.57.178 10.0.0.2 DNS 93 Standard query 0x73f3 AAAA www.bemytravelmuse.com OPT
497 5684154… 10.0.0.2 10.10.57.178 DNS 149 Standard query response 0x73f3 AAAA www.bemytravelmuse.com AA
498 5684154… 10.0.0.2 10.10.57.178 DNS 152 Standard query response 0xff00 A www.prd.map.nytimes.xovr.nyt
499 5684154… 10.0.0.2 10.10.57.178 DNS 197 Standard query response 0x89e9 AAAA www.prd.map.nytimes.xovr.
Frame 13: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 145.253.2.203
User Datagram Protocol, Src Port: 3009, Dst Port: 53
Source Port: 3009
Destination Port: 53
Length: 55
Checksum: 0x10af [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Domain Name System (query)
Transaction ID: 0x0023
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
0000 fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45 00
0010 00 4b 0f 49 00 00 80 11 63 a5 91 fe a0 ed 91 fd
0020 02 cb 0b c1 00 35 00 37 10 af 00 23 01 00 00 01
0030 00 00 00 00 00 00 07 70 61 67 65 61 64 32 11 67
0040 6f 6f 67 6c 65 73 79 6e 64 69 63 61 74 69 6f 6e
0050 03 63 6f 6d 00 00 01 00 01
Source or Destination Port: Unsigned integer, 2 bytes
Packets: 58653 · Displayed: 103 (0.2%)
Comments: 1
Profile: Default

Filter	Description	Filter	Description
`http`	Show all HTTP packets	`dns`	Show all DNS packets
`http.response.code == 200`	Show all packets with HTTP response code "200"	`dns.flags.response == 0`	Show all DNS requests
`http.request.method == "GET"`	Show all HTTP GET requests	`dns.flags.response == 1`	Show all DNS responses
`http.request.method == "POST"`	Show all HTTP POST requests	`dns.qry.type == 1`	Show all DNS "A" records


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response.code == 200
No. Time Source Destination Protocol Length Info
Exercise.pcapng
Packets: 58653 · Displayed: 19 (0.0%) Comments: 1 Profile: Default


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.flags.response == 0
No. Time Source Destination Protocol Length Info
Response: Boolean
Packets: 58653 · Displayed: 54 (0.1%) Comments: 1 Profile: Default