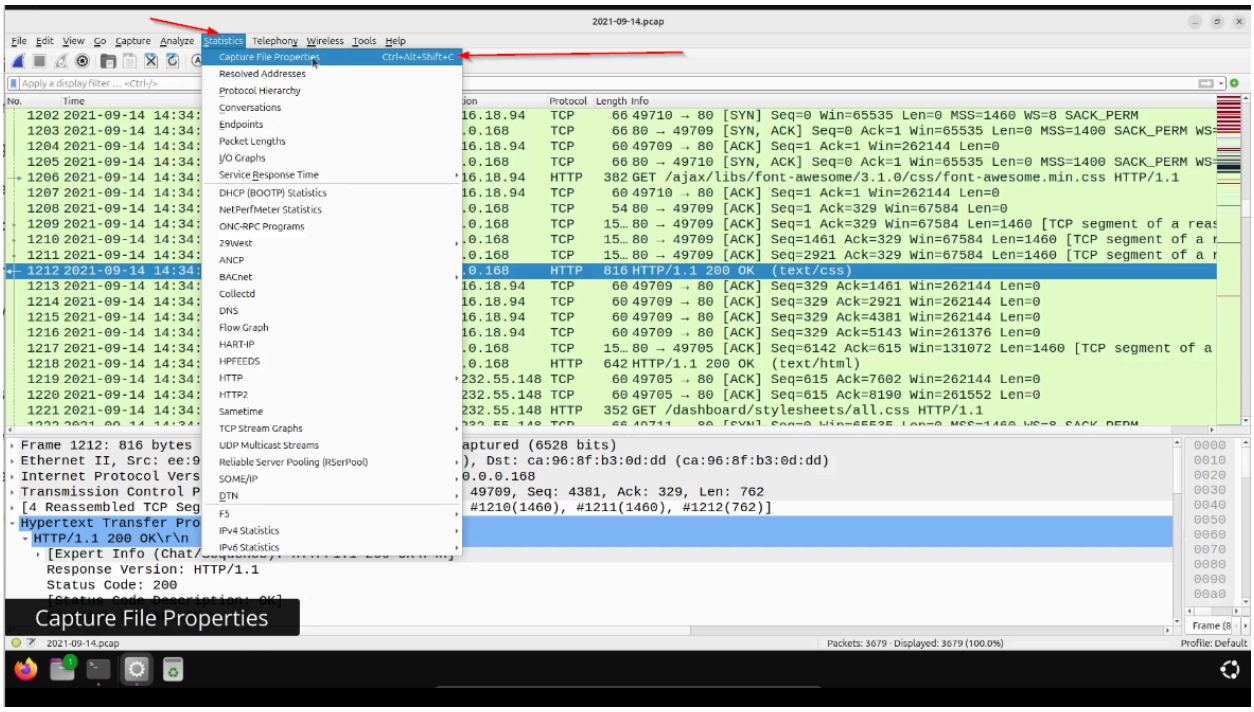
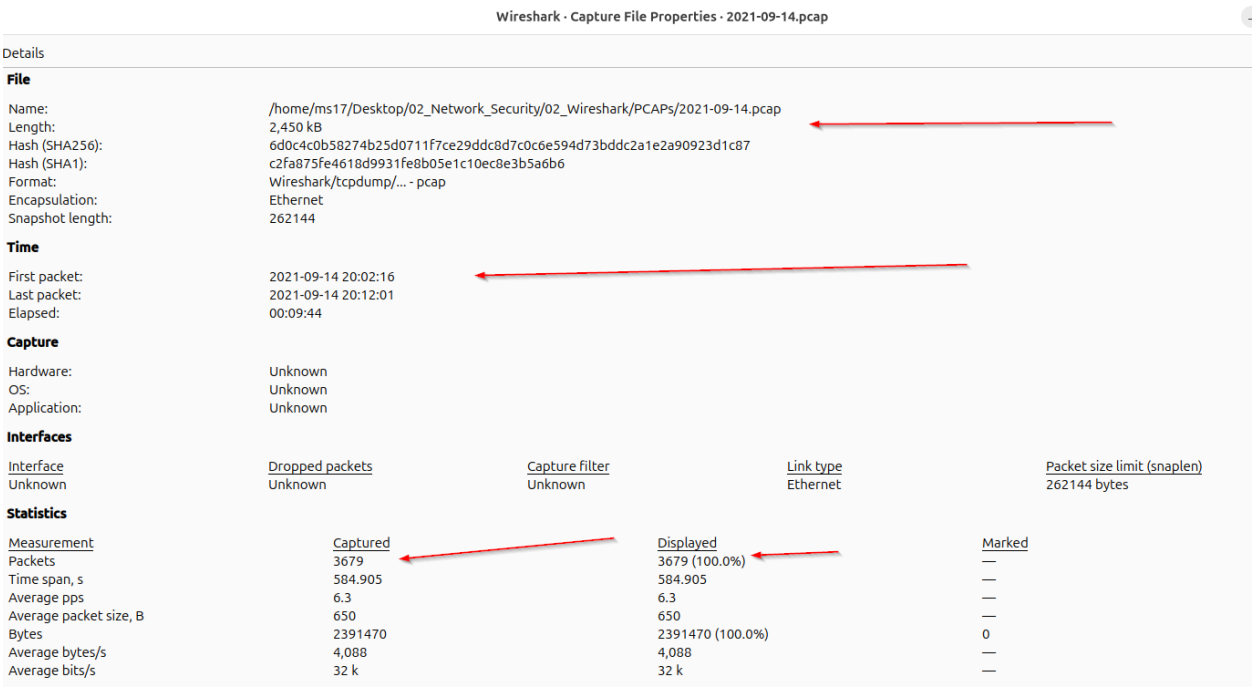
11. Wireshark - Statistics

⇒ In **Wireshark**, the **Statistics** menu provides powerful tools to analyze and summarize the captured network traffic. It helps **Security Analysts, Network Engineers, and SOC teams** quickly identify patterns, anomalies, and key metrics from a `.pcap` file or live capture.

1.) Capture File Properties

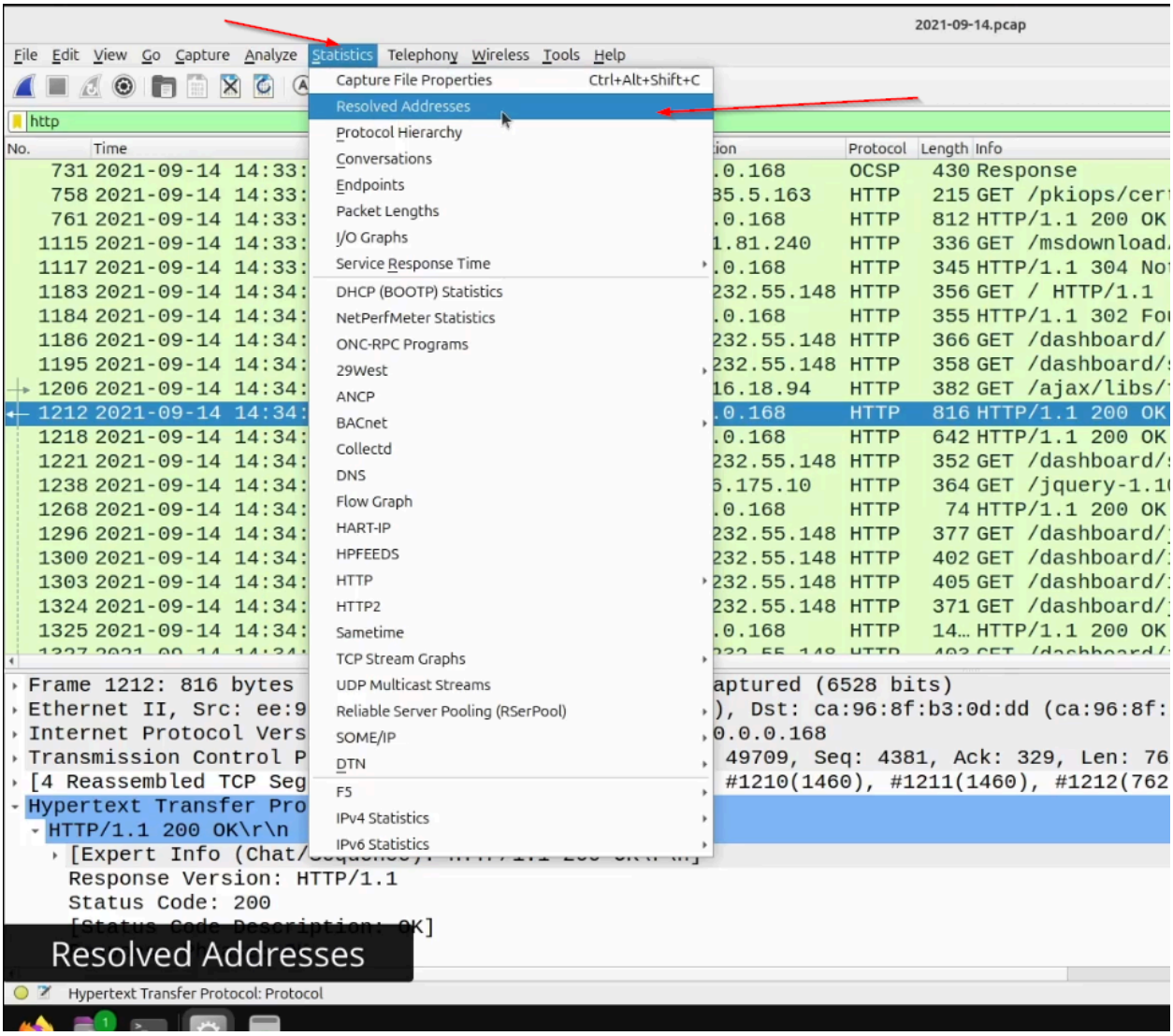
Shows details about the `.pcap` file—file size, packet count, duration, average packet rate, etc.

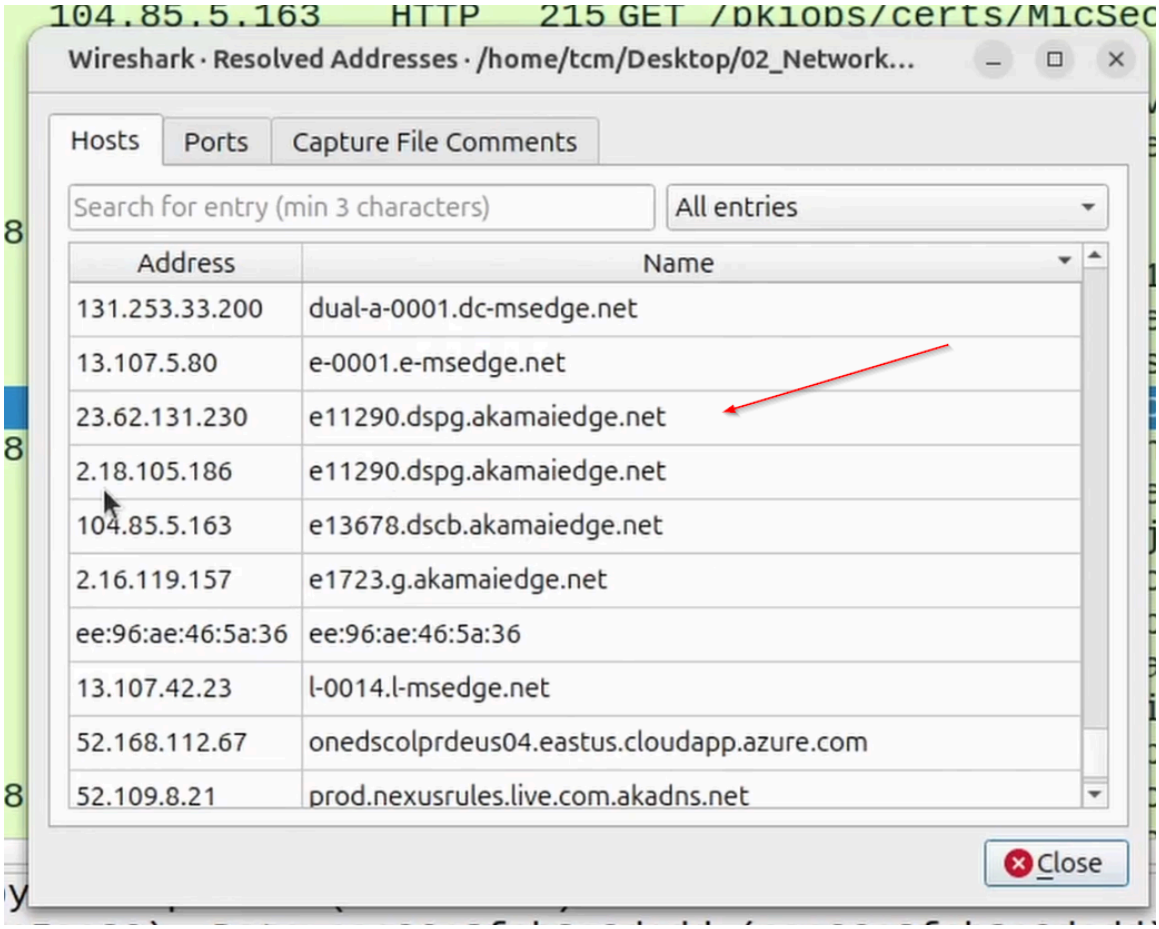




2.) Resolved Addresses

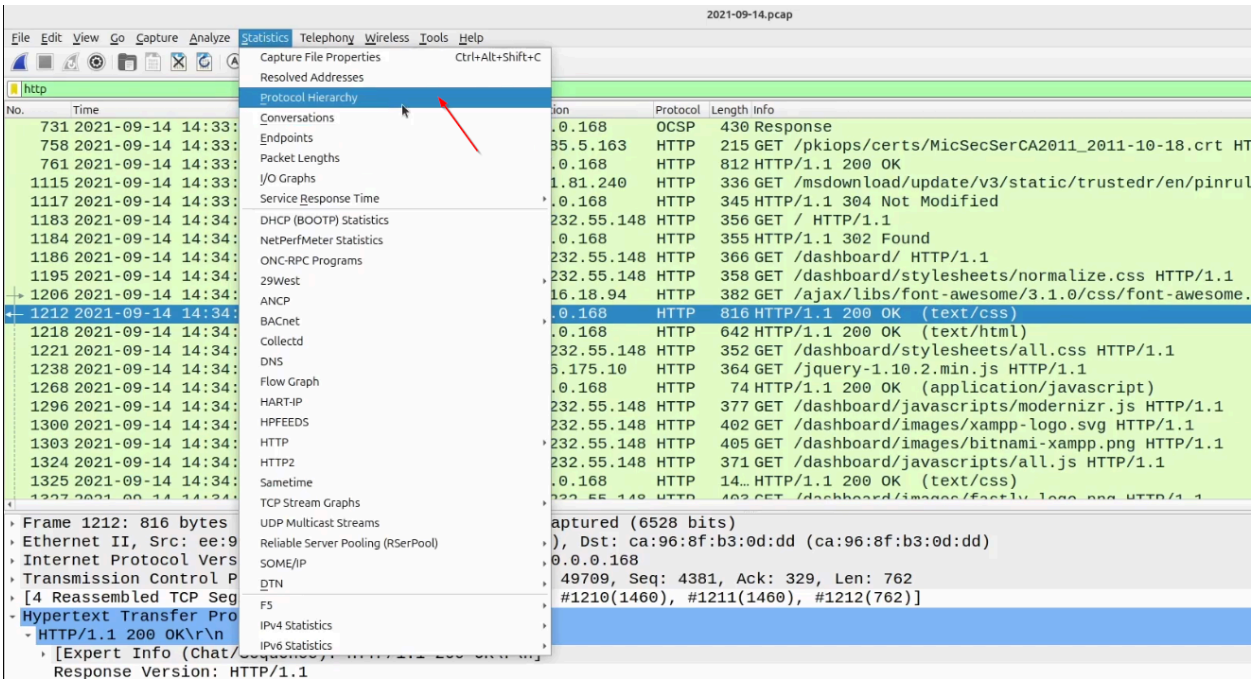
Lists hostnames (via DNS) and MAC vendor names if address resolution is enabled.

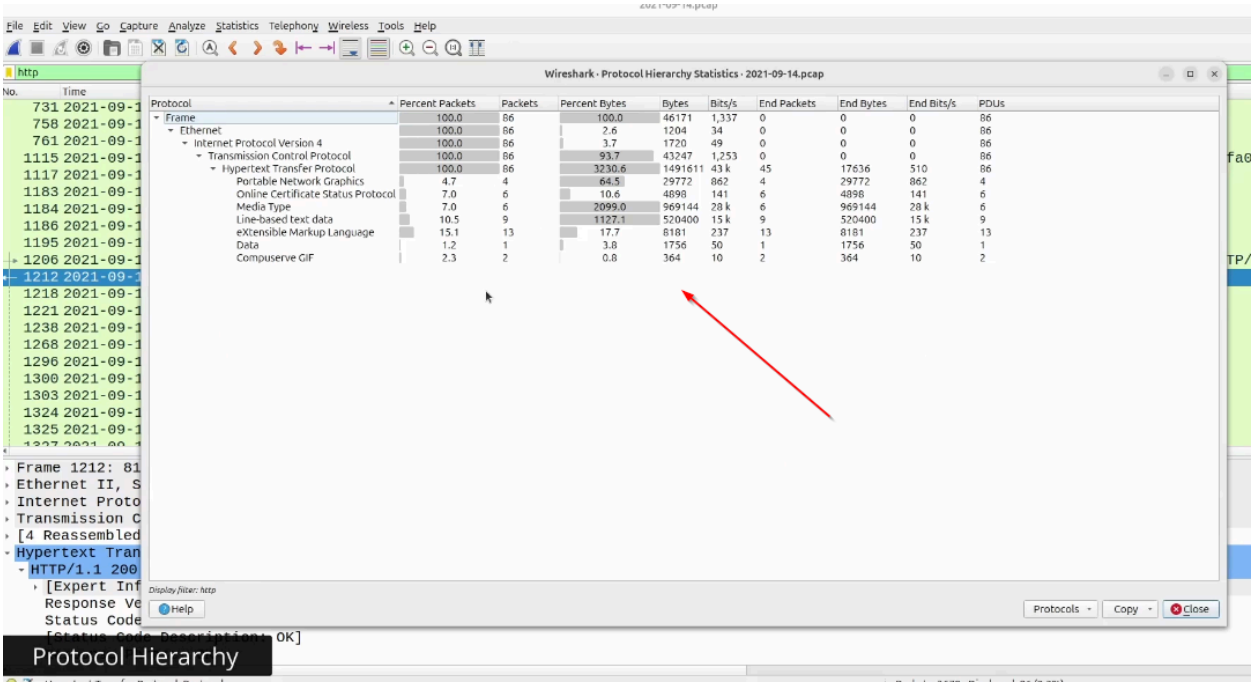

2021-09-14.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
SOME/IP
DTN
F5
IPv4 Statistics
IPv6 Statistics
http
No. Time Protocol Length Info
731 2021-09-14 14:33: OCSP 430 Response
758 2021-09-14 14:33: HTTP 215 GET /pkiops/cer
761 2021-09-14 14:33: HTTP 812 HTTP/1.1 200 OK
1115 2021-09-14 14:33: HTTP 336 GET /msdownload
1117 2021-09-14 14:33: HTTP 345 HTTP/1.1 304 No
1183 2021-09-14 14:34: HTTP 356 GET / HTTP/1.1
1184 2021-09-14 14:34: HTTP 355 HTTP/1.1 302 Fo
1186 2021-09-14 14:34: HTTP 366 GET /dashboard/
1195 2021-09-14 14:34: HTTP 358 GET /dashboard/
1206 2021-09-14 14:34: HTTP 382 GET /ajax/libs/
1212 2021-09-14 14:34: HTTP 816 HTTP/1.1 200 OK
1218 2021-09-14 14:34: HTTP 642 HTTP/1.1 200 OK
1221 2021-09-14 14:34: HTTP 352 GET /dashboard/
1238 2021-09-14 14:34: HTTP 364 GET /jquery-1.1
1268 2021-09-14 14:34: HTTP 74 HTTP/1.1 200 OK
1296 2021-09-14 14:34: HTTP 377 GET /dashboard/
1300 2021-09-14 14:34: HTTP 402 GET /dashboard/
1303 2021-09-14 14:34: HTTP 405 GET /dashboard/
1324 2021-09-14 14:34: HTTP 371 GET /dashboard/
1325 2021-09-14 14:34: HTTP 14... HTTP/1.1 200 OK
Frame 1212: 816 bytes aptured (6528 bits)
Ethernet II, Src: ee:9), Dst: ca:96:8f:b3:0d:dd (ca:96:8f:
Internet Protocol Vers 0.0.0.168
Transmission Control P 49709, Seq: 4381, Ack: 329, Len: 76
[4 Reassembled TCP Seg #1210(1460), #1211(1460), #1212(762
Hypertext Transfer Pro
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Resolved Addresses
Hypertext Transfer Protocol: Protocol

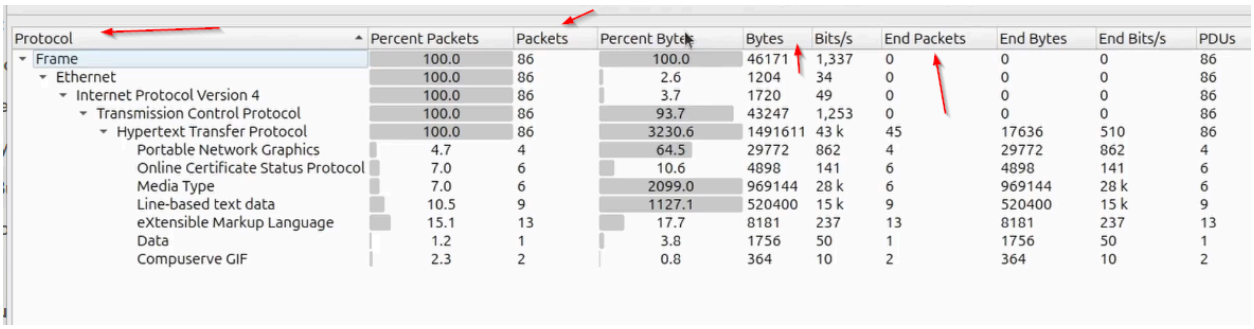


3.) Protocol Hierarchy

Breaks down all observed protocols in the capture by percentage, bytes, and packet count (e.g., TCP, HTTP, DNS).


2021-09-14.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
SOME/IP
DTN
F5
IPv4 Statistics
IPv6 Statistics
http
No. Time Protocol Length Info
731 2021-09-14 14:33: OCSP 430 Response
758 2021-09-14 14:33: HTTP 215 GET /pkiops/certs/MicSecSerCA2011_2011-10-18.crt HT
761 2021-09-14 14:33: HTTP 812 HTTP/1.1 200 OK
1115 2021-09-14 14:33: HTTP 336 GET /msdownload/update/v3/static/trustedr/en/pinrul
1117 2021-09-14 14:33: HTTP 345 HTTP/1.1 304 Not Modified
1183 2021-09-14 14:34: HTTP 356 GET / HTTP/1.1
1184 2021-09-14 14:34: HTTP 355 HTTP/1.1 302 Found
1186 2021-09-14 14:34: HTTP 366 GET /dashboard/ HTTP/1.1
1195 2021-09-14 14:34: HTTP 358 GET /dashboard/stylesheets/normalize.css HTTP/1.1
1206 2021-09-14 14:34: HTTP 382 GET /ajax/libs/font-awesome/3.1.0/css/font-awesome.
1212 2021-09-14 14:34: HTTP 816 HTTP/1.1 200 OK (text/css)
1218 2021-09-14 14:34: HTTP 642 HTTP/1.1 200 OK (text/html)
1221 2021-09-14 14:34: HTTP 352 GET /dashboard/stylesheets/all.css HTTP/1.1
1238 2021-09-14 14:34: HTTP 364 GET /jquery-1.10.2.min.js HTTP/1.1
1268 2021-09-14 14:34: HTTP 74 HTTP/1.1 200 OK (application/javascript)
1296 2021-09-14 14:34: HTTP 377 GET /dashboard/javascripts/modernizr.js HTTP/1.1
1300 2021-09-14 14:34: HTTP 402 GET /dashboard/images/xampp-logo.svg HTTP/1.1
1303 2021-09-14 14:34: HTTP 405 GET /dashboard/images/bitnami-xampp.png HTTP/1.1
1324 2021-09-14 14:34: HTTP 371 GET /dashboard/javascripts/all.js HTTP/1.1
1325 2021-09-14 14:34: HTTP 14... HTTP/1.1 200 OK (text/css)
Frame 1212: 816 bytes
Ethernet II, Src: ee:9
Internet Protocol Vers
Transmission Control P
[4 Reassembled TCP Seg
Hypertext Transfer Pro
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
aptured (6528 bits)
), Dst: ca:96:8f:b3:0d:dd (ca:96:8f:b3:0d:dd)
0.0.0.168
49709, Seq: 4381, Ack: 329, Len: 762
#1210(1460), #1211(1460), #1212(762)]

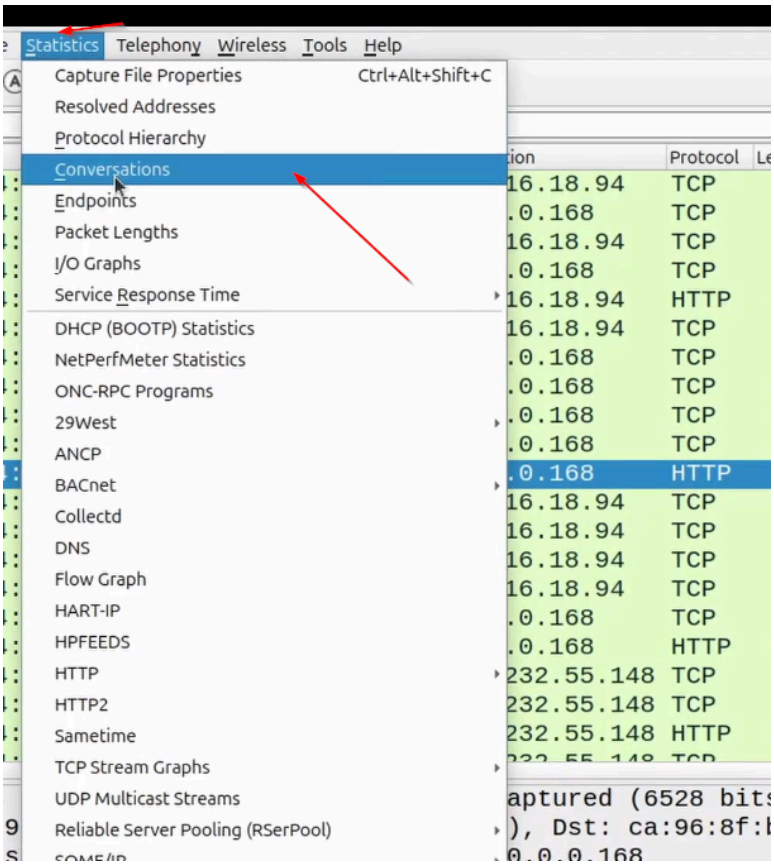

Wireshark · Protocol Hierarchy Statistics · 2021-09-14.pcap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes End Bits/s PDUs
Frame 100.0 86 100.0 46171 1,337 0 0 0 86
Ethernet 100.0 86 2.6 1204 34 0 0 0 86
Internet Protocol Version 4 100.0 86 3.7 1720 49 0 0 0 86
Transmission Control Protocol 100.0 86 93.7 43247 1,253 0 0 0 86
Hypertext Transfer Protocol 100.0 86 3230.6 1491611 43 k 45 17636 510 86
Portable Network Graphics 4.7 4 64.5 29772 862 4 29772 862 4
Online Certificate Status Protocol 7.0 6 10.6 4898 141 6 4898 141 6
Media Type 7.0 6 2099.0 969144 28 k 6 969144 28 k 6
Line-based text data 10.5 9 1127.1 520400 15 k 9 520400 15 k 9
eXtensible Markup Language 15.1 13 17.7 8181 237 13 8181 237 13
Data 1.2 1 3.8 1756 50 1 1756 50 1
Compuserve GIF 2.3 2 0.8 364 10 2 364 10 2
Display filter: http
Help
Protocols
Copy
Close
Protocol Hierarchy

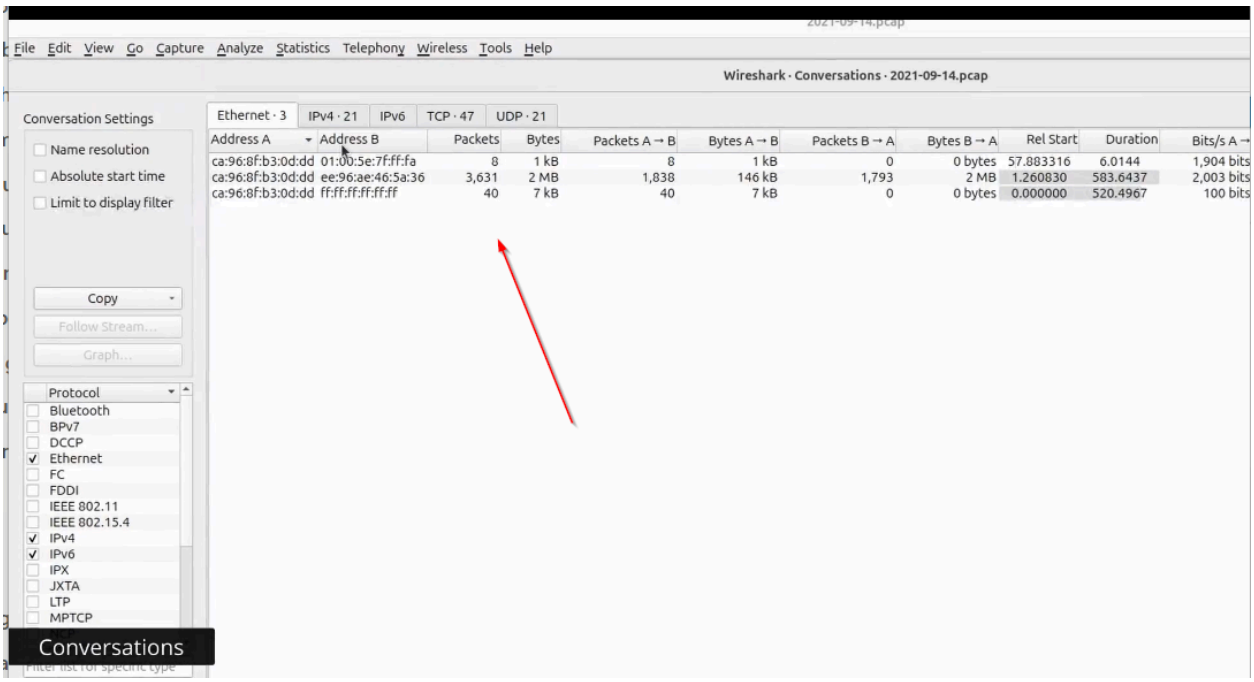


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	86	100.0	46171	1,337	0	0	0	86
Ethernet	100.0	86	2.6	1204	34	0	0	0	86
Internet Protocol Version 4	100.0	86	3.7	1720	49	0	0	0	86
Transmission Control Protocol	100.0	86	93.7	43247	1,253	0	0	0	86
Hypertext Transfer Protocol	100.0	86	3230.6	1491611	43 k	45	17636	510	86
Portable Network Graphics	4.7	4	64.5	29772	862	4	29772	862	4
Online Certificate Status Protocol	7.0	6	10.6	4898	141	6	4898	141	6
Media Type	7.0	6	2099.0	969144	28 k	6	969144	28 k	6
Line-based text data	10.5	9	1127.1	520400	15 k	9	520400	15 k	9
eXtensible Markup Language	15.1	13	17.7	8181	237	13	8181	237	13
Data	1.2	1	3.8	1756	50	1	1756	50	1
Compuserve GIF	2.3	2	0.8	364	10	2	364	10	2

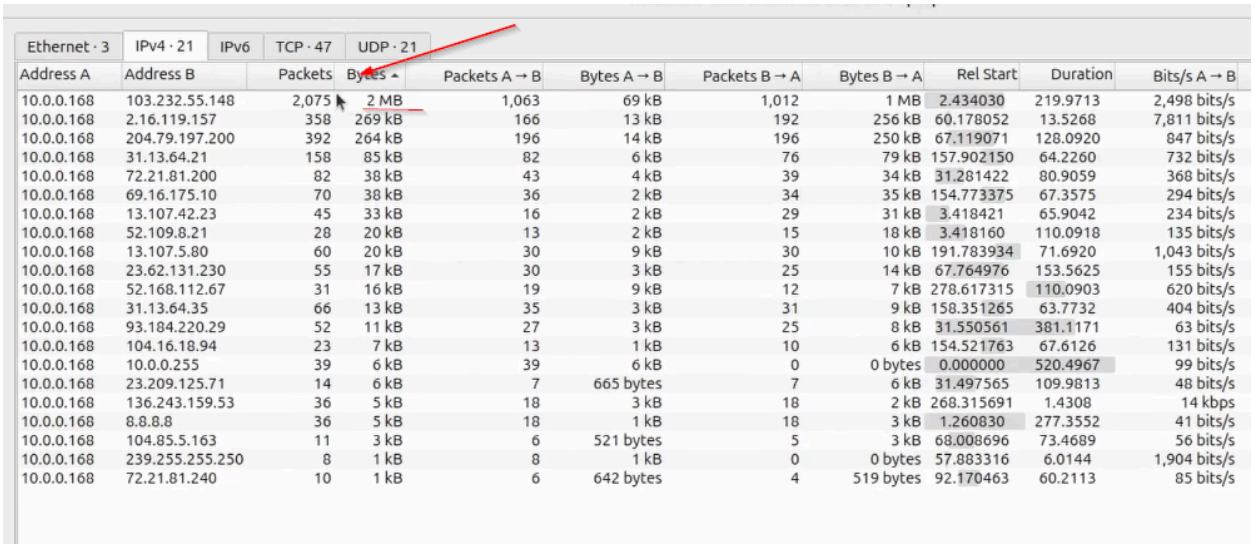
4.) Conversations

Displays communication between hosts (IP ↔ IP, port ↔ port), showing how much data they exchanged.

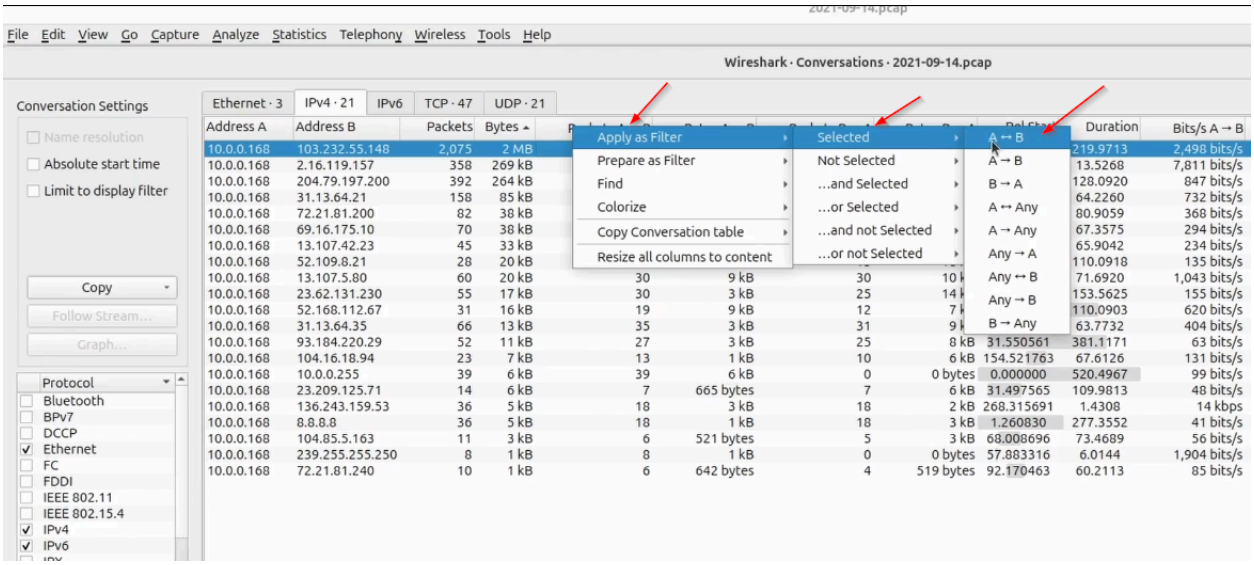




Double click to bytes then you can see most IP communicate find

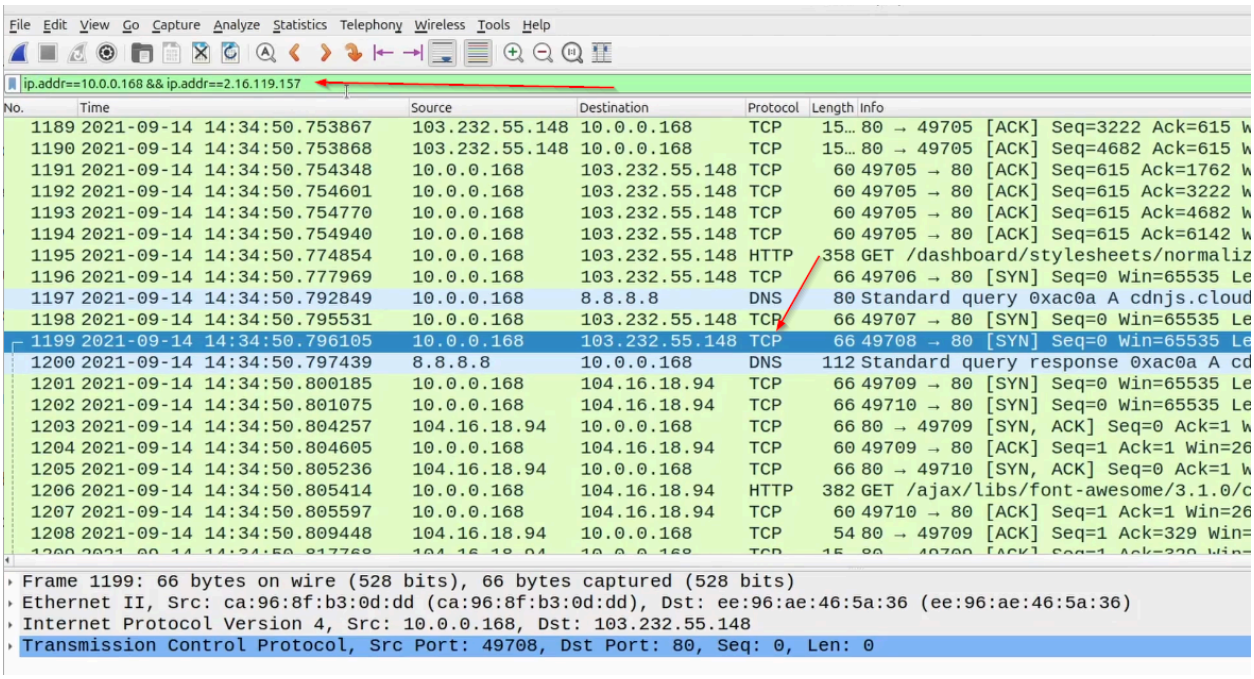


Filter apply



Result

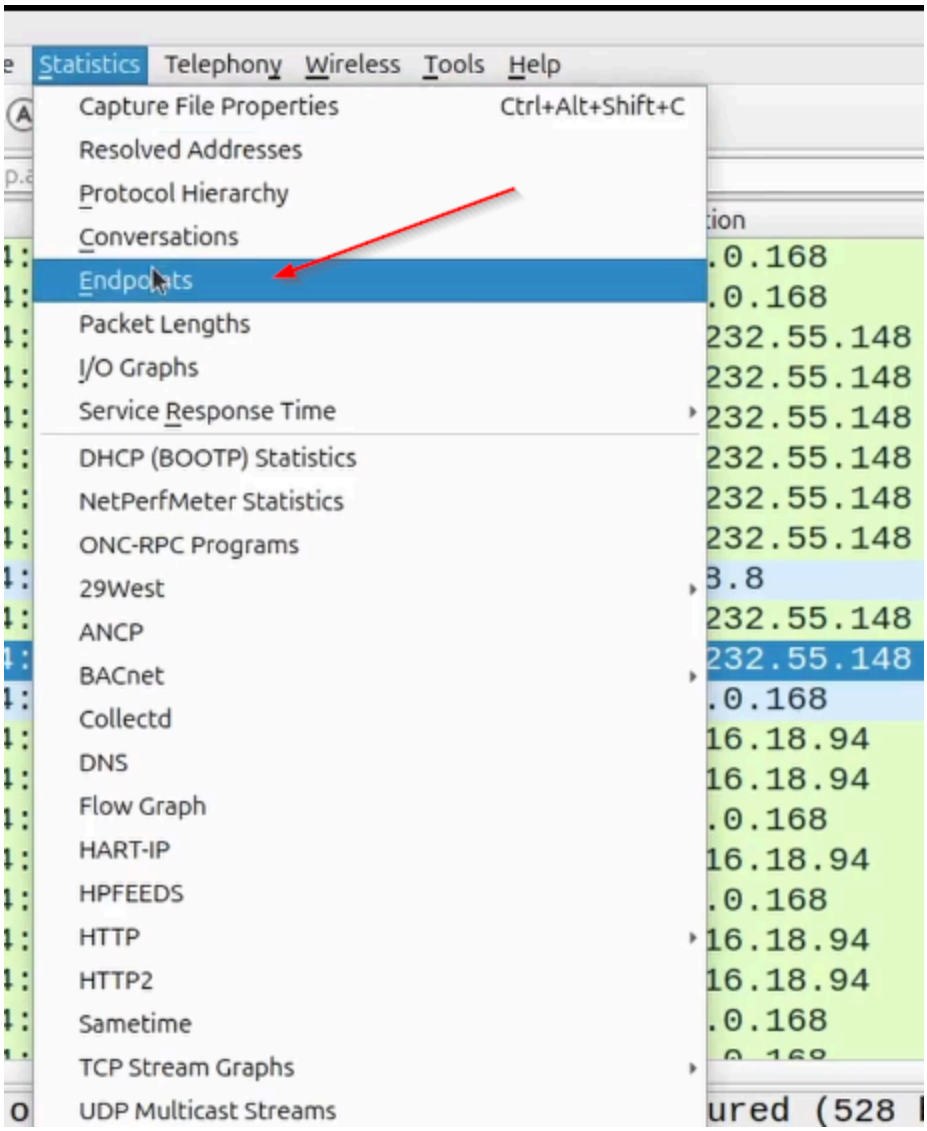
See A → B conversation show

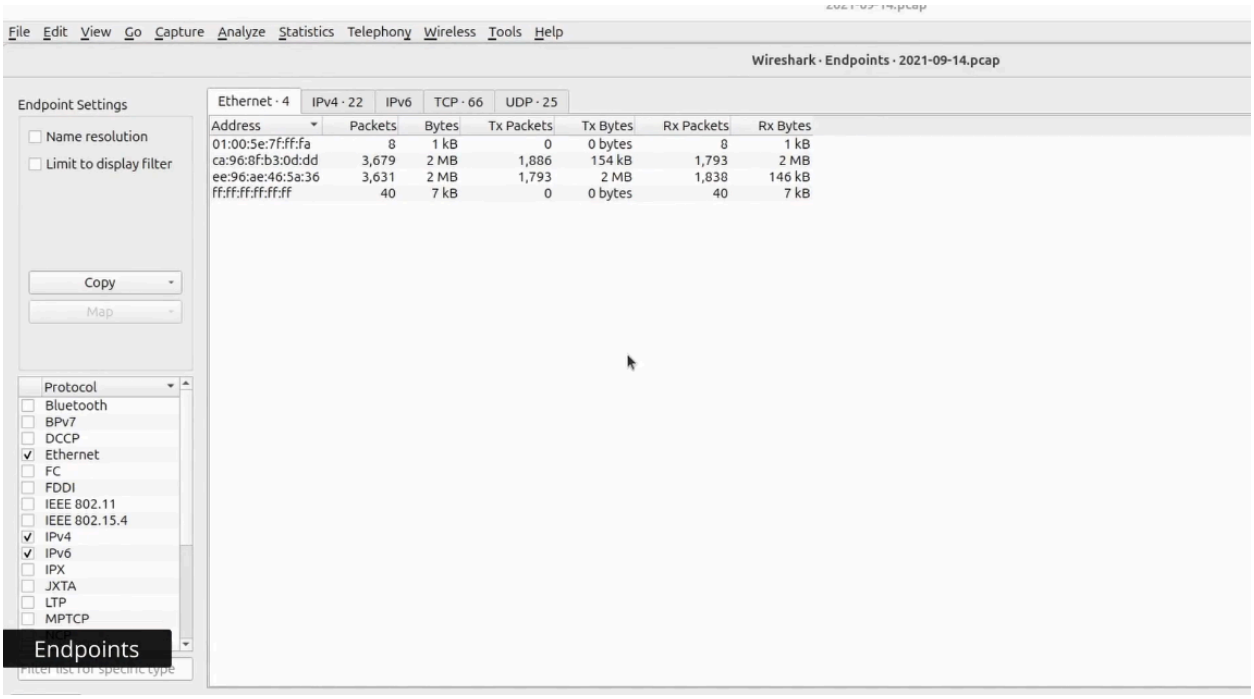


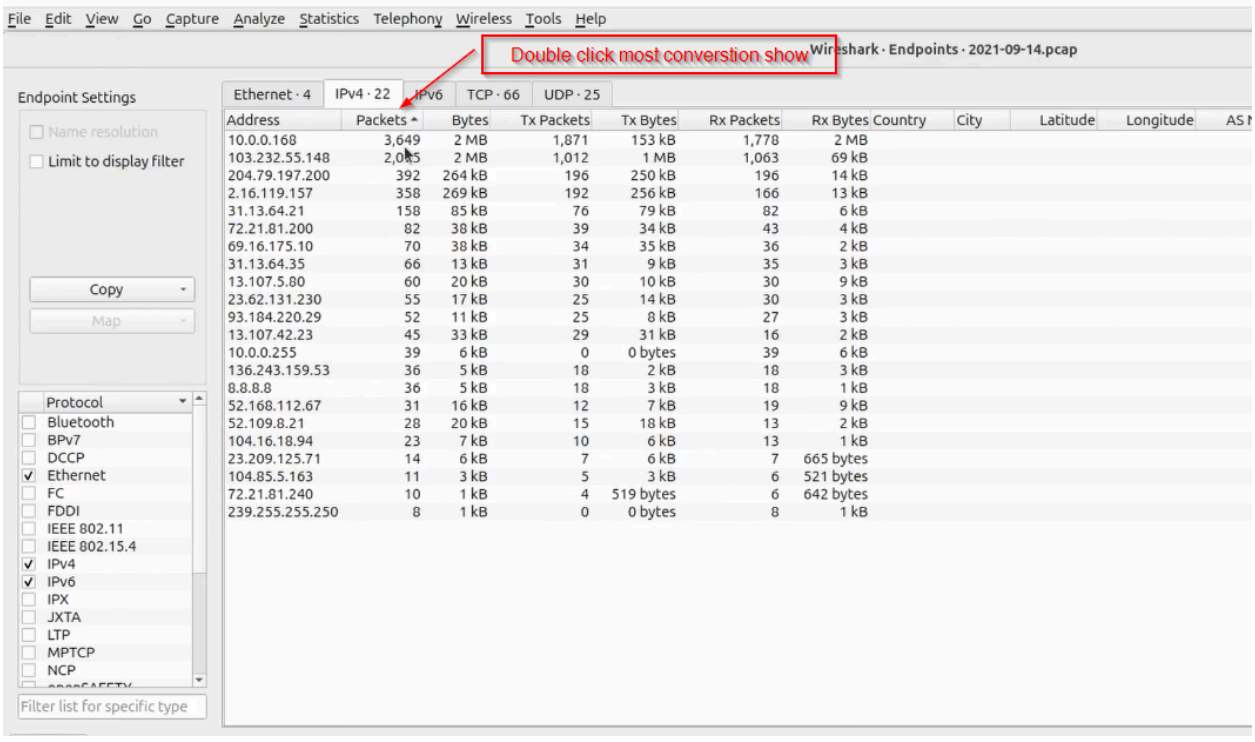
5.) Endpoints

Lists all IP/MAC addresses seen in the capture and how much traffic each sent or received.

And use tcpdum (cut , sort uniq) same do that features

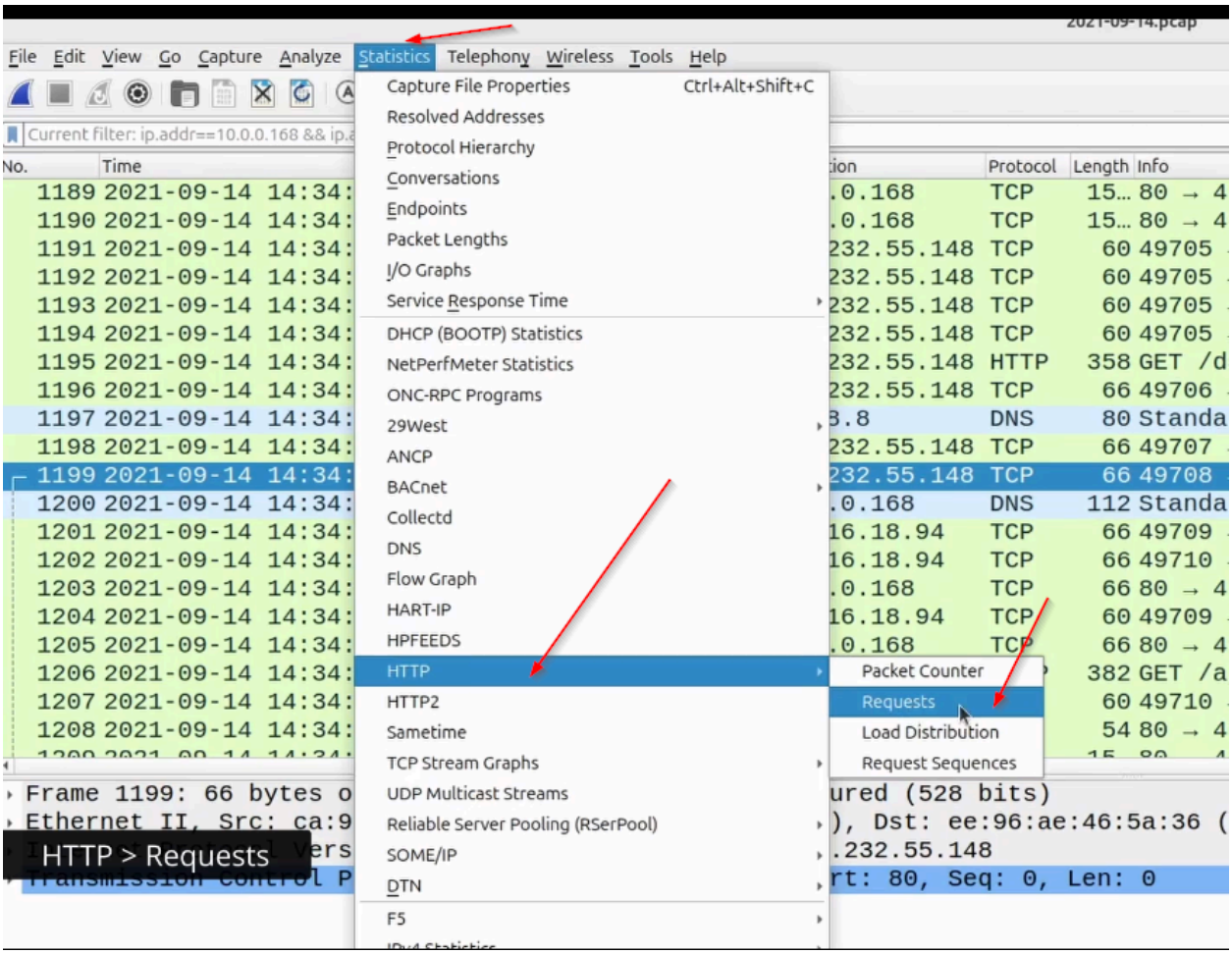

Statistics
Telephony
Wireless
Tools
Help
Capture File Properties
Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams

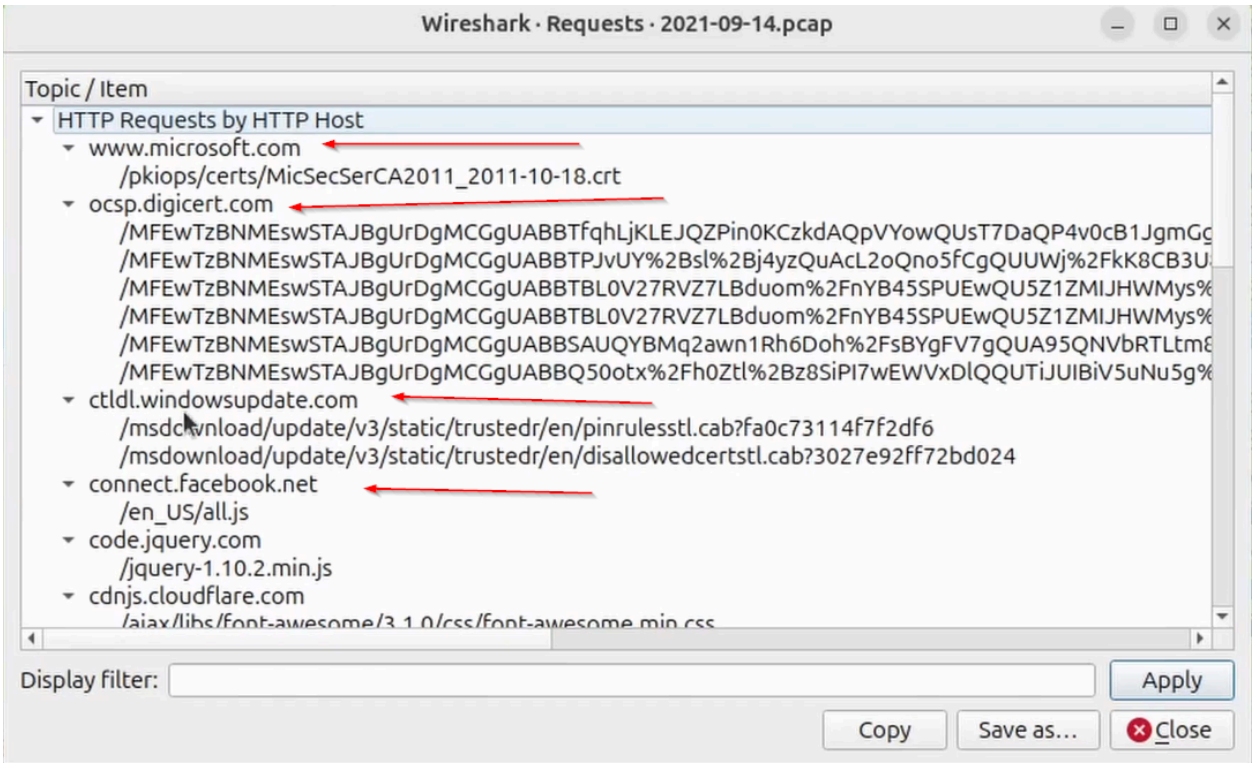

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Endpoints · 2021-09-14.pcap
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
Ethernet · 4
IPv4 · 22
IPv6
TCP · 66
UDP · 25
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes
01:00:5e:7f:ff:fa 8 1 kB 0 0 bytes 8 1 kB
ca:96:8f:b3:0d:dd 3,679 2 MB 1,886 154 kB 1,793 2 MB
ee:96:ae:46:5a:36 3,631 2 MB 1,793 2 MB 1,838 146 kB
ff:ff:ff:ff:ff:ff 40 7 kB 0 0 bytes 40 7 kB
Endpoints

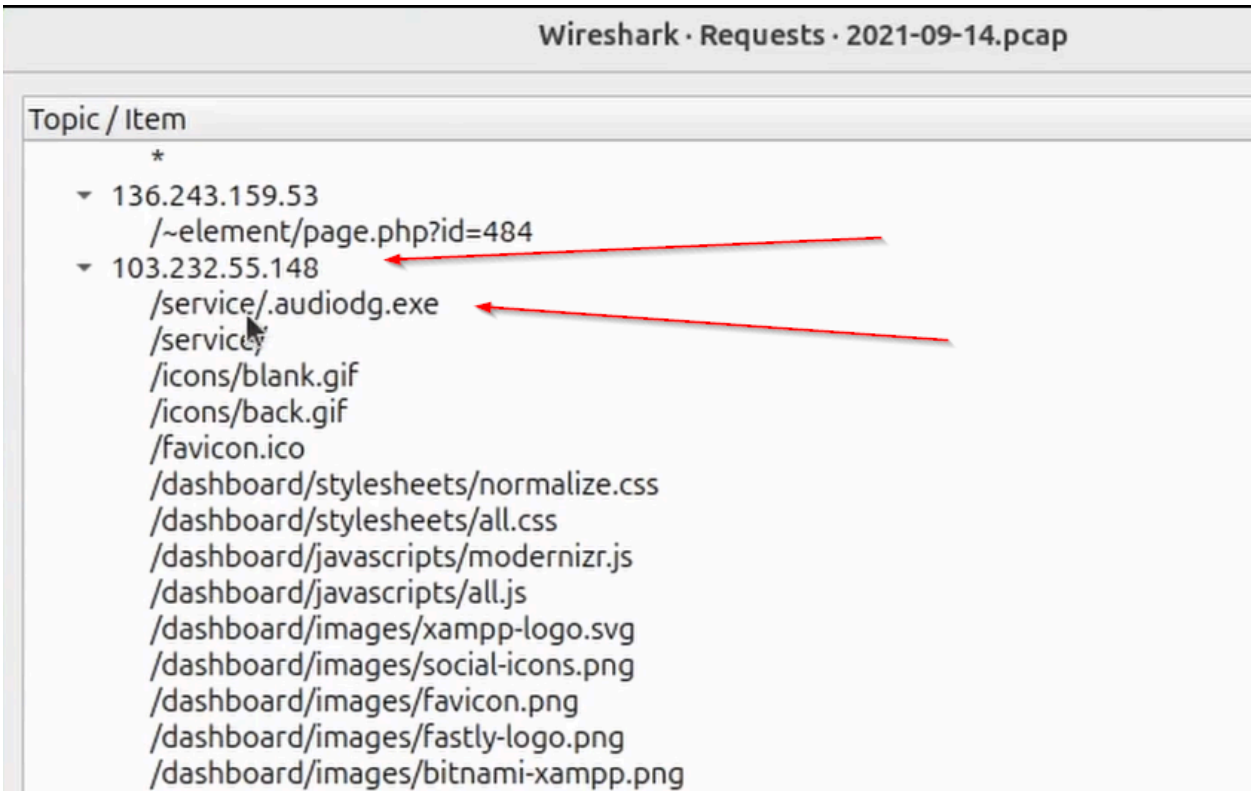

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Double click most converstion show
Wireshark · Endpoints · 2021-09-14.pcap
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
Filter list for specific type
Ethernet · 4
IPv4 · 22
IPv6
TCP · 66
UDP · 25
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City Latitude Longitude
10.0.0.168 3,649 2 MB 1,871 153 kB 1,778 2 MB
103.232.55.148 2,065 2 MB 1,012 1 MB 1,063 69 kB
204.79.197.200 392 264 kB 196 250 kB 196 14 kB
2.16.119.157 358 269 kB 192 256 kB 166 13 kB
31.13.64.21 158 85 kB 76 79 kB 82 6 kB
72.21.81.200 82 38 kB 39 34 kB 43 4 kB
69.16.175.10 70 38 kB 34 35 kB 36 2 kB
31.13.64.35 66 13 kB 31 9 kB 35 3 kB
13.107.5.80 60 20 kB 30 10 kB 30 9 kB
23.62.131.230 55 17 kB 25 14 kB 30 3 kB
93.184.220.29 52 11 kB 25 8 kB 27 3 kB
13.107.42.23 45 33 kB 29 31 kB 16 2 kB
10.0.0.255 39 6 kB 0 0 bytes 39 6 kB
136.243.159.53 36 5 kB 18 2 kB 18 3 kB
8.8.8.8 36 5 kB 18 3 kB 18 1 kB
52.168.112.67 31 16 kB 12 7 kB 19 9 kB
52.109.8.21 28 20 kB 15 18 kB 13 2 kB
104.16.18.94 23 7 kB 10 6 kB 13 1 kB
23.209.125.71 14 6 kB 7 6 kB 7 665 bytes
104.85.5.163 11 3 kB 5 3 kB 6 521 bytes
72.21.81.240 10 1 kB 4 519 bytes 6 642 bytes
239.255.255.250 8 1 kB 0 0 bytes 8 1 kB

6.) HTTP Requests

Extracts all HTTP GET, POST, and other methods. Helps identify visited URLs and domains.

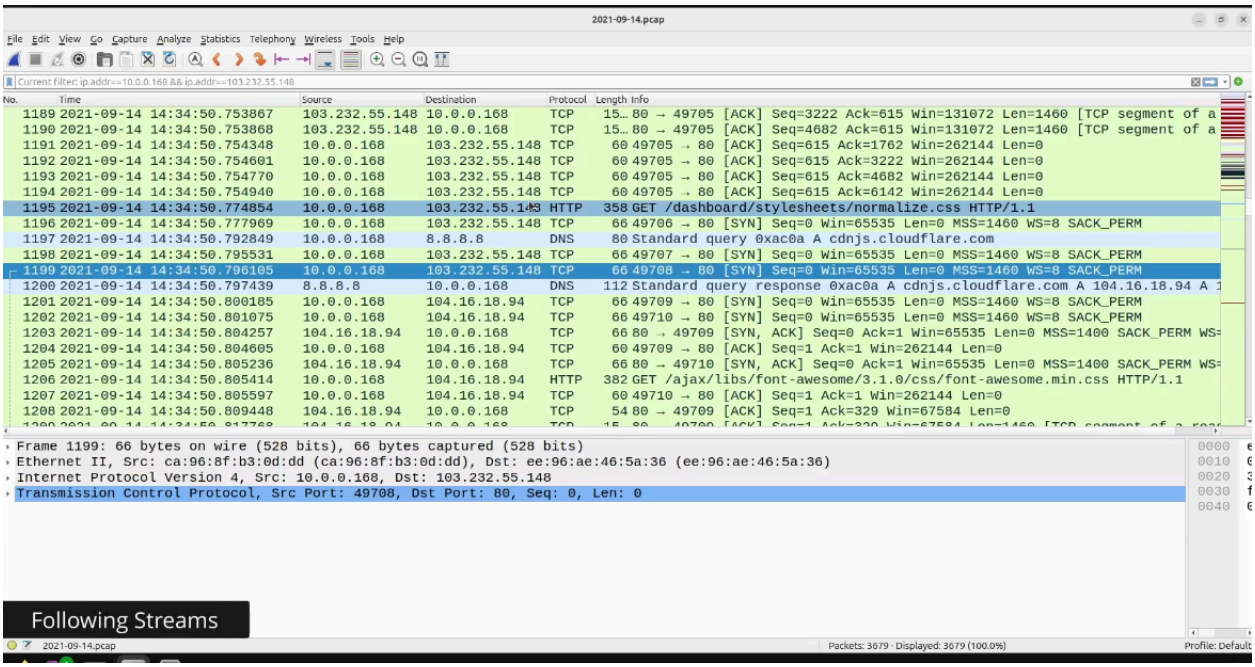


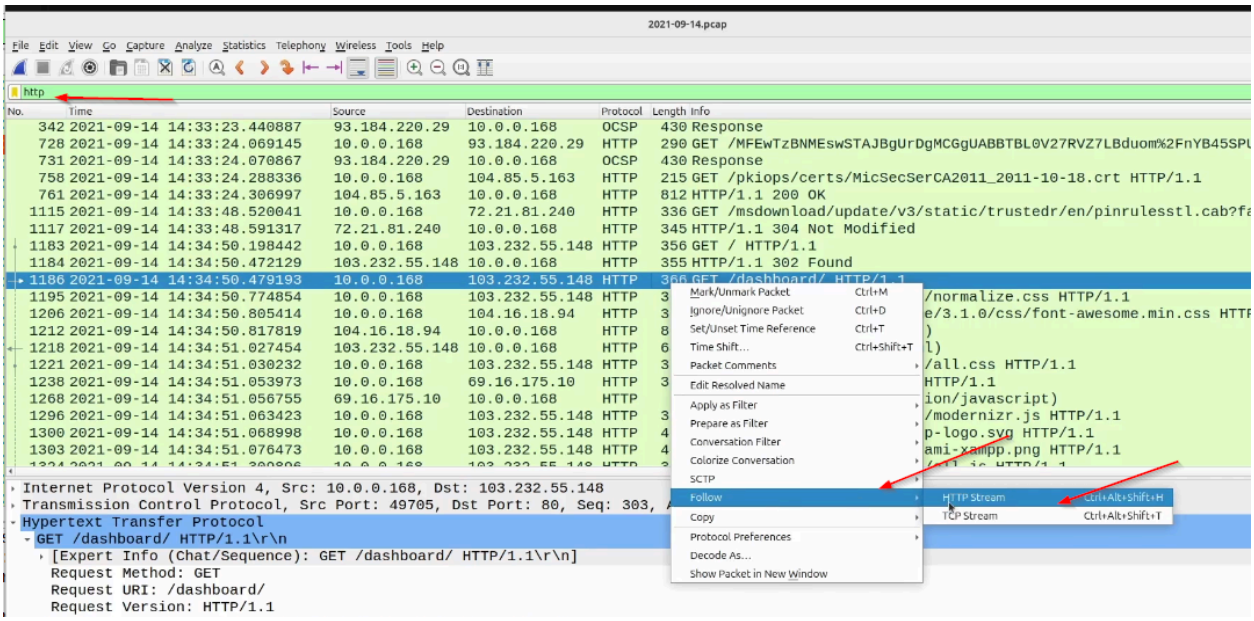

Wireshark · Requests · 2021-09-14.pcap
Topic / Item
HTTP Requests by HTTP Host
www.microsoft.com
/pkiops/certs/MicSecSerCA2011_2011-10-18.crt
ocsp.digicert.com
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGg
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bsl%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%
ctldl.windowsupdate.com
/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?fa0c73114f7f2df6
/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?3027e92ff72bd024
connect.facebook.net
/en_US/all.js
code.jquery.com
/jquery-1.10.2.min.js
cdnjs.cloudflare.com
Display filter:
Apply
Copy
Save as...
Close


Wireshark · Requests · 2021-09-14.pcap
Topic / Item
*
136.243.159.53
/~element/page.php?id=484
103.232.55.148
/service/.audiodg.exe
/service/
/icons/blank.gif
/icons/back.gif
/favicon.ico
/dashboard/stylesheets/normalize.css
/dashboard/stylesheets/all.css
/dashboard/javascripts/modernizr.js
/dashboard/javascripts/all.js
/dashboard/images/xampp-logo.svg
/dashboard/images/social-icons.png
/dashboard/images/favicon.png
/dashboard/images/fastly-logo.png
/dashboard/images/bitnami-xampp.png

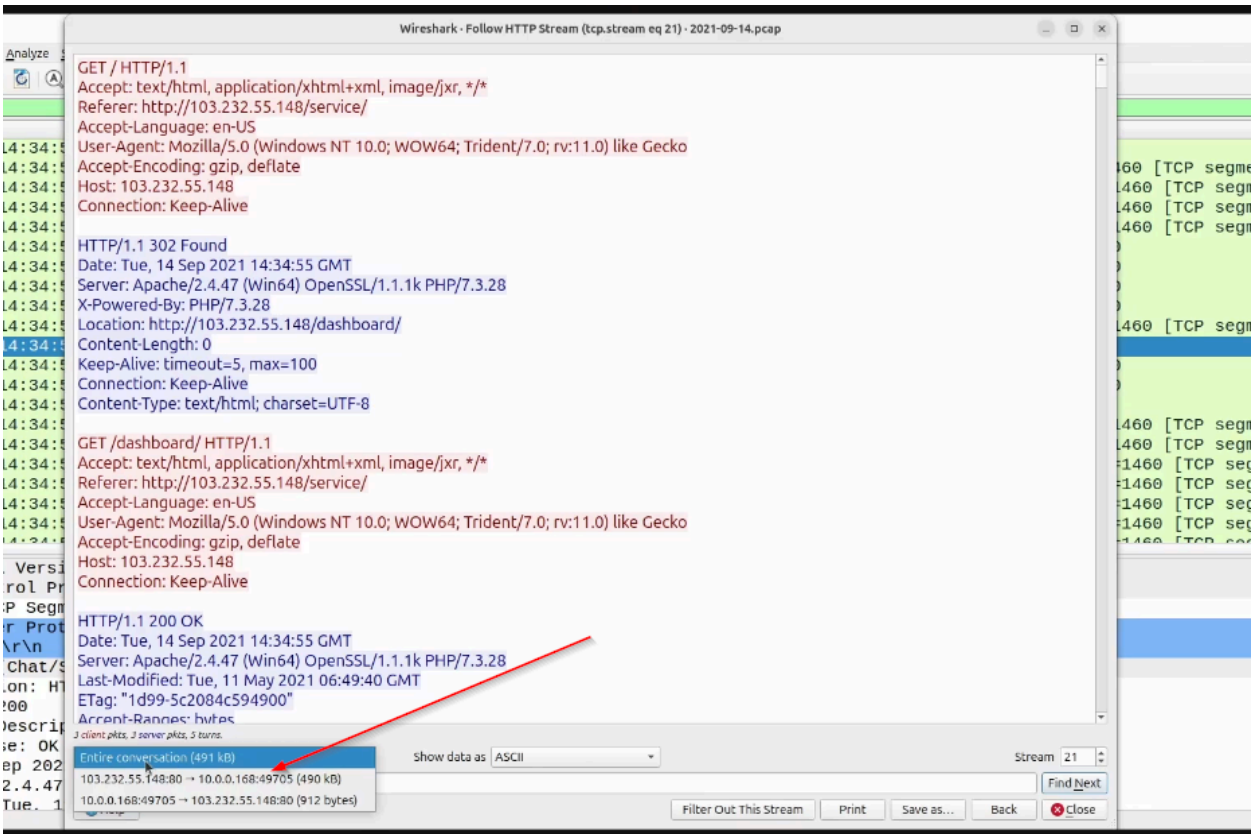
7.) Following Streams

Lets you follow full TCP/UDP sessions (like chat, file transfer, C2) in a readable format.



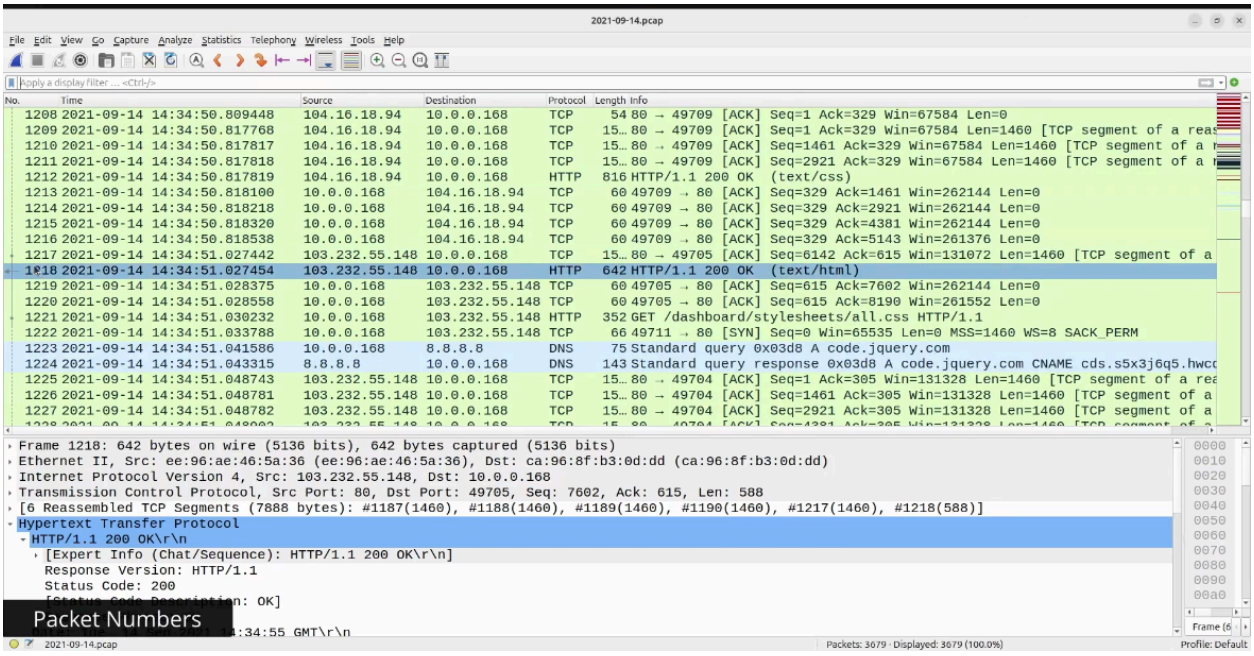


Edit conversation like only show request or response

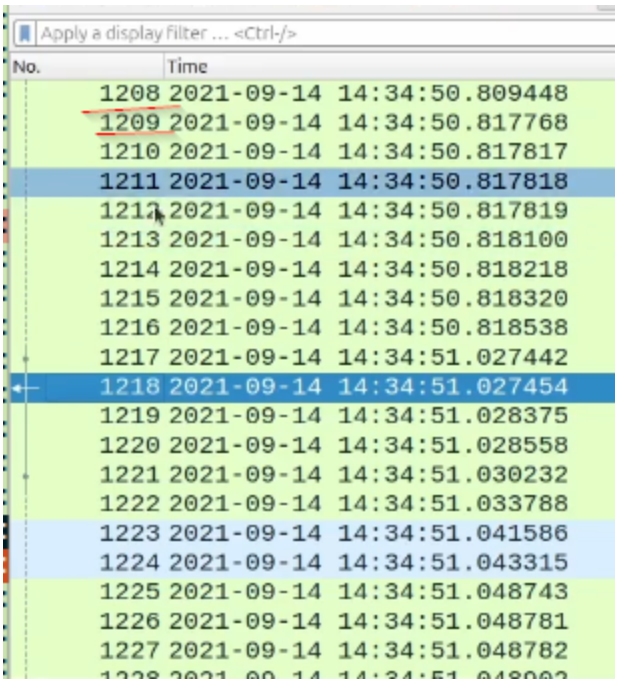


8.) Packet Numbers

Each captured packet is assigned a unique number. Useful for bookmarking and tracking flows.

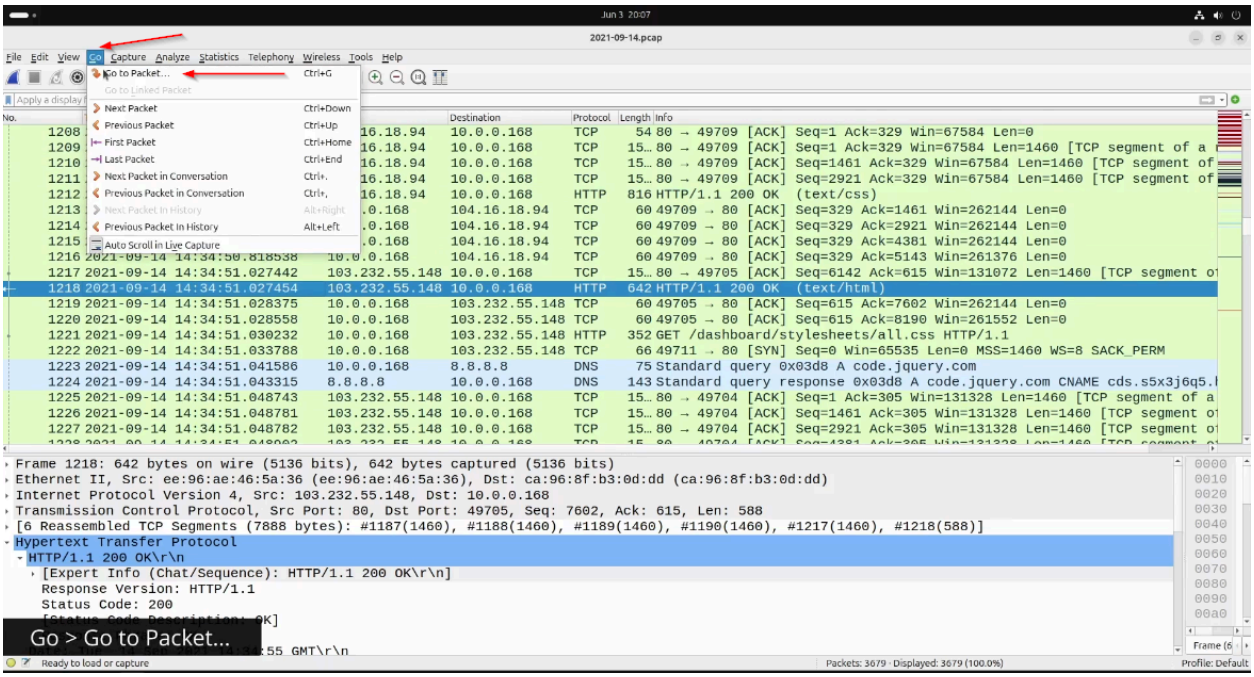


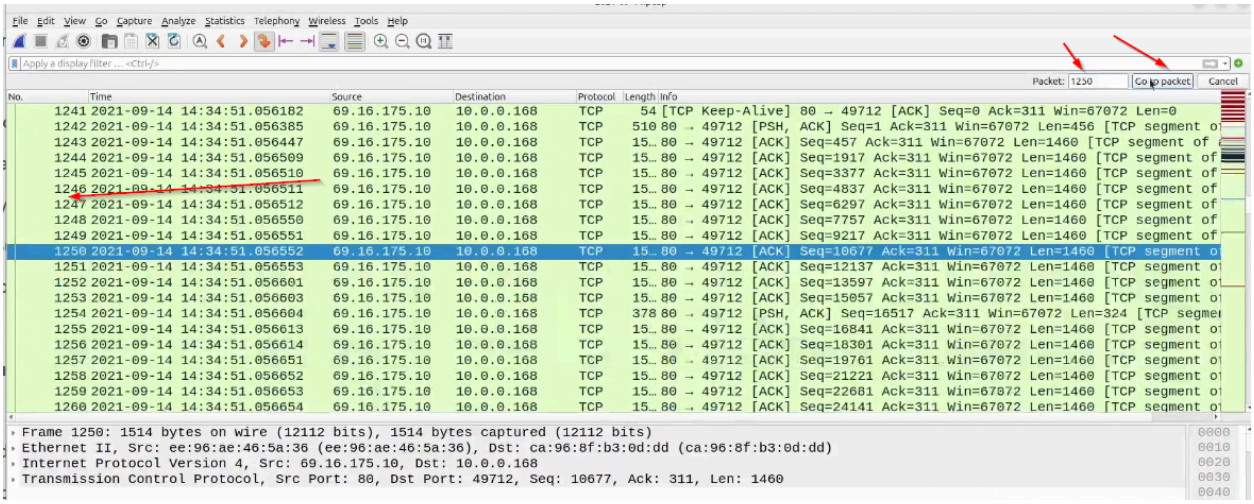
⇒ Packet Number very important



9.) Go > Go to Packet

Quickly jump to a specific packet number for focused analysis.

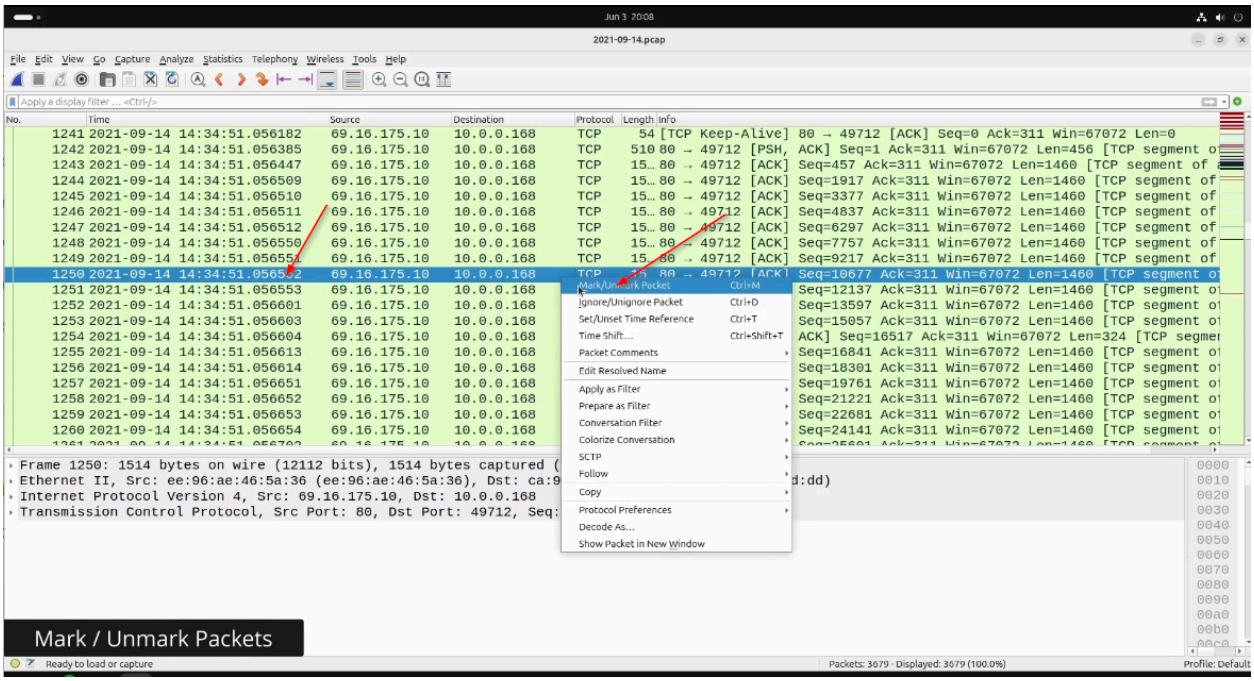


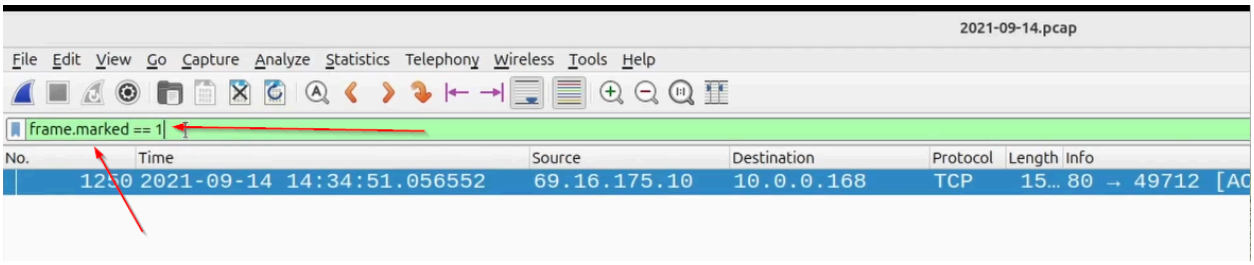


10.) Mark / Unmark Packets

Highlight important packets for easy review, filtering, or exporting later.

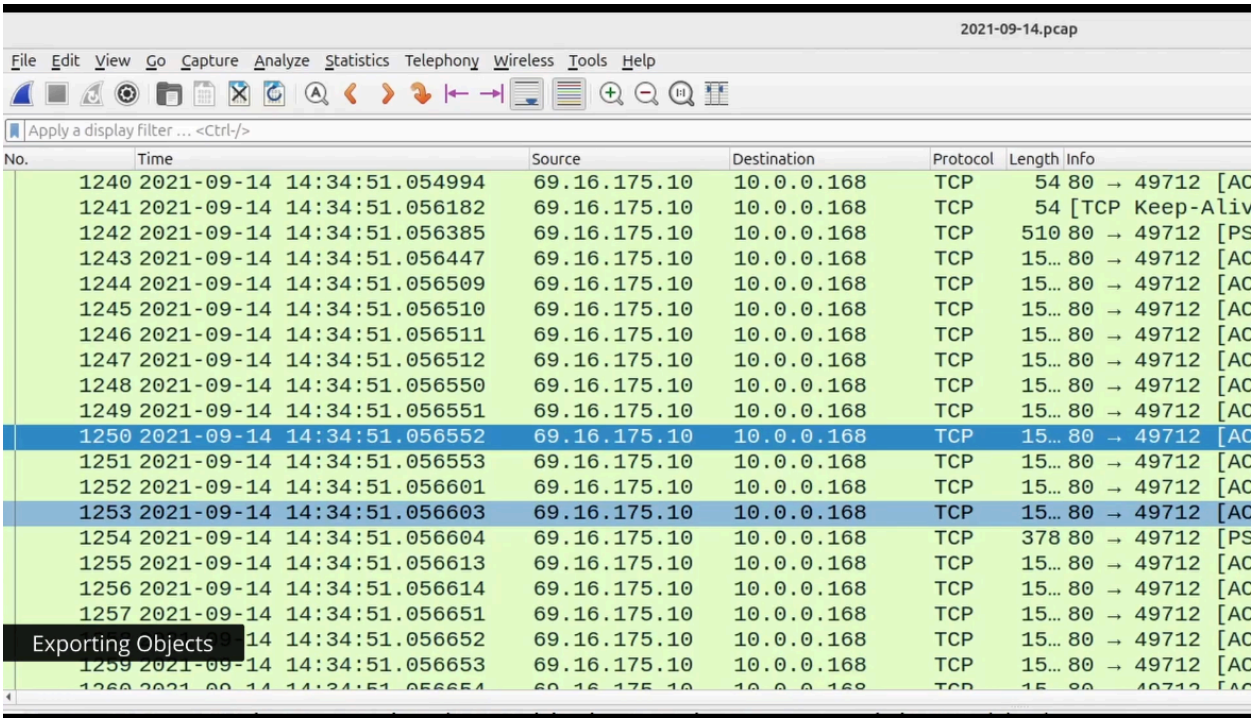
⇒ Keyboard case (CLT + N)

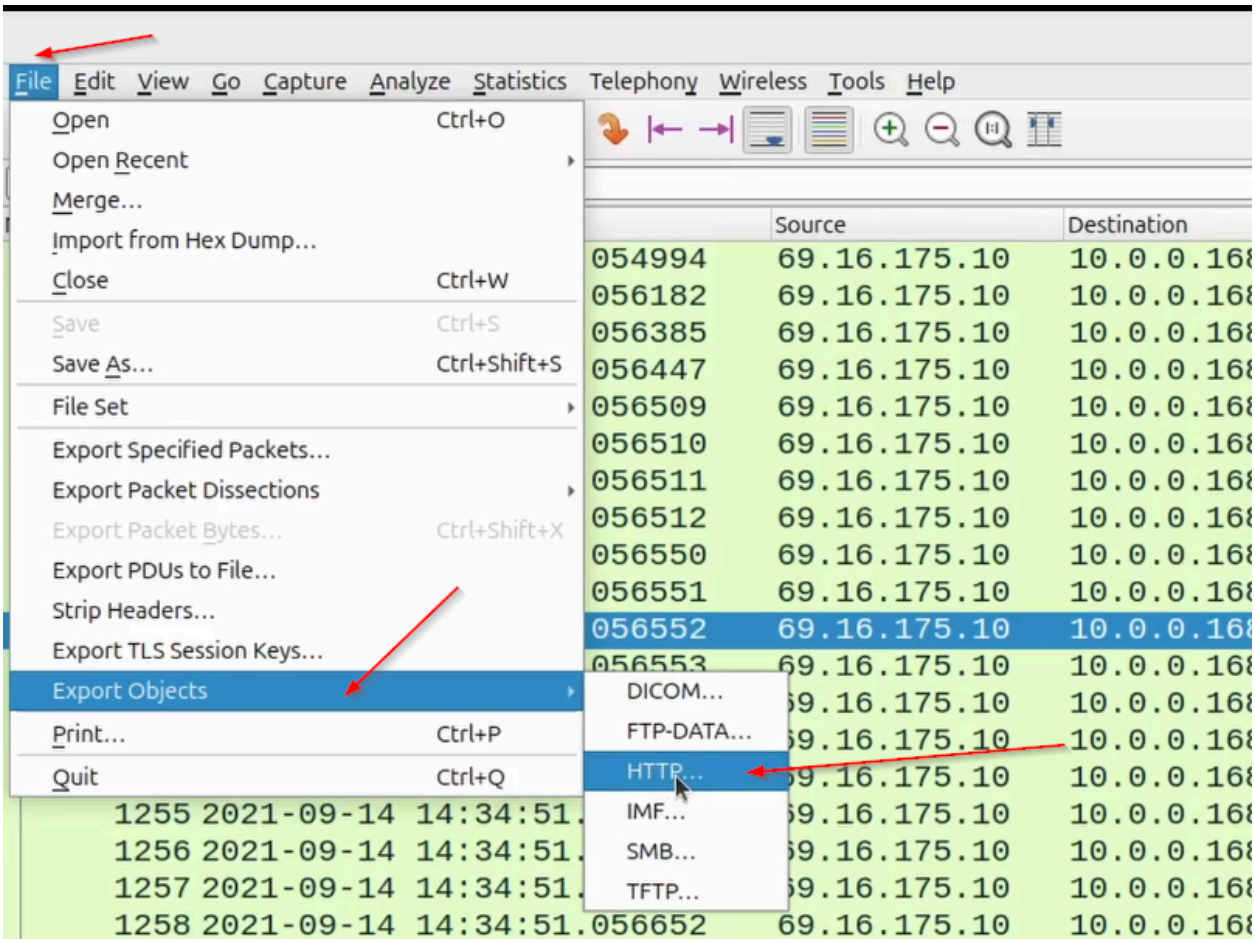




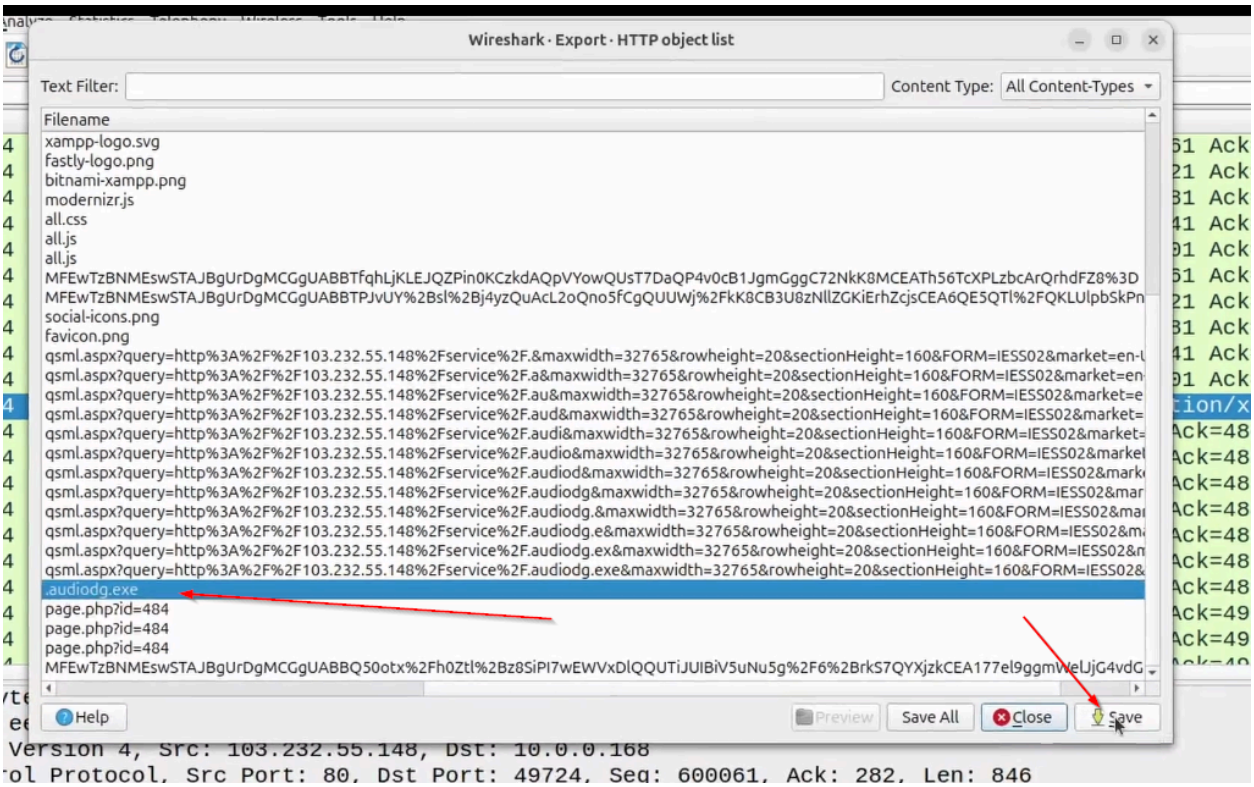
11.) Exporting Objects

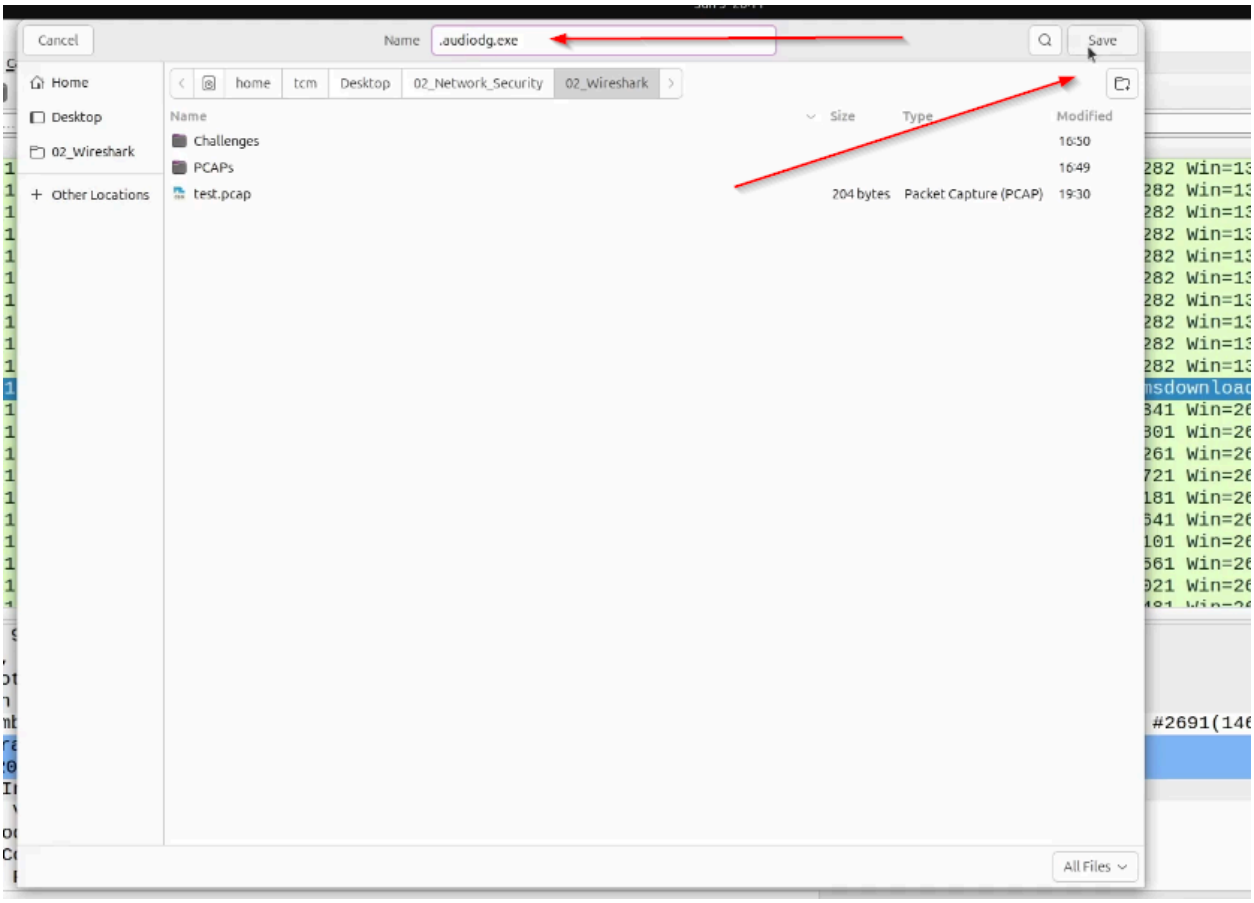
Extracts files transferred via HTTP, SMB, FTP, etc. (e.g., download an `.exe` seen in traffic).


2021-09-14.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1240 2021-09-14 14:34:51.054994 69.16.175.10 10.0.0.168 TCP 54 80 → 49712 [AC
1241 2021-09-14 14:34:51.056182 69.16.175.10 10.0.0.168 TCP 54 [TCP Keep-Aliv
1242 2021-09-14 14:34:51.056385 69.16.175.10 10.0.0.168 TCP 510 80 → 49712 [PS
1243 2021-09-14 14:34:51.056447 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1244 2021-09-14 14:34:51.056509 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1245 2021-09-14 14:34:51.056510 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1246 2021-09-14 14:34:51.056511 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1247 2021-09-14 14:34:51.056512 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1248 2021-09-14 14:34:51.056550 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1249 2021-09-14 14:34:51.056551 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1250 2021-09-14 14:34:51.056552 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1251 2021-09-14 14:34:51.056553 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1252 2021-09-14 14:34:51.056601 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1253 2021-09-14 14:34:51.056603 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1254 2021-09-14 14:34:51.056604 69.16.175.10 10.0.0.168 TCP 378 80 → 49712 [PS
1255 2021-09-14 14:34:51.056613 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1256 2021-09-14 14:34:51.056614 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1257 2021-09-14 14:34:51.056651 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
14:34:51.056652 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
1259 2021-09-14 14:34:51.056653 69.16.175.10 10.0.0.168 TCP 15… 80 → 49712 [AC
Exporting Objects



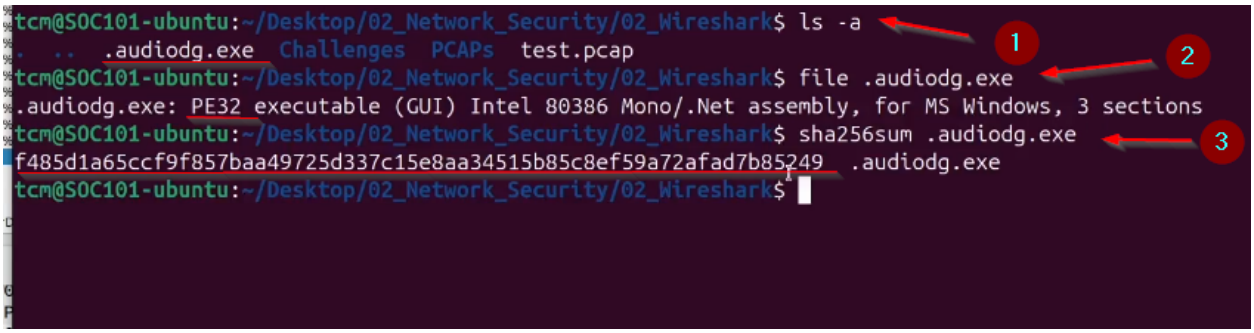
Find malware file and download or save


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Filename
xampp-logo.svg
fastly-logo.png
bitnami-xampp.png
modernizr.js
all.css
all.js
all.js
social-icons.png
favicon.png
.audiodg.exe
page.php?id=484
page.php?id=484
page.php?id=484
Help
Preview
Save All
Close
Save
Version 4, Src: 103.232.55.148, Dst: 10.0.0.168
ol Protocol, Src Port: 80, Dst Port: 49724, Seq: 600061, Ack: 282, Len: 846



Check File repetition:

Collect that file details like meta data file type and hash



Finally Virus total to scan