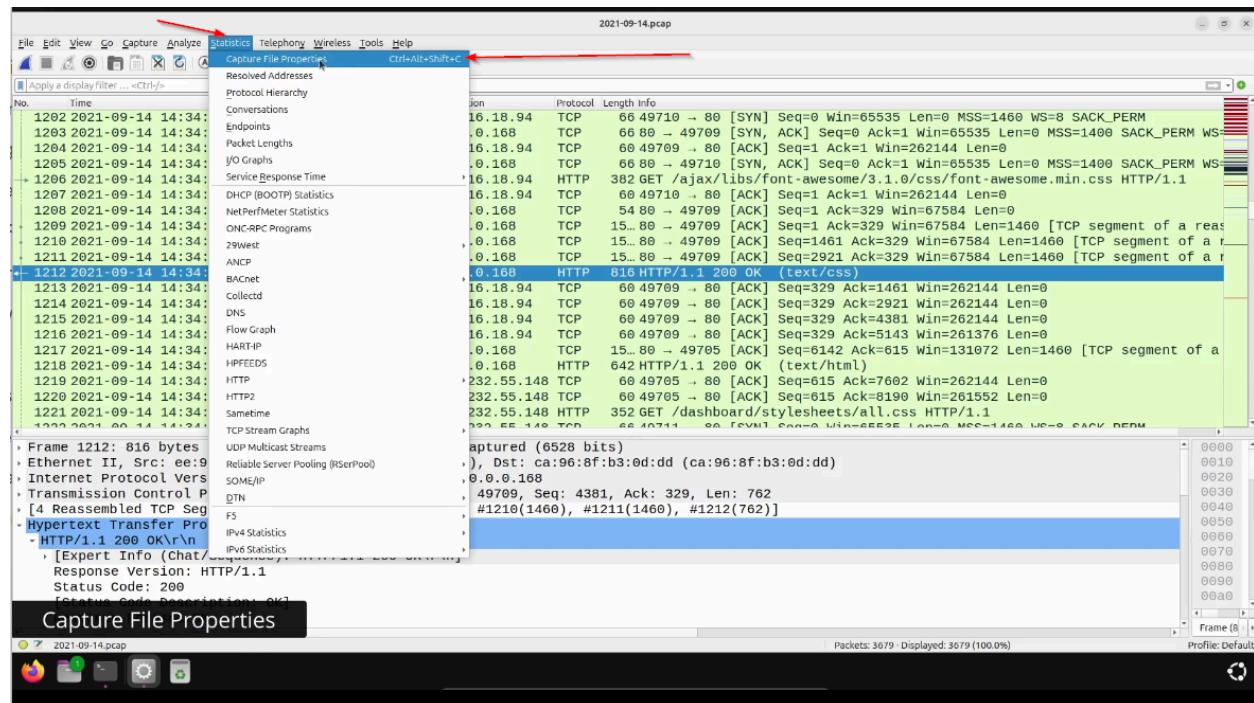


# 11. Wireshark - Statistics

⇒ 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

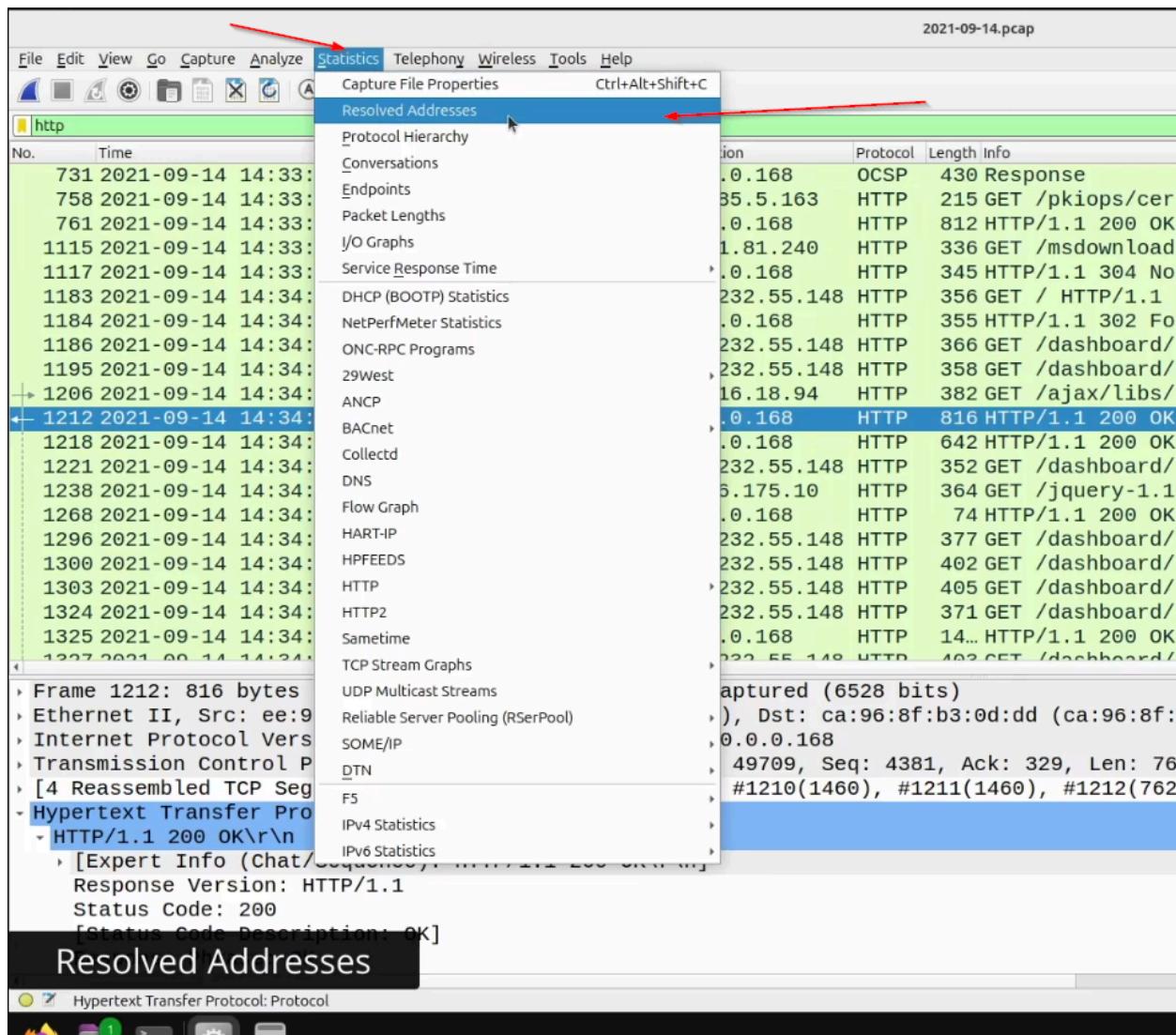
Shows details about the **.pcap** file—file size, packet count, duration, average packet rate, etc.

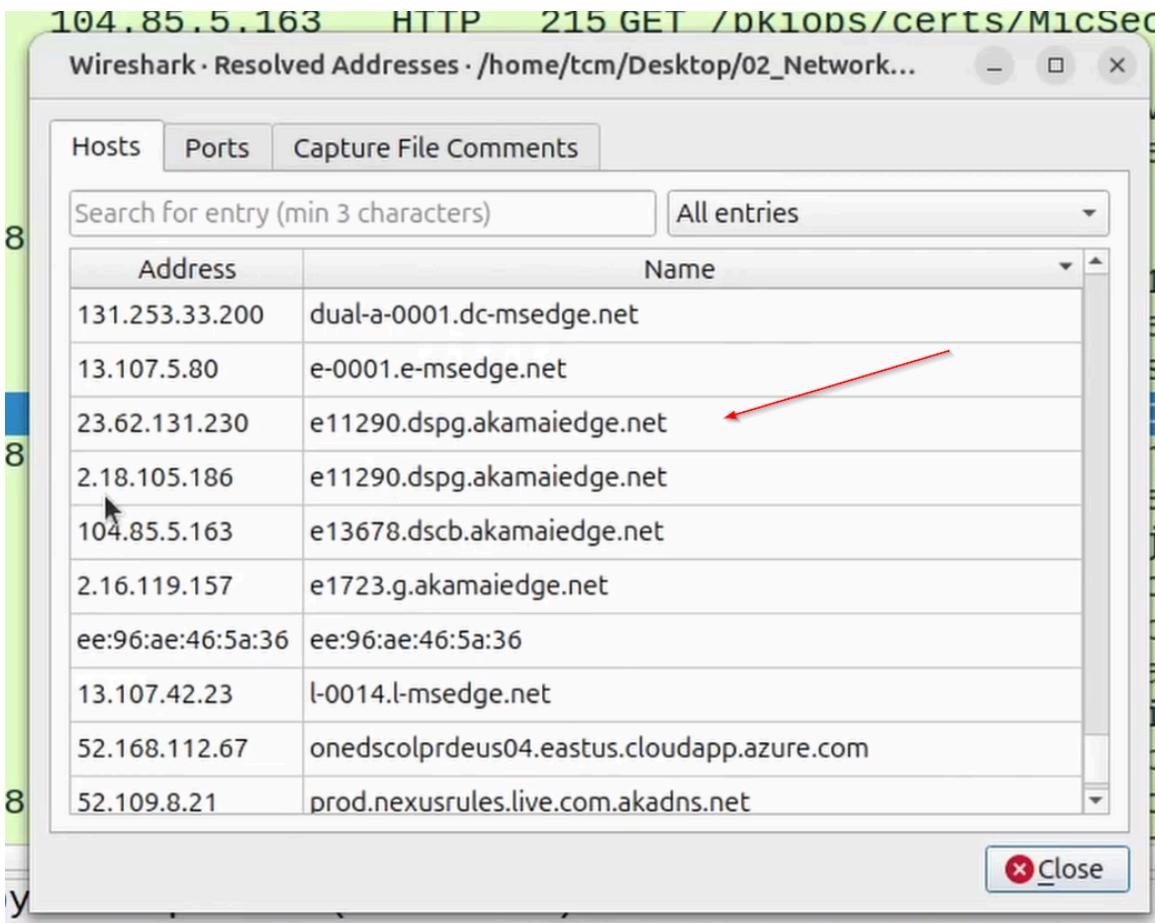


Wireshark - Capture File Properties - 2021-09-14.pcap				
Details				
<b>File</b>				
Name:	/home/ms17/Desktop/02_Network_Security/02_Wireshark/PCAPs/2021-09-14.pcap			
Length:	2,450 kB			
Hash (SHA256):	6d0c4c0b58274b25d0711f7ce29ddc0d7c0c6e594d73bddc2a1e2a90923d1c87			
Hash (SHA1):	c2fa875fe4610d9931fe8b05e1c10ec0e3b5a6b6			
Format:	Wireshark/tcpdump/... - pcap			
Encapsulation:	Ethernet			
Snapshot length:	262144			
<b>Time</b>				
First packet:	2021-09-14 20:02:16			
Last packet:	2021-09-14 20:12:01			
Elapsed:	00:09:44			
<b>Capture</b>				
Hardware:	Unknown			
OS:	Unknown			
Application:	Unknown			
<b>Interfaces</b>				
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	262144 bytes
<b>Statistics</b>				
Measurement	Captured	Displayed	Marked	
packets	3679	3679 (100.0%)	—	
Time span, s	584.905	584.905	—	
Average pps	6.3	6.3	—	
Average packet size, B	650	650	—	
Bytes	2391470	2391470 (100.0%)	0	
Average bytes/s	4,088	4,088	—	
Average bits/s	32 k	32 k	—	

## 2.) Resolved Addresses

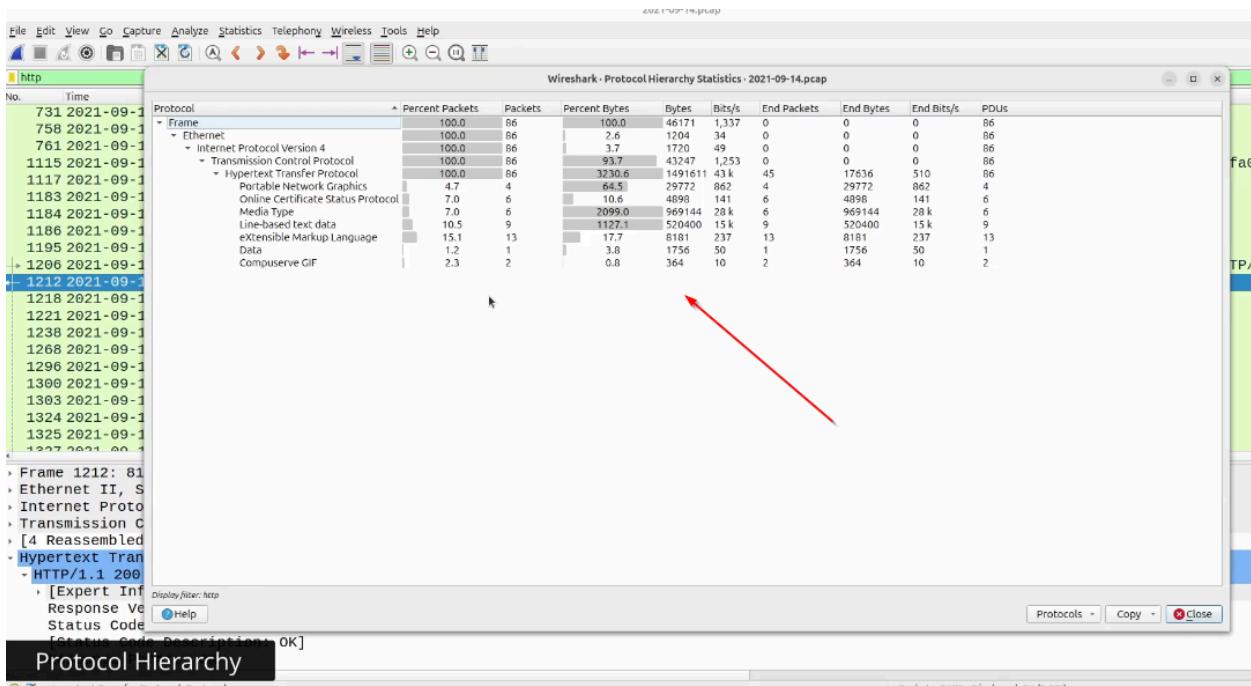
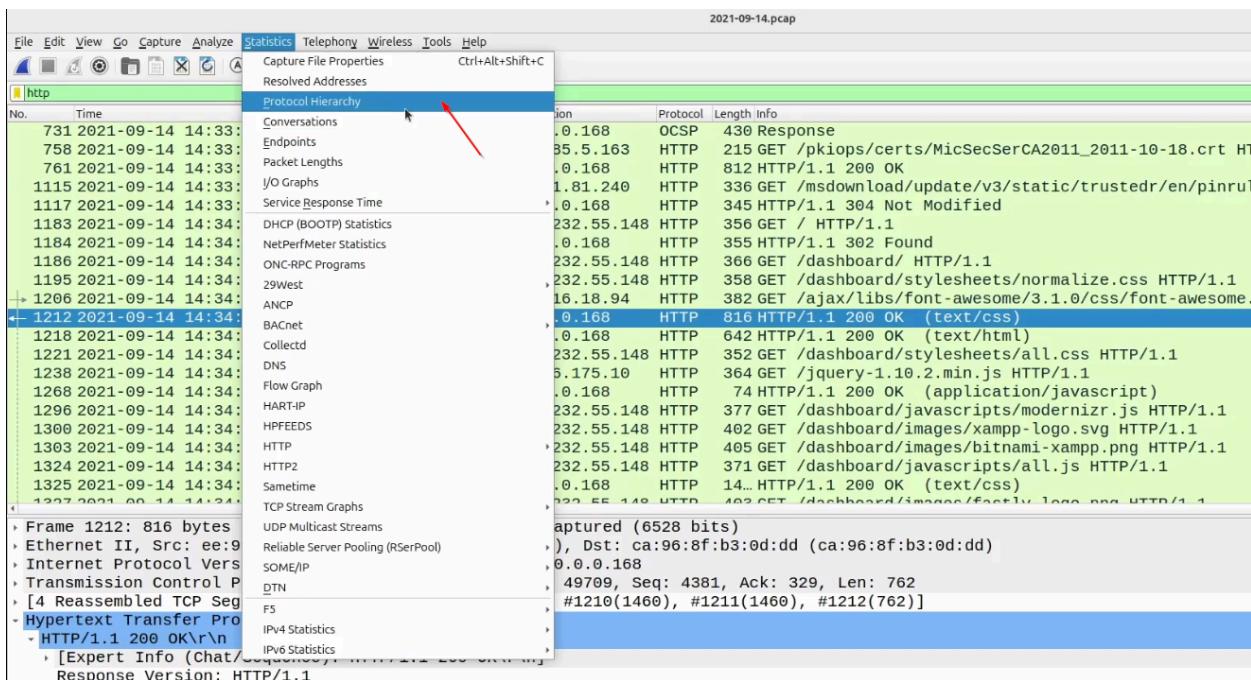
Lists hostnames (via DNS) and MAC vendor names if address resolution is enabled.





### 3.) Protocol Hierarchy

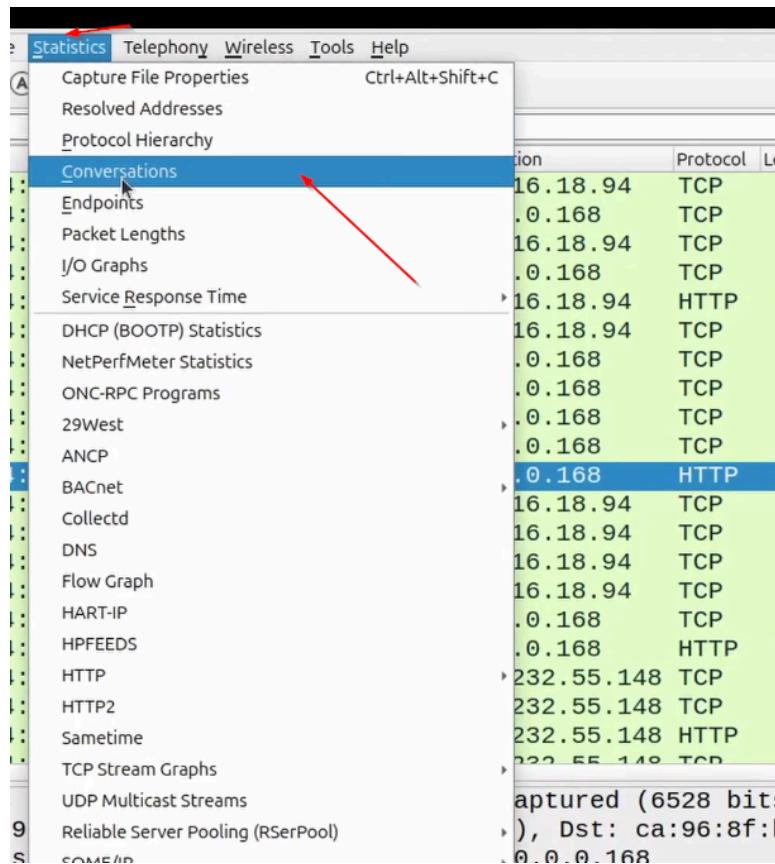
Breaks down all observed protocols in the capture by percentage, bytes, and packet count (e.g., TCP, HTTP, DNS).



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.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A →
ca:96:0f:b3:0d:dd	01:00:5e:7fff:fa	8	1 kB	8	1 kB	0	0 bytes	57.883316	6.0144	1,904 bits
ca:96:0f:b3:0d:dd	ee:96:ae:46:5a:36	3,631	2 MB	1,838	146 kB	1,793	2 MB	1.260830	583.6437	2,003 bits
ca:96:0f:b3:0d:dd	ffff:ffff:ff:ff	40	7 kB	40	7 kB	0	0 bytes	0.000000	520.4967	100 bits

Protocol

- Bluetooth
- BPV7
- DCCP
- Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- IPv4
- IPv6
- IPX
- JXTA
- LTP
- MPTCP

Conversations

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

Ethernet · 3	IPv4 · 21	IPv6	TCP · 47	UDP · 21	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
10.0.0.168	103.232.55.148		2,075	2 MB		1,063	69 kB	1,012	1 MB	2.434030	219.9713	2,498 bits/s	
10.0.0.168	2.16.119.157		358	269 kB		166	13 kB	192	256 kB	60.178052	13.5268	7,811 bits/s	
10.0.0.168	204.79.197.200		392	264 kB		196	14 kB	196	250 kB	67.119071	128.0920	847 bits/s	
10.0.0.168	31.13.64.21		158	85 kB		82	6 kB	76	79 kB	157.902150	64.2260	732 bits/s	
10.0.0.168	72.21.81.200		82	38 kB		43	4 kB	39	34 kB	31.281422	80.9059	368 bits/s	
10.0.0.168	69.16.175.10		70	38 kB		36	2 kB	34	35 kB	154.773375	67.3575	294 bits/s	
10.0.0.168	13.107.42.23		45	33 kB		16	2 kB	29	31 kB	3.418421	65.9042	234 bits/s	
10.0.0.168	52.109.8.21		28	20 kB		13	2 kB	15	18 kB	3.418160	110.0918	135 bits/s	
10.0.0.168	13.107.5.80		60	20 kB		30	9 kB	30	10 kB	191.783934	71.6920	1,043 bits/s	
10.0.0.168	23.62.131.230		55	17 kB		30	3 kB	25	14 kB	67.764976	153.5625	155 bits/s	
10.0.0.168	52.168.112.67		31	16 kB		19	9 kB	12	7 kB	278.617315	110.0903	620 bits/s	
10.0.0.168	31.13.64.35		66	13 kB		35	3 kB	31	9 kB	158.351265	63.7732	404 bits/s	
10.0.0.168	93.184.220.29		52	11 kB		27	3 kB	25	8 kB	31.550561	381.1171	63 bits/s	
10.0.0.168	104.16.18.94		23	7 kB		13	1 kB	10	6 kB	154.521763	67.6126	131 bits/s	
10.0.0.168	10.0.0.255		39	6 kB		39	6 kB	0	0 bytes	0.000000	520.4967	99 bits/s	
10.0.0.168	23.209.125.71		14	6 kB		7	665 bytes	7	6 kB	31.497565	109.9813	48 bits/s	
10.0.0.168	136.243.159.53		36	5 kB		18	3 kB	18	2 kB	268.315691	1.4308	14 kbps	
10.0.0.168	8.8.8.8		36	5 kB		18	1 kB	18	3 kB	1.260830	277.3552	41 bits/s	
10.0.0.168	104.85.5.163		11	3 kB		6	521 bytes	5	3 kB	68.008696	73.4689	56 bits/s	
10.0.0.168	239.255.255.250		8	1 kB		8	1 kB	0	0 bytes	57.883316	6.0144	1,904 bits/s	
10.0.0.168	72.21.81.240		10	1 kB		6	642 bytes	4	519 bytes	92.170463	60.2113	85 bits/s	

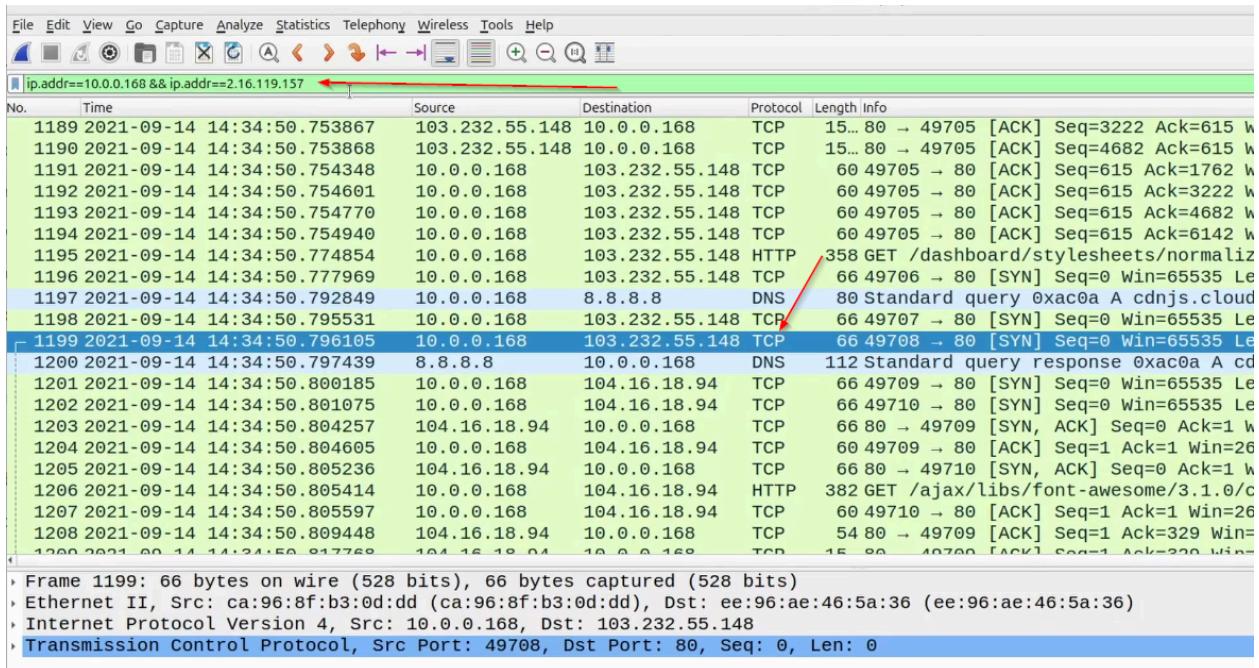
## Filter apply

The screenshot shows the Wireshark interface with the 'Conversations' tab selected. A right-click context menu is open over a row in the table, specifically over the 'Selected' item. Three red arrows point from the top of the image to the 'Selected' item, the 'A → B' item, and the 'Duration' column header respectively. The table lists network conversations with columns for Address A, Address B, Packets, Bytes, Rel. Sh., Duration, and Bits/s A → B.

Address A	Address B	Packets	Bytes	Rel. Sh.	Duration	Bits/s A → B
10.0.0.168	103.232.55.148	2,075	2 MB	A → B	219.9713	2,498 bits/s
10.0.0.168	2.16.119.157	358	269 kB	A → B	13.5268	7,811 bits/s
10.0.0.168	204.79.197.200	392	264 kB	A → B	128.0920	847 bits/s
10.0.0.168	31.13.64.21	158	85 kB	A → Any	64.2260	732 bits/s
10.0.0.168	72.21.81.200	82	38 kB	A → Any	80.9059	368 bits/s
10.0.0.168	69.16.175.10	70	38 kB	A → Any	67.3575	294 bits/s
10.0.0.168	13.107.42.23	45	33 kB	A → Any	65.9042	234 bits/s
10.0.0.168	52.109.8.21	28	20 kB	Any → A	110.0918	135 bits/s
10.0.0.168	13.107.5.80	60	20 kB	Any → B	71.6920	1,043 bits/s
10.0.0.168	23.62.131.230	55	17 kB	Any → B	141.5625	155 bits/s
10.0.0.168	52.168.112.67	31	16 kB	B → Any	153.5625	620 bits/s
10.0.0.168	31.13.64.35	66	13 kB	B → Any	110.0903	404 bits/s
10.0.0.168	93.184.220.29	52	11 kB	B → Any	63.7732	63 bits/s
10.0.0.168	104.16.18.94	23	7 kB	B → Any	6 KB 31.550561	381.1171
10.0.0.168	10.0.0.255	39	6 kB	0 bytes	6 KB 154.521763	67.6126
10.0.0.168	23.209.125.71	14	6 kB	0 bytes	0 bytes 0.000000	520.4967
10.0.0.168	136.243.159.53	36	5 kB	665 bytes	6 kB 31.497565	109.9813
10.0.0.168	8.8.8.8	36	5 kB	3 kB	2 kB 268.315691	14 kbps
10.0.0.168	104.85.5.163	11	3 kB	1 kB	3 kB 1.260830	277.3552
10.0.0.168	239.255.255.250	8	1 kB	521 bytes	3 kB 68.008696	73.4689
10.0.0.168	72.21.81.240	10	1 kB	1 kB	0 bytes 57.883316	6.0144
				642 bytes	519 bytes 92.170463	1,904 bits/s
					4	85 bits/s

## Result

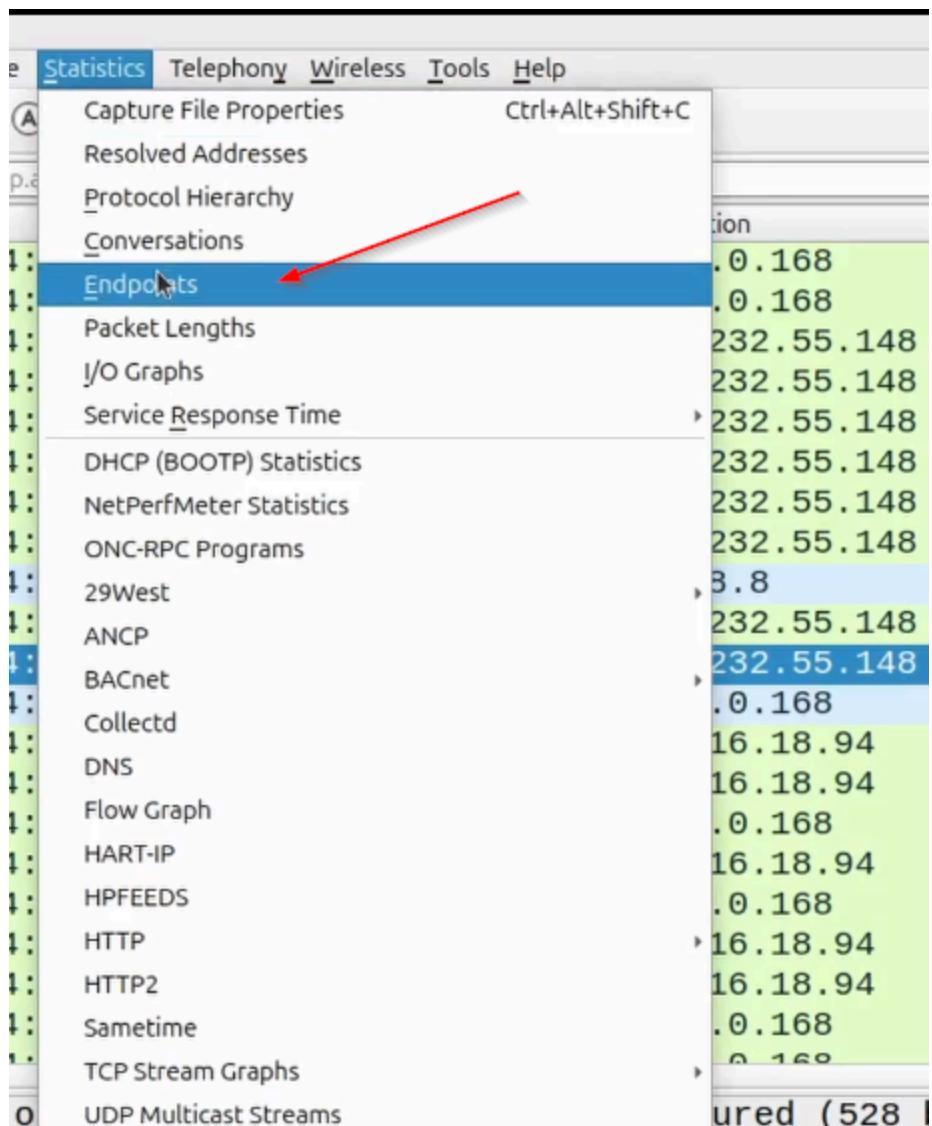
See A → B conversation show



## 5.) Endpoints

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

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



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark - Endpoints - 2021-09-14.pcap

Endpoint Settings							
Protocol		Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
<input type="checkbox"/> Name resolution	Address	8	1 kB	0	0 bytes	8	1 kB
<input type="checkbox"/> Limit to display filter	01:00:5e:7f:ff:fa	3,679	2 MB	1,886	154 kB	1,793	2 MB
	ca:96:8f:b3:0d:dd	3,631	2 MB	1,793	2 MB	1,838	146 kB
	ee:96:ae:46:5a:36	40	7 kB	0	0 bytes	40	7 kB
	ff:ff:ff:ff:ff:ff						

Copy Map

Endpoints

Filter list for specific type

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Double click most conversion show

Endpoint Settings												
Protocol		Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number
<input type="checkbox"/> Name resolution	Address	3,649	2 MB	1,871	153 kB	1,778	2 MB					
<input type="checkbox"/> Limit to display filter	10.0.0.168	2,045	2 MB	1,012	1 MB	1,063	69 kB					
	103.232.55.148	392	264 kB	196	250 kB	196	14 kB					
	204.79.197.200	358	269 kB	192	256 kB	166	13 kB					
	2.16.119.157	158	85 kB	76	79 kB	82	6 kB					
	31.13.64.21	82	38 kB	39	34 kB	43	4 kB					
	72.21.81.200	70	38 kB	34	35 kB	36	2 kB					
	69.16.175.10	66	13 kB	31	9 kB	35	3 kB					
	31.13.64.35	60	20 kB	30	10 kB	30	9 kB					
	13.107.5.80	55	17 kB	25	14 kB	30	3 kB					
	23.62.131.230	52	11 kB	25	8 kB	27	3 kB					
	93.184.220.29	45	33 kB	29	31 kB	16	2 kB					
	13.107.42.23	39	6 kB	0	0 bytes	39	6 kB					
	10.0.0.255	36	5 kB	18	2 kB	18	3 kB					
	136.243.159.53	8.8.8.8	36	5 kB	18	3 kB	18	1 kB				
	8.8.8.8	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	14	6 kB	10	6 kB	13	1 kB					
	23.209.125.71	11	3 kB	5	3 kB	6	521 bytes					
	104.85.5.163	10	1 kB	4	519 bytes	6	642 bytes					
	72.21.81.240	8	1 kB	0	0 bytes	8	1 kB					
	239.255.255.250											

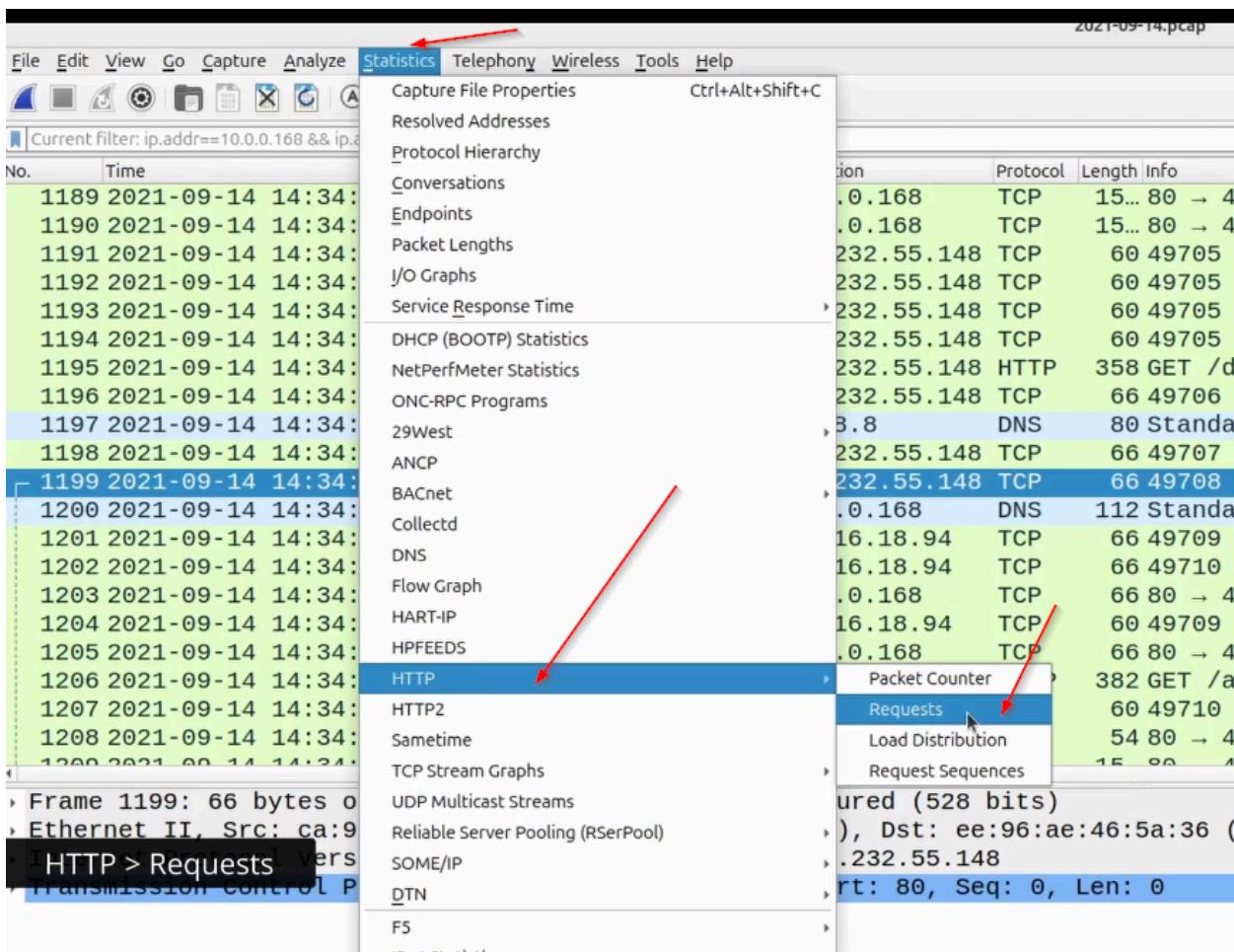
Copy Map

Endpoints

Filter list for specific type

## 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
    - /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdaQpVYowQUsT7DaQP4v0cB1JgmGc
    - /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfJvUY%2Bs!%2Bj4yzQuAcl2oQno5fCgQUUWj%2FkK8CB3U
    - /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%
    - /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%
    - /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm%
    - /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPi7wEWVxDlQQUTiJUIBiV5uNu5g%
  - ctldl.windowsupdate.com
    - /msdcDownload/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
    - /ajax/libs/fontawesome/3.1.0/css/fontawesome\_min.css

Display filter:  Apply

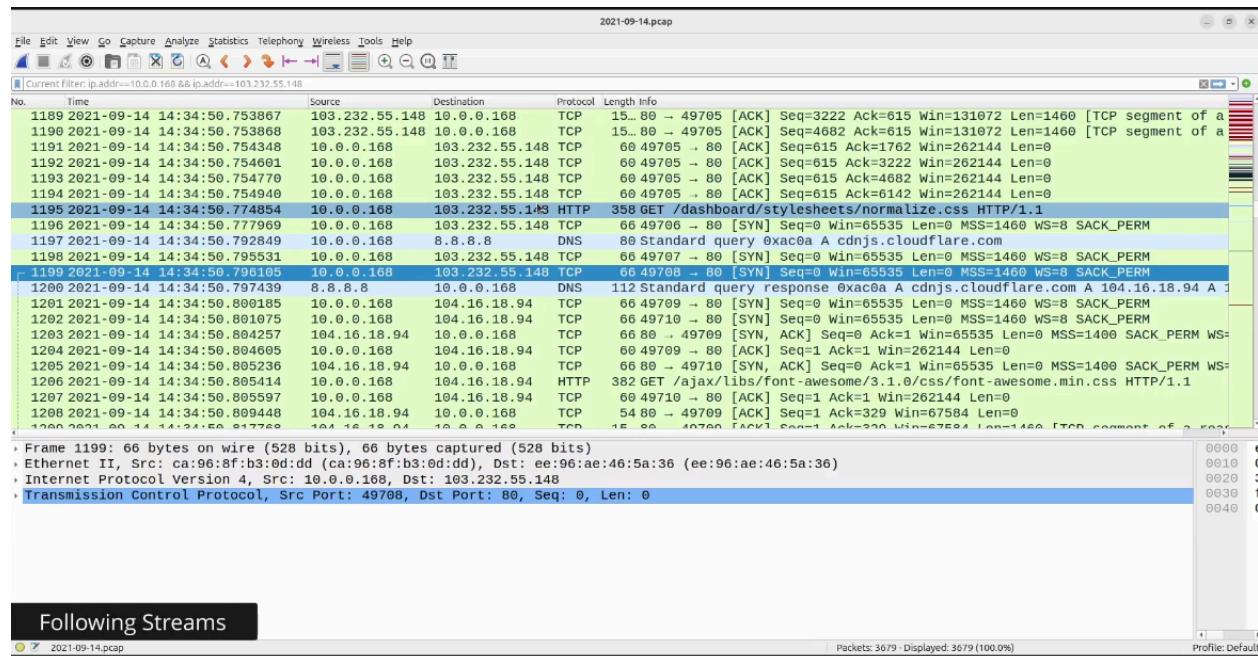
Wireshark · Requests · 2021-09-14.pcap

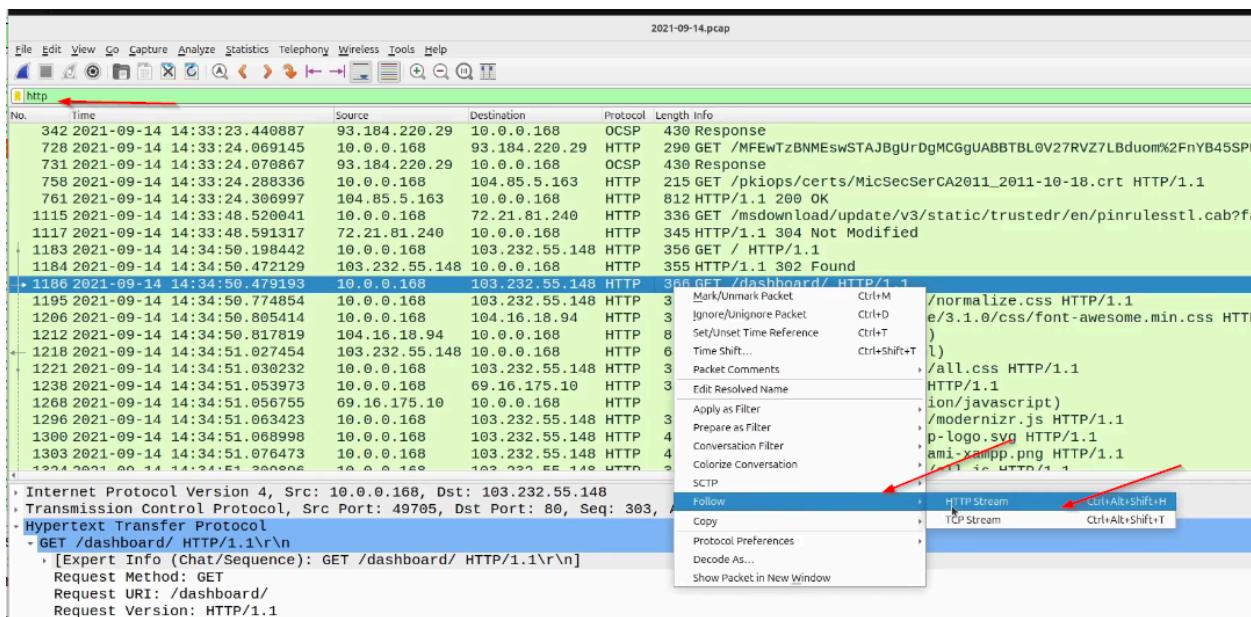
Topic / Item

- \*
- 136.243.159.53
  - /~element/page.php?id=484
- 103.232.55.148
  - /service/.audiogd.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

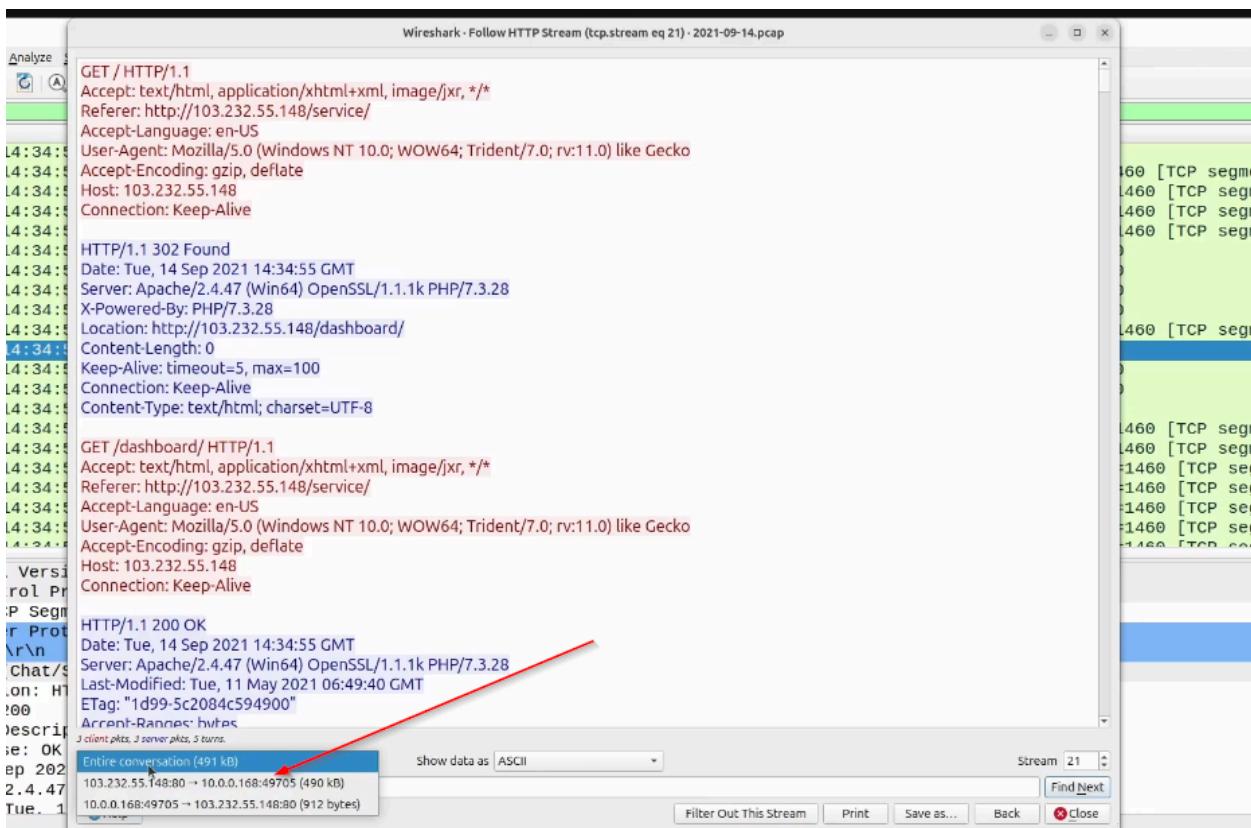
## 7.) Following Streams

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



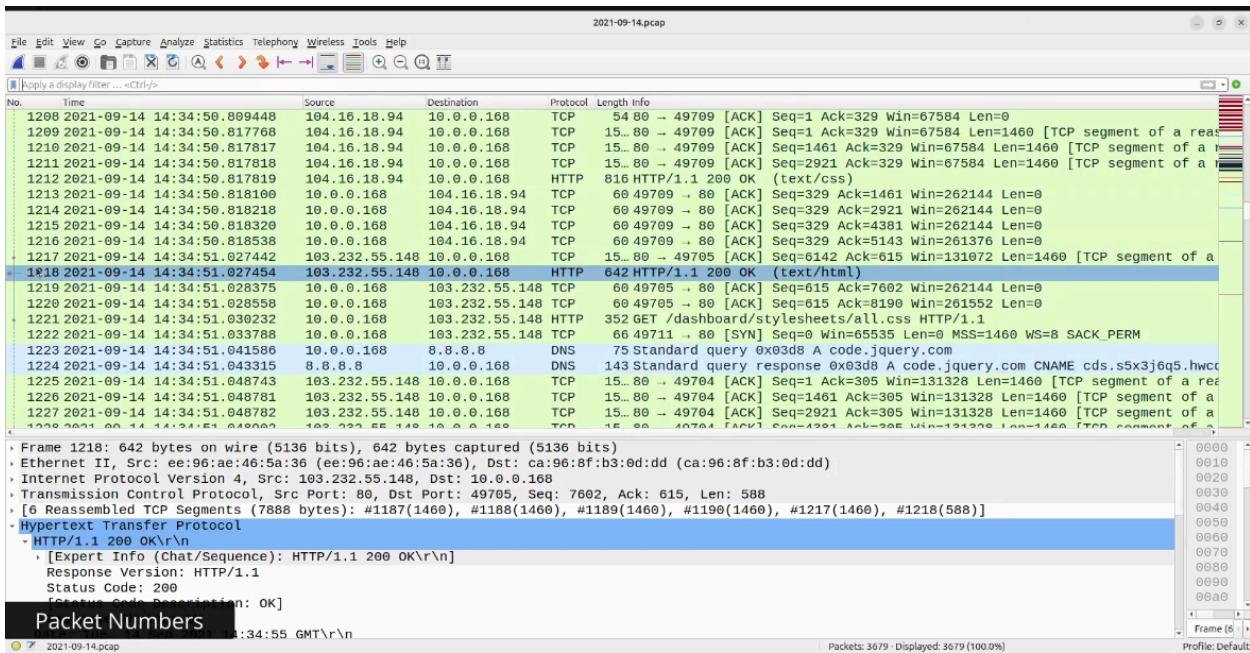


Edit conversation like only show request or response



## 8.) Packet Numbers

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

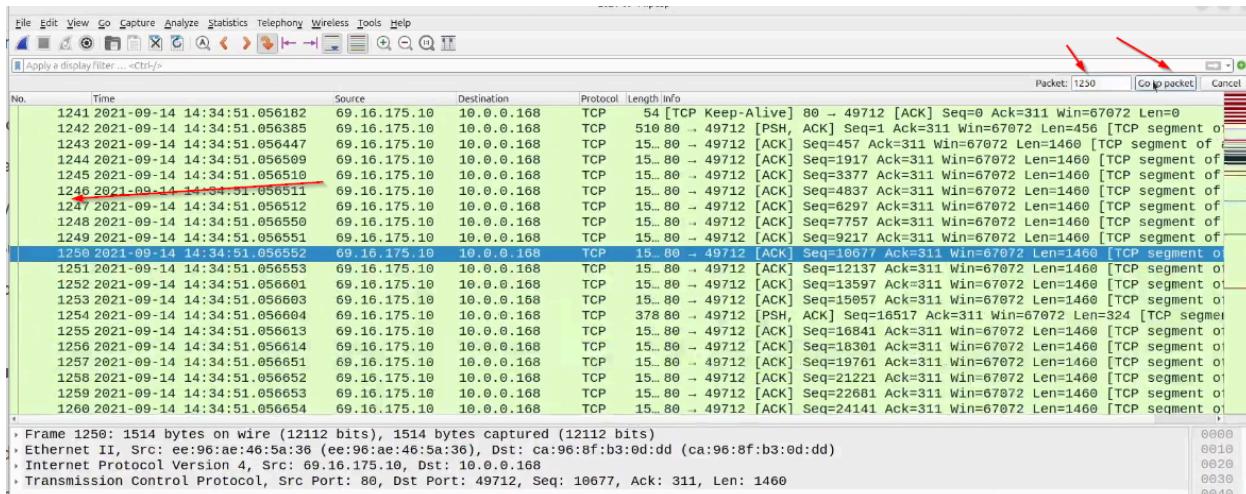
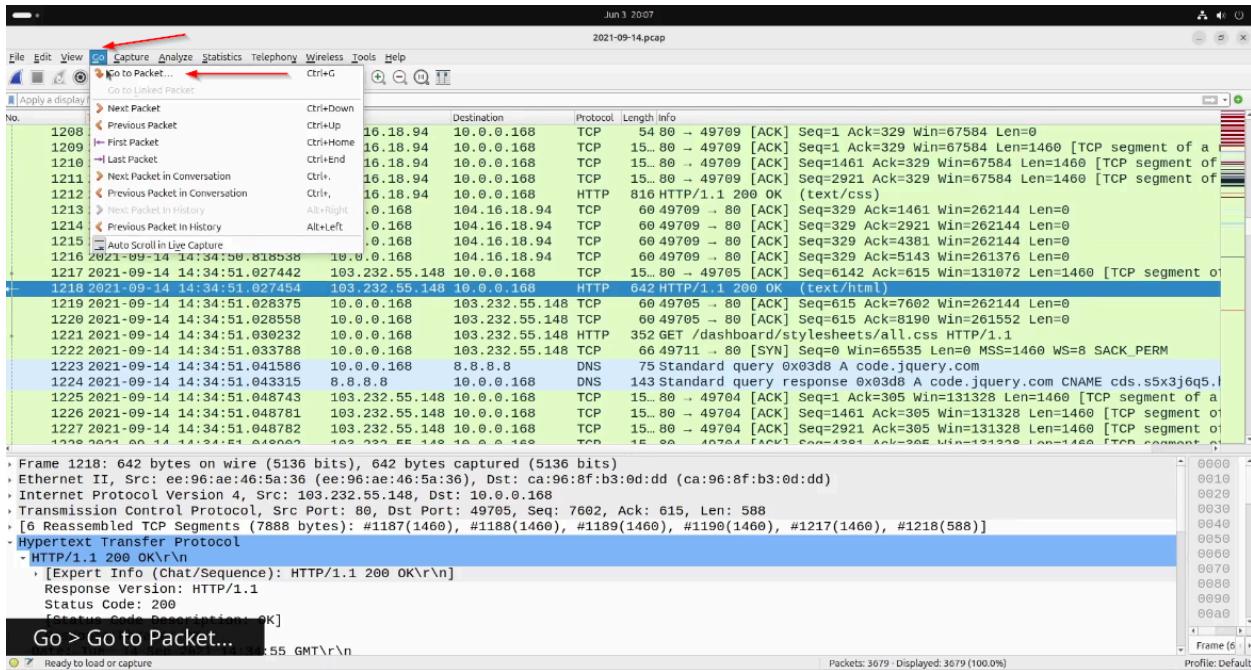


⇒ Packet Number very important

No.	Time
1208	2021-09-14 14:34:50.809448
1209	2021-09-14 14:34:50.817768
1210	2021-09-14 14:34:50.817817
1211	2021-09-14 14:34:50.817818
1212	2021-09-14 14:34:50.817819
1213	2021-09-14 14:34:50.818100
1214	2021-09-14 14:34:50.818218
1215	2021-09-14 14:34:50.818320
1216	2021-09-14 14:34:50.818538
1217	2021-09-14 14:34:51.027442
1218	2021-09-14 14:34:51.027454
1219	2021-09-14 14:34:51.028375
1220	2021-09-14 14:34:51.028558
1221	2021-09-14 14:34:51.030232
1222	2021-09-14 14:34:51.033788
1223	2021-09-14 14:34:51.041586
1224	2021-09-14 14:34:51.043315
1225	2021-09-14 14:34:51.048743
1226	2021-09-14 14:34:51.048781
1227	2021-09-14 14:34:51.048782
1228	2021-09-14 14:34:51.048902

## 9.) Go > Go to Packet

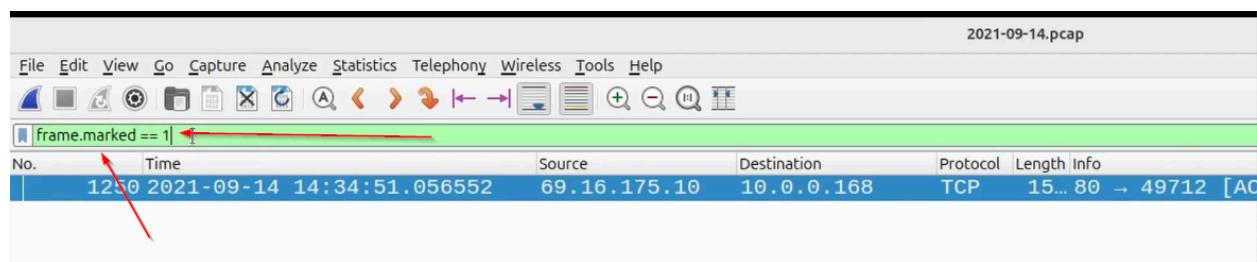
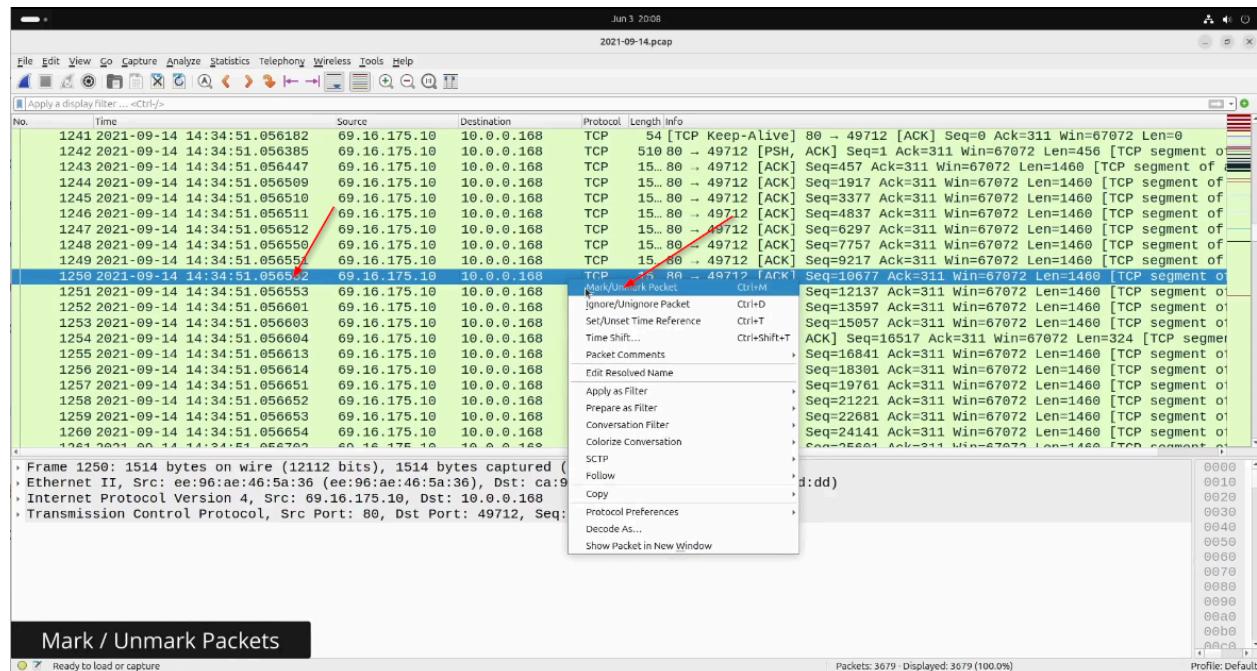
Quickly jump to a specific packet number for focused analysis.



## 10.) Mark / Unmark Packets

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

⇒ Keyboard case ( CLT + N )



## 11.) Exporting Objects

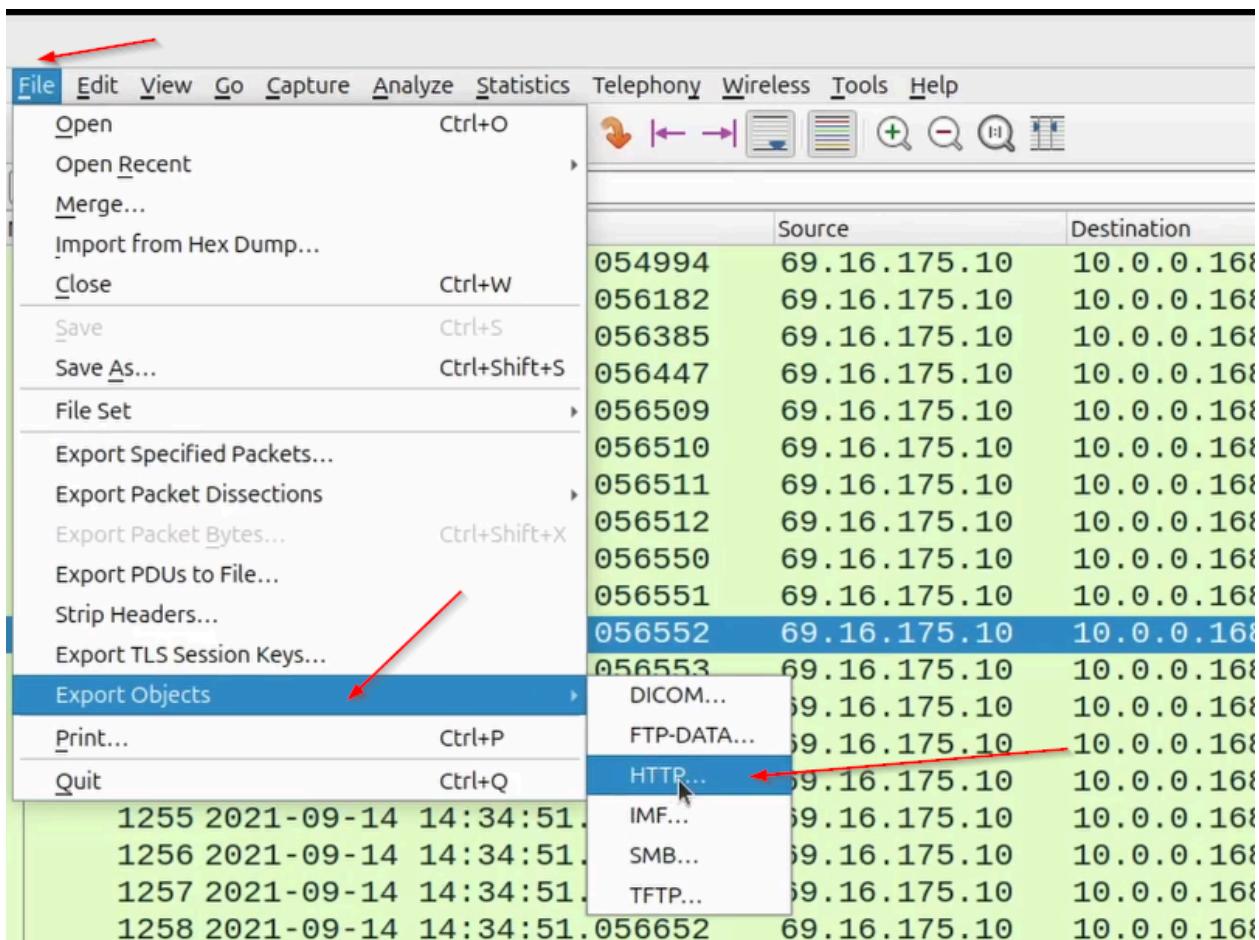
Extracts files transferred via HTTP, SMB, FTP, etc. (e.g., download an .exe seen in traffic).

2021-09-14.pcap

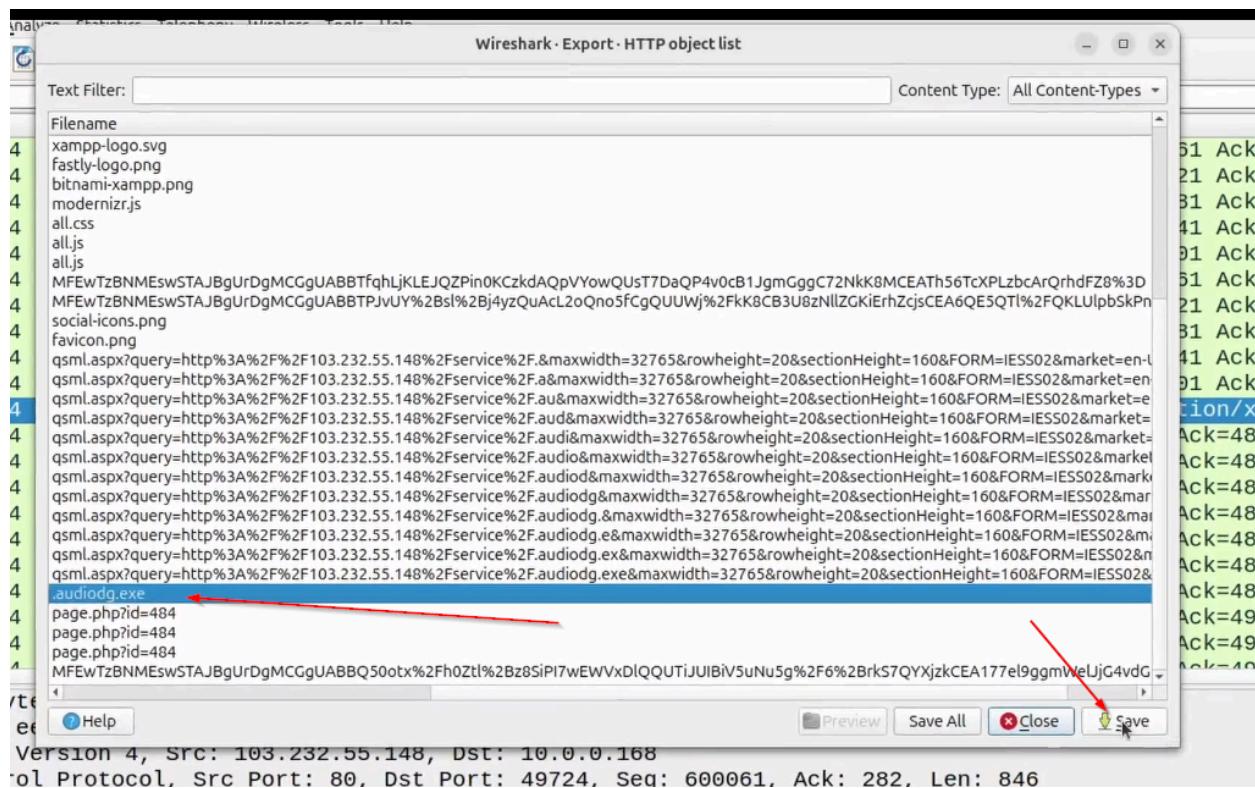
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

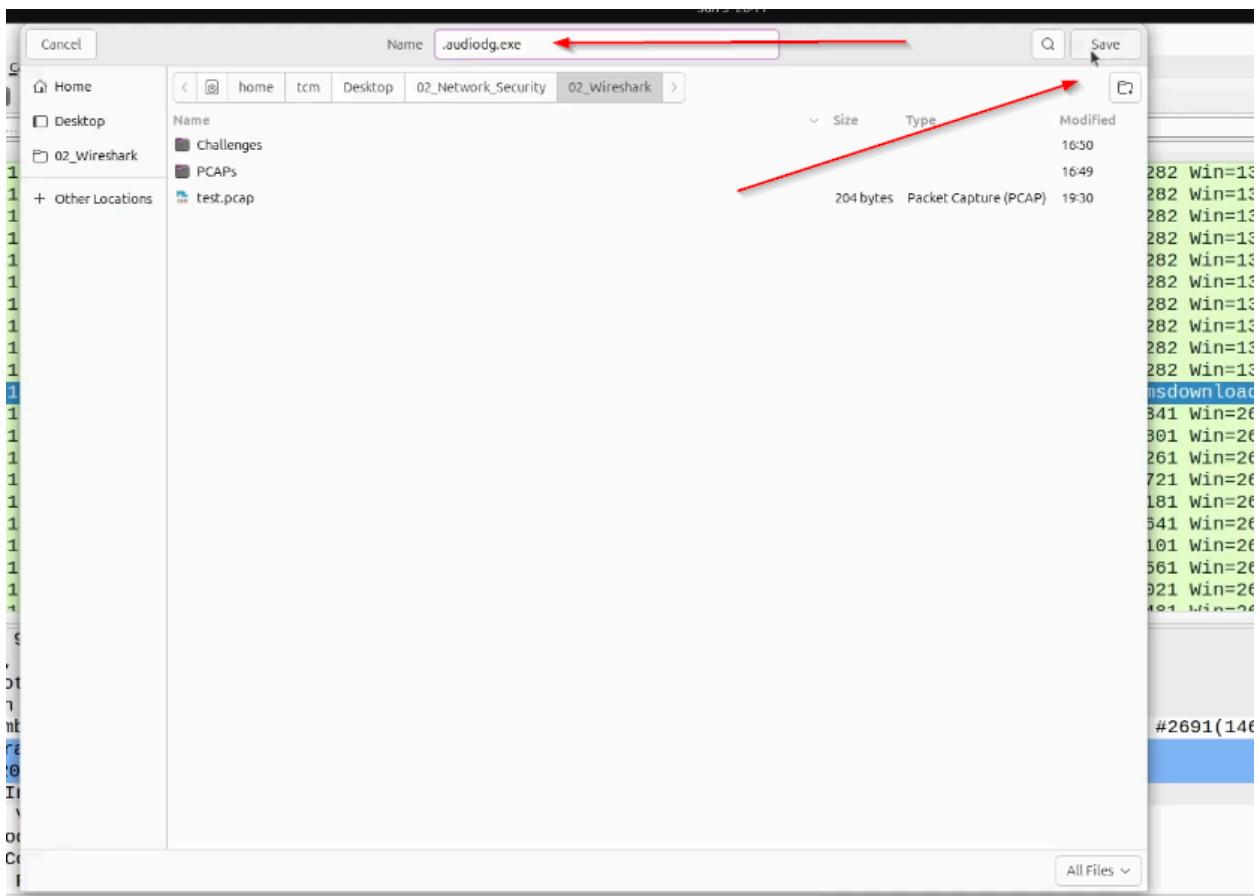
Apply a display filter ... <Ctrl-/>

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-Alive]
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]
Exporting Objects		14	14:34:51.056652	69.16.175.10	10.0.0.168	TCP
				69.16.175.10	10.0.0.168	TCP
				69.16.175.10	10.0.0.168	TCP
				69.16.175.10	10.0.0.168	TCP



Find malware file and download or save





## Check File repetition:

Collect that file details like meta data file type and hash

tcm@SOC101-ubuntu:~/Desktop/02\_Network\_Security/02\_Wireshark\$ ls -a

.. .audiog.exe Challenges PCAPs test.pcap

tcm@SOC101-ubuntu:~/Desktop/02\_Network\_Security/02\_Wireshark\$ file .audiog.exe

.audiog.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections

tcm@SOC101-ubuntu:~/Desktop/02\_Network\_Security/02\_Wireshark\$ sha256sum .audiog.exe

f485d1a65ccf9f857baa49725d337c15e8aa34515b85c8ef59a72afad7b85249 .audiog.exe

tcm@SOC101-ubuntu:~/Desktop/02\_Network\_Security/02\_Wireshark\$

The terminal session shows three steps: 1. Listing files with 'ls -a', 2. Checking the file type with 'file .audiog.exe', and 3. Generating a SHA-256 hash with 'sha256sum .audiog.exe'.

Finally Virus total to scan

VirusTotal - File - f485d1a65ccf9f857baa49725d337c15e8aa34515b85c8ef59a72afad7b85249

52/72 security vendors and 4 sandboxes flagged this file as malicious

f485d1a65ccf9f857baa49725d337c15e8aa34515b85c8ef59a72afad7b85249

CallerFilePathAttribu.exe

Community Score: 52 / 72

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

The screenshot shows the VirusTotal interface with a search bar containing the file hash. The main summary indicates a high detection rate of 52 out of 72 security vendors flagged it as malicious. Below this, the file name and path are listed, along with its file type (EXE).