Lab Assignment
& Solution

Cybersecurity Professional Program

Network Security

Network Traffic Analysis

NS-04-LS2
Advanced Analysis

Note: Solutions for the instructor are shown in the green box.

Lab Objective

The lab aims to practice analyzing data packets using a packet analysis tool.

Lab Mission

Practice the new ways you learned to capture traffic and analyze a .pcap file.

Lab Duration

25–30 minutes

Requirements

- Advanced knowledge of Wireshark

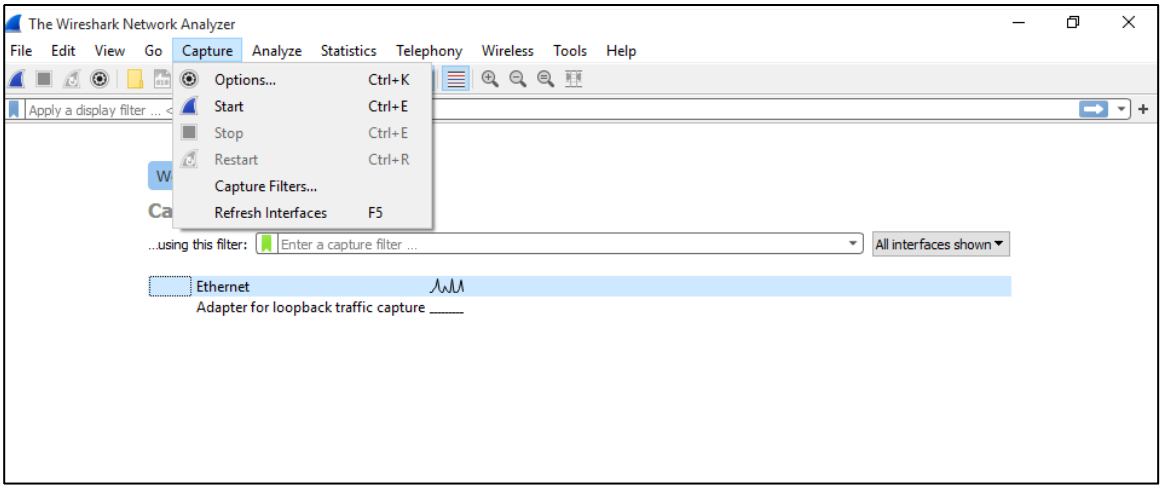
Resources

- Environment & Tools
  - VirtualBox
    - Windows 10 VM (NAT)
  - Wireshark
- Extra Lab Files
  - ***Advanced Analysis.pcap***

Lab Task 1: Filter Configuration

In this task, you will set predefined filters for a network interface controller (NIC).

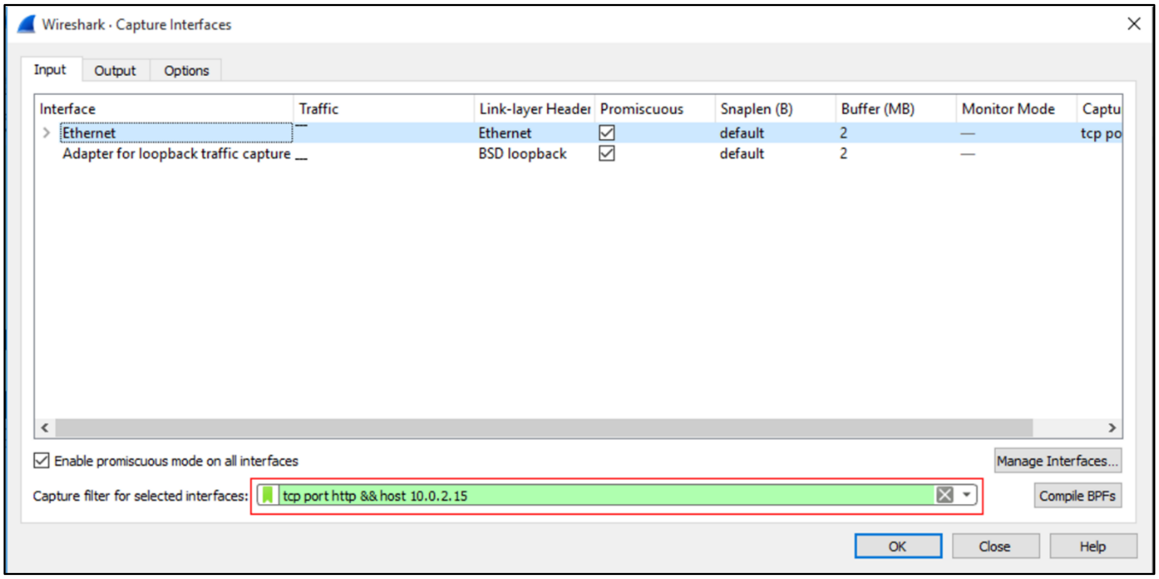
1 On your Windows 10 machine, launch Wireshark, click the **Capture** menu at the top, and select ***Options…*** or press ***Ctrl+K***.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Apply a display filter ...
...using this filter:
Enter a capture filter ...
All interfaces shown
Ethernet
Adapter for loopback traffic capture

2 On the **Options** screen, identify and select the interface with which you are connected to the internet. Apply the following filters at the bottom of the screen:

tcp port http && host [your Win7 VM IP]

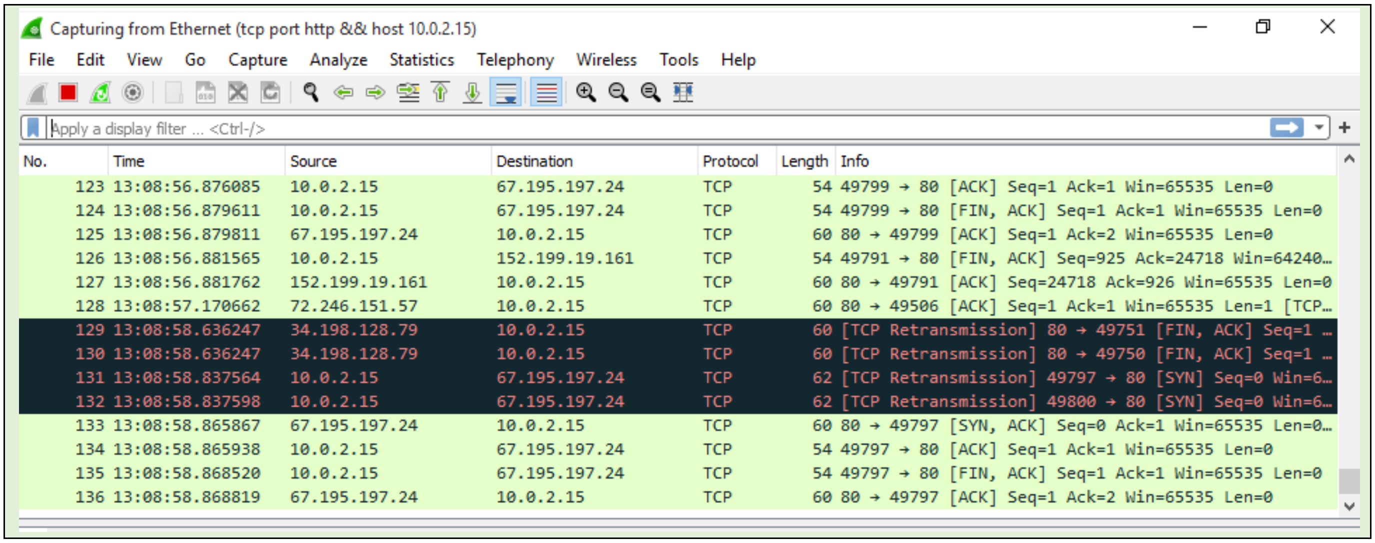
This filter will tell Wireshark to capture only traffic related to that IP address and HTTP traffic.


Wireshark · Capture Interfaces
Input
Output
Options
☑ Enable promiscuous mode on all interfaces
Manage Interfaces...
Compile BPFs
OK
Close
Help

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Captu
Ethernet		Ethernet	☑	default	2	—	tcp po
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	

Capture filter for selected interfaces: tcp port http && host 10.0.2.15

3 Open a browser on your Windows 10 VM and navigate to an HTTP site, such as *pdf995.com/*. You should see only traffic belonging to your VM and part of the HTTP traffic.


Capturing from Ethernet (tcp port http && host 10.0.2.15)
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

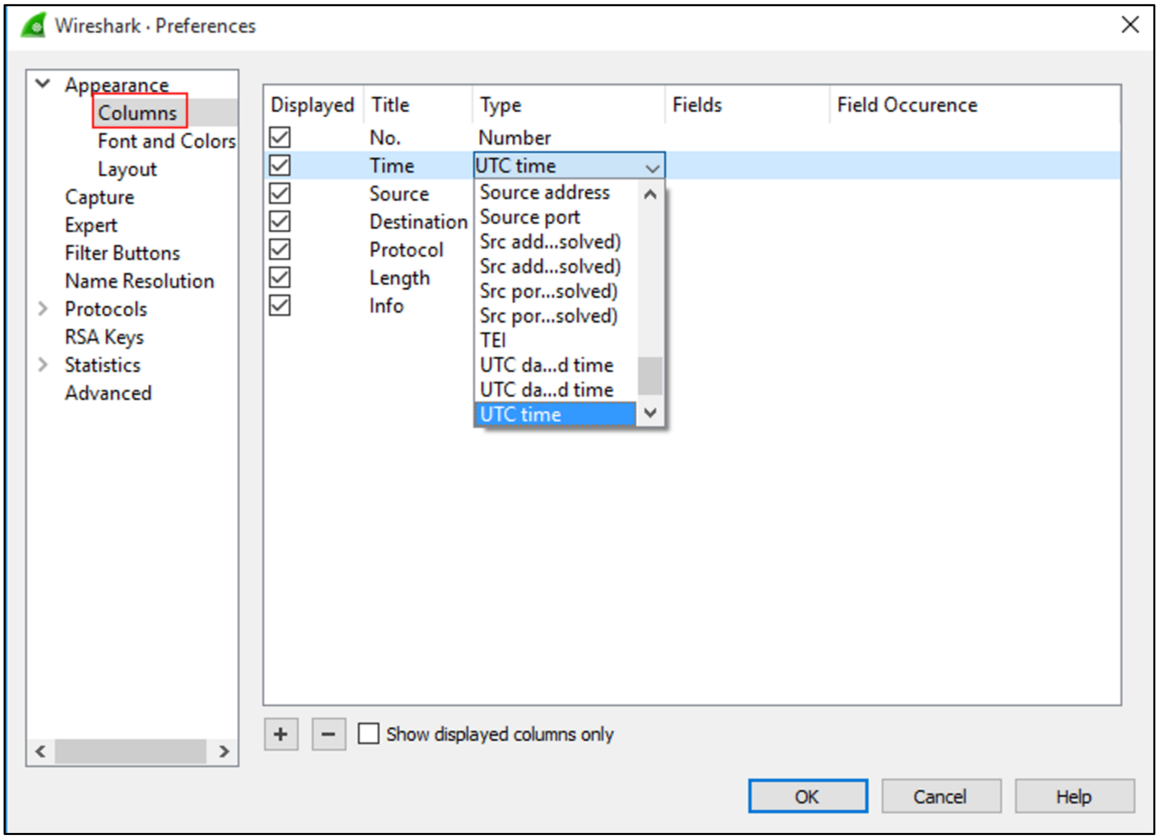
```
No.    Time             Source          Destination     Protocol  Length Info
   123 13:08:56.876085  10.0.2.15       67.195.197.24   TCP       54 49799 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   124 13:08:56.879611  10.0.2.15       67.195.197.24   TCP       54 49799 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
   125 13:08:56.879811  67.195.197.24   10.0.2.15       TCP       60 80 → 49799 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   126 13:08:56.881565  10.0.2.15       152.199.19.161  TCP       54 49791 → 80 [FIN, ACK] Seq=925 Ack=24718 Win=64240…
   127 13:08:56.881762  152.199.19.161  10.0.2.15       TCP       60 80 → 49791 [ACK] Seq=24718 Ack=926 Win=65535 Len=0
   128 13:08:57.170662  72.246.151.57   10.0.2.15       TCP       60 80 → 49506 [ACK] Seq=1 Ack=1 Win=65535 Len=1 [TCP…
   129 13:08:58.636247  34.198.128.79   10.0.2.15       TCP       60 [TCP Retransmission] 80 → 49751 [FIN, ACK] Seq=1 …
   130 13:08:58.636247  34.198.128.79   10.0.2.15       TCP       60 [TCP Retransmission] 80 → 49750 [FIN, ACK] Seq=1 …
   131 13:08:58.837564  10.0.2.15       67.195.197.24   TCP       62 [TCP Retransmission] 49797 → 80 [SYN] Seq=0 Win=6…
   132 13:08:58.837598  10.0.2.15       67.195.197.24   TCP       62 [TCP Retransmission] 49800 → 80 [SYN] Seq=0 Win=6…
   133 13:08:58.865867  67.195.197.24   10.0.2.15       TCP       60 80 → 49797 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0…
   134 13:08:58.865938  10.0.2.15       67.195.197.24   TCP       54 49797 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   135 13:08:58.868520  10.0.2.15       67.195.197.24   TCP       54 49797 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
   136 13:08:58.868819  67.195.197.24   10.0.2.15       TCP       60 80 → 49797 [ACK] Seq=1 Ack=2 Win=65535 Len=0
```

Lab Task 2: Packet Capture

In this task, you will create and modify columns and set up filters based on existing traffic.

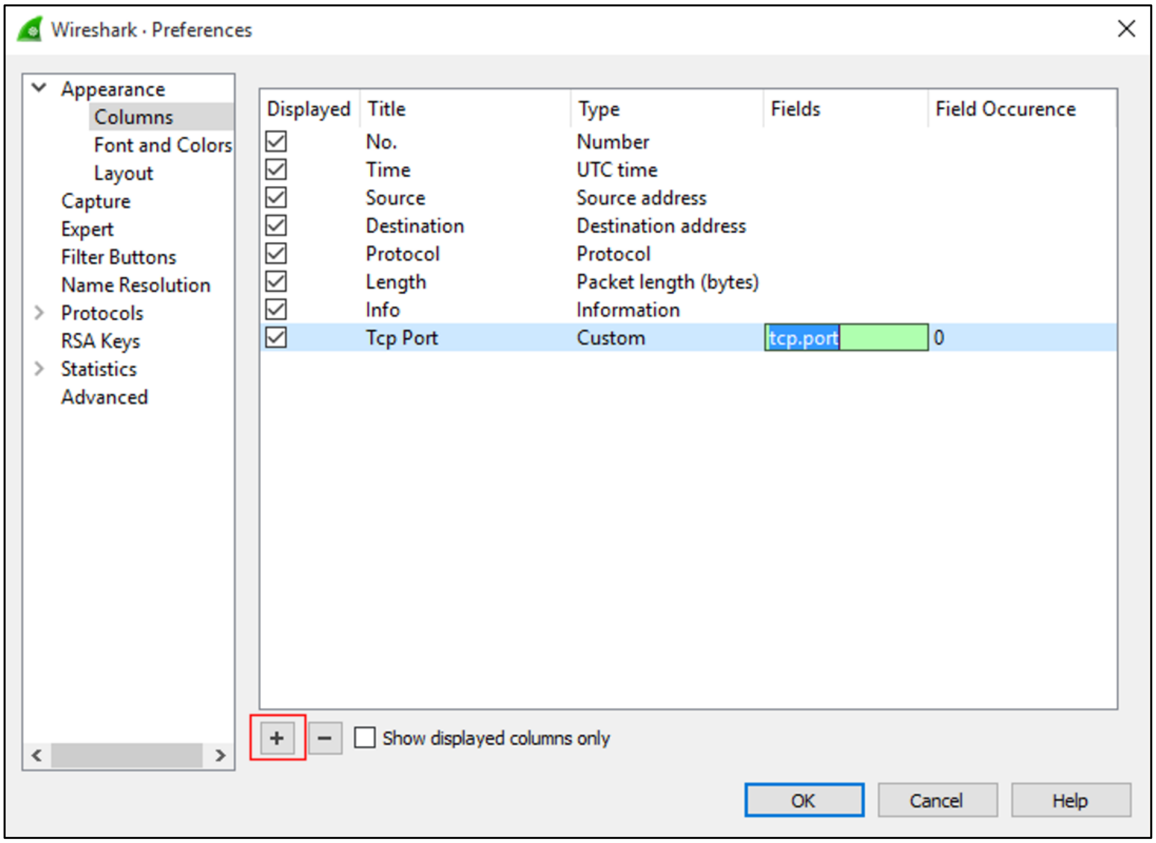
1 In your Windows 10 VM, start Wireshark and configure it to capture traffic. Then browse to *pdf995.com*.

2 Change the time type to UTC by going back to Wireshark, navigating to the **Edit** tab, and selecting ***Preferences***. In the **Preferences** window, go to **Appearance** > ***Columns*** and change the type of time in the ***Time*** column to UTC.



Displayed	Title	Type	Fields	Field Occurence
☑	No.	Number		
☑	Time	UTC time		
☑	Source			
☑	Destination			
☑	Protocol			
☑	Length			
☑	Info			

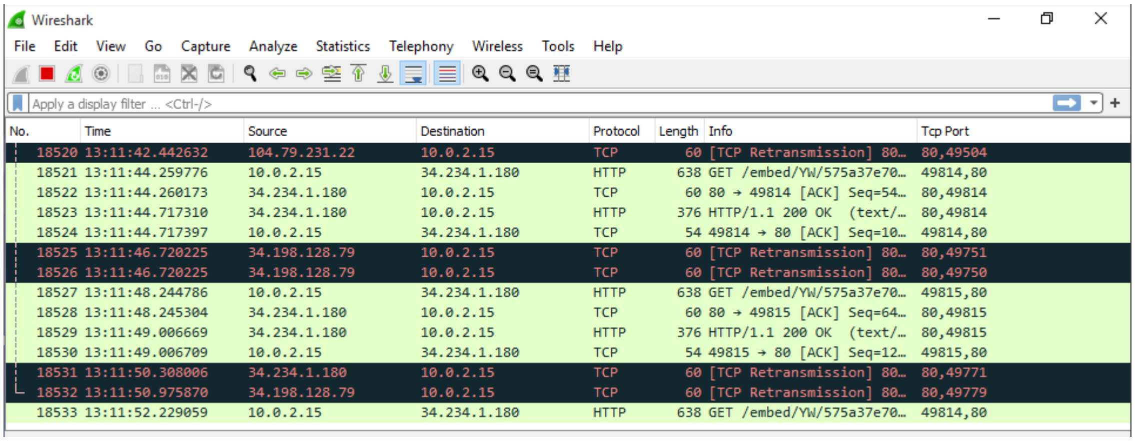
3 Add a new column with the name **TCP Port** by clicking the plus sign at the bottom of the window to add a new column. Then change its name to **Tcp Port**, its type to **Custom**, and enter ***tcp.port*** under **Fields**.
Note: The field shows the source and destination port details.



Displayed	Title	Type	Fields	Field Occurence
☑	No.	Number		
☑	Time	UTC time		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		
☑	Tcp Port	Custom	tcp.port	0

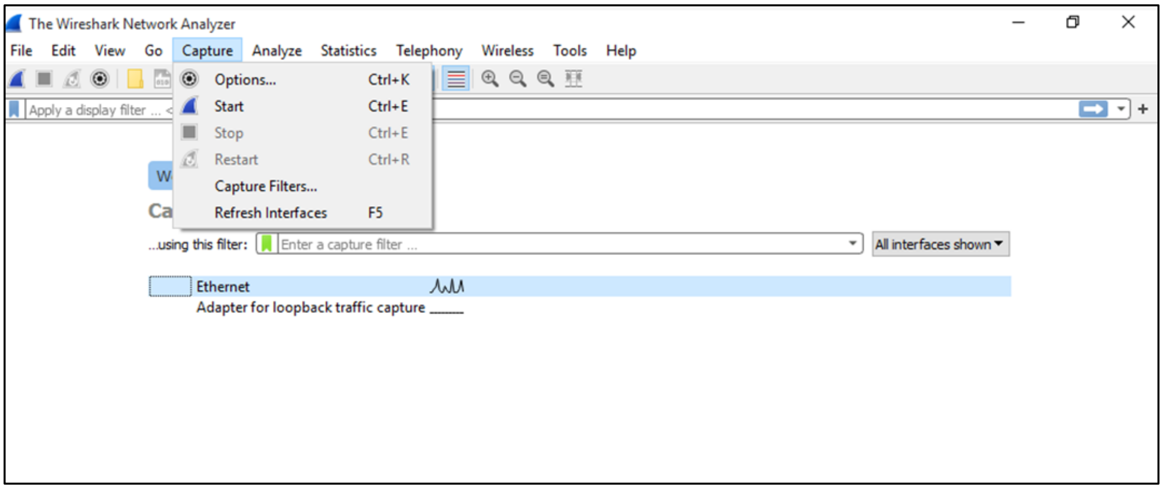
□ Show displayed columns only

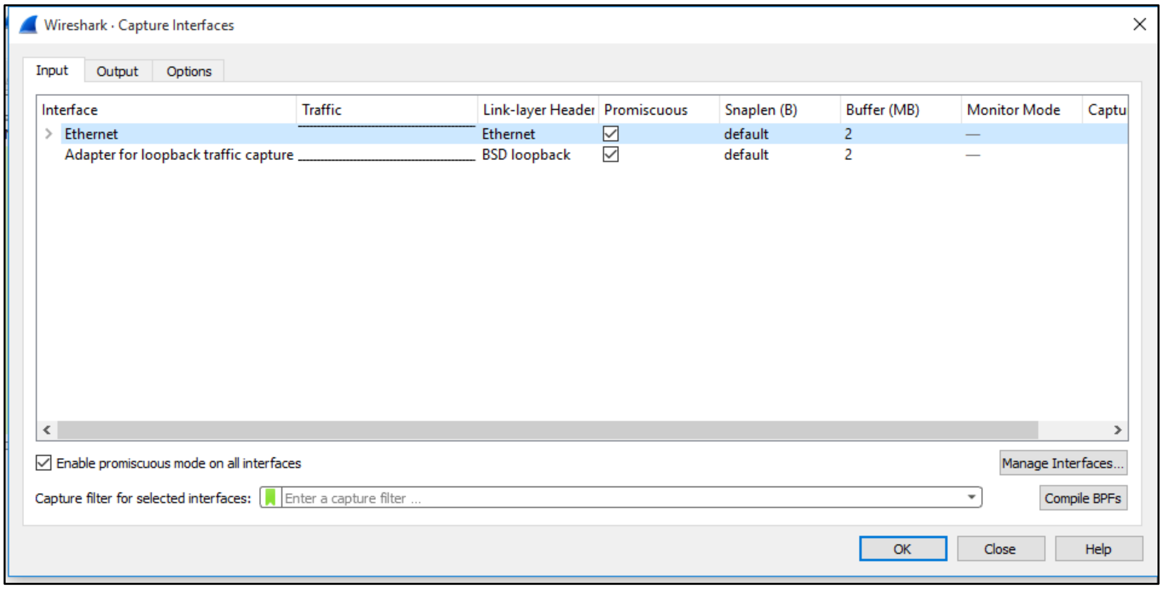
4 Click the new column to sort the traffic by **TCP Port**.
Note: The time changed on all packets.



No.	Time	Source	Destination	Protocol	Length	Info	Tcp Port
18520	13:11:42.442632	104.79.231.22	10.0.2.15	TCP	60	[TCP Retransmission] 80…	80,49504
18521	13:11:44.259776	10.0.2.15	34.234.1.180	HTTP	638	GET /embed/YW/575a37e70…	49814,80
18522	13:11:44.260173	34.234.1.180	10.0.2.15	TCP	60	80 → 49814 [ACK] Seq=54…	80,49814
18523	13:11:44.717310	34.234.1.180	10.0.2.15	HTTP	376	HTTP/1.1 200 OK (text/…	80,49814
18524	13:11:44.717397	10.0.2.15	34.234.1.180	TCP	54	49814 → 80 [ACK] Seq=10…	49814,80
18525	13:11:46.720225	34.198.128.79	10.0.2.15	TCP	60	[TCP Retransmission] 80…	80,49751
18526	13:11:46.720225	34.198.128.79	10.0.2.15	TCP	60	[TCP Retransmission] 80…	80,49750
18527	13:11:48.244786	10.0.2.15	34.234.1.180	HTTP	638	GET /embed/YW/575a37e70…	49815,80
18528	13:11:48.245304	34.234.1.180	10.0.2.15	TCP	60	80 → 49815 [ACK] Seq=64…	80,49815
18529	13:11:49.006669	34.234.1.180	10.0.2.15	HTTP	376	HTTP/1.1 200 OK (text/…	80,49815
18530	13:11:49.006709	10.0.2.15	34.234.1.180	TCP	54	49815 → 80 [ACK] Seq=12…	49815,80
18531	13:11:50.308006	34.234.1.180	10.0.2.15	TCP	60	[TCP Retransmission] 80…	80,49771
18532	13:11:50.975870	34.198.128.79	10.0.2.15	TCP	60	[TCP Retransmission] 80…	80,49779
18533	13:11:52.229059	10.0.2.15	34.234.1.180	HTTP	638	GET /embed/YW/575a37e70…	49814,80

5 Remove all capture filters and recapture packets without preconfigured filtering. Click the *red square* icon, navigate to the **Capture** menu at the top, and select ***Options…*** or press ***Ctrl+K***. Remove the capture filter and click **OK**.





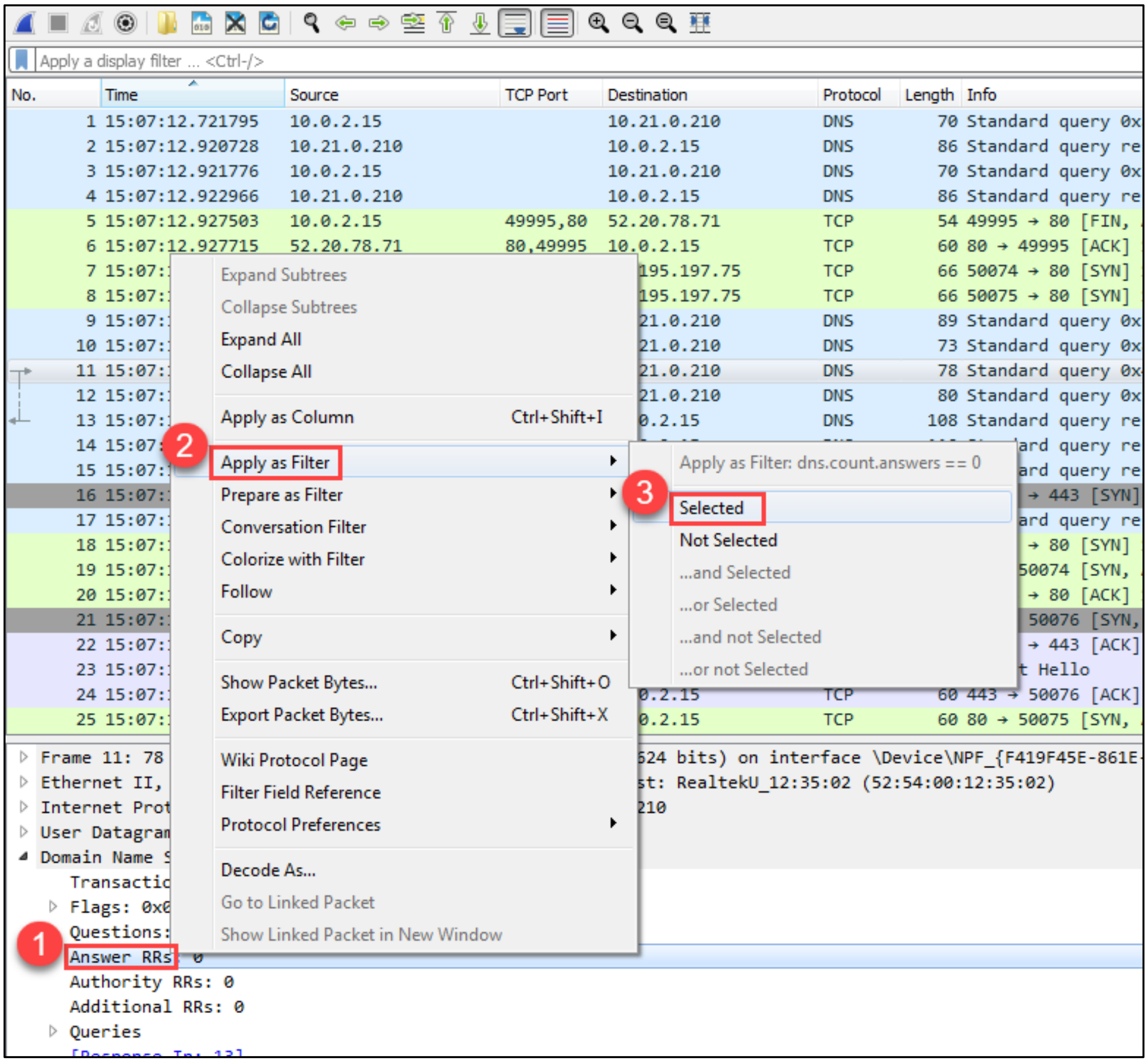
Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Captu
Ethernet		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

6 Start capturing again, go to the details of a DNS packet, right-click ***Answer RRs***, and apply them as a filter.

Note: To generate a DNS query answer, access a site you have not accessed before from this VM via the web browser.

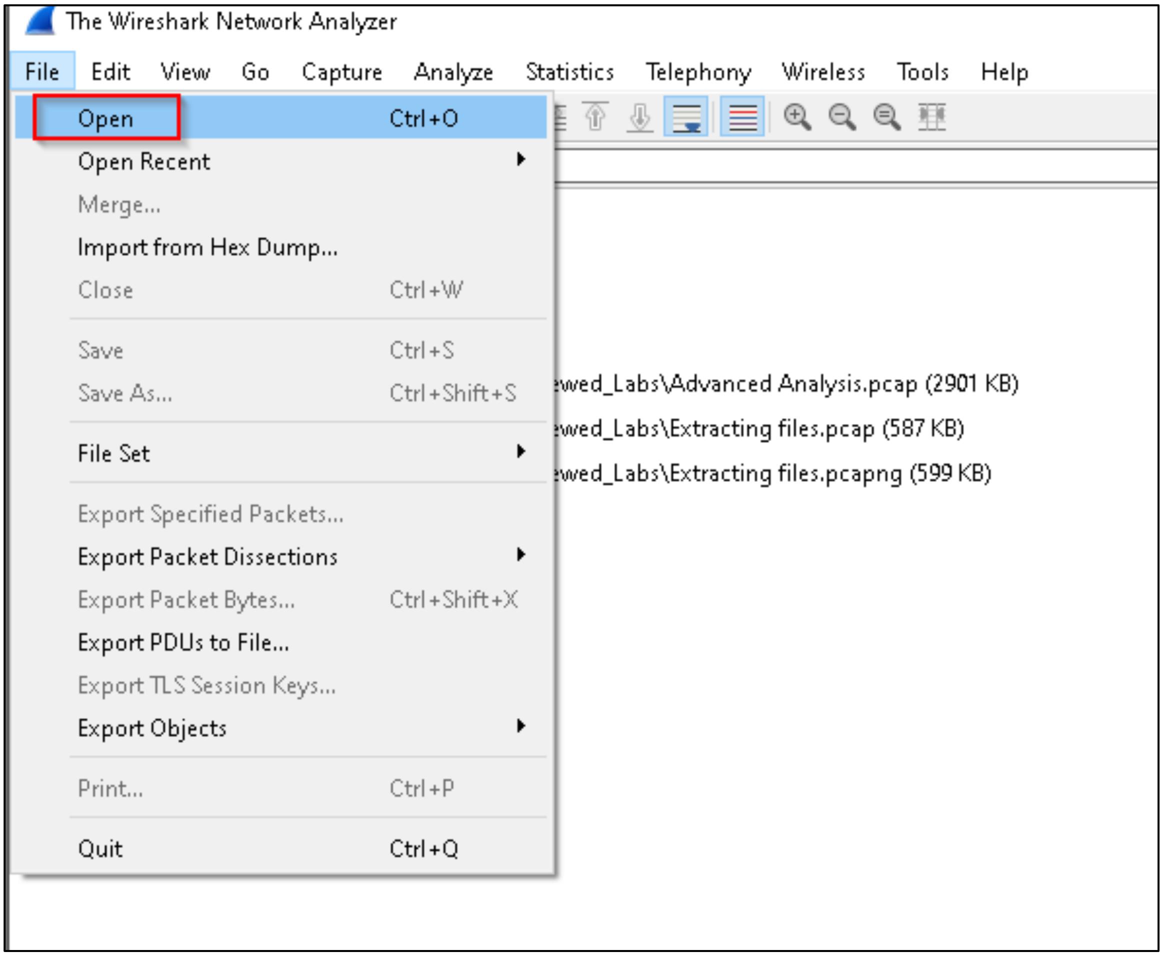


```
Apply a display filter ... <Ctrl-/>

No.  Time             Source        TCP Port   Destination    Protocol  Length  Info
  1 15:07:12.721795   10.0.2.15                10.21.0.210    DNS         70 Standard query 0x
  2 15:07:12.920728   10.21.0.210              10.0.2.15      DNS         86 Standard query re
  3 15:07:12.921776   10.0.2.15                10.21.0.210    DNS         70 Standard query 0x
  4 15:07:12.922966   10.21.0.210              10.0.2.15      DNS         86 Standard query re
  5 15:07:12.927503   10.0.2.15     49995,80   52.20.78.71    TCP         54 49995 → 80 [FIN,
  6 15:07:12.927715   52.20.78.71   80,49995   10.0.2.15      TCP         60 80 → 49995 [ACK]
  7 15:07:                                    195.197.75      TCP         66 50074 → 80 [SYN]
  8 15:07:                                    195.197.75      TCP         66 50075 → 80 [SYN]
  9 15:07:                                    21.0.210        DNS         89 Standard query 0x
 10 15:07:                                    21.0.210        DNS         73 Standard query 0x
 11 15:07:                                    21.0.210        DNS         78 Standard query 0x
 12 15:07:                                    21.0.210        DNS         80 Standard query 0x
 13 15:07:                                    0.2.15          DNS        108 Standard query re
 14 15:07:                                                                  ard query re
 15 15:07:                                                                  ard query re
 16 15:07:                                                                  → 443 [SYN]
 17 15:07:                                                                  ard query re
 18 15:07:                                                                  → 80 [SYN]
 19 15:07:                                                                 50074 [SYN,
 20 15:07:                                                                  → 80 [ACK]
 21 15:07:                                                                  50076 [SYN,
 22 15:07:                                                                  → 443 [ACK]
 23 15:07:                                                                 t Hello
 24 15:07:                                    0.2.15          TCP         60 443 → 50076 [ACK]
 25 15:07:                                    0.2.15          TCP         60 80 → 50075 [SYN,

▷ Frame 11: 78                                624 bits) on interface \Device\NPF_{F419F45E-861E-
▷ Ethernet II,                                st: RealtekU_12:35:02 (52:54:00:12:35:02)
▷ Internet Prot                               210
▷ User Datagram
◢ Domain Name S
    Transactic
  ▷ Flags: 0x0
    Questions:
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▷ Queries
    [Response In: 13]
```

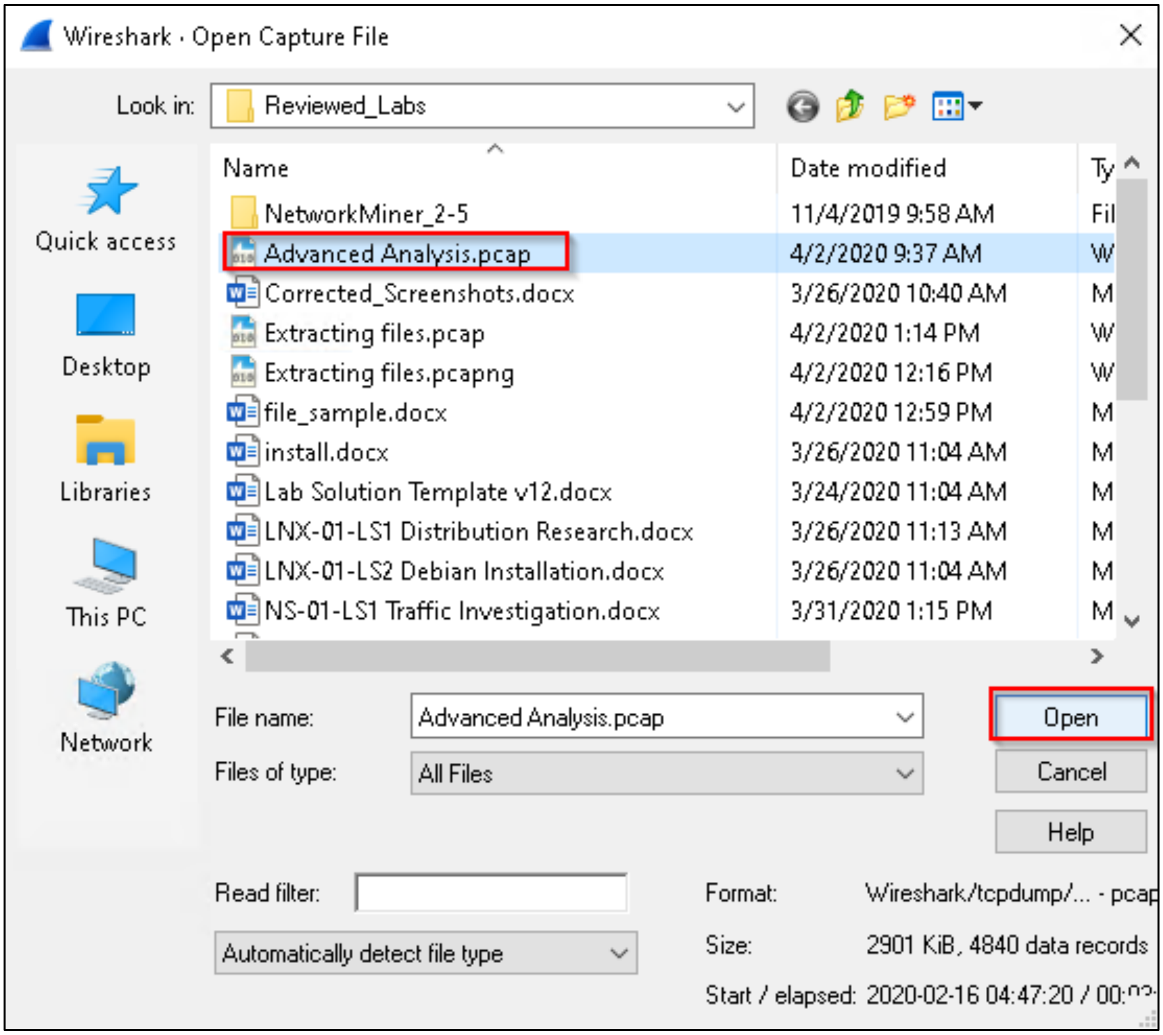
Lab Task 3: PCAP Analysis

This task will analyze the ***Advanced Analysis.pcap*** file using techniques you learned in this module.

1 Transfer the file ***Advanced Analysis.pcap*** to the Windows 10 VM by using the drag-and-drop feature of VB Guest Additions, which can be viewed in the Windows 10 Installation Guide. Open the ***Advanced Analysis.pcap*** file with Wireshark.
Note: Open the file using the drop-down menu.



wed_Labs\Advanced Analysis.pcap (2901 KB)
wed_Labs\Extracting files.pcap (587 KB)
wed_Labs\Extracting files.pcapng (599 KB)



Look in: Reviewed_Labs

Name	Date modified	Ty
NetworkMiner_2-5	11/4/2019 9:58 AM	Fil
Advanced Analysis.pcap	4/2/2020 9:37 AM	W
Corrected_Screenshots.docx	3/26/2020 10:40 AM	M
Extracting files.pcap	4/2/2020 1:14 PM	W
Extracting files.pcapng	4/2/2020 12:16 PM	W
file_sample.docx	4/2/2020 12:59 PM	M
install.docx	3/26/2020 11:04 AM	M
Lab Solution Template v12.docx	3/24/2020 11:04 AM	M
LNX-01-LS1 Distribution Research.docx	3/26/2020 11:13 AM	M
LNX-01-LS2 Debian Installation.docx	3/26/2020 11:04 AM	M
NS-01-LS1 Traffic Investigation.docx	3/31/2020 1:15 PM	M

File name: Advanced Analysis.pcap

Files of type: All Files

Read filter:

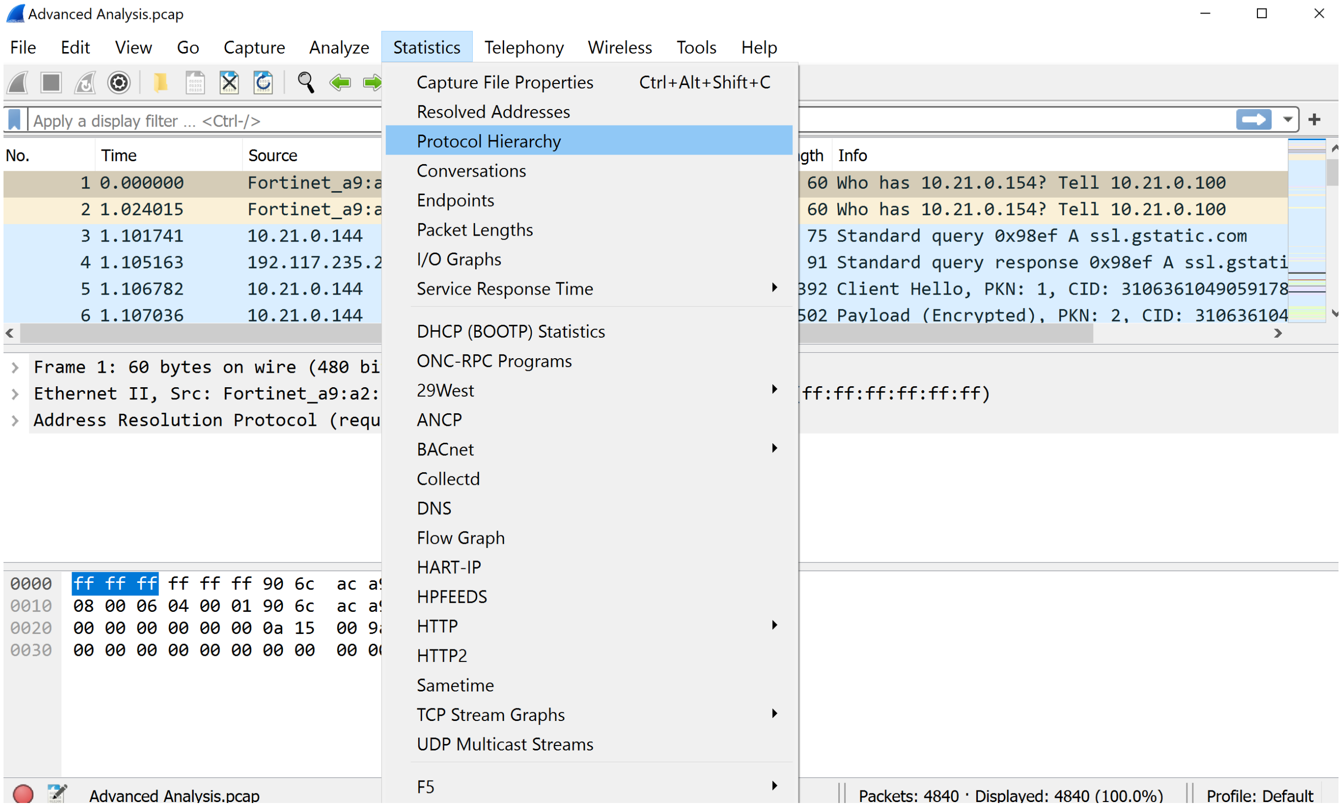
Automatically detect file type

Format: Wireshark/tcpdump/... - pcap

Size: 2901 KiB, 4840 data records

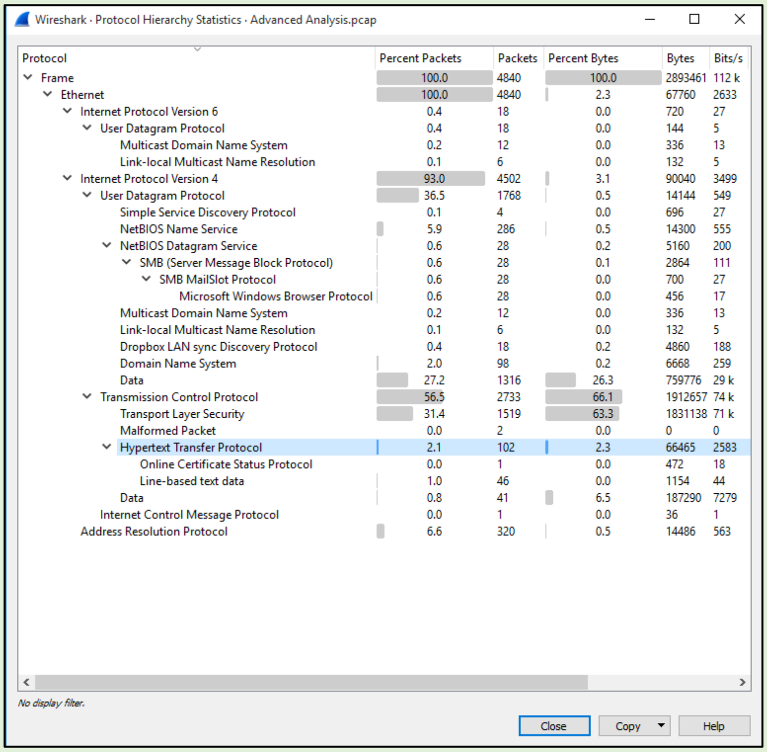
Start / elapsed: 2020-02-16 04:47:20 / 00:0

2 What is the percentage of HTTP traffic in the captured file? Examine the statistics to understand the results. In the menu bar at the top, go to **Statistics** > ***Protocol Hierarchy***.



```
No.   Time        Source              ngth  Info
    1 0.000000    Fortinet_a9:a        60 Who has 10.21.0.154? Tell 10.21.0.100
    2 1.024015    Fortinet_a9:a        60 Who has 10.21.0.154? Tell 10.21.0.100
    3 1.101741    10.21.0.144          75 Standard query 0x98ef A ssl.gstatic.com
    4 1.105163    192.117.235.2        91 Standard query response 0x98ef A ssl.gstati
    5 1.106782    10.21.0.144         392 Client Hello, PKN: 1, CID: 3106361049059178
    6 1.107036    10.21.0.144         502 Payload (Encrypted), PKN: 2, CID: 310636104

> Frame 1: 60 bytes on wire (480 bi
> Ethernet II, Src: Fortinet_a9:a2:                    ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (requ

0000  ff ff ff ff ff ff 90 6c  ac a
0010  08 00 06 04 00 01 90 6c  ac a
0020  00 00 00 00 00 00 0a 15  00 9
0030  00 00 00 00 00 00 00 00  00 0

Advanced Analysis.pcap          Packets: 4840 · Displayed: 4840 (100.0%)    Profile: Default
```

You should see that the percentage is 2.1%.



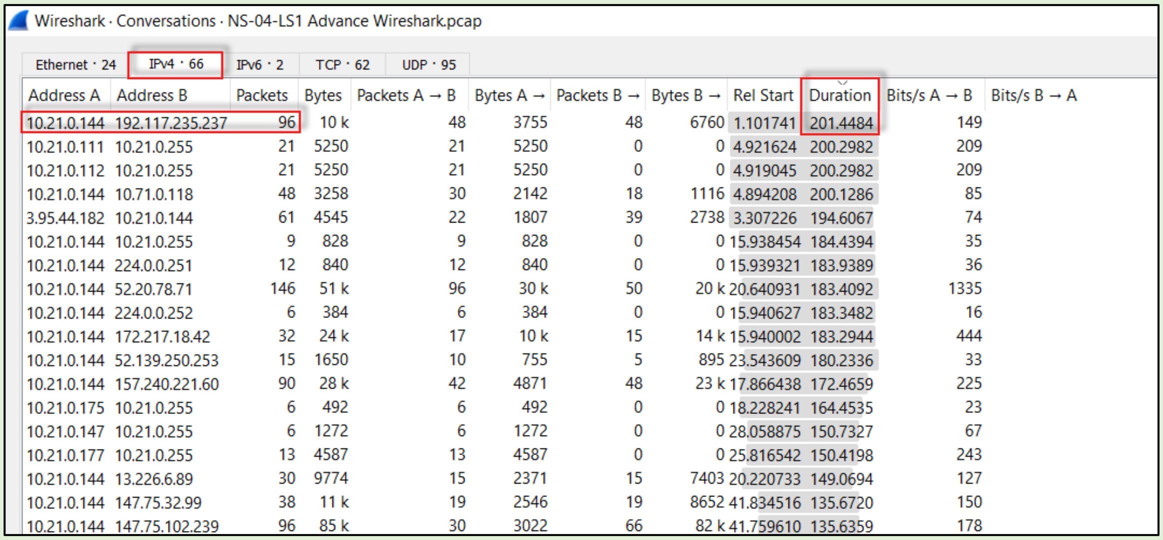
Wireshark · Protocol Hierarchy Statistics · Advanced Analysis.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	4840	100.0	2893461	112 k
Ethernet	100.0	4840	2.3	67760	2633
Internet Protocol Version 6	0.4	18	0.0	720	27
User Datagram Protocol	0.4	18	0.0	144	5
Multicast Domain Name System	0.2	12	0.0	336	13
Link-local Multicast Name Resolution	0.1	6	0.0	132	5
Internet Protocol Version 4	93.0	4502	3.1	90040	3499
User Datagram Protocol	36.5	1768	0.5	14144	549
Simple Service Discovery Protocol	0.1	4	0.0	696	27
NetBIOS Name Service	5.9	286	0.5	14300	555
NetBIOS Datagram Service	0.6	28	0.2	5160	200
SMB (Server Message Block Protocol)	0.6	28	0.1	2864	111
SMB MailSlot Protocol	0.6	28	0.0	700	27
Microsoft Windows Browser Protocol	0.6	28	0.0	456	17
Multicast Domain Name System	0.2	12	0.0	336	13
Link-local Multicast Name Resolution	0.1	6	0.0	132	5
Dropbox LAN sync Discovery Protocol	0.4	18	0.2	4860	188
Domain Name System	2.0	98	0.2	6668	259
Data	27.2	1316	26.3	759776	29 k
Transmission Control Protocol	56.5	2733	66.1	1912657	74 k
Transport Layer Security	31.4	1519	63.3	1831138	71 k
Malformed Packet	0.0	2	0.0	0	0
Hypertext Transfer Protocol	2.1	102	2.3	66465	2583
Online Certificate Status Protocol	0.0	1	0.0	472	18
Line-based text data	1.0	46	0.0	1154	44
Data	0.8	41	6.5	187290	7279
Internet Control Message Protocol	0.0	1	0.0	36	1
Address Resolution Protocol	6.6	320	0.5	14486	563

No display filter.

3 Determine which two IPv4s had the longest IP conversation and the number of packets sent in that conversation. Go to **Statistics** > ***Conversations***.

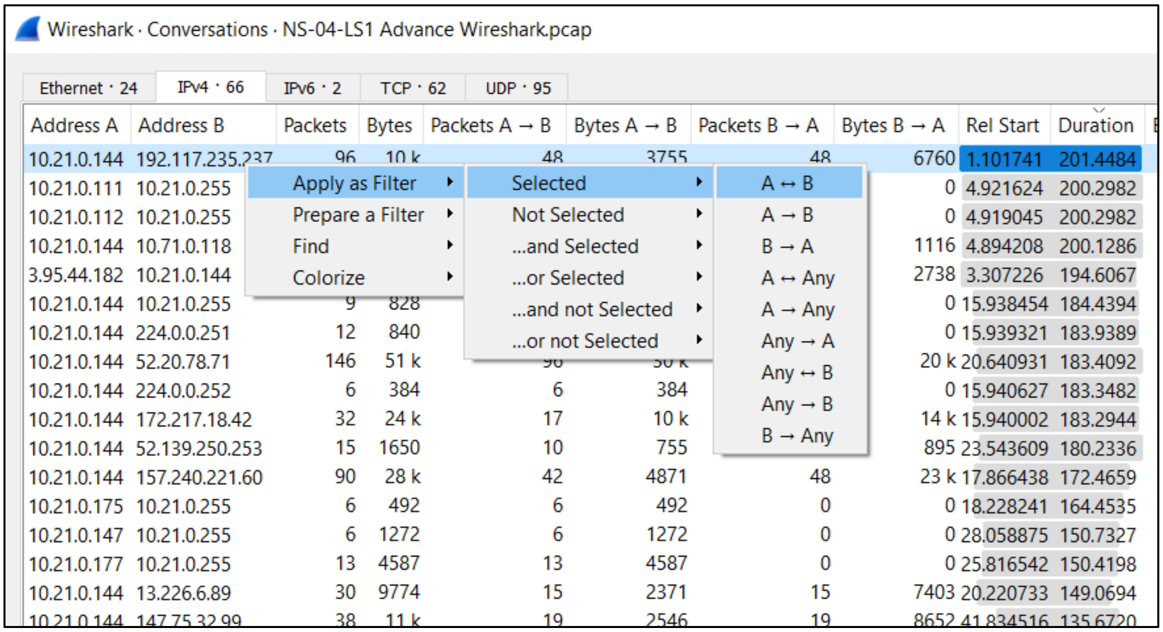
The two IPs are ***192.117.235.237*** and ***10.21.0.144***, and 96 packets were sent.



Wireshark · Conversations · NS-04-LS1 Advance Wireshark.pcap

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A →	Packets B →	Bytes B →	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.21.0.144	192.117.235.237	96	10 k	48	3755	48	6760	1.101741	201.4484	149	
10.21.0.111	10.21.0.255	21	5250	21	5250	0	0	4.921624	200.2982	209	
10.21.0.112	10.21.0.255	21	5250	21	5250	0	0	4.919045	200.2982	209	
10.21.0.144	10.71.0.118	48	3258	30	2142	18	1116	4.894208	200.1286	85	
3.95.44.182	10.21.0.144	61	4545	22	1807	39	2738	3.307226	194.6067	74	
10.21.0.144	10.21.0.255	9	828	9	828	0	0	15.938454	184.4394	35	
10.21.0.144	224.0.0.251	12	840	12	840	0	0	15.939321	183.9389	36	
10.21.0.144	52.20.78.71	146	51 k	96	30 k	50	20 k	20.640931	183.4092	1335	
10.21.0.144	224.0.0.252	6	384	6	384	0	0	15.940627	183.3482	16	
10.21.0.144	172.217.18.42	32	24 k	17	10 k	15	14 k	15.940002	183.2944	444	
10.21.0.144	52.139.250.253	15	1650	10	755	5	895	23.543609	180.2336	33	
10.21.0.144	157.240.221.60	90	28 k	42	4871	48	23 k	17.866438	172.4659	225	
10.21.0.175	10.21.0.255	6	492	6	492	0	0	18.228241	164.4535	23	
10.21.0.147	10.21.0.255	6	1272	6	1272	0	0	28.058875	150.7327	67	
10.21.0.177	10.21.0.255	13	4587	13	4587	0	0	25.816542	150.4198	243	
10.21.0.144	13.226.6.89	30	9774	15	2371	15	7403	20.220733	149.0694	127	
10.21.0.144	147.75.32.99	38	11 k	19	2546	19	8652	41.834516	135.6720	150	
10.21.0.144	147.75.102.239	96	85 k	30	3022	66	82 k	41.759610	135.6359	178	

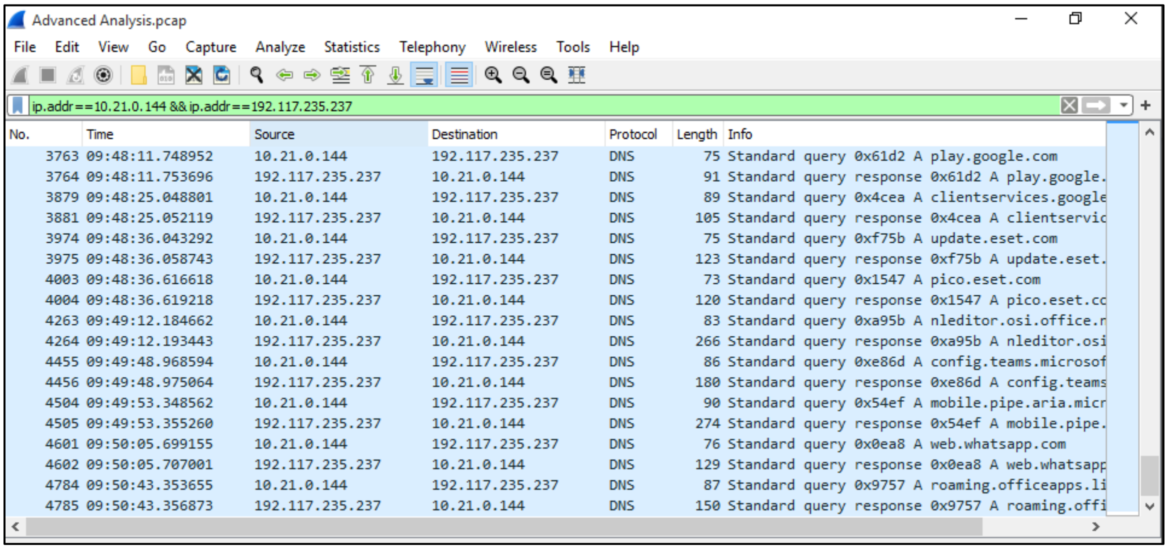
4 Regarding the previous question, which protocol was used between the two IPs? Right-click the top row where the two IPs are ***10.21.0.144*** and ***192.117.235.247*** and apply an ***A<->B*** bidirectional filter.



Wireshark · Conversations · NS-04-LS1 Advance Wireshark.pcap

Ethernet · 24 | IPv4 · 66 | IPv6 · 2 | TCP · 62 | UDP · 95

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
10.21.0.144	192.117.235.237	96	10 k	48	3755	48	6760	1.101741	201.4484
10.21.0.111	10.21.0.255						0	4.921624	200.2982
10.21.0.112	10.21.0.255						0	4.919045	200.2982
10.21.0.144	10.71.0.118						1116	4.894208	200.1286
3.95.44.182	10.21.0.144						2738	3.307226	194.6067
10.21.0.144	10.21.0.255	9	828				0	15.938454	184.4394
10.21.0.144	224.0.0.251	12	840				0	15.939321	183.9389
10.21.0.144	52.20.78.71	146	51 k	96	30 k		20 k	20.640931	183.4092
10.21.0.144	224.0.0.252	6	384	6	384		0	15.940627	183.3482
10.21.0.144	172.217.18.42	32	24 k	17	10 k		14 k	15.940002	183.2944
10.21.0.144	52.139.250.253	15	1650	10	755		895	23.543609	180.2336
10.21.0.144	157.240.221.60	90	28 k	42	4871	48	23 k	17.866438	172.4659
10.21.0.175	10.21.0.255	6	492	6	492	0	0	18.228241	164.4535
10.21.0.147	10.21.0.255	6	1272	6	1272	0	0	28.058875	150.7327
10.21.0.177	10.21.0.255	13	4587	13	4587	0	0	25.816542	150.4198
10.21.0.144	13.226.6.89	30	9774	15	2371	15	7403	20.220733	149.0694
10.21.0.144	147.75.32.99	38	11 k	19	2546	19	8652	41.834516	135.6720



Advanced Analysis.pcap

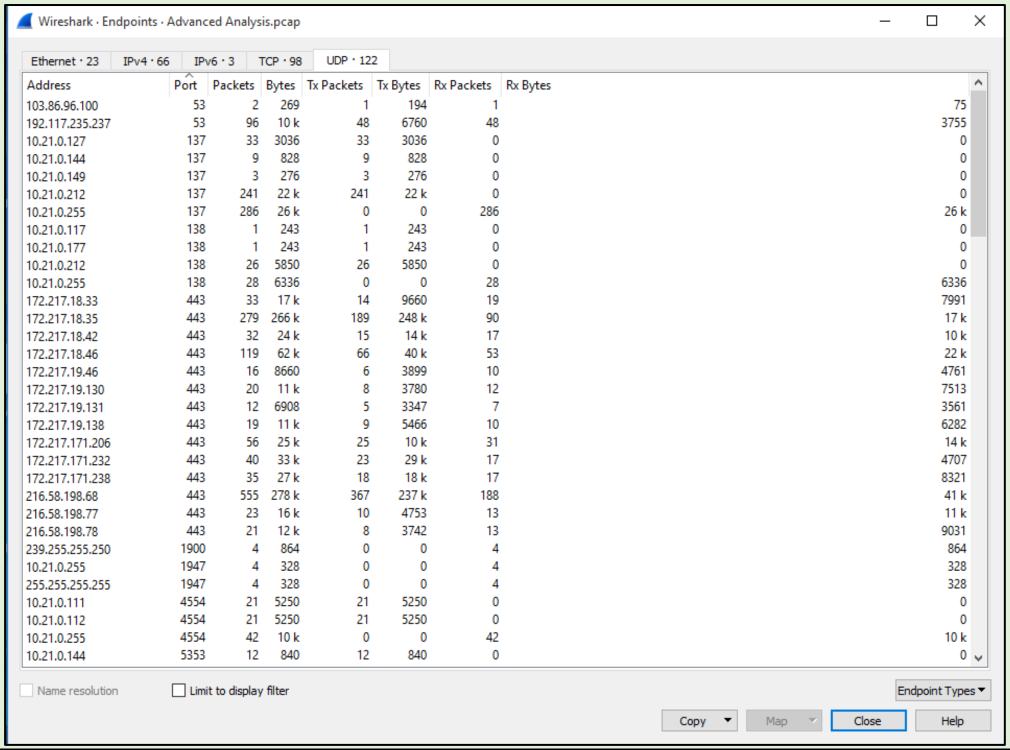
ip.addr==10.21.0.144 && ip.addr==192.117.235.237

No.	Time	Source	Destination	Protocol	Length	Info
3763	09:48:11.748952	10.21.0.144	192.117.235.237	DNS	75	Standard query 0x61d2 A play.google.com
3764	09:48:11.753696	192.117.235.237	10.21.0.144	DNS	91	Standard query response 0x61d2 A play.google.
3879	09:48:25.048801	10.21.0.144	192.117.235.237	DNS	89	Standard query 0x4cea A clientservices.google
3881	09:48:25.052119	192.117.235.237	10.21.0.144	DNS	105	Standard query response 0x4cea A clientservic
3974	09:48:36.043292	10.21.0.144	192.117.235.237	DNS	75	Standard query 0xf75b A update.eset.com
3975	09:48:36.058743	192.117.235.237	10.21.0.144	DNS	123	Standard query response 0xf75b A update.eset.
4003	09:48:36.616618	10.21.0.144	192.117.235.237	DNS	73	Standard query 0x1547 A pico.eset.com
4004	09:48:36.619218	192.117.235.237	10.21.0.144	DNS	120	Standard query response 0x1547 A pico.eset.co
4263	09:49:12.184662	10.21.0.144	192.117.235.237	DNS	83	Standard query 0xa95b A nleditor.osi.office.r
4264	09:49:12.193443	192.117.235.237	10.21.0.144	DNS	266	Standard query response 0xa95b A nleditor.osi
4455	09:49:48.968594	10.21.0.144	192.117.235.237	DNS	86	Standard query 0xe86d A config.teams.microsof
4456	09:49:48.975064	192.117.235.237	10.21.0.144	DNS	180	Standard query response 0xe86d A config.teams
4504	09:49:53.348562	10.21.0.144	192.117.235.237	DNS	90	Standard query 0x54ef A mobile.pipe.aria.micr
4505	09:49:53.355260	192.117.235.237	10.21.0.144	DNS	274	Standard query response 0x54ef A mobile.pipe.
4601	09:50:05.699155	10.21.0.144	192.117.235.237	DNS	76	Standard query 0x0ea8 A web.whatsapp.com
4602	09:50:05.707001	192.117.235.237	10.21.0.144	DNS	129	Standard query response 0x0ea8 A web.whatsapp
4784	09:50:43.353655	10.21.0.144	192.117.235.237	DNS	87	Standard query 0x9757 A roaming.officeapps.li
4785	09:50:43.356873	192.117.235.237	10.21.0.144	DNS	150	Standard query response 0x9757 A roaming.offi

The protocol was DNS.

5 Using endpoint statistics, determine which IPs use the DNS protocol on UDP. Go to **Statistics** > ***Endpoints*** and see which IPs used port 53 (DNS) UDP.

Answer: ***103.86.96.100*** and ***192.117.235.237*** used port 53.



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
103.86.96.100	53	2	269	1	194	1	75
192.117.235.237	53	96	10 k	48	6760	48	3755
10.21.0.127	137	33	3036	33	3036	0	0
10.21.0.144	137	9	828	9	828	0	0
10.21.0.149	137	3	276	3	276	0	0
10.21.0.212	137	241	22 k	241	22 k	0	0
10.21.0.255	137	286	26 k	0	0	286	26 k
10.21.0.117	138	1	243	1	243	0	0
10.21.0.177	138	1	243	1	243	0	0
10.21.0.212	138	26	5850	26	5850	0	0
10.21.0.255	138	28	6336	0	0	28	6336
172.217.18.33	443	33	17 k	14	9660	19	7991
172.217.18.35	443	279	266 k	189	248 k	90	17 k
172.217.18.42	443	32	24 k	15	14 k	17	10 k
172.217.18.46	443	119	62 k	66	40 k	53	22 k
172.217.19.46	443	16	8660	6	3899	10	4761
172.217.19.130	443	20	11 k	8	3780	12	7513
172.217.19.131	443	12	6908	5	3347	7	3561
172.217.19.138	443	19	11 k	9	5466	10	6282
172.217.171.206	443	56	25 k	25	10 k	31	14 k
172.217.171.232	443	40	33 k	23	29 k	17	4707
172.217.171.238	443	35	27 k	18	18 k	17	8321
216.58.198.68	443	555	278 k	367	237 k	188	41 k
216.58.198.77	443	23	16 k	10	4753	13	11 k
216.58.198.78	443	21	12 k	8	3742	13	9031
239.255.255.250	1900	4	864	0	0	4	864
10.21.0.255	1947	4	328	0	0	4	328
255.255.255.255	1947	4	328	0	0	4	328
10.21.0.111	4554	21	5250	21	5250	0	0
10.21.0.112	4554	21	5250	21	5250	0	0
10.21.0.255	4554	42	10 k	0	0	42	10 k
10.21.0.144	5353	12	840	12	840	0	0