## CSCI 5010 – Fundamentals of Data Communications

Lab 6 Wireshark

University of Colorado Boulder Department of Computer Science Network Engineering

Professor Levi Perigo, Ph.D.

Lab 6: Wireshark

## Objectives

- Learn the basic operations of Wireshark
- Learn how to capture and analyze ICMP traffic
- Demonstrate best practices for analyzer placement
- Differentiate Wireshark captures between switches and routers
- Display which NICs on analyzer are capturing traffic
- Display IPv4 and/or IPv6 addresses on NICs
- Learn how to perform continuous captures for HTTP requests
- Explain and display different ways to demonstrate top talkers on the network
- Learn how to create coloring rules in Wireshark
- Learn how to create graphs for visual representation
- Learn how to capture and analyze application specific traffic DHCP, HTTP

#### **Summary**

One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" – observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences. This can be done in simulated scenarios or in a "real" network environment such as the Internet. In the Wireshark lab you'll be doing in this course, you'll be running various network applications in different scenarios using your own computer or in a virtual machine environment. You'll observe the network protocols "in action," interacting and exchanging messages with protocol entities executing elsewhere in the Internet. Thus, you and your computer will be an integral part of these "live" labs. You'll observe, and you'll learn, by doing.

In this Wireshark lab, you'll get acquainted with Wireshark, and make some simple packet captures and observations.

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine. The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer.

The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string "GET," "POST," or "HEAD."

We will be using the Wireshark packet sniffer [http://www.wireshark.org/] for this lab, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer). Wireshark is a free network protocol analyzer that runs on Windows, Linux/Unix, and Mac computers.

## Prefer using VM1 - UBUNTU – 22.04 Part 1 Objective 1.1 - Downloading Wireshark and Navigation Overview

1. Download and install Wireshark:

For Ubuntu 22.04 refer - <u>How to Install and Configure Wireshark on Ubuntu 22.04</u> (linuxhint.com)

For Windows and MAC:

- Go to <u>http://www.wireshark.org/download.html</u>, download and install Wireshark.
- The Wireshark FAQ has many helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.
- Helpful install video: <a href="https://www.youtube.com/watch?v=flDzURAm8wQ">https://www.youtube.com/watch?v=flDzURAm8wQ</a>
- 2. Wireshark Navigation

Helpful navigation video: https://www.youtube.com/watch?v=PYrCS21sPbA

Note: after installing you might need to reboot once.

## **Objective 1.2 - Running Wireshark**

When you run the Wireshark program, you'll get a startup screen, as shown below (note: this screenshot may be an older version of Wireshark):



Figure 1: Initial Wireshark Screen

Take a look at the upper left-hand side of the screen – you'll see an "Interface list". This is the list of network interfaces on your computer. Once you choose an interface, Wireshark will capture all packets on that interface. In the example above, there is an Ethernet interface (Gigabit network connection) and a wireless interface ("Wi-Fi").

If you click on one of these interfaces to start packet capture (i.e., for Wireshark to begin capturing all packets being sent to/from that interface), a screen like the one below will be displayed, showing information about the packets being captured. Once you start packet capture, you can stop it by using the Capture pull down menu and selecting Stop.



hexadecima and ASCII

Figure 2: Wireshark Graphical User Interface, during packet capture and analysis

The Wireshark interface has five major components:

• The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu

allows you to save captured packet data or open a file containing previously captured packet data and exit the Wireshark application. The Capture menu allows you to begin packet capture.

- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.
- The packet-header details window provides details about the packet selected (highlighted) in the packet-listing window. (To select a packet in the packet-listing window, place the cursor over the packet's one-line summary in the packet-listing window and click with the left mouse button.). These details include information about the Ethernet frame (assuming the packet was sent/received over an Ethernet interface) and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the plus minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.
- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
- Towards the top of the Wireshark graphical user interface, is the **packet display filter field**, into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

#### Part 2

#### Objective 2.1 – ICMP

- 1. Open command prompt/terminal (depending on the operating system)
- 2. Start Wireshark and begin capture
- Ping any "hostname" (where the "hostname" is a URL, example: ping www.google.com)
- 4. When the Ping finishes, stop the capture. [Press Ctrl + C in MAC to stop the ping]
- 5. Filter the capture to only display DNS traffic
  - Provide a screenshot of the DNS reply from the server that shows the IP address of the URL. [5 points]

	<b>1</b> *W	i-Fi																													_	0	×
1	File	Edit	View	Go	Capture	Analy	70 S	tatistics	Tele	phony	/ Wire	less	Tools	Help																		_	
	4			- 1		0 🛥	-						TT D																				
							-7 1		×	-		~ ~	315 D	D															_			1972	
L	dn	s					_						_																				* +
1	lo.	dns	con/or		Sou	rce			Desti	nation	۱		Proto	ocol I	Lengt	Info																	
-	+	uns	server	93	2601	1:280:5	f00:1	af0:	2001	:558:	feed::	1	DNS		94	Stand	lard o	query	0x6b1	d A w	ww.go	oogle.	com										
		3	0.814	667	2601	1:280:5	f00:1	af0:	2001	:558:	feed::	2	DNS		94	Stand	lard o	query	0x6b1	d A w	www.go	ogle.	com										
*	_	4	0.825	147	2001	1:558:f	eed::	1	2601	:280:	5f00:1	.af0:	. DNS		110	Stand	lard o	query	respo	nse e	0x6b1d	1 A w	w.goo	gle.co	om A :	142.2	50.72.	68					
		6	0.837	992	2001	1:558:6	eed::	2	2601	:280:	5f00:1	.af0:	DNS		110	Stand	lard o	query	respo	nse e	0x6b10	1 A w	w.goo	gle.co	om A:	142.2	50.72.	4					
		22	0.838	720	260	1:280:5	F00:1	at0:	2001	:558:	feed::	2	ICMP	76	158	Desti	natio	on Unr	reacha	DIE (	(Port	unrea	icnabl	e)				<u> </u>					
		34	7 552	152	260	1 - 280 - 5	F00:1	af0:	2001	.558.	feed	1	DNS		90	Stand	land d	query	0x204		wtalk	aik.go	le com	com									
		35	7 561	864	2601	1 • 280 • 5	f00.1	af0	2001	.558.	food	1	DNS		104	Stand	land o	query	6v304	6 4 4	wood k	acd1		cast r	net								
		36	7.562	192	2601	1:280:5	f00:1	af0:	2001	:558:	feed::	1	DNS		104	Stand	land o	query	0xda3		AA wna	ad.hsc	11.00.	comcas	st.ne	t t							
		37	7.573	902	2001	1:558:f	eed::	1	2601	:280:	5f00:1	- af0:	DNS		153	Stand	lard d	auerv	respo	nse e	0xe841		mtal	k.goog	zle.c	om CN/	AME mo	bile-r	talk.	l.goog]	le.com	AAAA 26	07:f8b
		38	7.580	662	2001	1:558:f	eed::	1	2601	:280:	5f00:1	af0:	DNS		141	Stand	lard o	query	respo	nse e	9x313d	d A mt	alk.g	oogle.	com	CNAME	mobil	e-gtal	k.1.g	pogle.c	om A 2	09.85.1	45.188
		40	7.764	548	2001	1:558:f	eed::	1	2601	:280:	5f00:1	af0:	DNS		156	Stand	lard d	query	respo	nse Ø	0x3946	5 No s	uch n	ame A	wpad	.hsd1	.co.co	mcast.	net S	DA dns1	LØ1.com	<pre>ncast.ne</pre>	t
		41	7.764	924	2001	1:558:f	eed::	1	2601	:280:	5f00:1	af0:	DNS		156	Stand	lard o	query	respo	nse e	0xda3e	NO s	uch n	ame AA	AAA w	pad.h:	sd1.co	.comca	ist.net	t SOA d	ins101.	comcast	.net
Ē	Fr	ame	2: 94	bytes	on wir	0000	c4 5	50 9c	6d 1d	18f (	cc d9	ac d	5 3d 4	<b>1 86</b>	dd 6	0 00	٠P٠	m	· · =A														
	Et	herr	net II,	Src:	Intel	0010	00 0	90 00	28 11	40 2	26 01	02 8	9 5f 6	90 la	f0 4	d 84		(.@&.	1.0	M -													
	> In	terr	net Pro	otocol	Versio	0020	bd e	2 3c	14 47	ef 2	20 01	05 5	B fe e	ed 00	00 0	0 00		G- · ·	-X	114.													
	> Us	er D	Datagra	am Prot	ocol,	0040	01 6	00 00	01 00	000 0	00 00	00 0	0 03 7	77 77	77 0	6 67				WW-R													
	Do	mair	n Name	System	ı (quer	0050	6f (	5f 67	6c 65	03 6	63 6f	6d Ø	00 0	91 00	01		oog	le·co	m · · · ·														
	0	7	Domain	Name S	vstem: P	rotocol																	P	ackets: 7	72 · Di	splayed	1: 13 (18	.1%) · D	ropped:	0 (0.0%)		Profil	e: Default
									_				•		_			-	_	_	-5								- P P C C			7.05.0	
	-	0.							Q	ь.	- 🍫	- 4	Y		0	-		48	5	C	Ç	w		Ð		2		^		() ()	<b>D</b>	7:05 P 15/10/202	24 <b>a</b>

I had pinged <u>www.google.com</u> it shows a DNS reply from the server that shows the ip address 142.250.72.68.

Explain why DNS would be in this capture when you pinged? [5 points]
 When I pinged the domain name the system resolves the domain into an IP address using DNS (Domain Name System). The DNS lookup converts the

URL into its corresponding IP address before the actual ping packets can be sent to the server.

- 6. Filter the capture to only display the Ping traffic
  - a. Were the Pings successful?

Yes, the ping was successful.

b. Provide the filtered Wireshark screenshot, and explain how you know they

were/were not successful? [10 points]

	(*Wi	Fi																											-	٥	×
F	ile	Edit V	liew Go	Captur	e Analy	ze Sta	atistics	Telep	ohony	Wire	eless	Tool	s He	elp																	
		20		XC	୍ ୧ 🔶	•	1 🕈 .	Ł 🛄		•	୍ତ	11	122																	-	
L	icm	р																												$\times \rightarrow$	· +
Ν	lo.	icmp		Sou	irce			Destir	nation	1		Pr	otoco	l Len	gtł Inf	o															
-	Þ	icmpve	907	10.	0.0.25			142.2	50.7	2.68		IC	MP		74 Ec	ho (p	ing)	reques	t id:	=0×0001,	, seq	=13/3328	, ttl=12	8 (rep	ly in	8)					
4-	-	8 0.	848689	142	.250.72	2.68		10.0.	0.25	2 60		IC	MP мр		74 Ec	ho (p	ing)	reply	id: + id:	=0x0001,	, seq	=13/3328	, ttl=11	5 (req	uest i	in 5)					
		10 1.	859163	10.	0.0.25	.68		19.0.	0.25	2.00		TC	MP		74 EC 74 EC	ho (p	ing)	reply	id:	=0x0001, =0x0001.	seq:	1=14/3584 1=14/3584	, ttl=12 . ttl=11	5 (rep	uest i	in 10)	)				
		13 2.	861675	10.	0.0.25			142.2	50.7	2.68		IC	MP		74 Ec	ho (p	ing)	reques	t id:	=0×0001,	seq	=15/3840	ttl=12	8 (rep	ly in	14)					
		14 2.	903700	142	.250.72	2.68		10.0.	0.25			IC	MP		74 Ec	ho (p	ing)	reply	id	=0×0001,	seq	=15/3840	, ttl=11	5 (req	uest i	in 13)	)				
		16 3.	875191	10.	0.0.25			142.2	50.7	2.68		IC	MP		74 Ec	ho (p	ing)	reques	t id:	=0×0001,	seq	=16/4096	, ttl=12	8 (rep	ly in	17)					
		17 3.3	891205	142	.250.72	2.68		10.0.	0.25			IC	MP		74 Ec	ho (p	ing)	reply	10:	=0×0001,	, seq	=16/4096	, ttl=11	.5 (req	uest 1	in 16)	)				
2	Fra	me 5:	74 byte:	s on wi	n 0000 0010	C4 5	09C0 c12;	5d 1d ae 00	8† c 00 8	C d9	ac ( 00 (	d6 30 00 0a	1 41	08 00 00 19	9456 98e1	a i	• P • m •		=A··E·												
Ś	Int	ernet	Protoco	l Versi	0020	48 4	4 08 0	90 4d	4e 0	00 01	00	0d 61	62	63 64	65 6	56 H	HD · · M	N · · · ·	abcdef												
5	Int	ernet	Control	Messag	e 0030	67 6	8 69 0 1 62 0	5a 6b	6C 6	5d 6e	6f 68	70 71 69	1 72	73 74	1 75 7	6	ghijk vabcd	lmn op efg hi	qrstuv	,											
				-	0040				05 0		00						abcu	erg na													
	-																														
(	2	Inte	rnet Contro	ol Messag	e Protoco	ol: Proto	col															Packe	ts: 72 · Dis	played: {	3 (11.1%	) - Droj	pped: 0	(0.0%)		Profil	e: Default
	-28	19						Q	•	•		P		C		-	48	6	C	Ç	w		2			^	0	<b>଼ି</b> ଦ	<b>ک</b>	7:11 P	M 🌲

The ping will run 4 times by default and the ICMP echo requests and ICMP echo replies and since both are there the ping was successful.

7. What is the IP address of your host? (show within Wireshark) [5 points]

From the above screenshot the source IP address is 10.0.0.25.

- 8. What is the IP address of the destination host?
  - a. Show within Wireshark, and explain how this address was selected? [10 points]

From the above screenshot, the IP address of <u>www.google.com</u> which is the destination IP address is 142.250.72.68.

Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields? [10 points]



#### ICMP Type:8

ICMP Code:0

Other Fields are checksum:0x4d4e

Identifier (BE): 1(0x0001)

Identifier (LE): 256(0x0100)

Sequence number:13(0x000d)

Sequence number:3328(0x0d00)

Sizes of Fields are Checksum: 2 bytes

Identifier: 2 bytes

Sequence Number: 2 bytes.

10. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields? [**10** points]

📕 WF-FI		C	)	×
File Edit View Go Canture Analyze Statistics Telephony. Wireless Tools Help.				
<pre>&gt; Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_(@C9BD223-0F34-4B3E-B9AA-E7FD58687ABF), id 0 &gt; Chernet II, Src: VantivaConne_6d:1d:8f (c4:58:9c:6d:1d:8f), Dst: Intel_d6:3d:41 (cc:d9:ac:d6:3d:41) &gt; Internet Protocol Version 4, Src: 142.250.72.68, Dst: 10.0.0.25</pre>			•	+
B 8,84868         V Internet Control Message Protocol           10 1.84636         Type: 0 (Echo (ping) reply)           11 1.8516         Code: 0           13 2.86167         Checksum: 0x554e [correct]           14 2.98376         [Checksum: 0x554e [correct]           16 3.8719         Identifier (BE): 1 (0x0001)           17 3.89122         Identifier (LE): 256 (0x0100)				
Sequence Number (EE): 13 (8x080d) Sequence Number (LE): 3328 (0x0d0) [Request frame: 5] [Response time: 13.782 ms] > Data (32 bytes) Data: 6162636465666768696a6b6c5d6e6f70717273747576776162636465566676869 [Length: 32] PROMO Cr dP ar d6 31 d1 rd 50 9r 6d 14 8f 88 8P 45 9PP. must F.				
ORI0         OB         26         08         66         68         67         48         44         68         00	P n f	n····E j··HD ∙abcdet pqrstu	f	
I dentifier No. 8 · Time: 0.846689 · Source: 142.250.72.68 · Destination: 10.0.025 · Protocol: ICMP · Length: 74 · Info: Echo (ping) reply id -0.00001, seq=13/3328, ttl=115 (request in 5) Sequence N Sequence N I Reduest f I Reduest f	g hi			
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869				
• ✓ Identifier (little endian representation) (icmp:ident.le). 2 bytes           Packets: 72 · Displayed: 8 (11.1%) · Dropped: 0 (0.0%)             • ✓          • ✓          • ✓	<b>b</b>	Pr 7:4 15/10/	ofile: De 1 PM /2024	efault

### ICMP Type:0

ICMP Code:0

Other Fields are checksum:0x554e

Identifier (BE) :1(0x0001)

Identifier (LE) :256(0x0100)

Sequence number (BE):13(0x000d)

Sequence number (LE):3328(0x0d00)

Sizes of Fields are Checksum: 2 bytes

Identifier: 2 bytes

Sequence Number: 2 bytes.

11. Start a new Wireshark Capture. Ping a hostname or IP that gives you a "Request Timed Out" message. (e.g. You can try <u>www.wellsfargo.com</u> or any another website/IP of your choice.). Filter the ICMP traffic. Find the Type and Code of the packet in the above scenario. Paste the relevant screenshots. [5 points]

<b>/</b> *1	Wi-Fi											-	- 0	×
File	Edit View	Go Capture Analyze St	atistics Telephony Wirel	ess Tools Help										
	🔳 🧷 💿 🚞	। 🛅 🖹 🏹 । ९ 👄 🔿 🕯	i 7 🛃 📃 📃 🔍 e	l el 🎹 📅										
. i	cmp												$\times \rightarrow$	- +
No.	Time	Source	Destination	Protocol Lengtl Inf	0									
	2 1.17565	8 10.0.0.25	192.0.2.1	ICMP 74 Ec	no (ping)	request	id=0x0001,	seq=41/10496,	ttl=128	(no response	found!)			
	25 5.84660	10.0.0.25	192.0.2.1	ICMP 74 Ecl	no (ping)	request	id=0x0001,	seq=42/10752,	ttl=128	(no response	found!)			
	28 10.8313	67 10.0.0.25	192.0.2.1	ICMP 74 Ec	no (ping)	request	id=0x0001,	seq=43/11008,	ttl=128	(no response	found!)			
	34 15.8300	35 10.0.0.25	192.0.2.1	ICMP 74 Eci	no (ping)	request	1d=0x0001,	seq=44/11264,	tt1=128	(no response	found!)			
> F > E > J	Frame 2: 74 b thernet II, Internet Prot Internet Cont Type: 8 (E	ytes on wire (592 bits) Src: Intel_d6:3d:41 (co ocol Version 4, Src: 16 <mark>rol Message Protocol</mark> cho (ping) request)	), 74 bytes captured ( c:d9:ac:d6:3d:41), Dst ð.0.0.25, Dst: 192.0.2	592 bits) on interface : VantivaConne_6d:1d:8 !.1	e ∖Device 8f (c4:50	NPF 0000 9c: 0010 0030 0030	c4 50 9c 00 3c 50 02 01 08 67 68 69 77 61 62	6d 1d 8f cc d9 02 00 00 80 00 00 4d 32 00 00 6a 6b 6c 6d 66 63 64 65 66 67	ac d6 00 00 00 29 6f 70 68 69	3d 41 08 00 4 0a 00 00 19 0 61 62 63 64 6 71 72 73 74 7	5 00 · P 0 00 · < 5 66 · · 5 76 gh wa	··M2 <mark>··</mark> nijklmn op abcdefg h	·=A··E· )abcdef pqrstuv i	
	Code: 0 Checksum: [Checksum: Identifier	0x4d32 [correct] Status: Good] (BE): 1 (0x0001) (LE): 255 (0x0100)												
	Sequence N	(LE): 258 (0x0100) umber (BE): 41 (0x0029)												
	Sequence N	umber (LE): 10496 (0x29	900)											
	> [No respon > Data (32 b	se seen] ytes)												
	Data: 6 [Length:	.62636465666768696a6b6c : 32]	6d6e6+707172737475767	7616263646566676869										
0	Identifier (	little endian representation) (ic	:mp.ident_le), 2 bytes					Packets:	55 · Display	red: 4 (7.3%) · Dro	opped: 0 (0.0	1%)	Profil	e: Default
4	29*		🛯 Q 🖬 🥠	🥵 🖪 O 🕽	-	0	0 🧳	🖷 🗾 I	2	·		r 🕁 🕼	7:58 P 15/10/202	M Q

#### ICMP Type:8

ICMP Code:0 Other Fields are checksum:0x4d32 Identifier (BE) :1(0x0001) Identifier (LE) :256(0x0100)

Sequence number (BE)41(0x0029)

Sequence number (LE):10496(0x2900)

Sizes of Fields are Checksum: 2 bytes

Identifier: 2 bytes

Sequence Number: 2 bytes.

#### 12. Do you see both ICMP Echo Request and Echo Reply messages? [5 points]

In this scenario, we can see only see ICMP Echo request messages in Wireshark since there was a request time out message during ping and therefore there was no echo reply (server did not reply).

#### Objective 2.2 – ICMP and Traceroute

- 1. Open command prompt/terminal (depending on the operating system)
- 2. Start Wireshark and begin capture

- Traceroute to a "hostname" (where the "hostname" is a URL, example: tracert www.google.com)
- 4. When trace completes, stop capture.
- 5. Provide a screenshot of the trace. Was it successful? How do you know? [5

points]

Com	mand Prom	nt	×	+	~		_	a	×
		· · ·							
C:\Us	ers\a	bey>	>trace	ert	-4 www	N.go	pogle.com		
Traci	ina ro	ute	to ww	vw.a	ooale	.com	1 [142.250.72.68]		
over	a max	imun	n of 3	30 h	ops:				
1	8	ms	4	ms	1	ms	10.0.0.1		
2	16	ms	10	ms	12	ms	100.93.92.131		
3	13	ms	14	ms	13	ms	po-319-340-rur302.arvada.co.denver.comcast.net [96.216.161.181	] ,	
4	44	ms	13	ms	10	ms	po-2-rur301.arvada.co.denver.comcast.net [162.151.8.93]		
5	15	ms	37	ms	10	ms	po-300-xar01.arvada.co.denver.comcast.net [162.151.50.57]		
6	28	ms	15	ms	13	ms	be-308-arsc1.denver.co.denver.comcast.net [96.216.147.73]		
7	21	ms	*		*		be-36021-cs02.1601milehigh.co.ibone.comcast.net [96.110.43.245	] ,	
8	12	ms	*		14	ms	<pre>be-3311-pe11.910fifteenth.co.ibone.comcast.net [96.110.33.122]</pre>		
9	20	ms	13	ms	15	ms	23.30.206.218		
10	26	ms	19	ms	14	ms	216.239.47.247		
11	132	ms	17	ms	13	ms	142.251.51.155		
12	21	ms	11	ms	42	ms	den16s09-in-f4.1e100.net [142.250.72.68]		
Trace	e comp	lete	₽.						
C:\Us	sers\a	bev>	>						
		-							
27°					0			:28 PM	0
-				-	Q	-		0/2024	~

The last line says the trace complete which confirms that the packets successfully reached their target. The traceroute reached the final destination 142.250.72.68.

6. Filter the Wireshark capture to only show the relevant trace route data. Examine the ICMP traffic in Wireshark. What is different in the capture from the trace when compared to the capture of the Ping in previous objective? Explain what is different between the Ping and the trace route, and how this relates to how trace route works [15 points]

🚄 *Wi-Fi										-	0	×
File Edit View Go	Capture Analyze Statist	ics Telephony Wireless	Tools Hel	p								
🥖 🔳 🖉 🛞 🚞 🛅	🖹 🙆 🍳 🗢 🏓 🖀 7	F 🛨 📃 📃 લ લ	🔍 🎹 📅									
icmp											$\times$	• +
No. Time	Source	Destination	Protocol	Lengtł Info								_
10 2.273188	10.0.25	142.250.72.68	ICMP	106 Echo (ping) r	equest i	id=0x0001,	seq=111/28416	, ttl=1 (no	response found!	)		
13 2.281433	10.0.0.1	10.0.0.25	ICMP	134 Time-to-live	exceeded	(Time to	live exceeded	in transit)				
14 2.283955	10.0.25	142.250.72.68	ICMP	106 Echo (ping) r	equest i	id=0x0001,	seq=112/28672	, ttl=1 (no	response found!	)		
15 2.288106	10.0.0.1	10.0.0.25	ICMP	134 Time-to-live	exceeded	(Time to	live exceeded	in transit)				
16 2.291443	10.0.0.25	142.250.72.68	ICMP	106 Echo (ping) r	equest i	id=0x0001,	seq=113/28928	, ttl=1 (no	response found!	)		
17 2.292889	10.0.0.1	10.0.0.25	TCMP	134 Time-to-live	exceeded	(lime to	live exceeded	in transit)				
25 2.754200	10.0.0.1	10.0.0.25	TCMP	120 Destination (	inreachab]	le (Port u	nreachable)					
59 5.751639	10.0.0.1	10.0.0.25	TCMP	120 Destination (	inreachabl	le (Port u	nreachable)					
61 8,268502	10.0.0.25	142,250,72,68	ICMP	106 Echo (ping) r	equest i	id=0x0001.	seg=114/29184	. ttl=2 (no	response found!	)		_
62 8.284424	100.93.92.131	10.0.0.25	ICMP	134 Time-to-live	exceeded	(Time to	live exceeded	in transit)		,		
63 8.294451	10.0.0.25	142.250.72.68	ICMP	106 Echo (ping) r	equest i	id=0x0001,	seq=115/29440	, ttl=2 (no	response found!	)		
66 8.304348	100.93.92.131	10.0.0.25	ICMP	134 Time-to-live	exceeded	(Time to	live exceeded	in transit)				
67 8.306139	10.0.25	142.250.72.68	ICMP	106 Echo (ping) r	equest i	id=0x0001,	seq=116/29696	, ttl=2 (no	response found!	)		
68 8.318272	100.93.92.131	10.0.25	ICMP	134 Time-to-live	exceeded	(Time to	live exceeded	in transit)				
84 14.265844	10.0.25	142.250.72.68	ICMP	106 Echo (ping) r	equest i	id=0x0001,	seq=117/29952	, ttl=3 (no	response found!	)		_
85 14.279354	96.216.161.181	10.0.0.25	ICMP	134 Time-to-live	exceeded	(Time to	live exceeded	in transit)				
> Frame 10: 106 byte	es on wire (848 bits),	106 bytes captured	(848 bits)	on interface \Devi	0000	c4 50 9c	6d 1d 8f cc d9	ac d6 3d 4	41 08 00 45 00	• P • m • • • • •	=A··E·	
> Ethernet II, Src:	<pre>Intel_d6:3d:41 (cc:d9</pre>	e:ac:d6:3d:41), Dst:	VantivaConr	ne_6d:1d:8f (c4:50:	0010	00 5c 12	b2 00 00 01 01	00 00 0a 0	00 00 19 8e fa	-\		
> Internet Protocol	Version 4, Src: 10.0.	0.25, Dst: 142.250.7	2.68		0030	00 00 00	00 00 00 00 00 00	00 00 00 0	80 80 80 80 80	HU		
<ul> <li>Internet Control I</li> </ul>	Message Protocol				0040	00 00 00	00 00 00 00 00	00 00 00	00 00 00 00 00			
Type: 8 (Echo	(ping) request)				0050	00 00 00	00 00 00 00 00	00 00 00 0	00 00 00 00 00			
Code: 0					0060	00 00 00	00 00 00 00 00	00 00				
Checksum: 0x1/8	st [correct]											
Identifier (BE	15: 0000j											
Identifier (LE)	): 256 (0x0100)											
Sequence Number	(BE): 111 (0x006f)											
🔵 🍸 Internet Control	Message Protocol: Protocol						Packets:	716 · Displayed	: 72 (10.1%) · Droppe	d: 0 (0.0%)	Profile	: Default
30°		Q 🖬 🍫	af 🖪	0 📮 🗳	6 6	9 🧳	🖷 🗾 E	8 💋	~ 🖄	< 🗘 🖢	9:39 PN 15/10/202	4 Q

In the previous objective there was only ping request, only ICMP echo request (type 8) and ICMP Echo reply messages are exchanged. In Traceroute you can see ICMP echo requests but the ICMP Time to live (TTL) exceeded responses from routers. It is essential for mapping the path to the target host. Traceroute sends out packets with increasing TTL values starting with 1. Each router along the path decreases the TTL by 1. When the TTL reaches zero, the router sends back an ICMP time exceeded message. This takes place in the capture of every hop until the destination is reached. Ping is a simple ICMP tool that checks the reachability of a host by sending a echo request and receiving an echo reply whereas traceroute not only checks reachability but also maps the path by incrementally adjusting the TTL and provides the IP address and response time of each router.

### Part 3 – Wireshark NICs and IPv4/IPv6 addresses

#### **Objective 3.1**

 Provide a screenshot of the NICs that Wireshark has to choose from on the PC. [10 points]

🚄 The Wireshark Network	nalyzer				-	0	×
File Edit View Go	Capture Analyze Statistics Telephony Wireless Tools Help						
🧉 🔳 🖉 💿 🚞 🛅	x 6   4 + + # 7 ± 📃 📃 e. 4 4 II II						
Apply a display filter •	Ctrl-/>					-	+
	Welcome to Wireshark						
	Open						
	C:\Users\abey\Downloads\wireshark obj3.pcapng (77 KB)						
	C:\Users\abey\Downloads\wireshark onj 2.1 capture 11q&12q.pcapng (16 KB)						
	C:\Users\abey\Downloads\wireshark obj 1 capture.pcapng (19 KB)						
	Capture						
	using this filter: 📕 Enter a capture filter		▼ All ir	nterfaces shown -			
	we re						
	Local Area Connection* 10						
	Local Area Connection* 9						
	Local Area Connection* 8 Plusteeth Network Connection						
	Mwaro Notwork Adapter VMnot8						
	Learn						
	User's Guide 🔹 Wiki 🔹 Questions and Answers 🐁 Mailing Lists 🐁 SharkFest 🐳 Wireshark Discord 🕤 Donate						
	You are running Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e). You receive automatic updates.						
Ready to load or cap	ure	No Packets				Profile: D	efault
9	📕 Q 🖬 🧐 🗰 🖪 💽 🐂 🗳 Q 🖉 🛋 🕴	<u>&gt;</u>		^ @ <b>⊜</b> Φ)	10 16/1	:57 AM 0/2024	Q

Which interface is currently capturing traffic? How do you know? (Provide a screenshot) [10 points]

	*Wi-Fi						- 0	×
Fi	ile Edit View Go	Capture Analyze Statistic	s Telephony Wireless	Tools Hel	p			
1	( 🔳 🦪 🛞 🚞 🚺	🕅 🔁 🧣 👄 📽 🐐	! 📜 🔲 લ લ લ	亚品				
ſ	Apply a display filter .	<ctrl-></ctrl->		state todad			<b>—</b> •	+
N	Time	Courses	Destination	Destorel	Length Jofe			-
1.4	1 9 999999	10 0 0 25	23 222 27 4	TCP	66 64765 + 80 [SVN]	Sen-P	Win-64240 Lan-0 MSS-1460 WS-256 SACK PERM	
-	2 0.015490	23.222.27.4	10.0.0.25	TCP	66 80 → 64765 [SYN,	ACK1	Seg=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK PERM WS=128	
	3 0.015997	10.0.0.25	23.222.27.4	TCP	54 64765 → 80 [ACK]	Sea=1	L Ack=1 Win=262656 Len=0	
	4 0.016594	10.0.0.25	23.222.27.4	HTTP	136 GET /ncc.txt HTT	P/1.1		=
	5 0.035423	23.222.27.4	10.0.0.25	TCP	54 80 → 64765 [ACK]	Seq=1	1 Ack=83 Win=64256 Len=0	-
	6 0.035423	23.222.27.4	10.0.0.25	HTTP	205 HTTP/1.1 200 OK	(text	t/html)	
	7 0.036292	2601:280:5f00:1af0:.	2600:1405:7400:b::1.	. TCP	86 64766 → 80 [SYN]	Seq=0	0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM	
	8 0.068101	2600:1405:7400:b::1	2601:280:5f00:1af0:.	. TCP	86 80 → 64766 [SYN,	ACK]	Seq=0 Ack=1 Win=64800 Len=0 MSS=1440 SACK_PERM WS=128	-
1	9 0.068548	2601:280:5f00:1af0:.	2600:1405:7400:b::1.	. TCP	74 64766 → 80 [ACK]	Seq=1	1 Ack=1 Win=263424 Len=0	=
	10 0.069031	2601:280:5f00:1af0:.	2600:1405:7400:b::1.	. HTTP	156 GET /ncc.txt HTT	P/1.1		
	11 0.087881	2600:1405:7400:b::1	2601:280:5f00:1af0:.	. TCP	74 80 → 64766 [ACK]	Seq=1	L Ack=83 Win=64768 Len=0	
	12 0.087881	2600:1405:7400:b::1	2601:280:5f00:1af0:.	. HTTP	225 HTTP/1.1 200 OK	(text	c/html)	=
	13 0.088469	2601:280:5f00:1af0:.	2600:1405:7400:b::1.	. TCP	74 64766 → 80 [FIN,	ACK]	Seq=83 Ack=152 Win=263168 Len=0	-
	14 0.088878	10.0.25	23.222.27.4	TCP	54 64765 → 80 [FIN,	ACK]	Seq=83 Ack=152 Win=262400 Len=0	
	15 0.100493	2600:1405:7400:b::1.	2601:280:5f00:1af0:.	. TCP	74 80 → 64766 [FIN,	ACK]	Seq=152 Ack=84 Win=64768 Len=0	-
	16 0.100709	2601:280:5f00:1af0:.	2600:1405:7400:b::1.	. TCP	74 64766 → 80 [ACK]	Seq=8	34 Ack=153 Win=263168 Len=0	
	17 0.121010	23.222.27.4	10.0.0.25	TCP	54 80 → 64765 [FIN,	ACK]	Seq=152 Ack=84 Win=64256 Len=0	
> >	Frame 1: 66 byte Ethernet II. Src	s on wire (528 bits), 66	5 bytes captured (528 ac:d6:3d:41), Dst: Va	bits) on ntivaConn	interface \Device\NPF	<b>0000</b>	C4         50         9c         6d         1d         8f         cc         d9         ac         d6         3d         41         08         00         45         00         ••••=A·E·         eac           00         34         79         f0         40         00         80         66         00         00         0a         19         17         de         ····································	
>	Internet Protoco	1 Version 4. Src: 10.0.6	0.25. Dst: 23.222.27.4			0020	1b 04 fc fd 00 50 69 21 e6 71 00 00 00 00 80 02 ····Pi! ·q·····	
>	Transmission Con	trol Protocol, Src Port:	: 64765, Dst Port: 80,	Seq: 0,	Len: 0	0030	ta to 3d 21 00 00 02 04 05 b4 01 03 03 08 01 01=!	
						0040	04 02	
	12							
(	🔵 🍸 wireshark_Wi-	FilD5MV2.pcapng					Packets: 300 - Dropped: 0 (0.0%) Profile: De	efault
	<b>9</b>		Q 🖬 🥠 🖬		0 들 🔮 😆		🖢 💣 🚄 🔀 🖷 💌 🔹 ^ 🗞 👳 🕫 🖬 16/10/2024	Q

 What is the easiest way to determine the IPv4/IPv6 address of the NICs before a capture is started? Provide a screenshot where some NICs show IPv6 addresses and some show IPv4 addresses. [10 points]



In my windows I ran the command ipconfig will display the IP addresses for each NIC. IPv4 address is 10.0.0.25 and IPv6 address is 2601

## Part 4 – Continuous Captures, Filtering, and Analysis

#### **Objective 4.1**

 Initiate a Wireshark capture that uses multiple files, where it creates a new file every 5 minutes, for a total of 15 minutes. (Provide a screenshot of the Capture Options you selected). Remember where you save this file, as we will use it in the future. Also, try to use the wireless NIC if possible, as there will be more traffic in the capture to analyze. [15 points]

Rod 🦪 Wireshark - Capture Ontions		— п × / /=
00 Mileshark Capture Options		Editor
Input Output Options		
Capture to a permanent file —		Editor
File: C:\Users\abey\Download	ds\wireshark capt.pcapng	Browse
Output format: 🔘 pcapng 🝳	pcap	
Create a new file automatica		
after	100000    packets	
after	1 kilobytes ~	
🕑 after	5 iminutes ~	
when time is a multiple of	1 hours ~	
compression	File infix pattern	
None		
gzip		
Use a ring buffer with 3	➡ files	
		Start Close Help
Q Search		[L] Focus 때 [] 등
Image: States     Text Product       Image: States     Text Product       Analyzer     Statistics       Capture     Analyze       Statistics     Telep       Image: Statistics     Telep       Image: Statistics     Telep	accont of the Accessioning Investigate	<u>()</u> Foods 때 📒 👸
English (United States) Text Pre     Q Search  Analyzer Capture Analyze Statistics Teleg      Q Q Search      (Ctpl./s      (Wireshark - Capture Options	accontro UN Accessioning Investigate	
English (United States) Text Pro     Q Search  Analyzer Capture Analyze Statistics Tele     Q     Q + + + = = + + + + + + + + + + + +	accontro UN Accessioning Investigate	
Image: Complexite Complexite     Text Processing Complexite       Image: Complexite Complexite     Complexite       Image: Complexite	accontro UN Accessioning Investigate	
English (United States) Text Pro     Q Search  Analyzer Capture Analyze Statistics Tele     Q O Q + + + + + + + + + + + + + + +	Account of the Accessioning Investigate	
English (United States) Text Pro     Q Search  Analyzer Capture Analyze Statistics Tele     Q O'      Q A A A A A A A A A A A A A A A A	Accounts of the Accessioning Investigate	
English (United States) Text Pro     Analyzer     Capture Analyze Statistics Teleg     Original Content of the states of th	Account of the Accessioning Investigate	
English (United States) Text Pre     Q Search  Analyzer Capture Analyze Statistics Teleg      O Q A A A A A A A A A A A A A A A A	Accessioning, investigate	
English (United States) Text Pre     Analyzer     Capture Analyze Statistics Tele     Organize Analyze Statistics     Organize Analyze     Organize     Organize Analyze     Organize     Organize Analyze     Organize     Org	Accessioning: Investigate	
English (United States) Text Pre     Analyzer     Capture Analyze Statistics Tele     Output Options     Display Options     Update list of packets in re     Automatically scroll during     Stop capture automatically after     Stop capture automatically after     1	Accessioning, investigate	
English (United States) Text Pre  Analyzer Capture Analyze Statistics Tele      Organize Statistics      O	Accessioning investigate	
English (United States) Text Pre  Analyzer Capture Analyze Statistics Tele      Or Q Search  Analyzer Capture Analyze Statistics Tele      Or Q Search      Or Q Search	Accessioning, investigate	
English (United States) Text Pre  Analyzer Capture Analyze Statistics Tele      Organize Statistics      O	Accessioning, investigate	
English (United States) Text Pre  Analyzer Capture Analyze Statistics Tele      Original Control of the states of the state	Accessioning, investigate	
English (United States) Text Pro     Analyzer     Capture Analyze Statistics Teleg     Original States)     Wireshark - Capture Options     Input Output Options     Display Options     Output Options     Display Options     Show capture information     Show capture automatically afte     I     ifies     Show capture automatically afte     I     ifies     Show capture automatically afte     I     ifies     Display Options     Show capture information     Show capture information     Show capture information     Display Options     Displ	Accessioning: Investigate     Image: Constraint of the constrain	
English (United States) Text Pro     Analyzer     Capture Analyze Statistics Tele     Original Control of the states of the	Accessioning investigate	
English (United States) Text Pro     Capture Analyzer     Capture Analyze Statistics Tele     O Sov a statistics Tele     O Sov a statistic Tele     O	Accord of the Accession in Investigate	
English (United States) Text Pro     Analyzer     Capture Analyze Statistics Tele     Capture Analyze Statistics Tele     Output Options     Display Options     Display Options     Display Options     Show capture information     Stop capture automatically scroll during     Show capture information     Stop capture automatically afte     1	Accord of the Accession in Investigate	Cose       Help
English (United States) Text Pro  Analyzer Capture Analyze Statistics Tele      Capture Analyze Statistics Tele      Output Options      Update list of packets in re      Update list of packets in re      Update list of packets in re      Output Options      Update list of packets      Input Output Options      Output Options      Disclory of temporary files      Cutters'abery/AppDa.      B   Update Wiki - Output	Accessioning investigate	
English (United States) Text Pro     Analyzer     Capture Analyze Statistics Tele     Capture Analyze Statistics Tele     Capture Analyze Statistics Tele     O () () () () () () () () () () () () ()	Accessioning investigate	

- 2. Browse ten different websites, during this 15-minute continual capture time window.
- 3. What are THREE reasons why you would want to create multiple files? **[15 points]** It's easier to navigate multiple smaller files and segmentation of data especially if we want to check the logs at a specific period.

Splitting larger files to smaller files prevents the creation of large files that are difficult to analyze.

Capturing logs in one file for a long period of time can cause issues if it is a large file, it has the potential to crash and lose data. Having multiple files can ensure the data is preserved.

4. How do you view the three files captured within Wireshark, and move between them, after they have been completed and saved? (Hint: File > File Set) [10 points]

apt4_20241023194954_00004.pcapng         File       Edit       View       Go       Capture       Analyze         Image: A construction of the construction of	Statistics Telephony Wireless Tools Help	- 0 X
Na Time Course	Wireshark - 3 Hiles in Set	X
No.         Time         Source           8911         83.749374         2601:288:           8912         83.749371         2601:288:           8913         83.749371         2601:280:           8914         83.749461         2601:280:           8915         83.749371         2601:280:           8916         83.749542         2601:280:           8916         83.749542         2601:280:           8917         83.749542         2601:280:           8918         83.765027         2601:1280:           8919         84.04077         2600:1485           8921         84.541639         2601:280:           8921         84.541639         2601:280:           8922         84.569145         Intel_d6:3:           8922         84.569145         Intel_d6:3:           8922         84.569145         Intel_d6:3:           9         Frame 11: 199 bytes on wire (972 I)         >           > Internet Protocol Version 6, Src         >           > User Datagram Protocol, Src Port         >           > Domain Name System (query)	Filename         Created         Modified         Size           capl4_02014023193954_00002,capng         2024-10-23 19:4453         721           capl4_20241023194454_000004,capng         2024-10-23 19:4454         2024-10-23 19:49:54         327           capl4_20241023194954_00004,capng         2024-10-23 19:49:54         2024-10-23 19:51:19         8498           Directory:         C <u>Utersitabeyi/Downloads</u> Close         Help	21 kB 21 kB 1440 1:0 Len=0 1:0 Len=0 1:
	nep	
O apt4_20241023194954_00004.pcapm	Packets: 8924 - Droppe	ped: 0 (0.0%) Profile: ICMP
● Q	🖬 🧐 🕸 🖪 O 🃜 📽 🍳 🧐 🧐 🦄 🖷 🚎 💆 🛤	ヘ 🗞 奈 Φ) 🆢 7:51 PM 🌲 23/10/2024

5. How do you see which websites you browsed during the capture? (Hint: Statistics > HTTP) [5 points]

<b>/</b> *W	n-Fi						- 0 X	(
File	Edit View Go Cap	oture Analyze Statistic	s Telephony Wireless To	ols Help				
	I 🖉 🛞 🚞 🛅 🕅	🙆 । ९ 👄 🔿 🖀 🐐	🛓 📃 🔳 લ લ લ 🤅	1 2 2				
📕 ip.	src == 23.32.252.145						×	
No.	Time	Source	Destination	Protocol	Lengtł Info			
	1486 13.098035	23.32.252.145	10.0.0.25	TCP	66 443 → 52:	120 [SYN,	, ACK] Seg=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK PERM WS=128	
	1491 13.146083	23.32.252.145	10.0.25	TCP	54 443 → 52	120 [ACK]	] Seq=1 Ack=1758 Win=63360 Len=0	
	1493 13.147641	23.32.252.145	10.0.25	TLSv1.3	1514 Server He	ello, Char	ange Cipher Spec, Application Data	
	1494 13.148684	23.32.252.145	10.0.25	TCP	1514 443 → 52	120 [PSH,	, ACK] Seq=1461 Ack=1758 Win=64128 Len=1460 [TCP PDU reassembled in 1495]	
	1495 13.148684	23.32.252.145	10.0.25	TLSv1.3	1230 Applicat:	ion Data,	, Application Data	
	1496 13.148684	23.32.252.145	10.0.25	TLSv1.3	61 Applicat:	ion Data		
	1508 13.189861	23.32.252.145	10.0.25	TLSv1.3	341 Applicat:	ion Data		
	1509 13.189861	23.32.252.145	10.0.25	TLSv1.3	341 Applicat:	ion Data		
	1514 13.216801	23.32.252.145	10.0.25	TCP	54 443 → 52	120 [ACK]	] Seq=4678 Ack=4427 Win=62336 Len=0	
	1517 13.241381	23.32.252.145	10.0.25	TLSv1.3	115 Applicat:	ion Data		-
	1518 13.241381	23.32.252.145	10.0.25	TLSv1.3	85 Applicat:	ion Data		
	1522 13.265064	23.32.252.145	10.0.25	TLSv1.3	483 Applicat:	ion Data		
	1592 13.331528	23.32.252.145	10.0.25	TCP	54 443 → 52:	120 [ACK]	] Seq=5199 Ack=4458 Win=64128 Len=0	
	1655 13.927937	23.32.252.145	10.0.0.25	TCP	1514 443 → 52	120 [ACK]	J Seq=5199 Ack=4458 Win=64128 Len=1460 [TCP PDU reassembled in 1670]	
> Er	ame 1486: 66 bytes	on wire (528 bits).	66 bytes captured (528	B bits) on	interface '	0000 cc	: d9 ac d6 3d 41 c4 50 9c 6d 1d 8f 08 00 45 00 ····=A·P ·m····E·	
> Et	hernet II. Src: Van	tivaConne 6d:1d:8f	(c4:50:9c:6d:1d:8f), D	st: Intel d	6:3d:41 (c	0010 00	34 00 00 40 00 37 06 25 fa 17 20 fc 91 0a 00 ·4··@·7· %·· ···	
> Ir	ternet Protocol Ver		252.145, Dst: 10.0.0.2	5 -		0020 00	9 19 01 bb cb 98 d0 10 dd ee 5c fd da d9 80 12 ······	
∨ Tr	ansmission Control	Protocol, Src Port:	443, Dst Port: 52120,	Seq: 0, Ac	k: 1, Len:	0030 ta	a 10 a3 10 00 00 02 04 05 04 01 01 04 02 01 03	
	Source Port: 443	-				0040 00		
	Destination Port:	52120					Command Prompt × + • - · · ·	
	[Stream index: 68]						Non-authoritative answer:	
	[Stream Packet Num	ber: 2]			-		Namo: walmant com	
>	[Conversation comp	leteness: Complete,	WITH_DATA (63)]				Address: $23 \ 32 \ 252 \ 1/15$	
	[TCP Segment Len:	0]					Address. 25.52.202.140	
	Sequence Number: 0	(relative seque	nce number)					
	Sequence Number (r	aw): 3490766318					C.\Ilsers\abev>	
	[Next Sequence Num	ber: 1 (relative	sequence number)]					
	Acknowledgment Num	her 1 (relative	ack number)					
0	wireshark_Wi-Fi8ETB <sup>1</sup>	W2.pcapng					Packets: 7431 · Displayed: 368 (5.0%) · Dropped: 0 (0.0%) Profile: IC	MP
8	6°		• 🐔 🖬 🖷	0 -		0	7:31 PM	
-		L C	0	•				

### Objective 4.2

- 1. Create two Display filter buttons. One for traffic sourced from your machine's IP address and one that only displays HTTP GET requests. (Hint: HTTP contains)
- Provide a screenshot of the buttons you created, and the corresponding filtered capture. [10 points]

🚄 *Wi-Fi								-	Ø	$\times$
File Edit	View Go Captu	ure Analyze Statistics	Telephony Wireless To	ols Help						
📕 🔳 🙇 (	۵ 🗀 🚞 🔇	े। ९ 👄 🏓 🖀 🛓	k 📃 📃 Q Q Q I							
ip.src == 1	10.200.128.123						X	+ IP trai	fic H	TTP GET
Filter Buttor	ns Preferences La	abel: Enter a description fo	r the filter button		Filter: htt	p.request.method == "GET"		OK	Ca	ncel
	G	omment: Enter a commen	t for the filter button					OK	cu	incer
🚄 *Wi-Fi								-	٥	×
File Edit	View Go Captu	ure Analyze Statistics	Telephony Wireless To	ols Help						
🛋 🔳 🙇 (	۵ 🗀 🛅 🎗 🔇	🕽 । ९ 👄 👄 🖀 🗿	k 📃 🔳 @ @ @ I							
http.reque	est.method == "GET	•					×	🔹 🛨 IP tra	fic H	TTP GET
Filter Buttor	ns Preferences La	abel: Enter a description fo	r the filter button		Filter: htt	p.request.method == "GET"		OK	Ca	ncel
	G	omment: Enter a commen	t for the filter button						Ca	licer
No.	Time	Source	Destination	Protocol Length	Info					
+ 131	56 72.757866	10.200.128.123	23.222.27.62	HTTP	136 GET /nc	c.txt HTTP/1.1				

### Objective 4.3

1. Create a coloring rule for HTTP traffic. [5 points]

Navigate to View-> Coloring Rules from the top menu.

Click on HTTP and change the background color to red and white lettering and click Ok to save the rule.

2. Provide a screenshot of your capture from above, showing where you changed the color of HTTP GET requests to Red background with White lettering. (Hint: Did you remember to move your color rule to the top?) **[10 points]** 

I 🔳 🧟 🛞 🚞 🛅 💈			ools Help	
	१ 🖸 । ९ 🗢 🖷 🐐	* <b>.</b>		
ip.src == 10.200.128.123				+ IP traffic HTT
filter Buttons Preferences	Label: Enter a description	for the filter button		Filter: http:request.method == "GET" OK Canc
	Comment: Enter a comme	ent for the filter button		
o. Time	Source	Destination	Protocol Length	Info
13132 72.356583 13139 72.39404	3 10.200.128.123 10.200.128.123	13.89.179.13 13.89.179.13	TLSv1.3 TCP	962 Application Data 54 58230 → 443 [ACK] Sec=1646 Ack=6589 Win=261376 Len=0
13140 72.39412	10.200.128.123	13.89.179.13	TCP	54 58230 → 443 [ACK] Seq=1646 Ack=7109 Win=260864 Len=0
13147 72.599172 13148 72.63030	2 10.200.128.123 3 10.200.128.123	128.138.129.76 128.138.240.1	DNS	73 Standard query 0x45c0 A ncc.avast.com 73 Standard guery 0x45c0 A ncc.avast.com
13152 72.737410	5 10.200.128.123	23.222.27.62	ТСР	66 58231 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13155 72.757647 13156 72.75786	7 10.200.128.123 5 10.200.128.123	23.222.27.62	тср нттр	54 58231 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 136 GET /ncc.txt HTTP/1.1
13159 72.76742	10.200.128.123	23.222.27.62	ТСР	54 58231 → 80 [FIN, ACK] Seq=83 Ack=152 Win=131072 Len=0
13161 72.786576	<pre>10.200.128.123 10.200.128.123</pre>	23.222.27.62 74.125.126.188	TCP	54 58231 → 80 [ACK] Seq=84 Ack=153 Win=131072 Len=0 55 [TCP Keep-Alive] 56305 → 5228 [ACK] Seg=1 Ack=1 Win=510 Len=1
13205 75.333110	3 10.200.128.123	74.119.118.154	TCP	54 58226 → 443 [FIN, ACK] Seq=2500 Ack=4218 Win=130048 Len=0
13206 75.333254	10.200.128.123 10.200.128.123	172.64.155.209	TCP	54 58229 → 443 [FIN, ACK] Seq=7855 Ack=2992 Win=130304 Len=0
Ethernet II, Src: I Internet Protocol V Transmission Contro Hypertext Transfer > GET /ncc.txt HTT Host: ncc.avast. User-Agent: Avas Accept: */*\r\n	intel_d6:3d:41 (cc:d9:a fersion 4, Src: 10.200. ol Protocol, Src Port: P/1.1\r\n com\r\n t NCC\r\n	ac:d6:3d:41), Dst: Cis .128.123, Dst: 23.222. 58231, Dst Port: 80,	cco_82:06:80 (70:db:) 27.62 Seq: 1, Ack: 1, Len	$\begin{array}{c c c c c c c c c c c c c c c c c c c $
1010				
wireshark_Wi-FiQ8	3K8V2.pcap			Packets: 13522 · Displayed: 5736 (42.4%) · Dropped: 0 (0.0%) Profile: 0
28°	Q	🖬 🍫 📫 🖪	I 🖸 📜 🚭	) 🖧 💽 🚰 🚾 🗖 💁 📶 🔚 🛛 🗠 🕾 🗇 🗁 339 PM
capt4_20241023194954_0	0004.pcapng	The second second second		- 0
capt4_20241023194954_0 Edit View Go ( @ 20 (***********************************	0004.pcapng Capture Analyze Statistics ﴿ 🌀 🍳 👄 🛸 警 🐐	: Telephony Wireless T 👱 📃 🗐 🍳 🍳 🍳	iools Help	- 0
capt4_20241023194954_0 Edit View Go (  Edit View Go (  Mttp  http  http  Time	0004.pcapng Capture Analyze Statistics Color Color Col	Telephony Wireless T	iools Help	- 0 fo
capt4_20241023194954_0           2           Edit           View         Go           Image: Constraint of the state	0004,pcapng Capture Analyze Statistics Control Control	: Telephony Wireless T 	ools Help	- 0 T /ncc.txt HTP/1.1 T/1.200 0K (favt/btnl)
capt4_20241023194954_C a Edit View Go ( a Edit View Go ( b 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0004.pcapng Capture Analyze Statistics Source 10.0.0.25 23.217.9.9 2601:280:5f00:1af6	E Telephony Wireless T	Protocol Lengti Ini HTTP 136 GE HTTP 205 HT 1 HTTP 156 GE	- 0 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1
capt4_20241023194954_C a Edit View Go ( Capt6_20241023194954_C bttp http http http http http 1_218374 66 9.279741 71 9.289426 72 9.289426	0004.pcapng apture Analyze Statistics 3 C Q A A A A A A A A A A A A A A A A A A	Telephony Wireless T     Destination     23.217.9.9     10.0.0.25     2600:1445:7440:b::     2600:145:7440:5:7400:b::     2600:145:7440:5:7400:b::     2600:145:7440:5:7400:b::     2600:145:7440:5:7400:b::     2600:145:7400:b::     2600:145:7400:150:140:145:7400:1500:140:145:7400:1500:140:145:7400:1500:140:145:7400:145:140:145:7400:145:145:145:145:145:145:145:145:145:145	Cools Help	- 0 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1
capt4_20241023194954_0 Edit View Go ( http http http http 12.28574 66 9.279741 71 9.289426 72 9.289426 75 9.303391	0004,pcapng apture Analyze Statistics 3 ℃ Q ↔ ↔ 至 至 Source 10.0.0.25 23.217.9.9 2601:280:5F00:1aff 2601:280:5F00:1aff 2601:280:5F00:1aff 2600:1405:7400.to:	Telephony Wireless T     Destination     23.217.9.9     10.0.0.25     Color: 1405:7400:b::     2600:1405:7400:b::     2600:1405:7400:1500:1400:1400:1400:1400:1400:1400:1	Protocol         Length           HTTP         136         66           HTTP         205         HT           L         HTTP         156         66           L.         HTTP         156         66           L.         HTTP         156         66           L.         HTTP         156         66           L.         HTTP         255         HT	- 0 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 TP/1.1200 0x (text/html)
capt4_20241023194954_C e Git View Go ( http http http http 12.28574 66 9.279741 71 9.289426 72 9.289426 75 9.363391 80 9.356979 81 9.356979	0004.pcapng apture Analyze Statistics 3 ℃ ♀ ↔ ↔ № № № ↓ Source 10.0.0.25 23.217.9.9 2601:280:5F00:1aff 2601:280:5F00:1aff 2600:1405:7400:b: 2600:1405:7400:b: 2600:1405:7400:b:	Telephony         Wireless         T           ■         ■         ■         ■           Destination         23.217.9.9         ■         ■           10.0.0.25         ■ <td>Protocol         Lengt         II           HTTP         136         6E           HTTP         265         HT           L         HTTP         156         6E           L         HTTP         256         HT           L         HTTP         225         HT           L         HTTP         225         HT</td> <td>- 0 T /ncc.txt HTTP/1.1 TP/1.1 200 0K (text/html) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 TP/1.1 200 0K (text/html) TP/1.1 200 0K (text/html)</td>	Protocol         Lengt         II           HTTP         136         6E           HTTP         265         HT           L         HTTP         156         6E           L         HTTP         256         HT           L         HTTP         225         HT           L         HTTP         225         HT	- 0 T /ncc.txt HTTP/1.1 TP/1.1 200 0K (text/html) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 TP/1.1 200 0K (text/html) TP/1.1 200 0K (text/html)
Appl4_20241023194954_C Edit View Go ( type of the second	0004.pcapng apture Analyze Statistics (Contemportant Contemportant Con	Telephony         Wireless         T           ■	Protocol         Lengtl         In           HTTP         136         66           HTTP         205         HT           1.         HTTP         136         66           HTTP         156         66         1.           1.         HTTP         156         66           1.         HTTP         156         62           1.         HTTP         125         67           2.         HTTP         225         HT           3:-         HTTP         225         HT	- 0 T /ncc.txt HTTP/1.1 TP/1.1 200 (K (text/html)) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1
capt4_20241023194954_C e Edit View Go ( http: http: http: http: http: 210374 220374 71 9.289916 72 9.289426 75 9.363391 80 9.350979 81 9.350979	0004.pcapng apture Analyze Statistics (Comparing the statistics (Comparing the statistics (Comparing the statistics (Comparing the statistics) (Comparing the statis	Image: Telephony       Wireless       T         Image: Telephony       Image: Telephony       Image: Telephony         Image: Telephony       Telephony       Image: Telephony       Image: Telephony         Image: Telephony       Telephony       Telephony       Image: Telephony       Image: Telephony         Image: Telephony       Telephony       Telephony       Telephony       Telephony       Image: Telephony         Image: Telephony       Telephony       <	iii iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	- 0 T /ncc.txt HTTP/1.1 TP/1.1 200 K (text/html) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1
capt4_20241023194954_0 Edit View Go ( http: http: http: http: http: http: 19.258154 C 2 9.289426 75 9.383391 80 9.350979 81 9.350979	0004.pcapng apture Analyze Statistics (Constraint) Source 19.0.0.25 23.217.9.9 2601:280:5F00:1af4 2601:280:5F00:1af4 2601:280:5F00:1af4 2601:280:5F00:1af4 2601:1405:7400:b: 2600:1405:7400:b:	Telephony Wireless T     Construction     Construct	image: second	CO T /ncc.txt HTTP/1.1 TP/1.1 200 OK (text/html) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 TP/1.1 200 OK (text/html) TP/1.1 200 OK (text/html) TP/1.1 200 OK (text/html)
Appl4_20241023194954_C Edit View Go ( http http http http http 1 9.2899166 72 9.289426 75 9.36391 80 9.350979 81 9.350979	0004.pcapng apture Analyze Statistics 3 C • • • • • • • • • • • • • • • • • •	Telephony Wireless T     Construction     Construct	image: constraint of the second sec	C T /ncc.txt HTTP/1.1 TP/1.1 200 0K (text/html) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 TP/1.1 200 0K (text/html) TP/1.1 200 0K (text/html) TP/1.1 200 0K (text/html)
caput, 20241023194954, € e Edit View Go ( 2 Edit View Go ( 2 Edit View Go ( 2 2 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	0004.pcapng apture Analyze Statistics 3 ℃ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ Source 10.0.0.25 23.217.9.9 2601:280:5F00:1aft 2601:280:5F00:1aft 2601:280:5F00:1aft 2601:280:5F00:1aft 2601:280:5F00:1aft 2600:1405:7400:b: 2600:1405:7400:b:	Telephony Wireless T     Construction     Construct	image: second	
caput. 2024/1023194954, c           c         Edit View Go (           d         C           d         C           http         Ime           http         1,213374           http         2,20154           66         9,279741           71         9,289016           72         9,289012           75         9,363971           80         9,350979           81         9,350979           Frame 58:         136 bytes           Ethernet 11, Src: 1         1	0004.pcapng apture Analyze Statistics (C) (C) (C) (C) (C) (C) (C) (C) (C) (C)	<ul> <li>Telephony Wireless T</li> <li>■ Q Q Q Q</li> <li>■ Destination</li> <li>23.217.9.9</li> <li>10.0.0.25</li> <li>00:00:1405:7400:b::</li> <li>00:00:1405:7400:b::</li> <li>10:00:1405:7400:b::</li> <li>2600:1405:7400:b::</li> <li>2600:280:5700:1476</li> <li>11:00:280:5700:1476</li> <li>136 bytes captured (1ac:d6:3d:41), Dst: Van</li> </ul>	cods         Help           II         III           Protocol         Lengti           HTTP         136           HTTP         205           III         HTTP           12         HTTP           HTTP         156           III         HTTP           III         HTP           12         HTTP           13         HTTP           14         HTTP           15         GE           III         TTP           25         HT           13         HTTP           225         HT           14         HTTP           225         HT           13         HTTP           225         HT           14         HTTP           225         HT           12         HTTP           225         HT           14         HTTP           23         HT           24         HT           25         HT           26         HT           27         HT           28         HT           29	Comparing the set of
Frame 58: 136 bytes           Frame 58: 136 bytes	0004.pcapng apture Analyze Statistics (C) (C) (C) (C) (C) (C) (C) (C) (C) (C)	<ul> <li>Telephony Wireless T</li> <li>■ ■ ■ ■ ■ ■ ■</li> <li>■ ■ ■<td>Cools Help Protocol Lengti Ini HTTP 136 GE HTTP 205 HT 205 HTTP 205 HT 156 GE 1. HTTP 156 GE 1. HTTP 156 GE 1. HTTP 225 HT 3 HTTP 225 HT 888 bits) HTTP 225 HT 888 bits) tivaConne_6d:1d:8f 4 Seg: 1, Ack: 1, Len</td><td>Comparing    </td></li></ul>	Cools Help Protocol Lengti Ini HTTP 136 GE HTTP 205 HT 205 HTTP 205 HT 156 GE 1. HTTP 156 GE 1. HTTP 156 GE 1. HTTP 225 HT 3 HTTP 225 HT 888 bits) HTTP 225 HT 888 bits) tivaConne_6d:1d:8f 4 Seg: 1, Ack: 1, Len	Comparing
Frame 58: 136 bytes           Frame 58: 136 bytes           Ethernet II, Src: I	0004.pcapng apture Analyze Statistics (C) Q ← ← ← ← ← ← ← ← ← ← ← ← ← ← ← ← ← ←	<ul> <li>Telephony Wireless T</li> <li>■ ■ ■ ■ ■ ■ ■</li> <li>■ ■<td>Tools         Help           Image: Constraint of the second se</td><td>Image: Control of the state of the stat</td></li></ul>	Tools         Help           Image: Constraint of the second se	Image: Control of the state of the stat
Capit 20241023194954, C           e         Edit View Go (           e         Edit View Go (           it         ime           1,21374           http           http           http           http           ine           2,31374           66 9,279741           71 9,289016           72 9,289426           75 9,303391           80 9,358979           81 9,358979           81 9,358979           81 9,358979           1           Transmission Contro           Source Port: 524           Destination Port           Stimation Port	0004.pcapng apture Analyze Statistics (Conversion of the state of t	<ul> <li>Telephony Wireless T</li> <li>■ ■ ■ ■ ■ ■ ■</li> <li>■ ■</li></ul>	Tools         Help           Image: Constraint of the second se	Composition of the set of the se
cap42.20241023194954_C         cap42.20241023194954_C           e         Edit View Go ()           e         Edit View Go ()           http            http            http            http            http <td>0004,pcapng apture Analyze Statistics (C) Q ← ← ← ① (C) Source 10.0.0.25 23.217.9.9 2601:280:5f00:1aff 2601:280:5f00:1aff 2601:280:5f00:1aff 2601:1280:5f00:1aff 2600:1405:7400:b: 2600:1405:74</td> <td>Telephony Wireless T     Destination     23.217.9.9     10.e.0.25     Control 1005:7400:b:     Control 1005:7400:b:     12601:1405:7400:b:     12601:280:5f00:1af6     L2601:280:5f00:1af6     L2601:280     L460:200     L4600:200     L4600     L46</td> <td>Cools         Help           Image: Constraint of the state of t</td> <td>0         7         0         7          7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7           7</td>	0004,pcapng apture Analyze Statistics (C) Q ← ← ← ① (C) Source 10.0.0.25 23.217.9.9 2601:280:5f00:1aff 2601:280:5f00:1aff 2601:280:5f00:1aff 2601:1280:5f00:1aff 2600:1405:7400:b: 2600:1405:74	Telephony Wireless T     Destination     23.217.9.9     10.e.0.25     Control 1005:7400:b:     Control 1005:7400:b:     12601:1405:7400:b:     12601:280:5f00:1af6     L2601:280:5f00:1af6     L2601:280     L460:200     L4600:200     L4600     L46	Cools         Help           Image: Constraint of the state of t	0         7         0         7          7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7         7           7
Capit 20241023194954_C           e         Edit View Go (           it         Jie (           it	0004.pcapng apture Analyze Statistics (C) Q ← ← ← ① (C) Source 10.0.0.25 23.217.9.9 2601:280:5700:1aff 2601:280:5700:1aff 2601:280:5700:1aff 2601:280:5700:1aff 2601:1280:5700:1aff 2600:1405:7400:b: 2600:1405:7	Telephony Wireless T     Destination     23.217.9.9     10.0.0.25     10.2600:1405:7400:b:    2600:1405:7400:b:    2600:1405:7400:b:    2601:280:5f00:1af0	Cods Help Protocol Length Init HTTP 136 GE HTTP 205 HT 205 HTTP 205 HT 156 GE 1. HTTP 156 GE 2. HTTP 156 GE 2. HTTP 225 HT 2. HTTP 225 HT 2. HTTP 225 HT 2. HTTP 225 HT 2. HTTP 225 HT Seg: 1, Ack: 1, Len	<pre></pre>
Capit 20241023194954.c           e         Edit View Go ()           it         View Go ()           75 9.303301         S 9.356979           81 9.356979         S 356979           81 9.356979         S 356979           81 9.356979         S 356979           91 9.356979         S 356979           92 9.356979         S 356979           93 9.356979         S 356979           93 9.356979         S 356979           94 9.356979         S 356979           93 9.356979         S 356979           93 9.356979         S 356979           94 9.356979         S 356979           95 0.070707         S 356979           95 0.070707         S 356979      <	0004.pcapng apture Analyze Statistics (C) Q ← ← ← ① (C) Source 10.0.0.0.25 23.217.9.9 2601:280:5F00:1aff 2601:280:5F00:1aff 2601:280:5F00:1aff 2601:280:5F00:1aff 2601:280:5F00:1aff 2600:1405:7400:b: 2600:1405:	<ul> <li>Telephony Wireless T</li> <li>Destination</li> <li>23.217.9.9</li> <li>10.e. 0.25</li> <li>2602:1405:7400:b::</li> <li>2602:1405:7400:b::</li> <li>2602:1280:5f00:1af6</li> <li>2601:280:5f00:1af6</li> <li>2601:</li></ul>	Cools         Help           II         III           Protocol         Length           HTTP         136           HTTP         265           HTTP         156           II         TTP           III         156           III         156           III         TTP           III         156           IIII         156           IIII         156           IIII         156           IIIII         156           IIIIIIII         156           IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	<pre></pre>
Frame 58: 136 bytes Ethernet II, Src: I Internet Protocol V Transmission Control V Source Protocol V Transmission Control Source Protocol V Transmission Contro Source Protocol V Source Protocol V Transmission Contro Source Protocol V Source Protoco	0004.pcapng apture Analyze Statistics (C) (Q) (Q) (Q) (Q) (Q) (Q) Source 18.0.0.25 23.217.9.9 2601:280:5F00:1aff 2601:280:5F00:1aff 2601:280:5F00:1aff 2600:1405:7400:b: 2600	<ul> <li>Telephony Wireless T</li> <li>Destination</li> <li>23.217.9.9</li> <li>10.0.0.25</li> <li>2600:1405:7400:b::</li> <li>2600:1405:7400:b::</li> <li>2600:1280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>250:51:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601</li></ul>	ioods         Help           II         III           Protocol         Lengtl           HTTP         136           HTTP         205           IT         III           III         III           III         156           III         III           IIII         IIII           IIII         IIIIIIII           IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Co T /ncc.txt HTTP/1.1 TP/1.1 200 OK (text/html) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 TP/1.1 200 OK (text/html) TP/1.1 200 OK (text
Frame 58: 136 bytes Ethernet II, Src: I Internet Protocol V Transmission Control V Source Number: Sequence Number: Network Sequence Number: N	0004.pcapng apture Analyze Statistics (apture Analyze S	<ul> <li>Telephony Wireless T</li> <li>Destination</li> <li>23.217.9.9</li> <li>10.0.0.25</li> <li>2600:1405:7400:b::</li> <li>2600:1405:7400:b::</li> <li>2600:260:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2501:280:5700:1af6</li> <li>32.478, Dst Port: 88,</li> <li>WITH_DATA (31)]</li> <li>ace number)</li> <li>2 sequence number)]</li> </ul>	cods         Help           II         III           Protocol         Lengtl           HTTP         136           HTTP         205           HTTP         156           II         TTP           E         HTTP           HTTP         156           II         HTTP           E         HTTP           III         156           III         TP           E         HTTP           III         III           E         HTTP           III         III           III         III           E         HTTP           225         HT           E         HTTP           225         HT           E         HTTP           225         HT           E         HTTP           225         HT           Seq: 1, Ack: 1, Len	Co T /ncc.txt HTTP/1.1 TP/1.1 200 OK (text/html) T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 T /ncc.txt HTTP/1.1 TP/1.1 200 OK (text/html) TP/1.1 200 OK
Frame 58: 136 bytes Frame 58: 136 bytes Ethernet II, Src: I Internet Protocol V Frame 58: 136 bytes Ethernet II, Src: I Internet Protocol V Frames 58: 136 bytes Ethernet II, Src: I Internet Protocol V Framsuission Contro Conversation contro [Stream Index: 2] Sequence Number: Sequence N	0004.pcapng apture Analyze Statistics (apture Analyze Statistics (apture Analyze Statistics Source 10.0.0.25 23.217.9.9 2601:280:5F00:1aff 2601:280:5F00:1aff 2601:280:5F00:1aff 2600:1405:7400:b: 2700:7400:5400:5400:5400:5400:5400:5400:5	<ul> <li>Telephony Wireless T</li> <li>Destination</li> <li>23.217.9.9</li> <li>10.0.0.25</li> <li>2600:1405:7400:b:</li> <li>2600:1405:7400:b:</li> <li>2600:260:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>2601:280:5700:1af6</li> <li>32478, Dst Port: 88,</li> <li>WITH_DATA (31)]</li> <li>ace number)</li> <li>sequence number)]</li> </ul>	Cods Help Protocol Lengti Ini HTTP 136 GE HTTP 205 HT 156 GE L. HTTP 156 GE L. HTTP 156 GE L. HTTP 156 GE L. HTTP 225 HT E. HTTP 225 HT E. HTTP 225 HT Seq: 1, Ack: 1, Len	0     Image: Control of the second state of the second stat

## Part 5 - Top Talkers, Profiles, and Graphs

### Objective 5.1

1. Determine Top Talkers on the network. [10 points]

Top Talkers in the network were determined by going to statistics and click on conversations.

	A 4 4 4		0 0 0	77 L .											
Wireshark - Conversations - wires	hark onj 2.1 captu	ure 11q&12q.pcap	ong											- 0	×
Conversation Settings	Ethernet -	4 IPv4 · 6	IPv6 · 4 TO	P·5 UD	0P · 13										
Name resolution	Address A	Address B	Packets	Bytes Stre	am ID	$Packets\;A\toB$	Bytes A $ ightarrow$ B	$Packets\;B\toA$	Bytes $B \rightarrow A$	Rel Start	Duration	$Bits/s\;A\toB$	Bits/s B $\rightarrow$ A		
Absolute start time	10.0.0.1	239.255.255.250	20	11 kB	2	20	11 kB	0	0 bytes	5.032798	0.1030	823 kbps	0 bits/s		
🗌 Limit ta dianlas filtas	10.0.0.25	192.0.2.1	4 290	bytes	1	4	296 bytes 247 bytes	0	0 bytes	1.175058	14.6544	101 Dits/s	0 bits/s		
Cirnic to display litter	10.0.0.25	13.67.10.228	3 224	bytes	4	2	139 bytes	1	85 bytes	24.572610	0.2501	4446 bits/s	2718 bits/s		
-	10.0.0.25	20.42.144.52	2 121	bytes	3	1	55 bytes	1	66 bytes	23.303464	0.0463	9511 bits/s	11 kbps		
Сору •	34.75.3.10	10.0.0.25	2 108	bytes	5	1	54 bytes	1	54 bytes	28.869421	0.0002				
Follow Stream															
Graph															
. ^															
Protocol															
Bluetooth															
DCCP															
Ethernet															
FC															
FDDI															
IEEE 802.11															
IEEE 802.15.4															
ilter list for specific type															
													Close	e H	lelp
							0090	00 00 00 00	00 b4 00 0	00 00 00	00 00 0	00 00 00 00			
							00a0	00 00 00 00	00 00 01 0	1 c4 50	9c 6d 1	d 8f 15 03		• P • m • • • •	
							00-0	00 01 00 01							
							00b0 00c0	80 01 00 01 03 6e 65 74	03 70 76 6	4 0/63	6f 6d 6	3 61 /3 /4	net	·comcast	
			_				00b0 00c0	80 01 00 01 03 6e 65 74	00 00	4 0/63	6† 6d 6	3 61 /3 /4	net	·comcast	

 What are two ways you can determine what device/IP address is transmitting the most traffic on the network? Provide a screenshot of one of those ways. (Hint: Protocol Hierarchy; Conversations; Endpoints) [10 points]

	wireshark onj 2.1 ca	apture 11q&12q.pcapng											- 0	×
Fi	le Edit View	Go Capture Analyze Statistics Telephony Wireless	Tools Help	)										
	. 🔳 🧟 🔘 🖿	Wireshark · Protocol Hierarchy Statistics · wireshark onj 2.1 c	capture 11q8	12q.pcapng							- 0	ı x		
	Apply a display fil	Protocol	Percer	nt Packets	Packets	Percent Byte	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs	<ul> <li>IP traffic</li> </ul>	HTTP GET
No	o. Time	✓ Frame		100.0	55	100.	1461	3897	0	0	0	55		
	1 0.00000	✓ Ethernet		100.0	55	5.3	770	205	0	0	0	55		
	2 1.17565	<ul> <li>Internet Protocol Version 6</li> </ul>		34.5	19	5.2	760	202	0	0	0	19	)	
	3 1.29801	<ul> <li>Transmission Control Protocol</li> </ul>		7.3	4	0.6	92	24	2	52	13	4		
	4 2.96710	Transport Layer Security	I.	1.8	1	0.2	28	7	1	28	7	1		
	5 5.03279	Data		1.8	1	0.0	1	0	1	1	0	1		
	6 5.03279	Internet Control Message Protocol v6		27.3	15	11.7	1704	454	15	1704	454	15		
	7 5.03279	<ul> <li>Internet Protocol Version 4</li> </ul>		58.2	32	4.4	640	170	0	0	0	32		
	8 5.03279	<ul> <li>User Datagram Protocol</li> </ul>		38.2	21	1.1	168	44	0	0	0	21		
	9 5.03279	Simple Service Discovery Protocol		36.4	20	66.8	9762	2602	20	9762	2602	20		
	10 5.03279	<ul> <li>NetBIOS Datagram Service</li> </ul>		1.8	1	0.6	82	21	0	0	0	1		
	11 5.03279	<ul> <li>SMB (Server Message Block Protocol)</li> </ul>		1.8	1	0.8	123	32	0	0	0	1		
	12 5.03279	<ul> <li>SMB MailSlot Protocol</li> </ul>		1.8	1	0.2	25	6	0	0	0	1		
	13 5.03279	Microsoft Windows Browser Pro	otocol	1.8	1	0.3	37	9	1	37	9	1		
	14 5.03279	<ul> <li>Transmission Control Protocol</li> </ul>		12.7	7	1.0	152	40	5	112	29	7		
	15 5.11862	Transport Layer Security		3.6	2	0.4	62	16	2	62	16	2		
	16 5.12355	Internet Control Message Protocol		7.3	4	1.1	160	42	4	160	42	4		
1		Address Resolution Protocol		7.3	4	0.8	112	29	4	112	29	4		
>	Frame 1: 198												P .m	
>	Ethernet II,												• • • • • • • P	
>	Internet Prot													
>	Internet Cont													
		No display filter.											• • • • • • • • •	
								<i>c</i> 1					• •,•••&•	
								Close	Сору	Proto	cols •	Help		
						00a0 00	00 00 00 00	00 01	01 c4 50	9c 6d 1d	8f 15 03		· .P.m	
						00b0 80	01 00 01 03	70 76	64 07 63	6f 6d 63	61 73 74	····•pv	′d ∙comcast	
_						00c0 03	6e 65 74 00	00				·net··		
														0
0	🔰 🗶 wireshark o	onj 2.1 capture 11q&12q.pcapng						Pack	ets: 55				Pro	ofile: Default
	<b>\$</b>	📕 Q 🖬 🤇	<b>i</b>	🖪 C	) 📜 (	<b>4</b> 🗘	C 🔮	w			~ @	) 🗇 ଦ	9:43 21/10/2	2024 Q

Two ways to determine the top talkers are through conversations or through protocol hierarchy. The above screenshot is done using protocol hierarchy.

#### **Objective 5.2**

- 1. Create a graph that displays the top 4 protocols from the capture.
- 2. Provide screenshot of the graph. [10 points]





<b>_</b> \	wireshark onj 2.1 captur	e 11q&12q.pcapng										- 0	×
File	e Edit View Go	Capture Analyze	🚄 Wireshark · I/O	Graphs · wiresharl	onj 2.1 capture 11q	&12q.pcapng					) ×		
1	🔳 🖉 🕥 🚞 🗎	X C											
	Apply a display filter	<ctrl-></ctrl->			Wireshark	: I/O Graphs: wii	reshark onj 2.1 c	apture 11q&12q.pca	png			+ IP traffic	HTTP GET
	roppy a applay meet m	- Curry -		ł								- In cruine	
NO.	. Time	Source	2 packe	ts -						1 sec Inter	vals		
	1 0.000000	te80::c650:9ct							Λ	tcp			
	2 1.1/5058	10.0.0.25		-								)	_
	5 1.298014	10.0.0.25	15 packet										
	4 2.96/101	10.0.0.1		~ -					1				
	6 5 032798	10.0.0.1	Sec	[									
	7 5 032798	10.0.0.1	ts/1	-									
	9 5 022758	10.0.0.1	3 1 packe	ts -									
	9 5 032798	10.0.0.1	Pa	-									
	10 5 032798	10.0.0.1		-									
	11 5 032798	10.0.0.1	500 mpacket										
	12 5.032798	10.0.0.1		-									
	13 5.032798	10.0.0.1		[									
	14 5 032798	10.0.0.1		-									
	15 5.118624	10.0.0.1	0 packe	is Literation in the second	-5			5	10	15			
	16 5.123553	10.0.0.1			5	0	Tim	., 	10	15			
		_						ic (3)				-	
>	Frame 3: 247 byte:	s on wire (1976 b:	No packets in interval	'Os).								· · · = A · · E ·	
Ś	Ethernet II, Src:	Intel d6:3d:41 (	Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y7		
>	Internet Protocol	Version 4, Src: :		TCP Errors	tcp.analysis.flags		Bar	Packets		None	1	-\	
>	User Datagram Prot	tocol, Src Port: :		Filtered packets	http		Line	Packets		None	1		
>	NetBIOS Datagram	Service	Ū.	udp .	udp		Line	Packets		None	1	C A . FHEPF	- 1
>	SMB (Server Messag	ge Block Protocol		arro	arp		Line	Packets		None		E PFFFACAC	- 1
>	SMB MailSlot Prote	ocol		icmp	icmp	-	Line	Packots		None		C ABN ··· SMB	
>	Microsoft Windows	Browser Protocol		ten	temp		Line	Packets		None	1		
				цср	tcp		Line	Fackets		None			- I
												• • • • • • 6	
			+		use 🔿 drags 🔿 7	ome Interval	1 sec 🗸 🗍		a scale 🔽 Automa	tic undate 🔽 Enak	le legend	L OT BROWS	
						Joins Interval	1300		g scale a Automa		ne legena	DESKTOP	
0	wireshark onj 2.	1 capture 11q&12q.pca	Reset				S	ave As Cop	Copy from	Close	Help	Pro	ofile: Default
	4				nii 💼 4		-76	n 🙋 👼		A #		9:56	PM O
-	-			· · · · ·		-				. 6	4 4 40	21/10/3	2024

## Objective 5.3

1. Create three profiles that you will use for future analysis objectives. For example,

Security, Troubleshooting, VoIP, etc. [10 points]

🛋 *Wi-f	7										-	0	×
File E	dit View Go Ca	pture Analyze Statistics	Telephony Wireless T	ools Help									
	/ @ = 🗅 🕅	T T T + D		Ξ									
			<u> </u>										٦.
Cum	ent filter: tcp												• +
No.	Time	Source	Destination	Protocol	Lengtł Info								=.
	1 0.000000	10.201.49.16	173.194.206.188	TCP	55 54178 → 443	[ACK] S	Seq=1 Ack=	1 Win=510	Len=1				
	2 0.015126	173.194.206.188	10.201.49.16	TCP	66 443 → 54178	[ACK] :	Seq=1 Ack=	2 Win=1047	Len=0 SLE=1 SRE=2				_
	3 0.142048	10.201.49.16	20.42.144.52	TCP	55 54179 → 443	[ACK] 3	Seq=1 Ack=	1 Win=512	Len=1				
	4 0.170842	20.42.144.52	10.201.49.16	TCP	66 443 → 54179	[ACK] :	Seq=1 Ack=	2 Win=251	Len=0 SLE=1 SRE=2				
	7 4.866357	10.201.49.16	152.199.4.33	TCP	55 54206 → 443	[ACK] :	Seq=1 Ack=	1 Win=512	Len=1				
	8 4.870495	152.199.4.33	10.201.49.16	TCP	66 443 → 54206	[ACK] S	Seq=1 Ack=	2 Win=146	Len=0 SLE=1 SRE=2				
	9 5.358663	10.201.49.16	204.79.197.239	TCP	55 54207 → 443	[ACK] S	Seq=1 Ack=	1 Win=512	Len=1				
	10 5.363339	204.79.197.239	10.201.49.16	TCP	66 443 → 54207	[ACK] :	Seq=1 Ack=	2 Win=1638	6 Len=0 SLE=1 SRE=2				
	90 5.979395	10.201.49.16	142.250.72.35	TCP	66 54210 → 443	[SYN] S	Seq=0 Win=	64240 Len=	0 MSS=1460 WS=256 SACK	_PERM			
	97 5.983355	142.250.72.35	10.201.49.16	TCP	66 443 → 54210	[SYN, /	ACK] Seq=0	Ack=1 Win	=65535 Len=0 MSS=1250	SACK_PERM WS=25	6		
	98 5.983608	10.201.49.16	142.250.72.35	TCP	54 54210 → 443	[ACK] S	Seq=1 Ack=	1 Win=1310	72 Len=0				
	99 5.985188	10.201.49.16	142.250.72.35	TCP	1304 54210 → 443	[ACK] S	Seq=1 Ack=	1 Win=1310	72 Len=1250 [TCP PDU n	eassembled in 1	00 ]		
	100 5.985188	10.201.49.16	142.250.72.35	TLSV1.3	534 Client Hello	(SN1=)	beacons.gc	p.gvt2.com	) 1 A-b 1 bi- 20024		CDE 1701		
a Free	101 3.992334	142.230.72.33	10.201.49.16			97#1	443 7 342	10 ACK 3	eq=1 ACK=1 W11=209024	00	SKC=1/51		_
> Fran	ne 3405: 310 Dyte	s on wire (2480 bits)	, 310 bytes captured	(2480 D1TS)	on interface 0000	0 a0 e	18 5c 39 40	00 00 00	00 00 0a c9 31 10 36	ed (\9@			1.1
> Ethe	ernet II, Src: In	tel_d6:3d:41 (cc:d9:a	C:06:30:41), DST: C15	CO_04:Da:80	(a0:e0:a1:04 0020	e2 a	4 fa 23 00	50 c5 02	ff c1 c5 48 68 7a 50	18 ···#·P···	· · · HhzP ·		- 1
> Inte	ernet Protocol ve	Protocol Crc Dont	49.16, DST: 54.257.22	6.164 Sec. 1 Ack	0030	04 0	0 56 85 00	0 00 47 45	54 20 2f 66 61 76 69	63 ··· V ··· GE T	/favic		- 1
> Inar	artext Transfer P	rotocol	04055, DSt POPt: 00,	Sed: 1, MCK	.: 1, Len: 250 0040	6f 6	e 2e 69 63	3 6f 20 48	54 54 50 2f 31 2e 31	0d on.ico H T	TP/1.1		- 1
> nyp	er cext in ansier Pi	100001			0050	2d 4	13 50 55 30	20 41 4d	20 2a 2T 2a 00 0a 55 44 36 34 0d 0a 41 63	41 Accept: 63 -CPU: AM D	064 · · Acc		- 1
					0070	65 7	0 74 2d 45	6 6e 63 6f	64 69 6e 67 3a 20 67	7a ept-Enco d	ling: gz		- 1
					0086	69 7	70 2c 20 64	4 65 66 6c	61 74 65 0d 0a 55 73	65 ip, defl a	te Use		- 1
					0090	72 2	d 41 67 65	6e 74 3a	20 4d 6f 7a 69 6c 6c	61 r-Agent:	Mozilla		- 1
					00a6	2+3	4 2e 30 2e	28 63 61	60 70 61 74 69 62 6c	65 /4.0 (com	patible A: Wind		- 1
					0000	6f 7	7 73 20 4e	20 37	2e 32 3b 20 57 69 6e	36 OWS NT 6 .	2: Win6		- 1
					00de	34 3	b 20 78 36	5 34 3b 20	54 72 69 64 65 6e 74	2f 4; x64; T	'rident/		- 1
					00e0	37 2	le 30 3b 20	2e 4e 45	54 34 2e 30 43 3b 20	2e 7.0; .NE T	4.0C; .		
					0010	9 4e 4	5 54 34 26	2 30 45 3b	20 54 61 62 66 65 74	20 NET4.0E;	Tablet		
					0110	65 7	4 66 6c 69	78 2e 63	6f 6d 0d 0a 43 6f 6e	6e etflix.co	m··Conn		
07	wireshark Wi-FiCHT	7V2 pcappg							Packets: 12393 - Displayed: 10	935 (88 2%) · Dronne	-d: 0 (0.0%)	Pro	file: TCP
					-		-		denetal lease bispidyed. It.	ses (see of broppe			
R			Q 🖬 🥠 📫	1 🖪 🌔	) 📜 🖆 🕻		0	×	S 🖉	∧ ∅ ⊕ ⊄	25	8:49 AM 5/10/2024	Q

🚄 *Wi-Fi					- 0	×
File Edi	t View Go Cap	ture Analyze Statistics	Telephony Wireless To	ols Help		
🛋 🔳 🖉	1 🐵 🚞 🛅 🕅	🙆 🤇 🗢 🕈 🖀 🐔	<u>* 📃 📃 @ @ @ }</u>	1 12		
Curren	it filter: dns					- +
No.	Time	Source	Destination	Protocol Ler	ıgti Info	
_►	11 5.754257	10.201.49.16	128.138.129.76	DNS	74 Standard query 0x16b9 A www.google.com	
	12 5.754513	10.201.49.16	128.138.129.76	DNS	74 Standard query 0x371b HTTPS www.google.com	
ęL_	13 5.765782	128.138.129.76	10.201.49.16	DNS 1	90 Standard query response 0x1609 A www.google.com A 142.250.72.68	
	29 5.803903	10.201.49.16	128.138.129.76	DNS	81 Standard query 0x65f0 A wpad.int.colorado.edu	
	30 5.805793	128.138.129.76	10.201.49.16	DNS 1	146 Standard query response 0x65f0 No such name A wpad.int.colorado.edu SOA boulder.colorado	
	54 5.929363	10.201.49.16	128.138.129.76	DNS	80 Standard query 0x24ed A beacons.gcp.gvt2.com	
	55 5.930733	10.201.49.16	128.138.129.76	DNS	80 Standard query 0x5b9d HTTPS beacons.gcp.gvt2.com	
	56 5.933461	10.201.49.16	128.138.129.76	DNS	80 Standard query 0xa065 A beacons.gcp.gvt2.com	
	57 5.933664	128.138.129.76	10.201.49.16	DNS 1	126 Standard query response 0x24ed A beacons.gcp.gvt2.com CNAME beacons-handott.gcp.gvt2.com	
	59 5.934267	10.201.49.16	128.138.129.76	DNS .	80 Standard query 0x677a HTTPS beacons.gcp.gvt2.com	
	60 5.936357	128.138.129.76	10.201.49.16	DNS 1	126 Standard query response 0xa065 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com	
	65 5.939825	128.138.129.76	10.201.49.16	DNS :	178 Standard query response 0x677a HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2	
> Frame > Ether > Inter > User > Domai	: 11: 74 bytes or net II, Src: Int net Protocol Ver Datagram Protoco n Name System (c	wire (592 bits), 74 er_de6:33:41 (cc:d9:a sion 4, Src: 10.201. 1, Src Port: 64259, uuery)	bytes captured (592 t c:d6:3d:41), Dst: Ci36 49.16, Dst: 128.138.12 Dst Port: 53	pits) on inter :o_04:ba:80 (a 19.76	face (Dev)       0000 a0 e0 af 04 ba 80 cc d9 ac d5 30 41 08 00 45 00	
2	wireshark_Wi-FiCHT7	V2.pcapng	Q 🖬 🤣 🏺	<b>0</b>	Packets: 12393 · Displayed: 298 (2.4%) · Dropped: 0 (0.0%) Packets: 12393 · Displayed: 298 (2.4%) · Dropped: 0 (0.0%) Profi	ile: DI
udp.pca File Edi	ap t View Go Cap	ture Analyze Statistics	Telephony Wireless To	ols Help	- 0	×
	1 🛛 🗀 🗋 🕅	🙆 । ९ 🗢 🕈 著 🐔	* 📃 📃 @ @ @ }	1 7 7		_
Apply	a display filter <ctr< td=""><td>-/&gt;</td><td></td><td></td><td></td><td>- +</td></ctr<>	-/>				- +
No.	Time	Source	Destination	Protocol Le	ingti Info	
	1 0.000000	10.200.203.136	10.200.203.255	UDP	74 52207 → 33890 Len=32	
	2 0.002812	142.250.69.234	10.200.202.202	UDP	120 443 → 49704 Len=78	
	3 0.006177	10.200.202.202	142.250.69.234	UDP	75 49704 → 443 Len=33	
	5 0 206705	10.200.201.70	255.255.255.255	UDP	8/ 1046 → 1046 LEN=45 74 52280 → 33890 Len=32	
	6 0.212873	10.200.202.202	142.250.69.234	UDP	71 49704 → 443 Len=29	
	7 0.216320	10.200.202.57	239.255.255.250	SSDP	213 M-SEARCH * HTTP/1.1	
	8 0.230423	142.250.69.234	10.200.202.202	UDP	67 443 → 49704 Len=25	
	9 0.305663	10.200.200.129	239.255.255.250	UDP/XML	698 64913 → 3702 Len=656	
	10 0.305663	10.200.203.45	10.200.203.255	NBNS	92 Name query NB BRNB42200410B2B<00>	
	11 0.436380	10.200.202.202	142.250.69.234	UDP	71 49704 → 443 Len=29	
	13 0.613396	10.200.203.136	10.200.203.255	UDP	74 52210 → 33890 Len=32	_
Frame Ether Inter User Data	e 1: 74 bytes on net II, Src: Int net Protocol Ver Datagram Protoco (32 bytes)	wire (592 bits), 74 el_5f:b0:31 (38:fc:9 sion 4, Src: 10.200. l, Src Port: 52207,	bytes captured (592 bi 8:5f:b0:31), Dst: Broa 203.136, Dst: 10.200.2 Dst Port: 33890	its) Wdcast (ff:ff: 103.255	0000         ff ff ff ff ff ff ff 38 fc 98 5f b0 31 08 00 45 00	
2	udp.pcap		o <b>a</b> -		Packets: 330 Profi	ile: L

# Explain what you would use each profile for, what you changed, and provide a screenshot of one of them. [10 points]

TCP Profile: Useful for analyzing transmission control protocol traffic, including connection establishment, termination and packet retransmission. The profile is ideal for troubleshooting issues related to reliable data transmission.

UDP Profile: Since UDP is connectionless and suitable for real-time applications such as monitoring packet loss in VoIP calls or detect incorrect configuration in services like DHCP.

DNS Profile: Specifically for analyzing DNS traffic, which includes queries, responses. The profile is used for diagnosing DNS resolution issues, such as misconfigured DNS servers, slow responses.

#### Part 6 - DHCP Release and Renew

#### **Objective 6.1**

- 1. Start Wireshark and begin capture
- 2. Release the DHCP IP address your machine has obtained
- 3. Renew the DHCP IP address (for your machine to obtain a new address)
- 4. After your machine receives an IP address from the DHCP server, stop the capture
- 5. Filter the capture to only show the DHCP traffic. From the capture indicate the following:

#### i. DHCP server address [2 points]

DHCP server address is 10.0.0.25.

- ii. The IP address your machine was offered and accepted [2 points]The IP address the machine was offered and accepted is 10.0.0.25. SinceI'm running the DHCP server in the same machine as the DHCP client it is giving the same IP address.
- iii. Explain the DHCP process, include a screenshot [10 points]

🚄 *Wi-Fi				- 0 ×	
File Edit View Go Capture Analyze Statisti	cs Telephony Wireless Tool	s Help			
🧸 🔳 🖉 🐵 🚞 🛅 🕱 🙆 🔍 👄 🋸 🖀 🐐	ં 🛃 📃 લ લ લ 🎹	1			
Bootp				▲ 🖬 📼 🔹 +	
No. Time Source	Destination	Protocol Lengtł Info			
23 9.643047 0.0.0.0	255.255.255.255	DHCP 370 DHCP Reques	t - Transaction ID 0xfcd169d		
56 11.487596 0.0.0.0	255.255.255.255	DHCP 370 DHCP Reques	t - Transaction ID 0xfcd169d		
93 14.195255 10.0.0.25	10.0.0.1	DHCP 342 DHCP Releas	e - Transaction ID 0x3e2419ea		
171 16.922071 0.0.0.0	255.255.255.255	DHCP 350 DHCP Discov	er - Transaction ID 0x73436da7		
184 17.182529 0.0.0.0	255.255.255.255	DHCP 350 DHCP Discov	er - Transaction ID 0xa000ca85		
451 20.280827 10.0.0.1	10.0.25	DHCP 359 DHCP Offer	- Transaction ID 0xa000ca85		
452 20.283348 0.0.0.0	255.255.255.255	DHCP 376 DHCP Reques	t - Transaction ID 0xa000ca85		
453 20.291468 10.0.0.1	10.0.25	DHCP 399 DHCP ACK	- Transaction ID 0xa000ca85		
1890 32.289918 10.0.0.25	10.0.0.1	DHCP 364 DHCP Reques	t - Transaction ID 0xb2a655b		
1891 32.298820 10.0.0.1	10.0.25	DHCP 399 DHCP ACK	- Transaction ID 0xb2a655b		
> Frame 1891: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interfi b Ethernet II, Src: VantivaConne_6d:1d:sf (c4:50:9c:6d:1d:sf), Dst: Intel_6d:3d:41 (ct) Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.25          00000       cc d9 ac d6 3d 41 c4 50       9c 6d 1d 8f 08 00 45 c0					
		011	0 00 00 00 00 00 00 63 82 53 63 35 01 05 36 04 0a	·····c· Sc5··6··	
wireshark_Wi-FiQRNTV2.pcapng			Packets: 2277 · Displayed: 10 (0.4%	- Dropped: 0 (0.0%) Profile: ICMP	
<i></i>	📕 Q 🖬 🥠	🏟 🖪 O 📮 🛙	😤 🕼 😋 🗳 🖷 🧕 🖉		

DHCP does DORA process.

Discover: The client sends a DHCP Discover packet to find available DHCP servers.

Offer: The DHCP server responds with an offer packet, offering an IP address to the client.

Request: The client responds with a Request packet, requesting the IP address from the DHCP server.

Acknowledgment: The DHCP server sends an ACK packet to confirm that the IP address has been leased to the client.

## Part 7 – Web traffic (HTTP) and TCP Connection

#### **Objective 7.1**

- 1. Start Wireshark and select the appropriate interface to begin capturing packets.
- 2. Go to <u>http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html</u> in your browser and capture the web session on Wireshark.
- 3. How is the TCP connection established? Explain the process. What is it called? Locate it in your Wireshark capture. Paste relevant screenshots. **[5 points]**

- The TCP connection establishment process is known as three-way handshake. It provides reliable connection between the client and server. The steps are :
- SYN: The client sends a SYN (synchronize) packet to the server, indicating the desire to open a connection and specifying the initial sequence number (Seq = X).
- SYN-ACK: The server responds with a SYN-ACK (synchronize-acknowledge ) packet, acknowledging its own sequence number(ISN) and acknowledgement number (ISN+1).
- ACK: The clients send an ACK packet to the server, confirming the connection (ACK= ISN + 1)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	- +
	<b>*</b> +
	-+
	- +
No. Time Source Destination Protocol Lengt Info	
46 2.290565 2603:1036:2407:1::29 2601:280:5f00:1af0: TCP 74 443 → 57758 [ACK] Seq=1 Ack=29 Win=49153 Len=0	
88 13.592743 10.0.0.25 128.119.245.12 TCP 66 57902 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
89 13.654589 128.119.245.12 10.0.0.25 TCP 66 80 → 57902 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128	
90 13.654832 10.0.0.25 128.119.245.12 TCP 54 57902 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0	
91 13.757813 10.0.0.25 128.119.245.12 HTTP 624 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
95 13.760615 10.0.0.25 128.119.245.12 TCP 66 57903 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
110 13.836343 128.119.245.12 10.8.8.25 10 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
111 13.855551 10.0.0.25 128.119.245.12 (CP 54.5/985 + 80 [Atk] 580±1 ACK=1 WIDHEISISZ8 LEH=0	
112 13:030001 120:113:245:12 10:0:0:25 ICF 34:00 7 5/302 [ACK] 54(41-1044) Letter	
13 13 13 636001 120 110 (100 110 100 120 11) 110 245 12 TCP 54 5700 0 (LEX/ILLING VAR) 120 120 120 120 120 120 120 120 120 120	
127 13 98363 10 0 25 128 119 245 12 HTTP 485 6FT / 60 (not, ) 642/57 HTTP 485 6FT / 1	
128 13.971838 128.119.245.12 10.0.0.25 HTTP 538 HTTP/1.1 404 Not Found (text/html)	
129 14.021314 10.0.0.25 128.119.245.12 TCP 54 57902 → 80 [ACK] Sea=1002 Ack=923 Win=130304 Len=0	
> Internet Protocol Version 4, Src: 10.0.0.25, Dst: 128,119,245,12 0000 c4 50 9c 6d 1d 8f cc d9 ac d6 3d 41 08 00 45 00 Prm·····=A··E·	
✓ Transmission Control Protocol, Src Port: 57992, Dst Port: 80, Seq: 0, Len: 0 0010 00 34 b2 6f 40 00 80 06 00 00 00 00 01 80 77 4 00 ·······W	
Source Port: 57902	
Destination Port: 80	
[Stream index: 4]	
[Stream Packet Number: 1]	
> [Conversation completeness: Complete, WITH_DATA (31)]	
[TCP Segment Len: 0]	
Sequence Number: 0 (relative sequence number)	
Sequence Number (raw): 2708121731	
[Next Sequence Number: 1 (Pelative sequence number)]	
Acknowledgment Number: 0	
Acknowledgment humber (raw). 0	
1000 Header Length. 22 bytes (b)	
P Transmission Control Protocol: Protocol	file: ICMP
	me retvir
	M 🐥

- 4. Inspect information within the first packet of the TCP connection process.
  - i. What is the destination port number? How would you classify it? [1 point]

The destination port number is 80, which is the default port for HTTP. It is classified as well-known port which permanent and assigned for a application protocol.

ii. Which control flag (or flags) is set? What does it imply? [1 point]

The SYN flag is set in the first packet, it implies that this is packet is part of the initial connection request, starting the TCP three-way handshake.

#### iii. What is the relative sequence number set to? [1 point]

The relative sequence number in the first packet is 0, which marks the start of the sequence for this TCP connection.

5.Inspect the next packet in the TCP connection process.

#### i. Which control flag (or flags) is set? What do they imply? [1 point]

The control flags set in this packet are SYN and ACK, these flags together imply that the server is responding to the client's SYN request, providing its own sequence number and acknowledging the client with Sequence number +1.

ii. What is the relative sequence number and relative acknowledgement number set to? [1 point]

The relative sequence number in this packet is 0. This is the server's Initial Sequence Number (ISN). The relative acknowledgment number is 1. This means that the server is acknowledging the client ISN by adding 1 which was 0 initially and expects the client to have a sequence number 1.

#### 6. Finally, inspect the third packet of the connection process.

i. Which control flag (or flags) is set? What do they imply? [1 point]

The ACK flag is set, it implies that client is acknowledging the servers SYN-ACK packet. This means that the client has received the servers sequence number and acknowledges it therefore completing the three-way handshake and the connection is established.

## ii. What is the relative sequence number and relative acknowledgement number set to? What do they imply? [1 point]

The relative sequence number in this packet is 1. This indicates that the client has incremented its sequence number by 1 after the initial SYN packet and is now ready to start sending data.

Relative Acknowledgement Number is 1. This implies that the client has received the servers initial sequence number and is acknowledging it by sending Ack = 1.

 In your Wireshark Capture display only the HTTP (Web) traffic. (Paste screenshot). [5 points]

•Wi-Fi File Edit View Go Capture Analyze Statistics	Telephony Wireless Too	ls Help					-	0	×
▲ ■ 2 ♥ <mark>=</mark> : 2 ♥ ¬ ♥ ₩ ₽ .   http								×	- +
No.         Time         Source           91         13.757813         10.0.25           113         13.816661         128.119.245.12           127         13.982663         128.119.245.12           128         13.971838         128.119.245.12           566         25.269759         2601.280.5760:1.4697.880           569         25.87616         2667.7680:4067.883           599         25.301863         2667.7680:4067.883	Destination 128.119.245.12 10.0.0.25 128.119.245.12 10.0.0.25 2607:f8b0:400f:803: 2607:f8b0:400f:803: 2607:f8b0:400f:803: 2601:280:5f00:1af0:	Protocol         Lengtl         II           HTTP         624 G         6           HTTP         495 H         6           HTTP         485 G         6           HTTP         538 H         1           HTTP         256 H         6           HTTP         226 G         6           HTTP         226 H         226 H	fo TT /wireshar TTP/1.1 200 TT /favicon. TTP/1.1 404 TT /r/gsr1.c TTP/1.1 304 TTP/1.1 304	<pre>rk-labs/INTRO-wi OK (text/html) ico HTTP/1.1 Not Found (tex rl HTTP/1.1 Not Modified HTTP/1.1 Not Modified</pre>	ireshark-fi ) xt/html)	lel.html HTTP/1.1			
<ul> <li>&gt; Frame 91: 624 bytes on wire (4992 bits),</li> <li>&gt; Ethernet II, Src: Intel_d6:3d:41 (cc:d9:a)</li> <li>&gt; Internet Protocol Version 4, Src: 10.0.0.;</li> <li>&gt; Transmission Control Protocol, Src Port: 1</li> <li>&gt; Source Port: 57962</li> <li>Destination Port: 80</li> <li>[Stream index: 4]</li> <li>[Stream Facket Number: 4]</li> <li>&gt; [Conversation completeness: Complete, 4]</li> <li>[TCP Segment Len: S70]</li> <li>&gt; Sequence Number: 10(relative sequence Sumber: 10(relative sequence Number: 10(relative sequence Number: 571)</li> <li>(Rext Sequence Number: 1)</li> <li>(relative addressed)</li> <li>Weptext Transfer Protocol</li> </ul>	524 bytes captured (49 ::d6:3d:41), Dst: Vant: 25, Dst: 128.119.245.1: 77902, Dst Port: 80, Sr WITH_DATA (31)] :e number) p sequence number)] tock number)	12 bits) on inter vaConne_6d:1d:8f ; q; 1, Ack: 1, Ler	Saci         00000           (c')         0010           0020         0030           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           00400         00400           01400         01400	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	d 8f cc d9 e 00 80 66 e 50 a1 65 d 6c 61 622 0 45 54 e 65 65 70 1 65 65 7 65 66 7 65 66 1 7 65 1 7 7 7 65 1 7 65 1 7 65 1 7 7 7 7 65 1 7 7 7 7 7 65 1 7 7 7 65 1 7 7 7 7 65 1 7 7 7 65 1 7 7 7 7 7 65 1 7 7 7 7 7 65 1 7 7 7 65 1 7 7 7 7 7 65 1 7 7 7 7 7 65 1 7 7 7 7 7 65 1 7 7 7 7 7 7 65 1 7 7 7 7 7 65 1 7 7 7 7 7 7 65 1 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	ac d6 3d 41 68 00 $\frac{15}{10}$ 66 00 00 0a 00 69 19 80 77 38 44 52 77 69 72 65 72 73 24 49 48 45 24 76 64 20 24 77 69 72 64 52 64 23 10 40 a4 52 64 72 64 23 10 40 a4 52 64 72 64 23 10 40 a4 53 72 64 23 10 40 a4 55 73 32 64 97 36 56 33 72 65 73 32 64 36 77 65 64 69 49 66 73 65 63 75 72 65 73 32 64 36 77 65 26 46 99 66 46 77 73 22 46 98 73 32 09 64 46 77 73 29 96 64 46 77 73 72 46 57 69 66 33 34 30 20 76 65 57 65 56 36 75 77 73 20 64 55 76 55 46 86 72 67 66 72 92 04 36 77 73 20 73 20 64 55 74 65 63 75 76 65 67 20 20 43 68 72 67 66 cackets 511 - Displayed: 8 (1.6%)	P.m. =A.	Profil	le: ICMP

 Examine the HTTP request packet. What is the destination IP address and destination port number? Which TCP control flag (or flags) is set, and what do they mean? Paste relevant screenshots. [5 points]

The Destination IP address is 128.119.245.12 and the destination port number is 80. ACK flag is set, it implies that client is acknowledging the server's previous message and is ready for communication. After acknowledging the handshake with the ACK flag, the client is now making an HTTP GET request to retrieve a specific resource.

🖌 "Wi-Fi File Edit View Co. Capture Analyze Statistics Telephony Wiselace Technology	- 0 X
No. Time Source Destination	Protocol Lengti Info
→ 91 13.757813 10.0.0.25 128.119.245.12	HTTP 624 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
<pre>91 13.72/613 10.00.25 120.119.49.12 113.13.836661 128.119.245.12 10.00.25 127 13.988563 10.0.0.25 128.119.245.12 128 13.971838 128.119.245.12 10.0.0.25 506 25.269739 2601:280:5f00:1af0: 2607:f8b0:400f:803 508 25.287616 2607:f8b0:400f:803 2601:280:5f00:1af0 509 25.306107 2601:280:5f00:1af0 2607:f8b0:400f:803 510 25.319863 2607:f8b0:400f:803 2601:280:5f00:1af0 510 25.319863 2607:f8b0:400f:803 2601:280:5f00:1af0 520 25.287616 (2007) 510 25.319863 2607:f8b0:400f:803 2601:280:5f00:1af0 510 25.319863 2607:f8b0:400f:803 2601:280:5f00:1af0 520 25.500:c0 2005:500 c0 520 2500:c0 2005:500 c0</pre>	hTP       624 GeT / Waresmark-1203/AN NO-AREsmark-T162.html HTP/1.1         HTP       495 GET / favicon.ico HTTP/1.1         HTTP       495 GET //r/gsrl.crl HTTP/1.1         HTTP       296 HTTP/1.1 304 Not Modified         bits) on interfact.       0000 cd 50 get fall 000 get 26 get 27 140 00 80 06 00 00 00 00 19 80 77       br q0
Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 134499001 0101 = Header Length: 20 bytes (5) > Flags: 0x018 (PSH, ACK) Windows S13 [Calculated window size: 131328] [Window size scaling factor: 256]	0100       35       33       32       22       38       42       28       44       54       44       42       20       c5       c5       12       33       32       22       38       52       64       58       56       57       32       36       26       36       57       56       d17       14       68       26       56       15       32       39       28       30       22       30       23       56       66       12       12       30       28       30       22       30       23       56       66       12       47       30       28       30       22       30       26       30       28       30       28       30       28       30       28       30       28       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       26       30       27
◯ Z Hypertext Transfer Protocol: Protocol	Packets: 511 · Displayed: 8 (1.6%) · Dropped: 0 (0.0%) Profile: ICMP
🗳 📑 Q Search 🚈 🖬 🥠	📫 🖪 🚫 🏣 🚭 🕼 😢 🧬 🚄 🥦 💆 🔹 🗞 🗞 🗞 🕫 🕩 🔒

- 9. Examine the HTTP packets and answer the following questions
  - i. What HTTP version is running on the client? What version of HTTP is the server running? [2 points]

The client is running HTTP/1.1 as seen in the request packet and HTTP server version is also running HTTP/1.1.

ii. What is the status code returned from the server to your browser? [1 point]

The status code returned from the server is 200 OK.

iii. When was the HTML file that you are retrieving last modified at the server? [1 point]

The If- Modified-Since field in the HTTP request indicates that the client is requesting a file that may have been modified since Mon, 21 Oct 2024 05.59:01 GMT. The actual Last-Modified date from the server is Tue, 22 Oct 2024 05:59:01 GMT.

🚄 *Wi-Fi			- 0 ×
File Edit View Go Capture Analyze Statistics Telephor	ony Wireless Tools Help		
🚄 🔳 🖉 🐵 🖿 🛅 🗙 🙆 🍳 👄 🔿 🖀 🛒 👤 🌉	📄 @, @, @, 🏦 🔡		
http			× +
No. Time Source Destir	ination Protocol Lengtl Info		
→ 91 13.757813 10.0.0.25 128.1	119.245.12 HTTP 624 GET	/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
113 13.836661 128.119.245.12 10.0.	.0.25 HTTP 492 HTTP,	(1.1 200 OK (text/html)	
127 13.908363 10.0.0.25 128.1	119.245.12 HTTP 485 GET ,	favicon.ico HTTP/1.1	
128 13.971838 128.119.245.12 10.0.	0.0.25 HTTP 538 HTTP,	(1.1 404 Not Found (text/html)	
506 25.269739 2601:280:5†00:1a†0: 2607:	:+860:400+:803: HTTP 276 GET ,	r/gsrl.crl HTTP/1.1	
508 25.28/616 260/:T800:400T:805: 2601: 509 25 306107 2601:280:5f00:1af0: 2607:	.:280:5100:1410: HIIP 296 HIIP,	1.1 304 NOT MODIFIED	
510 25.319863 2607:f8b0:400f:803: 2601:	:280:5f00:1af0: HTTP 296 HTTP	1.1 304 Not Modified	
<pre>[Checksum Status: Unverified] Urgent Pointer: 0 &gt; [Timestamps] &gt; [SEQ/ACK analysis] TCP payload (438 bytes) &gt; Hypertext Transfer Protocol &gt; HTTP/1.1 200 0K\r\n Date: Wed, 23 Oct 2024 04:54:23 GMT\r\n Server: Apache/2.4.6 (CantOS) OpenSSL/1.0.2k-f Last-Modified: Tue, 22 Oct 2024 05:59:01 GMT\r ETag: "51-6250a7750544d"\r\n Accept-Ranges: bytes\r\n Accept-Ranges: bytes\r\n Accept-Ranges: bytes\r\n Content-Length: 81\r\n Keep-Alive: timeout=5, max=100\r\n Content-Type: text/html; charset=UTF-8\r\n \r\n [Request in frame: 91] [Time since request: 0.078848000 seconds] [Request URI: /wireshark-labs/INTRO-wireshark-</pre>	fips PHP/7.4.33 mod_perl/2.0.11 Perl r\n -file1.html]	0070         65         72         3a         20         41         70         61         63         68         65         27         32         2a         34         2a         56         67         44         75         32         2a         34         2a         55         53           0080         42         27         32         2a         34         2a         56         66         57         72         53         33           0080         62         71         2a         82         82         82         82         82         56         57         2a         54         82         83         32         86         66         67         77         72         56         57         2a         54         82         82         82         82         82         82         82         82         82         82         82         82         82         82         2a         84         83         82         22         84         83         83         83         83         83         83         83         83         83         83         83         83         83         83         83 <td< td=""><td>er: Apac he/2.4.6 (CentOS ) OpenSS [J.10.2k - fips PH P/7.4.33 mod_per J/2.0.11 PerJ/v5 1.6.3 · L ast-Modi fied: Tue, 2.2 Oc t 2024 Ø 5:59:01 GMT-ETag : "51-6 250a7750 544d" · A ccept-Ra nges: by tes · Content-Len gith: 81 · Keep-Al jve: tim eout=5, max:100 · Connect ion: Kee p-Alive- Content -Type: t ext/html; charse tuTF-8 · .chnl &gt; Congra tulation Si You' ve downl oaded th e first Nireshark Lab fi le! </td></td<>	er: Apac he/2.4.6 (CentOS ) OpenSS [J.10.2k - fips PH P/7.4.33 mod_per J/2.0.11 PerJ/v5 1.6.3 · L ast-Modi fied: Tue, 2.2 Oc t 2024 Ø 5:59:01 GMT-ETag : "51-6 250a7750 544d" · A ccept-Ra nges: by tes · Content-Len gith: 81 · Keep-Al jve: tim eout=5, max:100 · Connect ion: Kee p-Alive- Content -Type: t ext/html; charse tuTF-8 · .chnl > Congra tulation Si You' ve downl oaded th e first Nireshark Lab fi le!
HTTP Last Modified (http.last_modified), 46 bytes		Packets: 511 · Displayed: 8 (1.6%) · Dro	pped: 0 (0.0%) Profile: ICMP
92° 🕂 C	२ 🖬 🤣 🏟 🖪 💽	📮 📽 🍳 🤨 🦉 💻 👰 👘 🔨	

iv. How many bytes of content are being returned to your browser? [1 point]492 bytes of content were returned by the server to the client based on the response packet.

# Can you see the text displayed on the browser in your Wireshark packets as well? Why/why not? Paste relevant screenshots. [5 points]

Yes, you can see the text displayed on the browser in the Wireshark packets if it is transmitted in an unencrypted form. In the case of HTTP, which operates under plaintext and does not use encryption. So, we can see both client and the response returned by the server, including any HTML content. HTTP traffic is not encrypted, so it is visible to see the actual HTML text, headers when we capture. The TCP payload highlighted in blue in that the content is visible.

🚄 *Wi-Fi	- 0 ×
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Hel	p
📕 🖩 🖉 💿 🐂 🖺 🖉 🍳 କ 🔿 🖀 🐺 👤 📃 🔍 Q. Q. X 🗄 🔛	
📙 http	
No. Time Source Destination Proto	col Lengti Info
→ 91 13.757813 10.0.0.25 128.119.245.12 HTTP	624 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
- 113 13.836661 128.119.245.12 10.0.0.25 HTTP	492 HTTP/1.1 200 OK (text/html)
127 13.908363 10.0.0.25 128.119.245.12 HTTP	485 GET /favicon.ico HTTP/1.1
128 13.971838 128.119.245.12 10.0.0.25 HTTP	538 HTTP/1.1 404 Not Found (text/html)
506 25.269739 2601:280:5†00:1a†0: 2607:†8b0:400†:803: HTTP	276 GET /r/gsrl.cri HTTP/.1
508 25.28/616 260/:T800:400T:803: 2601:280:5700:1470: HTTP 509 25 306107 2601:280:5500:1550: 2607:58b0:4005:803: HTTP	256 HIP/1.1 364 NOT MODITIED 274 GET (b/c4 cc) HITD/1 1
510 25.319863 2607:f8b0:400f:803: 2601:280:5f00:1af0: HTTP	296 HTTP/1.1 304 Not Modified
<pre>[Checksum Status: Unverified] Urgent Pointer: 0 &gt; [Timestamps] &gt; [SEQ/ACK analysis] TCP payLoad (438 bytes) VHypertext Transfer Protocol &gt; HTTP/1.1 200 0K/r/n Date: Wed, 23 Oct 2024 04:54:23 GMT/r/n Server: Apache/2.4.6 (CentOS) OpenSL/1.0.2k-fips PHP/7.4.33 mod_pe [Last-Modified: Tue, 22 Oct 2024 05:59:01 GMT/r/n ETag: "51-62508775044d"r/r/n Accept-Ranges: bytes/r/n &gt; Contert-Length: 81/r/n Keep-Alive: timeouts, max=100/r/n Connection: Keep-Alive/r/n Contert-Type: text/htl; charst=UTF-8\r/n /r/n [Request in frame: 91] [Time since request: 0.078848000 seconds] [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]</pre>	<ul> <li>er: Apac he/2.4.6</li> <li>er: Apac he/2.4.6</li> <li>er: Apac he/2.4.6</li> <li>er: Apac he/2.4.6</li> <li>(Centos ) OpenSS</li> <li>(Centos ) OpenSS</li></ul>
○ Z HTTP Last Modified (http.last_modified), 46 bytes	Packets: 511 · Displayed: 8 (1.6%) · Dropped: 0 (0.0%) Profile: ICMP
🗳 📑 Q 🖬 🧖 📫	📴 💽 📜 省 🕼 😧 🧳 🥖 🧰 🎽 🔹 ^ 🗞 🗞 🖗

## Part 8 – Parsing .pcap using Python [Extra Credit]

#### **Objective 8.1**

1. Start a new capture in Wireshark using the capture filter of 'icmp'. Open the command prompt/terminal and execute these commands -

ping -4 google.com

ping wellsfargo.com

[Use -c 4 option if pinging from MAC.]

- 2. Stop the capture and save the file as .pcap.
- 3. Write a script using Python that parses the saved .pcap file and prints out only the source and destination IPs of each packet of the file sequentially. You can use the Python library pcapfile for this purpose

[https://pythonhosted.org/pypcapfile/installing.html]. [20 points]

Total Score = \_\_\_\_/291 [+20 Extra Credit]