Old Dominion University

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment 1.2: Basic Wireshark Practice

Jordan Sustarsic

- Use Wireshark to capture and save ALL related packets when you ping the URL "<u>www.odu.edu</u>".
 - Locate the DNS queries and responses in the traffic.

	IS						
).	Time	Source	Destination	Protocol	Length Info		
	14 6.308170	192.168.1.8	192.168.1.1	DNS	77 Standard que	ry 0x5851 A	beacons4.gvt2.com
	15 6.326320	192.168.1.1	192.168.1.8	DNS	93 Standard que	ry response	0x5851 A beacons4.
	59 6.913599	192.168.1.8	192.168.1.1	DNS	71 Standard quer	y Øxce54 A	www.odu.edu
	60 6.939802	192.168.1.8	192.168.1.1	DNS	/1 Standard quer	у 0хсе54 А	www.odu.edu
	01 0.040771	172.100.1.1	192.100.110	0115		y response	UNCCOT A MINIOUSIC
_							
	wireshark_Wi-Fi4	WC190.pcapng					

The IP address of the server is: 192.168.1.1

• What information is answered from the DNS server?

It gives us the host name's associated IP address

	Wi-Fi							
File	Edit View Go	Capture Analyze Sta	tistics Telephony Wireles	s Tools H	lelp			
	n src==192 168 1 8 88			<u>ч н</u>				
	p.arc==152, 100, 1.0 da	Course	Deeller	Destand	1			
NO.	rime	Source	Destination	Protocol	Length Into		11 0.0001	12/2220
	62 0.900045	192.100.1.0	120.02.112.29	TCMP	74 Echo (ping) request	id=0x0001,	seq=15/5526
	64 7.900039	192.100.1.0	120.02.112.29	TCMP	74 Echo (ping) request	id=0x0001,	5eq=15/3940
	74 10 003816	192.108.1.8	128 82 112 29	TCMP	74 Echo (ping) request	id=0x0001,	seg=16/4096
0	wireshark_Wi-Fi4	WC 190.pcapng						
	ク Type her	e to search	0	Ħ 🤇	S 🖬 💼 🕯	a	₩ ≯	1

• Apply the proper display filter in Wireshark to show ICMP requests.

• Apply the proper display filter in Wireshark to show ICMP responses.

о.		1.1		+28024V	122 1335 CO15462			
	Time	Source	Destination	Protocol	Length Info		193	
	63 6.974193	128.82.112.29	192.168.1.8	ICMP	74 Echo (pi	ing) reply	id=0x0001,	seq=13/3328
	65 7.987233	128.82.112.29	192.168.1.8	ICMP	74 Echo (pi	ing) reply	id=0x0001,	seq=14/3584
	09 0.999495 70 10 004107	120.02.112.29	192.100.1.0	TCMP	74 Echo (p)	ing) reply	id=0x0001,	seq=15/3640
	/ 10.02410/	120.02.112.25	132.100.170	IC.	74 ceno (p.	ing) (cpi)	10-000001,	304-10/403

• Show the Protocol Hierarchy Statistics of the traffic.

🚄 Wireshark · Protocol Hierarchy Statistics · Wi-Fi

 ✓ Frame 100.0 146 100.0 54109 30k 0 0 ✓ Ethernet 100.0 146 3.8 2044 1139 0 0 ✓ User Datagram Protocol 45.9 67 1.0 536 298 0 0 QUIC IETF 39.0 57 43.1 23341 13k 54 19759 Domain Name System 3.4 5.5 8 2.0 1057 599 1057 Transmission Control Protocol 47.3 69 46.7 25248 14k 45 14135 Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 26429 14k 23 26429 24 24k 25 26429 14k 23 26429 2	Bytes Bits/s End Packets End Bytes End Bits/	Bytes	Percent Bytes	Packets	Percent Packets	Protocol
✓ Ethernet 100.0 146 3.8 2044 1139 0 0 ✓ Internet Protocol Version 4 100.0 146 5.4 2928 1633 0 0 ✓ User Datagram Protocol 45.9 67 1.0 536 298 0 0 QUIC IETF 39.0 57 43.1 23341 13k 54 19759 Domain Name System 3.4 5 0.3 189 105 5 189 Data 5.5 8 2.0 1057 59 8 1057 × Transmission Control Protocol 47.3 69 46.7 25248 14k 45 14135 Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 Data 0.7 1 0.0 1 0 1 1 Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 Internet Con	54109 30k 0 0 0	54109	100.0	146	100.0	Y Frame
 ✓ Internet Protocol Version 4 100.0 146 5.4 2928 1633 0 0 QUIC IETF 39.0 57 43.1 23341 13k 54 19759 Domain Name System 3.4 5 0.3 189 105 189 1057 589 1057 132 144 14135 14135 144 14135 14135 144 144 145 14135 144 145<td>2044 1139 0 0 0</td><td>2044</td><td>3.8</td><td>146</td><td>100.0</td><td>✓ Ethernet</td>	2044 1139 0 0 0	2044	3.8	146	100.0	✓ Ethernet
✓ User Datagram Protocol 45.9 67 1.0 536 298 0 0 QUIC IETF 39.0 57 43.1 23341 13k 54 19759 Domain Name System 3.4 5 0.3 189 105 5 189 Data 5.5 8 2.0 1057 589 8 1057 Transmission Control Protocol 47.3 69 446.7 25248 14k 45 14135 Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 Data 0.7 1 0.0 1 0 1 1 Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 Internet Control Message Protocol 5.5 8 0.6 320 178 8 320	2928 1633 0 0 0	2928	5.4	146	100.0	 Internet Protocol Version 4
QUIC IETF 39.0 57 43.1 23341 13k 54 19759 Domain Name System 3.4 5 0.3 189 105 5 189 Data 5.5 8 2.0 1057 589 8 1057 * Transmission Control Protocol 47.3 69 46.7 25248 14k 45 14135 Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 Data 0.7 1 0.0 1 0 1 1 Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 Internet Control Message Protocol 5.5 8 0.6 320 178 8 320	536 298 0 0 0	536	1.0	67	45.9	 User Datagram Protocol
Domain Name System 3.4 5 0.3 189 105 5 189 Data 5.5 8 2.0 1057 589 8 1057 * Transmission Control Protocol 47.3 69 46.7 25248 14k 45 14135 Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 Data 0.7 1 0.0 1 0 1 1 Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 Internet Control Message Protocol 5.5 8 0.6 320 178 8 320	23341 13k 54 19759 11k	23341	43.1	57	39.0	QUIC IETF
Data 5.5 8 2.0 1057 589 8 1057 ✓ Transmission Control Protocol 47.3 69 46.7 25248 14k 45 14135 Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 Data 0.7 1 0.0 1 0 1 1 Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 Internet Control Message Protocol 5.5 8 0.6 320 178 8 320	189 105 5 189 105	189	0.3	5	3.4	Domain Name System
 ✓ Transmission Control Protocol 47.3 69 46.7 25248 14k 45 14135 Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 14k 2429 14k 23 26 26 26 26 26 26 26 27 26 28 29 26 26 27 26 26 26 26 26 26 27 26 26 27 26 28 29 26 26<	1057 589 8 1057 589	1057	2.0	8	5.5	Data
Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 Data 0.7 1 0.0 1 0 1 1 Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 Internet Control Message Protocol 5.5 8 0.6 320 178 8 320	25248 14k 45 14135 7883	25248	46.7	69	47.3	 Transmission Control Protocol
Data 0.7 1 0.0 1 0 1 1 Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 Internet Control Message Protocol 5.5 8 0.6 320 178 8 320	26429 14k 23 26429 14k	26429	48.8	23	15.8	Transport Layer Security
Internet Group Management Protocol1.420.0168216Internet Control Message Protocol5.580.63201788320	1 0 1 1 0	1	0.0	1	0.7	Data
Internet Control Message Protocol 5.5 8 0.6 320 178 8 320	16 8 2 16 8	16	0.0	2	1.4	Internet Group Management Protocol
	320 178 8 320 178	320	0.6	8	5.5	Internet Control Message Protocol

- Use Wireshark to capture and save ALL related packets when you visit the URL <u>www.odu.edu</u> in a new Incognito window. Stop capturing after the ODU website is fully loaded.
 - Locate all DNS queries and responses after you open the website and highlight the DNS query for the ODU website.

dr	ns									
No.	Time	Source	Destination	Protocol	Length	Info				
-	20 6.438296	192.168.1.8	192.168.1.1	DNS	71	Standard	query	0x7f5a A	www.odu.e	du
1	21 6.453751	192.168.1.1	192.168.1.8	DNS	87	Standard	query	response	0x7f5a A	www.odu.ed
	47 6.723597	192.168.1.8	192.168.1.1	DNS	75	Standard	query	0xc359 A	code.jque	ery.com
	49 6.725698	192,168.1.8	192.168.1.1	DNS	80	Standard	query	0x3209 A	fonts.goo	gleapis.co
	50 6.726507	192.168.1.8	192.168.1.1	DNS	79	Standard	query	0xf506 A	kit.fonta	wesome.com
	53 6.728747	192.168.1.8	192.168.1.1	DNS	83	Standard	query	0xd577 A	maxcdn.bo	otstrapcdr
	74 6.762143	192.168.1.1	192.168.1.8	DNS	96	Standard	query	response	0x3209 A	fonts.goog
	82 6.762870	192.168.1.1	192.168.1.8	DNS	163	Standard	query	response	0xf506 A	kit.fontav
	83 6.762870	192.168.1.1	192.168.1.8	DNS	143	Standard	query	response	0xc359 A	code.jquer
	84 6.762870	192.168.1.1	192.168.1.8	DNS	115	Standard	query	response	0xd577 A	maxcdn.boo
	471 7.075896	192.168.1.8	192.168.1.1	DNS	77	Standard	query	0x10d0 A	hello.myt	onts.net
	525 7.097569	192.168.1.1	192.168.1.8	DNS	109	Standard	query	response	0x10d0 A	hello.myfo
	802 7.216849	192.168.1.8	192.168.1.1	DNS	80	Standard	query	0x06f9 A	ka-p.font	awesome.co
-	803 7 246224	192 168 1 8	192 168 1 1	DNS	88	Standard	nuerv	AVARTA A	ka-n font	awesome co
> 0	ser Datagram Prot omain Name System	tocol, Src Port: 620	32, Dst Port: 53							
∨ D		n (query)								
✓ D	Transaction ID:	n (query) : 0x7f5a								
~ D	Transaction ID: Flags: 0x0100 S	n (query) : 0x7f5a Standard query								
~ D	Transaction ID: Flags: 0x0100 S Questions: 1	m (query) : 0x7f5a Standard query								
ם ~ ג	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0	m (query) : 0x7f5a Standard query								
• D	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs:	m (query) : 0x7f5a Standard query 0								
> D	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs:	m (query) : 0x7f5a Standard query 0 : 0								
ם י י	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries	m (query) : 0x7f5a Standard query 0 : 0								
ם י י	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu:	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN								
> D >	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu: [Response In: 2	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN 21]								
> D >	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu: [Response In: 2	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN 21]								
ם `	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu: [Response In: 2	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN 21]								
ם ~ د	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu: [Response In: 2	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN 21]								
ם ~ د	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries www.odu.edu: [Response In: 2	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN 21]								
• • •	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu: [Response In: 2	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN 21]								
· D	Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu: [Response In: 2 Domain Name Sys	m (query) : 0x7f5a Standard query 0 : 0 type A, class IN 21] tem: Protocol								
· D	<pre>Transaction ID: Transaction ID: Flags: 0x0100 S Questions: 1 Answer RRs: 0 Authority RRs: Additional RRs: Queries > www.odu.edu: [Response In: 2 Domain Name Sys</pre>	<pre>m (query) : 0x7f5a itandard query 0 : 0 type A, class IN 21] tem: Protocol</pre>							• 4	

• How many other DNS queries have been captured after the ODU website is

loaded? Can you explain why this happens?

Too many other packets have been captured to count. I believe this happens due to all the other stuff linked to the odu site: ads, widgets, external links, etc....

• Combine what you have observed in the previous questions. Can you identify the widgets (external links) loaded on the ODU website?

Any of the social media capture would be since there are links to them on the main website: facebook, twitter, youtube, etc...

• Show the Protocol Hierarchy Statistics of the traffic.

*Wi-Fi											
Wireshark · Protocol Hierarchy Statist	ics · Wi-Fi										
Protocol	Percent Packets	Packets	Percent	Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bit	s/s	
✓ Frame	100.0	92	1	100.0	11055	21k	0	0	0		
✓ Ethernet	100.0	92	100	11.7	1288	2552	0	0	0		
Internet Protocol Version 4	100.0	92	1000	16.6	1840	3645	0	0	0		
 User Datagram Protocol 	100.0	92	1	6.7	736	1458	0	0	0		
Domain Name Syste	m 100.0	92	Ú.	65.0	7191	14k	92	7191	14k		
splay filter: dns											
			~	iiii (ee)	1 1			· · · ·	1		

• Study two Protocol Hierarchy Statistics in Task 1. f and Task 2.d, respectively. Explain the main differences between the two types of traffic.

When we pinged <u>www.odu.edu</u> there were less packets in the "User Datagram Protocol" than when we visited the site, so the DNS server was being used more when we visited the site due to all the external links connected to the website.

Also when we pinged the site in part 1, there was use of the "Transmission Control Protocol" as opposed to part two which did not include that at all. This means when we pinged the website we were trying to communicate with it and send messages over the network.