CISCO Academy

Lab - Exploring DNS Traffic

Objectives

Part 1: Capture DNS Traffic

Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Required Resources

• 1 PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

- a. Download the latest stable version of Wireshark from <u>www.wireshark.org</u>. Choose the software version you need based on your PC's architecture and operating system.
- b. Follow the on-screen instructions to install Wireshark. If you are prompted to install USBPcap, do NOT install USBPcap for normal traffic capture. USBPcap is experimental, and it could cause USB problems on your PC.

Step 2: Capture DNS traffic.

- a. Start Wireshark. Select an active interface with traffic for packet capture.
- b. Clear the DNS cache.
 - 1) In Windows, enter **ipconfig /flushdns** in Command Prompt.
 - For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd -Resolved, DNSMasq, and NSCD. If your Linux distribution does not use one of the listed utilities, please perform an internet search for the DNS caching utility for your Linux distribution.
 - (i) Identify the utility used in your Linux distribution by checking the status:

Systemd-Resolved: systemctl status systemd-resolved.service

DNSMasq: systemctl status dnsmasq.service

NSCD: systemctl status nscd.service

 (ii) If you are using system-resolved, enter systemd-resolve --flush-caches to flush the cache for Systemd-Resolved before restarting the service. The following commands restart the associated service using elevated privileges:

Systemd-Resolved: sudo systemctl restart systemd-resolved.service

DNSMasq: sudo systemctl restart dnsmasq.service

NSCD: sudo systemctl restart nscd.service

- 3) For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.
- c. At a command prompt or terminal, type **nslookup** enter the interactive mode.
- d. Enter the domain name of a website. The domain name <u>www.cisco.com</u> is used in this example.
- e. Type exit when finished. Close the command prompt.
- f. Click **Stop capturing packets** to stop the Wireshark capture.

Part 2: Explore DNS Query Traffic

a. Observe the traffic captured in the Wireshark Packet List pane. Enter udp.port == 53 in the filter box and click the arrow (or press enter) to display only DNS packets. Note: The provided screenshots are just examples. Your output maybe slightly different.

	*Etherr	et																_		×
<u>E</u> il	e <u>E</u> dit	<u>V</u> iew	<u>G</u> o <u>C</u>	apture	<u>A</u> naly	ze <u>S</u> ta	tistics	Teleph	ony	<u>W</u> irel	ess <u>T</u> e	ools	<u>H</u> elp							
		۲	010	K 🖸 🤇	₹ ∉	⇒ ≦	1	<u>}</u>		€. 0	2, ⊜,									
	udp.port ==53 Expression +																			
No	. Tim	e	Source	ce	۵	estinatio	n	Prot	ocol	Length	Info									
	16 8.5	597003	192.	168.1.1	6 1	92.168	.1.1	DNS		84	Stand	ard	query	0x00	01 P1	FR 1.1	.16	8.192.	in-addr	.arpa
	17 8.6	511953	192.	168.1.1	1	92.168	.1.16	DNS		161	Stand	ard	query	resp	onse	0x000)1 N	o such	name P	TR 1
_+	33 15.	952381	192.	168.1.1	61	92.168	.1.1	DNS		73	Stand	ard	query	0x00	02 A	www.c	isc	o.com		
⊸⊢	34 15	963198	192.	168.1.1	1	92.168	.1.16	DNS		254	Stand	ard	query	resp	onse	0x000	2 A	www.c	isco.co	m CN
	35 15	966100	192.	168.1.1	61	92.168	.1.1	DNS		73	Stand	ard	query	0x00	03 A4	AAA www	w.c	isco.co	om	
	36 15.	977273	192.	168.1.1	1	92.168	.1.16	DNS		294	Stand	ard	query	resp	onse	0x000)3 A	AAA www	w.cisco	.com
	-				150		72.1					••• •								
1	Frame	33: 73	bytes	on wire	(584	bits)	, /3 b	oytes	capt	ured	584 0	1ts)	on 11	itert	ace e	,	-	10.7		
1	Ethern	et II,	SFC: P	cssyste_	_09:1	4:64 (08:00:	27:09	:14:	(4), 1	JST: N	etge	ar_ea	D1:/	a (86	:::/:/	5:e	a:D1:/a	•)	
10	Intern User D	et Prot	OCOL V	ersion 4	+, Sr	.C: 197	.100.1	.10,	DSC:	192.1	100.1.	T								
10	Domain	Nomo S	vetor	(auony)	POI	1: 5//	29, 05	at Por												
1	Domain	Name 5	ystem	(query)																
-														(10.00			. (2			c
		rame (frar	me), 73 b	oytes						Pad	(ets: 49	· Disp	layed: 6	(12.24	‰)•Dr	opped:	0 (0.	.0%) P	ronie: De	rauit

- b. Select the DNS packet contains Standard query and A www.cisco.com in the Info column.
- c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

d. Expand Ethernet II to view the details. Observe the source and destination fields.

	🚄 *Ethernet — 🗆 🗙									
<u>F</u> i	e <u>E</u> dit <u>V</u> ie	v <u>e</u>	<u>5</u> o <u>C</u> apture <u>A</u> n	alyze <u>S</u> tatistics	Telephon <u>y</u>	<u>W</u> ireless <u>T</u> ools	<u>H</u> elp			
	🛋 🔳 🖉 🐵 📴 🕿 🖆 🔍 👄 🗢 🗟 🗿 🖢 🚍 📃 Q. Q. Q. X									
	udp.port == 53 Expression +									
No	Time		Source	Destination	Length Info					
	16 8.59700	3	192.168.1.16	192.168.1.1	84 Standard	query	0x0001 PTR 1.1.168.192.in-addr.	arpa		
	17 8.61195	3	192.168.1.1	192.168.1.16	DNS	161 Standard	query	response 0x0001 No such name PT	R 1	
>	33 15.9523	81	192.168.1.16	192.168.1.1	DNS	73 Standard	query	0x0002 A www.cisco.com		
*	34 15.9631	98	192.168.1.1	192.168.1.16	DNS	254 Standard	query	response 0x0002 A www.cisco.com	CN	
	35 15.9661	00	192.168.1.16	192.168.1.1	DNS	73 Standard	query	0x0003 AAAA www.cisco.com		
	36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com									
<u></u>	Ename 33: 73 butes on wine (584 bits) 73 butes cantured (584 bits) on interface 0									
Ú	Fehanet JI: José on Ware (584 bits), /S bytes captured (584 bits) on interface 0 Statement JI: See Decision (584 bits), /S bytes captured (584 bits) on interface 0									
	V Destinat	ion.	· Netgear each1	·7= (80·37·73·	aa•h1•7a)	(C4), D3C. NCCE	cui _cu			
	Addre		Netgear eath1:	7a (80.37.73.ez	a•h1•7a)					
	Addite		neegeen_eerbri	= 16 hit	t. Global	ly unique addr	ess (fa	actory default)		
			 a	= TG bit	t. Indivi	dual address (unicast	-)		
	× Source:	Dee	Sveta 00.14.c4	(08.00.27.09.1)	4.64)		unicus	-)		
	Addre		Presvete 09:14	·c4 (08.00.27.0	39·14·c4)					
	, autorite			= 16 hit	t. Global	ly unique addr	ess (fa	actory default)		
	- I G bit: Globally Unique address (unicath)									
	Type: Tpyd (4v4840)									
5	Type: 1794 (0x000)									
Ś	I lise net group Control - Src Parts 5720 - Dit Dorts 53									
Ś	> Domain Name System (query)									
-										
) 📝 🛛 Frame	frame	e), 73 bytes			Packets: 49 · Dis	played: 6	6 (12.2%) · Dropped: 0 (0.0%) Profile: Defa	ult 🔡	

What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

e. Expand Internet Protocol Version 4. Observe the source and destination IPv4 addresses.

File Edit View Go Capture Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Wireless Iools Help Image: Construct Analyze Statistics Telephony Statistics Telephony Statistics Iools Ioon Image: Con		*Ethern	et																	_			×
Image: Source Destination Protocol Length Info 16 8.597003 192.168.1.16 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa 17 8.611953 192.168.1.1 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa 13 15.952381 192.168.1.1 192.168.1.1 DNS 73 Standard query 0x0002 A www.cisco.com 34 15.963198 192.168.1.16 192.168.1.1 DNS 254 Standard query 0x0003 AAAA www.cisco.com 35 15.966100 192.168.1.16 192.168.1.16 DNS 254 Standard query response 0x0003 AAAA www.cisco.com 36 15.977273 192.168.1.1 DNS 294 Standard query response 0x0003 AAAA www.cisco.com 9100 = Version: 4 ONS 294 Standard query response 0x0003 AAAA www.cisco.com 92.168.1.16 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com 93 Internet Protocol Version 4, Src: 192.168.1.16, DNS 294 Standard query response 0x0003 AAAA www.cisco.com 94 Internet Protocol Version 4, Src: 192.168.1.16, DNS 294 Standard query response 0x0003 AAAA www.cisco.com 95	<u>F</u> ile	e <u>E</u> dit	View	<u>G</u> o	<u>C</u> aptu	re	Anal	yze	<u>S</u> tatistics	Те	elephon	<u>y W</u> ire	ess	<u>T</u> ools	<u>H</u> elp								
udp.port ==53 Expression + No. Time Source Destination Protocol Length Info 16 8.597003 192.168.1.16 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa 17 8.611953 192.168.1.1 192.168.1.1 DNS 161 Standard query response 0x0001 No such name PTR 1 33 15.952381 192.168.1.16 192.168.1.1 DNS 73 Standard query response 0x0002 A www.cisco.com 34 15.966100 192.168.1.16 DNS 254 Standard query vesponse 0x0003 AAAA www.cisco.com 35 15.966100 192.168.1.16 DNS 294 Standard query vesponse 0x0003 AAAA www.cisco.com 36 15.977273 192.168.1.16 DNS 294 Standard query vesponse 0x0003 AAAA www.cisco.com 10100 Version: 4 0101 Header Length: 20 bytes (5) 10 Differentiated Services Field: 0x00 DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) Flags: 0x000			0	010			२ 🤅	• •	2 👔	Ŧ		. ⊕	a, e	Q. 🎹									
No. Time Source Destination Protocol Length Info 16 8.597003 192.168.1.16 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa 17 8.611953 192.168.1.16 DNS 161 Standard query response 0x0001 No. name PTR 1 33 15.952381 192.168.1.16 DNS 73 Standard query 0x0002 www.cisco.com 34 15.965106 192.168.1.1 DNS 73 Standard query response 0x0002 www.cisco.com No. 35 15.966100 192.168.1.1 DNS 73 Standard query response 0x0002 A www.cisco.com No. 36 15.977273 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com V Internet Protocol Version: 4, Src: 192.168.1.16 DNS 294 Standard query response 0x0003<		udp.port ==53															>	< -		Expressio	n	+	
<pre>16 8.597003 192.168.1.16 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa 17 8.611953 192.168.1.1 192.168.1.16 DNS 161 Standard query response 0x0001 No such name PTR 1 33 15.952381 192.168.1.1 192.168.1.1 DNS 73 Standard query response 0x0002 A www.cisco.com 4 34 15.966100 192.168.1.1 192.168.1.1 DNS 73 Standard query response 0x0002 A www.cisco.com (NL. 35 15.966100 192.168.1.1 192.168.1.1 DNS 73 Standard query response 0x0003 AAA www.cisco.com 36 15.977273 192.168.1.1 192.168.1.1 DNS 73 Standard query response 0x0003 AAA www.cisco.com 7 Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) 9 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) 9 Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum status: Unverified] Source: 192.168.1.16 Destination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]</pre>	No.	No. Time Source Destination Protocol L										l Length	Infe	ō									
<pre>17 8.611953 192.168.1.1 192.168.1.16 DNS 161 Standard query response 0x0001 No such name PTR 1 33 15.952381 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0002 A www.cisco.com 34 15.963198 192.168.1.1 192.168.1.16 DNS 254 Standard query response 0x0002 A www.cisco.com 36 15.977273 192.168.1.1 192.168.1.1 DNS 73 Standard query 0x0003 AAAA www.cisco.com 36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com</pre> <pre> TInternet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum status: Unverified] Source: 192.168.1.1 Source GeoIP: Unknown] [Destination GeoIP: Unknown] </pre>		16 8.597003 192.168.1.16 192.168.1.1 DNS										84	Sta	andard	query	0x0001	PTI	R 1.1	.16	8.192	in-add	lr.a	rpa
<pre>33 15.952381 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0002 A www.cisco.com 34 15.963198 192.168.1.1 192.168.1.16 DNS 254 Standard query response 0x0002 A www.cisco.com CN 35 15.966100 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0003 AAAA www.cisco.com 36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com</pre> <pre> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 Ol00 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.16 Destination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] </pre>		17 8.6	11953	1	92.168	.1.1	L :	192.1	68.1.1	6	DNS	161	Sta	andard	query	respon	se (000x8	1 No	o sucl	n name	PTR	1
<pre> 4 34 15.963198 192.168.1.1 192.168.1.16 DNS 254 Standard query response 0x0002 A www.cisco.com CN 35 15.966100 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0003 AAAA www.cisco.com 36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com * Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum: 0x0000 [validation disabled] [Header checksum: 0x0000 [validation disabled] [Header checksum: 0x0000 [validation disabled] [Bestination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] </pre>		33 15.	952381	1	92.168	.1.1	.6	192.1	68.1.1		DNS	73	Sta	andard	query	0x0002	A	ww.c	isco	o.com			
<pre>35 15.966100 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0003 AAAA www.cisco.com 36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com</pre> * Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) > Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum status: Unverified] Source: 192.168.1.16 Destination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]	⊸⊢	34 15.	963198	1	92.168	.1.1	. :	192.1	68.1.1	6	DNS	254	Sta	andard	query	respon	se (000x6	2 A	www.	isco.	om	CN
<pre>36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com V Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum status: Unverified] Source: 192.168.1.16 Destination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]</pre>		35 15.	966100	1	92.168	.1.1	.6	192.1	68.1.1		DNS	73	Sta	andard	query	0x0003	AA	AA www	w.c	isco.	om		
<pre> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.16 Destination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] </pre>		36 15.	977273	1	92.168	.1.1	L :	192.1	68.1.1	6	DNS	294	Sta	andard	query	respon	se (000x8	3 A	AAA wa	w.ciso	c	om
<pre> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467) Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.16 Destination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] v </pre>																							
		<pre>0100 = Version: 4 0100 = Version: 4 0101 = Header Length: 20 bytes (5)) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x24fb (9467)) Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: UDP (17) Header checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.16 Destination: 192.168.1.1 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]</pre>											~										

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

f. Expand the User Datagram Protocol. Observe the source and destination ports.

_												
	🚄 *Ethernet — 🗆 🗙											
<u>E</u> il	e <u>E</u> dit <u>V</u> iew <u>G</u>	o <u>C</u> apture <u>A</u> na	lyze <u>S</u> tatistics	Telephony	<u>W</u> ireless <u>T</u> ools	<u>H</u> elp						
	📶 🔳 🖉 🔘 📙 🔚 🗙 🖆 I 9. 👄 🔿 🕸 🐨 🎍 🚍 🔚 9. 9. 9. 9. 19.											
	udp.port == 53 Expression +											
No.	Time	Source	Destination	Protocol	Length Info							
	16 8.597003	192.168.1.16	192.168.1.1	DNS	84 Standard	query	0x0001 PTR 1.1.168.192.in-addr.	.arpa				
	17 8.611953	192.168.1.1	192.168.1.16	DNS	161 Standard	query	response 0x0001 No such name PT	FR 1				
_	33 15.952381	192.168.1.16	192.168.1.1	DNS	73 Standard	query	0x0002 A www.cisco.com					
ℯ上	34 15.963198	192.168.1.1	192.168.1.16	DNS	254 Standard	query	response 0x0002 A www.cisco.com	n CN				
	35 15.966100	192.168.1.16	192.168.1.1	DNS	73 Standard	query	0x0003 AAAA www.cisco.com					
	36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com											
>	Frame 33: 73 by	rtes on wire (5	84 bits), 73 b	ytes capt	tured (584 bits)) on ir	iterface 0					
>	Ethernet II, Sr	c: PcsSyste_09	:14:c4 (08:00:	27:09:14	:c4), Dst: Netge	ear_ea:	b1:7a (80:37:73:ea:b1:7a)					
>	Internet Protoc	ol Version 4,	Src: 192.168.1	.16, Dst:	: 192.168.1.1							
~	User Datagram P	rotocol, Src P	ort: 57729, Ds	t Port: S	53							
	Source Port:	57729										
	Destination	Port: 53										
	Length: 39											
	Checksum: 0x839a [unverified]											
	[Checksum Status: Unverified]											
	[Stream index: 2]											
>	> Domain Name System (query)											
C	🔘 🝸 User Datagram Protocol (udp), 8 bytes 🛛 Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)											

What are the source and destination ports? What is the default DNS port number?

- g. Determine the IP and MAC address of the PC.
 - 1) In a Windows command prompt, enter **arp** –**a** and **ipconfig /all** to record the MAC and IP addresses of the PC.
 - 2) For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

h. Expand **Domain Name System (query**) in the Packet Details pane. Then expand the **Flags** and **Queries**.

i. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.

_ *I	Ethernet								_		×
<u>F</u> ile	<u>E</u> dit <u>V</u> iew (<u>5</u> o <u>C</u> apture	<u>A</u> nalyze	<u>S</u> tatistics	Telephony	<u>W</u> ireless	<u>T</u> ools	<u>H</u> elp			
		💼 🗙 🖾	۹ 👄 🖻	» 🗟 ү	₺ 🔳 🔳	€. €. (Q. 🎹				
📕 ud	udp.port ==53 Expression +										
No.	Time	Source	Desti	nation	Protocol	Length Inf	ò				
1	6 8.597003	192.168.1.3	16 192.	168.1.1	DNS	84 St	andard	query	0x0001 PTR 1.1.168.19	2.in-addr.	arpa
1	7 8.611953	192.168.1.	1 192.	168.1.16	DNS	161 St	andard	query	response 0x0001 No su	ch name PT	R 1
► 3	3 15.952381	192.168.1.3	16 192.	168.1.1	DNS	73 St	andard	query	0x0002 A www.cisco.co	m	
ال علم	4 15.963198	192.168.1.3	1 192.	168.1.16	DNS	254 St	andard	query	response 0x0002 A www	.cisco.com	n CN
3	5 15.966100	192.168.1.3	16 192.	168.1.1	DNS	73 St	andard	query	0x0003 AAAA www.cisco	.com	
3	6 15.977273	192.168.1.	1 192.	168.1.16	DNS	294 St	andard	query	response 0x0003 AAAA	www.cisco.	com
> In	ternet Proto	col Version	4, Src:	192.168.	1.16, Dst:	192.168	.1.1				^
> Us	er Datagram	Protocol, Sr	rc Port:	57729, 0	st Port: 5	3					
∨ Do	main Name Sy	stem (query))								
	[Response I	n: 34]									
	Transaction	ID: 0x0002									
~	Flags: 0x01	00 Standard	query								
	0		= Respon	ise: Mess	age is a q	uery					
	.000 0		= Opcode	: Standa	rd query (0)					
	0		= Trunca	ted: Mes	sage is no	t truncat	ted				
		1	= Recurs	ion desi	red: Do qu	ery recur	rsively				
		0	= Z: res	erved (0)						
		0	= Non-au	thentica	ted data:	Unaccepta	able				
	Questions:	1									
	Answer RRs:	0									
	Authority R	Rs: 0									
	Additional	RRs: 0									
~	Queries										
	✓ www.cisc	o.com: type	A, class	IN							
	Name:	www.cisco.c	om								
	[Name Length: 13]										
	[Label Count: 3]										
	Type: A (Host Address) (1)										
	Class	: IN (0x0001	.)								~
0	Z Domain Name	e System (dns), 3	31 bytes			Packets:	: 49 · Disp	layed: 6	(12.2%) · Dropped: 0 (0.0%)	Profile: Def	ault

Part 3: Explore DNS Response Traffic

a. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.

	*Ethern	et															_		×
Ei	le <u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> na	lyze g	<u>S</u> tatistics	Te	lephon	<u>W</u> irel	ess <u>T</u> o	ols	<u>H</u> elp						
		۲	010	🗙 🗋	٩ (⇔ ⇒	肇 👔	Ŧ		€ (
	udp.port ==53																		
No	. Time		Sou	urce		Destina	ation		Protoco	Length	Info								
	16 8.5	97003	19	2.168.1	.16	192.1	.68.1.1		DNS	84	Standa	nd	query	0x0001	PTR 1.1	1.16	8.192.	in-addr	.arpa
	17 8.6	11953	19	2.168.1	.1	192.1	.68.1.1	6	DNS	161	Standa	and	query	respons	e 0x000	01 N	o such	name P	TR 1
→	33 15.	952381	19	2.168.1	.16	192.1	.68.1.1		DNS	73	Standa	and	query	0x0002	A www.c	isc	o.com		
<u>مل</u>	34 15.	963198	19	2.168.1	.1	192.1	68.1.1	6	DNS	254	Standa	ind	query	respons	e 0x000	02 A	www.c	isco.co	n CN
	35 15.	966100	19	2.168.1	.16	192.1	68.1.1		DNS	73	Standa	ind	query	0x0003	AAAA ww	w.c	isco.co	om	
	36 15.	977273	19	2.168.1	.1	192.1	.68.1.1	6	DNS	294	Standa	ard	query	respons	e 0x000	93 A	AAA www	w.cisco	. com
>	Ename 3	34 · 254	1 hvte	es on wi	ire (2032 h	its)	254	hytes	cantur	ed (203	2 h	its) (n inter	face Ø				
Ś	Etherne	et II.	Src:	Netgear	ea:	b1:7a	(80:37	:73:	ea:b1:	7a), D	st: Pcs	Svs	te 09:	14:c4 ()	38:00:2	7:09	9:14:c4	1)	
>	Interne	et Prot	tocol	Version	4.	Src: 1	.92.168	.1.1	, Dst:	192.1	58.1.16	í.	-	``				·	
>	User Da	atagram	n Prot	tocol, S	inc P	ort: 5	3, Dst	Por	t: 577	29									
>	Domain	Name S	Syster	n (respo	onse)														
) 🗹 Fi	rame (fra	ime), 2	54 bytes						Pad	(ets: 49 ·	Disp	layed: 6	(12.2%) ·	Dropped:	0 (0.	.0%) F	Profile: Def	ault

What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

- b. Expand Domain Name System (response). Then expand the Flags, Queries, and Answers.
- c. Observe the results.

Can the DNS server do recursive queries?

🚄 *Ethernet	- 🗆 ×
File Edit View Go Capture Analyze Statistics Telephony	Wireless Tools Help
udp.port ==53	Expression +
No. Time Source Destination Protocol	Length Info
16 8.597003 192.168.1.16 192.168.1.1 DNS	84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17 8.611953 192.168.1.1 192.168.1.16 DNS	161 Standard query response 0x0001 No such name PTR 1
33 15.952381 192.168.1.16 192.168.1.1 DNS	73 Standard query 0x0002 A www.cisco.com
← 34 15.963198 192.168.1.1 192.168.1.16 DNS	254 Standard query response 0x0002 A www.cisco.com CNA
35 15.966100 192.168.1.16 192.168.1.1 UNS	73 Standard query 0x0003 AAAA www.clsco.com
50 15.9//2/5 192.100.1.1 192.100.1.10 DNS	294 Scandard query response 0x0005 AAAA www.cisco.com
✓ Domain Name System (response)	^
[Request In: 33]	
[Time: 0.010817000 seconds]	
Transaction ID: 0x0002	
✓ Flags: 0x8180 Standard query response, No error	
I I I Response: Message is a	'esponse
.000 0 = Opcode: Standard query	v) not an authority for domain
- Truncated: Message is n	at truncated
1 = Recursion desired: Do a	erv recursively
1 = Recursion available: Se	ever can do recursive queries
0 = Z: reserved (0)	
0 = Answer authenticated: A	nswer/authority portion was not authenticated by the serv
0 = Non-authenticated data:	Unacceptable
0000 = Reply code: No error (0	
Questions: 1	
Answer RRs: 5	
Authority RRs: 0	
Additional RRs: 0	
✓ Queries	
www.cisco.com: type A, class IN	
Name: www.cisco.com	
[Name Length: 15]	
Type: A (Host Address) (1)	
Class: IN (0x0001)	
✓ Answers	
> www.cisco.com: type CNAME, class IN. cname ww	.cisco.com.akadns.net
> www.cisco.com.akadns.net: type CNAME, class I	I, cname www.ds.cisco.com.edgekey.net
> www.ds.cisco.com.edgekey.net: type CNAME, clas	IN, cname www.ds.cisco.com.edgekey.net.globalredir.akadn
> www.ds.cisco.com.edgekey.net.globalredir.akadn	.net: type CNAME, class IN, cname e144.dscb.akamaiedge.n
> e144.dscb.akamaiedge.net: type A, class IN, a	dr 23.52.234.158 V
<	>
Frame (frame), 254 bytes	Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) Profile: Default

d. Observe the CNAME and A records in the Answers details.

How do the results compare to nslookup results?

Reflection

- 1. From the Wireshark results, what else can you learn about the network when you remove the filter?
- 2. How can an attacker use Wireshark to compromise your network security?