Pauline Criste



Above is the installer for Wireshark

🧂 MyOdu Main view	X 🛛 👾 Hands On #9	× 🔇 it315.girlsgeekout.org	x 🚍 Untitled document - Google Do: x +	× -	٥	×
\leftrightarrow \rightarrow C A Not secure	it315.girlsgeekout.org			le ☆	• •	:
This is a placeholder	r					
First name: Pauline Last name: Criste						
Submit						

This is the website to input our first and last name. We will capture the traffic on this website.

Pauline Criste

		0		🔀 🙆	୍ 📢	⊨ 🔿	警 쥼			Ð		e, 🕛													
dns	.qry.nam	e==it315.gir	lsgeekout.o	rg																				C	
No.	Tim	e	Source		Desti	nation		Protocol	Length	Info															
_+ 3	399 5.5	27826	2600:40	40:16d3:a70	 2600	:4040:16	6d3:a70	DNS	102	Standar	d query	0x9d10	A it31	15.girl	.sgeeko	ut.org									
4	400 5.5	28561	2600:40	40:16d3:a70	2600	:4040:16	5d3:a70	DNS	102	Standar	d query	0xa41e	AAAA i	it315.g	irlsge	ekout.or	g								
4	402 5.5	28779	2600:40	40:16d3:a70	2600	:4040:16	5d3:a70	DNS	102	Standar	d query	0x24d0	A it31	15.girl	sgeeko	ut.org									
4	403 5.5	29058	2600:40	40:16d3:a70	2600	:4040:16	5d3:a70	DNS	102	Standar	d query	0x1d7d	AAAA i	it315.g	irlsge	ekout.or	g								
4	404 5.5	29273	2600:40	40:16d3:a70	2600	:4040:16	5d3:a70	DNS	102	Standar	d query	0x4219	HTTPS	it315.	girlsg	eekout.o	rg								
ها له	405 5.5	33666	2600:40	40:16d3:a70	2600	:4040:10	5d3:a70	DNS	118	Standar	d query	respon	se Øx90	10 A 1	t315.g	irlsgeek	out.org	A 216.9	2.30.10	94					
	105 5.5	346/1	2600:40	40:16d3:a/0	2600	:4040:10	5d3:a/0	DNS	102	Standar	a query	respon	se Øxa4	110 AAA	A 1131	5.girlsg	eekout.o	rg							
	407 J.J	34907	2000:40	40:1603:070		.4040:10	543.070	DNC	100	Standar	a query	respon	se 0x24	1 A 004	.t315.g	E airlea	out.org	A 210.9	2.30.10	14					
	400 J.J	00620	2000:40	40:1603:070	2000	.4040:10	5d2.570	DNC	102	Standar	d query	respon		170 AAA	DC 1+3	15 girls	eekout.o	rg org 604	dec1 r				-		
	118 5 6	08020	2600:40	40:16d3:a70	2600	.4040.10	5d3 + a70	TCMPv6	223	Destina	tion Un	reachab			achahl	a)	geekout.	org SOA	unsi.r	egisti	ar=ser	vers.co	411		-
_	10 510	00714	2000.40	40.1005.070	2000	. 4040. 10	Juj . u / U	1011 00	225	Destina	01011 011	reaction		i e unite	achab c	<i>c</i> ,									
> Fra > Eth > Int > Use	ame 399 hernet i ternet i er Data	: 102 byte II, Src: / Protocol gram Prote	es on wire Apple_21:0 Version 6, ocol, Src	e (816 bits d0:18 (d4:6 , Src: 2600 Port: 3536), 102 b 1:9d:21: :4040:10 <mark>6, Dst P</mark>	bytes ca :d0:18), 6d3:a700 Port: 53	ptured (Dst: Ar fcc4:7d	816 bits cadyan_7 d1:99aa:) on i 2:dc:1 edc5,	nterface 1 (b8:f8: Dst: 2600	en0, id :53:72:0 0:4040:1	d 0 dc:11) 16d3:a70	0::1												
> Don	nain Na	me System	(query)																						
0000 0010 0020 0030 0040 0050 0050	b8 f8 05 00 7d d1 00 00 01 00 0c 67 67 00	53 72 dc 00 30 11 99 aa ed 00 00 00 00 01 00 69 72 6c 00 01 00	11 d4 61 40 26 00 c5 26 00 01 8a 26 00 00 00 73 67 65 01	9d 21 d0 2 40 40 16 40 40 16 60 35 00 2 00 00 05 65 6b 6f	18 86 dd d3 a7 00 d3 a7 01 30 79 14 69 74 33 75 74 03	1 60 0b 9 fc c4 9 00 00 3 31 35 3 6f 72	• Sr • 0 @ } • girls	∙a •!••• &• @@••• &• @@••• •& •5•Øy •• ••it ge ekout	.`. 315 •or																
. 🔍 🖬	User	Datagram Pro	tocol (udp), 8	bytes												Packet	s: 1254 · Dis	played: 11	(0.9%) · D	ropped:	0 (0.0%)		• P	rofile: Def	ault

1. I entered on the capture filter dns.qry.name==it315.girlsgeekout.org and it displayed all traffic sent through the website

	Wi-Fi: en0							
📶 🔳 🗟 🕲 🚞 🕋 🖹 🙆 🔍 🖛	🜢 🤷 🗗 🛃 🔳 🔍 🔍 🔍 🎬							
arp		+						
No. Time Source Destination	∣ Protocol Lenç ∧ Info							
108 8.465586 Apple_21:d0:18 Arcadyar	_72:dc:11 ARP 42 192.168.1.181 is at d4:61:9d:21:d0:18							
154 17.509971 Apple_21:d0:18 Arcadyar	72:dc:11 ARP 42 192.168.1.181 is at d4:61:9d:21:d0:18							
13 3.993427 Arcadyan_72:dc:11 Broadcas	ARP 60 Who has 192.168.1.2197 Tell 192.168.1.1							
107 8.465528 Arcadyan_72:dc:11 Apple_22	d0:18 ARP 60 Who has 192.168.1.1817 Tell 192.168.1.1							
153 17.509899 Arcadyan_72:dc:11 Broadcas	ARP 60 Who has 192.1881.1817 (ett 192.188.1.1							
189 23.653555 Arcadyan_/2:dc:11 Broadcas	ARP 60 Who has 192.108.1.2051 [ett 192.108.1.1							
190 23.653562 Arcadyan_/2:dc:11 Broadcas	ARY 00 Who has 192.106.1.108 [101 192.106.1.1							
194 23:490004 Arcadyan_72:dc.11 Broadcas	ARE 08 WID Has 192.106.1.1001 HELC 192.106.1.1							
	🛢 🔴 🔮 Wireshark - Packet 108 · Wi-Fi: en0							
> Frame 108: 42 bytes on wire (336 bits), 42 bytes								
> Ethernet II, Src: Apple_21:d0:18 (d4:61:9d:21:d0)	Protocol type: IPv4 (0x0800)							
> Address Resolution Protocol (reply)	Hardware size: 6							
	Protocol size: 4							
	Opcode: reply (2)							
	Sender MAC address: Apple_21:d0:18 (d4:61:9d:21:d0:18)							
	Sender IP address: 192.168.1.181							
Target MAC address: Arcadyan_72:dc:11 (b8:f8:53:72:dc:11)								
	Target IP address: 192.168.1.1							
	0000 b8 f8 53 72 dc 11 d4 61 9d 21 d0 18 08 06 00 01 ···Sr···a ·!·····							
	0010 08 00 06 04 00 02 d4 61 9d 21 d0 18 c0 a8 01 b5a .!							
0000 b8 f8 53 72 dc 11 d4 61 9d 21 d0 18 08 06 00								
0010 08 00 06 04 00 02 d4 61 9d 21 d0 18 c0 a8 01								
0020 b8 f8 53 72 dc 11 c0 a8 01 01								
	Help							
Address Resolution Protocol: Protocol	Packets: 195 - Displayed: 8 (4.1%) - Dropped: 0 (0.0%)	Profile: Default						

I looked at the information from the DNS packet to see the source and destination. My wireshark was not working properly on Windows so I used my Macbook that has wireshark in it as well. It says that I am the sender (Apple) and the target is

Pauline Criste

it315.girlsgeekout.org. I used the arp as a filter and it I clicked on where is says source apple, sender arcadyan_72:dc:31 and matched the information from the DNS packet.



2. The ip address that was provided from the ARP for it315.girlsgeekout.org is 192.168.1.1 and so I filtered ip.addr==192.168.1.1 and it displayed packets that included that information. It then includes the GET command under HTTP which has my first and last name.



3. When I right clicked on the GET command with my name on it, went to follow, and clicked on TCP stream, it displayed this information. It contained information about the website and the data that was entered in it. It also says the connection is keep-alive

4. Sniffing this traffic, I was able to capture the information that I input on the website. This means that the website is not encrypted and anyone can access the information that was being entered in the website. It is important to encrypt the network traffic because it is harder to capture rather than plain text.