

Do the following in Wireshark and submit answers to the questions:

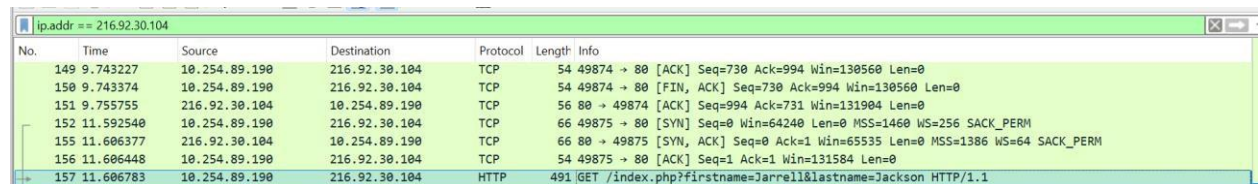
Q1. Use the display filter "dns". Find the packet with the info that says "Standard Query Response" for IT315.girlsgeekout.org. What is the IP address of http://IT315.girlsgeekout.org? Hint: It's the IP address on the far right of the entry, next to "A".

Q2. Use the display filter "ip.addr == " with the IP address of http://IT315.girlsgeekout.org to limit the display to show only traffic to and from http://IT315.girlsgeekout.org. Find the packet where your browser application sent a GET command with your name. How did the website know your first and last name?

Q3. Find the server's response to that GET command (it should say "HTTP/1.1 200 OK"). What type of data is contained in this packet?

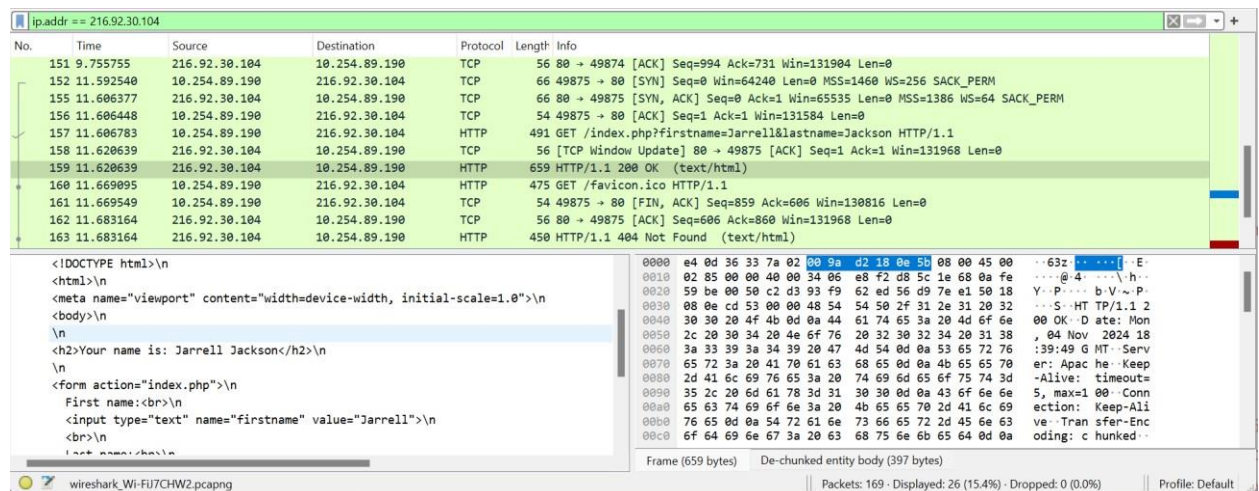
Q4. Think about what you have seen in this packet capture. Why is it important to have network traffic encrypted rather than appearing in clear text?

1. The IP address is: 216.92.30.104
2. The website knew my name because I put my first and last name in the boxes.



No.	Time	Source	Destination	Protocol	Length	Info
149	9.743227	10.254.89.190	216.92.30.104	TCP	54	49874 → 80 [ACK] Seq=730 Ack=994 Win=130560 Len=0
150	9.743374	10.254.89.190	216.92.30.104	TCP	54	49874 → 80 [FIN, ACK] Seq=730 Ack=994 Win=130560 Len=0
151	9.755755	216.92.30.104	10.254.89.190	TCP	56	80 → 49874 [ACK] Seq=994 Ack=731 Win=131904 Len=0
152	11.592540	10.254.89.190	216.92.30.104	TCP	66	49875 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
155	11.606377	216.92.30.104	10.254.89.190	TCP	66	80 → 49875 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 WS=64 SACK_PERM
156	11.606448	10.254.89.190	216.92.30.104	TCP	54	49875 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
157	11.606783	10.254.89.190	216.92.30.104	HTTP	491	GET /index.php?firstname=Jarrell&lastname=Jackson HTTP/1.1

3. The data in this packet seems to be the HTML code from the website where it displays the information I gave it after clicking submit.



No.	Time	Source	Destination	Protocol	Length	Info
151	9.755755	216.92.30.104	10.254.89.190	TCP	56	80 → 49874 [ACK] Seq=994 Ack=731 Win=131904 Len=0
152	11.592540	10.254.89.190	216.92.30.104	TCP	66	49875 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
155	11.606377	216.92.30.104	10.254.89.190	TCP	66	80 → 49875 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 WS=64 SACK_PERM
156	11.606448	10.254.89.190	216.92.30.104	TCP	54	49875 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
157	11.606783	10.254.89.190	216.92.30.104	HTTP	491	GET /index.php?firstname=Jarrell&lastname=Jackson HTTP/1.1
158	11.620639	216.92.30.104	10.254.89.190	TCP	56	[TCP Window Update] 80 → 49875 [ACK] Seq=1 Ack=1 Win=131968 Len=0
159	11.620639	216.92.30.104	10.254.89.190	HTTP	659	HTTP/1.1 200 OK (text/html)
160	11.669095	10.254.89.190	216.92.30.104	HTTP	475	GET /favicon.ico HTTP/1.1
161	11.669549	10.254.89.190	216.92.30.104	TCP	54	49875 → 80 [FIN, ACK] Seq=859 Ack=606 Win=130816 Len=0
162	11.683164	216.92.30.104	10.254.89.190	TCP	56	80 → 49875 [ACK] Seq=606 Ack=860 Win=131968 Len=0
163	11.683164	216.92.30.104	10.254.89.190	HTTP	450	HTTP/1.1 404 Not Found (text/html)

<pre><!DOCTYPE html>\n<html>\n<meta name="viewport" content="width=device-width, initial-scale=1.0">\n<body>\n\n<h2>Your name is: Jarrell Jackson</h2>\n\n<form action="index.php">\n First name:
\n <input type="text" name="firstname" value="Jarrell">\n
\n Last name:
</pre>	<pre>0000 e4 0d 36 33 7a 02 80 9a d2 18 0e 5b 08 00 45 00 ...63z ...[E]\n0010 02 85 00 00 40 00 34 06 e8 f2 d8 5c 1e 68 0a fe ...@-4-...h..\n0020 59 be 00 50 c2 d3 93 f9 62 ed 56 d9 7e e1 50 18 ...P...b V~P..\n0030 08 0e cd 53 00 00 48 54 54 50 2f 31 28 31 20 32 ...S~HT P/1.1 2..\n0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e ...00 OK~O ate: Non..\n0050 2c 20 30 34 20 4e 6f 76 20 32 30 32 34 20 31 38 ... , 04 Nov 2024 18..\n0060 3a 33 39 3a 34 39 20 47 4d 54 0d 0a 53 65 72 76 ...:39:49 G MT. Serv..\n0070 65 72 3a 20 41 70 61 63 68 65 0d 0a 4b 65 65 70 ...er: Apac he~Keep..\n0080 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d ...-Alive: timeout=..\n0090 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e ...5, max=1 00~Conn..\n00a0 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 ...ection: Keep-Alli..\n00b0 76 65 0d 0a 54 72 61 6e 73 66 65 72 2d 45 6e 63 ...ve~Tran sfer~Enc..\n00c0 6f 64 69 6e 67 3a 20 63 68 75 6e 6b 65 64 0d 0a ...oding: c hunked~..</pre>
--	---

4. Think about what you have seen in this packet capture. Why is it important to have network traffic encrypted rather than appearing in clear text? I think its important to encrypt network traffic rather than having it appear in clear text because not only would it be easy for anyone listening on your network to get information but it's also a huge security issue to just have everything non encrypted leaving information just out there.