

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.

ip.addr == 216.92.30.104						
No.	Time	Source	Destination	Protocol	Length	Info
149	9.743227	10.254.89.198	216.92.30.104	TCP	54	49874 → 80 [ACK] Seq=730 Ack=994 Win=130560 Len=0
150	9.743374	10.254.89.198	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	10.254.89.198	TCP	56	80 → 49874 [ACK] Seq=994 Ack=731 Win=131904 Len=0
152	11.592548	10.254.89.198	216.92.30.104	TCP	66	49875 → 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
155	11.606377	216.92.30.104	10.254.89.198	TCP	66	80 → 49875 [SYN, ACK] Seq=0 Ack=65535 Win=0 MSS=1386 WS=64 SACK_PERM
156	11.606448	10.254.89.198	216.92.30.104	TCP	54	49875 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
157	11.606783	10.254.89.198	216.92.30.104	HTTP	491	GET /index.php?firstname=Jarrell&lastname=Jackson HTTP/1.1

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

ip.addr == 216.92.30.104						
No.	Time	Source	Destination	Protocol	Length	Info
151	9.755755	216.92.30.104	10.254.89.198	TCP	56	80 → 49874 [ACK] Seq=994 Ack=731 Win=131904 Len=0
152	11.592548	10.254.89.198	216.92.30.104	TCP	66	49875 → 80 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
155	11.606377	216.92.30.104	10.254.89.198	TCP	66	80 → 49875 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 WS=64 SACK_PERM
156	11.606448	10.254.89.198	216.92.30.104	TCP	54	49875 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
157	11.606783	10.254.89.198	216.92.30.104	HTTP	491	GET /index.php?firstname=Jarrell&lastname=Jackson HTTP/1.1
158	11.626639	216.92.30.104	10.254.89.198	TCP	56	[TCP Window Update] 80 → 49875 [ACK] Seq=1 Ack=1 Win=131968 Len=0
159	11.626639	216.92.30.104	10.254.89.198	HTTP	659	HTTP/1.1 200 OK (text/html)
160	11.669095	10.254.89.198	216.92.30.104	HTTP	475	GET /favicon.ico HTTP/1.1
161	11.669549	10.254.89.198	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	10.254.89.198	TCP	56	80 → 49875 [ACK] Seq=606 Ack=860 Win=131968 Len=0
163	11.683164	216.92.30.104	10.254.89.198	HTTP	450	HTTP/1.1 404 Not Found (text/html)

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.