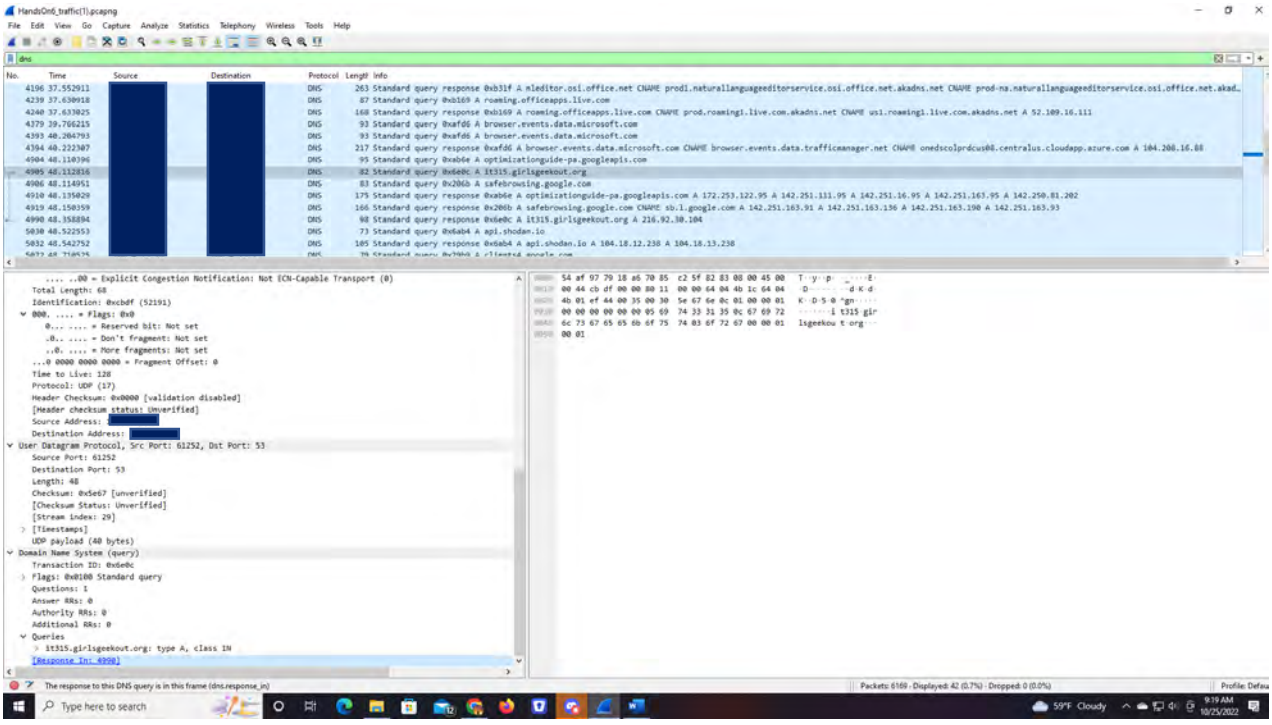
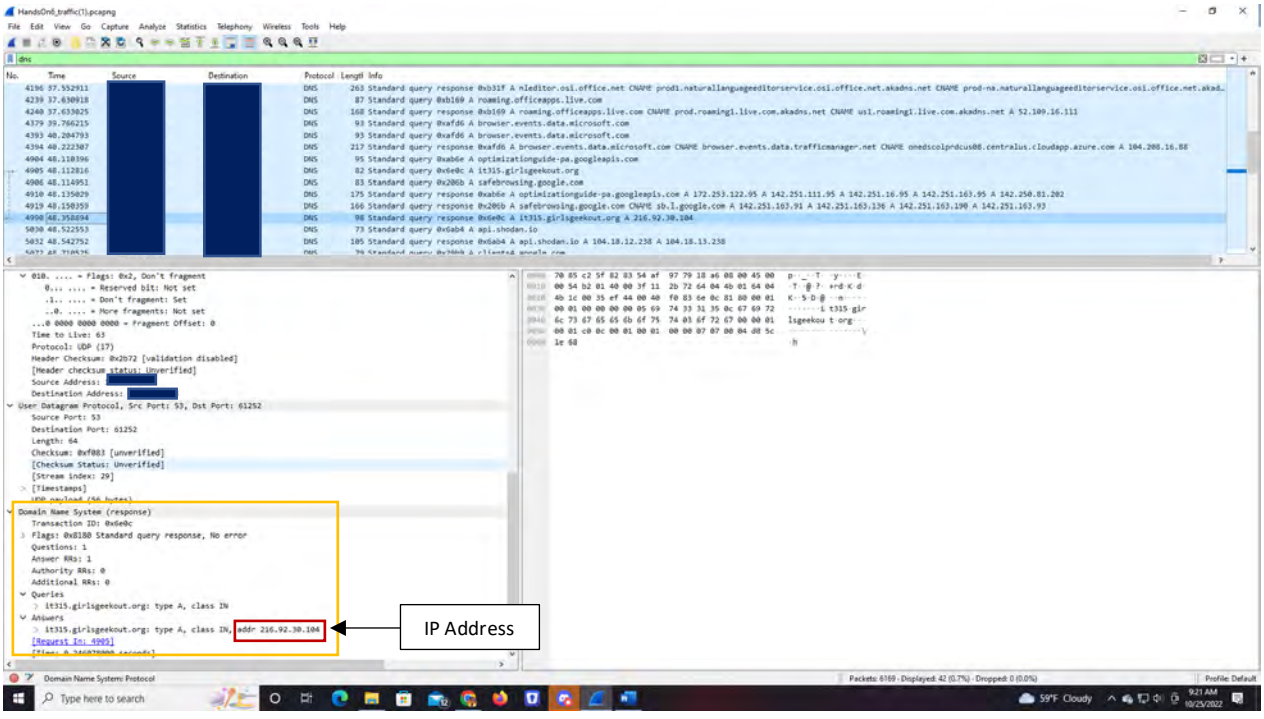
HANDS ON #6

1) 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?



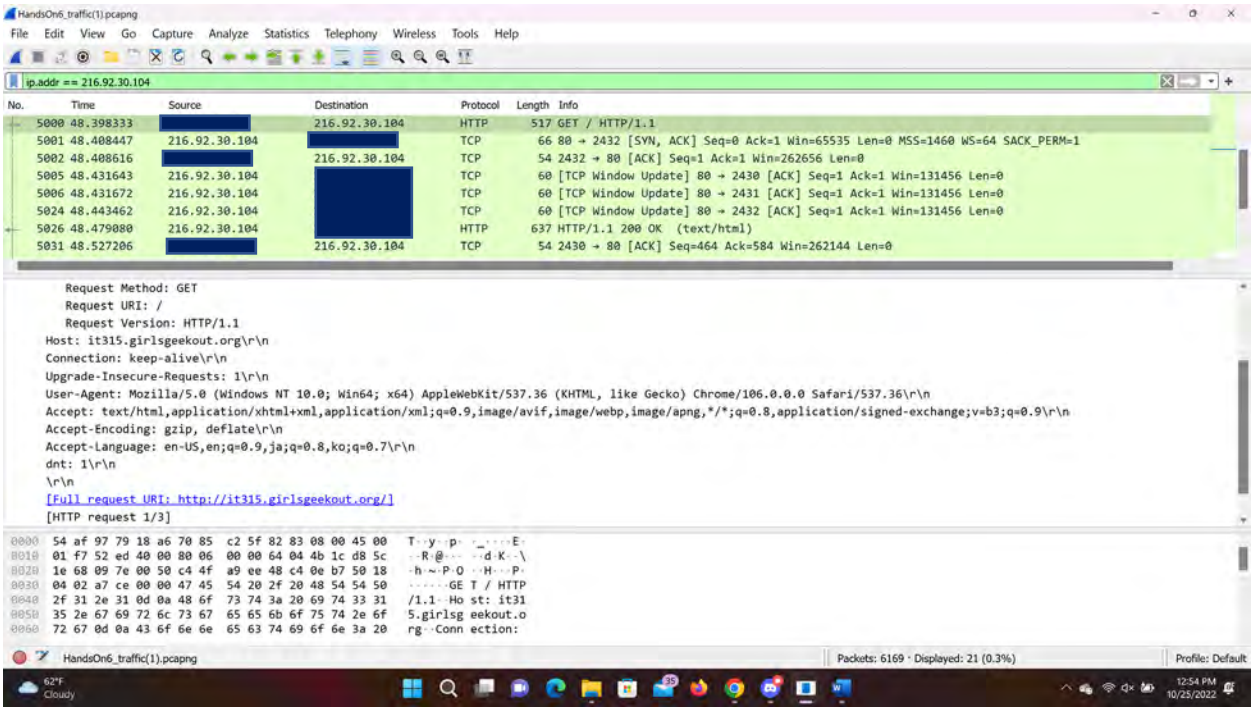


a) Ip address is: 216.92.30.104

b) How did that happen? Once the user inputs the website name http://it315.girlsgeekout.org the computers send a “standard query” to the Domain Name System (DNS) through the User Datagram Protocol (UDP) to ask the IP address associated with http://it315.girlsgeekout.org. Once the DNS finds the information the DNS sends a “standard query response” back to the host that sent the “standard query”. This is because the hosts do not know how to send the information by the name; for the information to be send through the network the address needs to be in IPv4 or IPv6 format.

c) 1st picture is of the “standard query”; 2nd picture is of the “standard query response”

2) 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 in it. How did the website know your first and last name?



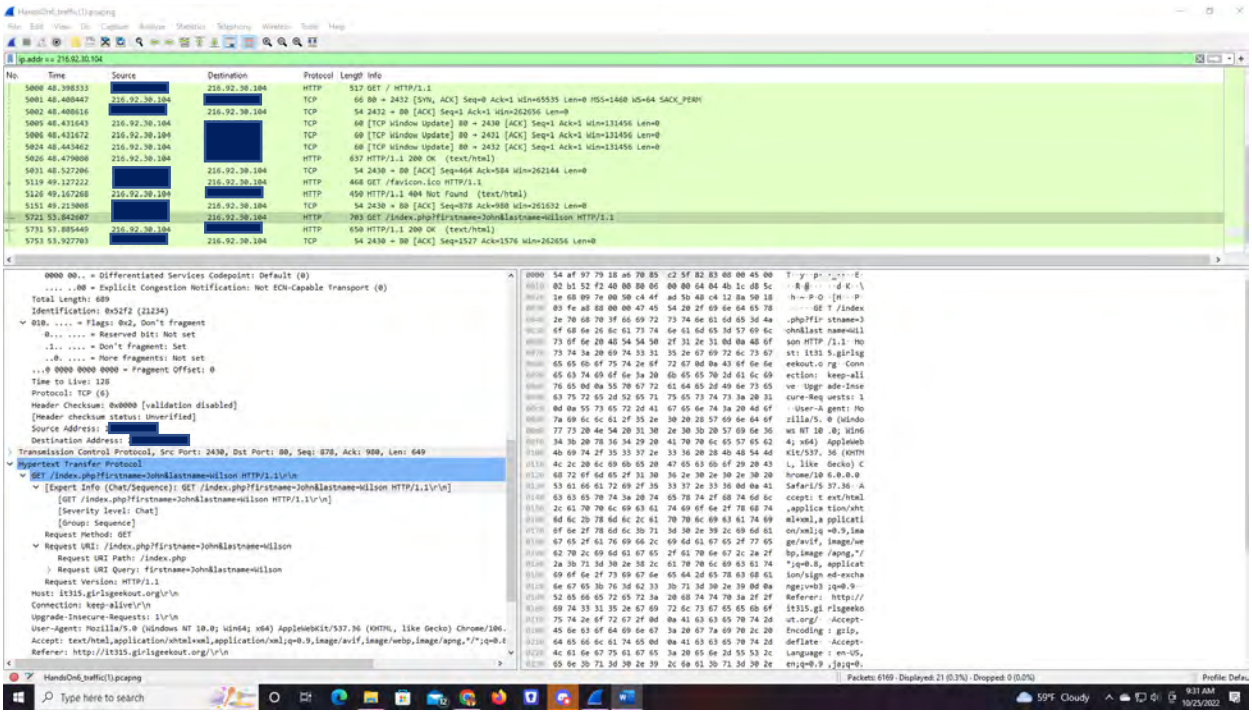
a) The website knew by the Hypertext Transfer Protocol (HTTP) that sends an HTTP GET requests which asks for a specific request from the server, where the website is located. In this case the GET command requested the for two pieces of information, a first and last name.

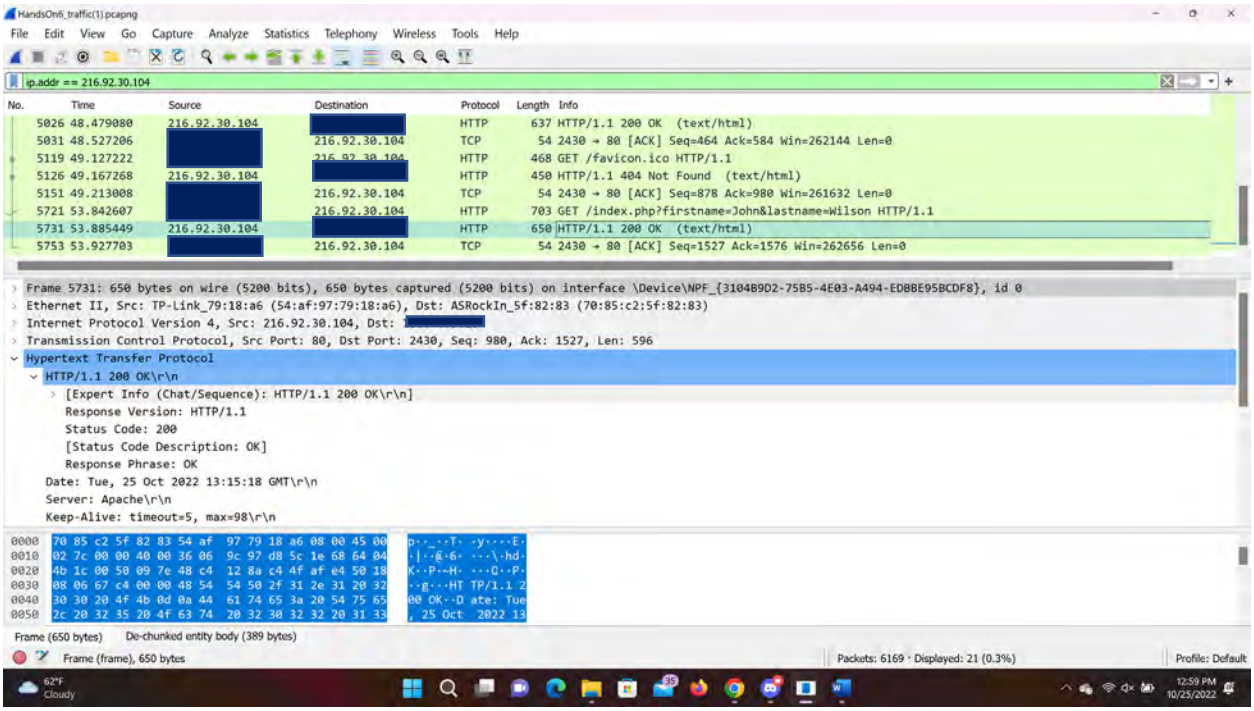
b) The GET command happens within the HTTP area which is located at the application network layer.

c) The first image is a snapshot of an example of the GET command. Once again, the information was sent in the clear (HTTP), which allows anyone to observe the information.

3) 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?

HANDS ON #6





a) The data contained within this packet is the Frame, Ethernet II, Internet Protocol (IP), Transmission Control Protocol (TCP), and Hypertext Transfer Protocol (HTTP).
   i) The Frame section has information like the arrival date-time stamp, the Frame number and length.
   ii) The Ethernet II section has the source and destination router IDs
   iii) The IP section has the source and destination IP addresses.

iv) The TCP section has the source and destination port numbers, sequence numbers, and TCP flags
v) The HTTP section contains the Date time stamp, HTTP responses along with status code, how long to keep the life of the message (when to timeout), and how big (in bites) the file is.
vi) Then final piece is the Line-based text data which has the information (code) of the website. This is where the information of your first and last name is located.

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?

a) (For obvious reasons) Sending anything in the clear allows anyone to read the content. You want your information private, which includes any sensitive information like bank account numbers, passwords, SSN's, or anything else that might be considered Personal Identifiable Information (PII).