Hands-On #9 Questions

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 it315.girlsgeekout.org? (If there are a lot of entries, try the filter "dns.a" or "dns.qry.name==it315.girlsgeekout.org")**

The IP address of it315.girlsgeekout.org is 216.92.30.104. It was found in the Answers section of the specific packet as well as shown in the info section before inspecting the packet.

2. **Use the display filter "ip.addr == " with the IP address of it315.girlsgeekout.org to limit the display to show only traffic to and from it315.girlsgeekout.org. Find the packet where your browser application sent a GET command with your name in it. What is the command that was sent to the web server so that it knows your first and last name?**

The full GET command sent to the web server to learn about my first and last name is “GET /index.php?firstname=Eric&lastname=Preston HTTP/1.1\r\n”. It was in the HTTP and info sections of the packet and capture timeline.

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?**

This packet includes the source and destination address in IP address and MAC address forms, the TCP and HTTP protocols and the specific version of HTTP, my first and last name, the HTML code of the website, and the HTTP and TCP data streams that also disclose the versions of my device and the applications.

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?**

Encryption is a critical tool for protecting this kind of traffic from being visible to anyone who can easily download Wireshark and use this information to compromise any online website without security features. This also ensures that people who are supposed to see this information are the only ones who can see it if need be.