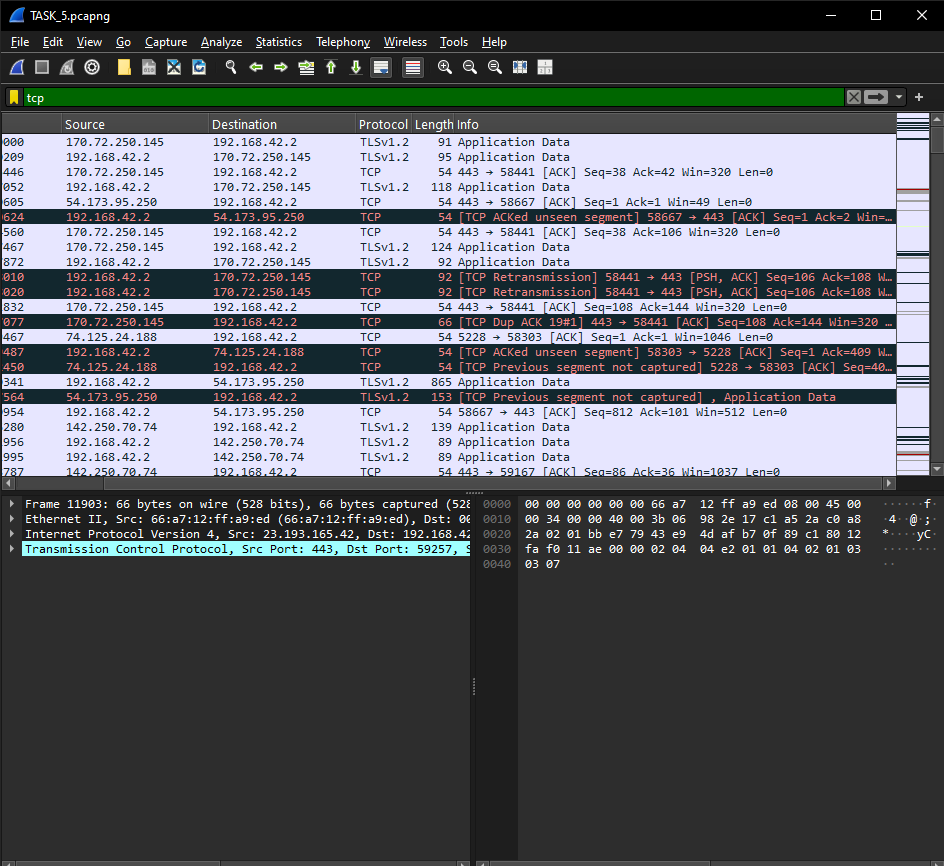
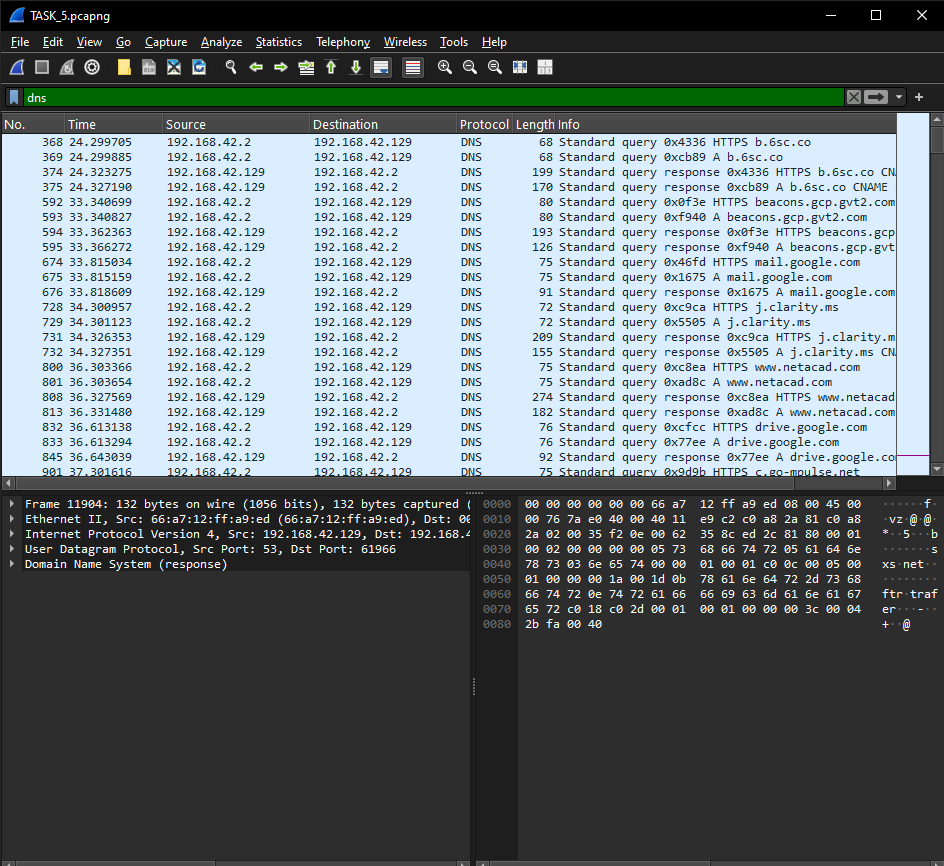
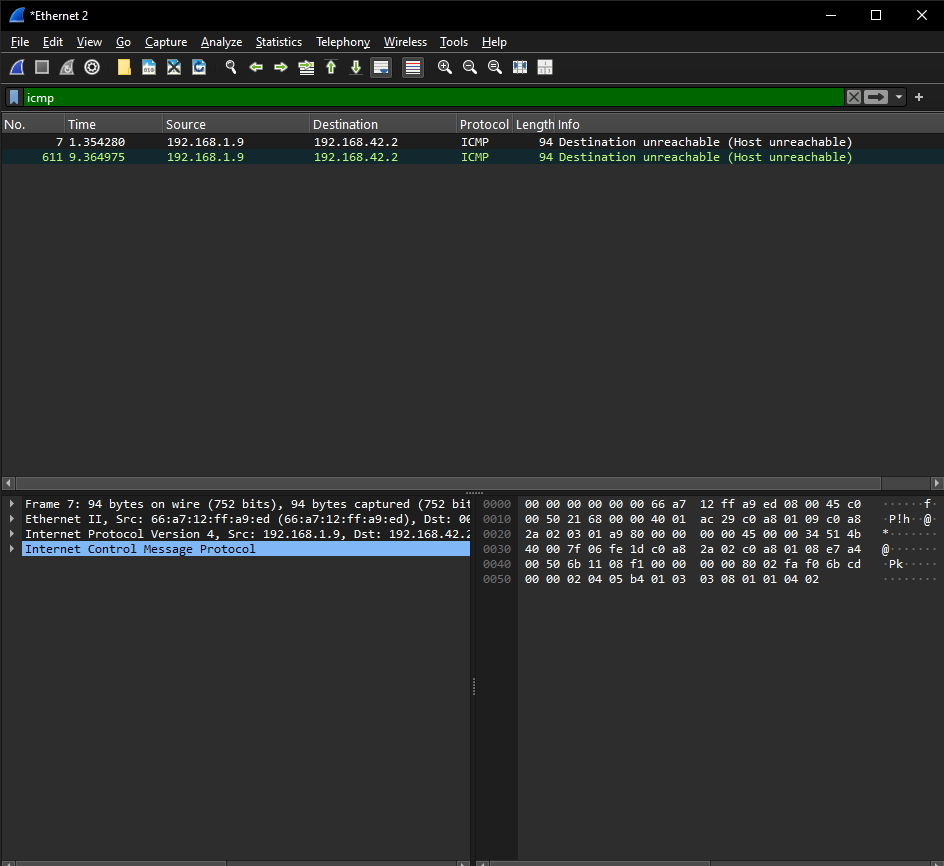
***Elevate Labs Cyber Security Internship***

***Task5: Capture and Analyze Network traffic using Wireshark ***

### DNS (Domain Name System): The packet capture contains numerous DNS queries and responses, which are used to resolve domain names to IP addresses. The file shows traffic to and from various domains, including www.netacad.com, j.clarity.ms, and several Google and Microsoft domains. These queries are often sent over UDP, a connectionless protocol that prioritizes speed.

### TCP (Transmission Control Protocol): The majority of the traffic in the file uses TCP, a connection-oriented protocol that ensures reliable and ordered data delivery. You can observe TCP's three-way handshake (SYN, SYN-ACK, ACK) at the beginning of many conversations, which establishes a connection before data is transferred. TCP is often used by applications where data accuracy is more important than speed, such as web browsing and email.

### ICMP (Internet Control Message Protocol): The packet capture also includes ICMP traffic. ICMP is primarily used for network troubleshooting and diagnostics, such as the ping command, to determine if a host is reachable and to measure the round-trip time. It provides error reporting and status updates for the network.

***Interview Questions***

**1. What is Wireshark used for?**

Wireshark is a powerful, free, and open-source packet analyzer (or "packet sniffer"). It's used to capture and interactively browse the data traveling on a computer network. Network administrators, security professionals, and developers use it for network troubleshooting, analysis, software development, and education.

**2. What is a packet?**

A packet is a small, formatted unit of data that is transmitted over a network. When you send data, like an email or a website request, it is broken down into these small packets, each containing a header with control information (like the source and destination addresses) and a payload, which is the actual user data. The packets travel independently across the network and are reassembled at their destination.

**3. How to filter packets in Wireshark?**

Wireshark has two main types of filters.

* **Capture Filters:** These are applied before a capture begins to restrict the amount of data Wireshark collects. They help you avoid capturing irrelevant traffic, which can be useful for performance. You can filter by protocol (e.g., tcp, udp), host (host 192.168.1.1), or port (port 80).
* **Display Filters:** These are applied after a capture is complete to show only the packets that match your criteria. You can be very specific with display filters, using a wide range of fields like ip.addr == 192.168.1.1 to find traffic to or from a specific IP address, or http.request.method == "POST" to see only HTTP POST requests.

**4. What is the difference between TCP and UDP?**

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two of the most fundamental protocols in the transport layer of the internet.

| **Feature** | TCP (Transmission Control Protocol) | UDP (User Datagram Protocol) |
| --- | --- | --- |
| **Connection** | Connection-oriented (requires a "handshake" to establish a connection) | Connectionless (sends data without a prior connection) |
| **Reliability** | **Reliable**. It guarantees that data is delivered in order and without errors. If a packet is lost, it will be retransmitted. | **Unreliable**. It does not guarantee delivery, order, or error checking. |
| **Speed** | Slower due to the overhead of connection setup and reliability features. | Faster due to minimal overhead. |
| **Use Cases** | Web browsing (HTTP/S), email (SMTP), file transfers (FTP). Used when data integrity is critical. | Live video streaming, online gaming, and Voice over IP (VoIP). Used when speed and low latency are more important than guaranteed delivery. |

**5. What is a DNS query packet?**

A DNS (Domain Name System) query packet is the request your computer sends to a DNS server to resolve a human-readable domain name (like www.google.com) into its corresponding IP address. The packet contains the domain name you are looking for, and the DNS server responds with a packet containing the IP address. This process is essential for navigating the internet, as network devices communicate using IP addresses, not domain names.

**6. How can packet capture help in troubleshooting?**

Packet capture tools like Wireshark provide an "ultimate source of truth" for what is actually happening on a network. By capturing and analyzing packets, you can:

* **Diagnose connectivity issues:** See if packets are reaching their destination.
* **Identify performance bottlenecks:** Analyze latency and determine if delays are caused by the network, a server, or a client application.
* **Troubleshoot application problems:** See the exact data being sent and received to pinpoint errors in an application's communication.
* **Detect security threats:** Identify unauthorized or suspicious traffic, malware activity, or port scans.

**7. What is a protocol?**

A protocol is a set of rules and conventions that govern how data is formatted, transmitted, and received between devices on a network. Protocols enable different types of devices and software to communicate with each other effectively, regardless of their internal design. Examples include TCP, UDP, HTTP, and IP. Think of it as the shared language that computers use to talk to one another.

**8. Can Wireshark decrypt encrypted traffic?**

By default, no, Wireshark cannot decrypt encrypted traffic like HTTPS, as it would be a major security vulnerability. However, it can decrypt some types of traffic if you have access to the necessary encryption keys. For example, you can configure your browser to log TLS session keys to a file, which Wireshark can then use to decrypt the captured traffic for analysis. This is a manual process and is only possible if you control the client or server whose traffic you are capturing. It's not a way to "hack" or snoop on someone else's encrypted communications.