**School of Information Technologies and Engineering, ADA University**

**CSCI2303 – Intro to Computer Networks**

**Fall 2024 – 10/23/2024**

**Assignment 3 by Laman Panakhova 16882**

**Instructions:**

1. *Capture and Analyze Local* ***ICMP*** *Data in Wireshark.*
2. *Use WireShark to analyze the packet in* ***http*** *request. Highlight the SRC and DST ports and Mac Addresses. What is the source and destination ip addresses on network layer?*
3. *Analyze DNS packages using WireShark and nslookup tool.*
4. *Create a small network (use your imagination) and simulate an OSI layer. Screenshot each layer how the request goes through each OSI layers.*

**Solutions:**

1. **I have started the process with opening the Wireshark application and capturing the traffic on Wi-Fi network interface. Then by running the command ping** [**www.google.com**](http://www.google.com) **in the command line interface I generated ICMP traffic. Next, I filtered the packets by command icmp and analyzed the details such as source IP, destination IP, and ICMP type. Also, analyzed the Ethernet data, Echo Request, and Echo Reply: (Then I stopped the capturing)**  
   A screenshot of a computer

   Description automatically generatedA computer screen with white text

   Description automatically generatedA screenshot of a computer

   Description automatically generated

**A screenshot of a computer

Description automatically generated**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **The simulation in the Wireshark again is needed for the second task. Now I have tried to capture the traffic from a website that uses HTTP. I have chosen** [**http://example.com**](http://example.com) **for simplicity. Then I have expanded my packet details for getting information about source (SRC) port, destination (DST) port, MAC addresses, IP addresses:** A screenshot of a computer

   Description automatically generatedA screenshot of a computer

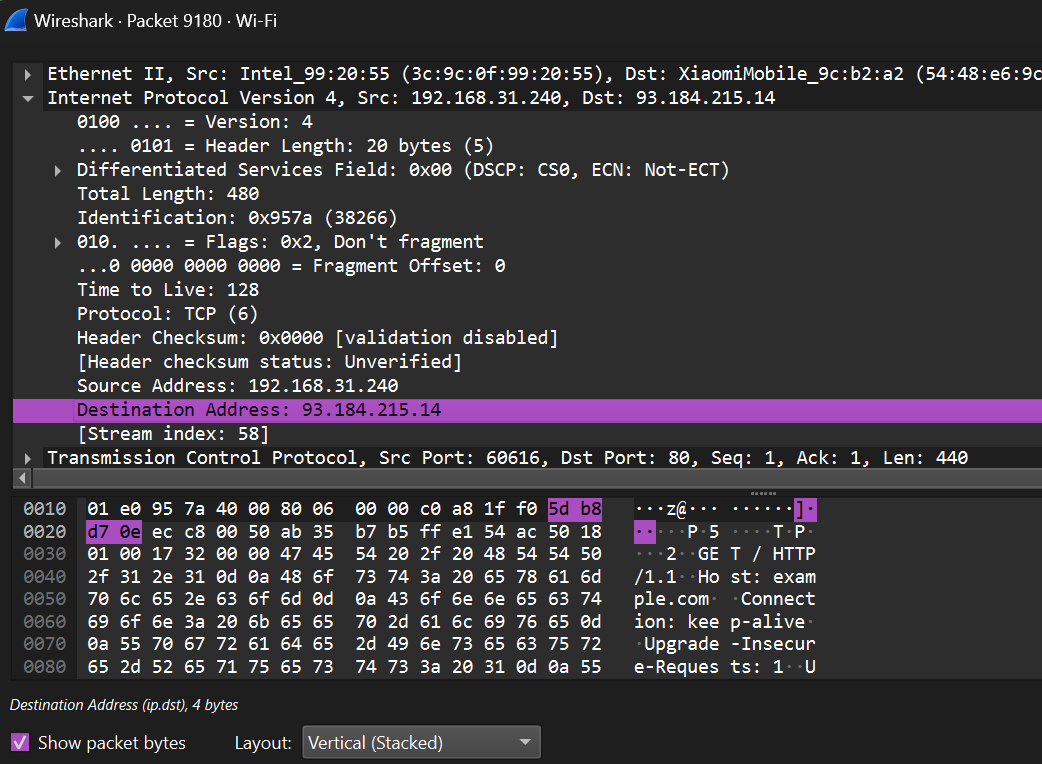
   Description automatically generatedA screenshot of a computer

   Description automatically generatedA screenshot of a computer

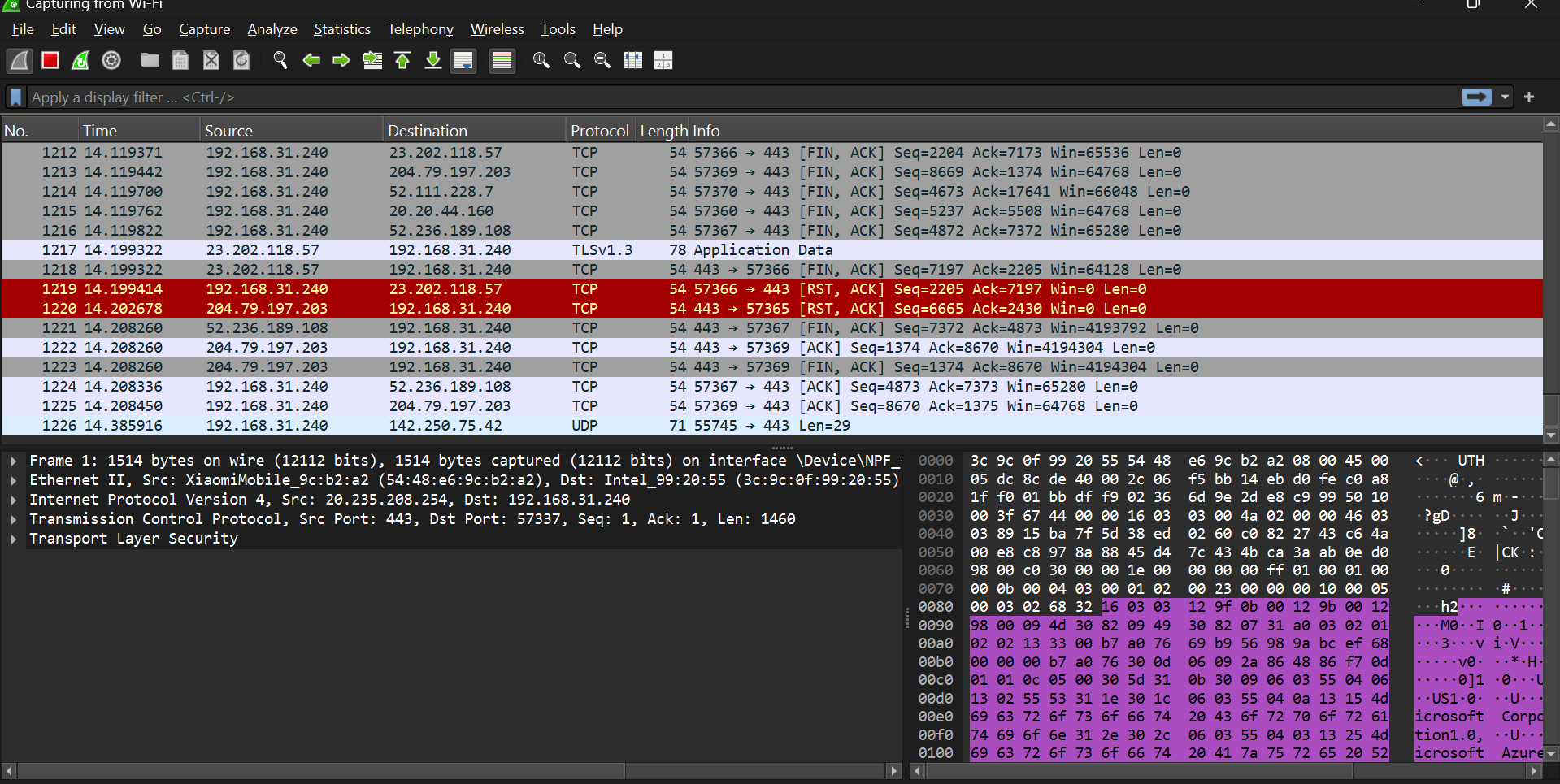
   Description automatically generated

A screenshot of a computer program

Description automatically generatedA computer screen shot of a program

Description automatically generated**A screenshot of a computer

Description automatically generated**

1. **Coming to the third question I did the starting point in a similar manner. Capturing the traffic in Wireshark I tried to use the DNS packets to analyze. Running the nslookup www.google.com I filtered the dns packets in the application. Here I analyzed DNS Query and Response Packets:A computer screen with white text

   Description automatically generatedA screenshot of a computer

   Description automatically generatedA screenshot of a computer

   Description automatically generatedA screenshot of a computer program

   Description automatically generatedA screenshot of a computer program

   Description automatically generatedA computer screen shot of a program

   Description automatically generatedA screenshot of a computer

   Description automatically generated**
2. **In the last question I tried to simulate the same process on a small network setup that I created in Cisco Packet Tracer application. After creating a small network setup by pinging the device, I analyzed each layer by commands. For the physical layer I opened Frame and Ethernet details where bit transformations were shown. For the Data Link Layer, I analyzed the source and destination MAC addresses. For Network Layer I analyzed the IP addresses. For Transport Layer I checked the TCP packet details such as source or destination ports. For Session Layer I started by checking the TCP Stream for observing the exchange between client and server. For Presentation Layer I filtered the TLS packets for checking the protocol encryption. In the last for Application Layer I finalized my job by checking the details by ICMP command.** A blue rectangular object with orange dots and black lines

   Description automatically generatedA computer screen with white text

   Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Additionally, just for further analysis of the same task I repeated the steps in Wireshark. These are the results of the same steps in Wireshark application:A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generatedA computer screen shot of a computer program

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generated**A screenshot of a computer

Description automatically generated**A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generatedA screen shot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated