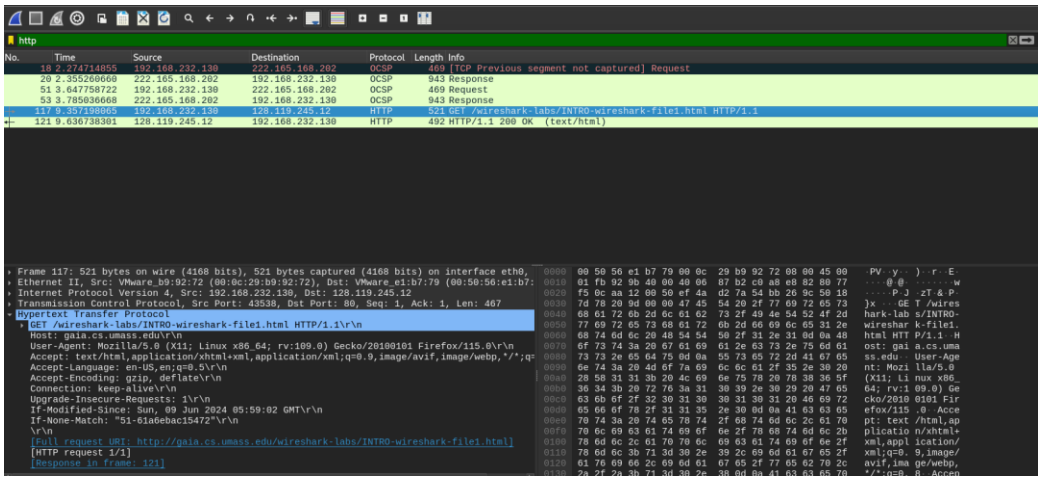
Week 5 – Task 5.1 P

1. Question1
   a. What is the HTTP version your browser is running?
      - The browser is currently using version 1.1

   b. Include a screenshot of your Kali VM that has the Wireshark window running. Ensure that your screenshot shows that have selected the packet with HTTP GET message and details of the packet are visible either as minimized or maximized.



   c. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
      - Source address : 192.168.232.130
      - Destination address : 128.119.245.12

   d. Check the packet details for HTTP Get message (refer to `Details of the selected packet' section of Wireshark window). What type of Web browser issued the HTTP request? Hint: "User-Agent:" field in the expanded HTTP message display. This field value in the HTTP message is how a web server learns what type of browser you are using.
      - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n

   e. What is the destination port number (Hint: the number following "Dest Port:" for the TCP segment containing the HTTP request) to which this HTTP request is being sent? What is the source port number?
      - Source Port : 43538
      - Destination Port : 80

2. Question 2
    a. What is HTTP used for in the World Wide Web? At what network-layer is HTTP located?
        - HTTP serves as the foundation for data transmission on the World Wide Web and is used to convey hypertext data in websites. The application layer contains HTTP

    b. What is an HTTP request? What is included in a typical HTTP request?
        - A request for resources sent by the client to the server is known as an HTTP request. A request line, HTTP headers, and a message body make up a standard HTTP request.

    c. What is an HTTP method? How do get and Post methods differ.
        - An HTTP method indicates what should be done with a selector resource.

    d. What is an HTTP response? What is included in a typical HTTP response?
        - A post is used to send data to a server, which has the ability to modify server state, whereas a get is used to obtain data from a server without altering server state.

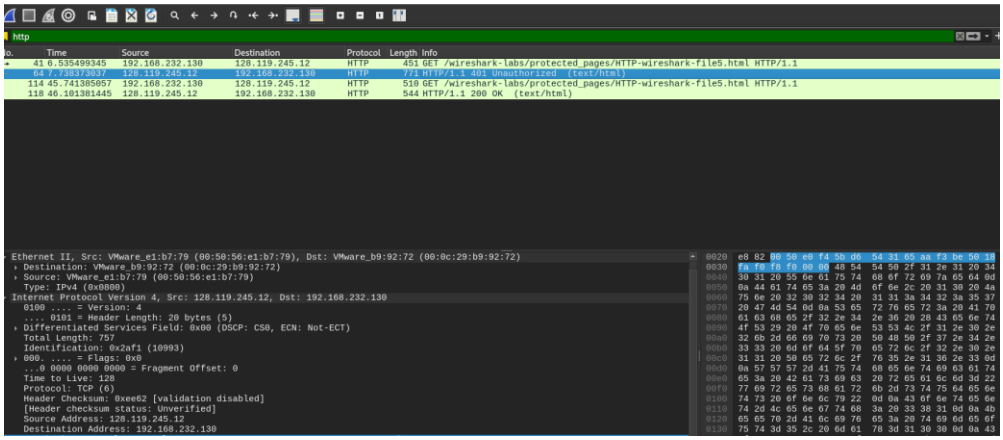
    e. Is HTTP a stateless or a stateful protocol?
        - Due to the server not keeping track of requests, HTTP is a stateless protocol.

3. Question 3
    a. Summarize DoS attack in your own Words
        - An international attempt to stop a specific server from operating server from operating by flooding it with unsanctioned traffic is known as a denial of service (DoS) attack.

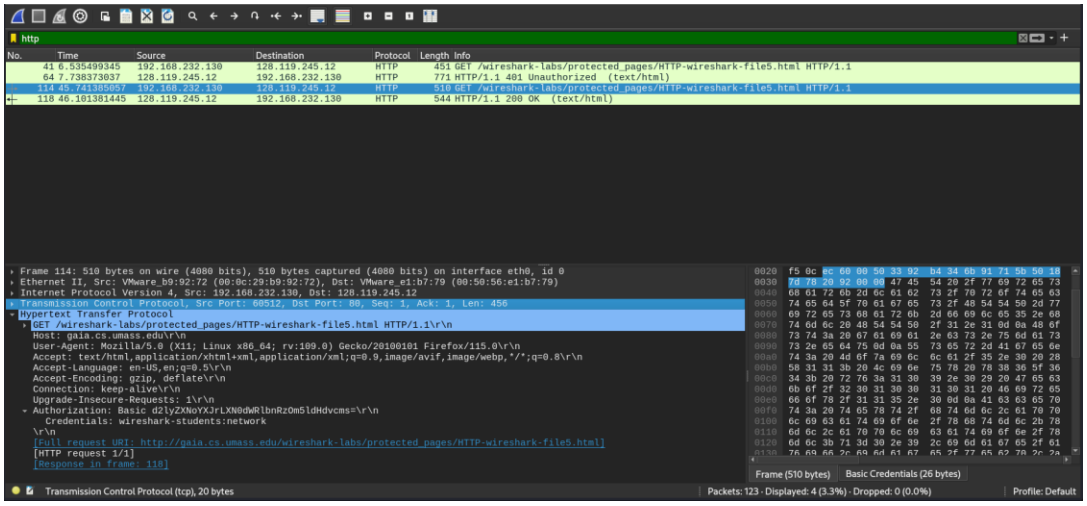
    b. Can HTTP be used to execute a DoS attack?
        - One way to carry out a DoS attack is over HTTP.

4. Question 4
   a. Check the packet details in the middle Wireshark packet details pane. Can you identify the details in Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol / Hypertext Transfer Protocol frames?
      - Yes, the following is what each part shows :
        - ✓ Ethernet II: Shows the MAC addresses of the source and destination.
        - ✓ IPv4: Shows the protocol type, source and destination IP addresses, and other information.
        - ✓ TCP: Shows sequence number, source and destination ports, and other information.
        - ✓ HTTP: Displays the request or answer from HTTP.

   b. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? (i.e., before you provided the credentials) Include a screenshot of the Wireshark window showing the relevant packet and its details.



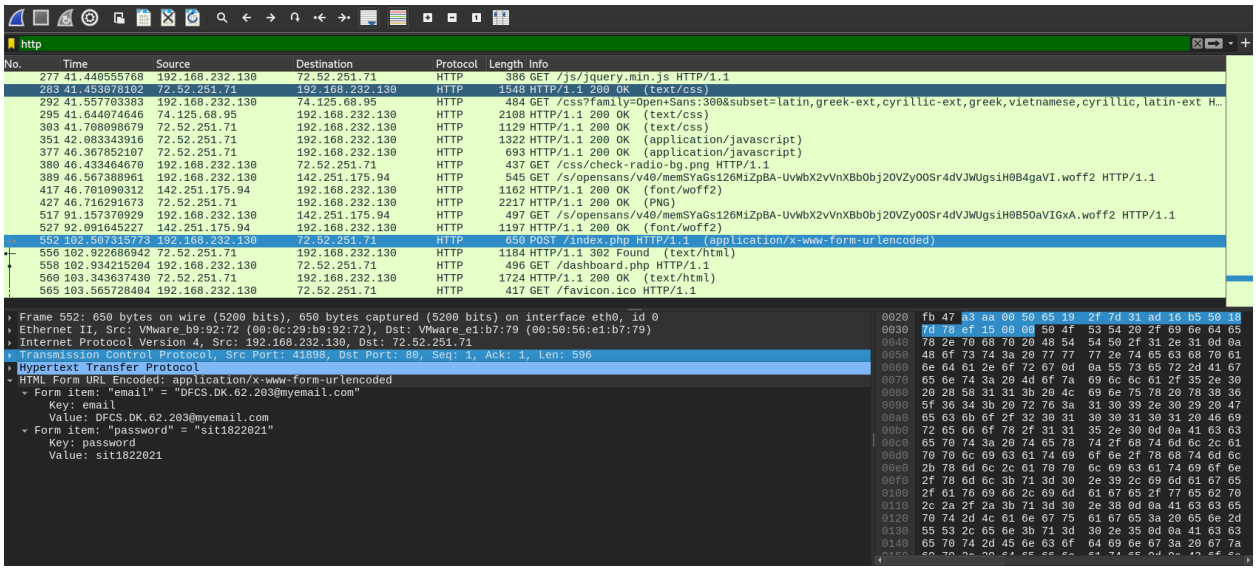
   c. Expand Authorization in Hypertext Transfer Protocol in packet detail section of Wireshark, can you find the username and password are shown in clear text? Include the screenshot



5. Question 5
    a. Was techpanda.org using Base64 encoding?
        - The credential were displayed in clear text since Techpanda was not utilizing base64 encoding.

    b. Did you find the password in an HTTP GET or POST message? Why?
        - Wireshark was able to sniff the packets from the client during the password upload, and the password was discovered through an HTTP Post massage.

    c. Include a screenshot of Wireshark window that shows the packet with Email and Password you used (i.e. the email and password should be clearly visible in packet details section of Wireshark.)



6. Question 6
    a. What did you learn that was new to you? How interesting you find network security compared to other topics covered? How did this task complement the theoretical concepts covered in Week 4 lecture?
        - I learned how to sniff passwords, decrypt Base64 encoding, and trace packets thanks to this task. Overall, this was a well-rounded work that was made much more enjoyable its interests and obstacles.