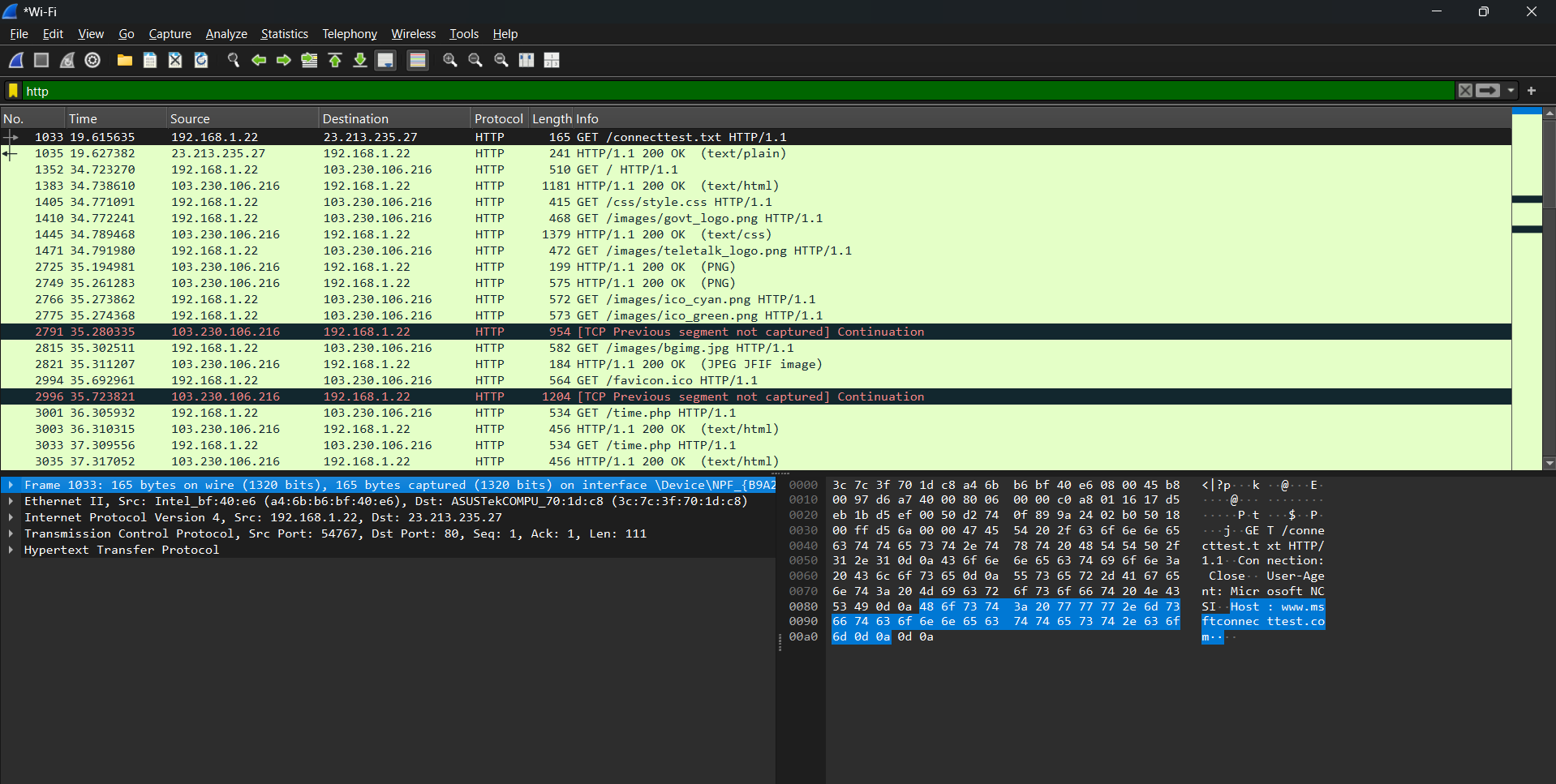
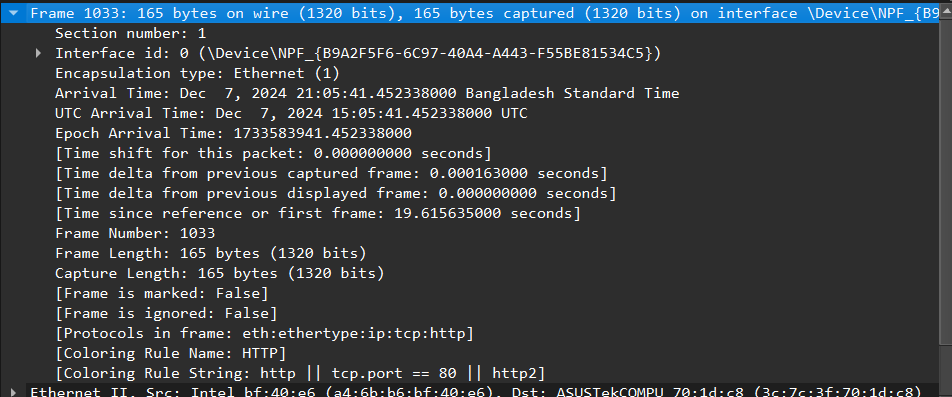
**Name: Md.Rumman Shahriar**

**Id – 22101334 / 24241284**

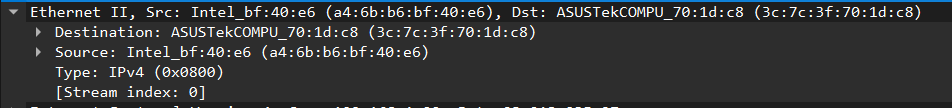
**Entire Screen Image**

****

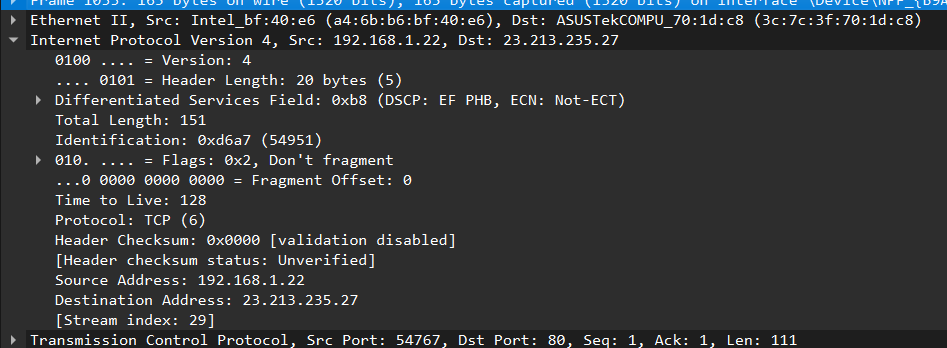
**Wireshark Tasks**



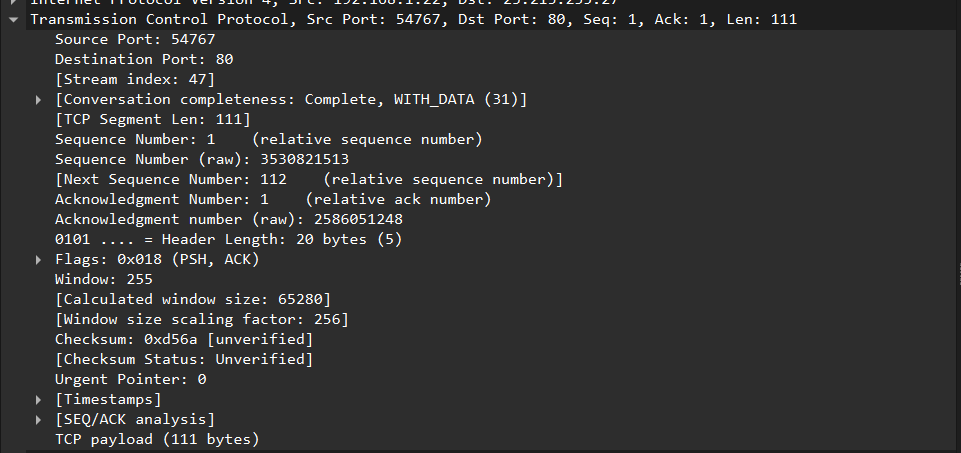
The screenshot shows details of a captured network packet in Wireshark. The packet is transmitted over Ethernet (Data Link Layer) using Interface ID 0. The packet has an arrival timestamp of December 7, 2024, in both local (Bangladesh Standard Time) and UTC. The frame is numbered 1033, with a size of 165 bytes (1320 bits) on the wire, and protocols identified include Ethernet, IP, TCP, and HTTP (Application Layer). The frame is associated with an HTTP coloring rule and follows a specific condition (tcp. port == 80). At the Data Link Layer, the Ethernet II frame contains source and destination MAC addresses: Intel (bf:40: e6) as the source and ASUS Tek (70:1d:c8) as the destination.



The image shows an Ethernet II frame captured at the Data Link Layer. The source MAC address is Intel\_bf:40: e6 (a4:6b: b6:bf:40: e6), and the destination MAC address is ASUSTekCOMPU\_70:1d:c8 (3c:7c:3f:70:1d:c8). The frame encapsulates an IPv4 packet, as indicated by the Type field (0x0800). The frame is part of Stream index 0, which helps track related frames in a communication session. At this layer, the Ethernet II protocol ensures reliable delivery between devices on the same network segment.



This image shows a packet capture, highlighting details of an IPv4 packet. At the **Data Link layer**, the Ethernet II frame specifies the source MAC address (Intel\_bf:40:e6) and destination MAC address (ASUSTekCOMPU\_70:1d:c8). At the **Network layer**, the packet is using IPv4 with a source IP address of 192.168.1.22 and a destination IP of 23.213.235.27. It includes a total length of 151 bytes, a TTL of 128, and a protocol value of 6 (indicating TCP). At the **Transport layer**, the TCP segment shows a source port of 54767 and a destination port of 80 (HTTP), with a sequence and acknowledgment number of 1, and a payload length of 111 bytes.



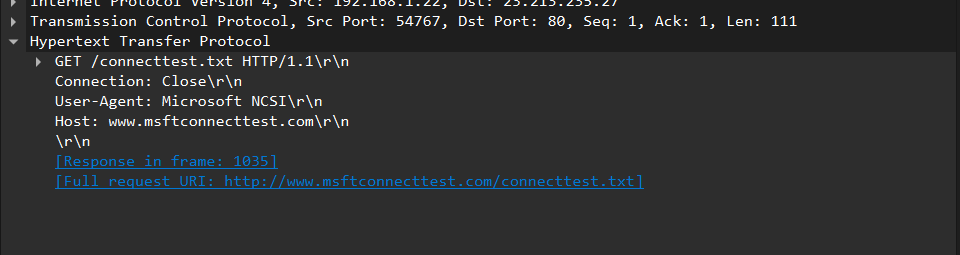
This packet capture provides details about a TCP segment transmitted within an Ethernet frame.

At the **Data Link layer**, the Ethernet II frame facilitates the communication between devices, using source and destination MAC addresses to identify the hardware involved. This is the layer that ensures the packet reaches the next-hop device in the local network.

At the **Network layer**, the IPv4 protocol is responsible for routing the packet between the source IP address (192.168.1.22) and the destination IP address (23.213.235.27).

At the **Transport layer**, the packet details a TCP segment with a source port of 54767 and a destination port of 80, signifying an HTTP communication. The segment's sequence number is 1 (raw: 3530821513), and its acknowledgment number is 1 (raw: 2586051248), confirming receipt of earlier data. The TCP flags include PSH (indicating data should be pushed to the application immediately) and ACK (acknowledging receipt of data). The calculated window size is 65280, which determines how much more data can be received before acknowledgment is required. The segment carries 111 bytes of application-layer payload.

The checksum field provides error-checking for data integrity but is marked unverified in this capture. Additionally, the urgent pointer is set to 0, meaning there is no urgent data. This segment is part of a complete TCP conversation that includes data transmission.



This image shows the analysis of an HTTP GET request captured within a packet. At the **Data Link layer**, the Ethernet II frame is responsible for transferring this packet between the source and destination hardware using their respective MAC addresses. At the **Transport layer**, the TCP segment originates from source port 54767 and is destined for port 80, indicating HTTP traffic.

At the **Application layer**, the captured HTTP request specifies the GET method to retrieve the resource /connecttest.txt using HTTP/1.1. The request headers include Connection: Close (indicating the TCP connection should close after the response), User-Agent: Microsoft NCSI (indicating the client making the request), and the Host header specifying the domain www.msftconnecttest.com. The full request URI is http://www.msftconnecttest.com/connecttest.txt. This request likely forms part of a connectivity checks typically performed by operating systems to verify internet access.

The captured packet demonstrates a standard HTTP GET request sent from a local machine (192.168.1.22) to a web server (23.213.235.27) as part of a network communication. At the **Data Link layer**, the Ethernet II protocol ensures the packet is transmitted between devices over the local network using MAC addresses. At the **Network layer**, the IPv4 protocol handles the routing of the packet between the source and destination IP addresses. At the **Transport layer**, TCP provides reliable data transfer, with acknowledgment and flow control mechanisms. Finally, at the **Application layer**, the HTTP protocol is used to request the file /connecttest.txt from www.msftconnecttest.com, likely as part of an internet connectivity check. This packet illustrates the seamless cooperation between network layers to facilitate communication.