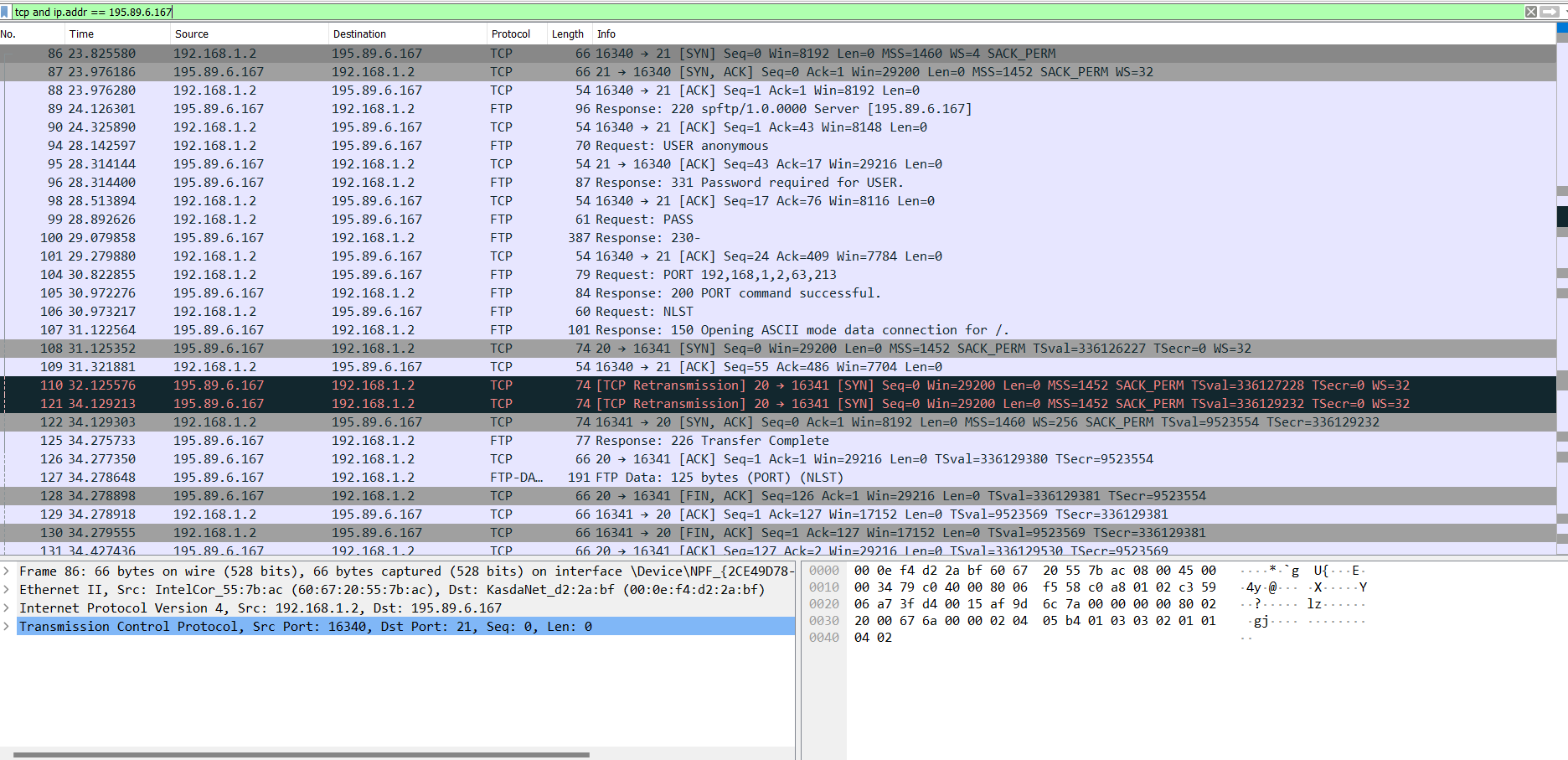
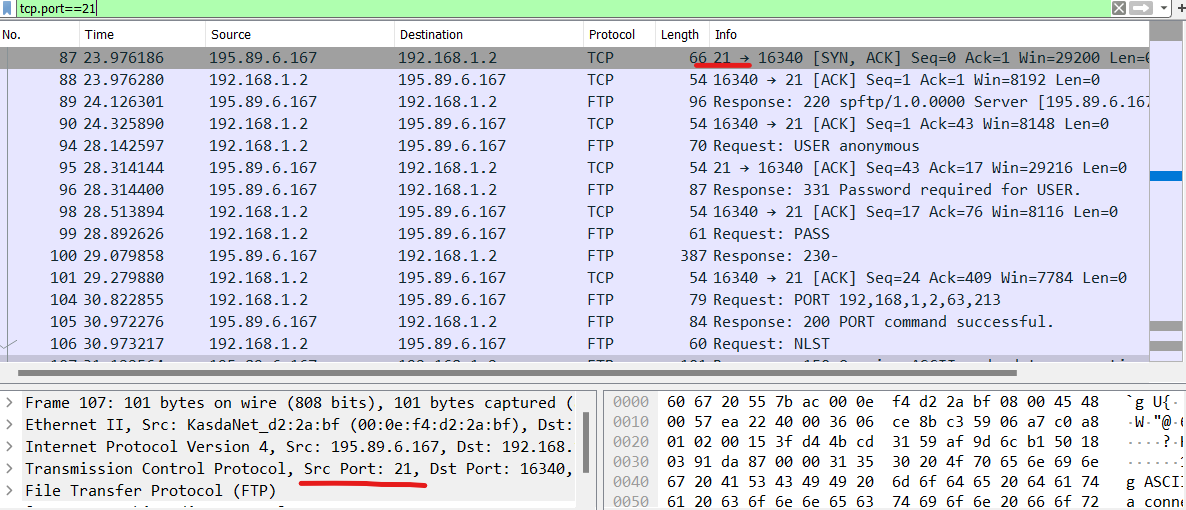
LAB - 4

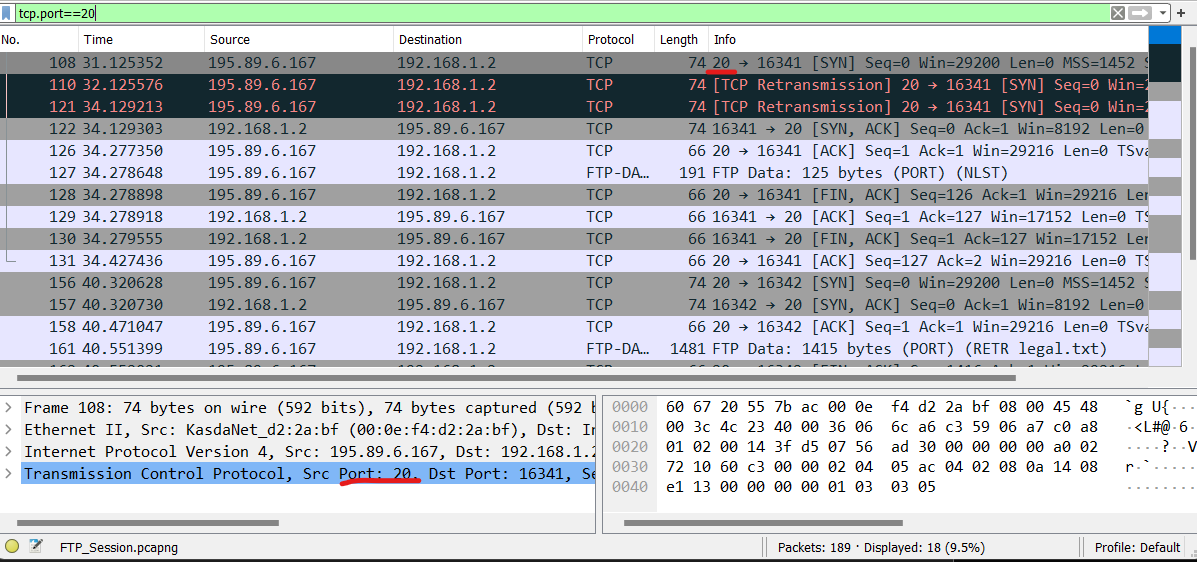
LAB STATEMENT 1



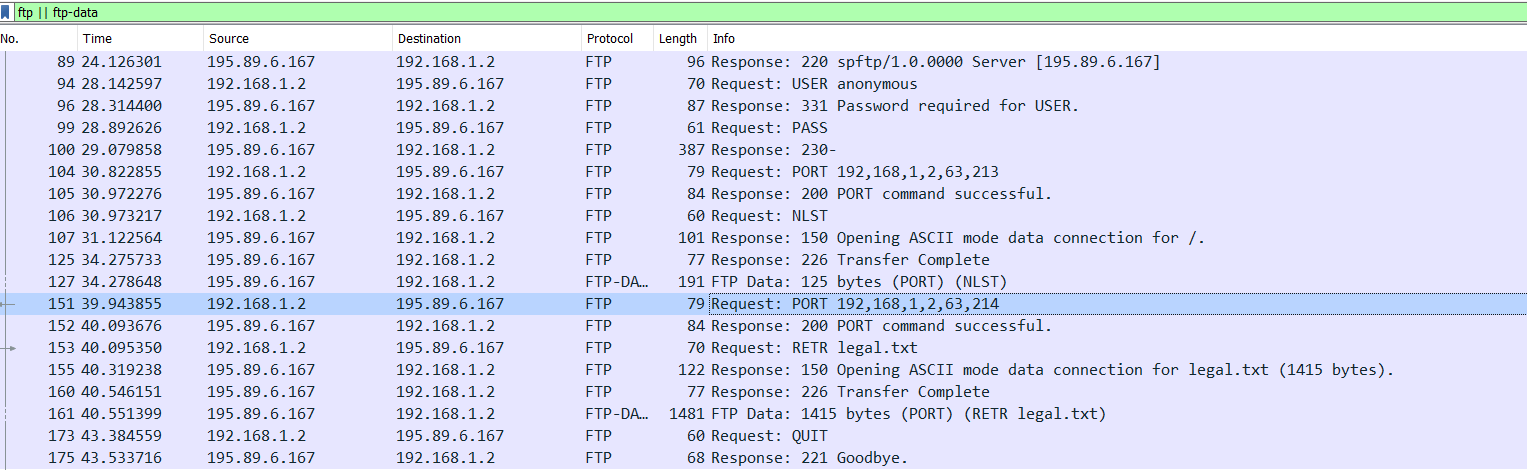
1. Port 21 is used to establish a connection and to send control bits using FTP protocol



Port 20 is used send data through network



2.



**Packet 89:** server respond that service is ready for new user

**Packet 94:** client enters anonymous in User

**Packet 96:** server responds with user name okay, need password

**Packet 99:** client enters empty password

**Packet 100:** server accepts the login credentials and process with displaying

230-

230- ---------------------------------------------------------------------------

230- WARNING: This is a restricted access system. If you do not have explicit

230- permission to access this system, please disconnect immediately!

230 ----------------------------------------------------------------------------

**Packet 104:** client asks server to send the data on IP:192.168.1.2 and Port:16341

**Packet 105:** server tells the client that port:16341 is connected successfully.

**Packet 106:** client enters ls command which sends NLST request to the server

**Packet 107:** server tells the client:  
 Opening ASCII mode data connection for /.

**Packet 125:** server tells that transfer was successful and is closing the connection

**Packet 127:** server sends 11 line-based text data to the client which was asked using NLST

commonupdater\r\n

commonupdater2\r\n

commonupdater3\r\n

f20tools\r\n

legal.txt\r\n

licensed\r\n

products\r\n

pub\r\n

spamdefs\r\n

usage.txt\r\n

virusdefs\r\n

**Packet 151:** client asks server to send the data on IP:192.168.1.2 and Port:16342

**Packet 152:** server tells the client that port:16342 is connected successfully.

**Packet 153:** client asks to download legal.txt file by sending request RETR legal.txt

**Packet 155:** server tells the client:  
 Opening ASCII mode data connection for /.

**Packet 160:** server tells that transfer was successful an is closing the connection

**Packet 161:** server sends 1415 bytes long legal.txt file to client

**Packet 173:** client asks to end the communication using QUIT

**Packet 175:** server ends the connection and says Goodbye to the client

LAB STATEMENT 2

1. ICMP is a connectionless protocol. Messages are not sent over UDP or TCP

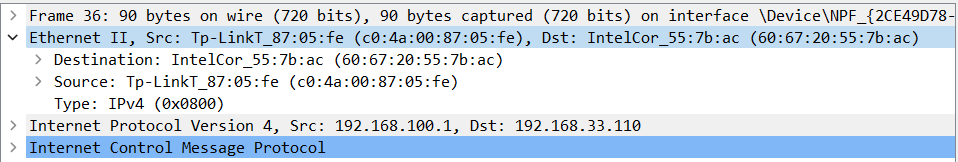
A screenshot of a computer

Description automatically generated

1. Link-layer address of hosts are:

**Source:** Tp-LinkT\_87:05:fe (c0:4a:00:87:05:fe)

**Destination:** IntelCor\_55:7b:ac (60:67:20:55:7b:ac)



1. Echo (ping) request are sent through these ICMP packets to test connectivity



1. Four Echo requests are sent through the host in packet no 48, 77, 101, 135
2. IP address of host: 192.168.33.110

IP address of dest: 172.217.27.36



1. ICMP packets do not have source and destination port numbers because ICMP operates at the network layer of the OSI model, while source and destination port numbers are associated with transport layer protocols like TCP and UDP.
2. The “ttl” value differentiates ICMP request message from ICMP reply message. For request: ttl = 128, For reply: ttl = 52

 A close up of text

Description automatically generated

1. ICMP type: 8 , ICMP code: 0. Moreover it has Checksum, Identifier, Sequence number and Data.

Number of bytes of checksum: 2

Number of bytes of identifier: 2

Number of bytes of sequence number: 2

1. ICMP type: 0

ICMP code: 0

Moreover it has Checksum, Identifier, Sequence number and Data.

Number of bytes of checksum: 2

Number of bytes of identifier: 2

Number of bytes of sequence number: 2

1. ICMP type: 3

ICMP code: 3

LAB STATEMENT 3

1. A network sniffer, known as a packet analyzer or network traffic interceptor, serves as a software or hardware tool within a computer network. It actively intercepts and records the flow of network data passing through a specific network location. Its central purpose revolves around capturing and scrutinizing data packets to furnish insights into network activities, resolve issues, and oversee network performance and security.
2. The packet sniffer seizes data packets during their journey across a network. Upon capture, it proceeds to evaluate the content of each packet, encompassing the examination of packet headers and payload. This analysis involves the extraction of pertinent details, such as source and destination IP addresses, port numbers, protocol types (e.g., TCP, UDP), and payload data. The sniffer interprets and deciphers packets based on the employed protocols, understanding the structural nuances of diverse protocols (e.g., TCP, UDP, ICMP) and retrieving pertinent information for analysis. The packet sniffer then archives the captured and analyzed data, offering the option to store it for subsequent review or analysis. Packet sniffers extend the capability to filter captured packets according to precise criteria (e.g., IP addresses, protocols, port numbers).
3. Tools like Wireshark, which are packet sniffers, assume a pivotal role in network troubleshooting and monitoring. They emerge as indispensable aids in the identification and resolution of network issues, the diagnosis of connectivity problems, and the pinpointing of errors through the capture and examination of network traffic. Furthermore, they prove invaluable in monitoring bandwidth consumption, singling out applications that strain resources, and optimizing network performance. The extensive capabilities of Wireshark render it a precious asset for network professionals, simplifying network management and the resolution of issues.
4. In the context of Wireshark, a "capture filter" emerges as a mechanism facilitating the selective capture of network packets predicated on predefined criteria, which may include IP addresses, port numbers, or protocols. This feature lends itself to the efficient focus on pertinent traffic during analysis, particularly in settings characterized by high volumes of network activity. Consequently, it enables more effective network monitoring and troubleshooting.
5. Network security and privacy introduce ethical considerations concerning packet sniffers, emphasizing concerns about unauthorized interception of sensitive data that infringes upon privacy and confidentiality. Such interception may lead to encroachments on privacy, risks to data security, legal non-compliance, absence of informed consent, and potential misuse or abuse. These ethical concerns underscore the imperative of deploying packet sniffers in a responsible and lawful manner, emphasizing the respect of individuals' privacy and the safeguarding of data.
6. In the case of Wireshark, it boasts the capacity to decode an extensive array of protocols and technologies. This encompasses decoding for Ethernet frames, both IPv4 and IPv6, TCP, UDP, HTTP, DNS, SSL/TLS, SMTP, and more. It offers valuable insights into network communication, encompassing source and destination addresses, ports, headers, and payload data for these protocols. This capacity significantly aids in the analysis and troubleshooting of network issues.