CS3009D: NETWORK LABORATORY

Assignment 2 - Network Analysis

Adeeb Hadi Seeyad (B190737CS)

Introduction

This assignment uses a packet sniffer, Wireshark. Wireshark is a free open source network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and displays them in human-readable format. It provides many advanced features including live capture and offline analysis, three-pane packet browser, coloring rules for analysis.

Answers

Answer 1

1. Get the IP address

First it fetches an ip address corresponding to the domain name ‘minerva.nitc.ac.in’ from the default DNS server.

	IP Address
Client (Host machine)	196.168.0.112
Server (Minera NITC)	103.160.223.7

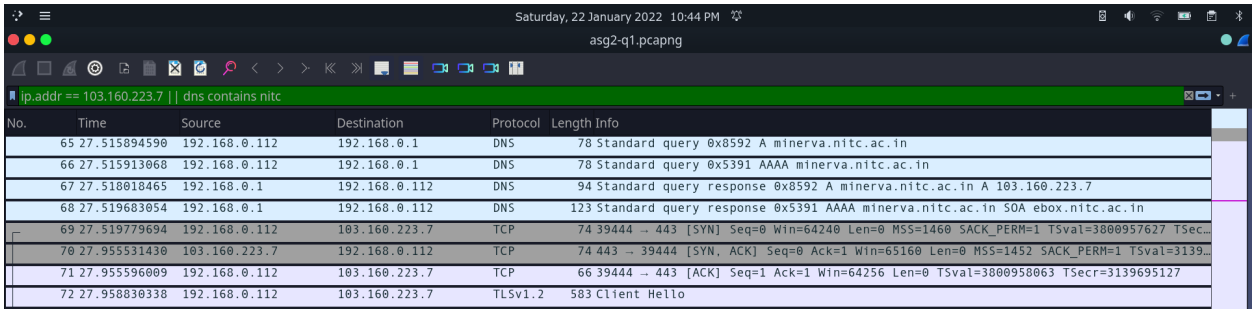
2. Establish the connection

Establishes a connection to the minerva.nitc.ac.in server with a three way handshake ie,

I. The client sends a segment with SYN bit set and a random sequence number.

II. The server returns a segment with ACK and SYN bits set and a new random number as sequence number and acknowledgement number as the number previously sent by the client plus an offset of 1.

III. The client sends a segment with ACK bit set to acknowledge the server's packet.



3. Negotiate secure exchange of data

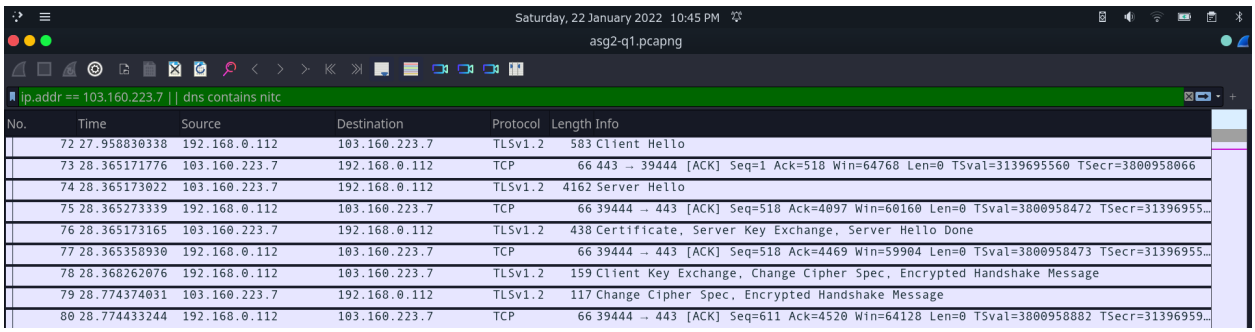
The client and the server use a hand-shake protocol to negotiate on how to securely exchange data over the internet.

I. Client sends a **client hello** message that lists information such as TLS version, the cryptographic algorithms and the data compression methods supported by the client machine.

II. Server responds with a **server hello** message that chooses TLS version 1.2, a cryptographic algorithm from the list sent by the client, session ID etc.

III. Server sends its public key to the client in a process known as **server key exchange** and the server hello is completed.

IV. Client sends it's private key to the server encrypted by server's public key in a process known as **client key exchange**.



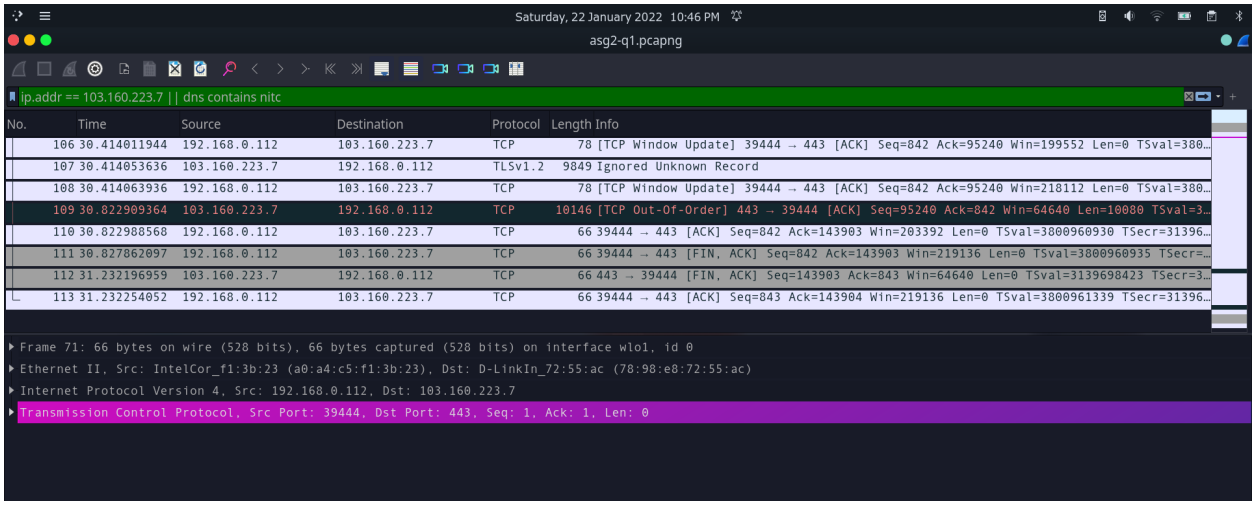
4. Data transfer

Data is transferred from server to client using TLSv1.2 protocol in the application layer and once the packet is received by the client it sends the server a TCP segment with ACK bit set to acknowledge that the right packet is received without any error. The sequence numbers and acknowledgement numbers are updated according to the data being transmitted.

5. Connection termination

When the client has finished downloading the PDF it initiates a connection termination for a graceful connection release.

I. The client sends the server a segment with FIN bit set which implies the client doesn't have any more data to send to the server.
II. The server sends back a segment with FIN and ACK bits set to acknowledge the client's segment and to close the connection.
III. The client sends a segment to the server with ACK bit set to acknowledge the server's segment and the connection is closed.



Answer 2

Sub answer a

IP address of source - 192.168.44.53

IP address of destination - 192.168.44.1

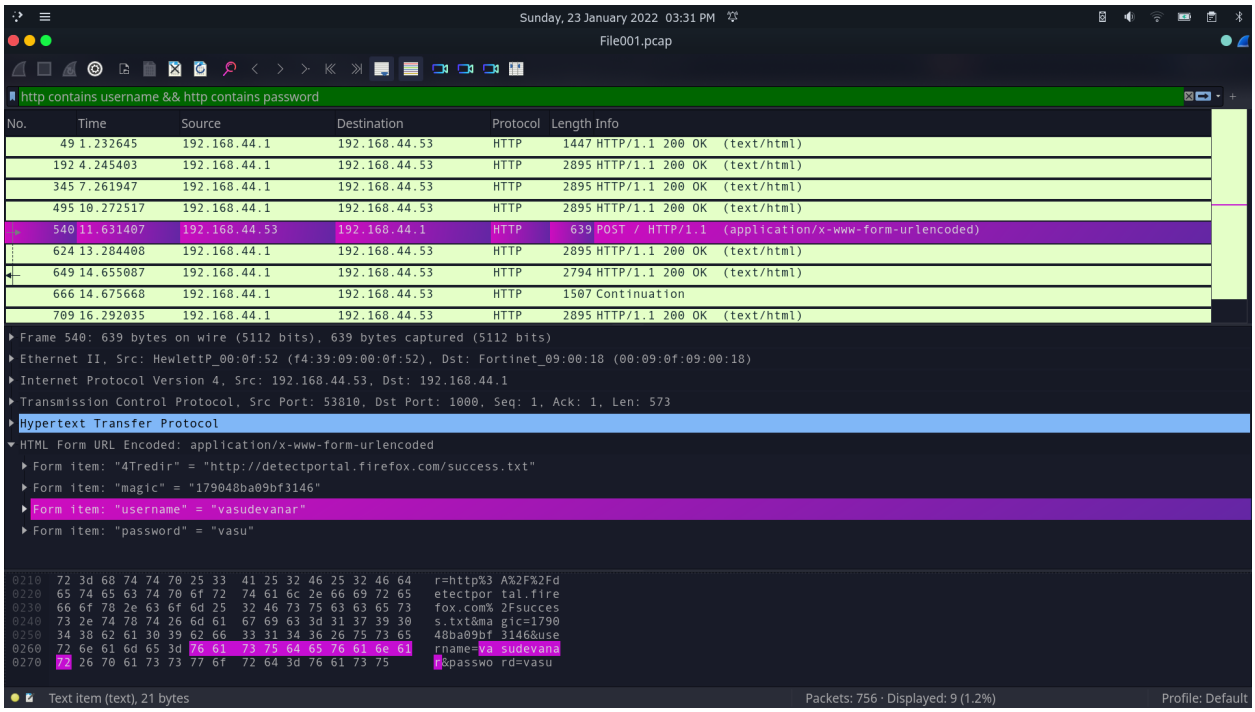
Sub answer b

HTTP was the protocol used

Sub answer c

Username - vasudevanar

Password - vasu



Answer 3

Packet 27

443								59138
3056868986								
1084580465								
5	0	0	1	0	0	0	1	60
0x5442								0
0								
0								

Packet 32

59138								443
1660956066								
3861199010								
5	0	0	1	0	1	0	0	0
0xfaec								0
0								
0								