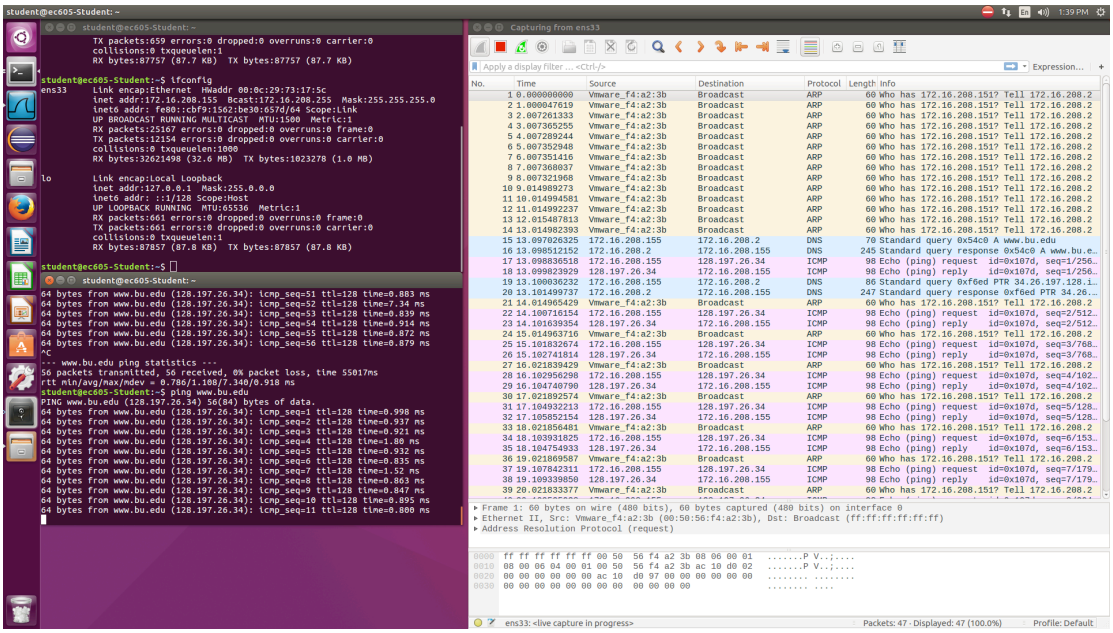
Lab7 Report

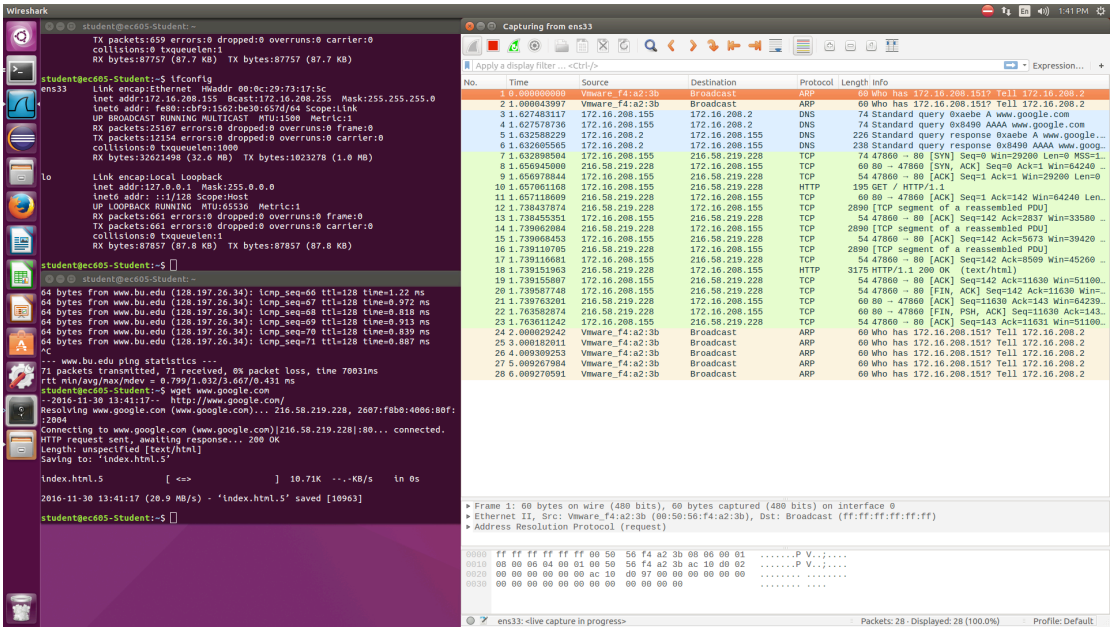
Jiahao Chen

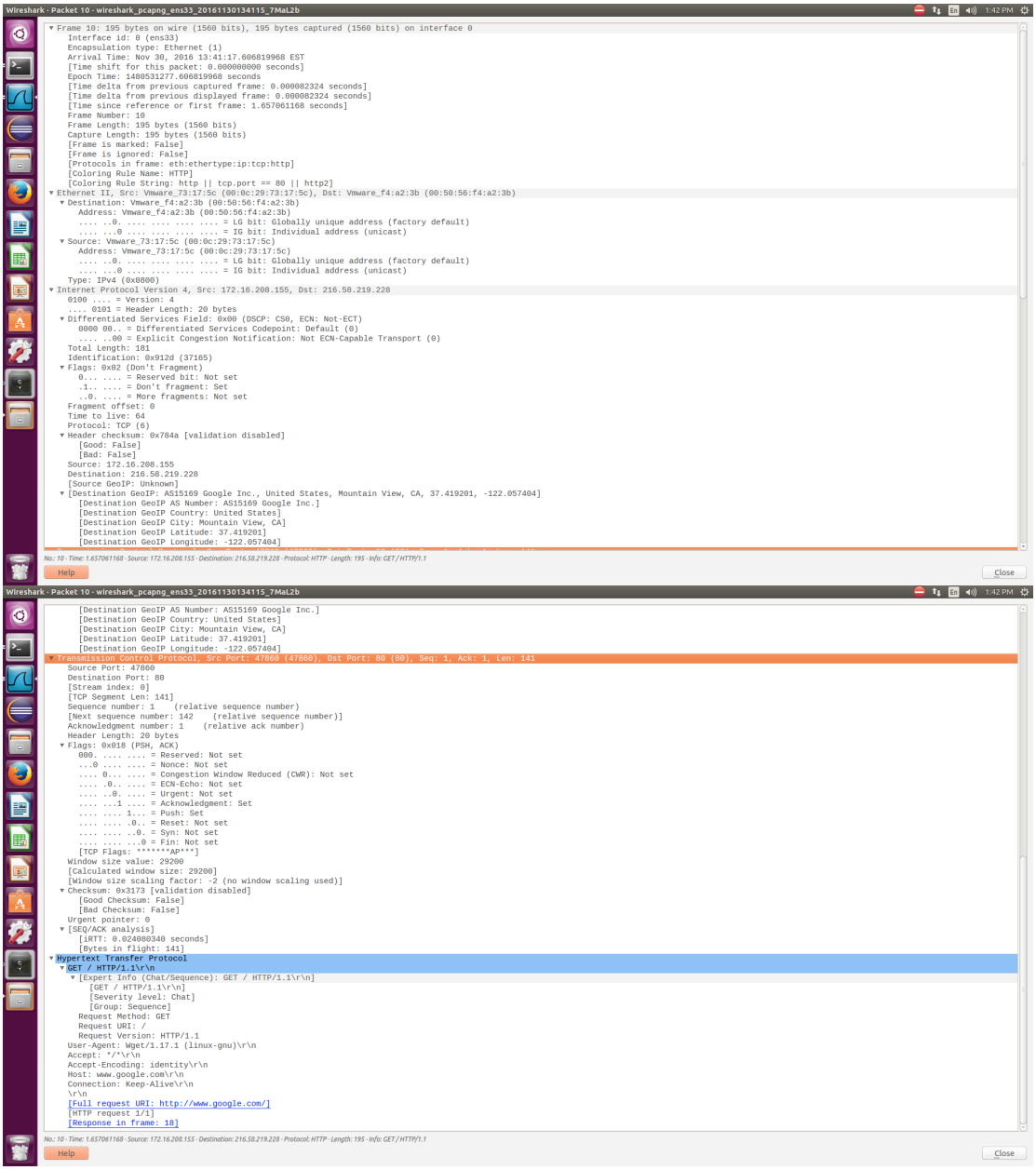
Task 1



1. The ICMP protocol is used when performing a ping command.
2. The information that if the server is available is transferred in this protocol. It is used to get response on TTL(Time to live).

Task 2

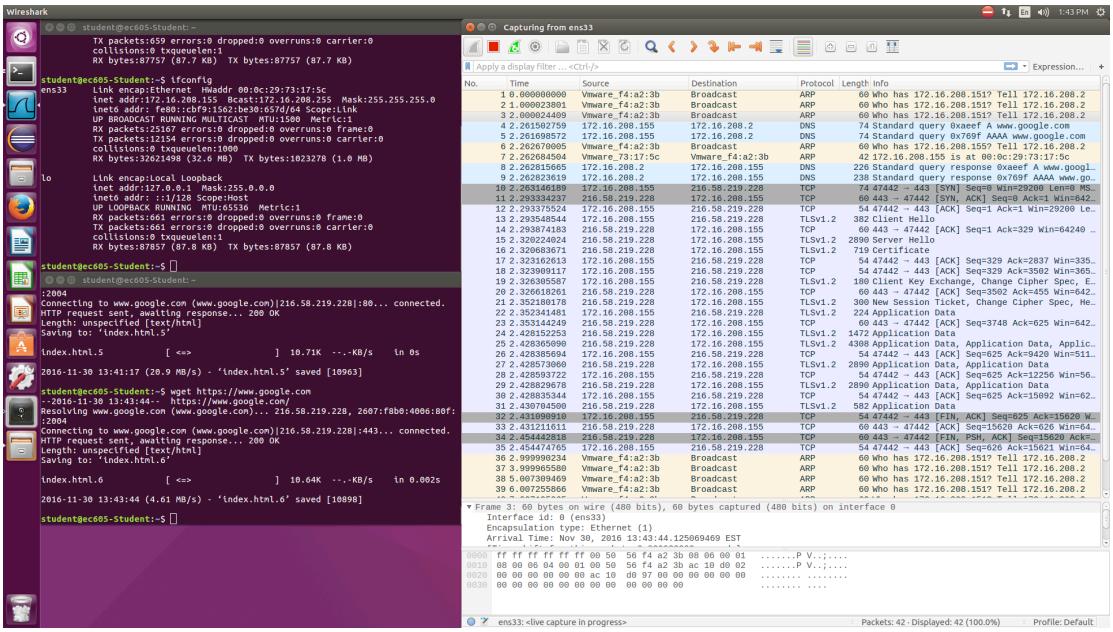




1. 216.58.219.228
2. 00:50:56:f4:a2:3b
3. 4
4. Source Port: 47860

   Destination Port: 80
5. Wget/1.17.1
6. 0x02

Task 3



Compare:

The https connection has TLS in the communication and the port is 443 rather than 80. And during the communication, the data will not be sent until the client and server both sent Hello to each other. In this way, it is much safer.

Packets:

1) Client Hello: the sender(client) send the confirmation to receiver(server) in order to figure out if it is the correct receiver.
2) Server Hello: the receiver(server) send the confirmation to sender(client) in order to tell the sender if it is the correct receiver. Besides, it responds a random number which will be used to create the key. And it generates the session ID and the way to encrypt the data.
3) Certificate: It is used to verify if the server is the correct one.
4) Certificate Key Exchange: In the TLS protocol, every communication between client and server is encrypted. The key is used by both client and server to decrypt the message sent by each other. The certificate key exchange is used to provide parameters for encryption.
5) Change Cipher Spec: It tells the server that the message will be encrypted before sending. This also use random numbers to calculate the key to encrypted data.
6) New Session Ticket: It is used to restore the communication between client and server.
7) Application Data: It the encrypted data.

Task 4

1.

1) 192.168.1.17, 128.197.26.34, 74.125.29.189, 216.58.219.238
2) 192.168.1.17
3) 192.168.1.17: Internet Assigned Numbers Authority
   128.197.26.34: Boston University
   74.125.29.189: Google Inc.
   216.58.219.238: Google Inc.

2.