CSE 3231 – Fall 2020 Assignment # 2 Due: before midnight on Tuesday, Sept. 29

You can complete this assignment in CloudShark:

Answer the following questions and submit your report in Canvas by the due date shown above.

https://www.cloudshark.org/captures/d8b7d3c4bcce

You can use the CloudShark User Guide for information on using filters and analysis tools:

https://support.cloudshark.io/user-guide/

Information about the traffic in the capture file:

1. How many packets are in the capture file?
2. What is the average packet size (in bytes)?
3. What are the dates and times the capture began and ended?
4. What is the size (in bytes) of the largest frame or packet in this traffic capture file?
5. List all of the IP addresses found in this capture file.
6. How many ARP frames were transmitted (count both request and reply messages)?
7. The ARP requests are seeking the MAC address for a certain IP address. What is the MAC address that the ARP requests are seeking?

Information about the FTP traffic in the capture file:

8. What is the IP address of the FTP server?
9. How many separate FTP connnections were there between 172.16.31.3 and the FTP server?
10. What version of FTP Server software was used?
11. What is the username and password for the FTP connection from 172.16.31.3 to the server?

Information about the email (SMTP) traffic in the capture file:

12. What is the MAC address for the email (SMTP) server?
13. Find all of the email messages that were sent between 172.16.31.3 and the email server and list all of the individual email addresses that were used.
14. When an email client connects to an email server, the server sends a message to the client, what is this message (hint: the first line of the exchange of messages)?
15. The email server puts a number in front of each SMTP command that it sends to the client. What is the text that follows the command that starts with *354*?