- **Question 1:** What does FTP stand for? What does RFC stand for? What are RFCs, and who issues them? (Search for answers to these questions on the internet, and cite your sources)

FTP stands for file transfer protocol. RFC stands for requests for comments. It is issued by the Internet Engineering Task Force (IETF). (https://en.wikipedia.org/wiki/Request_for_Comments).

- **Question 2:** Use `grep` on the UDP RFC to **list all the line numbers of the file** where the word "Internet" appears. Include the command that you used to generate this output in your answer to this question.

grep -n Internet rfc768.txt

18:protocol assumes that the Internet Protocol (IP) [1] is used as the

138:The major uses of this protocol is the Internet Name Server [3], and the

144:This is protocol 17 (21 octal) when used in the Internet Protocol.

150:[1] Postel, J., "Internet Protocol," RFC 760, USC/Information

156:[3] Postel, J., "Internet Name Server," USC/Information Sciences

- **Question 3:** Use `grep` on the TCP RFC for the word "RFC" to output **how many times the word occurs**. Write both the command and the output of that command when used on the TCP RFC file .

grep "RFC" rfc793.txt -o | wc -l

5

Question 4: Run ping from both your local machine and the Khoury servers to the www.northeastern.edu. several times on both machines. (Ctrl-C will stop ping.) Read man ping and then explain, based on what ping is doing, and you think why the times from your local machine and the Khoury servers to www.northeastern.edu. are different (you may have to make an educated guess about why they're different, but you can make a very good guess!)

The ping command uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. They are different because when

ping www.northeastern.edu, local machine and Khoury remote server do not go through the same network paths, and they are not in same internet condition, Khoury server is faster because it goes through shorter network paths.

Question 5: Which internet protocol is SSH built on top of?

The latest version of SSH, version 2, consists of three protocols:
SSH-TRANS, a transport layer protocol
SSH-AUTH, an authentication protocol
SSH-CONN, a connection protocol
SSH-TRANS provides an encrypted channel between the client and server machines, and it runs on top of a TCP connection
(https://book.systemsapproach.org/security/systems.html#secure-shell-ssh)

Question 6: What algorithm does SSH use during authentication when a client authenticates a server for the first time, when the secure channel is being established? What algorithm does SSH use after authentication?

The two machines establish this secure channel by first having the client authenticate the server using RSA, which is Rivest–Shamir–Adleman.

Once established, SSH commonly uses the The AES Encryption algorithm (also known as the Rijndael algorithm.
https://book.systemsapproach.org/security/systems.html#secure-shell-ssh