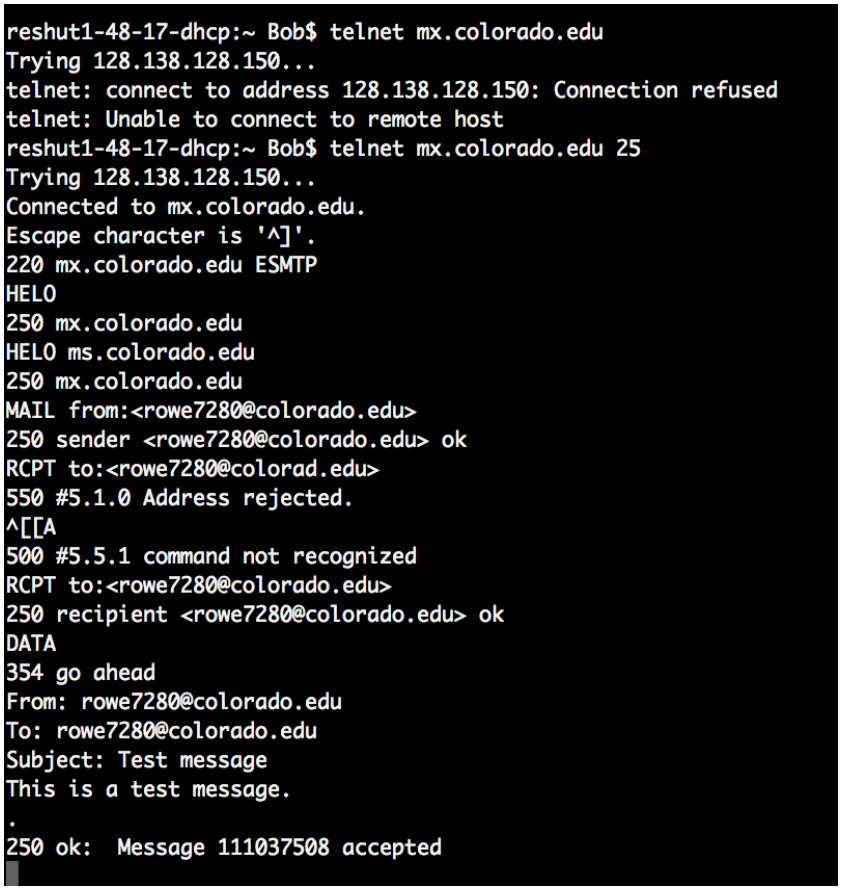
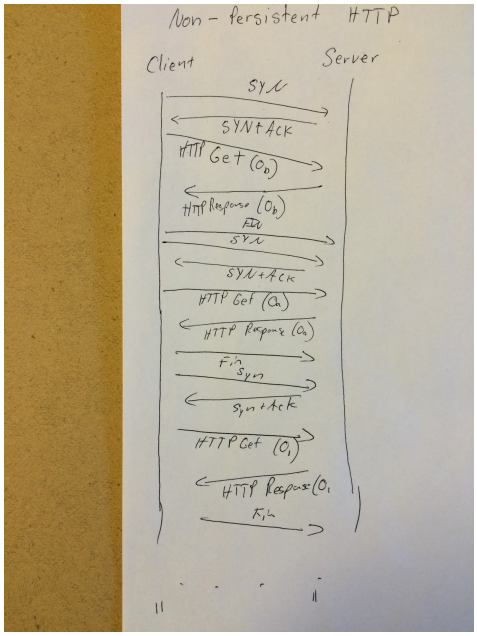
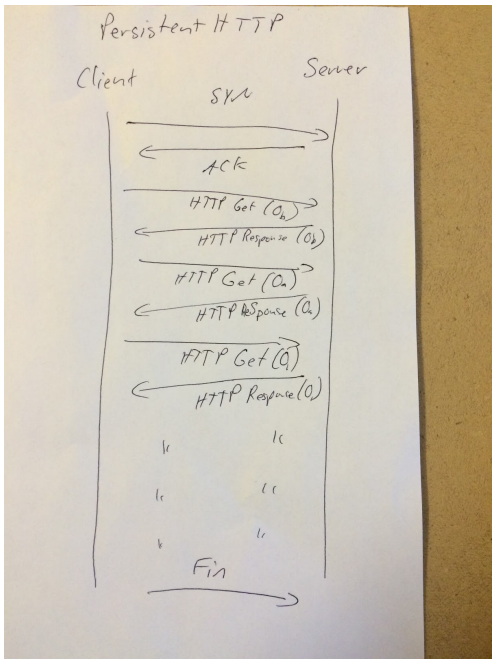
CSCI 4273: Homework 2

1. SMS uses a client/server architecture where messages from one client are sent and received by a server to other clients. Different types of SMS include Application-to-Person SMS where, for example, a bank can automatically alert you to unusual bank account activity and Multimedia SMS where pictures can be sent and received through text messages.

2. 

3. Persistent vs. Non-persistent http

a. 

b. 

4. A *whois* database is a registry of who owns domains and ip addresses.
    a. whios.net
        i. nameserver for google.com
            1. ns1.google.com
            2. ns2.google.com

b. who.godaddy.com
    i. nameserver for google.com
        1. ns1.google.com
        2. ns2.google.com

5.

a. Well-known port numbers
    i. NNTP
        1. 119
    ii. NETBIOS
        1. 139
    iii. ISO-IP
        1. 147
b. IANA manages the dns root zone, i.e. .uk or .com, and who contains information about those domains. They process requests that concern top-level domain delegation.

6. root-servers
    a. Data rate
        i. max
            1. incoming and outgoing max occurred around week 39 which I believe is towards the end of september
        ii. min
            1. incoming and outgoing min appears to have occurred at week 35 which I believe was in august

b. There is more than a hundred thousand byte difference in the amount of data being sent via IPv4 than IPv6. Significantly more data is being sent with IPv4.

7. Definition and Views
    a. Definition
        i. Key Escrow - Third parties have access to cryptographic keys not belonging to them.
        ii. Mandatory Key Disclosure Law - Individuals must surrender cryptographic keys to law enforcement.
        iii. Mandatory Decryption Law - Owners of encrypted data must give decrypted data to law enforcement.
    b. Opinion
        i. I try to follow the law the best I can. I do not try to purposefully break the law in order to subvert the authority of the government and law enforcement or the principles that the United States stands for. If information is requested I will supply it.
8. Exercise 14
    a. Chrome trusts certification authorities supplied by my operating system.
    b. I have no reason to not trust any of the agencies who act as certification authorities.
    c. When you disable a trust you get warnings about websites' identities being unverifiable.
9. If there is a firewall blocking ports that ftp may use, you won't be able to download a file from an outside server. You can use the passive mode of ftp to get around this which

lets you use an arbitrary port on your side to create an ftp connection to a server and port.

10. A digital signature uses a mathematical scheme to demonstrate the authenticity of a message while user authentication relies on a username and password to authenticate an identity. An example of user authentication is having to login to facebook while an example of a digital signature is receiving an email that has been digitally signed and is from the person it says it's from.