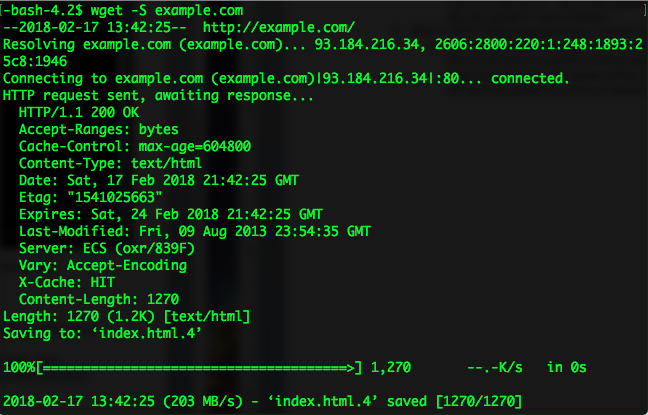
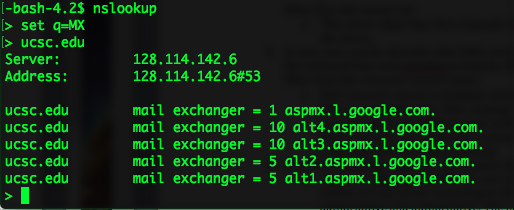
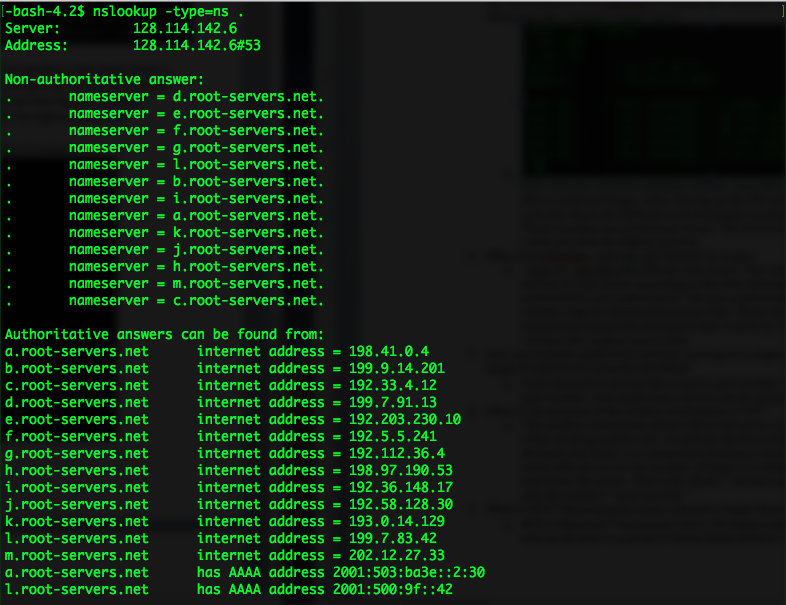
Kevin Loi

CMPE 150

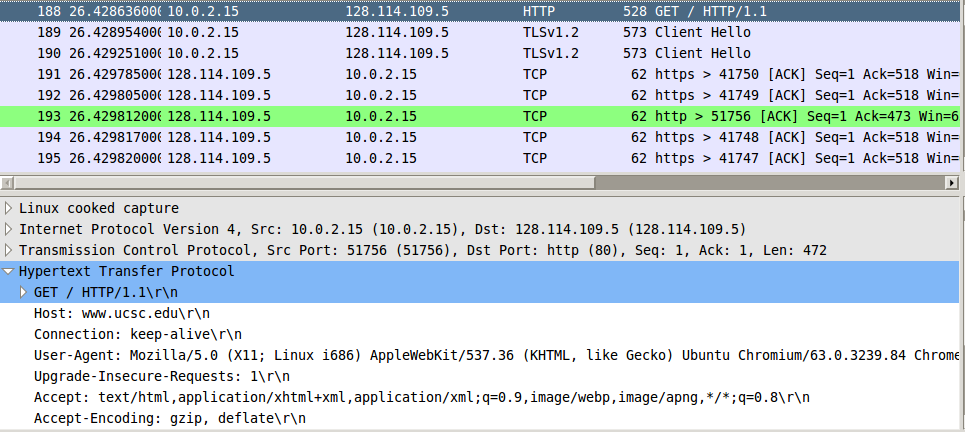
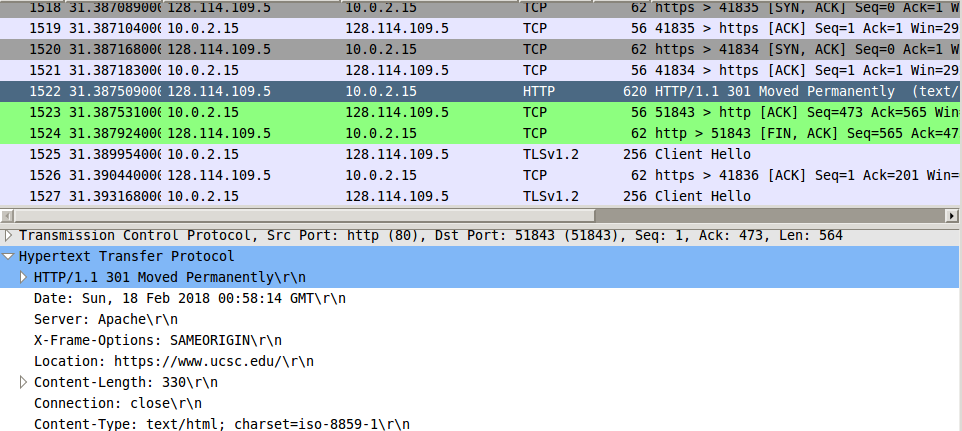
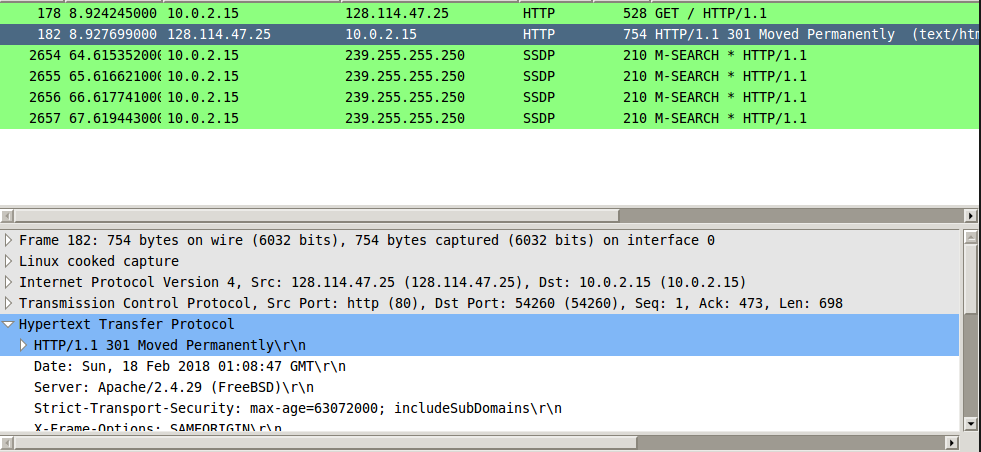
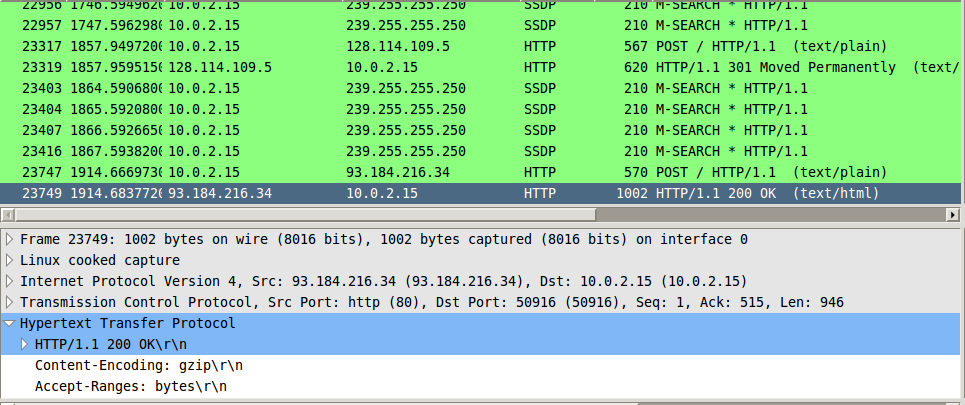
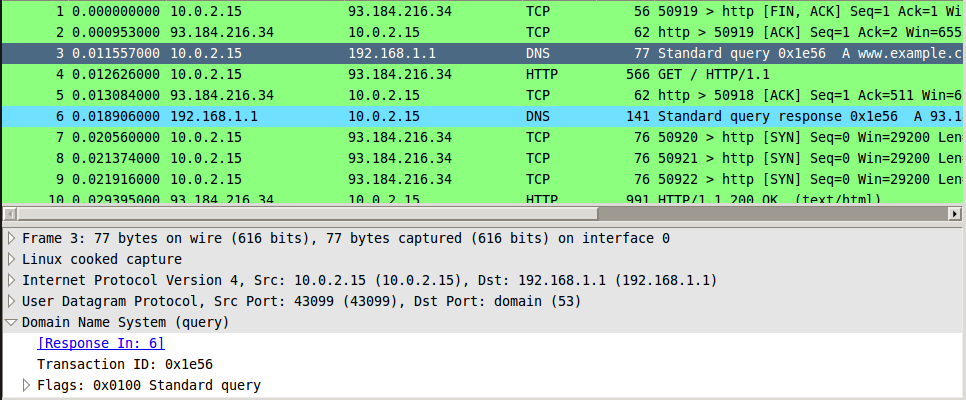
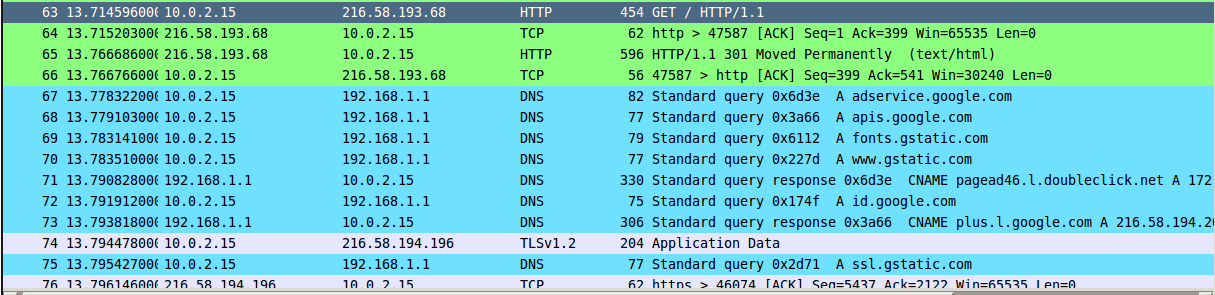
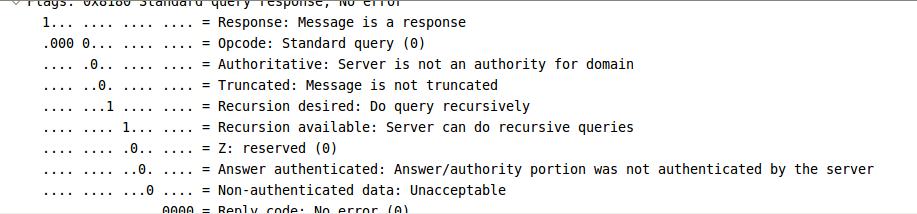
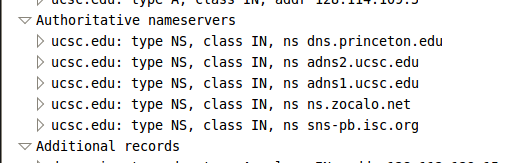
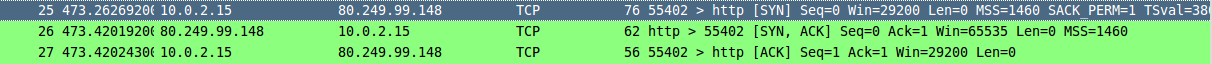
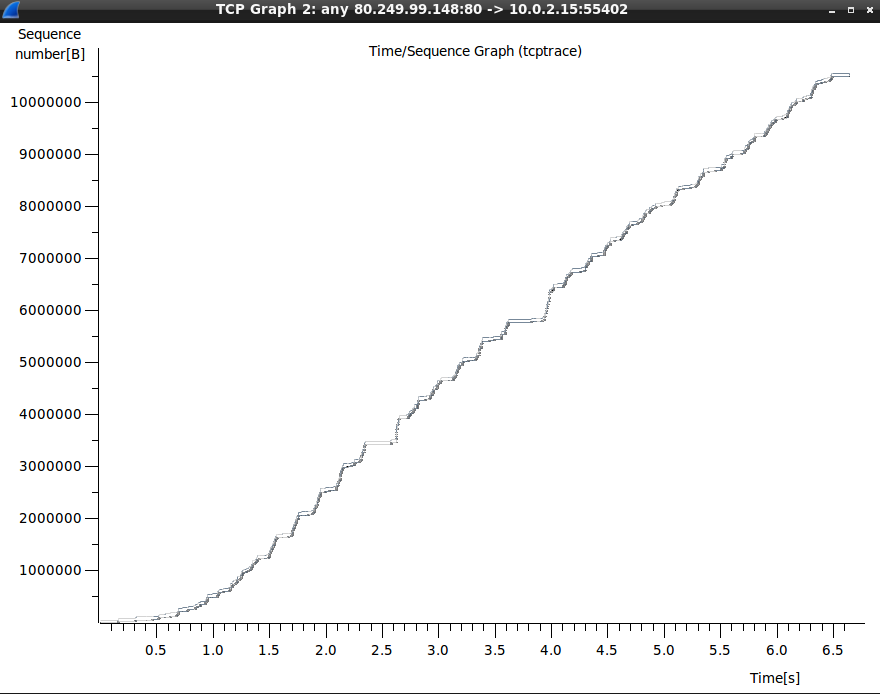
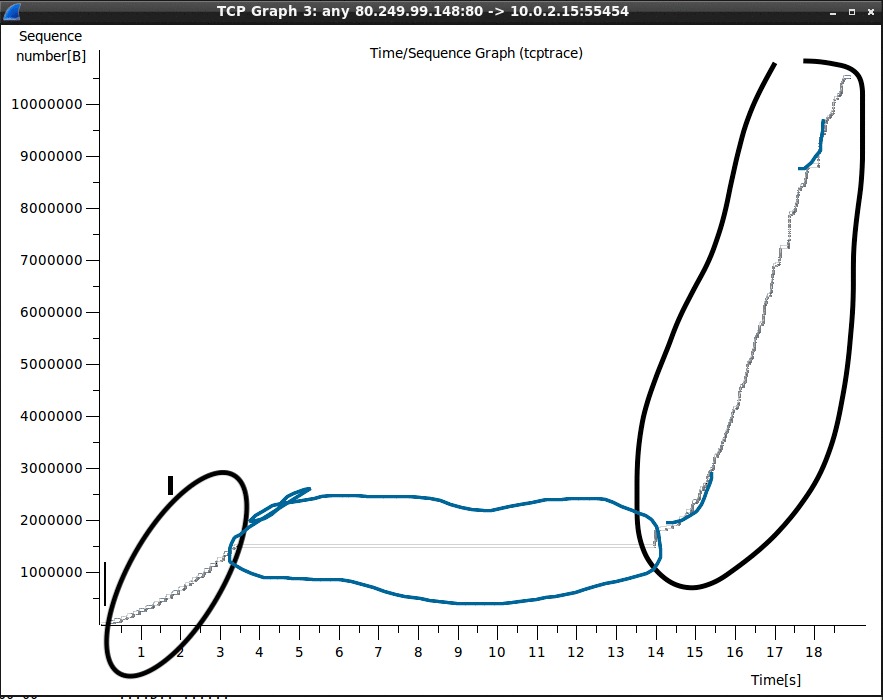
2/16/18

Pre-Lab & Lab 2 Solutions

Pre-Lab 2

1. Choose 5 HTTP status codes and describe each one.
   1. 200 – OK. Shows Request was successful.
   2. 301 – Moved Permanently. Request object moved, new location later specified in message.
   3. 400 – Bad Request. Request message not understood by server.
   4. 404 – Not Found. Request document not found on this server.
   5. 410 – Gone. Target resource is no longer reachable/available.
2. List the 8 HTTP 1.1 methods and explain what they do
   1. OPTIONS – Requests information about communication options. Allows client to see what options they can use with the request.
   2. GET – Retrieves specific information for Request
   3. POST – Submits data to be processed from a specified source
   4. DELETE – Deletes a specified resource
   5. HEAD – Requests data from a specified source but only returns HTTP headers and no document body
   6. PUT – Uploads a representation of a specified URI
   7. TRACE – Invoke a remote, application layer loopback of a request message
   8. CONNECT – Converts the request connection to a transparent TCP/IP channel
3. Use *wget* on *example.com* to view the last modified date of the webpage. What was the HTTP return status given and what command was used to do this?
   1. HTTP return status given is 200 OK. The command used to do this is “wget –S <http://example.com>”
4. Look up the *telnet* command. Use *telnet* to connect to *towel.blinkenlights.nl*. What does this server do?
   1. This server plays Star Wars Episode IV. Uses ASCII animation to lay the movie.
5. In your own words, describe what DNS resource record (RR) is. Now using the command line tool *nslookup* to find the MX resource record of *ucsc.edu.* What does this resource record mean?
   1. DNS resource record is database entries, separated by the data types. MX is a mail exchanger. After looking up the MX resource record of ucsc.edu, there are different mail exchanger numbers (1, 10, 10, 5, 5). Those numbers are preference values. The lowest preference number is the one with the highest priority.
6. What does *nslookup –type=ns* *.* do? Explain its output.
   1. –type-ns . specifies the DNS for root server. The output provides name servers of root server according to the DNS information. There is non-authoritative and authoritative. The non-authoritative ns does not contain original information/source files. Those are temporary/cached files that have been looked up. Authoritative ns contains the original source files.
7. How can multiple application services running on a single machine with a single IP address be uniquely identified?
   1. Each application service has a source port number. With the source port number, each application service can be uniquely identified.
8. What is the purpose of the window mechanism in TCP?
   1. The window mechanism allows client and server to communicate when sending packets over. It controls the flow of data/packets between two hosts. In a connection between a client and a server, the client tells the server the number of bytes it is willing to receive at one time from the server. This is the client’s “receive window” which is also the sender’s “send window.”
9. What is MTU? What happens when a packet is larger than the MTU?
   1. MTU is Maximum Transmission Unit is the largest sized frame or packet that can be sent in a packet or frame-based network. When a packet is larger than the MTU, the packet will be sent, but the network interface will send the packet in a series of network transmissions.

Lab 2

1. Find the HTTP packet that corresponds to the initial request that your computer made. Take a screenshot of this packet. What HTTP method did your computer use to make this request? What URI did your computer request from the server?
   1. GET method, URI = <http://www.ucsc.edu>
2. Find the HTTP packet that corresponds to the initial response the server made to your request. Take a screenshot of this packet. What HTTP status code did the server return? What is the content type of the response the server is sending back?
   1. Status Code: 301 Moved Permanently. Content Type: text/html
3. Find the HTTP packets that correspond to the initial request and response that your computer made. Take a screenshot of these packets. What’s different? Explain.
   1. The response status of the code received is 301 Moved Permanently, which indicates the link requested moved permanently to the URL given by the location header.
4. Using HTTP Chromium, Take a screenshot of your packet, and explain what you did to create it.
   1. I googled POSTMAN, which is an extension from Chrome. I used POSTMAN to create a POST Request. I did a POST request for <http://ucsc.edu>, and <http://example.com>. They both worked, as you can see in the screenshot.
5. Were any steps taken by your computer before the web page was loaded? If so, using your captured packets in Wireshark, find the packets that allowed your computer to successfully load <http://www.example.com>. Take a screenshot of these packets, and explain why you think these are the correct packets. If not, explain why your computer did not need to take these steps.
   1. After sending a request for example.com, the browser checks the cache to see if there is any DNS that matches the domain name. The dark blue line does that. The light blue line sends a DNS query response. These are the correct packets, because they follow the procedure of checking the cache before connecting with DNS root servers, top-level domain name servers, and authoritative name servers.
6. In Chromium, navigate to <http://216.58.193.68>. Were any steps taken by your computer before the web page was loaded? If so, using your captured packets in Wireshard, find the packets that allowed your computer to successfully load <http://216.58.193.68>. Take a screenshot of those packets, and explain why you think these are the correct packets. If not, explain why your computer did not need to take these steps.
   1. These packets are correct, because all the DNS queries map the IP address to google.com. There is a HTTP GET request, and after it gets the request, the DNS maps to google.com. Then it queries all the links within google.com, e.g. apis.google.com, fonts.gstatic.com, etc. These DNS queries are necessary to successfully load google.com from the IP address.
7. Open a terminal window. Using nslookup, find the A records for google.com. Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for google.com?
   1. Request was resolved, and the IP address is 172.217.0.46
8. Did your computer want to complete the request recursively? How do you know that? Take a screenshot proving your answer.
   1. Yes, the computer wanted to complete the request recursively. It says “Recursion desired”, with a 1, indicating that it did want to complete the request recursively.
9. Using nslookup, find the A records for cmpe150.ucsc.edu. Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for cmpe150.ucsc.edu?
   1. There was no IP address given. The DNS response returns no such name
10. What is the authoritative name server for the ucsc.edu domain? How do you know? Screenshot proving your answer.
    1. The authoritative name servers are dns.princeton.edu, adns2.ucsc.edu, adns1.ucsc.edu, ns.zocalo.net, sns-pb.isc.org, as stated in wireshark
11. Find the packets corresponding with the SYN, SYN-ACK, and ACK that initiated the TCP connection for this file transfer. Take a screenshot of these packets. What was the initial window size that your computer advertised to the server? What was the initial window size the server advertised to you?
    1. The initial window size that my computer advertised to the server was 29200. The initial window size the server advertised to me was 65535.
12. Find a packet from the download with a source of the server and a destination of your computer. Create a tcptrace graph with this packet selected. Take a screenshot of the graph and explain what it is showing. Look into the Wireshark documentation if you need assistance making this graph.
    1. This graph shows the how the data increases overtime. This stream moves in almost a linear fashion, growing almost linearly. The x-axis denotes the time, in seconds, and the y-axis denotes the sequence number in bytes. The slope of the line denotes the bandwidth. There are two lines, the lighter one is ACKs, and the darker line is the data sent. As the line gets steeper, the sequence numbers get higher, and more packets are being successfully sent.
13. Find a packet from the download with a source of the server and a destination of your computer. Create a tcptrace graph with this packet selected. Take a screenshot of the graph and explain what it is showing. Using and image editing program, circle the areas where the 0% loss is shown, as well as where TCP is in slow-start and congestion-avoidance.
    1. The black circles indicate where there was 0% loss. The blue circle indicates that there was 100% loss. The blue lines indicate where there is slow start/congestion avoidance. This graph shows the rate at which the packets are sent. In the beginning, the packets are sending at a steady rate. Then, after I changed dev to 100% loss, the sequence number remained the same, indicating that 100% of the packets were lost in that amount of time. Then the last part shows what happens after I changed dev back to 0% loss.