**CIDM 6340 Network Management & Information Security – Summer 2022**

**West Texas A&M University**

Homework #1

***[N.B: You can work with a team/group of MAX 5 students, but you need to submit your own Homework report. Also, please mention all group members name in the cover page]***

**Name : Joshua Correa, Burkleigh Hund, Karteek Kotamsetty, Anna Smith**

**Id:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Rubrics:**

*Full points:* Correct and complete answer.

*Partial points:* Correct but not complete answer.

*No points:* No answer or Incorrect AND incomplete answers.

**Q1. Book Chapter 20 [ 10 points: Network management]**

1. What do you mean by network management?
   1. Network management is the process of administering and managing computer networks. This discipline includes services such as fault analysis, performance management, provisioning of networks and maintaining quality of service. These tools help support the complexity of managing large networks that cannot be managed by human efforts alone.
   2. The requirements for Network Management include:
      1. Fault Management (enable the detection, isolation, and correction of abnormal operation of the OSI environment)
      2. Accounting Management (enable charges to align for managed objects)
      3. Configuration and Name Management (exercise control over, identify, collect data from, and provide data to managed objects to provide continuous operation of interconnection services)
      4. Performance Management (evaluate the behavior of managed objects and effectiveness of communication flow)
      5. Security Management (aspects essential to operating OSI network management correctly and to protect managed objects)
2. Briefly explain a simple network management protocol.
   1. Refers to a collection of specification for network management that include the protocol itself, the definition of the database and the associated concepts. It’s an application-level protocol.
   2. Key Elements include: Management station (manager), Agent, Management information base and Network management protocol
   3. From a standalone management station, a manager provides an interface to the network manager. The manager process achieves network management by using SNMP, which is implemented on top of UDP, IP and the relevant network-dependent protocols. Every agent must implement SNMP, UDP and IP. Also, agents have a process that interprets the SNMP messages and controls the agent’s MIB. If agent devices support other applications, such as FTP, TCP and UDP are required.
   4. From the management station, three types of SNMP messages are issues for the management application: GetRequest, GetNextRequest, and SetRequest. The first two are variations of the get function. All three are acknowledged by the agent via a GetResponse message, passed by the management application. The agent may also issue a Trap message in response to an event that affects the MIB and the underlying managed resources. Management requests are sent to UDP post 161, while the agent sends traps to UDP port 162.
   5. SNMP is connectionless so no ongoing connection is maintained between a management station and its agents. Each exchange is a separate transaction between them.

**Q2. CE Chapter-1 [ 15 points]**

1. How is personal information safeguarded?
   1. Through the use of devices such as Firewalls, proxy servers and intrusion detection systems and activities such as authentication and auditing. There are also network security paradigms such as: CIA triangle, Least privileges, perimeter security approach, layered security approach, proactive versus reactive and hybrid security method.
2. What are the vulnerabilities and how can you compute security risk?
   1. Vulnerabilities can present themselves in the form of viruses, unauthorized use of a system and in people like hackers, sneakers, etc. These vulnerabilities could result in some of the threats mentioned in the section below (c.).
   2. Computing Risk includes the following elements:
      1. Exposure Factor (EF) - % of value an asset lost due to an incident
      2. Single Loss Expectancy (SLE) – cost of single loss
         1. SLE = Asset Value (AV) \* Exposure Factor (EF)
      3. Annual Rate of Occurrence (ARO) - # of losses you suffer per year
      4. Annualized Loss Expectancy (ALE) – yearly cost due to risk
         1. ALE = Single Loss Expectancy (SLE) \* Annual Rate of Occurrence (ARO)
      5. Risk = Probability of Risk \* Cost of the Eventuality
3. Name different types of threats in computer network.
   1. Malware (virus, trojan horse, spyware, logic bomb), intrusions, security breaches, Denial of Service attacks, web attacks, session hijacking, DNS poisoning, insider threats

**Q3. CE Chapter-2 [ 10 points]**

1. Compare various connection methods and speeds used in networks. [Hints see table from ch2 slides].
   1. **DS0** – Standard phone line is the slowest connection type of 64Kbps
   2. 2 DS0 lines together provide the **ISDN** connection at 128Kbps
   3. 24 DS0 lines where 23 carry data + 1 carries info about the other lines make up the **T1** connection at a speed of 1.54 Mbps. Speed common for schools and businesses
   4. 672 DS0 line or 28 T1 lines make up **T3** with 43.2Mbps
   5. **OC3** – optical line which is fast at 155 Mbps but very expensive. Mainly found in telecommunication companies
   6. **OC12** – would compare to 336 T1 lines with speed of 622Mbps
   7. **0C48** – would compare to 4 OC12 lines with speed of 2.5Gbps
2. What are different error messages?
   1. 100 series – informational
   2. 200s – not seen because they indicate successful transaction
   3. 300s – redirects
   4. 400s – client errors
   5. 500s – server errors
3. Name five basic network utilities and give example of their functions.
   1. IPConfig – gets info about your system like IP address, subnet mask and default gateway
   2. Ping – tells if system is connected to network and how long for an “echo request” to arrive to host.
   3. Tracert – “ping deluxe” and has same syntax as ping. Shows every “hop” between host and destination address. Can be used by technicians and hackers.
   4. Netstat – shows network status and active connections
   5. NSLookup – connects to NSServer and executes dns related commands

**Q4. KS Chapter-1 [ 10 points] :**

1. What is network Management? What are Network Management Requirements? Briefly explain each of them.
   1. Network management is the process of administering and managing computer networks. This discipline includes services such as fault analysis, performance management, provisioning of networks and maintaining quality of service. These tools help support the complexity of managing large networks that cannot be manages by human efforts alone.
   2. The requirements for Network Management include:
      1. Fault Management (enable the detection, isolation, and correction of abnormal operation of the OSI environment)
      2. Accounting Management (enable charges to align for managed objects)
      3. Configuration and Name Management (exercise control over, identify, collect data from, and provide data to managed objects to provide continuous operation of interconnection services)
      4. Performance Management (evaluate the behavior of managed objects and effectiveness of communication flow)
      5. Security Management (aspects essential to operating OSI network management correctly and to protect managed objects)
2. Suppose Alice and Bob are sending packets to each other over a computer network. Suppose Trudy positions herself in the network so that she can capture all the packets sent by Alice and send whatever she wants to Bob; she can also capture all the packets sent by Bob and send whatever she wants to Alice. List some of the malicious things Trudy can do from this position.
   1. Trudy can breach confidential information that is meant to be exchanged between Alice and Bob. She can also send false information or malicious files to each person who might trust the received information thinking it came from a trusted source. Trudy can also block the messages from going through (DoS) so that end users never receive the information intended for them. Trudy can choose to blackmail or exploit sensitive information gained through this position. Trudy can also gain some personal information from each user to create a fake identity.

**Q5. KS Chapter-2 [ 15 points]** Consider a short, 10-meter link, over which a sender can transmit at a rate of 150 bits/sec in both directions. Suppose that packets containing data are 100,000 bits long, and packets containing only control (e.g., ACK or handshaking) are 200 bits long. Assume that N parallel connections each get 1/N of the link bandwidth. Now consider the HTTP protocol, and suppose that each downloaded object is 100 Kbits long, and that the initial downloaded object contains 10 referenced objects from the same sender.

a. Would parallel downloads via parallel instances of non-persistent HTTP make sense in this case? Now consider persistent HTTP. It would not be ideal to use parallel downloads in non-persistent HTTP because they will slow down the bandwidth by having to share it for each object. Bandwidth would be 150bits/sec divided by 10 objects = 15bits/sec per download.

For non persistent HTTP:

The time it would take to send the first packet would take into account the data packet of 100,000 bits and the handshake packets of 200bits and 150bits/sec speed to form: (200/150 + 200/150 + 200/150 + 100,000/150) = 671 seconds. **Then** we take into account the parallel bandwidth speed of 15bits/sec to get (200/15+200/15+200/15+100,000/15) = 6707 seconds **for a total of ~7377 seconds**

For persistent HTTP:

We take the same first packet speed and then we only need to account for one handshake for the 1 object = 10\*(200/150 + 100,000/150) = **~7351 seconds**

b. Do you expect significant gains over the non-persistent case? Justify and explain your answer.

a. Looking at the calculations above the persistent option only has a slight advantage of ~26 seconds

c. Now suppose that the link is shared by Bob with four other users. Bob uses parallel instances of non-persistent HTTP, and the other four users use non-persistent HTTP without parallel downloads.

i. Do Bob’s parallel connections help him get Web pages more quickly?

Why or why not?

Bob’s parallel connections provide a faster response time compared to the single connection that the others have to use.

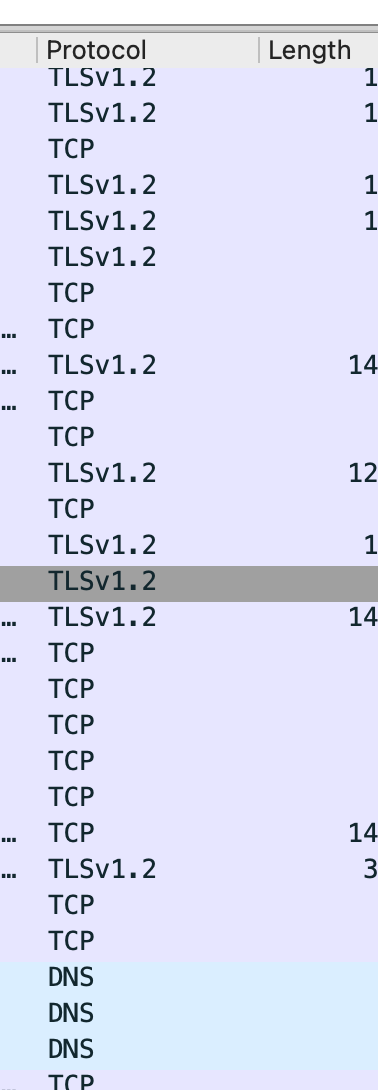
ii. If all five users open five parallel instances of non-persistent HTTP, then would Bob’s parallel connections still be beneficial? Why or why not?

The parallel connections would still be faster for Bob even if others are using them since they still increase the response time compared to non-parallel connections.

**Q6. [15 points] Wireshark Lab (see attachment#1 : first lab)**

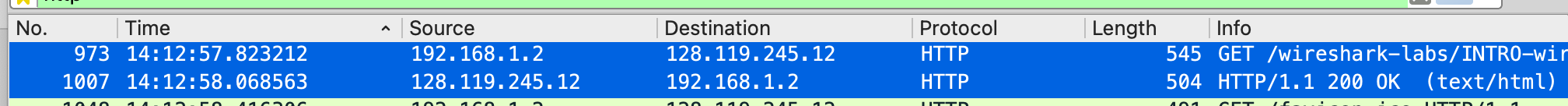
Please add screenshots and answer the questions from the attachment#1.

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   * TCP, TLCv1.2, DNS

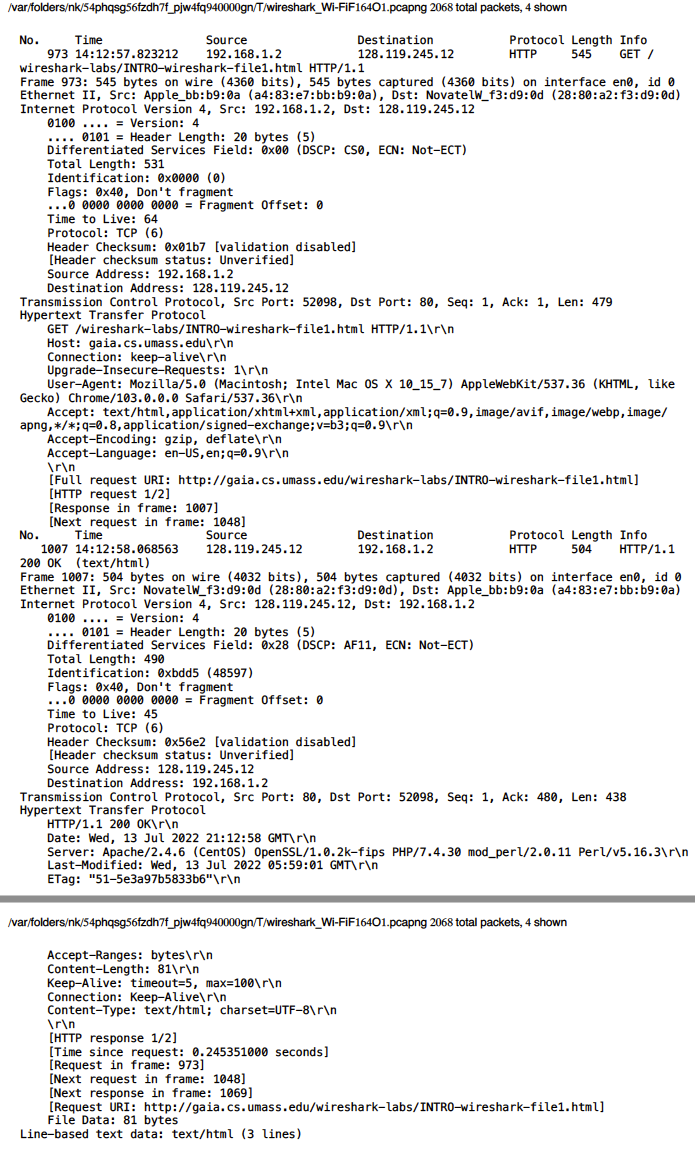


1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

Start time 14:12:57.82 for GET and OK received at 14:12:58.07 so about 25milliseconds



1. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? - 128.119.245.12
   * What is the Internet address of your computer? 192.168.1.2
2. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the “*Selected Packet Only”* and *“Print as displayed”* radial buttons, and then click OK.



**Q7. [25 points] Wireshark Lab: HTTP (see Attachment#2 : second lab)**

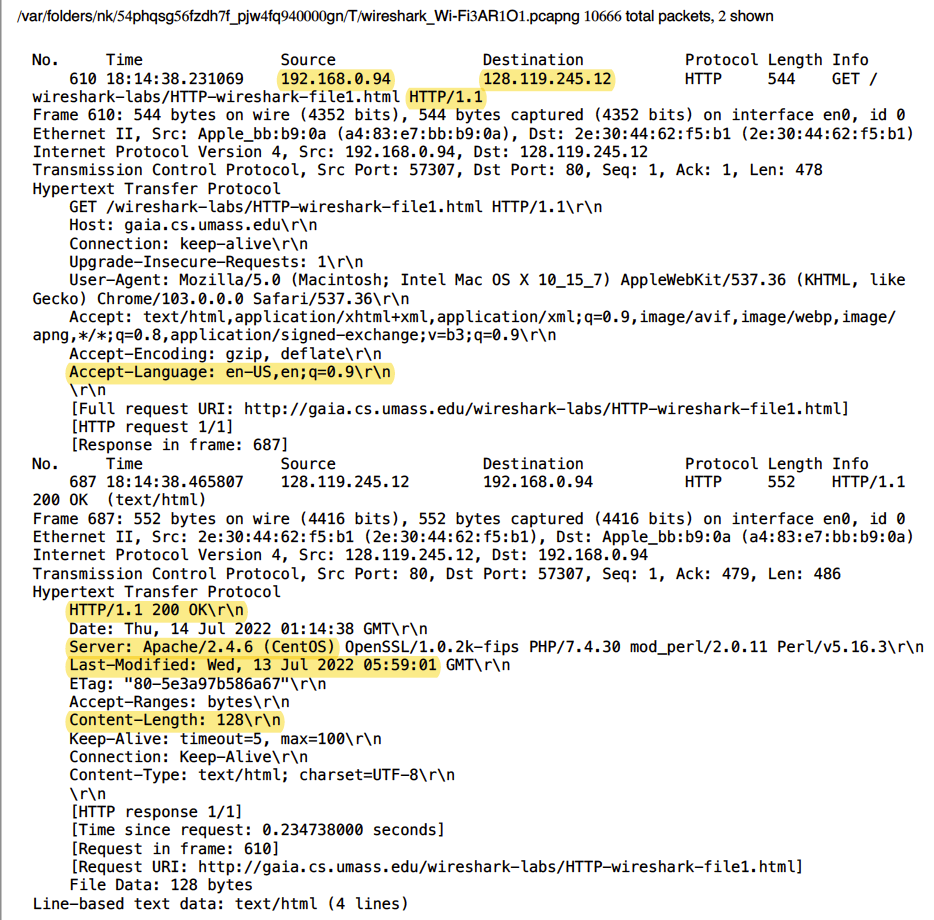
Please add screenshots and answer the questions from the attachment#2.

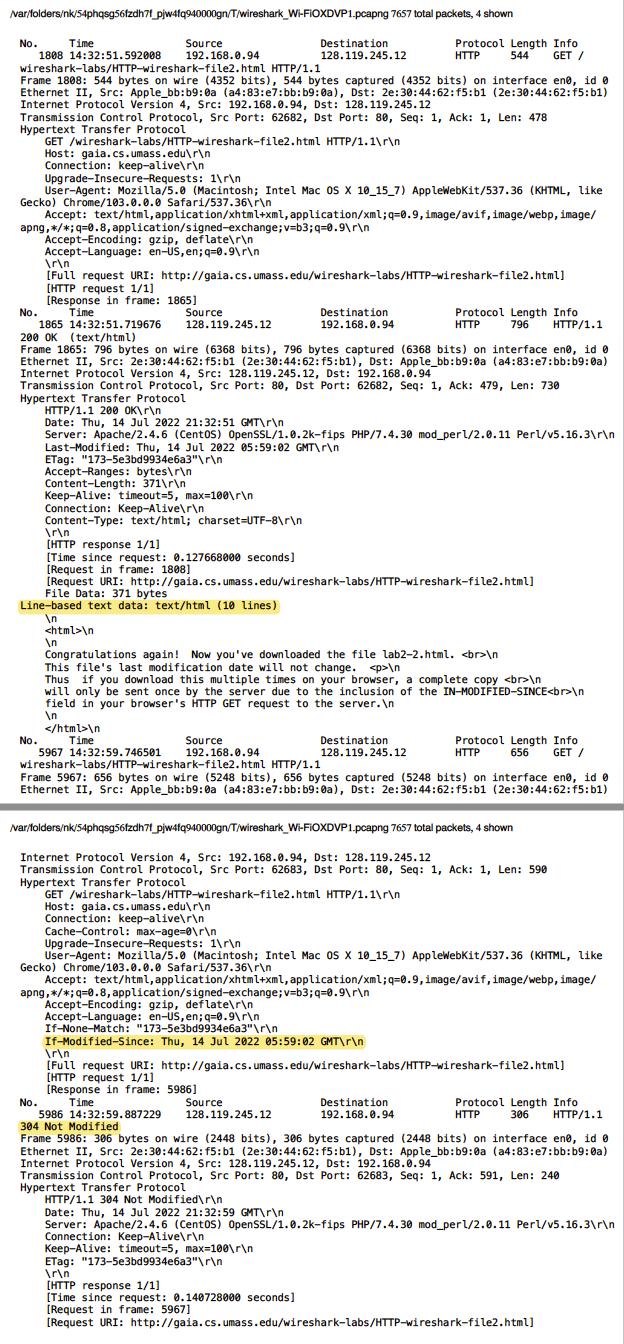
For each labs, please try to answer as many questions possible.

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? HTTP 1.1

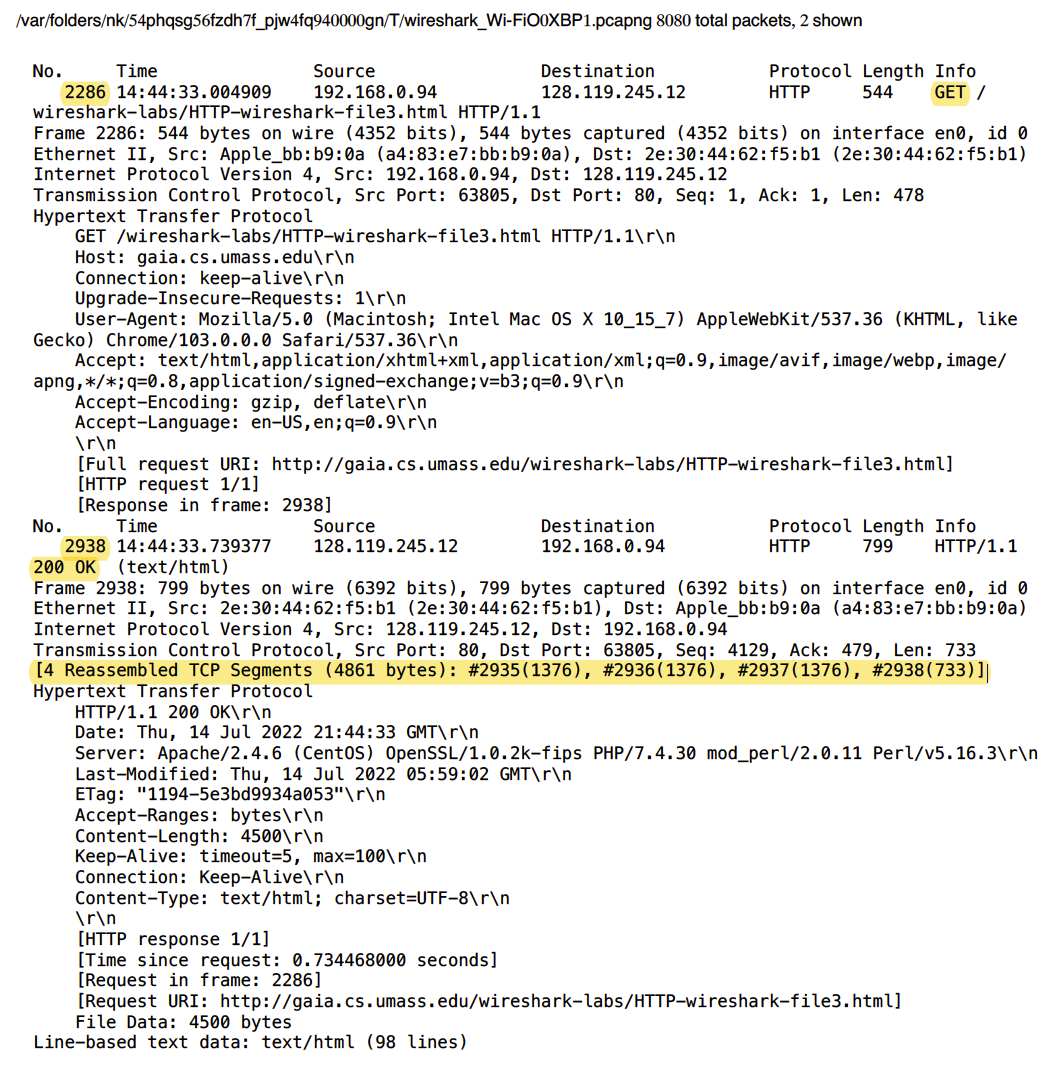
1. What languages (if any) does your browser indicate that it can accept to the server? en-US,en;q=0.9

1. What is the IP address of your computer? Src: 192.168.0.94, Of the gaia.cs.umass.edu server? Dst: 128.119.245.12
2. What is the status code returned from the server to your browser? 200
3. When was the HTML file that you are retrieving last modified at the server? Wed, 13 Jul 2022 05:59:01 GMT
4. How many bytes of content are being returned to your browser? 128 bytes
5. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? I do not see any headers missing



1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
   1. No
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   1. Yes it did as shown in the line-based text data section
3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header? Yes, If-Modified-Since: Thu, 14 Jul 2022 05:59:02 GMT
4. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? 304 Not Modified
   1. Did the server explicitly return the contents of the file? Explain. No it did not since no modifications were made and there is no line-based text data section

1. How many HTTP GET request messages did your browser send? 1
   1. Which packet number in the trace contains the GET message for the Bill or Rights? 2286
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? 2938
3. What is the status code and phrase in the response? HTTP/1.1 200 OK\r\n
4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? 4

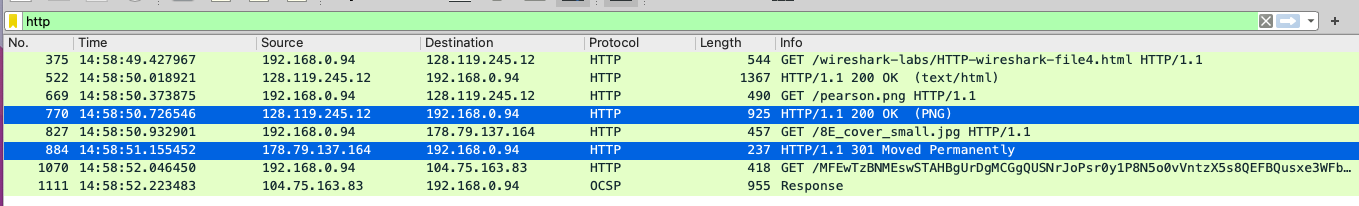


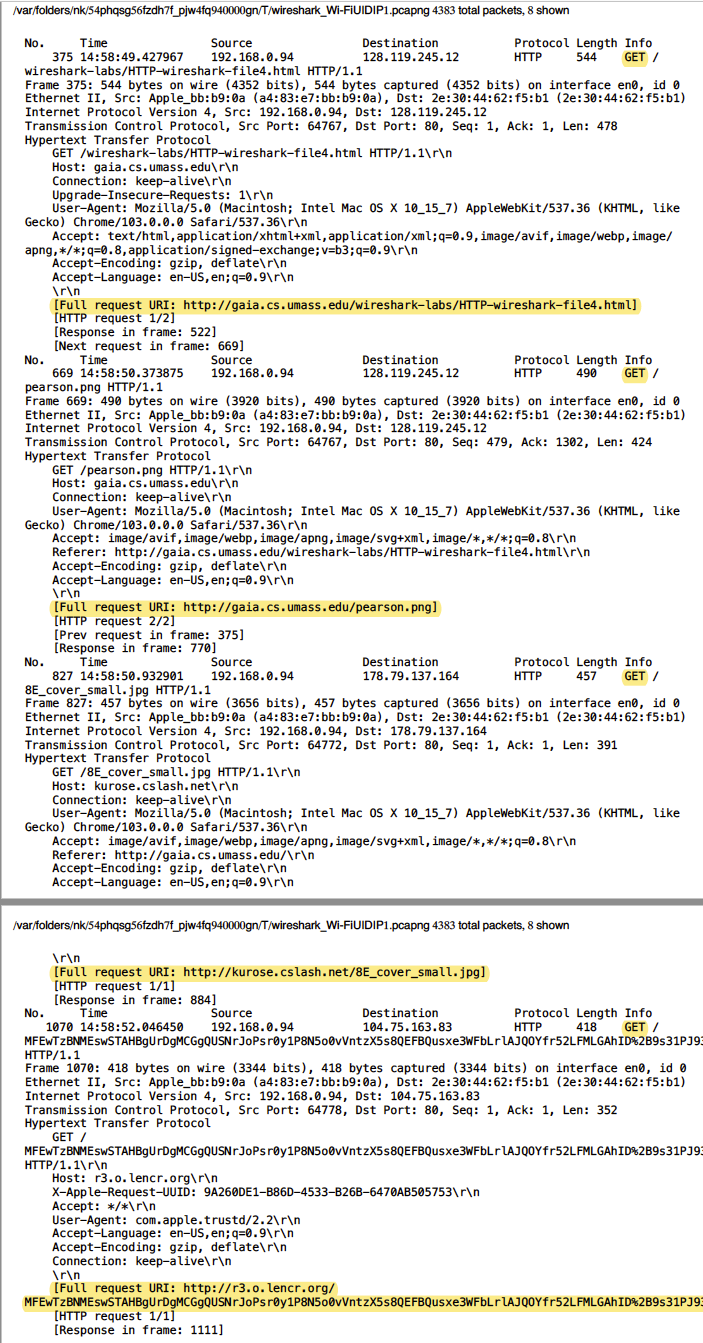
16. How many HTTP GET request messages did your browser send? 4 To which Internet addresses were these GET requests sent?

* 1. <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>
  2. <http://gaia.cs.umass.edu/pearson.png>
  3. <http://kurose.cslash.net/8E_cover_small.jpg>
  4. <http://r3.o.lencr.org/MFEwTzBNMEswSTAHBgUrDgMCGgQUSNrJoPsr0y1P8N5o0vVntzX5s8QEFBQusxe3WFbLrlAJQOYfr52LFMLGAhID%2B9s31PJ93sEiWCBXwrX2n1w%3D>

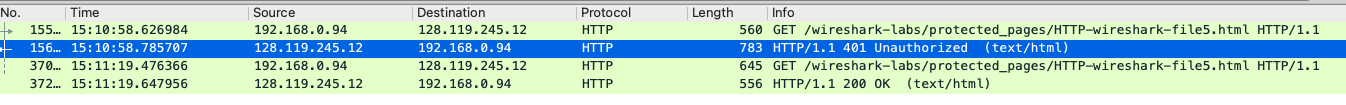
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

* 1. The images appear to be requested serially since one was requested and sent before the other





18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser? HTTP/1.1 401 Unauthorized\r\n



19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

