Homework #1

Mike Pendleton

John Hulett

West Texas A@M University

**CIDM 6340 Network Management & Information Security – Fall 2021**

**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 :Mike Pendleton Id:** **1058201\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**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, managing, and operating a data network, using a network management system. Modern network management systems use software and hardware to constantly collect and analyze data and push out configuration changes for improving performance, reliability, and security.
2. Briefly explain a simple network management protocol.
   1. SNMP was developed for use as a network management tool for networks and internetworks operating TCP/IP. Simple network management protocol (SNMP) is actually used to refer to a collection of specifications for network management that include the protocol itself, the definition of a database, and associated concepts.

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

1. How is personal information safeguarded?
   * 1. Personal information is safeguard by Firewalls and proxy servers. These tools guard the perimeter by analyzing traffic (at least inbound and in many cases outbound as well) and blocking traffic that has been disallowed by the administrator. These two safeguards are often augmented by an intrusion-detection system (IDS). An IDS simply monitors traffic, looking for suspicious activity that might indicate an attempted intrusion. The most basic security device is the firewall. A firewall is a barrier between a network and the outside world. Sometimes a firewall takes the form of a standalone server, sometimes a router, and sometimes software running on a machine. Whatever its physical form, a firewall filters traffic entering and exiting the network. A proxy server is often used with a firewall to hide the internal network’s IP address and present a single IP address (its own) to the outside world.
2. What are the vulnerabilities and how can you compute security risk?

A vulnerability refers to a weak point inside any system that can be exploited by any individual or group of individuals for personal interests. A vulnerability can be present anywhere inside different components of the network system and it may due to the carelessness of the developers and designers of the network system.

To compute security risk you can use the Exposure Factor (EF), Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO), and Annualized Loss Expectancy (ALE).

These are defined as

**Exposure Factor:** The Exposure Factor (EF) is the percentage of value an asset lost due to an incident. **Single Loss Expectancy (SLE)** is the cost of a single loss. SLE is the Asset Value (AV) times the Exposure Factor (EF). **Annual Rate of Occurrence (ARO)** is the number of losses you suffer per year. **Annualized Loss Expectancy (ALE)** is your yearly cost due to a risk. It is calculated by multiplying the Single Loss Expectancy (SLE) times the Annual Rate of Occurrence (ARO).

The formulas are

* SLE = Asset Value (AV) \* Exposure Factor (EF)
* Risk = Probability of the Risk \* Cost of the Eventuality
* ALE = Single Loss Expectancy (SLE) \* Annual Rate of Occurrence (ARO)

1. Name different types of threats in computer network.
   * 1. Malware: MALicious softWARE
     2. Security Breaches
     3. DoS: Denial of Service attacks
     4. Web Attacks
     5. Session Hijacking
     6. DNS Poisoning
     7. Insider Threats

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

1. Compare various connection methods and speeds used in networks. [Hints see table from ch2 slides]. What are different error messages?
   1. DSO – 64Kbps
   2. ISDN – 128Kbps
   3. T1 – 1.544Mbps
   4. T3 – 43.2Mbps
   5. OC3 – 155Mbps
   6. OC12 – 622Mbps
   7. OC48 – 2.5Gbps
      1. Error messages that can occur are
         1. 100 – informational
         2. 200s – success
         3. 300s – redirects
         4. 400s – client errors
         5. 500s – server errors
2. Name five basic network utilities and give example of their functions.
   1. Combined answer for this question:
   2. IPConfig – this is used to get information about your computer. Such as Ethernet adapter addresses, to include your IPv6 address, IPv4 address, default gateway, wireless lan adapter, and wireless lan adapter local area connection
   3. Ping – checks to see if a system is connected to the network, it also provides statistics on how long it takes for an echo request to arrive at a destination host
   4. Tracert – similar to ping, however it provides the statistics of every hop between the host and the destination address
   5. Netstat – displays the network status and the active connections
   6. NSLookup -  querys the [Domain Name System](https://en.wikipedia.org/wiki/Domain_Name_System) (DNS) to obtain the mapping between [domain name](https://en.wikipedia.org/wiki/Domain_name) and [IP address](https://en.wikipedia.org/wiki/IP_address), or other [DNS records](https://en.wikipedia.org/wiki/DNS_record).

**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, managing, and operating a data network, using a network management system. Modern network management systems use software and hardware to constantly collect and analyze data and push out configuration changes for improving performance, reliability, and security.
     2. Network Management Requirements are
        1. Fault Management – the facilities that enable the detection, isolation, and correction of abnormal operation of the OSI environment
        2. Accounting Management – The facilities that enable charges to be established for the use of managed objects and costs to be identified for the use of those managed objects
        3. Configuration and Name Management – the facilities that exercise control over, identify, collect data from, and provide data to managed objects for the purpose of assisting in providing for continuous operation of interconnection services
        4. Performance Management – the facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities
        5. Security Management – the aspects of OSI security essential to operate 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 do one or all of the following

* Read all your emails
* See all your passwords
* Know what websites you have visited
* See all the images from the websites you were on
* Capture account information (banks, credit cards) in detail

With the information gathered by Trudy she can then, steal from you financial accounts, she can log into websites and purchases items, she can send malicious emails to your contact list

**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.

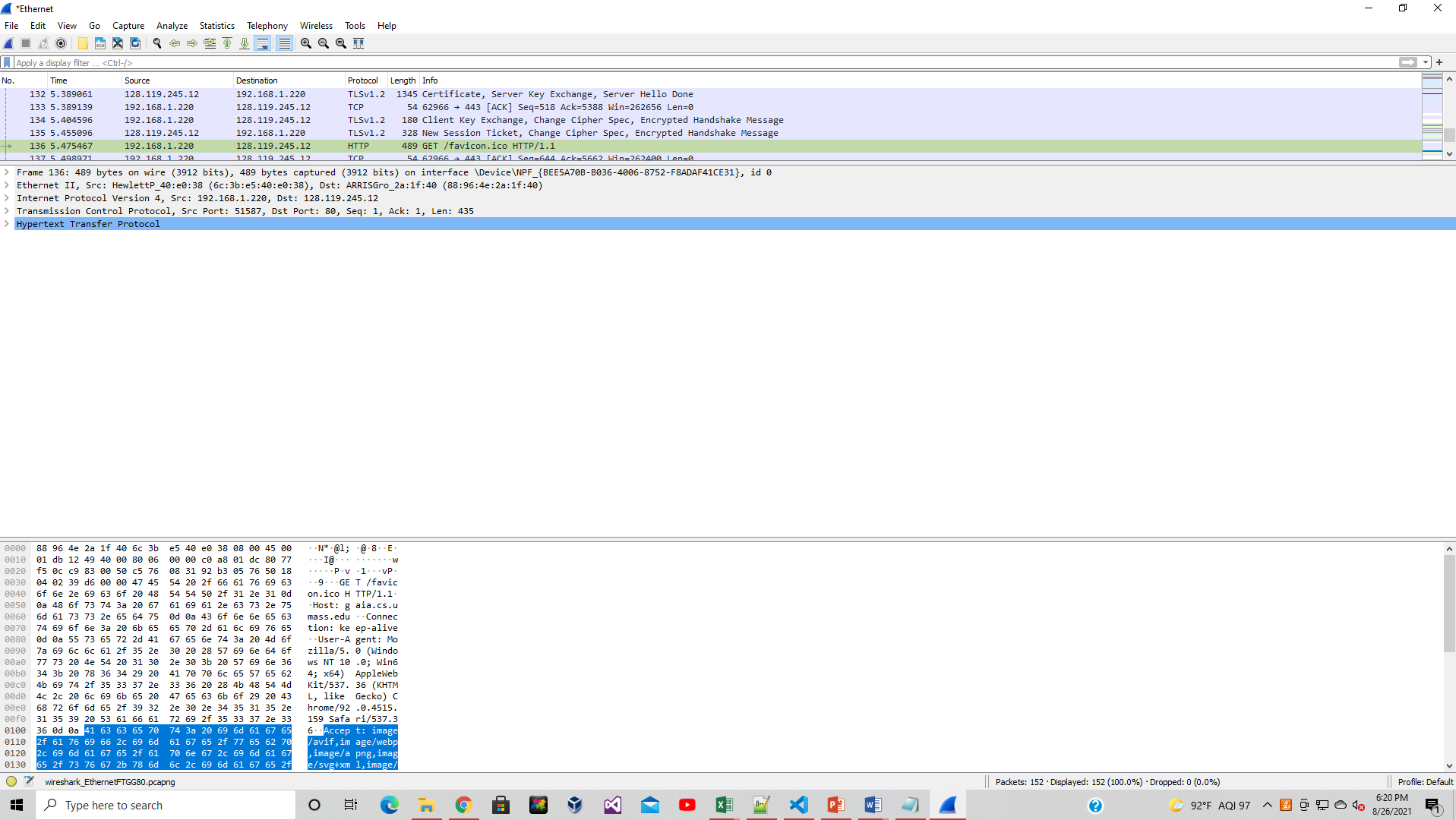
1. Would parallel downloads via parallel instances of non-persistent HTTP make sense in this case? Now consider persistent HTTP.
   * 1. Yes, parallel downloads would make sense as they would dedicate more bandwidth and have a lower RTT per transmission.
2. Do you expect significant gains over the non-persistent case? Justify and explain your answer.
   1. Dependent on how much is being downloaded there would be a significant gain.
      1. Non persistent utilizes 2 RTT, where parallel only uses 1 RTT and the connection is left open until the transmission is complete.
3. 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.
   1. Do Bob’s parallel connections help him get Web pages more quickly?

Why or why not?

1. Yes, not only will it load faster to the eye, but the page load would be loaded first and the parallel download would also dedicate more bandwidth than the non-persistent http connections.
   1. 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?
      1. Yes, due to the connection remaining open and not where the other 4 users new consistent connections created opened and closed. This with the amount off RTT of the parallel download with the persistent connection. Where the other 4 users have a higher RTT rate combined with the connections becoming opened and closed consistently.

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

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



1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   * **Answer**
     + The 3 protocols are Internet Protocol, Transmission Control Protocol and HyperText Transfer Protocol
2. 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*.)
   * **Answer**
     + It took approximately 0.23504 seconds
3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
   * **Answer**
     + The edu address is 128.119.245.12
     + My computer address is 192.168.1.220
4. 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.
   * **Answer**

No. Time Source Destination Protocol Length Info

138 18:12:39.541825 128.119.245.12 192.168.1.220 TCP 60 80 → 51587 [ACK] Seq=1 Ack=436 Win=30336 Len=0

Frame 138: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface\Device\NPF\_{BEE5A70B-B036-4006-8752-F8ADAF41CE31}, id

0

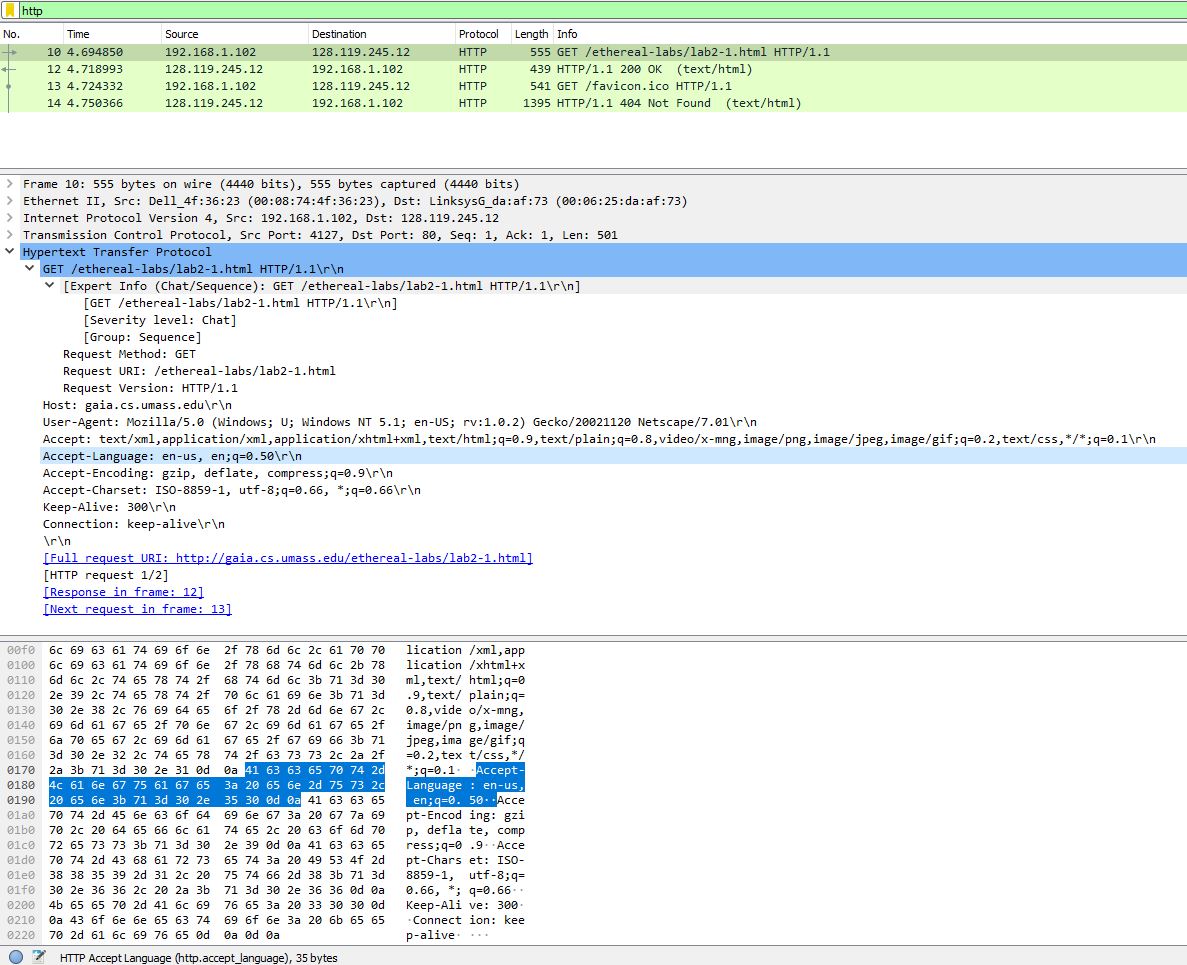
Ethernet II, Src: ARRISGro\_2a:1f:40 (88:96:4e:2a:1f:40), Dst: HewlettP\_40:e0:38 (6c:3b:e5:40:e0:38)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.220

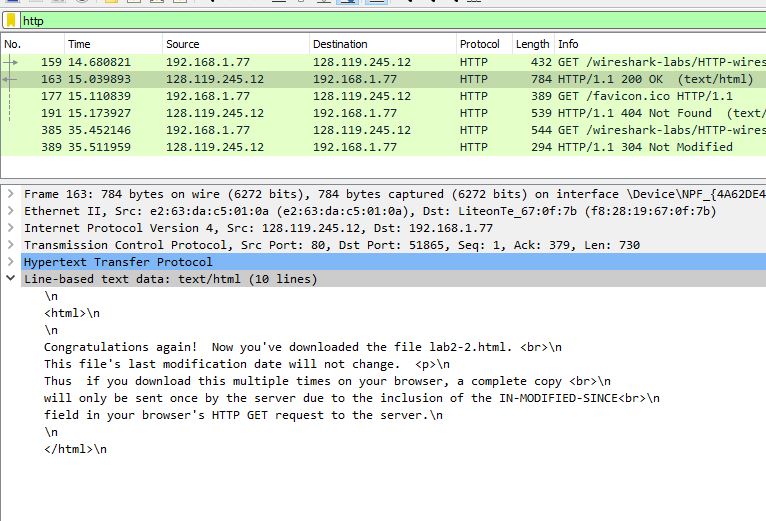
Transmission Control Protocol, Src Port: 80, Dst Port: 51587, Seq: 1, Ack: 436, Len: 0

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

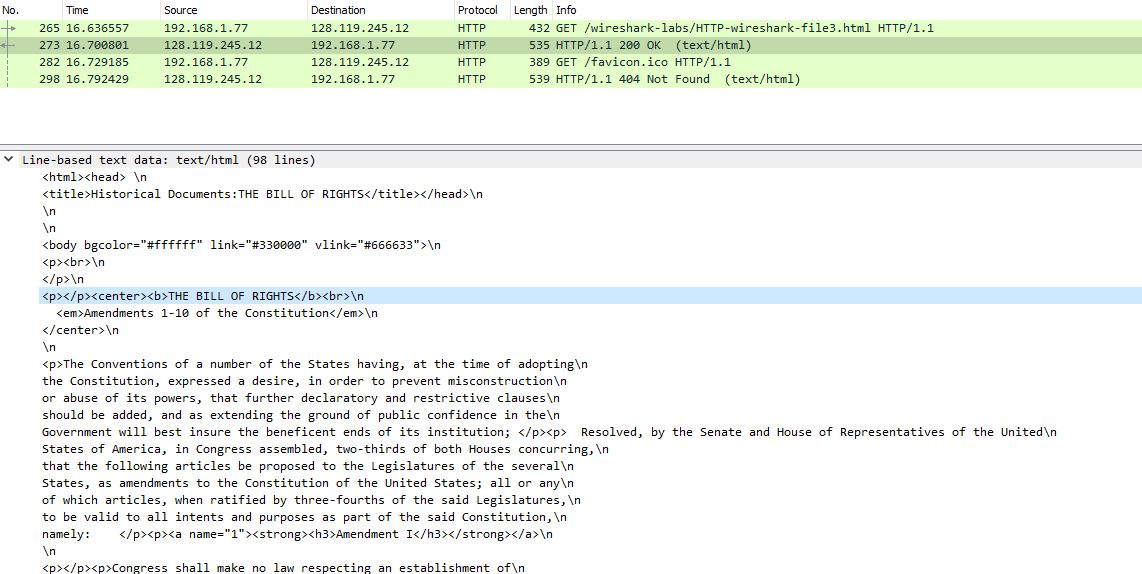
Please add screenshots and answer the questions from the attachemnet#2.

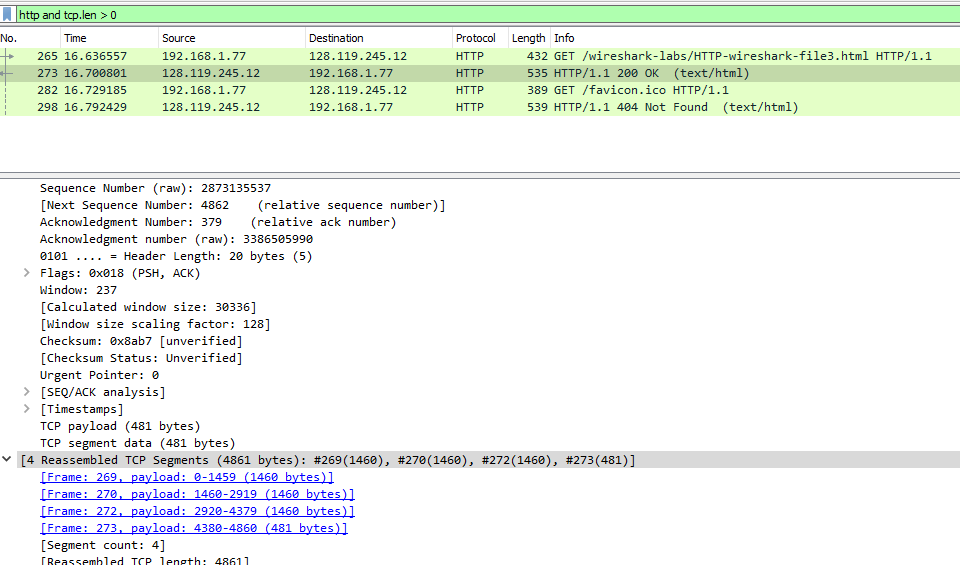


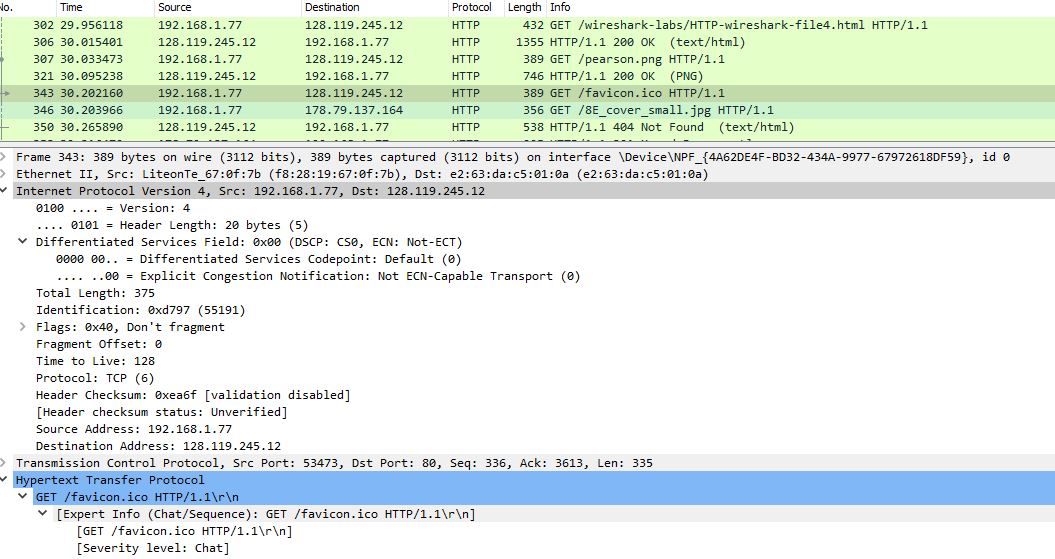
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   1. Both client and server is 1.1
      1. Client: GET /ethereal-labs/lab2-1.html **HTTP/1.1**\r\n
      2. Server: Request Version: **HTTP/1.1**
2. What languages (if any) does your browser indicate that it can accept to the server?
   1. http.accept\_language: en-us, en;q=0.50
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   1. ip: Internet Protocol Version 4,server: 128.119.245.12, client: 192.168.1.77
4. What is the status code returned from the server to your browser?
   1. http.response.code: 200
5. When was the HTML file that you are retrieving last modified at the server?
   1. http.last\_modified: Fri, 03 Sep 2021 05:59:01 GMT
6. How many bytes of content are being returned to your browser?
   1. http.content\_length: 73
7. 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? If so, name one.
   1. I can see all of the headers
8. 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, there is not a line on the first GET
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   1. Yes because of the data-text-lines



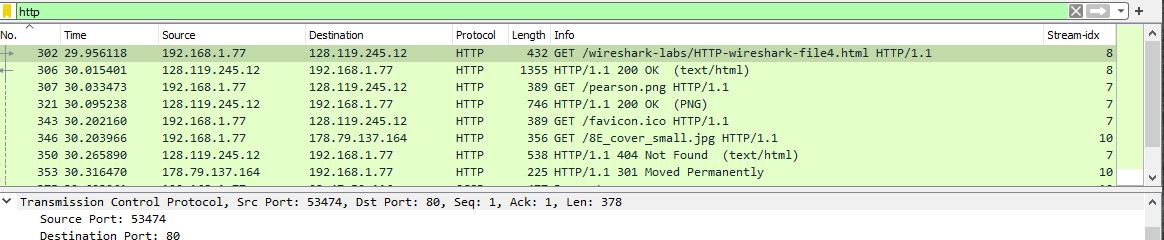
1. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
   1. Yes - If-Modified-Since: Fri, 03 Sep 2021 05:59:01 GMT
2. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
   1. [HTTP/1.1 304 Not Modified\r\n], The server did not return a response due to cache
3. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
   1. 1 get rerequest was sent
   2. **273** 16.700801 128.119.245.12 192.168.1.77 HTTP 535 HTTP/1.1 200 OK (text/html)



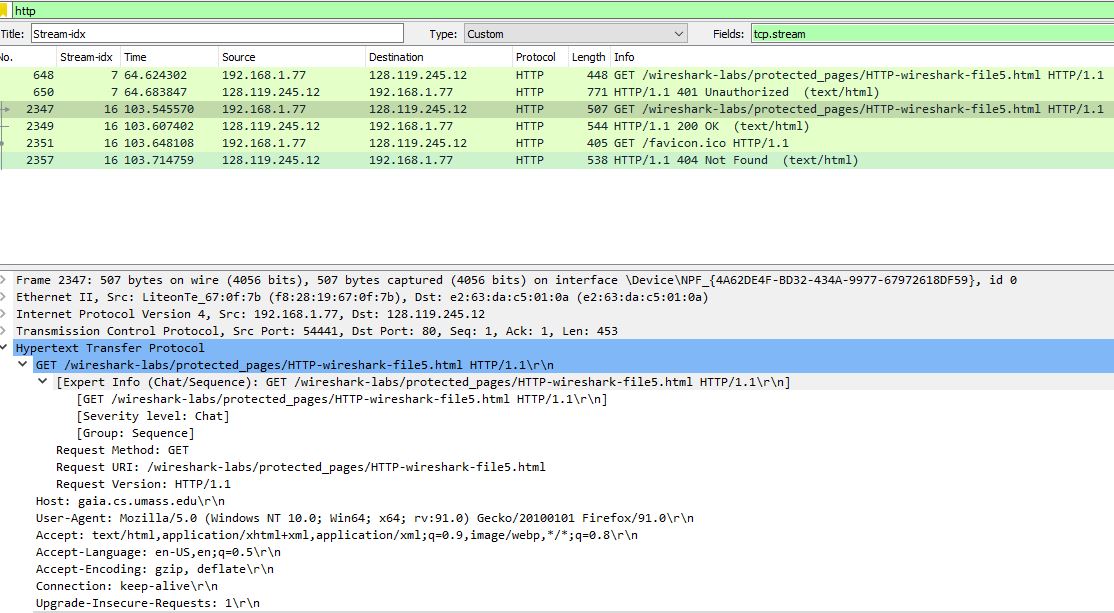
1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
   1. Packet number is 273
2. What is the status code and phrase in the response?
   1. Status Code: 200 - Response Phrase: OK
3. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
   1. 4 - [4 Reassembled TCP Segments (4861 bytes): #269(1460), #270(1460), #272(1460), #273(481)]
   2. 
4. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
   1. There were three responses sent
   2. Two addresses were sent to:
      1. 128.119.245.12
      2. 178.79.137.164



1. 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. This download was serially, As you can see with the stream idx column I created(last column to the right “field value = tcp.stream”), these get requests were from different tcp connections.



1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
   1. Status Code: 401 and Response Phrase: Unauthorized
2. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
   1. Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n



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