Assignment

**Homework 13**

P12. Describe how loops in paths can be detected in BGP.

**Answer**: Detecting loops in paths within BGP is important for maintaining the stability and efficiency of the network. BGP uses several mechanisms to detect and prevent routing loops. The following information are the primary methods:

1. AS-Path Attribute – The AS-Path is a list of Autonomous Systems (ASes) that a route has traversed. When a BGP router receives an update, it checks the AS-Path attribute which are

- Loop Detection: If the router’s own AS number is already in the AS-path, it indicates a loop, and the route is discarded.

- Path Selection: Among multiple paths, the path with the shortest AS-Path is typically preferred.

2. Route Reflection and Cluster IDs

In more complex BGP topologies, such as those using route reflectors, additional attributes help prevent loops:

- Cluster List: Route reflectors use a Cluster ID to identify the route reflector cluster. The Cluster List attribute tracks the clusters a route has traversed.

- Loop Detection: If a route reflector sees its own Cluster ID in the Cluster List, it detects a loop and discards the route.

3. Confederations

BGP confederations are used to manage very large networks by dividing them into smaller, more manageable sub-ASes. Each sub-AS has its own AS number, and additional attributes are used to prevent loops:

- Sub-AS Path: Within a confederation, the Sub-AS Path attribute records the sub-ASes a route has passed through.

- Loop Detection: Similar to the AS-Path, if a sub-AS sees its own number in the Sub-AS Path, it detects a loop and discards the route.

4. Originator ID and Router ID

For routes propagated by route reflectors, the Originator ID and Router ID attributes help prevent loops:

- Originator ID: This attribute contains the Router ID of the BGP router that originated the route within the AS. Loop Detection: If a route reflector receives a route with an Originator ID that matches its own Router ID, it detects a loop and discards the route.

- Router ID: Generally, each BGP router has a unique Router ID. Loop Detection: In some scenarios, comparing Router IDs can help identify loops, especially in complex topologies with multiple connections.

These mechanisms collectively ensure that BGP can effectively detect and prevent routing loops, maintaining the stability and efficiency of the network. Understanding and configuring these attributes correctly is crucial for network operators managing BGP in their networks.

P16. Consider the following network. ISP B provides national backbone service to regional ISP A. ISP C provides national backbone service to regional ISP D. Each ISP consists of one AS. B and C peer with each other in two places using BGP. Consider traffic going from A to D. B would prefer to hand that traffic over to C on the West Coast (so that C would have to absorb the cost of carrying the traffic cross-country), while C would prefer to get the traffic via its East Coast peering point with B (so that B would have carried the traffic across the country). What BGP mechanism might C use, so that B would hand over A-to-D traffic at its East Coast peering point? To answer this question, you will need to dig into the BGP specification.

**Answer**:

P20. Suppose ASs X and Z are not directly connected but instead are connected by AS Y. Further suppose that X has a peering agreement with Y, and that Y has a peering agreement with Z. Finally, suppose that Z wants to transit all of Y’s traffic but does not want to transit X’s traffic. Does BGP allow Z to implement this policy?

**Answer**: Yes, BGP allows Autonomous System (AS) Z to implement a policy where it transits traffic from AS Y but not from AS X. This can be achieved using BGP policy mechanisms such as route filtering and setting specific policies based on AS-Path attributes.

P22. In Section 5.7, we saw that it was preferable to transport SNMP messages in unreliable UDP datagrams. Why do you think the designers of SNMP chose UDP rather than TCP as the transport protocol of choice for SNMP?

**Answer**: The designers of SNMP chose UDP over TCP for the following reasons:

* Simplicity and Low Overhead: UDP is simpler and has less overhead compared to TCP, making SNMP more efficient.
* Speed: UDP allows for faster message transmission since it doesn't involve connection setup or management.
* Tolerance for Loss: SNMP can handle occasional message loss, so the reliability of TCP isn't necessary.
* Scalability: UDP's stateless nature makes it easier to manage many devices without the burden of maintaining multiple connections.
* Resource Constraints: UDP is more suitable for devices with limited processing power and memory.

In summary, UDP's simplicity, efficiency, and suitability for network management tasks make it the preferred choice for transporting SNMP messages.

**Homework 12**

P3. Consider the following network. With the indicated link costs, use Dijkstra’s shortest-path algorithm to compute the shortest path from x to all network nodes. Show how the algorithm works by computing a table similar to Table 5.1.

Answer:

x->z = 8

x->y = 6

x->w = 6

x->v = 3

x->v->u = 3 + 3 =6

x->v->t = 7

P5. Consider the network shown below, and assume that each node initially knows the costs to each of its neighbors. Consider the distance-vector algorithm and show the distance table entries at node z.

Answer:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Cost To | | | | | | |
| From |  | u | v | x | y | Z |
| V | Infinity | Infinity | Infinity | Infinity | Infinity |
| X | Infinity | Infinity | Infinity | Infinity | Infinity |
| Z | Infinity | 6 | 2 | Infinity | 0 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Cost To | | | | | | |
| From |  | u | v | x | y | Z |
| V | 1 | 0 | 3 | Infinity | 6 |
| X | Infinity | 3 | 0 | 3 | 2 |
| Z | 7 | 5 | 2 | 5 | 0 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Cost To | | | | | | |
| From |  | u | v | x | y | Z |
| V | 1 | 0 | 3 | 3 | 5 |
| X | 4 | 3 | 0 | 3 | 2 |
| Z | 6 | 5 | 2 | 5 | 0 |

P9. Consider the count-to-infinity problem in the distance vector routing. Will the count-to-infinity problem occur if we decrease the cost of a link? Why? How about if we connect two nodes which do not have a link?

Answer:

The count-to-infinity problem can occur in distance vector routing when:

1) The cost of a link is decreased:

The reduced cost can trigger a chain reaction of routing table updates, leading to the count-to-infinity issue. Two nodes without a direct link are connected:

The new link can introduce a routing loop or a path with increasing cost, causing the routers to keep updating their routing tables indefinitely.

2) Split Horizon:

Preventing a router from advertising a route back to the router from which it learned the route. Poison Reverse: Advertising an infinite cost for a route to effectively "poison" it. Triggered Updates: Triggering immediate updates to neighboring routers upon significant topology changes. Timers and Thresholds: Setting appropriate timers and cost thresholds to limit the growth of routing tables.

By implementing these or other techniques, network administrators can effectively manage the count-to-infinity problem and ensure efficient distance vector routing in their networks.

**Homework 11**

P11. Consider a router that interconnects three subnets: Subnet 1, Subnet 2, and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also suppose that Subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces, and Subnet 3 is to support at least 12 interfaces. Provide three network addresses (of the form a.b.c.d/x) that satisfy these constraints.

Answer: To provide three network addresses that satisfy the given constraints, we need to divide the given prefix, which is 223.1.17/24, into smaller subnets while ensuring that each subnet can support the required number of interfaces.

Step 1: Determine the subnet sizes:

* Subnet 1 needs to support at least 60 interfaces.
* Subnet 2 needs to support at least 90 interfaces.
* Subnet 3 needs to support at least 12 interfaces.

Step 2: Understand the address space (223.1.17.0/24):

* The prefix /24 there are 256 addresses in this range from 223.1.17.0 – 223.1.17.225.

Step 3: Find the smallest power of 2 that could accommodate each subnet:

* Subnet 1: 64 addresses (2^6) -> /26 subnet mask because 32 – 6 = 26.
* Subnet 2: 128 addresses (2^7) -> /25 subnet mask because 32 – 7 = 25.
* Subnet 3: 16 addresses (2^4) -> /28 subnet mask because 32 – 4 = 28.

Step 4: Allocating addresses starts from subnet that requires most addresses to smallest.

Start from the beginning of the 223.1.17.0/24 range and allocate addresses to each subnet without overlapping.

* Subnet 2 (requires 128 addresses): User the first block of addresses.

# Network address: 223.1.17.0/25

# This gives addresses from 223.1.17.0 to 223.1.17.127 (128 addresses).

* Subnet 1 (requires 64 addresses): Use the next block of addresses.

# Network address: 223.1.17.128/26

# This gives addresses from 223.1.17.128 to 223.1.17.191 (64 addresses).

* Subnet 3 (requires 16 addresses): Use the next block of addresses.

# Network address: 223.1.17.192/26

# This gives addresses from 223.1.17.192 to 223.1.17.207 (16 addresses).

Summary:

* Subnet 2: 223.1.17.0/25 (supports up to 128 interfaces)
* Subnet 1: 223.1.17.128/26 (supports up to 64 interfaces)
* Subnet 3: 223.1.17.192/28 (supports up to 16 interfaces)

These network addresses ensure that each subnet has enough addresses for the required number of interfaces without overlapping each other.

P17. Suppose datagrams are limited to 1,500 bytes (including header) between source Host A and destination Host B. Assuming a 20-byte IP header, how many datagrams would be required to send an MP3 consisting of 5 million bytes? Explain how you computed your answer.

Answer:

Step 1: Understand the constraints:

* Maximum datagram size = 1,500 bytes
* IP header size = 20 bytes
* Maximum payload size per datagram = 1,500 bytes – 20 bytes = 1,480 bytes

Step 2: Calculate the number of datagrams needed:

* Total size of the MP3 file = 5,000,000 bytes
* Each datagram can carry up to 1,480 bytes of the MP3 file.

Step 3: Compute the total number of datagrams required:

* Divid the total file size by the payload size per datagram:

Number of datagrams = 5,000,000 bytes / 1,480 bytes = 3,378.38 = 3,379

Conclusion:

To send a 5-million-byte MP3 file, 3,379 datagrams are required. Each datagram (except possibly the last one) will carry 1,480 bytes of the MP3 file, with the last datagram carrying the remaining bytes.

**Homework 10**

P1. Consider the network below.

a) Show the forwarding table in router A, such that all traffic destined to host H3 is forwarded through interface 3.

Answer: Data that send to host H3 is forwarded through interface 3

Destination Address: H3

Link Interface: 3

b) Can you write down a forwarding table in router A, such that all traffic from H1 destined to host H3 is forwarded through interface 3, while all traffic from H2 destined to host H3 is forwarded through interface 4? (Hint: This is a trick question.)

Answer: No, because forwarding rule is only based on destination address

P4. Consider the switch shown below. Suppose that all datagrams have the same fixed length, that the switch operates in a slotted, synchronous manner, and that in one time slot a datagram can be transferred from an input port to an output port. The switch fabric is a crossbar so that at most one datagram can be transferred to a given output port in a time slot, but different output ports can receive datagrams from different input ports in a single time slot. What is the minimal number of time slots needed to transfer the packets shown from input ports to their output ports, assuming any input queue scheduling order you want (i.e., it need not have HOL blocking)? What is the largest number of slots needed, assuming the worst-case scheduling order you can devise, assuming that a non-empty input queue is never idle?

Answer: The minimum number of time slots needed is 3. The scheduling is as follows. Slot 1: send X in the top input queue, and send Y in the middle input queue. Slot 2: send X in the middle input queue, and send Y in the bottom input queue Slot 3: send Z in the bottom input queue. The largest number of slots is still 3. Based on the assumption that a non-empty input queue is never idle, we see that the first time slot always consists of sending X in the top input queue and Y in the either middle or bottom input queue, also the second time slot, we can always send two more datagrams and the last datagram can be sent in the third time slot.

P6. Consider the figure below. Answer the following questions:

a. Assuming FIFO service, indicate the time at which packets 2 through 12 each leave the queue. For each packet, what is the delay between its arrival and the beginning of the slot in which it is transmitted? What is the average of this delay over all 12 packets?

Answer:

b. Now assume a priority service, and assume that odd-numbered packets are high priority, and even-numbered packets are low priority. Indicate the time at which packets 2 through 12 each leave the queue. For each packet, what is the delay between its arrival and the beginning of the slot in which it is transmitted? What is the average of this delay over all 12 packets?

Answer:

c. Now assume round robin service. Assume that packets 1, 2, 3, 6, 11, and 12 are from class 1, and packets 4, 5, 7, 8, 9, and 10 are from class 2. Indicate the time at which packets 2 through 12 each leave the queue. For each packet, what is the delay between its arrival and its departure? What is the average delay over all 12 packets?

Answer:

d. Now assume weighted fair queueing (WFQ) service. Assume that odd numbered packets are from class 1, and even-numbered packets are from class 2. Class 1 has a WFQ weight of 2, while class 2 has a WFQ weight of 1. Note that it may not be possible to achieve an idealized WFQ sched ule as described in the text, so indicate why you have chosen the particular packet to go into service at each time slot. For each packet what is the delay between its arrival and its departure? What is the average delay over all 12 packets?

Answer:

e. What do you notice about the average delay in all four cases (FIFO, RR, priority, and WFQ)?

Answer:

FIFO: High variability in delays; potential for high average delay if packet sizes vary greatly.

RR: More predictable and evenly distributed delays; may not be optimal for real-time requirements.

Priority Queuing: Minimal delay for high-priority traffic; potential for very high delays for low-priority traffic, which can raise the average delay.

WFQ: Balanced approach; generally, results in lower average delays due to weighted fair treatment of flows.

In summary, WFQ often provides the best trade-off in terms of average delay, balancing fairness and responsiveness, especially in environments with varied traffic types and priorities.

P9. Consider a datagram network using 8-bit host addresses. Suppose a router uses longest prefix matching and has the following forwarding table:

For each of the four interfaces, give the associated range of destination host addresses and the number of addresses in the range.

Answer:

Destination Address Link Interface

200.23.16/21 0

200.23.24/24 1

200.23.24/21 2

otherwise 3

**Homework 9**

P40. Consider Figure 3.61. Assuming TCP Reno is the protocol experiencing the

behavior shown above, answer the following questions. In all cases, you

should provide a short discussion justifying your answer.

a. Identify the intervals of time when TCP slow start is operating.

Answer: TCP slow start is operating in the intervals [1,6] and [23,26]

b. Identify the intervals of time when TCP congestion avoidance is operating.

Answer: TCP congestion avoidance is operating in the intervals [6,16] and [17,22]

c. After the 16th transmission round, is segment loss detected by a triple

duplicate ACK or by a timeout?

Answer: After the 16th transmission round, packet loss is recognized by a triple duplicate ACK. If there was a timeout, the congestion window size would have dropped to 1.

d. After the 22nd transmission round, is segment loss detected by a triple

duplicate ACK or by a timeout?

Answer: After the 22nd transmission round, segment loss is detected due to timeout, and the congestion window size is set to 1.

e. What is the initial value of ssthresh at the first transmission round?

Answer: The threshold is initially 32, since it is at this window size that slow start stops and congestion avoidance begins.

f. What is the value of ssthresh at the 18th transmission round?

Answer: The threshold is set to half the value of the congestion window when packet loss is detected. When loss is detected during transmission round 16, the congestion windows size is 42. Hence the threshold is 21 during the 18th transmission round.

g. What is the value of ssthresh at the 24th transmission round?

Answer: The threshold is set to half the value of the congestion window when packet loss is detected. When loss is detected during transmission round 22, the congestion window size is 29. Hence the threshold is 14 (taking a lower floor of 14.5) during the 24th transmission round.

h. During what transmission round is the 70th segment sent?

Answer: Packet 1 is sent in the 1st round, packets 2-3 in the 2nd, packets 4-7 in the 3rd, packets 8-15 in the 4th, packets 16-31 in the 5th, packets 32-63 in the 6th, and packets 64-96 in the 7th. Therefore, packet 70 is sent in the 7th round.

i. Assuming a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the values of the congestion window size and of ssthresh?

Answer: The threshold will be set to half the current value of the congestion window (8) when the loss occurs and the congestion window will be set to the new threshold value + 3 MSS. Thus the new values of the threshold and window will be 4 and 7 respectively.

j. Suppose TCP Tahoe is used (instead of TCP Reno), and assume that triple duplicate ACKs are received at the 16th round. What are the ssthresh and the congestion window size at the 19th round?

Answer: threshold is 21, and congestion window size is 1

k. Again suppose TCP Tahoe is used, and there is a timeout event at 22nd round. How many packets have been sent out from 17th round till 22nd round, inclusive?

Answer: round 17, 1 packet; round 18, 2 packets; round 19, 4 packets; round 20, 8 packets; round 21, 16 packets; round 22, 21 packets. So, the total number is 52.

P44. Consider sending a large file from a host to another over a TCP connection that has no loss.

a. Suppose TCP uses AIMD for its congestion control without slow start. Assuming cwnd increases by 1 MSS every time a batch of ACKs is received and assuming approximately constant round-trip times, how long does it take for cwnd increase from 6 MSS to 12 MSS (assuming no loss events)?

Answer: It takes one round-trip time (RTT) for the congestion window (CongWin) to increase to 7 maximum segment sizes (MSS). Subsequently, it takes two RTTs to increase to 8 MSS, three RTTs to reach 9 MSS, four RTTs to attain 10 MSS, five RTTs to achieve 11 MSS, and six RTTs to progress to 12 MSS.

b. What is the average throughput (in terms of MSS and RTT) for this connection up through time = 6 RTT?

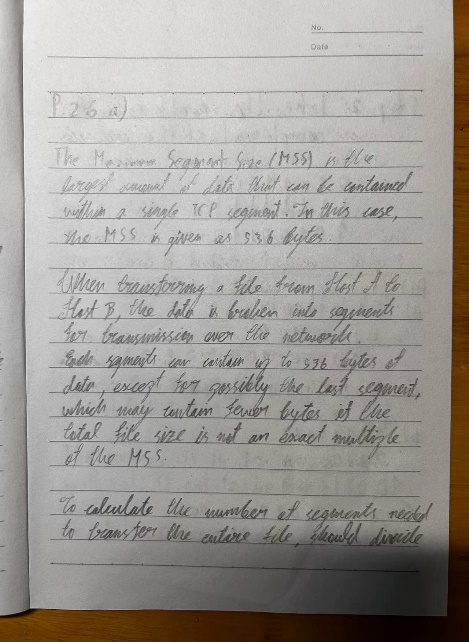
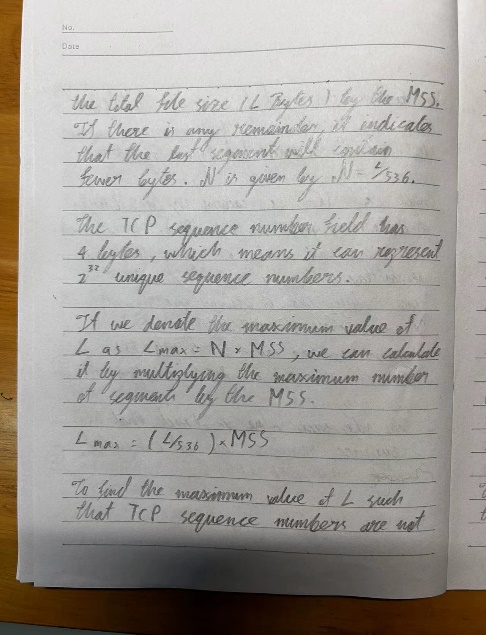
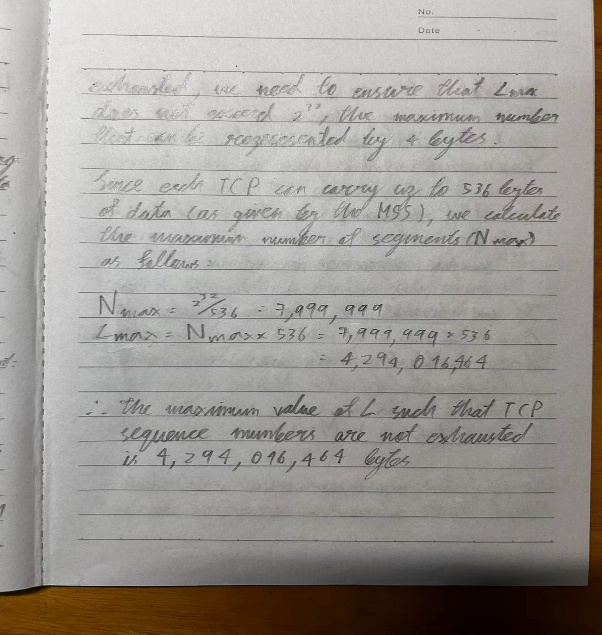
Answer: During the first round-trip time (RTT), 6 maximum segment sizes (MSS) were transmitted. In the subsequent RTT, 7 MSS were sent, followed by 8 MSS in the third RTT, 9 MSS in the fourth RTT, 10 MSS in the fifth RTT, and finally 11 MSS in the sixth RTT. Consequently, within the first 6 RTTs, this sequence of increasing MSS values was observed.

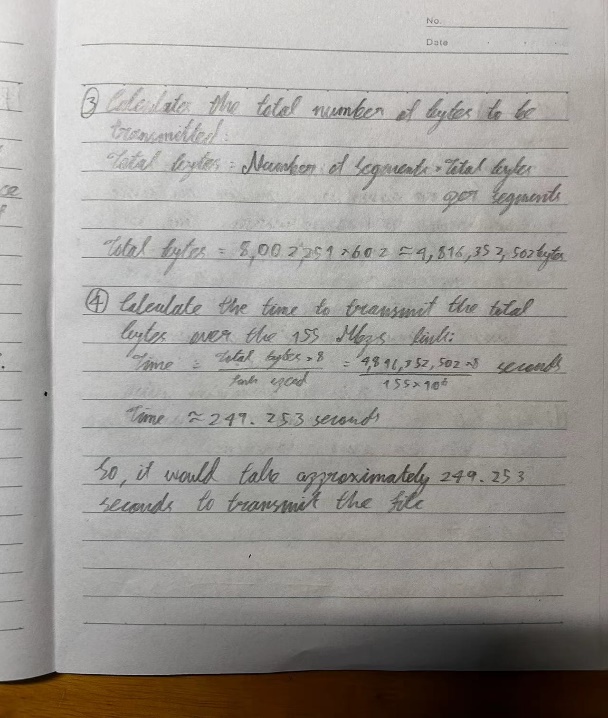
**Homework 8**

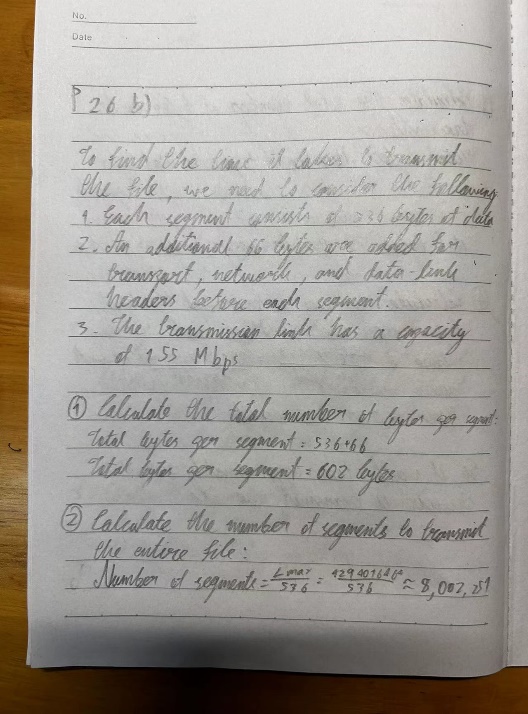
P26. Consider transferring an enormous file of L bytes from Host A to Host B. Assume an MSS of 536 bytes.

a. What is the maximum value of L such that TCP sequence numbers are not exhausted? Recall that the TCP sequence number field has 4 bytes.

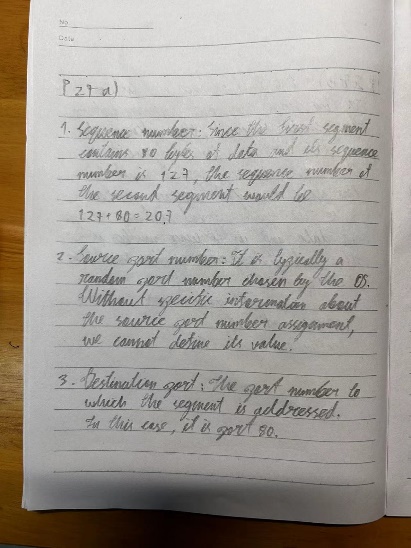
Answer:

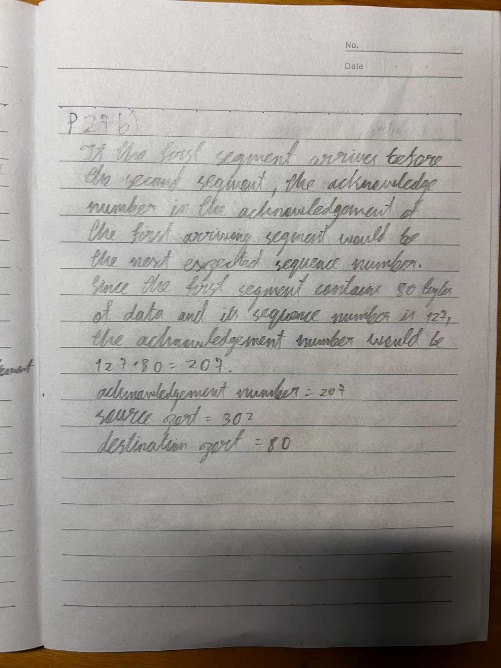


b. For the L you obtain in (a), find how long it takes to transmit the file. Assume that a total of 66 bytes of transport, network, and data-link header are added to each segment before the resulting packet is sent out over a 155 Mbps link. Ignore flow control and congestion control so A can pump out the segments back-to-back and continuously.

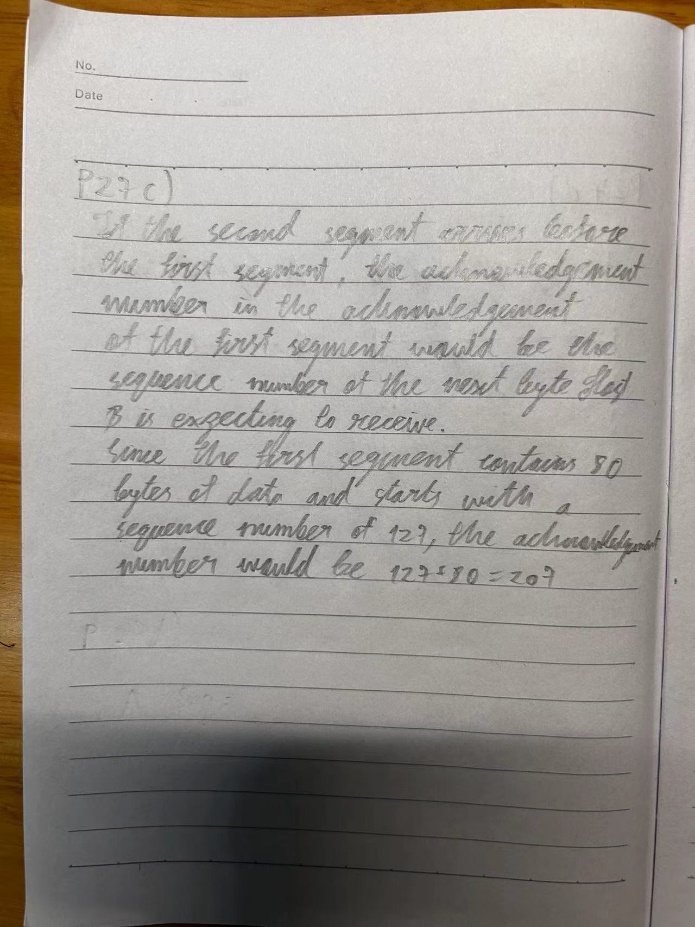
Answer:

P27. Host A and B are communicating over a TCP connection, and Host B has already received from A all bytes up through byte 126. Suppose Host A then sends two segments to Host B back-to-back. The first and second M03\_KURO1557\_08\_SE\_C03.indd 292 11/02/20 12:15 PM segments contain 80 and 40 bytes of data, respectively. In the first segment, the sequence number is 127, the source port number is 302, and the destination port number is 80. Host B sends an acknowledgment whenever it receives a segment from Host A.

a. In the second segment sent from Host A to B, what are the sequence number, source port number, and destination port number?

b. If the first segment arrives before the second segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number, the source port number, and the destination port number?

c. If the second segment arrives before the first segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number?



d. Suppose the two segments sent by A arrive in order at B. The first

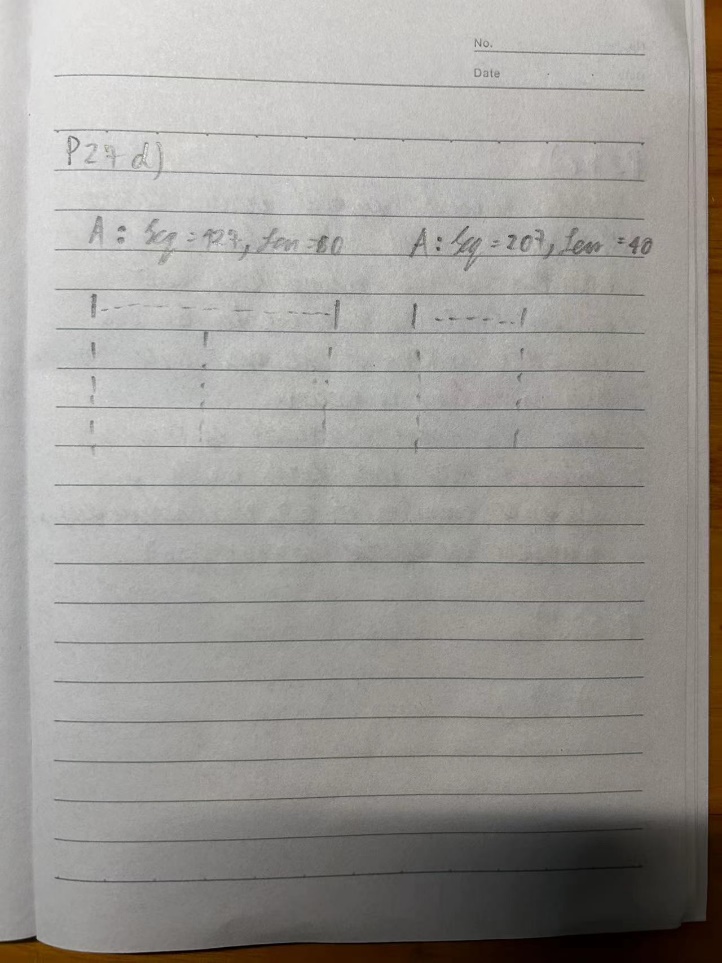
acknowledgment is lost and the second acknowledgment arrives after the

first timeout interval. Draw a timing diagram, showing these segments

and all other segments and acknowledgments sent. (Assume there is no

additional packet loss.) For each segment in your figure, provide the

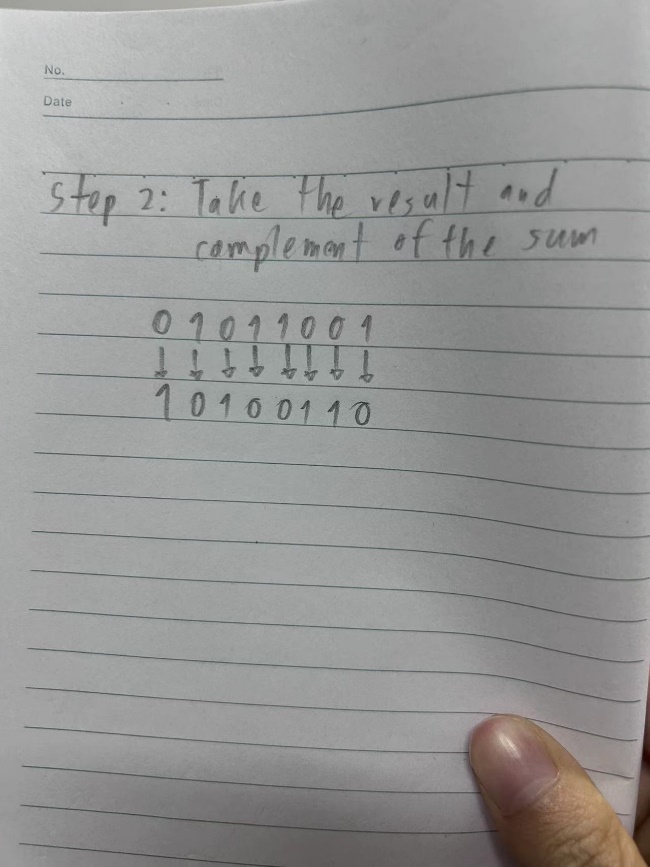
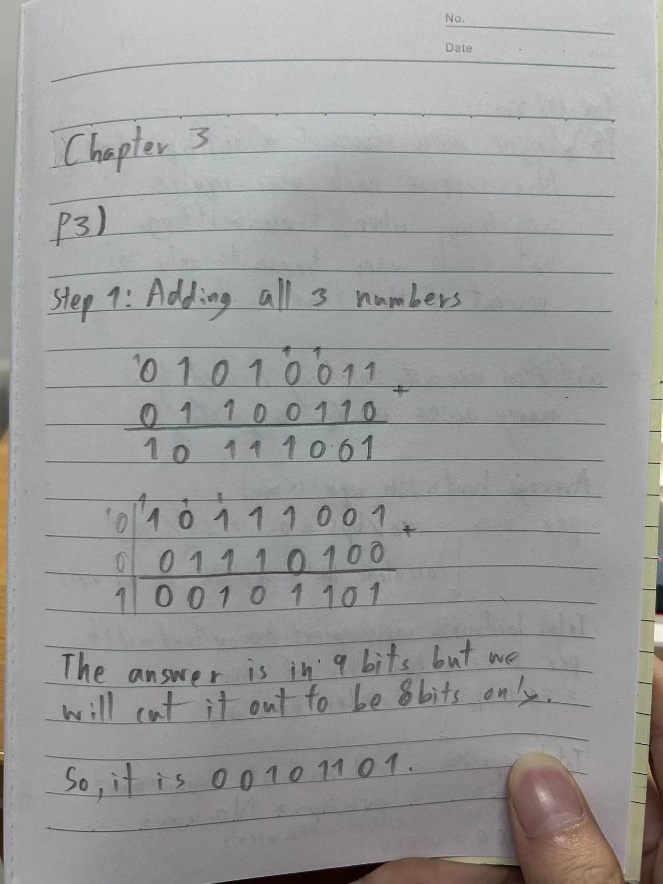
sequence number and the number of bytes of data; for each acknowledgment that you add, provide the acknowledgment number



**Homework 7**

P3. UDP and TCP use 1s complement for their checksums. Suppose you have the following three 8-bit bytes: 01010011, 01100110, 01110100. What is the 1s complement of the sum of these 8-bit bytes? (Note that although UDP and TCP use 16-bit words in computing the checksum, for this problem you are being asked to consider 8-bit sums.) Show all work.

**Answer:**

****

Why is it that UDP takes the 1s complement of the sum; that is, why not just use the sum?

**Answer:** UDP uses the one's complement of the sum to provide better error detection, helping to ensure the data is transmitted accurately.

With the 1s complement scheme, how does the receiver detect errors?

**Answer:** The receiver calculates its own checksum using the same method as the sender. It adds up all the parts of the data and takes the one's complement of the sum. Then it compares this calculated checksum with the one it received.

If the calculated checksum matches the received checksum, it means the data is likely to have no error. But if the calculated checksum is different from the received checksum, it means errors may have occurred during transmission.

So, by comparing the calculated checksum with the received checksum, the receiver can tell if there are errors in the data.

Is it possible that a 1-bit error will go undetected? How about a 2-bit error?

**Answer:** For 1 bit error, it will always be detected by the checksum, but for 2 bits errors sometimes it could not be detected because there are certain combinations of errors that can cancel each other out.

P4.

a. Suppose you have the following 2 bytes: 01011100 and 01100101. What is the 1s complement of the sum of these 2 bytes?

**Answer:** Adding = 11000001**,** Complement = 00111110

b. Suppose you have the following 2 bytes: 11011010 and 01100101. What is the 1s complement of the sum of these 2 bytes?

**Answer:** Adding = 100111111, Complement = 011000000

c. For the bytes in part (a), give an example where one bit is flipped in each of the 2 bytes and yet the 1s complement doesn’t change.

**Answer:** First byte = 01010100, Second byte = 01101101

**Homework 6**

P26. Suppose Bob joins a BitTorrent torrent, but he does not want to upload any data to any other peers (so called free-riding).

a. Bob claims that he can receive a complete copy of the file that is shared by the swarm. Is Bob’s claim possible? Why or why not?

**Answer**: It is possible because the system of BitTorrent decided to make the users being P2P in order to download and share data together. Nevertheless, in Bob’s case he wants to download the file only which he might be able to download, but the other peers will see that he does not upload anything, so they will not support him much and it is going to make Bob downloading file slower.

b. Bob further claims that he can further make his “free-riding” more efficient by using a collection of multiple computers (with distinct IP addresses) in the computer lab in his department. How can he do that?

**Answer**: In my own perspective, I think that Bob does is according to these following steps.

1. Install BitTorrent to computers: Bob would install BitTorrent into his main computer and into other computers.

2. Start download on each computer: Let say Bob downloaded the same file into every of his computers and with BitTorrent these computers will receive and share data between themselves, Bob’s main computer, and the server.

3. Combine downloaded parts: Once each computer has downloaded parts of the file, Bob can combine these parts manually or use synchronization tools to gather all the downloaded fragments into a complete file on one of the computers.

These are the steps that I think Bob does in order to make him available to download file without sharing back to the society, however, it violates the purpose of BitTorrent that would like very users share and receive the information together as if they are working in group project.

**Homework 5**

P12. Write a simple TCP program for a server that accepts lines of input from a client and prints the lines onto the server’s standard output. (You can do this by modifying the TCPServer.py program in the text.) Compile and execute your program. On any other machine that contains a Web browser, set the proxy server in the browser to the host that is running your server program; also, configure the port number appropriately. Your browser should now send its GET request messages to your server, and your server should display the messages on its standard output. Use this platform to determine whether your browser generates conditional GET messages for objects that are locally cached.

P15. What is the difference between MAIL FROM: in SMTP and From: in the mail message itself?

*MAIL FROM in SMTP:*

It is a part of the SMTP protocol used for sending emails. It is used by the sending mail server to the receiving mail server to start the process of delivering an email message. Moreover, the purpose of it is for routing the receiving email server to determine where non-delivery notifications should be sent in case of delivery failure.

*From: in the mail itself:*

The “From:” field is a header field in the email message itself. It is used to specify the email address of the sender that is displayed to the recipients. Furthermore, it identifies the sender of the message to the recipients.

In summary, while both "MAIL FROM" in SMTP and "From:" in the email message itself involve specifying the sender's email address, "MAIL FROM" is used in the email delivery process between mail servers, whereas "From:" is a header field in the email message that identifies the sender to the recipients.

P20. Suppose you can access the caches in the local DNS servers of your department. Can you propose a way to roughly determine the Web servers (outside your department) that are most popular among the users in your department? Explain.

**1. Access DNS Cache Records:**

Gain access to the DNS cache records in your department's local DNS servers.

**2. Extract Hostnames:**

Extract the hostnames or domain names from the DNS cache records.

**3. Count Frequency:**

Count the frequency of each hostname or domain name.

**4. Rank Websites:**

Rank the websites based on their frequency of access.

**5. Analyze Trends:**

Monitor trends over time to understand changes in website popularity.

**6. Consider Hosting Providers:**

Identify the hosting providers associated with popular websites.

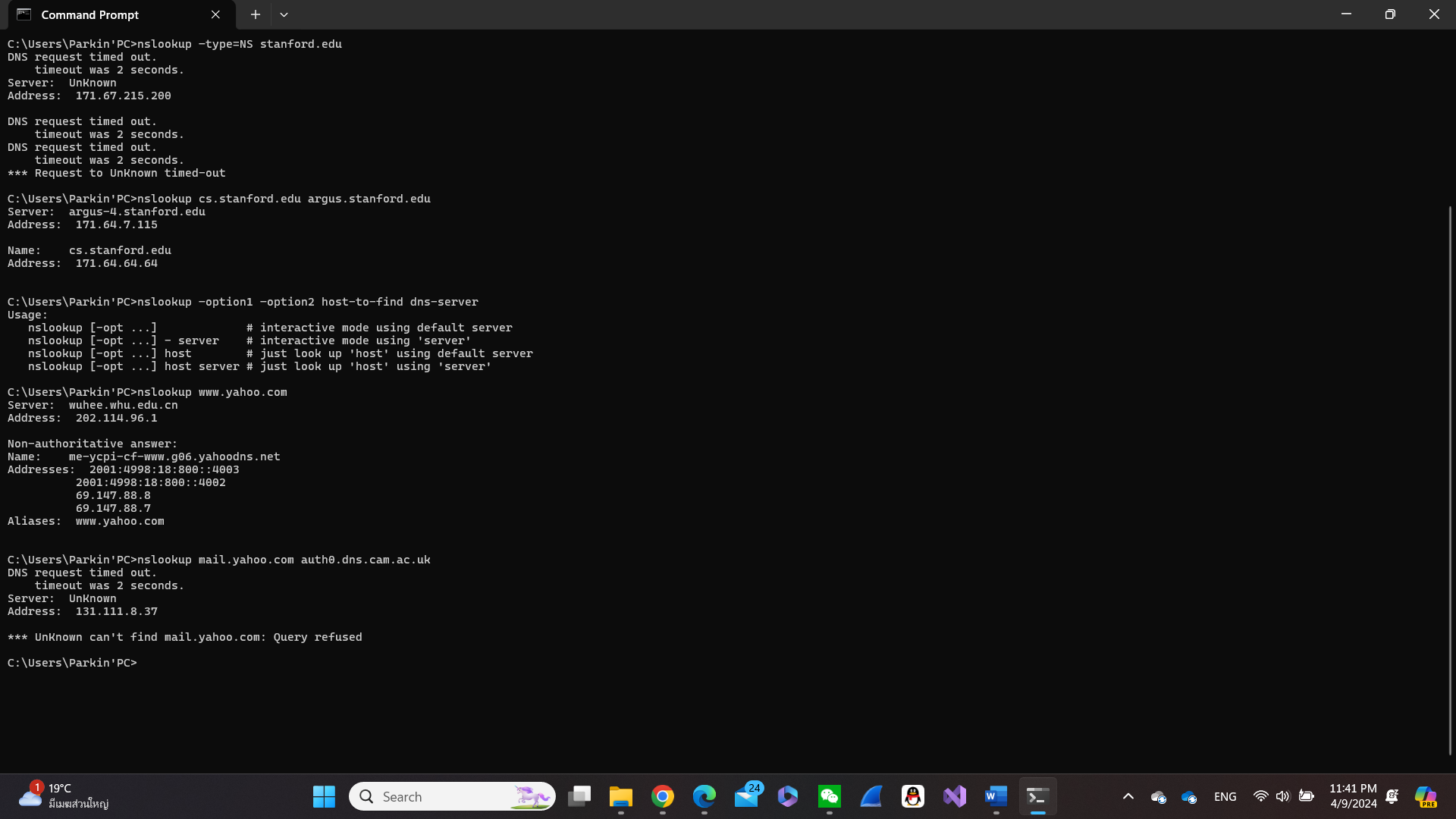
**7. Aggregate Data:**

Aggregate data over time for accuracy.

**8. Ensure Privacy:**

Respect user privacy and comply with relevant regulations

**Lab 4 Wireshark DNS1**

****

1. Run *nslookup* to obtain the IP address of a Web server in China. What is the IP address of that server?

Answer: Addresses: 2001:250:4001:2::1223

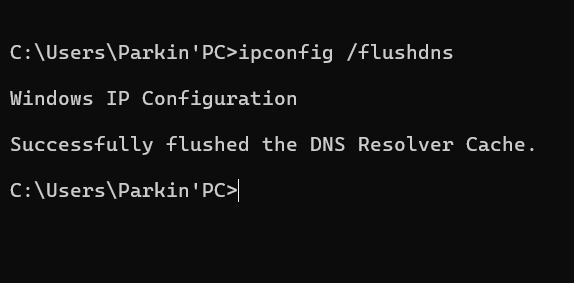
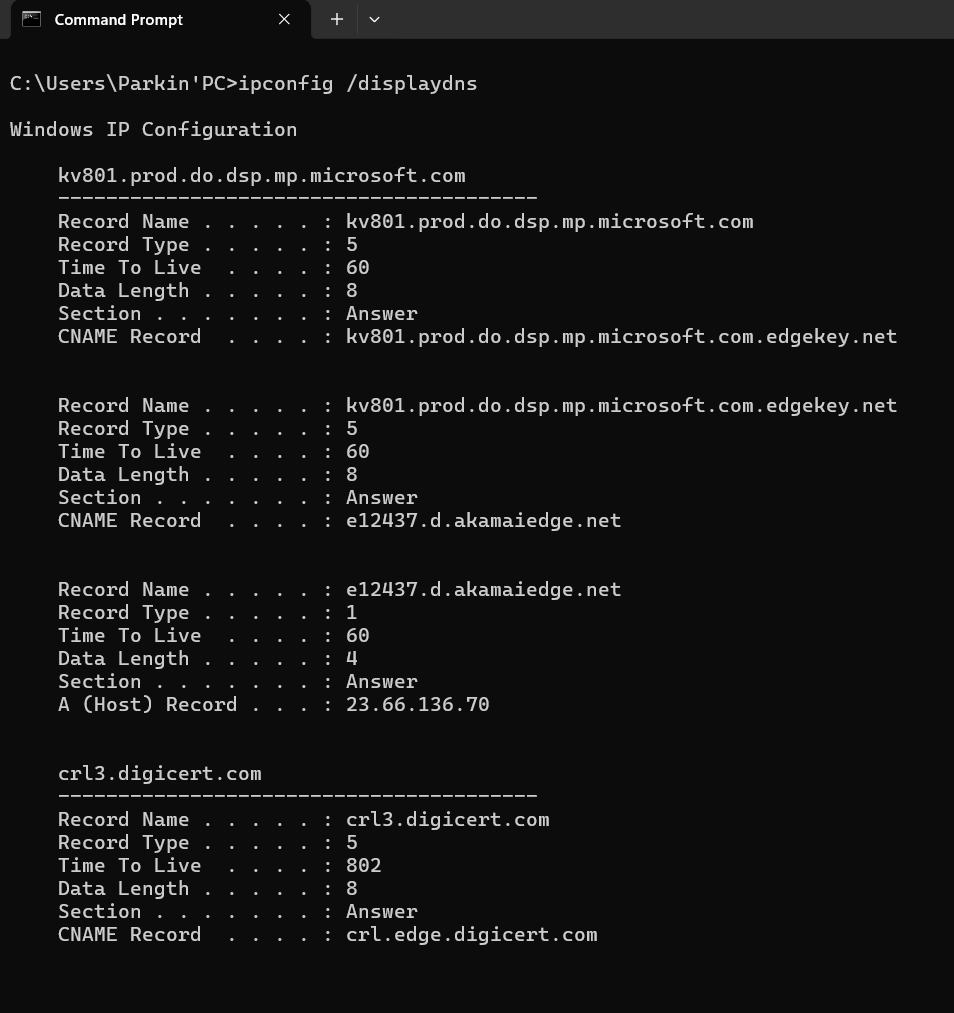
202.114.64.221

1. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

Answer: Address: 171.67.215.200

1. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Answer: Address: 131.111.8.37



1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer: Yes, they do. “User Datagram Protocol, Src Port: 63037, Dst Port: 53”

1. What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer: Destination of the port is Dst Port: 53

1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Answer: DNS query message sent Source: 10.131.191.53 and Destination: 202.114.96.1 Furthermore, they sent the same information.

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz

Physical Address. . . . . . . . . : D8-3B-BF-5B-1A-9E

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::b8e7:feb7:f398:efd5%17(Preferred)

IPv4 Address. . . . . . . . . . . : 10.131.191.53(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.128.0

Lease Obtained. . . . . . . . . . : Tuesday, April 9, 2024 9:41:02 PM

Lease Expires . . . . . . . . . . : Wednesday, April 10, 2024 1:37:25 AM

Default Gateway . . . . . . . . . : 10.131.255.254

DHCP Server . . . . . . . . . . . : 10.131.255.254

DHCPv6 IAID . . . . . . . . . . . : 282606527

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-0C-2A-74-F8-75-A4-E2-D9-B8

DNS Servers . . . . . . . . . . . : 202.114.96.1

202.114.64.1

NetBIOS over Tcpip. . . . . . . . : Enabled

1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: It is query type A and it did not contain any answers.

1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer: In my Wireshark, it appeared no answers.

1. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer: It is TCP destination: 199.16.156.11

1. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Answer: No, it did not contain any images.

1. What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer: Port53

1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer: Destination: 202.114.96.1 and it is the IP address of my local DNS server.

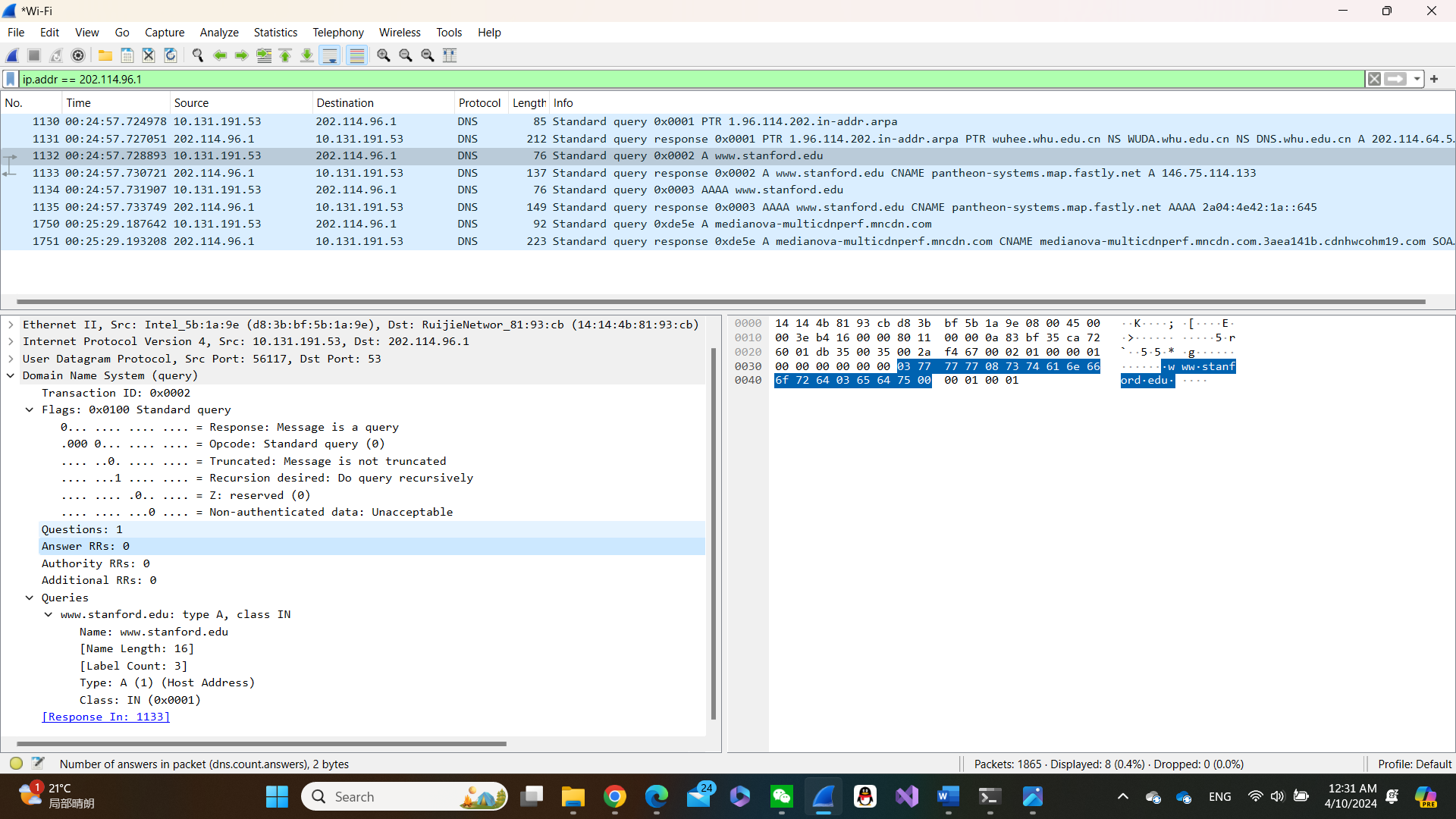
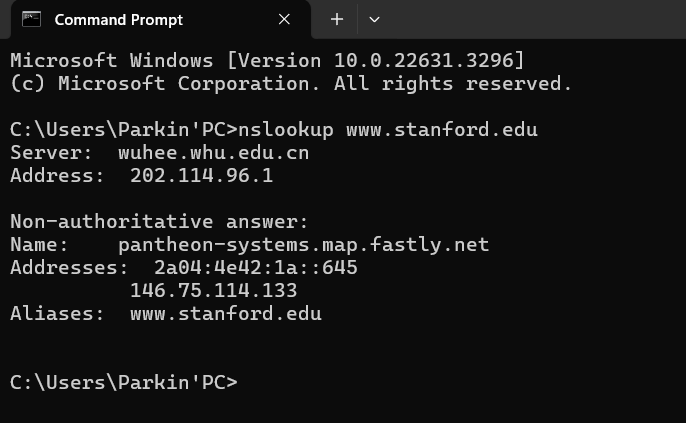
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: They said the query are types A and AAQ but did not contain any answers.

1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer: In my Wireshark it did not show the answers in the queries section.

1. Provide a screenshot.



16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer: Destination: 202.114.96.1 and it is the IP address of my local DNS server

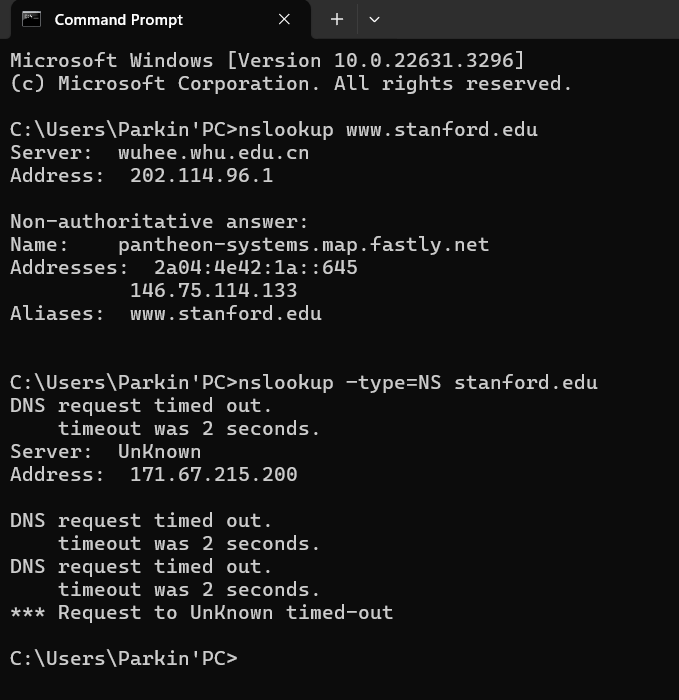
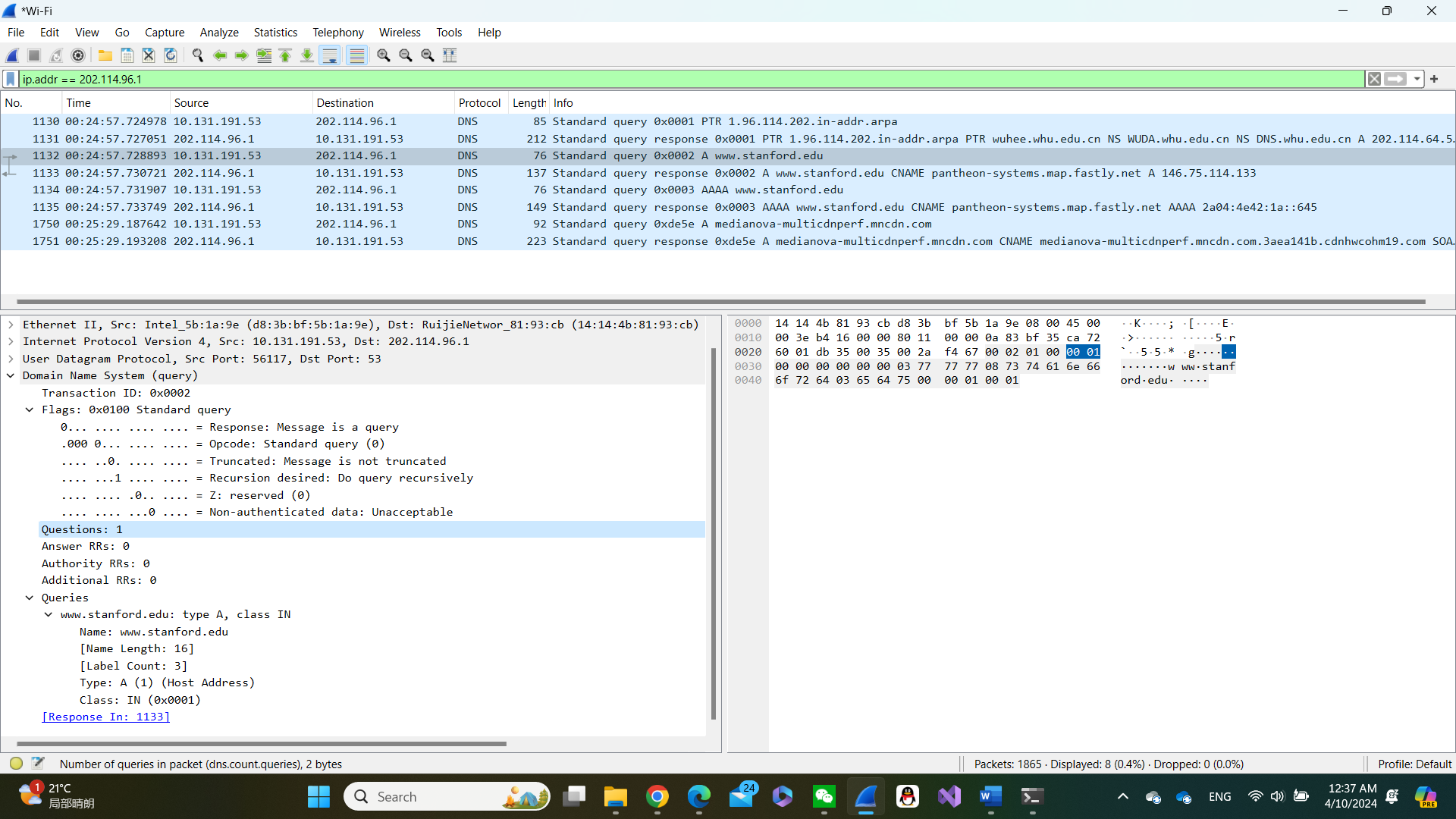
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: Query type A and it does not contain any message.

18. Examine the DNS response message. What Stanford nameservers does the response message provide? Does this response message also provide the IP addresses of the Stanford name servers?

Answer: In my Wireshark, it did not show any message.

19. Provide a screenshot

****

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Answer: First it is sent to get to default DNS query message to get address of [www.stanford.edu](http://www.stanford.edu) then it was sent to [www.stanford.edu](http://www.stanford.edu) .

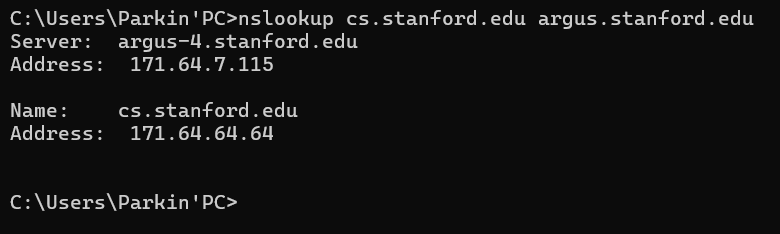
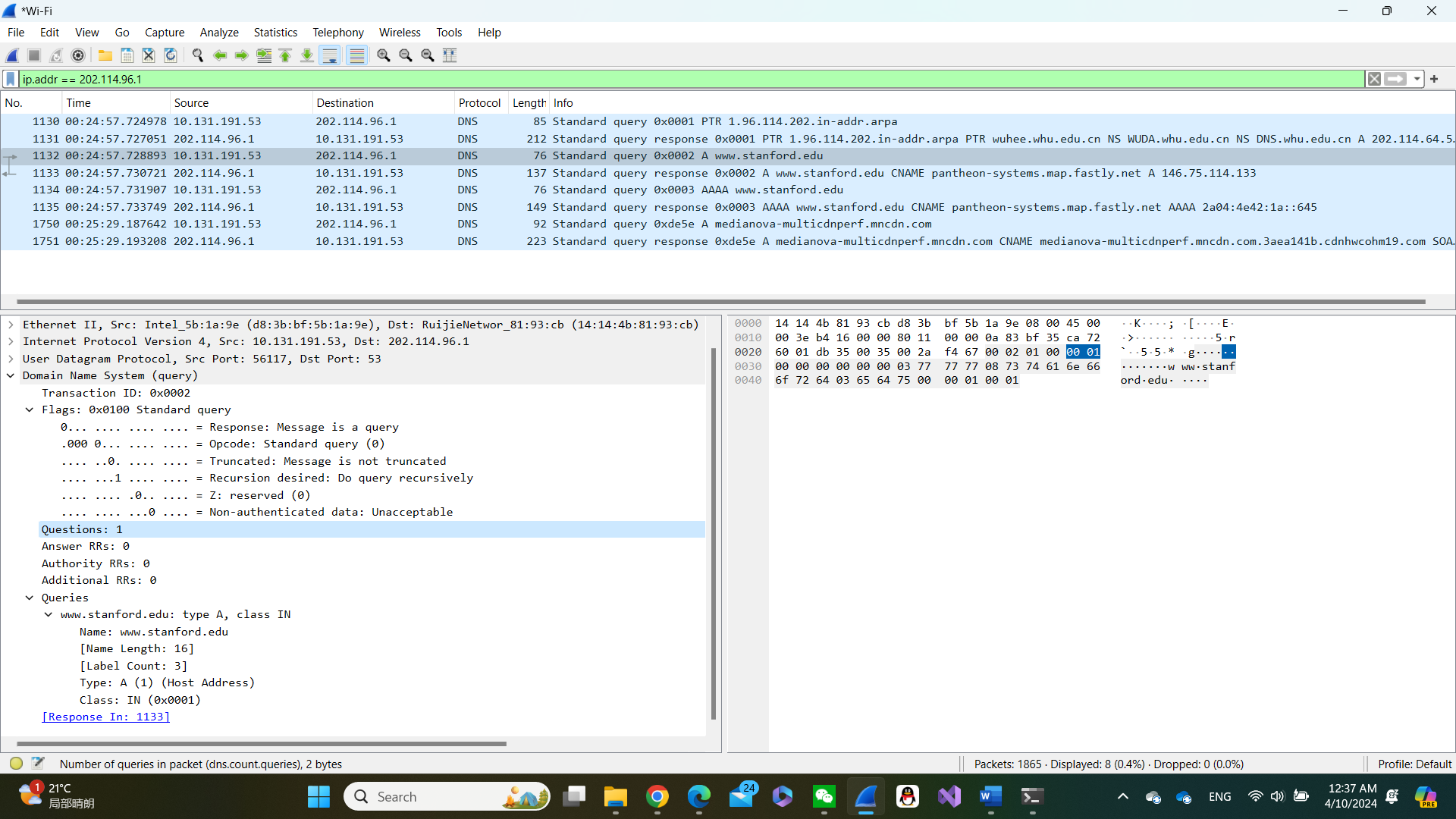
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: The types of queries are A and AAA, moreover, it does not contain any message

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Answer: In my Wireshark, it does not show any answers.

23. Provide a screenshot.

****

**Homework 4**

**P4**. Consider the following string of ASCII characters that were captured by Wireshark when the browser sent an HTTP GET message (i.e., this is the actual content of an HTTP GET message). The characters are carriage return and line-feed characters (that is, the italized character string in the text below represents the single carriage-return character that was contained at that point in the HTTP header). Answer the following questions, indicating where in the HTTP GET message below you find the answer.

GET /cs453/index.html HTTP/1.1Host: gai a.cs.umass.eduUser-Agent: Mozilla/5.0 ( Windows;U; Windows NT 5.1; en-US; rv:1.7.2) Gec ko/20040804 Netscape/7.2 (ax) Accept:ex t/xml, application/xml, application/xhtml+xml, text /html;q=0.9, text/plain;q=0.8,image/png,\*/\*;q=0.5 M02\_KURO1557\_08\_SE\_C02.indd 168 12/02/20 4:08 PM PROBLEMS 169 Accept-Language: en-us,en;q=0.5AcceptEncoding: zip,deflateAccept-Charset: ISO -8859-1,utf-8;q=0.7,\*;q=0.7Keep-Alive: 300 Connection:keep-alive

a. What is the URL of the document requested by the browser?

- The URL of the document requested by the browser is “cs453/index.html”.

b. What version of HTTP is the browser running?

- The version of HTTP that the browser is running is HTTP/1.1.

c. Does the browser request a non-persistent or a persistent connection?

- The browser requests a persistent connection because “Connection: keep-alive”.

d. What is the IP address of the host on which the browser is running?

- No, the provided string doesn't contain the IP address

e. What type of browser initiates this message? Why is the browser type needed in an HTTP request message?

- The browser initiating this HTTP request message is Mozilla/5.0, which is common use with Firefox browser. There are several reasons why some browsers are using HTTP request message according to the following:

1) Content Negotiation: The server can use the information about the browser type to determine the appropriate content to send back.

2) Feature Detection: Servers may need to detect the capabilities of the browser to provide appropriate content or functionality. Different browsers support different features or standards, so this information can help tailor the response.

3) Logging and Analytics: Knowing the browser type helps in logging and analytics on the server side. Website owners can analyze the distribution of browsers accessing their site, which can inform decisions about website design and optimization.

4) Compatibility: It helps in ensuring compatibility with various browsers. By knowing the browser type, developers can ensure that the website or web application functions correctly across different browsers and versions.

**Lab 2 HTTP**

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

* HTTP 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?

- The system has not told.

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

- My computer IP: 10.131.165.58

- Website IP: 128.119.245.12

4. What is the status code returned from the server to your browser?

- Status Code: 404

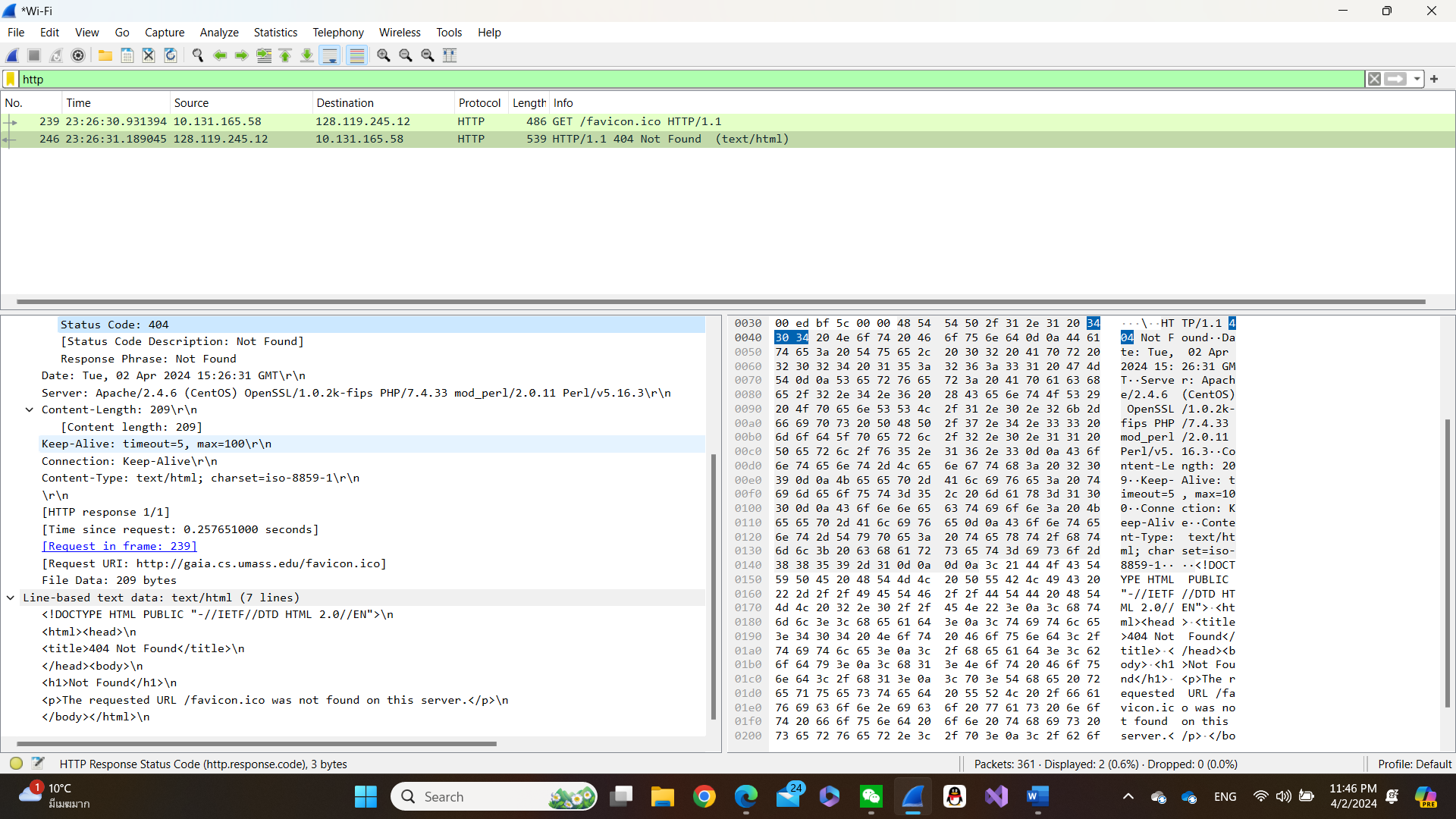
5. When was the HTML file that you are retrieving last modified at the server?

- Date: Tue, 02 Apr 2024 15:26:31 GMT\r\n

6. How many bytes of content are being returned to your browser?

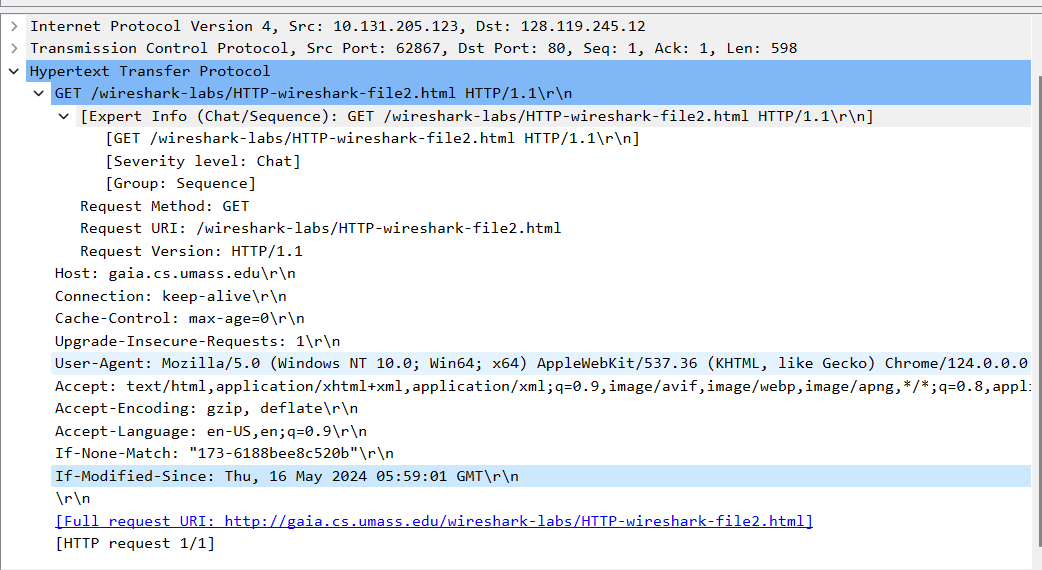
- File Data: 209 bytes

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.

- No, that's all

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?

- In the HTTP GET line I do not see “IF-MODIFIED-SINCE”.

Answer: If-Modified-Since: Thu, 16 May 2024 05:59:01 GMT

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

- The contents of the file in the response packet were discovered.

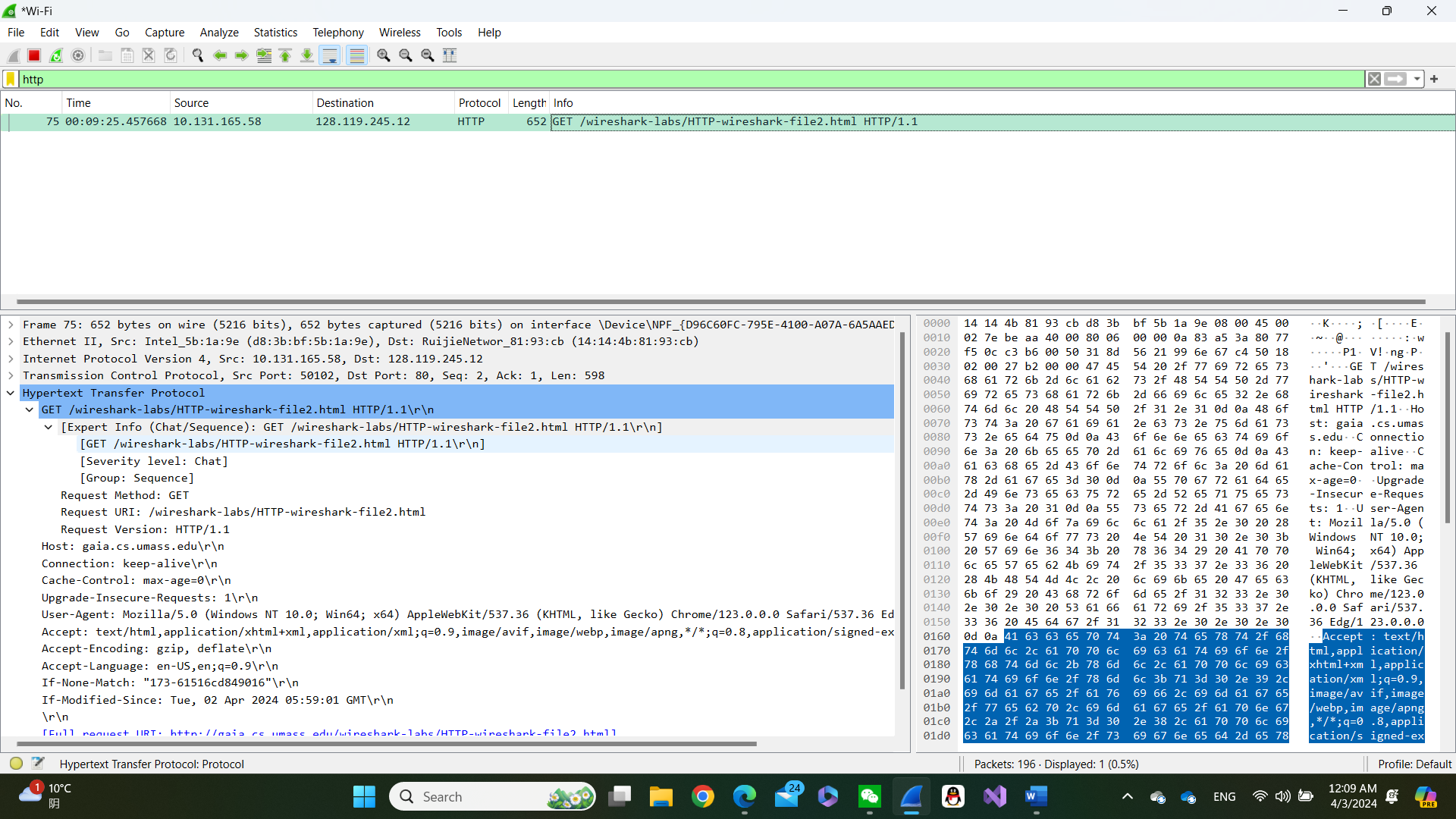
Answer:

10. 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?

- If-Modified-Since: Tue, 02 Apr 2024 05:59:01 GMT\r\n

11. 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.

- Status Code: 304 that is, it has not changed, and the text has not been retransmitted, but the existing text in the cache is directly called. This offloads servers and increases efficiency.



12. 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?

- I saw 1 GET methods and the trace number is 62.

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

- Packet number 638

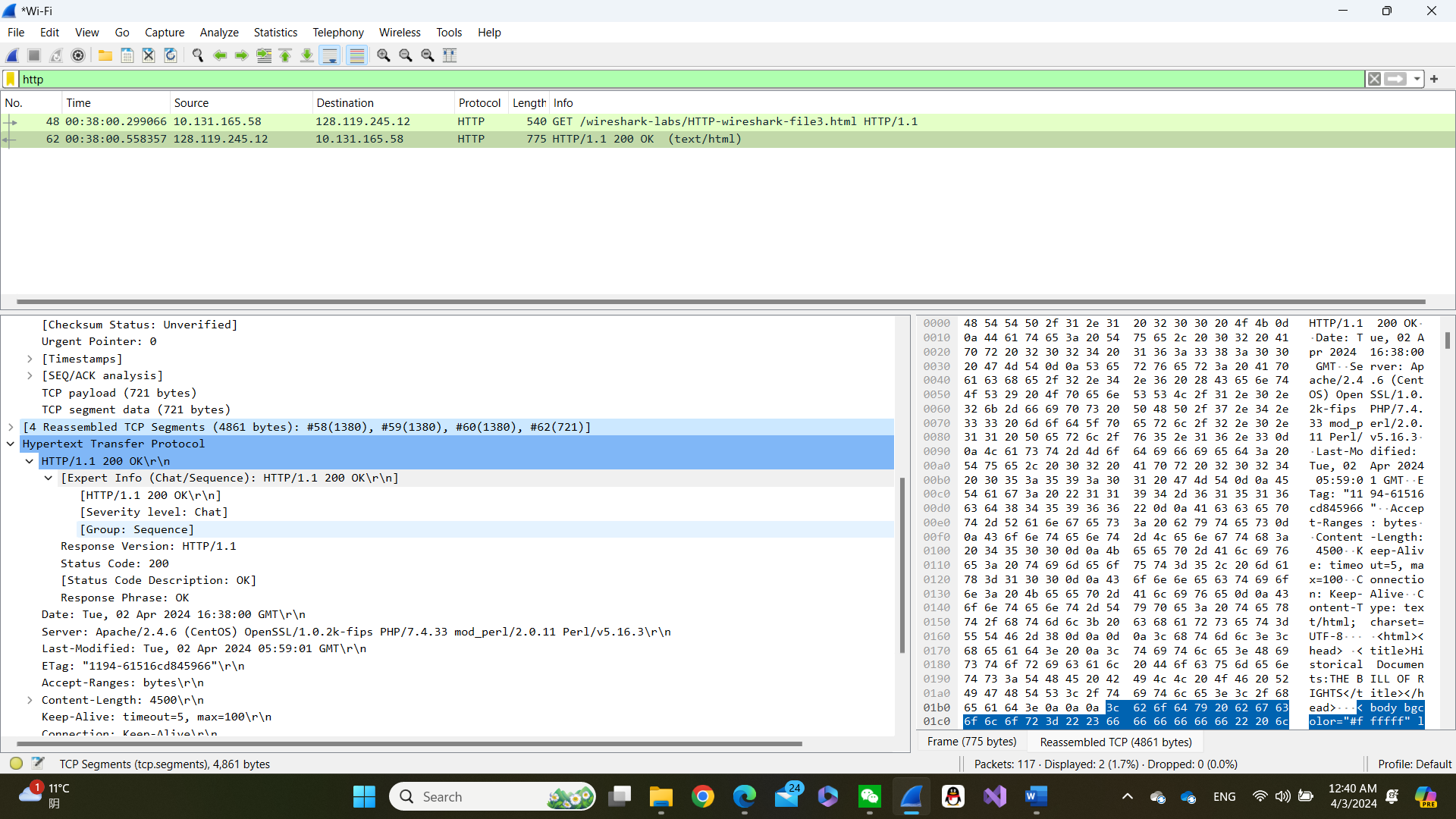
14. What is the status code and phrase in the response?

- Status Code: 200

- [Status Code Description: Not Modified]

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

- [4 Reassembled TCP Segments (4861 bytes): #58(1380), #59(1380), #60(1380), #62(721)]

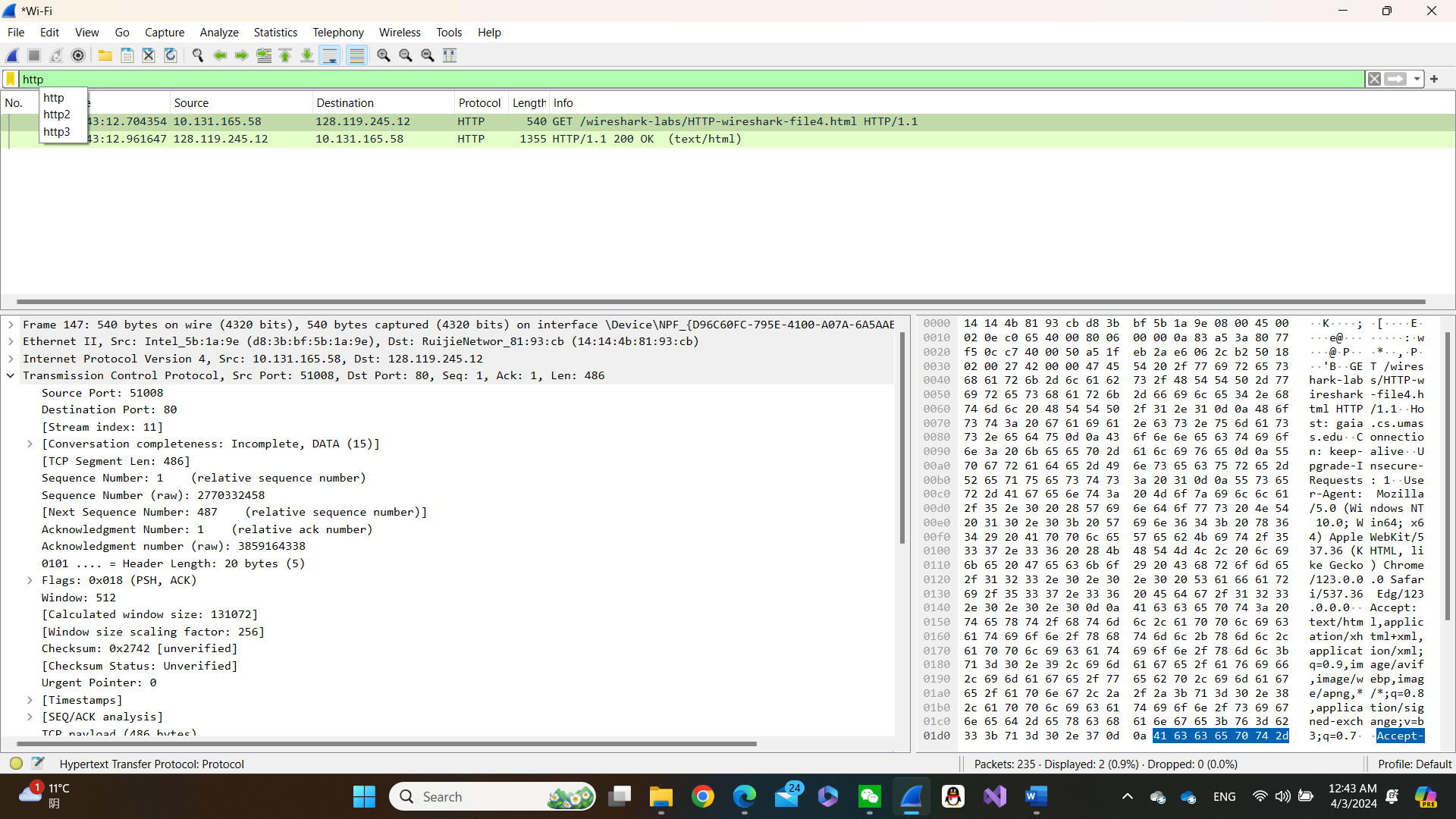


16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

- 1 GET requests

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.

- I'm not sure if this concurrency is really sent at the same time, but GET packets are sent at different times, so I think they should be sent sequential not parallel.

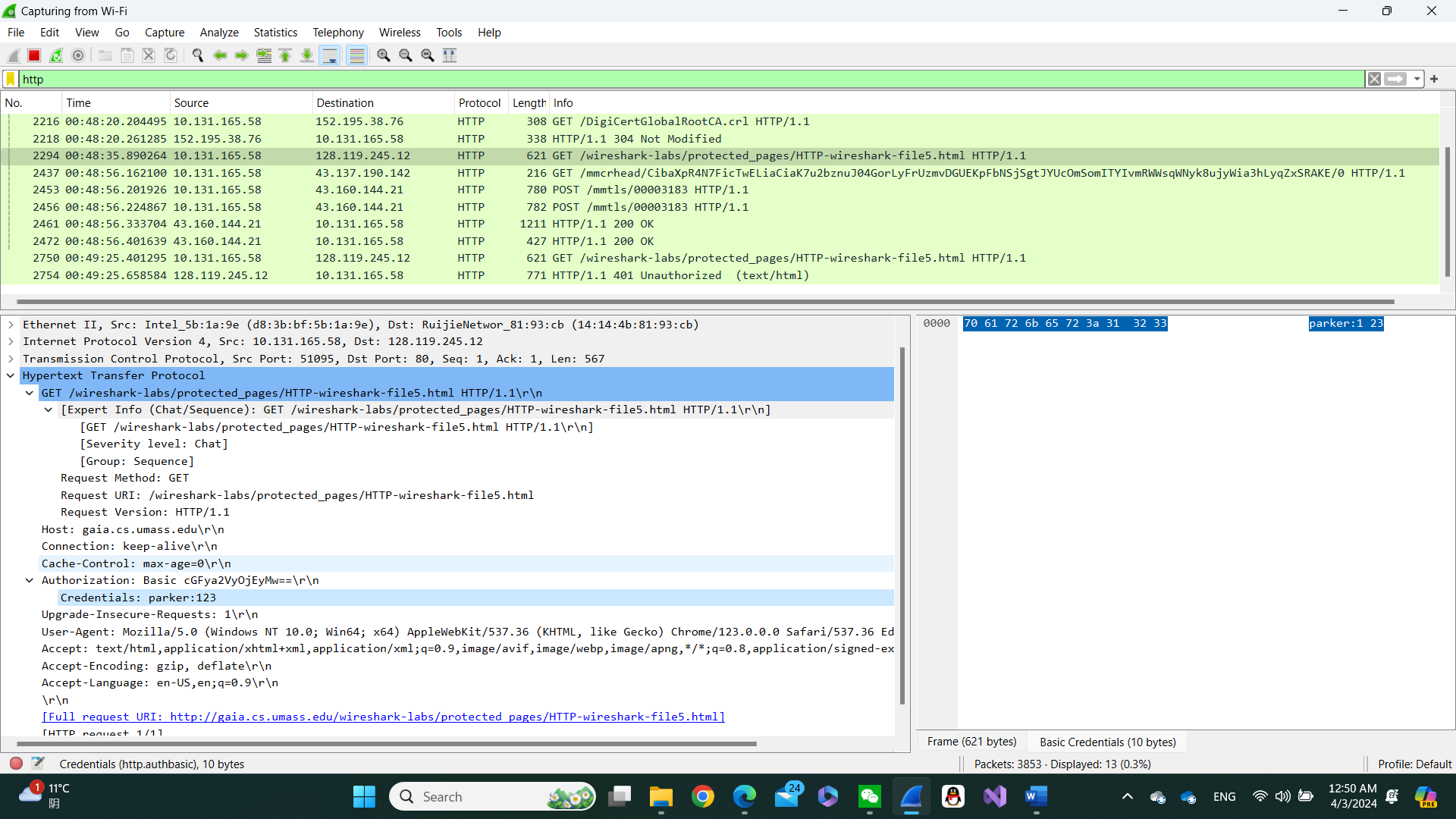


18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

- [HTTP/1.1 401 Unauthorized\r\n]

- [Severity level: Chat]

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 cGFya2VyOjEyMw==\r\n

- Credentials: parker:123

**Homework 3**

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

* UDP, TCP, ARP

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*.)

- GET message: 21:33:44.066485

- HTTP OK: 21:33:44.070267

Time to send = 0.01 seconds

3. What is the Internet address of the cs.whu.edu.cn? What is the Internet address of your computer?

* Address of cs.whu.ed.cn = 202.114.64.221
* Address of my computer = 10.131.166.249

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.

