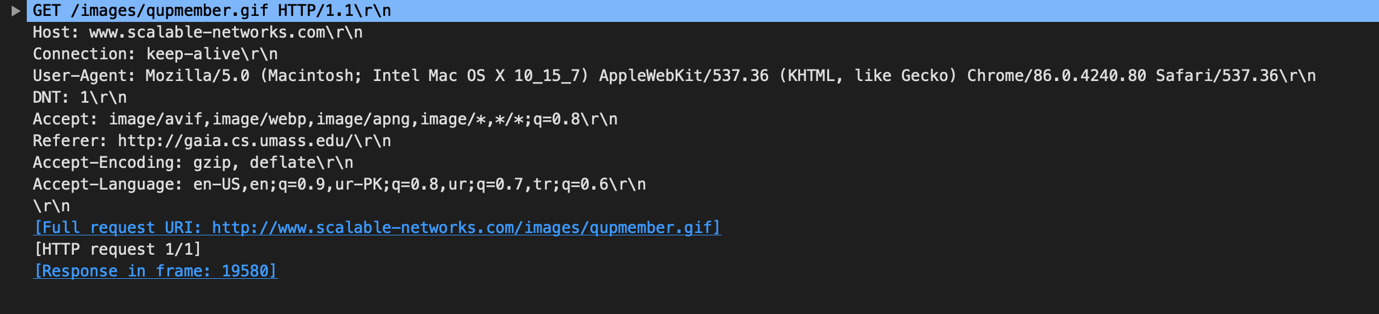
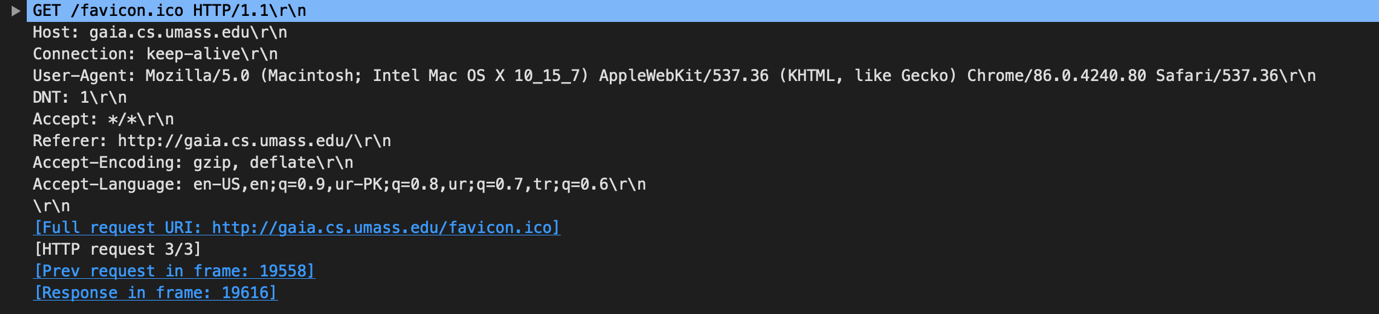
**Name: Muhammad Arham Khan**

**Section: CS421-1  
ID: 21701848**

Q1:

1. Ten protocols are: MDNS, LLMNR, HTTP, ARP, TCP, UDP, SSDP, DNS, DHCP, TLSv1.2.
2. 0.2183s
3. User Address : GAIA Address = 139.179.206.24 : 128.119.245.12



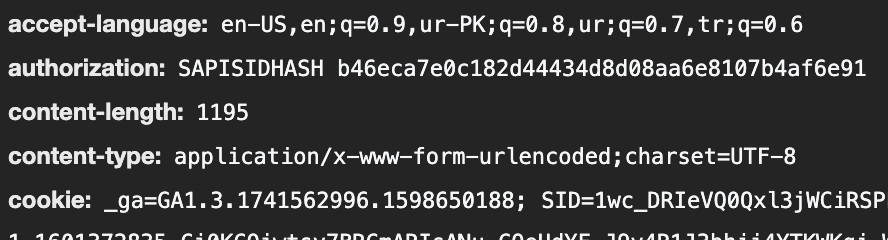


**PART 1: HTTP Requests**

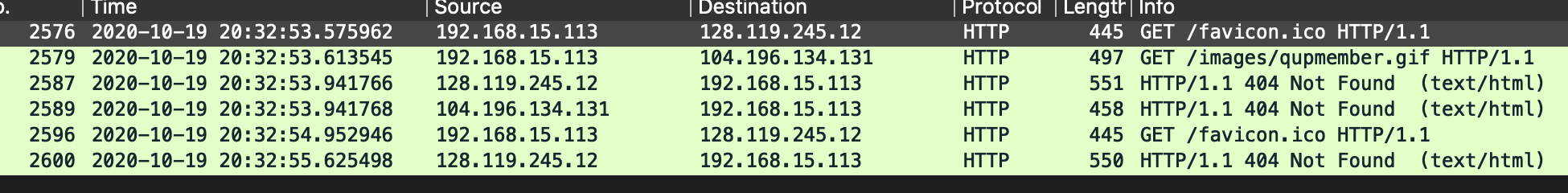
Q1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

* Yes, my browser and server both are running HTTP 1.1

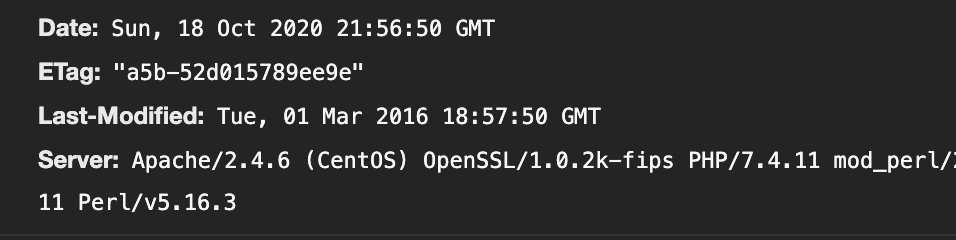
Q2) What languages (if any) does your browser indicate that it can accept to the server?

* Language = en
* 

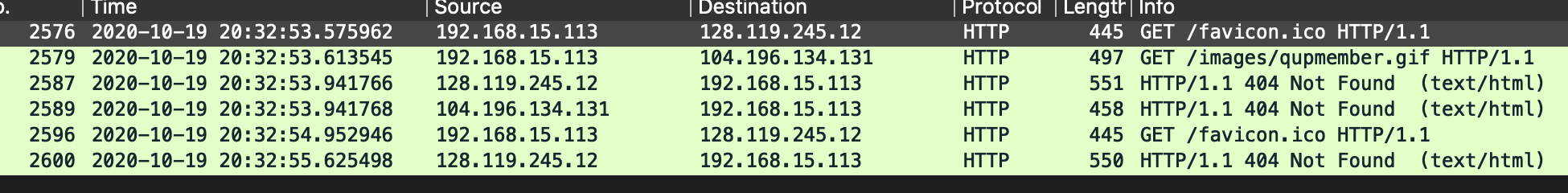
Q3) What is the IP address of your computer? Of the gaia.cs.umass.edu server?

* User Address : 139.179.206.181
* GAIA Address: 128.119.245.12
* 

Q4) When was the HTML file that you are retrieving last modified at the server?

* Tue, 01 Mar 2016 18:57:50 GMT\r\n
* 

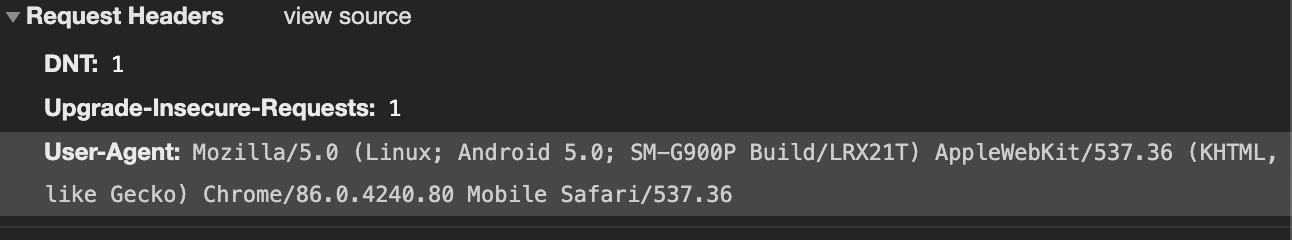
Q5) How many bytes of content are being returned to your browser?

* 497 bytes are being returned
* 

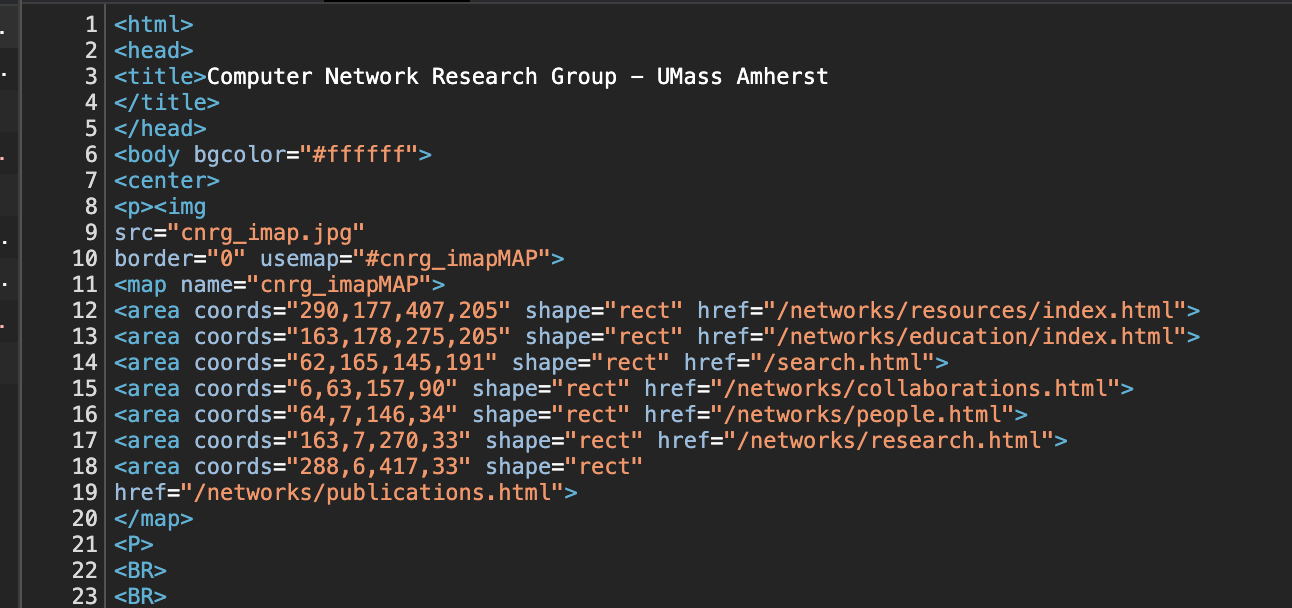
Q6) By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

* No, I don’t see any such headers

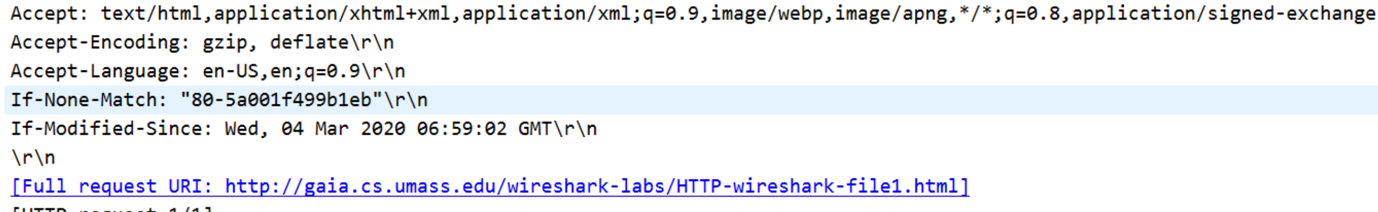
Q8) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

* No, I don’t see any such lines
* 

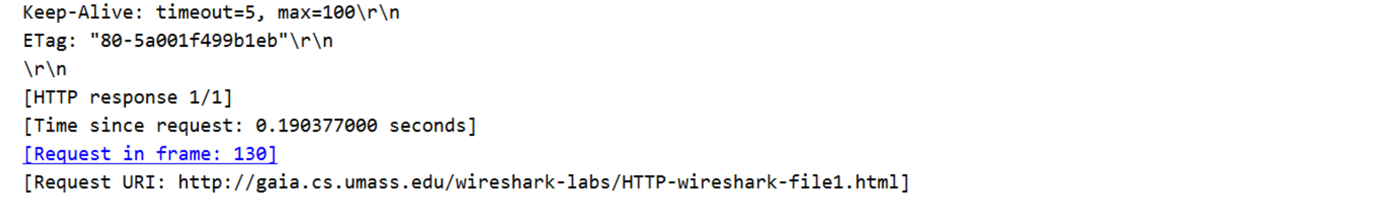
Q9) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

* It returned a full file in HTTP contents, and the status code was 200, that means the request was accepted
* 

Q10) 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: Wed, 04 Mar 2020 06:59:02 GMT
* 

Q11) 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.

* No, there were no contents returned, and the status code was 304, meaning the file has not been changes
* 

Q12) How many HTTP GET request messages were sent by your browser?

* Just one request was sent by my browser

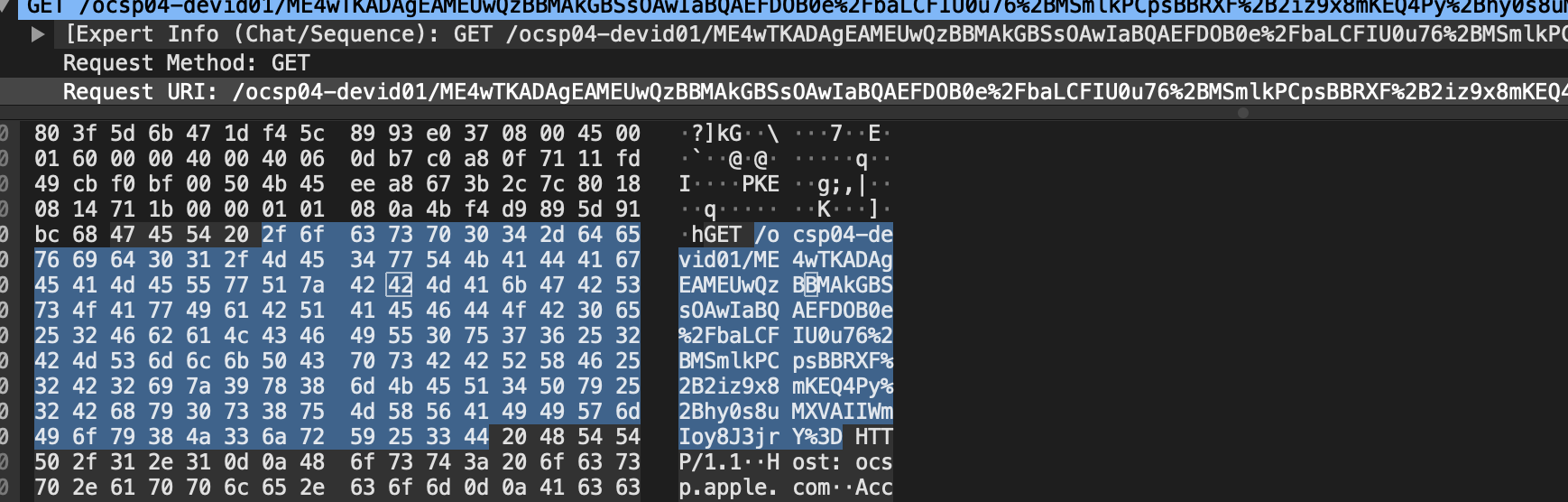
Q13) How many data-containing TCP segments were needed to carry the single HTTP response?

* TCP segments were 4
* 

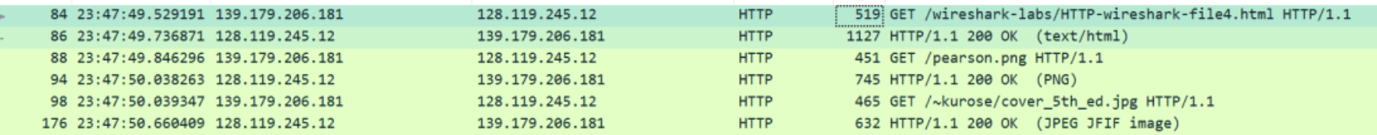
Q14) What is the status code and phrase associated with the response to the HTTP GET request?

* 200, OK
* 

Q15) Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?



Q16) How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

* 3 requests with different addresses but same IPs
* 

Q17) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

* They were downloaded serially because each GET request was made after the response was given for the prior request, seen by the timestamp

Q18) What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

* 401 unauthorized

Q19) When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

* Authorization was added in the second message, it contained the username and password

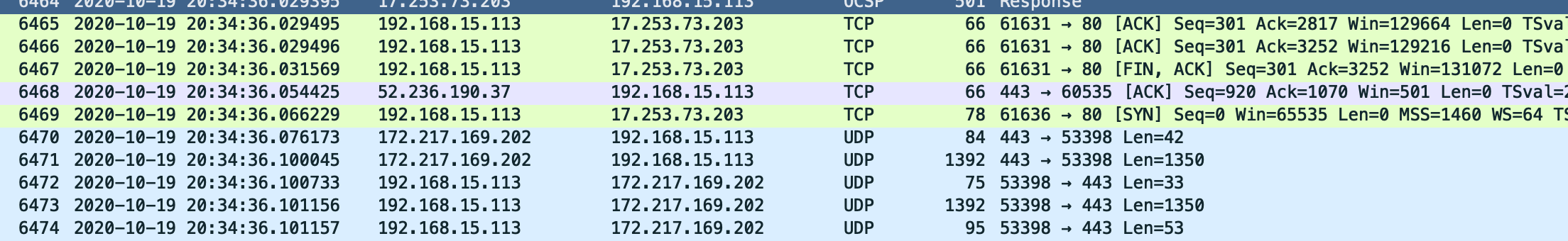
**PART 2: NSLOOKUP**

1. A web server in asia is: aliexpress.com
2. A web server of university in London is https://www.kingston.ac.uk/
3. firat.bcc.bilkent.edu.tr

**/sbin/ifconfig**



Q4) Locate the DNS query and response messages. Are they sent over UDP or TCP?

* It shows DNS on the listing, but in packet information, it shows UDP (User Datagram Protocol)
* 

Q5) What is the destination port for the DNS query message? What is the source port of DNS response message?

* Source Port: 62675, Destination Port: 53

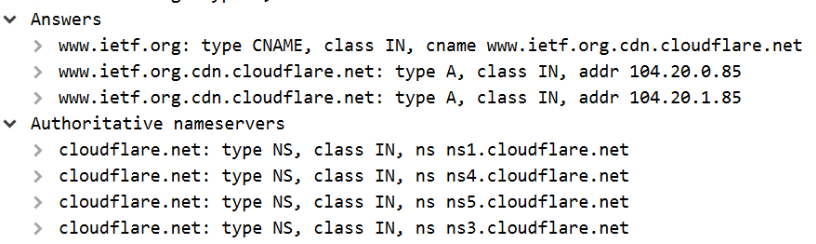
Q6) To what IP address is the DNS query message sent? Use *ipconfig* to determine the IP address of your local DNS server. Are these two IP addresses the same?

* The IP, DNS query was sent to, and the DNS servers listed in the ipconfig are both the same.

Q7) Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

* The query is Type ‘A’, The message does not contain any answers.

Q8) Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

* There are 3 answers in the response message and they contain the address for the Domain Searched for.
* 

Q9) 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?

* Yes, the Ip address for the SYN packet is the same as the address in answer by DNS response.