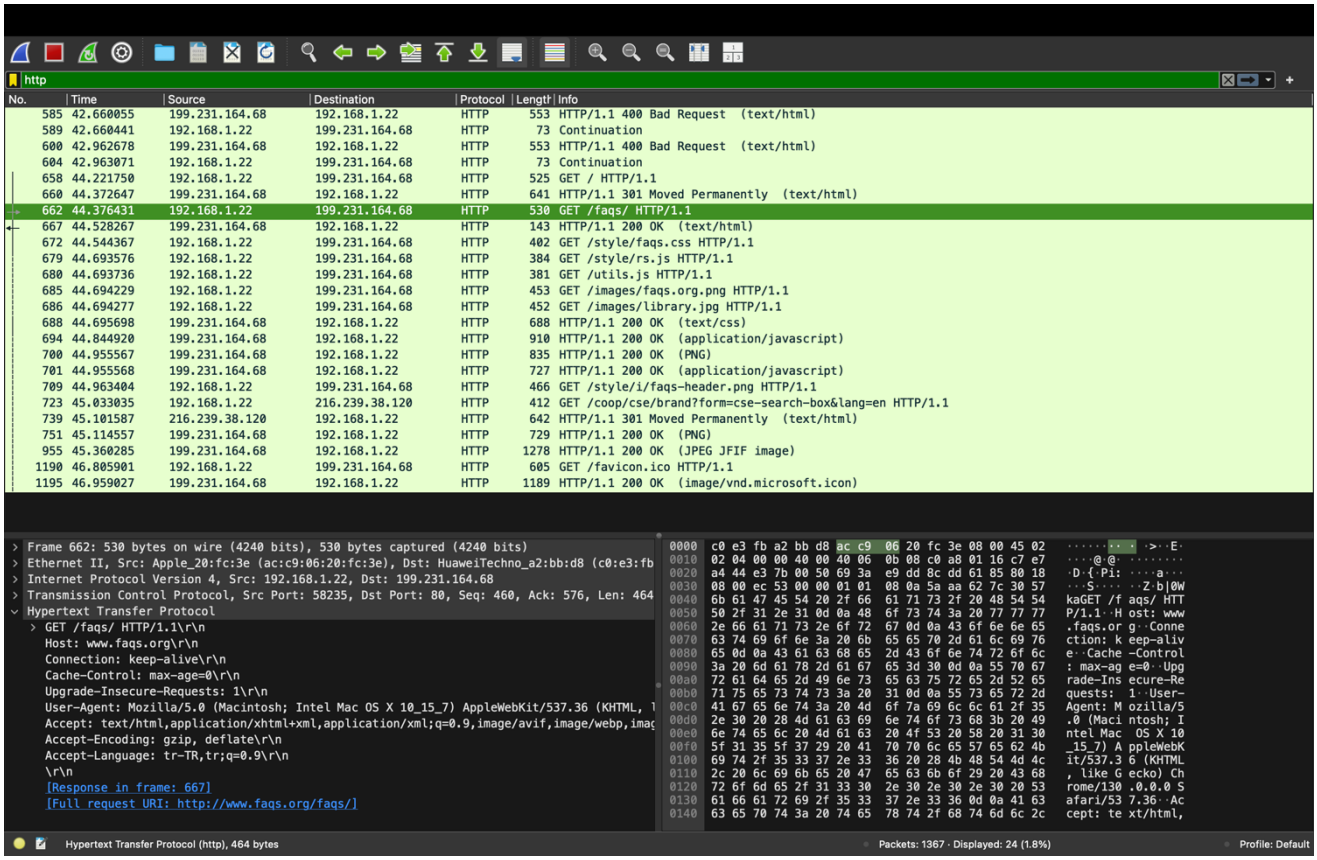
1. What is the IP address of http://www.faqs.org website? KORHAN ERDOĞDU 30838

- We should open the pcap file in Wireshark.
- We apply the filter http to display only HTTP traffic.
- We then look for an HTTP GET request to http://www.faqs.org.
- In the packet details, we locate the "Destination" field to find the IP address of www.faqs.org.

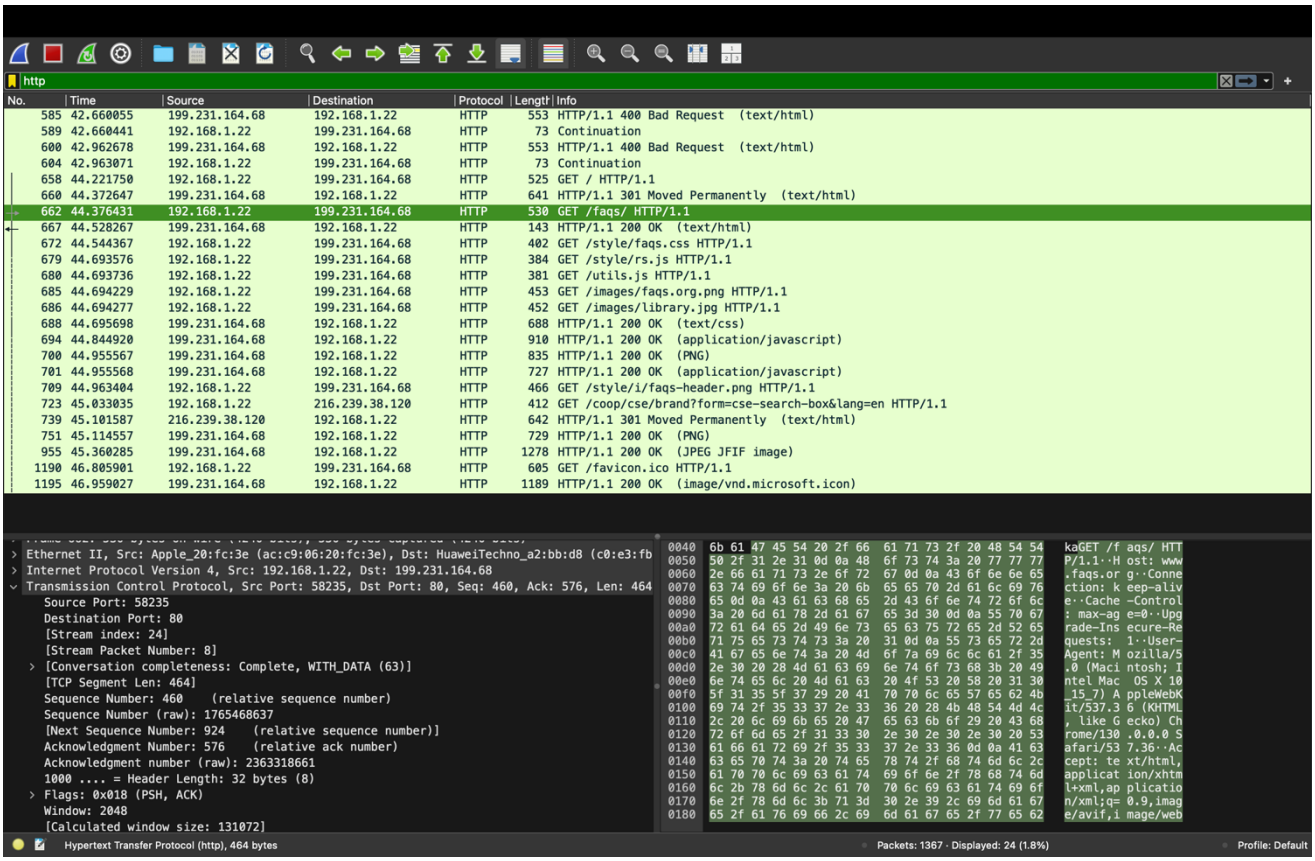
Answer: The IP address of http://www.faqs.org is 199.231.164.68



2. What are the source port and destination port numbers of the HTTP request used to get http://www.faqs.org ?

- We apply the http filter to find the HTTP GET request to http://www.faqs.org.
- In the packet details, we look for the "Source Port" and "Destination Port" fields under the TCP header.
- The destination port for HTTP traffic should be 80, and the source port will be a temporary port assigned by our browser.

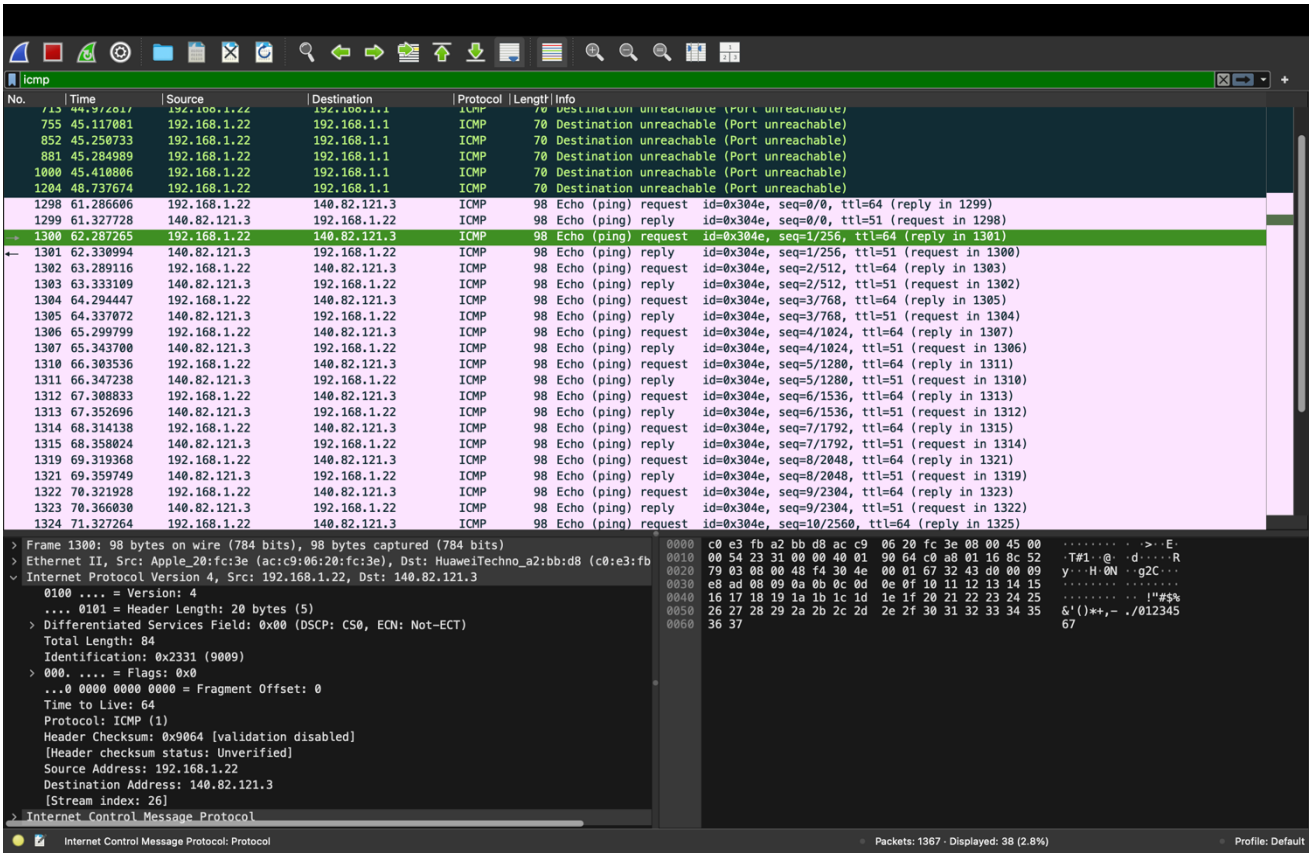
Answer: The source port is 58235 and the destination port is 80.



3. What is the IP address of github.com domain?

- We apply the icmp filter to locate the ICMP Echo Request sent to github.com when we pinged it.
- In the packet details, we find the "Destination" field in the IP header, which contains the IP address of github.com.

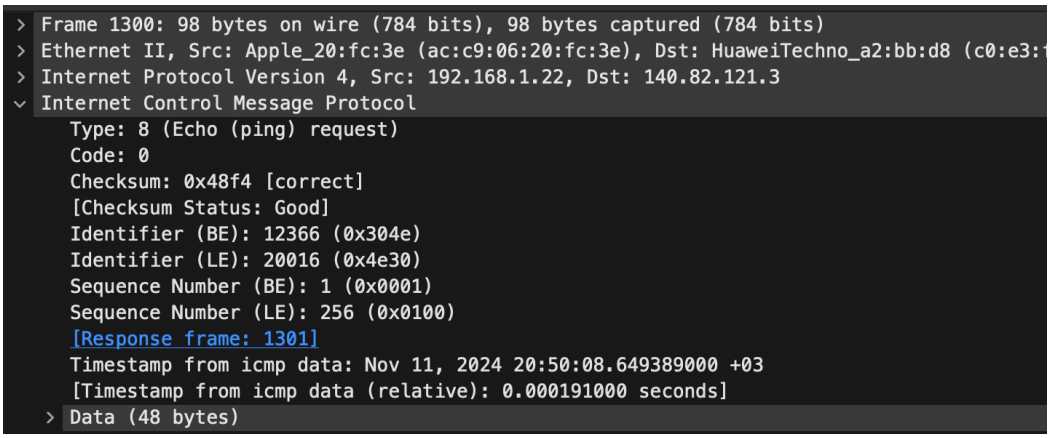
Answer: The IP address of github.com is: 140.82.121.3



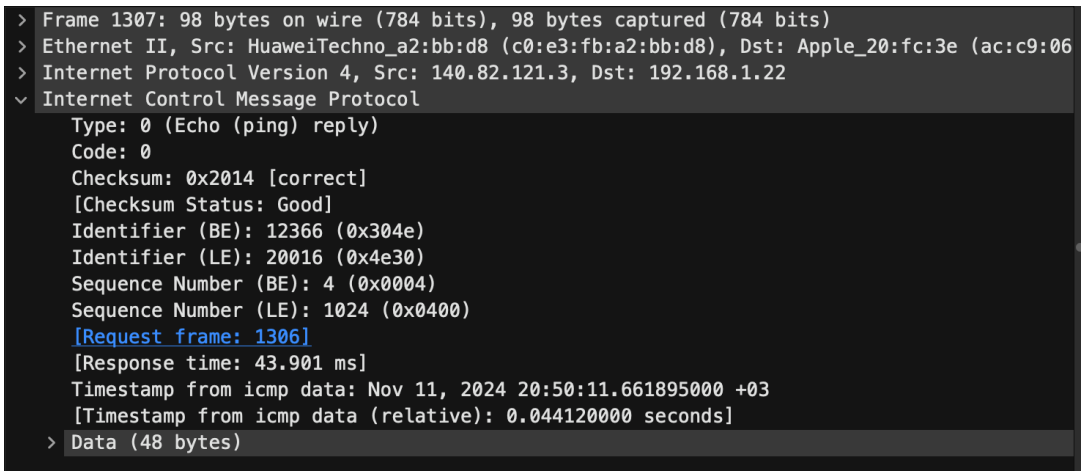
4. What are the type numbers of the ICMP Echo request and ICMP Echo reply (used for ping)?

- We use the icmp filter to display all ICMP packets.
- We select an ICMP Echo Request packet and an ICMP Echo Reply packet.
- In each packet's details, we look for the "Type" field under the ICMP header. Typically, Type 8 represents Echo Request, and Type 0 represents Echo Reply.

Echo Request:



Echo Reply:



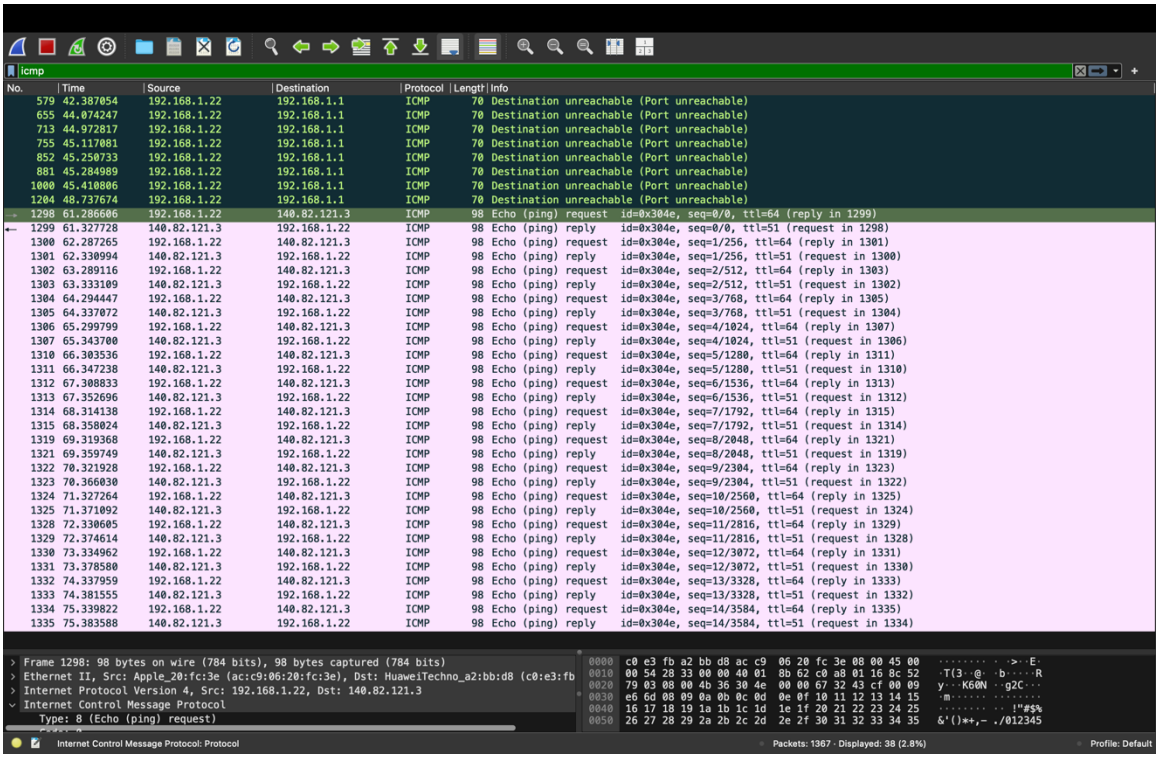
5. What is the range of sequence numbers in the ICMP Echo request and ICMP Echo reply packets captured when github.com was pinged? The range should start with the first request sent and end with the last reply received.

- We apply the icmp filter.
- We locate the first ICMP Echo Request packet sent to github.com and note its sequence number.
- Then we find the last ICMP Echo Reply received from github.com and note its sequence number.
- This gives us the range, starting with the first request's sequence number and ending with the last reply's sequence number.

We observe that the first ICMP Echo request has a sequence number of 0 (in frame 1298), and the final ICMP Echo request shown has a sequence number of 3584 (in frame 1335).

This range includes all sequence numbers from the first ICMP Echo Request to the last ICMP Echo Reply shown in the capture.

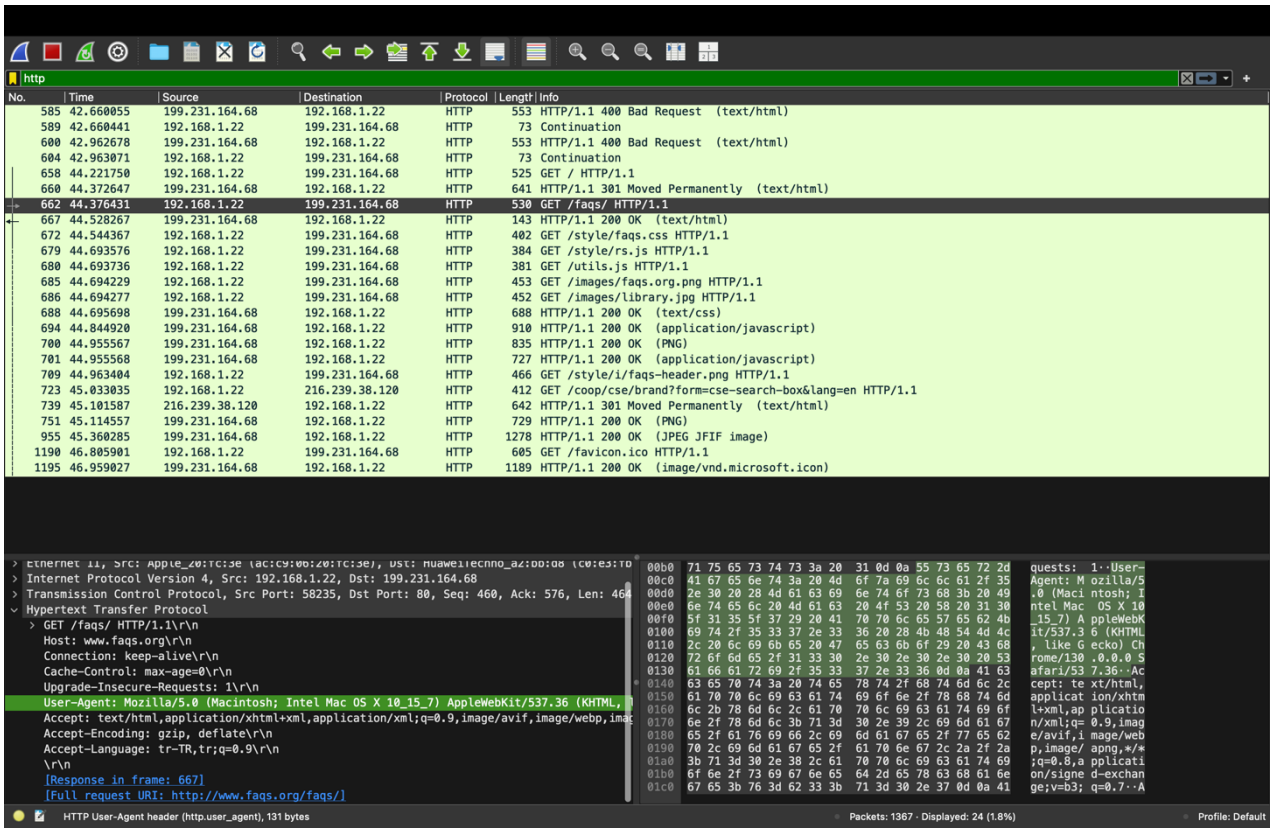
Answer: 0 to 3584.



6. What is the value of the User-Agent header field of HTTP requests sent by your browser?

- We use the http filter to locate an HTTP GET request sent by our browser.
- In the packet details, we expand the HTTP layer and look for the "User-Agent" field under "Request Header."
- This field contains our browser's User-Agent string.

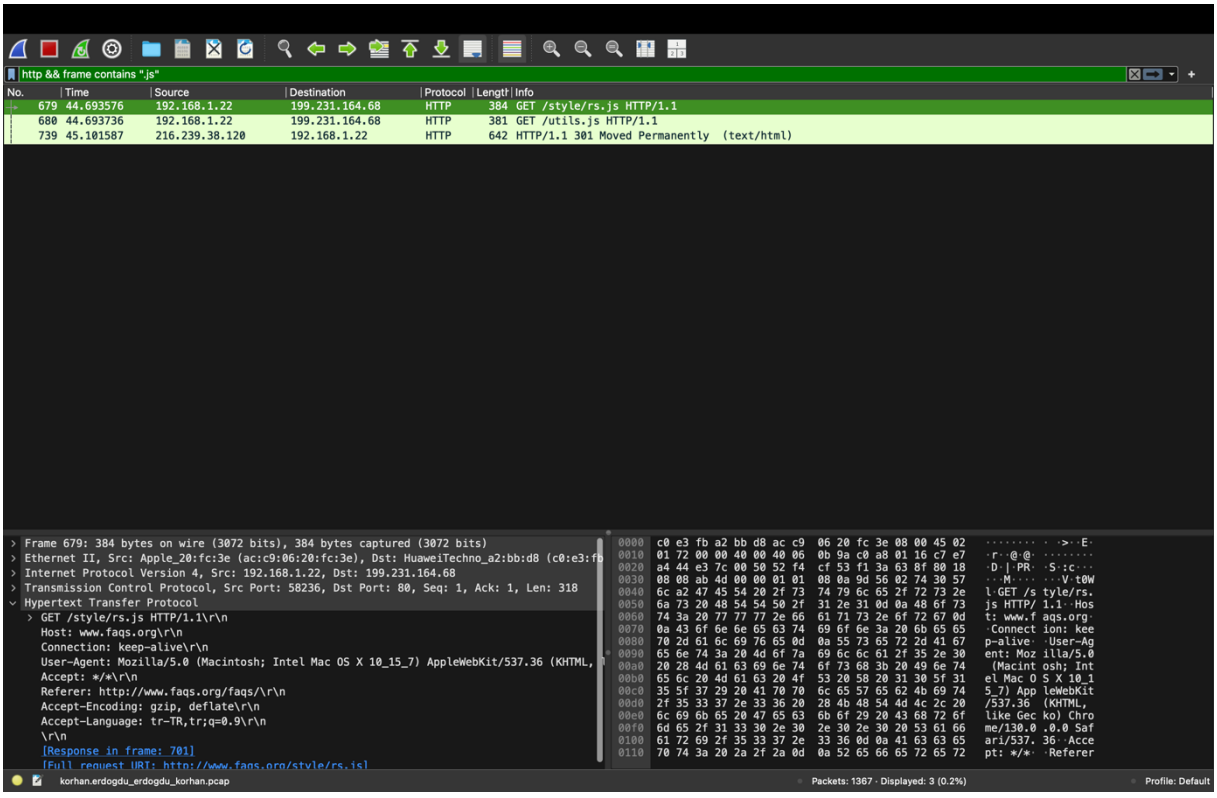
Answer: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36



7. How many .js files has/have been downloaded from http://www.faqs.org? What is/are the name(s) of these file(s)?

- We apply the http filter to locate all HTTP responses from http://www.faqs.org.
- We check the responses for entries where the "Content-Type" is "application/javascript" or the requested file has a .js extension.
- We count the number of .js files downloaded and note their names.

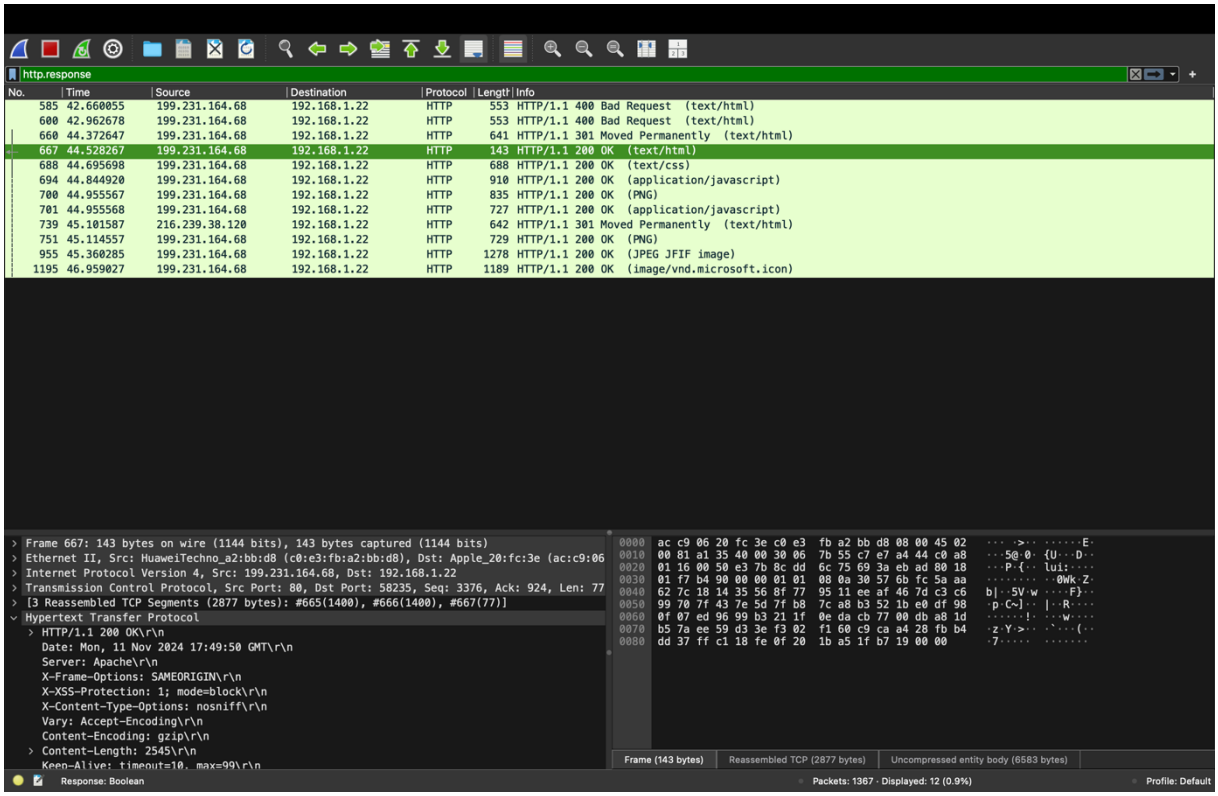
Answer: two JavaScript files, named rs.js and utils.js.



8. What is the Status Code of HTTP response for http://www.faqs.org?

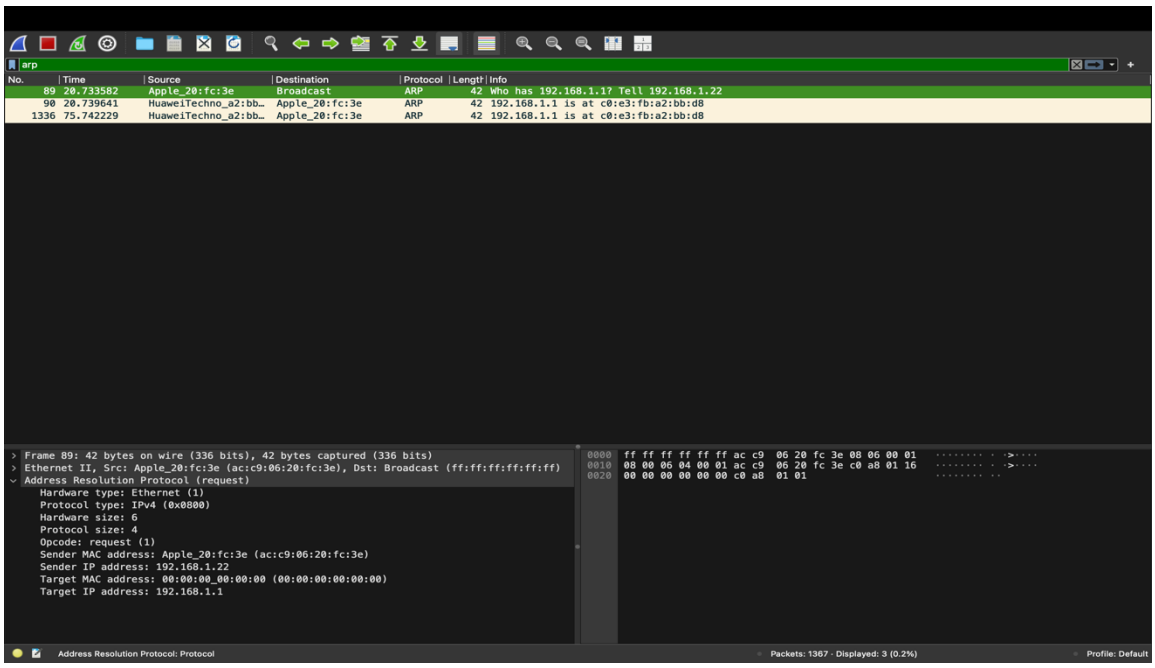
- We apply the http filter to find an HTTP response from www.faqs.org.
- In the packet details, we expand the HTTP header to locate the "Status Code" field, which shows the server's response code (e.g., 200 OK, 404 Not Found).

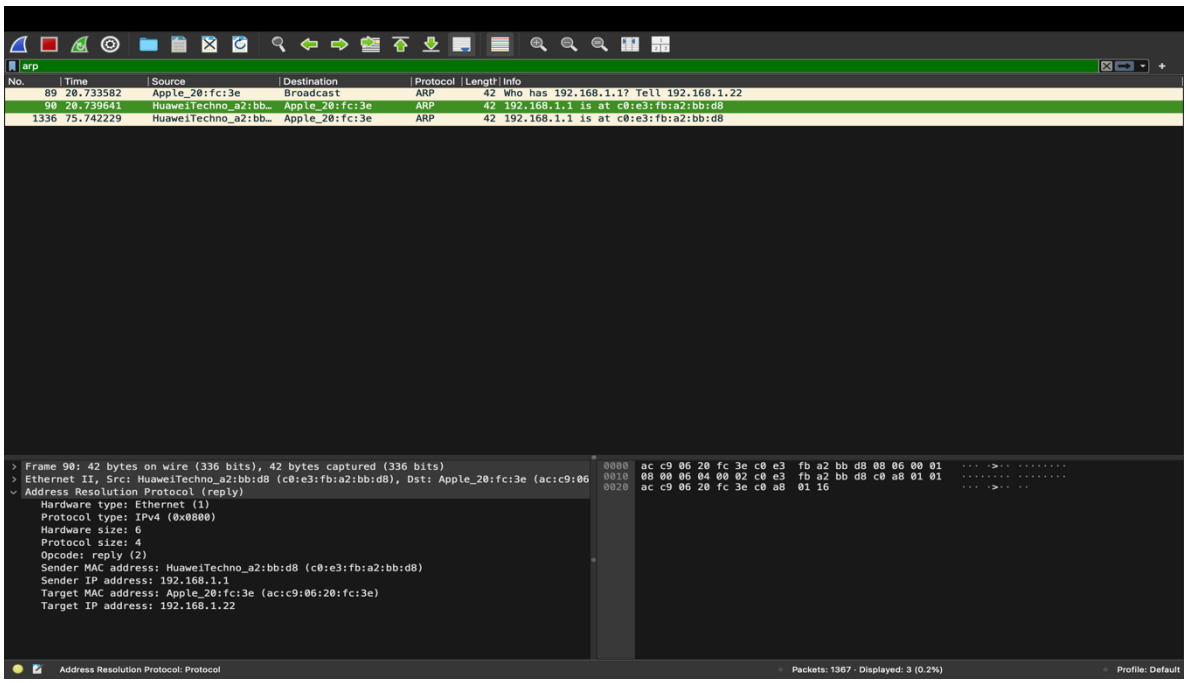
Answer: 200 OK



9. Locate an ARP request and reply pair. What are the Sender and Target MAC addresses, and Sender and Target IP addresses in the ARP request and reply packets?

- We use the arp filter to locate an ARP request packet.
- In the packet details, we note the Sender and Target MAC and IP addresses.
- Then we find the corresponding ARP reply packet, which contains the same addresses in reverse roles.





10. Write a Wireshark filter for showing packets where your IP address is the source and UDP is used. What is the application layer protocol that appears the most when you apply this filter?

- After applying the filter, we look at the Info column to observe the application layer protocol for each packet.
- We identify the most frequently appearing application layer protocol, which is likely to be DNS or another UDP-based protocol.