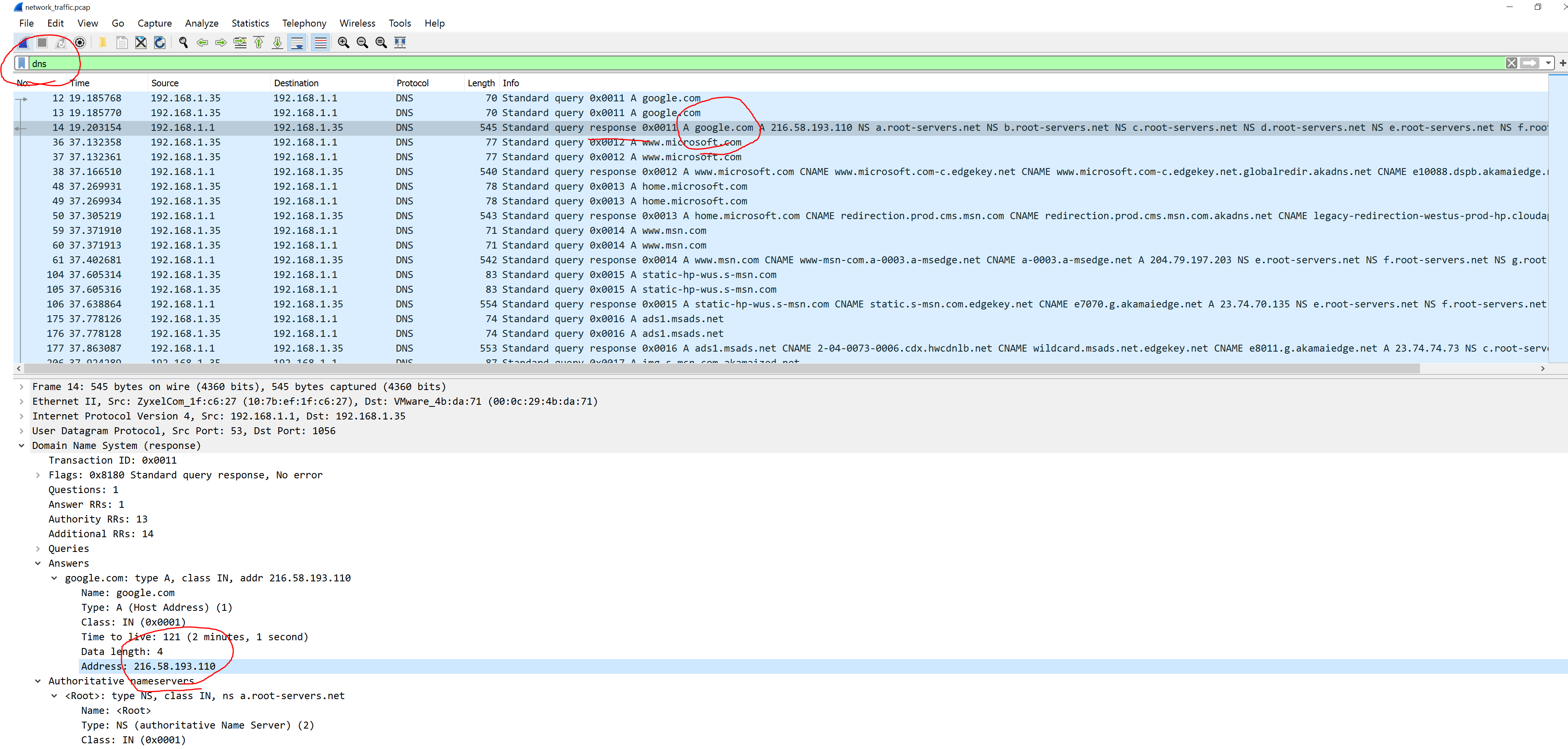
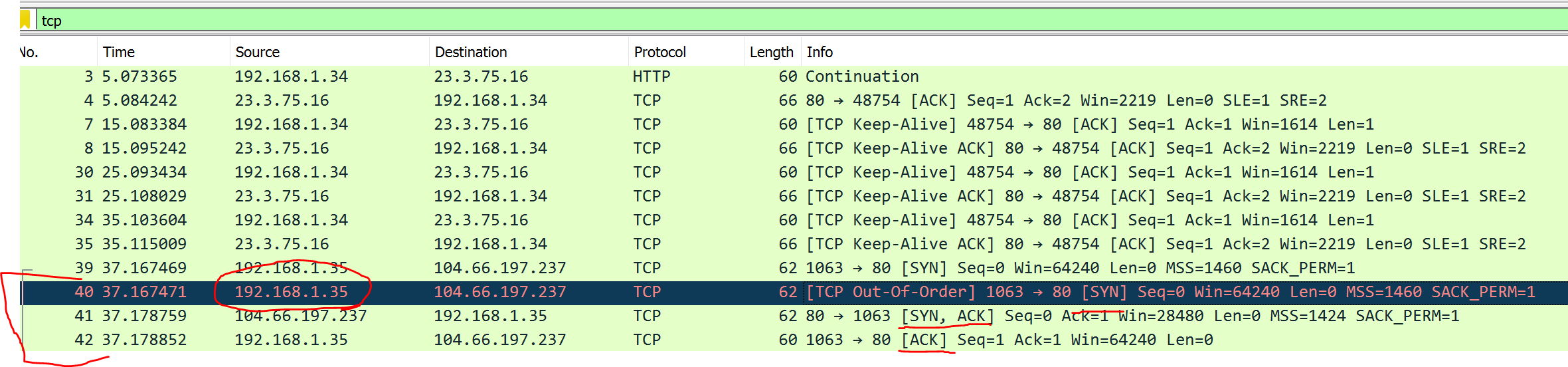
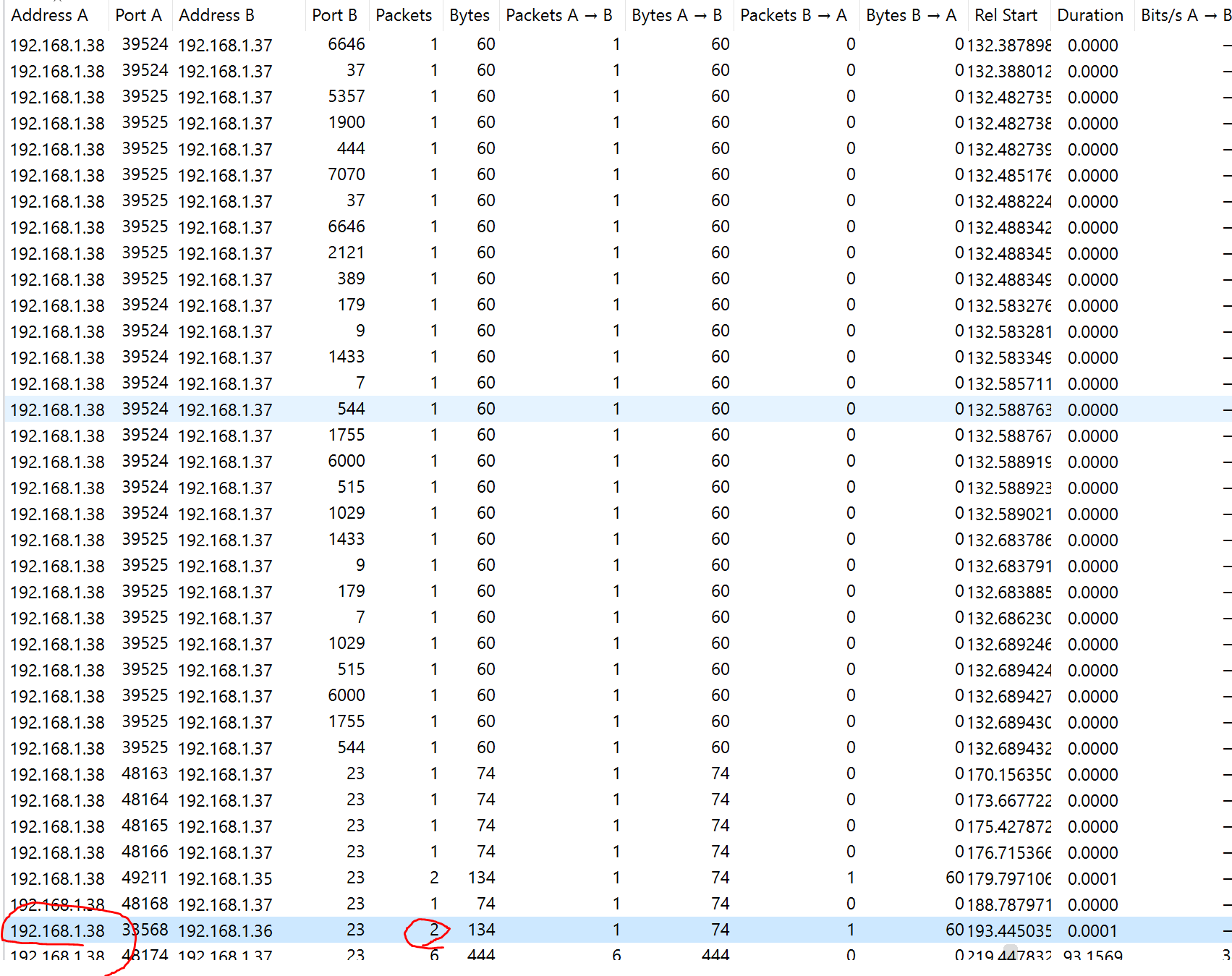
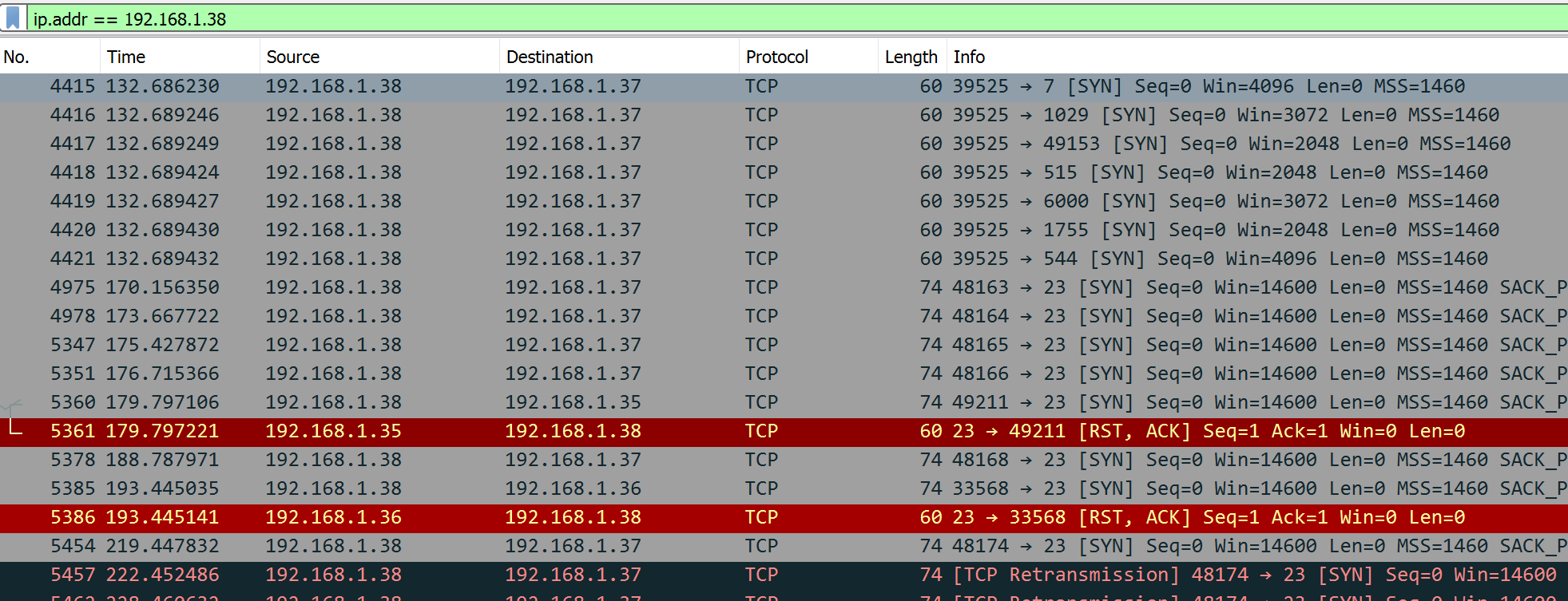
1. A computer making a DNS query and receiving an answer.  
- Which domain name was requested in the DNS query? **Several were returned, but the first one was google.com**  
- Which IP was returned in the DNS answer? **216.58.193.110**



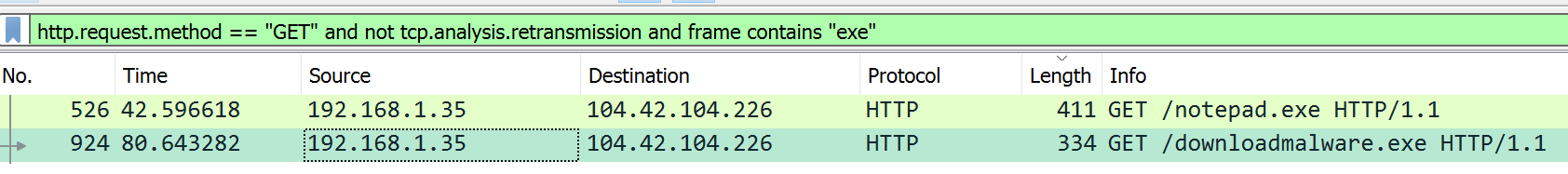
2. A TCP connection being made (3-way handshake)  
- Submit a screenshot of the 3-way handshake traffic **OK (below)**  
- Which IP address initiated the connection? **192.168.1.35**



3. A user running a port scan against another machine.  
- Which IP is running the port scan? **192.168.1.38**  
- Which IP is being targeted by the port scan? **198.168.1.37**  
- How did you identify the traffic as being port scan related? **I read this:** [**https://www.koenig-solutions.com/documents/PenTestExtra-06-2013.pdf**](https://www.koenig-solutions.com/documents/PenTestExtra-06-2013.pdf) **and checked the statistics section for small sets of packets (1 or 2) being sent to many different ports and also looked through to see a lot of SYN packets** **sent without responses (see below)**  
- Which port scan technique was used? **It appears that TCP SYN (stealth scan) was used.**



4. A victim downloading a malicious .EXE file from the web.   
- What is the name of the .EXE file? **downloadmalware.exe**  
- Which IP was it downloaded from? **The user (192.168.1.35) downloaded ‘downloadmaleware.exe’ from 104.42.104.226**



5. A Cross Site Scripting (XSS) attack.  
- We have not covered Cross Site Scripting in the course yet. You may read ahead here to learn what a basic XSS attack looks like: [https://www.owasp.org/index.php/Cross-site\_Scripting\_%28XSS%29 (Links to an external site.)](https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29) - Since XSS is a web based attack, which protocol will you be interested in filtering for in Wireshark? **I’d want to look at HTTP traffic.**  
- Submit a screenshot of the identified XSS traffic in Wireshark. **I don’t think this is the actual XSS attack, just a transmission that happens to be named XSS. I tried searching for ‘document’ and ‘<script>’ and ‘script’ but didn’t find anything useful. This was the closest thing I could find…**

