

1. Go to <https://www.cloudshark.org/captures/00089db884f6>. Once in, go to Analysis Tools and GeoIP World Map. Where are the endpoints?
2. Open the file in Wireshark. In DNS, a time to live (TTL) value specifies how long a resolver is supposed to cache the DNS query before the query expires. In frame 2, what is the IP address of ojsp.verisign.net, and what is the time to live for teach DNS response?
3. In frame 2, what is the source port?
4. A user agent in an HTTP header indicates the browser. Go to frame 7, right click, and follow the stream. What is the user agent?
5. Go to <https://www.cloudshark.org/captures/c109b95db0af> and open in Wireshark. Are DHCP messages sent via UDP or TCP?
6. Expand the Bootstrap Protocol (Discover) header. What is the Client IP address?
7. Look at the Parameter Request List. What requests are listed?
8. What is the value of the Transaction ID in all four packets?
9. Go to <https://www.cloudshark.org/captures/abdc8742488f>. Go to Analysis Tools and follow the stream. Did the FTP server require a password?
10. Did the client download any files?