Live Data Capture

Andrew Maddox

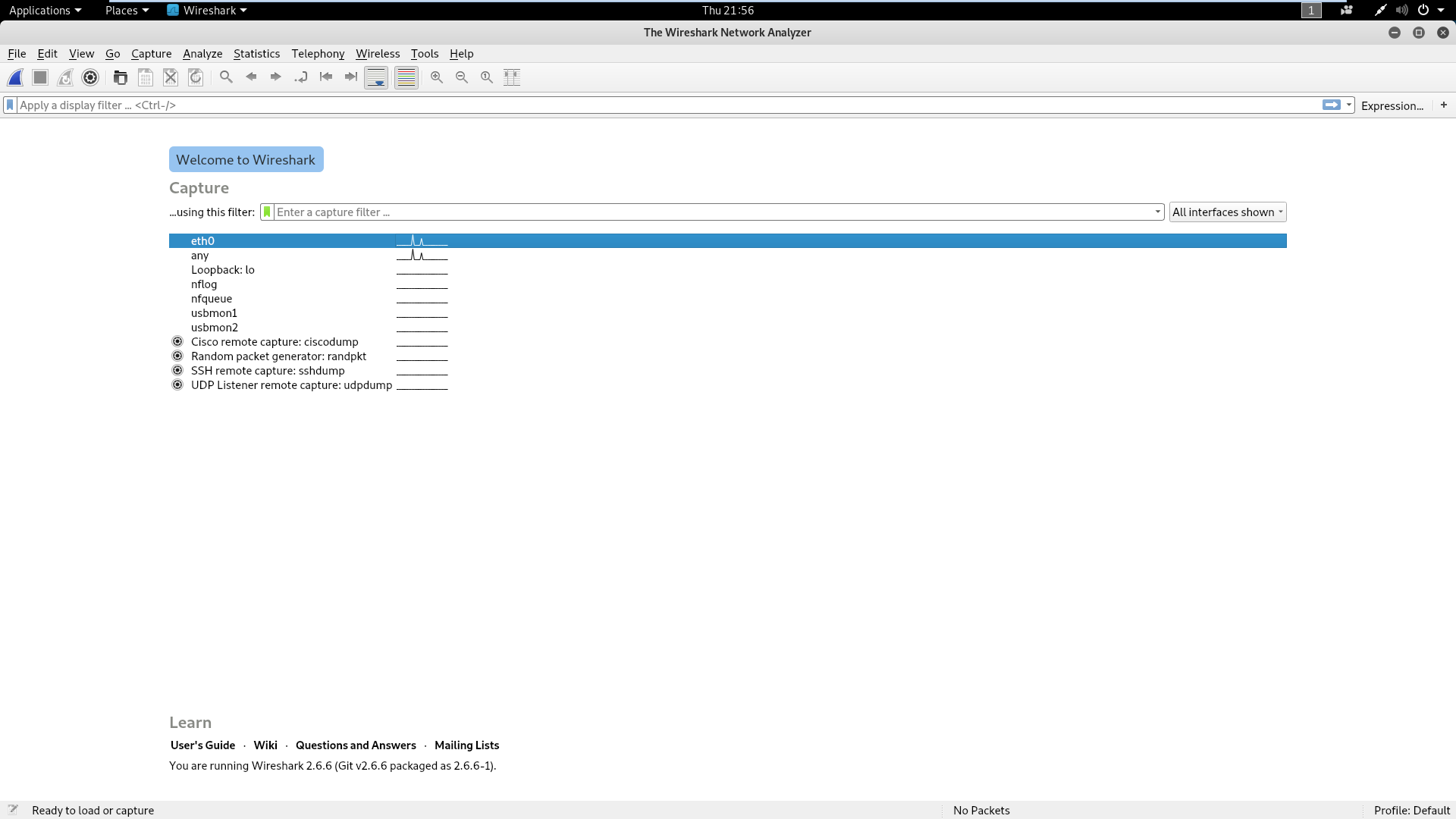
University of Advancing Technology

Author Note

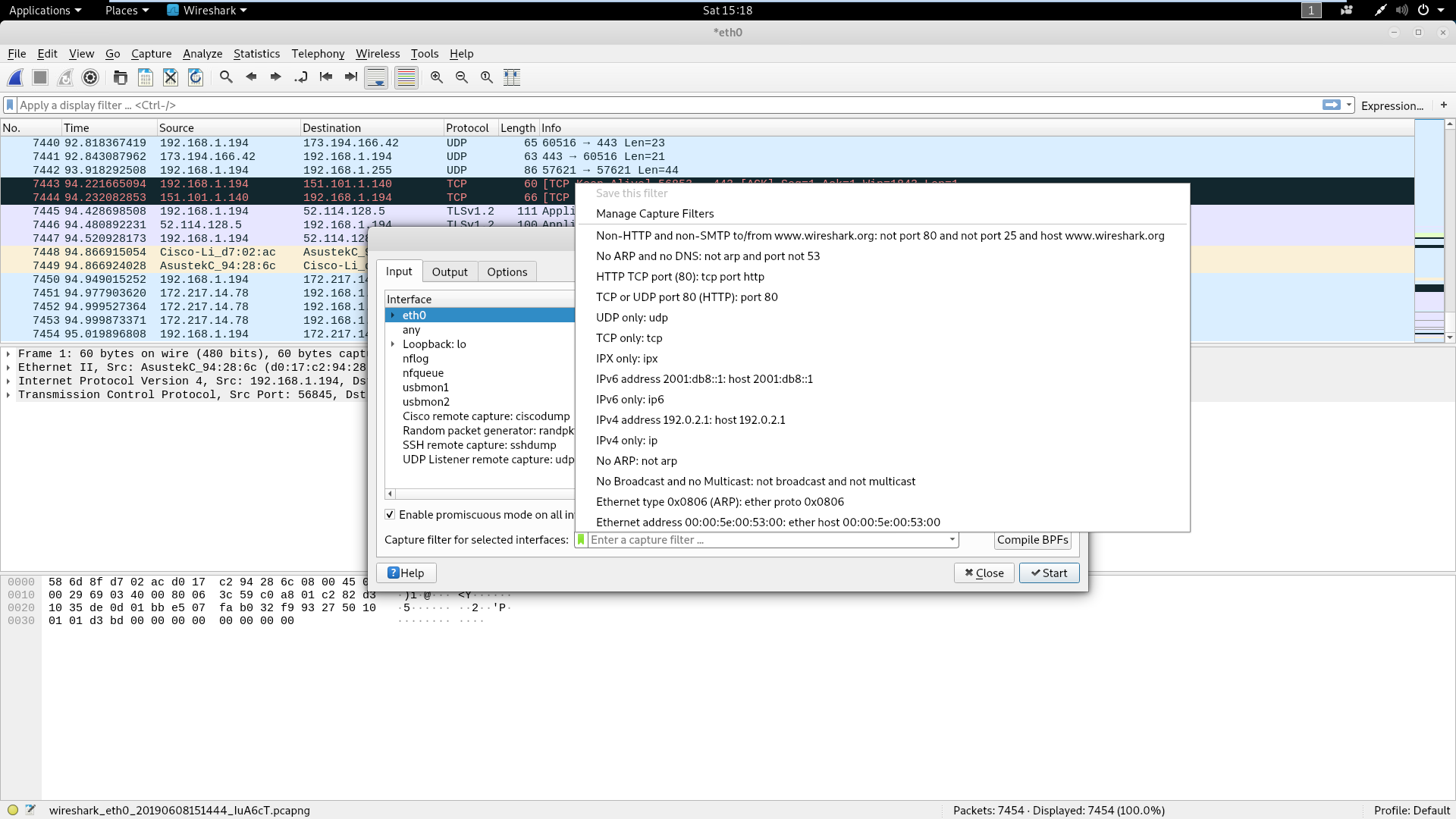
This paper was prepared for NTS405, taught by Aaron Jones.

Live Data Capture

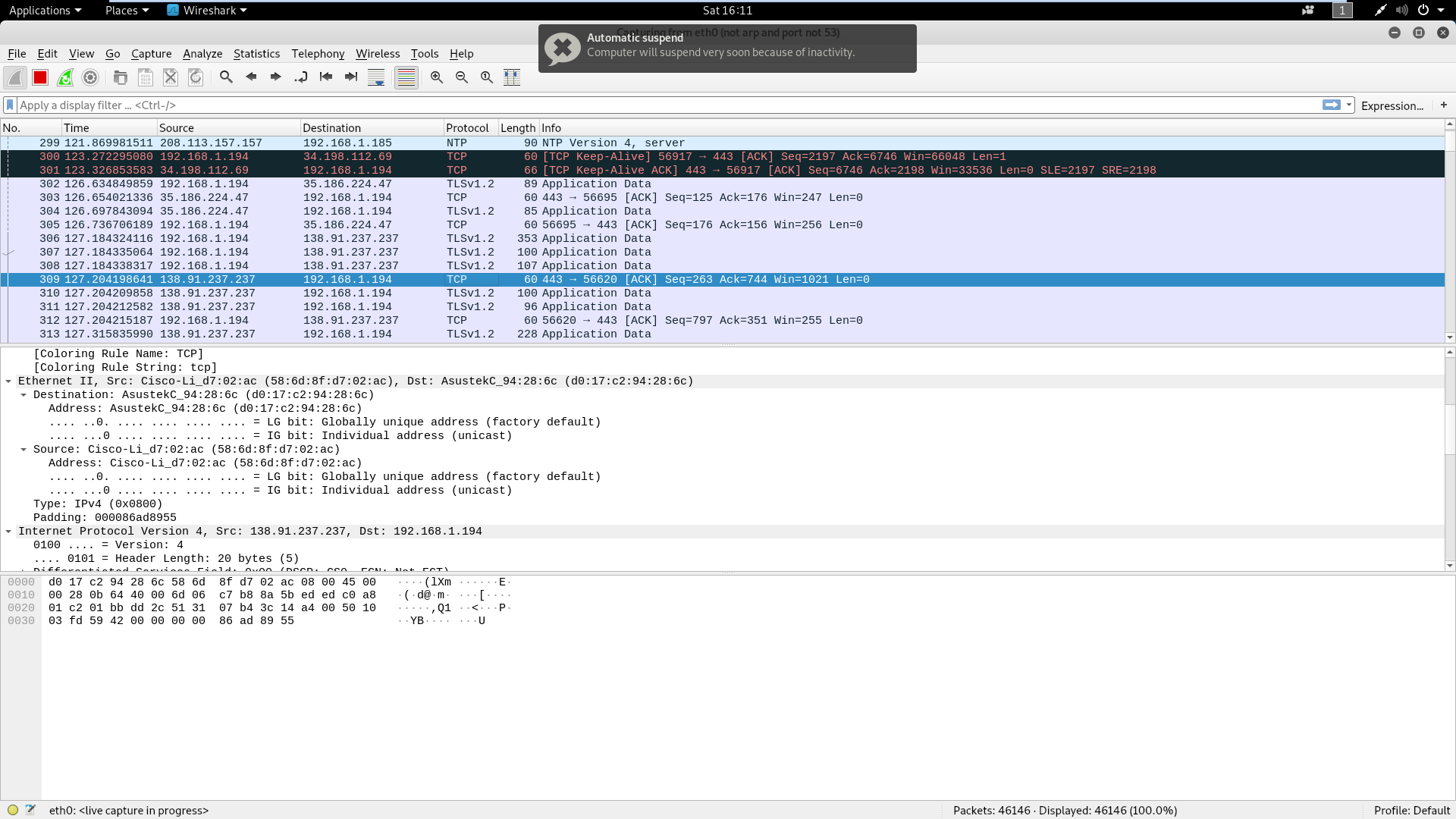
This is the layout for the Network Interfaces and the specific one on this virtual machine is the eth0 as the virtual machine is set to emulate an Ethernet connection. As seen the Ethernet is receiving data and can be selected. This could also be applied in different scenarios but is set to monitor traffic on this specific device. The device being used is Kali Linux 2019.1



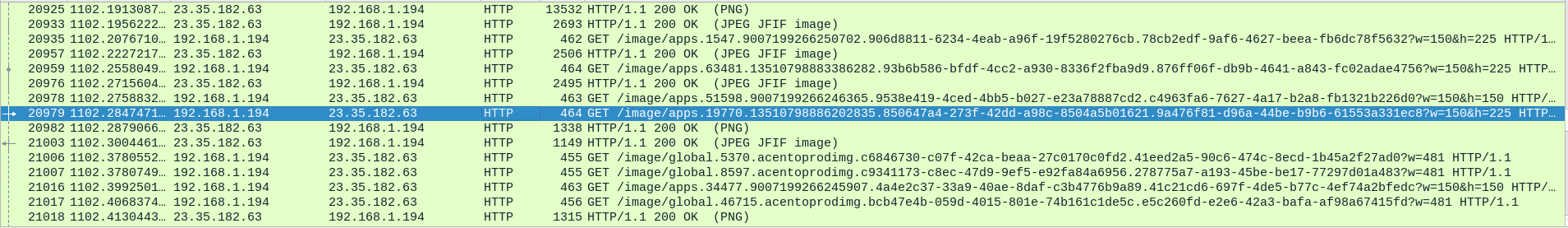
This is an example of the capture options specifically the no ARP and no DNS option. This picture also shows feed from tracking network activity through Wireshark.

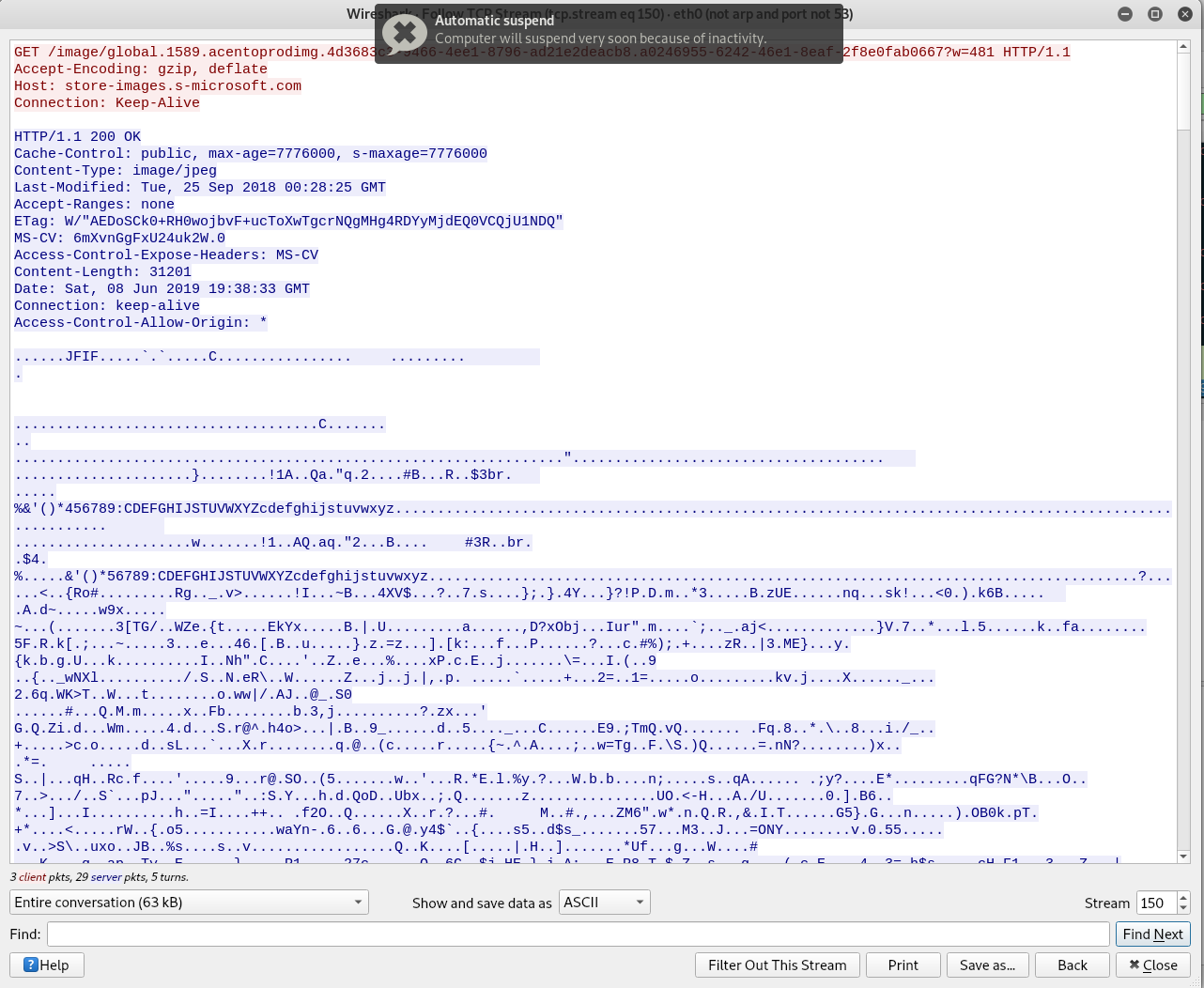


This is an example of a TCP packet. This has no filter applied and is followed with information involving the packet and the devices receiving the packet.

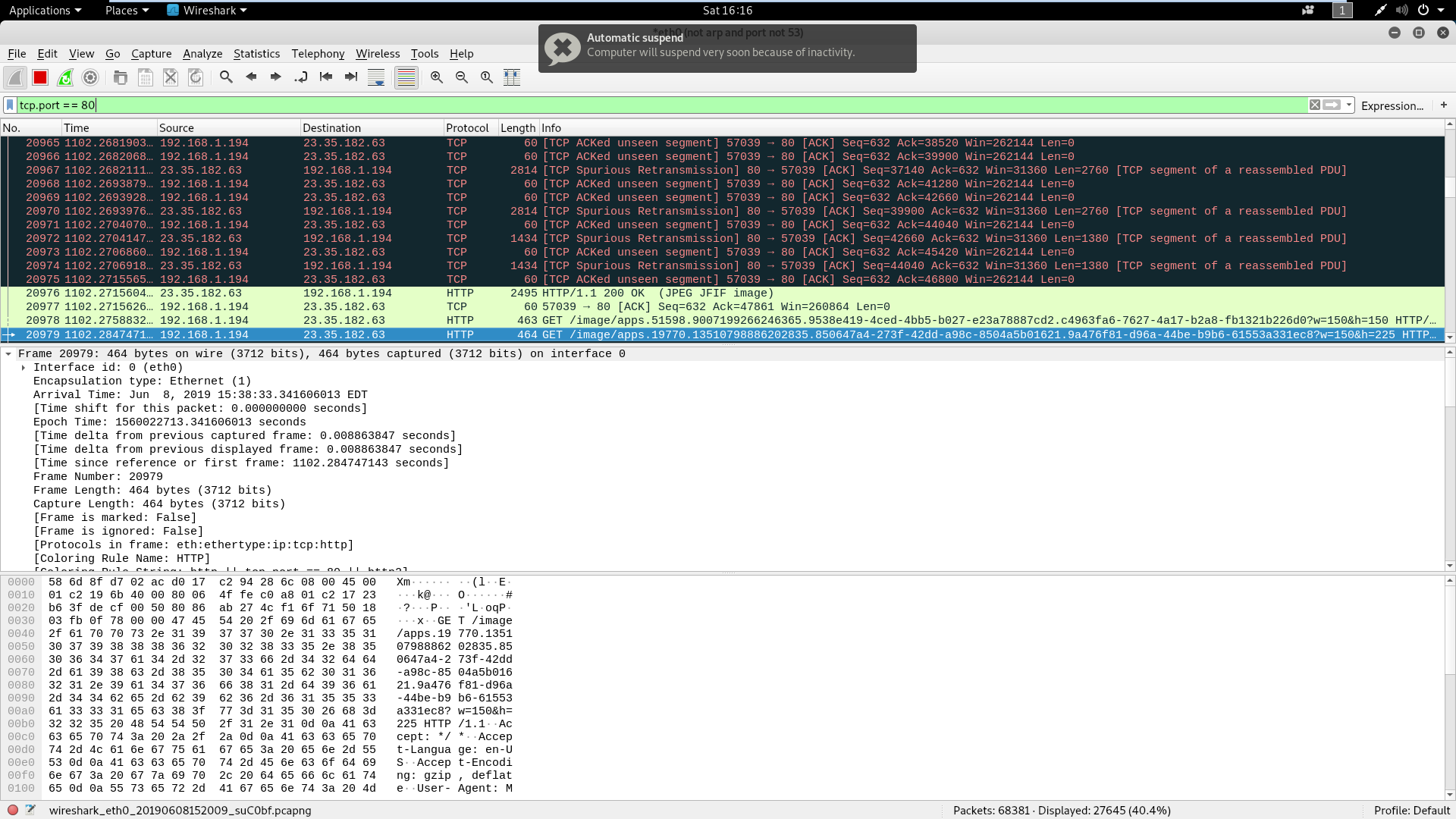


This is an example of HTTP requests along with examples of GET with the requests. These were found by applying an HTTP filter for easier access. There are other areas these interesting things will apply if you have experience working with Burpsuite or other tools some of the information applies including GET requests.

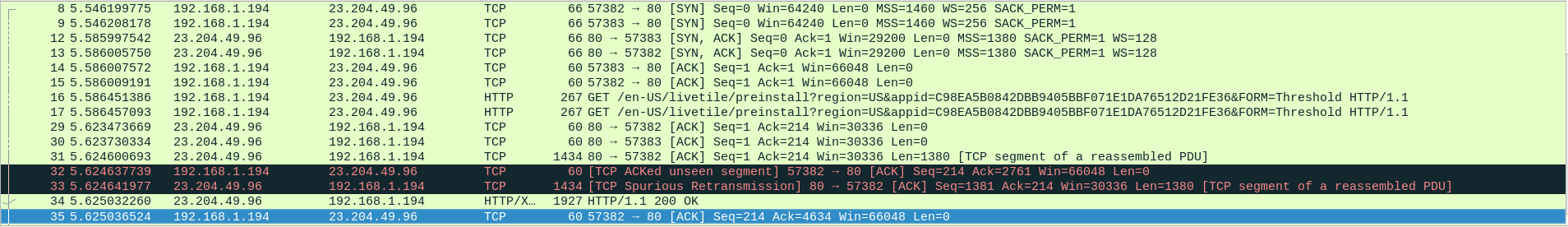


This is a picture of the TCP stream window along with what seems to be encoded information about the HTTP request.

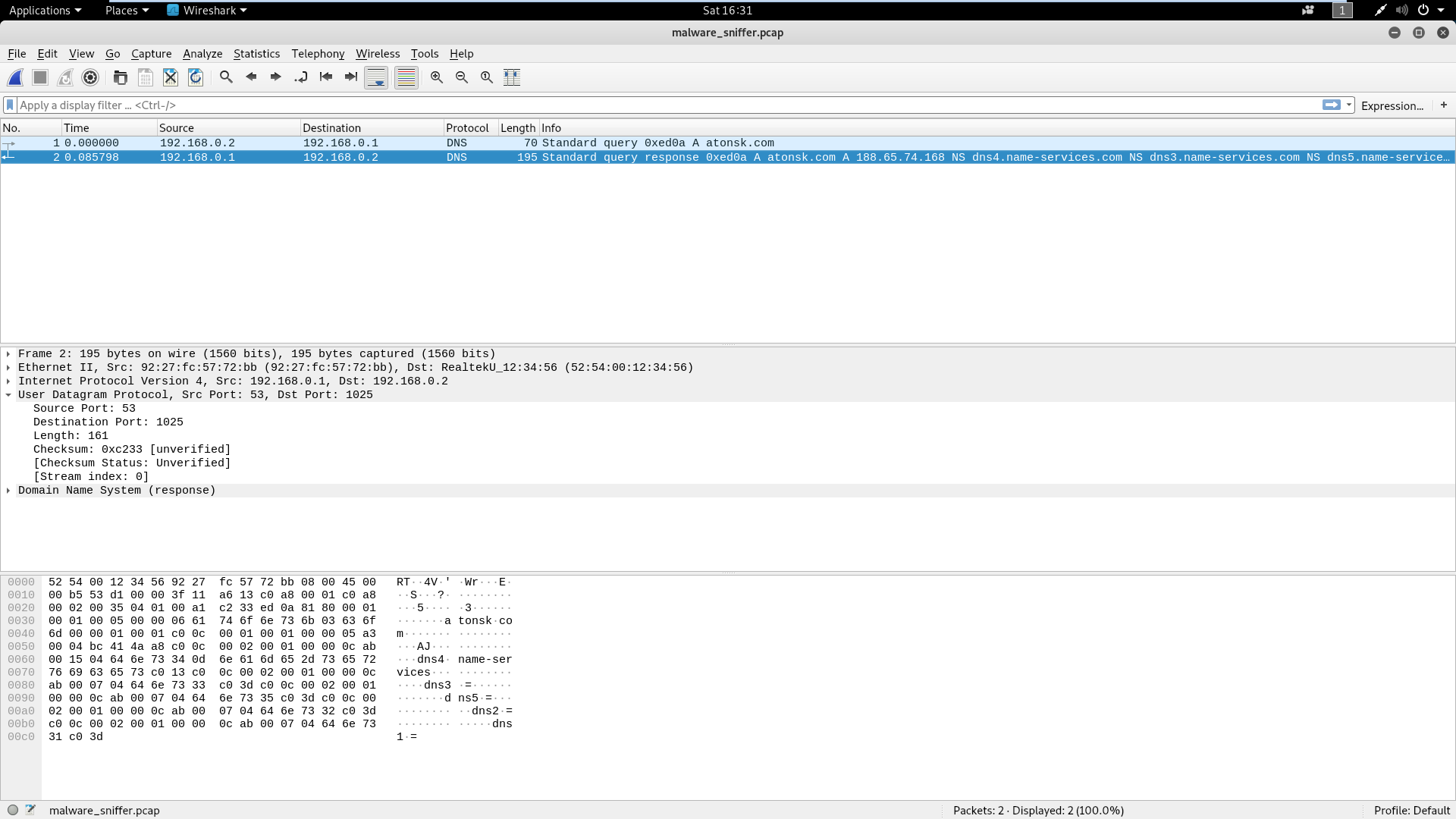
In this picture you can see that the TCP port 80 visual filter is applied for narrowing down results. The reason this cannot be observed in the current traffic is because it is a visual of previous traffic prior to the applying of the filter.



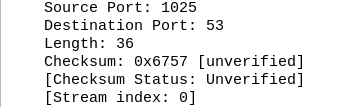
Here is an example after the filter is applied.



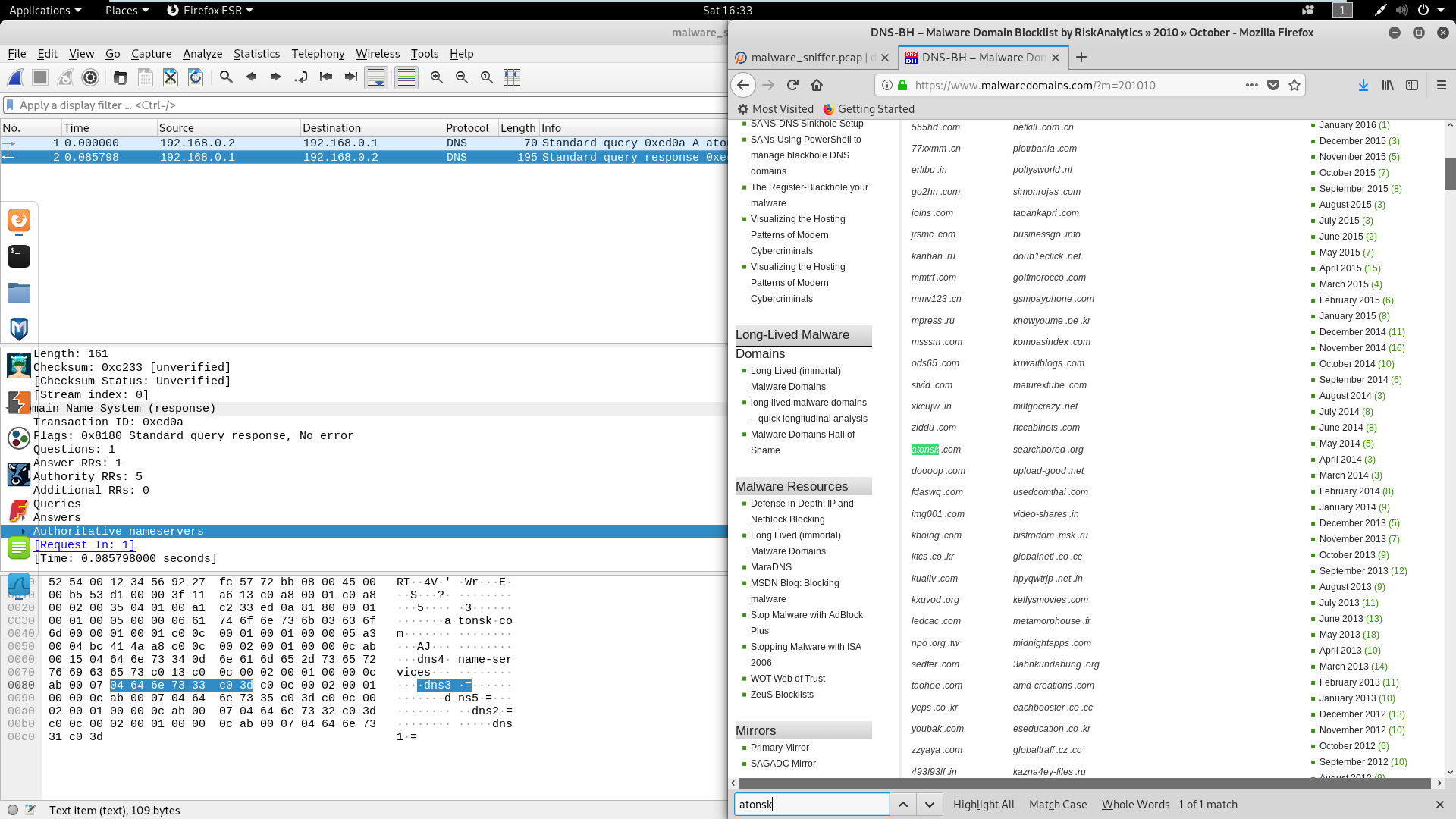
Here is the example of a malware sniffer pcap file. There are two DNS packets I will be looking over in this.



Something I found notable was that the checksum were unverified.



Another largely notable thing was after proceeding to do research on associated content linked with the packets I got multiple online responses that it is a known malware. This is not as notable as I already know it is an example of malware but for an individual who does not know that it would be beneficial to know that the domain is associated with known malware.



Some of the information is used from an assignment in NTS330 over sniffing a network.