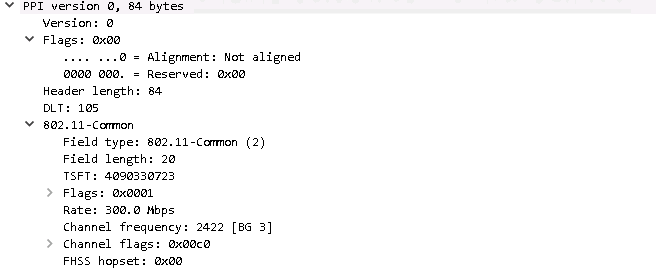
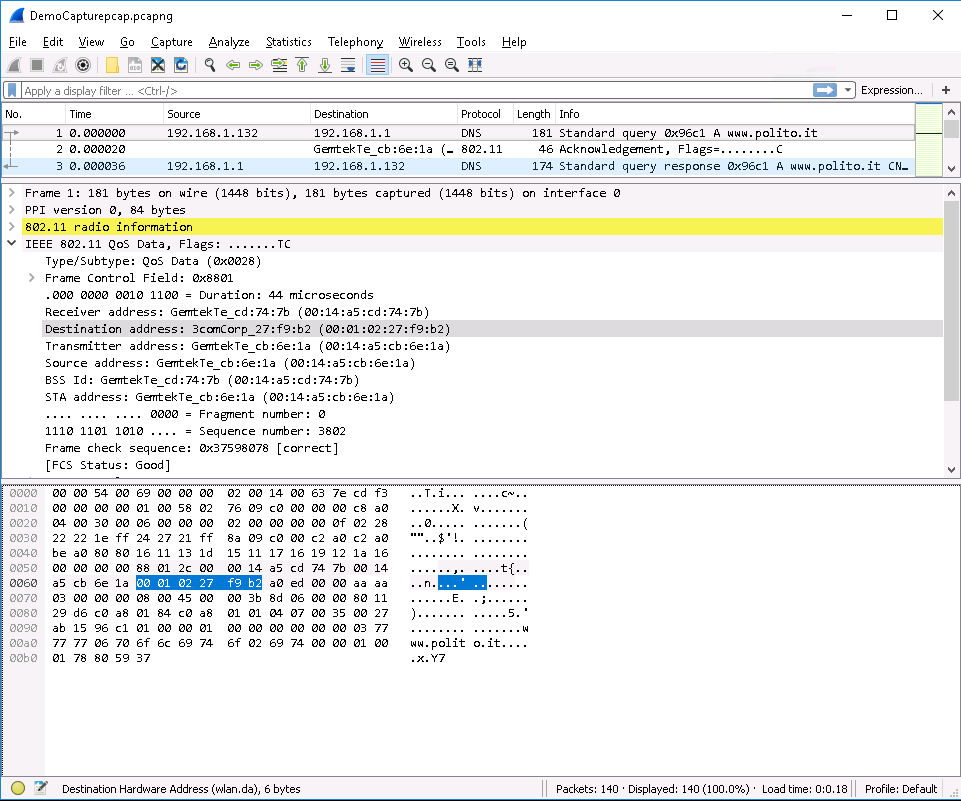
William Chen IST 323 – M002

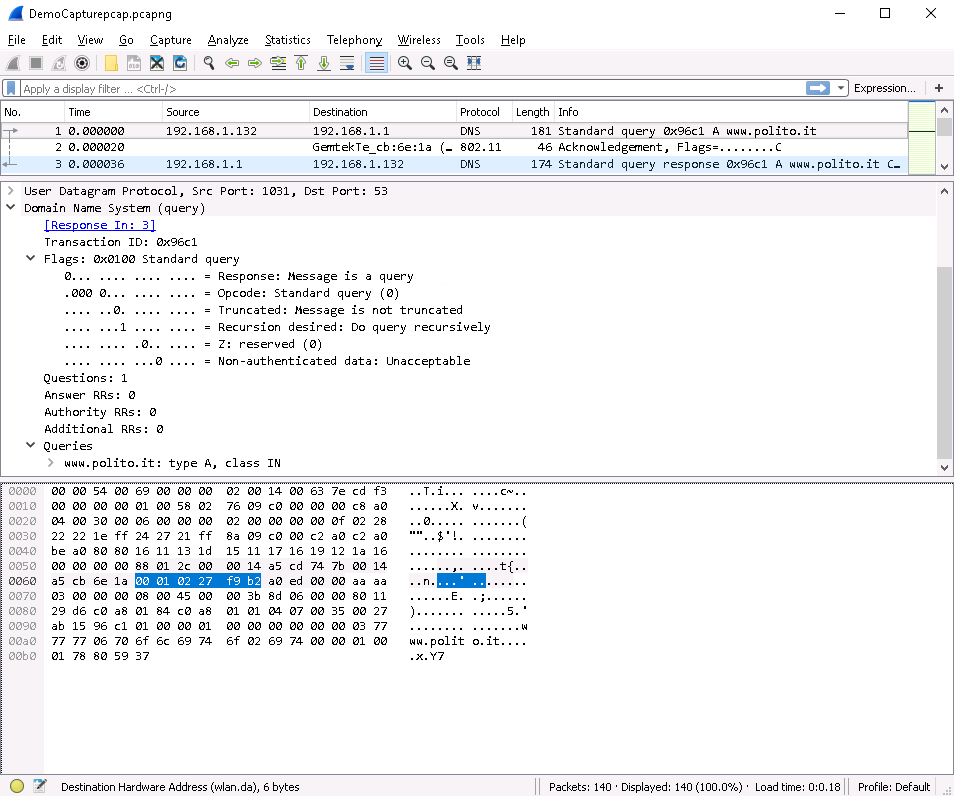
Professor Christopher Croad 11/19/2020

Bonus Lab – Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

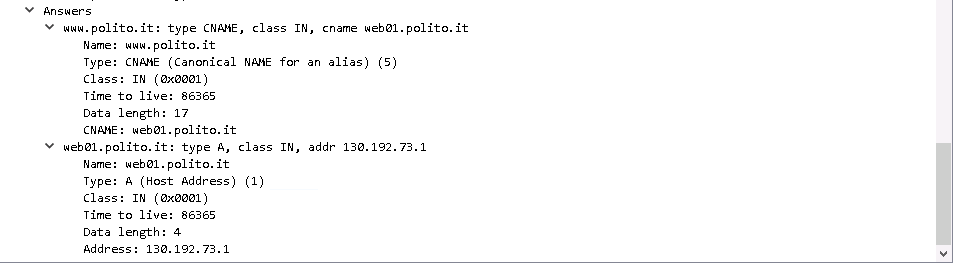
1. **Part 1, #10: Frame Details, Flags and 802.11-Common line**



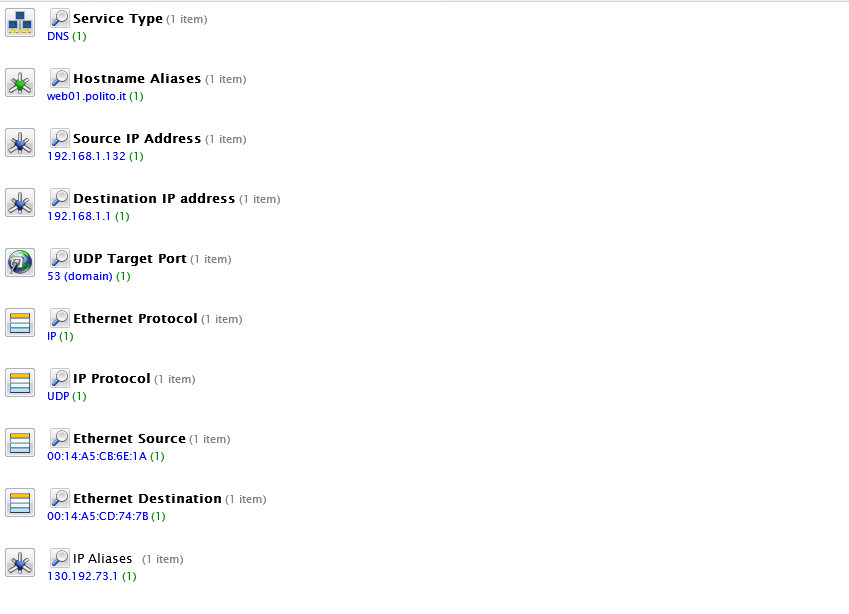
1. **Part 1, #12: Destination address: 3Com\_27:f9:b2 (00:01:02:27:f9:b2)**
2. **Part 1, #14: Queries line,** [**www.polito.it**](http://www.polito.it) **website**



1. **Part 1, #20: Answers heading in Frame 3**



1. **Part 2, #10: DNS query on NetWitness**



1. **Part 2, #11: Compare NetWitness to Wireshark**

I think Wireshark goes a little more in-depth compared to NetWitness. For example, Wireshark shows how long it takes to go live and the data length. Whereas NetWitness shows most of the things Wireshark already indicates. It has the hostname aliases and IP aliases. NetWitness also shows the protocols being used (IP and UDP), the source and destination IP, and the ethernet source and destination. Wireshark also has the class type (IN) and the type (CNAME and A). Wireshark also shows the site that someone was trying to access (polito.it). I think NetWitness focuses on the host more than Wireshark, where they focus a little bit on the host and the page itself.

1. **Part 2, #13: Compare Ethernet source and destination**

NetWitness has the IP address rather than the hexadecimal address. For example, the destination address on Wireshark is 3comCorp\_27:f9:b2 and the destination addresses on NetWitness are 192.168.1.255, 192.168.1.1, and 130.192.73.1. NetWitness goes more into depth with showing the hostname aliases, what content it is, how that content is being accessed (action event), the destination country and city, organization, and what kind of protocol is being used for both ethernet and IP, and IP alias. Wireshark shows mostly hexadecimal values. As mentioned earlier, NetWitness focuses more on the host details and gives you more understandable information compared to Wireshark. It is easier to read and understand the details on NetWitness than Wireshark.

1. **Part 3: Challenge Question**

If you wanted to access someone else’s packets, you’d have to log into the same Wi-Fi as the person you are trying to sniff. Sifting through the packet capture can also take a long time because of the large number of files it captures. Another limitation for Wireshark is that you can only gather information from the network, and it won’t show anything you send. While you can track the packets in real-time, Wireshark won’t notify you of an intrusion on the network. You also can’t save a packet as an editable file. One might want to edit a packet to share a trace file with a vendor but can’t because the packets contain sensitive information.