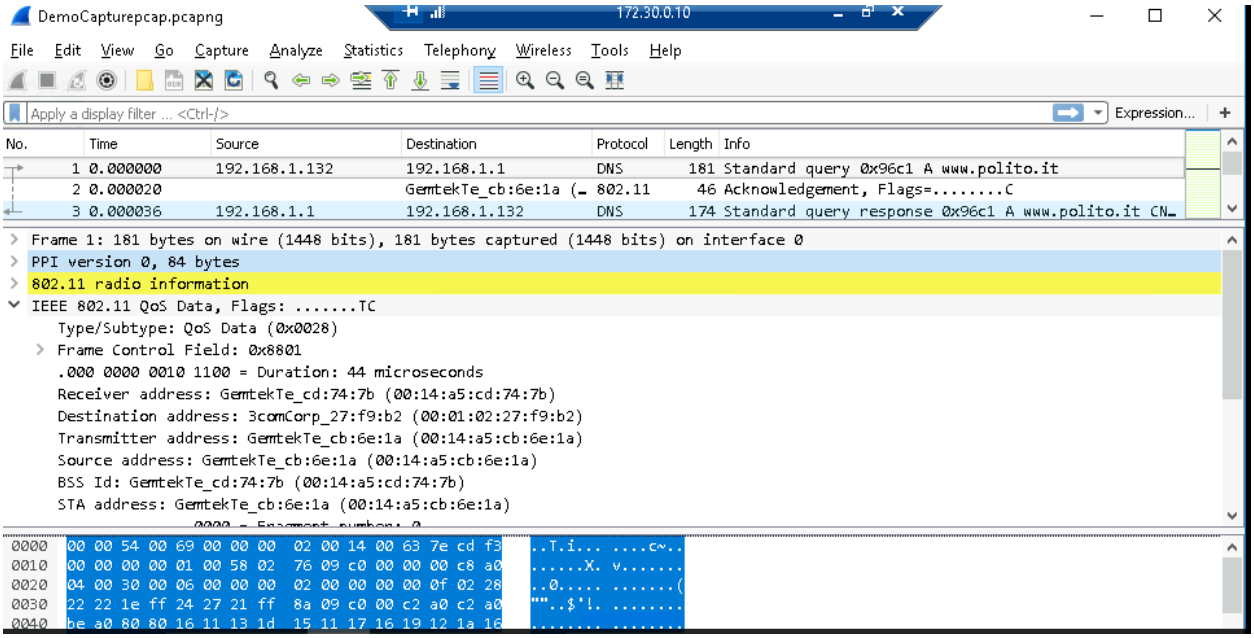
Marriah Lewis

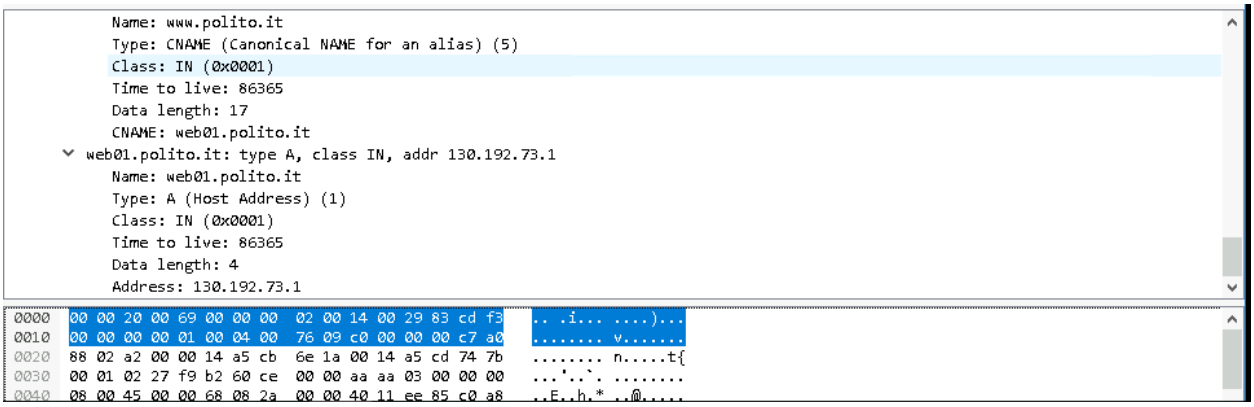
Lab Report #3: Network Security, Firewalls, and VPNs

Section 1 Part 1:

IEEE 802.11 QoS Data fields

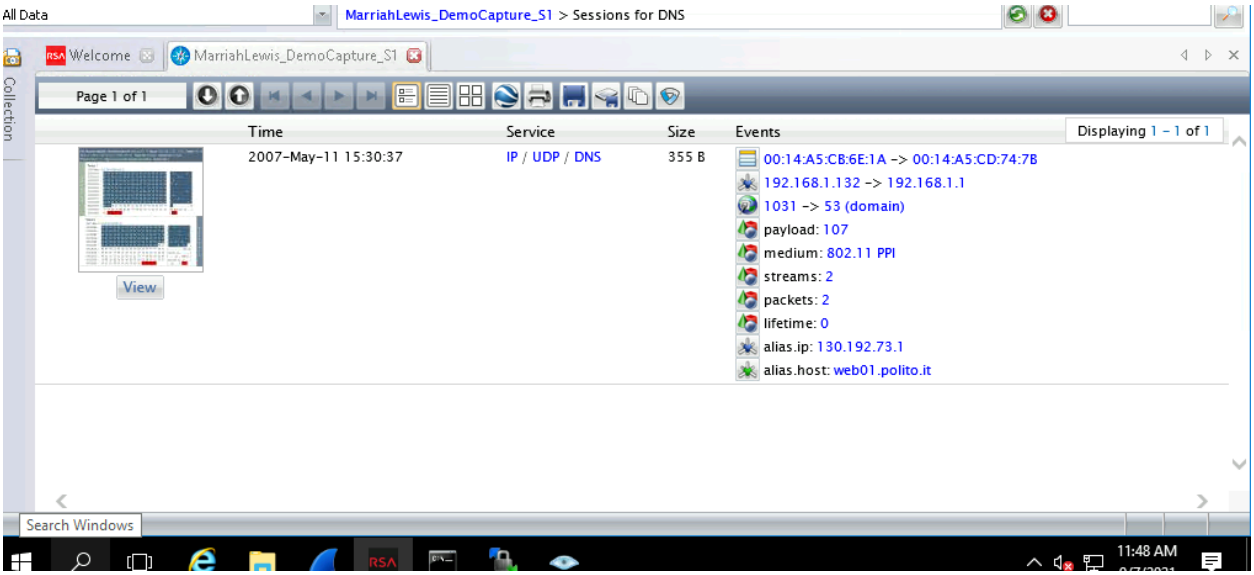


Query name (www.polito.it) The source IP address, and the destination IP address

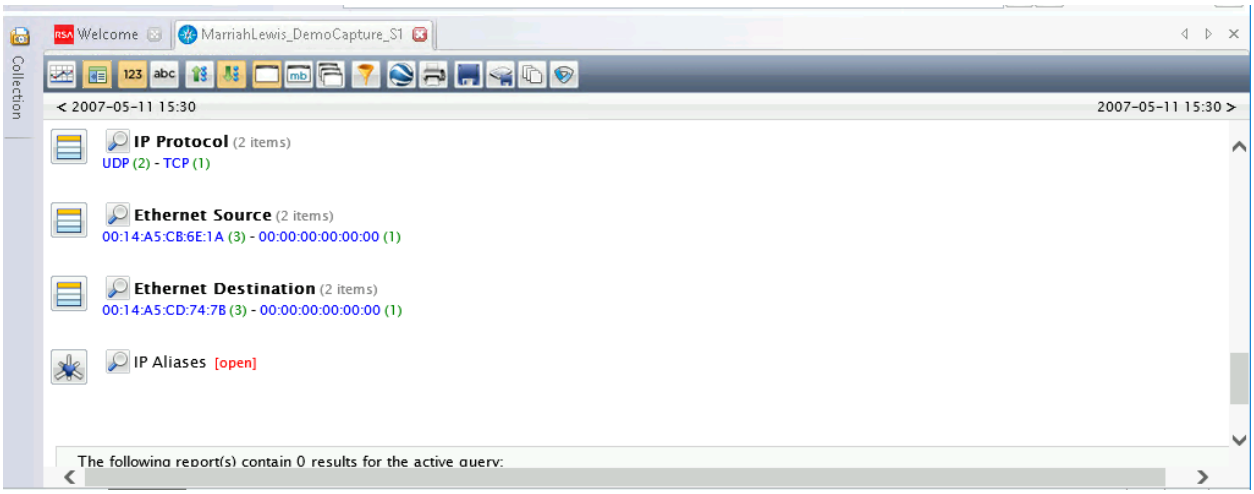


Section 1 Part 2: Analyze Wireless Traffic with NetWitness Investigator

Hostname Alias, the Source IP Address, and the Destination IP Address



Ethernet source and Ethernet destination addresses



Netwitness vs Wireshark- DNS view

Both applications provide essentially the same information, with the exception that Netwitness lacks some of the low-level wireless information, such as command and control, but it does it in a more user-friendly, graphical fashion. The DNS request and response packet information can be viewed side-by-side with the events aggregated summary on the Netwitness graphical display. Finding items like the alias host name and IP address is simple and quick with this approach but

recognizing similar details in Wireshark takes more time and skill. In Wireshark, the user must know the Canonical Name for an alias, which corresponds to the alias host name for which the request was made. In addition, Netwitness exposes attributes that are buried in Wireshark under other headers than DNS, making it difficult to traverse. The source and destination mac addresses in the first line of the Netwitness DNS event window displayed above is an example. In Wireshark, the user would have to search in other sections headers to find this critical information.

Netwitness vs Wireshark- Ethernet Source/Destination

The source/destination data is grouped in Netwitness for easy viewing of the detailed data components. The source information in the Netwitness window is divided down into three-service protocols that illustrate the communication hierarchy. Under the HTTP service, the user can observe briefly high-level information about the transmission that could be used for forensic investigation, such as country.dst, city.dst, latdec.dst, longdec.dst, domain.dst. Notwithstanding those fields, other applicable data like payload, medium, packet counts, lifetime, and more are displayed for fast investigation, while in Wireshark these fields are found in other segment headers making the task time intensive to pinpoint and difficult to understand what is going on in the communication. Nonetheless, Wireshark has lower-level data not showed in Netwitness, for example, Flags where the user can see that in the source information it shows that the ‘Protected flag: data is not protected’.