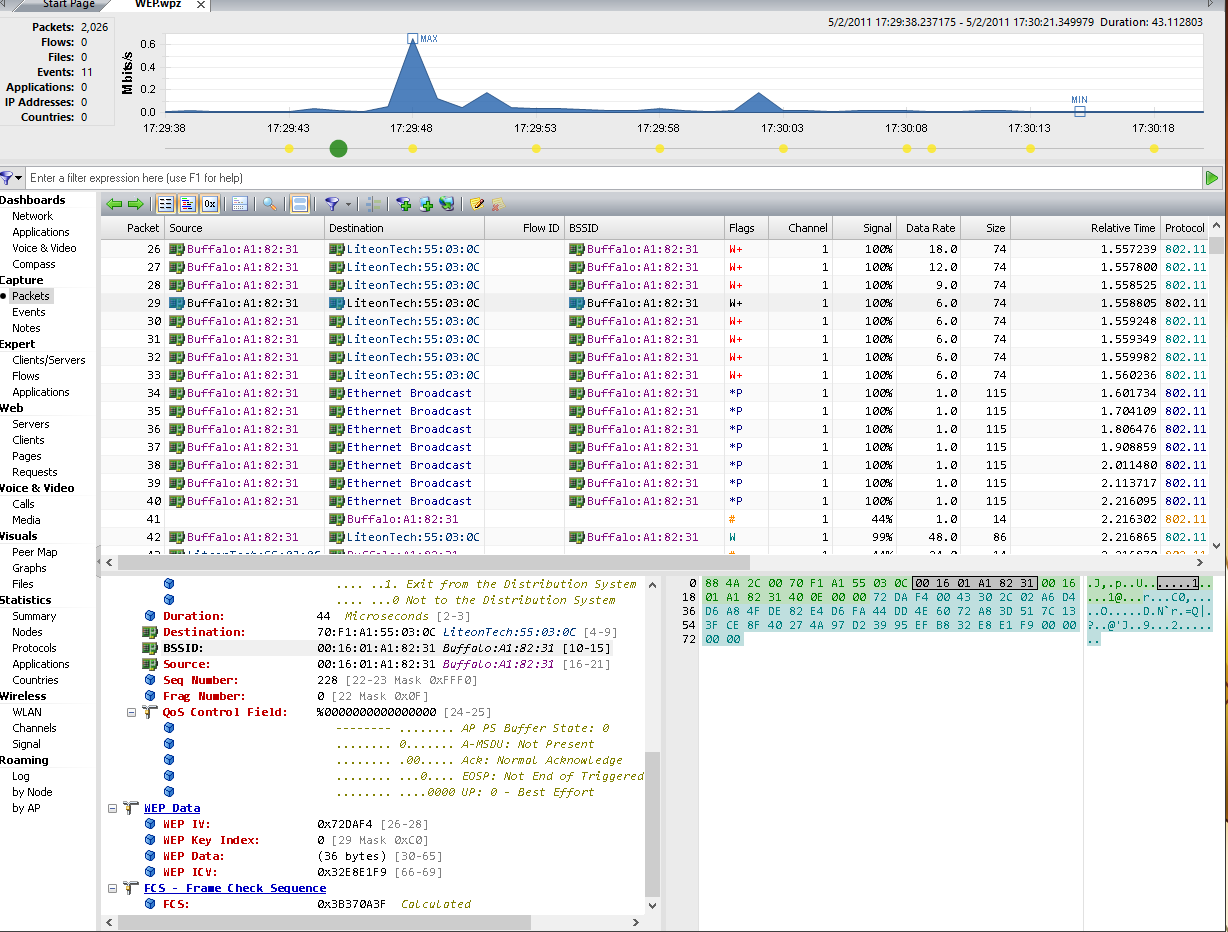
Nicholas Marshall

Dr. Nelbert St. Clair

ITEC 4344 – Ethical Hacking

September 15, 2018

Lab 4



When I ran the capture file WEP.wpz it shows communication between Buffalo and Ethernet Broadcast along with a few communications coming from and to Liteon Tech. It appears that it was easy to find the BSSID of these packets along with other useful information. This application seems to be a more advanced version of WireShark. I was also able to look at the graphs to find the % of package size along with the various Wireless packet types. After looking through a lot of the packets within this capture file I decided to take a capture from my computer. The picture below is a capture of my Ethernet packets. So, it appears that there is not much more communication from other IPs but, rather the exchanges that my IP was currently communicating with. I honestly am not sure what else can be done with these packets other than just observation and monitoring. I am sure that with the packets that were captured they could be used in Cain and Abel or maybe trying to sniff other IPs that would lead to ARP poisoning. It would be nice to learn a little more about the ARP poisoning like being able to poison my laptop for a test that way it is knocked offline momentarily.

