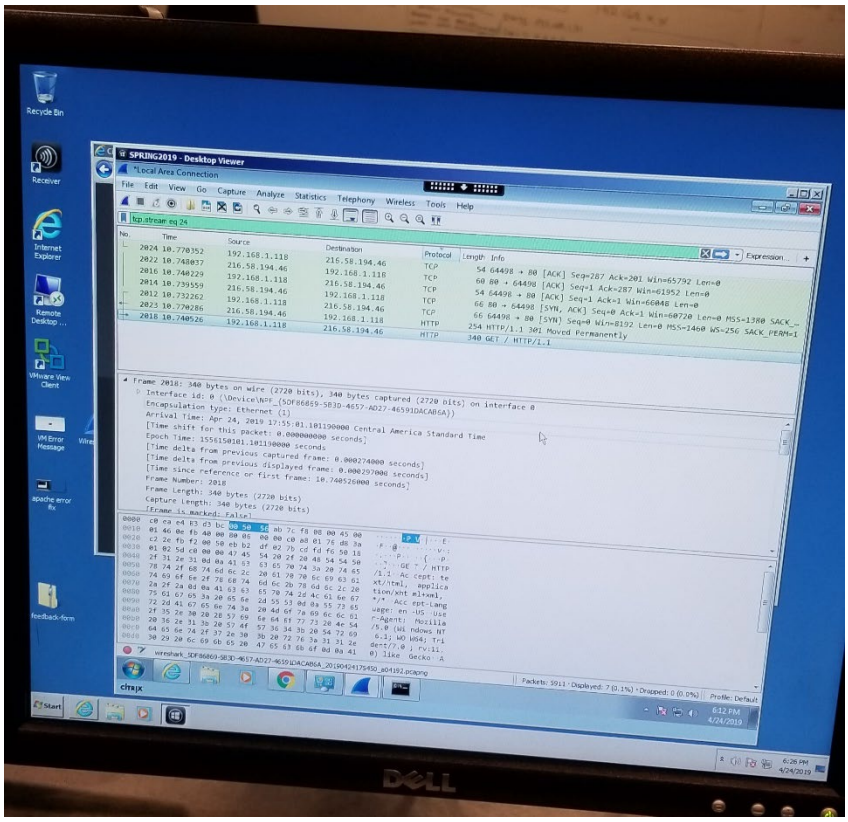
Abraham Elizarraras
PSID: 1438631

Wireshark Lab Assignment

Renewing a DHCP IP Address Lease:



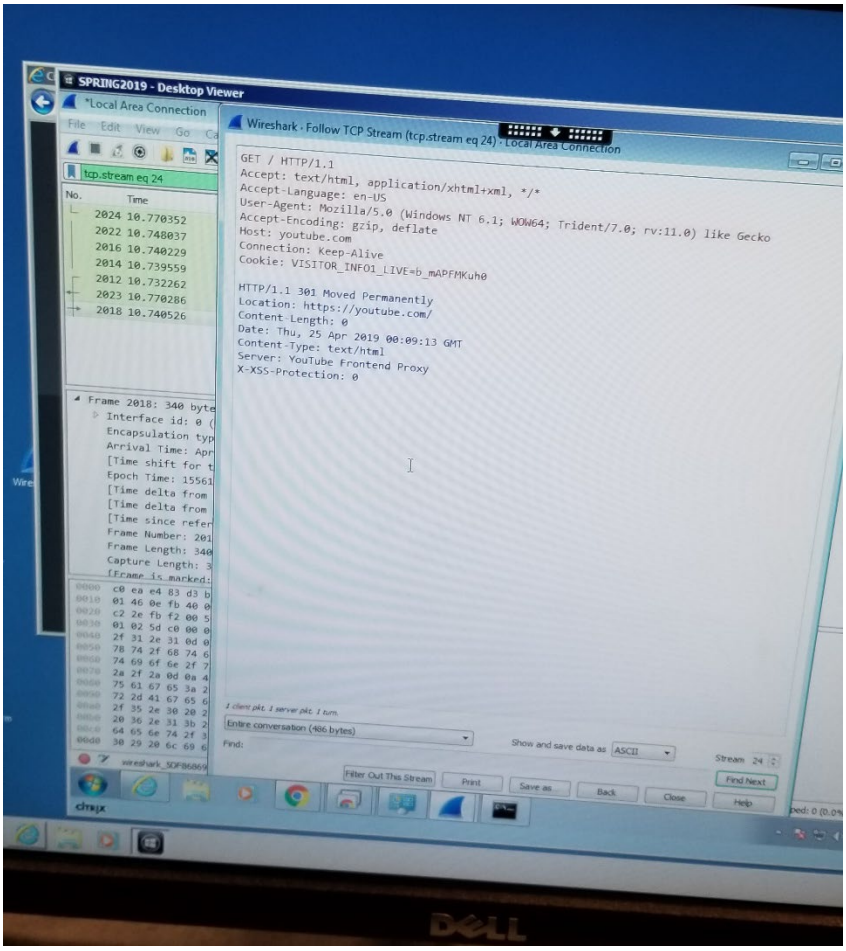
The first of these packets are from my computer to the DHCP server telling it to release the lease on your IP address. Then there's 4 packets that renew the lease.

It should be obvious to you why the first two packets are broadcasted, but what about the last two? The last two are Request and Acknowledgements of DHCP for getting the new IP address.

1. **Packet sniffing can be a controversial subject. Discuss any issues related to ethics that might arise when an organization monitors the electronic activity of its employees.**
   Packet sniffing is a tool used to capture and analyze data within a network with given predefined criterion. It is a network analyzing tool used to monitor traffic flows in a network.
   Packet sniffing is a controversial subject for debate because of property ethical issue.
   In an organization or company, employees use the internet and e-mail for their daily work to communicate and perform their tasks. So, when an employer intends to use a packet sniffing tool to monitor the employee's daily electronic activity, then there's risk of endangering their property rights. Although laws allow for monitoring, the question of property ethics still comes into play.
   As far as the organization is considered, they use this sniffing tool to monitor and protect their business from legal liabilities, such as violation of company policies, leakage of sensitive

information and to check the employee's activity for more efficiency. However, when it comes to the employees, their privacy is at risk in terms of their electronic activity such as bank transactions and personal mails. Another issue arises, in who owns the rights of a property or information. Nevertheless, this topic of packet sniffing is considered as a controversial topic that can entail lawsuits.

2. **You looked at packets captured during a web page request. What might this be useful for?**



From the above image we can clearly see the request and acknowledgements from my workstation that are in red, and the responses are in blue. This information allows an organization to predict issues relating to security and information about principal stakeholders. It is clearly visible and thus minimizes the threat of hackers in getting valuable information. It might also be used to monitor what websites employees are accessing during work hours, which impacts productivity. In turn, companies can take further steps to block or minimize access to specific websites during specific hours or days.

3. **Most computers are connected with switches (rather than hubs). How does this affect the packet capturing process?**

A hub connects multiple ethernet devices, contains many ports and acts as a single segment. Whereas, networking switches connect multiple devices within a single LAN.

The main reason why most computers are connected together with switches is because of security risks in a networking environment. In a hub, when a packet comes to one port, it is then transmitted to all other ports. So, this creates the issue of security concerns. However, with the usage of networking switches. When a frame or packet is received, it is sent to the right destination port, hence reducing the security issues. Therefore, with usage of switches, the packet capturing process is efficient and there's less security concerns of people sniffing packets since switches do not flood the network with packets like through a hub.

4. **Discuss how sniffing packets from wireless networks might differ from wired networks. Use the Internet to search for wireless packet sniffers. Where might someone go to sniff wireless packets and possibly obtain some "juicy" information?**
   Packet sniffing is more advantageous when done in a wireless network rather than through a wired network. Reason being that it is difficult for someone like a hacker to install sniffer software, in an effective way, in a wired network to then compromise the security of the network. On the other hand, in a wireless network one can get some "juicy" information very easily as the hacker doesn't need a physical link and just needs to crack the WEP and WPA passwords, which can be done easily.
   Some examples of wireless packet sniffing tools are RFGrabber, Wireshark, Cain and Abel, Carnivore, Kismet, and dSniff.