CYSE 301: Cybersecurity Technique and Operations

Assignment: Password Cracking (Part B - Wi-Fi Password Cracking)

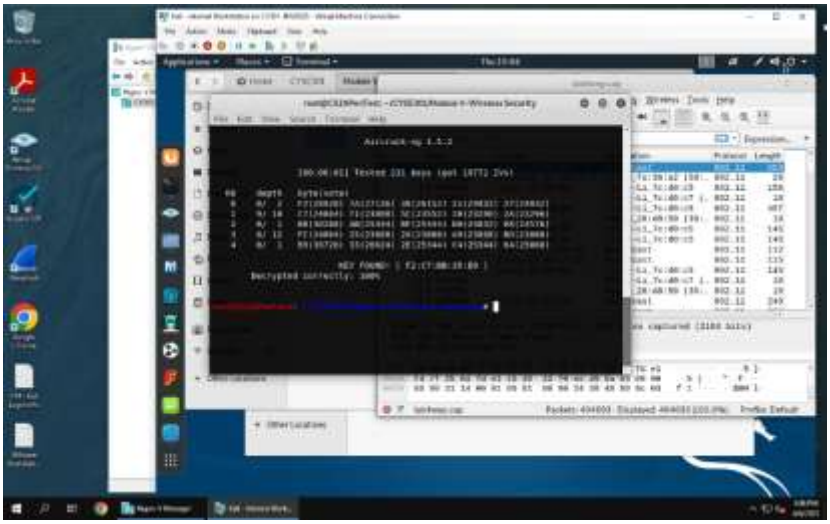
Jason Rivers

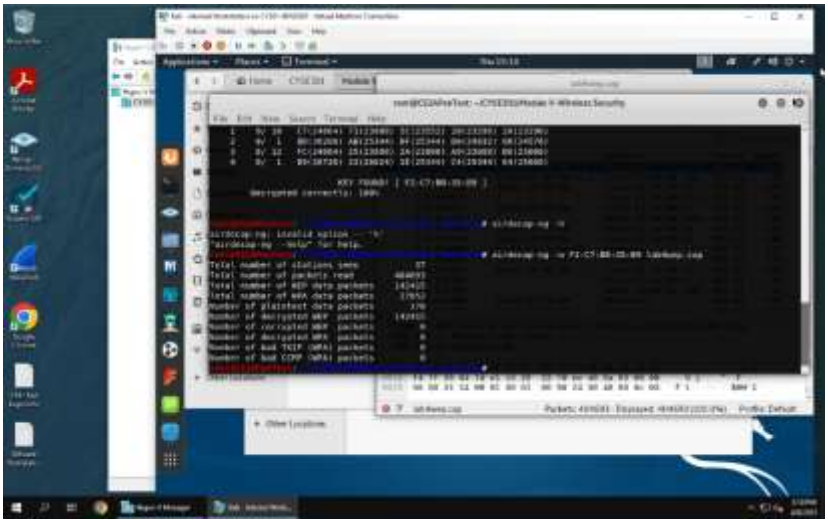
01236524

Task C: 20 points

Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

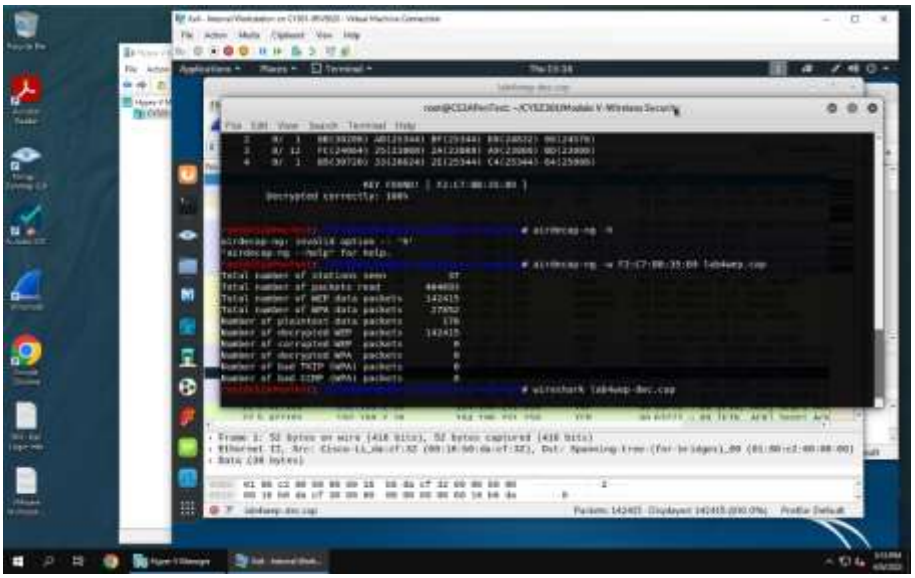
1. Decrypt the lab4wep. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)



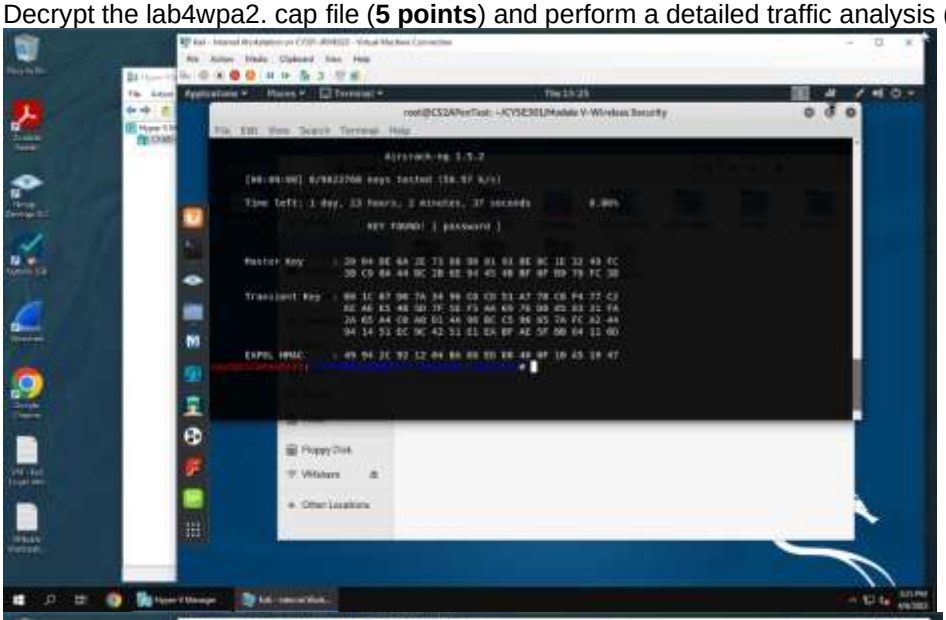


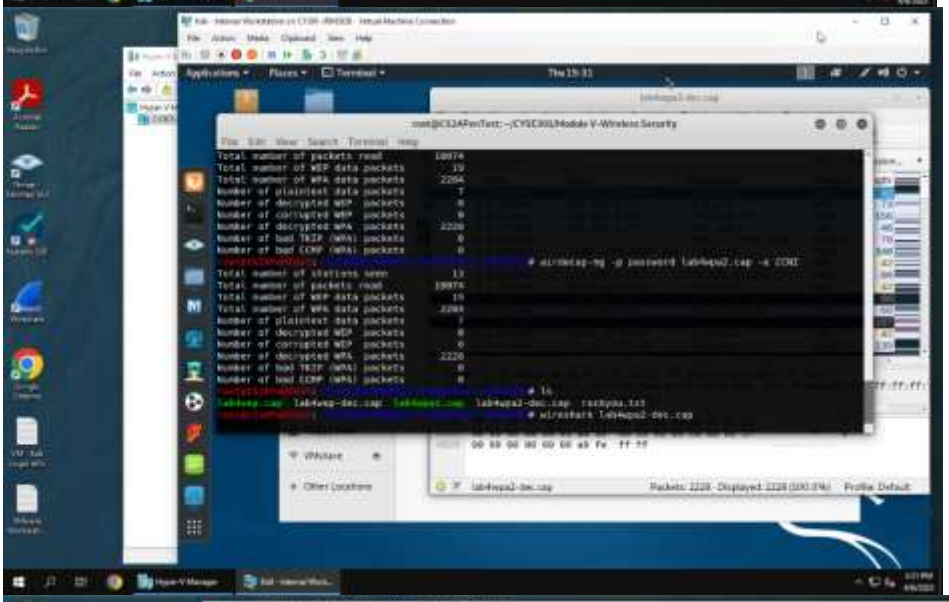
I followed the WEP steps to decrypt and get the traffic for this one.

I didn't feel the need to throw the Protocol Hierarchy like in the directions, so I just showed the command, and the Wireshark header.

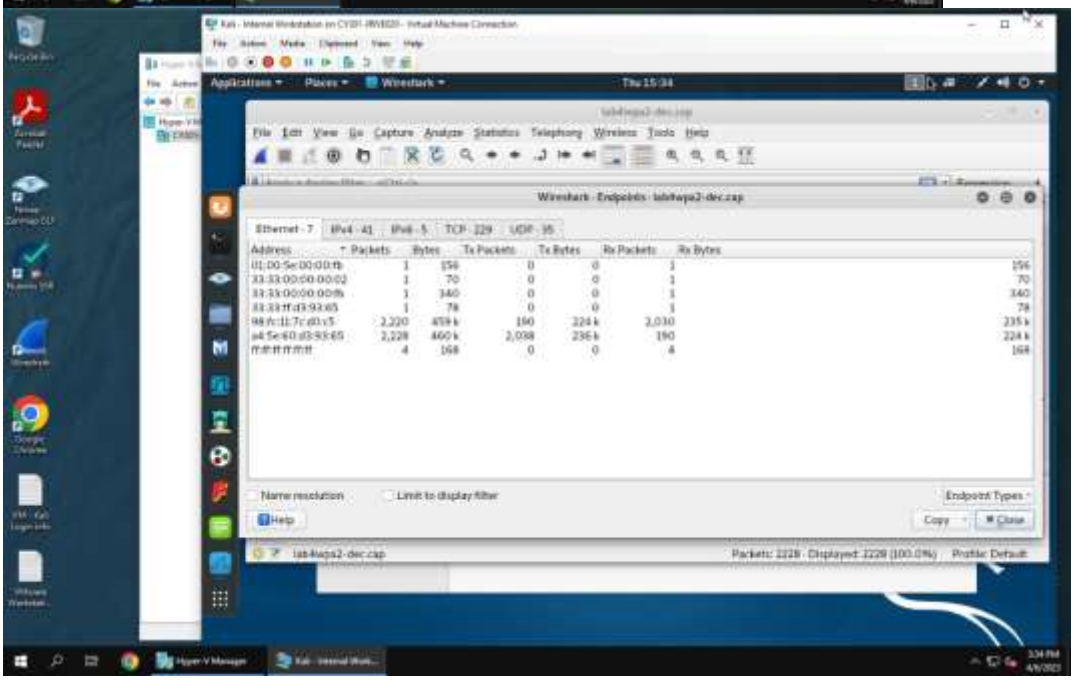


2. Decrypt the lab4wpa2. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)





I followed the directions again, but this time I displayed Endpoints to show I know what I'm doing in Wireshark.



Task D: 30 points

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the last digit of the hash for pjiang is **e**. Thus, I should pick up the file "WPA2-P5-01.cap."

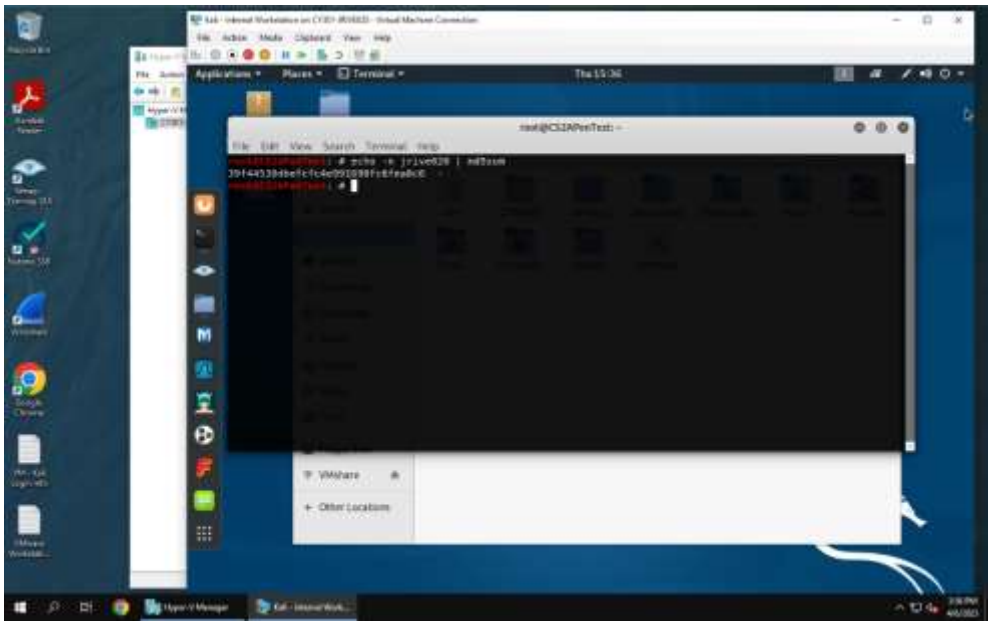
MD5 of pjiang is 5a618cdc3edffd8b4c661e7e9b70ce1e

You can find an online MD5 hash generator or the following command to get the hash of a text string,

```
root@CS2APenTest: # echo -n pjiang | md5sum
5a618cdc3edffd8b4c661e7e9b70ce1e  -
root@CS2APenTest: #
```

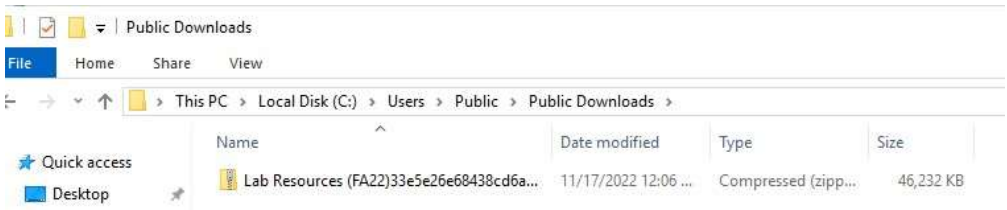
Figure 1 Command to get the MD5 hash.

Last digit of your MD5	Filename
0~3	WPA2-P1-01.cap
4~5	WPA2-P2-01.cap
6~8	WPA2-P3-01.cap
9~B	WPA2-P4-01.cap
C~F	WPA2-P5-01.cap



I'm going to be using WPA2-P3-01.cap

- The above files are zipped in a folder named "Lab Resources." You can locate the zipped folder in the Windows 10 Host Machine under C:/Users/Public/Public Downloads. Then, unzip the following zipped file and find the assigned WPA file under the sub-folder "Wireless Traffic."



- Copy the file assigned to you to the "C:/VMshare" in Windows 10 Host Machine to access it from the Kali VMs (you can use either Kali to complete the assignment).

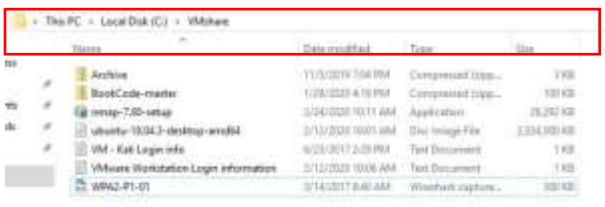
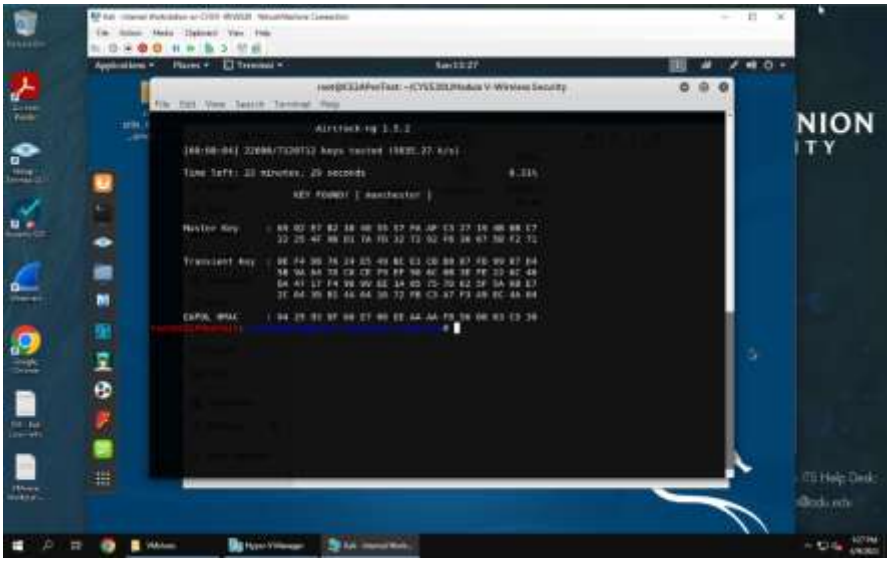


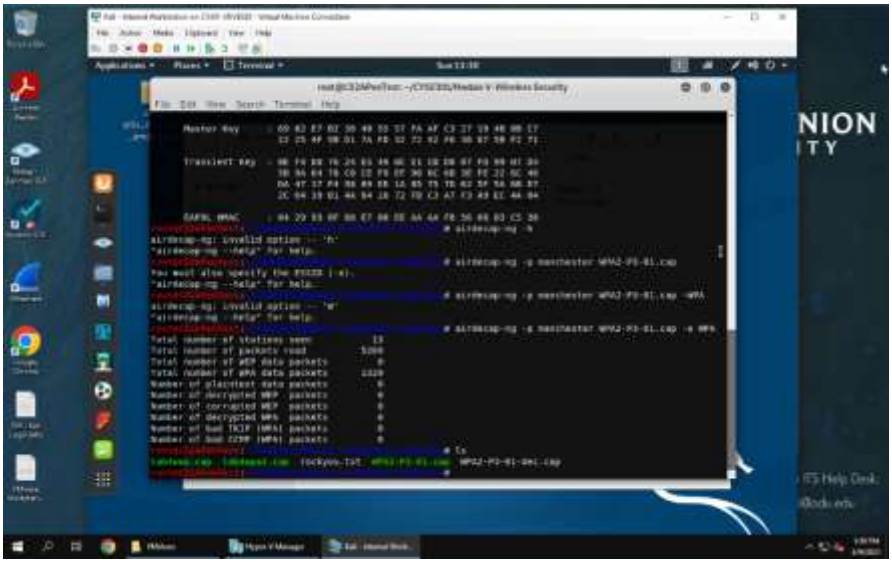
Figure left: Windows Host Machine *Figure right: VMshare folder on Kali Linux*

Then complete the following steps:

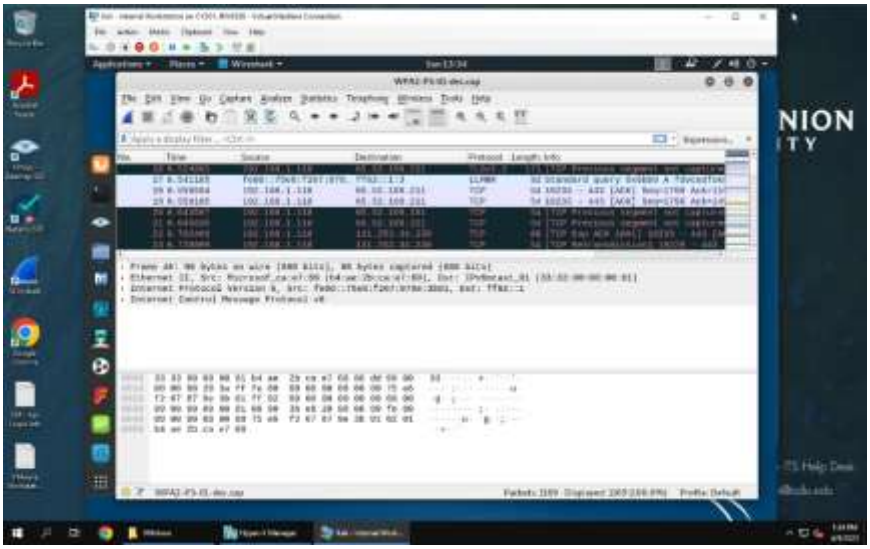
1. Implement a dictionary attack and decrypt the traffic. - 20 points



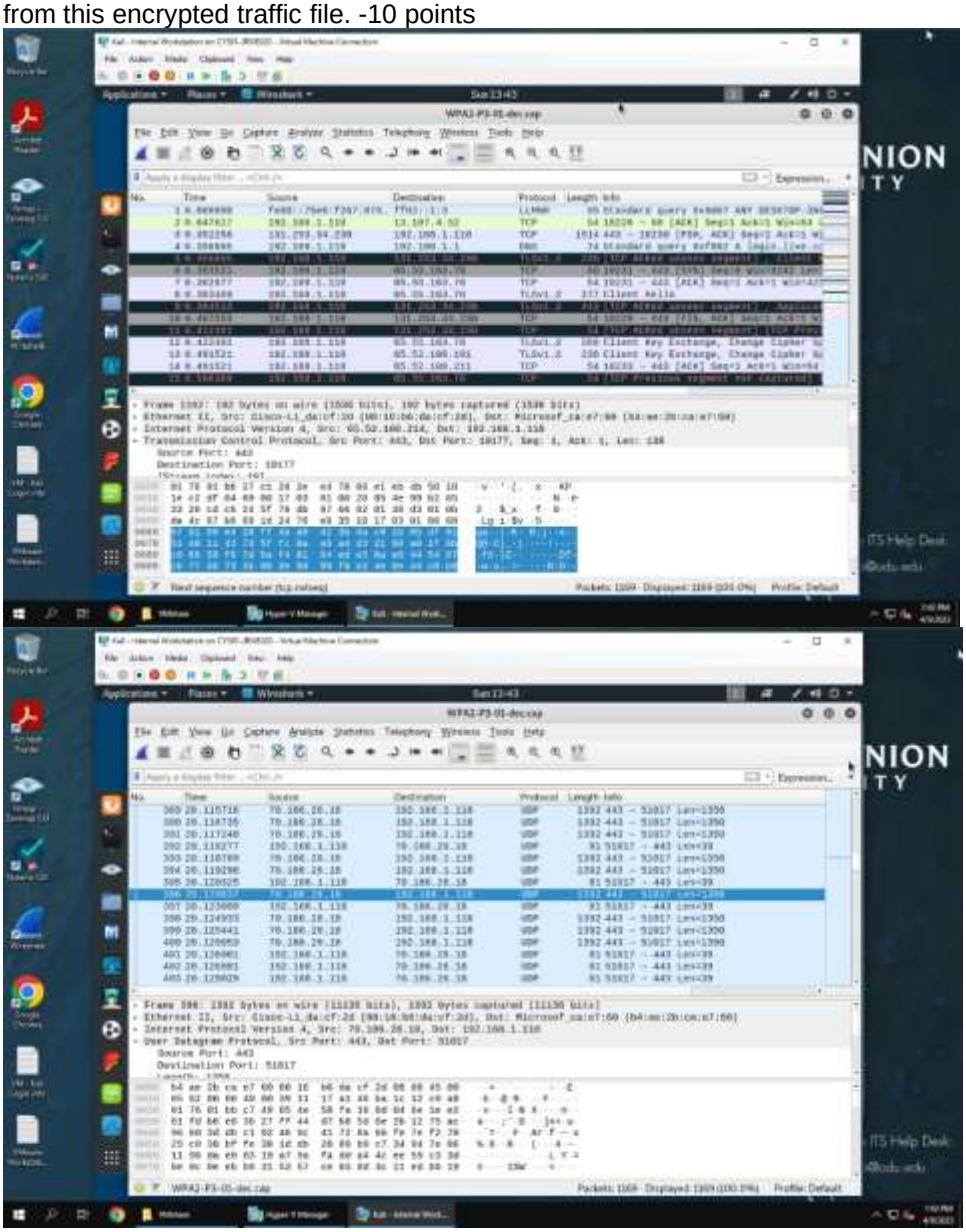
Dictionary attack using rockyou.txt



*Note: I realized my mistake, and went back to change **"-e WPA"** to using **"-e CyberPHY"***



2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -10 points



The beginning traffic is essentially just handshakes, establishing who is who during the connection using ARP, TCP, and ICMP protocols, as well as registering Users, and Groups. There seems to be a lot of traffic from a Microsoft device to IPv6, and a Cisco device as well.

After the handshakes, connection, registering and the like are complete, there's a LONG string of UDP traffic between a Microsoft and Cisco Device on port 443. This goes on for about 10 or so seconds, but the number of frames is staggering. When googling port $$# using UDP traffic, HTTP/HTTPS protocol comes up, which leads me to believe this traffic may have been a video.