**Blue Team Capstone**

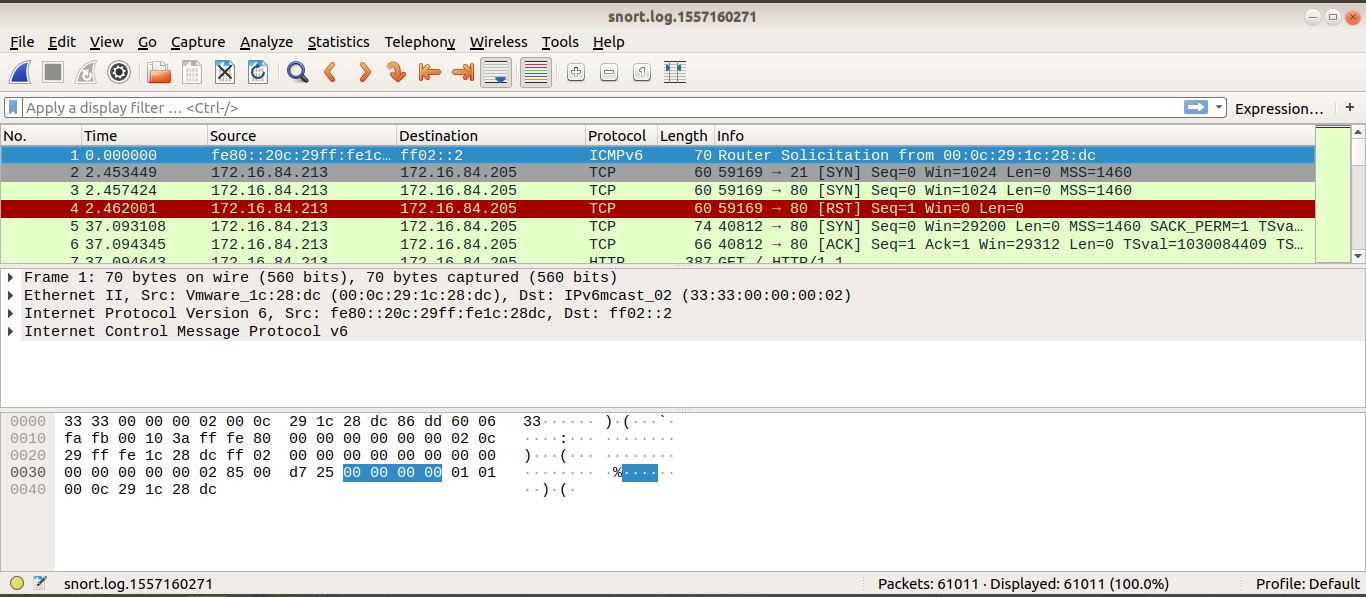
**Project**

Justin Smith

4/8/2020

**Loading the log**

I loaded snort.log.1557160271 into wireshark.

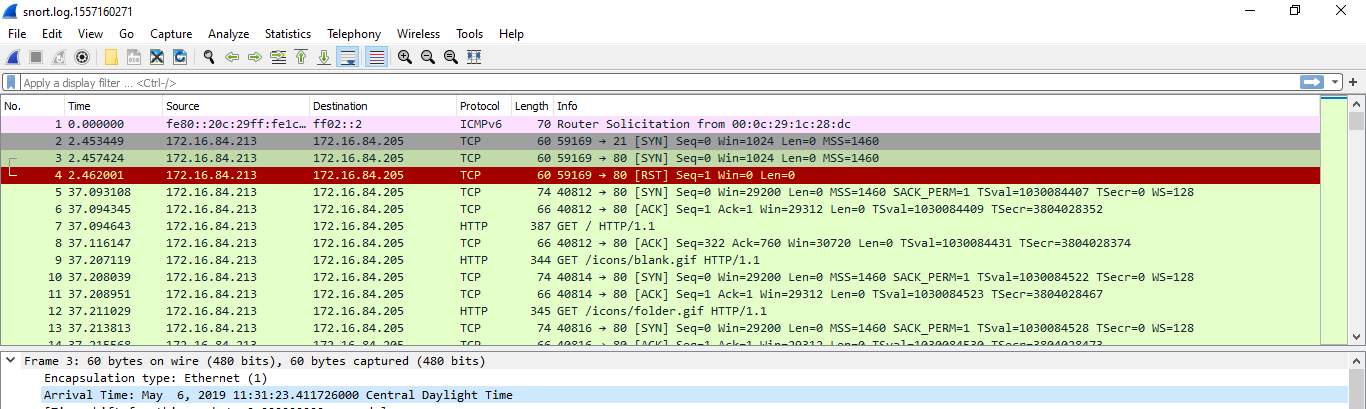


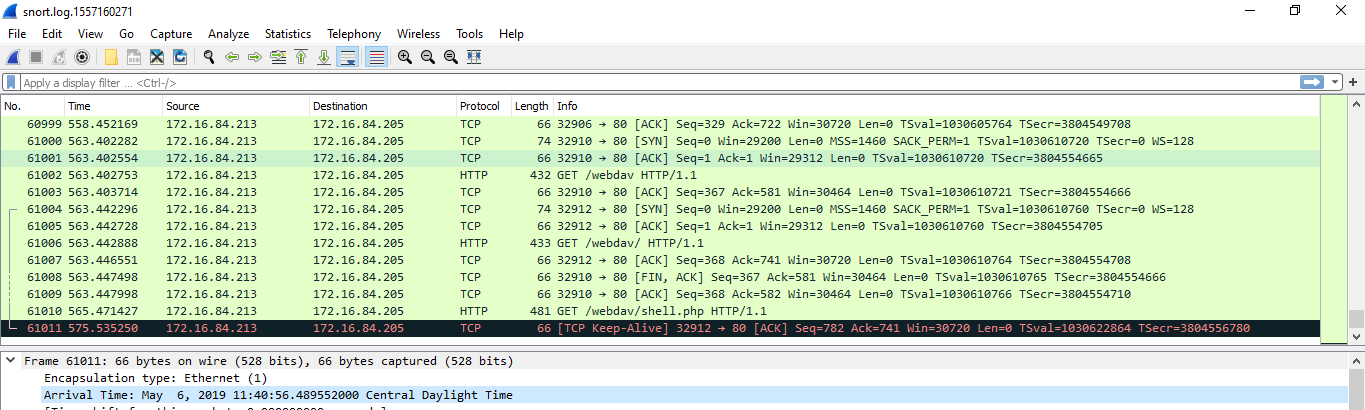
**Time of attack**

-The attack started at 11:31

- It ended at 11:40

- It lasted 9 minutes



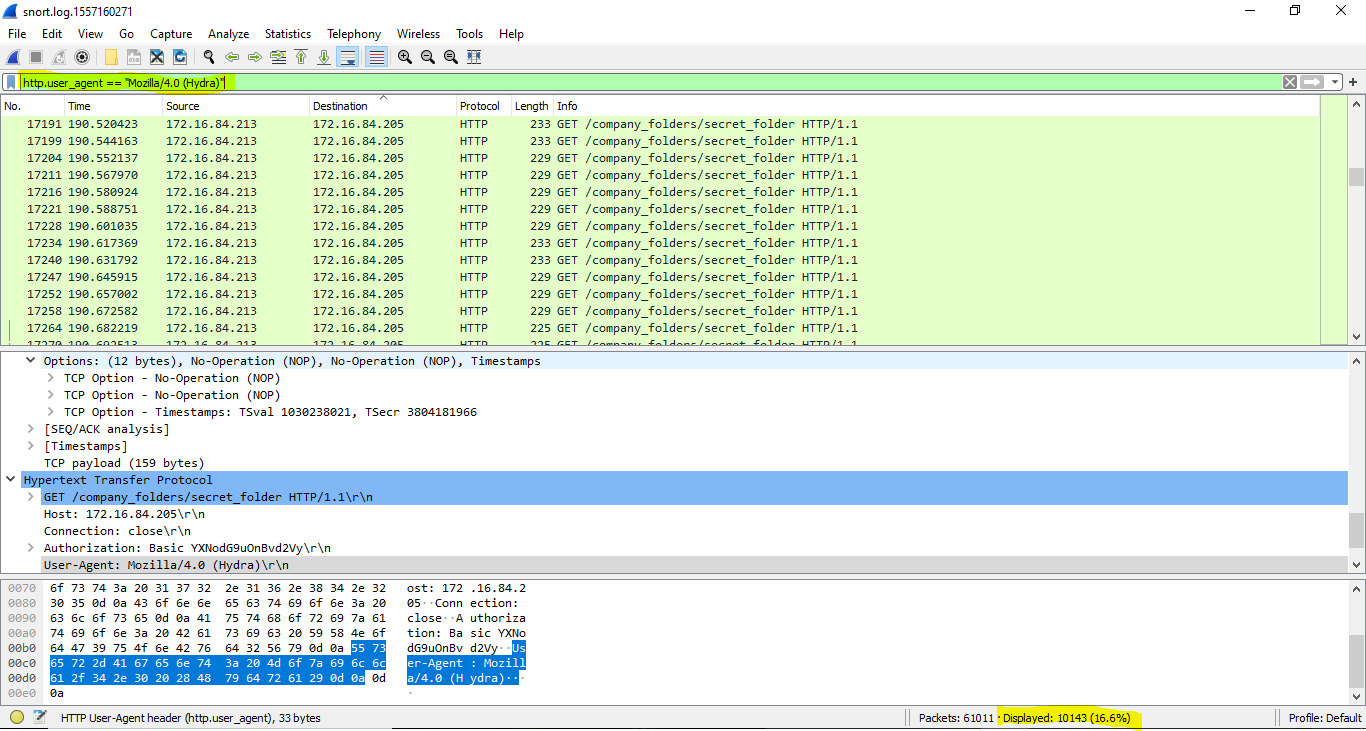


**Password Attempts**

By filtering our pcap file we can isolate the password attempts

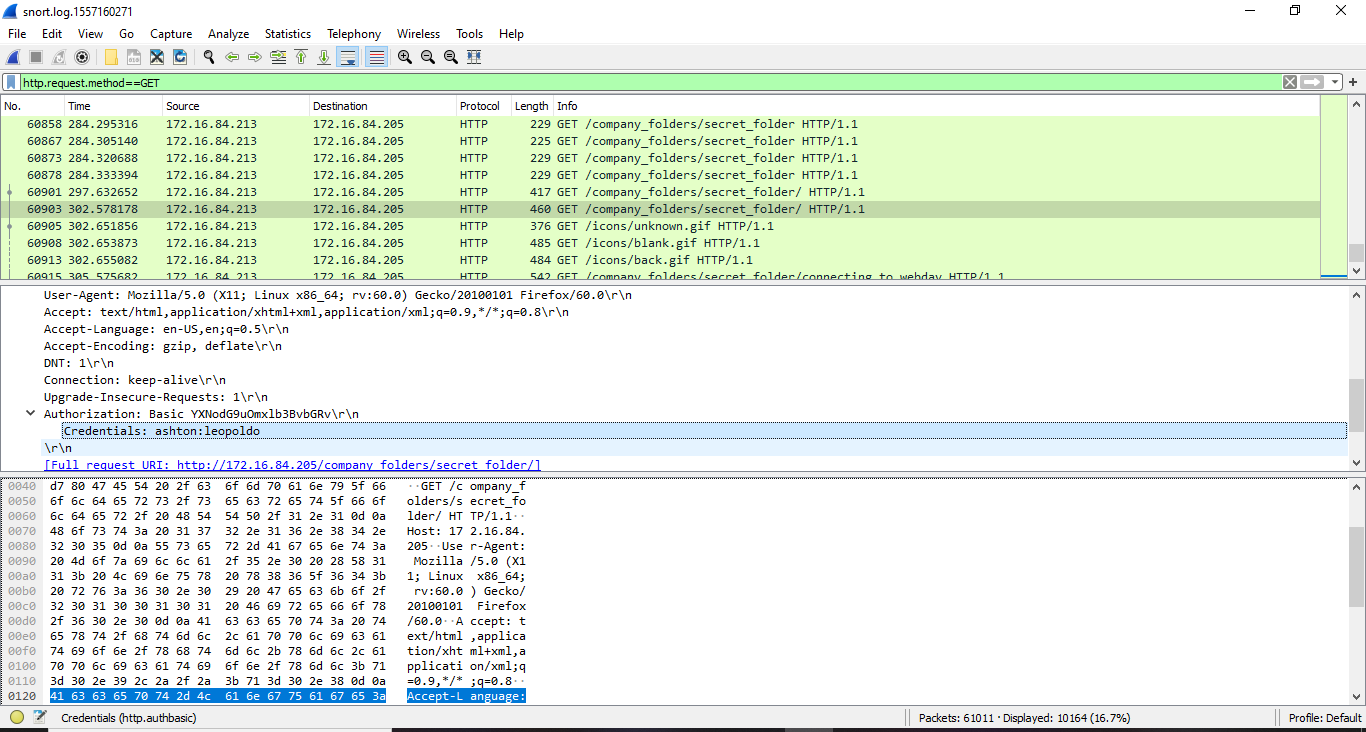
Http.user\_agent == “Mozilla/4.0 (Hydra)”

Total Attempts: 10143



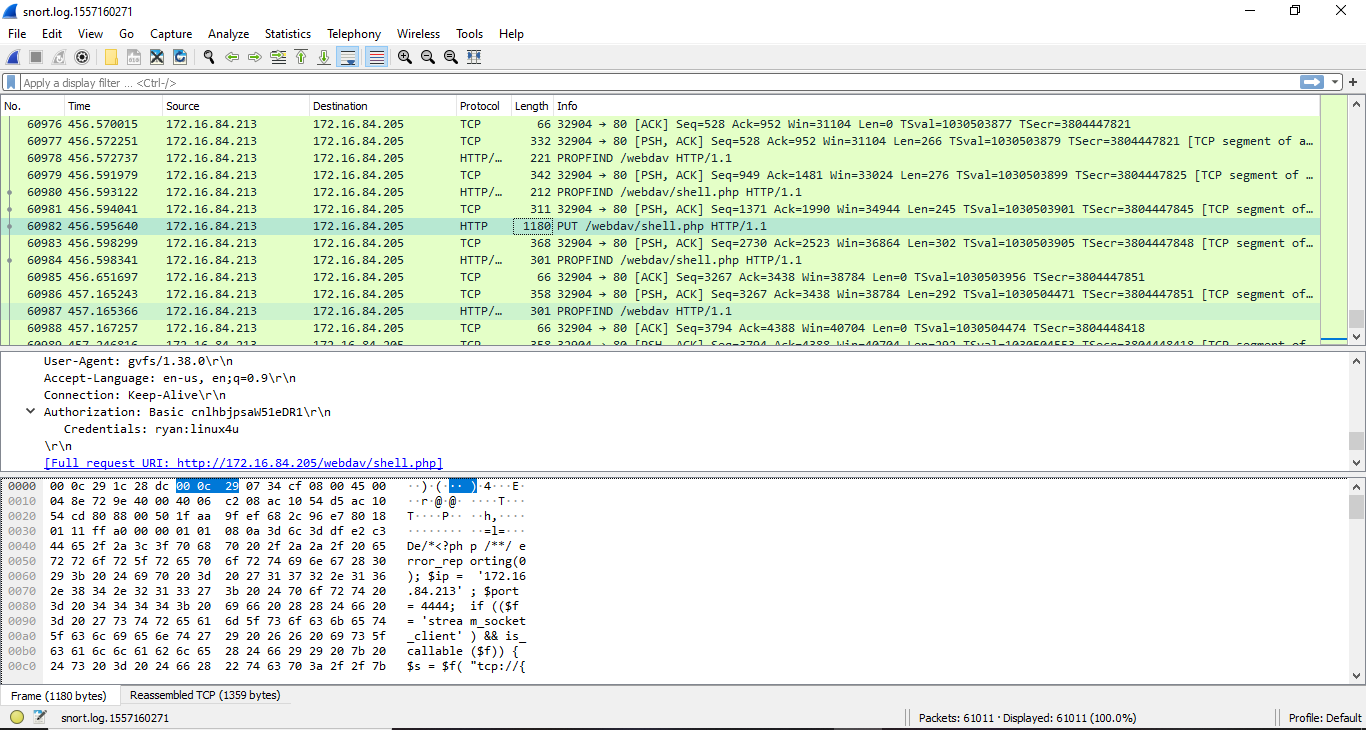
**Correct password found**

-Ashton’s password was found in packet 60903



**Shell placed on server**

-The shell was placed on to the server in packet 60982



**Shell was activated**

-The shell.php was activated in packet 61010

