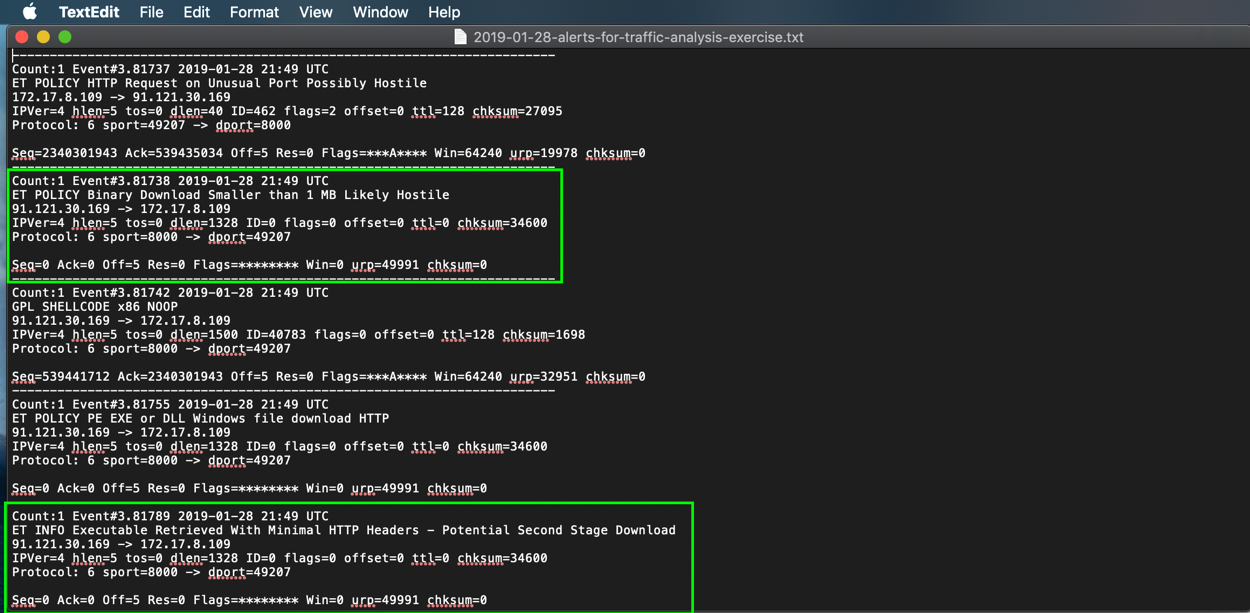
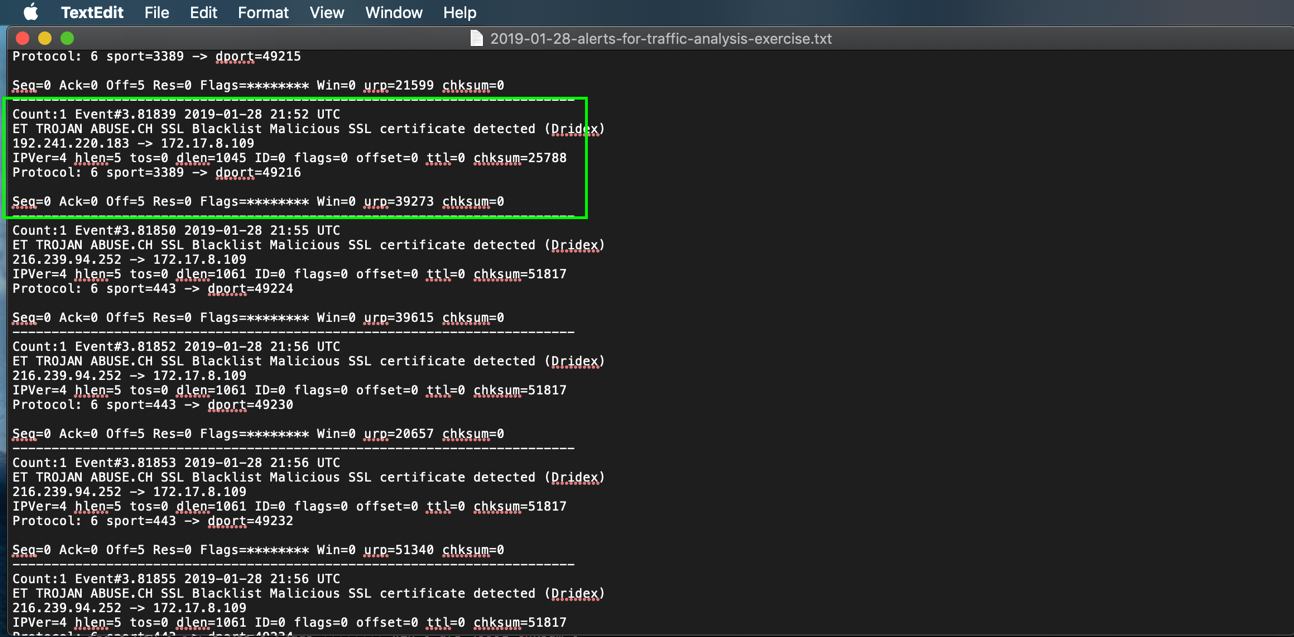
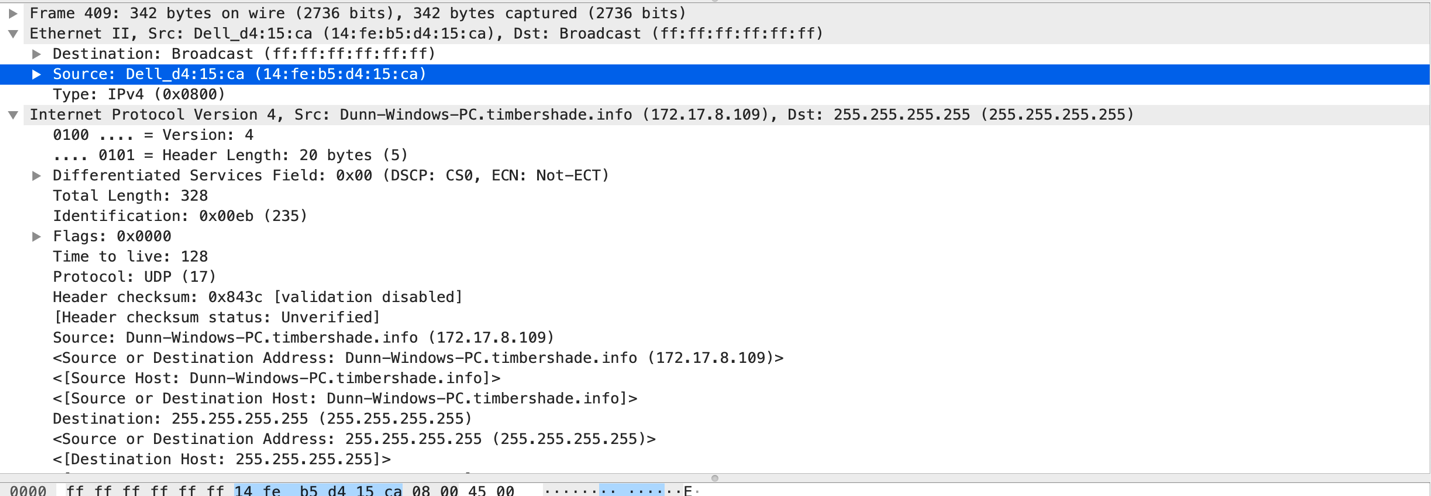
**Post-Incident Report**

|  |  |
| --- | --- |
| Date of investigation | July 11, 2019 |
| Date of incident | 2019-01-28 21:49 UTC |
| Outcome | True Positive – Dridex Trojan Virus Variant downloaded and found. |
| Action Taken | Identified the Virus and the infected host device.  Advise firewall rules to block traffic communication from the source.  Potential action to be taken as follows: Reformatting the device if virus is widespread, restoring from a backup prior to time of incident and running a virus scan to verify complete removal of Dridex Trojan. |
| Reporting tools | Snort and Wireshark for internet traffic investigation |
| Attack Vector | Web Virus Download |
| Source IP  Source Port | 172.12.8.109  80 |
| Destination IP  Destination Port | 91.121.30.169  49207 |

**Narrative**

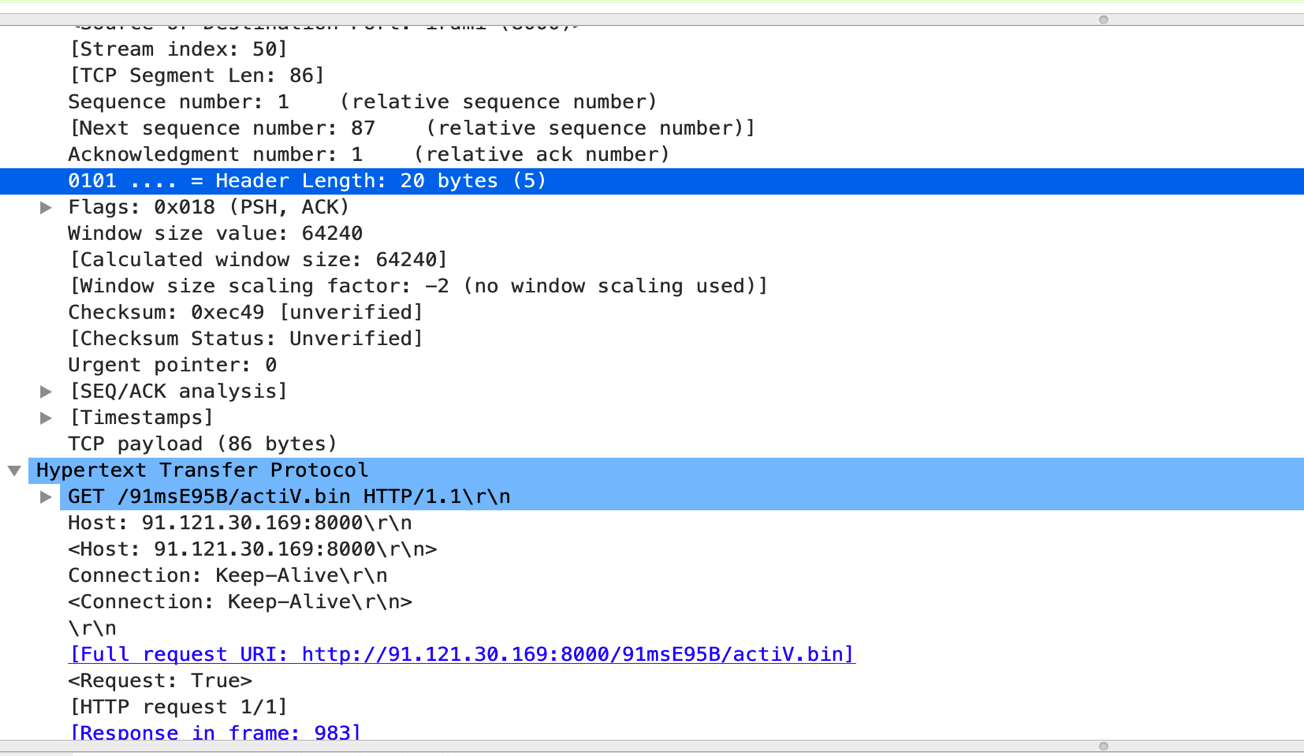
* Alerted by Snort:
  + “ET POLICY HTTP Request on Unusual Port Possibly Hostile”
  + “ET POLICY PE EXE or DLL Windows file download HTTP”
  + “ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download”
  + “ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)”
* Located the Source/Destination IP Addresses and timestamp from Alerts:
  + Src/Prt: 172.12.8.109: 80
  + Dst/Prt: 91.121.30.169: 49207
* Identified IP Addresses and communication from Snort Alerts.



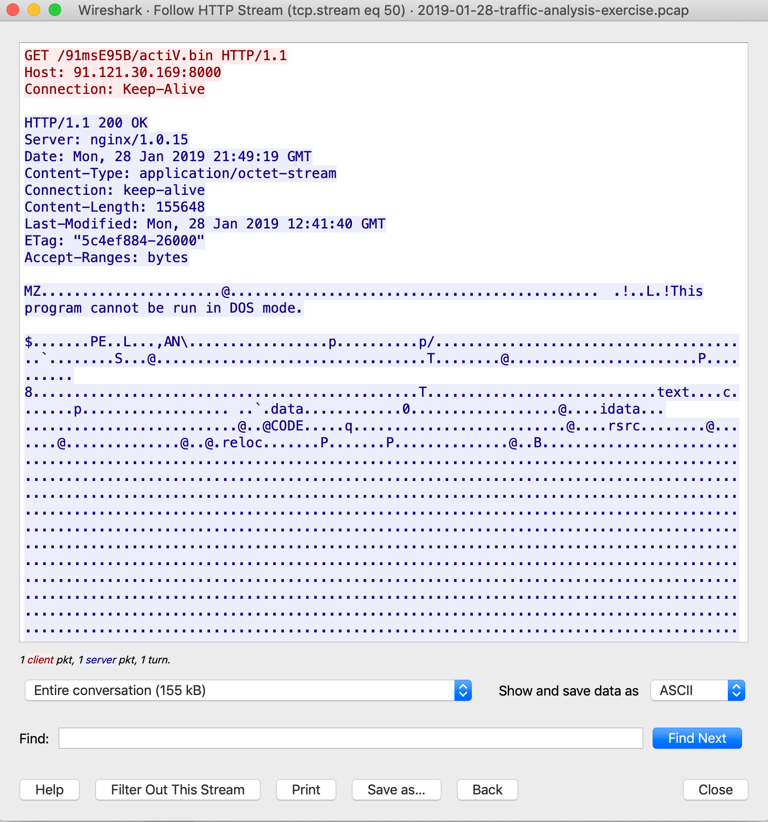
* Identified Hostname and MAC address of infected computer from \*.pcap:
  + MAC address: 14:fe:b5:d4:15:ca
  + Host Name: Dunn-Windows-PC

**Post-Incident Report**

* Identified download of file that contained the Trojan Virus in pcap HTTP traffic:

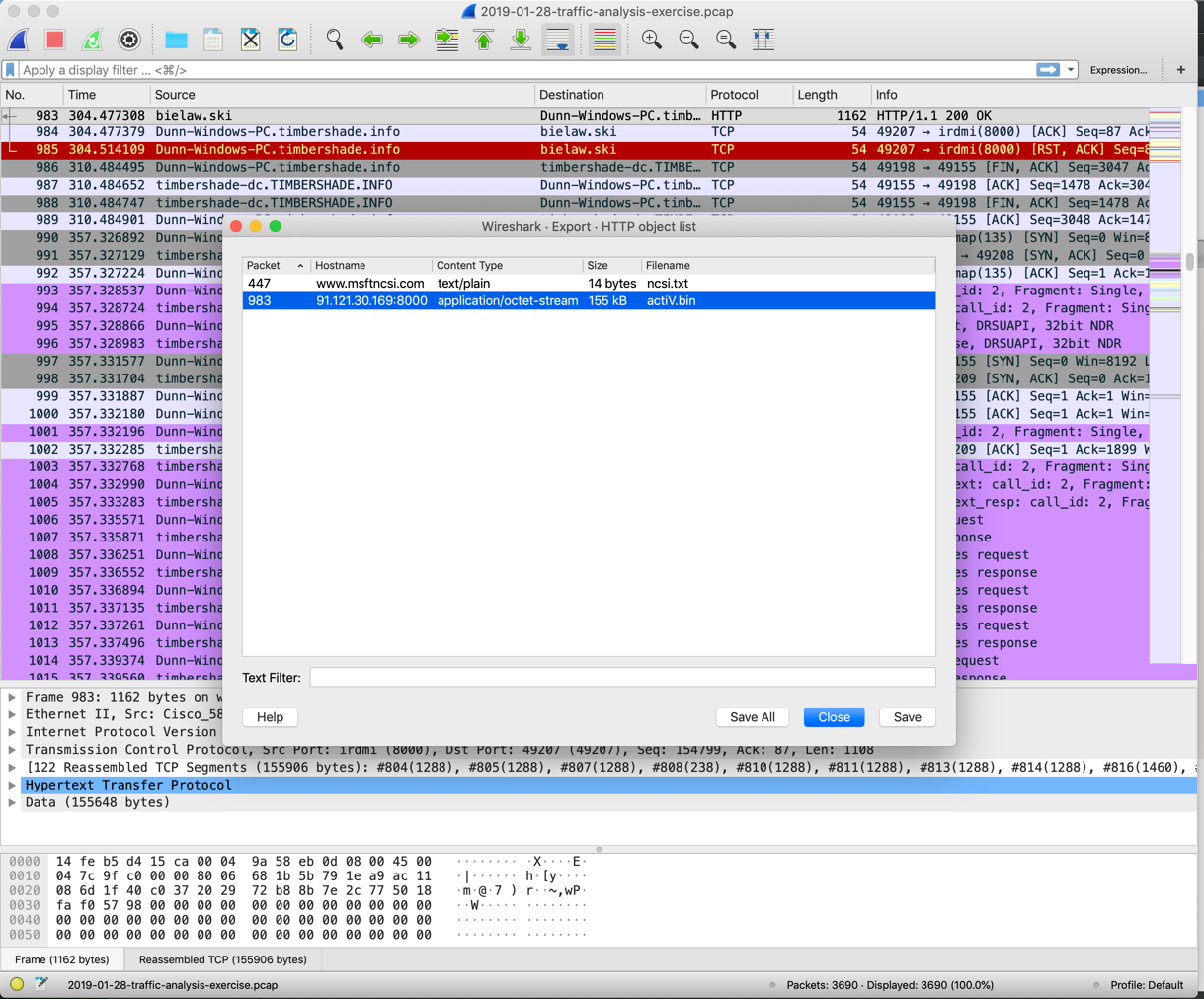


* Followed the HTTP Stream and found that a binary file was downloaded:
  + Downloaded on Monday, 28 Jan 2019 21:49:19 GMT
  + “This program cannot be run in DOS mode.” Is an indication of a potential threat



**Post-Incident Report**

* Exported HTTP objects from captured pcap file and also had the same file name from the above listed traffic.
  + actiVe.bin



* Uploaded SHA256 hash to virus total for confirmation:
  + 9f6e3e65aedca997c6445329663bd1d279392a34cfda7d1b56461eb41641fa08 actiVe.bin
* Used Wireshark to identify possible firewall rules to prevent further downloads and potential infection of other computers. Depending on other firewall configurations blocking IP might suffice instead of blocking port as well.
* # IPv4 destination address
  + iptables --append INPUT --in-interface eth0 --source 91.121.30.169/32 --jump DROP
  + iptables --append INPUT --in-interface eth0 --protocol tcp --source 91.121.30.169/32 --source-port 8000 --jump DROP