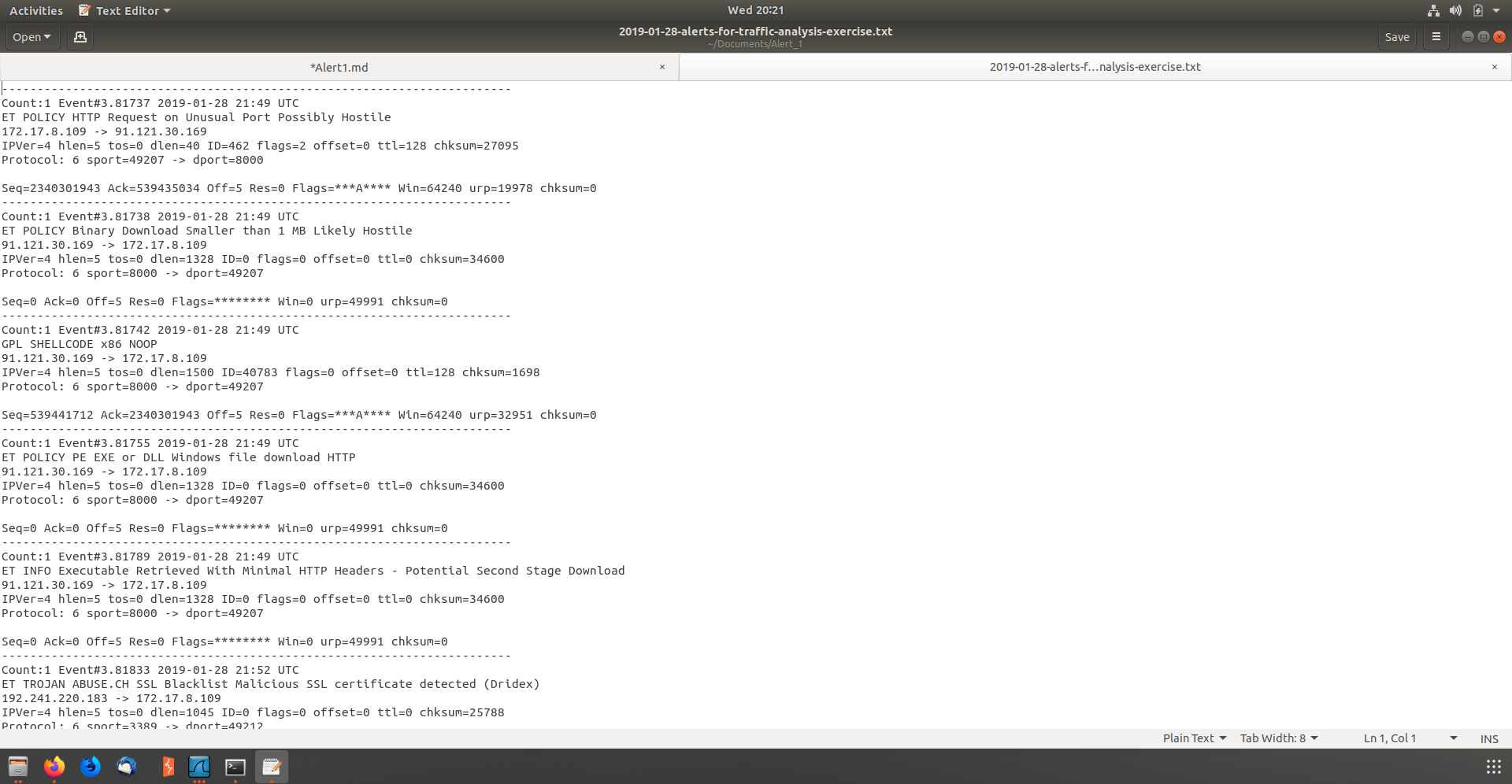
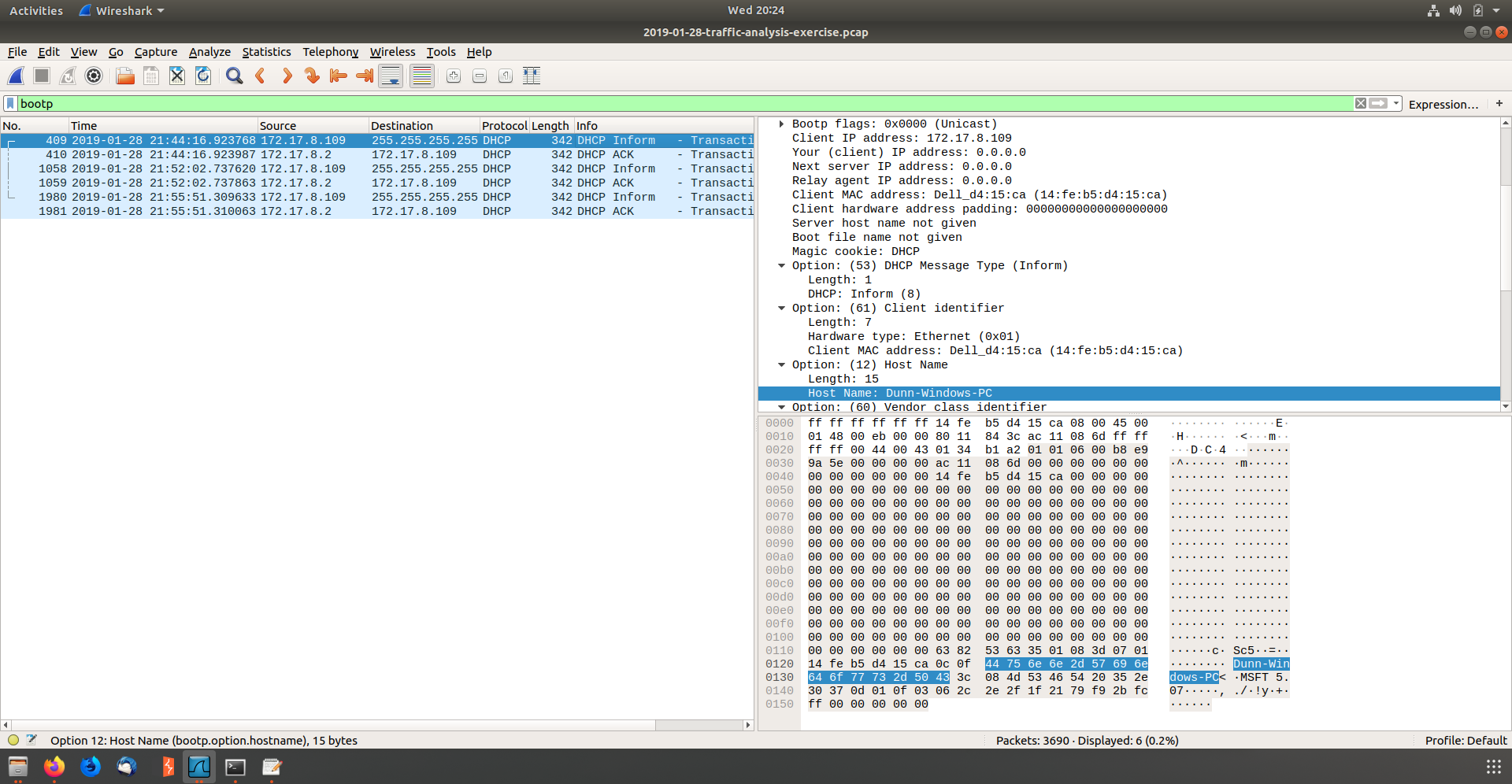
|  |  |
| --- | --- |
| Date of investigation | 2-29-20 |
| Date of incident | 1-28-2019 @ 21:49 UTC |
| Outcome | True positive Malware DirecPLL was detected |
| Action Taken | Identified malware affecting computer  Advised on firewall rules  Advised to restore to backups |
| Reporting Tool | Snort |
| Attack Vector (Web, Email, Network, etc…) | Web Malware Download |
| Source IP/ Email | 91.121.30.169 |
| Source port | 8000 |
| Destination IP/ Email | 172.17.8.109 |
| Destination port | 49207 |

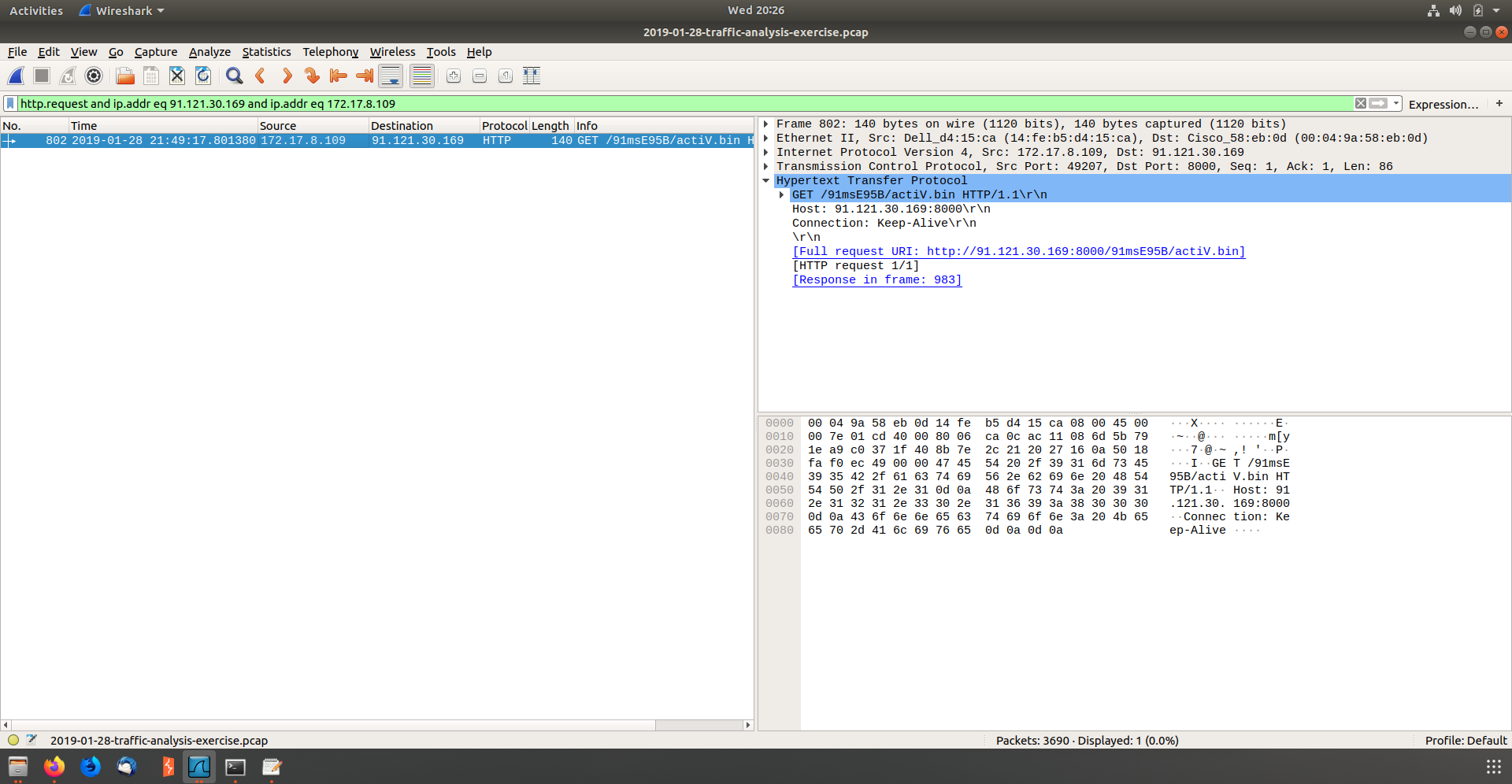
Narrative

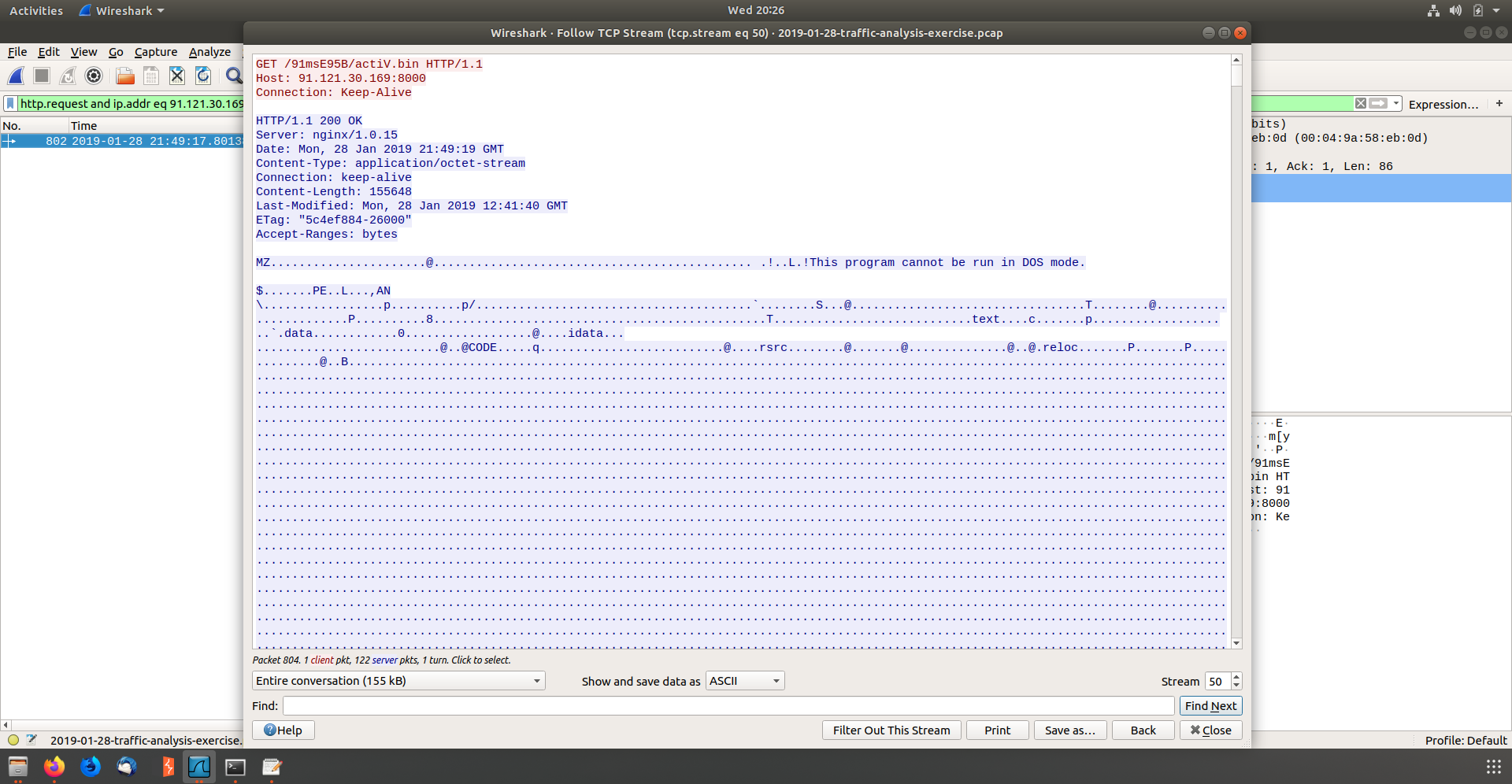
* Alerted by Snort
  + ET POLICY HTTP Request on Unusual Port Possibly Hostile
  + ET POLICY Binary Download Smaller than 1 MB Likely Hostile
  + ET INFO Executable Retrieved With Minimal HTTP Headers – Potential Second Stage Download
* located source/ destination ip
  + src/prt: 91.121.30.169:8000
  + dst/prt: 172.17.8.109

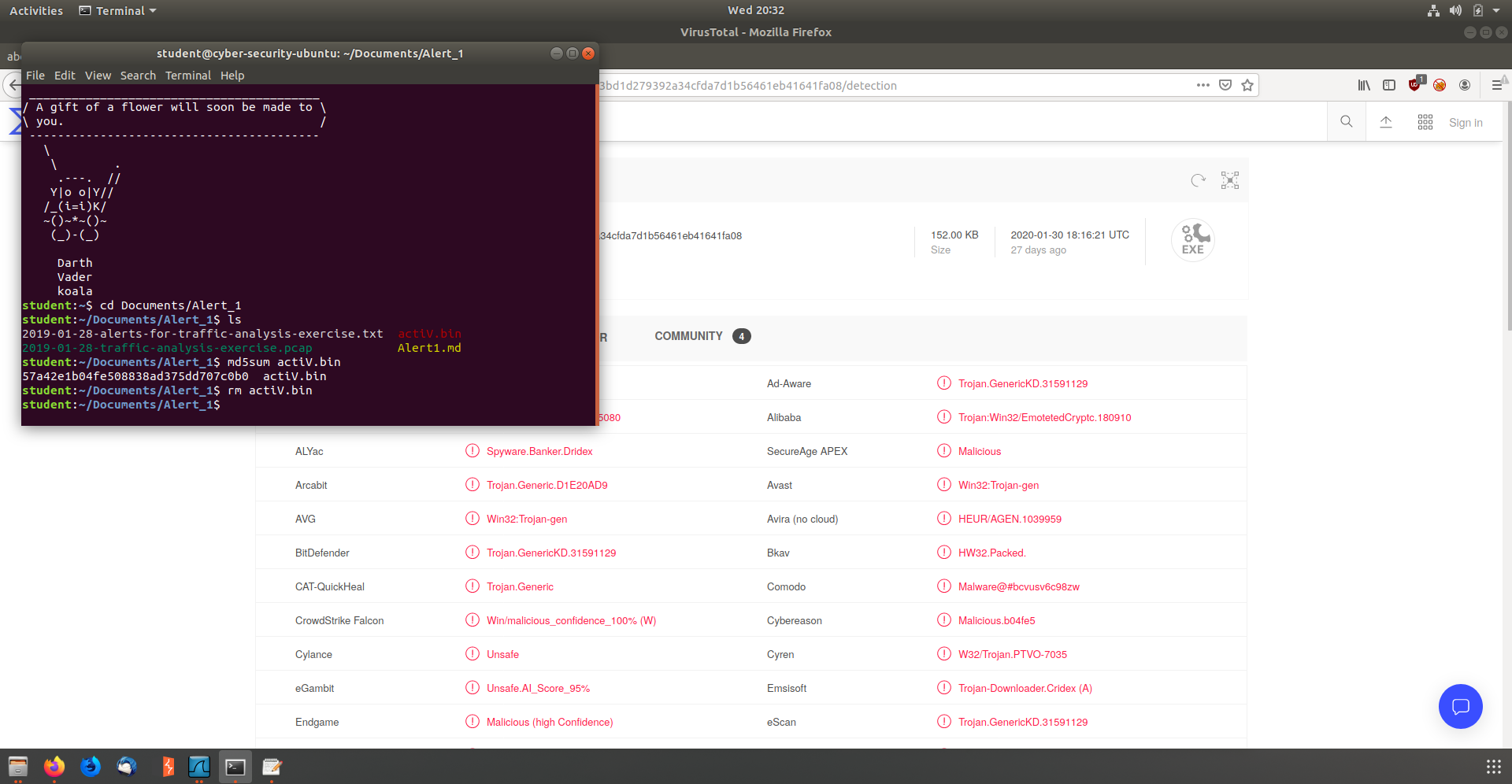


* Identified hostname and MACAddress of infected computer
  + MAC:14:fe:b5:15:ca
  + Host name Dunn-Windows-PC



* Identified the time that the attack took place
* Followed the TCP and found active.bin was downloaded



* Exported HTTP Objects and Hashed actiV.bin
  + Md5sum hash: 57a42e1b04fe508838ad375dd707c0b0
* Uploaded the Hash to virus total and found 57 engines detected the file

