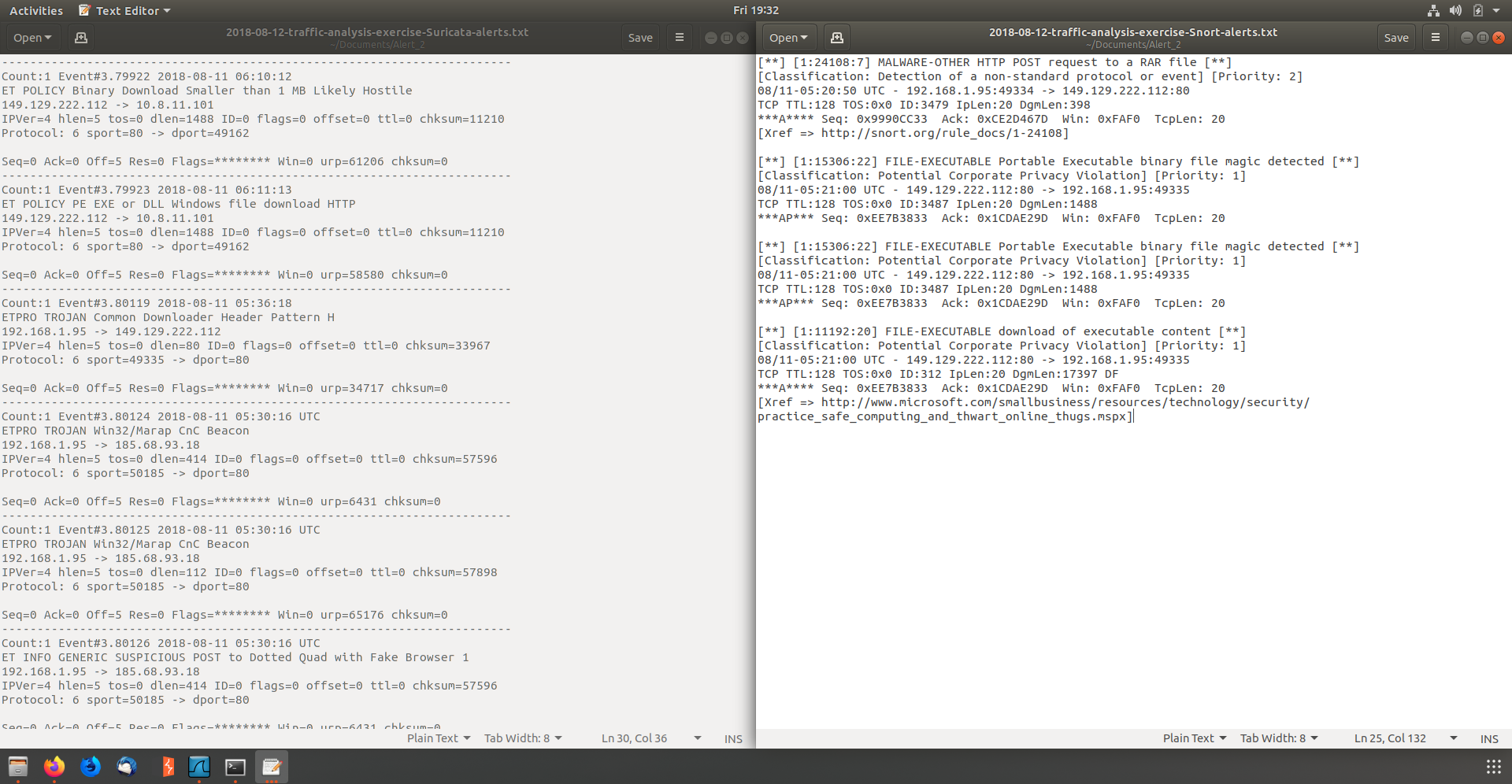
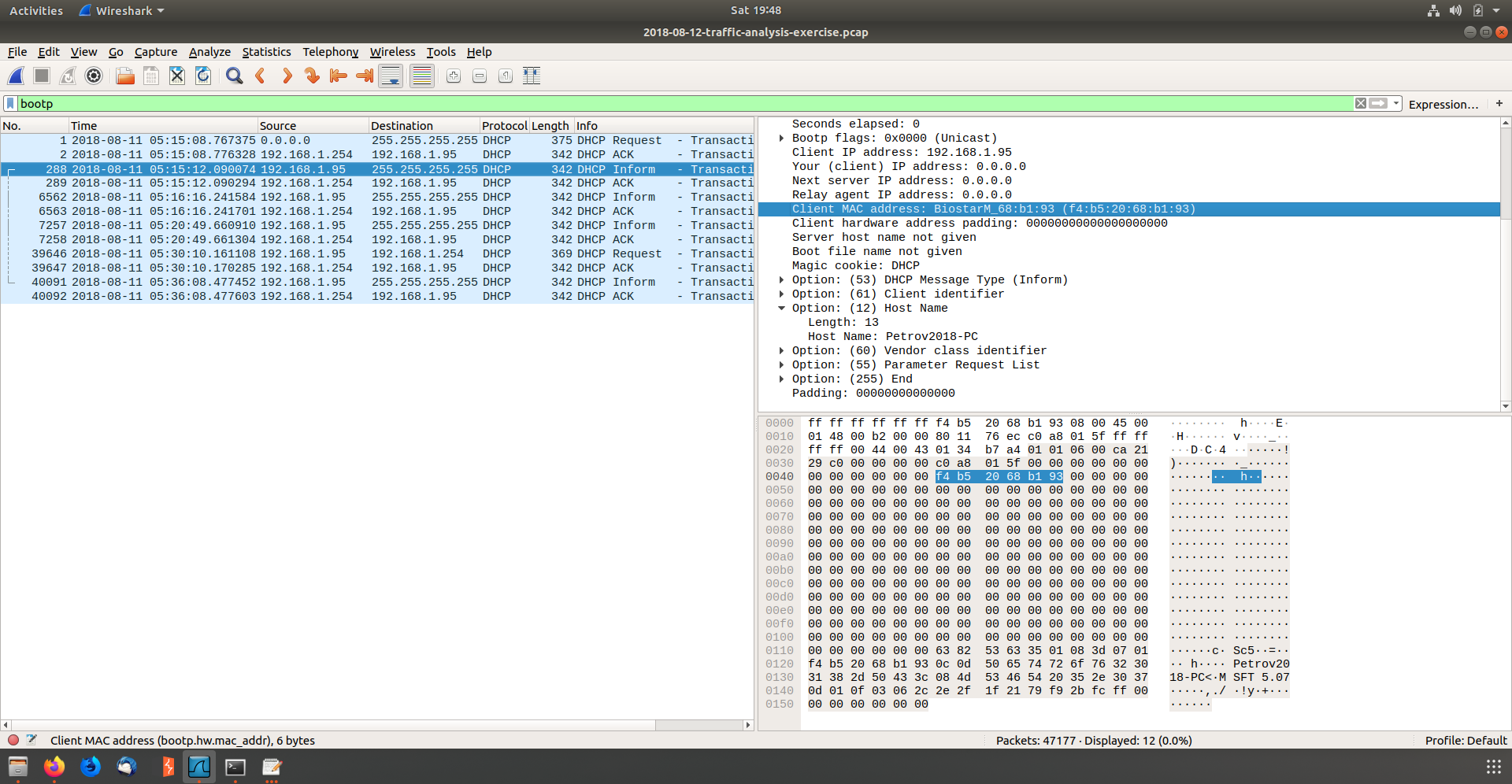
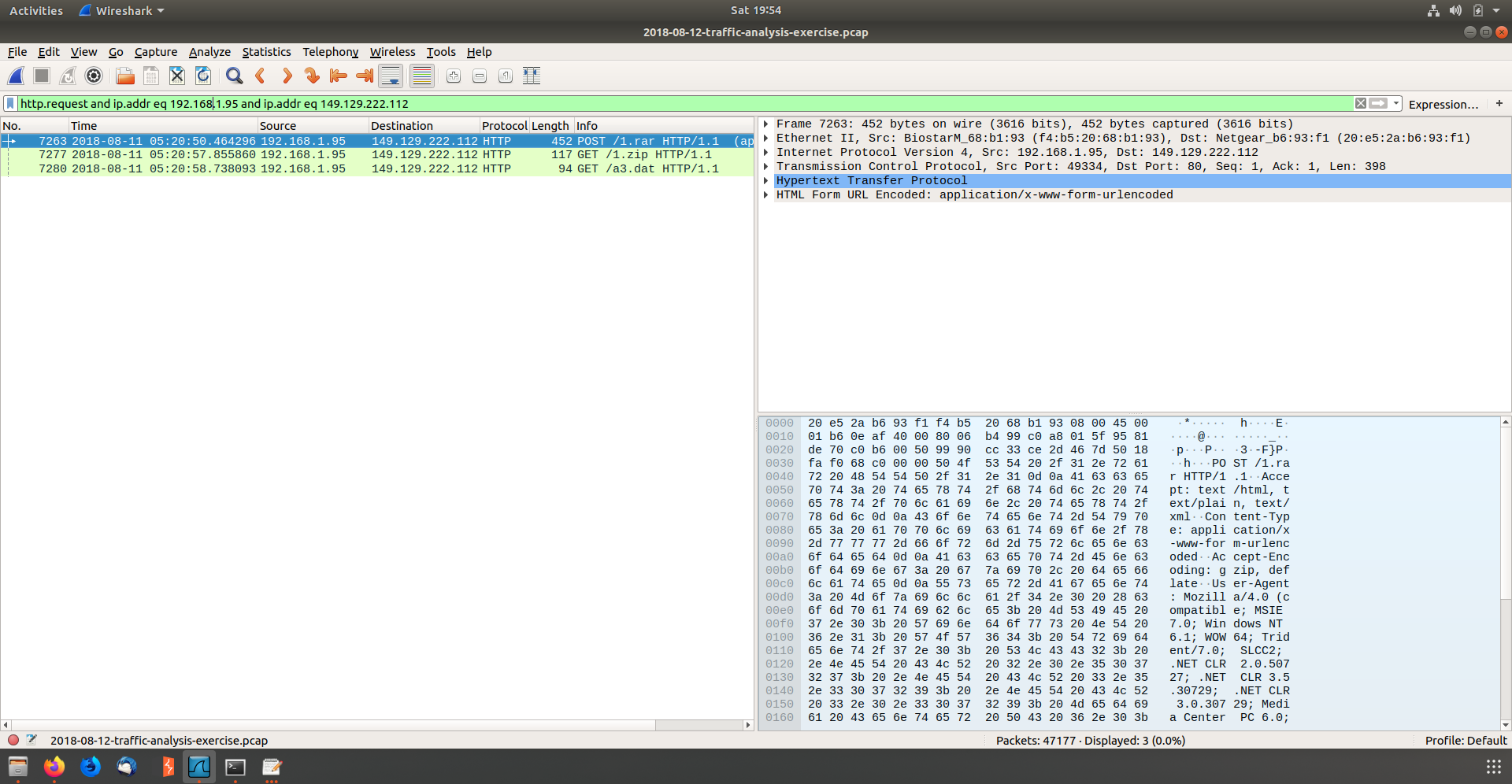
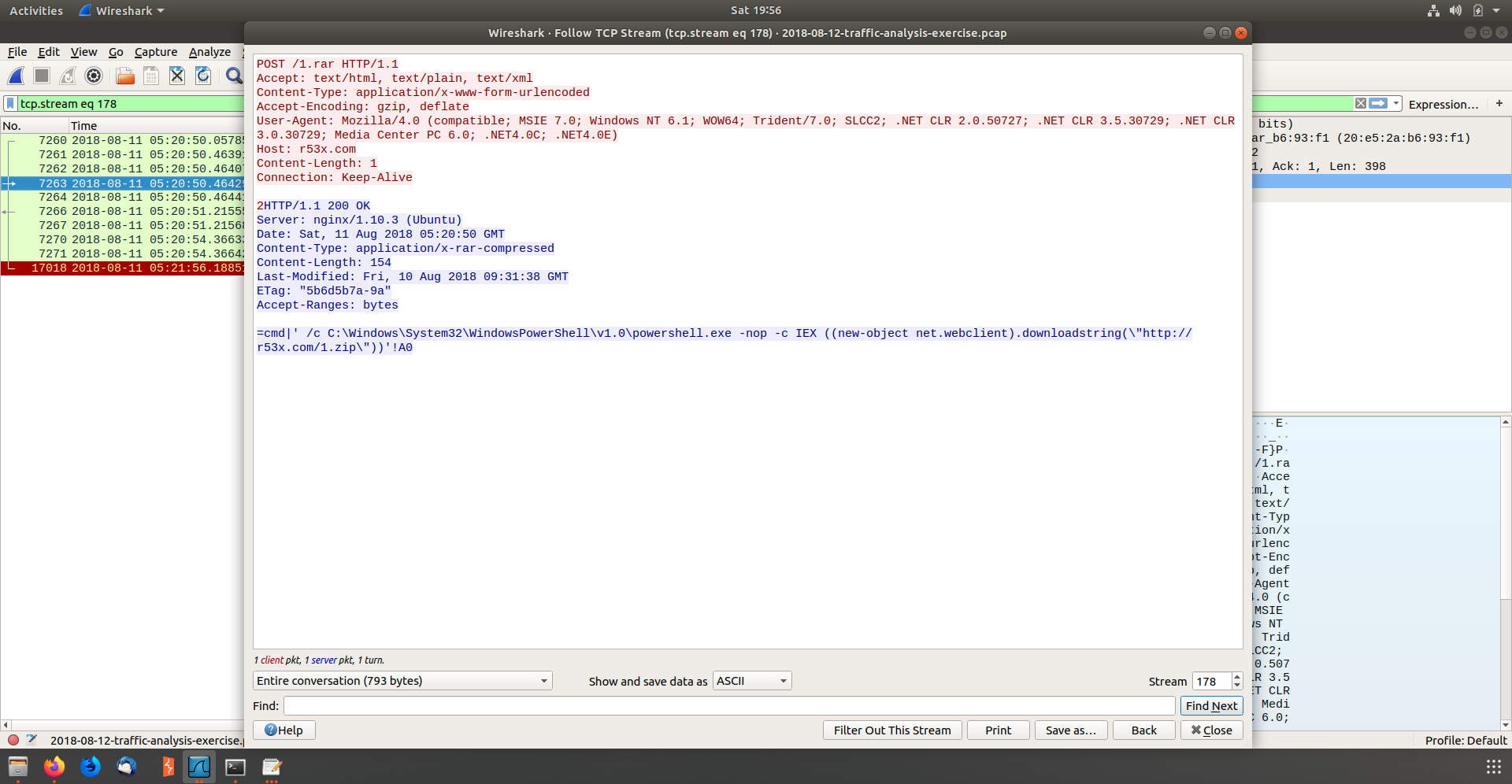
|  |  |
| --- | --- |
| Date of investigation | 2-29-20 |
| Date of incident | 8-11-2018 @ 6:16:22 UTC |
| Outcome | True Positive, 2 different types of malware were found |
| Action Taken | Identified malware and attacking host  Advised on firewall rules  Advised on restoring backups |
| Reporting Tool | Snort, Suricata |
| Attack Vector (Web, Email, Network, etc…) | Web Malware Download |
| Source IP/ Email | 149.129.222.112:80 |
| Source port | 80 |
| Destination IP/ Email | 10.8.11.10:49162 |
| Destination port | 49162 |

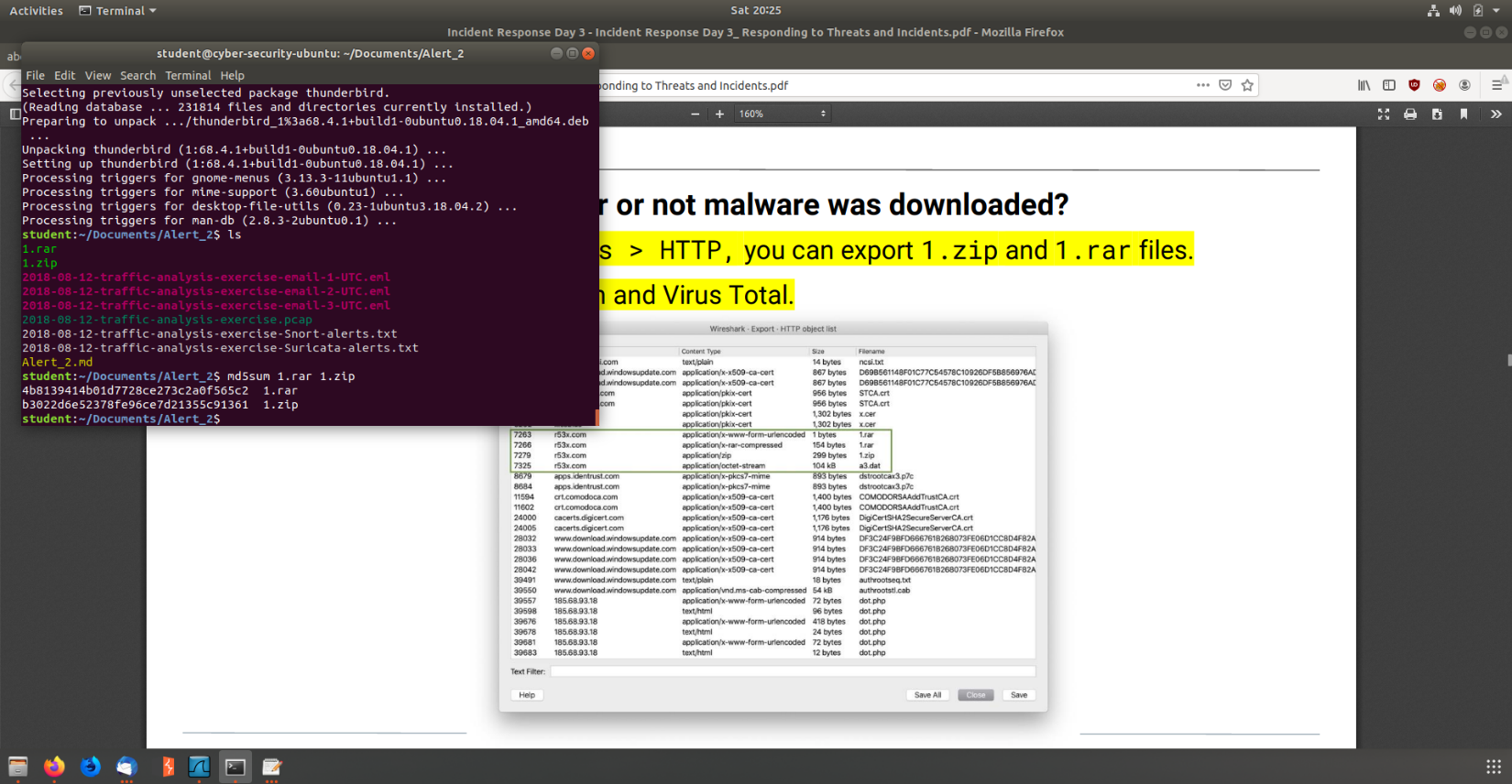
Narrative

* Alerted by Snort & Suricata
  + ET POLICY Binary Download Smaller than 1 MB Likely Hostile
  + ET POLICY PE EXE of DLL Windows file download HTTP
  + MALWARE\_OTHER HTTP POST request to a RAR file [\*\*]
* Located source/ destination ip
  + src/prt: 149.122.122:80
  + dst/prt: 10.8.1.10:49162
* identified hostname and MACAddress of infected computer
  + MAC: f4:b5:20:68:b1:93
  + Host name: Petrov2018-PC



* Identified the time that the attack took place
* Followed the TCP and found 1.zip and 1.rar was downloaded



* Exported HTTP Objects and Hashed
  + Md5sum hash:
    - 4b813941b01d778ce27c2a0f565c2 1.rar
    - b3022d6e52378fe96ce7d21355c91361 1.zip
* Uploaded the Hash to virus total and found a combination of 30 engines detected the file

