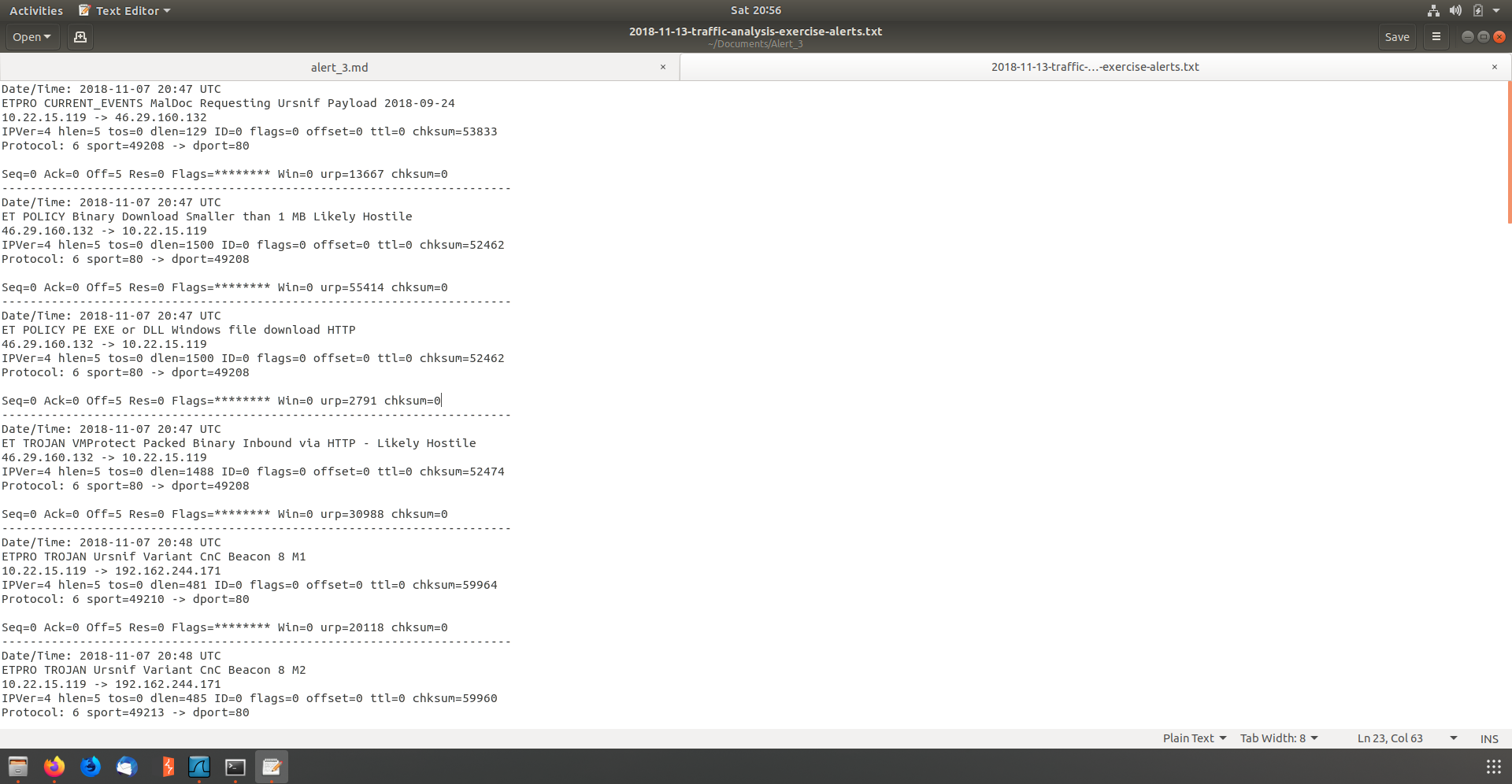
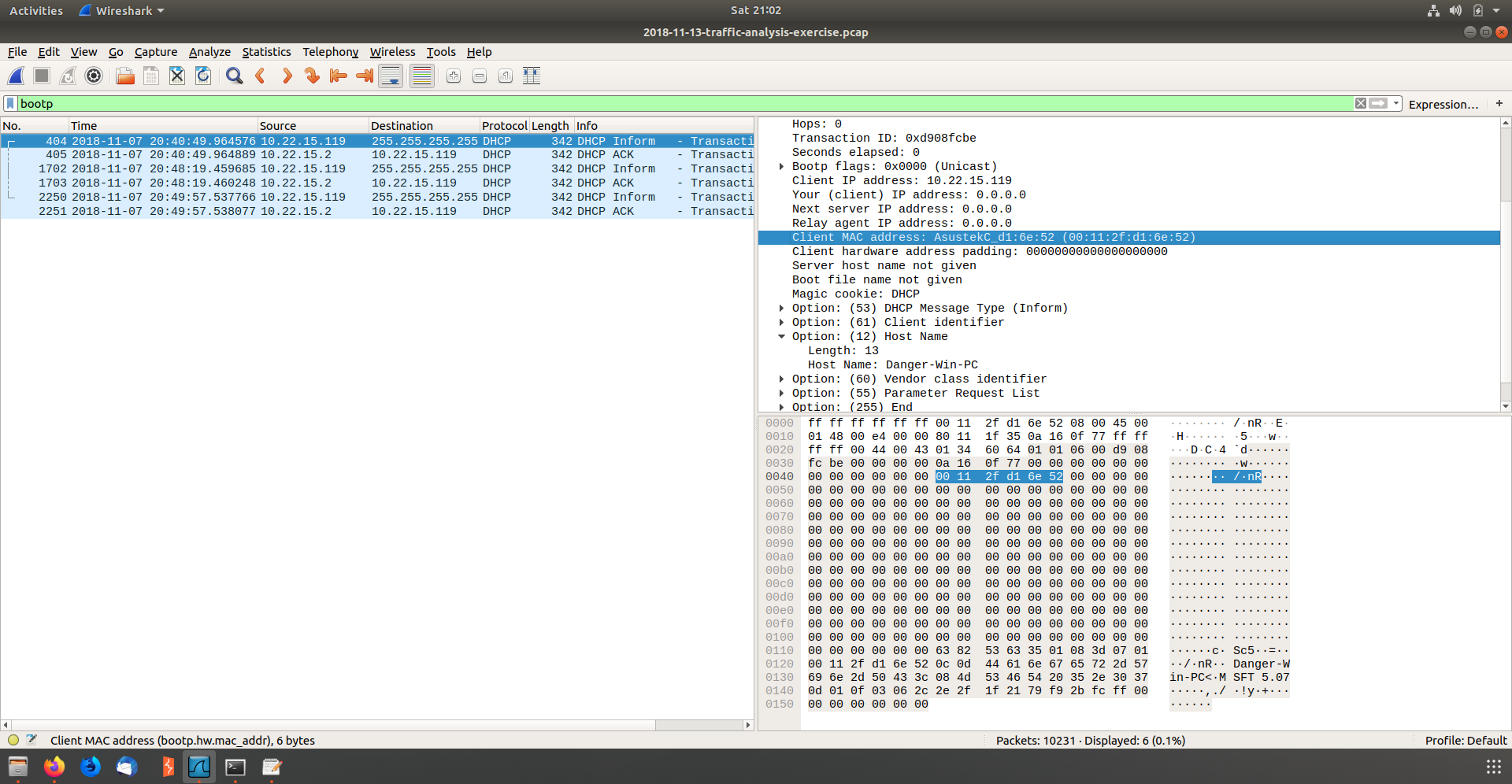
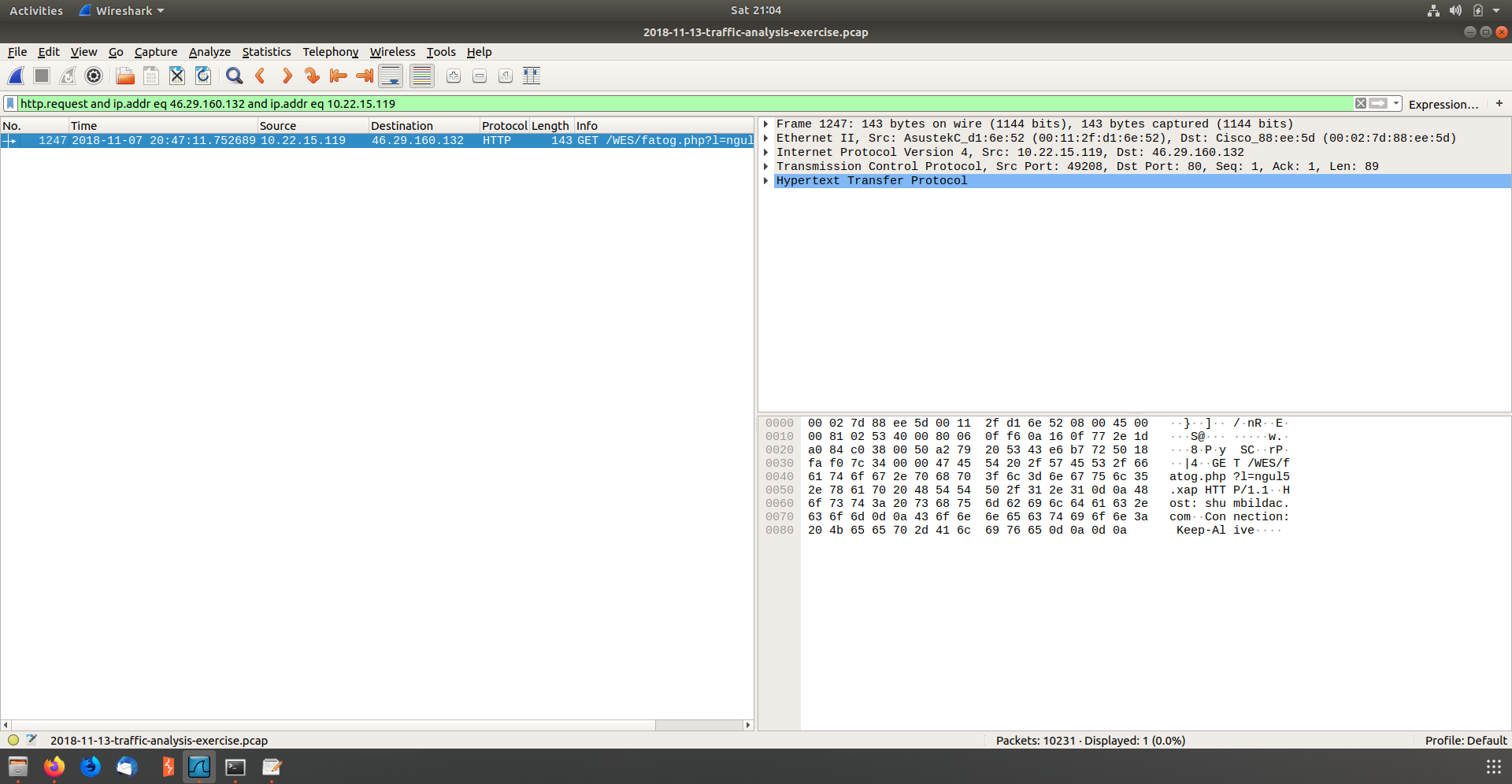
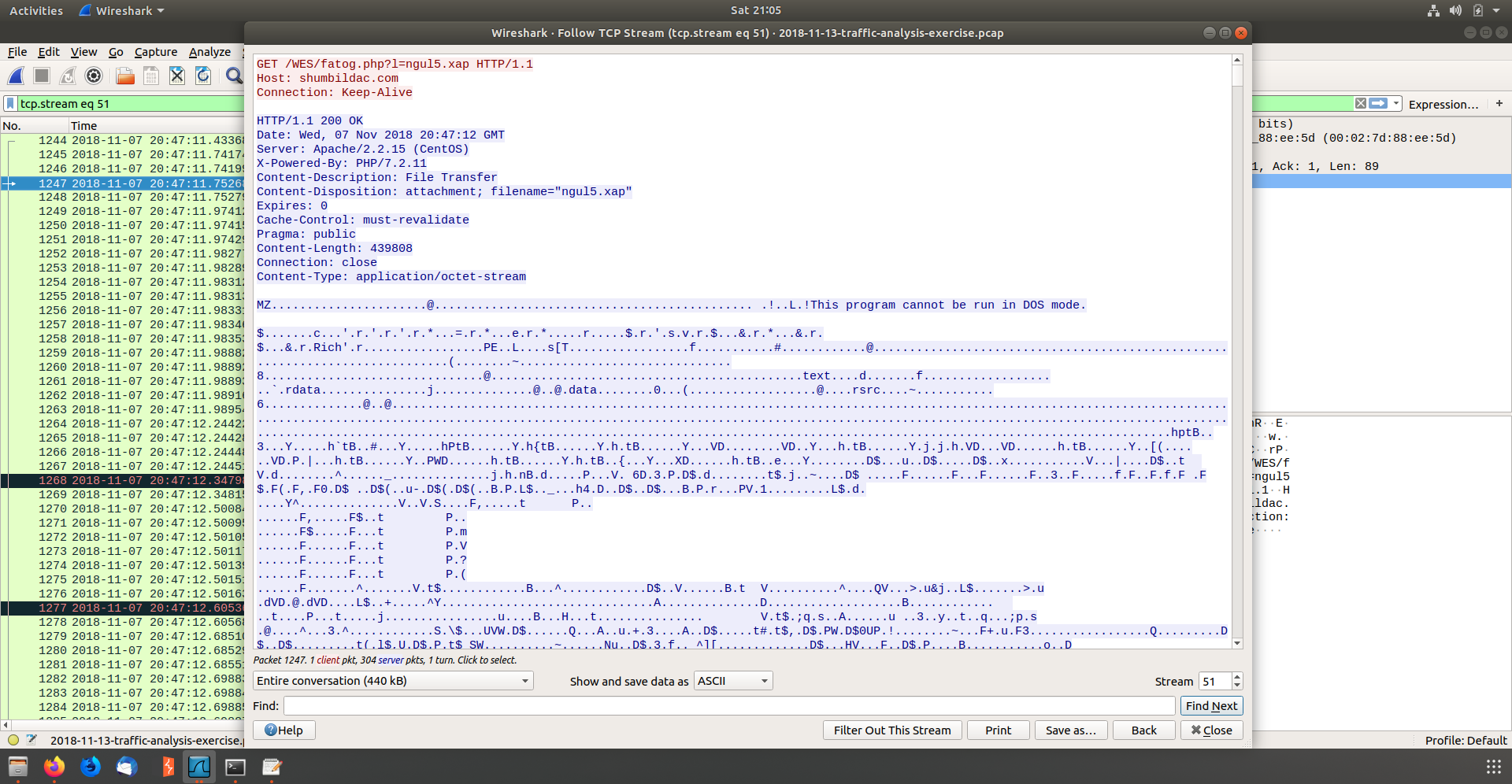
|  |  |
| --- | --- |
| Date of investigation | 3-1-20 |
| Date of incident | 11-7-2018 @ 20:47 UTC |
| Outcome | True Positive Malware was downloaded onto the PC |
| Action Taken | Identified Malware and infected host  Advised on firewall rules  Advised on restoring backups |
| Reporting Tool | Snort |
| Attack Vector (Web, Email, Network, etc…) | Web Malware Download |
| Source IP/ Email | 46.29.168.132:80 |
| Source port | 80 |
| Destination IP/ Email | 10.22.15.119:49208 |
| Destination port | 49208 |

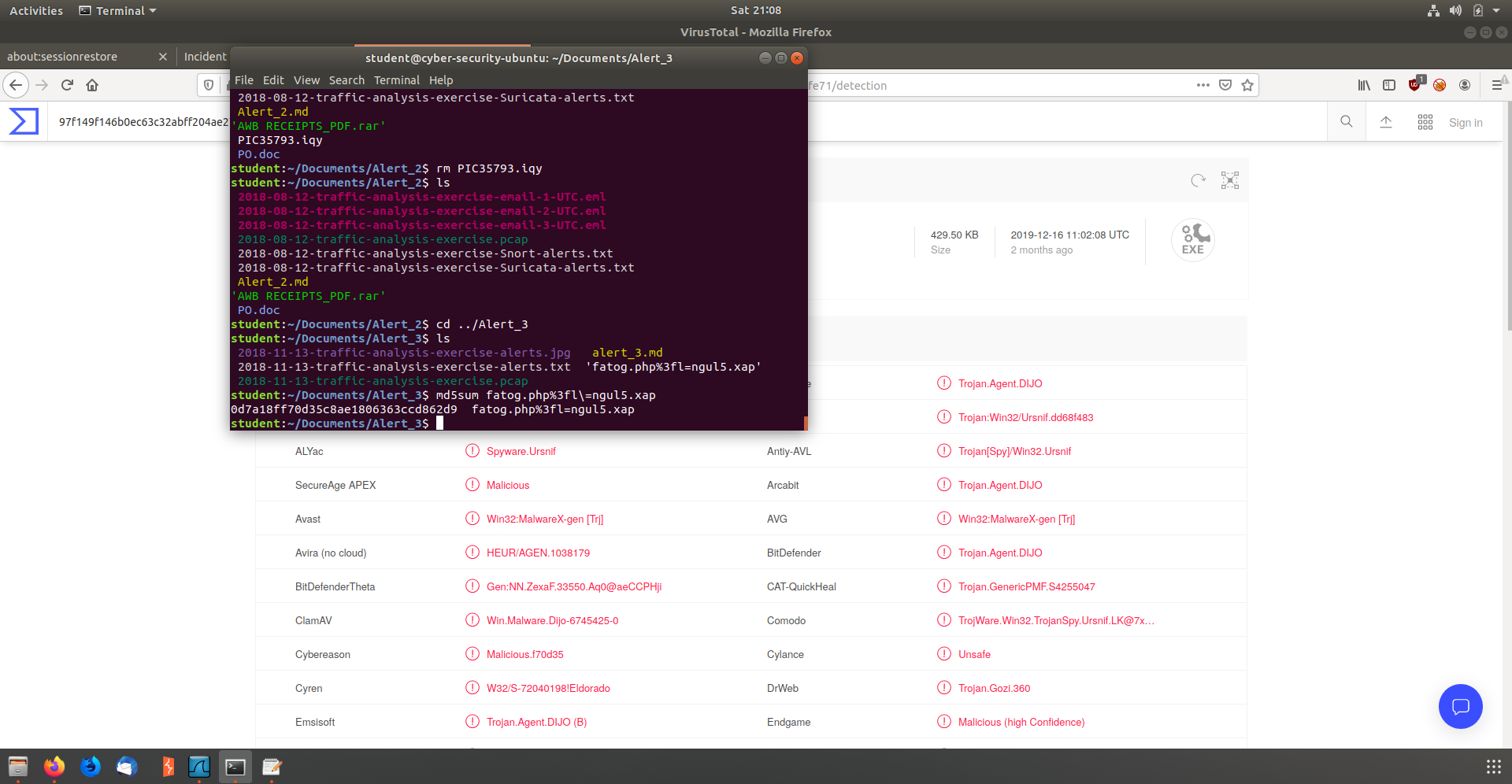
Narrative

* Alerted by Snort
  + ETPRO CURRENT\_EVENTS MaDoc Requesting Ursnif Payload 2018-09-24
  + ET POLICY Binary Download Smaller than 1 MB Likely Hostile
  + ET TROJAN VMProtect Packed Binary Inbound via HTTP – Likely Hostile
* located source/ destination ip
  + src/prt: 49.29.168.132:80
  + dst/prt: 10.22.15.119:49208
* identified hostname and MACAddress of infected computer
  + MAC: 00:11:2f:d1:6e:52
  + Host name: Danger-win-PC



* Identified the time that the attack took place
* Followed the TCP and found fatog.php?1=ngul5.xap was downloaded



* Exported HTTP Objects and Hashed
  + Md5sum hash: 0d7a18ff70d35c8ae1806363ccd862d9
* Uploaded the Hash to virus total and found 59 engines detected the file

