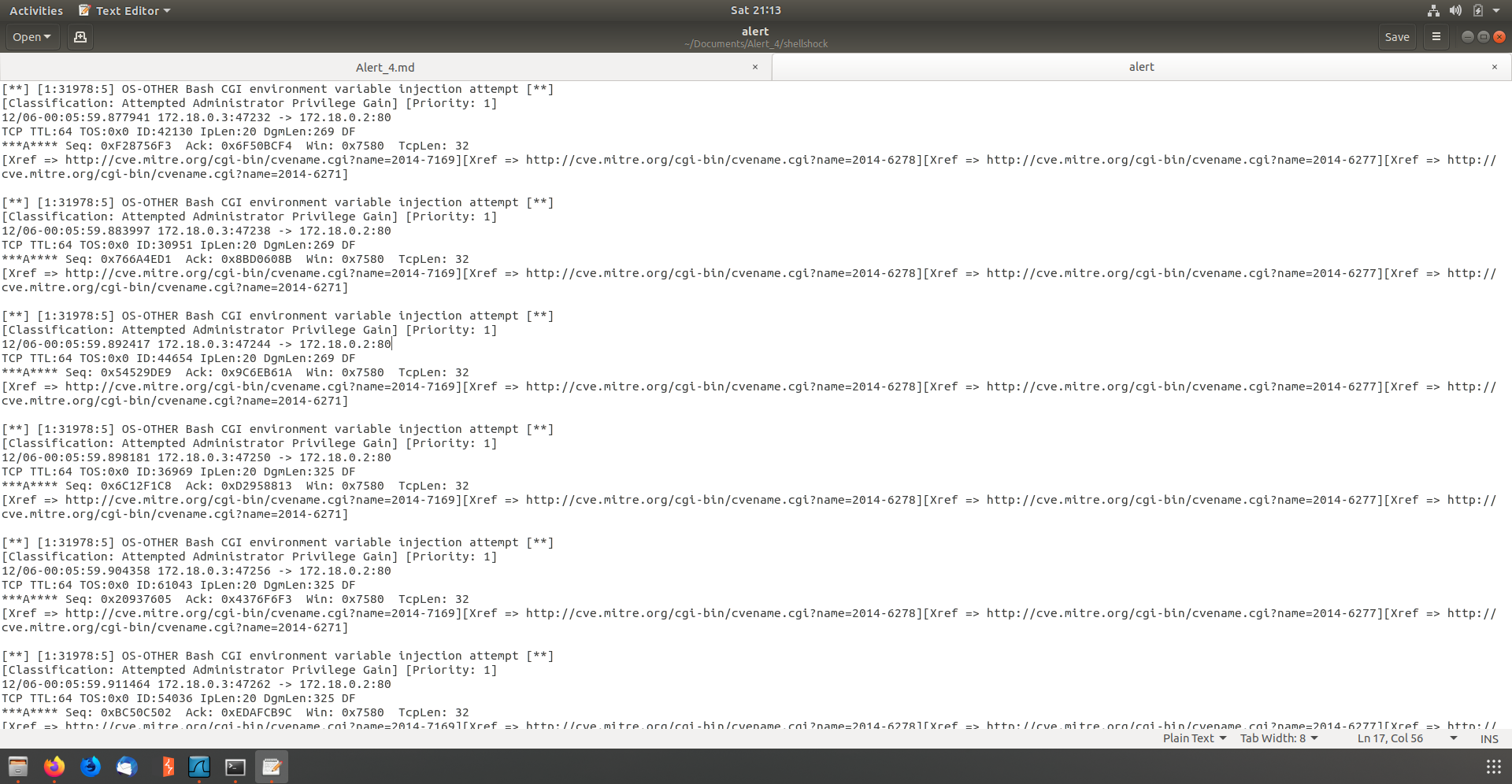
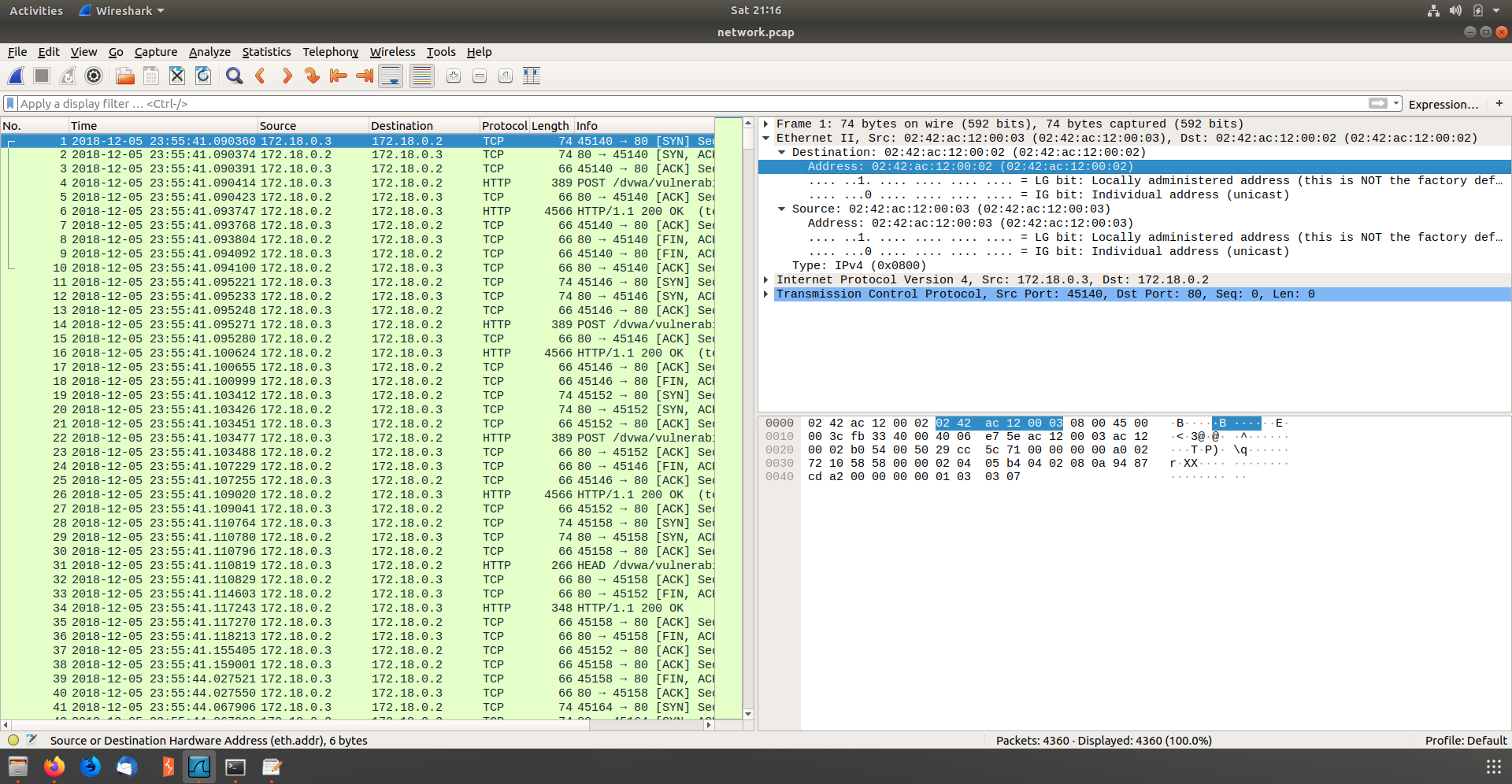
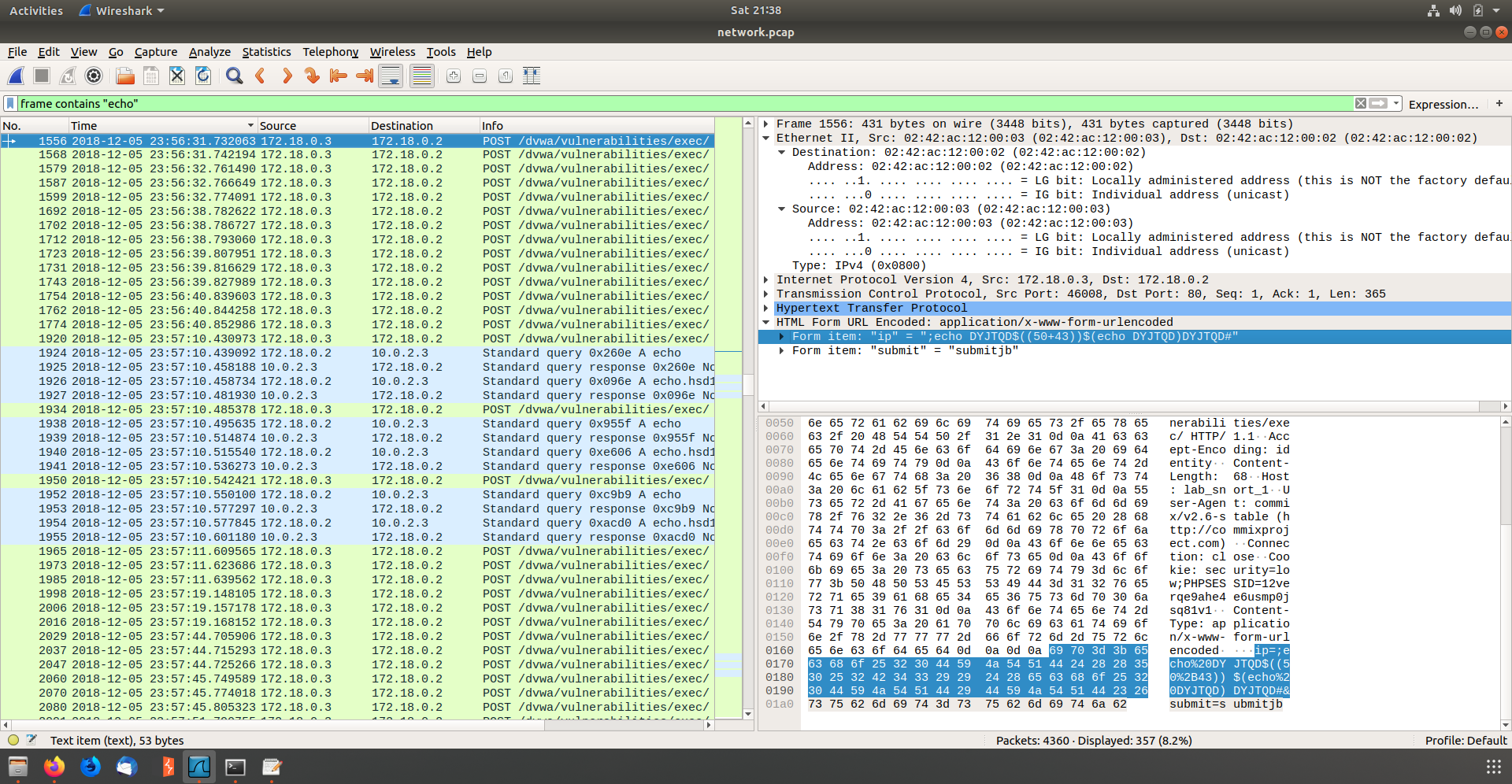
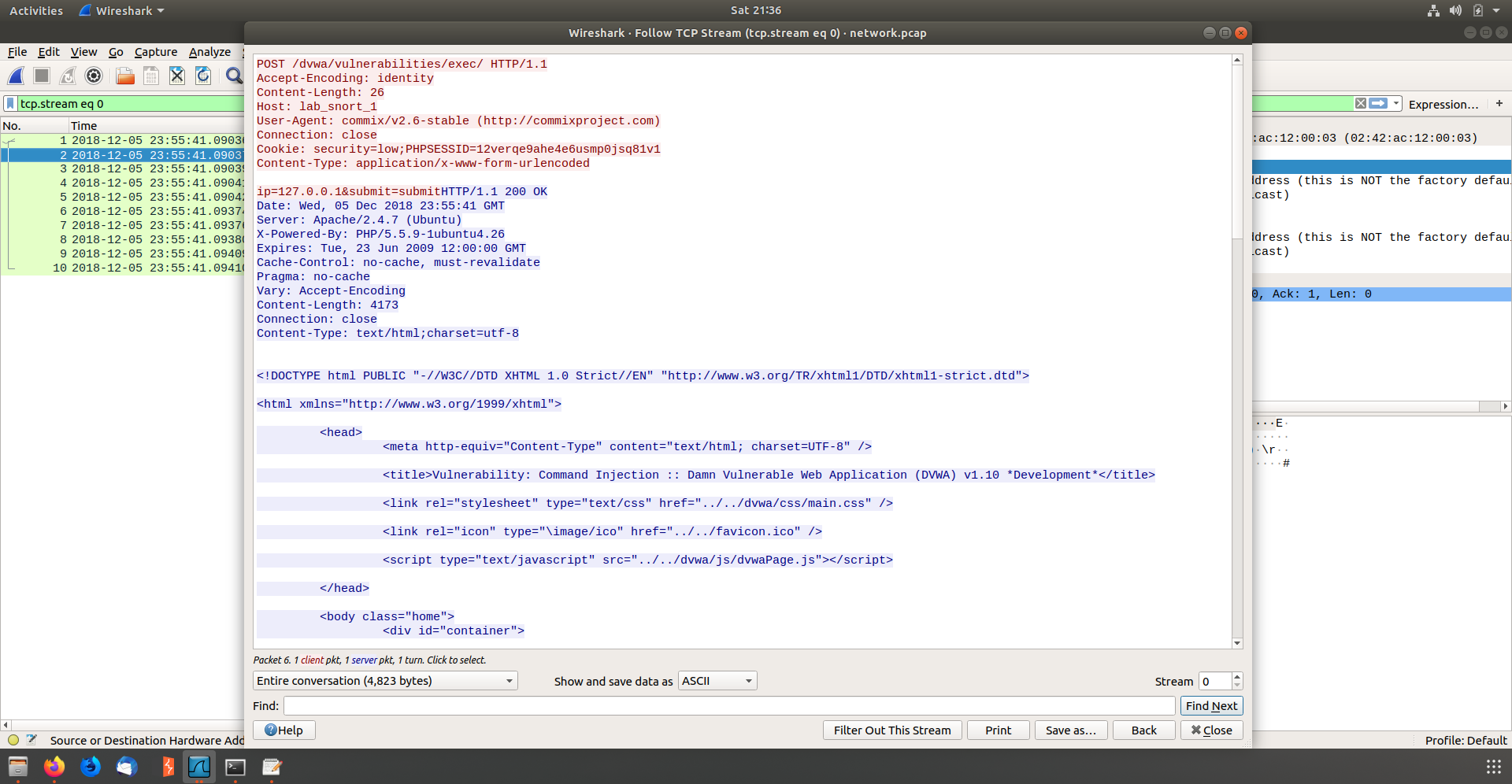
|  |  |
| --- | --- |
| Date of investigation | 3-1-20 |
| Date of incident | 12-5-2018 @ 23:55:41 UTC |
| Outcome | Detected a Command Injection attempt |
| Action Taken | Identified an attempt to gain Administrator Privilege  Advised on firewall rules  Advised on changing credentials |
| Reporting Tool | Snort |
| Attack Vector (Web, Email, Network, etc…) | Network Attack |
| Source IP/ Email | 172.18.0.3:47232 |
| Source port | 47232 |
| Destination IP/ Email | 172.18.0.2:80 |
| Destination port | 80 |

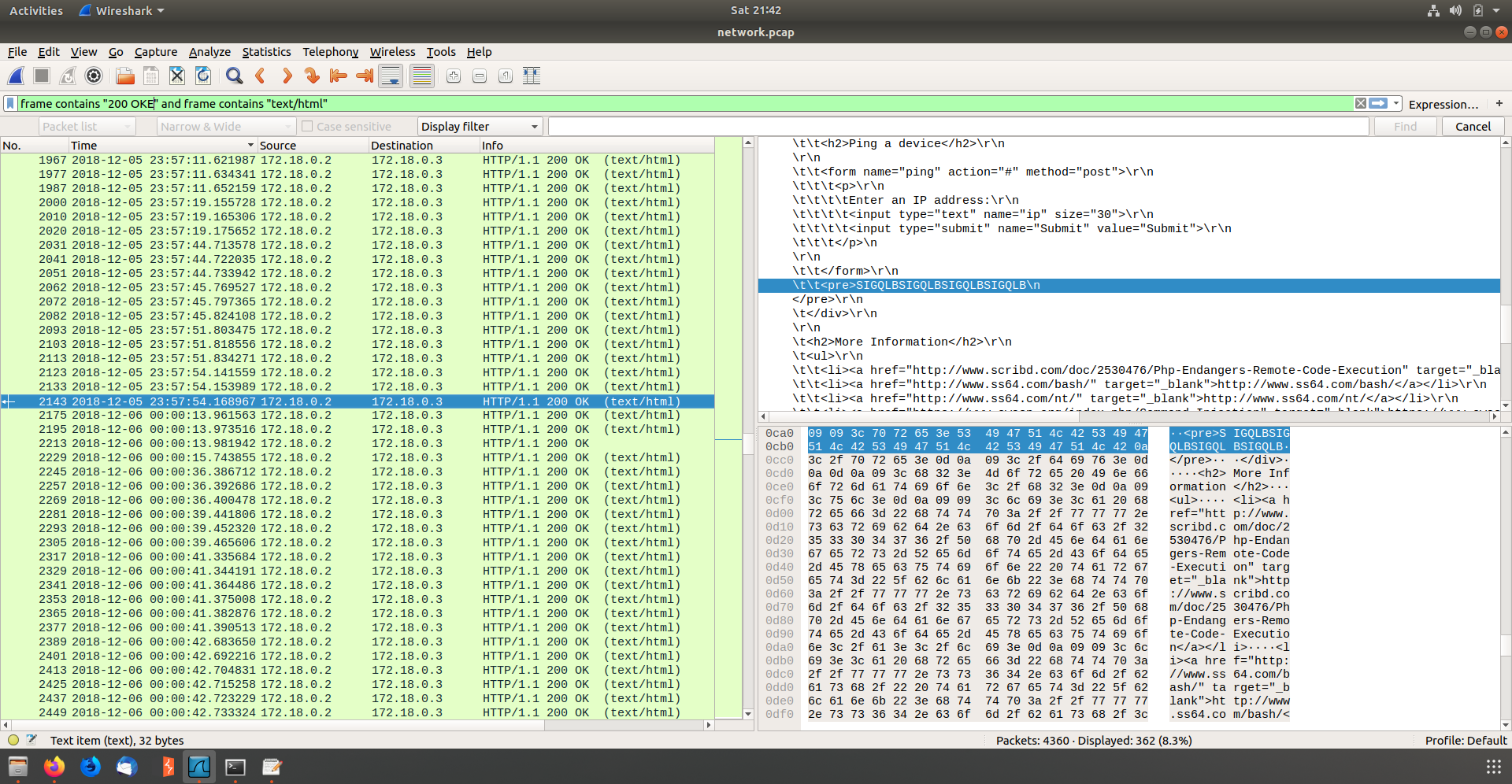
Narrative

* Alerted by Snort
  + [\*\*] [1:31978:5] OS-OTHER Bash CGI Environment variable injection attempt [\*\*]
  + [Classification: Attempted Administraor Privilege Gain] [Priority:1]
* located source/ destination ip
  + src/prt: 172.18.0.3:47232
  + dst/prt: 172.18.0.2:80
* Identified MACAddresses of both computers
  + Attacker: MAC: 02:42:ac:12:00:03
  + Victim: MAC: 02:42:ac:12:00:02



* Identified the time that the attack took place
* Identified Code injection attempt
* Followed the TCP and it confirms the code injection attempt



* Identitifed the result of the code injection