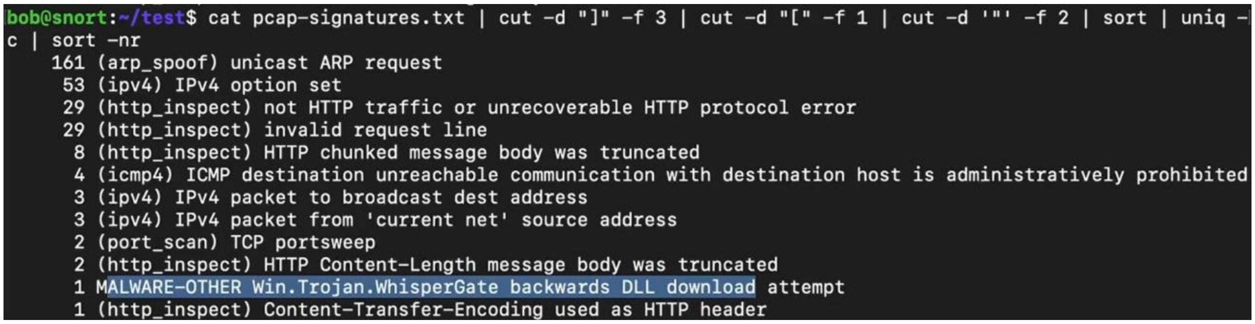
Detect potentially malicious activity

Problem – detect potentially malicious activity

Goal: find malware alerts from a signature

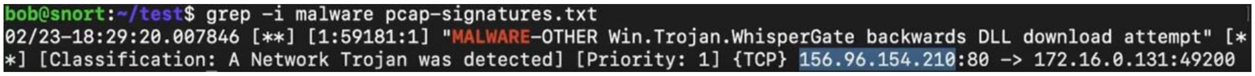
Process:

- extract relevant field and sort descending on the numeric field: found malware



```
bob@snort:~/test$ cat pcap-signatures.txt | cut -d "]" -f 3 | cut -d "[" -f 1 | cut -d '"' -f 2 | sort | uniq -
c | sort -nr
    161 (arp_spoof) unicast ARP request
     53 (ipv4) IPv4 option set
     29 (http_inspect) not HTTP traffic or unrecoverable HTTP protocol error
     29 (http_inspect) invalid request line
      8 (http_inspect) HTTP chunked message body was truncated
      4 (icmp4) ICMP destination unreachable communication with destination host is administratively prohibited
      3 (ipv4) IPv4 packet to broadcast dest address
      3 (ipv4) IPv4 packet from 'current net' source address
      2 (port_scan) TCP portsweep
      2 (http_inspect) HTTP Content-Length message body was truncated
      1 MALWARE-OTHER Win.Trojan.WhisperGate backwards DLL download attempt
      1 (http_inspect) Content-Transfer-Encoding used as HTTP header
```

- Identify the malware traffic characteristics



```
bob@snort:~/test$ grep -i malware pcap-signatures.txt
02/23-18:29:20.007846 [**] [1:59181:1] "MALWARE-OTHER Win.Trojan.WhisperGate backwards DLL download attempt" [*
*] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 156.96.154.210:80 -> 172.16.0.131:49200
```

- Use Wireshark to analyze the IP address highlighted above