Incident Response

Analysis of a Vulnerable Network

Presented by:
Edward Cruz and Clement Yang

Table of Contents

This document contains the following resources:

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205, 185.243.115.84, 166.62.111.64, 172.16.4.205	Machines that sent the most traffic.
Most Common Protocols	TCP (87.7%) UDP (12.2%) TLS (11.5%)	Three most common protocols on the network.
# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	10.6.12.0/24 172.16.4.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	1 (june11.dll)	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Browsing blogs, reading the news, checking emails

Suspicious Activity

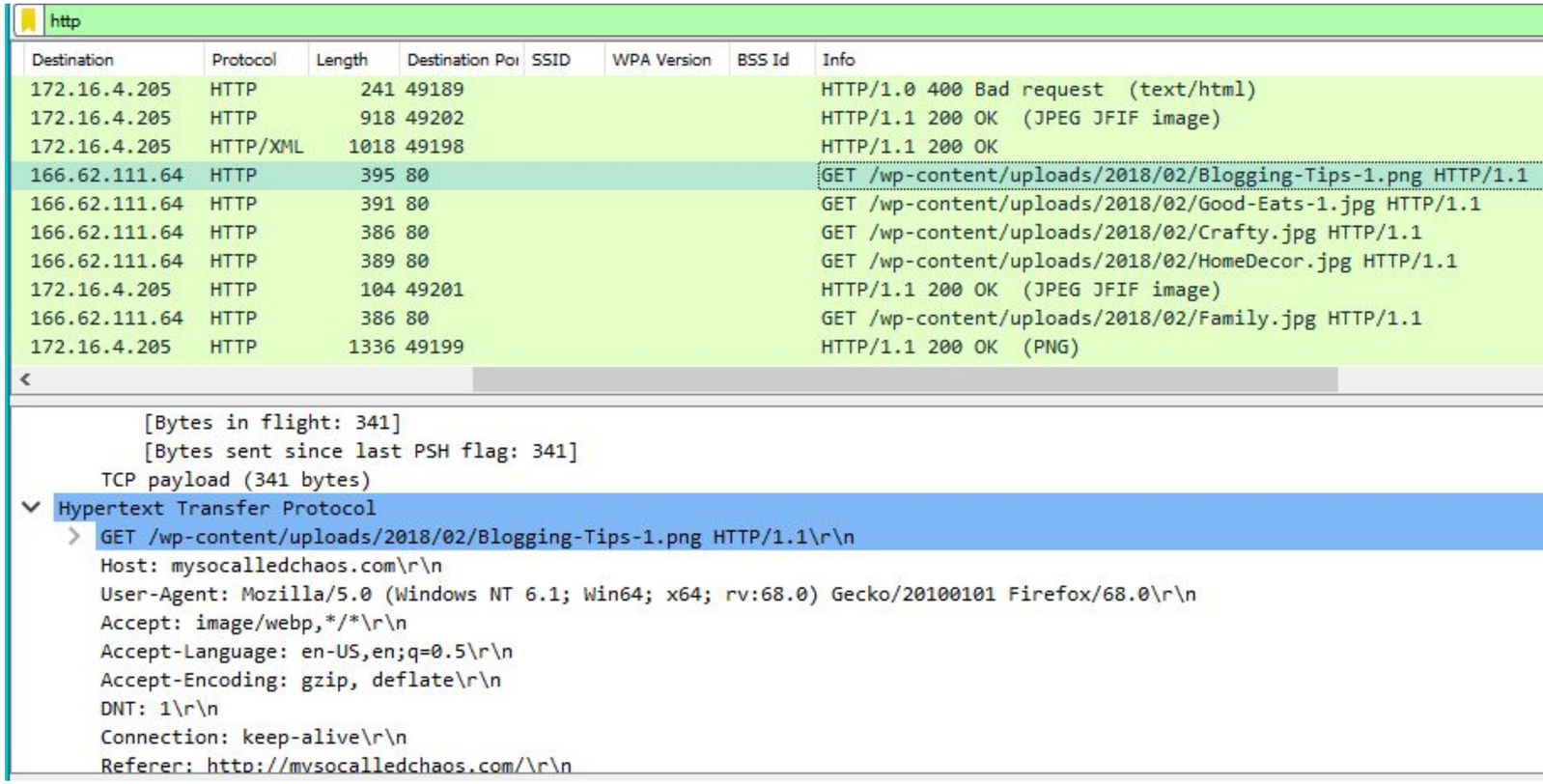
- Setting up an private Active Directory to watch YouTube videos at work, downloading malicious Trojan malware, and torrenting illegal/copyrighted content.

Normal Activity

Normal Activity: Browsing Blogs

Summarize the following:

- Normal web browsing behavior was observed by filtering through HTTP traffic.
- In one example, the user was browsing a blog site called “mysocalledchaos.com,” which is a blog site run by a mother and lifestyle blogger named Angie.
- An examination of http traffic revealed GET requests for image files named “Blogging-Tips-1.png,” “Good-Eats-1.jpg,” “Crafty.jpg,” and “HomeDecor.jpg,” suggesting that the blog covers lifestyle topics such as food and home decorations.



Normal Activity: Reading the news

Summarize the following:

- Normal browsing activity such as reading the news was detected by filtering for and examining HTTP traffic.
- One user was reading a TIME magazine article and photo essay covering ancient Roman ruins in Libya under Muammar Gaddafi
- An examination of http traffic revealed GET requests for image files including “libya_ruins_01.jpg”

ource	Destination	Protocol	Length	Destination Port	SSID	WPA Version	BSS Id	Info
3.33.255.25	10.11.11.179	HTTP	477	50235				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	450	80				GET /time/rd/trunk/www/web/feds/j/showLinks.js HTTP/1.1
0.11.11.94	52.218.228.130	HTTP	558	80				GET /core/scripts/lrs/tin-can.min.js?_=1573510907652 HTTP/1.1
43.204.29.89	10.11.11.179	HTTP	71	50234				HTTP/1.1 200 OK (text/css)
43.204.29.89	10.11.11.179	HTTP	71	50233				HTTP/1.1 200 OK (text/css)
43.204.29.89	10.11.11.179	HTTP	1343	50237				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	430	80				GET /time/js/photoessay.js HTTP/1.1
0.11.11.179	143.204.29.89	HTTP	448	80				GET /time/assets/js/frequency_capping.min.js HTTP/1.1
0.11.11.179	143.204.29.89	HTTP	457	80				GET /time/rd/trunk/www/web/feds/j/mobileExperience.js HTTP/1.1
43.204.29.89	10.11.11.179	HTTP	769	50236				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	460	80				GET /time/rd/trunk/www/web/feds/j/MobileCompatibility.js HTTP/1.1
43.204.29.89	10.11.11.179	HTTP	78	50232				HTTP/1.1 200 OK (application/javascript)
43.204.29.89	10.11.11.179	HTTP	71	50231				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	445	80				GET /tii/omniture/h/config/time_s_code.js HTTP/1.1
0.11.11.179	143.204.29.89	HTTP	519	80				GET /time/photoessays/2011/libya_ruins/libya_ruins_01.jpg HTTP/1.1

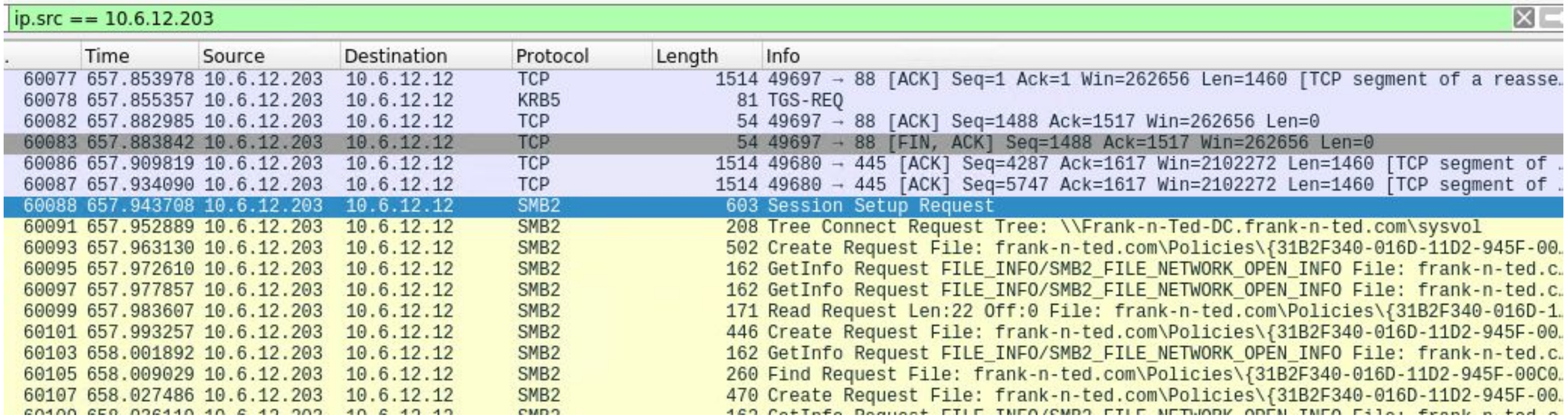
```
    [Bytes sent since last PSH flag: 453]
  TCP payload (453 bytes)
Hypertext Transfer Protocol
  GET /time/photoessays/2011/libya_ruins/libya_ruins_01.jpg HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /time/photoessays/2011/libya_ruins/libya_ruins_01.jpg HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /time/photoessays/2011/libya_ruins/libya_ruins_01.jpg
    Request Version: HTTP/1.1
  Host: img.timeinc.net\r\n
  Connection: keep-alive\r\n
  Accept: image/png,image/svg+xml,image/*;q=0.8,video/*;q=0.8,*/*;q=0.5\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Safari/605.1.15\r\n
  Accept-Language: en-us\r\n
  Referer: http://content.time.com/time/photogallery/0,29307,2077702,00.html\r\n
  Accept-Encoding: gzip, deflate\r\n
  \r\n
  [Full request URI: http://img.timeinc.net/time/photoessays/2011/libya_ruins/libya_ruins_01.jpg]
  [HTTP request 3/4]
```

Malicious Activity

Malicious Activity: Frank-n-Ted Server creation

Summarize the following:

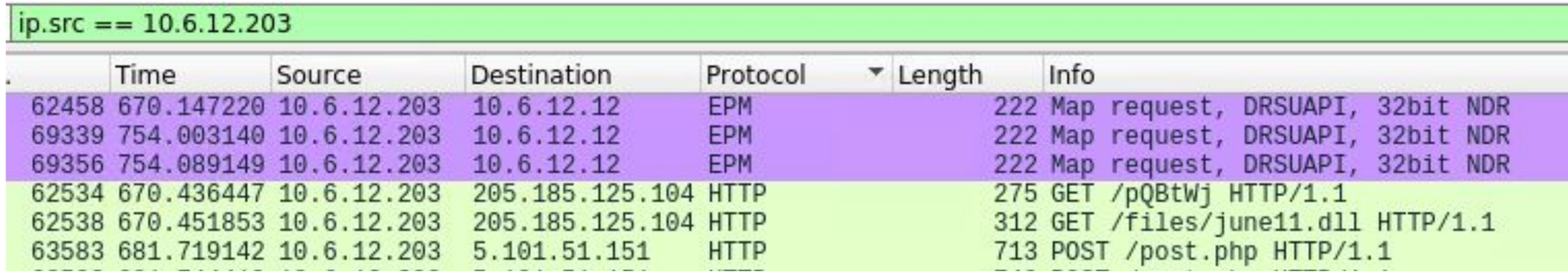
- When observing activity from 10.6.12.12, we saw SMB2 protocols where they requested a Session Setup and Created a Tree Connect Request Tree \\Frank-n-Ted-DC.frank-n-ted.com\sysvol
- These sessions identify that this user was creating a server for the site frank-n-ted.com.

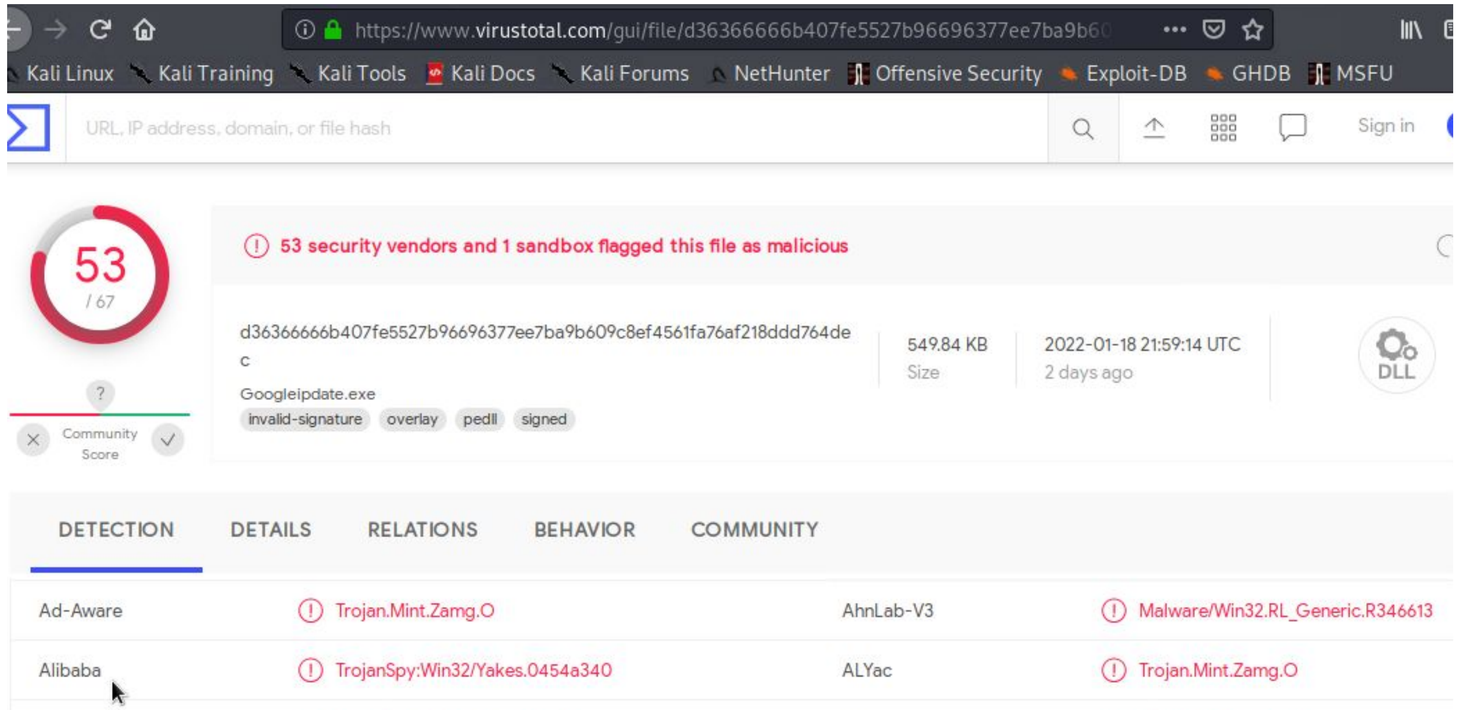


Malicious Activity: Downloading Trojan/Malware

Summarize the following:

- When observing traffic from 10.6.12.203, we noticed HTTP traffic where they requested to download a file from 205.185.125.104.
- The file in question was the called ‘june11.dll’, which when run through Virustotal.com, showed it was malicious.
- The Trojan found is named: Trojan.Mint.Zamg.O

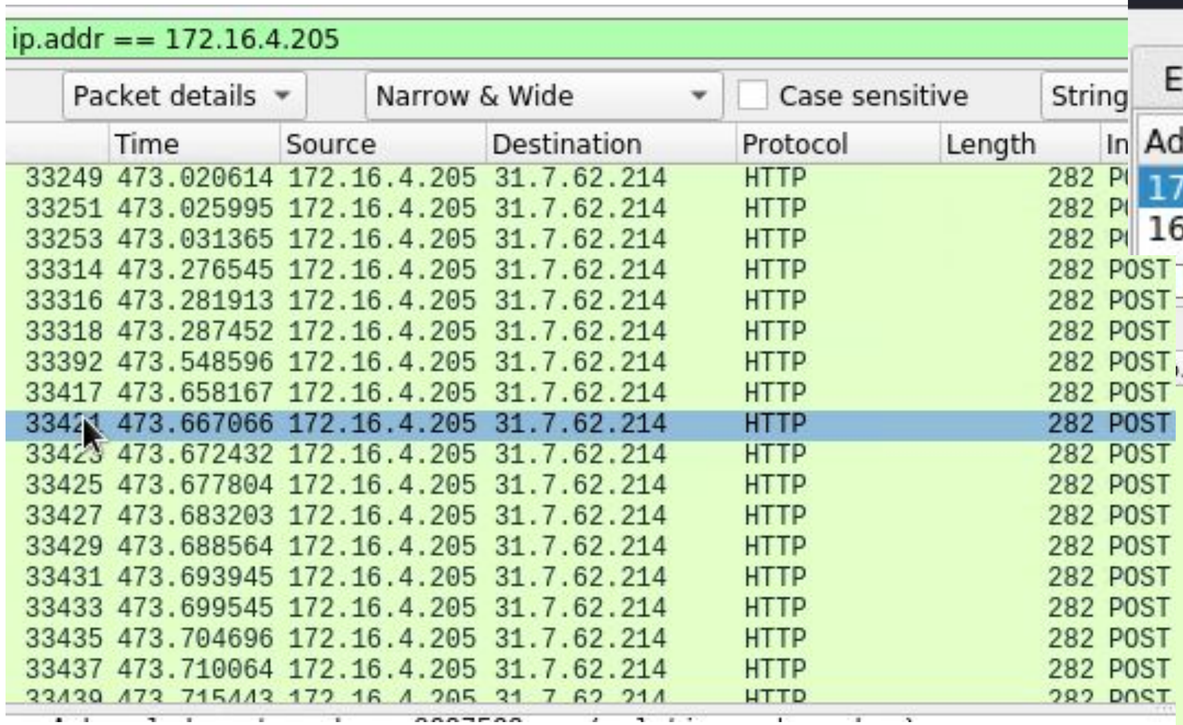


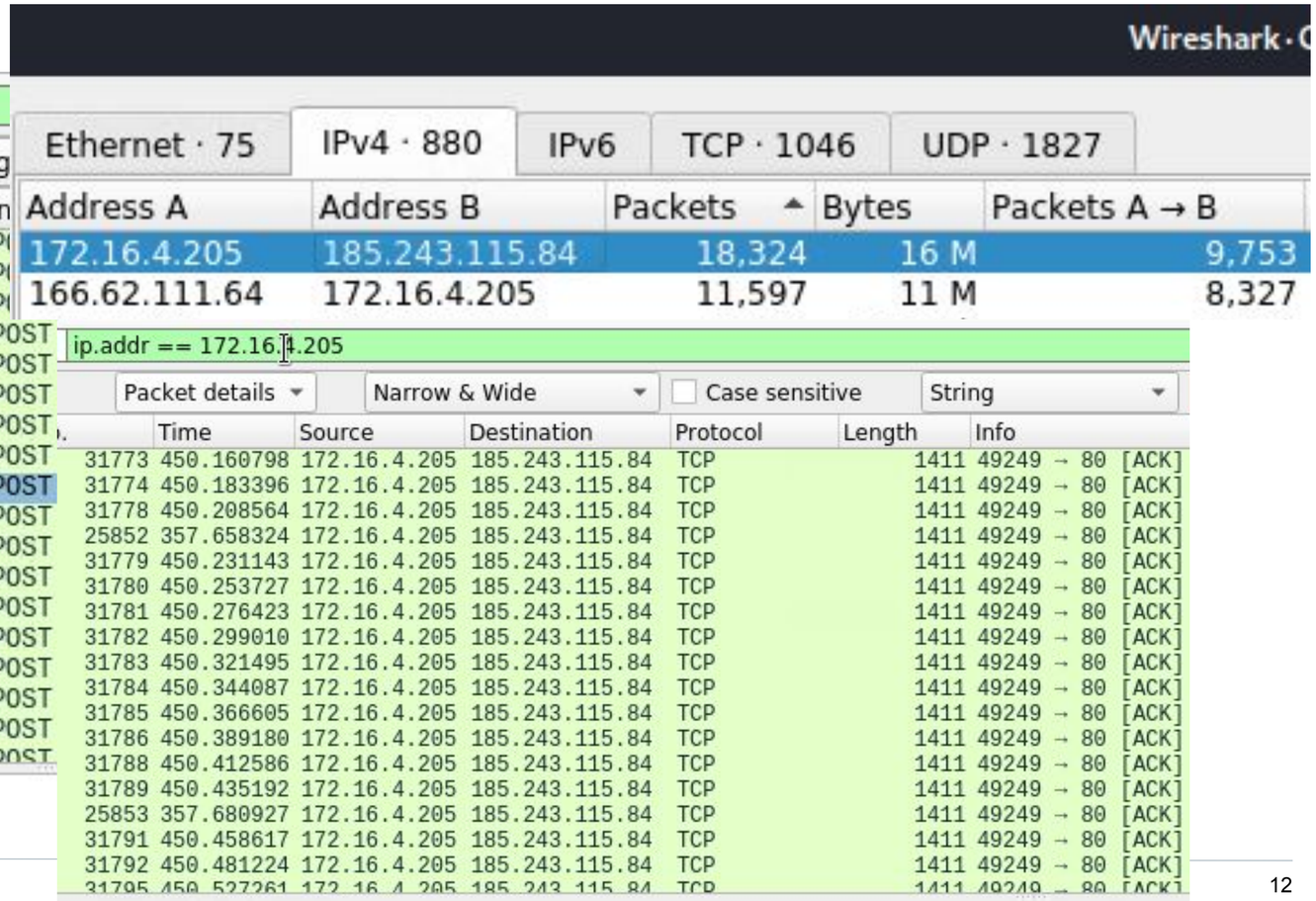


Malicious Activity: Infected Traffic

Summarize the following:

- We observed a large amount of suspicious HTTP and TCP traffic communicating with 172.16.4.205.
- The users PC was infected and requesting several POST methods and ACK flags, which is not normal activity within a short timespan.





Malicious Activity: Torrenting Copyrighted File

Summarize the following:

- When observing traffic from 10.0.0.201 we noticed HTTP and BitTorrent traffic.
- The user was requesting to download an AVI.Torrent file from http://www.publictorrents.com