Final Engagement

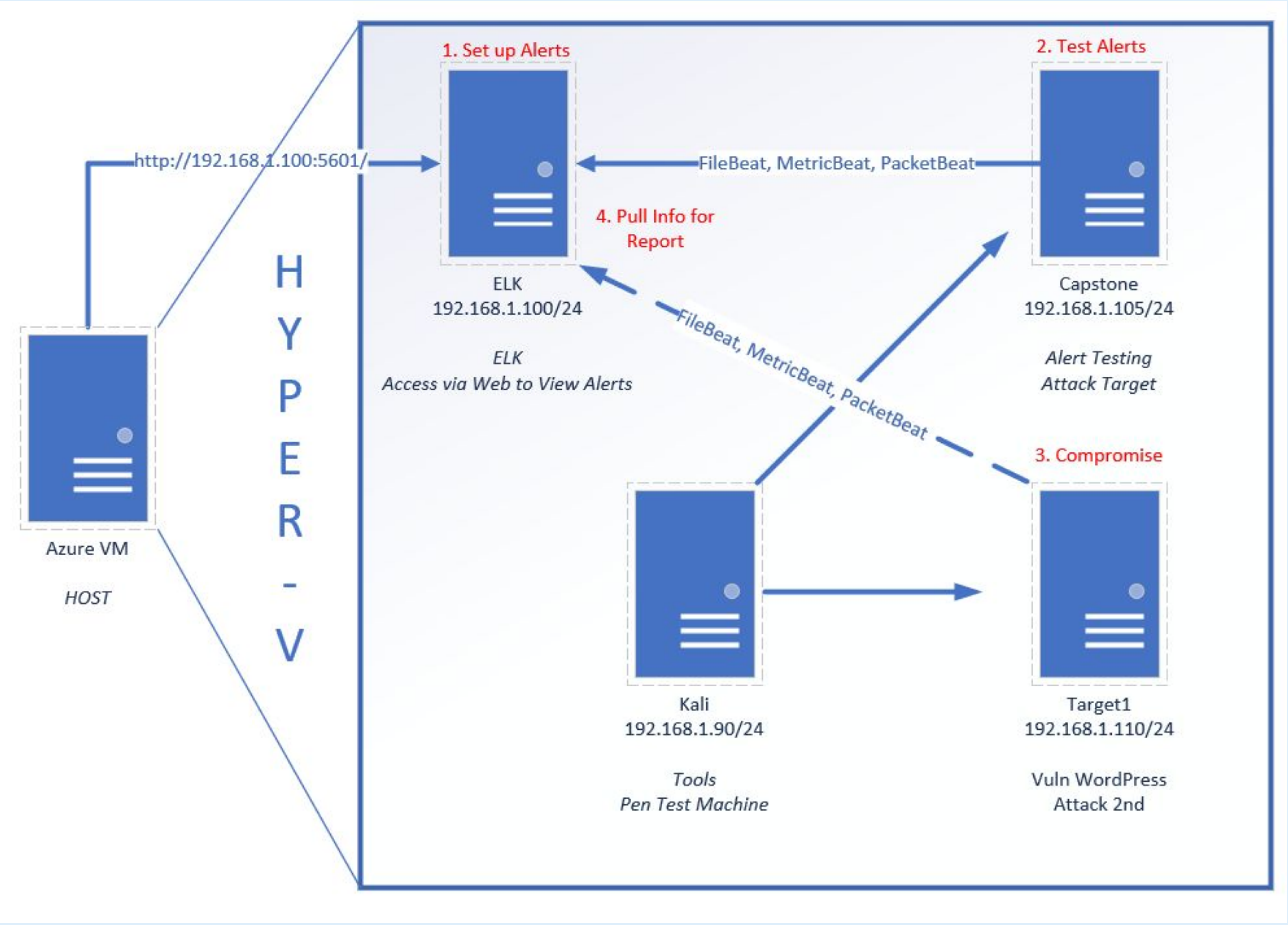
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: **255.255.255.0**
Gateway: **192.168.1.1**

Machines
IPv4: **192.168.1.105**
OS: **Linux**
Hostname: **Capstone**

IPv4: **192.168.1.90**
OS: **Linux**
Hostname: **Kali**

IPv4: **192.168.1.110**
OS: **Linux**
Hostname: **Target 1**

IPv4: **192.168.1.100**
OS: **Linux**
Hostname: **ELK**

Critical Vulnerabilities on the Network

Our assessment uncovered the following critical vulnerabilities on the host network.

Vulnerability	Description	Impact
june11.dll	A Trojan was downloaded from a streaming service.	The malware file was downloaded, thereby compromising the target machine.
Illegal torrenting	A user has been illegally streaming torrents on the network.	These torrent files could compromise network security if they have hidden viruses/malware.

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	224.0.0.252, 68.28.31.30, 72.21.80.5, 204.13.250.136	Machines that sent the most traffic.
Most Common Protocols	IPV4, TCP, HTTP	Three most common protocols on the network.
# of Unique IP Addresses	879	Count of observed IP addresses.
Subnets	255.255.255.0	Observed subnet ranges.
# of Malware Species	53	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 Youtube videos, browsing the web.

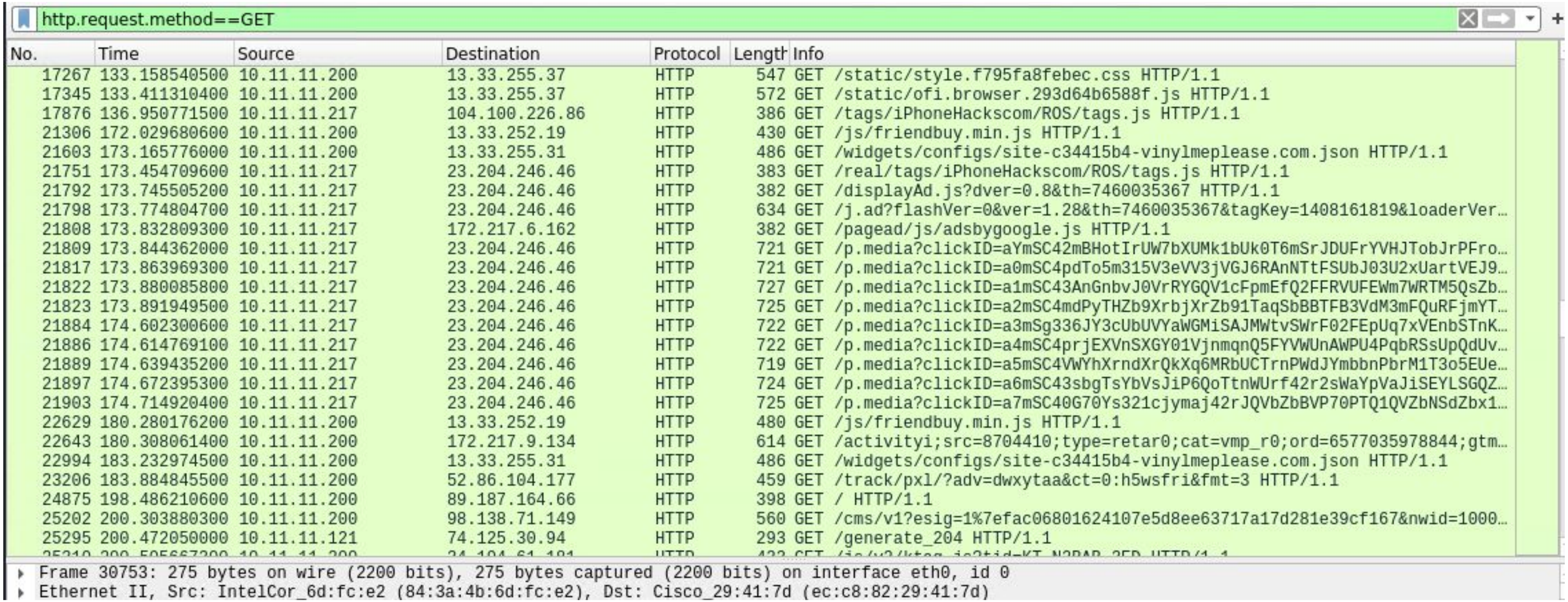
Suspicious Activity

- Downloading june11.dll, illegal torrenting.

Normal Activity

Streaming Youtube videos

- The traffic observed were GET requests using HTTP protocol.
- The user(s) were viewing media, such as streaming Youtube videos.



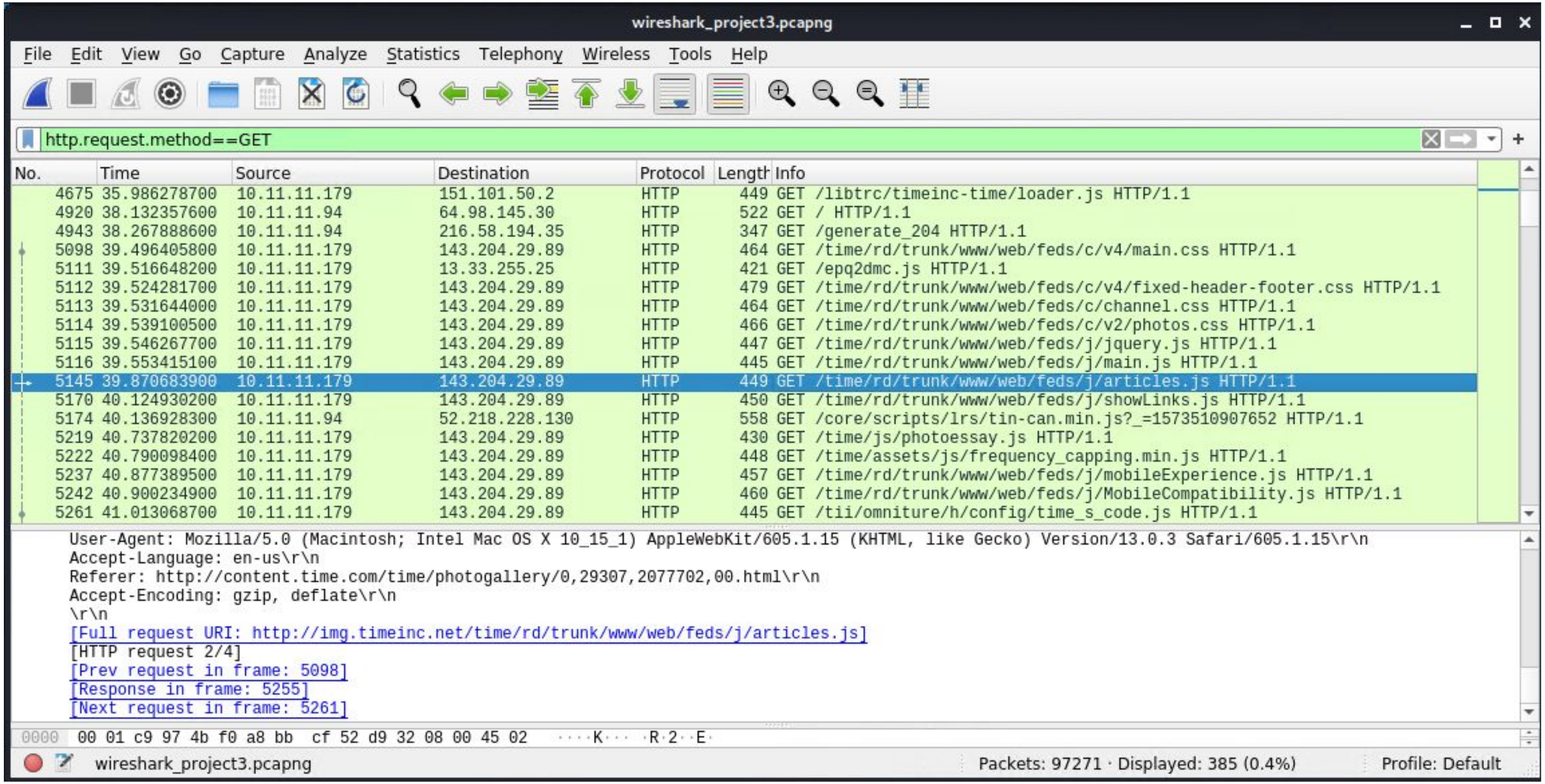
```
http.request.method==GET
```

```
No.     Time          Source          Destination       Protocol  Length Info
  17267 133.158540500 10.11.11.200    13.33.255.37      HTTP      547 GET /static/style.f795fa8febec.css HTTP/1.1
  17345 133.411310400 10.11.11.200    13.33.255.37      HTTP      572 GET /static/ofi.browser.293d64b6588f.js HTTP/1.1
  17876 136.950771500 10.11.11.217    104.100.226.86    HTTP      386 GET /tags/iPhoneHackscom/ROS/tags.js HTTP/1.1
  21306 172.029680600 10.11.11.200    13.33.252.19      HTTP      430 GET /js/friendbuy.min.js HTTP/1.1
  21603 173.165776000 10.11.11.200    13.33.255.31      HTTP      486 GET /widgets/configs/site-c34415b4-vinylmeplease.com.json HTTP/1.1
  21751 173.454709600 10.11.11.217    23.204.246.46     HTTP      383 GET /real/tags/iPhoneHackscom/ROS/tags.js HTTP/1.1
  21792 173.745505200 10.11.11.217    23.204.246.46     HTTP      382 GET /displayAd.js?dver=0.8&th=7460035367 HTTP/1.1
  21798 173.774804700 10.11.11.217    23.204.246.46     HTTP      634 GET /j.ad?flashVer=0&ver=1.28&th=7460035367&tagKey=1408161819&loaderVer…
  21808 173.832809300 10.11.11.217    172.217.6.162     HTTP      382 GET /pagead/js/adsbygoogle.js HTTP/1.1
  21809 173.844362000 10.11.11.217    23.204.246.46     HTTP      721 GET /p.media?clickID=aYmSC42mBHotIrUW7bXUMk1bUk0T6mSrJDUFrYVHJTobJrPFro…
  21817 173.863969300 10.11.11.217    23.204.246.46     HTTP      721 GET /p.media?clickID=a0mSC4pdTo5m315V3eVV3jVGJ6RAnNTtFSUbJ03U2xUartVEJ9…
  21822 173.880085800 10.11.11.217    23.204.246.46     HTTP      727 GET /p.media?clickID=a1mSC43AnGnbvJ0VrRYGQV1cFpmEfQ2FFRVUFEWm7WRTM5QsZb…
  21823 173.891949500 10.11.11.217    23.204.246.46     HTTP      725 GET /p.media?clickID=a2mSC4mdPyTHZb9XrbjXrZb91TaqSbBBTFB3VdM3mFQuRFjmYT…
  21884 174.602300600 10.11.11.217    23.204.246.46     HTTP      722 GET /p.media?clickID=a3mSg336JY3cUbUVYaWGMiSAJMWtvSWrF02FEpUq7xVEnbSTnK…
  21886 174.614769100 10.11.11.217    23.204.246.46     HTTP      722 GET /p.media?clickID=a4mSC4prjEXVnSXGY01VjnmqnQ5FYVWUnAWPU4PqbRSsUpQdUv…
  21889 174.639435200 10.11.11.217    23.204.246.46     HTTP      719 GET /p.media?clickID=a5mSC4VWYhXrndXrQkXq6MRbUCTrnPWdJYmbbnPbrM1T3o5EUe…
  21897 174.672395300 10.11.11.217    23.204.246.46     HTTP      724 GET /p.media?clickID=a6mSC43sbgTsYbVsJiP6QoTtnWUrf42r2sWaYpVaJiSEYLSGQZ…
  21903 174.714920400 10.11.11.217    23.204.246.46     HTTP      725 GET /p.media?clickID=a7mSC40G70Ys321cjymaj42rJQVbZbBVP70PTQ1QVZbNSdZbx1…
  22629 180.280176200 10.11.11.200    13.33.252.19      HTTP      480 GET /js/friendbuy.min.js HTTP/1.1
  22643 180.308061400 10.11.11.200    172.217.9.134     HTTP      614 GET /activityi;src=8704410;type=retar0;cat=vmp_r0;ord=6577035978844;gtm…
  22994 183.232974500 10.11.11.200    13.33.255.31      HTTP      486 GET /widgets/configs/site-c34415b4-vinylmeplease.com.json HTTP/1.1
  23206 183.884845500 10.11.11.200    52.86.104.177     HTTP      459 GET /track/pxl/?adv=dwxytaa&ct=0:h5wsfri&fmt=3 HTTP/1.1
  24875 198.486210600 10.11.11.200    89.187.164.66     HTTP      398 GET / HTTP/1.1
  25202 200.303880300 10.11.11.200    98.138.71.149     HTTP      560 GET /cms/v1?esig=1%7efac06801624107e5d8ee63717a17d281e39cf167&nwid=1000…
  25295 200.472050000 10.11.11.121    74.125.30.94      HTTP      293 GET /generate_204 HTTP/1.1
```

```
▸ Frame 30753: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits) on interface eth0, id 0
▸ Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
```

Browsing the Web

- The traffic observed were GET requests using HTTP protocol.
- The user(s) were browsing various websites, such as reading news articles.



http.request.method==GET

```
No.       Time          Source         Destination     Protocol  Length Info
     4675 35.986278700  10.11.11.179   151.101.50.2    HTTP       449 GET /libtrc/timeinc-time/loader.js HTTP/1.1
     4920 38.132357600  10.11.11.94    64.98.145.30    HTTP       522 GET / HTTP/1.1
     4943 38.267888600  10.11.11.94    216.58.194.35   HTTP       347 GET /generate_204 HTTP/1.1
     5098 39.496405800  10.11.11.179   143.204.29.89   HTTP       464 GET /time/rd/trunk/www/web/feds/c/v4/main.css HTTP/1.1
     5111 39.516648200  10.11.11.179   13.33.255.25    HTTP       421 GET /epq2dmc.js HTTP/1.1
     5112 39.524281700  10.11.11.179   143.204.29.89   HTTP       479 GET /time/rd/trunk/www/web/feds/c/v4/fixed-header-footer.css HTTP/1.1
     5113 39.531644000  10.11.11.179   143.204.29.89   HTTP       464 GET /time/rd/trunk/www/web/feds/c/channel.css HTTP/1.1
     5114 39.539100500  10.11.11.179   143.204.29.89   HTTP       466 GET /time/rd/trunk/www/web/feds/c/v2/photos.css HTTP/1.1
     5115 39.546267700  10.11.11.179   143.204.29.89   HTTP       447 GET /time/rd/trunk/www/web/feds/j/jquery.js HTTP/1.1
     5116 39.553415100  10.11.11.179   143.204.29.89   HTTP       445 GET /time/rd/trunk/www/web/feds/j/main.js HTTP/1.1
     5145 39.870683900  10.11.11.179   143.204.29.89   HTTP       449 GET /time/rd/trunk/www/web/feds/j/articles.js HTTP/1.1
     5170 40.124930200  10.11.11.179   143.204.29.89   HTTP       450 GET /time/rd/trunk/www/web/feds/j/showLinks.js HTTP/1.1
     5174 40.136928300  10.11.11.94    52.218.228.130  HTTP       558 GET /core/scripts/lrs/tin-can.min.js?_=1573510907652 HTTP/1.1
     5219 40.737820200  10.11.11.179   143.204.29.89   HTTP       430 GET /time/js/photoessay.js HTTP/1.1
     5222 40.790098400  10.11.11.179   143.204.29.89   HTTP       448 GET /time/assets/js/frequency_capping.min.js HTTP/1.1
     5237 40.877389500  10.11.11.179   143.204.29.89   HTTP       457 GET /time/rd/trunk/www/web/feds/j/mobileExperience.js HTTP/1.1
     5242 40.900234900  10.11.11.179   143.204.29.89   HTTP       460 GET /time/rd/trunk/www/web/feds/j/MobileCompatibility.js HTTP/1.1
     5261 41.013068700  10.11.11.179   143.204.29.89   HTTP       445 GET /tii/omniture/h/config/time_s_code.js HTTP/1.1
```

```
    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/rd/trunk/www/web/feds/j/articles.js]
    [HTTP request 2/4]
    [Prev request in frame: 5098]
    [Response in frame: 5255]
    [Next request in frame: 5261]
```

```
0000  00 01 c9 97 4b f0 a8 bb  cf 52 d9 32 08 00 45 02   ····K··· ·R·2··E·
```

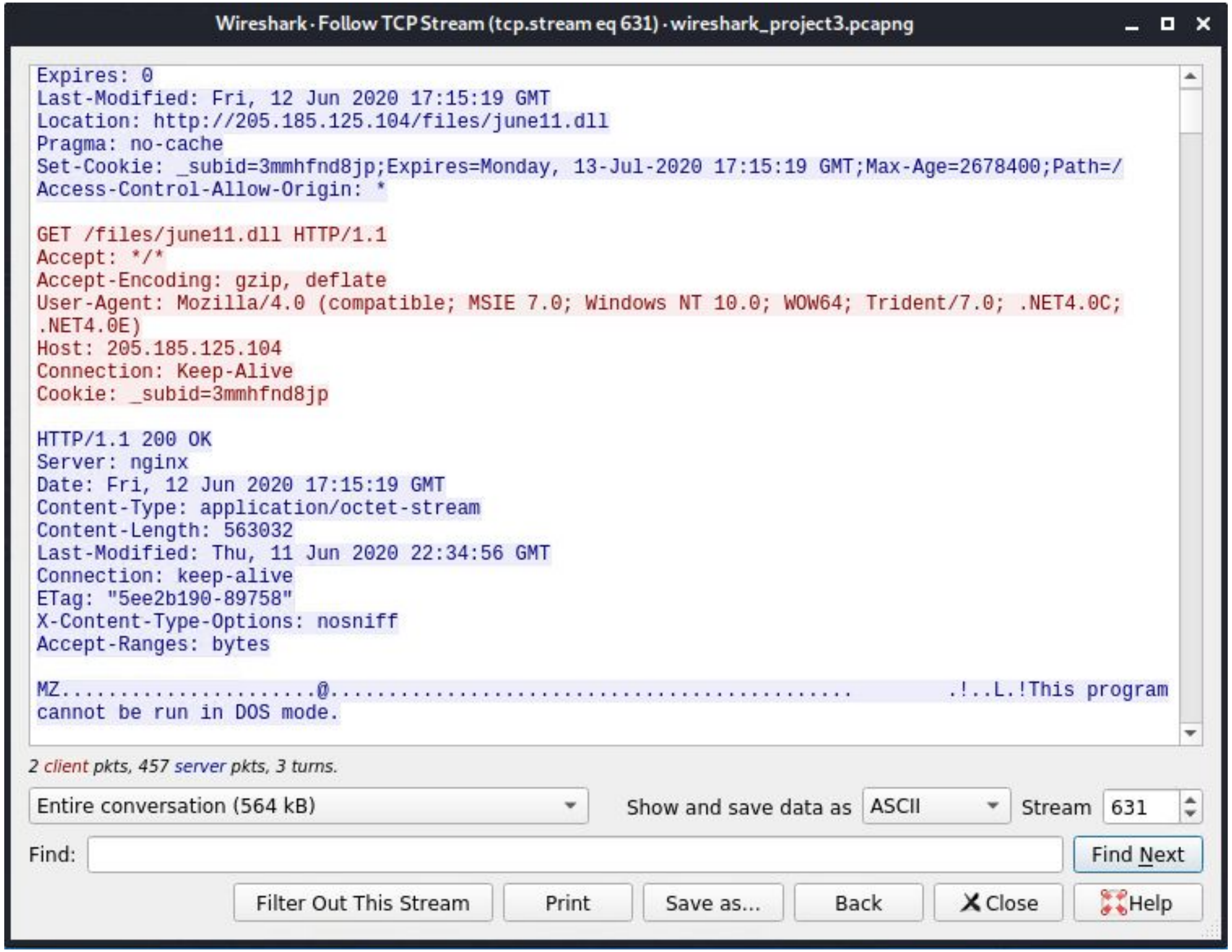
wireshark_project3.pcapng   Packets: 97271 · Displayed: 385 (0.4%)   Profile: Default

Malicious Activity

Downloading the Trojan

- This request used the HTTP protocol.

- The user downloaded the malicious file onto the host network.



Wireshark · Follow TCP Stream (tcp.stream eq 631) · wireshark_project3.pcapng

```
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-Age=2678400;Path=/
Access-Control-Allow-Origin: *

GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C;
.NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

MZ......................@..........................................        .!..L.!This program
cannot be run in DOS mode.
```

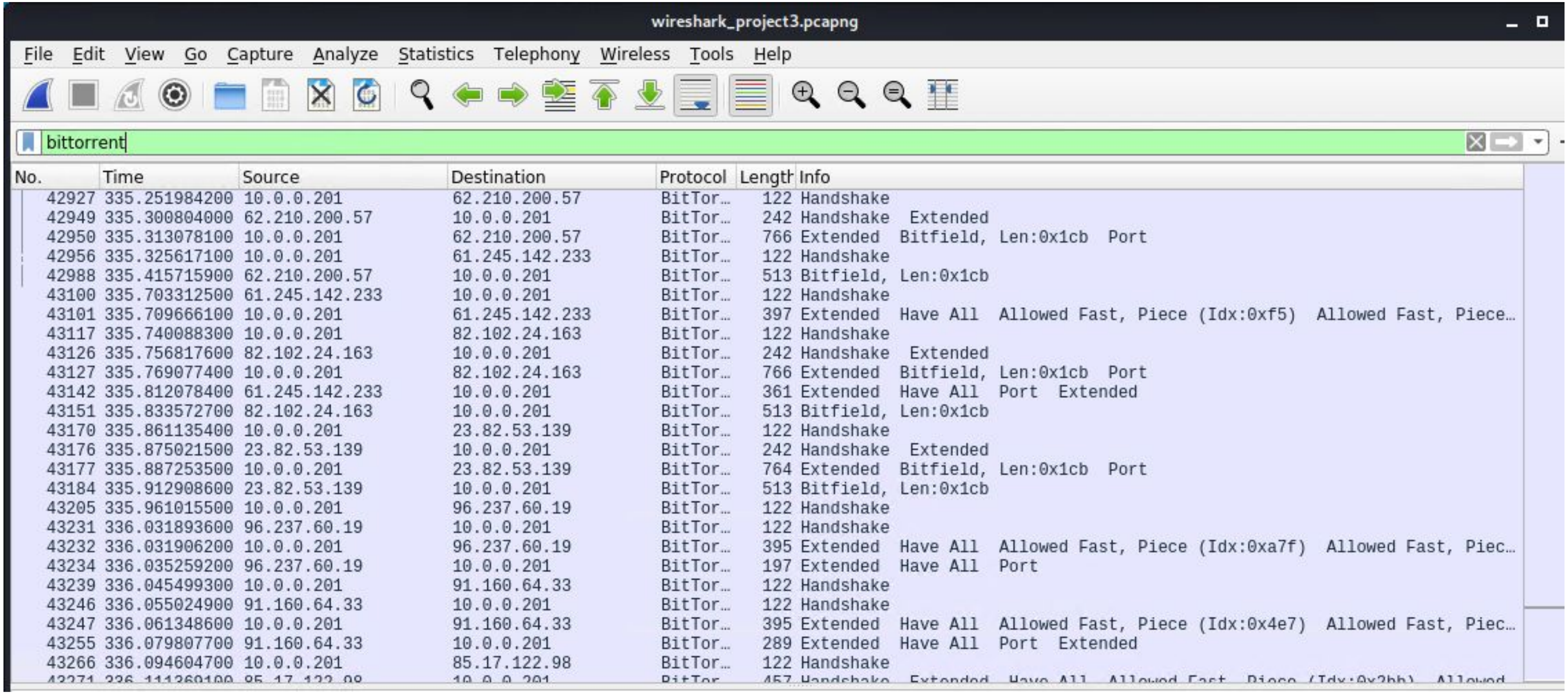
2 client pkts, 457 server pkts, 3 turns.

Entire conversation (564 kB) ▾ Show and save data as ASCII ▾ Stream 631

Find:

Illegal Torrenting

- The streaming traffic was using BitTorrent protocol.
- The user was illegally torrenting using the company network.



wireshark_project3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bittorrent

```
No.   Time          Source          Destination     Protocol Length Info
42927 335.251984200 10.0.0.201      62.210.200.57   BitTor…   122 Handshake
42949 335.300804000 62.210.200.57   10.0.0.201      BitTor…   242 Handshake  Extended
42950 335.313078100 10.0.0.201      62.210.200.57   BitTor…   766 Extended  Bitfield, Len:0x1cb  Port
42956 335.325617100 10.0.0.201      61.245.142.233  BitTor…   122 Handshake
42988 335.415715900 62.210.200.57   10.0.0.201      BitTor…   513 Bitfield, Len:0x1cb
43100 335.703312500 61.245.142.233  10.0.0.201      BitTor…   122 Handshake
43101 335.709666100 10.0.0.201      61.245.142.233  BitTor…   397 Extended  Have All  Allowed Fast, Piece (Idx:0xf5)  Allowed Fast, Piece…
43117 335.740088300 10.0.0.201      82.102.24.163   BitTor…   122 Handshake
43126 335.756817600 82.102.24.163   10.0.0.201      BitTor…   242 Handshake  Extended
43127 335.769077400 10.0.0.201      82.102.24.163   BitTor…   766 Extended  Bitfield, Len:0x1cb  Port
43142 335.812078400 61.245.142.233  10.0.0.201      BitTor…   361 Extended  Have All  Port  Extended
43151 335.833572700 82.102.24.163   10.0.0.201      BitTor…   513 Bitfield, Len:0x1cb
43170 335.861135400 10.0.0.201      23.82.53.139    BitTor…   122 Handshake
43176 335.875021500 23.82.53.139    10.0.0.201      BitTor…   242 Handshake  Extended
43177 335.887253500 10.0.0.201      23.82.53.139    BitTor…   764 Extended  Bitfield, Len:0x1cb  Port
43184 335.912908600 23.82.53.139    10.0.0.201      BitTor…   513 Bitfield, Len:0x1cb
43205 335.961015500 10.0.0.201      96.237.60.19    BitTor…   122 Handshake
43231 336.031893600 96.237.60.19    10.0.0.201      BitTor…   122 Handshake
43232 336.031906200 10.0.0.201      96.237.60.19    BitTor…   395 Extended  Have All  Allowed Fast, Piece (Idx:0xa7f)  Allowed Fast, Piec…
43234 336.035259200 96.237.60.19    10.0.0.201      BitTor…   197 Extended  Have All  Port
43239 336.045499300 10.0.0.201      91.160.64.33    BitTor…   122 Handshake
43246 336.055024900 91.160.64.33    10.0.0.201      BitTor…   122 Handshake
43247 336.061348600 10.0.0.201      91.160.64.33    BitTor…   395 Extended  Have All  Allowed Fast, Piece (Idx:0x4e7)  Allowed Fast, Piec…
43255 336.079807700 91.160.64.33    10.0.0.201      BitTor…   289 Extended  Have All  Port  Extended
43266 336.094604700 10.0.0.201      85.17.122.98    BitTor…   122 Handshake
43271 336.111369100 85.17.122.98    10.0.0.201      BitTor    457 Handshake  Extended  Have All  Allowed Fast  Piece (Idx:0x2bb)  Allowed
```

The End