Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Prepared By: Jesse Wiganowsky, Yeshua Salgado, Cortez Thomas, Yago Martins, and John Burnham

March, 2022

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

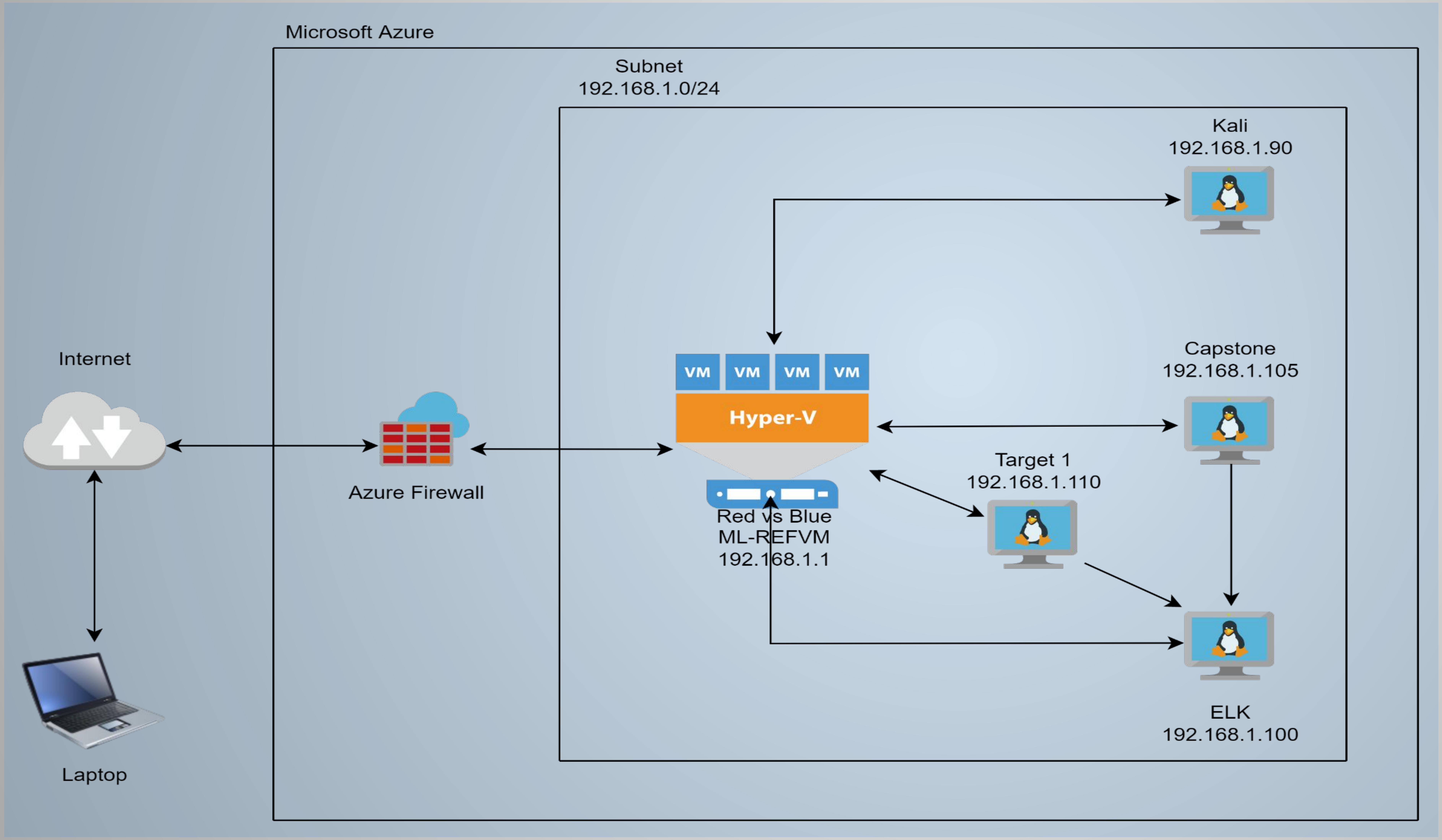
Traffic Profile

Normal Activity

Malicious Activity

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.90

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.115
OS: Debian/GNU Linux
Hostname: Target 1

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Unnecessary Service Running	Open SSH Port 22	Allowed the attacker to gain internal access
Wordpress User Enumeration	wpscan was used to enumerate web server users	Michael and Steven’s usernames we exposed
Weak Password Policy CWE-521	Weak password requirements	Michael’s password was easily guessed, Steven’s password was cracked
Plaintext Storage of a Password CWE-256	Storing a password in plaintext may result in a system compromise	Attacker logged into mySQL with root access

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Use of a One-Way Hash without a Salt CWE-759 Use of Weak Hash CWE-328	This makes it easier for attackers to pre-compute the hash value using dictionary attack techniques and or determine the original input	Michael and Steven’s usernames we exposed
Escalation of Privileges	Executed “ sudo python -c ‘import pty;pty.spawn (“bin/bash”)’ “	Attacker was able to gain root access and take complete control of the system

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	Machines that sent the most traffic.
Most Common Protocols	TLS(7272), HTTP(2848), NetBIOS Service Session	Three most common protocols on the network.
# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	/24	Observed subnet ranges.
# of Malware Species	1	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

- Watching YouTube
- Sending images
- Browsing websites

Suspicious Activity

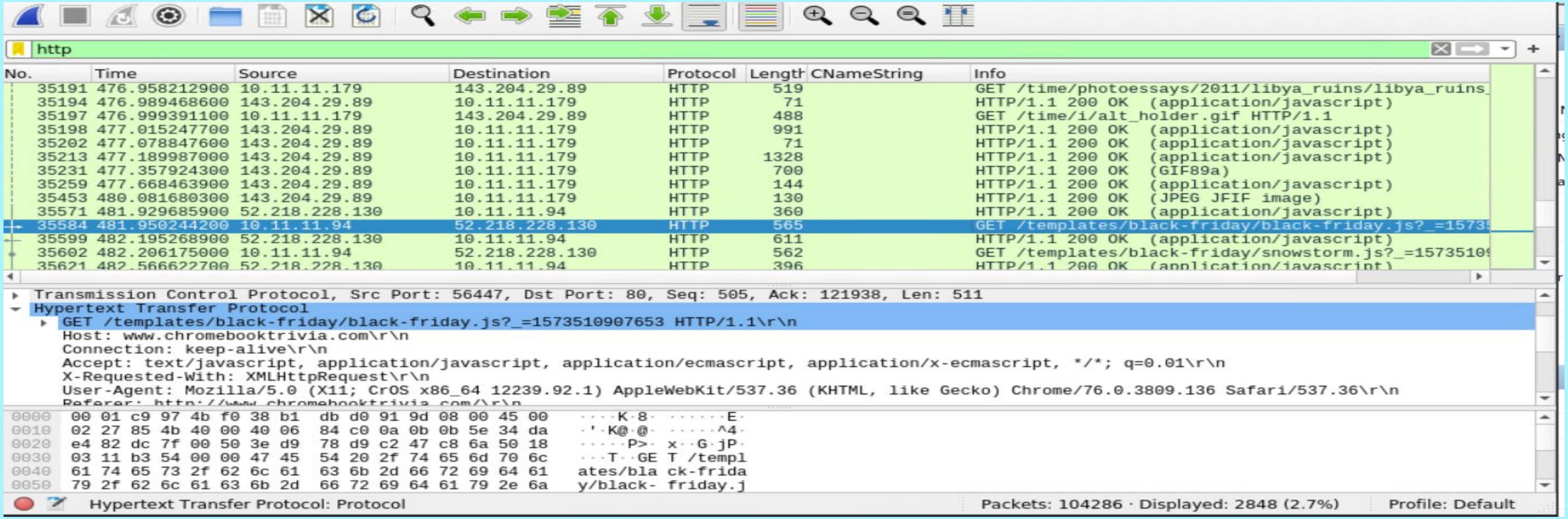
- Sending malware file (june11.dll)
- Downloaded torrent file (Betty_Boop_Rythm_on_the_Reservation.avi.torrent)
- frank-n-ted.com

Normal Activity

Normal Behavior #1

Summarize the following:

- We observed normal traffic such as web browsing. In these packets the GET method was used to access several websites.
- An example of this is a user accessing website: www.chromebooktrivia.com
- The user specifically accessed a Black Friday shopping website.



http

```
No.   Time             Source          Destination     Protocol Length CNameString Info
35191 476.958212900 10.11.11.179    143.204.29.89    HTTP     519             GET /time/photoessays/2011/libya_ruins/libya_ruins_
35194 476.989468600 143.204.29.89   10.11.11.179     HTTP      71             HTTP/1.1 200 OK  (application/javascript)
35197 476.999391100 10.11.11.179    143.204.29.89    HTTP     488             GET /time/i/alt_holder.gif HTTP/1.1
35198 477.015247700 143.204.29.89   10.11.11.179     HTTP     991             HTTP/1.1 200 OK  (application/javascript)
35202 477.078847600 143.204.29.89   10.11.11.179     HTTP      71             HTTP/1.1 200 OK  (application/javascript)
35213 477.189987000 143.204.29.89   10.11.11.179     HTTP    1328             HTTP/1.1 200 OK  (application/javascript)
35231 477.357924300 143.204.29.89   10.11.11.179     HTTP     700             HTTP/1.1 200 OK  (GIF89a)
35259 477.668463900 143.204.29.89   10.11.11.179     HTTP     144             HTTP/1.1 200 OK  (application/javascript)
35453 480.081680300 143.204.29.89   10.11.11.179     HTTP     130             HTTP/1.1 200 OK  (JPEG JFIF image)
35571 481.929685900 52.218.228.130  10.11.11.94      HTTP     360             HTTP/1.1 200 OK  (application/javascript)
35584 481.950244200 10.11.11.94     52.218.228.130   HTTP     565             GET /templates/black-friday/black-friday.js?_=15735
35599 482.195268900 52.218.228.130  10.11.11.94      HTTP     611             HTTP/1.1 200 OK  (application/javascript)
35602 482.206175000 10.11.11.94     52.218.228.130   HTTP     562             GET /templates/black-friday/snowstorm.js?_=15735109
35621 482.566622700 52.218.228.130  10.11.11.94      HTTP     396             HTTP/1.1 200 OK  (application/javascript)
```

```
Transmission Control Protocol, Src Port: 56447, Dst Port: 80, Seq: 505, Ack: 121938, Len: 511
Hypertext Transfer Protocol
  GET /templates/black-friday/black-friday.js?_=1573510907653 HTTP/1.1\r\n
  Host: www.chromebooktrivia.com\r\n
  Connection: keep-alive\r\n
  Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01\r\n
  X-Requested-With: XMLHttpRequest\r\n
  User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36\r\n
  Referer: http://www.chromebooktrivia.com/\r\n
```

```
0000  00 01 c9 97 4b f0 38 b1  db d0 91 9d 08 00 45 00   ····K·8· ······E·
0010  02 27 85 4b 40 00 40 06  84 c0 0a 0b 0b 5e 34 da   ·'·K@·@· ·····^4·
0020  e4 82 dc 7f 00 50 3e d9  78 d9 c2 47 c8 6a 50 18   ·····P>· x··G·jP·
0030  03 11 b3 54 00 00 47 45  54 20 2f 74 65 6d 70 6c   ···T··GE T /templ
0040  61 74 65 73 2f 62 6c 61  63 6b 2d 66 72 69 64 61   ates/bla ck-frida
0050  79 2f 62 6c 61 63 6b 2d  66 72 69 64 61 79 2e 6a   y/black- friday.j
```

Hypertext Transfer Protocol: Protocol

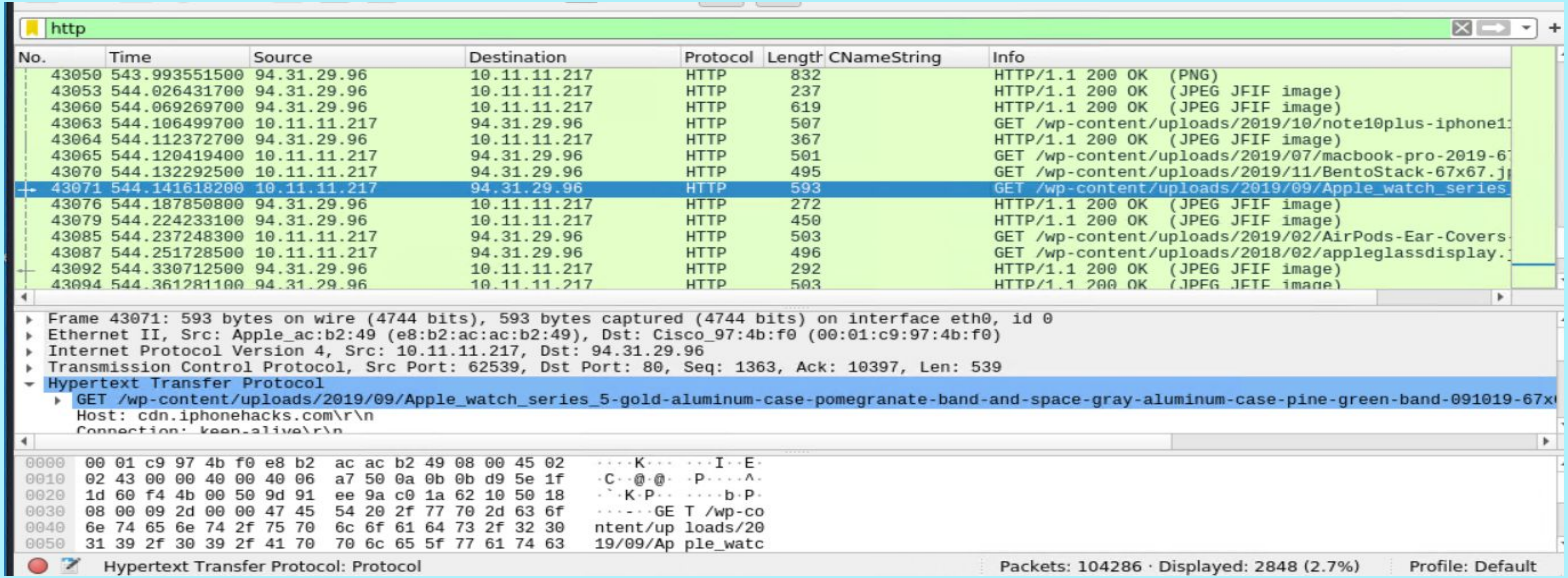
Packets: 104286 · Displayed: 2848 (2.7%)

Profile: Default

Normal Behavior #2

Summarize the following:

- We observed the user utilizing HTTP protocols to look at images.
- The user visited the following website: cdn.iphonehacks.com that contained pictures of an Apple watch series 5 case.



```
http
```

```
No.     Time           Source          Destination     Protocol  Length CNameString  Info
  43050 543.993551500  94.31.29.96     10.11.11.217    HTTP      832                 HTTP/1.1 200 OK  (PNG)
  43053 544.026431700  94.31.29.96     10.11.11.217    HTTP      237                 HTTP/1.1 200 OK  (JPEG JFIF image)
  43060 544.069269700  94.31.29.96     10.11.11.217    HTTP      619                 HTTP/1.1 200 OK  (JPEG JFIF image)
  43063 544.106499700  10.11.11.217    94.31.29.96     HTTP      507                 GET /wp-content/uploads/2019/10/note10plus-iphone1
  43064 544.112372700  94.31.29.96     10.11.11.217    HTTP      367                 HTTP/1.1 200 OK  (JPEG JFIF image)
  43065 544.120419400  10.11.11.217    94.31.29.96     HTTP      501                 GET /wp-content/uploads/2019/07/macbook-pro-2019-6
  43070 544.132292500  10.11.11.217    94.31.29.96     HTTP      495                 GET /wp-content/uploads/2019/11/BentoStack-67x67.j
  43071 544.141618200  10.11.11.217    94.31.29.96     HTTP      593                 GET /wp-content/uploads/2019/09/Apple_watch_series_
  43076 544.187850800  94.31.29.96     10.11.11.217    HTTP      272                 HTTP/1.1 200 OK  (JPEG JFIF image)
  43079 544.224233100  94.31.29.96     10.11.11.217    HTTP      450                 HTTP/1.1 200 OK  (JPEG JFIF image)
  43085 544.237248300  10.11.11.217    94.31.29.96     HTTP      503                 GET /wp-content/uploads/2019/02/AirPods-Ear-Covers
  43087 544.251728500  10.11.11.217    94.31.29.96     HTTP      496                 GET /wp-content/uploads/2018/02/appleglassdisplay.
  43092 544.330712500  94.31.29.96     10.11.11.217    HTTP      292                 HTTP/1.1 200 OK  (JPEG JFIF image)
  43094 544.361281100  94.31.29.96     10.11.11.217    HTTP      503                 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
▸ Frame 43071: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits) on interface eth0, id 0
▸ Ethernet II, Src: Apple_ac:b2:49 (e8:b2:ac:ac:b2:49), Dst: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
▸ Internet Protocol Version 4, Src: 10.11.11.217, Dst: 94.31.29.96
▸ Transmission Control Protocol, Src Port: 62539, Dst Port: 80, Seq: 1363, Ack: 10397, Len: 539
▾ Hypertext Transfer Protocol
  ▸ GET /wp-content/uploads/2019/09/Apple_watch_series_5-gold-aluminum-case-pomegranate-band-and-space-gray-aluminum-case-pine-green-band-091019-67x
    Host: cdn.iphonehacks.com\r\n
    Connection: keep-alive\r\n
```

```
0000  00 01 c9 97 4b f0 e8 b2  ac ac b2 49 08 00 45 02   ····K···  ···I··E·
0010  02 43 00 00 40 00 40 06  a7 50 0a 0b 0b d9 5e 1f   ·C··@·@·  ·P····^·
0020  1d 60 f4 4b 00 50 9d 91  ee 9a c0 1a 62 10 50 18   ·`·K·P··  ····b·P·
0030  08 00 09 2d 00 00 47 45  54 20 2f 77 70 2d 63 6f   ···-··GE T /wp-co
0040  6e 74 65 6e 74 2f 75 70  6c 6f 61 64 73 2f 32 30   ntent/up loads/20
0050  31 39 2f 30 39 2f 41 70  70 6c 65 5f 77 61 74 63   19/09/Ap ple_watc
```

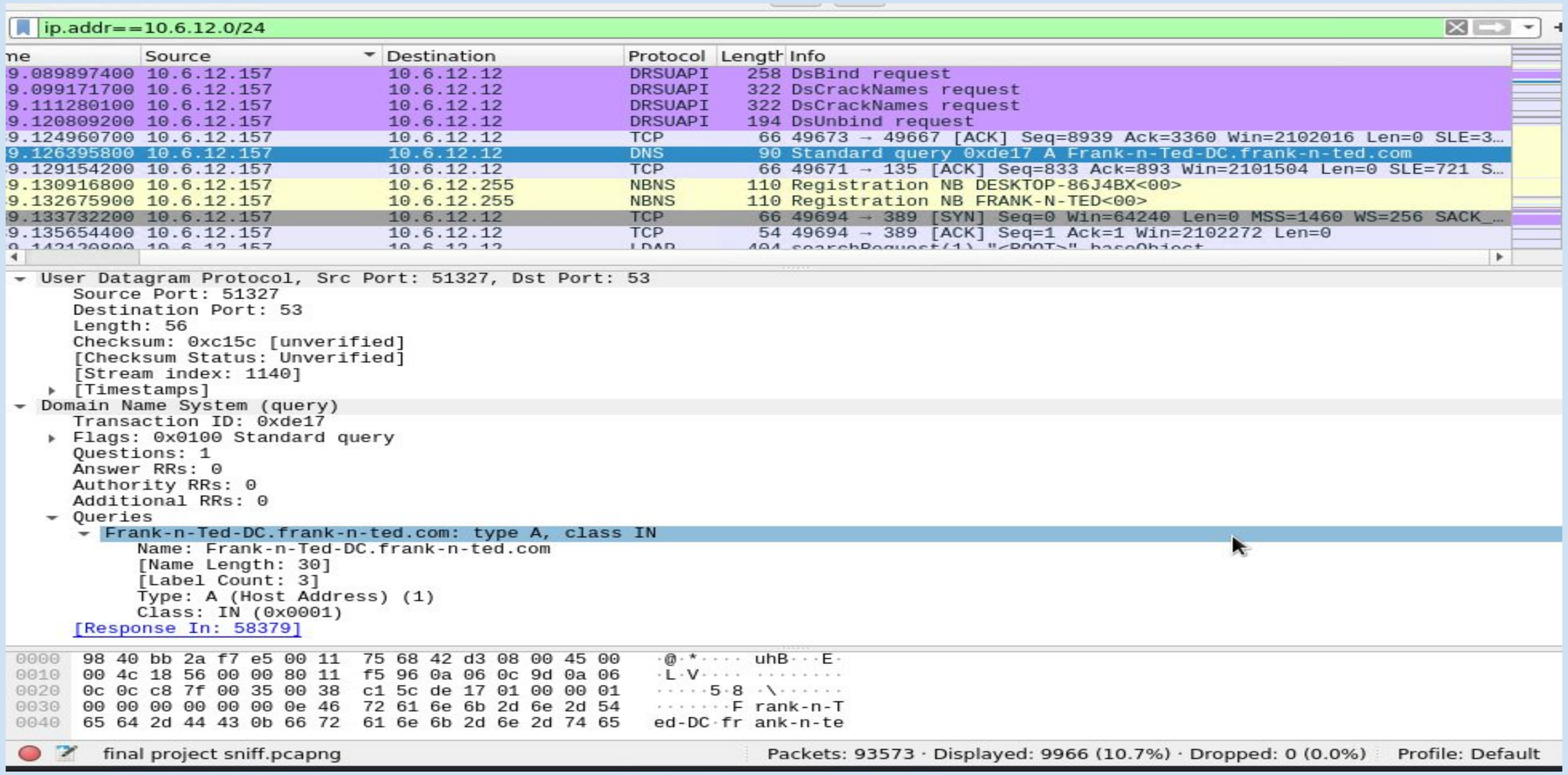
Hypertext Transfer Protocol: Protocol   Packets: 104286 · Displayed: 2848 (2.7%)   Profile: Default

Malicious Activity

Malicious Behavior #1

Summarize the following:

- We observed traffic containing malicious activity containing the protocols HTTP.
- What, specifically, was the user doing? Which site were they browsing? Etc
- The user was trying to send a malicious file containing a trojan through the network, that was captured in the HTTP protocol. The user also created their own website, in which they navigated into it multiple times.
    - .http://205.185.125.104/files/june11.dll
    - matthijs.devries
    - http://frank-n-ted-dc.frank-n-ted.com



```
ip.addr==10.6.12.0/24
```

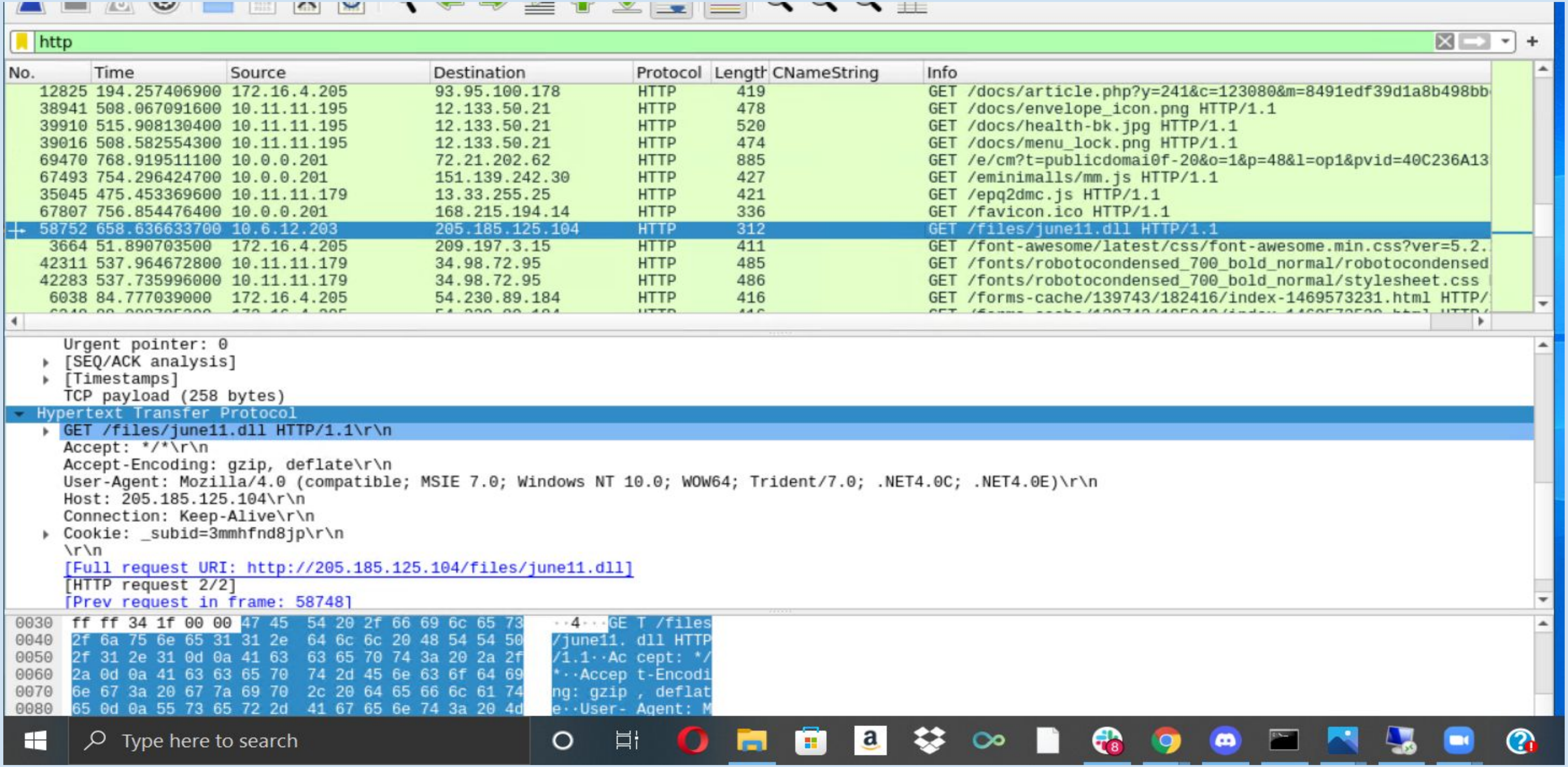
```
me           Source               Destination        Protocol  Length Info
9.089897400  10.6.12.157          10.6.12.12         DRSUAPI   258 DsBind request
9.099171700  10.6.12.157          10.6.12.12         DRSUAPI   322 DsCrackNames request
9.111280100  10.6.12.157          10.6.12.12         DRSUAPI   322 DsCrackNames request
9.120809200  10.6.12.157          10.6.12.12         DRSUAPI   194 DsUnbind request
9.124960700  10.6.12.157          10.6.12.12         TCP        66 49673 → 49667 [ACK] Seq=8939 Ack=3360 Win=2102016 Len=0 SLE=3…
9.126395800  10.6.12.157          10.6.12.12         DNS        90 Standard query 0xde17 A Frank-n-Ted-DC.frank-n-ted.com
9.129154200  10.6.12.157          10.6.12.12         TCP        66 49671 → 135 [ACK] Seq=833 Ack=893 Win=2101504 Len=0 SLE=721 S…
9.130916800  10.6.12.157          10.6.12.255        NBNS      110 Registration NB DESKTOP-86J4BX<00>
9.132675900  10.6.12.157          10.6.12.255        NBNS      110 Registration NB FRANK-N-TED<00>
9.133732200  10.6.12.157          10.6.12.12         TCP        66 49694 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
9.135654400  10.6.12.157          10.6.12.12         TCP        54 49694 → 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
9.142120800  10.6.12.157          10.6.12.12         LDAP      404 searchRequest(1) "<ROOT>" baseObject
```

```
▾ User Datagram Protocol, Src Port: 51327, Dst Port: 53
    Source Port: 51327
    Destination Port: 53
    Length: 56
    Checksum: 0xc15c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1140]
  ▸ [Timestamps]
▾ Domain Name System (query)
    Transaction ID: 0xde17
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ Frank-n-Ted-DC.frank-n-ted.com: type A, class IN
        Name: Frank-n-Ted-DC.frank-n-ted.com
        [Name Length: 30]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 58379]
```

```
0000  98 40 bb 2a f7 e5 00 11  75 68 42 d3 08 00 45 00   ·@·*···· uhB···E·
0010  00 4c 18 56 00 00 80 11  f5 96 0a 06 0c 9d 0a 06   ·L·V···· ········
0020  0c 0c c8 7f 00 35 00 38  c1 5c de 17 01 00 00 01   ·····5·8 ·\······
0030  00 00 00 00 00 00 0e 46  72 61 6e 6b 2d 6e 2d 54   ·······F rank-n-T
0040  65 64 2d 44 43 0b 66 72  61 6e 6b 2d 6e 2d 74 65   ed-DC·fr ank-n-te
```

```
final project sniff.pcapng    Packets: 93573 · Displayed: 9966 (10.7%) · Dropped: 0 (0.0%)    Profile: Default
```

Malicious Behavior #1 Cont.



```
No.    Time           Source        Destination      Protocol Length CNameString Info
 12825 194.257406900 172.16.4.205  93.95.100.178    HTTP     419                GET /docs/article.php?y=241&c=123080&m=8491edf39d1a8b498bb
 38941 508.067091600 10.11.11.195  12.133.50.21     HTTP     478                GET /docs/envelope_icon.png HTTP/1.1
 39910 515.908130400 10.11.11.195  12.133.50.21     HTTP     520                GET /docs/health-bk.jpg HTTP/1.1
 39016 508.582554300 10.11.11.195  12.133.50.21     HTTP     474                GET /docs/menu_lock.png HTTP/1.1
 69470 768.919511100 10.0.0.201    72.21.202.62     HTTP     885                GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13
 67493 754.296424700 10.0.0.201    151.139.242.30   HTTP     427                GET /eminimalls/mm.js HTTP/1.1
 35045 475.453369600 10.11.11.179  13.33.255.25     HTTP     421                GET /epq2dmc.js HTTP/1.1
 67807 756.854476400 10.0.0.201    168.215.194.14   HTTP     336                GET /favicon.ico HTTP/1.1
 58752 658.636633700 10.6.12.203   205.185.125.104  HTTP     312                GET /files/june11.dll HTTP/1.1
  3664 51.890703500  172.16.4.205  209.197.3.15     HTTP     411                GET /font-awesome/latest/css/font-awesome.min.css?ver=5.2.
 42311 537.964672800 10.11.11.179  34.98.72.95      HTTP     485                GET /fonts/robotocondensed_700_bold_normal/robotocondensed
 42283 537.735996000 10.11.11.179  34.98.72.95      HTTP     486                GET /fonts/robotocondensed_700_bold_normal/stylesheet.css
  6038 84.777039000  172.16.4.205  54.230.89.184    HTTP     416                GET /forms-cache/139743/182416/index-1469573231.html HTTP/
```

```
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (258 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET /files/june11.dll HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
    Host: 205.185.125.104\r\n
    Connection: Keep-Alive\r\n
  ▸ Cookie: _subid=3mmhfnd8jp\r\n
    \r\n
    [Full request URI: http://205.185.125.104/files/june11.dll]
    [HTTP request 2/2]
    [Prev request in frame: 58748]
```

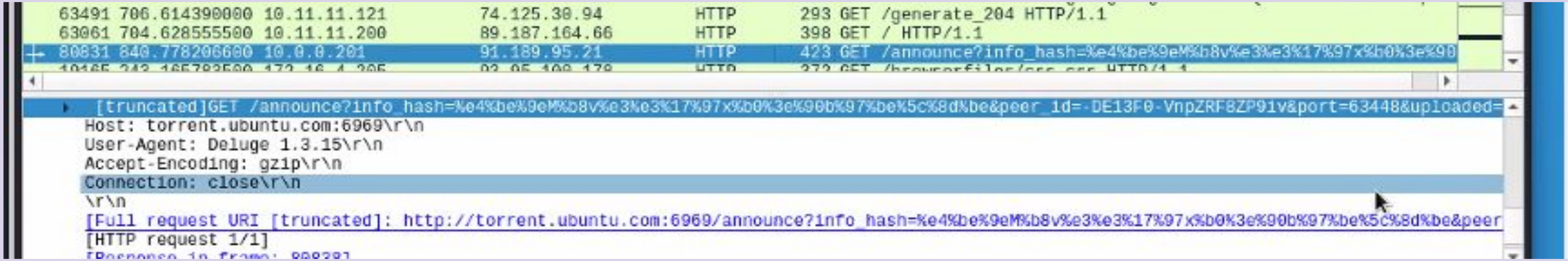
```
0030  ff ff 34 1f 00 00 47 45  54 20 2f 66 69 6c 65 73   ··4···GE T /files
0040  2f 6a 75 6e 65 31 31 2e  64 6c 6c 20 48 54 54 50   /june11. dll HTTP
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
0070  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0080  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
```

Malicious Behavior #2

Summarize the following:

- We observed traffic containing packets with HTTP protocols.
- The user was downloading files through torrent which could contain malicious content. They were trying to access the following websites containing torrent files.
  - /bt/btdownload.php?type=torrent&file=Betty_Boop_Rythm_on_the_Reservation.avi.torrent

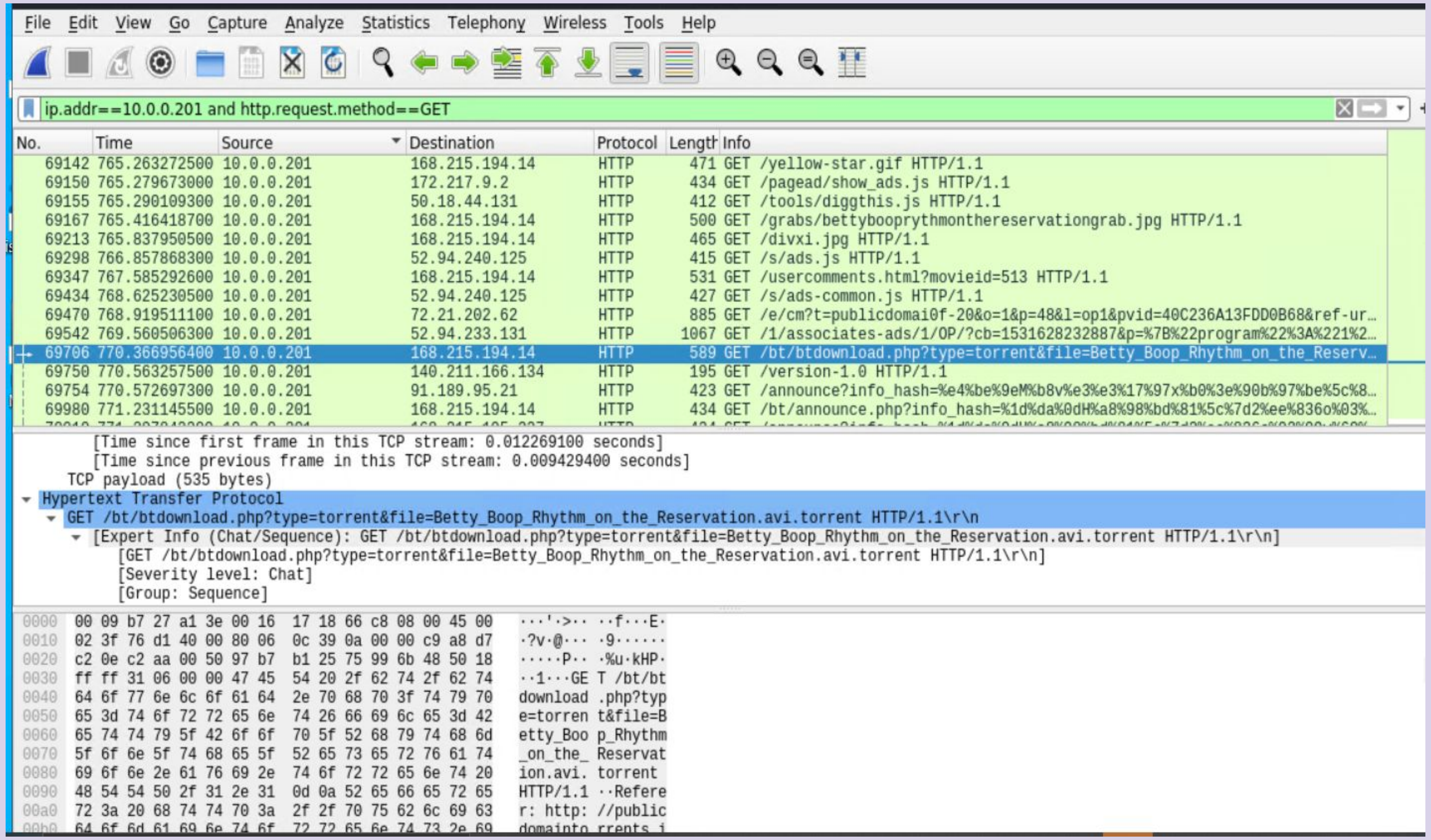
  orrent.org
  - publicdomaintorrents.info,
- Impact: Torrent files are open source and anyone can upload or download anything, which could potentially contain malicious content and unbeknownst to the recipient.



```
63491 706.614390000 10.11.11.121       74.125.30.94       HTTP       293 GET /generate_204 HTTP/1.1
63061 704.628555500 10.11.11.200       89.187.164.66      HTTP       398 GET / HTTP/1.1
80831 840.778206600 10.0.0.201         91.189.95.21       HTTP       423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90
10165 243.165783500 172.16.4.205       93.95.100.178      HTTP       372 GET /browserfiles/css.css HTTP/1.1

[truncated]GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be&peer_id=-DE13F0-VnpZRF8ZP91v&port=63448&uploaded=
   Host: torrent.ubuntu.com:6969\r\n
   User-Agent: Deluge 1.3.15\r\n
   Accept-Encoding: gzip\r\n
   Connection: close\r\n
   \r\n
   [Full request URI [truncated]: http://torrent.ubuntu.com:6969/announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be&peer
   [HTTP request 1/1]
   [Response in frame: 80838]
```

Malicious Behavior #2 Cont.

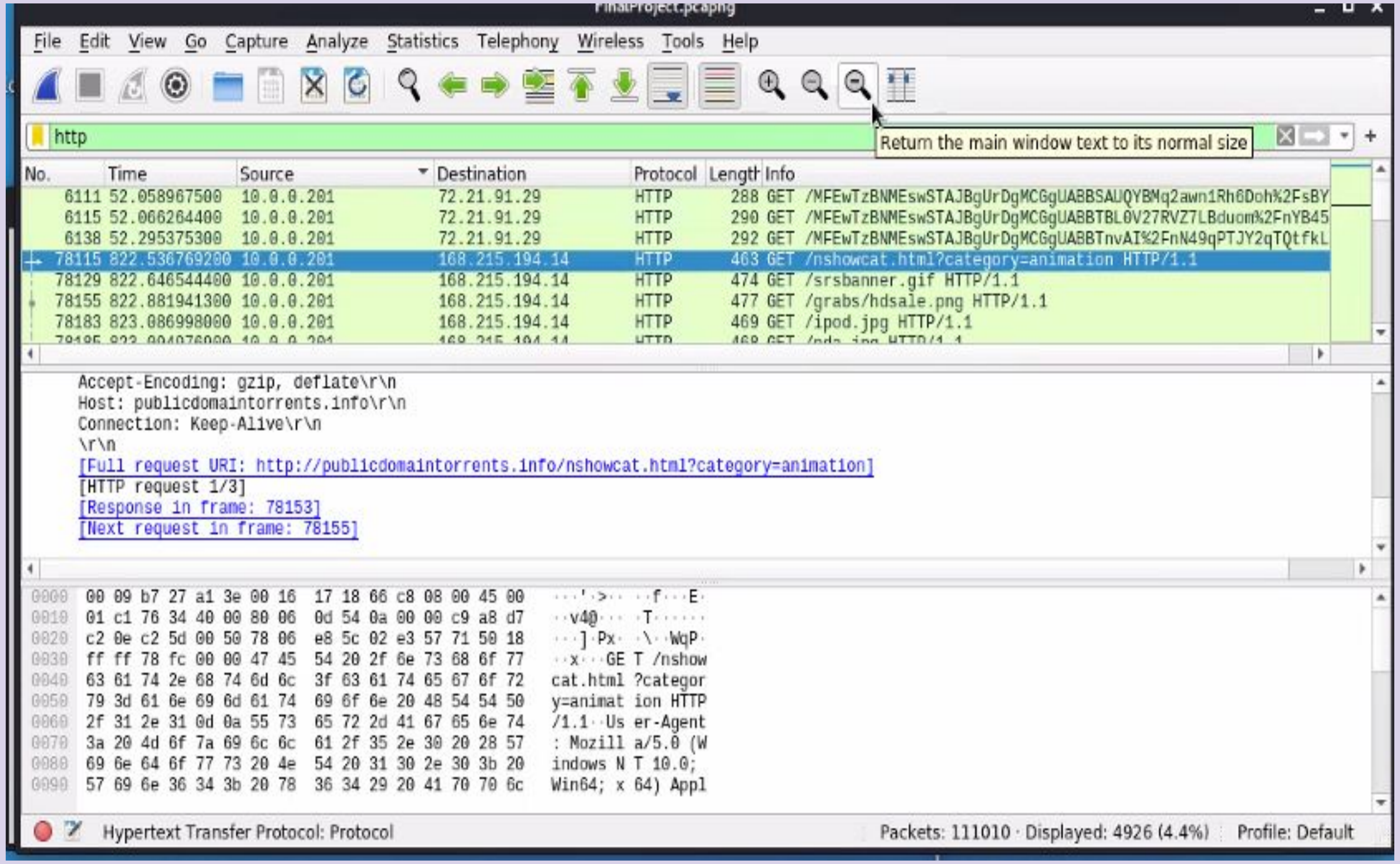

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==10.0.0.201 and http.request.method==GET

No.   Time           Source      Destination      Protocol Length Info
69142 765.263272500 10.0.0.201  168.215.194.14   HTTP      471 GET /yellow-star.gif HTTP/1.1
69150 765.279673000 10.0.0.201  172.217.9.2      HTTP      434 GET /pagead/show_ads.js HTTP/1.1
69155 765.290109300 10.0.0.201  50.18.44.131     HTTP      412 GET /tools/diggthis.js HTTP/1.1
69167 765.416418700 10.0.0.201  168.215.194.14   HTTP      500 GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213 765.837950500 10.0.0.201  168.215.194.14   HTTP      465 GET /divxi.jpg HTTP/1.1
69298 766.857868300 10.0.0.201  52.94.240.125    HTTP      415 GET /s/ads.js HTTP/1.1
69347 767.585292600 10.0.0.201  168.215.194.14   HTTP      531 GET /usercomments.html?movieid=513 HTTP/1.1
69434 768.625230500 10.0.0.201  52.94.240.125    HTTP      427 GET /s/ads-common.js HTTP/1.1
69470 768.919511100 10.0.0.201  72.21.202.62     HTTP      885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-ur…
69542 769.560506300 10.0.0.201  52.94.233.131    HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%221%2…
69706 770.366956400 10.0.0.201  168.215.194.14   HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reserv…
69750 770.563257500 10.0.0.201  140.211.166.134  HTTP      195 GET /version-1.0 HTTP/1.1
69754 770.572697300 10.0.0.201  91.189.95.21     HTTP      423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8…
69980 771.231145500 10.0.0.201  168.215.194.14   HTTP      434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%…

      [Time since first frame in this TCP stream: 0.012269100 seconds]
      [Time since previous frame in this TCP stream: 0.009429400 seconds]
    TCP payload (535 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    ▾ [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
        [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]

0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  02 3f 76 d1 40 00 80 06  0c 39 0a 00 00 c9 a8 d7   ·?v·@··· ·9······
0020  c2 0e c2 aa 00 50 97 b7  b1 25 75 99 6b 48 50 18   ·····P·· ·%u·kHP·
0030  ff ff 31 06 00 00 47 45  54 20 2f 62 74 2f 62 74   ··1···GE T /bt/bt
0040  64 6f 77 6e 6c 6f 61 64  2e 70 68 70 3f 74 79 70   download .php?typ
0050  65 3d 74 6f 72 72 65 6e  74 26 66 69 6c 65 3d 42   e=torren t&file=B
0060  65 74 74 79 5f 42 6f 6f  70 5f 52 68 79 74 68 6d   etty_Boo p_Rhythm
0070  5f 6f 6e 5f 74 68 65 5f  52 65 73 65 72 76 61 74   _on_the_ Reservat
0080  69 6f 6e 2e 61 76 69 2e  74 6f 72 72 65 6e 74 20   ion.avi. torrent 
0090  48 54 54 50 2f 31 2e 31  0d 0a 52 65 66 65 72 65   HTTP/1.1 ··Refere
00a0  72 3a 20 68 74 74 70 3a  2f 2f 70 75 62 6c 69 63   r: http: //public
```


FinalProject.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Return the main window text to its normal size

```
http

No.   Time           Source      Destination      Protocol Length Info
 6111 52.058967500  10.0.0.201  72.21.91.29      HTTP      288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBY
 6115 52.066264400  10.0.0.201  72.21.91.29      HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45
 6138 52.295375300  10.0.0.201  72.21.91.29      HTTP      292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI%2FnN49qPTJY2qTQtfkL
78115 822.536769200 10.0.0.201  168.215.194.14   HTTP      463 GET /nshowcat.html?category=animation HTTP/1.1
78129 822.646544400 10.0.0.201  168.215.194.14   HTTP      474 GET /srsbanner.gif HTTP/1.1
78155 822.881941300 10.0.0.201  168.215.194.14   HTTP      477 GET /grabs/hdsale.png HTTP/1.1
78183 823.086998000 10.0.0.201  168.215.194.14   HTTP      469 GET /ipod.jpg HTTP/1.1

    Accept-Encoding: gzip, deflate\r\n
    Host: publicdomaintorrents.info\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://publicdomaintorrents.info/nshowcat.html?category=animation]
    [HTTP request 1/3]
    [Response in frame: 78153]
    [Next request in frame: 78155]

0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  01 c1 76 34 40 00 80 06  0d 54 0a 00 00 c9 a8 d7   ··v4@··· ·T······
0020  c2 0e c2 5d 00 50 78 06  e8 5c 02 e3 57 71 50 18   ···]·Px· ·\··WqP·
0030  ff ff 78 fc 00 00 47 45  54 20 2f 6e 73 68 6f 77   ··x···GE T /nshow
0040  63 61 74 2e 68 74 6d 6c  3f 63 61 74 65 67 6f 72   cat.html ?categor
0050  79 3d 61 6e 69 6d 61 74  69 6f 6e 20 48 54 54 50   y=animat ion HTTP
0060  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0070  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
0080  69 6e 64 6f 77 73 20 4e  54 20 31 30 2e 30 3b 20   indows N T 10.0; 
0090  57 69 6e 36 34 3b 20 78  36 34 29 20 41 70 70 6c   Win64; x 64) Appl

Hypertext Transfer Protocol: Protocol        Packets: 111010 · Displayed: 4926 (4.4%)    Profile: Default
```

The End