

Network Analysis

NIKKI Ghadimi

Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

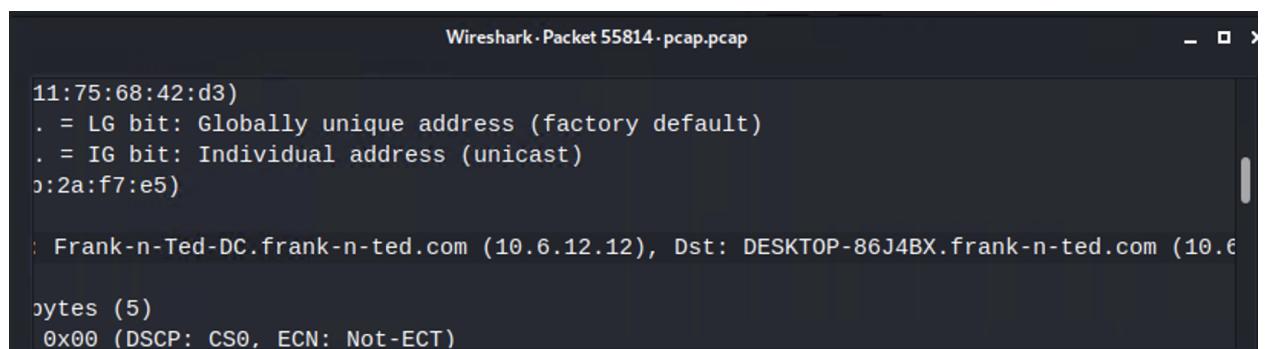
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

The domain name of the user's custom site is: Frank-n-Ted-DC.frank-n-ted.com

Filter: ip.addr==10.6.12.0/24



Wireshark - Packet 55814 · pcap.pcap

11:75:68:42:d3
· = LG bit: Globally unique address (factory default)
· = IG bit: Individual address (unicast)
0:2a:f7:e5
: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.11)
bytes (5)
0x00 (DSCP: CS0, ECN: Not-ECT)

2. What is the IP address of the Domain Controller (DC) of the AD network?

The IP address of the Domain Controller (DC) of the AD network is: 10.6.12.12

Filter: ip.addr==10.6.12.0/24

```

Wireshark - Packet 55814 - pcap.pcap

11:75:68:42:d3)
. = LG bit: Globally unique address (factory default)
. = IG bit: Individual address (unicast)
:b:2a:f7:e5)

: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6
bytes (5)
0x00 (DSCP: CS0, ECN: Not-ECT)

```

3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

The name of the malware downloaded to the 10.6.12.203 machine is june11.dll

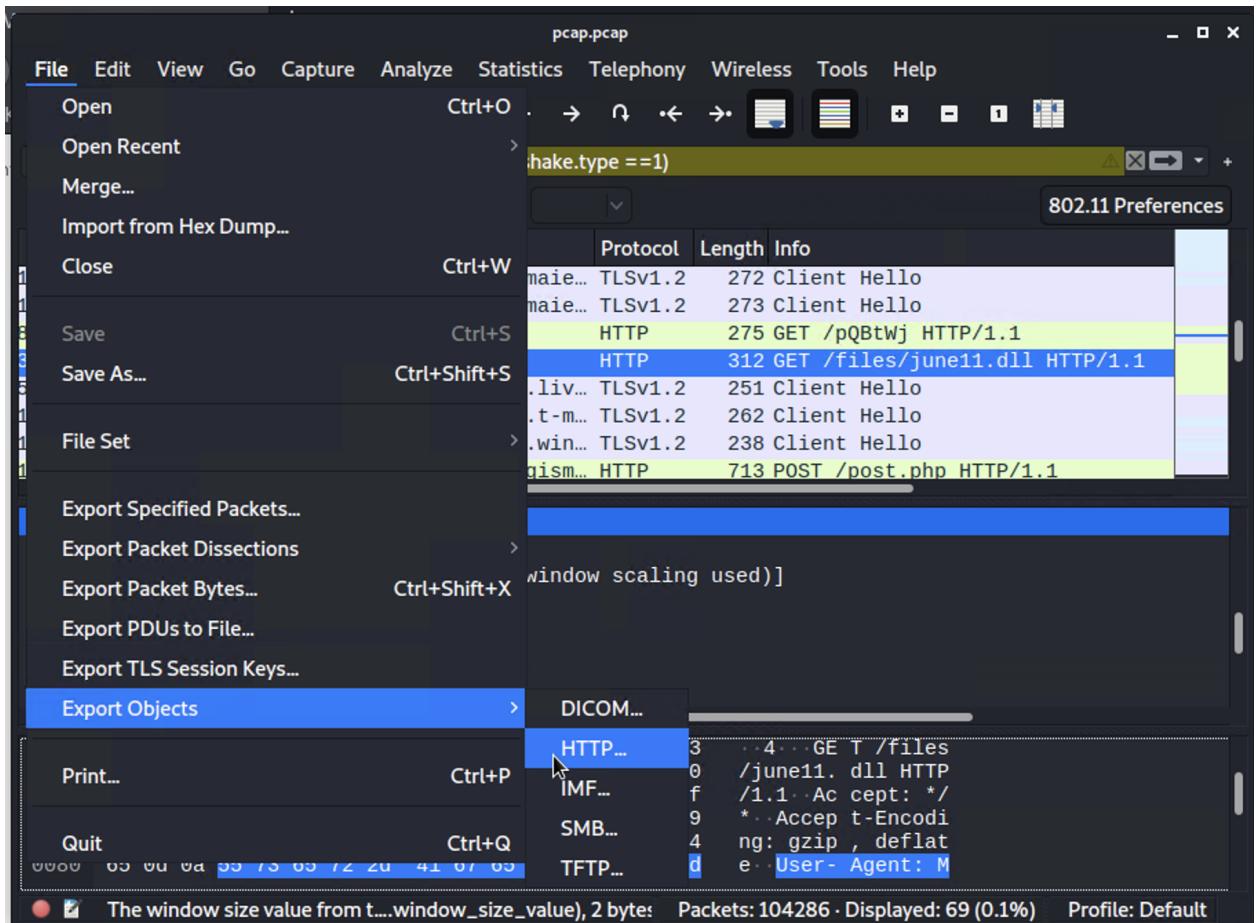
Filter: ip.addr==10.6.12.203 and http.request.method==GET

| Source | Destination | Protocol | Length | Info |
|-----------------------------|------------------------|----------|--------|--------------------------------|
| 1900 LAPTOP-5WKHX9YG.fra... | e16646.dspg.akamaie... | TLSv1.2 | 272 | Client Hello |
| 1700 LAPTOP-5WKHX9YG.fra... | e16646.dspg.akamaie... | TLSv1.2 | 273 | Client Hello |
| 3400 LAPTOP-5WKHX9YG.fra... | 205.185.125.104 | HTTP | 275 | GET /pQBtWj HTTP/1.1 |
| 3700 LAPTOP-5WKHX9YG.fra... | 205.185.125.104 | HTTP | 312 | GET /files/june11.dll HTTP/1.1 |
| 5700 LAPTOP-5WKHX9YG.fra... | prod.nexusrules.liv... | TLSv1.2 | 251 | Client Hello |
| 1700 LAPTOP-5WKHX9YG.fra... | standard.t-0001.t-m... | TLSv1.2 | 262 | Client Hello |

4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

Export: file>Export Objects>HTTP

The malware is this classified as Trojan- malicious 50/67



Wireshark · Export · HTTP object list

| Packet | Hostname | Content Type | Size | File |
|--------|-----------------|--------------------------|--------|------|
| 59388 | 205.185.125.104 | application/octet-stream | 563 kB | junk |

Text Filter: dll

Help

VirusTotal - File - d3636

https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b60

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Community Score: 50 / 67

50 security vendors and 1 sandbox flagged this file as malicious

File: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Size: 549.84 KB | Date: 2022-03-09 01:38:24 UTC | 3 days ago

Googleupdate.exe

invalid-signature overlay peddl signed spreader

DLL

| DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY |
|--------------------|-------------------------------------|-----------|---------------|------------------------------------|
| Ad-Aware | ! Trojan.Mint.Zamg.O | | AhnLab-V3 | ! Malware/Win32.RL_Generic.R346613 |
| Alibaba | ! TrojanSpy:Win32/Yakes.0454a340 | | ALYac | ! Trojan.Mint.Zamg.O |
| Antiy-AVL | ! Trojan/Generic.ASCommon.1BE | | Arcabit | ! Trojan.Mint.Zamg.O |
| Avast | ! Win32:DangerousSig [Trj] | | AVG | ! Win32:DangerousSig [Trj] |
| Avira (no cloud) | ! TR/AD.ZLoader.ladbd | | BitDefender | ! Trojan.Mint.Zamg.O |
| BitDefenderTheta | ! Gen:NN.ZedlaF.34264.lu9@aul7OQgi | | CAT-QuickHeal | ! Ransom.LockyCiR |
| CrowdStrike Falcon | ! Win/malicious_confidence_100% (W) | | Cylance | ! Unsafe |
| Cynet | ! Malicious (score: 100) | | DrWeb | ! Trojan.Inject3.53106 |

Status: Running

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

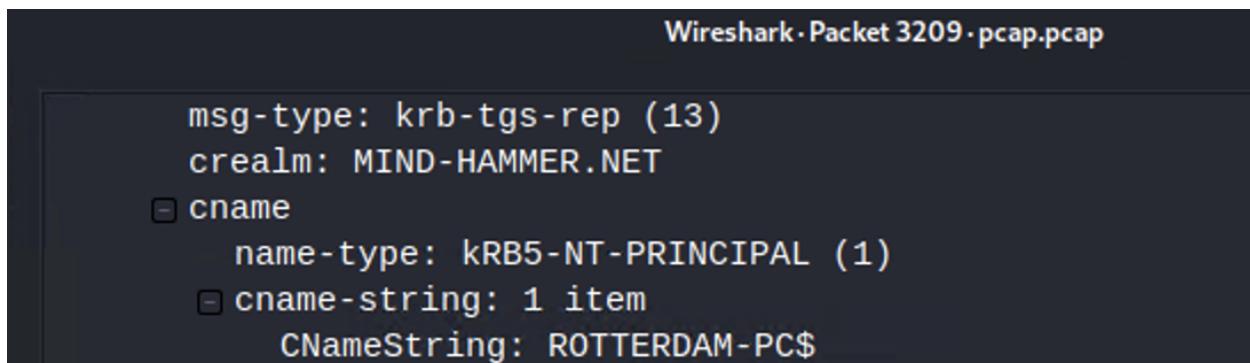
- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

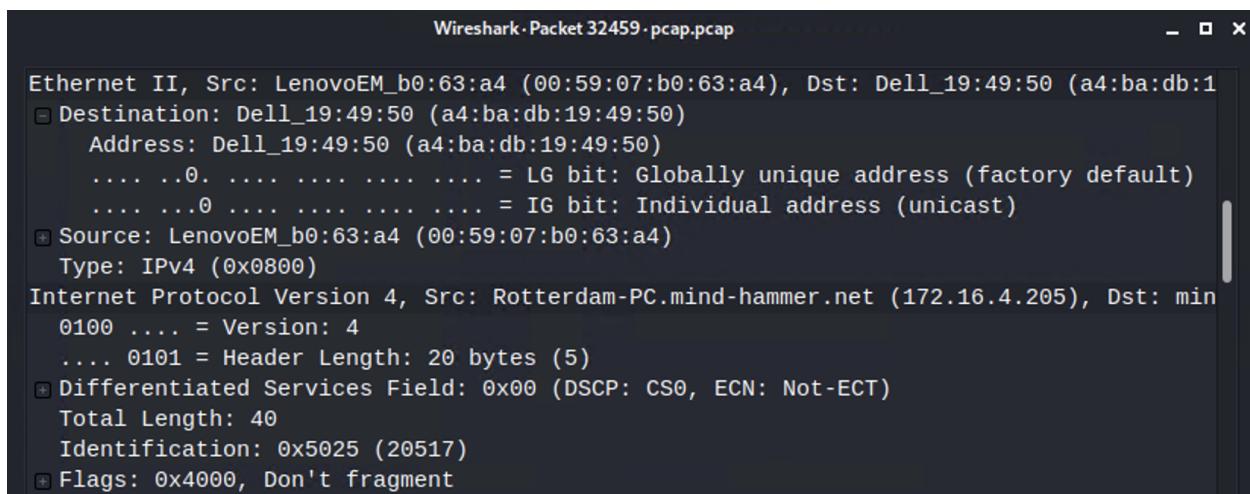
1. Find the following information about the infected Windows machine:

- Host name: ROTTERDAM-PC
- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4

Filter: ip.src==172.16.4.4 and kerberos.CNameString



```
msg-type: krb-tgs-rep (13)
crealm: MIND-HAMMER.NET
[cname]
    name-type: KRB5-NT-PRINCIPAL (1)
    [cname-string: 1 item]
        CNameString: ROTTERDAM-PC$
```

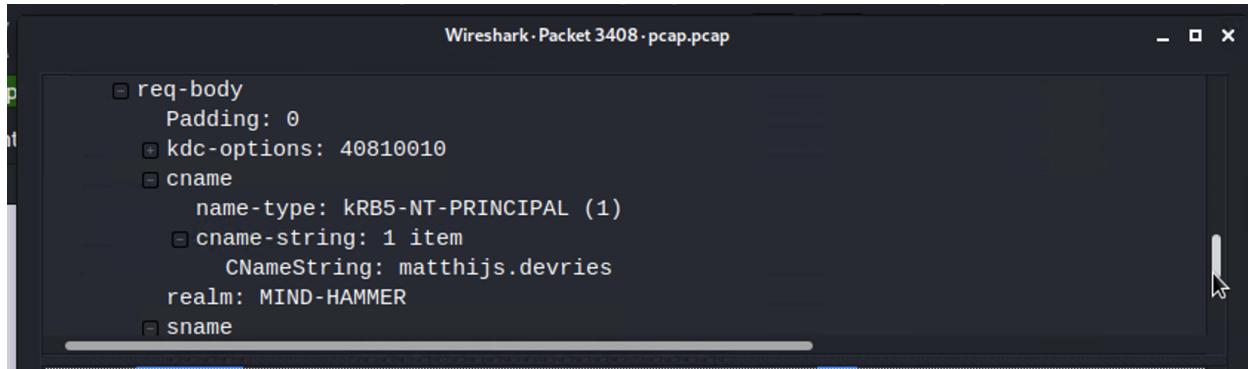


```
Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell_19:49:50 (a4:ba:db:19:49:50)
[Destination: Dell_19:49:50 (a4:ba:db:19:49:50)
 Address: Dell_19:49:50 (a4:ba:db:19:49:50)
 ....0.... .... .... = LG bit: Globally unique address (factory default)
 ....0.... .... .... = IG bit: Individual address (unicast)]
[Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
 Type: IPv4 (0x0800)]
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: min
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
[Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 40
 Identification: 0x5025 (20517)
[Flags: 0x4000, Don't fragment]
```

2. What is the username of the Windows user whose computer is infected?

The username of the Windows user whose computer is infected is:
matthijs.devries

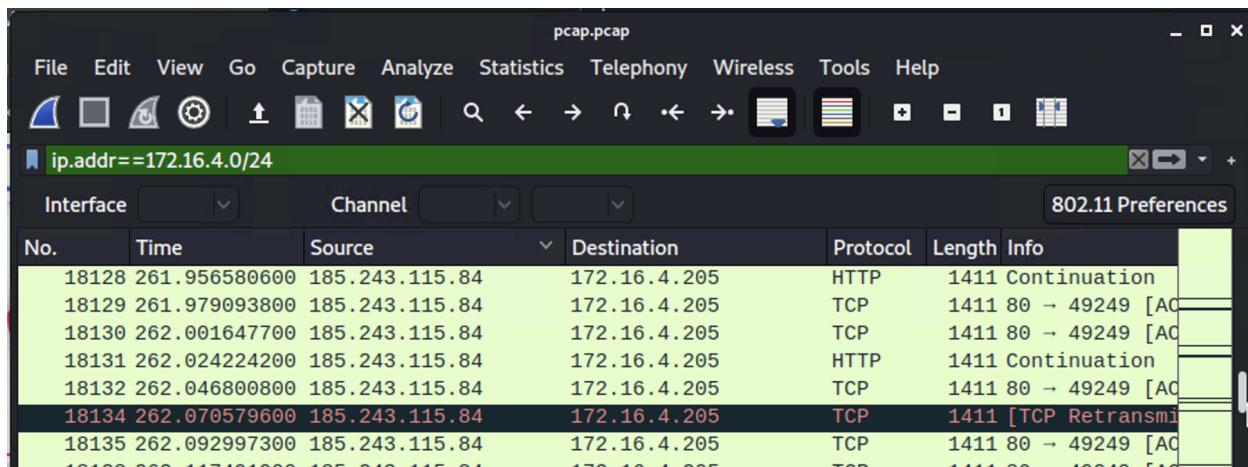
Filter: ip.src==172.16.4.205 and Kerberos.CNameString

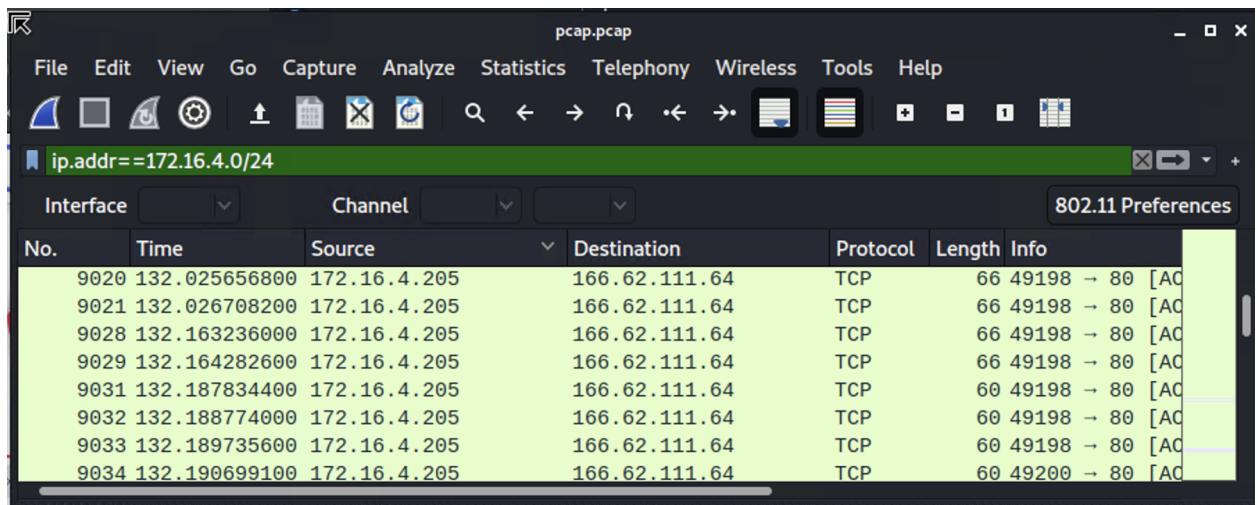


3. What are the IP addresses used in the actual infection traffic?

The IP addresses used in the actual infection traffic are: 172.16.4.205, 172.16.4.4, 166.62.11.64

Filter: ip.addr==172.16.4.205 and ip.add==185.243.115.84





4. As a bonus, retrieve the desktop background of the Windows host.

Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with IP address 10.0.0.201:
 - MAC address: 00:16:17:18:66:c8
 - Windows username: elmer.blanco
 - OS version: BLANCO-DESKTOP

Filter: ip.src==10.0.0.201 and kerberos.CNameString

Wireshark - Packet 67036 · pcap.pcap

Frame 67036: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
Destination: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
Source: Msi_18:66:c8 (00:16:17:18:66:c8)
Address: Msi_18:66:c8 (00:16:17:18:66:c8)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.2
Transmission Control Protocol, Src Port: 49744, Dst Port: 88, Seq: 1, Ack: 1, Len: 236

Wireshark - Packet 67036 · pcap.pcap

CNameString: elmer.blanco
realm: DOGOFTHEYEAR
sname
name-type: kRB5-NT-SRV-INST (2)
sname-string: 2 items
SNameString: krbtgt
SNameString: DOGOFTHEYEAR
till: 2037-09-13 02:48:05 (UTC)
rtime: 2037-09-13 02:48:05 (UTC)

```
Wireshark - Packet 67036 · pcap.pcap

□ etype: 6 items
    ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
    ENCTYPE: eTYPE-ARCFour-HMAC-MD5 (23) [Selected]
    ENCTYPE: eTYPE-ARCFour-HMAC-MD5-56 (24)
    ENCTYPE: eTYPE-ARCFour-HMAC-OLD-EXP (-135)
    ENCTYPE: eTYPE-DES-CBC-MD5 (3)
□ addresses: 1 item BLANCO-DESKTOP<20>
    + HostAddress BLANCO-DESKTOP<20>
```

2. Which torrent file did the user download?

The user downloaded: Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

Filter: ip.addr==10.0.0.201 and http.request.method==GET

```
Wireshark - Packet 69167 · pcap.pcap

[ iRTT: 0.002718200 seconds]
[ Bytes in flight: 446]
[ Bytes sent since last PSH flag: 446]
□ [Timestamps]
    [Time since first frame in this TCP stream: 0.292989200 seconds]
    [Time since previous frame in this TCP stream: 0.007990100 seconds]
    TCP payload (446 bytes)
□ Hypertext Transfer Protocol
    □ GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n
```

```
TCP payload (446 bytes)
HTTP/1.1
Hypertext Transfer Protocol
GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n]
Request Method: GET
Request URI: /grabs/bettybooprythmonthereservationgrab.jpg
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]
[HTTP request 2/2]
[Prev request in frame: 69126]
[Response in frame: 69417]
```