

Network Analysis

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?

- Filter: ip.addr==10.6.12.0/24
- The domain name is Frank-n-Ted-DC.frank-n-ted.com.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|---------------|-------------|-------------|----------|--------|--|
| 40777 | 397.097348100 | 10.6.12.157 | 224.0.0.251 | MDNS | 90 | Standard query response 0x6 |
| 40778 | 397.098468800 | 10.6.12.157 | 224.0.0.252 | LLMNR | 74 | Standard query 0x094f ANY D |
| 40779 | 397.099455500 | 10.6.12.157 | 224.0.0.22 | IGMPv3 | 62 | Membership Report / Join gr |
| 40780 | 397.109143100 | 10.6.12.157 | 10.6.12.12 | DNS | 96 | Standard query 0x9c26 SRV |
| 40781 | 397.109159300 | 10.6.12.12 | 10.6.12.157 | DNS | 162 | Standard query response 0x9 |
| 40782 | 397.109163300 | 10.6.12.157 | 10.6.12.12 | DNS | 90 | Standard query 0x838c A fra |
| 40783 | 397.109166800 | 10.6.12.12 | 10.6.12.157 | DNS | 106 | Standard query response 0x8 |
| 40784 | 397.110040200 | 10.6.12.157 | 10.6.12.12 | LDAP | 264 | searchRequest(1) "dc=Frank-n-Ted,dc=com" |

Answer RRs: 1
Authority RRs: 0
Additional RRs: 1

Queries

- _ldap._tcp.dc._msdcs.frank-n-ted.com: type SRV, class IN

Answers

- frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12

Additional records

- frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12

[Request In: 40780]
[Time: 0.000016200 seconds]

0000 00 11 75 68 42 d3 98 40 hh 2a f7 e5 08 00 45 00 ..uhR... *...F.

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

- IP address is 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
- Filter: ip.addr==10.6.12.0/24

| dhcp | | | | | | |
|-------|---------------|--------------------------------|------------------------------|----------|--------|------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 40771 | 397.091108700 | Frank-n-Ted-DC.frank-n-ted.com | 255.255.255.255 | DHCP | 351 | I |
| 41615 | 400.377685000 | Frank-n-Ted-DC.frank-n-ted.com | 255.255.255.255 | DHCP | 342 | I |
| 7063 | 92.073344300 | Rotterdam-PC.mind-hammer.net | 255.255.255.255 | DHCP | 342 | I |
| 15228 | 217.458410700 | Rotterdam-PC.mind-hammer.net | 255.255.255.255 | DHCP | 342 | I |
| 69121 | 658.134387400 | Rotterdam-PC.mind-hammer.net | 255.255.255.255 | DHCP | 342 | I |
| 7042 | 91.672246100 | mind-hammer-dc.mind-hammer.net | Rotterdam-PC.mind-hammer.net | DHCP | 342 | I |
| 15223 | 217.449107200 | mind-hammer-dc.mind-hammer.net | Rotterdam-PC.mind-hammer.net | DHCP | 342 | I |

| | | | | | | |
|--|--|--|--|--|--|--|
| Frame 40771: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0 | | | | | | |
| Interface id: 0 (eth0) | | | | | | |
| Encapsulation type: Ethernet (1) | | | | | | |
| Arrival Time: Nov 29, 2021 15:43:20.411329500 PST | | | | | | |
| [Time shift for this packet: 0.000000000 seconds] | | | | | | |
| Epoch Time: 1638229400.411329500 seconds | | | | | | |
| [Time delta from previous captured frame: 0.005616200 seconds] | | | | | | |
| [Time delta from previous displayed frame: 0.005616200 seconds] | | | | | | |
| [Time since reference or first frame: 397.091108700 seconds] | | | | | | |

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.

| http.request.method=="GET" and ip.addr==10.6.12.203 | | | | | | |
|---|---------------|---------------------------------|-----------------|----------|--------|---------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 44394 | 414.664864500 | LAPTOP-5WKHX9YG.frank-n-ted.com | 205.185.125.104 | HTTP | 275 | GET /pC |
| 44398 | 414.680262000 | LAPTOP-5WKHX9YG.frank-n-ted.com | 205.185.125.104 | HTTP | 312 | GET /f |

| | | | | | | |
|---|--|--|--|--|--|--|
| 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 | | | | | | |
| Cookie pair: _subid=3mmhfnd8jp\r\n | | | | | | |
| [Full request URI: http://205.185.125.104/files/june11.dll] | | | | | | |
| [HTTP request 2/2] | | | | | | |

| | | | |
|------|-------------------------|-------------------------|-----------------|
| 0000 | ec c8 82 29 41 7d 84 3a | 4b 6d fc e2 08 00 45 00 | ...A}.: Km...E. |
| 0010 | 01 2a ad fc 40 00 80 06 | e9 de 0a 06 0c cb cd b9 | ...@... |

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

| <div> <div>?</div> <div>Community Score</div> </div> | | <div> <div>ec</div> <div>Googleupdate.exe</div> <div>invalid-signature overlay pedll signed</div> </div> | <div> <div>347.04 KB</div> <div>Size</div> </div> | <div> <div>2021-11-27 09:20:47 UTC</div> <div>19 hours ago</div> </div> | <div> <div>DLL</div> </div> |
|--|----------------------------------|--|---|---|------------------------------------|
| DETECTION | | | | | |
| Ad-Aware | ① Trojan.Mint.Zamg.O | | AhnLab-V3 | | ① Malware/Win32.RL.Generic.R346613 |
| Alibaba | ① TrojanSpy:Win32/Yakes.8988e849 | | ALYac | | ① Trojan.Mint.Zamg.O |
| Antiy-AVL | ① GrayWare/Win32.Kryptik.ehls | | Arcabit | | ① Trojan.Mint.Zamg.O |

this is classified as a Trojan

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:174.16.4.205

MAC address:00:59:07:b0:63:a4

| No. | Time | Source | Destination | Protocol | Length |
|-------|---------------|------------------------------|------------------------------------|----------|--------|
| 15920 | 219.870867700 | 31.7.62.214 | Rotterdam-PC.mind-hammer.net | TCP | 54 |
| 15922 | 219.876246700 | 31.7.62.214 | Rotterdam-PC.mind-hammer.net | TCP | 54 |
| 15924 | 219.881616200 | 31.7.62.214 | Rotterdam-PC.mind-hammer.net | TCP | 54 |
| 15926 | 219.886994000 | 31.7.62.214 | Rotterdam-PC.mind-hammer.net | TCP | 54 |
| 4 | 0.046177900 | Rotterdam-PC.mind-hammer.net | b5689023.green.mattingsolutions.co | TCP | 66 |
| 6 | 0.069714400 | Rotterdam-PC.mind-hammer.net | b5689023.green.mattingsolutions.co | TCP | 60 |
| 10 | 0.138404900 | Rotterdam-PC.mind-hammer.net | b5689023.green.mattingsolutions.co | TCP | 60 |
| 11 | 0.120227500 | Rotterdam-PC.mind-hammer.net | b5689023.green.mattingsolutions.co | TCP | 60 |

Frame 15926: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0

Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Nov 29, 2021 15:40:23.207214800 PST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1638229223.207214800 seconds

[Time delta from previous captured frame: 0.000865900 seconds]

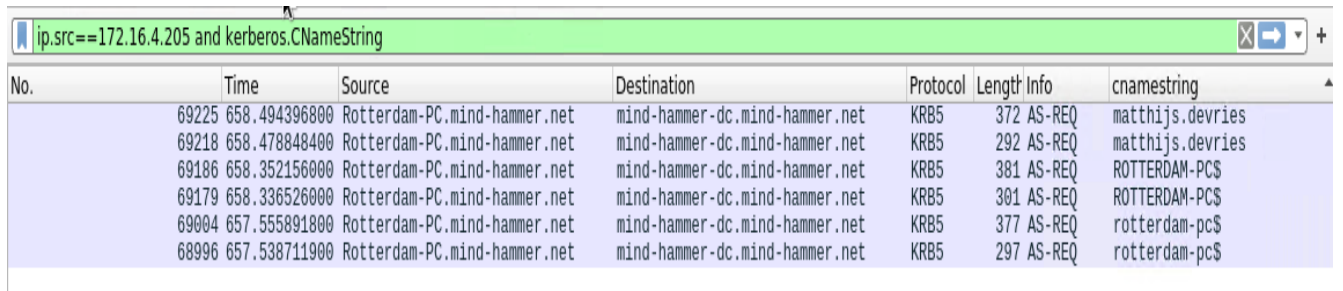
[Time delta from previous displayed frame: 0.000865900 seconds]

[Time since reference or first frame: 219.886994000 seconds]

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

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

user name: matthijs.devries



| No. | Time | Source | Destination | Protocol | Length | Info | cnamestring |
|-------|---------------|------------------------------|--------------------------------|----------|--------|--------|------------------|
| 69225 | 658.494396800 | Rotterdam-PC.mind-hammer.net | mind-hammer-dc.mind-hammer.net | KRB5 | 372 | AS-REQ | matthijs.devries |
| 69218 | 658.478848400 | Rotterdam-PC.mind-hammer.net | mind-hammer-dc.mind-hammer.net | KRB5 | 292 | AS-REQ | matthijs.devries |
| 69186 | 658.352156000 | Rotterdam-PC.mind-hammer.net | mind-hammer-dc.mind-hammer.net | KRB5 | 381 | AS-REQ | ROTTERDAM-PC\$ |
| 69179 | 658.336526000 | Rotterdam-PC.mind-hammer.net | mind-hammer-dc.mind-hammer.net | KRB5 | 301 | AS-REQ | ROTTERDAM-PC\$ |
| 69004 | 657.555891800 | Rotterdam-PC.mind-hammer.net | mind-hammer-dc.mind-hammer.net | KRB5 | 377 | AS-REQ | rotterdam-pc\$ |
| 68996 | 657.538711900 | Rotterdam-PC.mind-hammer.net | mind-hammer-dc.mind-hammer.net | KRB5 | 297 | AS-REQ | rotterdam-pc\$ |

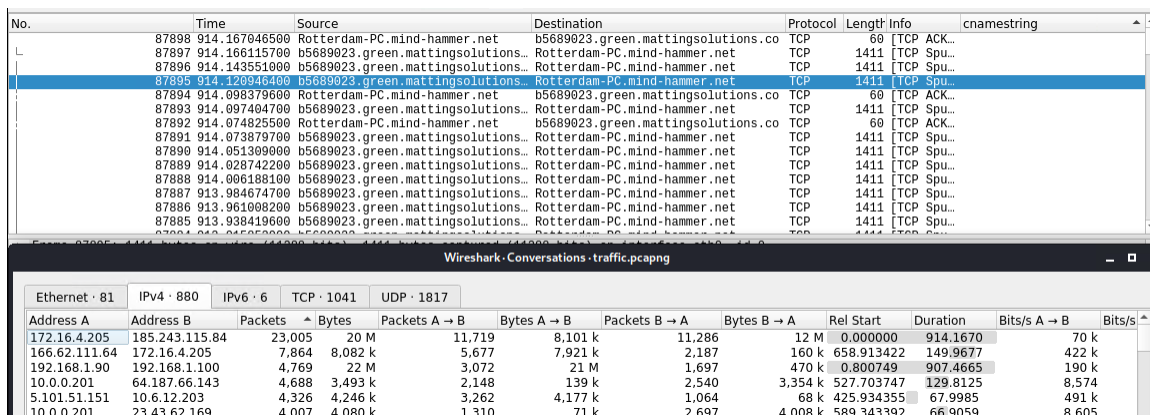
2.What are the IP addresses used in the actual infection traffic?

Based on the Conversations statistics and then filtering by the highest amount packets between IPs, 172.16.4.205, 185.243.115.84, 166.62.11.64 are the infected traffic.

Referencing 185.243.115.84 (b569023.green.mattingsolutions.co) there is a large amount of POST methods of empty.gif being sent without any originating GET request. This is suspicious.

Statistics > Conversations > IPv4 (tab) > Packets (high to low)

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



| No. | Time | Source | Destination | Protocol | Length | Info | cnamestring |
|-------|---------------|------------------------------------|------------------------------------|----------|--------|-------------|-------------|
| 87898 | 914.167046500 | Rotterdam-PC.mind-hammer.net | b5689023.green.mattingsolutions.co | TCP | 60 | [TCP ACK... | |
| 87897 | 914.166115700 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87896 | 914.143551000 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87895 | 914.120946400 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87894 | 914.098379600 | Rotterdam-PC.mind-hammer.net | b5689023.green.mattingsolutions.co | TCP | 60 | [TCP ACK... | |
| 87893 | 914.097494700 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87892 | 914.074825500 | Rotterdam-PC.mind-hammer.net | b5689023.green.mattingsolutions.co | TCP | 60 | [TCP ACK... | |
| 87891 | 914.073879700 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87890 | 914.051309000 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87889 | 914.028742200 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87888 | 914.006188100 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87887 | 913.984674700 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87886 | 913.961098200 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |
| 87885 | 913.938419600 | b5689023.green.mattingsolutions.co | Rotterdam-PC.mind-hammer.net | TCP | 1411 | [TCP Spu... | |

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
|---------------|----------------|---------|---------|---------------|-------------|---------------|-------------|------------|----------|--------------|--------------|
| 172.16.4.205 | 185.243.115.84 | 23,005 | 20 M | 11,719 | 8,101 k | 11,286 | 12 M | 0.000000 | 914.1670 | 70 k | |
| 166.62.111.64 | 172.16.4.205 | 7,864 | 8,082 k | 5,677 | 7,921 k | 2,187 | 160 k | 658.913422 | 149.9677 | 422 k | |
| 192.168.1.90 | 192.168.1.100 | 4,769 | 22 M | 3,072 | 21 M | 1,697 | 470 k | 0.800749 | 907.4665 | 190 k | |
| 10.0.0.201 | 64.187.66.143 | 4,688 | 3,493 k | 2,148 | 139 k | 2,540 | 3,354 k | 527.703747 | 129.8125 | 8,574 | |
| 5.101.51.151 | 10.6.12.203 | 4,326 | 4,246 k | 3,262 | 4,177 k | 1,064 | 68 k | 425.934355 | 67.9985 | 491 k | |
| 10.0.0.201 | 23.43.62.169 | 4,007 | 4,080 k | 1,310 | 71 k | 2,697 | 4,008 k | 589.343392 | 66.9059 | 8,605 | |

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
- Host Name (OS version): BLANCO-DESKTOP

| Source | Destination | Protocol | Length | Info | cnamestring | macAddress |
|-------------------------------------|----------------------------------|----------|--------|---------|------------------|--|
| 00 DogOfTheYear-DC.dogoftheyear.net | BLANCO-DESKTOP.dogoftheyear.net | KRB5 | 303 | TGS-REP | elmer.blanco | D... 00:16:17:18:66:c8,00:12:3f:f4:3b:96 |
| 00 DogOfTheYear-DC.dogoftheyear.net | BLANCO-DESKTOP.dogoftheyear.net | KRB5 | 175 | TGS-REP | elmer.blanco | D... 00:16:17:18:66:c8,00:12:3f:f4:3b:96 |
| 00 DogOfTheYear-DC.dogoftheyear.net | BLANCO-DESKTOP.dogoftheyear.net | KRB5 | 237 | AS-REP | elmer.blanco | D... 00:16:17:18:66:c8,00:12:3f:f4:3b:96 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 379 | AS-REQ | elmer.blanco | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 290 | AS-REQ | elmer.blanco | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 382 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 301 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 381 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 301 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 382 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 301 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 381 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |
| 00 BLANCO-DESKTOP.dogoftheyear.net | DogOfTheYear-DC.dogoftheyear.net | KRB5 | 301 | AS-REQ | blanco-desktop\$ | M... 00:12:3f:f4:3b:96,00:16:17:18:66:c8 |

```

Frame 5325: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface eth0, id 0
  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)
      Address: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
        ....0. .... = LG bit: Globally unique address (factory default)
        ....0. .... = IG bit: Individual address (unicast)
      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: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: DogOfTheYear-DC.dogoftheyear.net (10.0.0.2)
    0100 .... = Version: 4
  
```

Which torrent file did the user download?

Betty Boop Rythm on the Reservation.avi.torrent.

```

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
    Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\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 Edge/17.17134\r\n
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: www.publicdomaintorrents.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
    [HTTP request 1/1]
    [Response in frame: 56143]

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 00 06 0c 39 0a 00 00 c9 a8 d7  ?v@...9.....
```