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 th .6following questions:

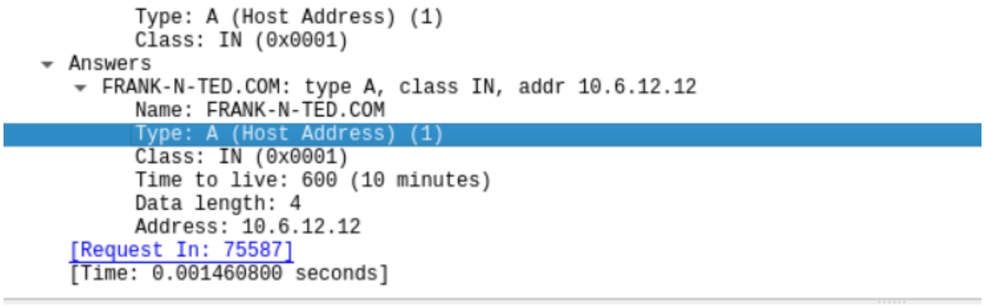
1. What is the domain name of the users' custom site?

   Search: ip.dst == 10.6.12.203

   Frank-N-Ted.com

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

   10.6.12.12

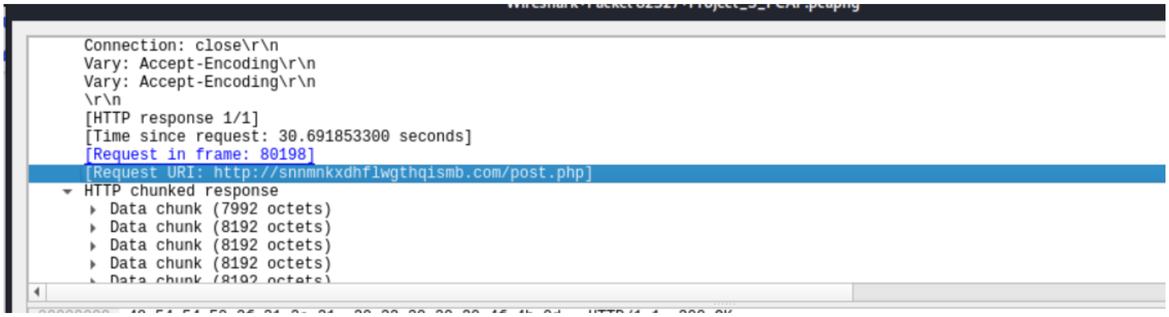


```
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ FRANK-N-TED.COM: type A, class IN, addr 10.6.12.12
        Name: FRANK-N-TED.COM
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 600 (10 minutes)
        Data length: 4
        Address: 10.6.12.12
  [Request In: 75587]
  [Time: 0.001460800 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.

   Filter Applied: dst.ip == 10.6.12.203

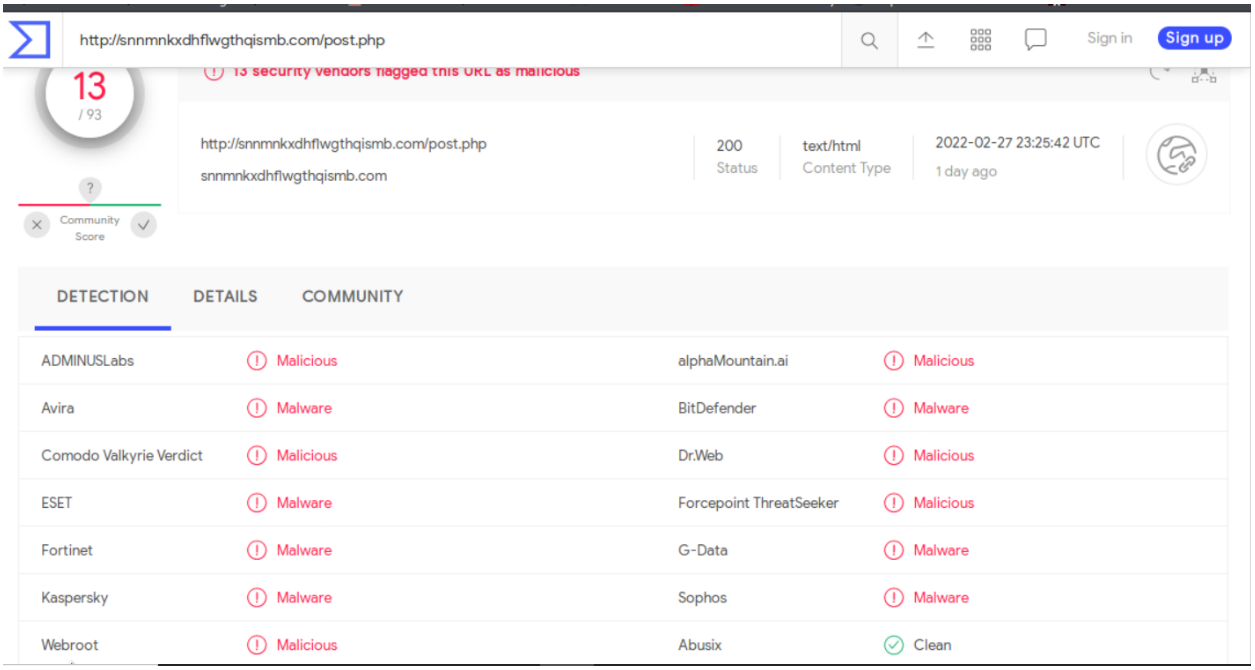
http://snnmnkxdhf1wgthqimb.com/post/php



```
Connection: close\r\n
Vary: Accept-Encoding\r\n
Vary: Accept-Encoding\r\n
\r\n
[HTTP response 1/1]
[Time since request: 30.691853300 seconds]
[Request in frame: 80198]
[Request URI: http://snnmnkxdhflwgthqismb.com/post.php]
HTTP chunked response
  Data chunk (7992 octets)
  Data chunk (8192 octets)
  Data chunk (8192 octets)
  Data chunk (8192 octets)
  Data chunk (8192 octets)
```

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

Classified as Malicious Malware.



http://snnmnkxdhflwgthqismb.com/post.php

13 security vendors flagged this URL as malicious

13 / 93

Community Score

http://snnmnkxdhflwgthqismb.com/post.php snnmnkxdhflwgthqismb.com	200 Status	text/html Content Type	2022-02-27 23:25:42 UTC 1 day ago

DETECTION DETAILS COMMUNITY

ADMINUSLabs	Malicious	alphaMountain.ai	Malicious
Avira	Malware	BitDefender	Malware
Comodo Valkyrie Verdict	Malicious	Dr.Web	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Kaspersky	Malware	Sophos	Malware
Webroot	Malicious	Abusix	Clean

Vulnerable Windows Machines

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

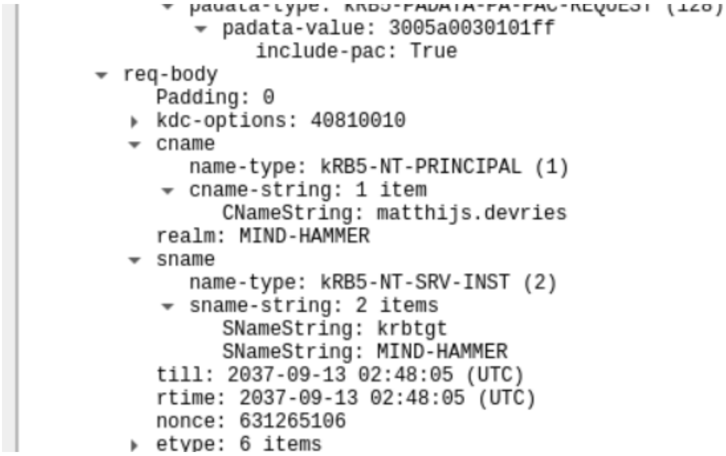
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

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

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

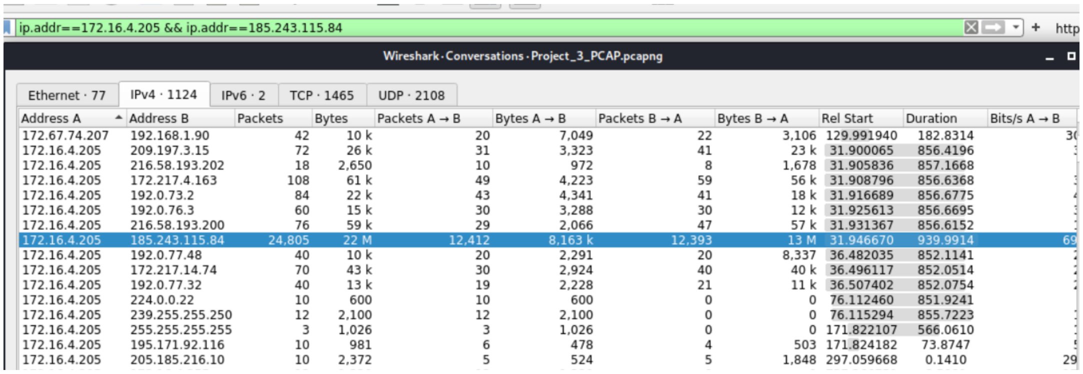
   matthijs.devries



```
      ▾ padata-type: kRB5-PADATA-PA-PAC-REQUEST (128)
        ▾ padata-value: 3005a0030101ff
              include-pac: True
  ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▾ cname
            name-type: kRB5-NT-PRINCIPAL (1)
          ▾ cname-string: 1 item
                CNameString: matthijs.devries
        realm: MIND-HAMMER
      ▾ sname
            name-type: kRB5-NT-SRV-INST (2)
          ▾ sname-string: 2 items
                SNameString: krbtgt
                SNameString: MIND-HAMMER
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 631265106
      ▸ etype: 6 items
```

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

   Source ip: 172.16.4.205 –   Destination ip:185.243.115.84



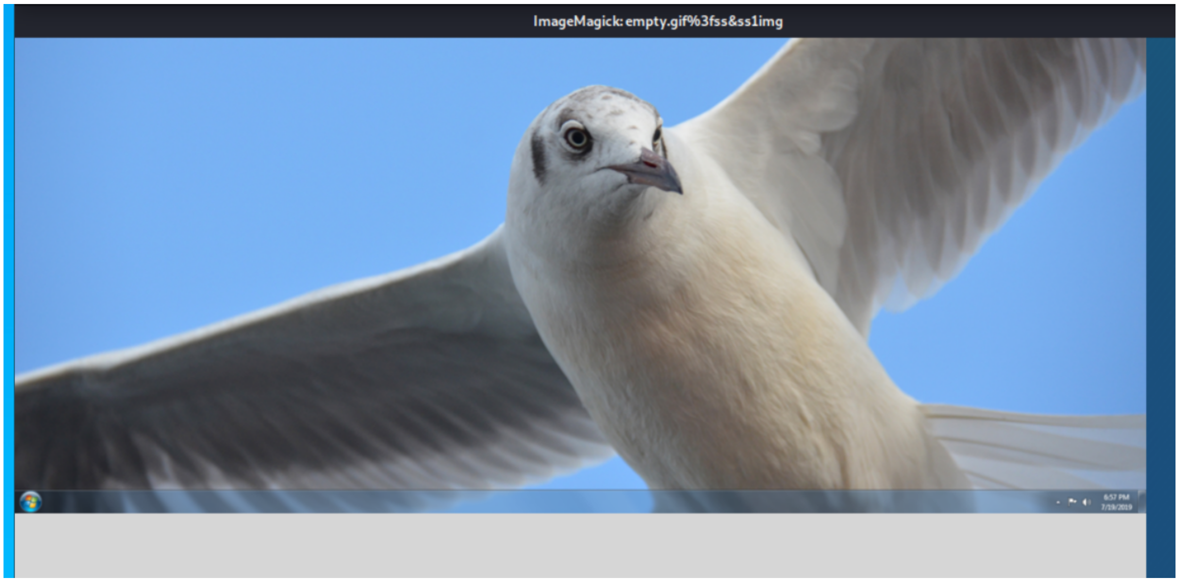
ip.addr==172.16.4.205 && ip.addr==185.243.115.84

Wireshark · Conversations · Project_3_PCAP.pcapng

Ethernet · 77 | IPv4 · 1124 | IPv6 · 2 | TCP · 1465 | UDP · 2108

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
172.67.74.207	192.168.1.90	42	10 k	20	7,049	22	3,106	129.991940	182.8314	30
172.16.4.205	209.197.3.15	72	26 k	31	3,323	41	23 k	31.900065	856.4196	3
172.16.4.205	216.58.193.202	18	2,650	10	972	8	1,678	31.905836	857.1668	
172.16.4.205	172.217.4.163	108	61 k	49	4,223	59	56 k	31.908796	856.6368	3
172.16.4.205	192.0.73.2	84	22 k	43	4,341	41	18 k	31.916689	856.6775	4
172.16.4.205	192.0.76.3	60	15 k	30	3,288	30	12 k	31.925613	856.6695	3
172.16.4.205	216.58.193.200	76	59 k	29	2,066	47	57 k	31.931367	856.6152	1
172.16.4.205	185.243.115.84	24,805	22 M	12,412	8,163 k	12,393	13 M	31.946670	939.9914	69
172.16.4.205	192.0.77.48	40	10 k	20	2,291	20	8,337	36.482035	852.1141	2
172.16.4.205	172.217.14.74	70	43 k	30	2,924	40	40 k	36.496117	852.0514	2
172.16.4.205	192.0.77.32	40	13 k	19	2,228	21	11 k	36.507402	852.0754	2
172.16.4.205	224.0.0.22	10	600	10	600	0	0	76.112460	851.9241	
172.16.4.205	239.255.255.250	12	2,100	12	2,100	0	0	76.115294	855.7223	1
172.16.4.205	255.255.255.255	3	1,026	3	1,026	0	0	171.822107	566.0610	1
172.16.4.205	195.171.92.116	10	981	6	478	4	503	171.824182	73.8747	5
172.16.4.205	205.185.216.10	10	2,372	5	524	5	1,848	297.059668	0.1410	29

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



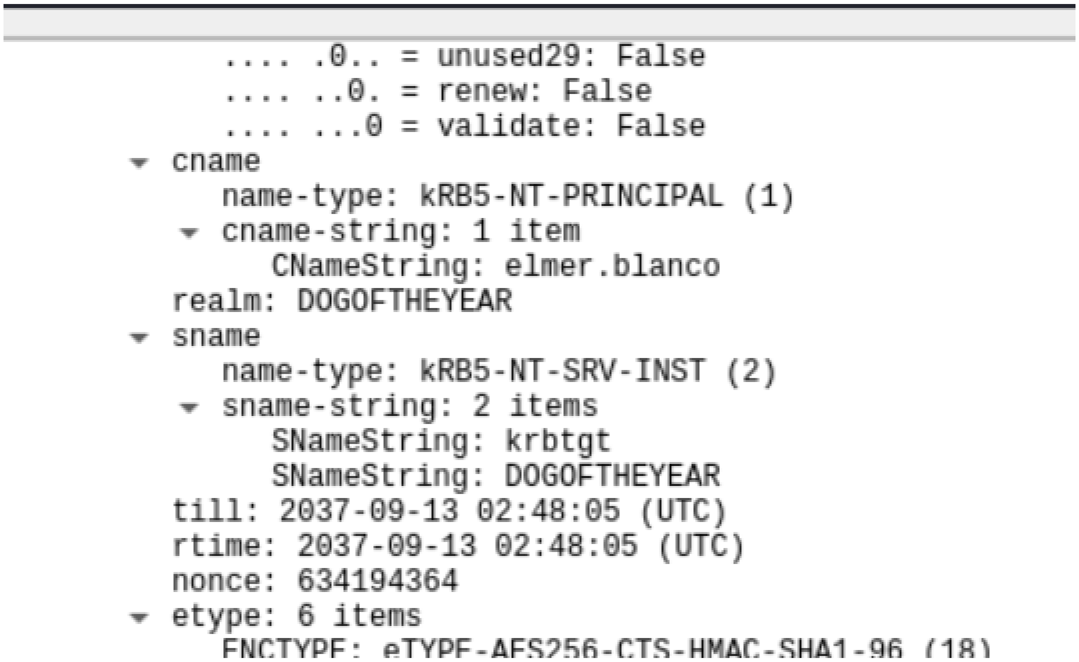
Illegal Downloads

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:

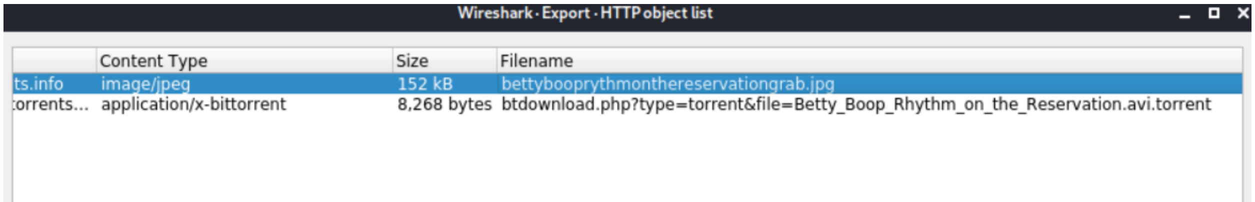
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

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
   - Host Name: BLANCO-DESKTOP
   - 

```
        .... .0.. = unused29: False
        .... ..0. = renew: False
        .... ...0 = validate: False
    ▾ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
            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)
    nonce: 634194364
    ▾ etype: 6 items
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
```

2. Which torrent file did the user download?



	Content Type	Size	Filename
ts.info	image/jpeg	152 kB	bettybooprythmonthereservationgrab.jpg
torrents...	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent