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:

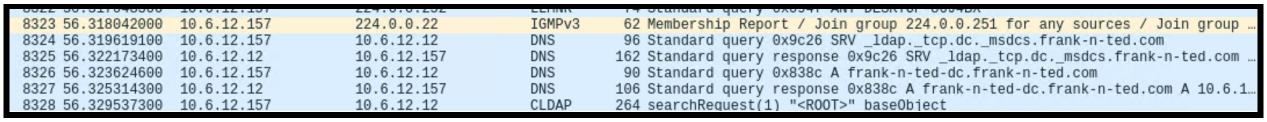
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

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

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

   Domain name: Frank-n-Ted-DC.frank-n-ted.com

   Filter: ip.addr==10.6.12.0/24

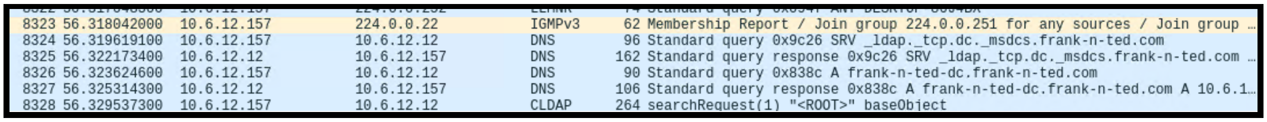


```
8323 56.318042000  10.6.12.157     224.0.0.22     IGMPv3    62 Membership Report / Join group 224.0.0.251 for any sources / Join group …
8324 56.319619100  10.6.12.157     10.6.12.12     DNS       96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
8325 56.322173400  10.6.12.12      10.6.12.157    DNS      162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
8326 56.323624600  10.6.12.157     10.6.12.12     DNS       90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
8327 56.325314300  10.6.12.12      10.6.12.157    DNS      106 Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1…
8328 56.329537300  10.6.12.157     10.6.12.12     CLDAP    264 searchRequest(1) "<ROOT>" baseObject
```

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

   IP address: 10.6.12.12

   Filter: ip.addr==10.6.12.0/24



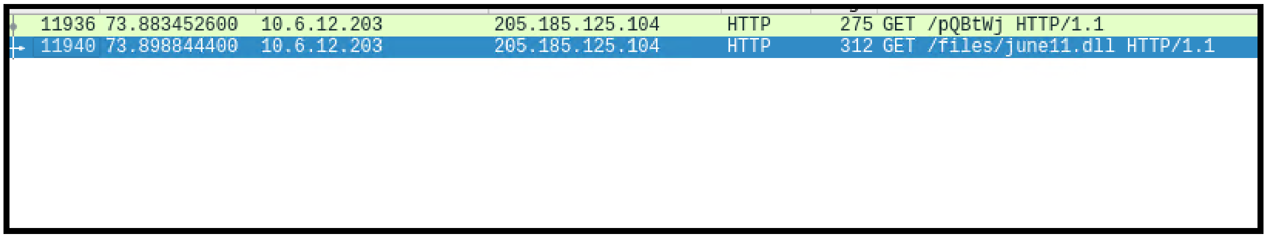
```
8323 56.318042000  10.6.12.157     224.0.0.22     IGMPv3    62 Membership Report / Join group 224.0.0.251 for any sources / Join group …
8324 56.319619100  10.6.12.157     10.6.12.12     DNS       96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
8325 56.322173400  10.6.12.12      10.6.12.157    DNS      162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
8326 56.323624600  10.6.12.157     10.6.12.12     DNS       90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
8327 56.325314300  10.6.12.12      10.6.12.157    DNS      106 Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1…
8328 56.329537300  10.6.12.157     10.6.12.12     CLDAP    264 searchRequest(1) "<ROOT>" baseObject
```

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.

   Malware: June11.dll

   Filter: ip.addr==10.16.12.203 and http.request.method==GET

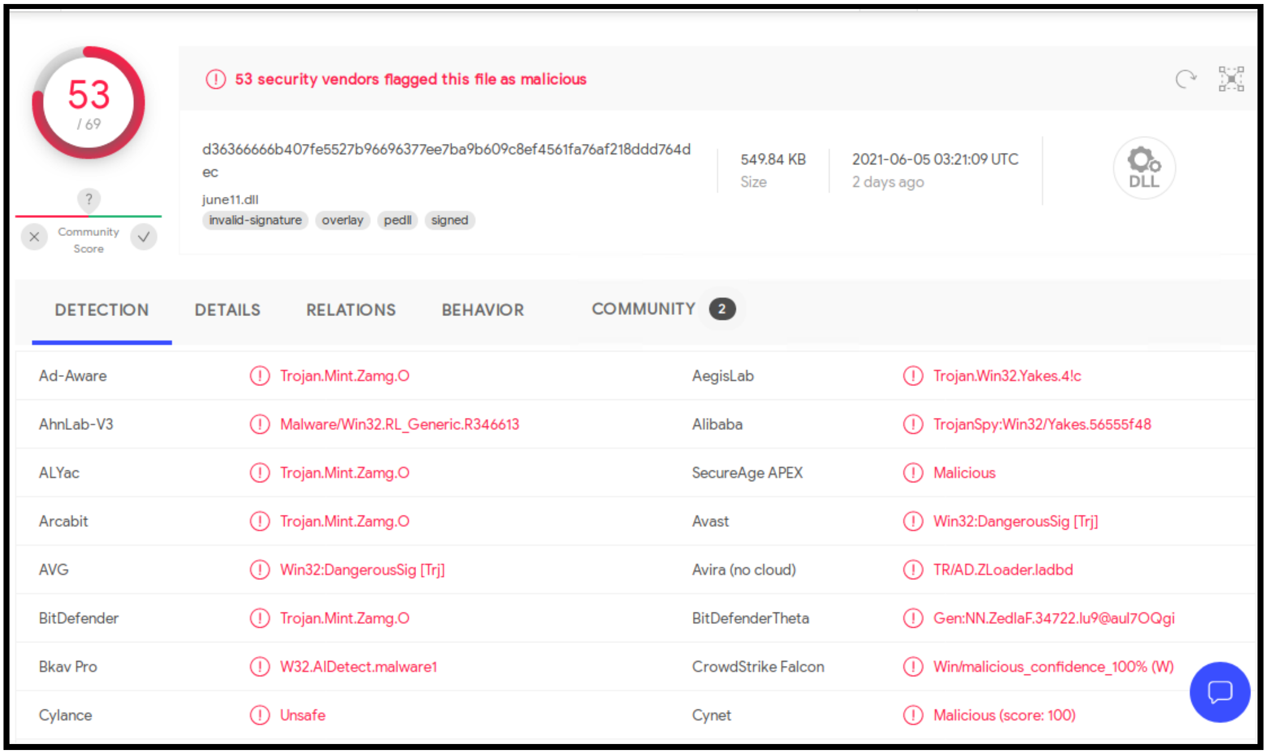
   File exported into Kali machine.



```
11936 73.883452600  10.6.12.203          205.185.125.104      HTTP       275 GET /pQBtWj HTTP/1.1
11940 73.898844400  10.6.12.203          205.185.125.104      HTTP       312 GET /files/june11.dll HTTP/1.1
```

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

   Malware file classified as a Trojan.



53
/ 69

Community Score

53 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764d
ec

june11.dll

invalid-signature overlay pedll signed

549.84 KB
Size

2021-06-05 03:21:09 UTC
2 days ago

DLL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	Trojan.Win32.Yakes.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	SecureAge APEX	Malicious
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.34722.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware1	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)

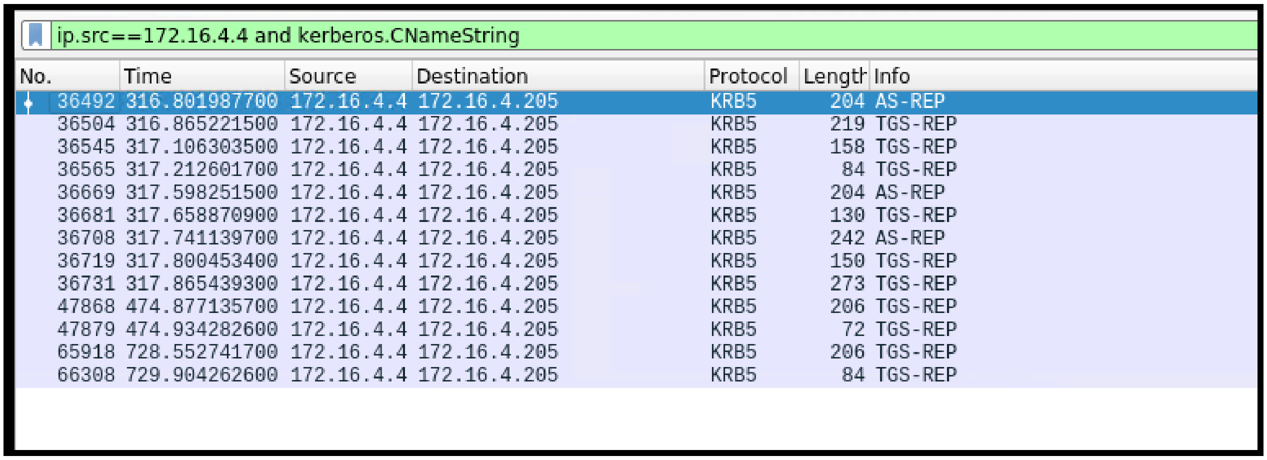
Vulnerable Windows Machines

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.CName.String**



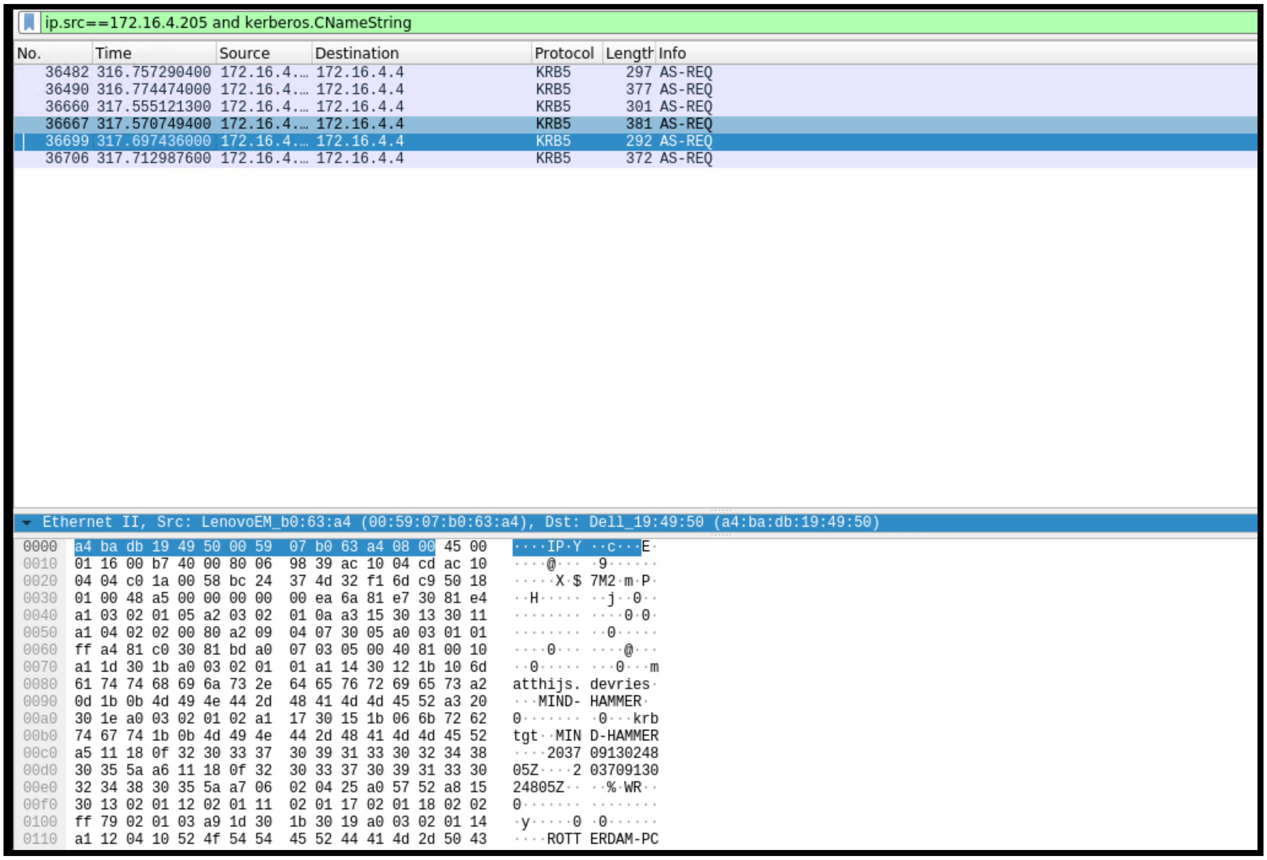
ip.src==172.16.4.4 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
36492	316.801987700	172.16.4.4	172.16.4.205	KRB5	204	AS-REP
36504	316.865221500	172.16.4.4	172.16.4.205	KRB5	219	TGS-REP
36545	317.106303500	172.16.4.4	172.16.4.205	KRB5	158	TGS-REP
36565	317.212601700	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP
36669	317.598251500	172.16.4.4	172.16.4.205	KRB5	204	AS-REP
36681	317.658870900	172.16.4.4	172.16.4.205	KRB5	130	TGS-REP
36708	317.741139700	172.16.4.4	172.16.4.205	KRB5	242	AS-REP
36719	317.800453400	172.16.4.4	172.16.4.205	KRB5	150	TGS-REP
36731	317.865439300	172.16.4.4	172.16.4.205	KRB5	273	TGS-REP
47868	474.877135700	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
47879	474.934282600	172.16.4.4	172.16.4.205	KRB5	72	TGS-REP
65918	728.552741700	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
66308	729.904262600	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP

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

    Username: matthjs.devries

    Filter: ip.src==172.16.4.205 and kerberos.CName.String



ip.src==172.16.4.205 and kerberos.CNameString

```
No.      Time           Source       Destination        Protocol  Length Info
   36482 316.757290400 172.16.4.… 172.16.4.4            KRB5         297 AS-REQ
   36490 316.774474000 172.16.4.… 172.16.4.4            KRB5         377 AS-REQ
   36660 317.555121300 172.16.4.… 172.16.4.4            KRB5         301 AS-REQ
   36667 317.570749400 172.16.4.… 172.16.4.4            KRB5         381 AS-REQ
   36699 317.697436000 172.16.4.… 172.16.4.4            KRB5         292 AS-REQ
   36706 317.712987600 172.16.4.… 172.16.4.4            KRB5         372 AS-REQ
```

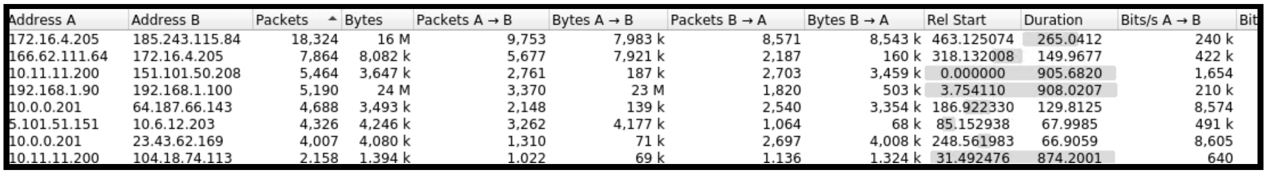
```
Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell_19:49:50 (a4:ba:db:19:49:50)
0000  a4 ba db 19 49 50 00 59  07 b0 63 a4 08 00 45 00   ····IP·Y ··c···E·
0010  01 16 00 b7 40 00 80 06  98 39 ac 10 04 cd ac 10   ····@··· ·9······
0020  04 04 c0 1a 00 58 bc 24  37 4d 32 f1 6d c9 50 18   ·····X·$ 7M2·m·P·
0030  01 00 48 a5 00 00 00 00  00 ea 6a 81 e7 30 81 e4   ··H····· ··j··0··
0040  a1 03 02 01 05 a2 03 02  01 0a a3 15 30 13 30 11   ········ ····0·0·
0050  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
0060  ff a4 81 c0 30 81 bd a0  07 03 05 00 40 81 00 10   ····0··· ····@···
0070  a1 1d 30 1b a0 03 02 01  01 a1 14 30 12 1b 10 6d   ··0····· ···0···m
0080  61 74 74 68 69 6a 73 2e  64 65 76 72 69 65 73 a2   atthijs. devries·
0090  0d 1b 0b 4d 49 4e 44 2d  48 41 4d 4d 45 52 a3 20   ···MIND- HAMMER·
00a0  30 1e a0 03 02 01 02 a1  17 30 15 1b 06 6b 72 62   0······· ·0···krb
00b0  74 67 74 1b 0b 4d 49 4e  44 2d 48 41 4d 4d 45 52   tgt··MIN D-HAMMER
00c0  a5 11 18 0f 32 30 33 37  30 39 31 33 30 32 34 38   ····2037 09130248
00d0  30 35 5a a6 11 18 0f 32  30 33 37 30 39 31 33 30   05Z····2 03709130
00e0  32 34 38 30 35 5a a7 06  02 04 25 a0 57 52 a8 15   24805Z·· ··%·WR··
00f0  30 13 02 01 12 02 01 11  02 01 17 02 01 18 02 02   0······· ········
0100  ff 79 02 01 03 a9 1d 30  1b 30 19 a0 03 02 01 14   ·y·····0 ·0······
0110  a1 12 04 10 52 4f 54 54  45 52 44 41 4d 2d 50 43   ····ROTT ERDAM-PC
```

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

   Infected traffic IP address: 172.16.4.205, 185.243.115.84, 166.62.11.64.

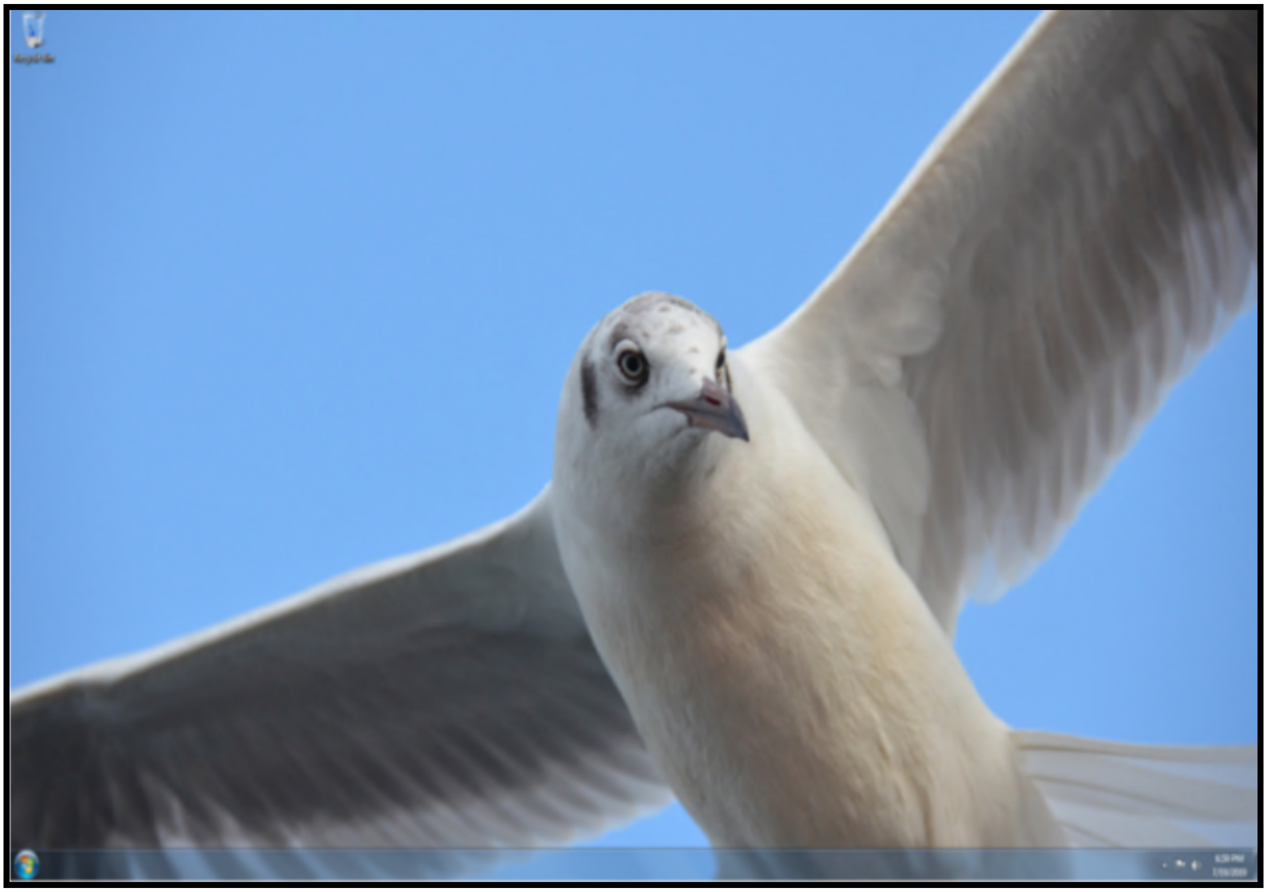
   Possible suspicious activity detected since IP 185.243.115.84 has a lot of POST methods of empty.gifs transmitted with no GET requests.

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



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	Bit
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	463.125074	265.0412	240 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	318.132008	149.9677	422 k	
10.11.11.200	151.101.50.208	5,464	3,647 k	2,761	187 k	2,703	3,459 k	0.000000	905.6820	1,654	
192.168.1.90	192.168.1.100	5,190	24 M	3,370	23 M	1,820	503 k	3.754110	908.0207	210 k	
10.0.0.201	64.187.66.143	4,688	3,493 k	2,148	139 k	2,540	3,354 k	186.922330	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	85.152938	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	248.561983	66.9059	8,605	
10.11.11.200	104.18.74.113	2,158	1,394 k	1,022	69 k	1,136	1,324 k	31.492476	874.2001	640	

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.

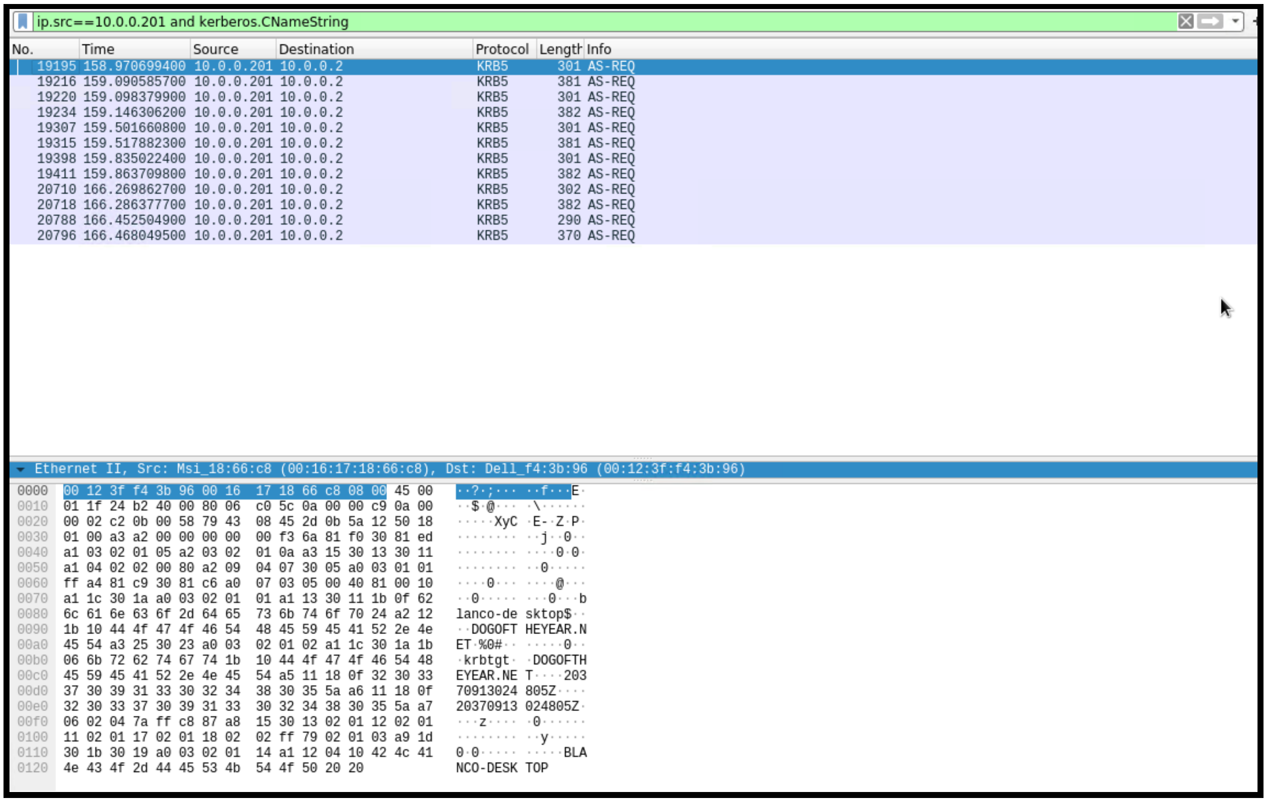
IT shared the following about the torrent activity:

- 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:

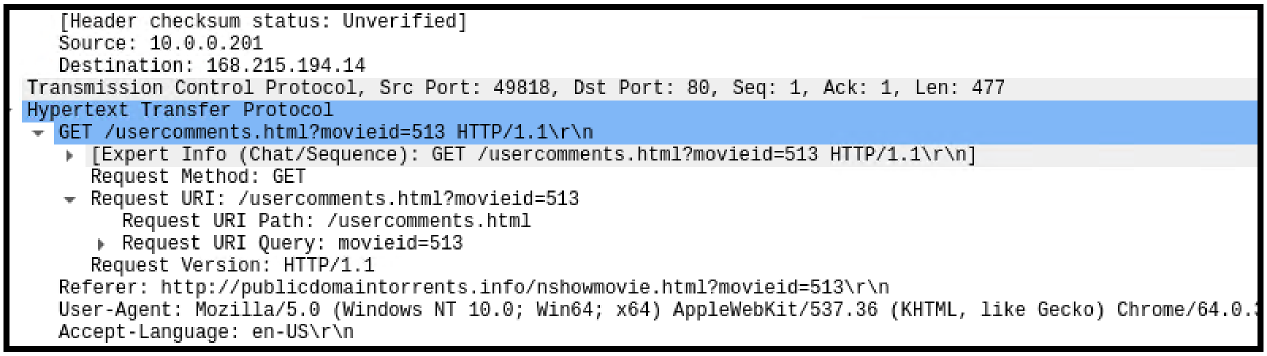
- MAC address: **00:16:17:18:66:c8**
- Windows username: **elmer.blanco**
- OS version: **BLANCO-DESKTOP, Windows NT 10 X64**
- **Filter: ip.src==10.0.0.201 and kerberos.CNameString**



```
ip.src==10.0.0.201 and kerberos.CNameString

No.     Time            Source      Destination     Protocol  Length Info
  19195 158.970699400 10.0.0.201 10.0.0.2         KRB5       301 AS-REQ
  19216 159.090585700 10.0.0.201 10.0.0.2         KRB5       381 AS-REQ
  19220 159.098379900 10.0.0.201 10.0.0.2         KRB5       301 AS-REQ
  19234 159.146306200 10.0.0.201 10.0.0.2         KRB5       382 AS-REQ
  19307 159.501660800 10.0.0.201 10.0.0.2         KRB5       301 AS-REQ
  19315 159.517882300 10.0.0.201 10.0.0.2         KRB5       381 AS-REQ
  19398 159.835022400 10.0.0.201 10.0.0.2         KRB5       301 AS-REQ
  19411 159.863709800 10.0.0.201 10.0.0.2         KRB5       382 AS-REQ
  20710 166.269862700 10.0.0.201 10.0.0.2         KRB5       302 AS-REQ
  20718 166.286377700 10.0.0.201 10.0.0.2         KRB5       382 AS-REQ
  20788 166.452504900 10.0.0.201 10.0.0.2         KRB5       290 AS-REQ
  20796 166.468049500 10.0.0.201 10.0.0.2         KRB5       370 AS-REQ

▾ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
0000  00 12 3f f4 3b 96 00 16  17 18 66 c8 08 00 45 00   ··?·;··· ··f···E·
0010  01 1f 24 b2 40 00 80 06  c0 5c 0a 00 00 c9 0a 00   ··$·@··· ·\······
0020  00 02 c2 0b 00 58 79 43  08 45 2d 0b 5a 12 50 18   ·····XyC ·E-·Z·P·
0030  01 00 a3 a2 00 00 00 00  00 f3 6a 81 f0 30 81 ed   ········ ··j··0··
0040  a1 03 02 01 05 a2 03 02  01 0a a3 15 30 13 30 11   ········ ····0·0·
0050  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
0060  ff a4 81 c9 30 81 c6 a0  07 03 05 00 40 81 00 10   ····0··· ····@···
0070  a1 1c 30 1a a0 03 02 01  01 a1 13 30 11 1b 0f 62   ··0····· ···0···b
0080  6c 61 6e 63 6f 2d 64 65  73 6b 74 6f 70 24 a2 12   lanco-de sktop$··
0090  1b 10 44 4f 47 4f 46 54  48 45 59 45 41 52 2e 4e   ··DOGOFT HEYEAR.N
00a0  45 54 a3 25 30 23 a0 03  02 01 02 a1 1c 30 1a 1b   ET·%0#·· ·····0··
00b0  06 6b 72 62 74 67 74 1b  10 44 4f 47 4f 46 54 48   ·krbtgt· ·DOGOFTH
00c0  45 59 45 41 52 2e 4e 45  54 a5 11 18 0f 32 30 33   EYEAR.NE T····203
00d0  37 30 39 31 33 30 32 34  38 30 35 5a a6 11 18 0f   70913024 805Z····
00e0  32 30 33 37 30 39 31 33  30 32 34 38 30 35 5a a7   20370913 024805Z·
00f0  06 02 04 7a ff c8 87 a8  15 30 13 02 01 12 02 01   ···z···· ·0······
0100  11 02 01 17 02 01 18 02  02 ff 79 02 01 03 a9 1d   ········ ··y·····
0110  30 1b 30 19 a0 03 02 01  14 a1 12 04 10 42 4c 41   0·0····· ·····BLA
0120  4e 43 4f 2d 44 45 53 4b  54 4f 50 20 20            NCO-DESK TOP
```

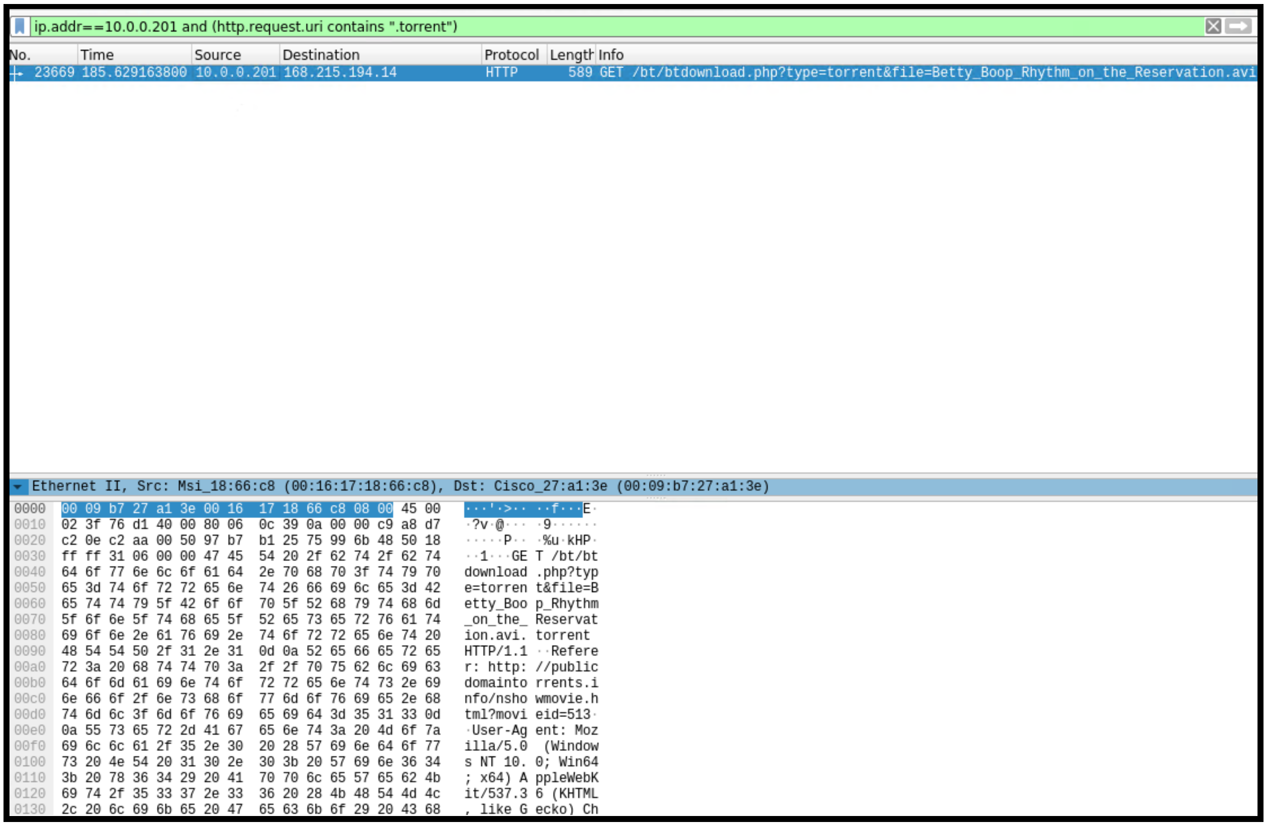


```
    [Header checksum status: Unverified]
    Source: 10.0.0.201
    Destination: 168.215.194.14
Transmission Control Protocol, Src Port: 49818, Dst Port: 80, Seq: 1, Ack: 1, Len: 477
Hypertext Transfer Protocol
  ▾ GET /usercomments.html?movieid=513 HTTP/1.1\r\n
      ▸ [Expert Info (Chat/Sequence): GET /usercomments.html?movieid=513 HTTP/1.1\r\n]
        Request Method: GET
      ▾ Request URI: /usercomments.html?movieid=513
            Request URI Path: /usercomments.html
          ▸ Request URI Query: movieid=513
        Request Version: HTTP/1.1
    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.
    Accept-Language: en-US\r\n
```

2. Which torrent file did the user download?

Torrent file: Betty_Boop_Rythm_on_the_Reservation.avi.torrent.

Filter: ip.addr==10.0.0.201 and (http.request.uri contains “.torrent”)



```
ip.addr==10.0.0.201 and (http.request.uri contains ".torrent")
```

```
No.   Time          Source      Destination     Protocol Length Info
23669 185.629163800 10.0.0.201  168.215.194.14  HTTP        589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi
```

```
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
```

```
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
00b0  64 6f 6d 61 69 6e 74 6f  72 72 65 6e 74 73 2e 69   domainto rrents.i
00c0  6e 66 6f 2f 6e 73 68 6f  77 6d 6f 76 69 65 2e 68   nfo/nsho wmovie.h
00d0  74 6d 6c 3f 6d 6f 76 69  65 69 64 3d 35 31 33 0d   tml?movi eid=513·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00f0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0100  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0110  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0120  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0130  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
```