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`.

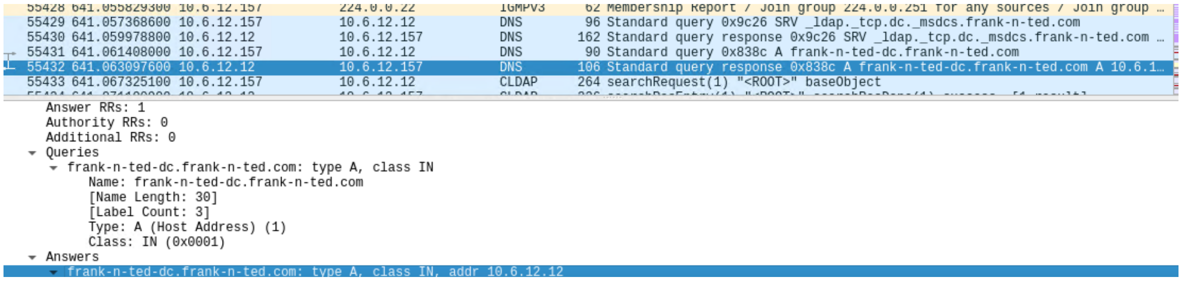
You must inspect your traffic capture to answer the following questions:

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

   Frank-n-ted.com

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

   10.6.12.12

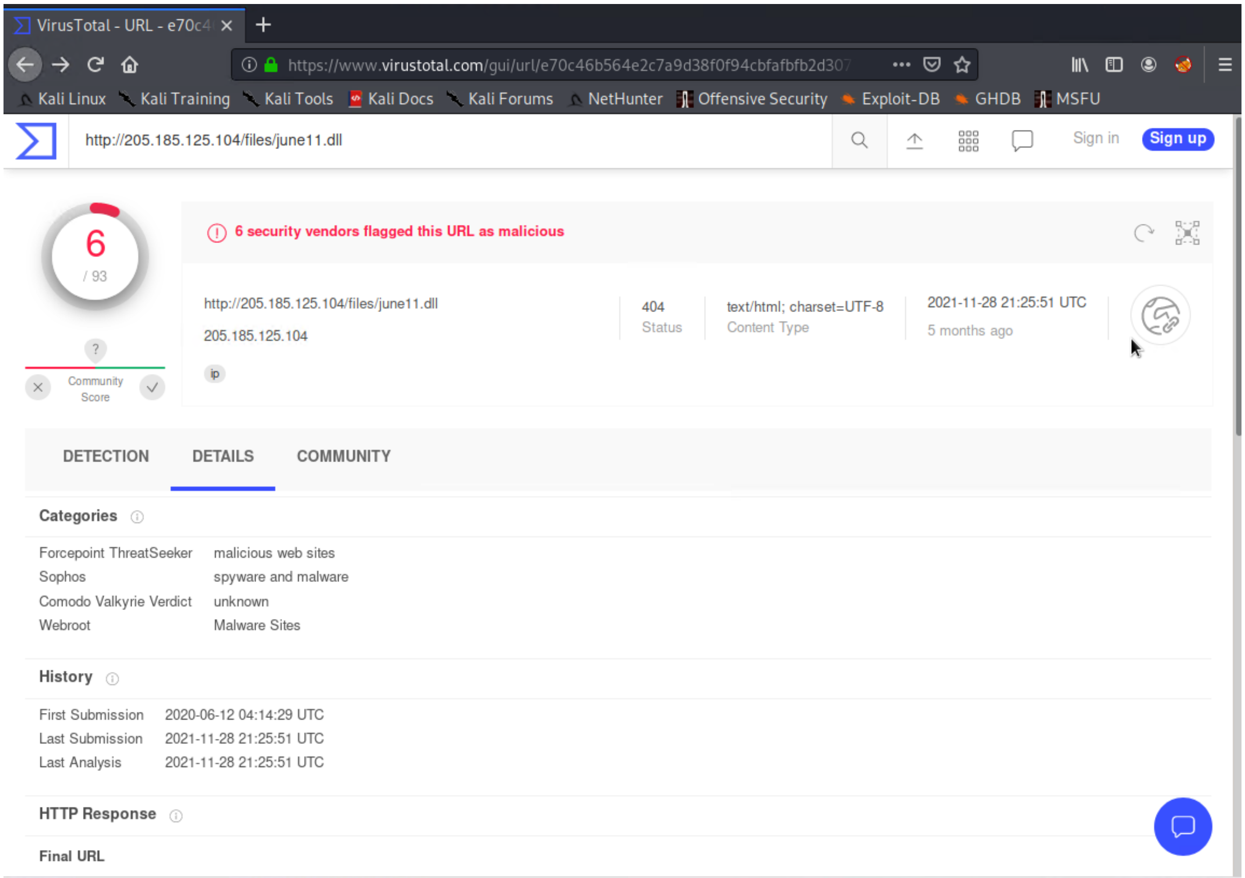
   ```
   55428 641.055829300 10.6.12.157        224.0.0.22          IGMPv3      62 Membership Report / Join group 224.0.0.251 for any sources / Join group …
   55429 641.057368600 10.6.12.157        10.6.12.12          DNS         96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
   55430 641.059978800 10.6.12.12         10.6.12.157         DNS        162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
   55431 641.061408000 10.6.12.157        10.6.12.12          DNS         90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
   55432 641.063097600 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…
   55433 641.067325100 10.6.12.157        10.6.12.12          CLDAP      264 searchRequest(1) "<ROOT>" baseObject
       Answer RRs: 1
       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)
     ▾ Answers
       ▾ frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12
   ```

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.

   June11.dll

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

   Spyware and Malware



http://205.185.125.104/files/june11.dll

6 / 93

Community Score

6 security vendors flagged this URL as malicious

http://205.185.125.104/files/june11.dll
205.185.125.104
ip

404
Status

text/html; charset=UTF-8
Content Type

2021-11-28 21:25:51 UTC
5 months ago

Categories

Forcepoint ThreatSeeker	malicious web sites
Sophos	spyware and malware
Comodo Valkyrie Verdict	unknown
Webroot	Malware Sites

History

First Submission	2020-06-12 04:14:29 UTC
Last Submission	2021-11-28 21:25:51 UTC
Last Analysis	2021-11-28 21:25:51 UTC

HTTP Response

Final URL

Vulnerable Windows Machines

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

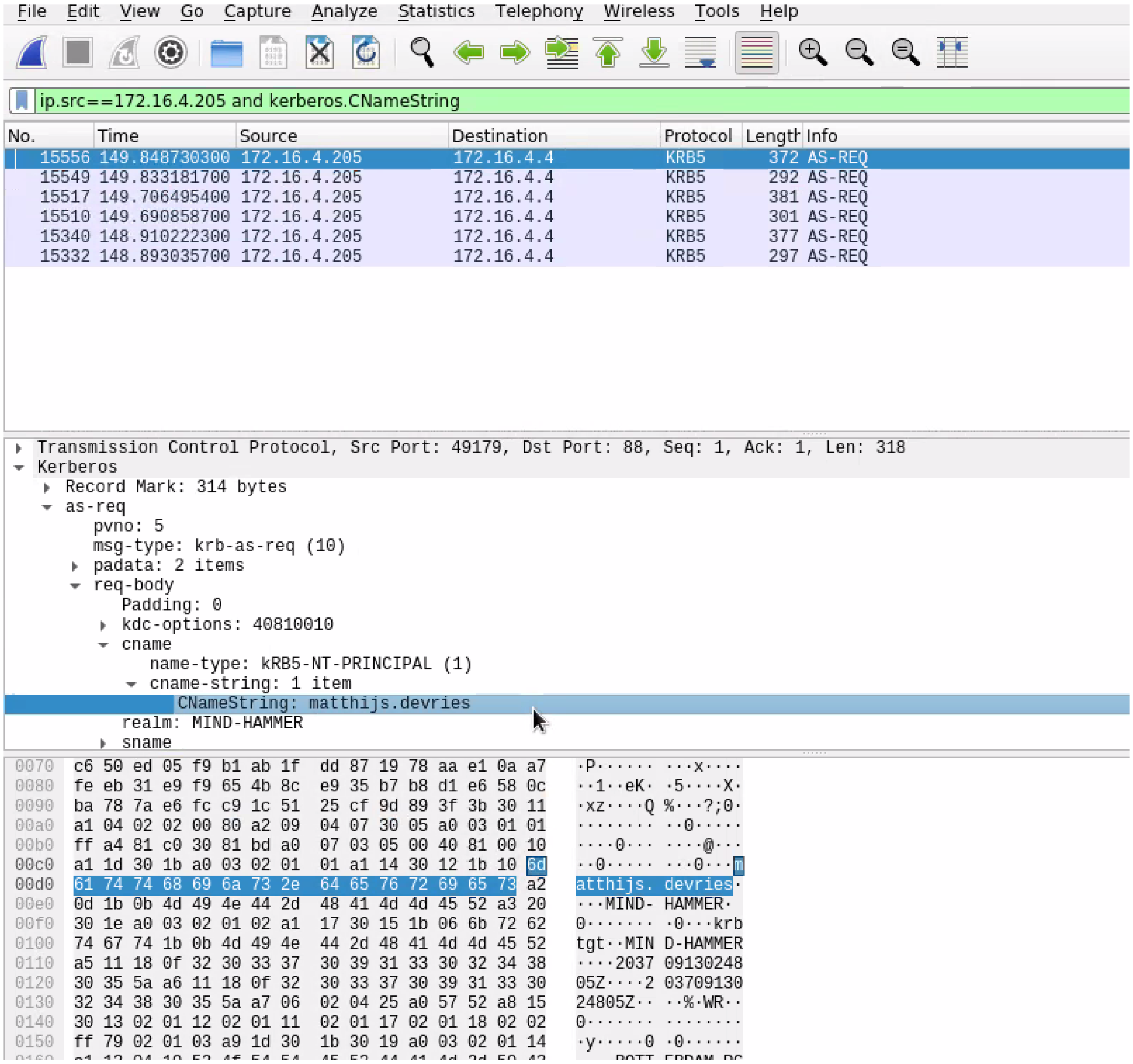
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

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



```
ip.src==172.16.4.205 and kerberos.CNameString
```

```
No.    Time          Source         Destination    Protocol Length Info
 15556 149.848730300 172.16.4.205   172.16.4.4     KRB5        372 AS-REQ
 15549 149.833181700 172.16.4.205   172.16.4.4     KRB5        292 AS-REQ
 15517 149.706495400 172.16.4.205   172.16.4.4     KRB5        381 AS-REQ
 15510 149.690858700 172.16.4.205   172.16.4.4     KRB5        301 AS-REQ
 15340 148.910222300 172.16.4.205   172.16.4.4     KRB5        377 AS-REQ
 15332 148.893035700 172.16.4.205   172.16.4.4     KRB5        297 AS-REQ
```

```
▸ Transmission Control Protocol, Src Port: 49179, Dst Port: 88, Seq: 1, Ack: 1, Len: 318
▾ Kerberos
  ▸ Record Mark: 314 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 2 items
    ▾ 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
```

```
0070  c6 50 ed 05 f9 b1 ab 1f  dd 87 19 78 aa e1 0a a7   ·P······ ···x····
0080  fe eb 31 e9 f9 65 4b 8c  e9 35 b7 b8 d1 e6 58 0c   ··1··eK· ·5····X·
0090  ba 78 7a e6 fc c9 1c 51  25 cf 9d 89 3f 3b 30 11   ·xz····Q %···?;0·
00a0  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
00b0  ff a4 81 c0 30 81 bd a0  07 03 05 00 40 81 00 10   ····0··· ····@···
00c0  a1 1d 30 1b a0 03 02 01  01 a1 14 30 12 1b 10 6d   ··0····· ···0···m
00d0  61 74 74 68 69 6a 73 2e  64 65 76 72 69 65 73 a2   atthijs. devries·
00e0  0d 1b 0b 4d 49 4e 44 2d  48 41 4d 4d 45 52 a3 20   ···MIND- HAMMER·
00f0  30 1e a0 03 02 01 02 a1  17 30 15 1b 06 6b 72 62   0······· ·0···krb
0100  74 67 74 1b 0b 4d 49 4e  44 2d 48 41 4d 4d 45 52   tgt··MIN D-HAMMER
0110  a5 11 18 0f 32 30 33 37  30 39 31 33 30 32 34 38   ····2037 09130248
0120  30 35 5a a6 11 18 0f 32  30 33 37 30 39 31 33 30   05Z····2 03709130
0130  32 34 38 30 35 5a a7 06  02 04 25 a0 57 52 a8 15   24805Z·· ··%·WR··
0140  30 13 02 01 12 02 01 11  02 01 17 02 01 18 02 02   0······· ········
0150  ff 79 02 01 03 a9 1d 30  1b 30 19 a0 03 02 01 14   ·y·····0 ·0······
```

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

   - The infected device is at 172.16.4.205
   - We see traffic interactions with 205.185.216.10, 185.243.115.84, 166.62.111.64

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

IllegalDownloads

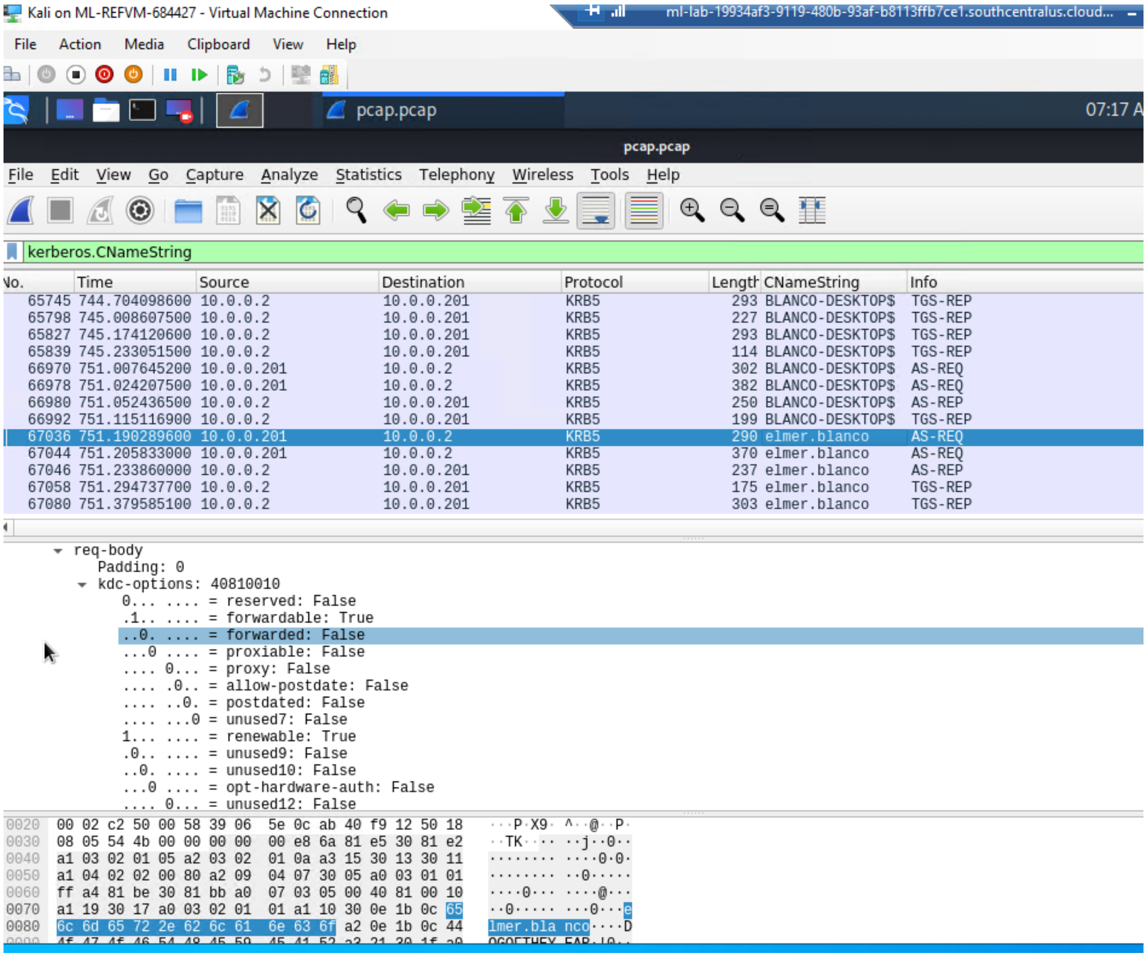
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

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 Windows NT 10.0

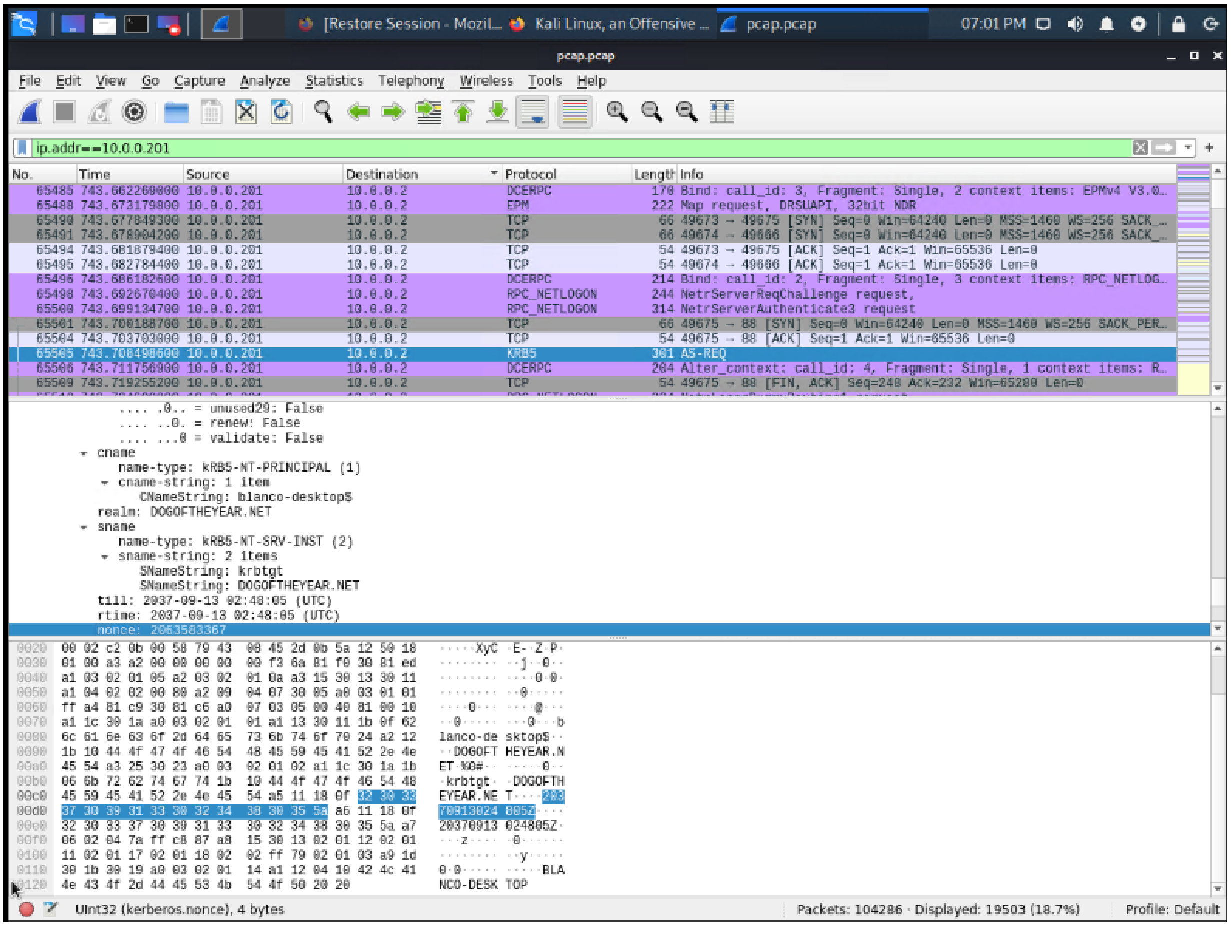


kerberos.CNameString

```
No.    Time          Source       Destination  Protocol  Lengtł CNameString       Info
 65745 744.704098600 10.0.0.2     10.0.0.201   KRB5        293 BLANCO-DESKTOP$   TGS-REP
 65798 745.008607500 10.0.0.2     10.0.0.201   KRB5        227 BLANCO-DESKTOP$   TGS-REP
 65827 745.174120600 10.0.0.2     10.0.0.201   KRB5        293 BLANCO-DESKTOP$   TGS-REP
 65839 745.233051500 10.0.0.2     10.0.0.201   KRB5        114 BLANCO-DESKTOP$   TGS-REP
 66970 751.007645200 10.0.0.201   10.0.0.2     KRB5        302 BLANCO-DESKTOP$   AS-REQ
 66978 751.024207500 10.0.0.201   10.0.0.2     KRB5        382 BLANCO-DESKTOP$   AS-REQ
 66980 751.052436500 10.0.0.2     10.0.0.201   KRB5        250 BLANCO-DESKTOP$   AS-REP
 66992 751.115116900 10.0.0.2     10.0.0.201   KRB5        199 BLANCO-DESKTOP$   TGS-REP
 67036 751.190289600 10.0.0.201   10.0.0.2     KRB5        290 elmer.blanco      AS-REQ
 67044 751.205833000 10.0.0.201   10.0.0.2     KRB5        370 elmer.blanco      AS-REQ
 67046 751.233860000 10.0.0.2     10.0.0.201   KRB5        237 elmer.blanco      AS-REP
 67058 751.294737700 10.0.0.2     10.0.0.201   KRB5        175 elmer.blanco      TGS-REP
 67080 751.379585100 10.0.0.2     10.0.0.201   KRB5        303 elmer.blanco      TGS-REP
```

```
    req-body
        Padding: 0
      kdc-options: 40810010
            0... .... = reserved: False
            .1.. .... = forwardable: True
            ..0. .... = forwarded: False
            ...0 .... = proxiable: False
            .... 0... = proxy: False
            .... .0.. = allow-postdate: False
            .... ..0. = postdated: False
            .... ...0 = unused7: False
            1... .... = renewable: True
            .0.. .... = unused9: False
            ..0. .... = unused10: False
            ...0 .... = opt-hardware-auth: False
            .... 0... = unused12: False
```

```
0020  00 02 c2 50 00 58 39 06  5e 0c ab 40 f9 12 50 18   ···P·X9· ^··@··P·
0030  08 05 54 4b 00 00 00 00  00 e8 6a 81 e5 30 81 e2   ··TK···· ··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 be 30 81 bb a0  07 03 05 00 40 81 00 10   ····0··· ····@···
0070  a1 19 30 17 a0 03 02 01  01 a1 10 30 0e 1b 0c 65   ··0····· ···0···e
0080  6c 6d 65 72 2e 62 6c 61  6e 63 6f a2 0e 1b 0c 44   lmer.bla nco····D
```


[Restore Session - Mozil...
Kali Linux, an Offensive ...
pcap.pcap
07:01 PM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.0.201

```
No.    Time          Source      Destination  Protocol      Length Info
 65485 743.662269000 10.0.0.201  10.0.0.2     DCERPC         170 Bind: call_id: 3, Fragment: Single, 2 context items: EPMv4 V3.0…
 65488 743.673179800 10.0.0.201  10.0.0.2     EPM            222 Map request, DRSUAPI, 32bit NDR
 65490 743.677849300 10.0.0.201  10.0.0.2     TCP             66 49673 → 49675 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
 65491 743.678904200 10.0.0.201  10.0.0.2     TCP             66 49674 → 49666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
 65494 743.681879400 10.0.0.201  10.0.0.2     TCP             54 49673 → 49675 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 65495 743.682784400 10.0.0.201  10.0.0.2     TCP             54 49674 → 49666 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 65496 743.686182600 10.0.0.201  10.0.0.2     DCERPC         214 Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOG…
 65498 743.692670400 10.0.0.201  10.0.0.2     RPC_NETLOGON   244 NetrServerReqChallenge request,
 65500 743.699134700 10.0.0.201  10.0.0.2     RPC_NETLOGON   314 NetrServerAuthenticate3 request
 65501 743.700188700 10.0.0.201  10.0.0.2     TCP             66 49675 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER…
 65504 743.703703000 10.0.0.201  10.0.0.2     TCP             54 49675 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 65505 743.708498600 10.0.0.201  10.0.0.2     KRB5           301 AS-REQ
 65506 743.711756900 10.0.0.201  10.0.0.2     DCERPC         204 Alter_context: call_id: 4, Fragment: Single, 1 context items: R…
 65509 743.719255200 10.0.0.201  10.0.0.2     TCP             54 49675 → 88 [FIN, ACK] Seq=248 Ack=232 Win=65280 Len=0
```

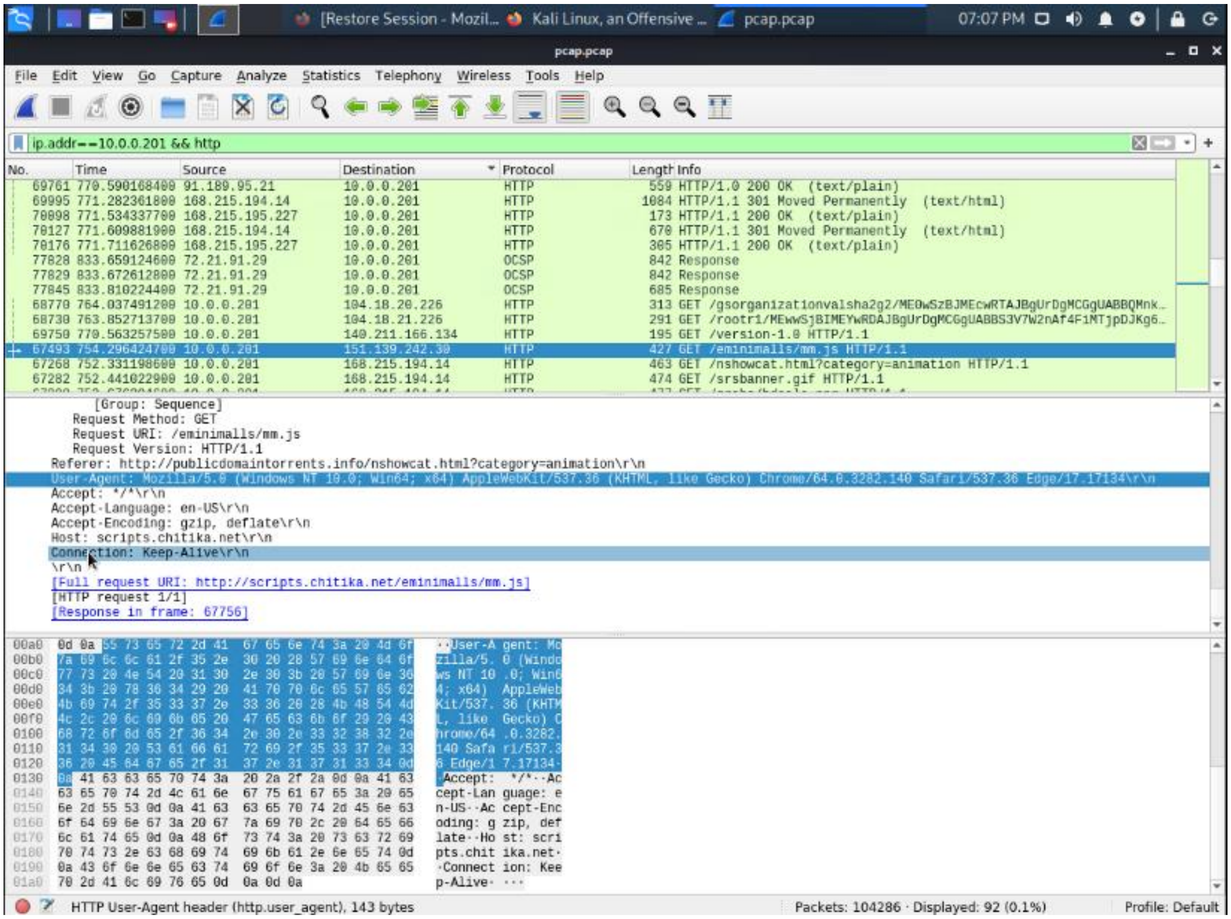
```
            .... .0.. = unused29: False
            .... ..0. = renew: False
            .... ...0 = validate: False
        ▾ cname
            name-type: kRB5-NT-PRINCIPAL (1)
          ▾ cname-string: 1 item
              CNameString: blanco-desktop$
          realm: DOGOFTHEYEAR.NET
        ▾ sname
            name-type: kRB5-NT-SRV-INST (2)
          ▾ sname-string: 2 items
              SNameString: krbtgt
              SNameString: DOGOFTHEYEAR.NET
          till: 2037-09-13 02:48:05 (UTC)
          rtime: 2037-09-13 02:48:05 (UTC)
          nonce: 2063583367
```

```
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
```

UInt32 (kerberos.nonce), 4 bytes

Packets: 104286 · Displayed: 19503 (18.7%)

Profile: Default



```
ip.addr==10.0.0.201 && http
```

```
No.    Time           Source           Destination      Protocol  Length Info
 69761 770.590168400 91.189.95.21     10.0.0.201       HTTP       559 HTTP/1.0 200 OK  (text/plain)
 69995 771.282361800 168.215.194.14   10.0.0.201       HTTP      1084 HTTP/1.1 301 Moved Permanently  (text/html)
 70098 771.534337700 168.215.195.227  10.0.0.201       HTTP       173 HTTP/1.1 200 OK  (text/plain)
 70127 771.609881900 168.215.194.14   10.0.0.201       HTTP       670 HTTP/1.1 301 Moved Permanently  (text/html)
 70176 771.711626800 168.215.195.227  10.0.0.201       HTTP       305 HTTP/1.1 200 OK  (text/plain)
 77828 833.659124600 72.21.91.29      10.0.0.201       OCSP       842 Response
 77829 833.672612800 72.21.91.29      10.0.0.201       OCSP       842 Response
 77845 833.810224400 72.21.91.29      10.0.0.201       OCSP       685 Response
 68770 764.037491200 10.0.0.201       104.18.20.226    HTTP       313 GET /gsorganizationvalsha2g2/MEOwSzBJMEcwRTAJBgUrDgMCGgUABBQMnk…
 68730 763.852713700 10.0.0.201       104.18.21.226    HTTP       291 GET /rootr1/MEwwSjBIMEYwRDAJBgUrDgMCGgUABBS3V7W2nAf4F1MTjpDJKg6…
 69750 770.563257500 10.0.0.201       140.211.166.134  HTTP       195 GET /version-1.0 HTTP/1.1
 67493 754.296424700 10.0.0.201       151.139.242.30   HTTP       427 GET /eminimalls/mm.js HTTP/1.1
 67268 752.331198600 10.0.0.201       168.215.194.14   HTTP       463 GET /nshowcat.html?category=animation HTTP/1.1
 67282 752.441022900 10.0.0.201       168.215.194.14   HTTP       474 GET /srsbanner.gif HTTP/1.1
```

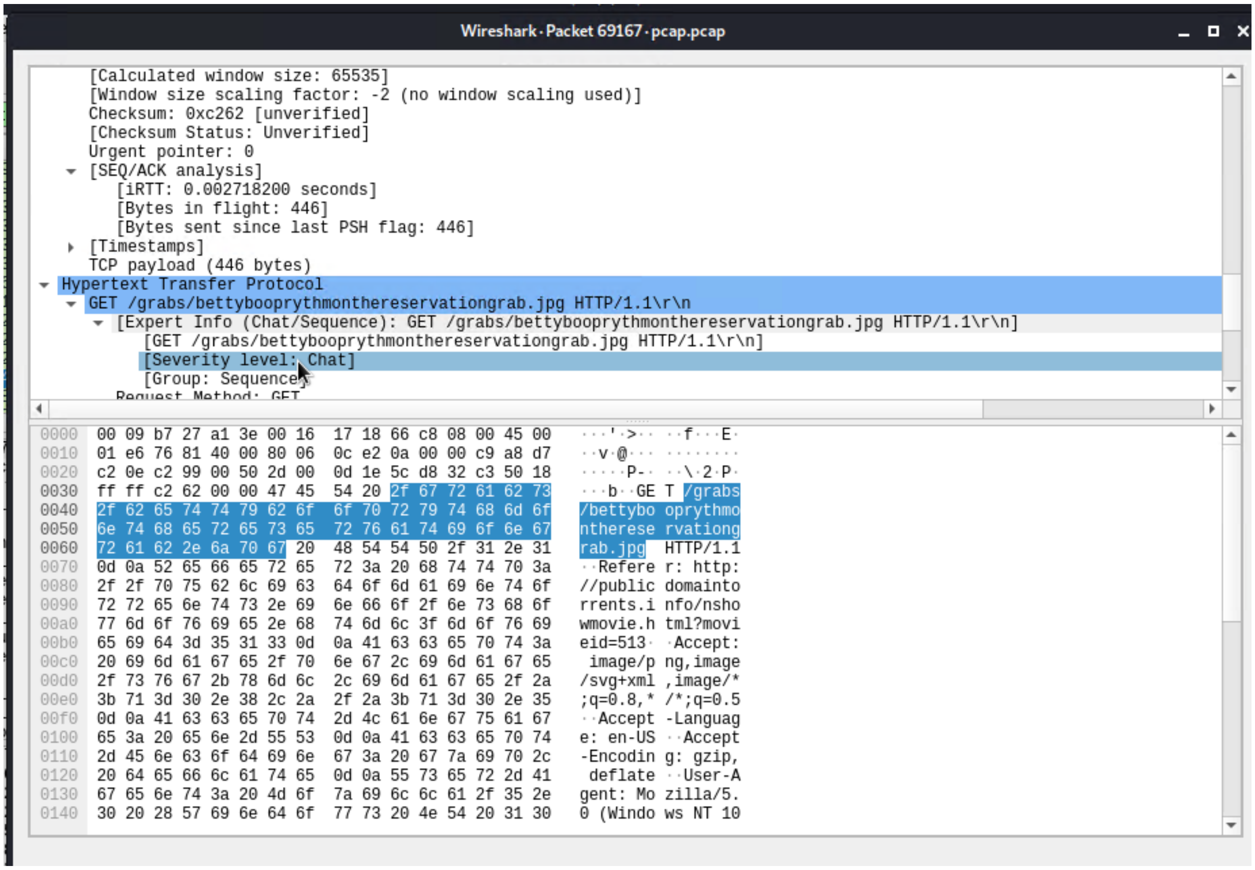
```
        [Group: Sequence]
      Request Method: GET
      Request URI: /eminimalls/mm.js
      Request Version: HTTP/1.1
    Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
    Accept: */*\r\n
    Accept-Language: en-US\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: scripts.chitika.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://scripts.chitika.net/eminimalls/mm.js]
    [HTTP request 1/1]
    [Response in frame: 67756]
```

```
00a0  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
00b0  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Windo
00c0  77 73 20 4e 54 20 31 30  2e 30 3b 20 57 69 6e 36   ws NT 10 .0; Win6
00d0  34 3b 20 78 36 34 29 20  41 70 70 6c 65 57 65 62   4; x64)  AppleWeb
00e0  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
00f0  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
0100  68 72 6f 6d 65 2f 36 34  2e 30 2e 33 32 38 32 2e   hrome/64 .0.3282.
0110  31 34 30 20 53 61 66 61  72 69 2f 35 33 37 2e 33   140 Safa ri/537.3
0120  36 20 45 64 67 65 2f 31  37 2e 31 37 31 33 34 0d   6 Edge/1 7.17134·
0130  0a 41 63 63 65 70 74 3a  20 2a 2f 2a 0d 0a 41 63   ·Accept:  */*··Ac
0140  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
0150  6e 2d 55 53 0d 0a 41 63  63 65 70 74 2d 45 6e 63   n-US··Ac cept-Enc
0160  6f 64 69 6e 67 3a 20 67  7a 69 70 2c 20 64 65 66   oding: g zip, def
0170  6c 61 74 65 0d 0a 48 6f  73 74 3a 20 73 63 72 69   late··Ho st: scri
0180  70 74 73 2e 63 68 69 74  69 6b 61 2e 6e 65 74 0d   pts.chit ika.net·
0190  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
01a0  70 2d 41 6c 69 76 65 0d  0a 0d 0a                  p-Alive· ···
```

```
HTTP User-Agent header (http.user_agent), 143 bytes    Packets: 104286 · Displayed: 92 (0.1%)    Profile: Default
```

2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_theReservation.avi.torrent HTTP/1.1\r\n



```
      [Calculated window size: 65535]
      [Window size scaling factor: -2 (no window scaling used)]
      Checksum: 0xc262 [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
    ▾ [SEQ/ACK analysis]
        [iRTT: 0.002718200 seconds]
        [Bytes in flight: 446]
        [Bytes sent since last PSH flag: 446]
    ▸ [Timestamps]
      TCP payload (446 bytes)
  ▾ 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]
            [GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  01 e6 76 81 40 00 80 06  0c e2 0a 00 00 c9 a8 d7   ··v·@··· ········
0020  c2 0e c2 99 00 50 2d 00  0d 1e 5c d8 32 c3 50 18   ·····P-· ··\·2·P·
0030  ff ff c2 62 00 00 47 45  54 20 2f 67 72 61 62 73   ···b··GE T /grabs
0040  2f 62 65 74 74 79 62 6f  6f 70 72 79 74 68 6d 6f   /bettybo oprythmo
0050  6e 74 68 65 72 65 73 65  72 76 61 74 69 6f 6e 67   nthערese rvationg
0060  72 61 62 2e 6a 70 67 20  48 54 54 50 2f 31 2e 31   rab.jpg  HTTP/1.1
0070  0d 0a 52 65 66 65 72 65  72 3a 20 68 74 74 70 3a   ··Refere r: http:
0080  2f 2f 70 75 62 6c 69 63  64 6f 6d 61 69 6e 74 6f   //public domainto
0090  72 72 65 6e 74 73 2e 69  6e 66 6f 2f 6e 73 68 6f   rrents.i nfo/nsho
00a0  77 6d 6f 76 69 65 2e 68  74 6d 6c 3f 6d 6f 76 69   wmovie.h tml?movi
00b0  65 69 64 3d 35 31 33 0d  0a 41 63 63 65 70 74 3a   eid=513· ·Accept:
00c0  20 69 6d 61 67 65 2f 70  6e 67 2c 69 6d 61 67 65    image/p ng,image
00d0  2f 73 76 67 2b 78 6d 6c  2c 69 6d 61 67 65 2f 2a   /svg+xml ,image/*
00e0  3b 71 3d 30 2e 38 2c 2a  2f 2a 3b 71 3d 30 2e 35   ;q=0.8,* /*;q=0.5
00f0  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
0100  65 3a 20 65 6e 2d 55 53  0d 0a 41 63 63 65 70 74   e: en-US ··Accept
0110  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0120  20 64 65 66 6c 61 74 65  0d 0a 55 73 65 72 2d 41    deflate ··User-A
0130  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
0140  30 20 28 57 69 6e 64 6f  77 73 20 4e 54 20 31 30   0 (Windo ws NT 10
```