ShibumiKat / Portfolio_CyberSecurityMonashBootcamp Private

generated from ShibumiKat/ShibumiKatTemplate

Code Issues Pull requests Actions Projects Security Insights Settings

master

Portfolio_CyberSecurityMonashBootcamp / 24-Final-Project / _PieterBooysen-NetworkReport.md

ShibumiKat Final Project Submitted

1 contributor

189 lines (116 sloc) 7.47 KB

Network Forensic Analysis Report

Overview

This report is from the Security Engineering Team of X-CORP, supporting the SOC infrastructure. The SOC analysts have noticed some discrepancies with alerting in the Kibana system and the Security Engineering team investigated.

Yesterday, the team confirmed that newly created alerts are working. Live traffic was monitored on the wire to detect any abnormalities that aren't reflected in the alerting system.

This report is the findings for review by both the SOC manager and the Engineering Manager with appropriate analysis.

Methodology

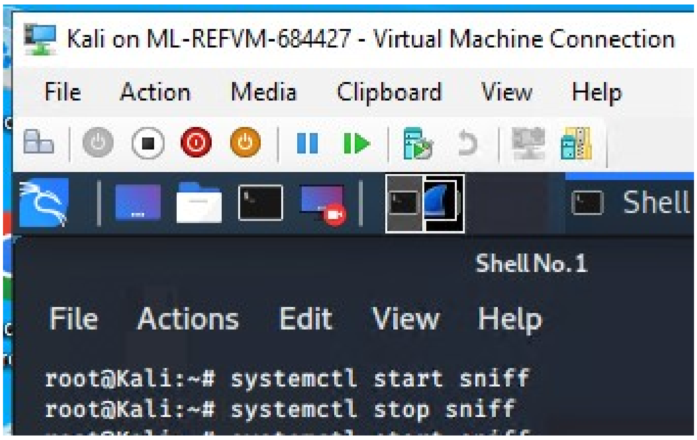
- Kali VM used for Analysis-* The following Commans were used to start and stop the WireShark Capture
- Open a terminal window and run the command `systemctl start sniff`.
  - This command uses `tcpreplay` to replay PCAPs in `/opt/pcaps` onto Kali's `eth0` interface.

- Launch Wireshark and capture traffic on the `eth0` interface.
- After 15 minutes have passed, run the command `systemctl stop sniff` to stop the `tcpreplay` .
  - Please note that replaying the PCAPs will use up the CPU memory. You will need to stop this service in order to avoid performance issues with your virtual machine.
- Save the capture to file. (**This is an important step**.)
- Profile users' behavior from their packet data.

If you are unable to find some of the solutions, it is possible you did not allow Wireshark to capture traffic for long enough. To save time, feel free to use the following PCAP file below to answer the questions:

- PCAP
- If copy and paste is not available on the VM, use `curl` to download the file with this alternate URL: http://tinyurl.com/yaajh8o8.
  - For example: `curl -L -o pcap.pcap http://tinyurl.com/yaajh8o8`

Note: You will be dealing with live malware in this activity. Please make sure all work is done on Azure machines.


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell
Shell No. 1
File Actions Edit View Help

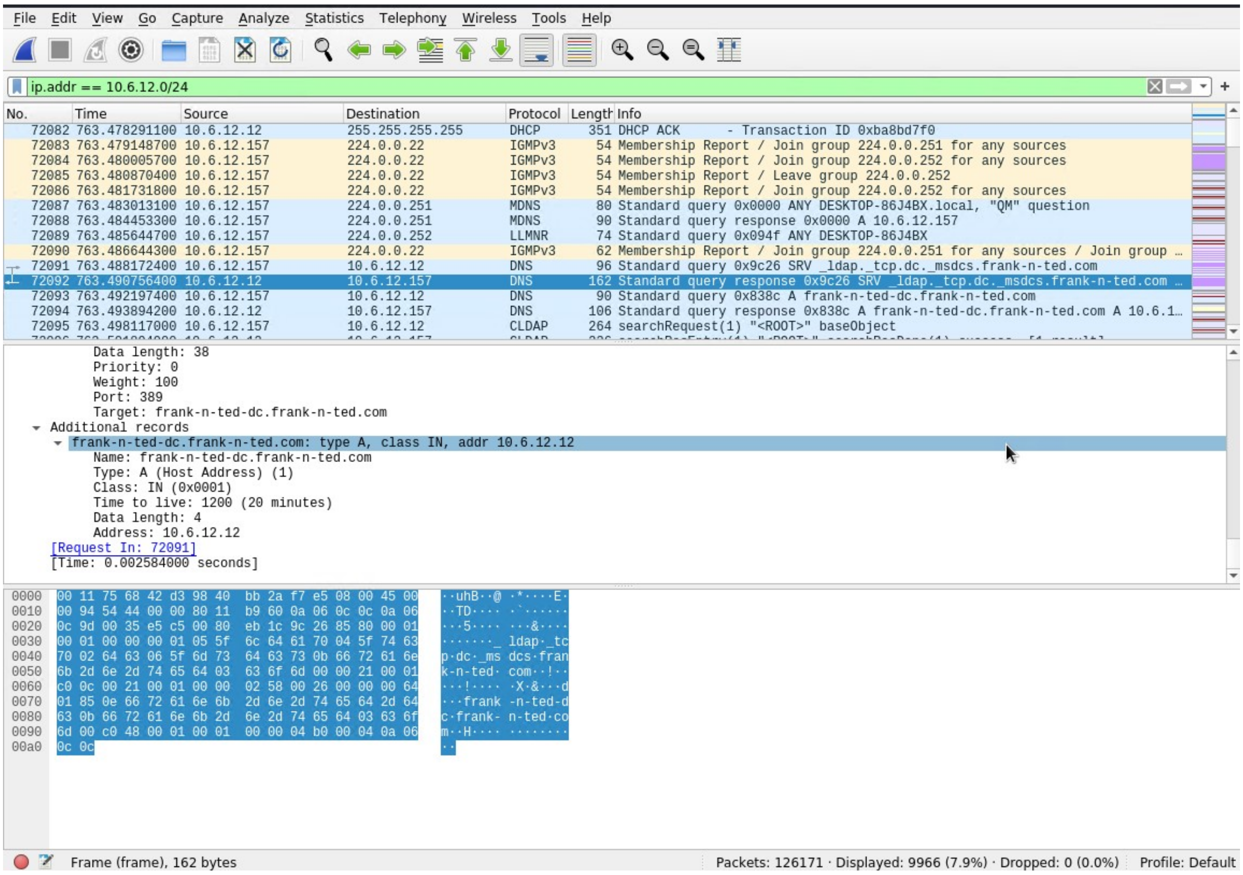
```
root@Kali:~# systemctl start sniff
root@Kali:~# systemctl stop sniff
```

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.

1. Domain name of the users' custom site

Domain Name: `frank-n-ted-dc.frank-n-ted.com` WireShark Filter: `ip.addr == 10.6.12.0/24`



ip.addr == 10.6.12.0/24

```
No.   Time          Source         Destination       Protocol Length Info
72082 763.478291100 10.6.12.12     255.255.255.255   DHCP     351 DHCP ACK      - Transaction ID 0xba8bd7f0
72083 763.479148700 10.6.12.157    224.0.0.22        IGMPv3    54 Membership Report / Join group 224.0.0.251 for any sources
72084 763.480005700 10.6.12.157    224.0.0.22        IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
72085 763.480870400 10.6.12.157    224.0.0.22        IGMPv3    54 Membership Report / Leave group 224.0.0.252
72086 763.481731800 10.6.12.157    224.0.0.22        IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
72087 763.483013100 10.6.12.157    224.0.0.251       MDNS      80 Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
72088 763.484453300 10.6.12.157    224.0.0.251       MDNS      90 Standard query response 0x0000 A 10.6.12.157
72089 763.485644700 10.6.12.157    224.0.0.252       LLMNR     74 Standard query 0x094f ANY DESKTOP-86J4BX
72090 763.486644300 10.6.12.157    224.0.0.22        IGMPv3    62 Membership Report / Join group 224.0.0.251 for any sources / Join group …
72091 763.488172400 10.6.12.157    10.6.12.12        DNS       96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
72092 763.490756400 10.6.12.12     10.6.12.157       DNS      162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
72093 763.492197400 10.6.12.157    10.6.12.12        DNS       90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
72094 763.493894200 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…
72095 763.498117000 10.6.12.157    10.6.12.12        CLDAP    264 searchRequest(1) "<ROOT>" baseObject
```

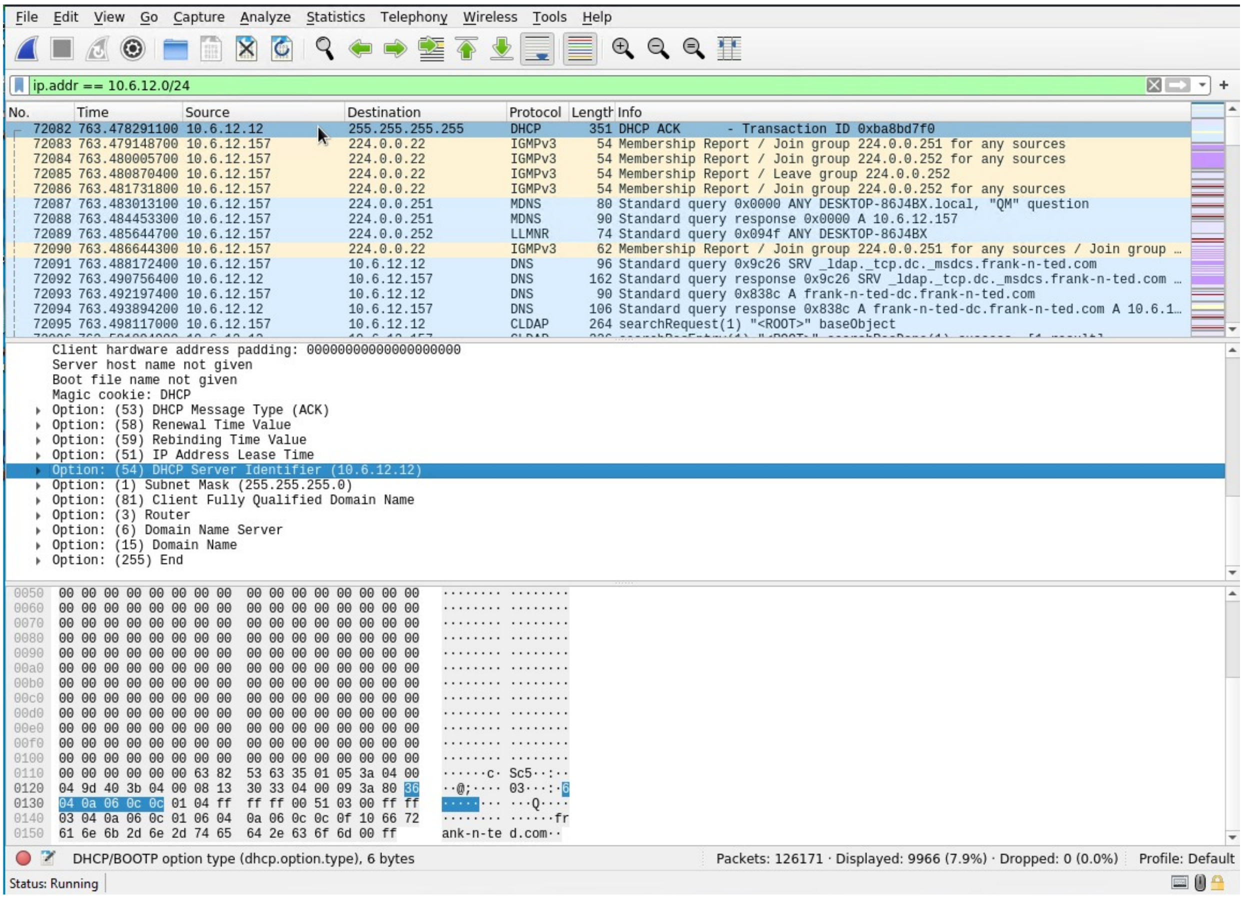
```
          Data length: 38
          Priority: 0
          Weight: 100
          Port: 389
          Target: frank-n-ted-dc.frank-n-ted.com
    Additional records
      frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12
          Name: frank-n-ted-dc.frank-n-ted.com
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 1200 (20 minutes)
          Data length: 4
          Address: 10.6.12.12
    [Request In: 72091]
    [Time: 0.002584000 seconds]
```

```
0000  00 11 75 68 42 d3 98 40  bb 2a f7 e5 08 00 45 00   ··uhB··@ ·*····E·
0010  00 94 54 44 00 00 80 11  b9 60 0a 06 0c 0c 0a 06   ··TD···· ·`······
0020  0c 9d 00 35 e5 c5 00 80  eb 1c 9c 26 85 80 00 01   ···5···· ···&····
0030  00 01 00 00 00 01 05 5f  6c 64 61 70 04 5f 74 63   ·······_ ldap·_tc
0040  70 02 64 63 06 5f 6d 73  64 63 73 0b 66 72 61 6e   p·dc·_ms dcs·fran
0050  6b 2d 6e 2d 74 65 64 03  63 6f 6d 00 00 21 00 01   k-n-ted· com··!··
0060  c0 0c 00 21 00 01 00 00  02 58 00 26 00 00 00 64   ···!···· ·X·&···d
0070  01 85 0e 66 72 61 6e 6b  2d 6e 2d 74 65 64 2d 64   ···frank -n-ted-d
0080  63 0b 66 72 61 6e 6b 2d  6e 2d 74 65 64 03 63 6f   c·frank- n-ted·co
0090  6d 00 c0 48 00 01 00 01  00 00 04 b0 00 04 0a 06   m··H···· ········
00a0  0c 0c                                              ··
```

Frame (frame), 162 bytes   Packets: 126171 · Displayed: 9966 (7.9%) · Dropped: 0 (0.0%)   Profile: Default

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

Domain Controller: `10.6.12.12` WireShark Filter: `ip.addr == 10.6.12.0/24` (and also refer to the previous screenshot)



```
ip.addr == 10.6.12.0/24
```

```
No.   Time          Source       Destination      Protocol Length Info
72082 763.478291100 10.6.12.12   255.255.255.255  DHCP     351 DHCP ACK      - Transaction ID 0xba8bd7f0
72083 763.479148700 10.6.12.157  224.0.0.22       IGMPv3    54 Membership Report / Join group 224.0.0.251 for any sources
72084 763.480005700 10.6.12.157  224.0.0.22       IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
72085 763.480870400 10.6.12.157  224.0.0.22       IGMPv3    54 Membership Report / Leave group 224.0.0.252
72086 763.481731800 10.6.12.157  224.0.0.22       IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
72087 763.483013100 10.6.12.157  224.0.0.251      MDNS      80 Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
72088 763.484453300 10.6.12.157  224.0.0.251      MDNS      90 Standard query response 0x0000 A 10.6.12.157
72089 763.485644700 10.6.12.157  224.0.0.252      LLMNR     74 Standard query 0x094f ANY DESKTOP-86J4BX
72090 763.486644300 10.6.12.157  224.0.0.22       IGMPv3    62 Membership Report / Join group 224.0.0.251 for any sources / Join group …
72091 763.488172400 10.6.12.157  10.6.12.12       DNS       96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
72092 763.490756400 10.6.12.12   10.6.12.157      DNS      162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
72093 763.492197400 10.6.12.157  10.6.12.12       DNS       90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
72094 763.493894200 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…
72095 763.498117000 10.6.12.157  10.6.12.12       CLDAP    264 searchRequest(1) "<ROOT>" baseObject
```

```
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (ACK)
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (54) DHCP Server Identifier (10.6.12.12)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (81) Client Fully Qualified Domain Name
  ▸ Option: (3) Router
  ▸ Option: (6) Domain Name Server
  ▸ Option: (15) Domain Name
  ▸ Option: (255) End
```

```
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 3a 04 00   ······c· Sc5··:··
0120  04 9d 40 3b 04 00 08 13  30 33 04 00 09 3a 80 36   ··@;···· 03···:·6
0130  04 0a 06 0c 0c 01 04 ff  ff ff 00 51 03 00 ff ff   ········ ···Q····
0140  03 04 0a 06 0c 01 06 04  0a 06 0c 0c 0f 10 66 72   ········ ······fr
0150  61 6e 6b 2d 6e 2d 74 65  64 2e 63 6f 6d 00 ff      ank-n-te d.com··
```

DHCP/BOOTP option type (dhcp.option.type), 6 bytes

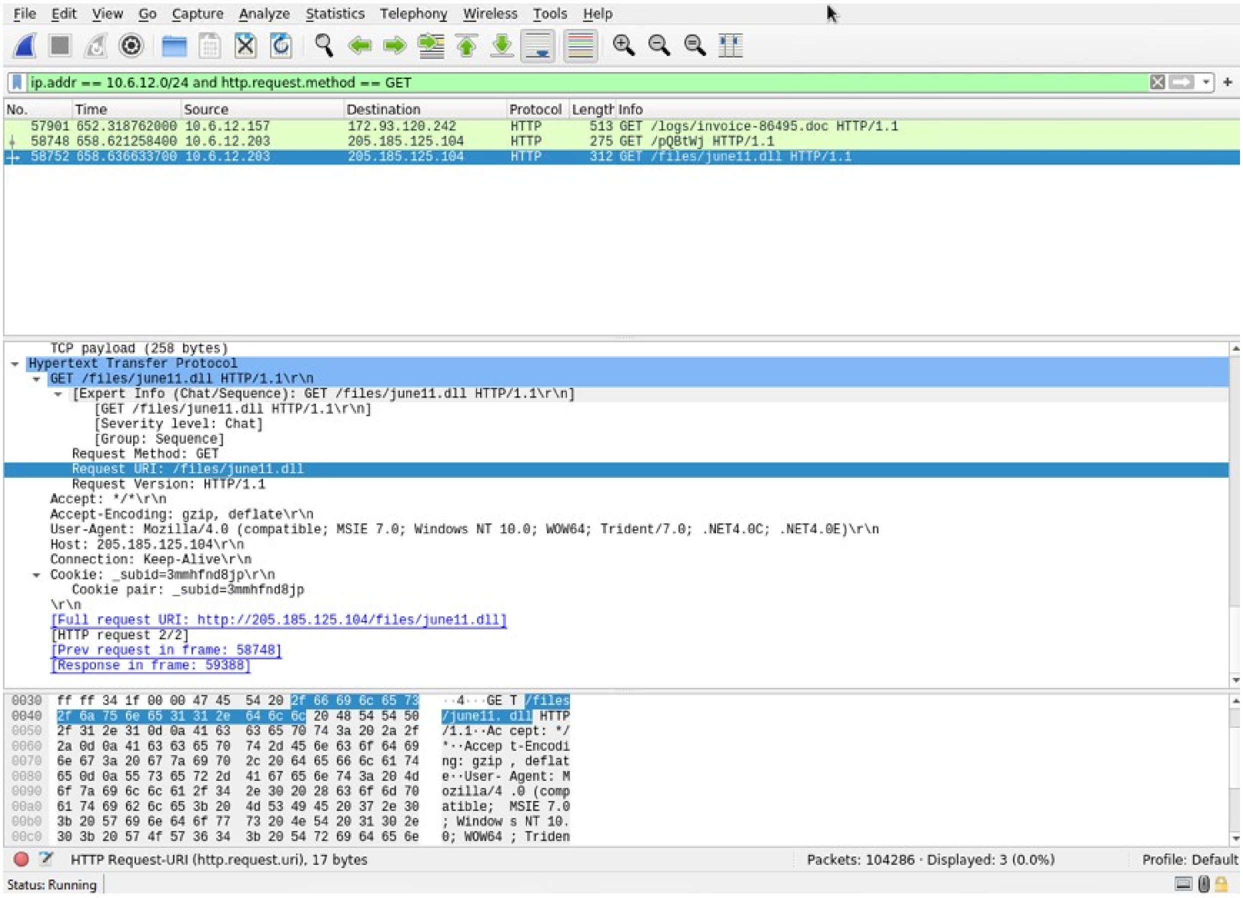
Packets: 126171 · Displayed: 9966 (7.9%) · Dropped: 0 (0.0%)

Profile: Default

Status: Running

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.

Filename: `june11.dll` WireShark Filter: `ip.addr == 10.6.12.0/24 and http.request.method == GET`


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.6.12.0/24 and http.request.method == GET

```
No.    Time           Source        Destination     Protocol Length Info
 57901 652.318762000 10.6.12.157   172.93.120.242  HTTP      513 GET /logs/invoice-86495.doc HTTP/1.1
 58748 658.621258400 10.6.12.203   205.185.125.104 HTTP      275 GET /pQBtWj HTTP/1.1
 58752 658.636633700 10.6.12.203   205.185.125.104 HTTP      312 GET /files/june11.dll HTTP/1.1
```

```
    TCP payload (258 bytes)
Hypertext Transfer Protocol
  GET /files/june11.dll HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
      [GET /files/june11.dll HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /files/june11.dll
    Request Version: HTTP/1.1
  Accept: */*\r\n
  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]
  [Prev request in frame: 58748]
  [Response in frame: 59388]
```

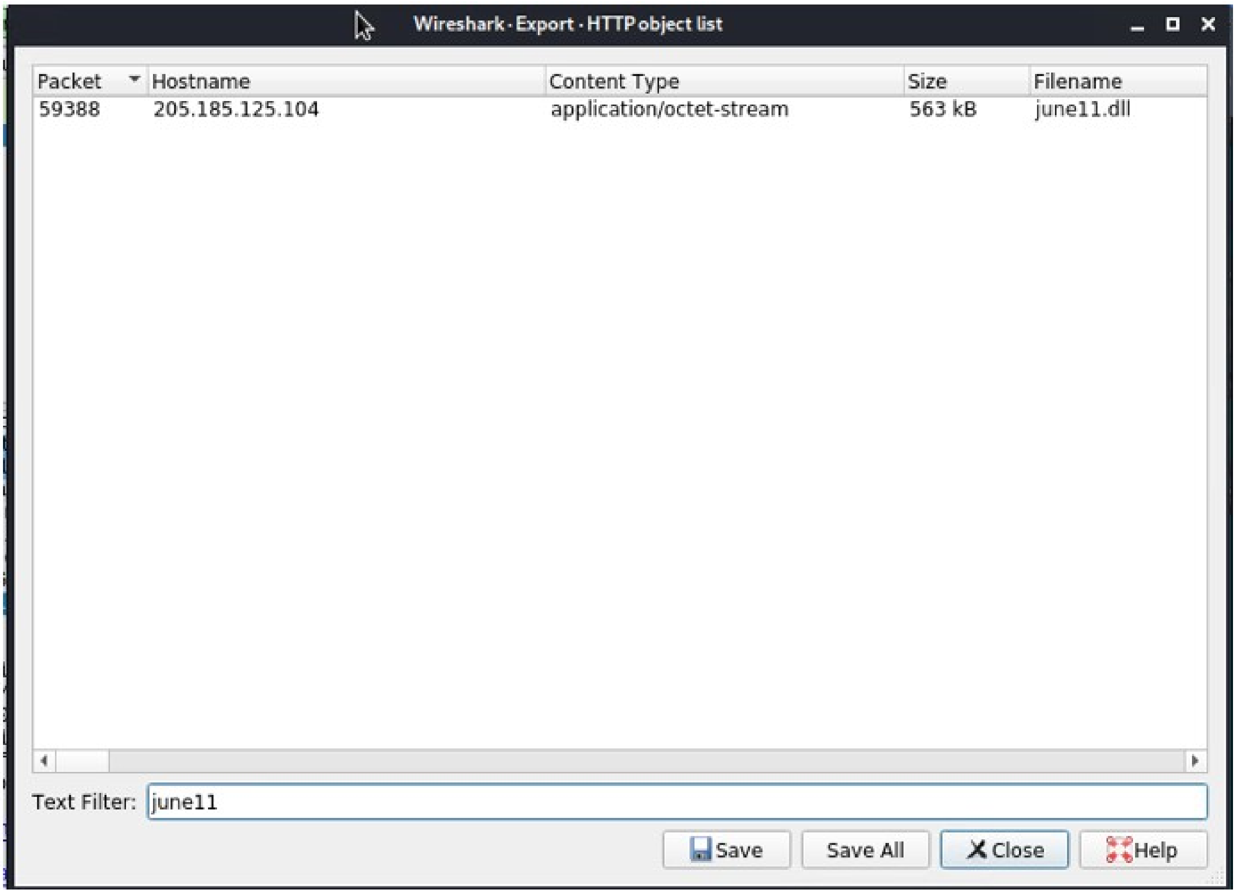
```
0030  ff ff 34 1f 00 00 47 45  54 20 2f 66 69 6c 65 73   ··4···GE T /files
0040  2f 6a 75 6e 65 31 31 2e  64 6c 6c 20 48 54 54 50   /june11. dll HTTP
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
0070  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0080  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
0090  6f 7a 69 6c 6c 61 2f 34  2e 30 20 28 63 6f 6d 70   ozilla/4 .0 (comp
00a0  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 37 2e 30   atible;  MSIE 7.0
00b0  3b 20 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e   ; Window s NT 10.
00c0  30 3b 20 57 4f 57 36 34  3b 20 54 72 69 64 65 6e   0; WOW64 ; Triden
```

HTTP Request-URI (http.request.uri), 17 bytes   Packets: 104286 · Displayed: 3 (0.0%)   Profile: Default

Status: Running

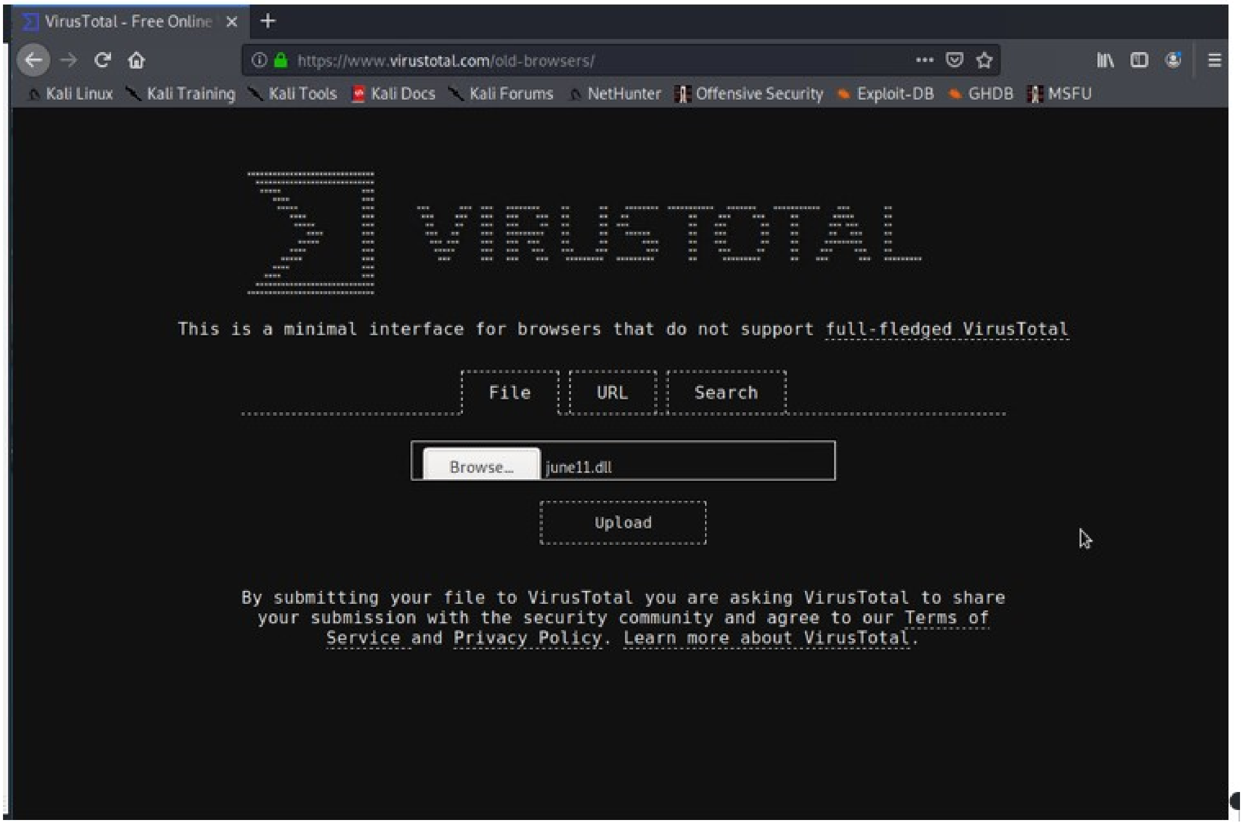
4. Upload the file to VirusTotal.com.

- `Wireshark//File//Export Objects//HTTP > filter: june11`
- Upload file to VirusTotal.com



Packet	Hostname	Content Type	Size	Filename
59388	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: june11

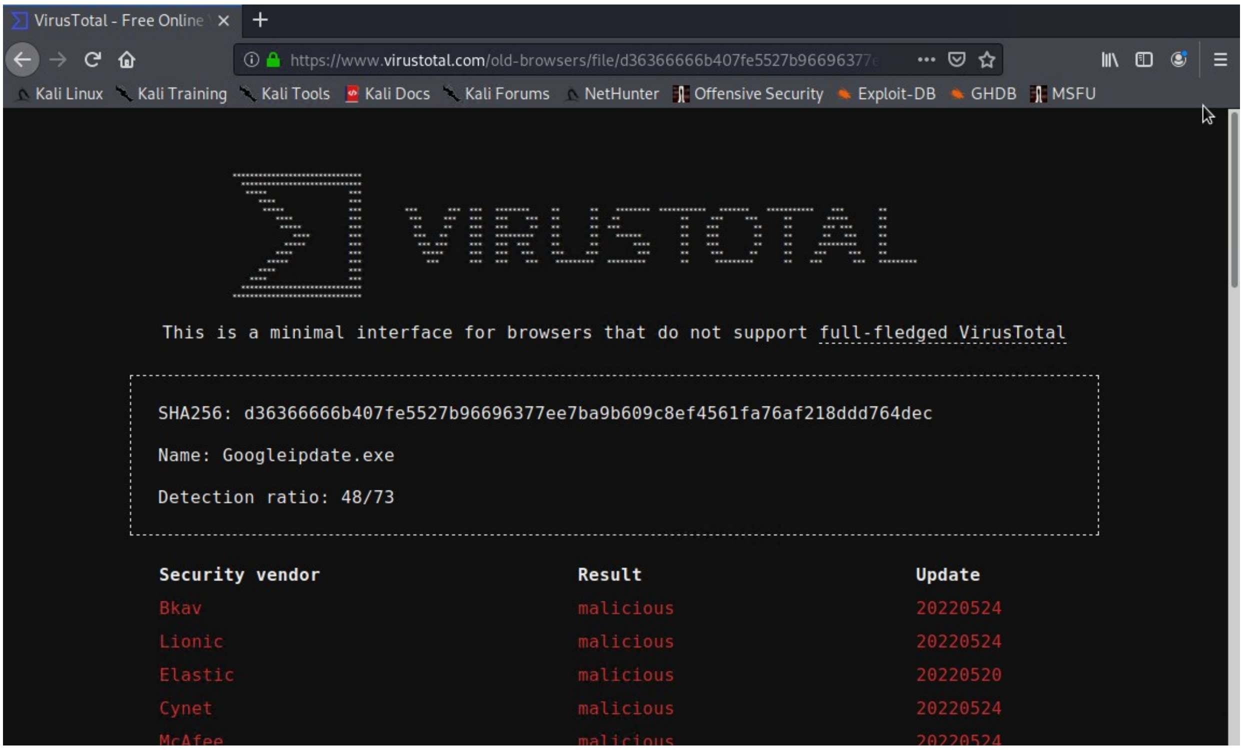


This is a minimal interface for browsers that do not support full-fledged VirusTotal

june11.dll

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more about VirusTotal.

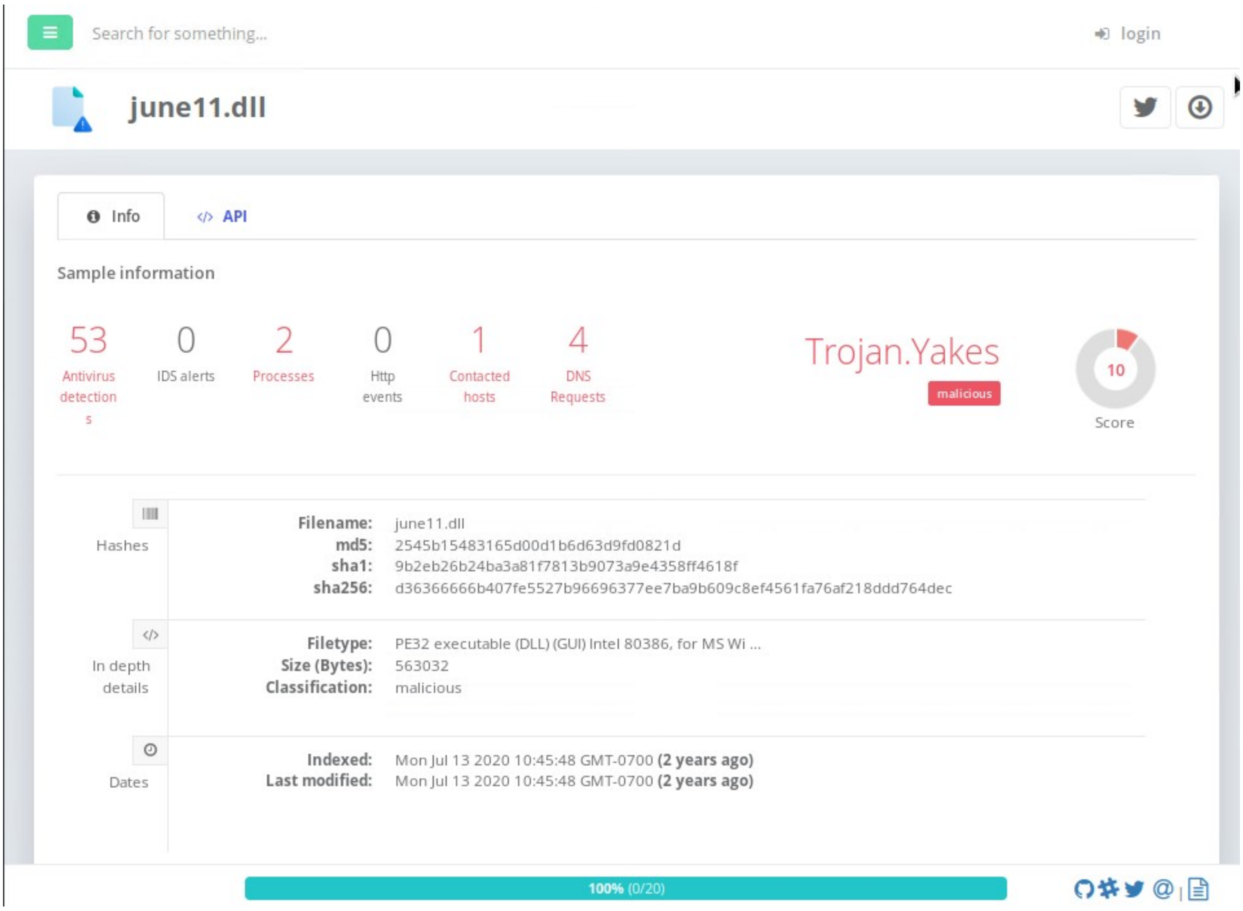
Malware Characteristics



```
This is a minimal interface for browsers that do not support full-fledged VirusTotal

SHA256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Name: Googleipdate.exe

Detection ratio: 48/73

Security vendor                      Result                         Update
Bkav                                 malicious                      20220524
Lionic                               malicious                      20220524
Elastic                              malicious                      20220520
Cynet                                malicious                      20220524
McAfee                               malicious                      20220524
```

5. What kind of malware is this classified as?

The malware goes by different names but maltiverse.com classify it as **Trojan**



Sample information

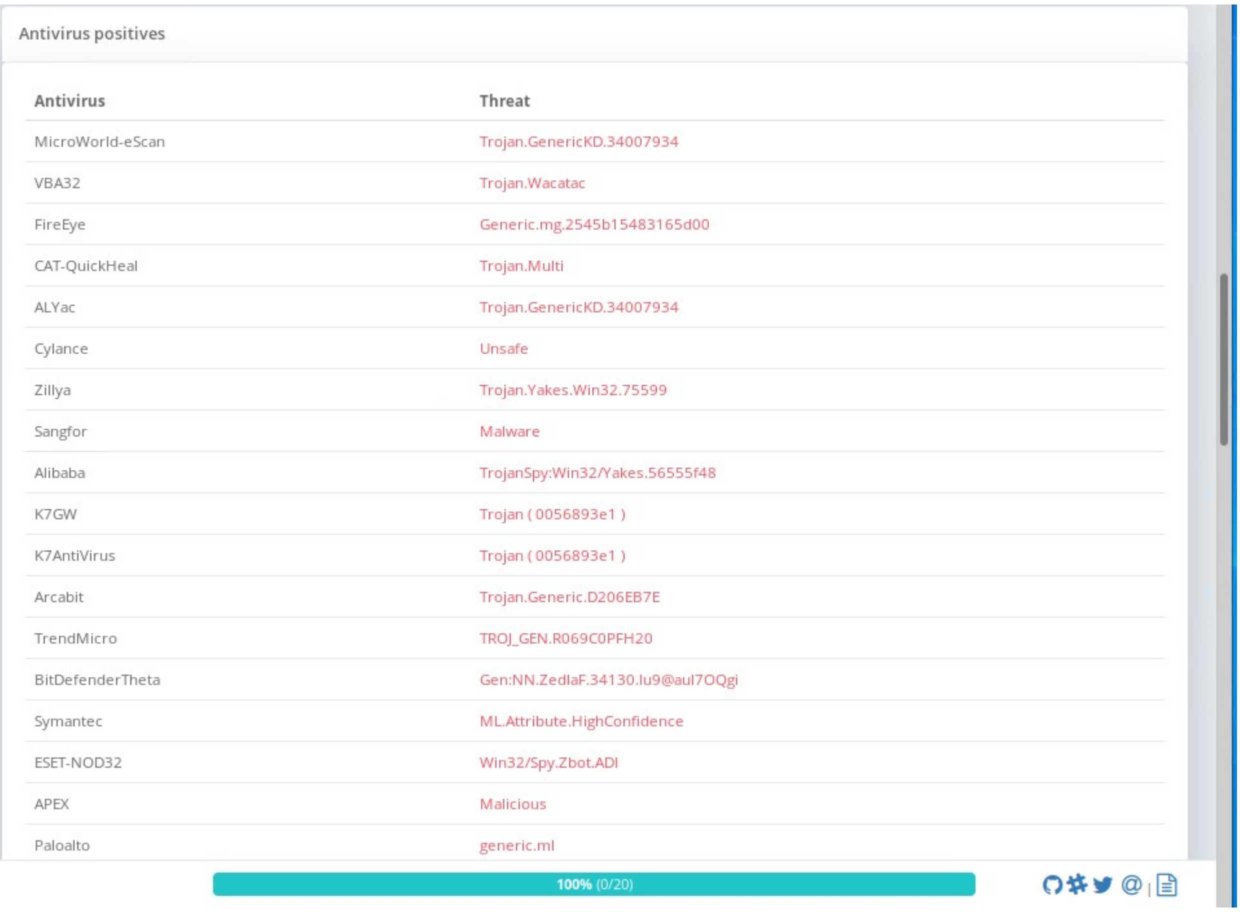
53 Antivirus detections | 0 IDS alerts | 2 Processes | 0 Http events | 1 Contacted hosts | 4 DNS Requests

Trojan.Yakes
malicious
10 Score

Hashes
Filename: june11.dll
md5: 2545b15483165d00d1b6d63d9fd0821d
sha1: 9b2eb26b24ba3a81f7813b9073a9e4358ff4618f
sha256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

In depth details
Filetype: PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ...
Size (Bytes): 563032
Classification: malicious

Dates
Indexed: Mon Jul 13 2020 10:45:48 GMT-0700 **(2 years ago)**
Last modified: Mon Jul 13 2020 10:45:48 GMT-0700 **(2 years ago)**



Antivirus positives

Antivirus	Threat
MicroWorld-eScan	Trojan.GenericKD.34007934
VBA32	Trojan.Wacatac
FireEye	Generic.mg.2545b15483165d00
CAT-QuickHeal	Trojan.Multi
ALYac	Trojan.GenericKD.34007934
Cylance	Unsafe
Zillya	Trojan.Yakes.Win32.75599
Sangfor	Malware
Alibaba	TrojanSpy:Win32/Yakes.56555f48
K7GW	Trojan (0056893e1)
K7AntiVirus	Trojan (0056893e1)
Arcabit	Trojan.Generic.D206EB7E
TrendMicro	TROJ_GEN.R069C0PFH20
BitDefenderTheta	Gen:NN.ZedlaF.34130.lu9@aul7OQgi
Symantec	ML.Attribute.HighConfidence
ESET-NOD32	Win32/Spy.Zbot.ADI
APEX	Malicious
Paloalto	generic.ml

Vulnerable Windows Machine

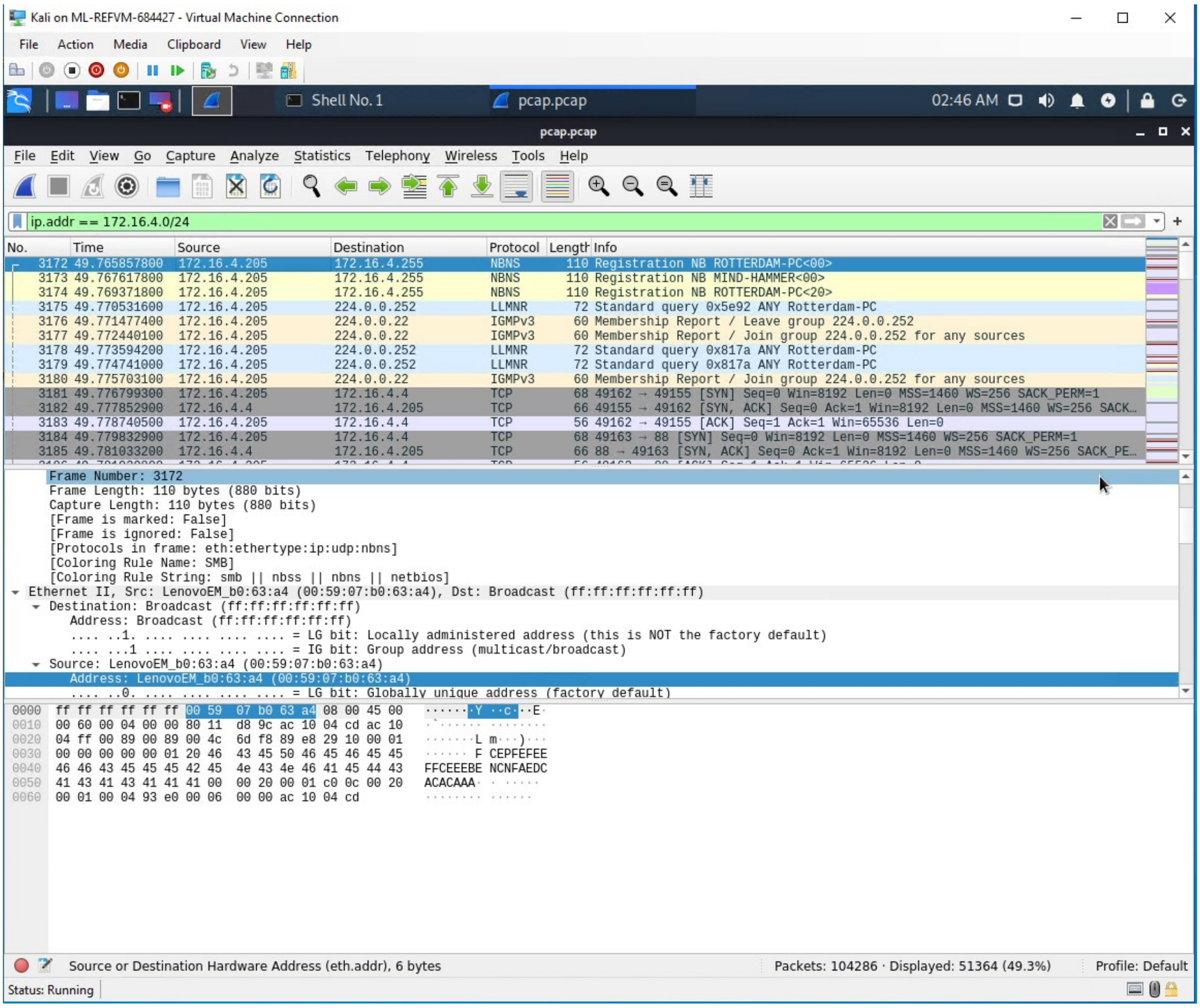
The Security team received reports of an infected Windows host on the network. They know the following:

- 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 in your network report:

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`
- Wireshark Filter: `ip.addr == 172.16.4.0/24`


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
pcap.pcap
02:46 AM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.4.0/24

```
No.   Time         Source        Destination   Protocol Length Info
3172 49.765857800  172.16.4.205  172.16.4.255  NBNS     110 Registration NB ROTTERDAM-PC<00>
3173 49.767617800  172.16.4.205  172.16.4.255  NBNS     110 Registration NB MIND-HAMMER<00>
3174 49.769371800  172.16.4.205  172.16.4.255  NBNS     110 Registration NB ROTTERDAM-PC<20>
3175 49.770531600  172.16.4.205  224.0.0.252   LLMNR     72 Standard query 0x5e92 ANY Rotterdam-PC
3176 49.771477400  172.16.4.205  224.0.0.22    IGMPv3    60 Membership Report / Leave group 224.0.0.252
3177 49.772440100  172.16.4.205  224.0.0.22    IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
3178 49.773594200  172.16.4.205  224.0.0.252   LLMNR     72 Standard query 0x817a ANY Rotterdam-PC
3179 49.774741000  172.16.4.205  224.0.0.252   LLMNR     72 Standard query 0x817a ANY Rotterdam-PC
3180 49.775703100  172.16.4.205  224.0.0.22    IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
3181 49.776799300  172.16.4.205  172.16.4.4    TCP       68 49162 → 49155 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3182 49.777852900  172.16.4.4    172.16.4.205  TCP       66 49155 → 49162 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK…
3183 49.778740500  172.16.4.205  172.16.4.4    TCP       56 49162 → 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0
3184 49.779832900  172.16.4.205  172.16.4.4    TCP       68 49163 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3185 49.781033200  172.16.4.4    172.16.4.205  TCP       66 88 → 49163 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
```

```
    Frame Number: 3172
    Frame Length: 110 bytes (880 bits)
    Capture Length: 110 bytes (880 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:nbns]
    [Coloring Rule Name: SMB]
    [Coloring Rule String: smb || nbss || nbns || netbios]
▾ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
      Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
```

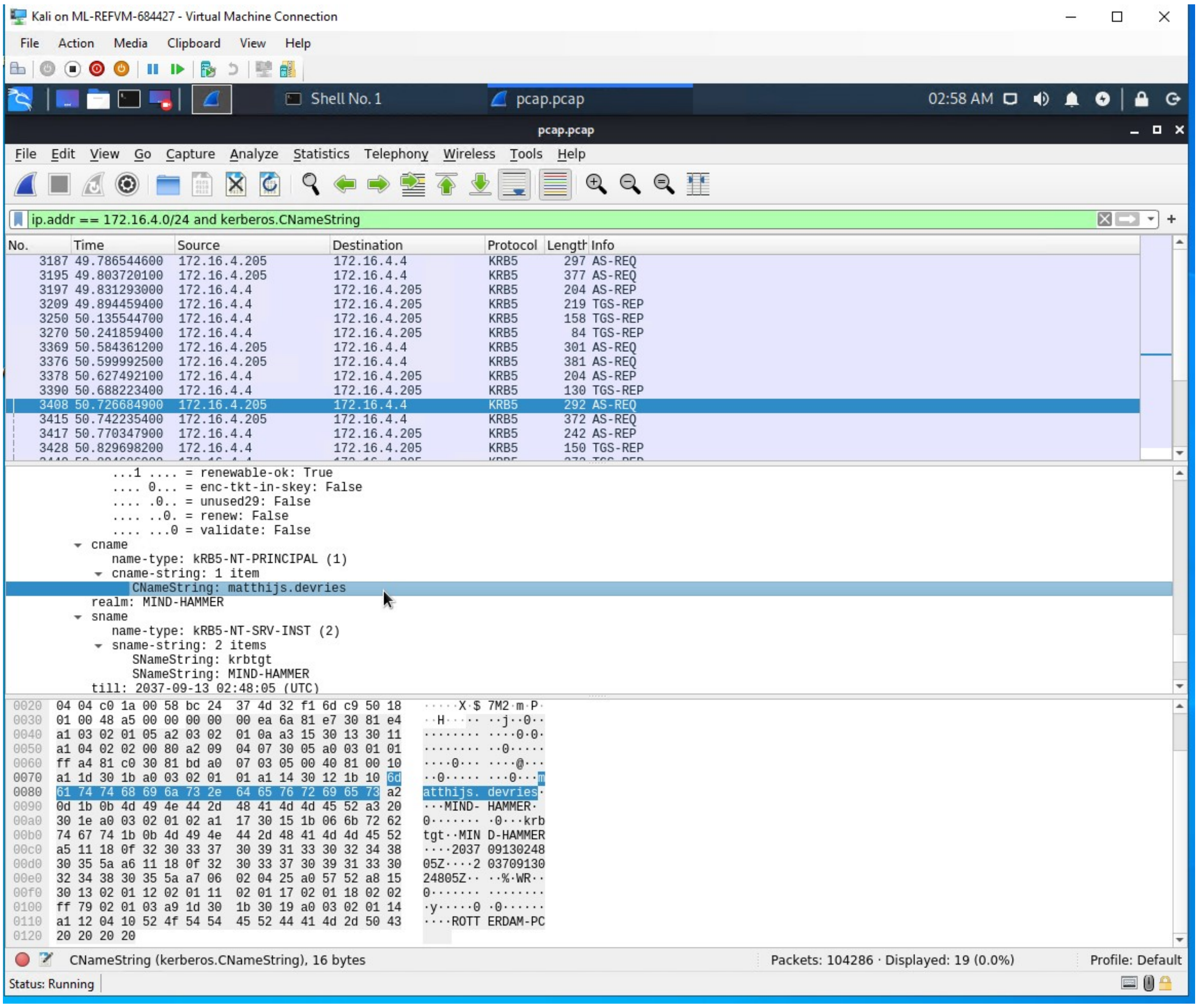
```
0000  ff ff ff ff ff ff 00 59  07 b0 63 a4 08 00 45 00   ······Y ··c···E·
0010  00 60 00 04 00 00 80 11  d8 9c ac 10 04 cd ac 10   ·`······ ········
0020  04 ff 00 89 00 89 00 4c  6d f8 89 e8 29 10 00 01   ·······L m···)···
0030  00 00 00 00 00 01 20 46  43 45 50 46 45 46 45 45   ······ F CEPFEFEE
0040  46 46 43 45 45 45 42 45  4e 43 4e 46 41 45 44 43   FFCEEEBE NCNFAEDC
0050  41 43 41 43 41 41 41 00  00 20 00 01 c0 0c 00 20   ACACAAA· · ······
0060  00 01 00 04 93 e0 00 06  00 00 ac 10 04 cd         ········ ······
```

Source or Destination Hardware Address (eth.addr), 6 bytes · Packets: 104286 · Displayed: 51364 (49.3%) · Profile: Default

Status: Running

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

- Username: `matthijs.devries`
- Wireshark Filter: `ip.src==172.16.4.205 && kerberos.CNameString`


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
pcap.pcap
02:58 AM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.4.0/24 and kerberos.CNameString

```
No.   Time         Source         Destination    Protocol Length Info
 3187 49.786544600 172.16.4.205   172.16.4.4     KRB5      297 AS-REQ
 3195 49.803720100 172.16.4.205   172.16.4.4     KRB5      377 AS-REQ
 3197 49.831293000 172.16.4.4     172.16.4.205   KRB5      204 AS-REP
 3209 49.894459400 172.16.4.4     172.16.4.205   KRB5      219 TGS-REP
 3250 50.135544700 172.16.4.4     172.16.4.205   KRB5      158 TGS-REP
 3270 50.241859400 172.16.4.4     172.16.4.205   KRB5       84 TGS-REP
 3369 50.584361200 172.16.4.205   172.16.4.4     KRB5      301 AS-REQ
 3376 50.599992500 172.16.4.205   172.16.4.4     KRB5      381 AS-REQ
 3378 50.627492100 172.16.4.4     172.16.4.205   KRB5      204 AS-REP
 3390 50.688223400 172.16.4.4     172.16.4.205   KRB5      130 TGS-REP
 3408 50.726684900 172.16.4.205   172.16.4.4     KRB5      292 AS-REQ
 3415 50.742235400 172.16.4.205   172.16.4.4     KRB5      372 AS-REQ
 3417 50.770347900 172.16.4.4     172.16.4.205   KRB5      242 AS-REP
 3428 50.829698200 172.16.4.4     172.16.4.205   KRB5      150 TGS-REP
```

```
        ...1 .... = renewable-ok: True
        .... 0... = enc-tkt-in-skey: False
        .... .0.. = unused29: False
        .... ..0. = renew: False
        .... ...0 = validate: False
    ▾ 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)
```

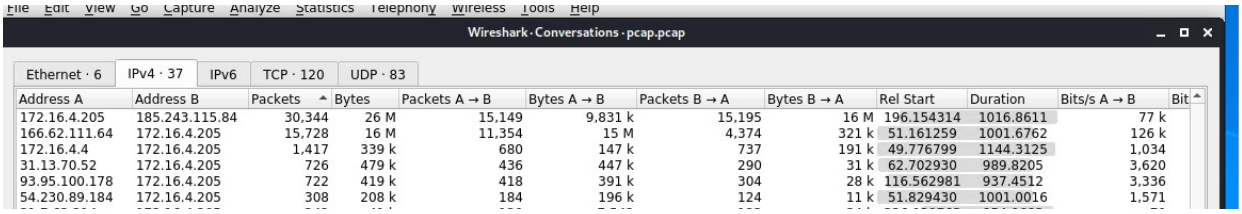
```
0020  04 04 c0 1a 00 58 bc 24  37 4d 32 f1 6d c9 50 18   ·····X·$ 7M2·m·P·
0030  01 00 48 a5 00 00 00 00  00 ea 6a 81 e7 30 81 e4   ··H····· ··j··0··
0040  a1 03 02 01 05 a2 03 02  01 0a a3 15 30 13 30 11   ········ ····0·0·
0050  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
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
0120  20 20 20 20
```

CNameString (kerberos.CNameString), 16 bytes | Packets: 104286 · Displayed: 19 (0.0%) | Profile: Default

Status: Running

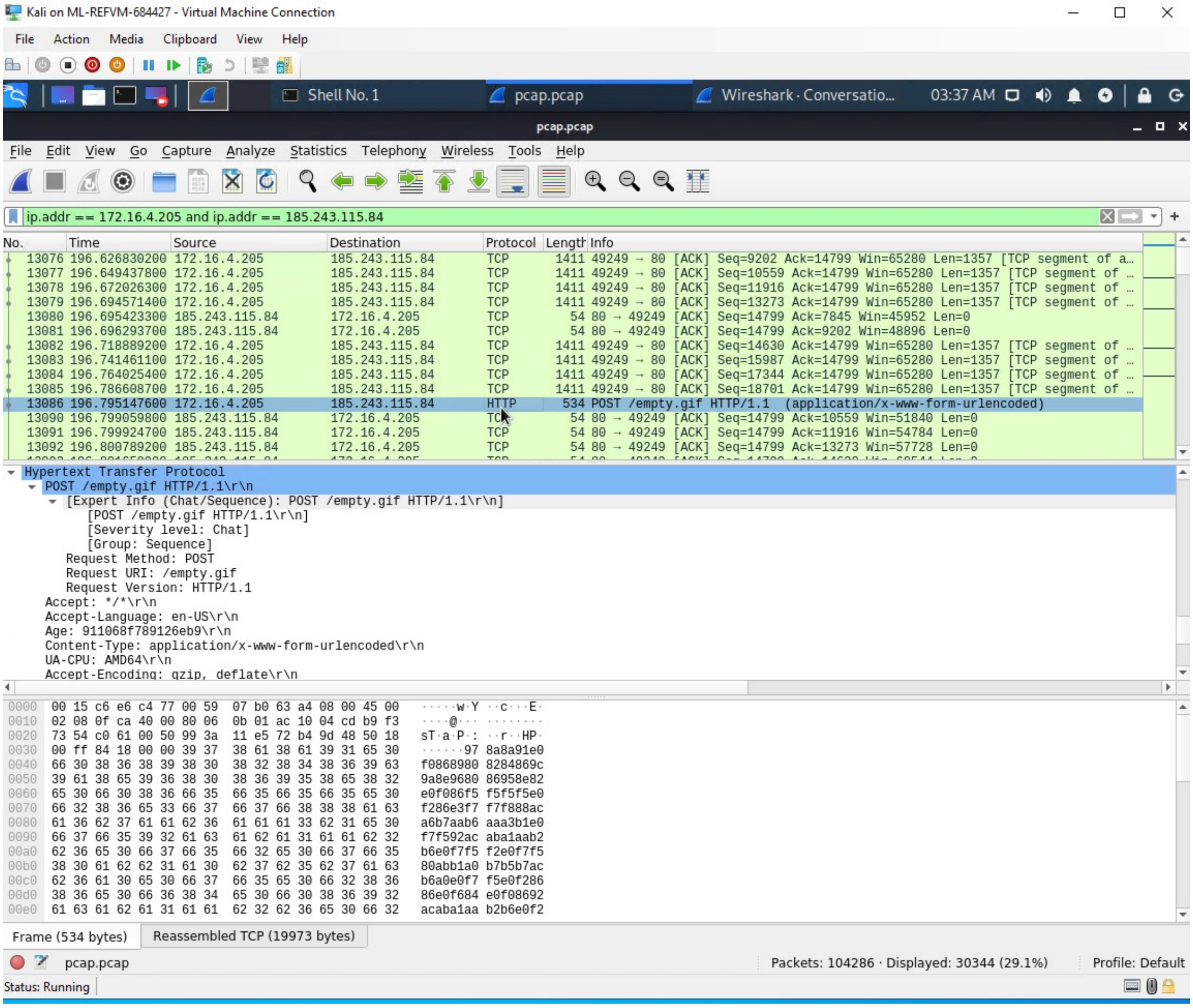
3. What are the IP addresses used in the actual infection traffic?

- 3 IP addresses involved with the majority of network traffic:
  - `172.16.4.205`
  - `185.243.115.84`
  - `166.62.11.64`
- WireShark Filter: `ip.src==172.16.4.205`
- Finding the IP addresses:
  - Click on the Statistics Tab
  - Select the Conversation
  - Select the IPv4
  - Sort Packets high to low
  - Select function "Limit to Display Filter"


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · pcap.pcap
Ethernet · 6
IPv4 · 37
IPv6
TCP · 120
UDP · 83

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	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611	77 k	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762	126 k	
172.16.4.4	172.16.4.205	1,417	339 k	680	147 k	737	191 k	49.776799	1144.3125	1,034	
31.13.70.52	172.16.4.205	726	479 k	436	447 k	290	31 k	62.702930	989.8205	3,620	
93.95.100.178	172.16.4.205	722	419 k	418	391 k	304	28 k	116.562981	937.4512	3,336	
54.230.89.184	172.16.4.205	308	208 k	184	196 k	124	11 k	51.829430	1001.0016	1,571	

With examples of the infected traffic being:


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
pcap.pcap
Wireshark · Conversatio...
03:37 AM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.4.205 and ip.addr == 185.243.115.84

```
No.   Time          Source          Destination     Protocol Length Info
13076 196.626830200 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=9202 Ack=14799 Win=65280 Len=1357 [TCP segment of a…
13077 196.649437800 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=10559 Ack=14799 Win=65280 Len=1357 [TCP segment of …
13078 196.672026300 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=11916 Ack=14799 Win=65280 Len=1357 [TCP segment of …
13079 196.694571400 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=13273 Ack=14799 Win=65280 Len=1357 [TCP segment of …
13080 196.695423300 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK] Seq=14799 Ack=7845 Win=45952 Len=0
13081 196.696293700 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK] Seq=14799 Ack=9202 Win=48896 Len=0
13082 196.718889200 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=14630 Ack=14799 Win=65280 Len=1357 [TCP segment of …
13083 196.741461100 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=15987 Ack=14799 Win=65280 Len=1357 [TCP segment of …
13084 196.764025400 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=17344 Ack=14799 Win=65280 Len=1357 [TCP segment of …
13085 196.786608700 172.16.4.205    185.243.115.84  TCP      1411 49249 → 80 [ACK] Seq=18701 Ack=14799 Win=65280 Len=1357 [TCP segment of …
13086 196.795147600 172.16.4.205    185.243.115.84  HTTP      534 POST /empty.gif HTTP/1.1  (application/x-www-form-urlencoded)
13090 196.799059800 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK] Seq=14799 Ack=10559 Win=51840 Len=0
13091 196.799924700 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK] Seq=14799 Ack=11916 Win=54784 Len=0
13092 196.800789200 185.243.115.84  172.16.4.205    TCP        54 80 → 49249 [ACK] Seq=14799 Ack=13273 Win=57728 Len=0
```

```
Hypertext Transfer Protocol
  POST /empty.gif HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /empty.gif HTTP/1.1\r\n]
        [POST /empty.gif HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
    Request Method: POST
    Request URI: /empty.gif
    Request Version: HTTP/1.1
  Accept: */*\r\n
  Accept-Language: en-US\r\n
  Age: 911068f789126eb9\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  UA-CPU: AMD64\r\n
  Accept-Encoding: gzip, deflate\r\n
```

```
0000  00 15 c6 e6 c4 77 00 59  07 b0 63 a4 08 00 45 00   ·····w·Y ··c···E·
0010  02 08 0f ca 40 00 80 06  0b 01 ac 10 04 cd b9 f3   ····@··· ········
0020  73 54 c0 61 00 50 99 3a  11 e5 72 b4 9d 48 50 18   sT·a·P·: ··r··HP·
0030  00 ff 84 18 00 00 39 37  38 61 38 61 39 31 65 30   ······97 8a8a91e0
0040  66 30 38 36 38 39 38 30  38 32 38 34 38 36 39 63   f0868980 8284869c
0050  39 61 38 65 39 36 38 30  38 36 39 35 38 65 38 32   9a8e9680 86958e82
0060  65 30 66 30 38 36 66 35  66 35 66 35 66 35 65 30   e0f086f5 f5f5f5e0
0070  66 32 38 36 65 33 66 37  66 37 66 38 38 38 61 63   f286e3f7 f7f888ac
0080  61 36 62 37 61 61 62 36  61 61 61 33 62 31 65 30   a6b7aab6 aaa3b1e0
0090  66 37 66 35 39 32 61 63  61 62 61 31 61 61 62 32   f7f592ac aba1aab2
00a0  62 36 65 30 66 37 66 35  66 32 65 30 66 37 66 35   b6e0f7f5 f2e0f7f5
00b0  38 30 61 62 62 31 61 30  62 37 62 35 62 37 61 63   80abb1a0 b7b5b7ac
00c0  62 36 61 30 65 30 66 37  66 35 65 30 66 32 38 36   b6a0e0f7 f5e0f286
00d0  38 36 65 30 66 36 38 34  65 30 66 30 38 36 39 32   86e0f684 e0f08692
00e0  61 63 61 62 61 31 61 61  62 32 62 36 65 30 66 32   acaba1aa b2b6e0f2
```

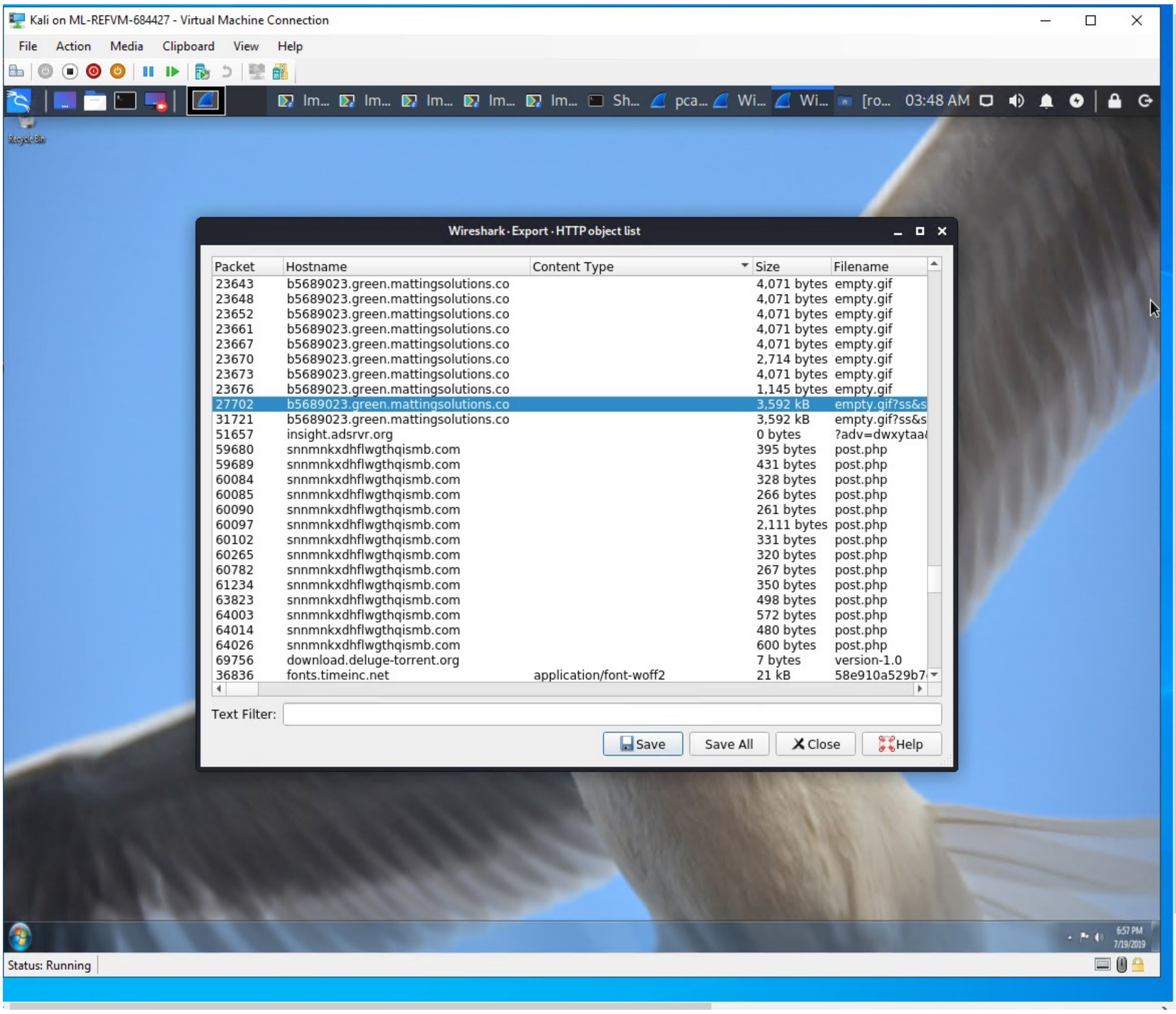
Frame (534 bytes) | Reassembled TCP (19973 bytes)

pcap.pcap — Packets: 104286 · Displayed: 30344 (29.1%) — Profile: Default

Status: Running

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

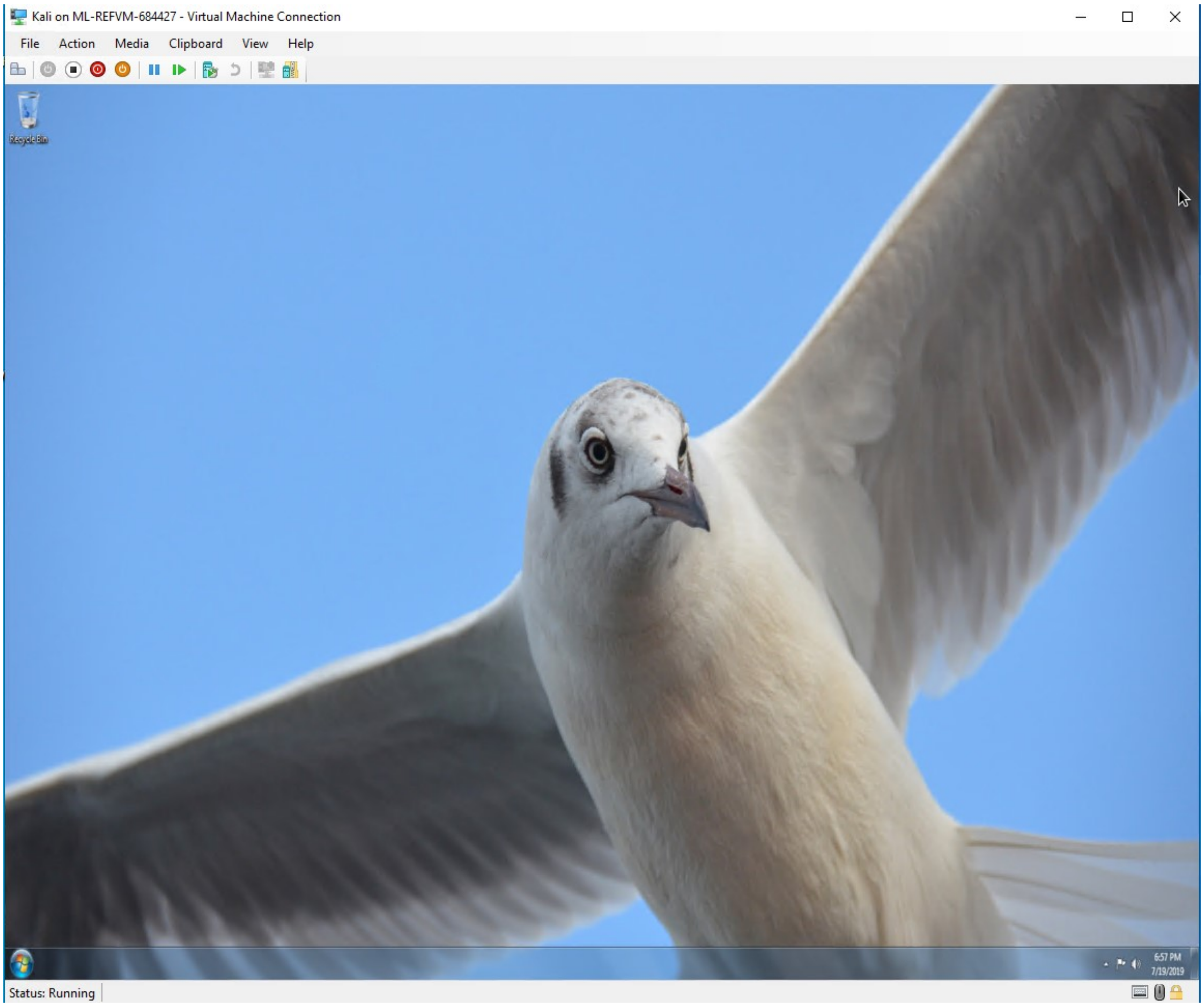
Using the Object Export/HTTP, and going through the gif and jpg images, we found the desktop image.



Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
23643	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
23648	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
23652	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
23661	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
23667	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
23670	b5689023.green.mattingsolutions.co		2,714 bytes	empty.gif
23673	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
23676	b5689023.green.mattingsolutions.co		1,145 bytes	empty.gif
27702	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&s
31721	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&s
51657	insight.adsrvr.org		0 bytes	?adv=dwxytaa
59680	snnmnkxdhflwgthqismb.com		395 bytes	post.php
59689	snnmnkxdhflwgthqismb.com		431 bytes	post.php
60084	snnmnkxdhflwgthqismb.com		328 bytes	post.php
60085	snnmnkxdhflwgthqismb.com		266 bytes	post.php
60090	snnmnkxdhflwgthqismb.com		261 bytes	post.php
60097	snnmnkxdhflwgthqismb.com		2,111 bytes	post.php
60102	snnmnkxdhflwgthqismb.com		331 bytes	post.php
60265	snnmnkxdhflwgthqismb.com		320 bytes	post.php
60782	snnmnkxdhflwgthqismb.com		267 bytes	post.php
61234	snnmnkxdhflwgthqismb.com		350 bytes	post.php
63823	snnmnkxdhflwgthqismb.com		498 bytes	post.php
64003	snnmnkxdhflwgthqismb.com		572 bytes	post.php
64014	snnmnkxdhflwgthqismb.com		480 bytes	post.php
64026	snnmnkxdhflwgthqismb.com		600 bytes	post.php
69756	download.deluge-torrent.org		7 bytes	version-1.0
36836	fonts.timeinc.net	application/font-woff2	21 kB	58e910a529b7

Text Filter:



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 in your Network Report:

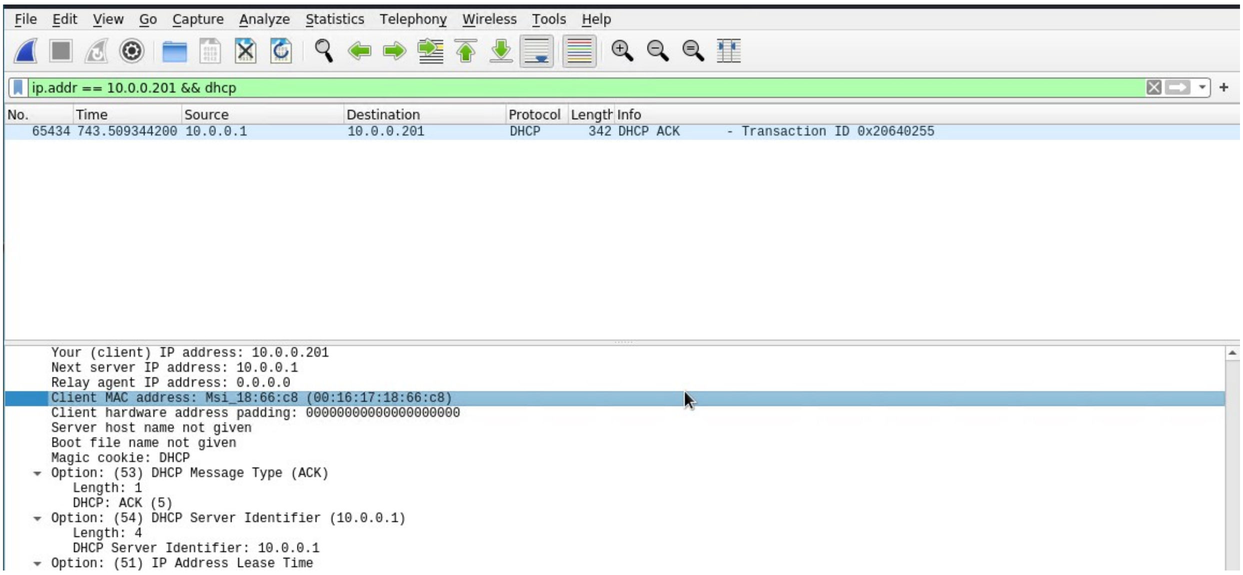
1. Find the following information about the machine with IP address `10.0.0.201` :

- MAC address: `00:16:17:18:66:c8`
- Windows username: `elmer.blanco`

- OS version: `Windows NT 10.0`

WireShark Filters

- Wireshark Filter for MAC Address: ip.addr == 10.0.0.201 && dhcp

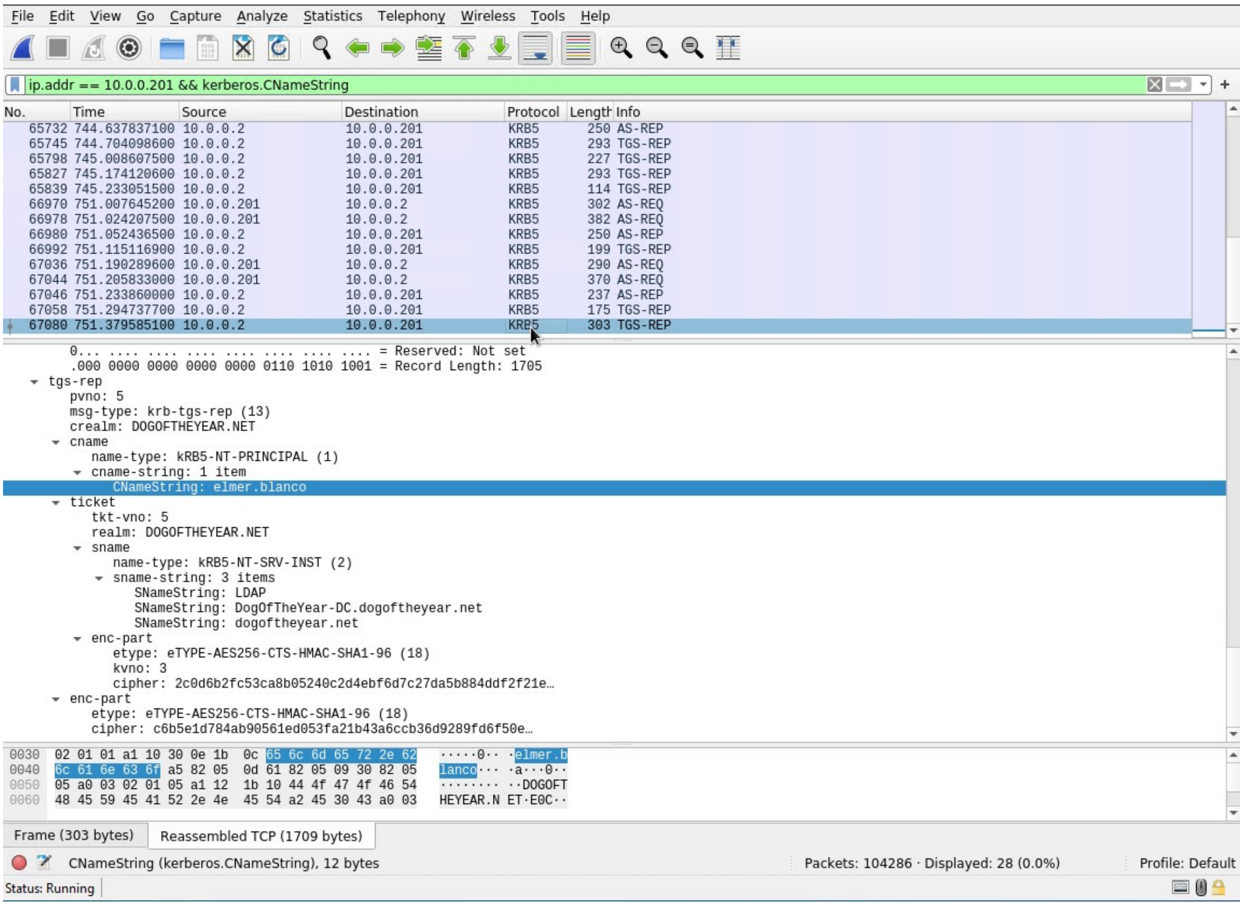

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.0.201 && dhcp

```
No.   Time          Source       Destination   Protocol Length Info
65434 743.509344200 10.0.0.1     10.0.0.201    DHCP      342 DHCP ACK      - Transaction ID 0x20640255
```

```
      Your (client) IP address: 10.0.0.201
      Next server IP address: 10.0.0.1
      Relay agent IP address: 0.0.0.0
      Client MAC address: Msi_18:66:c8 (00:16:17:18:66:c8)
      Client hardware address padding: 00000000000000000000
      Server host name not given
      Boot file name not given
      Magic cookie: DHCP
    ▾ Option: (53) DHCP Message Type (ACK)
         Length: 1
         DHCP: ACK (5)
    ▾ Option: (54) DHCP Server Identifier (10.0.0.1)
         Length: 4
         DHCP Server Identifier: 10.0.0.1
    ▾ Option: (51) IP Address Lease Time
```

- WireShark Filter for Username: ip.addr == 10.0.0.201 && kerberos.CNameString


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.0.201 && kerberos.CNameString

```
No.   Time          Source       Destination   Protocol Length Info
65732 744.637837100 10.0.0.2     10.0.0.201    KRB5      250 AS-REP
65745 744.704098600 10.0.0.2     10.0.0.201    KRB5      293 TGS-REP
65798 745.008607500 10.0.0.2     10.0.0.201    KRB5      227 TGS-REP
65827 745.174120600 10.0.0.2     10.0.0.201    KRB5      293 TGS-REP
65839 745.233051500 10.0.0.2     10.0.0.201    KRB5      114 TGS-REP
66970 751.007645200 10.0.0.201   10.0.0.2      KRB5      302 AS-REQ
66978 751.024207500 10.0.0.201   10.0.0.2      KRB5      382 AS-REQ
66980 751.052436500 10.0.0.2     10.0.0.201    KRB5      250 AS-REP
66992 751.115116900 10.0.0.2     10.0.0.201    KRB5      199 TGS-REP
67036 751.190289600 10.0.0.201   10.0.0.2      KRB5      290 AS-REQ
67044 751.205833000 10.0.0.201   10.0.0.2      KRB5      370 AS-REQ
67046 751.233860000 10.0.0.2     10.0.0.201    KRB5      237 AS-REP
67058 751.294737700 10.0.0.2     10.0.0.201    KRB5      175 TGS-REP
67080 751.379585100 10.0.0.2     10.0.0.201    KRB5      303 TGS-REP
```

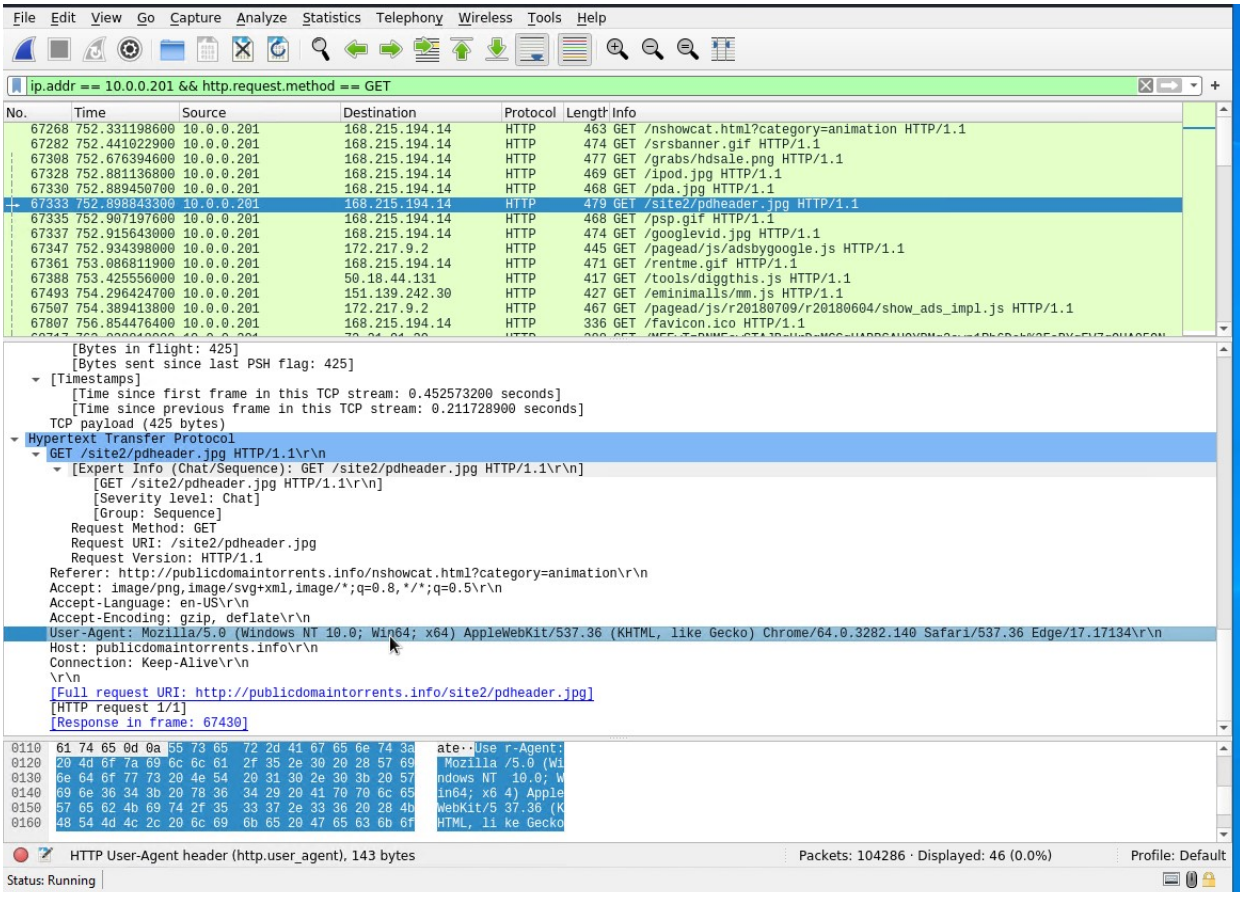
```
        0... .... .... .... .... .... .... .... = Reserved: Not set
        .000 0000 0000 0000 0000 0110 1010 1001 = Record Length: 1705
    ▾ tgs-rep
        pvno: 5
        msg-type: krb-tgs-rep (13)
        crealm: DOGOFTHEYEAR.NET
      ▾ cname
           name-type: kRB5-NT-PRINCIPAL (1)
         ▾ cname-string: 1 item
              CNameString: elmer.blanco
      ▾ ticket
           tkt-vno: 5
           realm: DOGOFTHEYEAR.NET
         ▾ sname
              name-type: kRB5-NT-SRV-INST (2)
            ▾ sname-string: 3 items
                 SNameString: LDAP
                 SNameString: DogOfTheYear-DC.dogoftheyear.net
                 SNameString: dogoftheyear.net
         ▾ enc-part
              etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
              kvno: 3
              cipher: 2c0d6b2fc53ca8b05240c2d4ebf6d7c27da5b884ddf2f21e…
      ▾ enc-part
           etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
           cipher: c6b5e1d784ab90561ed053fa21b43a6ccb36d9289fd6f50e…
```

```
0030  02 01 01 a1 10 30 0e 1b  0c 65 6c 6d 65 72 2e 62   ·····0·· ·elmer.b
0040  6c 61 6e 63 6f a5 82 05  0d 61 82 05 09 30 82 05   lanco··· ·a···0··
0050  05 a0 03 02 01 05 a1 12  1b 10 44 4f 47 4f 46 54   ········ ··DOGOFT
0060  48 45 59 45 41 52 2e 4e  45 54 a2 45 30 43 a0 03   HEYEAR.N ET·E0C··
```

CNameString (kerberos.CNameString), 12 bytes   Packets: 104286 · Displayed: 28 (0.0%)   Profile: Default

Status: Running

- Wireshark Filter for OS Type and Version: ip.addr == 10.0.0.201 && http.request/method == GET


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.0.0.201 && http.request.method == GET
```

```
No.    Time          Source      Destination     Protocol Length Info
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
67308 752.676394600 10.0.0.201  168.215.194.14  HTTP      477 GET /grabs/hdsale.png HTTP/1.1
67328 752.881136800 10.0.0.201  168.215.194.14  HTTP      469 GET /ipod.jpg HTTP/1.1
67330 752.889450700 10.0.0.201  168.215.194.14  HTTP      468 GET /pda.jpg HTTP/1.1
67333 752.898843300 10.0.0.201  168.215.194.14  HTTP      479 GET /site2/pdheader.jpg HTTP/1.1
67335 752.907197600 10.0.0.201  168.215.194.14  HTTP      468 GET /psp.gif HTTP/1.1
67337 752.915643000 10.0.0.201  168.215.194.14  HTTP      474 GET /googlevid.jpg HTTP/1.1
67347 752.934398000 10.0.0.201  172.217.9.2     HTTP      445 GET /pagead/js/adsbygoogle.js HTTP/1.1
67361 753.086811900 10.0.0.201  168.215.194.14  HTTP      471 GET /rentme.gif HTTP/1.1
67388 753.425556000 10.0.0.201  50.18.44.131    HTTP      417 GET /tools/diggthis.js HTTP/1.1
67493 754.296424700 10.0.0.201  151.139.242.30  HTTP      427 GET /eminimalls/mm.js HTTP/1.1
67507 754.389413800 10.0.0.201  172.217.9.2     HTTP      467 GET /pagead/js/r20180709/r20180604/show_ads_impl.js HTTP/1.1
67807 756.854476400 10.0.0.201  168.215.194.14  HTTP      336 GET /favicon.ico HTTP/1.1
```

```
      [Bytes in flight: 425]
      [Bytes sent since last PSH flag: 425]
    [Timestamps]
      [Time since first frame in this TCP stream: 0.452573200 seconds]
      [Time since previous frame in this TCP stream: 0.211728900 seconds]
    TCP payload (425 bytes)
  Hypertext Transfer Protocol
    GET /site2/pdheader.jpg HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /site2/pdheader.jpg HTTP/1.1\r\n]
        [GET /site2/pdheader.jpg HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /site2/pdheader.jpg
      Request Version: HTTP/1.1
    Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\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 Edge/17.17134\r\n
    Host: publicdomaintorrents.info\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://publicdomaintorrents.info/site2/pdheader.jpg]
    [HTTP request 1/1]
    [Response in frame: 67430]
```

```
0110  61 74 65 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   ate··Use r-Agent:
0120  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
0130  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
0140  69 6e 36 34 3b 20 78 36  34 29 20 41 70 70 6c 65   in64; x6 4) Apple
0150  57 65 62 4b 69 74 2f 35  33 37 2e 33 36 20 28 4b   WebKit/5 37.36 (K
0160  48 54 4d 4c 2c 20 6c 69  6b 65 20 47 65 63 6b 6f   HTML, li ke Gecko
```

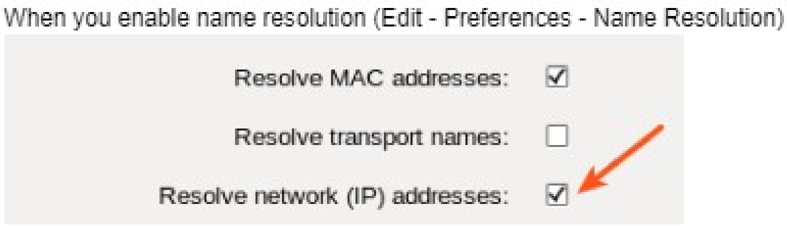
HTTP User-Agent header (http.user_agent), 143 bytes · Packets: 104286 · Displayed: 46 (0.0%) · Profile: Default

Status: Running

2. Which torrent file did the user download?

- Wireshark Filter for finding Torrent File: ip.addr == 10.0.0.201 && http.request/method == GET

First, set up WireShark to resolve the IP Addresses:


When you enable name resolution (Edit - Preferences - Name Resolution)

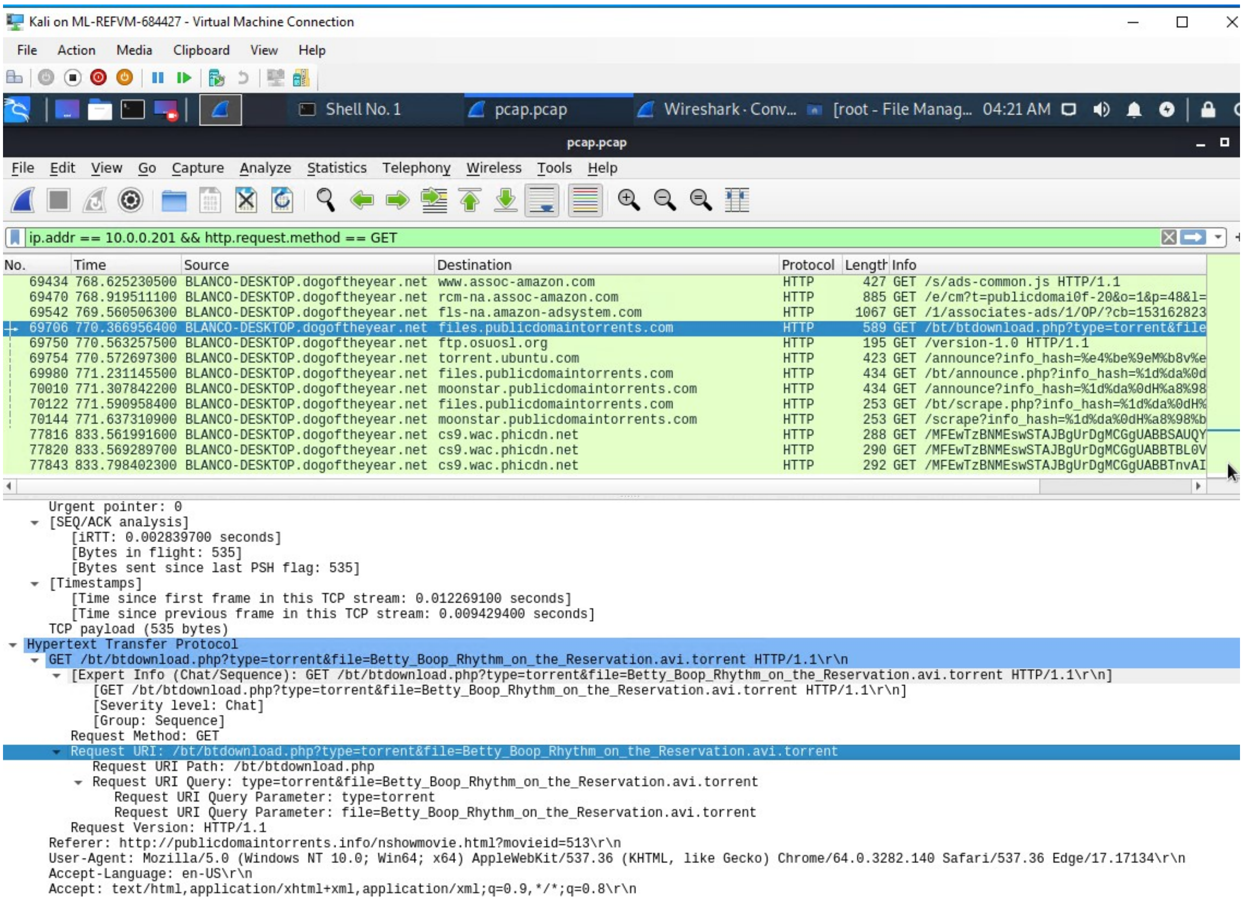
Resolve MAC addresses: ☑

Resolve transport names: □

Resolve network (IP) addresses: ☑

Once teh files.publicdomaintorrents.com Destination is found, look for the btdownload information, which shows that the file downloaded is

Betty_Boop_Rhythm_on_the_Reservation.avi.torrent


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
pcap.pcap
Wireshark · Conv...
[root - File Manag...
04:21 AM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

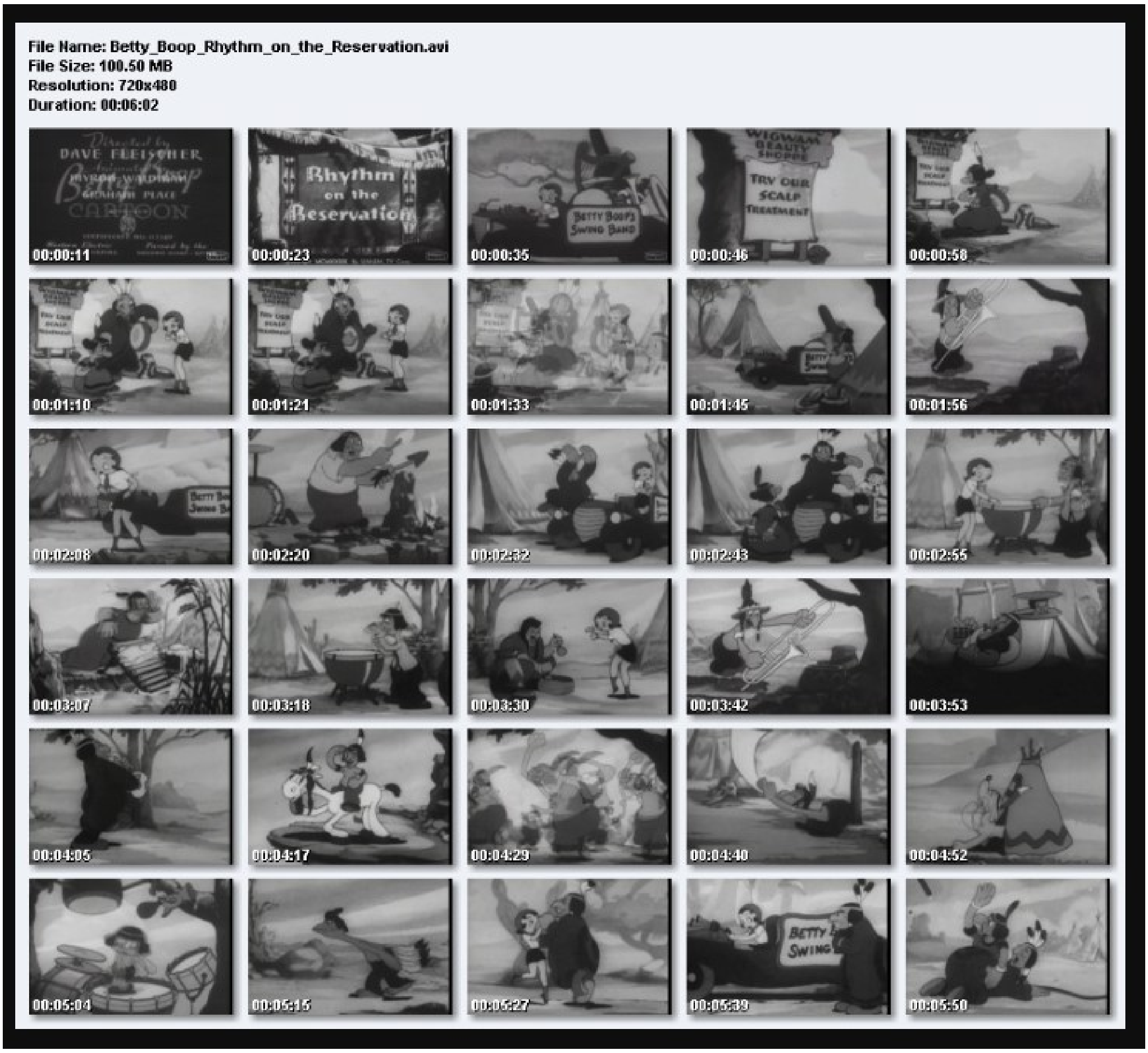
```
ip.addr == 10.0.0.201 && http.request.method == GET
```

```
No.     Time           Source                            Destination                         Protocol  Length Info
  69434 768.625230500 BLANCO-DESKTOP.dogoftheyear.net www.assoc-amazon.com                  HTTP       427 GET /s/ads-common.js HTTP/1.1
  69470 768.919511100 BLANCO-DESKTOP.dogoftheyear.net rcm-na.assoc-amazon.com               HTTP       885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=
  69542 769.560506300 BLANCO-DESKTOP.dogoftheyear.net fls-na.amazon-adsystem.com            HTTP      1067 GET /1/associates-ads/1/OP/?cb=153162823
  69706 770.366956400 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com        HTTP       589 GET /bt/btdownload.php?type=torrent&file
  69750 770.563257500 BLANCO-DESKTOP.dogoftheyear.net ftp.osuosl.org                        HTTP       195 GET /version-1.0 HTTP/1.1
  69754 770.572697300 BLANCO-DESKTOP.dogoftheyear.net torrent.ubuntu.com                    HTTP       423 GET /announce?info_hash=%e4%be%9eM%b8v%e
  69980 771.231145500 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com        HTTP       434 GET /bt/announce.php?info_hash=%1d%da%0d
  70010 771.307842200 BLANCO-DESKTOP.dogoftheyear.net moonstar.publicdomaintorrents.com     HTTP       434 GET /announce?info_hash=%1d%da%0dH%a8%98
  70122 771.590958400 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com        HTTP       253 GET /bt/scrape.php?info_hash=%1d%da%0dH%
  70144 771.637310900 BLANCO-DESKTOP.dogoftheyear.net moonstar.publicdomaintorrents.com     HTTP       253 GET /scrape?info_hash=%1d%da%0dH%a8%98%b
  77816 833.561991600 BLANCO-DESKTOP.dogoftheyear.net cs9.wac.phicdn.net                    HTTP       288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQY
  77820 833.569289700 BLANCO-DESKTOP.dogoftheyear.net cs9.wac.phicdn.net                    HTTP       290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V
  77843 833.798402300 BLANCO-DESKTOP.dogoftheyear.net cs9.wac.phicdn.net                    HTTP       292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI
```

```
    Urgent pointer: 0
  ▾ [SEQ/ACK analysis]
      [iRTT: 0.002839700 seconds]
      [Bytes in flight: 535]
      [Bytes sent since last PSH flag: 535]
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.012269100 seconds]
      [Time since previous frame in this TCP stream: 0.009429400 seconds]
    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
    ▾ [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
        [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
    ▾ Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
        Request URI Path: /bt/btdownload.php
      ▾ Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
          Request URI Query Parameter: type=torrent
          Request URI Query Parameter: file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
      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/64.0.3282.140 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
```

The file can be further researched, and a summary can be found here:

http://www.publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg



File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 100.50 MB
Resolution: 720x480
Duration: 00:06:02