Network Forensic Analysis Report

The Security team requested this analysis because they have evidence that people are misusing the network. 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. A number of machines from foreign subnets are sending traffic to this network. They have set up an Active Directory network. Their IP addresses are somewhere in the range `10.6.12.0/24`.

So far, Security knows the following about these time thieves:

1. "Time thieves" spotted watching YouTube during work hours - At least two users on the network have been wasting time on YouTube.
2. At least one Windows host is infected with a virus.
3. Noticed some Illegal downloads.

Below is the analysis done on the network traffic capture for the above 3 observations:

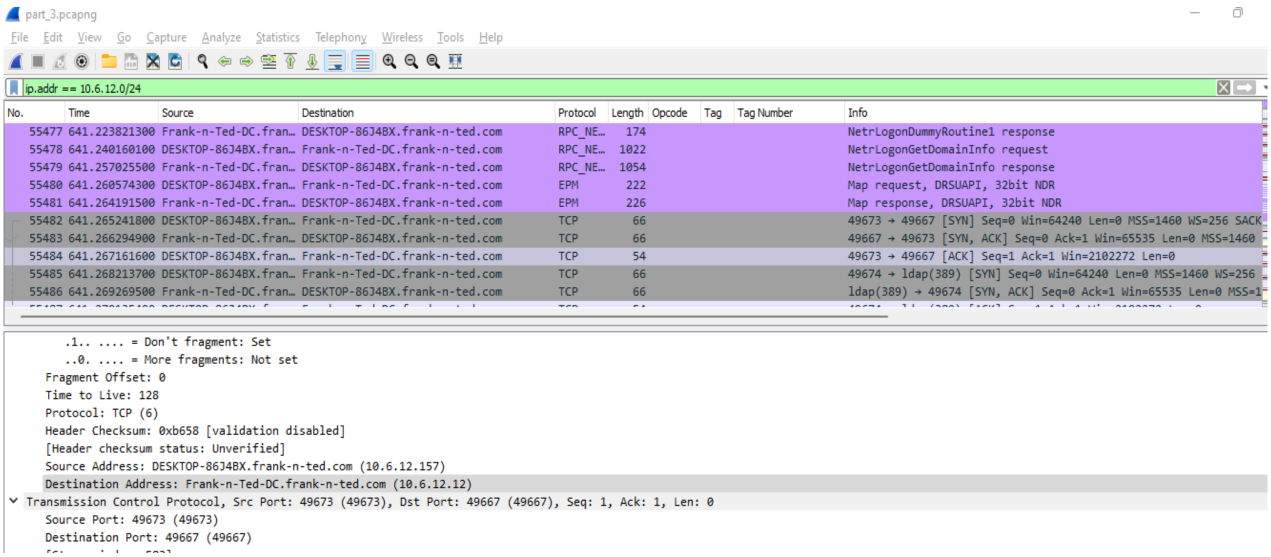
Time Thieves

After inspecting the traffic capture the following observations were made:

1. Domain name of the users' custom site **Frank-n-Ted-DC.frank-n-ted.com**

The Wireshark Filter used: **ip.addr==10.6.12.0/24**

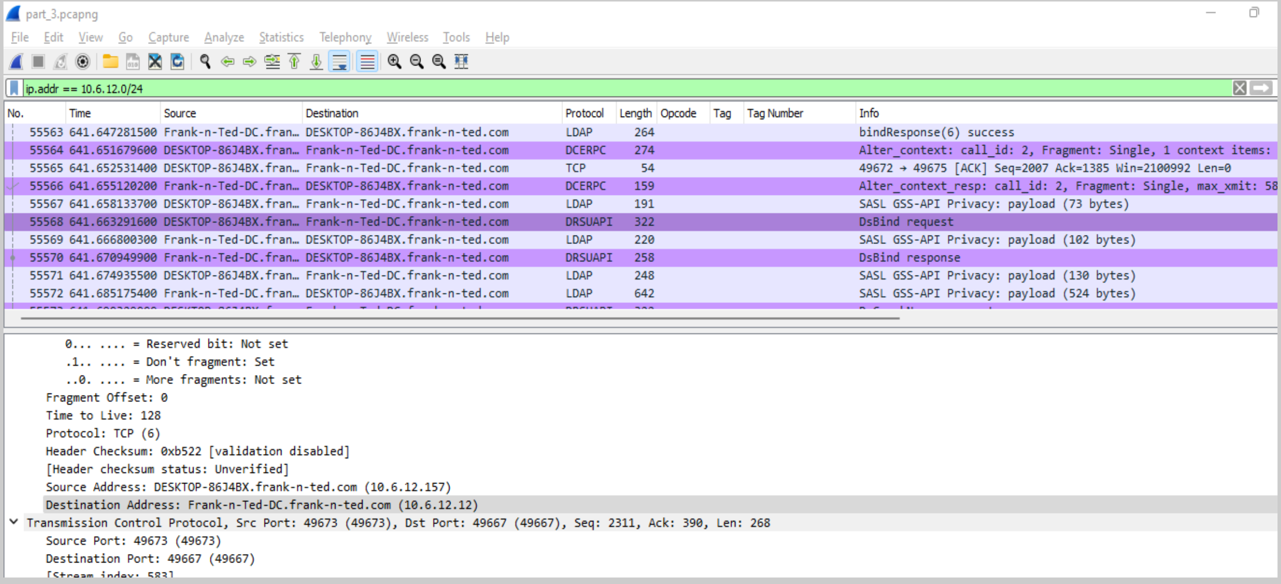
Below is a screenshot:


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.6.12.0/24

No.   Time           Source                   Destination                      Protocol  Length  Opcode  Tag  Tag Number  Info
55477 641.223821300 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  RPC_NE…  174   NetrLogonDummyRoutine1 response
55478 641.240160100 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  RPC_NE…  1022  NetrLogonGetDomainInfo request
55479 641.257025500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  RPC_NE…  1054  NetrLogonGetDomainInfo response
55480 641.260574300 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  EPM      222   Map request, DRSUAPI, 32bit NDR
55481 641.264191500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  EPM      226   Map response, DRSUAPI, 32bit NDR
55482 641.265241800 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  TCP      66    49673 → 49667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
55483 641.266294900 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  TCP      66    49667 → 49673 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
55484 641.267161600 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  TCP      54    49673 → 49667 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
55485 641.268213700 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  TCP      66    49674 → ldap(389) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
55486 641.269269500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  TCP      66    ldap(389) → 49674 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1

        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
      Fragment Offset: 0
      Time to Live: 128
      Protocol: TCP (6)
      Header Checksum: 0xb658 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
      Destination Address: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
  v Transmission Control Protocol, Src Port: 49673 (49673), Dst Port: 49667 (49667), Seq: 1, Ack: 1, Len: 0
      Source Port: 49673 (49673)
      Destination Port: 49667 (49667)
```

2. IP address of the Domain Controller (DC) of the AD network: **10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)**

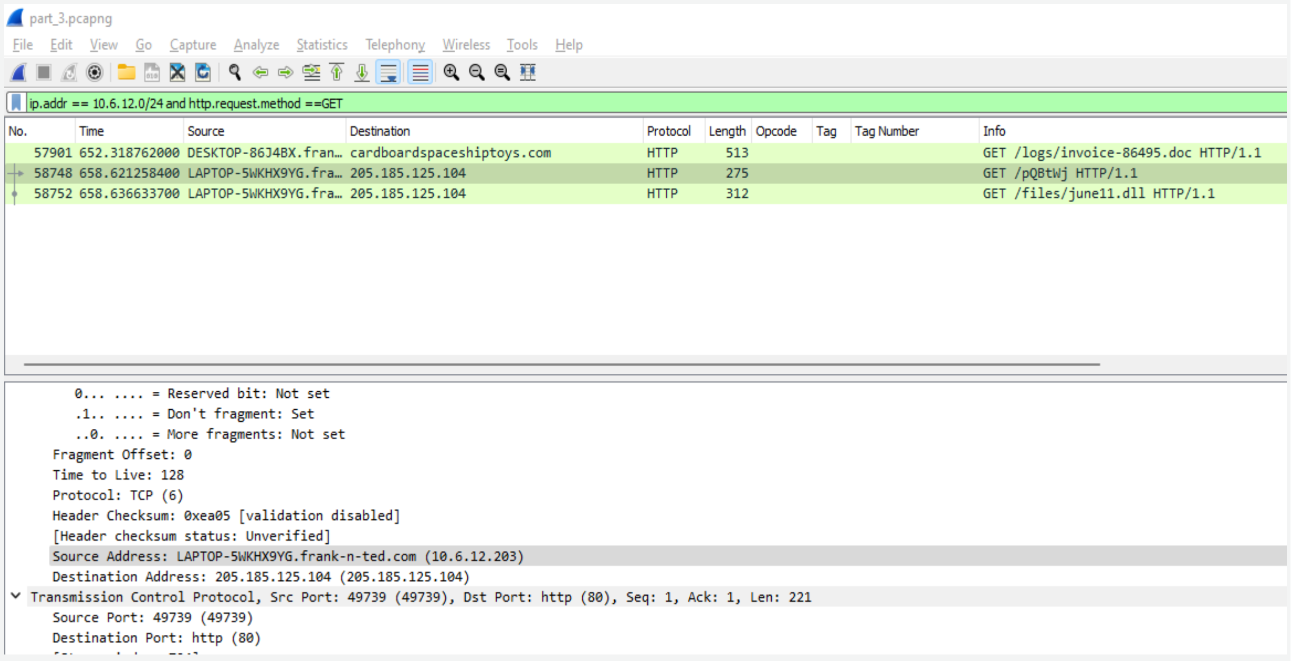
The Wireshark Filter used: **ip.addr==10.6.12.0/24**


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.6.12.0/24

No.   Time           Source                   Destination                      Protocol  Length  Opcode  Tag  Tag Number  Info
55563 641.647281500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  LDAP     264   bindResponse(6) success
55564 641.651679600 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  DCERPC   274   Alter_context: call_id: 2, Fragment: Single, 1 context items:
55565 641.652531400 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  TCP      54    49672 → 49675 [ACK] Seq=2007 Ack=1385 Win=2100992 Len=0
55566 641.655120200 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  DCERPC   159   Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 58
55567 641.658133700 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  LDAP     191   SASL GSS-API Privacy: payload (73 bytes)
55568 641.663291600 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  DRSUAPI  322   DsBind request
55569 641.666800300 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  LDAP     220   SASL GSS-API Privacy: payload (102 bytes)
55570 641.670949900 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  DRSUAPI  258   DsBind response
55571 641.674935500 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.frank-n-ted.com  LDAP     248   SASL GSS-API Privacy: payload (130 bytes)
55572 641.685175400 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.frank-n-ted.com  LDAP     642   SASL GSS-API Privacy: payload (524 bytes)

        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
      Fragment Offset: 0
      Time to Live: 128
      Protocol: TCP (6)
      Header Checksum: 0xb522 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
      Destination Address: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
  v Transmission Control Protocol, Src Port: 49673 (49673), Dst Port: 49667 (49667), Seq: 2311, Ack: 390, Len: 268
      Source Port: 49673 (49673)
      Destination Port: 49667 (49667)
```

3. Name of the malware downloaded to the 10.6.12.203 machine: **june11.dll**

The Wireshark Filter used: **ip.addr==10.16.12.203 and http.request.method==GET**


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

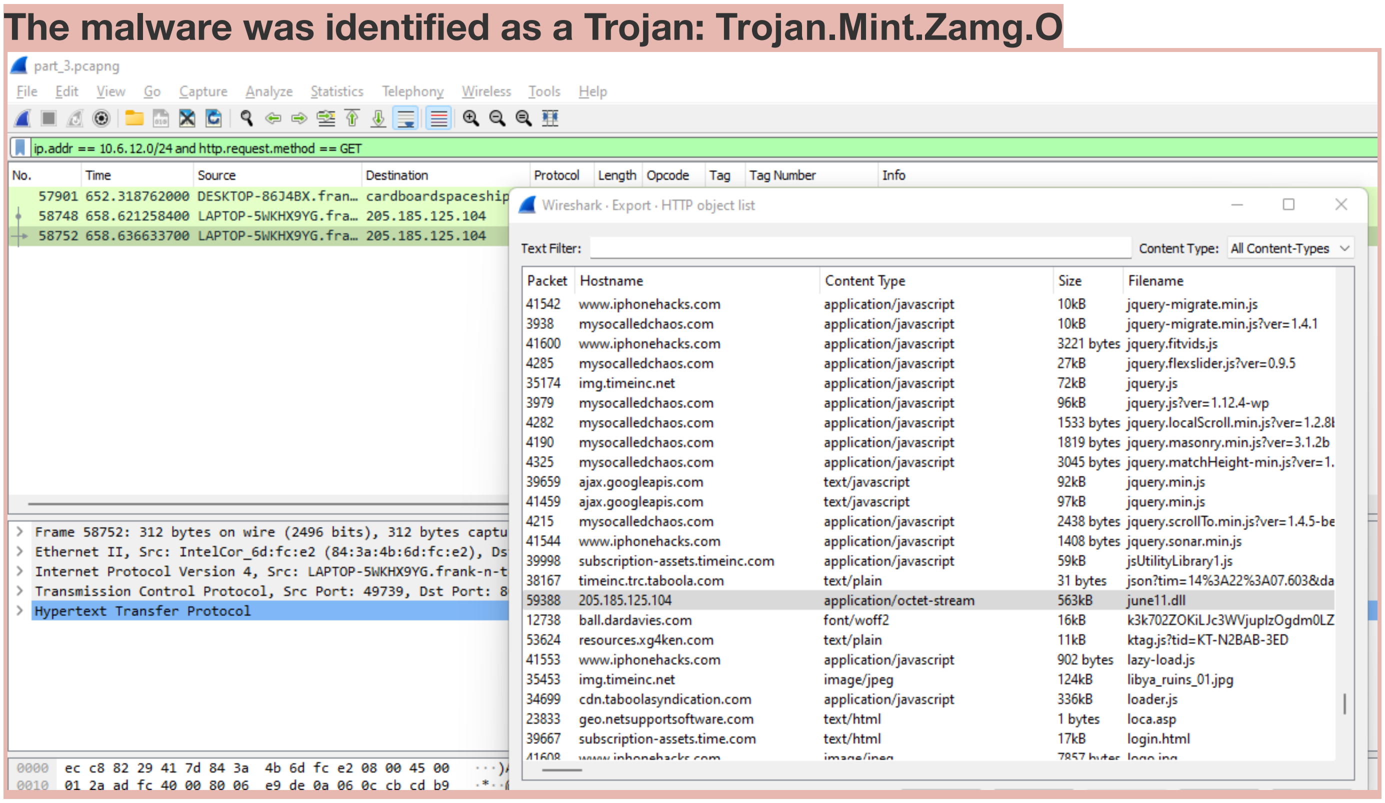
ip.addr == 10.6.12.0/24 and http.request.method ==GET

```
No.    Time          Source                    Destination                    Protocol  Length  Opcode  Tag  Tag Number  Info
57901 652.318762000 DESKTOP-86J4BX.fran… cardboardspaceshiptoys.com         HTTP      513                          GET /logs/invoice-86495.doc HTTP/1.1
58748 658.621258400 LAPTOP-5WKHX9YG.fra… 205.185.125.104                    HTTP      275                          GET /pQBtWj HTTP/1.1
58752 658.636633700 LAPTOP-5WKHX9YG.fra… 205.185.125.104                    HTTP      312                          GET /files/june11.dll HTTP/1.1
```

```
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
      Fragment Offset: 0
      Time to Live: 128
      Protocol: TCP (6)
      Header Checksum: 0xea05 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
      Destination Address: 205.185.125.104 (205.185.125.104)
  ∨ Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 1, Ack: 1, Len: 221
      Source Port: 49739 (49739)
      Destination Port: http (80)
```

4. Exporting this file to Kali machine's desktop, it was uploaded to VirusTotal.com to check if it was a malware. The file did classify as malware.

The malware was identified as a Trojan: Trojan.Mint.Zamg.O


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

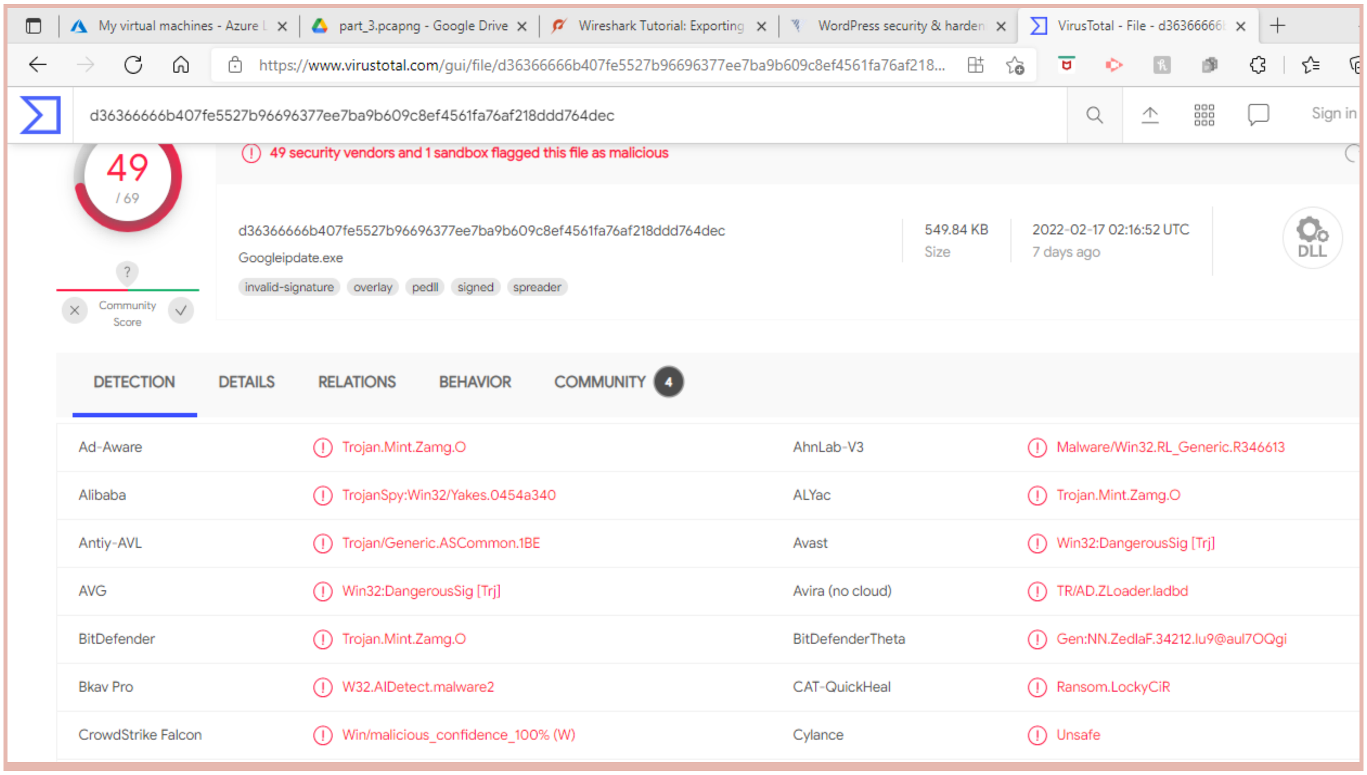
```
No.    Time          Source                    Destination           Protocol  Length  Opcode  Tag  Tag Number  Info
57901 652.318762000 DESKTOP-86J4BX.fran… cardboardspaceship
58748 658.621258400 LAPTOP-5WKHX9YG.fra… 205.185.125.104
58752 658.636633700 LAPTOP-5WKHX9YG.fra… 205.185.125.104
```

```
> Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captu
> Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Ds
> Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-t
> Transmission Control Protocol, Src Port: 49739, Dst Port: 8
> Hypertext Transfer Protocol

0000  ec c8 82 29 41 7d 84 3a  4b 6d fc e2 08 00 45 00   ···)A
0010  01 2a ad fc 40 00 80 06  e9 de 0a 06 0c cb cd b9   ·*··(
```

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
41542	www.iphonehacks.com	application/javascript	10kB	jquery-migrate.min.js
3938	mysocalledchaos.com	application/javascript	10kB	jquery-migrate.min.js?ver=1.4.1
41600	www.iphonehacks.com	application/javascript	3221 bytes	jquery.fitvids.js
4285	mysocalledchaos.com	application/javascript	27kB	jquery.flexslider.js?ver=0.9.5
35174	img.timeinc.net	application/javascript	72kB	jquery.js
3979	mysocalledchaos.com	application/javascript	96kB	jquery.js?ver=1.12.4-wp
4282	mysocalledchaos.com	application/javascript	1533 bytes	jquery.localScroll.min.js?ver=1.2.8
4190	mysocalledchaos.com	application/javascript	1819 bytes	jquery.masonry.min.js?ver=3.1.2b
4325	mysocalledchaos.com	application/javascript	3045 bytes	jquery.matchHeight-min.js?ver=1.
39659	ajax.googleapis.com	text/javascript	92kB	jquery.min.js
41459	ajax.googleapis.com	text/javascript	97kB	jquery.min.js
4215	mysocalledchaos.com	application/javascript	2438 bytes	jquery.scrollTo.min.js?ver=1.4.5-be
41544	www.iphonehacks.com	application/javascript	1408 bytes	jquery.sonar.min.js
39998	subscription-assets.timeinc.com	application/javascript	59kB	jsUtilityLibrary1.js
38167	timeinc.trc.taboola.com	text/plain	31 bytes	json?tim=14%3A22%3A07.603&da
59388	205.185.125.104	application/octet-stream	563kB	june11.dll
12738	ball.dardavies.com	font/woff2	16kB	k3k702ZOKiLJc3WVjuplzOgdm0LZ
53624	resources.xg4ken.com	text/plain	11kB	ktag.js?tid=KT-N2BAB-3ED
41553	www.iphonehacks.com	application/javascript	902 bytes	lazy-load.js
35453	img.timeinc.net	image/jpeg	124kB	libya_ruins_01.jpg
34699	cdn.taboolasyndication.com	application/javascript	336kB	loader.js
23833	geo.netsupportsoftware.com	text/html	1 bytes	loca.asp
39667	subscription-assets.time.com	text/html	17kB	login.html
41608	www.iphonehacks.com	image/jpeg	7857 bytes	logo.jpg


My virtual machines - Azure
part_3.pcapng - Google Drive
Wireshark Tutorial: Exporting
WordPress security & harden
VirusTotal - File - d36366666
https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218...
Sign in
49
/ 69
?
Community Score
DLL
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 4

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

49 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed spreader

549.84 KB
Size

2022-02-17 02:16:52 UTC
7 days ago

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	Gen:NN.ZedlaF.34212.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware2	CAT-QuickHeal	Ransom.LockyCiR
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe

Vulnerable Windows Machine

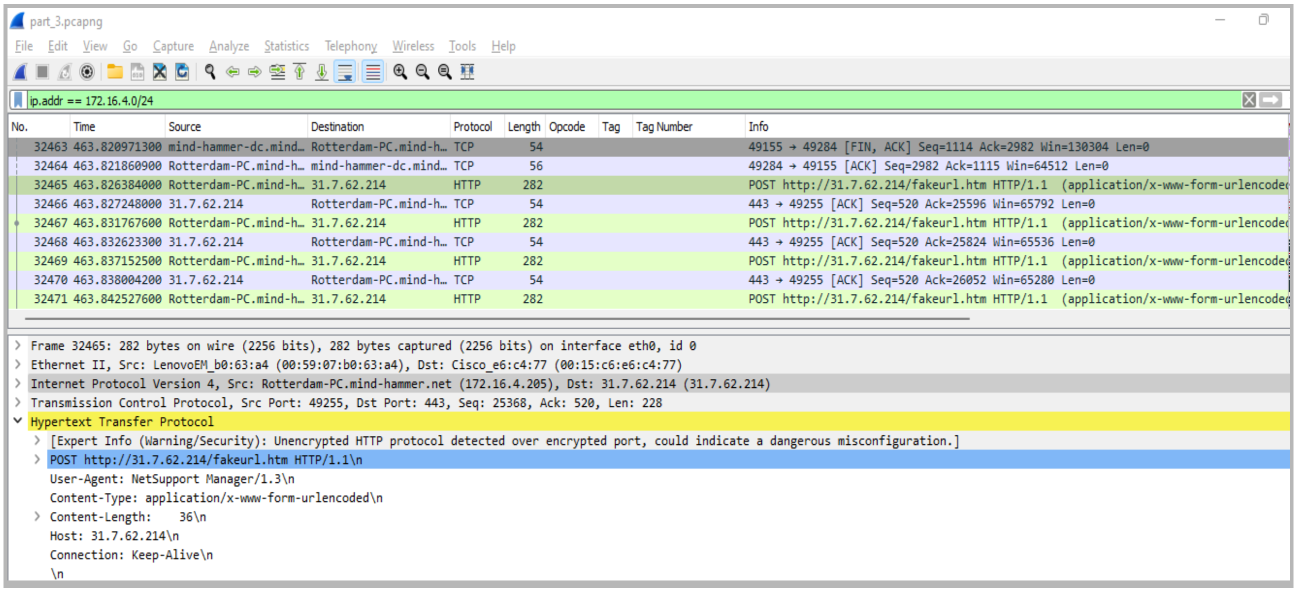
The Security team has received reports of an infected Windows host on the network. They know the following:

- 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.

Inspecting the traffic, below are the findings:

1. The following information was found about the infected Windows machine:
    - o Host name : **ROTTERDAM-PC**
    - o IP address: **172.16.4.205**
    - o MAC address: **00:59:07:b0:63:a4**

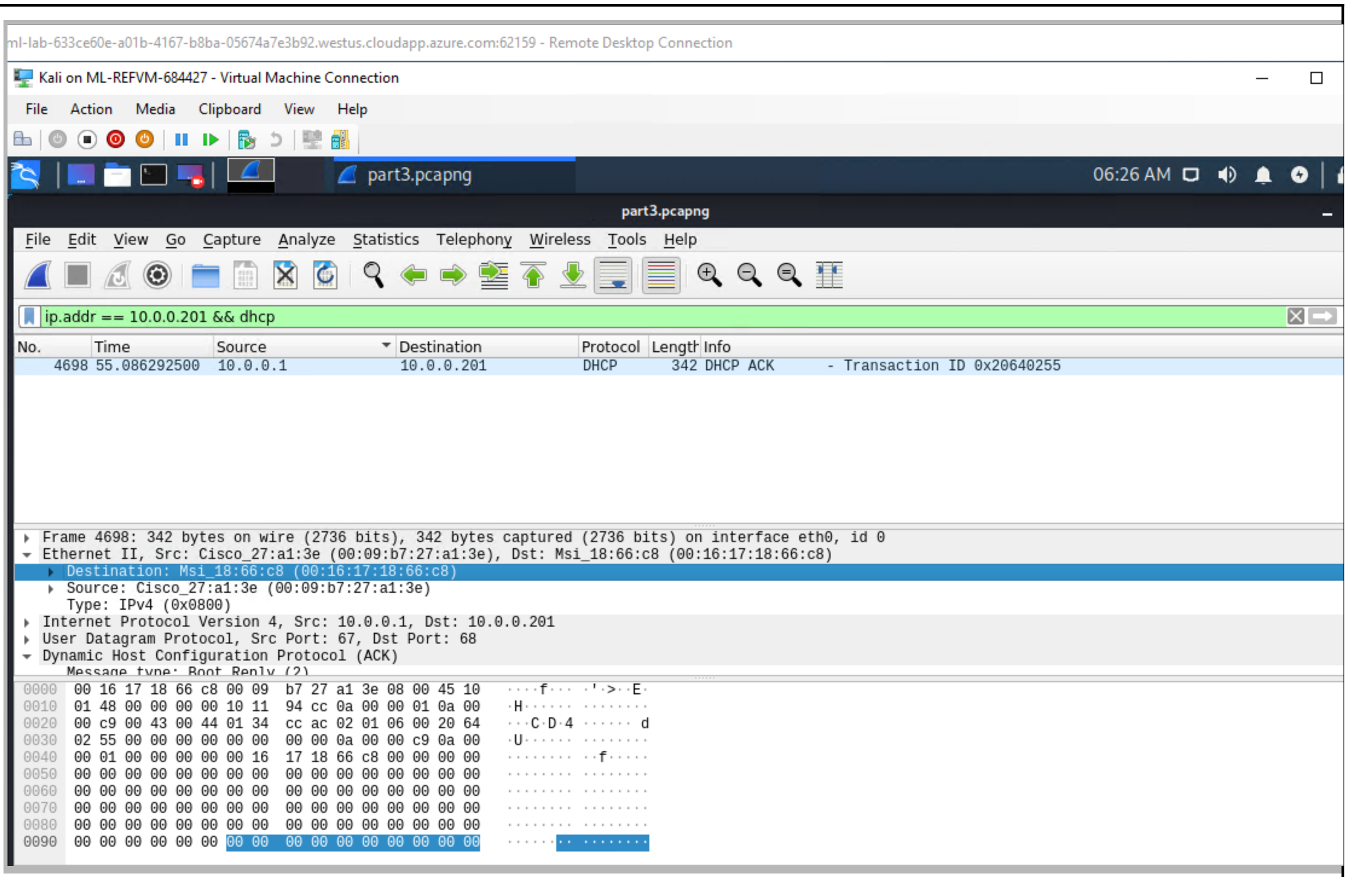
Wireshark Filter used: **ip.src==172.16.4.0/24**


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.4.0/24

No.	Time	Source	Destination	Protocol	Length	Opcode	Tag	Tag Number	Info
32463	463.820971300	mind-hammer-dc.mind…	Rotterdam-PC.mind-h…	TCP	54				49155 → 49284 [FIN, ACK] Seq=1114 Ack=2982 Win=130304 Len=0
32464	463.821860900	Rotterdam-PC.mind-h…	mind-hammer-dc.mind…	TCP	56				49284 → 49155 [ACK] Seq=2982 Ack=1115 Win=64512 Len=0
32465	463.826384000	Rotterdam-PC.mind-h…	31.7.62.214	HTTP	282				POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencode
32466	463.827248000	31.7.62.214	Rotterdam-PC.mind-h…	TCP	54				443 → 49255 [ACK] Seq=520 Ack=25596 Win=65792 Len=0
32467	463.831767600	Rotterdam-PC.mind-h…	31.7.62.214	HTTP	282				POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencode
32468	463.832623300	31.7.62.214	Rotterdam-PC.mind-h…	TCP	54				443 → 49255 [ACK] Seq=520 Ack=25824 Win=65536 Len=0
32469	463.837152500	Rotterdam-PC.mind-h…	31.7.62.214	HTTP	282				POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencode
32470	463.838004200	31.7.62.214	Rotterdam-PC.mind-h…	TCP	54				443 → 49255 [ACK] Seq=520 Ack=26052 Win=65280 Len=0
32471	463.842527600	Rotterdam-PC.mind-h…	31.7.62.214	HTTP	282				POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencode

```
> Frame 32465: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface eth0, id 0
> Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
> Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 31.7.62.214 (31.7.62.214)
> Transmission Control Protocol, Src Port: 49255, Dst Port: 443, Seq: 25368, Ack: 520, Len: 228
v Hypertext Transfer Protocol
  > [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
  > POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n
    User-Agent: NetSupport Manager/1.3\n
    Content-Type: application/x-www-form-urlencoded\n
  > Content-Length:    36\n
    Host: 31.7.62.214\n
    Connection: Keep-Alive\n
    \n
```


ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
part3.pcapng
06:26 AM
part3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.0.0.201 && dhcp
```

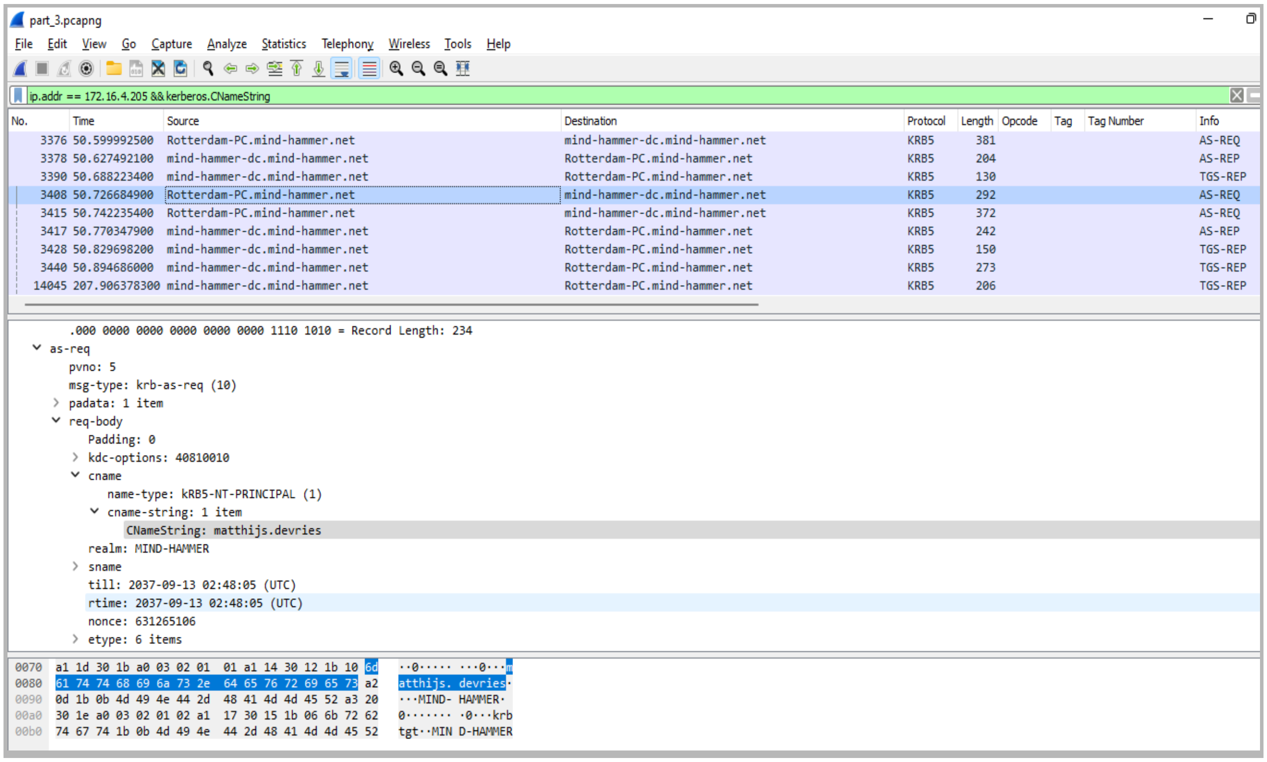
```
No.   Time          Source         Destination    Protocol Length Info
 4698 55.086292500  10.0.0.1       10.0.0.201     DHCP        342 DHCP ACK      - Transaction ID 0x20640255
```

```
▸ Frame 4698: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
▾ Ethernet II, Src: Cisco_27:a1:3e (00:09:b7:27:a1:3e), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)
   ▸ Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
   ▸ Source: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
     Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.201
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (ACK)
     Message type: Boot Reply (2)
```

```
0000  00 16 17 18 66 c8 00 09  b7 27 a1 3e 08 00 45 10   ····f··· ·'·>··E·
0010  01 48 00 00 00 00 10 11  94 cc 0a 00 00 01 0a 00   ·H······ ········
0020  00 c9 00 43 00 44 01 34  cc ac 02 01 06 00 20 64   ···C·D·4 ······ d
0030  02 55 00 00 00 00 00 00  00 00 0a 00 00 c9 0a 00   ·U······ ········
0040  00 01 00 00 00 00 00 16  17 18 66 c8 00 00 00 00   ········ ··f·····
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   ········ ········
```

2. Username of the Windows user whose computer is infected: **matthijs.devries.**

Wireshark Filter used: **ip.src==172.16.4.205 and kerberos.CNameString**


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 172.16.4.205 && kerberos.CNameString
```

No.	Time	Source	Destination	Protocol	Length	Opcode	Tag	Tag Number	Info
3376	50.599992500	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	381				AS-REQ
3378	50.627492100	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	204				AS-REP
3390	50.688223400	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	130				TGS-REP
3408	50.726684900	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	292				AS-REQ
3415	50.742235400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	372				AS-REQ
3417	50.770347900	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	242				AS-REP
3428	50.829698200	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	150				TGS-REP
3440	50.894686000	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	273				TGS-REP
14045	207.906378300	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	206				TGS-REP

```
    .000 0000 0000 0000 0000 0000 1110 1010 = Record Length: 234
  ˅ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    › padata: 1 item
    ˅ 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
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 631265106
      › etype: 6 items
```

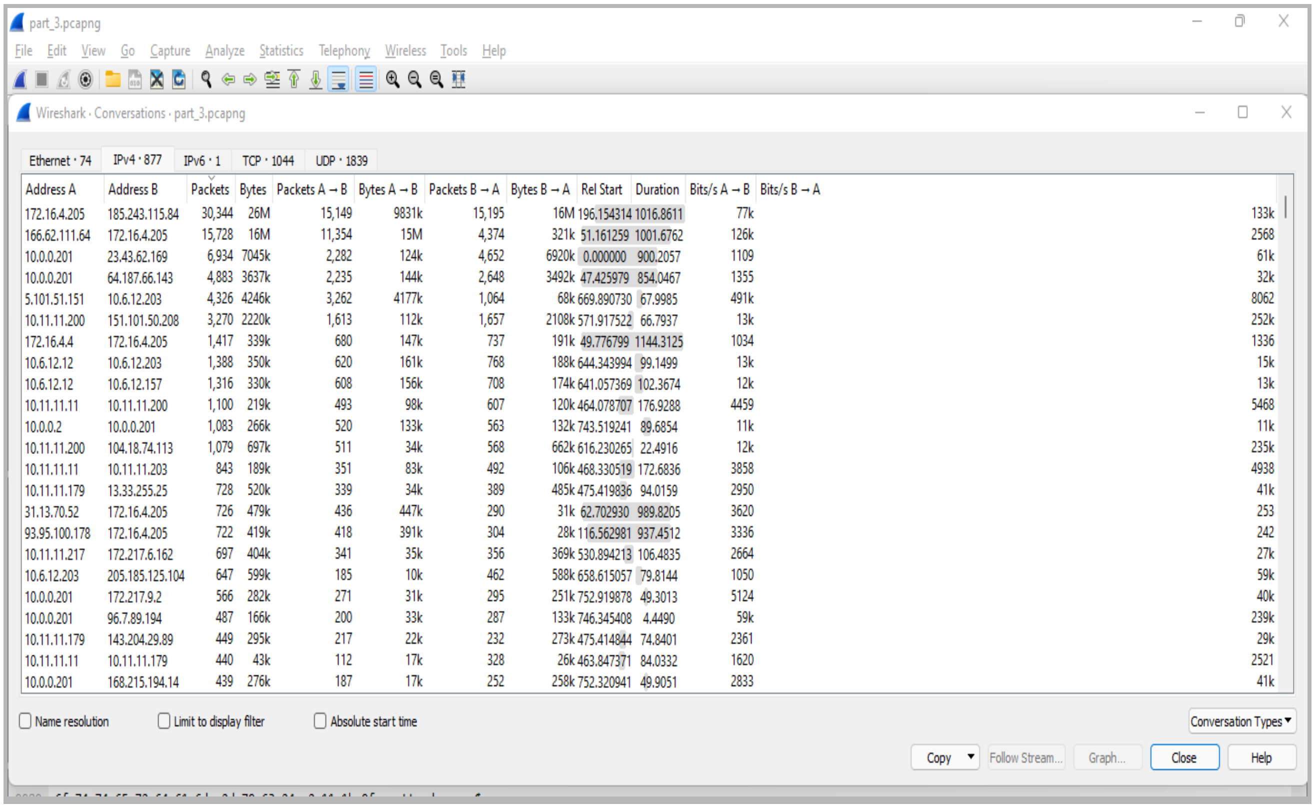
```
0070  a1 1d 30 1b a0 03 02 01  01 a1 14 30 12 1b 10 6d   ··0····· ···0···m
0080  61 74 74 68 69 6a 73 2e  64 65 76 72 69 65 73 a2   atthijs. devries·
0090  0d 1b 0b 4d 49 4e 44 2d  48 41 4d 4d 45 52 a3 20   ···MIND- HAMMER·
00a0  30 1e a0 03 02 01 02 a1  17 30 15 1b 06 6b 72 62   0······· ·0···krb
00b0  74 67 74 1b 0b 4d 49 4e  44 2d 48 41 4d 4d 45 52   tgt··MIN D-HAMMER
```

3. IP addresses used in the actual infection traffic:

Found 4 IP addresses: **172.16.4.205, 185.243.115.84, 64.187.66.143 and 23.43.62.169**

Wireshark Filter used: **ip.addr==172.16.4.205 and kerberos.CNameString (same as used for previous)**

I have used the Statistics feature of wireshark to filter the I/P addresses with the highest traffic. Select Statistics -> Select Conversation -> Select IPv4 -> Sort Packets high to low. The above mentioned 4 IP addresses have the highest no. of packets downloaded, hence indicating where the actual infection traffic is located.


part_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · part_3.pcapng
Ethernet · 74
IPv4 · 877
IPv6 · 1
TCP · 1044
UDP · 1839

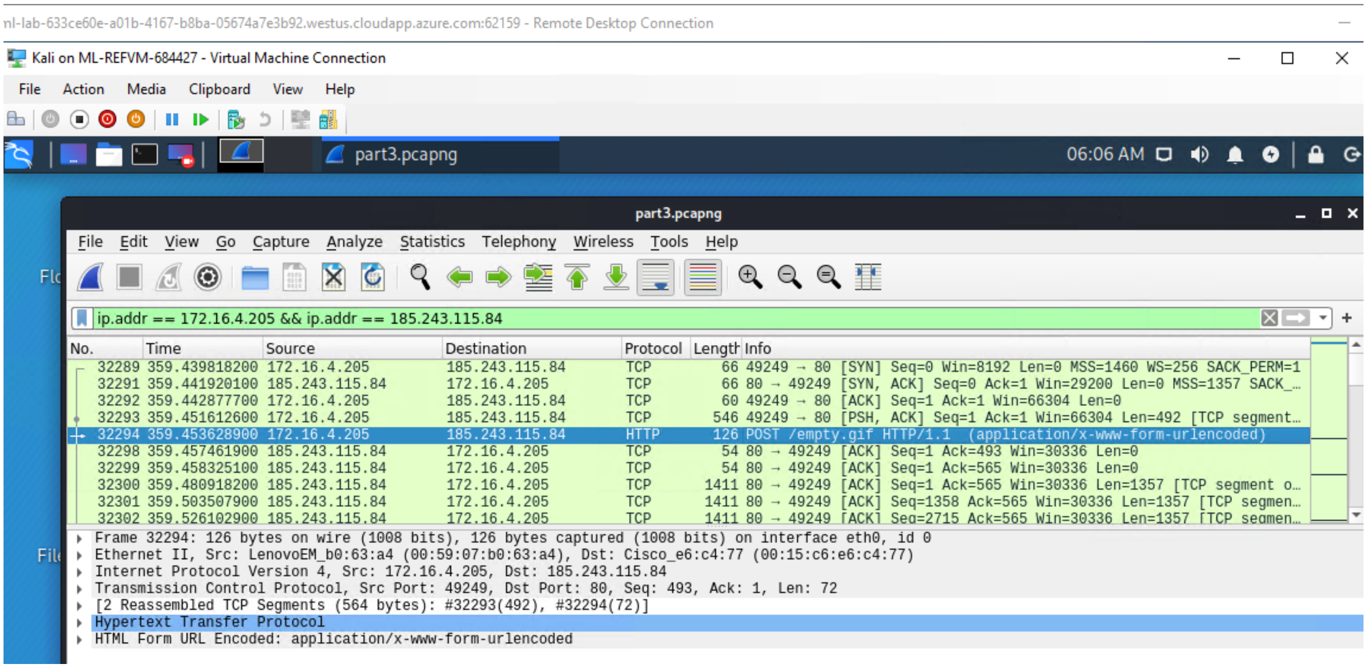
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.4.205	185.243.115.84	30,344	26M	15,149	9831k	15,195	16M	196.154314	1016.8611	77k	133k
166.62.111.64	172.16.4.205	15,728	16M	11,354	15M	4,374	321k	51.161259	1001.6762	126k	2568
10.0.0.201	23.43.62.169	6,934	7045k	2,282	124k	4,652	6920k	0.000000	900.2057	1109	61k
10.0.0.201	64.187.66.143	4,883	3637k	2,235	144k	2,648	3492k	47.425979	854.0467	1355	32k
5.101.51.151	10.6.12.203	4,326	4246k	3,262	4177k	1,064	68k	669.890730	67.9985	491k	8062
10.11.11.200	151.101.50.208	3,270	2220k	1,613	112k	1,657	2108k	571.917522	66.7937	13k	252k
172.16.4.4	172.16.4.205	1,417	339k	680	147k	737	191k	49.776799	1144.3125	1034	1336
10.6.12.12	10.6.12.203	1,388	350k	620	161k	768	188k	644.343994	99.1499	13k	15k
10.6.12.12	10.6.12.157	1,316	330k	608	156k	708	174k	641.057369	102.3674	12k	13k
10.11.11.11	10.11.11.200	1,100	219k	493	98k	607	120k	464.078707	176.9288	4459	5468
10.0.0.2	10.0.0.201	1,083	266k	520	133k	563	132k	743.519241	89.6854	11k	11k
10.11.11.200	104.18.74.113	1,079	697k	511	34k	568	662k	616.230265	22.4916	12k	235k
10.11.11.11	10.11.11.203	843	189k	351	83k	492	106k	468.330519	172.6836	3858	4938
10.11.11.179	13.33.255.25	728	520k	339	34k	389	485k	475.419836	94.0159	2950	41k
31.13.70.52	172.16.4.205	726	479k	436	447k	290	31k	62.702930	989.8205	3620	253
93.95.100.178	172.16.4.205	722	419k	418	391k	304	28k	116.562981	937.4512	3336	242
10.11.11.217	172.217.6.162	697	404k	341	35k	356	369k	530.894213	106.4835	2664	27k
10.6.12.203	205.185.125.104	647	599k	185	10k	462	588k	658.615057	79.8144	1050	59k
10.0.0.201	172.217.9.2	566	282k	271	31k	295	251k	752.919878	49.3013	5124	40k
10.0.0.201	96.7.89.194	487	166k	200	33k	287	133k	746.345408	4.4490	59k	239k
10.11.11.179	143.204.29.89	449	295k	217	22k	232	273k	475.414844	74.8401	2361	29k
10.11.11.11	10.11.11.179	440	43k	112	17k	328	26k	463.847371	84.0332	1620	2521
10.0.0.201	168.215.194.14	439	276k	187	17k	252	258k	752.320941	49.9051	2833	41k

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

4. Below are the screenshots related to getting the desktop background of the Windows host:

Wireshark Filter used: **ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84**

Using the source and destination address of the related computers, trying to filter and find the images/objects present in the network traffic capture for that specific filter. The images will be captured in the HTTP request.



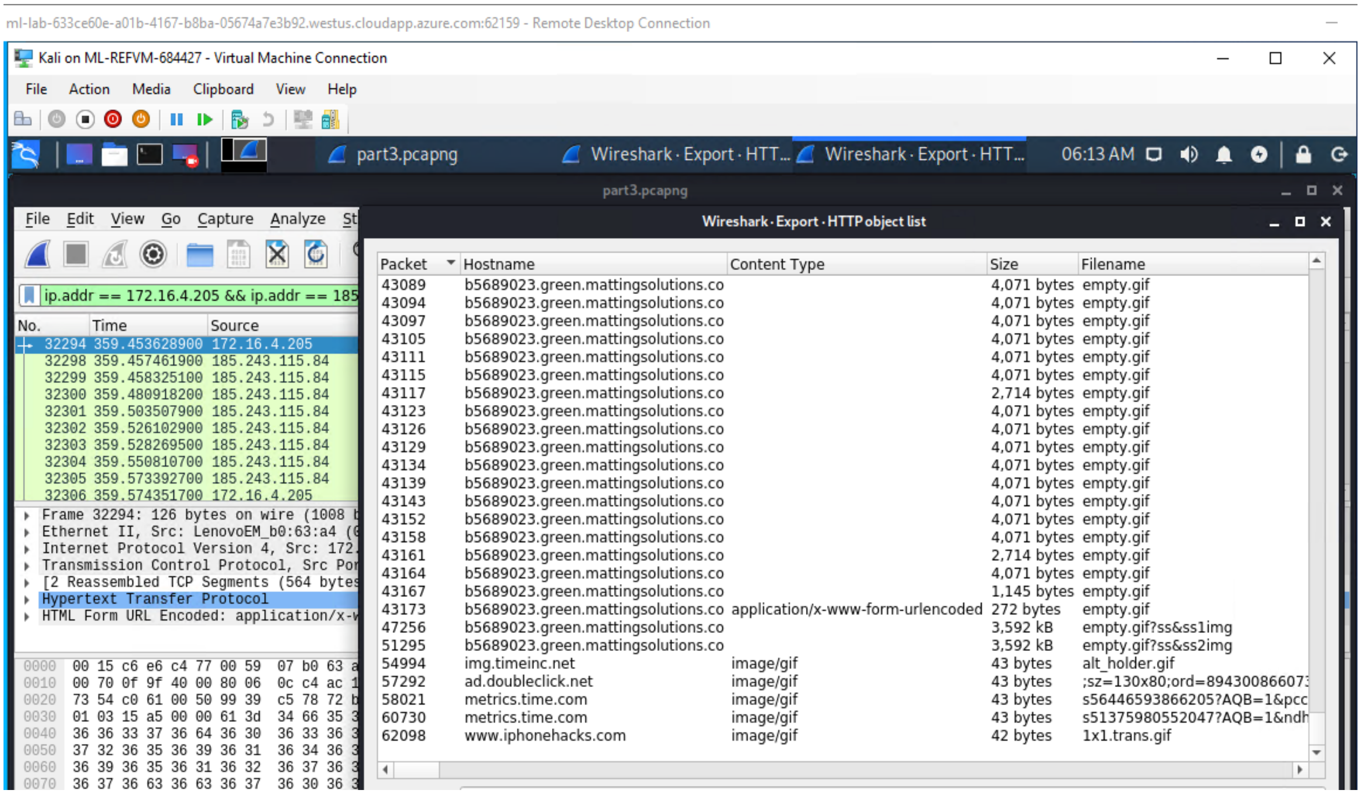
nl-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help
part3.pcapng
06:06 AM
part3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.   Time          Source         Destination    Protocol Length Info
32289 359.439818200 172.16.4.205   185.243.115.84 TCP        66 49249 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
32291 359.441920100 185.243.115.84 172.16.4.205   TCP        66 80 → 49249 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1357 SACK_…
32292 359.442877700 172.16.4.205   185.243.115.84 TCP        60 49249 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
32293 359.451612600 172.16.4.205   185.243.115.84 TCP       546 49249 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=492 [TCP segment…
32294 359.453628900 172.16.4.205   185.243.115.84 HTTP      126 POST /empty.gif HTTP/1.1  (application/x-www-form-urlencoded)
32298 359.457461900 185.243.115.84 172.16.4.205   TCP        54 80 → 49249 [ACK] Seq=1 Ack=493 Win=30336 Len=0
32299 359.458325100 185.243.115.84 172.16.4.205   TCP        54 80 → 49249 [ACK] Seq=1 Ack=565 Win=30336 Len=0
32300 359.480918200 185.243.115.84 172.16.4.205   TCP      1411 80 → 49249 [ACK] Seq=1 Ack=565 Win=30336 Len=1357 [TCP segment o…
32301 359.503507900 185.243.115.84 172.16.4.205   TCP      1411 80 → 49249 [ACK] Seq=1358 Ack=565 Win=30336 Len=1357 [TCP segmen…
32302 359.526102900 185.243.115.84 172.16.4.205   TCP      1411 80 → 49249 [ACK] Seq=2715 Ack=565 Win=30336 Len=1357 [TCP segmen…

▸ Frame 32294: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface eth0, id 0
▸ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
▸ Internet Protocol Version 4, Src: 172.16.4.205, Dst: 185.243.115.84
▸ Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 493, Ack: 1, Len: 72
▸ [2 Reassembled TCP Segments (564 bytes): #32293(492), #32294(72)]
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

Using the Import feature of wireshark, selecting the HTTP object, as that's where the image resides, the empty.gif image, which is the desktop image is downloaded.



ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection

Kali on ML-REFVM-684427 - Virtual Machine Connection

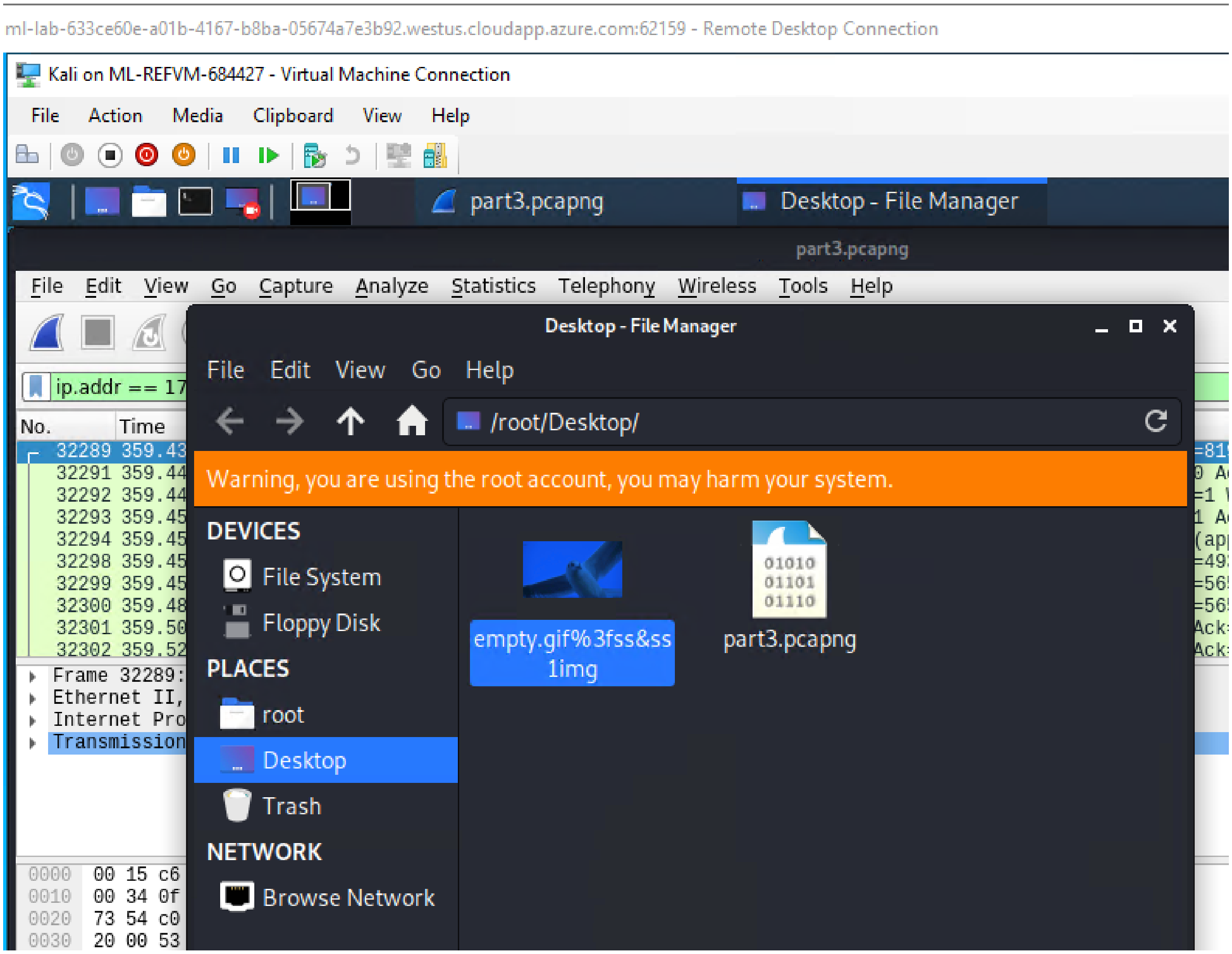
File Action Media Clipboard View Help
part3.pcapng
Wireshark · Export · HTT…
Wireshark · Export · HTT…
06:13 AM
part3.pcapng
File Edit View Go Capture Analyze St

```
ip.addr == 172.16.4.205 && ip.addr == 185

No.   Time          Source
32294 359.453628900 172.16.4.205
32298 359.457461900 185.243.115.84
32299 359.458325100 185.243.115.84
32300 359.480918200 185.243.115.84
32301 359.503507900 185.243.115.84
32302 359.526102900 185.243.115.84
32303 359.528269500 185.243.115.84
32304 359.550810700 185.243.115.84
32305 359.573392700 185.243.115.84
32306 359.574351700 172.16.4.205

▸ Frame 32294: 126 bytes on wire (1008 b
▸ Ethernet II, Src: LenovoEM_b0:63:a4 ((
▸ Internet Protocol Version 4, Src: 172.
▸ Transmission Control Protocol, Src Por
▸ [2 Reassembled TCP Segments (564 bytes
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-w

0000  00 15 c6 e6 c4 77 00 59  07 b0 63 a
0010  00 70 0f 9f 40 00 80 06  0c c4 ac 1
0020  73 54 c0 61 00 50 99 39  c5 78 72 b
0030  01 03 15 a5 00 00 61 3d  34 66 35 3
0040  36 36 33 37 36 64 36 30  36 33 36 3
0050  37 32 36 35 36 39 36 31  36 34 36 3
0060  36 39 36 35 36 31 36 32  36 37 36 3
0070  36 37 36 63 36 63 36 37  36 30 36 3
```

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
43089	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43094	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43097	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43105	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43111	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43115	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43117	b5689023.green.mattingsolutions.co		2,714 bytes	empty.gif
43123	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43126	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43129	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43134	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43139	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43143	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43152	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43158	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43161	b5689023.green.mattingsolutions.co		2,714 bytes	empty.gif
43164	b5689023.green.mattingsolutions.co		4,071 bytes	empty.gif
43167	b5689023.green.mattingsolutions.co		1,145 bytes	empty.gif
43173	b5689023.green.mattingsolutions.co	application/x-www-form-urlencoded	272 bytes	empty.gif
47256	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
51295	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2img
54994	img.timeinc.net	image/gif	43 bytes	alt_holder.gif
57292	ad.doubleclick.net	image/gif	43 bytes	;sz=130x80;ord=89430086607
58021	metrics.time.com	image/gif	43 bytes	s56446593866205?AQB=1&pcc
60730	metrics.time.com	image/gif	43 bytes	s51375980552047?AQB=1&ndh
62098	www.iphonehacks.com	image/gif	42 bytes	1x1.trans.gif

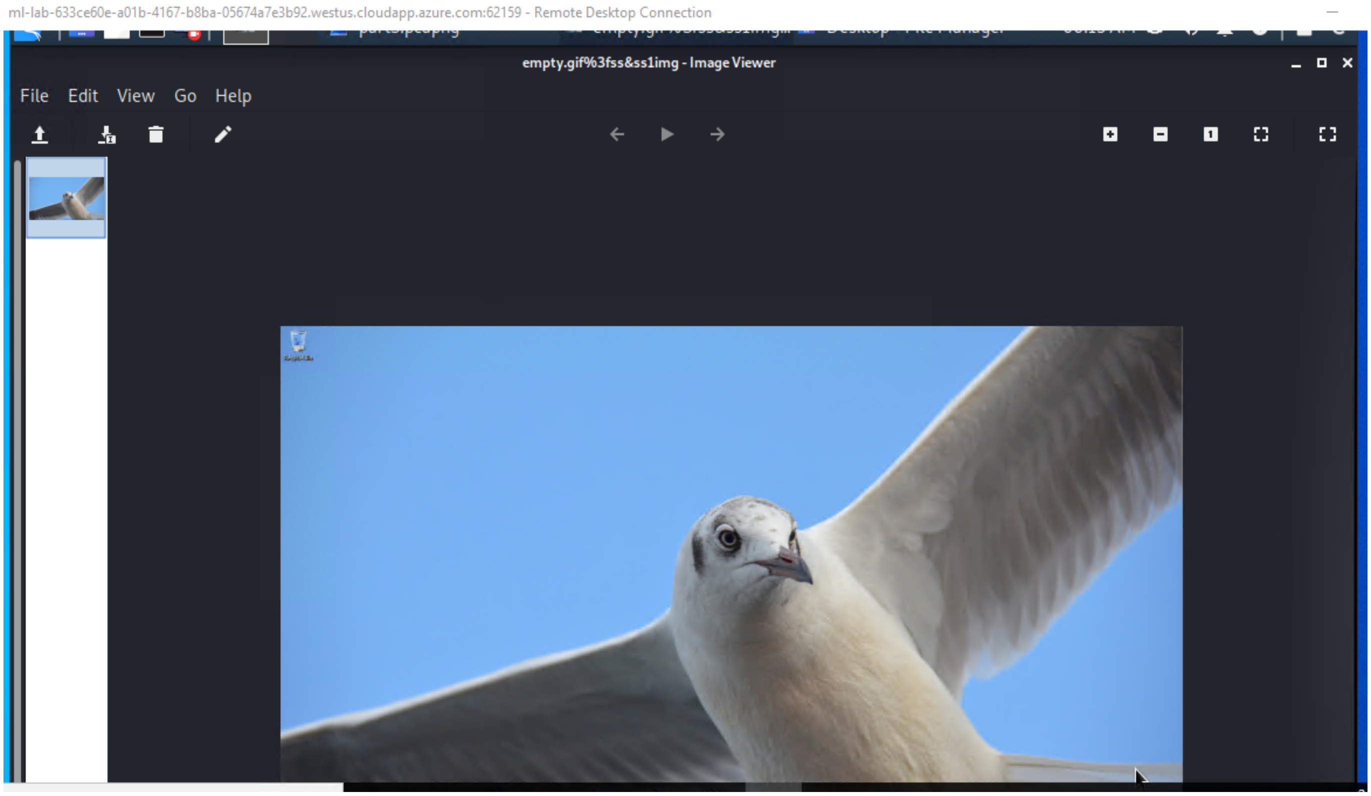
I have downloaded the image on the desktop.


ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
part3.pcapng
Desktop - File Manager
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 17
No. Time
Frame 32289:
Ethernet II,
Internet Pro
Transmission
File Edit View Go Help
/root/Desktop/
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Network
empty.gif%3fss&ss1img
part3.pcapng

Warning, you are using the root account, you may harm your system.

```
32289 359.43
32291 359.44
32292 359.44
32293 359.45
32294 359.45
32298 359.45
32299 359.45
32300 359.48
32301 359.50
32302 359.52
```

```
0000  00 15 c6
0010  00 34 0f
0020  73 54 c0
0030  20 00 53
```


ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection
empty.gif%3fss&ss1img - Image Viewer
File
Edit
View
Go
Help

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:

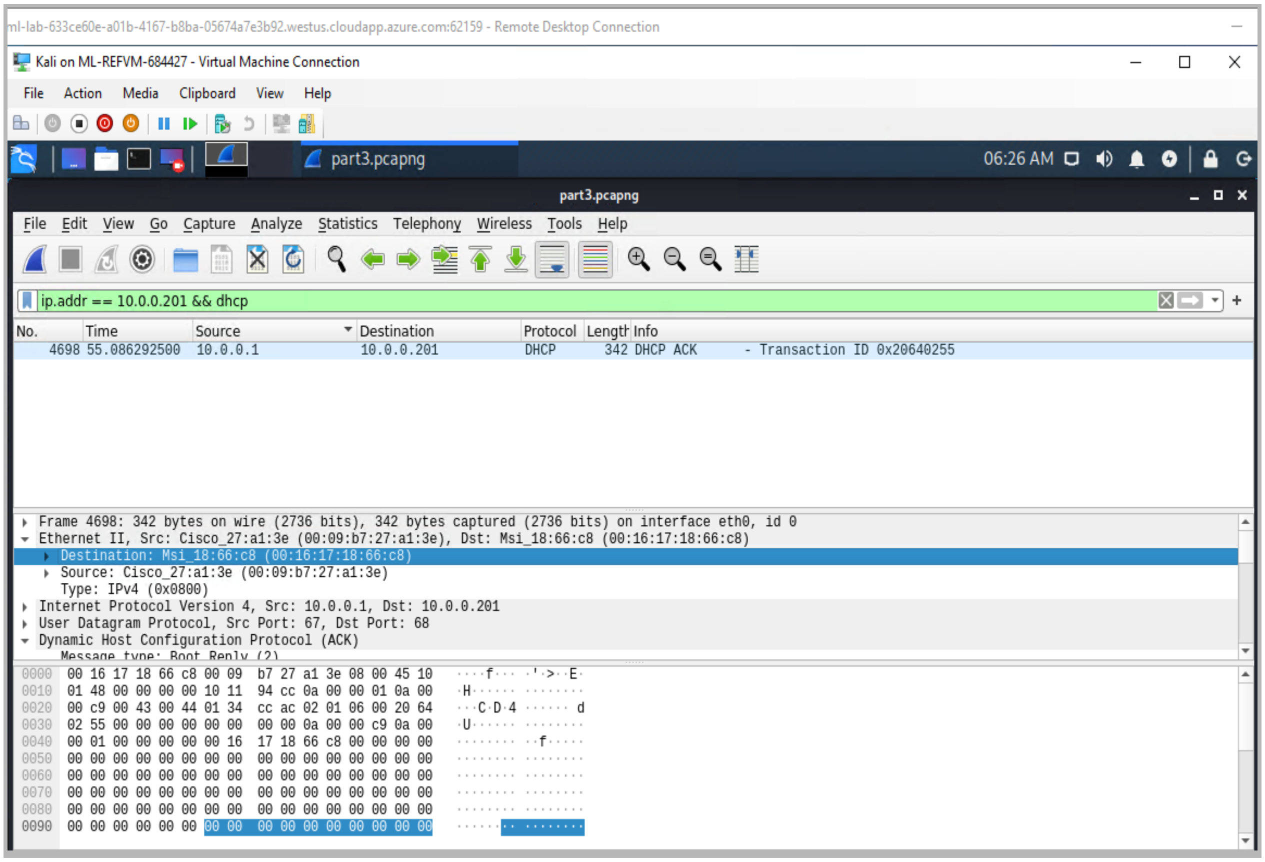
1. The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
2. The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
3. The DC is associated with the domain dogoftheyear.net.

After isolating the torrent traffic below are the observations:

1. The following information is found about the machine with IP address 10.0.0.201:
   a. MAC address: **00:16:17:18:66:c8**
   b. Windows username: **elmer.blanco**
   c. OS version: **BLANCO-DESKTOP** Windows NT 10.0

Wireshark Filter Used: **ip.src==10.0.0.201 and dhcp**

We know the IP address of the machine to be 10.0.0.201, to get the mac address, we use the above filter, dhcp configures the IP addresses and the filter helps find the machine details specifically.


ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
part3.pcapng
06:26 AM
part3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.0.0.201 && dhcp
```

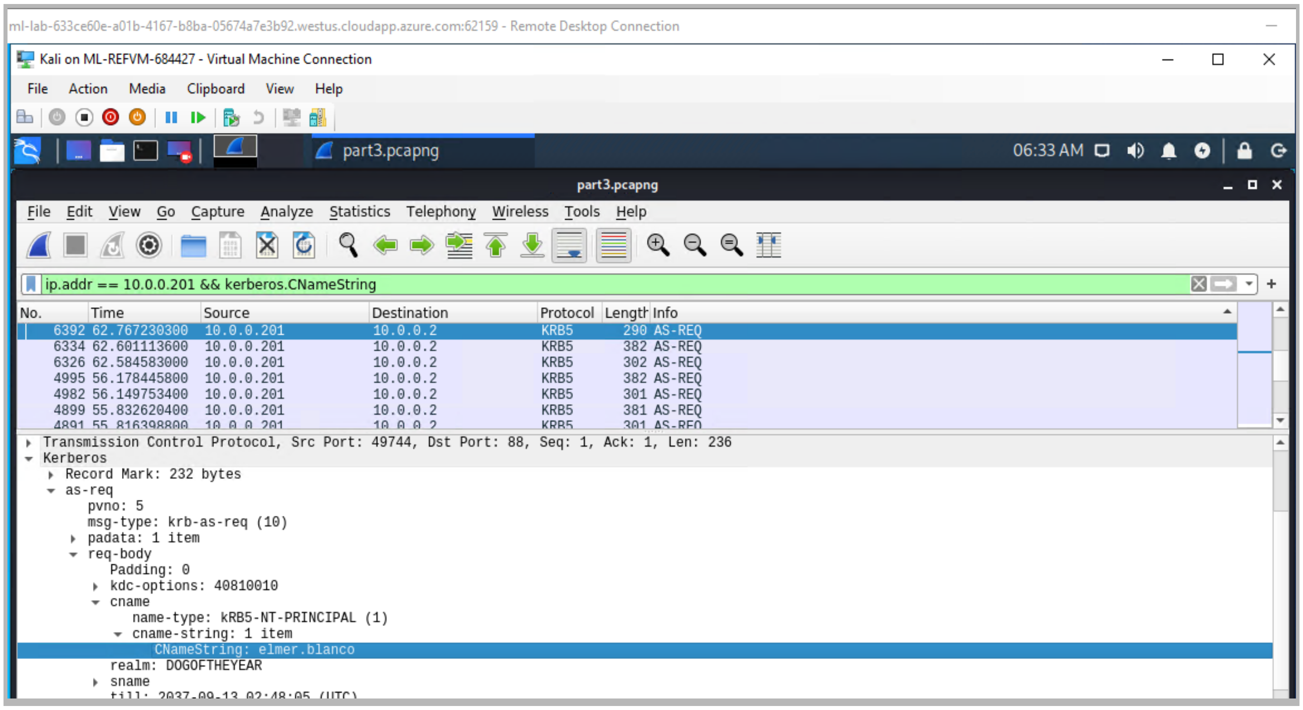
```
No.     Time          Source       Destination   Protocol Length Info
   4698 55.086292500  10.0.0.1     10.0.0.201    DHCP        342 DHCP ACK      - Transaction ID 0x20640255
```

```
▸ Frame 4698: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
▾ Ethernet II, Src: Cisco_27:a1:3e (00:09:b7:27:a1:3e), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)
   ▸ Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
   ▸ Source: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
     Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.201
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (ACK)
     Message type: Boot Reply (2)
```

```
0000  00 16 17 18 66 c8 00 09  b7 27 a1 3e 08 00 45 10   ····f··· ·'>··E·
0010  01 48 00 00 00 00 10 11  94 cc 0a 00 00 01 0a 00   ·H······ ········
0020  00 c9 00 43 00 44 01 34  cc ac 02 01 06 00 20 64   ···C·D·4 ······ d
0030  02 55 00 00 00 00 00 00  00 00 0a 00 00 c9 0a 00   ·U······ ········
0040  00 01 00 00 00 00 00 16  17 18 66 c8 00 00 00 00   ········ ··f·····
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   ········ ········
```

To find the username, the below is used:

Wireshark Filter used: **ip.addr == 10.0.0.201 and kerberos.CNameString**

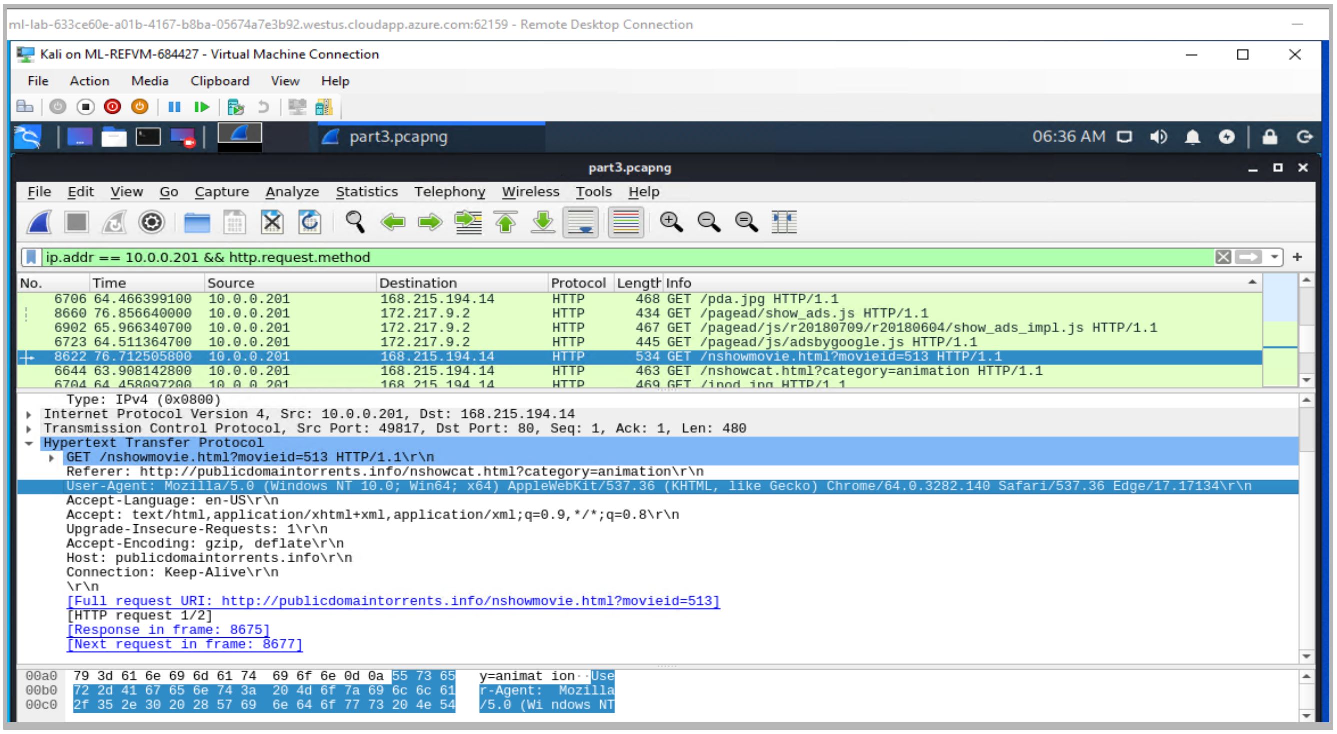

ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
part3.pcapng
06:33 AM
part3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.0.0.201 && kerberos.CNameString
```

```
No.   Time         Source      Destination  Protocol Length Info
 6392 62.767230300 10.0.0.201  10.0.0.2     KRB5       290 AS-REQ
 6334 62.601113600 10.0.0.201  10.0.0.2     KRB5       382 AS-REQ
 6326 62.584583000 10.0.0.201  10.0.0.2     KRB5       302 AS-REQ
 4995 56.178445800 10.0.0.201  10.0.0.2     KRB5       382 AS-REQ
 4982 56.149753400 10.0.0.201  10.0.0.2     KRB5       301 AS-REQ
 4899 55.832620400 10.0.0.201  10.0.0.2     KRB5       381 AS-REQ
 4891 55.816398800 10.0.0.201  10.0.0.2     KRB5       301 AS-REQ
```

```
▸ Transmission Control Protocol, Src Port: 49744, Dst Port: 88, Seq: 1, Ack: 1, Len: 236
▾ Kerberos
  ▸ Record Mark: 232 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 1 item
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▾ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ▾ cname-string: 1 item
            CNameString: elmer.blanco
        realm: DOGOFTHEYEAR
      ▸ sname
        till: 2037-09-13 02:48:05 (UTC)
```

To get the OS Type and Version, Wireshark Filter used: **ip.addr == 10.0.0.201 and http.request.method == GET**


ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
part3.pcapng
06:36 AM
part3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

```
No.   Time         Source      Destination     Protocol Length Info
 6706 64.466399100 10.0.0.201  168.215.194.14  HTTP       468 GET /pda.jpg HTTP/1.1
 8660 76.856640000 10.0.0.201  172.217.9.2     HTTP       434 GET /pagead/show_ads.js HTTP/1.1
 6902 65.966340700 10.0.0.201  172.217.9.2     HTTP       467 GET /pagead/js/r20180709/r20180604/show_ads_impl.js HTTP/1.1
 6723 64.511364700 10.0.0.201  172.217.9.2     HTTP       445 GET /pagead/js/adsbygoogle.js HTTP/1.1
 8622 76.712505800 10.0.0.201  168.215.194.14  HTTP       534 GET /nshowmovie.html?movieid=513 HTTP/1.1
 6644 63.908142800 10.0.0.201  168.215.194.14  HTTP       463 GET /nshowcat.html?category=animation HTTP/1.1
 6704 64.458097200 10.0.0.201  168.215.194.14  HTTP       469 GET /ipod.jpg HTTP/1.1
```

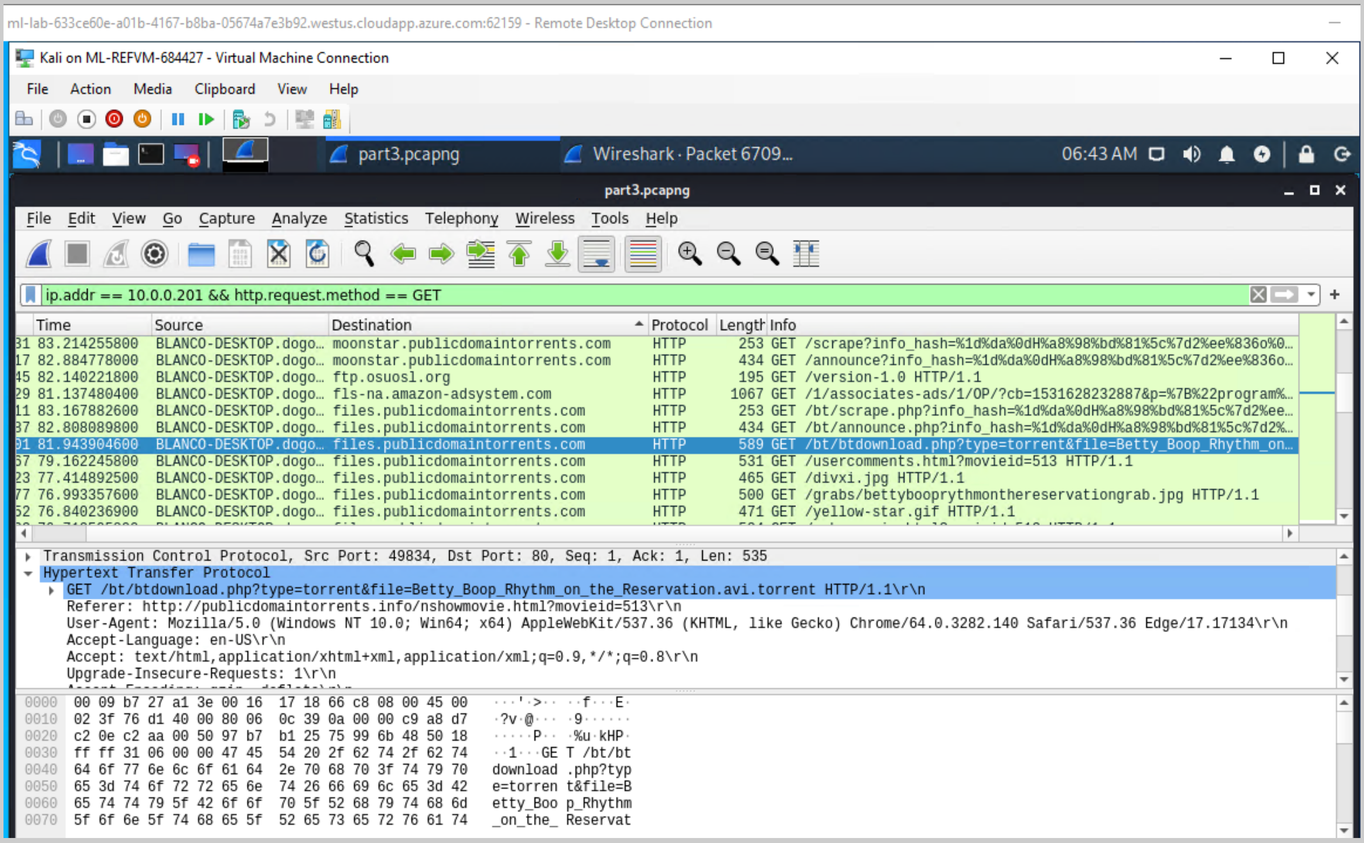
```
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14
▸ Transmission Control Protocol, Src Port: 49817, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
▾ Hypertext Transfer Protocol
  ▸ GET /nshowmovie.html?movieid=513 HTTP/1.1\r\n
    Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\r\n
    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-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: publicdomaintorrents.info\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://publicdomaintorrents.info/nshowmovie.html?movieid=513]
    [HTTP request 1/2]
    [Response in frame: 8675]
    [Next request in frame: 8677]
```

```
00a0  79 3d 61 6e 69 6d 61 74  69 6f 6e 0d 0a 55 73 65   y=animat ion··Use
00b0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00c0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
```

2. The torrent file the user downloaded was: **Betty_Boop_Rythm_on_the_Reservation.avi.torrent**.

Wireshark Filter used: **ip.addr==10.0.0.201 and http.request.method==GET**

There are quite a few downloads made, hence to find the specific torrent file - I looked specifically for download requests to find it.


ml-lab-633ce60e-a01b-4167-b8ba-05674a7e3b92.westus.cloudapp.azure.com:62159 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
part3.pcapng
Wireshark · Packet 6709...
06:43 AM
part3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

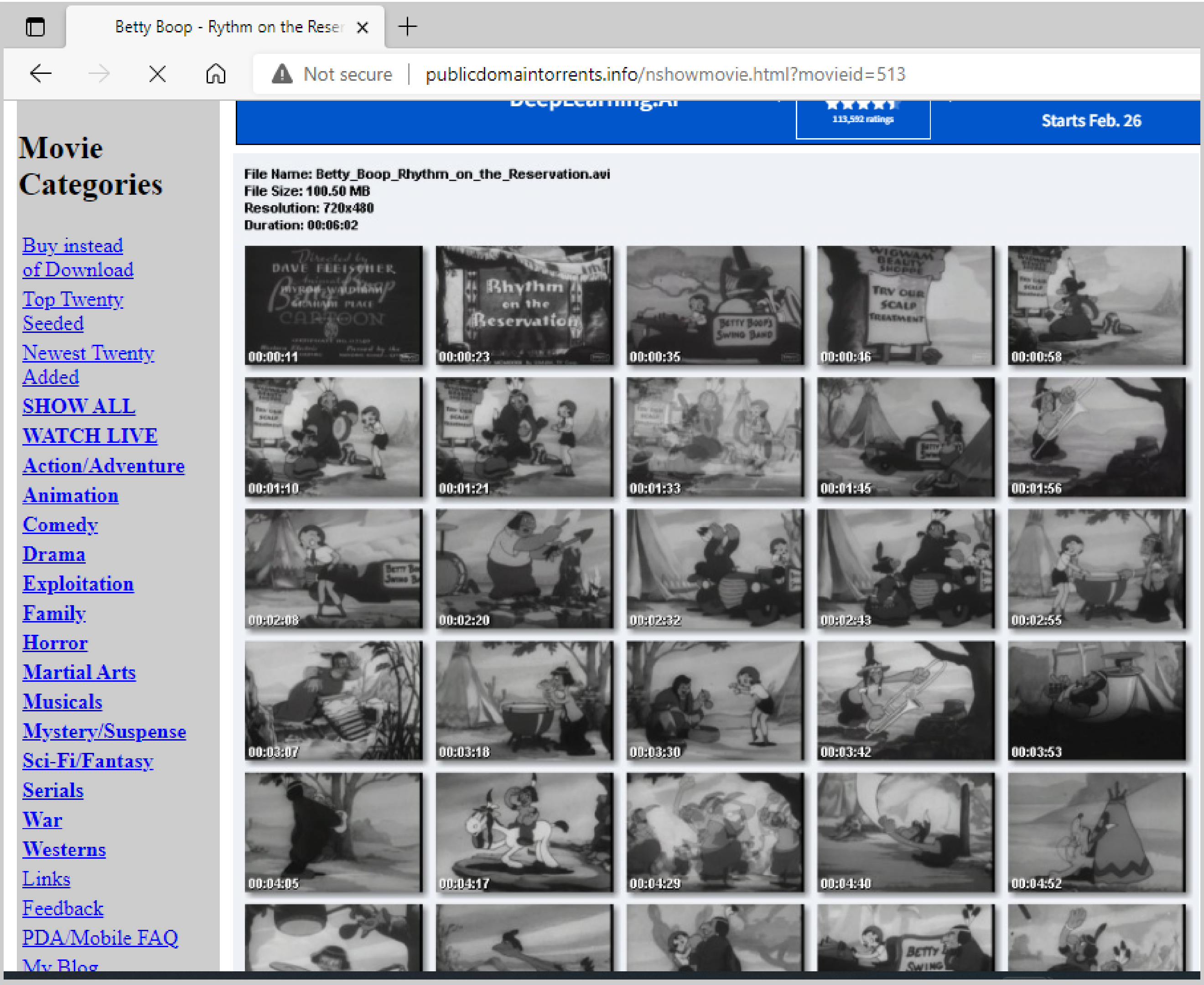
```
ip.addr == 10.0.0.201 && http.request.method == GET
```

```
   Time           Source               Destination                       Protocol Length Info
31 83.214255800   BLANCO-DESKTOP.dogo… moonstar.publicdomaintorrents.com HTTP      253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%0…
17 82.884778000   BLANCO-DESKTOP.dogo… moonstar.publicdomaintorrents.com HTTP      434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o…
45 82.140221800   BLANCO-DESKTOP.dogo… ftp.osuosl.org                    HTTP      195 GET /version-1.0 HTTP/1.1
29 81.137480400   BLANCO-DESKTOP.dogo… fls-na.amazon-adsystem.com        HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%…
11 83.167882600   BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com    HTTP      253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee…
37 82.808089800   BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com    HTTP      434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%…
91 81.943904600   BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com    HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on…
57 79.162245800   BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com    HTTP      531 GET /usercomments.html?movieid=513 HTTP/1.1
23 77.414892500   BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com    HTTP      465 GET /divxi.jpg HTTP/1.1
77 76.993357600   BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com    HTTP      500 GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
52 76.840236900   BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com    HTTP      471 GET /yellow-star.gif HTTP/1.1
```

```
▸ Transmission Control Protocol, Src Port: 49834, Dst Port: 80, Seq: 1, Ack: 1, Len: 535
▾ Hypertext Transfer Protocol
  ▸ GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

```
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
```

I retrieved the movie clip snapshot using the URL which I got from the above screenshot: http://publicdomaintorrents.info/nshowmovie.html?movieid=513



Movie Categories

Buy instead of Download
Top Twenty Seeded
Newest Twenty Added
SHOW ALL
WATCH LIVE
Action/Adventure
Animation
Comedy
Drama
Exploitation
Family
Horror
Martial Arts
Musicals
Mystery/Suspense
Sci-Fi/Fantasy
Serials
War
Westerns
Links
Feedback
PDA/Mobile FAQ
My Blog

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