Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Cameo Reindl, Phil Snell, Abdisalan Firin, Mary Yang, Georges Avenie, Omolabake Oladimeji, and Abdirahman Abdullahi

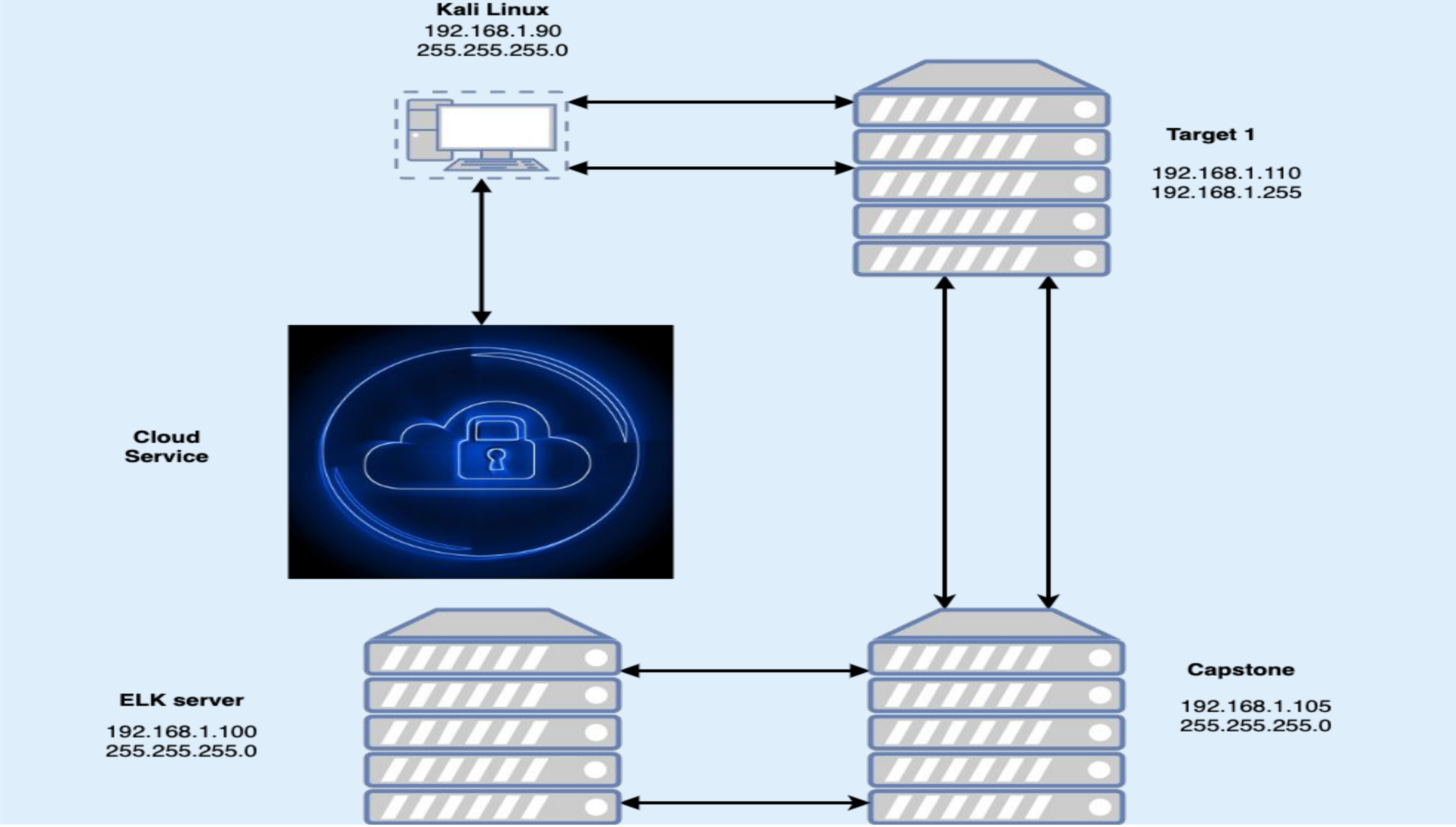
Table of Contents

This document contains the following resources:

- **Network Topology & Critical Vulnerabilities**
- **Traffic Profile**
- **Normal Activity**
- **Malicious Activity**

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 25.255.255.0
Gateway: 192.168.1.1
Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Apache Server
Hostname: Target-1

IPv4: 192.168.1.105
OS: Linux Server
Hostname: ELK Stack

IPv4: 192.168.1.100
OS: ELK
Hostname:Hyper-V
Azure Machine
ML-REFVM-6844247

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
CVE-2018-1000030 Python privilege escalation	It's a level of access and permissions needed to achieve the goal of accessing sensitive information	It takes advantage of vulnerability to provide the attacker with privileges
CVE-2021-28041 ssh remote login	It allows users to connect to different networks from their local machine	The connection between the client and the server is not encrypted and the attacker can easily recover packets and data in transfer also know as man in the middles
CVE-2019-15653 html password hash disclosure	Password disclosure via an insecure authentication mechanism	The password hash is viewable in plaintext and it is unsalted
CVE-2017-7760 exposed username and weak password	Michael's password was his name - there was no requirement or protocol in place to have a strong password	User access to the wp-config.php file via nano. This exposed MySQL password

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 166.62.111.64	Machines that sent the most traffic.
Most Common Protocols	TCP/IP HTTP UDP	Three most common protocols on the network.
# of Unique IP Addresses	2	Count of observed IP addresses.
Subnets	192.168.1.0/24	Observed subnet ranges.
# of Malware Species	1 malware File Name: JUNE11.dll Name: Trojan.Mint.Zamg.O	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity:

- Set up an Active Directory network.
- Users created their own web server on the corporate network
- Users watched videos on YouTube
- Used BitTorrent software to download movies

“Normal” Activity

- Watching YouTube, reading the news.
- Use BitTorrent to download work related files

Suspicious Activity

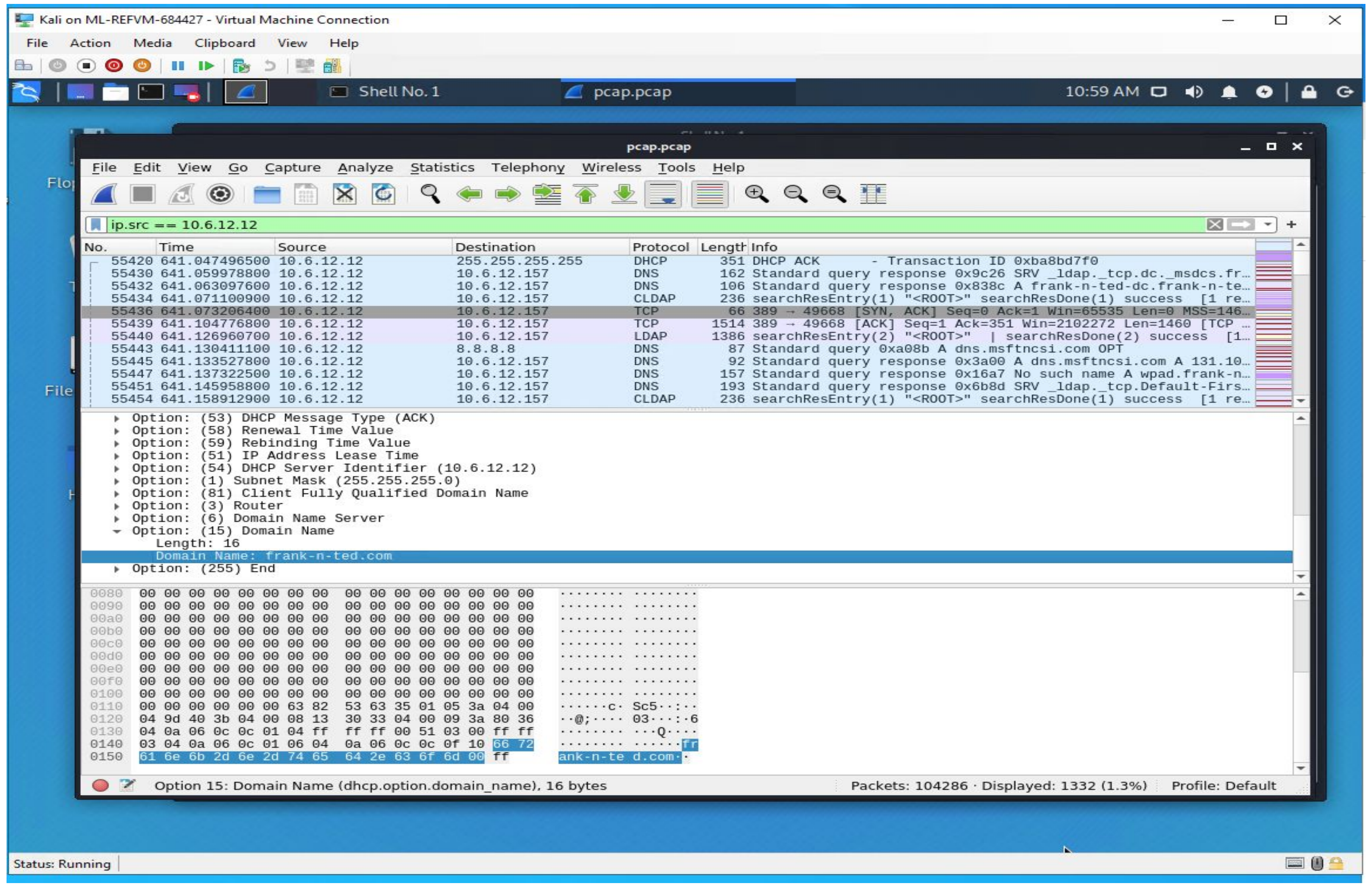
- Users created their own web server on the corporate network and set up Active Directory
    - New IP is in the range of 10.6.12.0/24 which is the same as the corporate
- Adware was downloaded as a result of their Youtube activity
- Use BitTorrent to download movies

Normal Activity

Watching YouTube, reading the news

Summarize the following:

- We observed a lot of traffic using DNS
- The user was watching YouTube videos


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
pcap.pcap
10:59 AM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Status: Running

```
ip.src == 10.6.12.12
```

```
No.   Time          Source      Destination      Protocol Length Info
55420 641.047496500 10.6.12.12  255.255.255.255  DHCP      351 DHCP ACK      - Transaction ID 0xba8bd7f0
55430 641.059978800 10.6.12.12  10.6.12.157      DNS       162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.fr…
55432 641.063097600 10.6.12.12  10.6.12.157      DNS       106 Standard query response 0x838c A frank-n-ted-dc.frank-n-te…
55434 641.071100900 10.6.12.12  10.6.12.157      CLDAP     236 searchResEntry(1) "<ROOT>" searchResDone(1) success  [1 re…
55436 641.073206400 10.6.12.12  10.6.12.157      TCP        66 389 → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=146…
55439 641.104776800 10.6.12.12  10.6.12.157      TCP      1514 389 → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP …
55440 641.126960700 10.6.12.12  10.6.12.157      LDAP     1386 searchResEntry(2) "<ROOT>"  | searchResDone(2) success  [1…
55443 641.130411100 10.6.12.12  8.8.8.8          DNS        87 Standard query 0xa08b A dns.msftncsi.com OPT
55445 641.133527800 10.6.12.12  10.6.12.157      DNS        92 Standard query response 0x3a00 A dns.msftncsi.com A 131.10…
55447 641.137322500 10.6.12.12  10.6.12.157      DNS       157 Standard query response 0x16a7 No such name A wpad.frank-n…
55451 641.145958800 10.6.12.12  10.6.12.157      DNS       193 Standard query response 0x6b8d SRV _ldap._tcp.Default-Firs…
55454 641.158912900 10.6.12.12  10.6.12.157      CLDAP     236 searchResEntry(1) "<ROOT>" searchResDone(1) success  [1 re…
```

```
  ▸ 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
        Length: 16
        Domain Name: frank-n-ted.com
  ▸ Option: (255) End
```

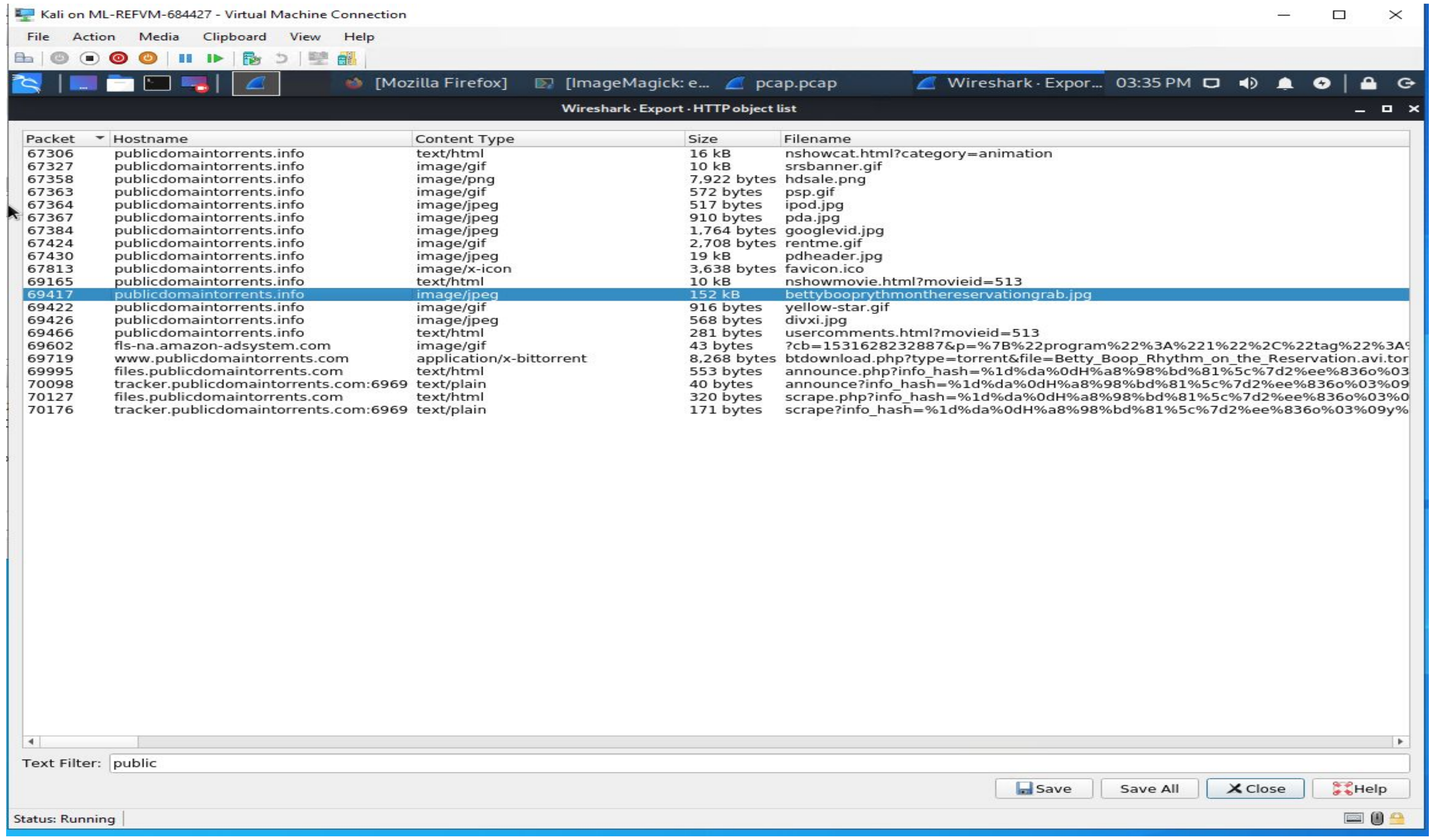
```
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
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··
```

Option 15: Domain Name (dhcp.option.domain_name), 16 bytes · Packets: 104286 · Displayed: 1332 (1.3%) · Profile: Default

BitTorrent used to download work related files:

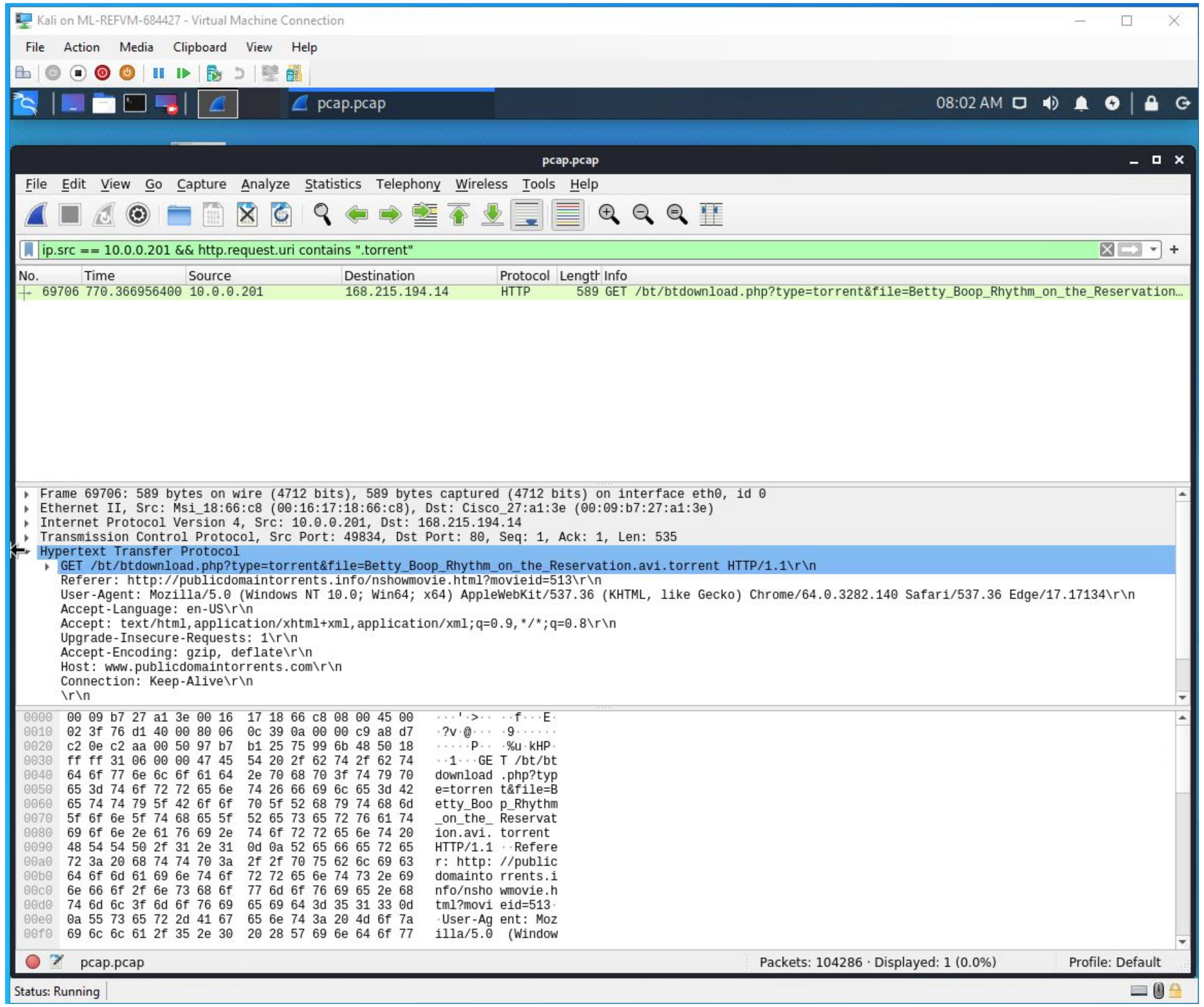
Summarize the following:

- We observed HTTP traffic
- Users were downloading work related files using BitTorrent



Packet	Hostname	Content Type	Size	Filename
67306	publicdomaintorrents.info	text/html	16 kB	nshowcat.html?category=animation
67327	publicdomaintorrents.info	image/gif	10 kB	srsbanner.gif
67358	publicdomaintorrents.info	image/png	7,922 bytes	hdsale.png
67363	publicdomaintorrents.info	image/gif	572 bytes	psp.gif
67364	publicdomaintorrents.info	image/jpeg	517 bytes	ipod.jpg
67367	publicdomaintorrents.info	image/jpeg	910 bytes	pda.jpg
67384	publicdomaintorrents.info	image/jpeg	1,764 bytes	googlevid.jpg
67424	publicdomaintorrents.info	image/gif	2,708 bytes	rentme.gif
67430	publicdomaintorrents.info	image/jpeg	19 kB	pdheader.jpg
67813	publicdomaintorrents.info	image/x-icon	3,638 bytes	favicon.ico
69165	publicdomaintorrents.info	text/html	10 kB	nshowmovie.html?movieid=513
69417	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationgrab.jpg
69422	publicdomaintorrents.info	image/gif	916 bytes	yellow-star.gif
69426	publicdomaintorrents.info	image/jpeg	568 bytes	divxi.jpg
69466	publicdomaintorrents.info	text/html	281 bytes	usercomments.html?movieid=513
69602	fls-na.amazon-adsystem.com	image/gif	43 bytes	?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag%22%3A%
69719	www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.tor
69995	files.publicdomaintorrents.com	text/html	553 bytes	announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03
70098	tracker.publicdomaintorrents.com:6969	text/plain	40 bytes	announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09
70127	files.publicdomaintorrents.com	text/html	320 bytes	scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%0
70176	tracker.publicdomaintorrents.com:6969	text/plain	171 bytes	scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%

Text Filter: public



ip.src == 10.0.0.201 && http.request.uri contains ".torrent"

```
No.    Time          Source       Destination     Protocol Length Info
 69706 770.366956400 10.0.0.201   168.215.194.14  HTTP       589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation…
```

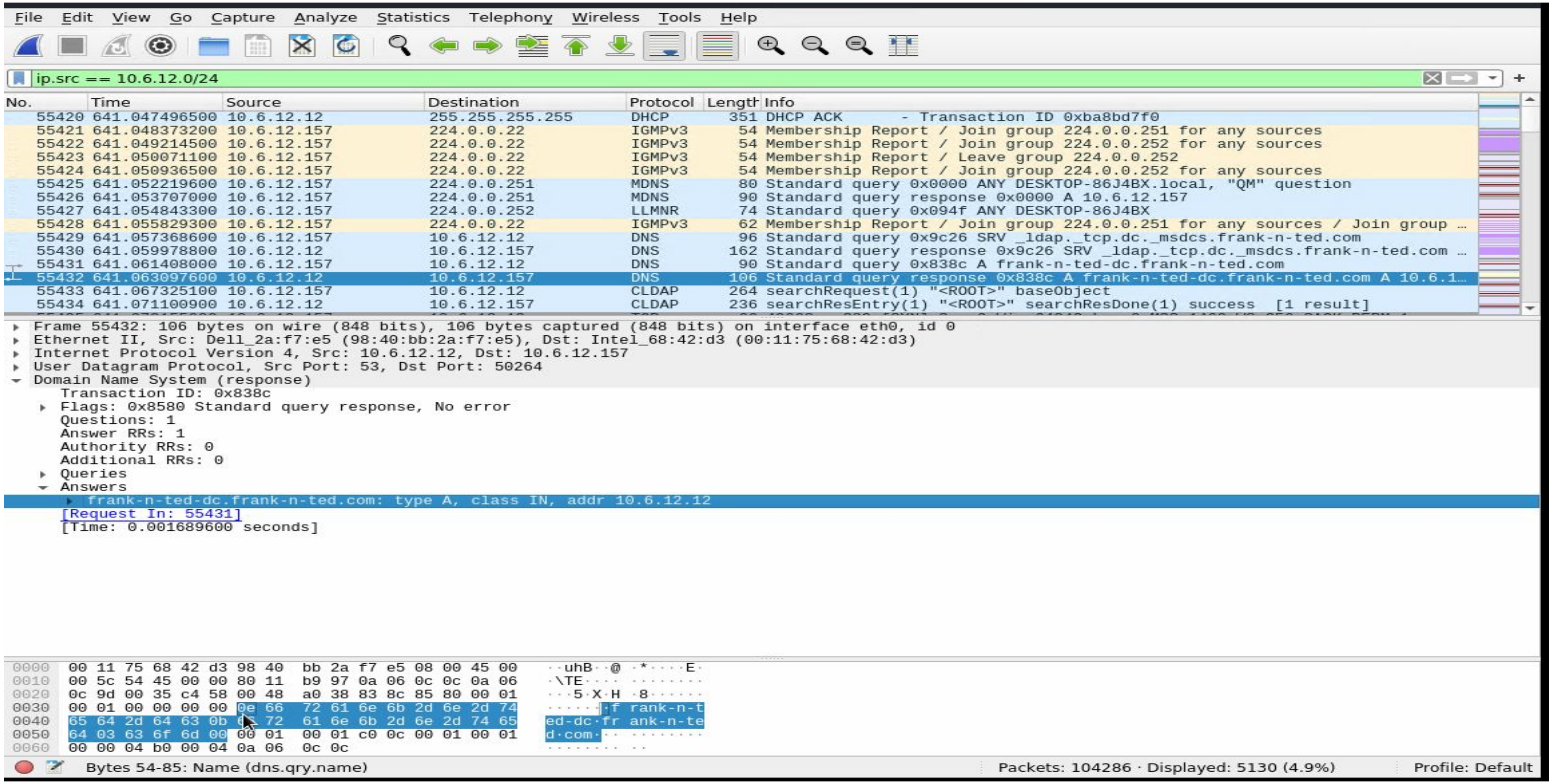
```
Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14
Transmission Control Protocol, Src Port: 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
  Accept-Encoding: gzip, deflate\r\n
  Host: www.publicdomaintorrents.com\r\n
  Connection: Keep-Alive\r\n
  \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
0080  69 6f 6e 2e 61 76 69 2e  74 6f 72 72 65 6e 74 20   ion.avi. torrent 
0090  48 54 54 50 2f 31 2e 31  0d 0a 52 65 66 65 72 65   HTTP/1.1 ··Refere
00a0  72 3a 20 68 74 74 70 3a  2f 2f 70 75 62 6c 69 63   r: http: //public
00b0  64 6f 6d 61 69 6e 74 6f  72 72 65 6e 74 73 2e 69   domainto rrents.i
00c0  6e 66 6f 2f 6e 73 68 6f  77 6d 6f 76 69 65 2e 68   nfo/nsho wmovie.h
00d0  74 6d 6c 3f 6d 6f 76 69  65 69 64 3d 35 31 33 0d   tml?movi eid=513·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00f0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
```

Malicious Activity

Users created their own web server on the corporate network and set up Active Directory

- Observed the DNS protocol
- It appears that the user has created a domain called frank-n-ted-dc.frank-n-ted.com
- IP address of the DC of the AD network is 10.6.12.12



```
ip.src == 10.6.12.0/24
```

```
No.     Time           Source        Destination      Protocol Length Info
  55420 641.047496500 10.6.12.12    255.255.255.255  DHCP      351 DHCP ACK      - Transaction ID 0xba8bd7f0
  55421 641.048373200 10.6.12.157   224.0.0.22       IGMPv3     54 Membership Report / Join group 224.0.0.251 for any sources
  55422 641.049214500 10.6.12.157   224.0.0.22       IGMPv3     54 Membership Report / Join group 224.0.0.252 for any sources
  55423 641.050071100 10.6.12.157   224.0.0.22       IGMPv3     54 Membership Report / Leave group 224.0.0.252
  55424 641.050936500 10.6.12.157   224.0.0.22       IGMPv3     54 Membership Report / Join group 224.0.0.252 for any sources
  55425 641.052219600 10.6.12.157   224.0.0.251      MDNS       80 Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
  55426 641.053707000 10.6.12.157   224.0.0.251      MDNS       90 Standard query response 0x0000 A 10.6.12.157
  55427 641.054843300 10.6.12.157   224.0.0.252      LLMNR      74 Standard query 0x094f ANY DESKTOP-86J4BX
  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
  55434 641.071100900 10.6.12.12    10.6.12.157      CLDAP     236 searchResEntry(1) "<ROOT>" searchResDone(1) success  [1 result]
```

```
▸ Frame 55432: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface eth0, id 0
▸ Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel_68:42:d3 (00:11:75:68:42:d3)
▸ Internet Protocol Version 4, Src: 10.6.12.12, Dst: 10.6.12.157
▸ User Datagram Protocol, Src Port: 53, Dst Port: 50264
▾ Domain Name System (response)
    Transaction ID: 0x838c
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▸ frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12
    [Request In: 55431]
    [Time: 0.001689600 seconds]
```

```
0000  00 11 75 68 42 d3 98 40  bb 2a f7 e5 08 00 45 00   ··uhB··@ ·*····E·
0010  00 5c 54 45 00 00 80 11  b9 97 0a 06 0c 0c 0a 06   ·\TE···· ········
0020  0c 9d 00 35 c4 58 00 48  a0 38 83 8c 85 80 00 01   ···5·X·H ·8······
0030  00 01 00 00 00 00 0e 66  72 61 6e 6b 2d 6e 2d 74   ·······f rank-n-t
0040  65 64 2d 64 63 0b 06 72  61 6e 6b 2d 6e 2d 74 65   ed-dc·fr ank-n-te
0050  64 03 63 6f 6d 00 00 01  00 01 c0 0c 00 01 00 01   d·com··· ········
0060  00 00 04 b0 00 04 0a 06  0c 0c                     ········ ··
```

Bytes 54-85: Name (dns.qry.name)

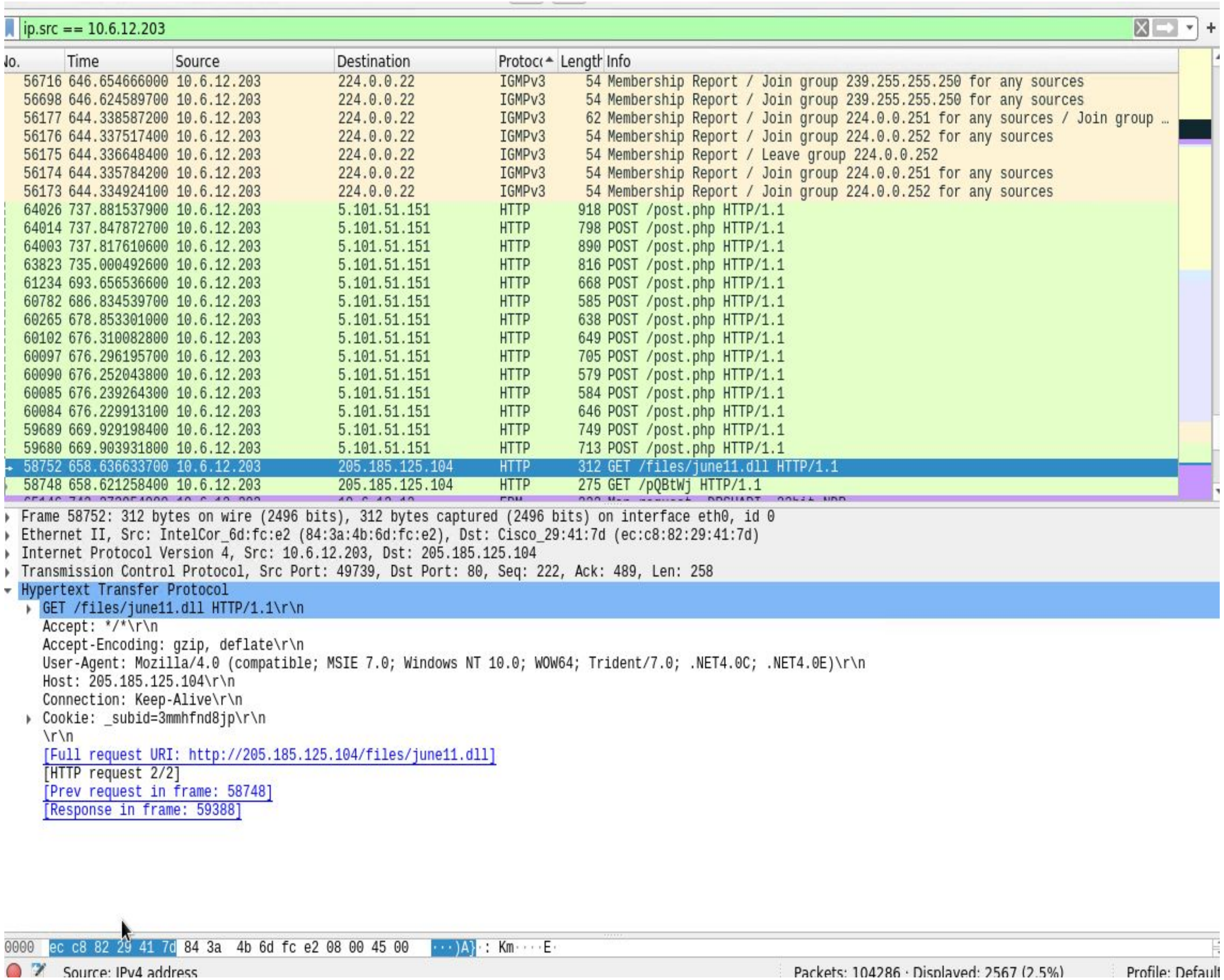
Packets: 104286 · Displayed: 5130 (4.9%)

Profile: Default

Adware was downloaded as a result of Users’ Browsing activity

Summarize the following:

- Observed the HTTP traffic
- The user was likely browsing various sites and as a result of that clicked on a malicious adware that downloaded a malicious script onto their computer.
- Found a suspicious file called june11.dll



```
ip.src == 10.6.12.203
```

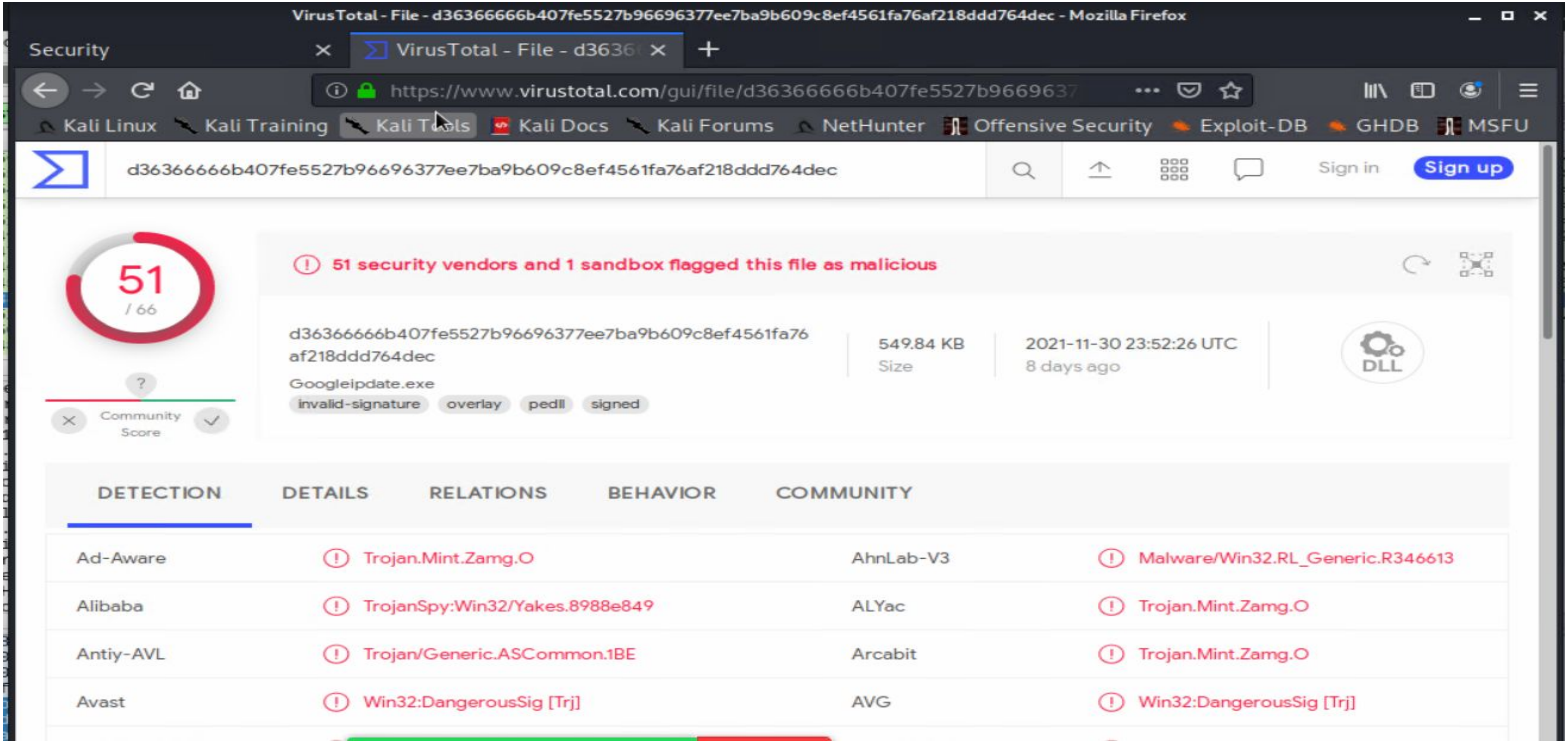
```
No.   Time          Source        Destination     Protocol Length Info
56716 646.654666000 10.6.12.203   224.0.0.22      IGMPv3     54 Membership Report / Join group 239.255.255.250 for any sources
56698 646.624589700 10.6.12.203   224.0.0.22      IGMPv3     54 Membership Report / Join group 239.255.255.250 for any sources
56177 644.338587200 10.6.12.203   224.0.0.22      IGMPv3     62 Membership Report / Join group 224.0.0.251 for any sources / Join group …
56176 644.337517400 10.6.12.203   224.0.0.22      IGMPv3     54 Membership Report / Join group 224.0.0.252 for any sources
56175 644.336648400 10.6.12.203   224.0.0.22      IGMPv3     54 Membership Report / Leave group 224.0.0.252
56174 644.335784200 10.6.12.203   224.0.0.22      IGMPv3     54 Membership Report / Join group 224.0.0.251 for any sources
56173 644.334924100 10.6.12.203   224.0.0.22      IGMPv3     54 Membership Report / Join group 224.0.0.252 for any sources
64026 737.881537900 10.6.12.203   5.101.51.151    HTTP      918 POST /post.php HTTP/1.1
64014 737.847872700 10.6.12.203   5.101.51.151    HTTP      798 POST /post.php HTTP/1.1
64003 737.817610600 10.6.12.203   5.101.51.151    HTTP      890 POST /post.php HTTP/1.1
63823 735.000492600 10.6.12.203   5.101.51.151    HTTP      816 POST /post.php HTTP/1.1
61234 693.656536600 10.6.12.203   5.101.51.151    HTTP      668 POST /post.php HTTP/1.1
60782 686.834539700 10.6.12.203   5.101.51.151    HTTP      585 POST /post.php HTTP/1.1
60265 678.853301000 10.6.12.203   5.101.51.151    HTTP      638 POST /post.php HTTP/1.1
60102 676.310082800 10.6.12.203   5.101.51.151    HTTP      649 POST /post.php HTTP/1.1
60097 676.296195700 10.6.12.203   5.101.51.151    HTTP      705 POST /post.php HTTP/1.1
60090 676.252043800 10.6.12.203   5.101.51.151    HTTP      579 POST /post.php HTTP/1.1
60085 676.239264300 10.6.12.203   5.101.51.151    HTTP      584 POST /post.php HTTP/1.1
60084 676.229913100 10.6.12.203   5.101.51.151    HTTP      646 POST /post.php HTTP/1.1
59689 669.929198400 10.6.12.203   5.101.51.151    HTTP      749 POST /post.php HTTP/1.1
59680 669.903931800 10.6.12.203   5.101.51.151    HTTP      713 POST /post.php HTTP/1.1
58752 658.636633700 10.6.12.203   205.185.125.104 HTTP      312 GET /files/june11.dll HTTP/1.1
58748 658.621258400 10.6.12.203   205.185.125.104 HTTP      275 GET /pQBtWj HTTP/1.1
```

```
Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
Internet Protocol Version 4, Src: 10.6.12.203, Dst: 205.185.125.104
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
Hypertext Transfer Protocol
  GET /files/june11.dll HTTP/1.1\r\n
  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
  \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]
```

```
0000  ec c8 82 29 41 7d 84 3a  4b 6d fc e2 08 00 45 00   ···)A}·: Km····E·
```

```
Source: IPv4 address                Packets: 104286 · Displayed: 2567 (2.5%)     Profile: Default
```

Proof of malicious file



VirusTotal - File - d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec - Mozilla Firefox
Security
VirusTotal - File - d3636
https://www.virustotal.com/gui/file/d36366666b407fe5527b9669637
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Sign in
Sign up

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

51 / 66

51 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed

549.84 KB
Size

2021-11-30 23:52:26 UTC
8 days ago

DLL

? Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.8988e849	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]

BitTorrent:

- BitTorrent, when downloading videos from the internet, will take bits and pieces from others who already have the video on their own computer. This makes the download process faster. The more people who have downloaded the video, the quicker the download.
- The users downloaded a movie through BitTorrent on HTTP.
  - Using BitTorrent for work purposes is allowed.
  - The movie downloaded was strictly against the company's copyright infringement policy and therefore illegal.

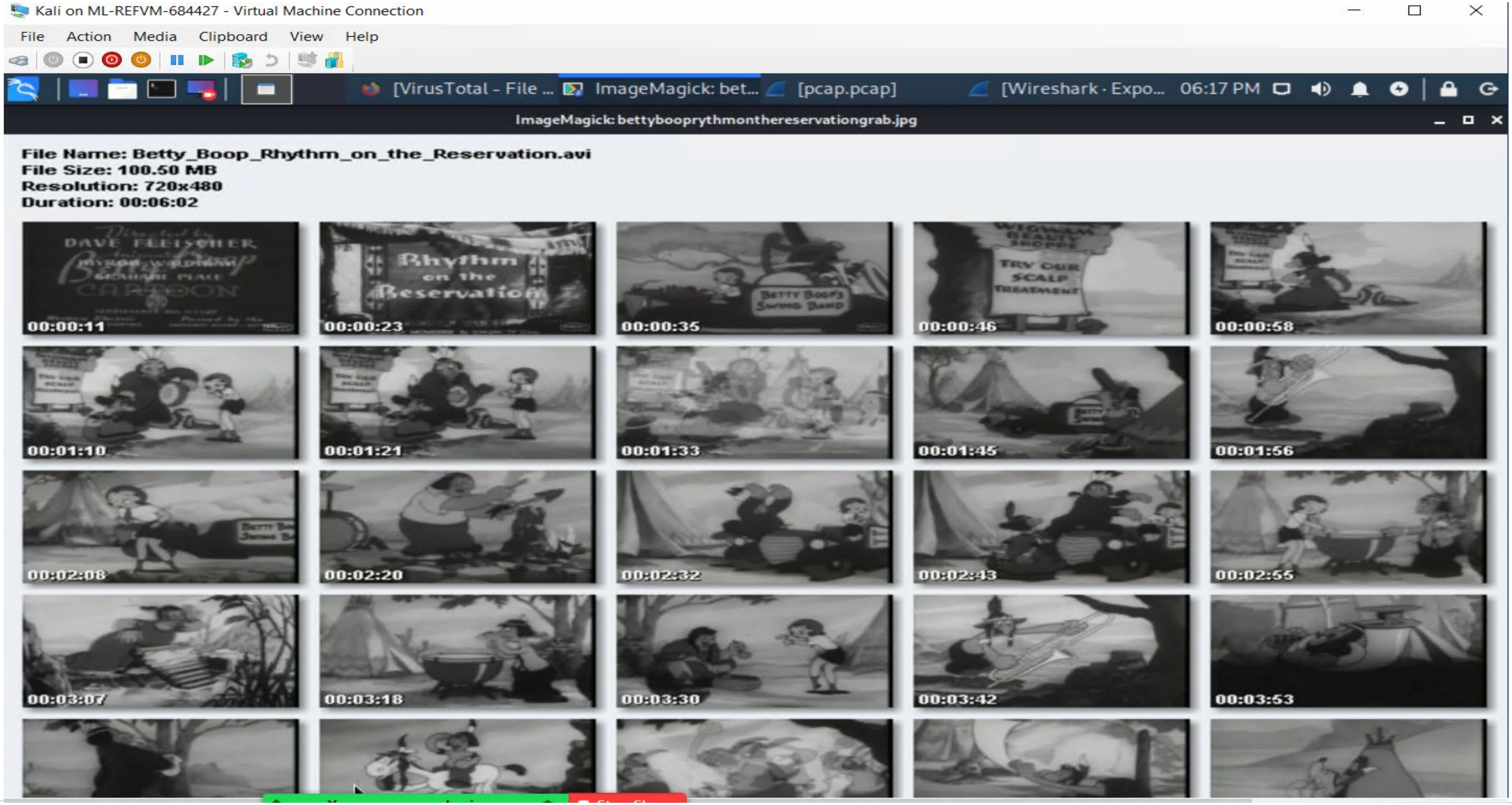
Betty Boop:

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

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

```
No.    Time          Source               Destination            Protocol Length Info
69706  770.366956400 BLANCO-DESKTOP.dogo… files.publicdomaint…   HTTP        589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the…
```

```
▸ Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
▸ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
▸ 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
    ▸ [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      Request Method: GET
    ▸ Request URI: /bt/btdownload.php?type=torrent&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/17.171
    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: www.publicdomaintorrents.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
```



ImageMagick: bettybooprythmonthereservationgrab.jpg

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

That’s all folks!

That’s all folks!

That’s all folks!

A little something special for all of you!

Next Slide.

© Trilogy Education Services, Inc.