Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

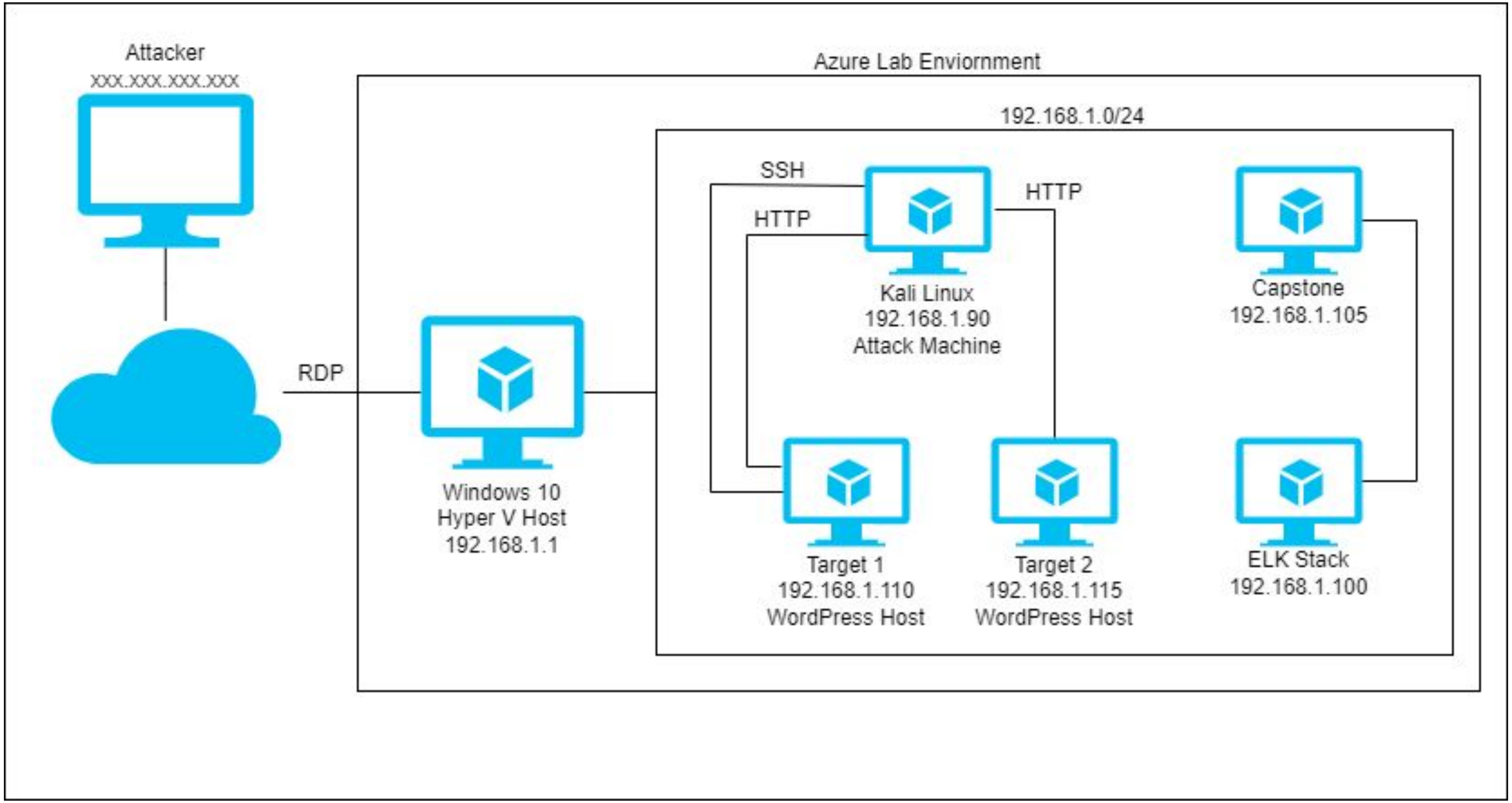
Traffic Profile

Normal Activity

Malicious Activity

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Debian Kali 5.4.0
Hostname: Kali

IPv4: 192.168.1.110
OS: Debian GNU/Linux 8
Hostname: Target 1

IPv4: 192.168.1.115
OS: Debian GNU/ Linux 8
Hostname: Target 2

IPv4: 192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
WordPress Core Username Enumeration CVE-2017-5487	WPScan will attempt to enumerate all users on a given WordPress installation. If successful it will output usernames back to the attacker.	Passwords can be easily bypassed manually and with commands like John the Ripper meaning users are not secure
CVE-2017-7494 SambaCry	Samba version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.	After exploitation Remote Code Execution can be performed by the attacker.
Open Port 80 Apache httpd 2.4.10 (Debian)	An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges.	The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service.

Critical Vulnerabilities: Target 1 Cont.

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

Vulnerability	Description	Impact
Weak User Passwords	Easily guessed/Brute Forced passwords.	Passwords can be easily bypassed manually and with commands like John the Ripper meaning users are not secure
Python 2.7.9 Privilege Escalation	Python sudo privileges for user allow for privilege escalation if user is compromised.	Compromised account can be used by attacker to gain root access.
WordPress xml rpc pingback CVE-2013-0235	The pingback feature of XML-RPC API allows attacks like DDOS and Server-Side Request Forgery (SSRF) either against the server hosting WordPress or against a target server	On a successful exploit, an attacker can control a WordPress site to conduct DDOS or Server-Side Request Forgery

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 (17M Bytes) ● 172.16.4.205 (15M Bytes) ● 166.62.111.64 (11M Bytes)	Machines that sent the most traffic.
Most Common Protocols	● TCP (85.9%) ○ TLS (8.2%) ○ HTTP (3.9%) ● UDP (14%)	Four most common protocols on the network
# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	● 10.6.12.0/24 ● 172.16.4.0/24 ● 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	Trojan (june11.dll)	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.

“Normal” Activity

- Browsing social media websites
- Browsing news sites
- Visiting healthcare websites

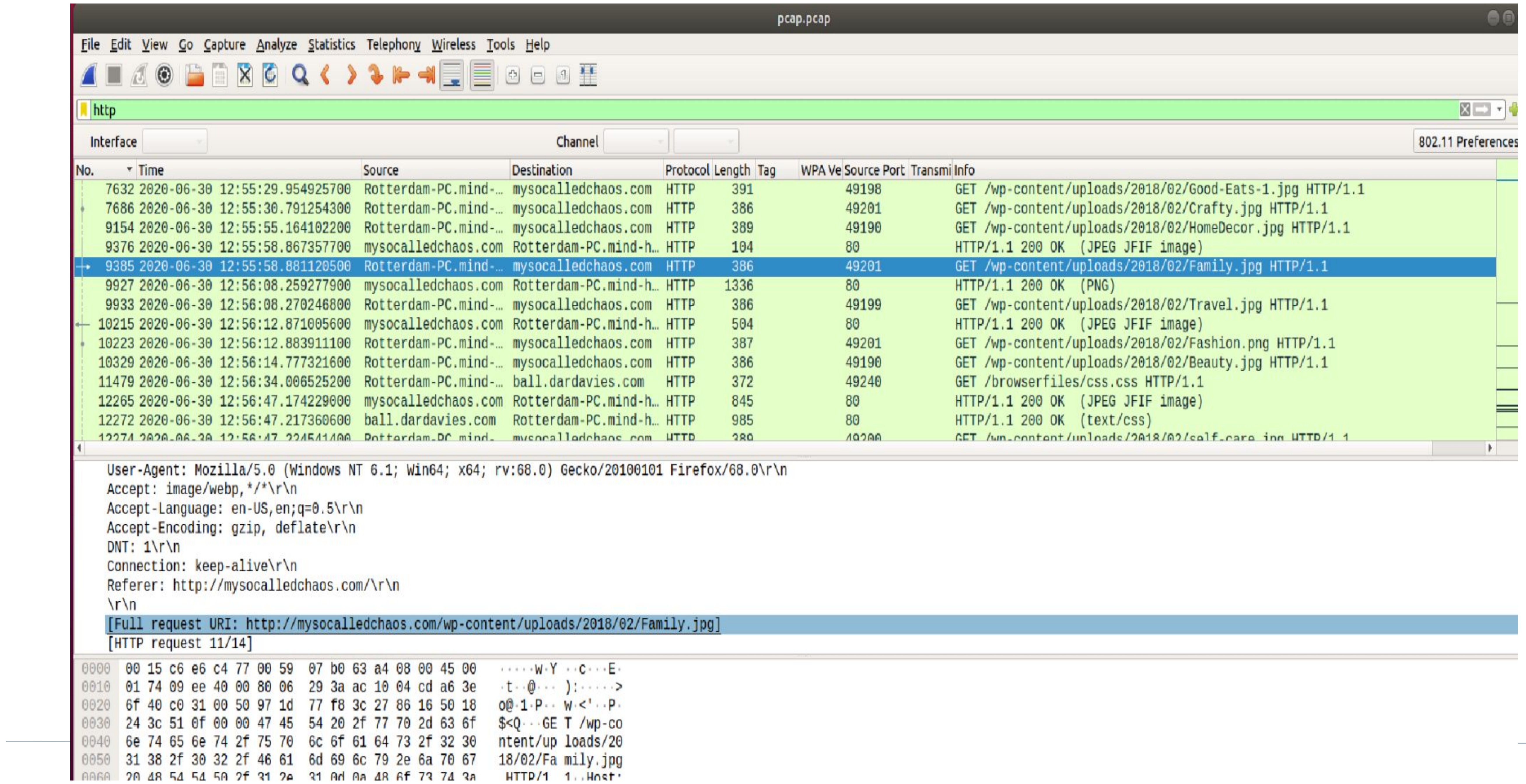
Suspicious Activity

- Setting up custom server to watch YouTube and also bypass security settings
- Users were exposed to malware and user machines were infected
- Illegal downloads from torrent sites

Normal Activity

Browsing Social Media

- Several HTTP requests to a social media website called mysocalledchaos.com were tracked
- GET requests to view selected images
- Although this activity is discouraged during work hours, social media browsing is not logged as suspicious behavior depending on the site and files involved
- A few pictures were viewed by this user, a image file named family.jpg which showed a baby. We can see with the GET request that these images were selected by the user to be viewed
- A few other images of plants, travel images, and other misc. images


pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Interface
Channel
802.11 Preferences

```
No.     Time                           Source                Destination            Protocol Length Tag  WPA Ve Source Port Transmi Info
   7632 2020-06-30 12:55:29.954925700  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     391              49198               GET /wp-content/uploads/2018/02/Good-Eats-1.jpg HTTP/1.1
   7686 2020-06-30 12:55:30.791254300  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     386              49201               GET /wp-content/uploads/2018/02/Crafty.jpg HTTP/1.1
   9154 2020-06-30 12:55:55.164102200  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     389              49190               GET /wp-content/uploads/2018/02/HomeDecor.jpg HTTP/1.1
   9376 2020-06-30 12:55:58.867357700  mysocalledchaos.com   Rotterdam-PC.mind-h…   HTTP     104              80                  HTTP/1.1 200 OK  (JPEG JFIF image)
   9385 2020-06-30 12:55:58.881120500  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     386              49201               GET /wp-content/uploads/2018/02/Family.jpg HTTP/1.1
   9927 2020-06-30 12:56:08.259277900  mysocalledchaos.com   Rotterdam-PC.mind-h…   HTTP     1336             80                  HTTP/1.1 200 OK  (PNG)
   9933 2020-06-30 12:56:08.270246800  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     386              49199               GET /wp-content/uploads/2018/02/Travel.jpg HTTP/1.1
  10215 2020-06-30 12:56:12.871005600  mysocalledchaos.com   Rotterdam-PC.mind-h…   HTTP     504              80                  HTTP/1.1 200 OK  (JPEG JFIF image)
  10223 2020-06-30 12:56:12.883911100  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     387              49201               GET /wp-content/uploads/2018/02/Fashion.png HTTP/1.1
  10329 2020-06-30 12:56:14.777321600  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     386              49190               GET /wp-content/uploads/2018/02/Beauty.jpg HTTP/1.1
  11479 2020-06-30 12:56:34.006525200  Rotterdam-PC.mind-…   ball.dardavies.com     HTTP     372              49240               GET /browserfiles/css.css HTTP/1.1
  12265 2020-06-30 12:56:47.174229000  mysocalledchaos.com   Rotterdam-PC.mind-h…   HTTP     845              80                  HTTP/1.1 200 OK  (JPEG JFIF image)
  12272 2020-06-30 12:56:47.217360600  ball.dardavies.com    Rotterdam-PC.mind-h…   HTTP     985              80                  HTTP/1.1 200 OK  (text/css)
  12274 2020-06-30 12:56:47.224541400  Rotterdam-PC.mind-…   mysocalledchaos.com    HTTP     389              49200               GET /wp-content/uploads/2018/02/self-care.jpg HTTP/1.1
```

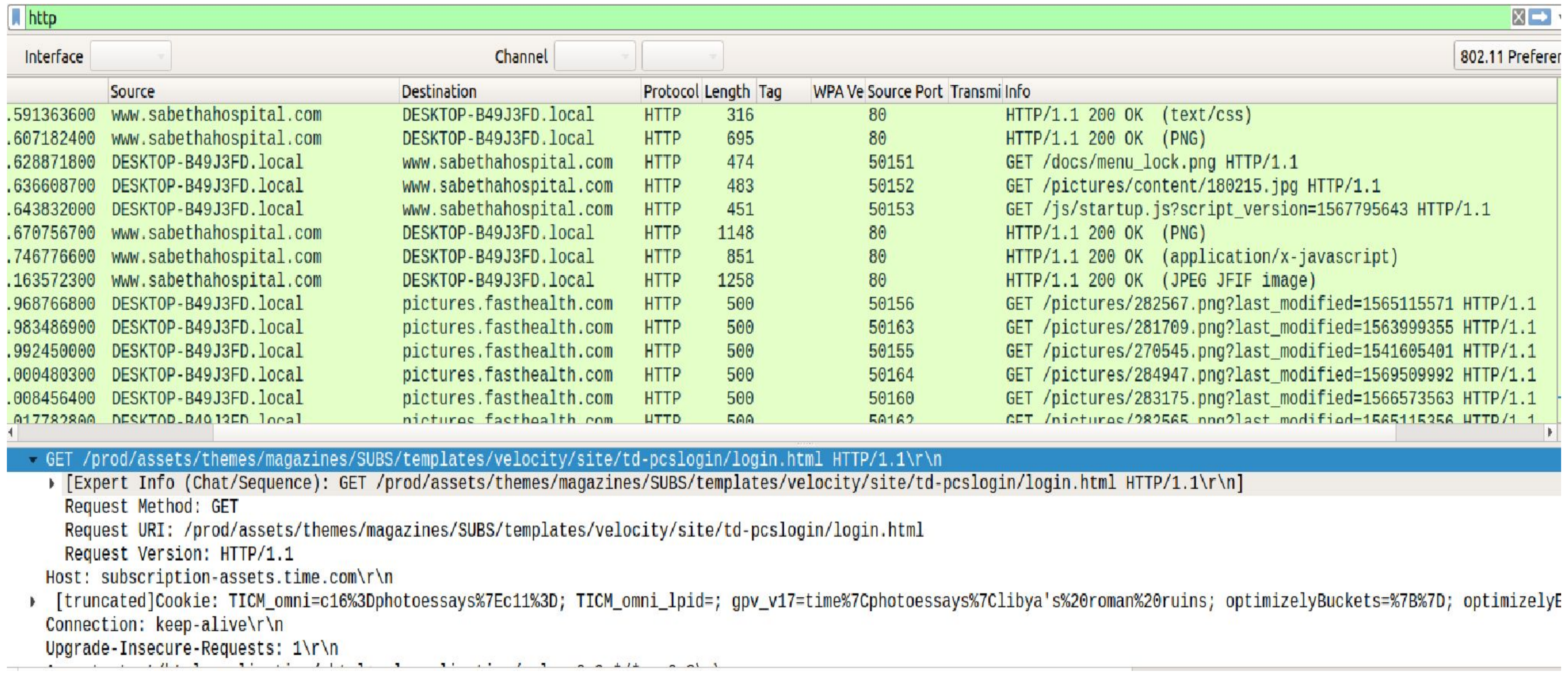
```
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
    Accept: image/webp,*/*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Referer: http://mysocalledchaos.com/\r\n
    \r\n
    [Full request URI: http://mysocalledchaos.com/wp-content/uploads/2018/02/Family.jpg]
    [HTTP request 11/14]
```

```
0000  00 15 c6 e6 c4 77 00 59  07 b0 63 a4 08 00 45 00   ·····w·Y ··c···E·
0010  01 74 09 ee 40 00 80 06  29 3a ac 10 04 cd a6 3e   ·t··@··· ):·····>
0020  6f 40 c0 31 00 50 97 1d  77 f8 3c 27 86 16 50 18   o@·1·P·· w·<'··P·
0030  24 3c 51 0f 00 00 47 45  54 20 2f 77 70 2d 63 6f   $<Q···GE T /wp-co
0040  6e 74 65 6e 74 2f 75 70  6c 6f 61 64 73 2f 32 30   ntent/up loads/20
0050  31 38 2f 30 32 2f 46 61  6d 69 6c 79 2e 6a 70 67   18/02/Fa mily.jpg
0060  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
```

Visiting healthcare and health related websites

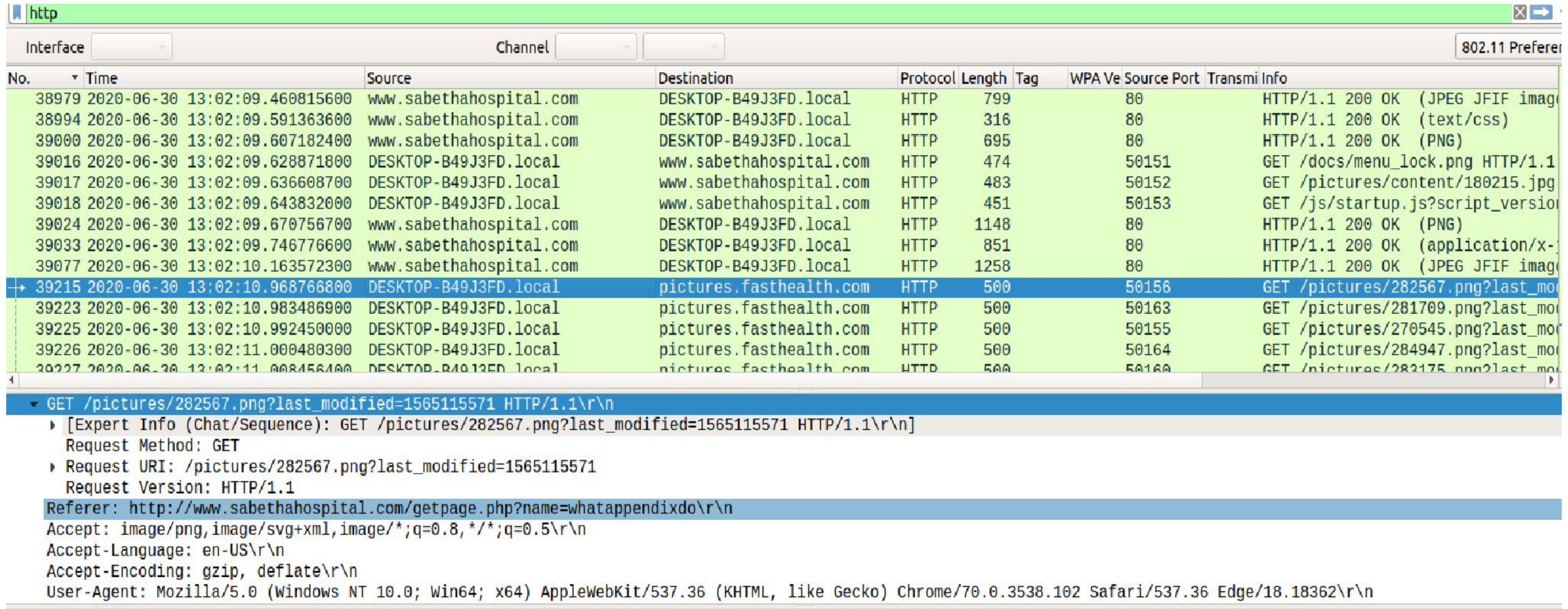
Summarize the following:

- User visited local hospital website. Several GET requests are tracked indicating navigation through several pages and loading of images on the website
- User selected a link from the hospital website that redirected to another health related site
- We can see in the traffic, the referer is the original hospital site



```
            Source                 Destination              Protocol Length Tag  WPA Ve Source Port Transmi Info
.591363600  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     316               80                  HTTP/1.1 200 OK  (text/css)
.607182400  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     695               80                  HTTP/1.1 200 OK  (PNG)
.628871800  DESKTOP-B49J3FD.local   www.sabethahospital.com HTTP     474               50151               GET /docs/menu_lock.png HTTP/1.1
.636608700  DESKTOP-B49J3FD.local   www.sabethahospital.com HTTP     483               50152               GET /pictures/content/180215.jpg HTTP/1.1
.643832000  DESKTOP-B49J3FD.local   www.sabethahospital.com HTTP     451               50153               GET /js/startup.js?script_version=1567795643 HTTP/1.1
.670756700  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     1148              80                  HTTP/1.1 200 OK  (PNG)
.746776600  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     851               80                  HTTP/1.1 200 OK  (application/x-javascript)
.163572300  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     1258              80                  HTTP/1.1 200 OK  (JPEG JFIF image)
.968766800  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50156               GET /pictures/282567.png?last_modified=1565115571 HTTP/1.1
.983486900  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50163               GET /pictures/281709.png?last_modified=1563999355 HTTP/1.1
.992450000  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50155               GET /pictures/270545.png?last_modified=1541605401 HTTP/1.1
.000480300  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50164               GET /pictures/284947.png?last_modified=1569509992 HTTP/1.1
.008456400  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50160               GET /pictures/283175.png?last_modified=1566573563 HTTP/1.1
.017782800  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50162               GET /pictures/282565.png?last_modified=1565115356 HTTP/1.1
```

```
▾ GET /prod/assets/themes/magazines/SUBS/templates/velocity/site/td-pcslogin/login.html HTTP/1.1\r\n
  ▸ [Expert Info (Chat/Sequence): GET /prod/assets/themes/magazines/SUBS/templates/velocity/site/td-pcslogin/login.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /prod/assets/themes/magazines/SUBS/templates/velocity/site/td-pcslogin/login.html
    Request Version: HTTP/1.1
  Host: subscription-assets.time.com\r\n
▸ [truncated]Cookie: TICM_omni=c16%3Dphotoessays%7Ec11%3D; TICM_omni_lpid=; gpv_v17=time%7Cphotoessays%7Clibya's%20roman%20ruins; optimizelyBuckets=%7B%7D; optimizelyE
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
```



```
No.   ▾ Time                          Source                  Destination             Protocol Length Tag  WPA Ve Source Port Transmi Info
38979 2020-06-30 13:02:09.460815600  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     799               80                  HTTP/1.1 200 OK  (JPEG JFIF imag
38994 2020-06-30 13:02:09.591363600  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     316               80                  HTTP/1.1 200 OK  (text/css)
39000 2020-06-30 13:02:09.607182400  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     695               80                  HTTP/1.1 200 OK  (PNG)
39016 2020-06-30 13:02:09.628871800  DESKTOP-B49J3FD.local   www.sabethahospital.com HTTP     474               50151               GET /docs/menu_lock.png HTTP/1.1
39017 2020-06-30 13:02:09.636608700  DESKTOP-B49J3FD.local   www.sabethahospital.com HTTP     483               50152               GET /pictures/content/180215.jpg
39018 2020-06-30 13:02:09.643832000  DESKTOP-B49J3FD.local   www.sabethahospital.com HTTP     451               50153               GET /js/startup.js?script_versio
39024 2020-06-30 13:02:09.670756700  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     1148              80                  HTTP/1.1 200 OK  (PNG)
39033 2020-06-30 13:02:09.746776600  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     851               80                  HTTP/1.1 200 OK  (application/x-
39077 2020-06-30 13:02:10.163572300  www.sabethahospital.com DESKTOP-B49J3FD.local   HTTP     1258              80                  HTTP/1.1 200 OK  (JPEG JFIF imag
39215 2020-06-30 13:02:10.968766800  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50156               GET /pictures/282567.png?last_mo
39223 2020-06-30 13:02:10.983486900  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50163               GET /pictures/281709.png?last_mo
39225 2020-06-30 13:02:10.992450000  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50155               GET /pictures/270545.png?last_mo
39226 2020-06-30 13:02:11.000480300  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50164               GET /pictures/284947.png?last_mo
39227 2020-06-30 13:02:11.008456400  DESKTOP-B49J3FD.local   pictures.fasthealth.com HTTP     500               50160               GET /pictures/283175.png?last_mo
```

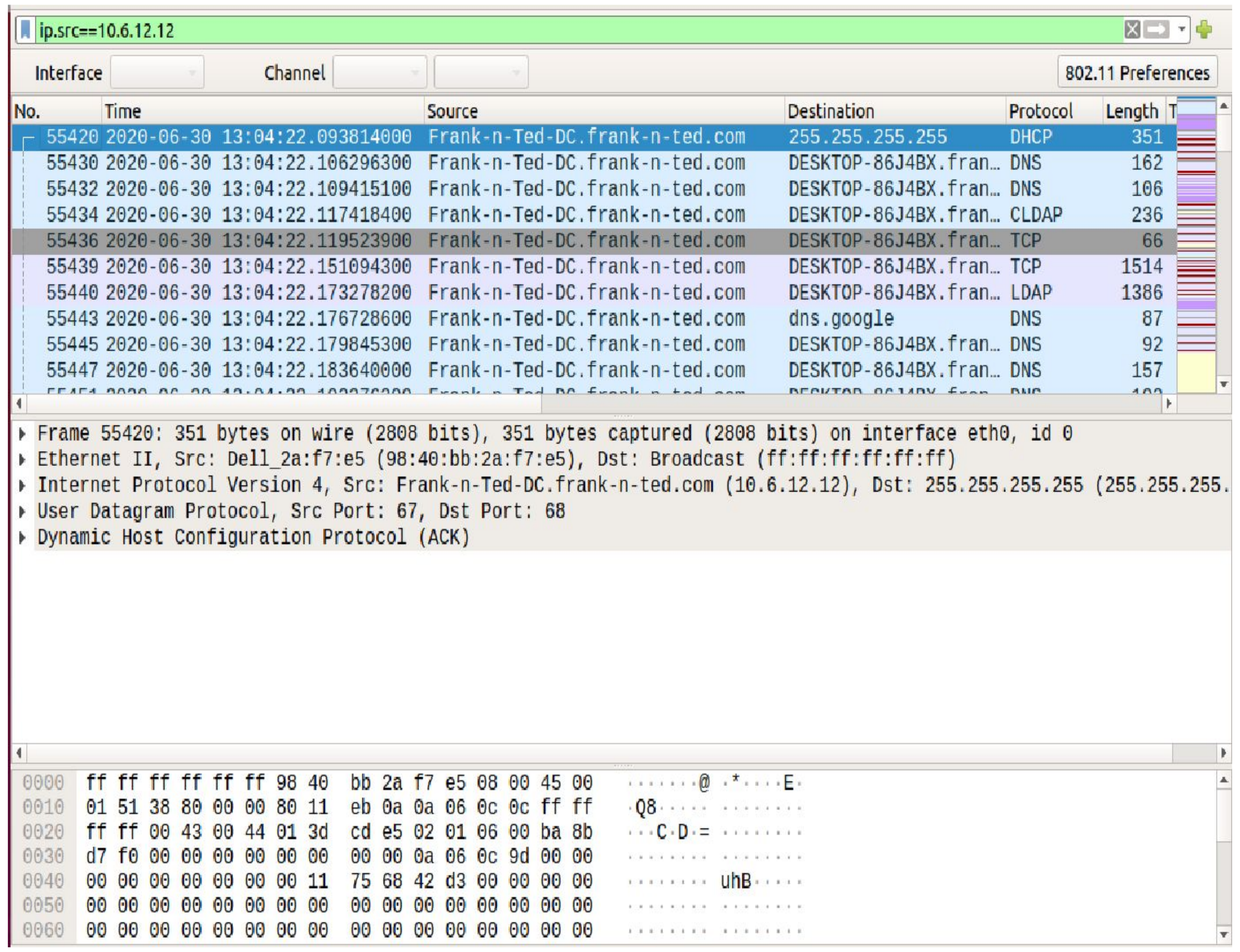
```
▾ GET /pictures/282567.png?last_modified=1565115571 HTTP/1.1\r\n
  ▸ [Expert Info (Chat/Sequence): GET /pictures/282567.png?last_modified=1565115571 HTTP/1.1\r\n]
    Request Method: GET
  ▸ Request URI: /pictures/282567.png?last_modified=1565115571
    Request Version: HTTP/1.1
  Referer: http://www.sabethahospital.com/getpage.php?name=whatappendixdo\r\n
  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/70.0.3538.102 Safari/537.36 Edge/18.18362\r\n
```

- Several PNG files were requested from health site (fasthealth.com)
- These appear to embedded images in the webpage as the user was navigating

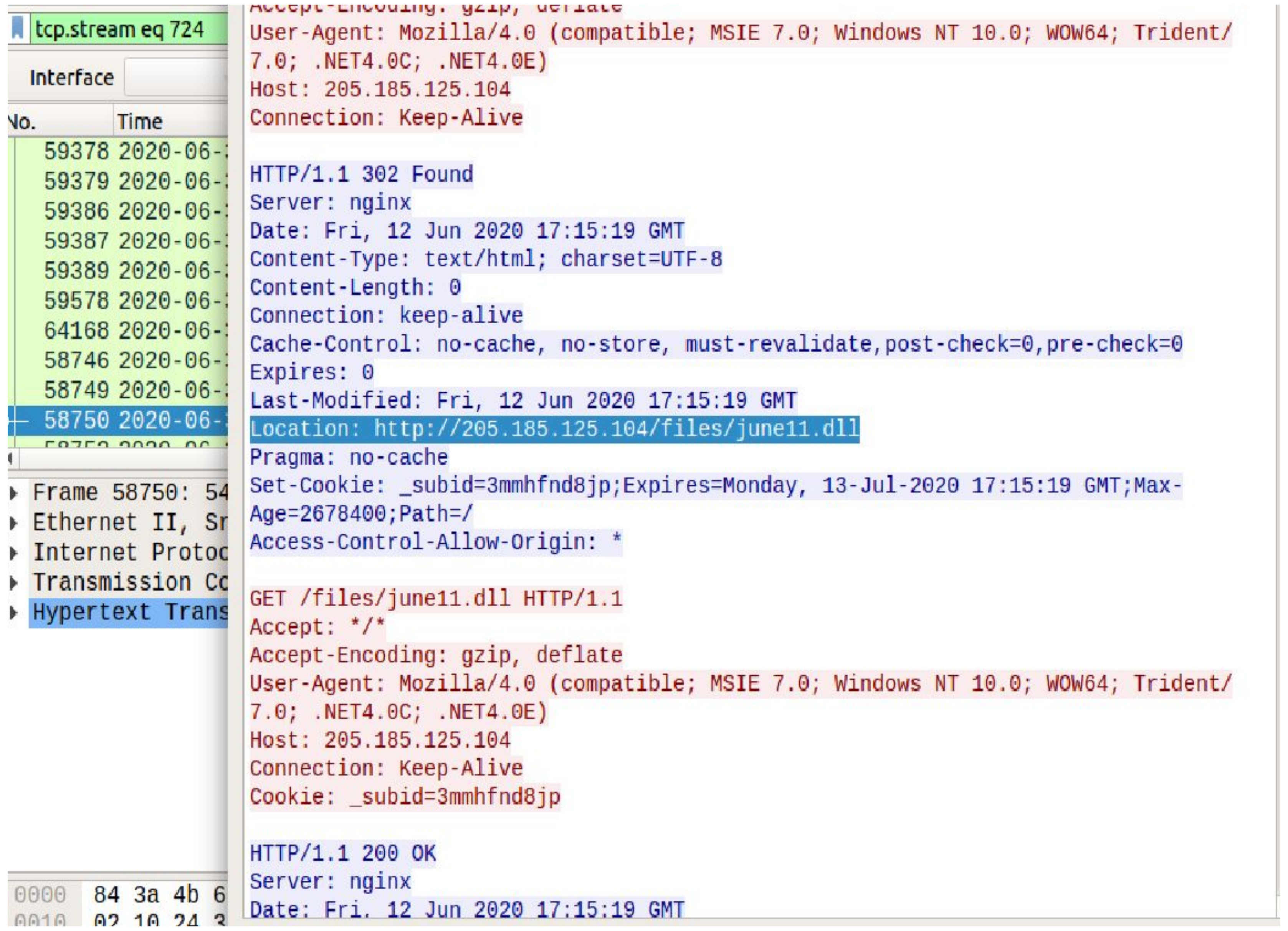
Malicious Activity

Time Theft

- It was determined that two employees were stealing time by browsing YouTube during work hours
- The users had created their own custom server within the network to use for this purpose, TCP and DNS traffic was tracked to the server
- Also, malware infected a machine on the network as a result of the activity.
- A trojan malware identified as June11.dll was detected being downloaded onto the infected machine.
- TCP traffic was traced to determine source of malware at 185.243.115.84

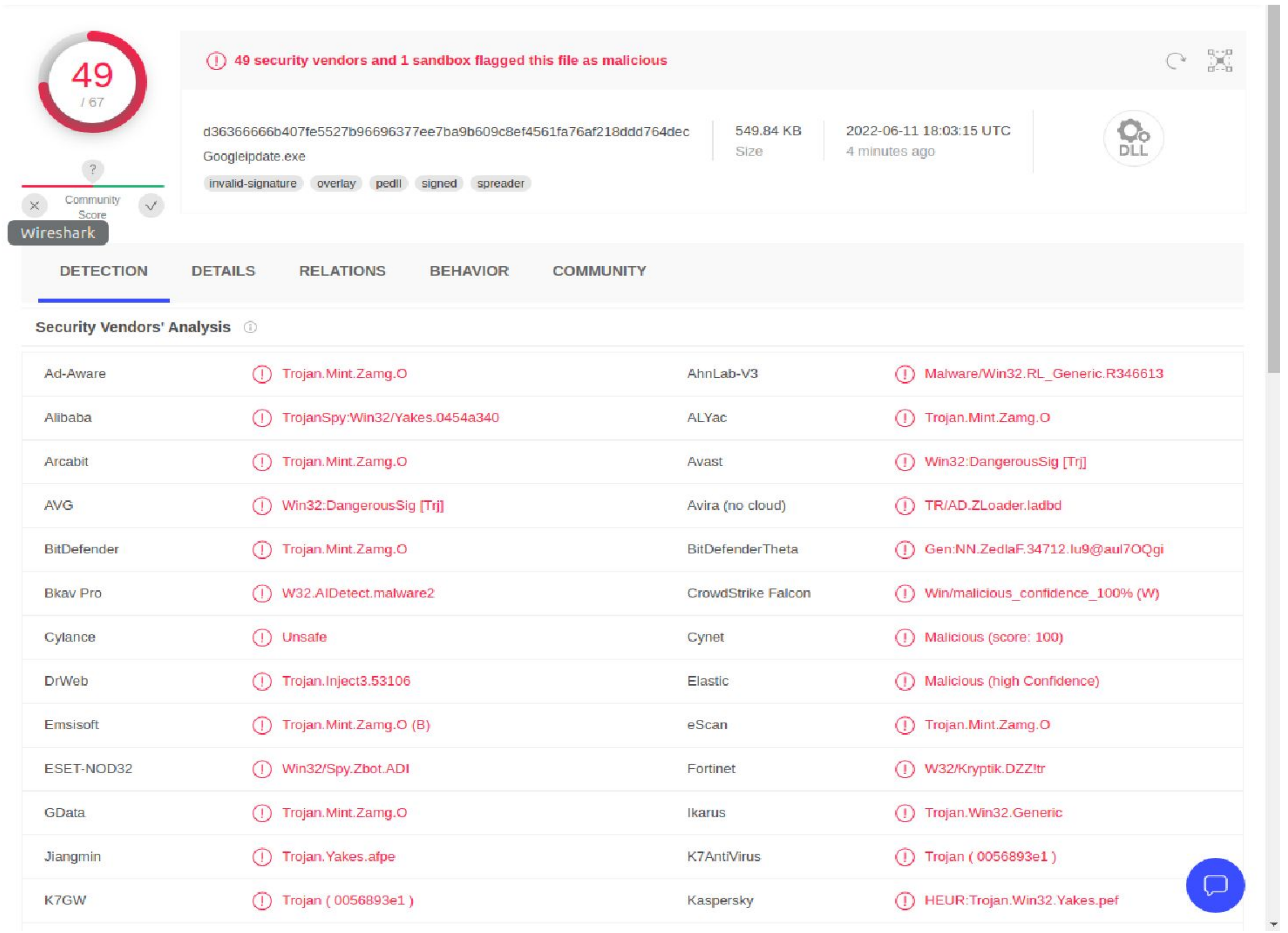


```
ip.src==10.6.12.12

No.   Time                           Source                         Destination            Protocol  Length
55420 2020-06-30 13:04:22.093814000  Frank-n-Ted-DC.frank-n-ted.com 255.255.255.255        DHCP       351
55430 2020-06-30 13:04:22.106296300  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   DNS        162
55432 2020-06-30 13:04:22.109415100  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   DNS        106
55434 2020-06-30 13:04:22.117418400  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   CLDAP      236
55436 2020-06-30 13:04:22.119523900  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   TCP         66
55439 2020-06-30 13:04:22.151094300  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   TCP       1514
55440 2020-06-30 13:04:22.173278200  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   LDAP      1386
55443 2020-06-30 13:04:22.176728600  Frank-n-Ted-DC.frank-n-ted.com dns.google             DNS         87
55445 2020-06-30 13:04:22.179845300  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   DNS         92
55447 2020-06-30 13:04:22.183640000  Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran…   DNS        157

▸ Frame 55420: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0
▸ Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: 255.255.255.255 (255.255.255.
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▸ Dynamic Host Configuration Protocol (ACK)

0000  ff ff ff ff ff ff 98 40  bb 2a f7 e5 08 00 45 00   ·······@ ·*····E·
0010  01 51 38 80 00 00 80 11  eb 0a 0a 06 0c 0c ff ff   ·Q8····· ········
0020  ff ff 00 43 00 44 01 3d  cd e5 02 01 06 00 ba 8b   ···C·D·= ········
0030  d7 f0 00 00 00 00 00 00  00 00 0a 06 0c 9d 00 00   ········ ········
0040  00 00 00 00 00 00 00 11  75 68 42 d3 00 00 00 00   ········ uhB·····
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   ········ ········
```



```
tcp.stream eq 724

No.   Time
59378 2020-06-
59379 2020-06-
59386 2020-06-
59387 2020-06-
59389 2020-06-
59578 2020-06-
64168 2020-06-
58746 2020-06-
58749 2020-06-
58750 2020-06-

▸ Frame 58750: 54
▸ Ethernet II, Sr
▸ Internet Protoc
▸ Transmission Cc
▸ Hypertext Trans

0000  84 3a 4b 6
0010  02 10 24 3
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/
7.0; .NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-
Age=2678400;Path=/
Access-Control-Allow-Origin: *

GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/
7.0; .NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
```



49 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Googleipdate.exe

549.84 KB
Size

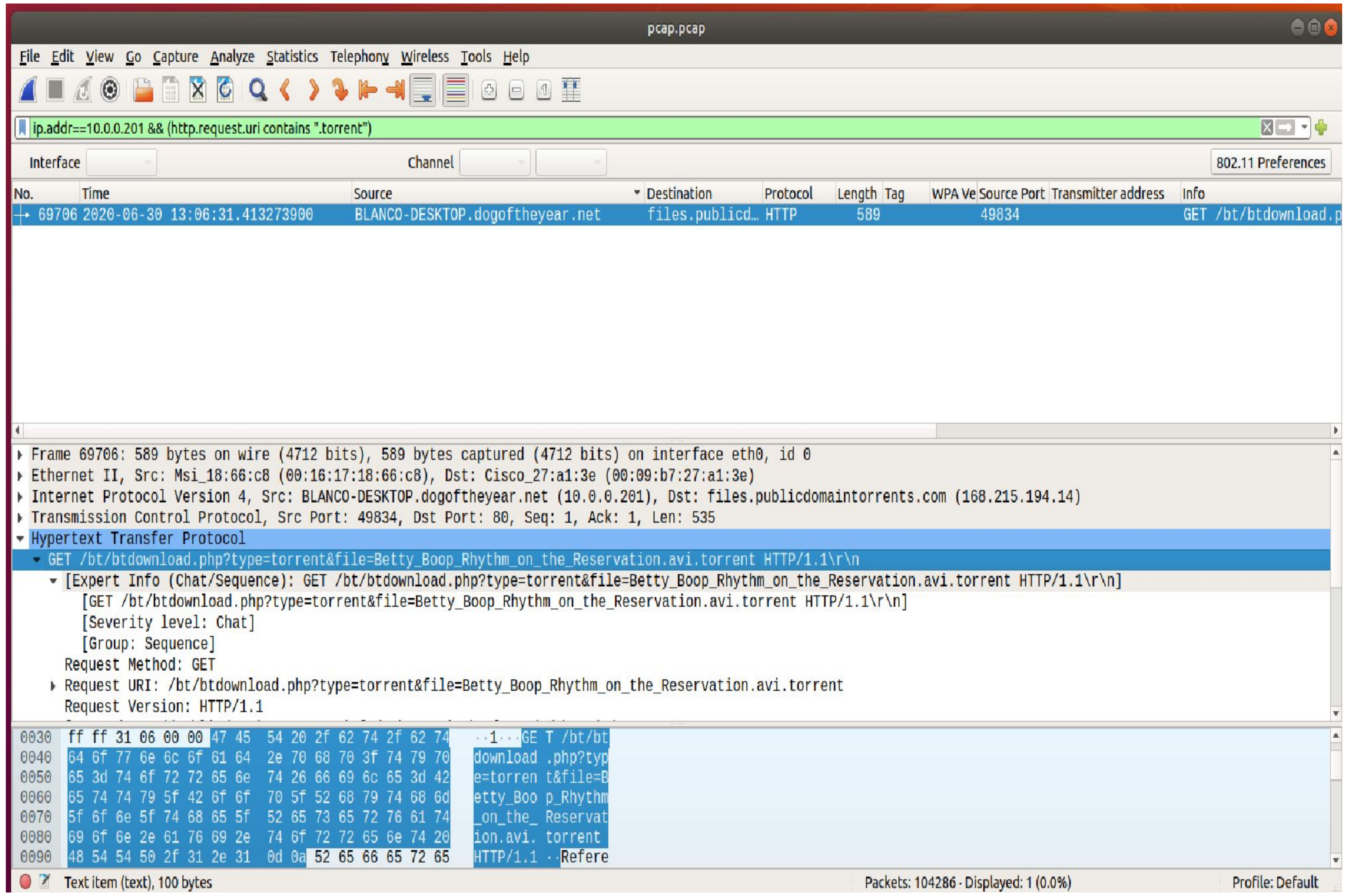
2022-06-11 18:03:15 UTC
4 minutes ago

Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Arcabit	Trojan.Mint.Zamg.O	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	Gen:NN.ZedlaF.34712.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.Inject3.53106	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Mint.Zamg.O (B)	eScan	Trojan.Mint.Zamg.O
ESET-NOD32	Win32/Spy.Zbot.ADI	Fortinet	W32/Kryptik.DZZ!tr
GData	Trojan.Mint.Zamg.O	Ikarus	Trojan.Win32.Generic
Jiangmin	Trojan.Yakes.afpe	K7AntiVirus	Trojan (0056893e1)
K7GW	Trojan (0056893e1)	Kaspersky	HEUR:Trojan.Win32.Yakes.pef

Illegal Downloads

- Capture analysis detected a user performing illegal downloads onto their work computer
- HTTP traffic was detected sending a GET request to a torrent site
- A file from a torrent file was downloaded by the user


pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface
Channel
802.11 Preferences

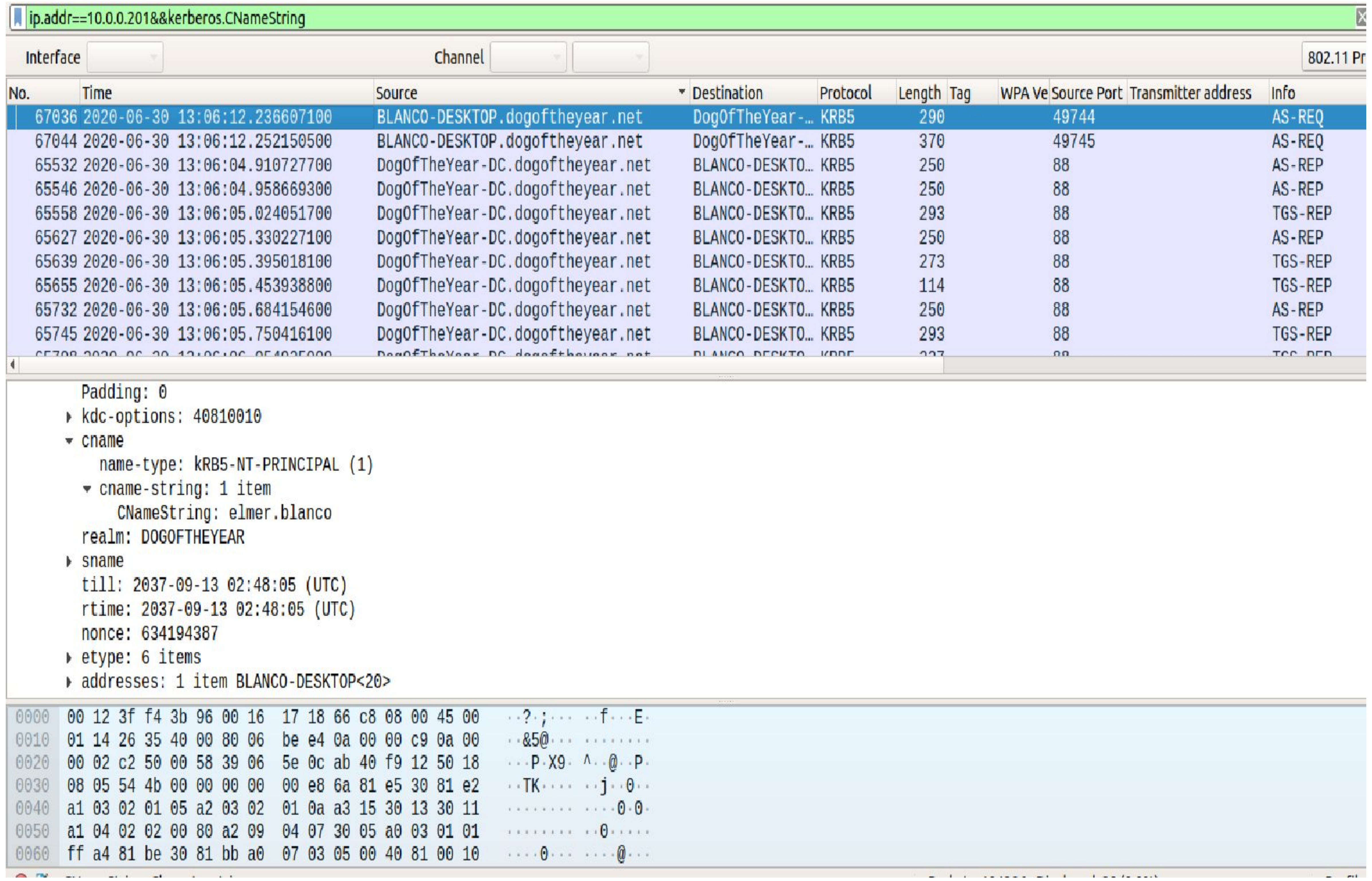
```
ip.addr==10.0.0.201 && (http.request.uri contains ".torrent")
```

```
No.   Time                          Source                          Destination      Protocol Length Tag WPA Ve Source Port Transmitter address Info
69706 2020-06-30 13:06:31.413273900 BLANCO-DESKTOP.dogoftheyear.net files.publicd… HTTP     589               49834                          GET /bt/btdownload.p
```

```
▸ 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]
        [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 Version: HTTP/1.1
```

```
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
```

Text item (text), 100 bytes Packets: 104286 · Displayed: 1 (0.0%) Profile: Default



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

```
No.   Time                          Source                          Destination     Protocol Length Tag WPA Ve Source Port Transmitter address Info
67036 2020-06-30 13:06:12.236607100 BLANCO-DESKTOP.dogoftheyear.net DogOfTheYear-… KRB5     290               49744                          AS-REQ
67044 2020-06-30 13:06:12.252150500 BLANCO-DESKTOP.dogoftheyear.net DogOfTheYear-… KRB5     370               49745                          AS-REQ
65532 2020-06-30 13:06:04.910727700 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    250               88                             AS-REP
65546 2020-06-30 13:06:04.958669300 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    250               88                             AS-REP
65558 2020-06-30 13:06:05.024051700 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    293               88                             TGS-REP
65627 2020-06-30 13:06:05.330227100 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    250               88                             AS-REP
65639 2020-06-30 13:06:05.395018100 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    273               88                             TGS-REP
65655 2020-06-30 13:06:05.453938800 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    114               88                             TGS-REP
65732 2020-06-30 13:06:05.684154600 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    250               88                             AS-REP
65745 2020-06-30 13:06:05.750416100 DogOfTheYear-DC.dogoftheyear.net BLANCO-DESKTO… KRB5    293               88                             TGS-REP
```

```
    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)
    rtime: 2037-09-13 02:48:05 (UTC)
    nonce: 634194387
  ▸ etype: 6 items
  ▸ addresses: 1 item BLANCO-DESKTOP<20>
```

```
0000  00 12 3f f4 3b 96 00 16  17 18 66 c8 08 00 45 00   ··?·;··· ··f···E·
0010  01 14 26 35 40 00 80 06  be e4 0a 00 00 c9 0a 00   ··&5@··· ········
0020  00 02 c2 50 00 58 39 06  5e 0c ab 40 f9 12 50 18   ···P·X9· ^··@··P·
0030  08 05 54 4b 00 00 00 00  00 e8 6a 81 e5 30 81 e2   ··TK···· ··j··0··
0040  a1 03 02 01 05 a2 03 02  01 0a a3 15 30 13 30 11   ········ ····0·0·
0050  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
0060  ff a4 81 be 30 81 bb a0  07 03 05 00 40 81 00 10   ····0··· ····@···
```

- The file Betty_Boop_Rhythm_on_the_reservation.avi.torrent was downloaded

The End