Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

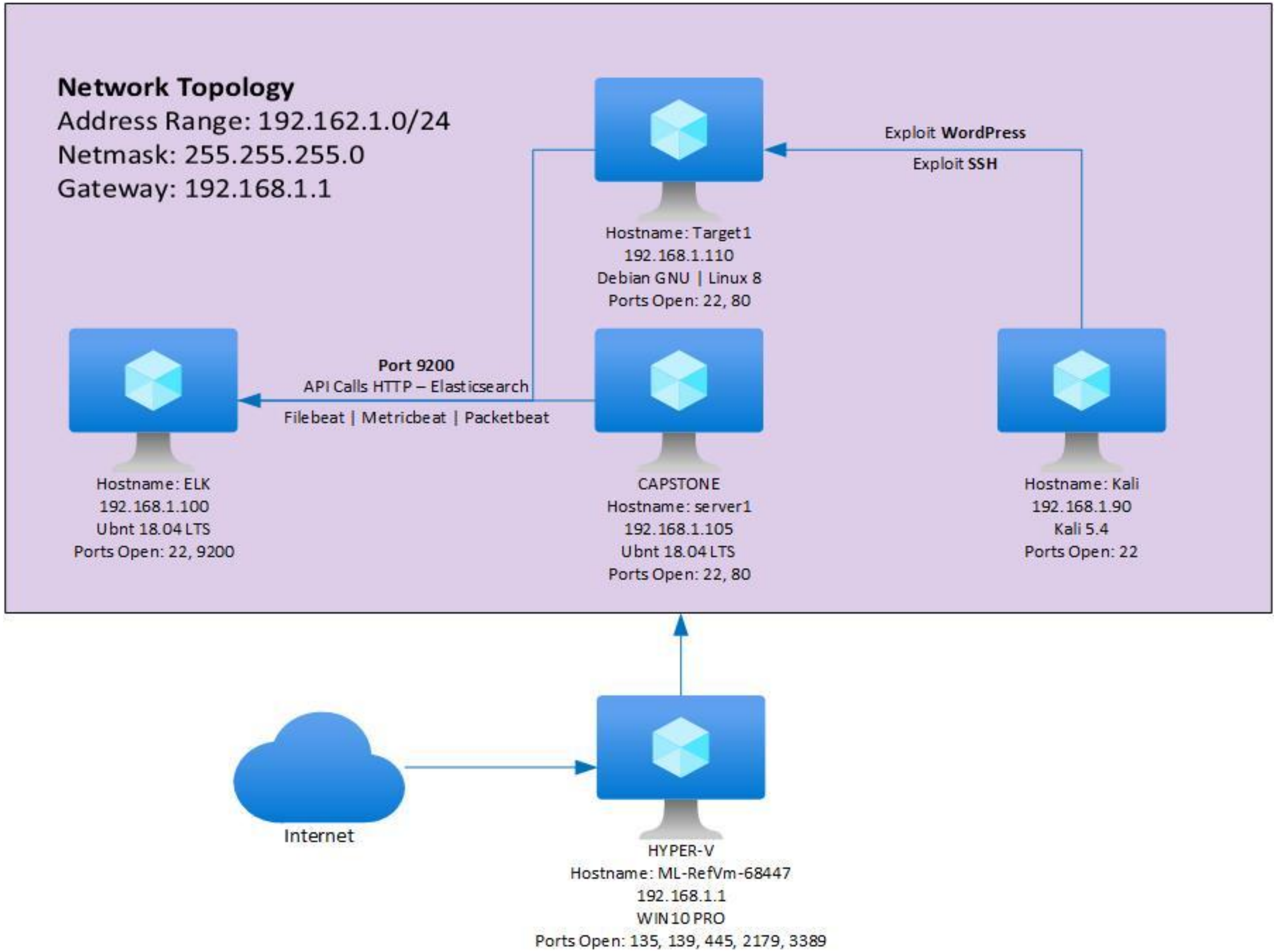
Table of Contents

This document contains the following resources:

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

Network Topology
& Critical Vulnerabilities

Network Topology



Network Topology
Address Range: 192.162.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Hostname: Target1
192.168.1.110
Debian GNU | Linux 8
Ports Open: 22, 80

Exploit WordPress
Exploit SSH

Port 9200
API Calls HTTP – Elasticsearch
Filebeat | Metricbeat | Packetbeat

Hostname: ELK
192.168.1.100
Ubnt 18.04 LTS
Ports Open: 22, 9200

CAPSTONE
Hostname: server1
192.168.1.105
Ubnt 18.04 LTS
Ports Open: 22, 80

Hostname: Kali
192.168.1.90
Kali 5.4
Ports Open: 22

Internet

HYPER-V
Hostname: ML-RefVm-68447
192.168.1.1
WIN10 PRO
Ports Open: 135, 139, 445, 2179, 3389

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

Machines
IPv4: 192.168.1.100
OS: Ubuntu 18.04 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04 LTS
Hostname: Capstone

IPv4: 192.168.1.110
OS: Debian GNU | Linux 8
Hostname: Target1

IPv4: 192.168.1.90
OS: Kali 5.4
Hostname: Kali

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Password	Passwords were simple to break as they were short in length and did not require special characters.	Brute force attack on passwords were made simple by using John to crack passwords.
User Enumeration	Enumeration was gathered to expose account usernames and unprotected files and directories.	Allowed us to gain to access to usernames which could then be used in the brute force attack.
Privilege Escalation	File permissions and exposed files allowed access to sensitive files.	Allowed access to wp_config.php which had the database password in plain text, which allowed further escalation.

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;
	172.16.4.205
		Machines that sent the most traffic.

Most Common Protocols	HTTP; Netbios (SMB); DNS	Three most common protocols on the network.
# of Unique IP Addresses	808	Count of observed IP addresses.
Subnets	*/24	Observed subnet ranges.
# of Malware Species	june11.dll | Trojan Reference: https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec	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

- Regular website browsing in WP content
- We can also see different types of media such as images
- Normal CSS content loading
- API calls related to website content

Suspicious Activity

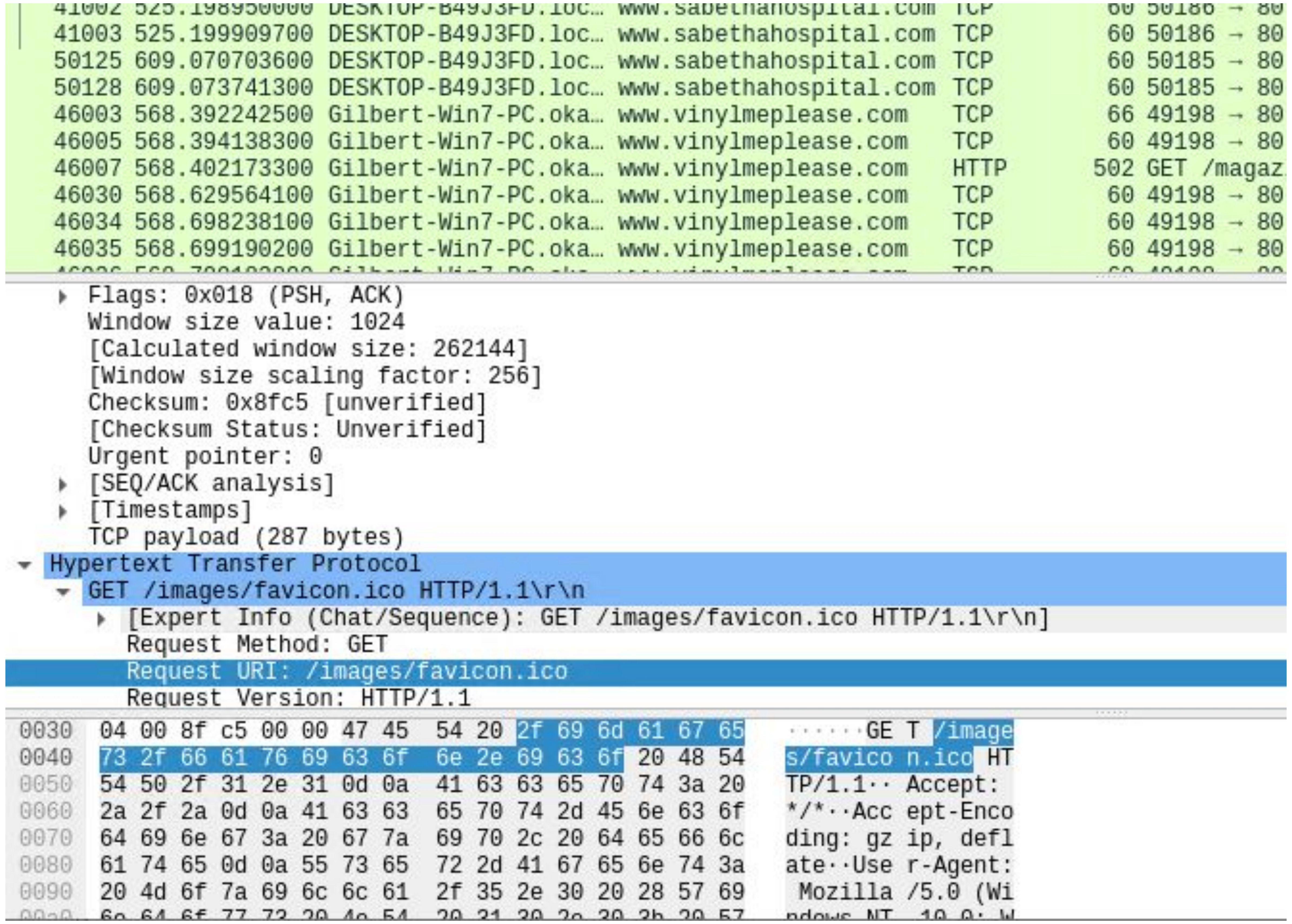
- http://205.185.125.104/files/june11.dll - **Trojan** activity
- www.publicdomaintorrents.com torrent download for **betty_boop_rhythm_on_the_reservation.avi.torrent**

Normal Activity

Normal Web Traffic

Summarize the following:

- **Which protocol(s)?**
  - HTTP
  - TCP
- **Which site were they browsing?**
  - time.com
  - vinylmeplease.com
  - sabethahospital.com



```
41002 525.198950000 DESKTOP-B49J3FD.loc… www.sabethahospital.com TCP    60 50186 → 80
41003 525.199909700 DESKTOP-B49J3FD.loc… www.sabethahospital.com TCP    60 50186 → 80
50125 609.070703600 DESKTOP-B49J3FD.loc… www.sabethahospital.com TCP    60 50185 → 80
50128 609.073741300 DESKTOP-B49J3FD.loc… www.sabethahospital.com TCP    60 50185 → 80
46003 568.392242500 Gilbert-Win7-PC.oka… www.vinylmeplease.com   TCP    66 49198 → 80
46005 568.394138300 Gilbert-Win7-PC.oka… www.vinylmeplease.com   TCP    60 49198 → 80
46007 568.402173300 Gilbert-Win7-PC.oka… www.vinylmeplease.com   HTTP  502 GET /magaz
46030 568.629564100 Gilbert-Win7-PC.oka… www.vinylmeplease.com   TCP    60 49198 → 80
46034 568.698238100 Gilbert-Win7-PC.oka… www.vinylmeplease.com   TCP    60 49198 → 80
46035 568.699190200 Gilbert-Win7-PC.oka… www.vinylmeplease.com   TCP    60 49198 → 80
```

```
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0x8fc5 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (287 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /images/favicon.ico HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /images/favicon.ico HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /images/favicon.ico
      Request Version: HTTP/1.1
```

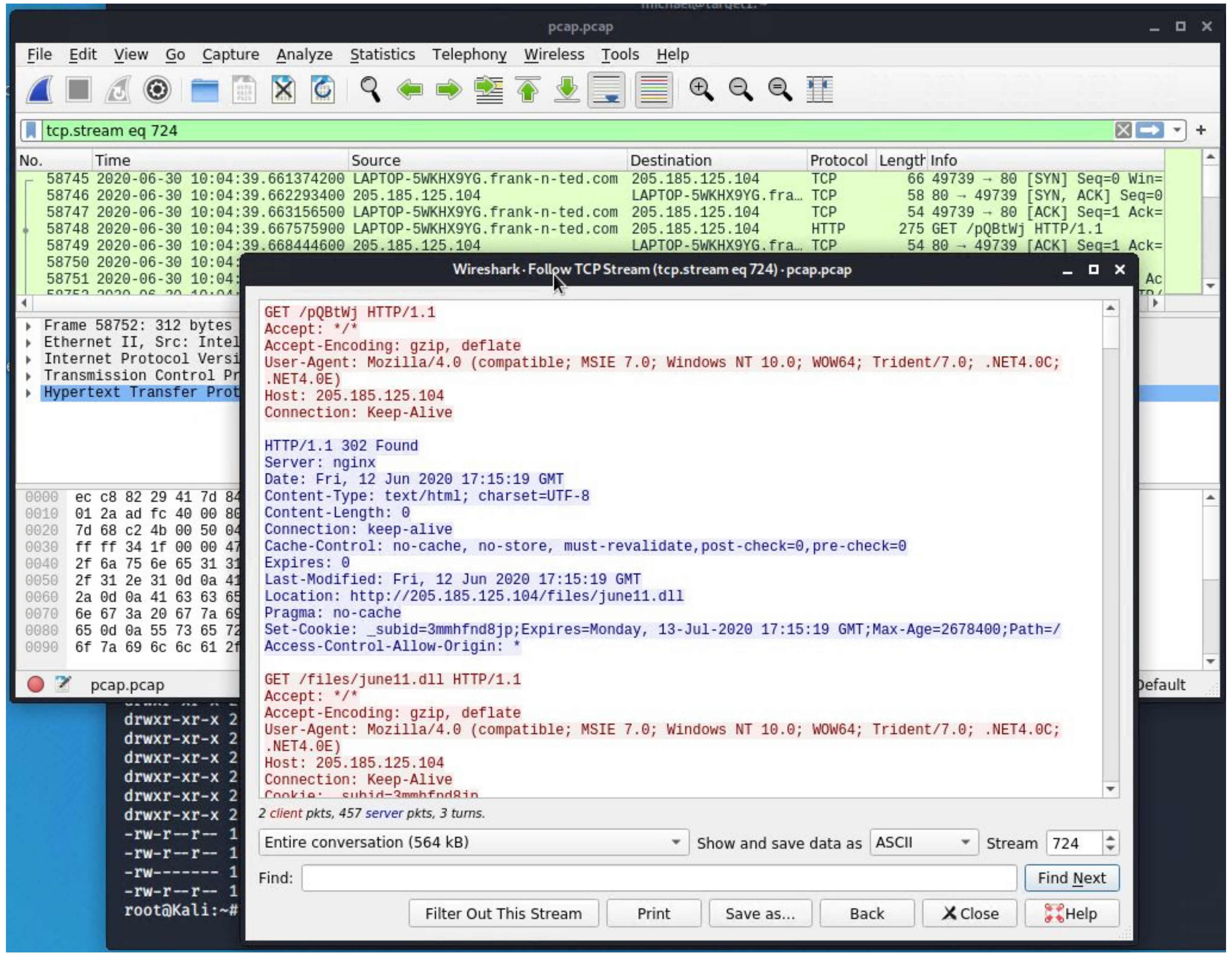
```
0030  04 00 8f c5 00 00 47 45  54 20 2f 69 6d 61 67 65   ······GE T /image
0040  73 2f 66 61 76 69 63 6f  6e 2e 69 63 6f 20 48 54   s/favico n.ico HT
0050  54 50 2f 31 2e 31 0d 0a  41 63 63 65 70 74 3a 20   TP/1.1·· Accept: 
0060  2a 2f 2a 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   */*··Acc ept-Enco
0070  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
0080  61 74 65 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   ate··Use r-Agent:
0090  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
00a0  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
```

Malicious Activity

Trojan Infection

Summarize the following:

- **Which protocol(s)?**
  - HTTP
- **What, specifically, was the user doing?**
  - A trojan file was downloaded by the end user while browsing from http://205.185.125.104.
- **Include a description of any interesting files.**
  - The file downloaded with the trojan payload was named **june11.dll**.
  - Reference: https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec



```
tcp.stream eq 724
```

```
No.    Time                          Source                               Destination              Protocol  Length Info
58745 2020-06-30 10:04:39.661374200 LAPTOP-5WKHX9YG.frank-n-ted.com 205.185.125.104          TCP        66 49739 → 80 [SYN] Seq=0 Win=
58746 2020-06-30 10:04:39.662293400 205.185.125.104                 LAPTOP-5WKHX9YG.fra…     TCP        58 80 → 49739 [SYN, ACK] Seq=0
58747 2020-06-30 10:04:39.663156500 LAPTOP-5WKHX9YG.frank-n-ted.com 205.185.125.104          TCP        54 49739 → 80 [ACK] Seq=1 Ack=
58748 2020-06-30 10:04:39.667575900 LAPTOP-5WKHX9YG.frank-n-ted.com 205.185.125.104          HTTP      275 GET /pQBtWj HTTP/1.1
58749 2020-06-30 10:04:39.668444600 205.185.125.104                 LAPTOP-5WKHX9YG.fra…     TCP        54 80 → 49739 [ACK] Seq=1 Ack=
58750 2020-06-30 10:04:
58751 2020-06-30 10:04:
```

```
▸ Frame 58752: 312 bytes
▸ Ethernet II, Src: Intel
▸ Internet Protocol Versi
▸ Transmission Control Pr
▸ Hypertext Transfer Prot
```

```
0000  ec c8 82 29 41 7d 84
0010  01 2a ad fc 40 00 80
0020  7d 68 c2 4b 00 50 04
0030  ff ff 34 1f 00 00 47
0040  2f 6a 75 6e 65 31 31
0050  2f 31 2e 31 0d 0a 41
0060  2a 0d 0a 41 63 63 65
0070  6e 67 3a 20 67 7a 69
0080  65 0d 0a 55 73 65 72
0090  6f 7a 69 6c 6c 61 2f
```

```
drwxr-xr-x 2
drwxr-xr-x 2
drwxr-xr-x 2
drwxr-xr-x 2
drwxr-xr-x 2
drwxr-xr-x 2
-rw-r--r-- 1
-rw-r--r-- 1
-rw------- 1
-rw-r--r-- 1
root@Kali:~#
```

Wireshark · Follow TCP Stream (tcp.stream eq 724) · pcap.pcap

```
GET /pQBtWj 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

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
```

2 client pkts, 457 server pkts, 3 turns.

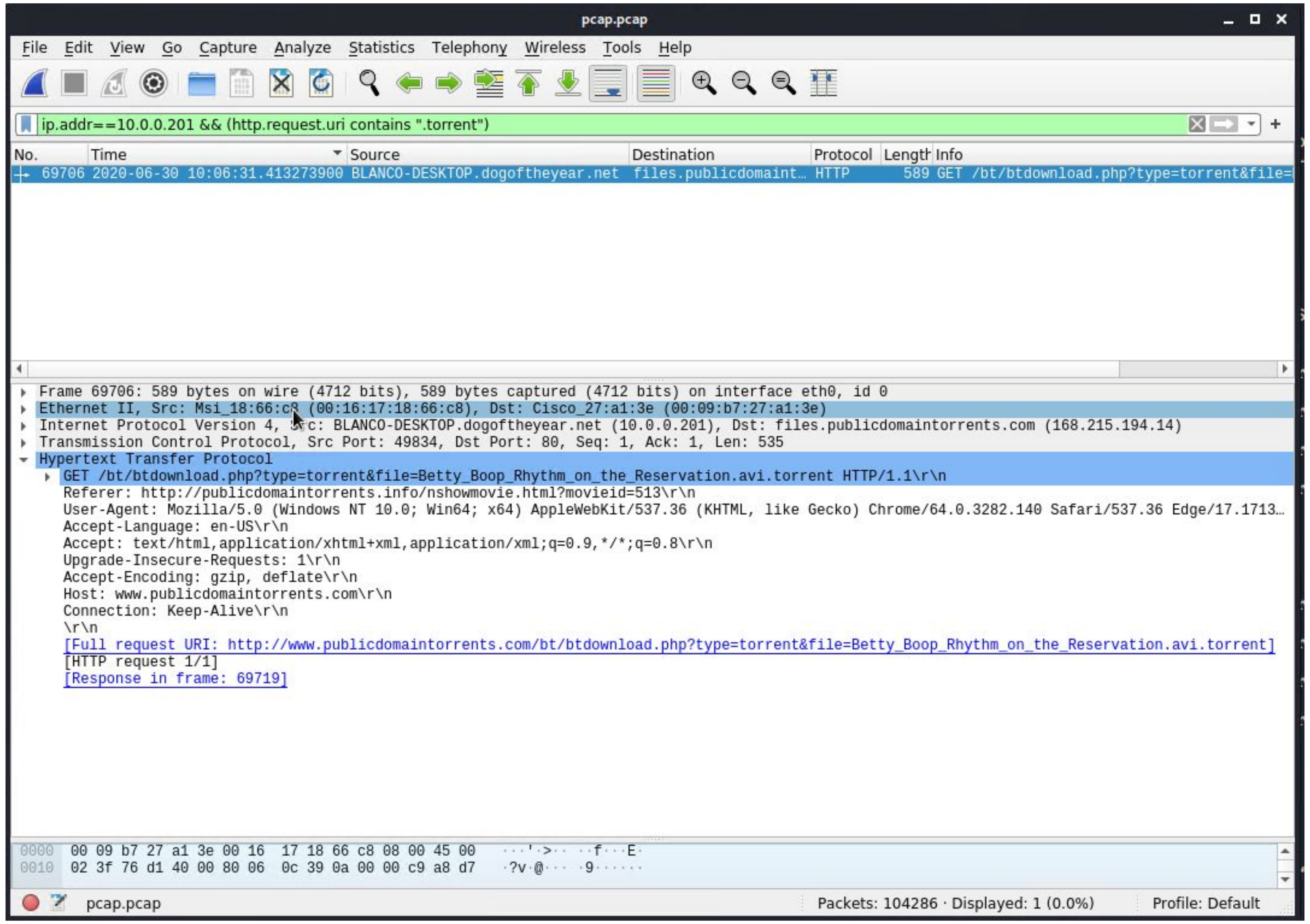
Entire conversation (564 kB) · Show and save data as: ASCII · Stream: 724

Find:

Torrent Download

Summarize the following:

- **Which protocol(s)?**
  - HTTP
  - TCP/Bittorrent Protocol
- **What, specifically, was the user doing?**
  - User was browsing and searching public domain videos on www.publicdomaintorrents.com. We can also see bitttorrent traffic to and from the end user.
- **Include a description of any interesting files.**
  - Betty_Boop_Rhythm_on_the_Reservation.avi.torrent was downloaded.


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

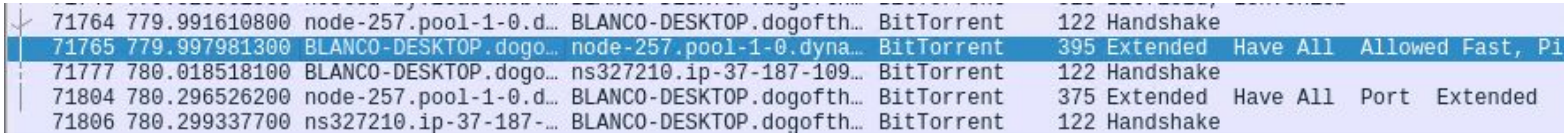
```
ip.addr==10.0.0.201 && (http.request.uri contains ".torrent")

No.   Time                          Source                         Destination             Protocol Length Info
69706 2020-06-30 10:06:31.413273900 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint… HTTP     589 GET /bt/btdownload.php?type=torrent&file=

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
  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/17.1713…
  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
  [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
  [HTTP request 1/1]
  [Response in frame: 69719]

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······

pcap.pcap          Packets: 104286 · Displayed: 1 (0.0%)          Profile: Default
```



```
71764 779.991610800 node-257.pool-1-0.d… BLANCO-DESKTOP.dogofth… BitTorrent   122 Handshake
71765 779.997981300 BLANCO-DESKTOP.dogo… node-257.pool-1-0.dyna… BitTorrent   395 Extended  Have All  Allowed Fast, Pi
71777 780.018518100 BLANCO-DESKTOP.dogo… ns327210.ip-37-187-109… BitTorrent   122 Handshake
71804 780.296526200 node-257.pool-1-0.d… BLANCO-DESKTOP.dogofth… BitTorrent   375 Extended  Have All  Port  Extended
71806 780.299337700 ns327210.ip-37-187-… BLANCO-DESKTOP.dogofth… BitTorrent   122 Handshake
```

The End