Final Engagement

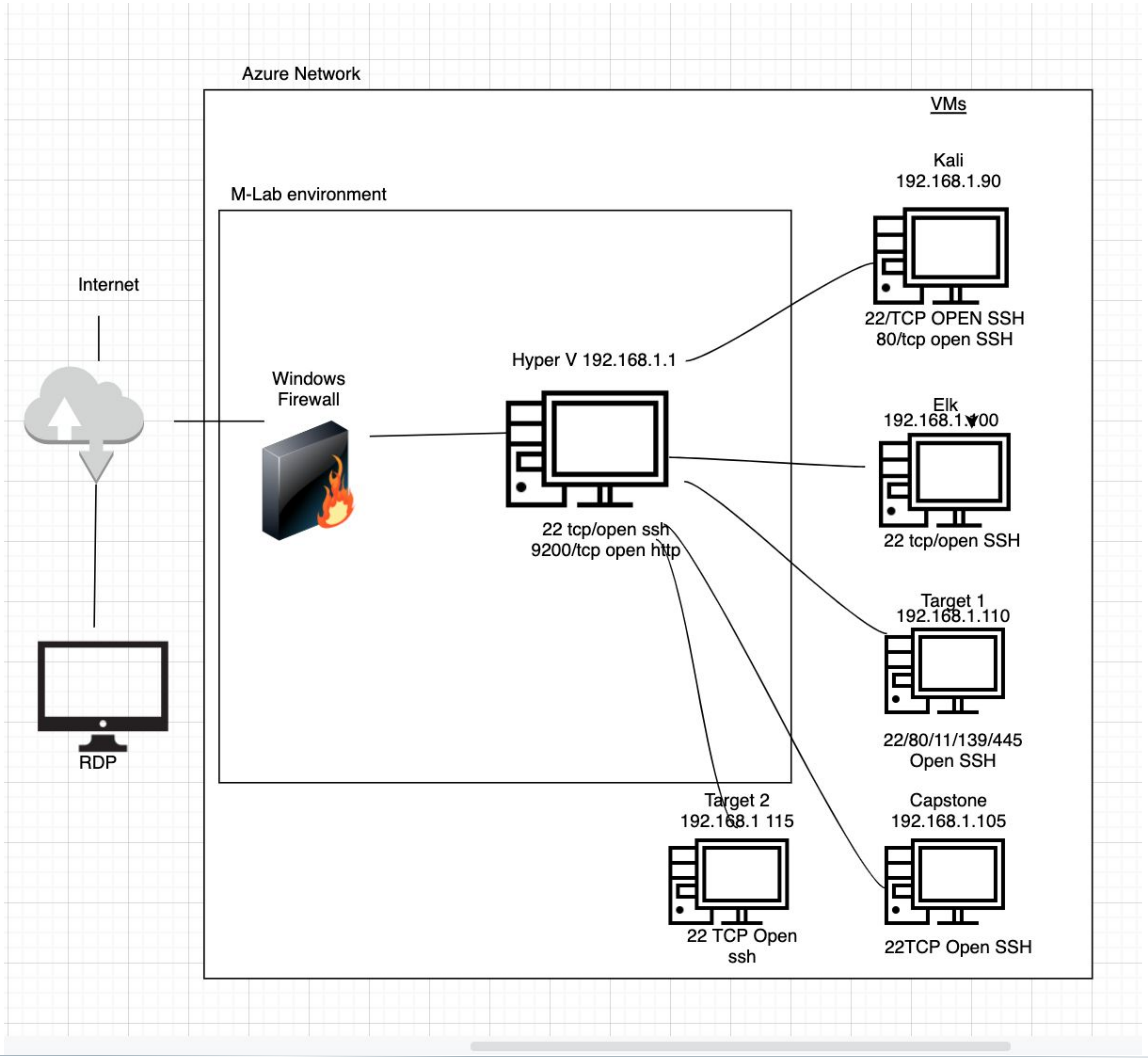
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.240.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux (WordPress)
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Password Policy	The company’s password policy allowed users to have passwords that were not complex and easily guessed, even without brute force tools.	This vulnerability allowed the attackers to easily guess user Michael’s password and access his account. This weakness also allowed the attackers to easily escalate their privileges because the password for root access was easily broken/guessed.
Open ports that do not need to be opened	Target 1 had numerous ports opened, specifically port 22 for SSH.	Having this port open and not filtered allowed the attackers the ability to use a broken password to SSH into the target’s system.
Sensitive Information Exposure/Poor Access Management	Sensitive configuration files were not secure and had improper access controls.	This vulnerability allowed the attackers to access the company’s database and steal their users’ password hashes, which were later cracked to gain deeper access.
wpscan vulnerability	Utilizing wpscan to easily discover vulnerabilities in the target’s wordpress server.	This scan allowed the attackers to easily identify usernames of the target company, and this allowed the attackers to target these specific users to break their passwords and gain access.

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 172.16.4.205	Machines that sent the most traffic.
Most Common Protocols	TCP HTTP DHCP Kerberos	Four of the most common protocols on the network.
# of Unique IP Addresses	879	Count of observed IP addresses.
Subnets	192.168.1.0/24	Observed subnet ranges.
# of Malware Species	55	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

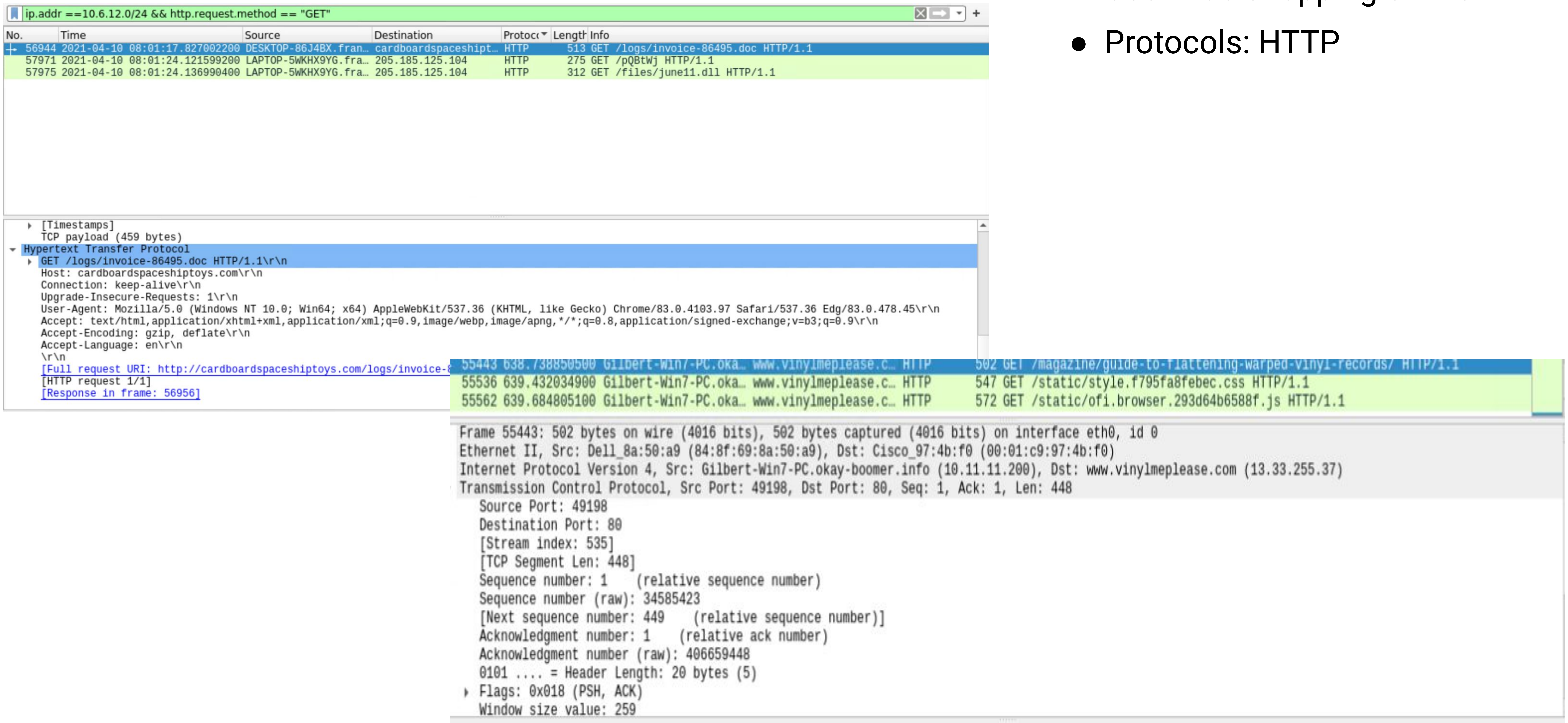
- Online shopping
- Normal website traffic and browsing

Suspicious Activity

- Set up a private web server on the company’s corporate network to steal company time undetected and then downloaded malware using this private server.
- Torrenting/downloading inappropriate/copyrighted content

Normal Activity

[Online Shopping]



```
ip.addr ==10.6.12.0/24 && http.request.method == "GET"

No.   Time                          Source              Destination          Protoc Length Info
56944 2021-04-10 08:01:17.827002200 DESKTOP-86J4BX.fran… cardboardspaceshipt… HTTP   513 GET /logs/invoice-86495.doc HTTP/1.1
57971 2021-04-10 08:01:24.121599200 LAPTOP-5WKHX9YG.fra… 205.185.125.104      HTTP   275 GET /pQBtWj HTTP/1.1
57975 2021-04-10 08:01:24.136990400 LAPTOP-5WKHX9YG.fra… 205.185.125.104      HTTP   312 GET /files/june11.dll HTTP/1.1
```

```
  [Timestamps]
  TCP payload (459 bytes)
Hypertext Transfer Protocol
  GET /logs/invoice-86495.doc HTTP/1.1\r\n
  Host: cardboardspaceshiptoys.com\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36 Edg/83.0.478.45\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en\r\n
  \r\n
  [Full request URI: http://cardboardspaceshiptoys.com/logs/invoice-8
  [HTTP request 1/1]
  [Response in frame: 56956]
```

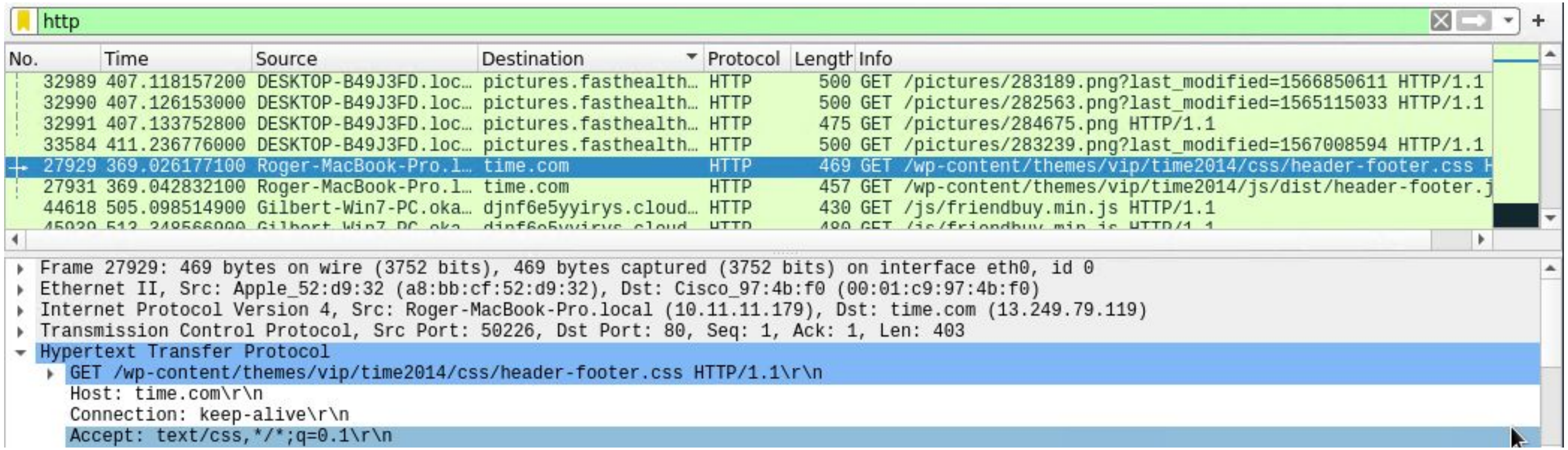
```
55443 638.738850500 Gilbert-Win7-PC.oka… www.vinylmeplease.c… HTTP    502 GET /magazine/guide-to-flattening-warped-vinyl-records/ HTTP/1.1
55536 639.432034900 Gilbert-Win7-PC.oka… www.vinylmeplease.c… HTTP    547 GET /static/style.f795fa8febec.css HTTP/1.1
55562 639.684805100 Gilbert-Win7-PC.oka… www.vinylmeplease.c… HTTP    572 GET /static/ofi.browser.293d64b6588f.js HTTP/1.1
```

```
Frame 55443: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface eth0, id 0
Ethernet II, Src: Dell_8a:50:a9 (84:8f:69:8a:50:a9), Dst: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
Internet Protocol Version 4, Src: Gilbert-Win7-PC.okay-boomer.info (10.11.11.200), Dst: www.vinylmeplease.com (13.33.255.37)
Transmission Control Protocol, Src Port: 49198, Dst Port: 80, Seq: 1, Ack: 1, Len: 448
  Source Port: 49198
  Destination Port: 80
  [Stream index: 535]
  [TCP Segment Len: 448]
  Sequence number: 1    (relative sequence number)
  Sequence number (raw): 34585423
  [Next sequence number: 449    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Acknowledgment number (raw): 406659448
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 259
```

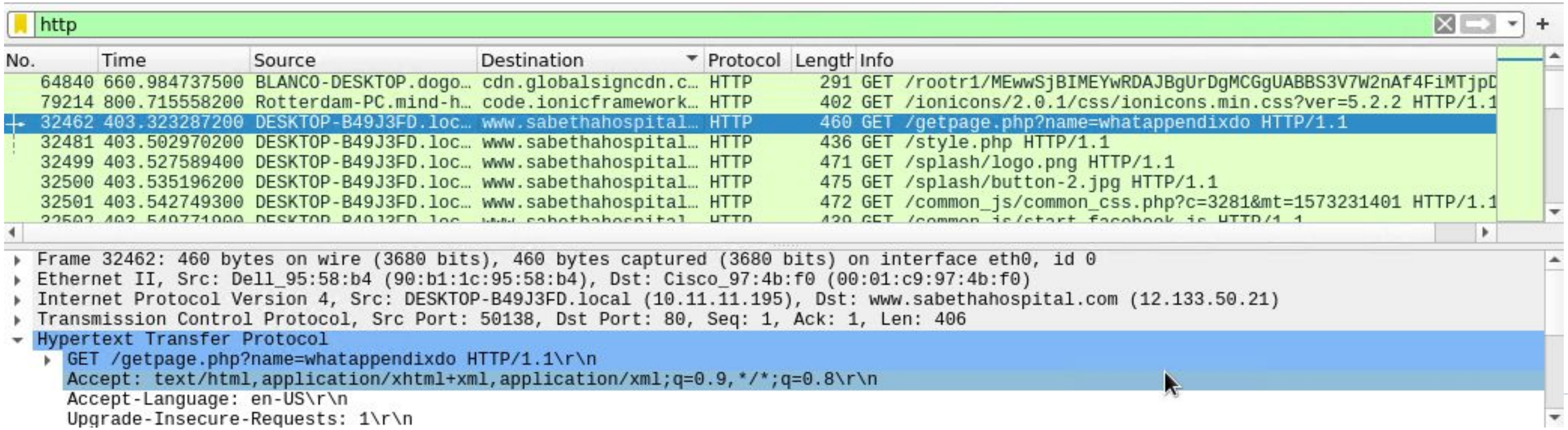
- User was shopping online
- Protocols: HTTP

[Watching Website Traffic and browsing]

- Normal website browsing traffic observed such as time.com and sabethahospital.com
- Protocol: HTTP



```
http
No.    Time          Source                Destination           Protocol Length Info
 32989 407.118157200 DESKTOP-B49J3FD.loc… pictures.fasthealth… HTTP      500 GET /pictures/283189.png?last_modified=1566850611 HTTP/1.1
 32990 407.126153000 DESKTOP-B49J3FD.loc… pictures.fasthealth… HTTP      500 GET /pictures/282563.png?last_modified=1565115033 HTTP/1.1
 32991 407.133752800 DESKTOP-B49J3FD.loc… pictures.fasthealth… HTTP      475 GET /pictures/284675.png HTTP/1.1
 33584 411.236776000 DESKTOP-B49J3FD.loc… pictures.fasthealth… HTTP      500 GET /pictures/283239.png?last_modified=1567008594 HTTP/1.1
 27929 369.026177100 Roger-MacBook-Pro.l… time.com             HTTP      469 GET /wp-content/themes/vip/time2014/css/header-footer.css H
 27931 369.042832100 Roger-MacBook-Pro.l… time.com             HTTP      457 GET /wp-content/themes/vip/time2014/js/dist/header-footer.j
 44618 505.098514900 Gilbert-Win7-PC.oka… djnf6e5yyirys.cloud… HTTP      430 GET /js/friendbuy.min.js HTTP/1.1
 45939 513.348566000 Gilbert-Win7-PC.oka… djnf6e5yyirys.cloud… HTTP      480 GET /js/friendbuy.min.js HTTP/1.1

Frame 27929: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface eth0, id 0
Ethernet II, Src: Apple_52:d9:32 (a8:bb:cf:52:d9:32), Dst: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
Internet Protocol Version 4, Src: Roger-MacBook-Pro.local (10.11.11.179), Dst: time.com (13.249.79.119)
Transmission Control Protocol, Src Port: 50226, Dst Port: 80, Seq: 1, Ack: 1, Len: 403
Hypertext Transfer Protocol
  GET /wp-content/themes/vip/time2014/css/header-footer.css HTTP/1.1\r\n
  Host: time.com\r\n
  Connection: keep-alive\r\n
  Accept: text/css,*/*;q=0.1\r\n
```

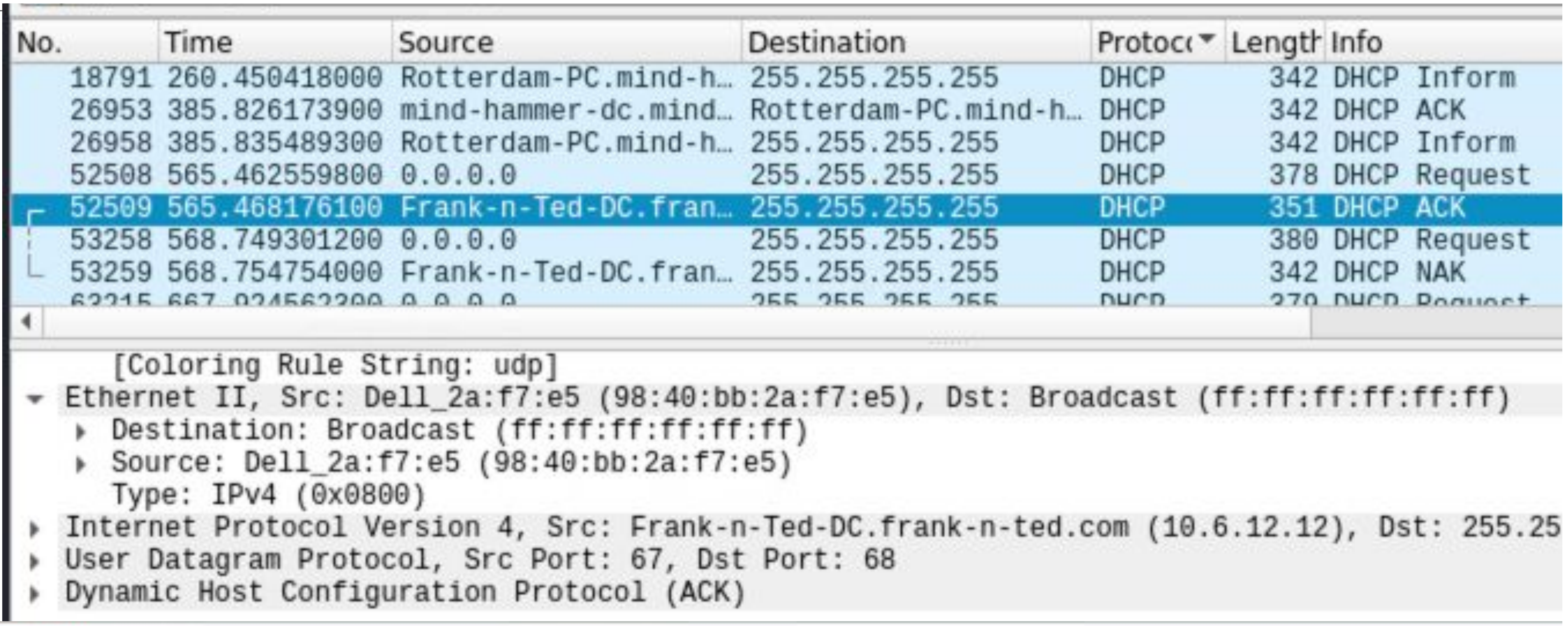


```
http
No.    Time          Source                Destination           Protocol Length Info
 64840 660.984737500 BLANCO-DESKTOP.dogo… cdn.globalsigncdn.c… HTTP      291 GET /rootr1/MEwwSjBIMEYwRDAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpD
 79214 800.715558200 Rotterdam-PC.mind-h… code.ionicframework… HTTP      402 GET /ionicons/2.0.1/css/ionicons.min.css?ver=5.2.2 HTTP/1.1
 32462 403.323287200 DESKTOP-B49J3FD.loc… www.sabethahospital… HTTP      460 GET /getpage.php?name=whatappendixdo HTTP/1.1
 32481 403.502970200 DESKTOP-B49J3FD.loc… www.sabethahospital… HTTP      436 GET /style.php HTTP/1.1
 32499 403.527589400 DESKTOP-B49J3FD.loc… www.sabethahospital… HTTP      471 GET /splash/logo.png HTTP/1.1
 32500 403.535196200 DESKTOP-B49J3FD.loc… www.sabethahospital… HTTP      475 GET /splash/button-2.jpg HTTP/1.1
 32501 403.542749300 DESKTOP-B49J3FD.loc… www.sabethahospital… HTTP      472 GET /common_js/common_css.php?c=3281&mt=1573231401 HTTP/1.1
 32502 403.549771900 DESKTOP-B49J3FD.loc… www.sabethahospital… HTTP      439 GET /common_js/start_facebook.js HTTP/1.1

Frame 32462: 460 bytes on wire (3680 bits), 460 bytes captured (3680 bits) on interface eth0, id 0
Ethernet II, Src: Dell_95:58:b4 (90:b1:1c:95:58:b4), Dst: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
Internet Protocol Version 4, Src: DESKTOP-B49J3FD.local (10.11.11.195), Dst: www.sabethahospital.com (12.133.50.21)
Transmission Control Protocol, Src Port: 50138, Dst Port: 80, Seq: 1, Ack: 1, Len: 406
Hypertext Transfer Protocol
  GET /getpage.php?name=whatappendixdo HTTP/1.1\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US\r\n
  Upgrade-Insecure-Requests: 1\r\n
```

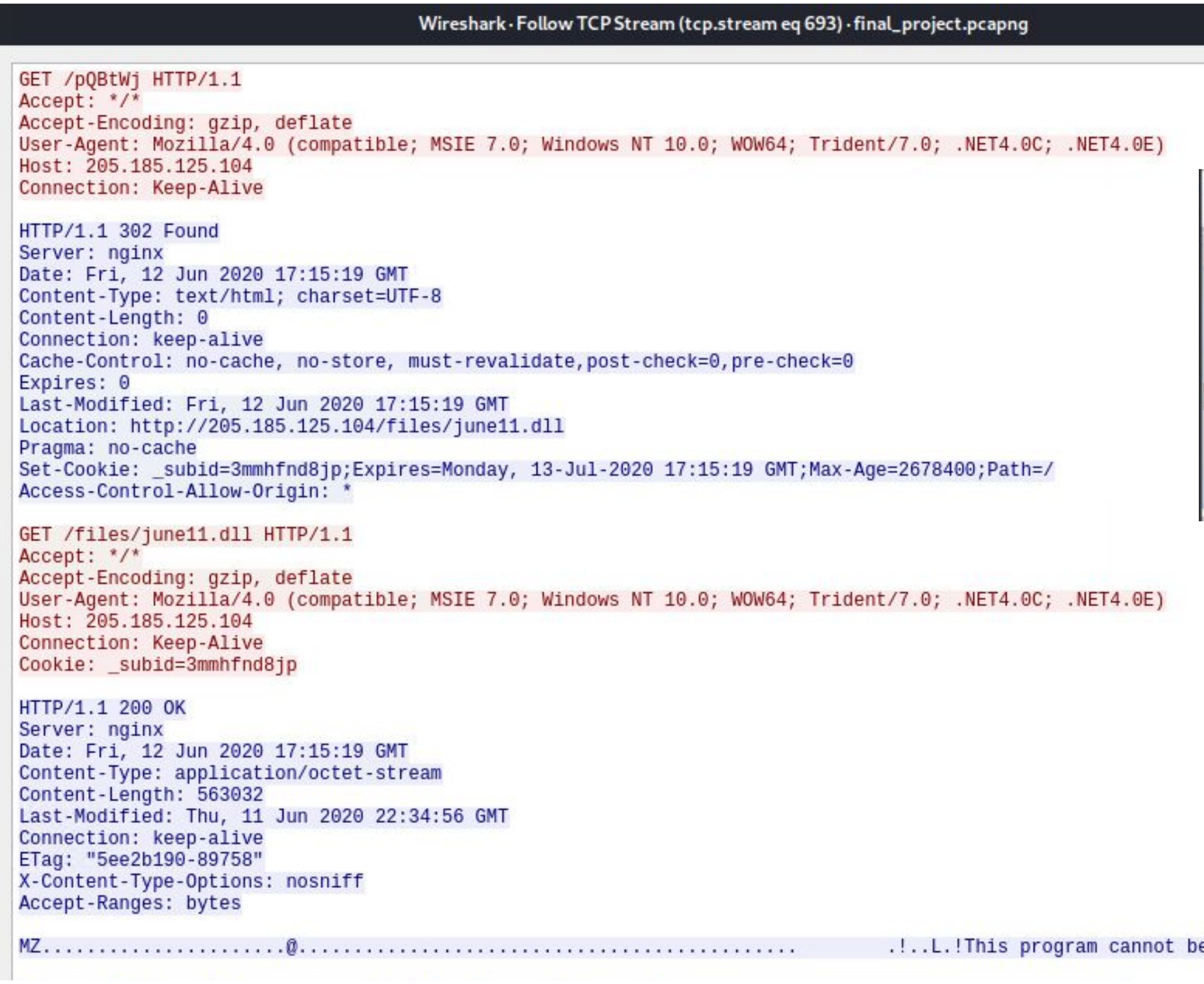
Malicious Activity

Stealing Company Time and Downloading Malware

- Created a private web server on the corporate network named frank-n-ted.com.
- Protocols observed: DHCP, HTTP, and TCP
- **June11.dll** trojan file was downloaded to the computer that accessed Frank-n-Ted.com, IP address 10.6.12.203, from the source IP 205.185.125.104.

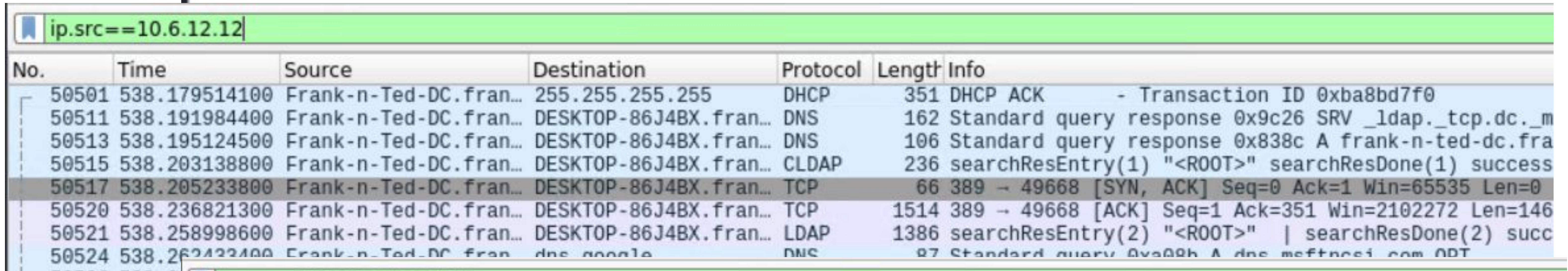


```
No.    Time          Source                   Destination              Protocol  Length Info
18791 260.450418000 Rotterdam-PC.mind-h…  255.255.255.255           DHCP        342 DHCP Inform
26953 385.826173900 mind-hammer-dc.mind…  Rotterdam-PC.mind-h…      DHCP        342 DHCP ACK
26958 385.835489300 Rotterdam-PC.mind-h…  255.255.255.255           DHCP        342 DHCP Inform
52508 565.462559800 0.0.0.0               255.255.255.255           DHCP        378 DHCP Request
52509 565.468176100 Frank-n-Ted-DC.fran…  255.255.255.255           DHCP        351 DHCP ACK
53258 568.749301200 0.0.0.0               255.255.255.255           DHCP        380 DHCP Request
53259 568.754754000 Frank-n-Ted-DC.fran…  255.255.255.255           DHCP        342 DHCP NAK

   [Coloring Rule String: udp]
Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   Source: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: 255.25
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
```



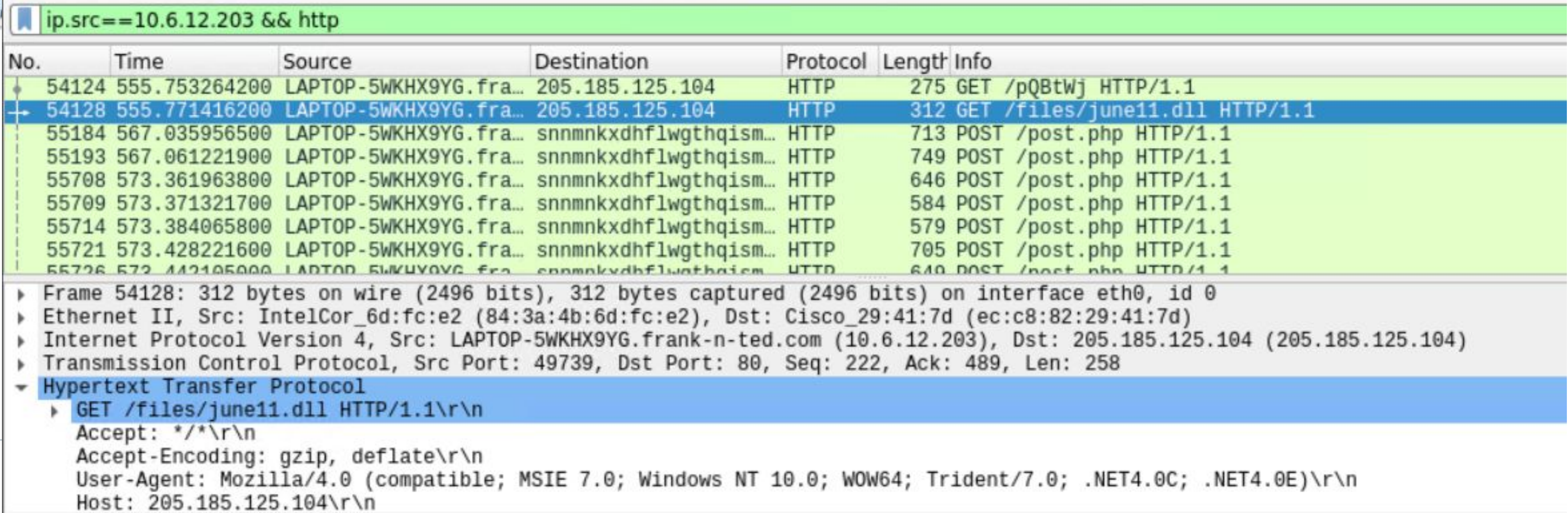
Wireshark · Follow TCP Stream (tcp.stream eq 693) · final_project.pcapng

```
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

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

MZ......................@..............................................        .!..L.!This program cannot be run in DOS mode.
```



ip.src==10.6.12.12

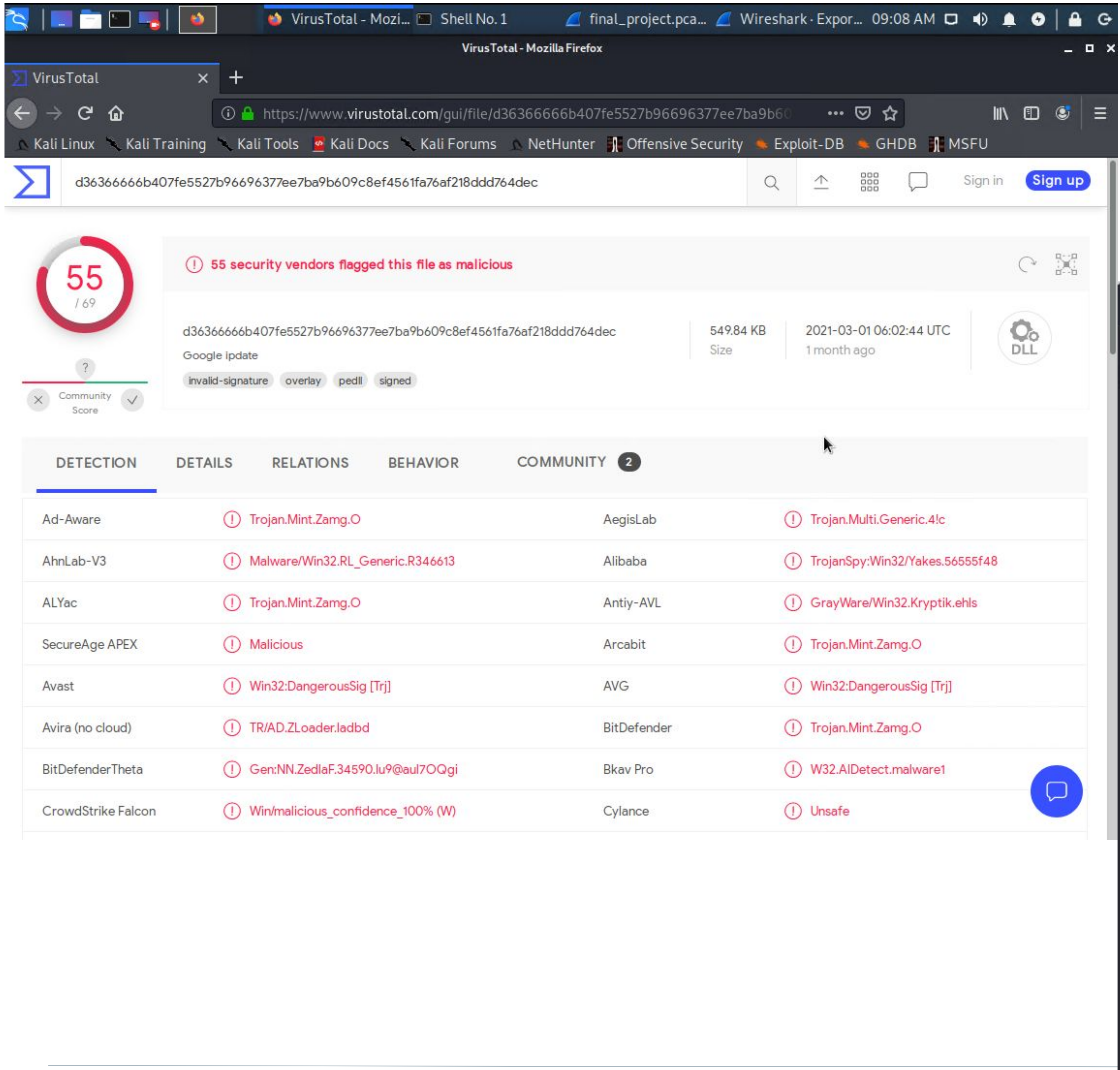
```
No.    Time          Source                   Destination              Protocol  Length Info
50501 538.179514100 Frank-n-Ted-DC.fran…  255.255.255.255           DHCP        351 DHCP ACK       - Transaction ID 0xba8bd7f0
50511 538.191984400 Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.fran…      DNS         162 Standard query response 0x9c26 SRV _ldap._tcp.dc._m
50513 538.195124500 Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.fran…      DNS         106 Standard query response 0x838c A frank-n-ted-dc.fra
50515 538.203138800 Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.fran…      CLDAP       236 searchResEntry(1) "<ROOT>" searchResDone(1) success
50517 538.205233800 Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.fran…      TCP          66 389 → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
50520 538.236821300 Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.fran…      TCP        1514 389 → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=146
50521 538.258998600 Frank-n-Ted-DC.fran…  DESKTOP-86J4BX.fran…      LDAP       1386 searchResEntry(2) "<ROOT>"  | searchResDone(2) succ
50524 538.262433400 Frank-n-Ted-DC.fran…  dns.google                DNS          87 Standard query 0xa08b A dns.msftncsi.com OPT
```



ip.src==10.6.12.203 && http

```
No.    Time          Source                   Destination              Protocol  Length Info
54124 555.753264200 LAPTOP-5WKHX9YG.fra…  205.185.125.104           HTTP        275 GET /pQBtWj HTTP/1.1
54128 555.771416200 LAPTOP-5WKHX9YG.fra…  205.185.125.104           HTTP        312 GET /files/june11.dll HTTP/1.1
55184 567.035956500 LAPTOP-5WKHX9YG.fra…  snnmnkxdhflwgthqism…      HTTP        713 POST /post.php HTTP/1.1
55193 567.061221900 LAPTOP-5WKHX9YG.fra…  snnmnkxdhflwgthqism…      HTTP        749 POST /post.php HTTP/1.1
55708 573.361963800 LAPTOP-5WKHX9YG.fra…  snnmnkxdhflwgthqism…      HTTP        646 POST /post.php HTTP/1.1
55709 573.371321700 LAPTOP-5WKHX9YG.fra…  snnmnkxdhflwgthqism…      HTTP        584 POST /post.php HTTP/1.1
55714 573.384065800 LAPTOP-5WKHX9YG.fra…  snnmnkxdhflwgthqism…      HTTP        579 POST /post.php HTTP/1.1
55721 573.428221600 LAPTOP-5WKHX9YG.fra…  snnmnkxdhflwgthqism…      HTTP        705 POST /post.php HTTP/1.1
55726 573.442105000 LAPTOP-5WKHX9YG.fra…  snnmnkxdhflwgthqism…      HTTP        649 POST /post.php HTTP/1.1

Frame 54128: 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: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (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
```

Stealing Company Time and Downloading Malware



https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b60

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

55 / 69

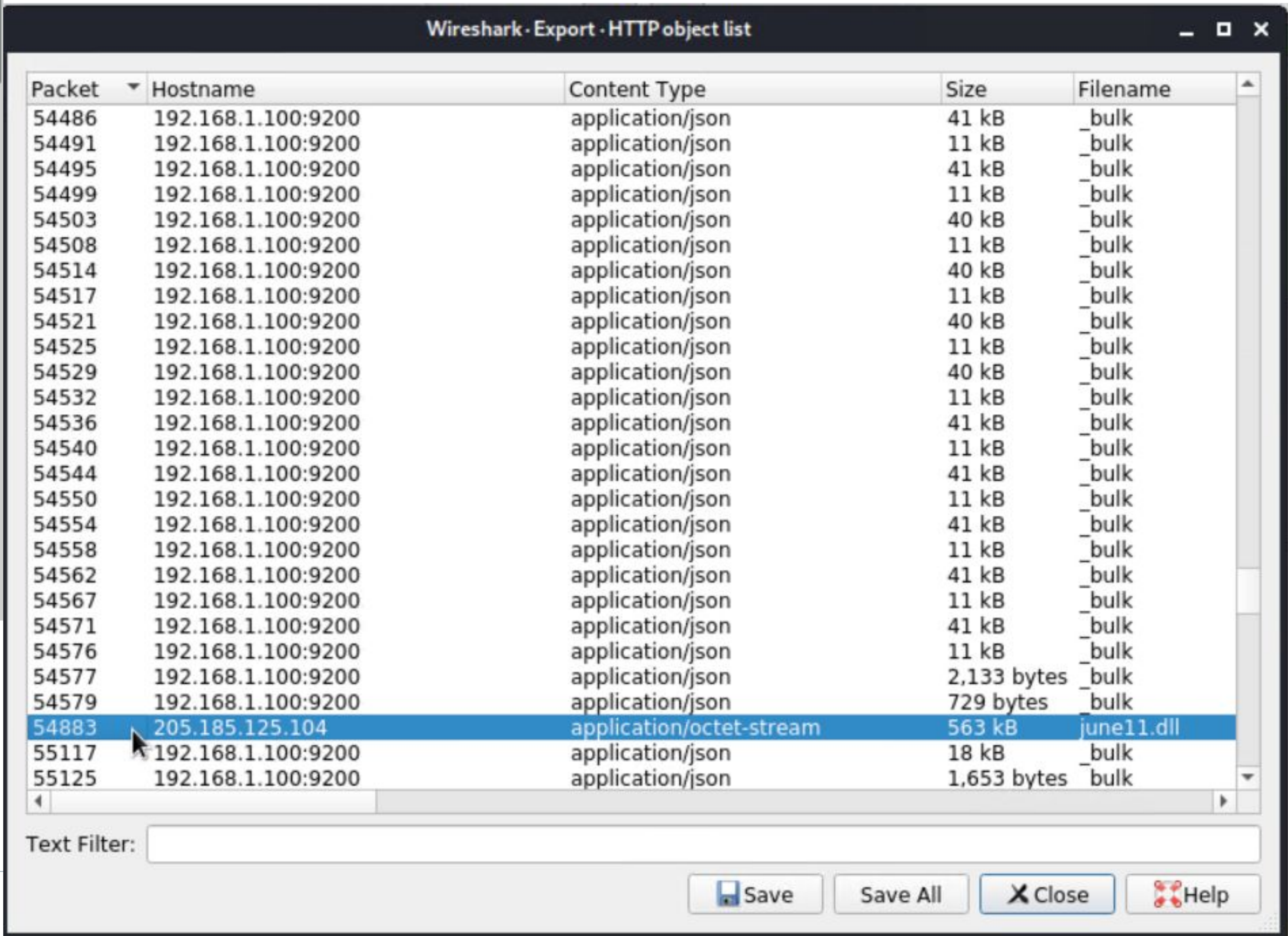
55 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Google ipdate
invalid-signature overlay pedll signed

549.84 KB
Size

2021-03-01 06:02:44 UTC
1 month ago

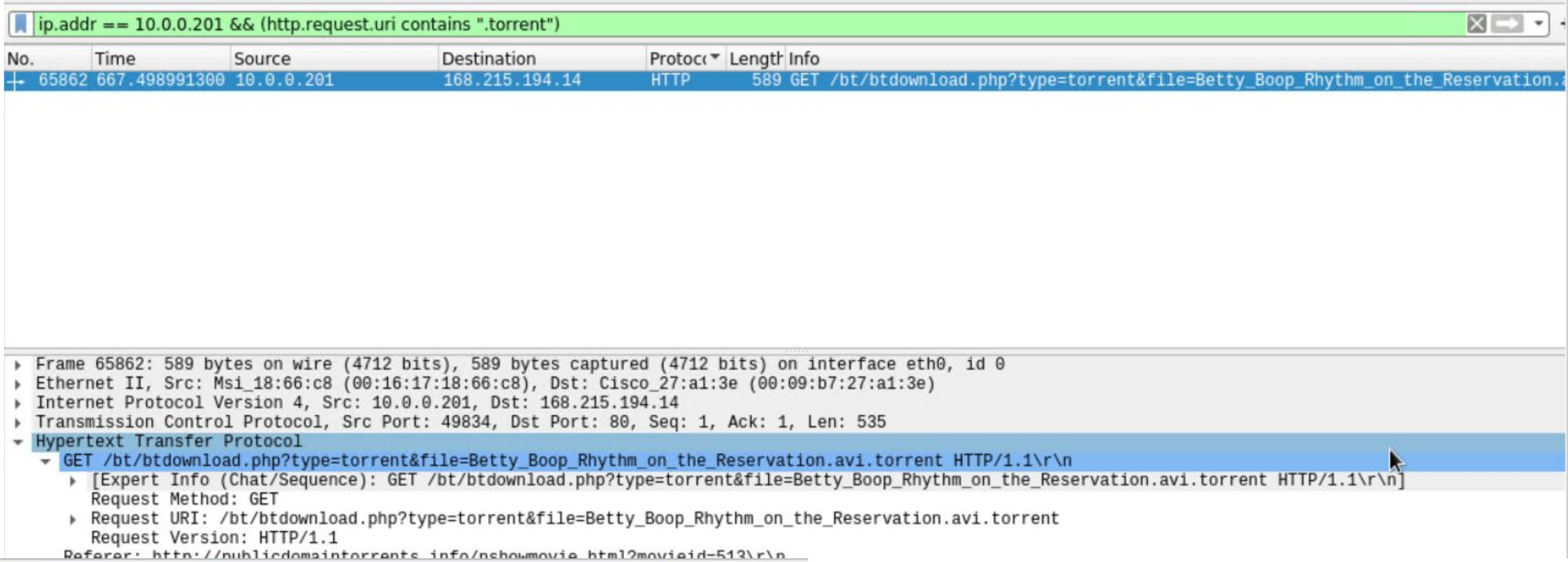
Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	Trojan.Multi.Generic.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
SecureAge APEX	Malicious	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34590.lu9@aul7OQgi	Bkav Pro	W32.AIDetect.malware1
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe



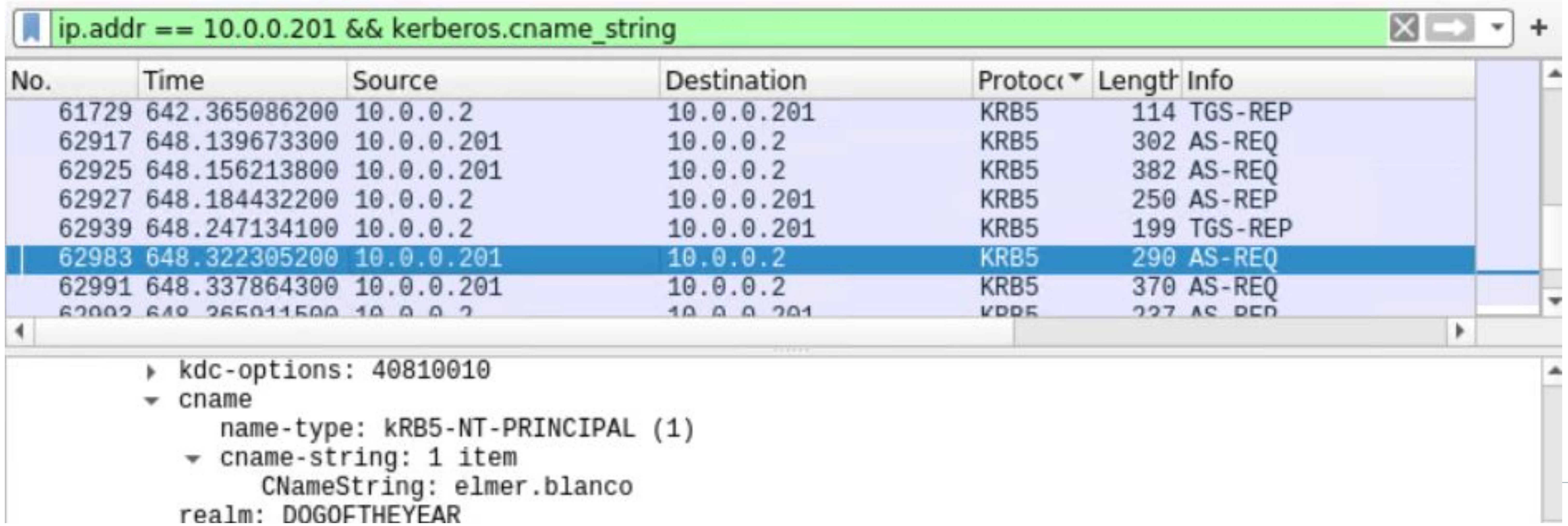
Packet	Hostname	Content Type	Size	Filename
54486	192.168.1.100:9200	application/json	41 kB	_bulk
54491	192.168.1.100:9200	application/json	11 kB	_bulk
54495	192.168.1.100:9200	application/json	41 kB	_bulk
54499	192.168.1.100:9200	application/json	11 kB	_bulk
54503	192.168.1.100:9200	application/json	40 kB	_bulk
54508	192.168.1.100:9200	application/json	11 kB	_bulk
54514	192.168.1.100:9200	application/json	40 kB	_bulk
54517	192.168.1.100:9200	application/json	11 kB	_bulk
54521	192.168.1.100:9200	application/json	40 kB	_bulk
54525	192.168.1.100:9200	application/json	11 kB	_bulk
54529	192.168.1.100:9200	application/json	40 kB	_bulk
54532	192.168.1.100:9200	application/json	11 kB	_bulk
54536	192.168.1.100:9200	application/json	41 kB	_bulk
54540	192.168.1.100:9200	application/json	11 kB	_bulk
54544	192.168.1.100:9200	application/json	41 kB	_bulk
54550	192.168.1.100:9200	application/json	11 kB	_bulk
54554	192.168.1.100:9200	application/json	41 kB	_bulk
54558	192.168.1.100:9200	application/json	11 kB	_bulk
54562	192.168.1.100:9200	application/json	41 kB	_bulk
54567	192.168.1.100:9200	application/json	11 kB	_bulk
54571	192.168.1.100:9200	application/json	41 kB	_bulk
54576	192.168.1.100:9200	application/json	11 kB	_bulk
54577	192.168.1.100:9200	application/json	2,133 bytes	_bulk
54579	192.168.1.100:9200	application/json	729 bytes	_bulk
54883	205.185.125.104	application/octet-stream	563 kB	june11.dll
55117	192.168.1.100:9200	application/json	18 kB	_bulk
55125	192.168.1.100:9200	application/json	1,653 bytes	_bulk

Torrenting/Illegal Downloading

- Torrent activity was observed that was illegally used to download copyrighted material.
- Protocols observed: HTTP and Kerberos
- User Activity: The user, elmer.blanco downloaded the torrent file Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



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

No.    Time           Source       Destination     Protocol Length Info
65862  667.498991300  10.0.0.201   168.215.194.14  HTTP     589    GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.a

▸ Frame 65862: 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
    ▸ [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
```



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

No.    Time           Source       Destination  Protocol Length Info
61729  642.365086200  10.0.0.2     10.0.0.201   KRB5     114    TGS-REP
62917  648.139673300  10.0.0.201   10.0.0.2     KRB5     302    AS-REQ
62925  648.156213800  10.0.0.201   10.0.0.2     KRB5     382    AS-REQ
62927  648.184432200  10.0.0.2     10.0.0.201   KRB5     250    AS-REP
62939  648.247134100  10.0.0.2     10.0.0.201   KRB5     199    TGS-REP
62983  648.322305200  10.0.0.201   10.0.0.2     KRB5     290    AS-REQ
62991  648.337864300  10.0.0.201   10.0.0.2     KRB5     370    AS-REQ
62993  648.365911500  10.0.0.2     10.0.0.201   KRB5     227    AS-REP

    ▸ kdc-options: 40810010
    ▾ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
          CNameString: elmer.blanco
    realm: DOGOFTHEYEAR
```

The End