Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

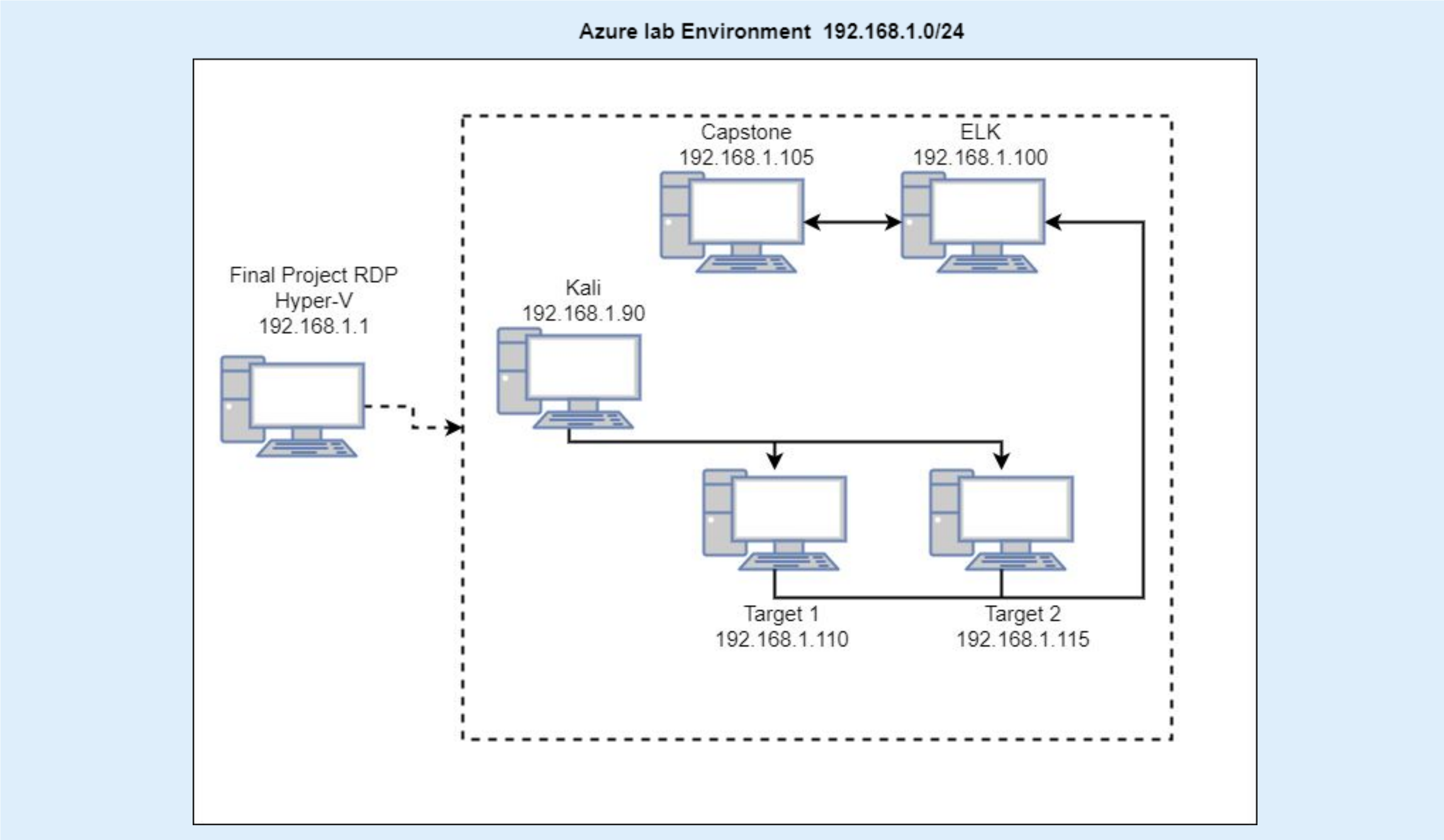
Presentation by:
James Byford, Daniela Lugo, Zaid Zuhair

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Linux 2.6
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux Ubuntu 4.0.3
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux 3.2 - 4.9
Hostname: Target 1

IPv4: 192.168.1.105
OS: Linux Ubuntu protocol 2.0
Hostname: Capstone

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Nmap and User Enumeration	Using nmap we were able to discover open ports on the network.	We were able to find vulnerabilities with the open ports and plan attacks accordingly.
Weak user passwords	Easily guessed password	Gained unauthorized access to system and files
Unsalted user passwords	wpscan was utilized in order to gain username information	We were able to use the username found to gain access to the web server.
MySQL Data Exfiltration	Browsing through the MySQL database we were able to view various tables and databases from the wordpress site.	This allowed us to view the hashes for certain users passwords.
Wrong configuration of User privileges for privilege escalation	One of the users had sudo access for python.	Using sudo with python we were able to run a python script to gain a root shell.

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 166.62.111.64 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	TCP (88.5%) UDP (11.2%) ARP (0.2%)	Three most common protocols on the network.
# of Unique IP Addresses	IPv4 - 877	Count of observed IP addresses.
Subnets	172.16.4.0/24 185.243.115.0/24 10.0.0.0/24 10.6.13.0/24	Observed subnet ranges.
# of Malware Species	2 pQBtWj & 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

- Watching various things on Youtube
- Visiting the Sabetha Hospital website
- Shopping for toys and records

Suspicious Activity

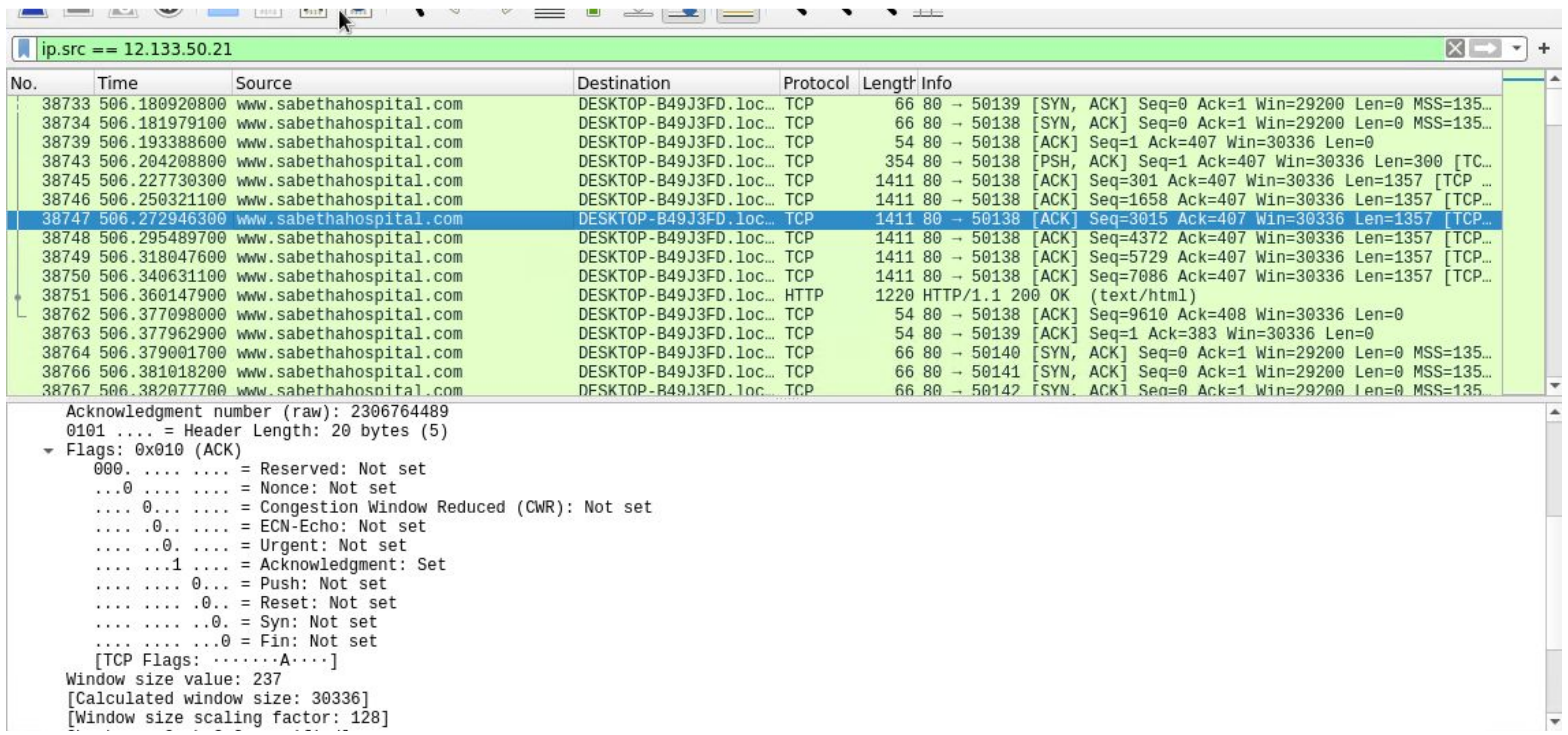
- Downloaded Trojan malware
  - June11.dll & pQBtWJ (webhook)
- Bought something from “cardboardspaceshiptoys.com”
- Visited a random website “snnmnkxdhflwgthqismb.com”
  - This site had multiple POST requests.
- Illegal Download of “Betty_Boop_Rythm_on_the_Reservation.avi.torrent”
- The ip 185.243.115.84 which is also (b569023.green.mattingsolutions.co)
  - This is labeled as malicious by some security vendors.

Normal Activity

Visiting Sabetha Hospital Site

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - TCP
  - HTTP
- What, specifically, was the user doing? Which site were they browsing?
  - The user visited Sabetha Hospital site (12.133.50.21)
- Looking into the packets, we couldn't find anything abnormal.

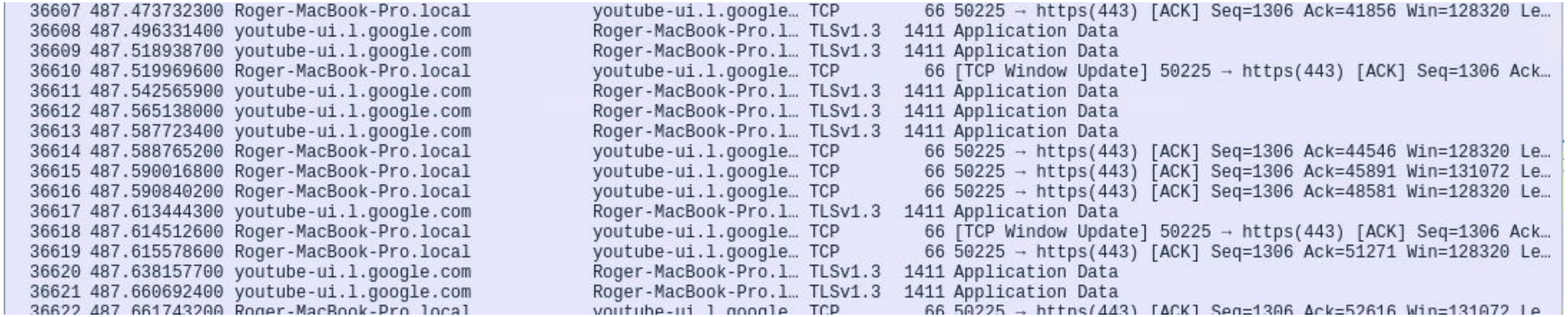


```
ip.src == 12.133.50.21

No.   Time          Source                     Destination            Protocol Length Info
38733 506.180920800 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        66 80 → 50139 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=135…
38734 506.181979100 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        66 80 → 50138 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=135…
38739 506.193388600 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        54 80 → 50138 [ACK] Seq=1 Ack=407 Win=30336 Len=0
38743 506.204208800 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP       354 80 → 50138 [PSH, ACK] Seq=1 Ack=407 Win=30336 Len=300 [TC…
38745 506.227730300 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP      1411 80 → 50138 [ACK] Seq=301 Ack=407 Win=30336 Len=1357 [TCP …
38746 506.250321100 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP      1411 80 → 50138 [ACK] Seq=1658 Ack=407 Win=30336 Len=1357 [TCP…
38747 506.272946300 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP      1411 80 → 50138 [ACK] Seq=3015 Ack=407 Win=30336 Len=1357 [TCP…
38748 506.295489700 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP      1411 80 → 50138 [ACK] Seq=4372 Ack=407 Win=30336 Len=1357 [TCP…
38749 506.318047600 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP      1411 80 → 50138 [ACK] Seq=5729 Ack=407 Win=30336 Len=1357 [TCP…
38750 506.340631100 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP      1411 80 → 50138 [ACK] Seq=7086 Ack=407 Win=30336 Len=1357 [TCP…
38751 506.360147900 www.sabethahospital.com    DESKTOP-B49J3FD.loc… HTTP     1220 HTTP/1.1 200 OK  (text/html)
38762 506.377098000 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        54 80 → 50138 [ACK] Seq=9610 Ack=408 Win=30336 Len=0
38763 506.377962900 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        54 80 → 50139 [ACK] Seq=1 Ack=383 Win=30336 Len=0
38764 506.379001700 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        66 80 → 50140 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=135…
38766 506.381018200 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        66 80 → 50141 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=135…
38767 506.382077700 www.sabethahospital.com    DESKTOP-B49J3FD.loc… TCP        66 80 → 50142 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=135…

    Acknowledgment number (raw): 2306764489
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x010 (ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Nonce: Not set
       .... 0... .... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...1 .... = Acknowledgment: Set
       .... .... 0... = Push: Not set
       .... .... .0.. = Reset: Not set
       .... .... ..0. = Syn: Not set
       .... .... ...0 = Fin: Not set
       [TCP Flags: ·······A····]
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
```

Watching Youtube

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - TCP
- What, specifically, was the user doing?
  - The user was accessing youtube from his MacBook (Roger-Macbook-Pro - 10.11.11.179)



```
36607 487.473732300 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=1306 Ack=41856 Win=128320 Le…
36608 487.496331400 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36609 487.518938700 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36610 487.519969600 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 [TCP Window Update] 50225 → https(443) [ACK] Seq=1306 Ack…
36611 487.542565900 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36612 487.565138000 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36613 487.587723400 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36614 487.588765200 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=1306 Ack=44546 Win=128320 Le…
36615 487.590016800 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=1306 Ack=45891 Win=131072 Le…
36616 487.590840200 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=1306 Ack=48581 Win=128320 Le…
36617 487.613444300 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36618 487.614512600 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 [TCP Window Update] 50225 → https(443) [ACK] Seq=1306 Ack…
36619 487.615578600 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=1306 Ack=51271 Win=128320 Le…
36620 487.638157700 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36621 487.660692400 youtube-ui.l.google.com           Roger-MacBook-Pro.l… TLSv1.3  1411 Application Data
36622 487.661743200 Roger-MacBook-Pro.local           youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=1306 Ack=52616 Win=131072 Le…
```

- This communication is using TLSv1.3 that is considered secure.

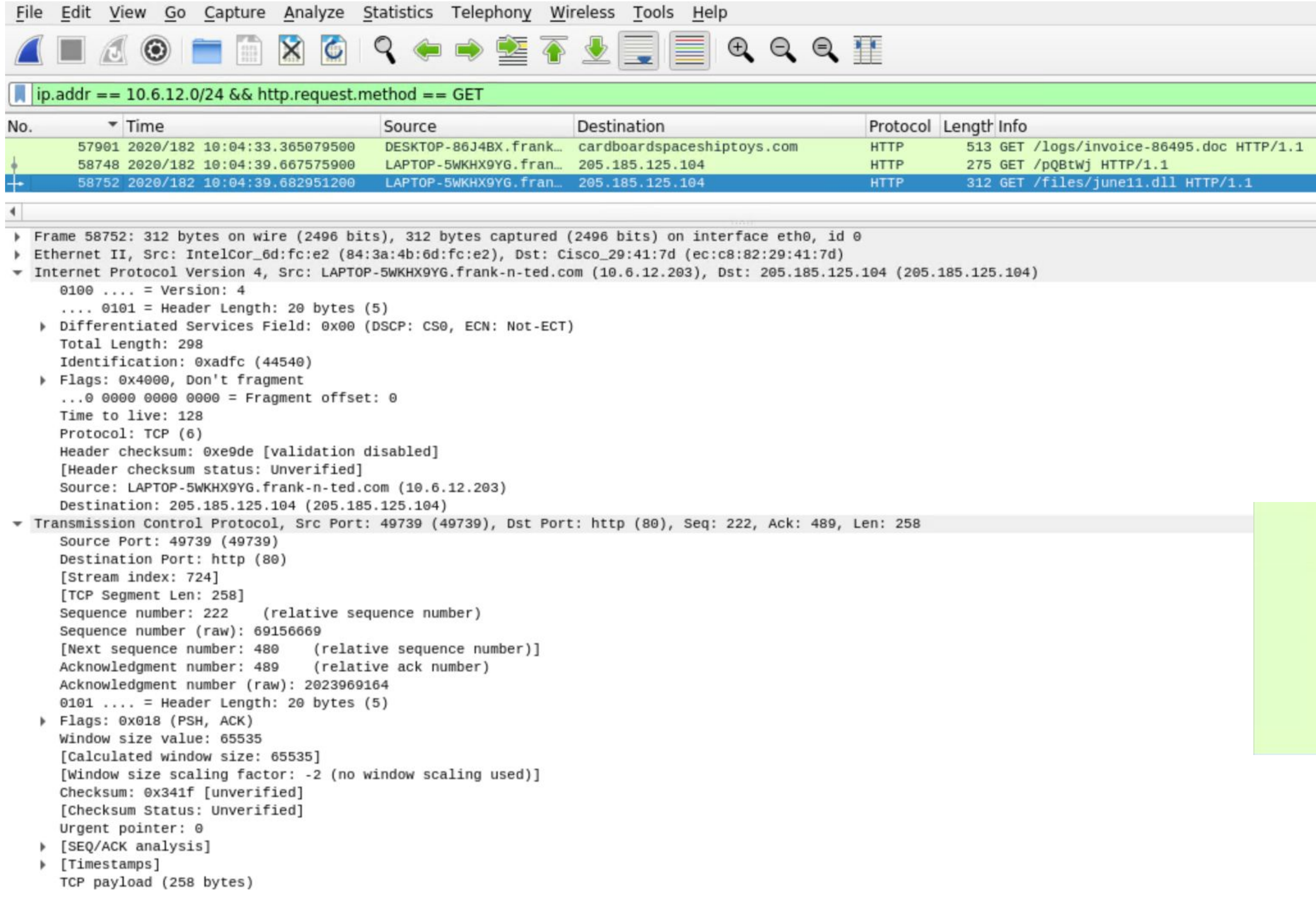
Malicious Activity

Trojan Malware

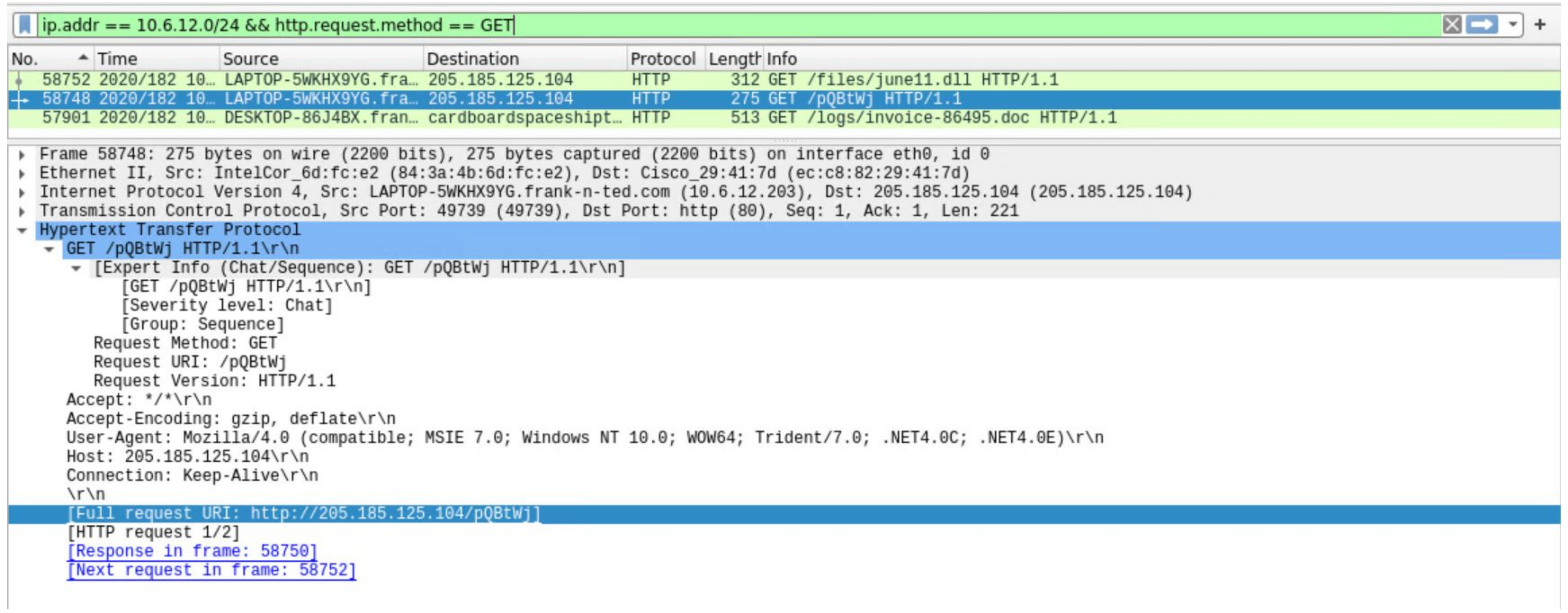
Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - HTTP
  - TCP
- What, specifically, was the user doing? Which site were they browsing?
  - The user made a purchase on cardboardspaceshiptoys.com
  - Downloaded a Trojan malware from 205.185.125.104
  - Multiple POST requests made to snnmnkxdhflwgthqismb.com
- Include a description of any interesting files.
  - The user downloaded a file called “June11.dll” which was a Trojan malware.
  - We also found the link “http://205.185.125.104/pQBtWJ” and using virustotal.com 6 security vendors flagged this URL malicious.
  - Another file found was the invoice from cardboardspaceshiptoys.com.

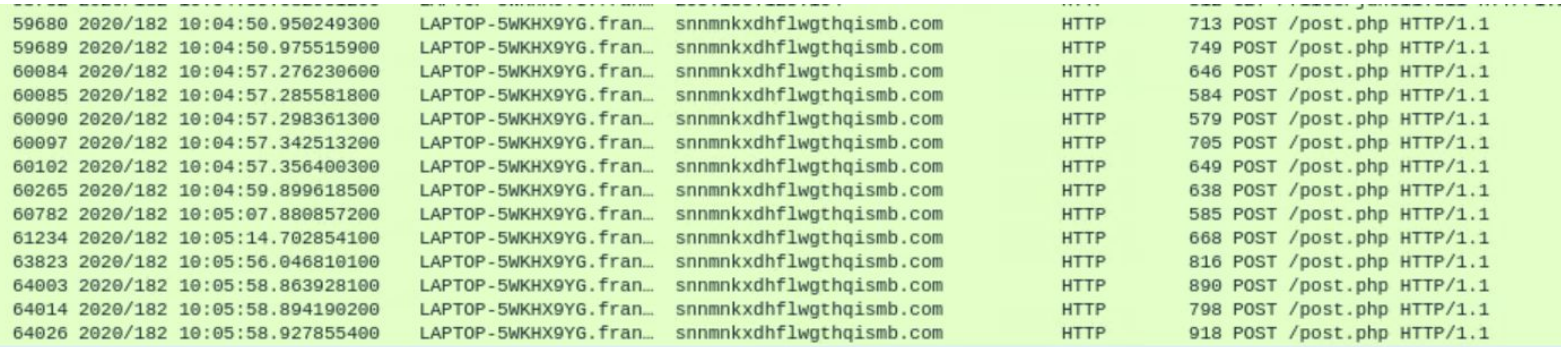
Trojan Malware Screenshots



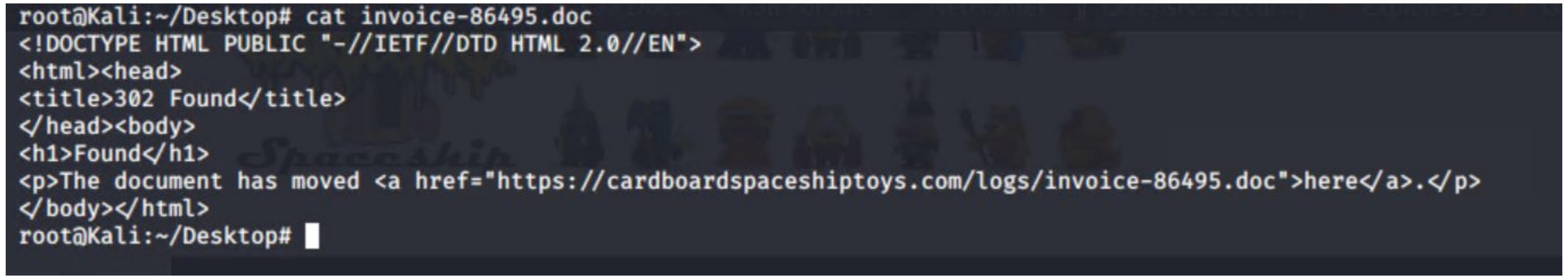
```
ip.addr == 10.6.12.0/24 && http.request.method == GET

No.   Time                         Source                 Destination                  Protocol Length Info
 57901 2020/182 10:04:33.365079500 DESKTOP-86J4BX.frank… cardboardspaceshiptoys.com   HTTP     513 GET /logs/invoice-86495.doc HTTP/1.1
 58748 2020/182 10:04:39.667575900 LAPTOP-5WKHX9YG.fran… 205.185.125.104              HTTP     275 GET /pQBtWj HTTP/1.1
 58752 2020/182 10:04:39.682951200 LAPTOP-5WKHX9YG.fran… 205.185.125.104              HTTP     312 GET /files/june11.dll 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: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 298
    Identification: 0xadfc (44540)
  ▸ Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xe9de [validation disabled]
    [Header checksum status: Unverified]
    Source: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
    Destination: 205.185.125.104 (205.185.125.104)
▾ Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 222, Ack: 489, Len: 258
    Source Port: 49739 (49739)
    Destination Port: http (80)
    [Stream index: 724]
    [TCP Segment Len: 258]
    Sequence number: 222    (relative sequence number)
    Sequence number (raw): 69156669
    [Next sequence number: 480    (relative sequence number)]
    Acknowledgment number: 489    (relative ack number)
    Acknowledgment number (raw): 2023969164
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x341f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (258 bytes)
```



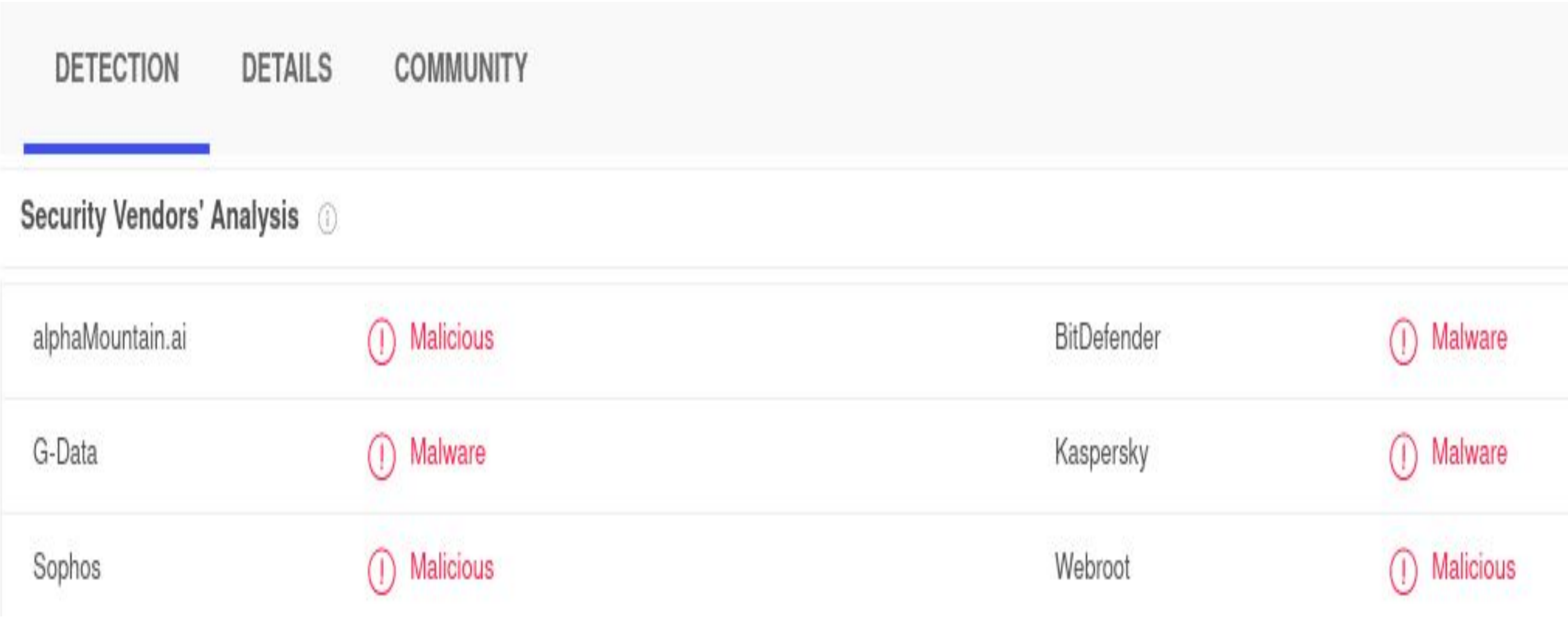
```
ip.addr == 10.6.12.0/24 && http.request.method == GET

No.   Time          Source                Destination              Protocol Length Info
 58752 2020/182 10… LAPTOP-5WKHX9YG.fra… 205.185.125.104          HTTP     312 GET /files/june11.dll HTTP/1.1
 58748 2020/182 10… LAPTOP-5WKHX9YG.fra… 205.185.125.104          HTTP     275 GET /pQBtWj HTTP/1.1
 57901 2020/182 10… DESKTOP-86J4BX.fran… cardboardspaceshipt…     HTTP     513 GET /logs/invoice-86495.doc HTTP/1.1

▸ Frame 58748: 275 bytes on wire (2200 bits), 275 bytes captured (2200 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 (49739), Dst Port: http (80), Seq: 1, Ack: 1, Len: 221
▾ Hypertext Transfer Protocol
  ▾ GET /pQBtWj HTTP/1.1\r\n
    ▾ [Expert Info (Chat/Sequence): GET /pQBtWj HTTP/1.1\r\n]
        [GET /pQBtWj HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /pQBtWj
      Request Version: HTTP/1.1
    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
    \r\n
    [Full request URI: http://205.185.125.104/pQBtWj]
    [HTTP request 1/2]
    [Response in frame: 58750]
    [Next request in frame: 58752]
```



```
59680 2020/182 10:04:50.950249300   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    713 POST /post.php HTTP/1.1
59689 2020/182 10:04:50.975515900   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    749 POST /post.php HTTP/1.1
60084 2020/182 10:04:57.276230600   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    646 POST /post.php HTTP/1.1
60085 2020/182 10:04:57.285581800   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    584 POST /post.php HTTP/1.1
60090 2020/182 10:04:57.298361300   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    579 POST /post.php HTTP/1.1
60097 2020/182 10:04:57.342513200   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    705 POST /post.php HTTP/1.1
60102 2020/182 10:04:57.356400300   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    649 POST /post.php HTTP/1.1
60265 2020/182 10:04:59.899618500   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    638 POST /post.php HTTP/1.1
60782 2020/182 10:05:07.880857200   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    585 POST /post.php HTTP/1.1
61234 2020/182 10:05:14.702854100   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    668 POST /post.php HTTP/1.1
63823 2020/182 10:05:56.046810100   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    816 POST /post.php HTTP/1.1
64003 2020/182 10:05:58.863928100   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    890 POST /post.php HTTP/1.1
64014 2020/182 10:05:58.894190200   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    798 POST /post.php HTTP/1.1
64026 2020/182 10:05:58.927855400   LAPTOP-5WKHX9YG.fran…   snnmnkxdhflwgthqismb.com    HTTP    918 POST /post.php HTTP/1.1
```



```
root@Kali:~/Desktop# cat invoice-86495.doc
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://cardboardspaceshiptoys.com/logs/invoice-86495.doc">here</a>.</p>
</body></html>
root@Kali:~/Desktop# 
```



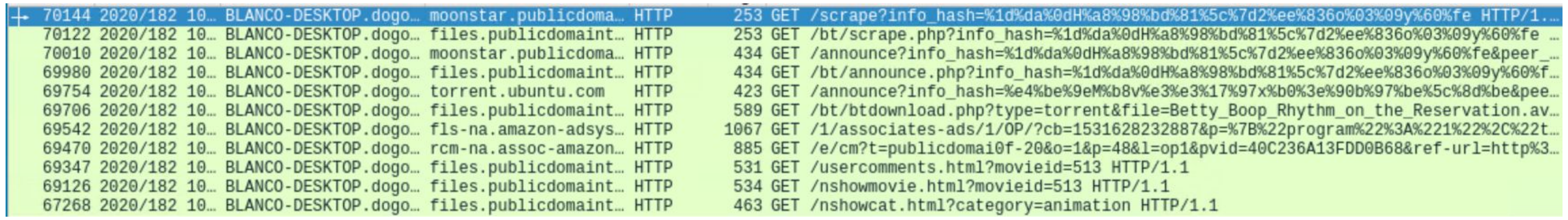
Security Vendors' Analysis

alphaMountain.ai	Malicious	BitDefender	Malware
G-Data	Malware	Kaspersky	Malware
Sophos	Malicious	Webroot	Malicious

Movie Torrent

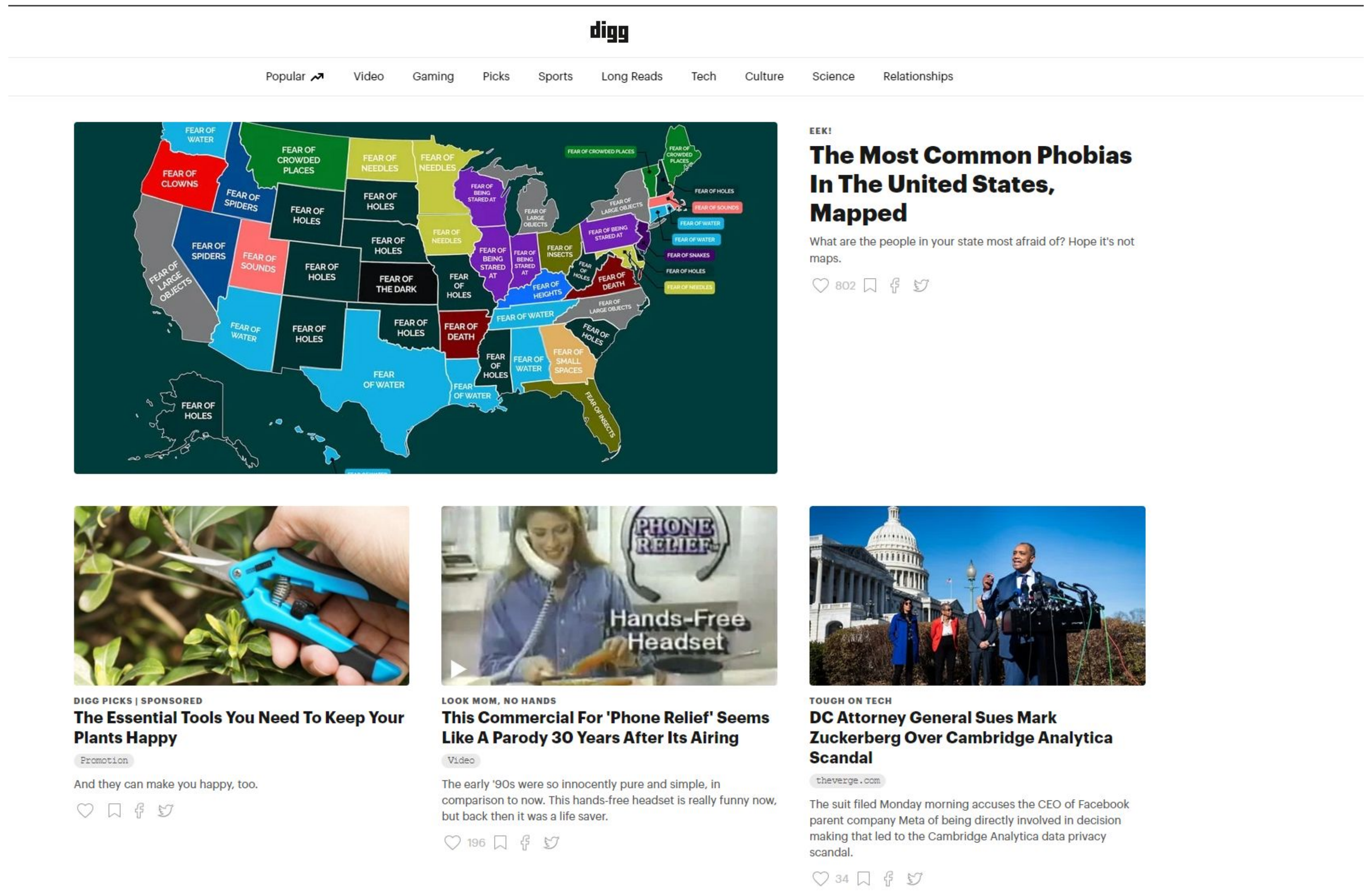
Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - HTTP
  - TCP
  - UDP
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - The user was browsing for movies on “publicdomaintorrents.com”
  - User also visited digg.com, which is a news website.



```
70144 2020/182 10… BLANCO-DESKTOP.dogo… moonstar.publicdoma… HTTP      253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe HTTP/1.…
70122 2020/182 10… BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe …
70010 2020/182 10… BLANCO-DESKTOP.dogo… moonstar.publicdoma… HTTP      434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe&peer_…
69980 2020/182 10… BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%f…
69754 2020/182 10… BLANCO-DESKTOP.dogo… torrent.ubuntu.com   HTTP      423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be&pee…
69706 2020/182 10… BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.av…
69542 2020/182 10… BLANCO-DESKTOP.dogo… fls-na.amazon-adsys… HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22t…
69470 2020/182 10… BLANCO-DESKTOP.dogo… rcm-na.assoc-amazon… HTTP      885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-url=http%3…
69347 2020/182 10… BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      531 GET /usercomments.html?movieid=513 HTTP/1.1
69126 2020/182 10… BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      534 GET /nshowmovie.html?movieid=513 HTTP/1.1
67268 2020/182 10… BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      463 GET /nshowcat.html?category=animation HTTP/1.1
```

- Include a description of any interesting files.
  - The user downloaded a file called “Betty_Boop_Rhythm_on_the_Reservation.avi.torrent”



EEK!

The Most Common Phobias In The United States, Mapped

What are the people in your state most afraid of? Hope it's not maps.

802

DIGG PICKS | SPONSORED

The Essential Tools You Need To Keep Your Plants Happy

Promotion

And they can make you happy, too.

LOOK MOM, NO HANDS

This Commercial For 'Phone Relief' Seems Like A Parody 30 Years After Its Airing

Video

The early '90s were so innocently pure and simple, in comparison to now. This hands-free headset is really funny now, but back then it was a life saver.

196

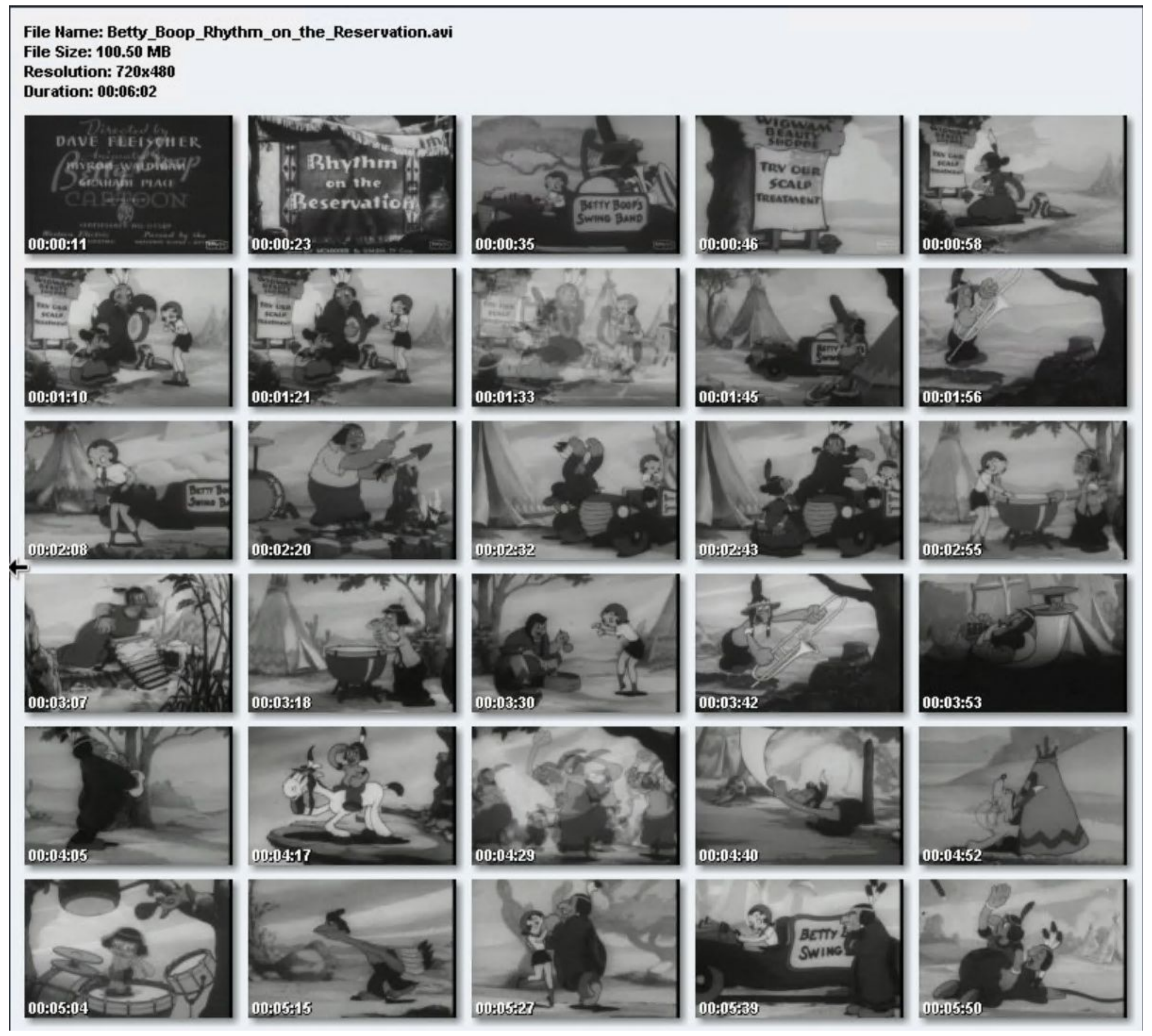
TOUGH ON TECH

DC Attorney General Sues Mark Zuckerberg Over Cambridge Analytica Scandal

theverge.com

The suit filed Monday morning accuses the CEO of Facebook parent company Meta of being directly involved in decision making that led to the Cambridge Analytica data privacy scandal.

34



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

The End