Network Forensic Analysis Report Done
By: Darrel Mills SOC

Darrel Mills, Security Engineers for X-Corp, supports the SOC team to analyze some discrepancies with alerting in the Kibana system and the manager has asked us to investigate. Yesterday our team confirmed that all the new alerts are working fine. Today we are going to monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system and report back to the SOC manager and the Engineer Manager with all our findings.

.

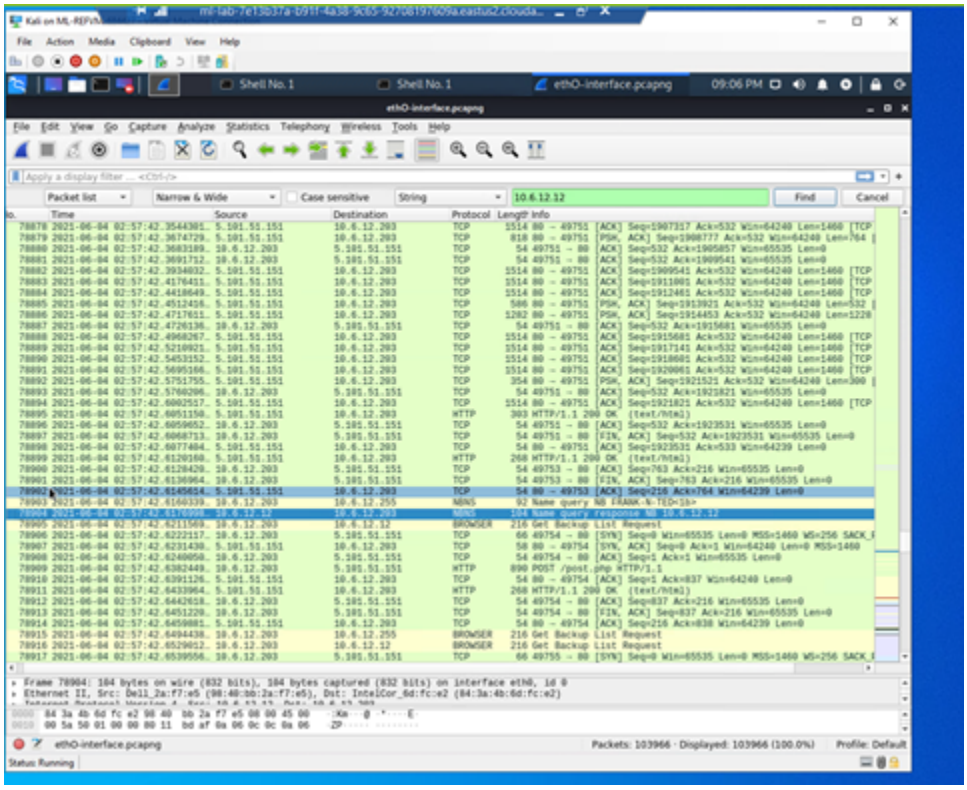
Time Thieves

You must inspect your traffic capture to answer the following questions:

Report was done by: Darrel Mills Cybersecurity Specialist

1. What is the domain name of the users' custom site?

Answer: Frank-n-ted.com IP 10.6.12.12 destination.



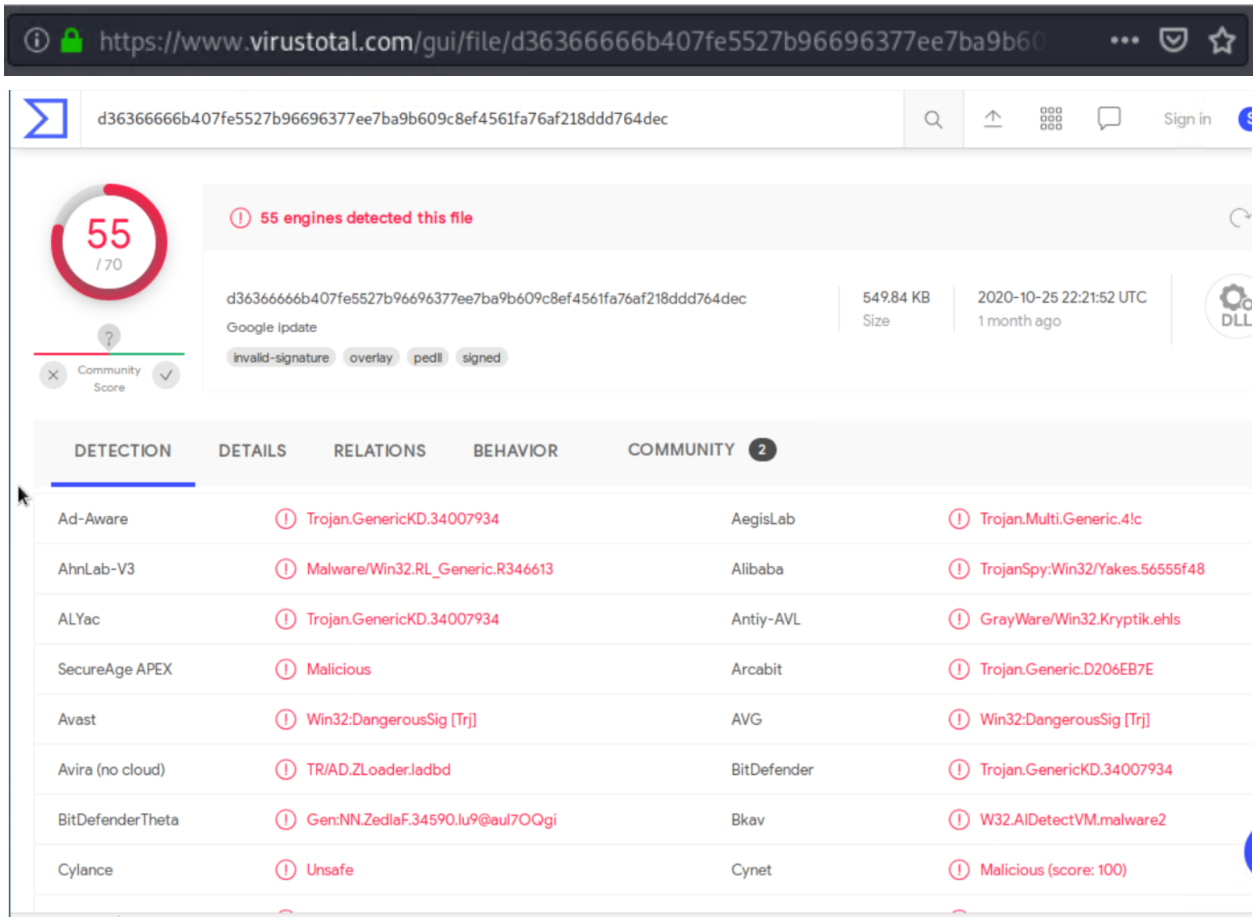
2. What is the IP address of the Domain Controller (DC) of the AD network?

Answer: 10.6.12.157

3. What is the name of the malware downloaded to the 10.6.12.203 machine?
Answer: june11.dll HTTP/1.1

- Once you have found the file, export it to your Kali machine's desktop.

4. Upload the file to VirusTotal.com (https://www.virustotal.com/gui/).
5. What kind of malware is this classified as?
Answer: Malware was a Trojan



Vulnerable Windows Machine

- **Network range 172.16.4.0/24**
- **IP 10.6.12.12 Frank-n-Ted-DC**
- **Domain mind-hammer.net is part of the infected computer**
- **DC Network lives at 172.16.4.4 and is named Mind-Hammer-DC.**

- **Network standard Gateway and Broadcast addresses.**

1. Find the following information about the infected Windows machine:

- Host name ROTTERDAMPC

- IP address 172.16.4.205

- MAC address 00:59:07:b0:63:a4

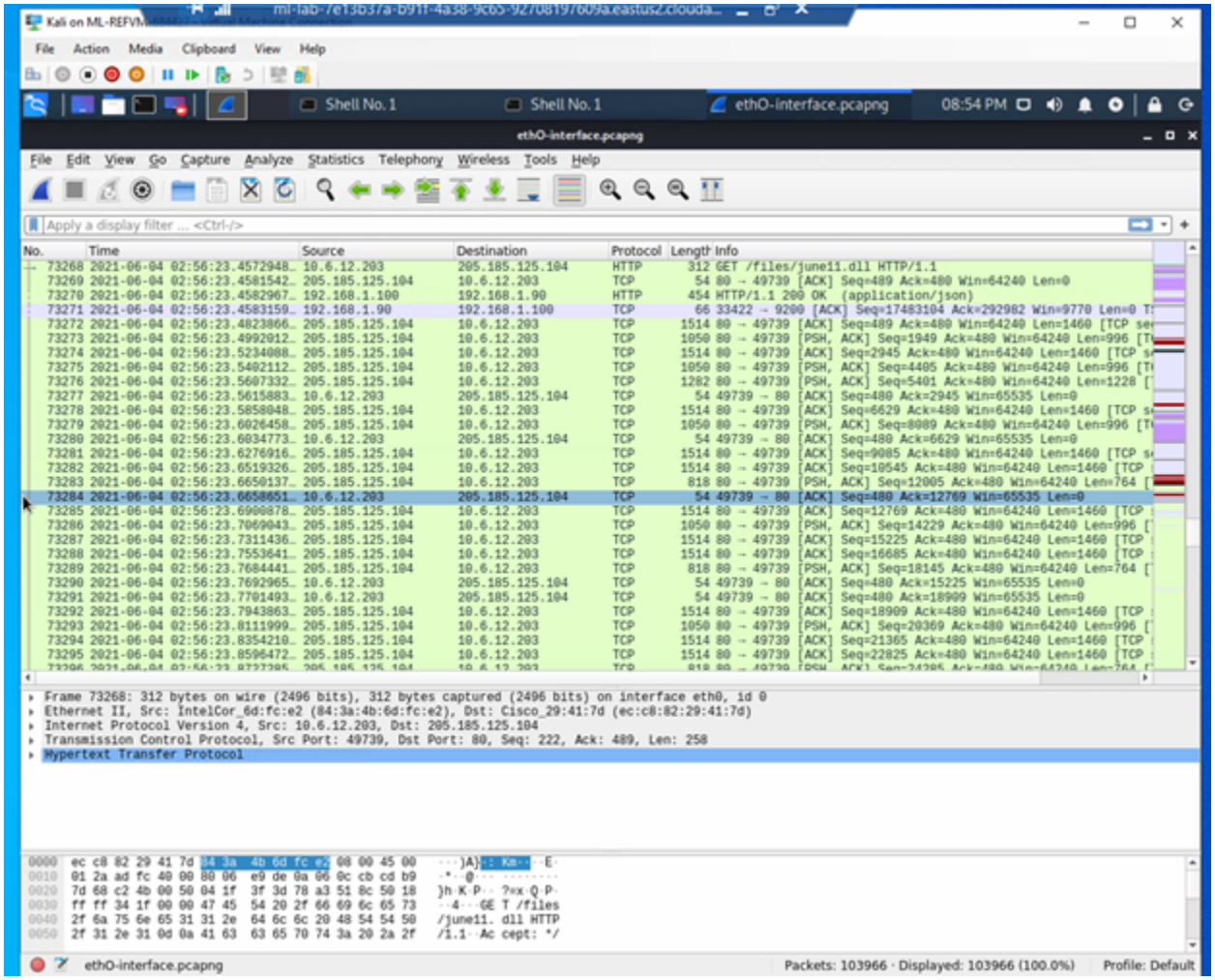
Report was done by: Darrel Mills Cybersecurity Specialist

2. What is the username of the Windows user whose computer is infected?

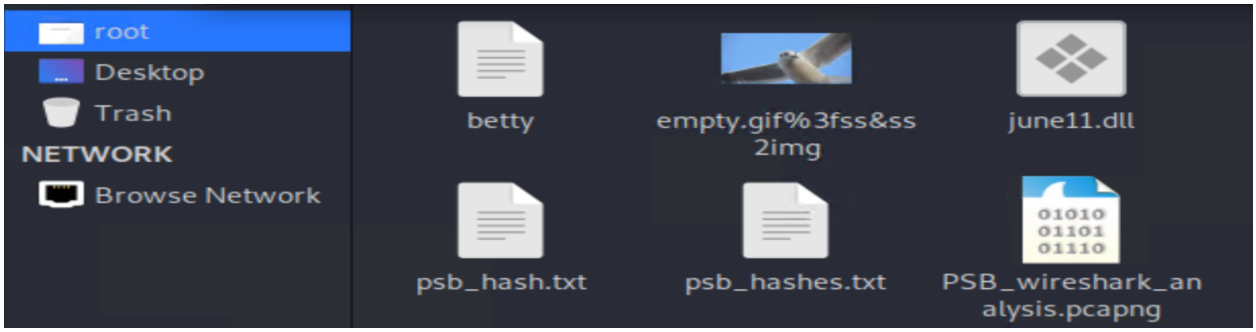
Answer: Mind-Hammer-DC

3. What are the IP addresses used in the actual infection traffic?

Answer: 205.185.125.104



4. As a bonus, retrieve the desktop background of the Windows host.below:



Report was done by: Darrel Mills Cybersecurity Specialist

Illegal Downloads: IT found users torrenting on the network. Darrel was instructed that the Security Team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringements.

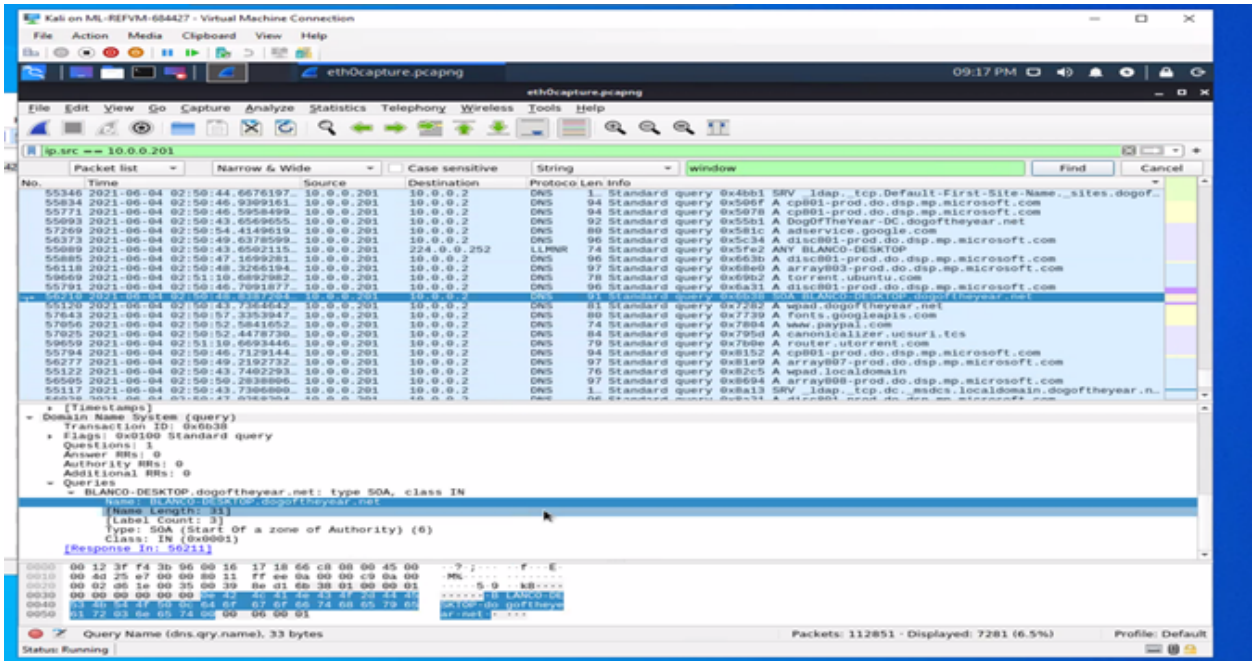
1. Find the following information about the machine with IP address `10.0.0.201`:

- MAC address: 00:16:17:18:66:c8

- Windows username: PC BLANCODESKTOP

- OS version: Windows. NT 10.0; Win64; x 64

_ Host: Publicdomaintorrents.info/r/n

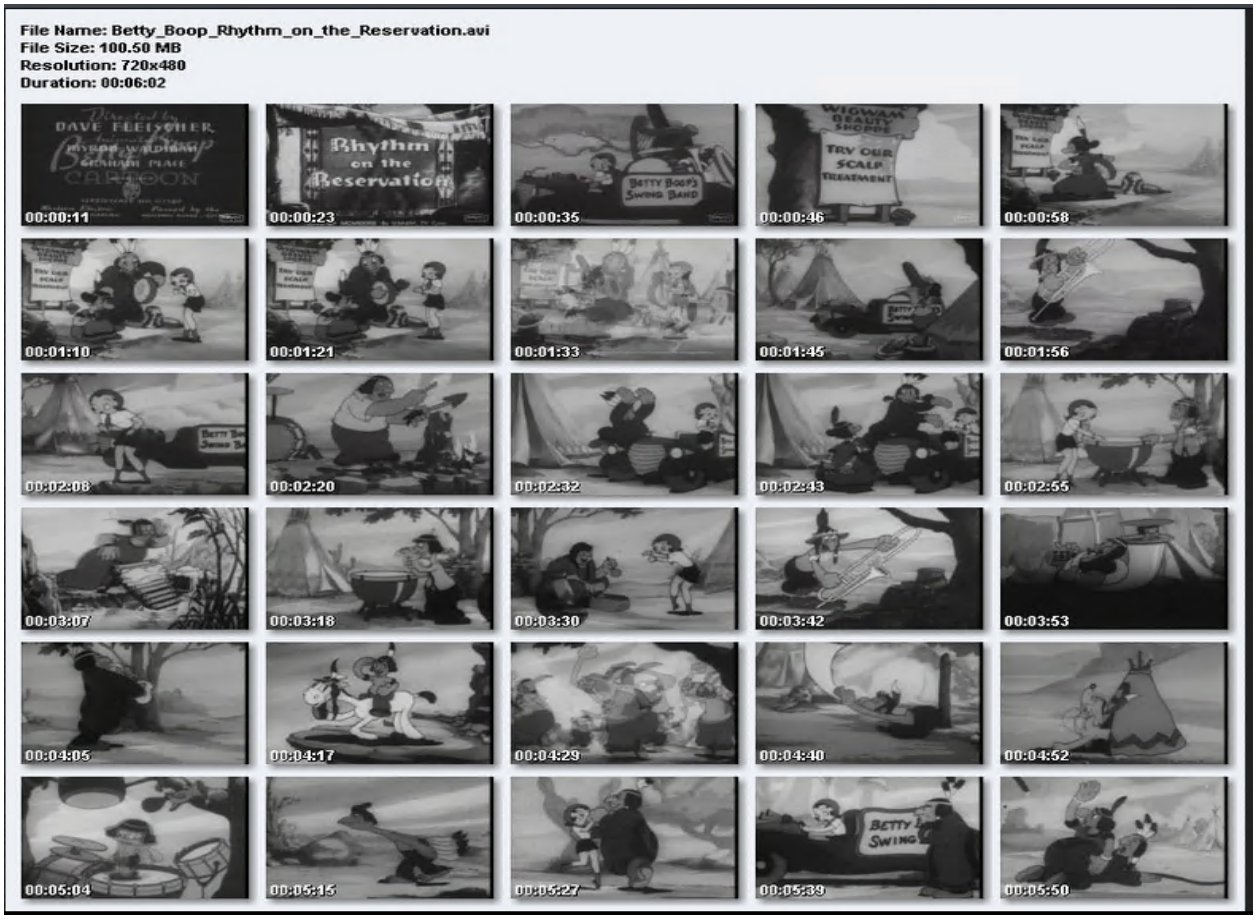


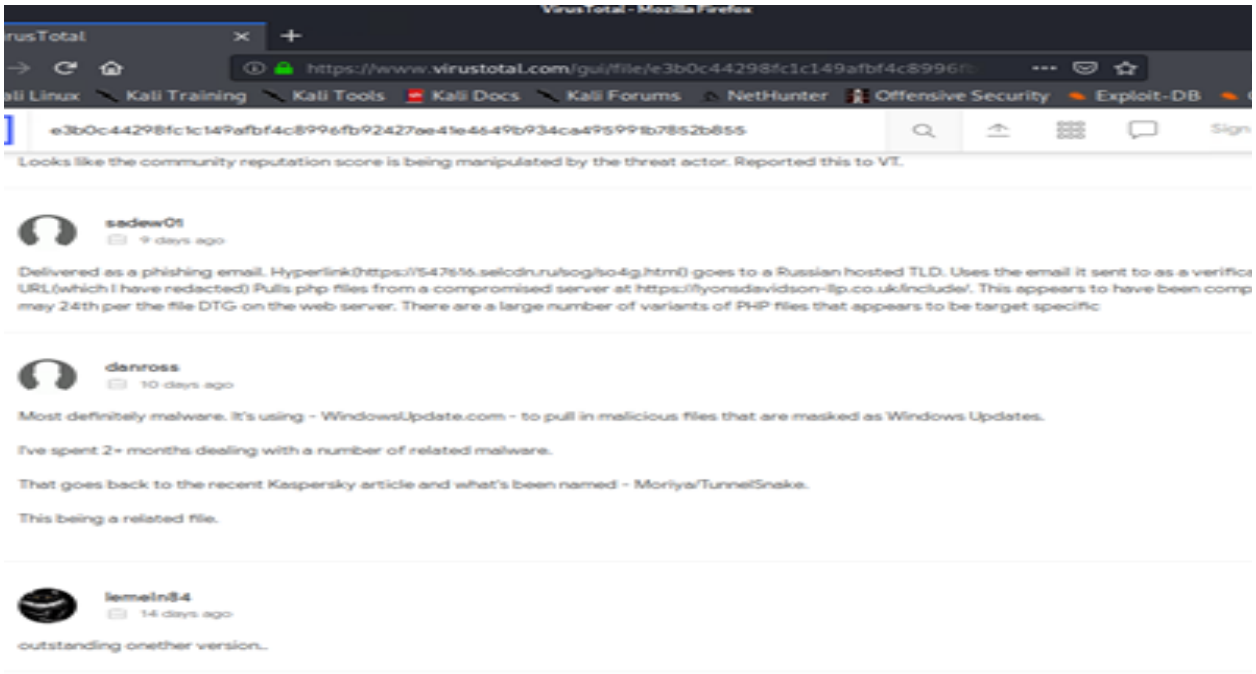
2. Which torrent file did the user download?

Answer: Betty_Boop_Rhythm_on_the_Reservation.avi

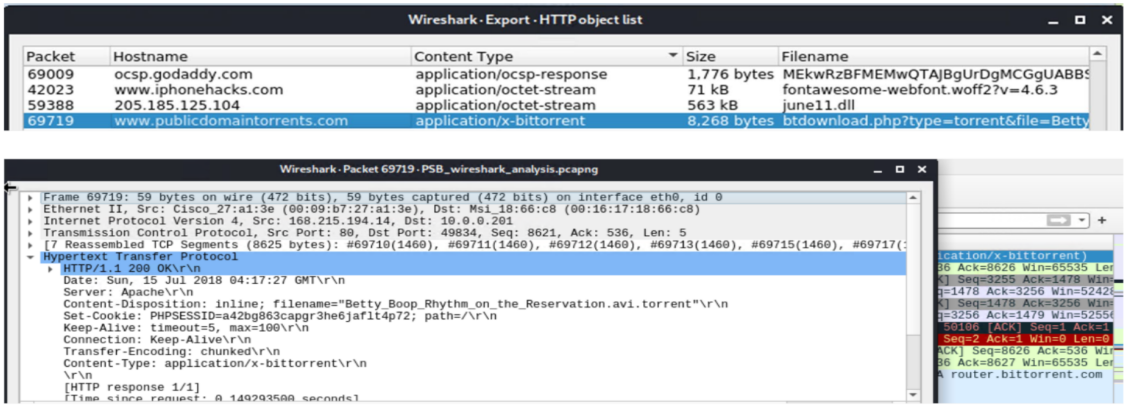
Trojan Malware

And carrys the malicious package.





Report was done by: Darrel Mills Cybersecurity Specialist



Wireshark · Endpoints · PSB_wireshark_analysis.pcapng

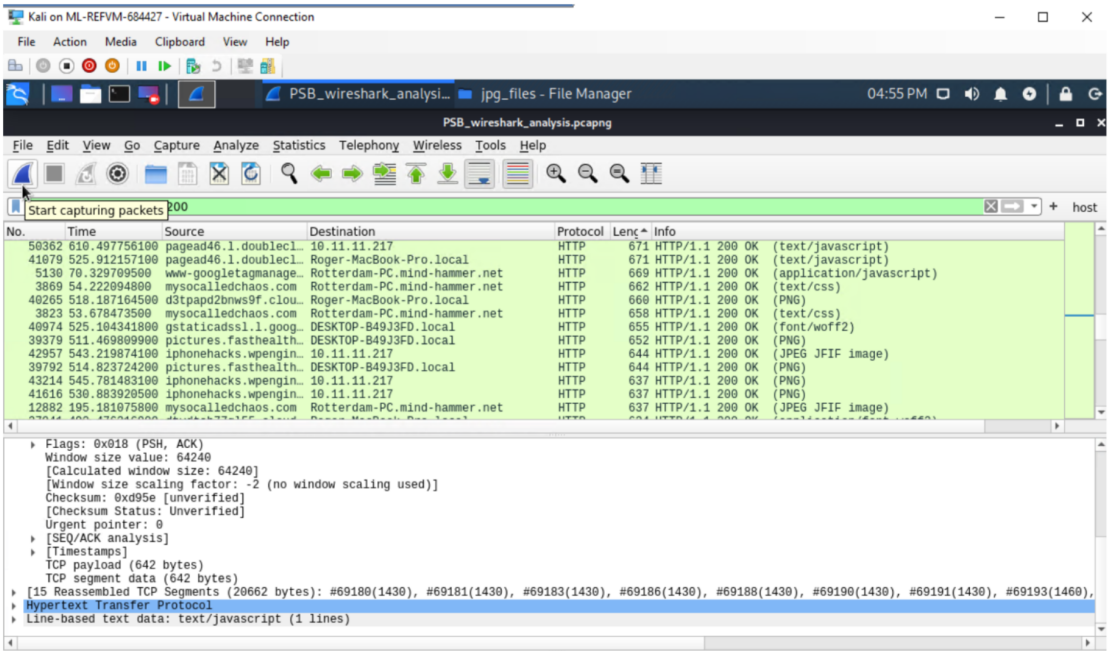
Ethernet · 30 | IPv4 · 808 | IPv6 · 2 | TCP · 1372 | UDP · 1977

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number
172.16.4.205	51,364	45 M	21,973	10 M	29,391	34 M	—	—	—
185.243.115.84	30,344	26 M	15,195	16 M	15,149	9,831 k	—	—	—
10.0.0.201	19,503	12 M	8,355	841 k	11,148	12 M	—	—	—
166.62.111.64	15,728	16 M	11,354	15 M	4,374	321 k	—	—	—
10.11.11.200	7,536	3,911 k	3,912	399 k	3,624	3,511 k	—	—	—
10.6.12.203	7,410	5,574 k	2,567	399 k	4,843	5,175 k	—	—	—
23.43.62.169	6,934	7,045 k	4,652	6,920 k	2,282	124 k	—	—	—
10.11.11.179	5,806	3,215 k	2,942	320 k	2,864	2,894 k	—	—	—
64.187.66.143	4,883	3,637 k	2,648	3,492 k	2,235	144 k	—	—	—
5.101.51.151	4,326	4,246 k	3,262	4,177 k	1,064	68 k	—	—	—
10.11.11.11	4,139	700 k	1,712	274 k	2,427	426 k	—	—	—
10.11.11.217	4,037	1,954 k	2,094	238 k	1,943	1,715 k	—	—	—
151.101.50.208	3,270	2,220 k	1,657	2,108 k	1,613	112 k	—	—	—
10.6.12.12	2,852	700 k	1,332	329 k	1,520	371 k	—	—	—
10.6.12.157	2,408	809 k	1,231	285 k	1,177	524 k	—	—	—

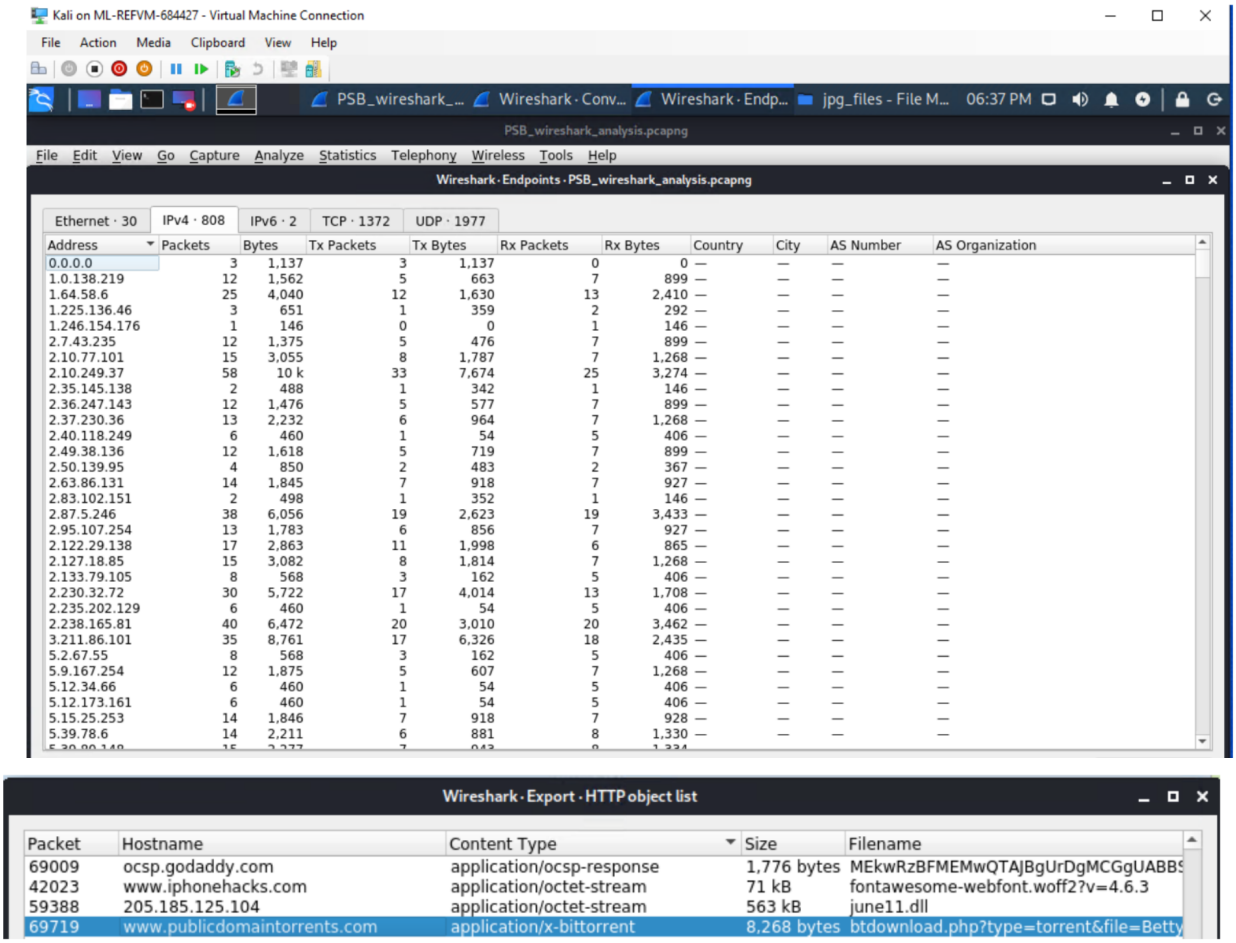
Wireshark · Endpoints · PSB_wireshark_analysis.pcapng

Ethernet · 30 | IPv4 · 808 | IPv6 · 2 | TCP · 1372 | UDP · 1977

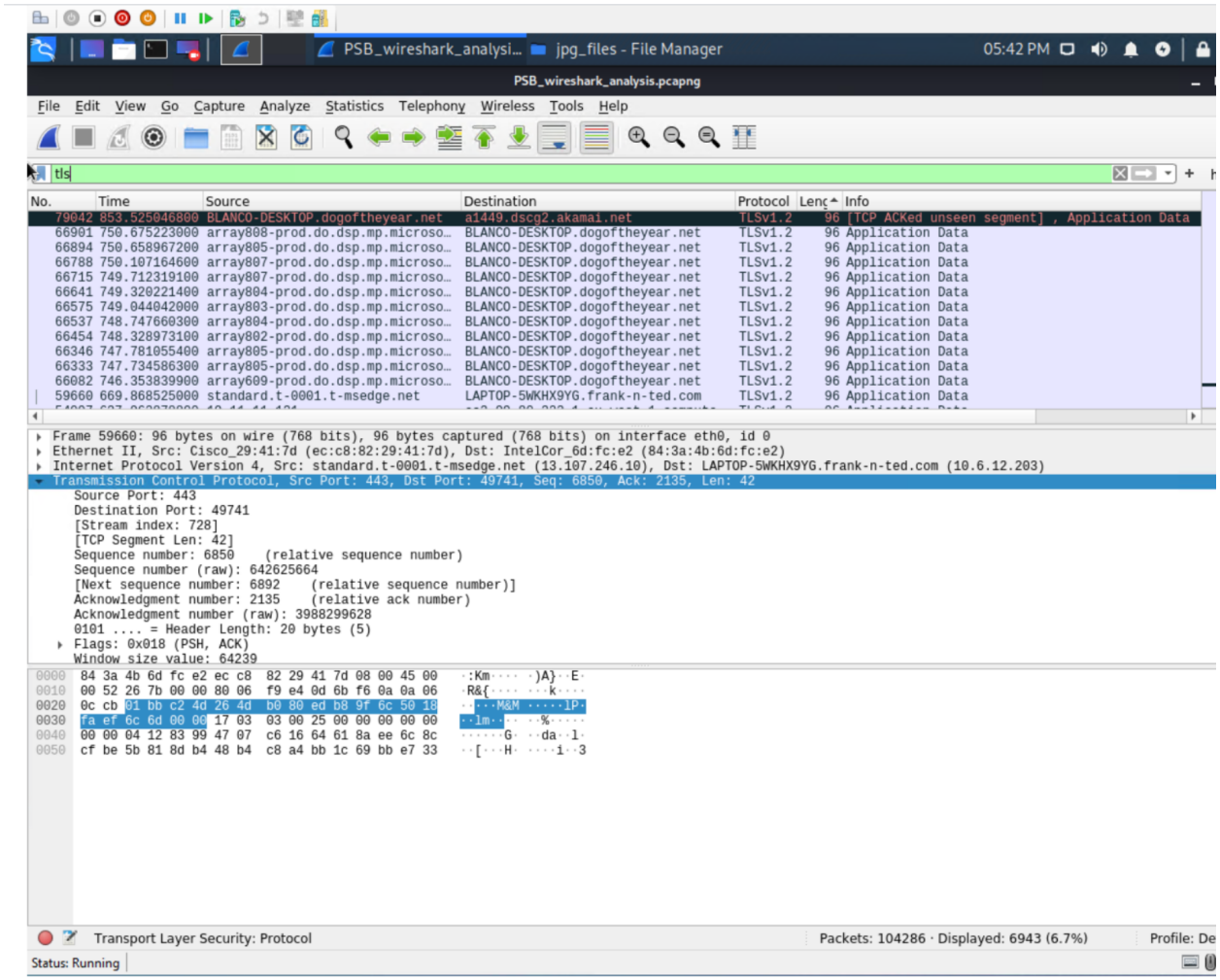
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country
Rotterdam-PC.mind-hammer.net	51,364	45 M	21,973	10 M	29,391	34 M	—
b5689023.green.mattingsolutions.co	30,344	26 M	15,195	16 M	15,149	9,831 k	—
BLANCO-DESKTOP.dogoftheyear.net	19,503	12 M	8,355	841 k	11,148	12 M	—
mysocalledchaos.com	15,728	16 M	11,354	15 M	4,374	321 k	—
Gilbert-Win7-PC.okay-boomer.info	7,536	3,911 k	3,912	399 k	3,624	3,511 k	—
LAPTOP-5WKHX9YG.frank-n-ted.com	7,410	5,574 k	2,567	399 k	4,843	5,175 k	—
a1449.dscg2.akamai.net	6,934	7,045 k	4,652	6,920 k	2,282	124 k	—
Roger-MacBook-Pro.local	5,806	3,215 k	2,942	320 k	2,864	2,894 k	—
64-187-66-143.iprev.kci.net	4,883	3,637 k	2,648	3,492 k	2,235	144 k	—
snnmnkxdhflwgthqismb.com	4,326	4,246 k	3,262	4,177 k	1,064	68 k	—
okay-boomer-dc.okay-boomer.info	4,139	700 k	1,712	274 k	2,427	426 k	—
10.11.11.217	4,037	1,954 k	2,094	238 k	1,943	1,715 k	—
dualstack.com.imgix.map.fastly.net	3,270	2,220 k	1,657	2,108 k	1,613	112 k	—
Frank-n-Ted-DC.frank-n-ted.com	2,852	700 k	1,332	329 k	1,520	371 k	—
DESKTOP-86J4BX.frank-n-ted.com	2,408	809 k	1,231	285 k	1,177	524 k	—



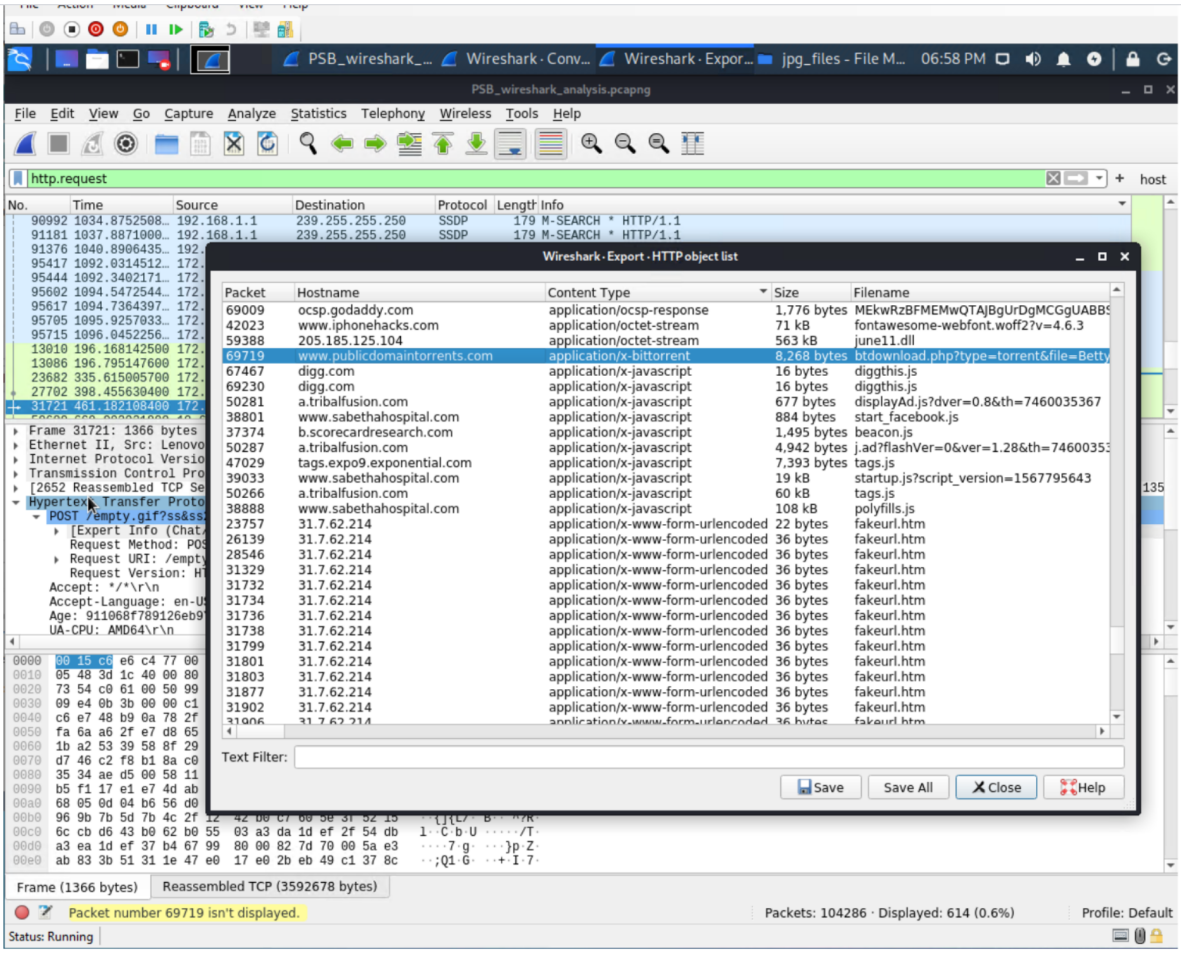
Report was done by: Darrel Mills Cybersecurity Specialist



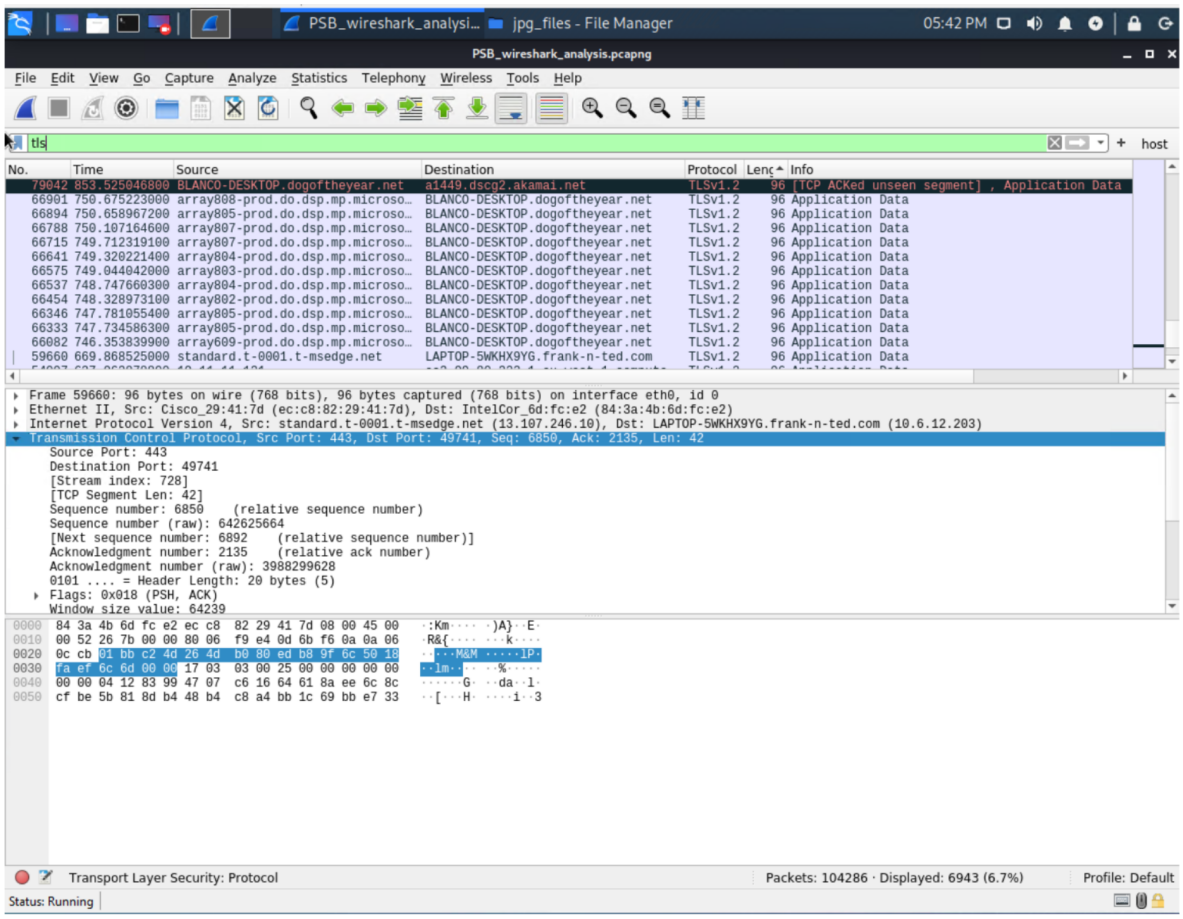
Wireshark_bittorrent.png



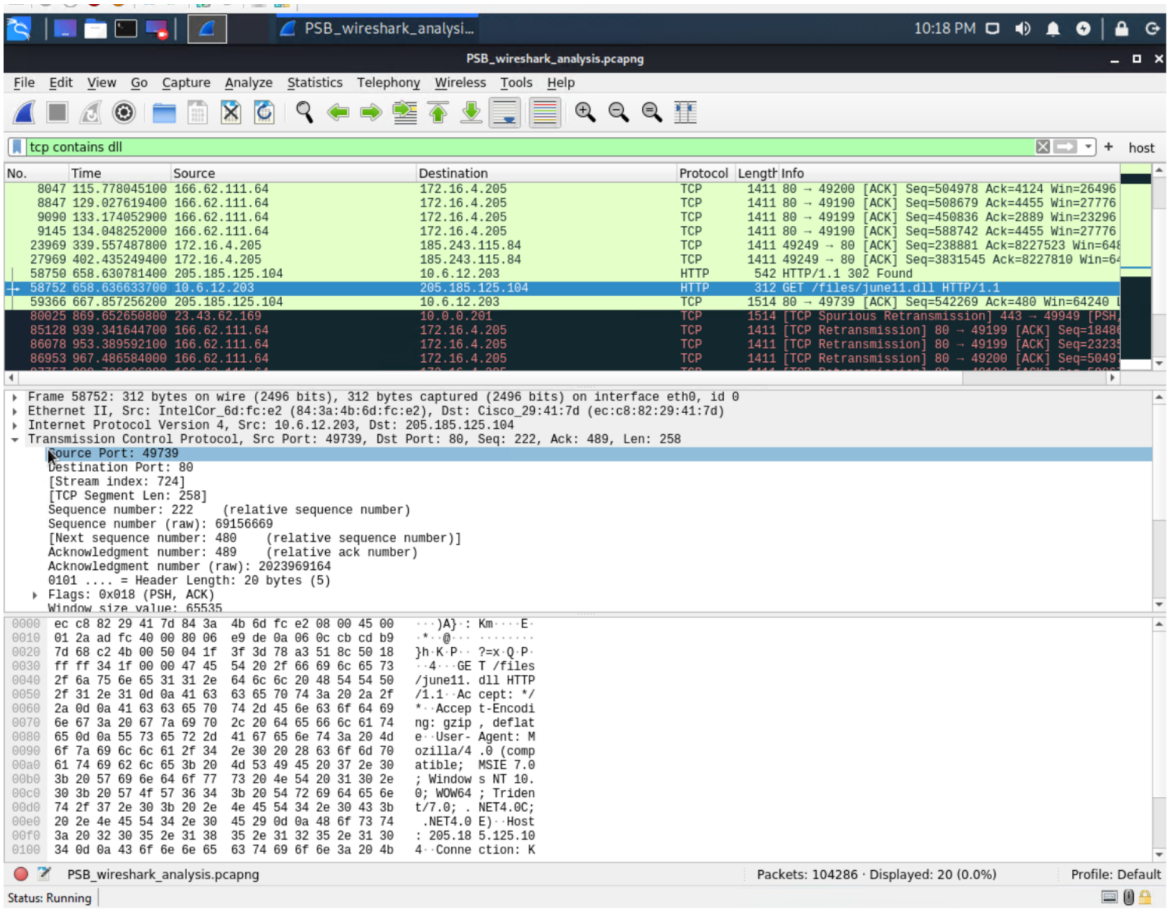
Wireshark BLANCODESKTOP.png



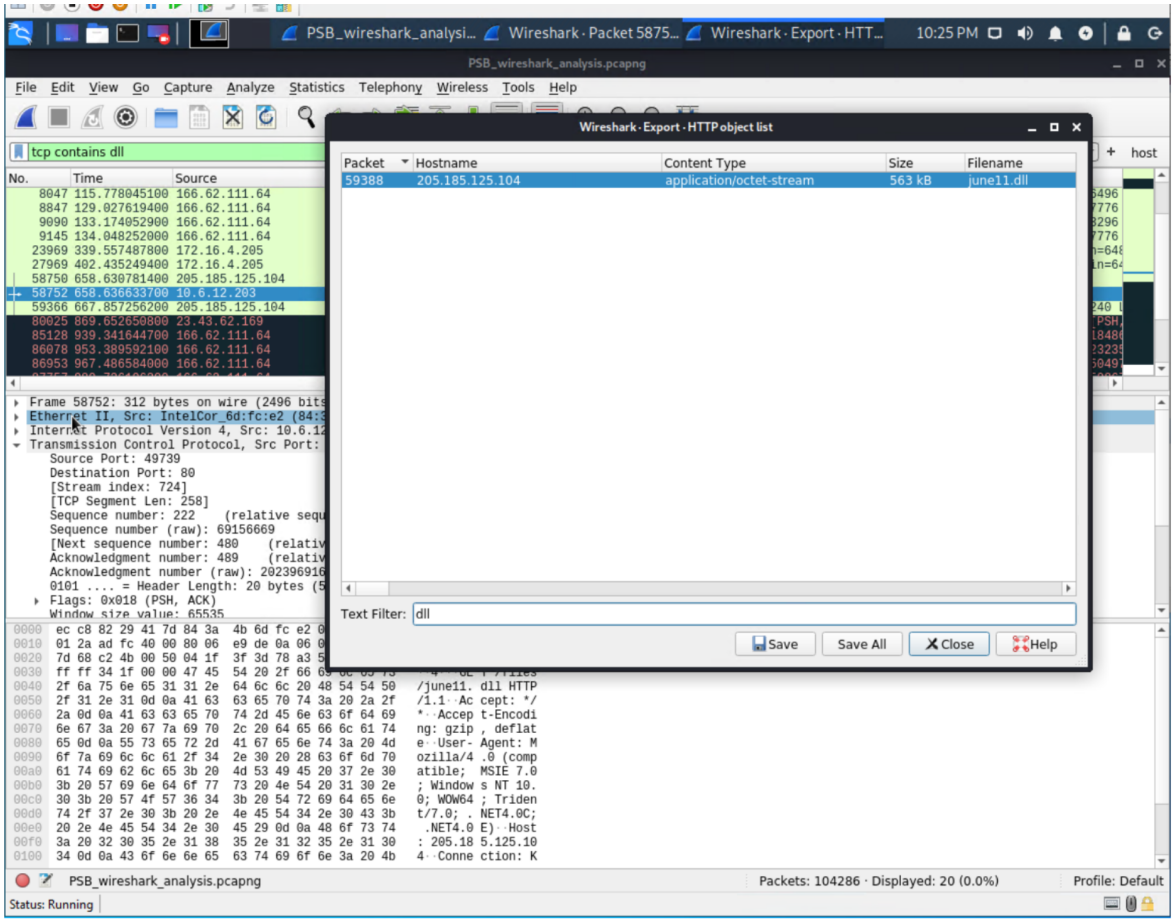
Wireshark_bittorrent1.png



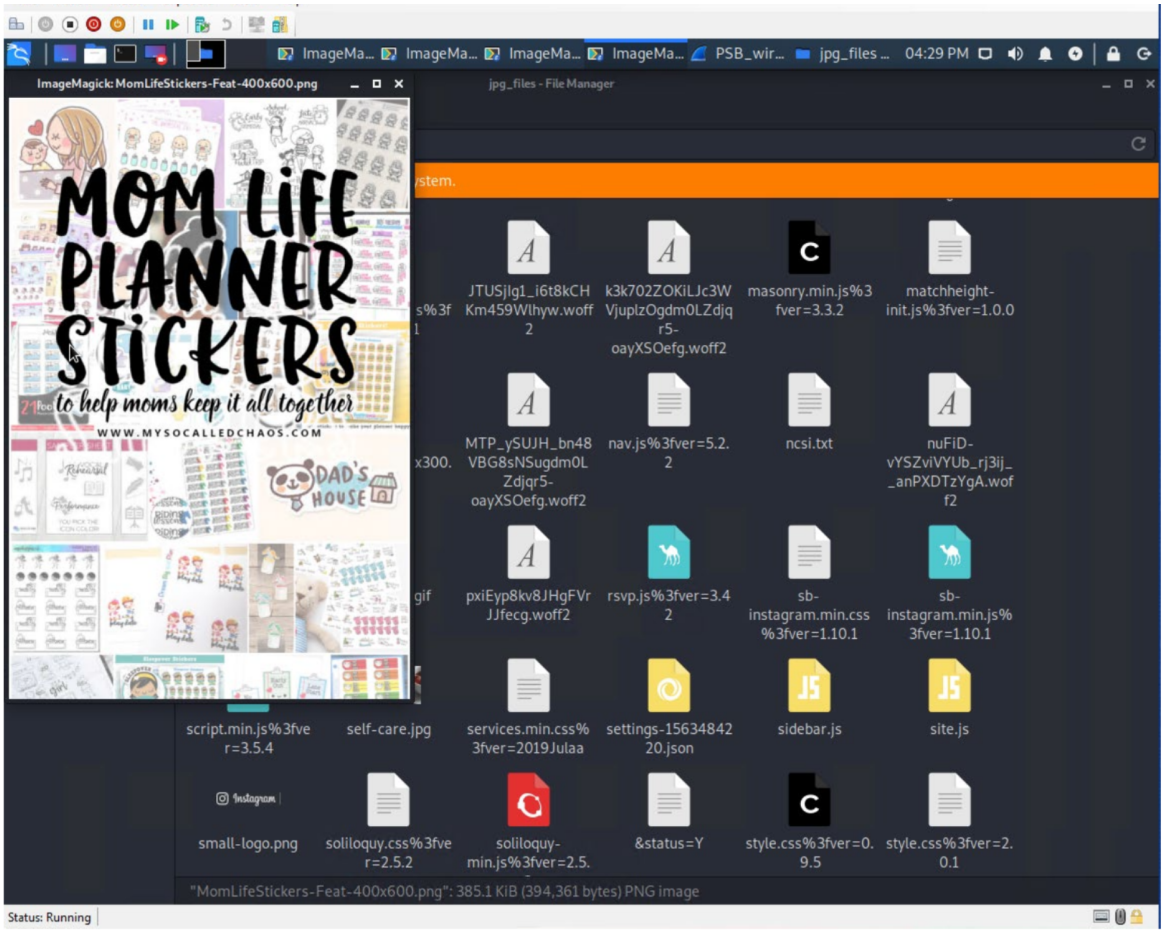
Wireshark_BLANCODESKTOP.png



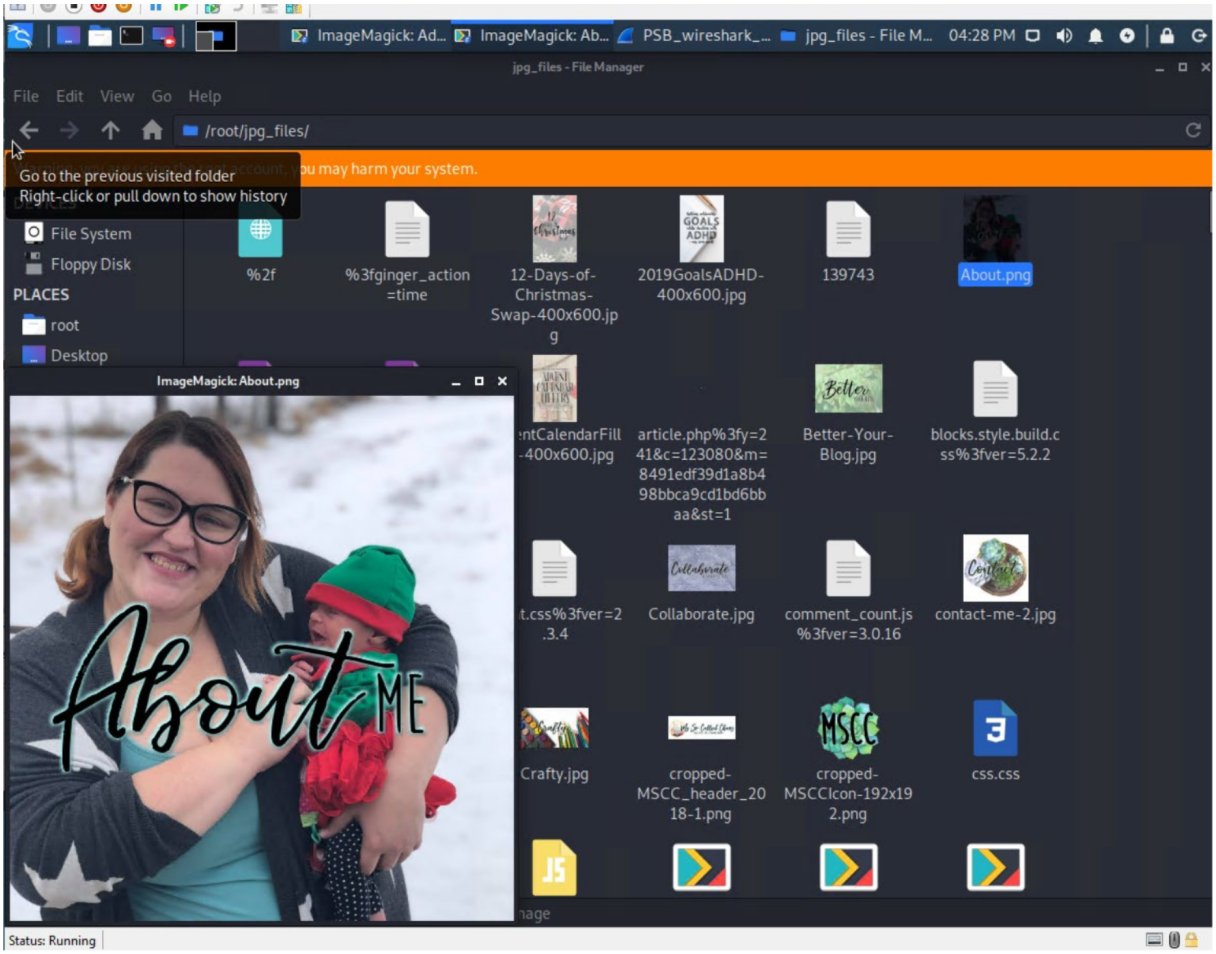
Wireshark_dll_file_to_test1



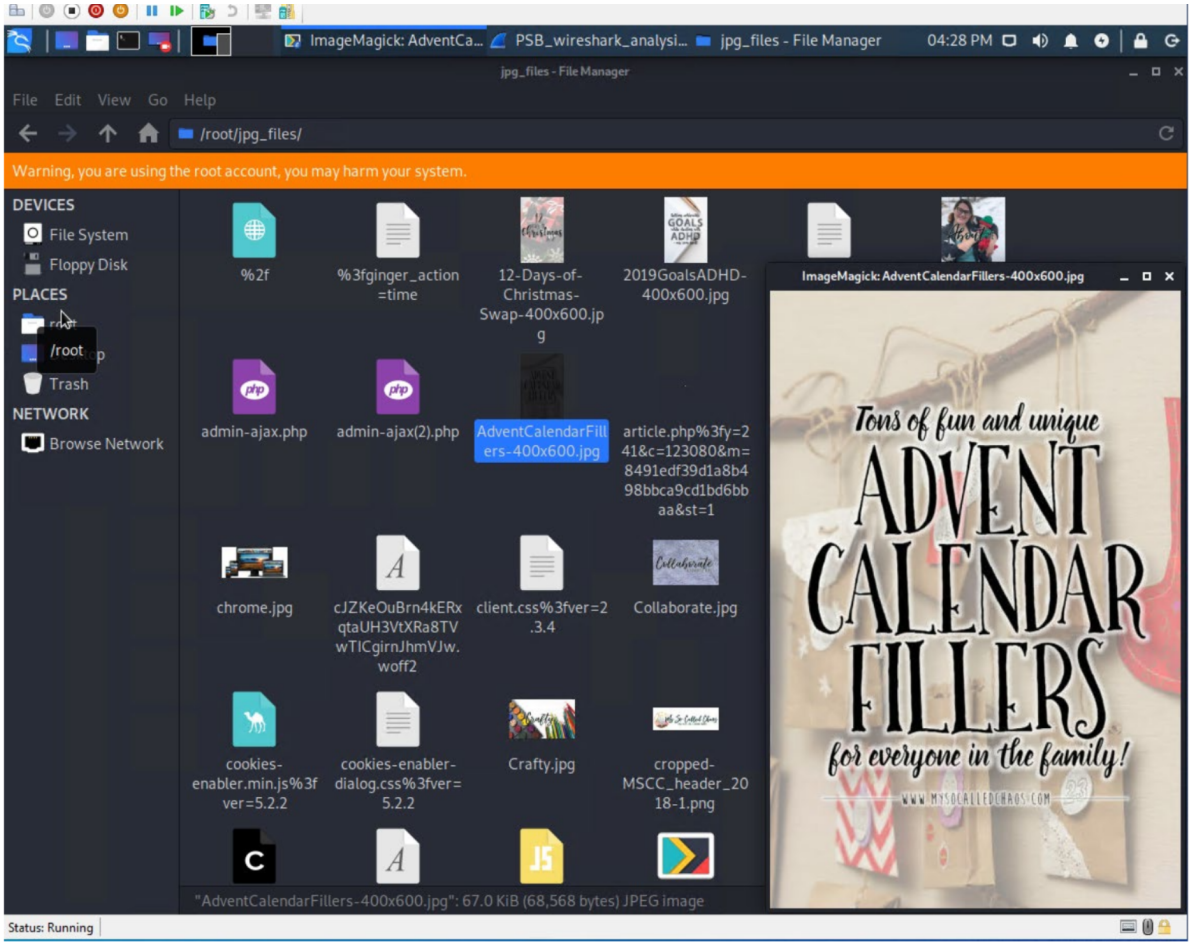
Wireshark_dll_file_to_test2



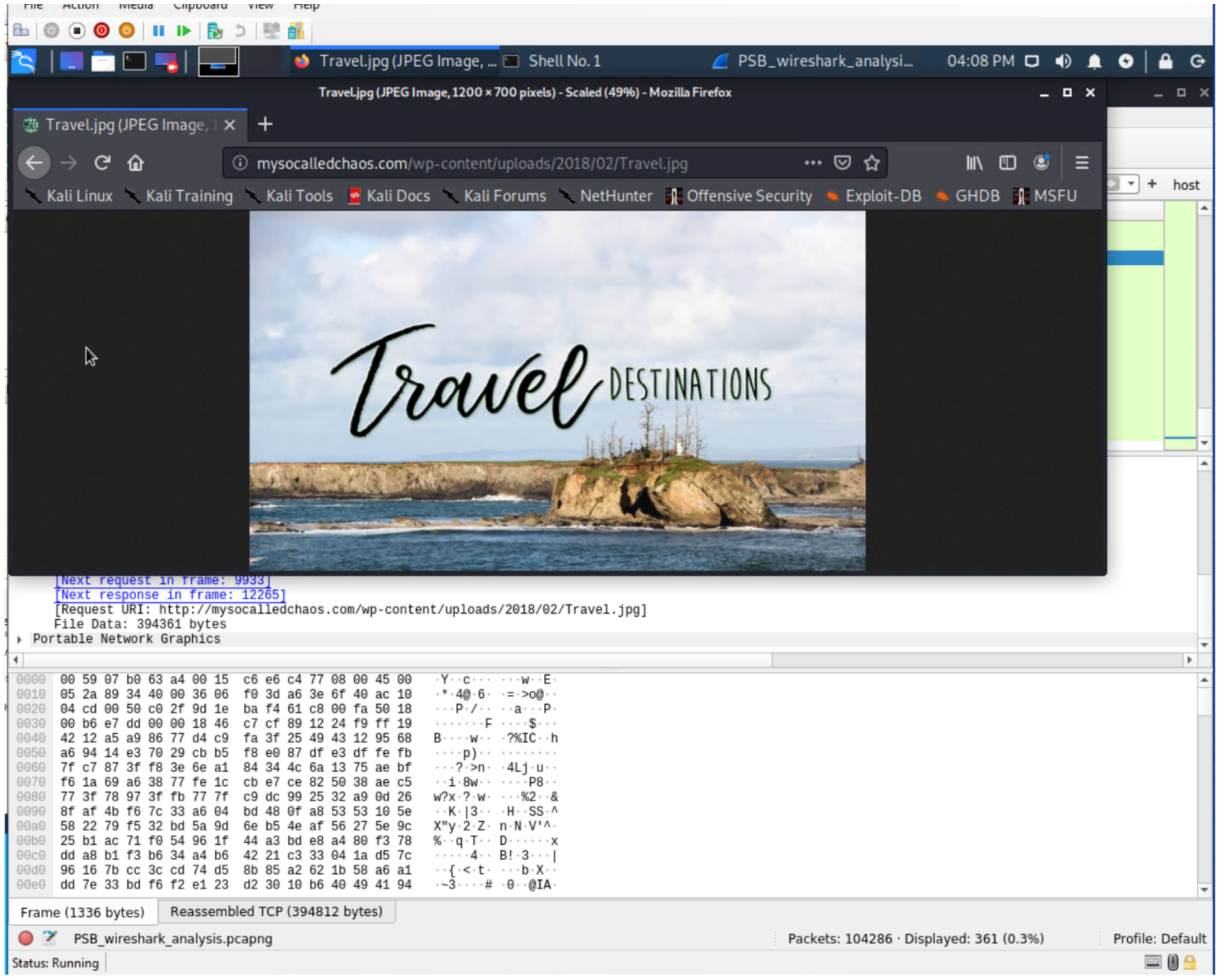
Wireshark html evidence1



Wireshark_html_evidence3



Wireshark_html_evidence4



Wireshark html evidence5

The End

Report was done by: Darrel Mills Cybersecurity Specialist

This Concludes my Report

By

Darrel Mills Cybersecurity Specialist