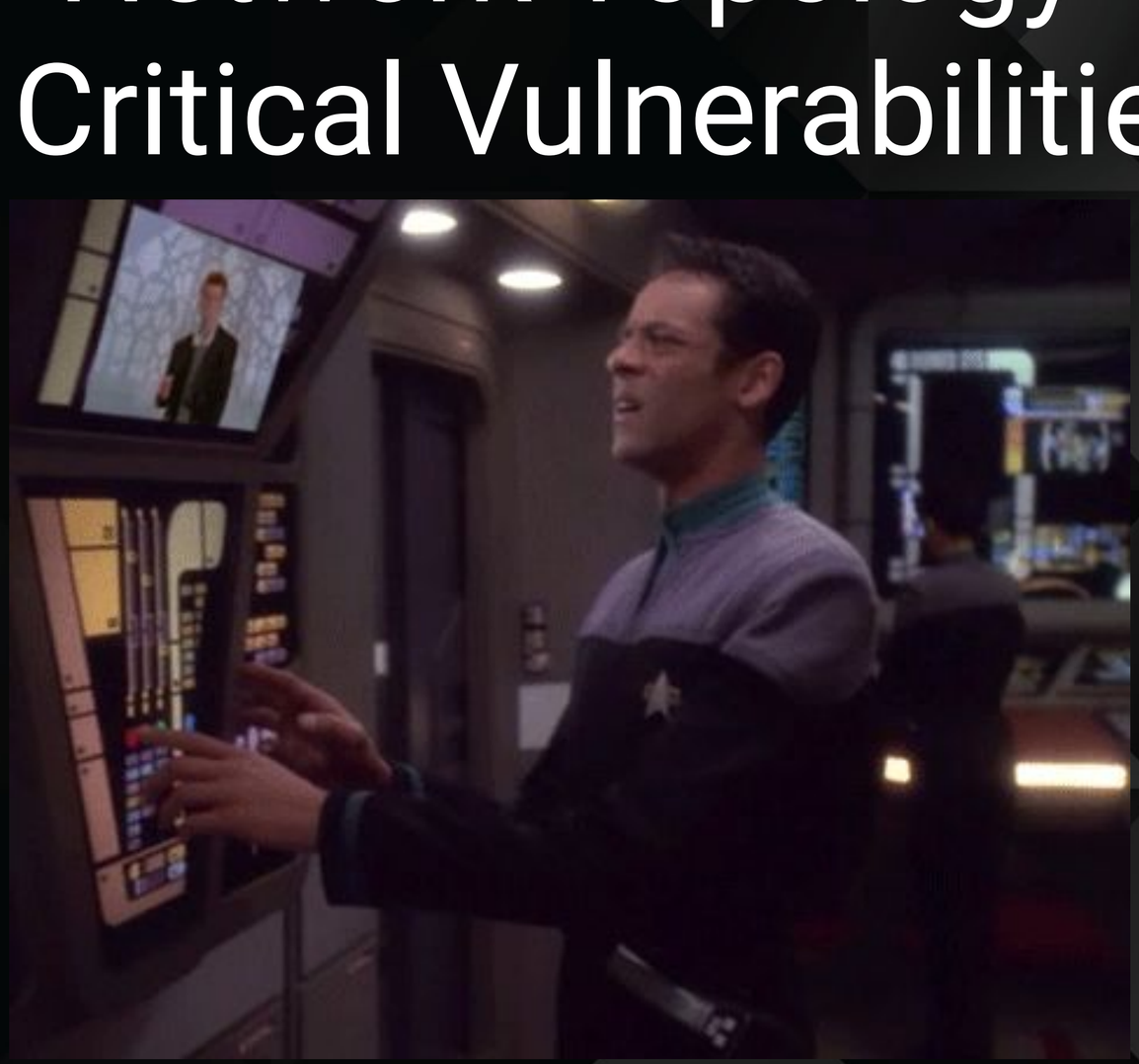
Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

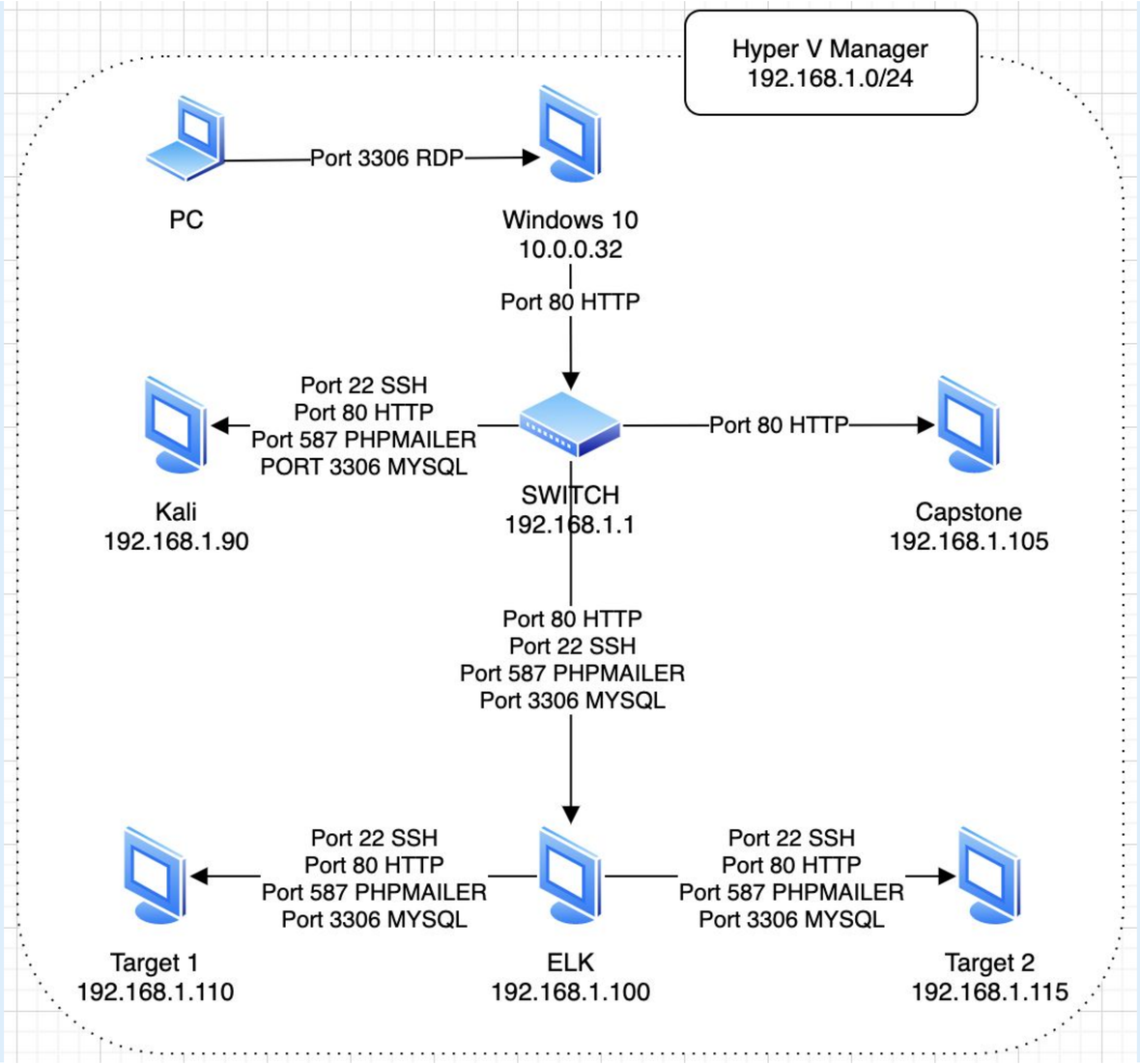
Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities



Network Topology



Network

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

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4:.192.168.1.110
OS: Linux
Hostname: TARGET1

IPv4: 192.168.1.115
OS: Linux
Hostname: TARGET2

Critical Vulnerabilities: Target 1

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

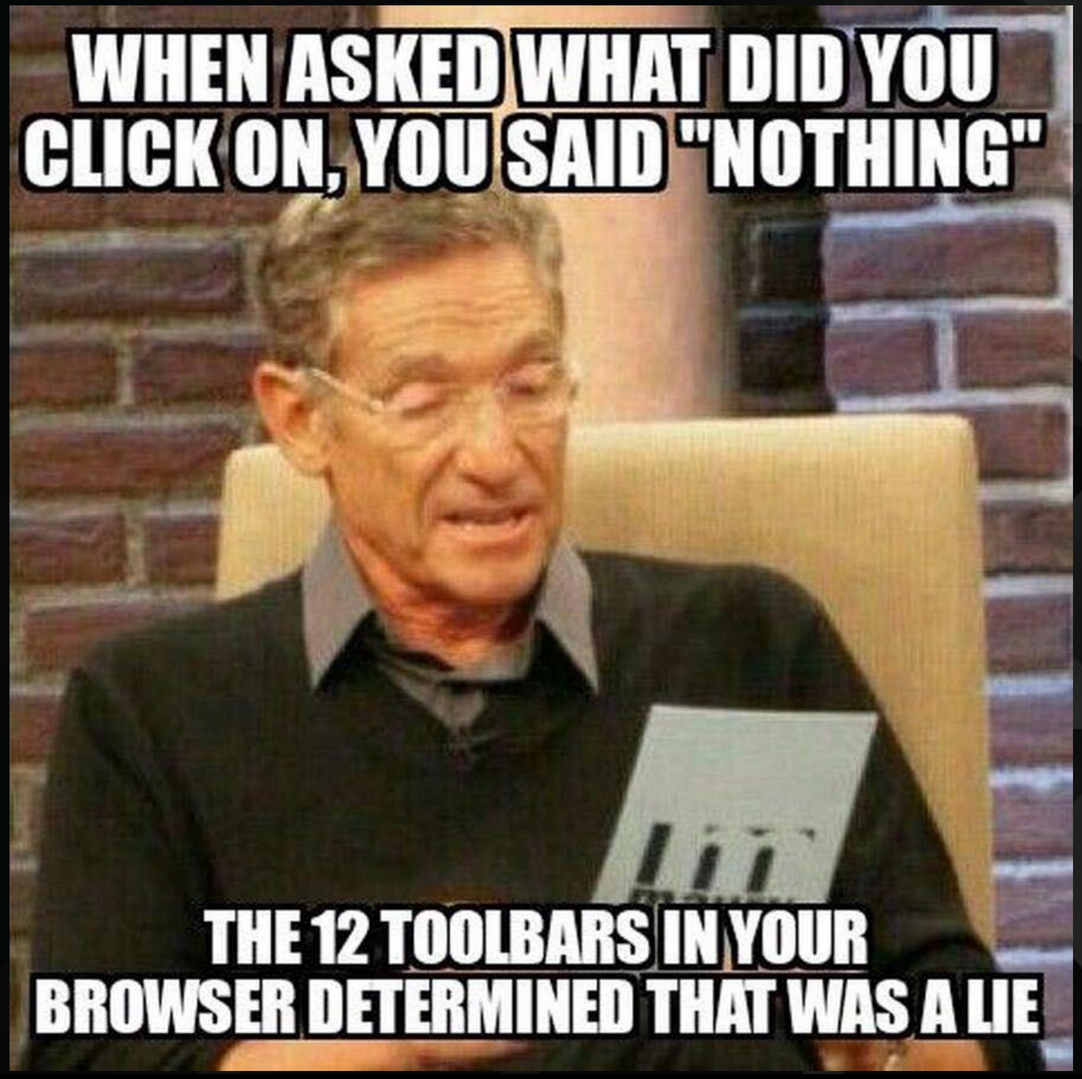
Vulnerability	Description	Impact
WordPress Site Enumeration	Use of WordPress Security Scanner (wpscan) against server (192.168.1.110) reveals sensitive information	The WordPress Security Scanner reveals the usernames: “michael” and “steven”
Brute Force Attack (michael)	By using Metasploit’s ssh_login module, user michael’s password can be cracked on the target	Malicious attackers can ssh into the TARGET1 server as user michael
wp-config.php readability	wp-config.php reveals sensitive information about root password for MySQL database	Vulnerable user michael has access to viewing wp-config.php which reveals root password for MySQL
John the Ripper (steven)	Using John on a hashed password for Steven found in MySQL	User steven’s hashed password cracked and obtained
Privilege escalation with Python	Exploit steven’s sudo permissions on python to gain root access of system: sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’	Steven’s sudo permissions with Python can be leveraged to gain root access of the system

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
Wordpress Scan	• WPScan Tool to scan a server's Wordpress database for any vulnerabilities. • Can also be done using an nmap script.	• Hidden folders such as "manual" and "vendor" were revealed in the scan. • Accessing "vendor" folder and the VERSION page leads to a single flag.
PHPMailer 5.2.16	• Exploitdb search revealed an RCE vulnerability for PHPMailer versions below 5.2.18	• Uploading a unique PHP script into the server and calling on it will send a shell to the attacker machine.
MySQL Root Access	• Access to server's MySQL database as 'root' allows the attacker to administer the database.	• Attacker can create tables and functions that can allow the attacker to take control from MySQL.

Traffic Profile



Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 185.243.115.84 166.62.111.64 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	DNS, HTTP, TCP	Three most common protocols on the network.
# of Unique IP Addresses	809	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	2	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 inconspicuous websites such as Instagram, or purchasing toys

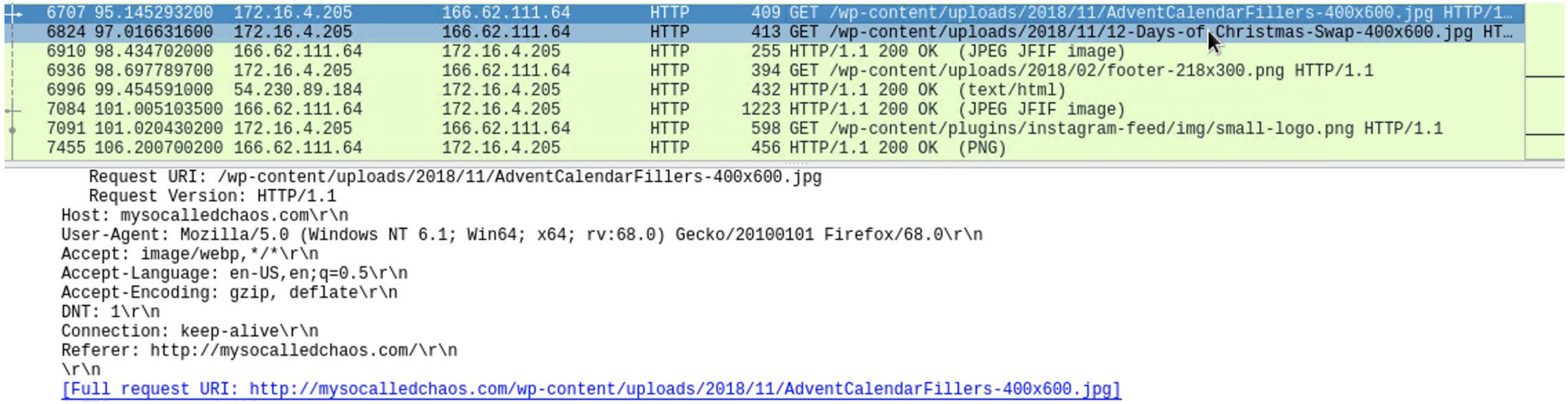
Suspicious Activity

- Trojan, Malware and Illegal downloads via Torrent

Normal Activity

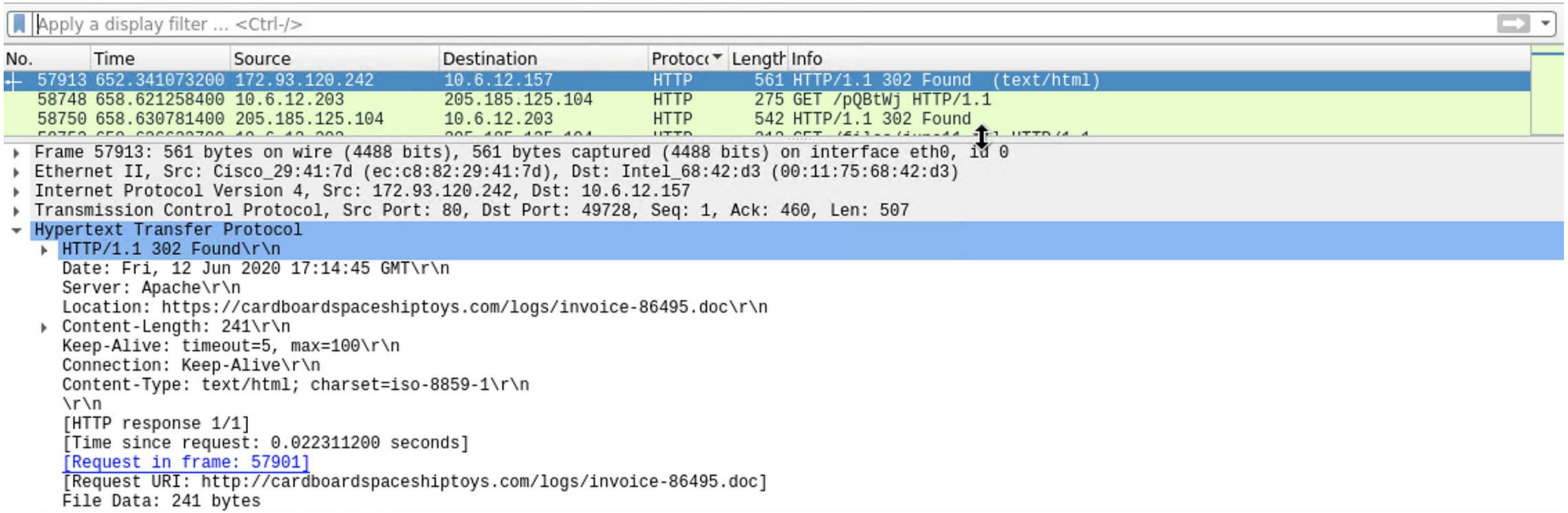
MySoCalledChaos

- Through ordinary HTTP traffic we are able to see that the user browses the site mysocalledchaos rather regularly, a blog for mothers that also sells niche products through Amazon
- A quick check via VirusTotal.com shows that the site and its plugins are not malicious

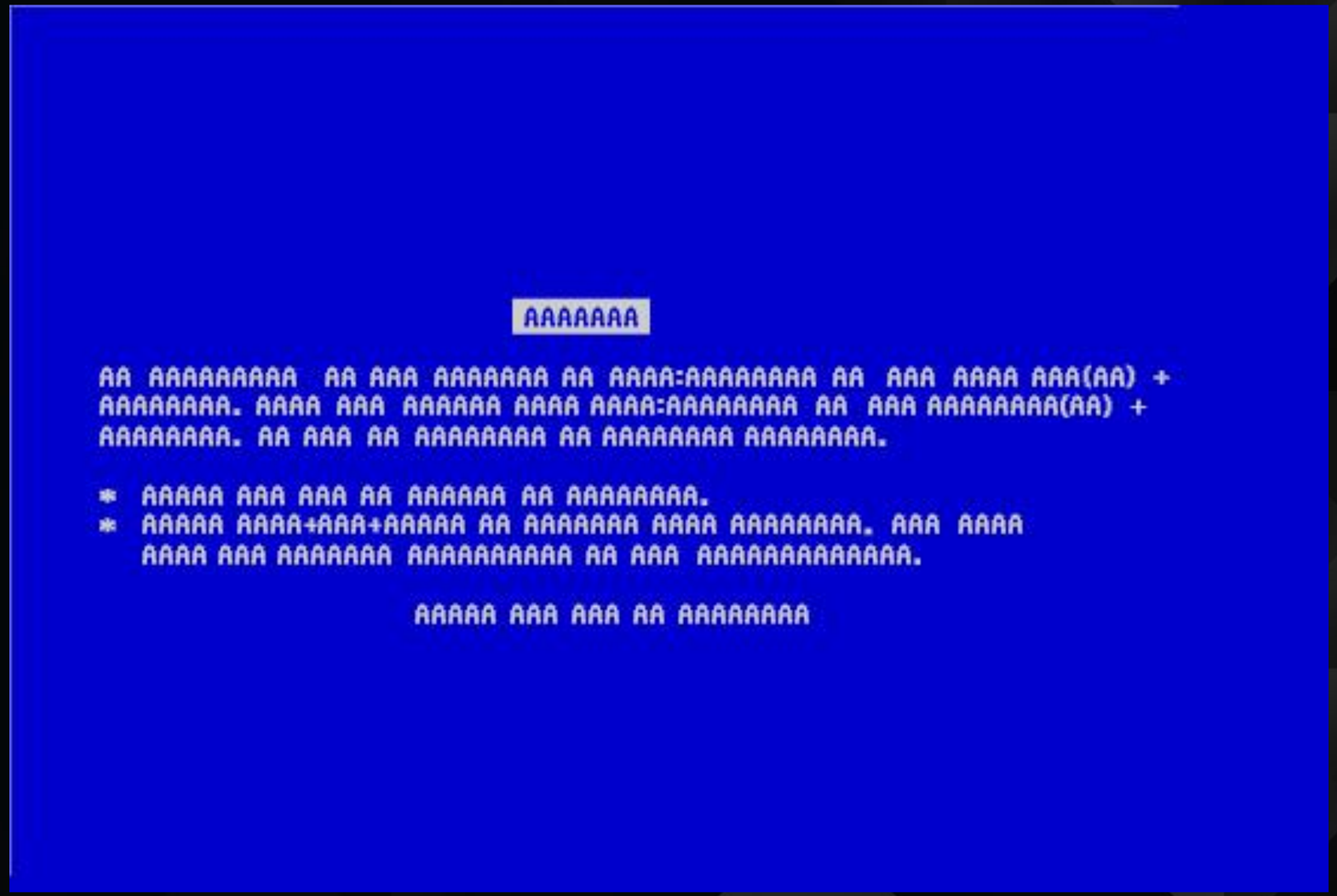


Cardboard Spaceship Toys

- Through HTTP Get protocols we are able to see additional normal behaviour such as an invoice for a purchase at Cardboard Spaceship Toys
- As shown below, and with further inspection via VirusTotal.com, the invoice file holds no malicious activity

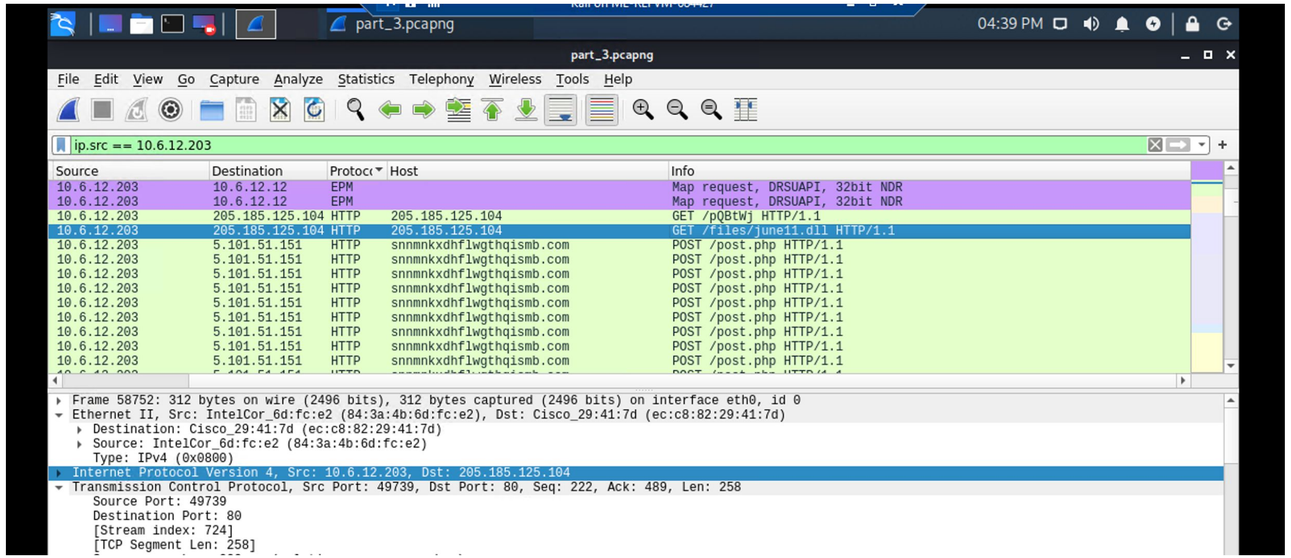


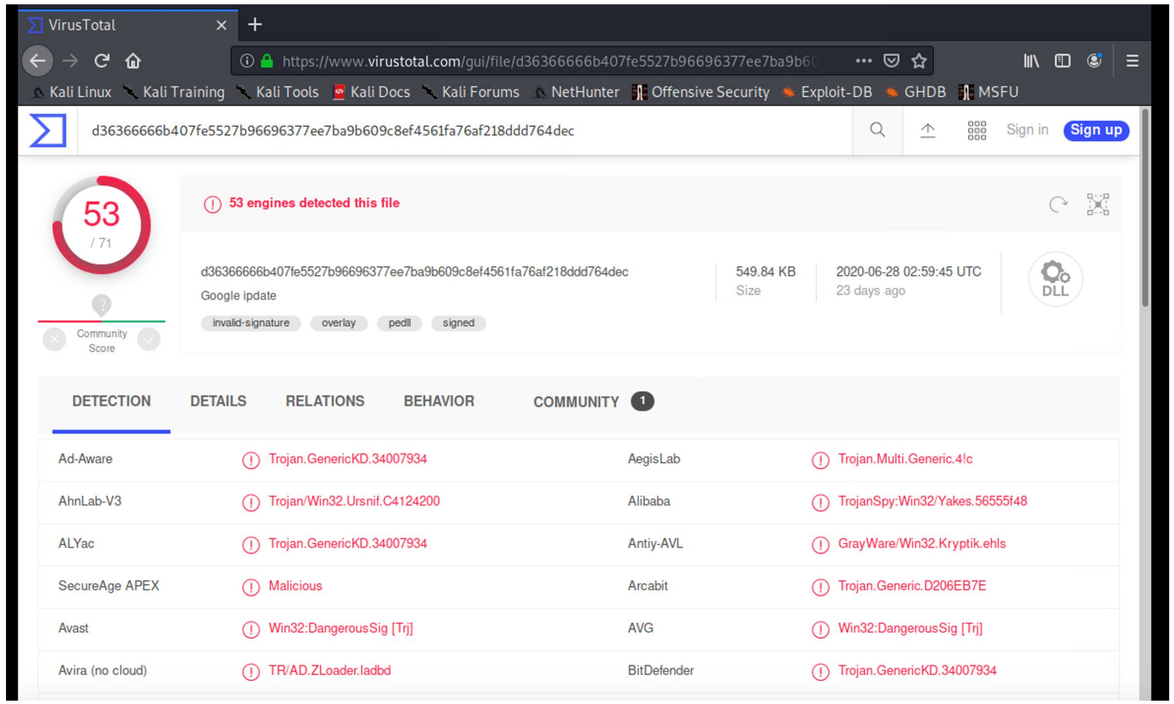
Malicious Activity



Time Thieves

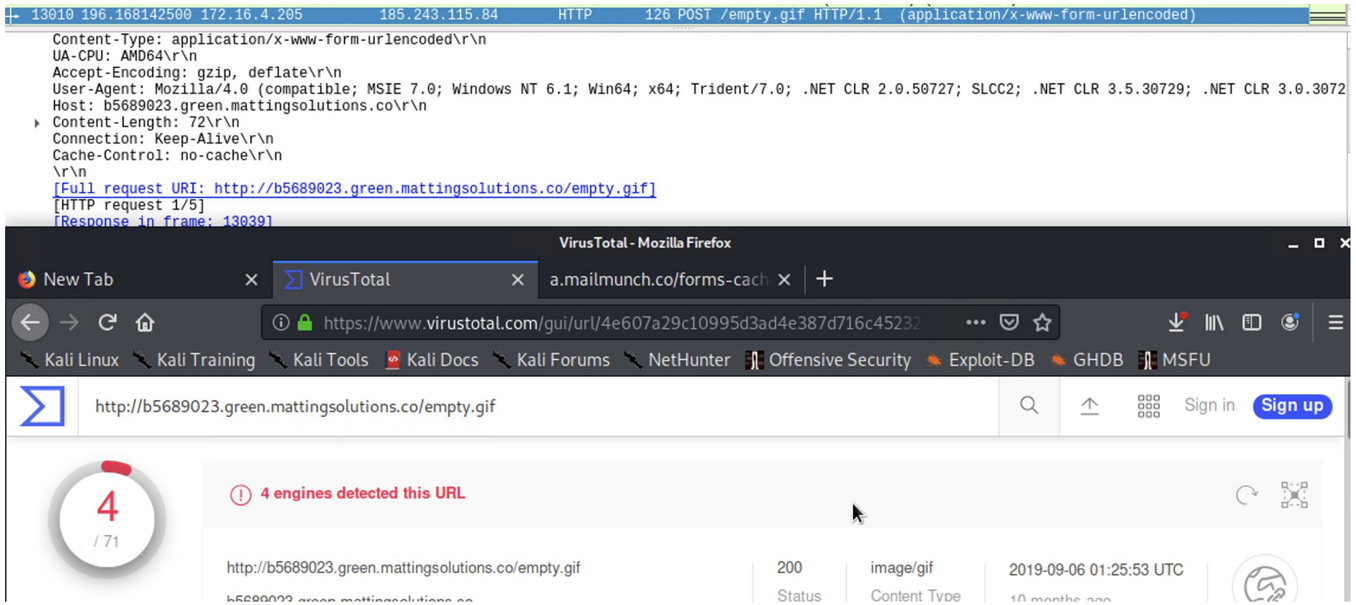
- Via a custom site, frank-n-ted.com, two users were able to watch Youtube videos during work hours
- A Domain Controller (DC) with an IP of 10.6.12.12 on their custom Active Directory (AD) Network was established
- Trojan Malware named june11.dll was downloaded on 10.6.12.203
- Using VirusTotal.com we are able to determine that the file has 53 engines

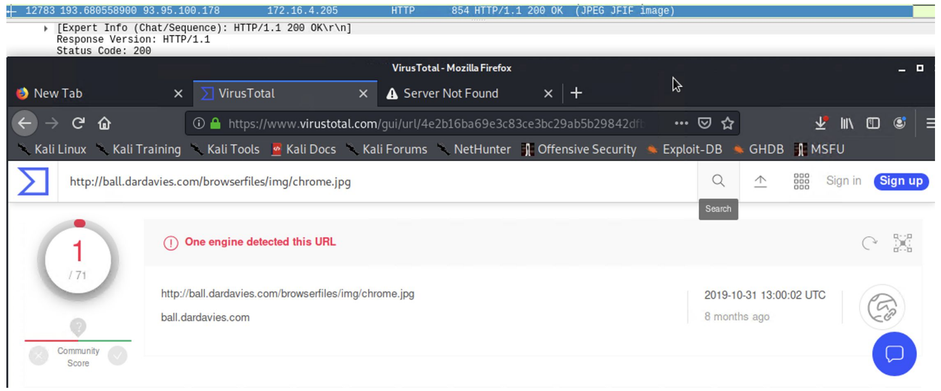




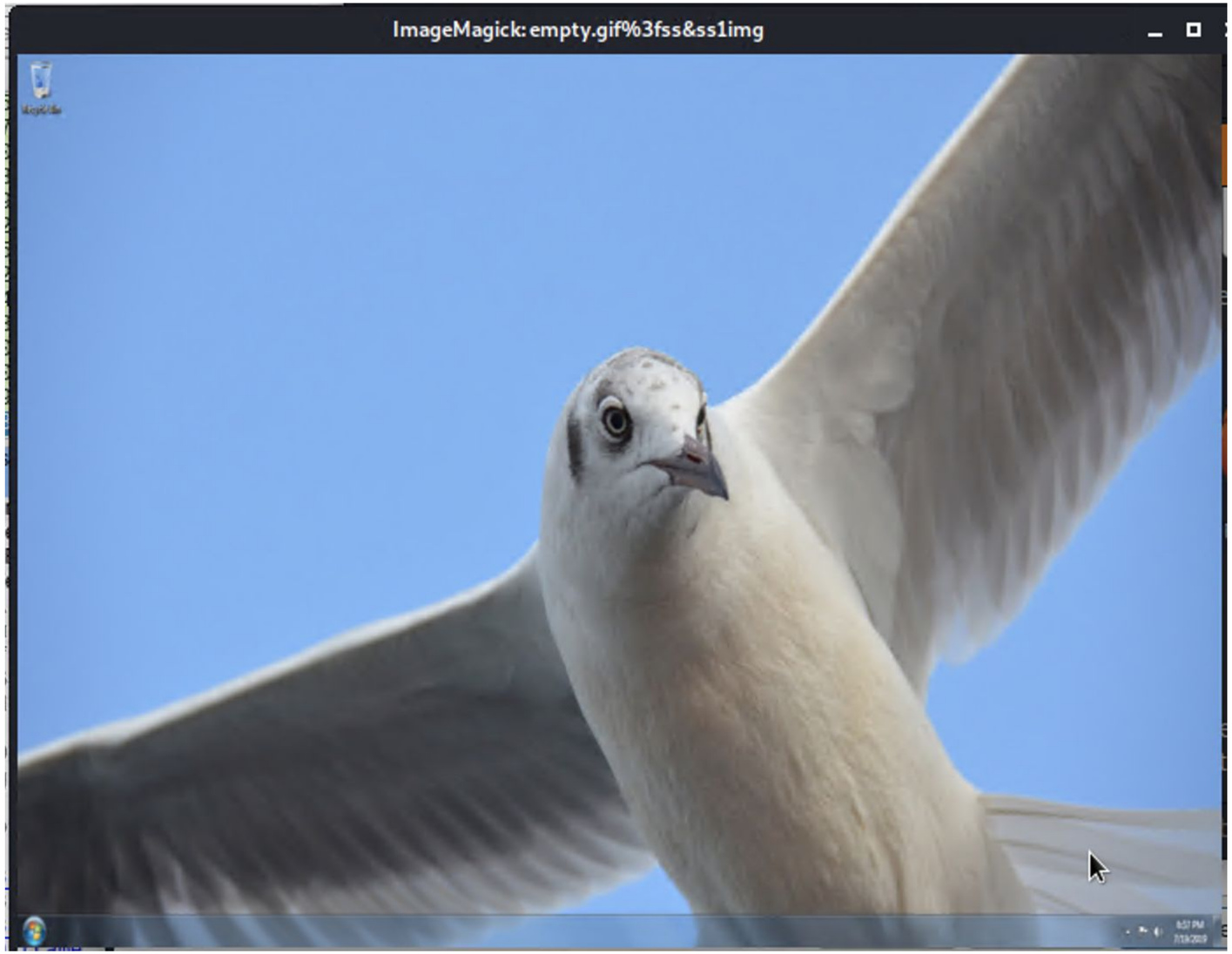
Malware

- The infected Windows machine on the network is Rotterdam-PC with an IP address of 172.16.4.205 and a MAC address of 00:59:07:b0:63:a4
- The user name of the Windows user with the infected machine is matthjis.devries
- IP addresses involved in the infection traffic include 185.243.115.84, 93.95.100.178



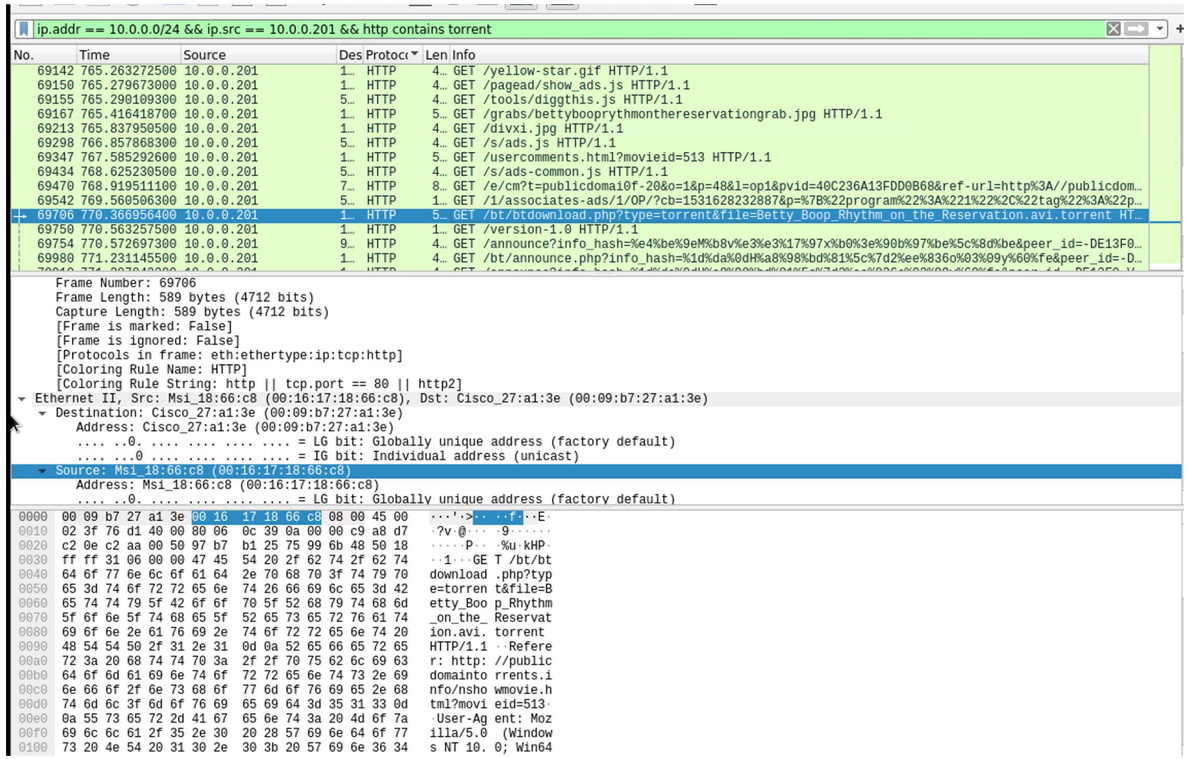


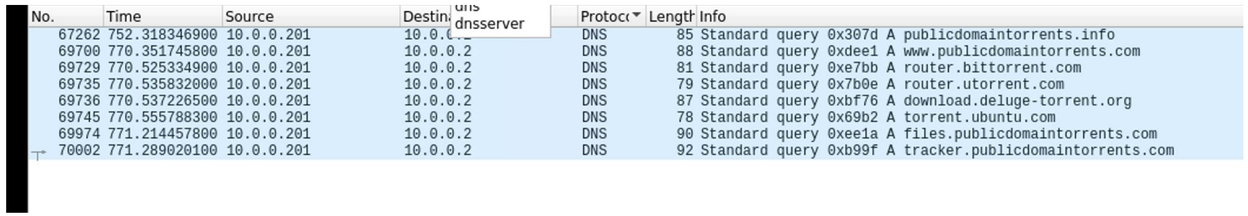
Hidden Desktop Background

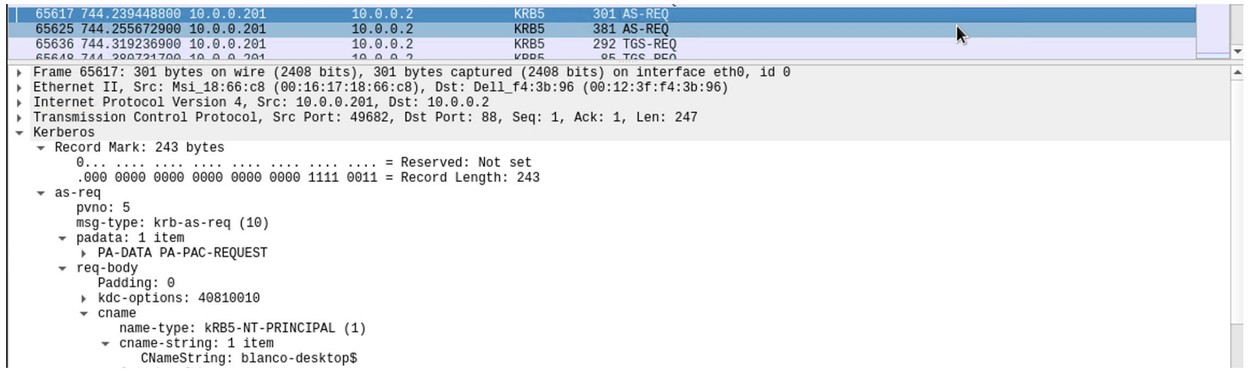


Illegal Downloads via Torrent

- Web traffic via HTTP Get protocol was used to torrent Betty Boop Rhythm on the Reservation.avi.torrent
- The offending party under the involved was elmer.blanco with a Windows NT 10.0 OS and a MAC address of (00:16:18:66:c8)







The End