



Final Engagement

Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



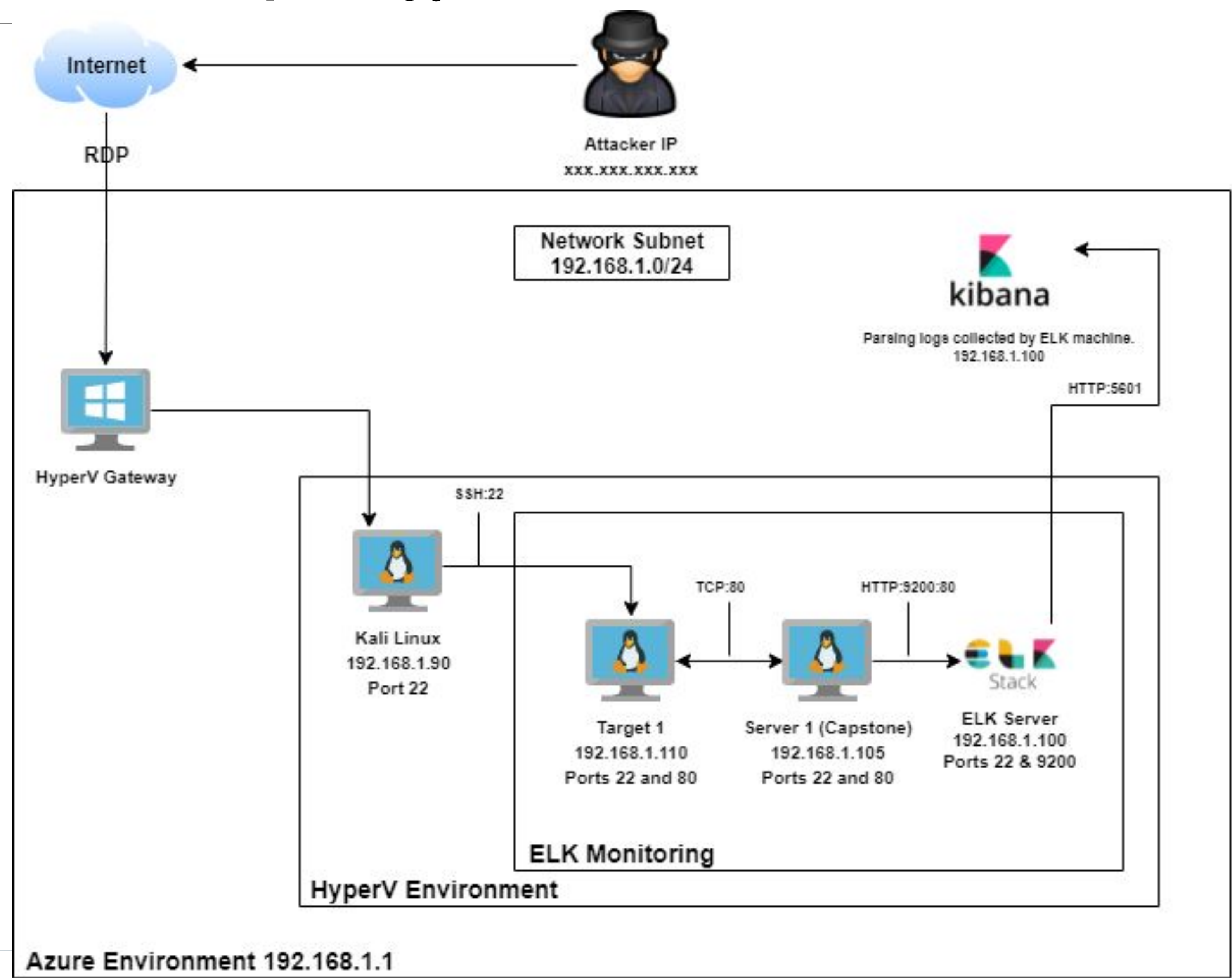
Normal Activity



Malicious Activity

Network Topology & Critical Vulnerabilities

Network Topology



Network

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

Machines

IPv4: 192.168.1.1
OS: Windows 10
Hostname: ML-RefVm-684427

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: kali

IPv4: 192.168.1.110
OS: Debian GNU/Linux 8
Hostname: target1

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: server1

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4 LTS
Hostname: ELK

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Security Misconfiguration	Port 22 is unrestricted. Port is vulnerable to internet.	We were able to SSH into 192.168.1.110 and set up a user shell as Michael.
Weak Password Policy	Password rules are too weak.	Michael's password was found using Hydra.
During Enumeration, a dated version of WordPress was found. (version 4.8.7)	The attacker used an outdated version of WordPress to gain access to usernames on the network.	This allows the attacker to find credentials for the SQL database passwords. Hashes were also found on the database.
Privilege Escalation	An attacker found Steven has sudo privileges using <i>sudo -l</i> .	Using a Python shell, we were able to gain root access.

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	Machines that sent the most traffic.
Most Common Protocols	TCP, UDP, HTTP	Three most common protocols on the network.
# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	255.255.255.0	Observed subnet ranges.
# of Malware Species	1 confirmed (Trojan)	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

- Viewing videos on YouTube
- Downloading desktop backgrounds

Suspicious Activity

- Downloading Malware
- Downloading movies using torrent
- Setting up Domain Controller (DC) and Active Directory (AD) network

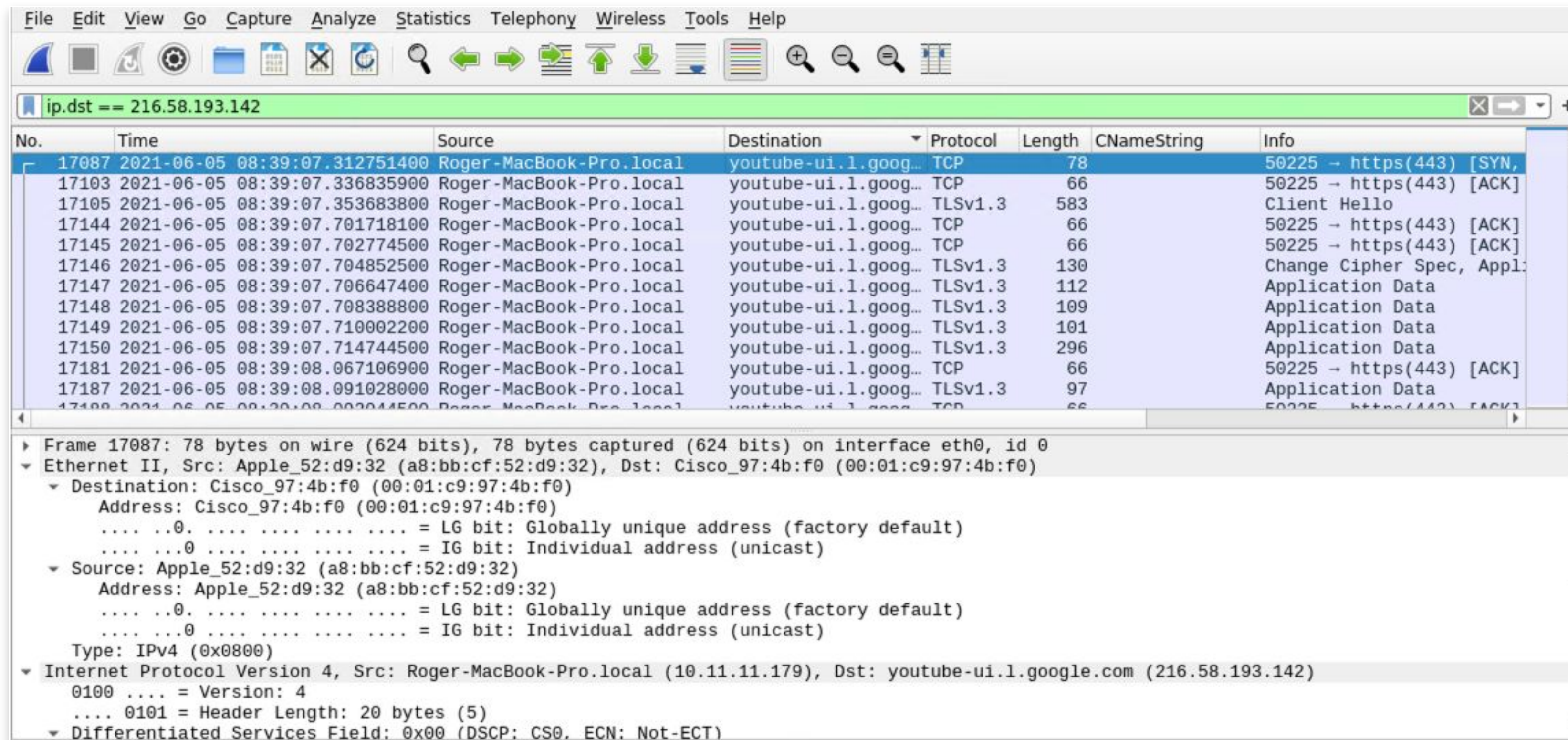
The background is a dark gray field filled with a complex, repeating pattern of geometric shapes. These shapes include squares and triangles of various sizes, some of which are further divided into smaller triangles, creating a tessellated effect. The colors are monochromatic, ranging from very dark gray to a slightly lighter, charcoal gray, which gives the background a textured, three-dimensional appearance.

Normal Activity

Viewing YouTube Videos

Summary:

- Traffic protocol(s) observed were TCP and TLSv1.3
- The user was spending a lot of time watching YouTube videos.



The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A filter bar shows the filter 'ip.dst == 216.58.193.142'. The main packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
17087	2021-06-05 08:39:07.312751400	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TCP	78		50225 → https(443) [SYN,
17103	2021-06-05 08:39:07.336835900	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TCP	66		50225 → https(443) [ACK]
17105	2021-06-05 08:39:07.353683800	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TLSv1.3	583		Client Hello
17144	2021-06-05 08:39:07.701718100	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TCP	66		50225 → https(443) [ACK]
17145	2021-06-05 08:39:07.702774500	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TCP	66		50225 → https(443) [ACK]
17146	2021-06-05 08:39:07.704852500	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TLSv1.3	130		Change Cipher Spec, Appl
17147	2021-06-05 08:39:07.706647400	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TLSv1.3	112		Application Data
17148	2021-06-05 08:39:07.708388800	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TLSv1.3	109		Application Data
17149	2021-06-05 08:39:07.710002200	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TLSv1.3	101		Application Data
17150	2021-06-05 08:39:07.714744500	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TLSv1.3	296		Application Data
17181	2021-06-05 08:39:08.067106900	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TCP	66		50225 → https(443) [ACK]
17187	2021-06-05 08:39:08.091028000	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TLSv1.3	97		Application Data
17188	2021-06-05 08:39:08.092044500	Roger-MacBook-Pro.local	youtube-ui.1.goog...	TCP	66		50225 → https(443) [ACK]

The bottom pane shows the details of the selected frame (Frame 17087):

- Frame 17087: 78 bytes on wire (624 bits), 78 bytes captured (624 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)
 - Destination: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
 - Address: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Source: Apple_52:d9:32 (a8:bb:cf:52:d9:32)
 - Address: Apple_52:d9:32 (a8:bb:cf:52:d9:32)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: Roger-MacBook-Pro.local (10.11.11.179), Dst: youtube-ui.1.google.com (216.58.193.142)
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Downloading Desktop Background

Summary:

- An image file was downloaded using HTTP.
- The user downloaded the file from 185.243.115.84 (*green.mattingssolutions.co*) to 172.16.4.205 .

```
[HTTP response 4/4]
[Prev request in frame: 14102]
[Prev response in frame: 14110]
[Request URI: http://b5689023.green.mattingssolutions.co/empty.gif?ss&ss1img]
  HTTP chunked response
    File Data: 14460 bytes
  Line-based text data: text/html (1 lines)
```

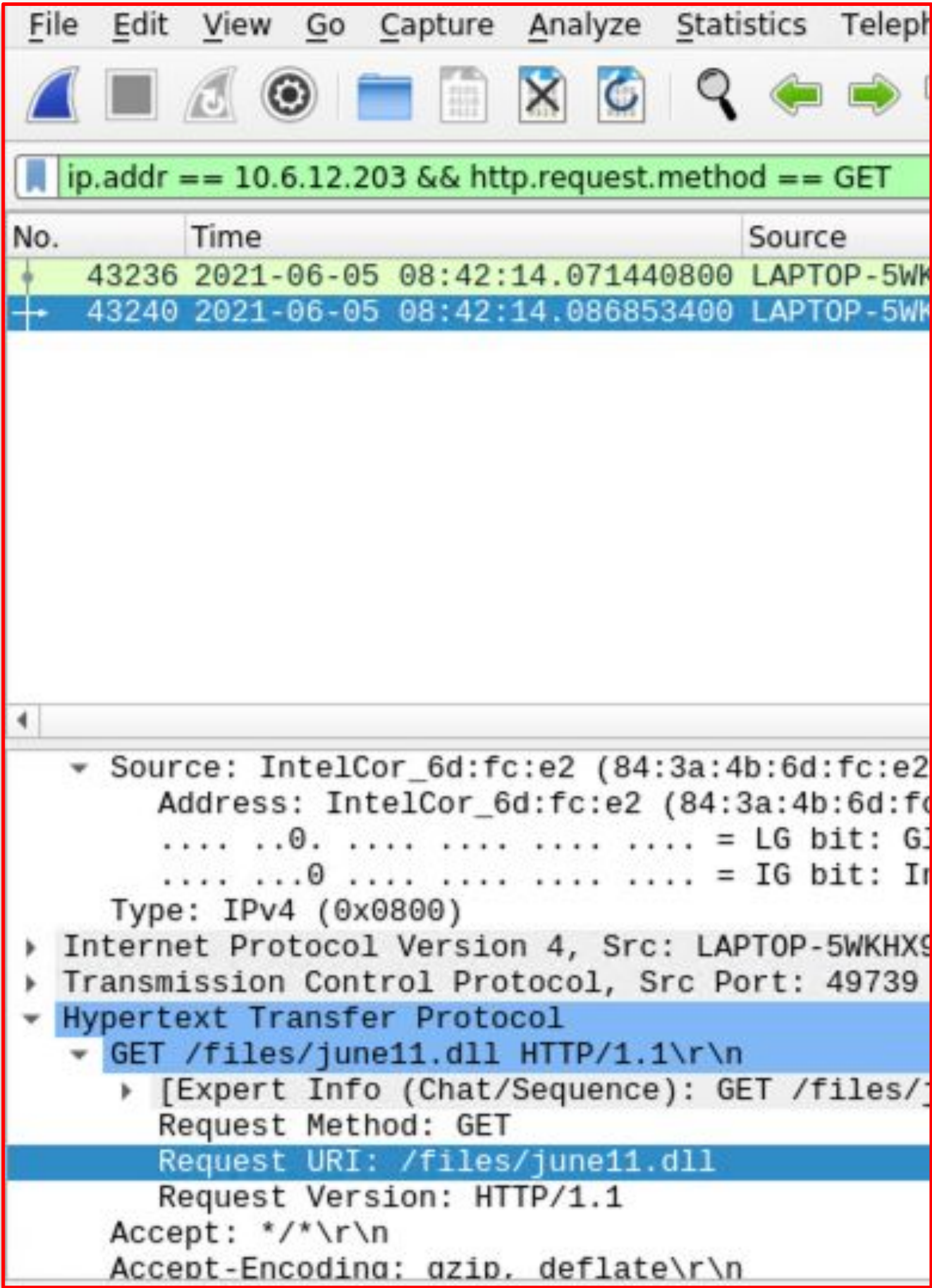
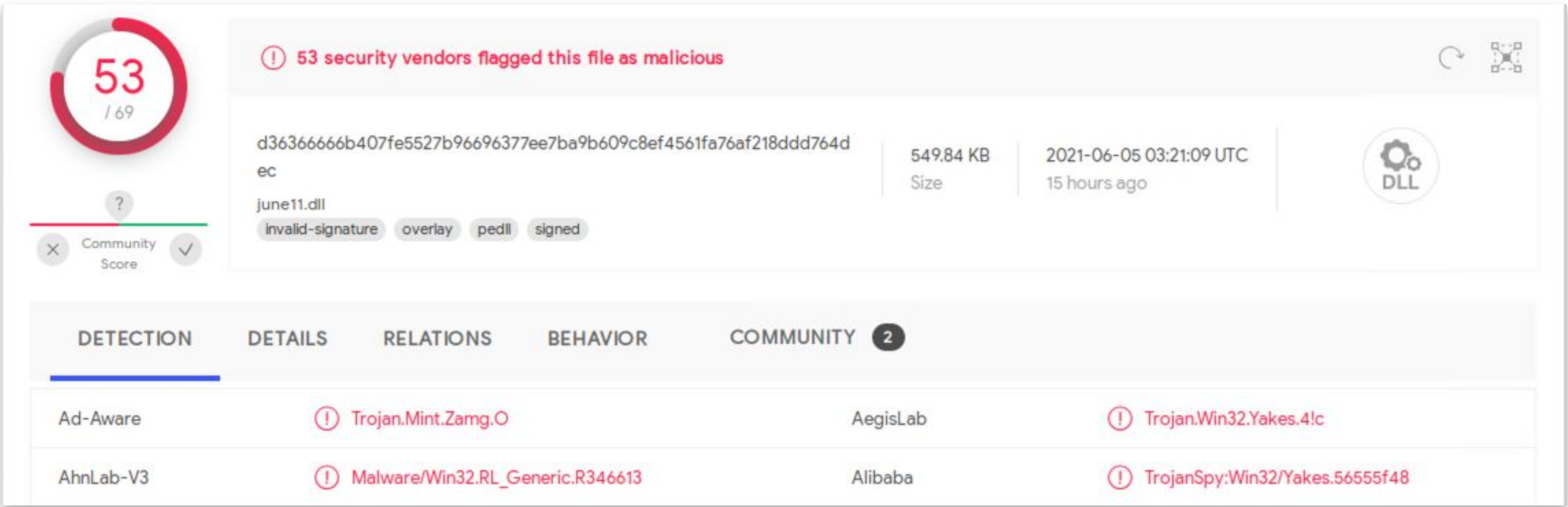


Malicious Activity

Downloading Malware

Summary:

- A file named june11.dll was downloaded from 205.185.125.104 to IP address 10.6.12.203 on the Frank-n-Ted web server using HTTP(80).
- The file was submitted to *virustotal.com* and found to be a malicious Trojan.



Setting Up A Domain Controller and Active Directory Network

Summary:

- The *frank-n-ted.com* webserver was set up on the company network.

Protocol: UDP (17)
Header checksum: 0xb90d [validation disabled]
[Header checksum status: Unverified]
Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
Destination: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
▼ User Datagram Protocol, Src Port: ldap (389), Dst Port: 60443 (

- The largest percentage of packets were transferred using TCP (91.8%).

▼ Internet Protocol Version 4	100.0
▼ Transmission Control Protocol	91.8
Transport Layer Security	5.6

- The largest percentage of bytes were transferred via TCP/HTTP (93.5%/71.5%)

Domain Name System	0.0
▼ Transmission Control Protocol	93.5
▼ Hypertext Transfer Protocol	71.5

Downloading Torrents

Summary:

- An illegal download was observed from 168.215.194.14 (*files.publicdomaintorrents.com*) using HTTP(80).
- The user downloaded an AVI file titled *Betty-Boop_Rhythm-on-the-Reservation.avi.torrent*.

eth.addr == 00:16:17:18:66:c8 && http.request.method == GET				
No.	Time	Source	Destination	Protocol
54422	2021-06-05 08:44:00.86660700	BLANCO-DESKTOP.dogoftheye...	files.publicdomaintorrents.com	HTTP
54488	2021-06-05 08:44:01.288135800	BLANCO-DESKTOP.dogoftheye...	files.publicdomaintorrents.com	HTTP
54573	2021-06-05 08:44:02.308006500	BLANCO-DESKTOP.dogoftheye...	www.assoc-amazon.com	HTTP
54627	2021-06-05 08:44:03.035488500	BLANCO-DESKTOP.dogoftheye...	files.publicdomaintorrents.com	HTTP
54714	2021-06-05 08:44:04.075417500	BLANCO-DESKTOP.dogoftheye...	www.assoc-amazon.com	HTTP
54750	2021-06-05 08:44:04.369677000	BLANCO-DESKTOP.dogoftheye...	rcm-na.assoc-amazon.com	HTTP
54822	2021-06-05 08:44:05.010704100	BLANCO-DESKTOP.dogoftheye...	fls-na.amazon-adsystem.com	HTTP
54995	2021-06-05 08:44:05.817147400	BLANCO-DESKTOP.dogoftheye...	files.publicdomaintorrents.com	HTTP
55039	2021-06-05 08:44:06.013456100	BLANCO-DESKTOP.dogoftheye...	ftp.osuosl.org	HTTP
55043	2021-06-05 08:44:06.022871200	BLANCO-DESKTOP.dogoftheye...	torrent.ubuntu.com	HTTP
55280	2021-06-05 08:44:06.681353400	BLANCO-DESKTOP.dogoftheye...	files.publicdomaintorrents.com	HTTP
55310	2021-06-05 08:44:06.758024900	BLANCO-DESKTOP.dogoftheye...	moonstar.publicdomaintorrents...	HTTP
55404	2021-06-05 08:44:07.041127000	BLANCO-DESKTOP.dogoftheye...	files.publicdomaintorrents.com	HTTP

.....0 = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheye.net (10.0.0.201), Dst: files.publicdomaintor...

Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (80), Seq: 1, Ack: 1, Len: 535

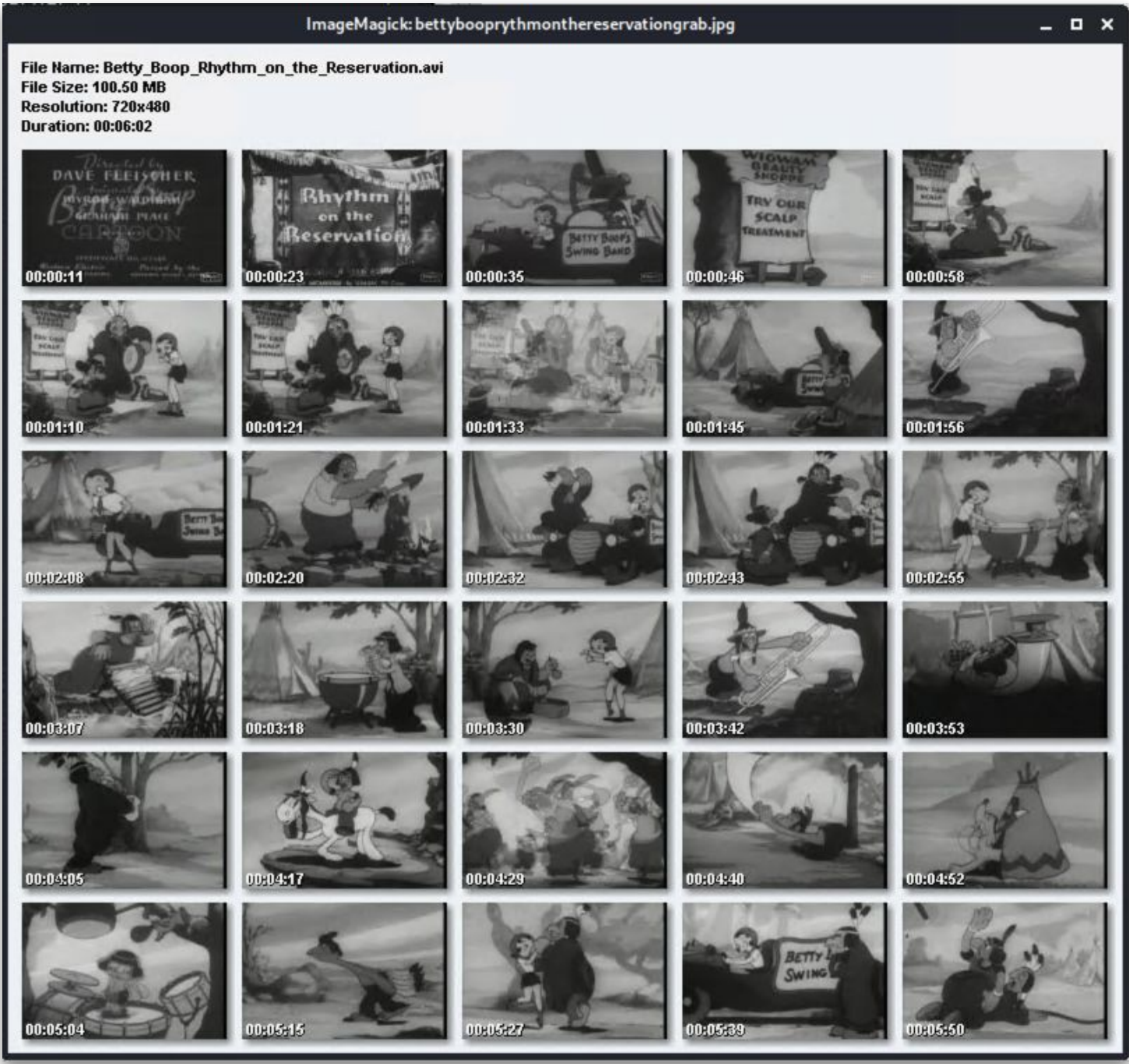
Hypertext Transfer Protocol

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_Rese...

Request Method: GET

Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent





The End