Final Engagement

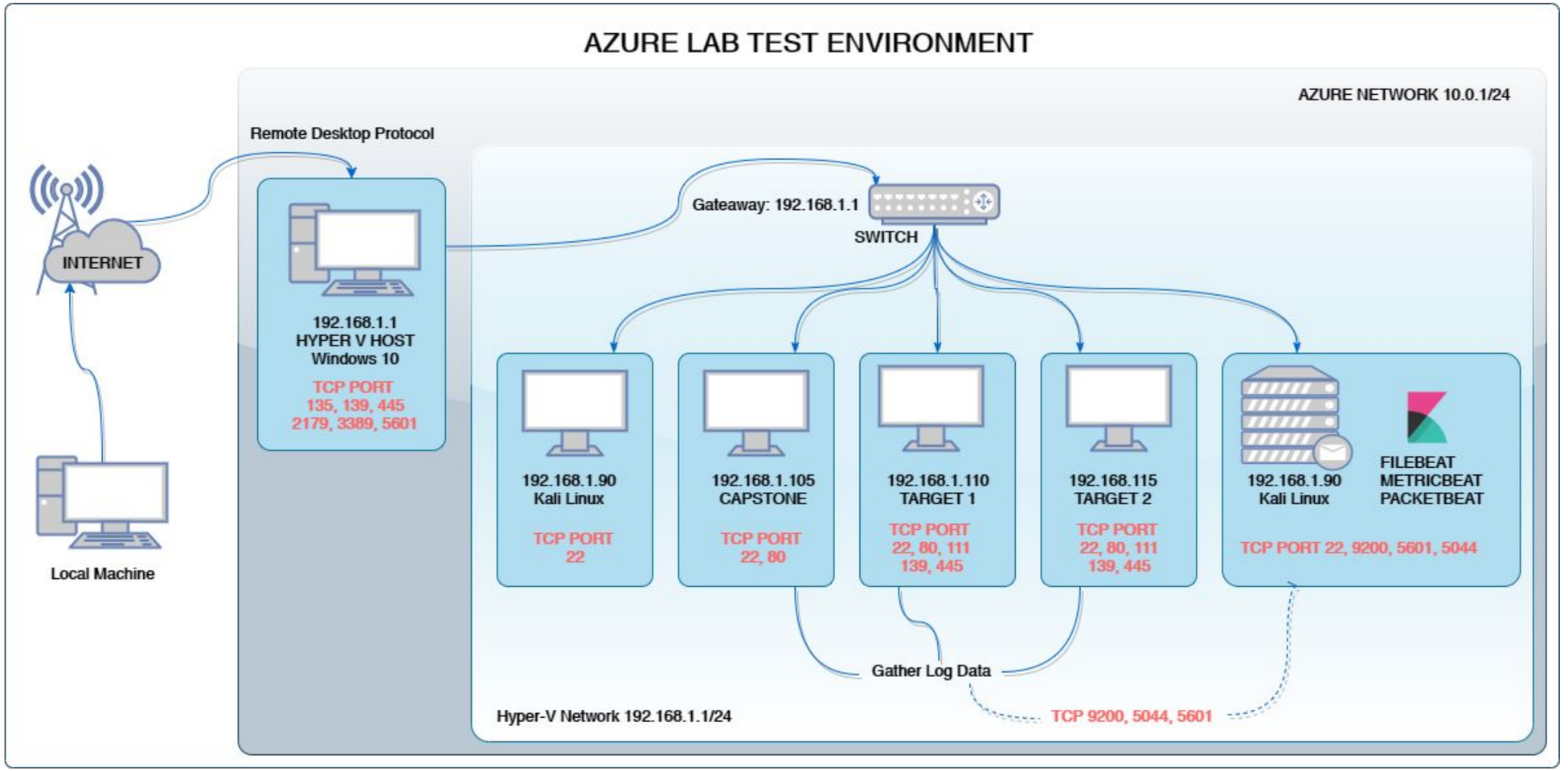
Attack, Defense & Analysis of a Vulnerable Network

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: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
Hostname: ELK

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
Hostname: Capstone

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

IPv4: 192.168.1.115
OS: Linux 3.2-4.9
Hostname: Target 2

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	HTTP, TCP, UDP	Three most common protocols on the network.
# of Unique IP Addresses	808 +2 (IPv4 +IPv6)	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	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

- Web browsing, dns queries, dhcp request.

Suspicious Activity

- malware downloaded, malware outbound traffic, torrent downloads

Normal Activity

Web Browsing

Summarize the following:

- What kind of traffic did you observe? **Browsing the internet - HTTP Traffic**
- Which protocol(s)? **Common Protocol Used: HTTP using TCP Port:80**
- What, specifically, was the user doing? Which site were they browsing? Etc.

Downloading Files http://detectportal.firefox.com/success.txt

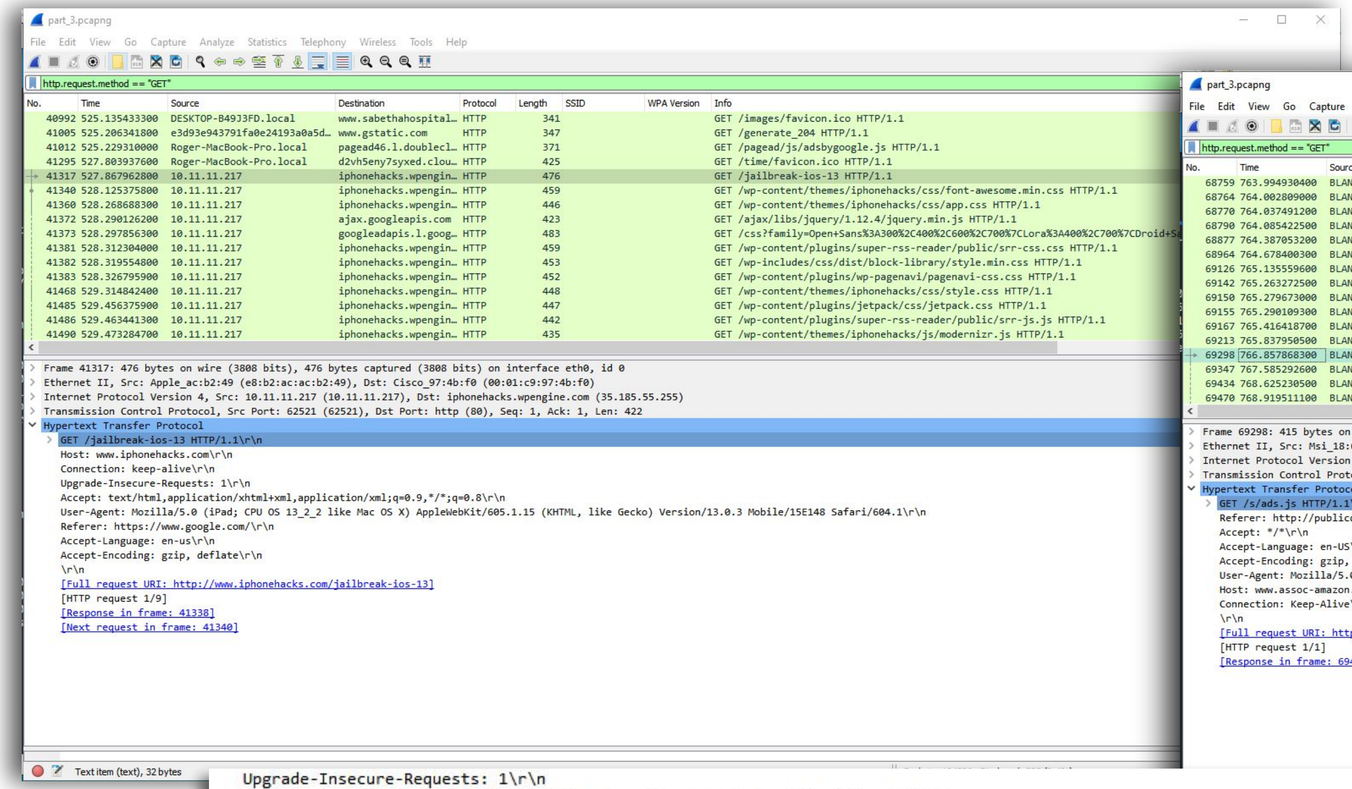
Uploading Files http://mysocalledchaos.com/wp-content/upload/2018/02/Beauty.jpg

Online Shopping http://www.assoc-amazon.com/s/ads.js

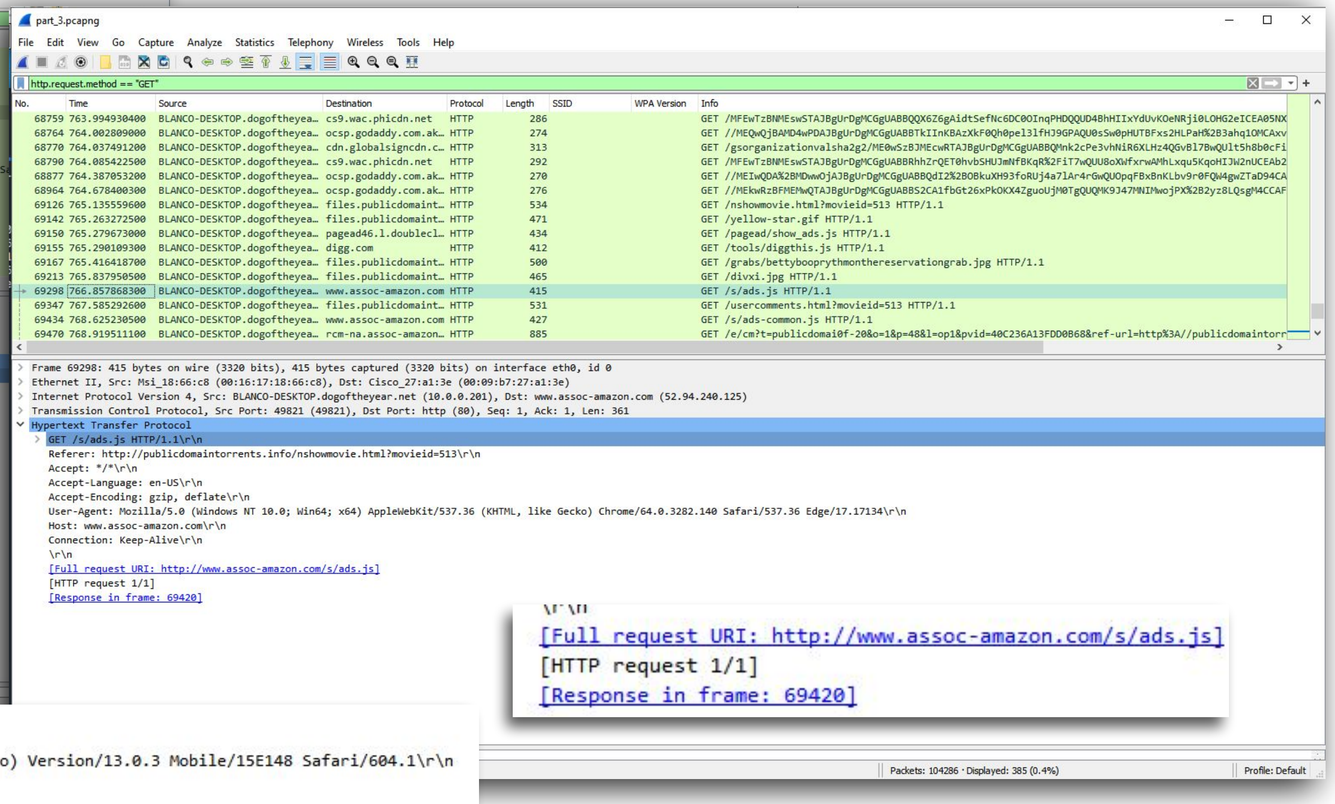
Searching http://www.iphonehacks.com/jailbreak-ios-13

Web Brosing

Searching (Example)

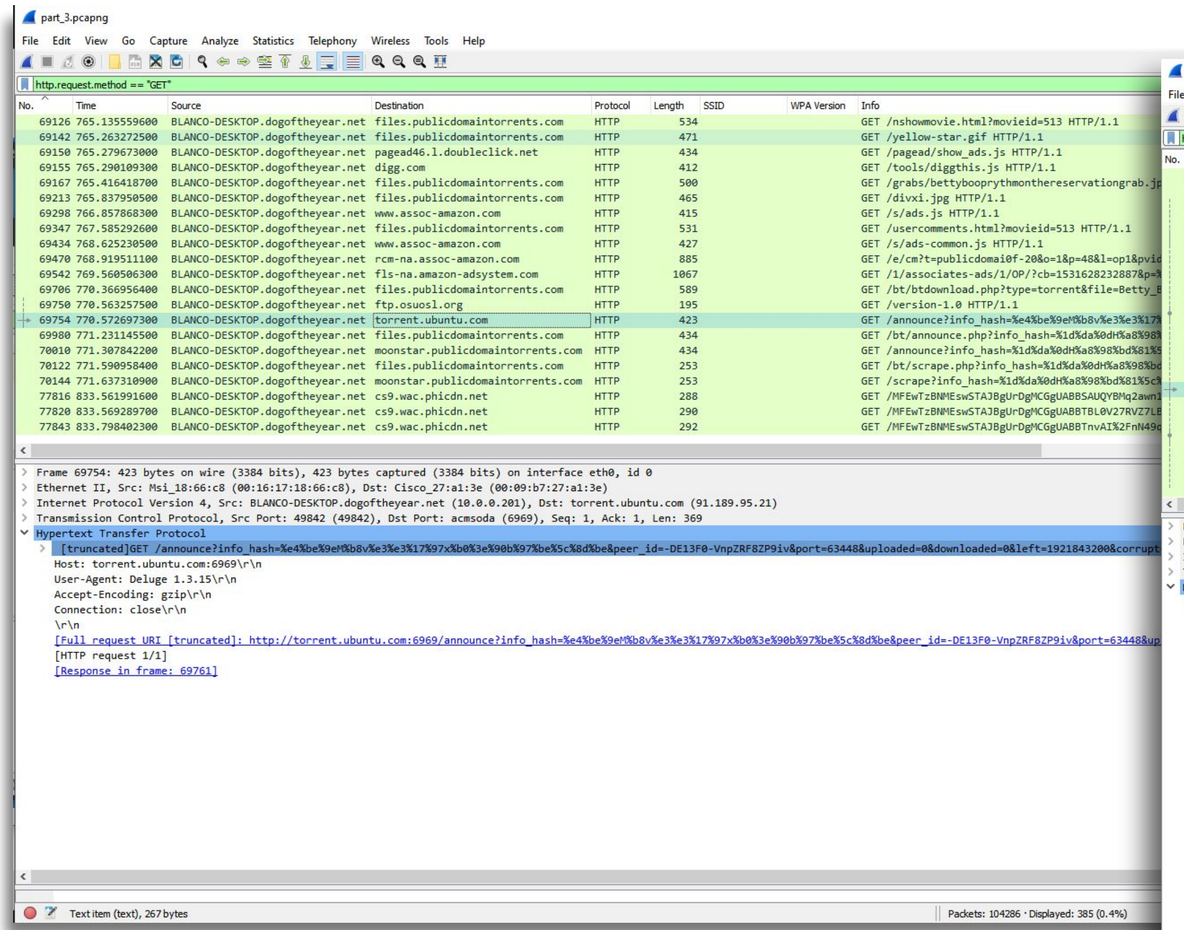


Online Shopping, Browsing ads (Example)

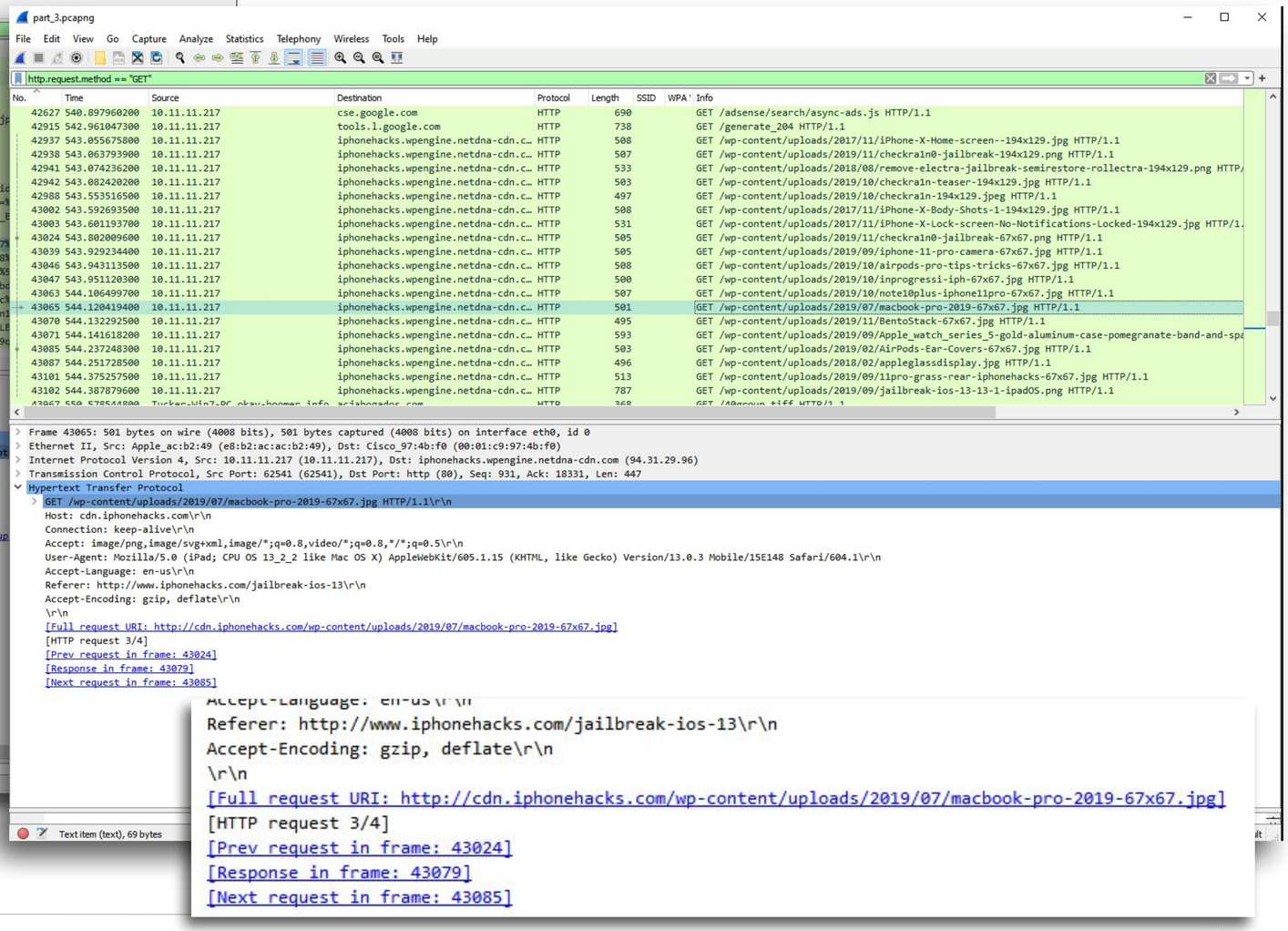


Web Browsing

Downloading a File (Example)

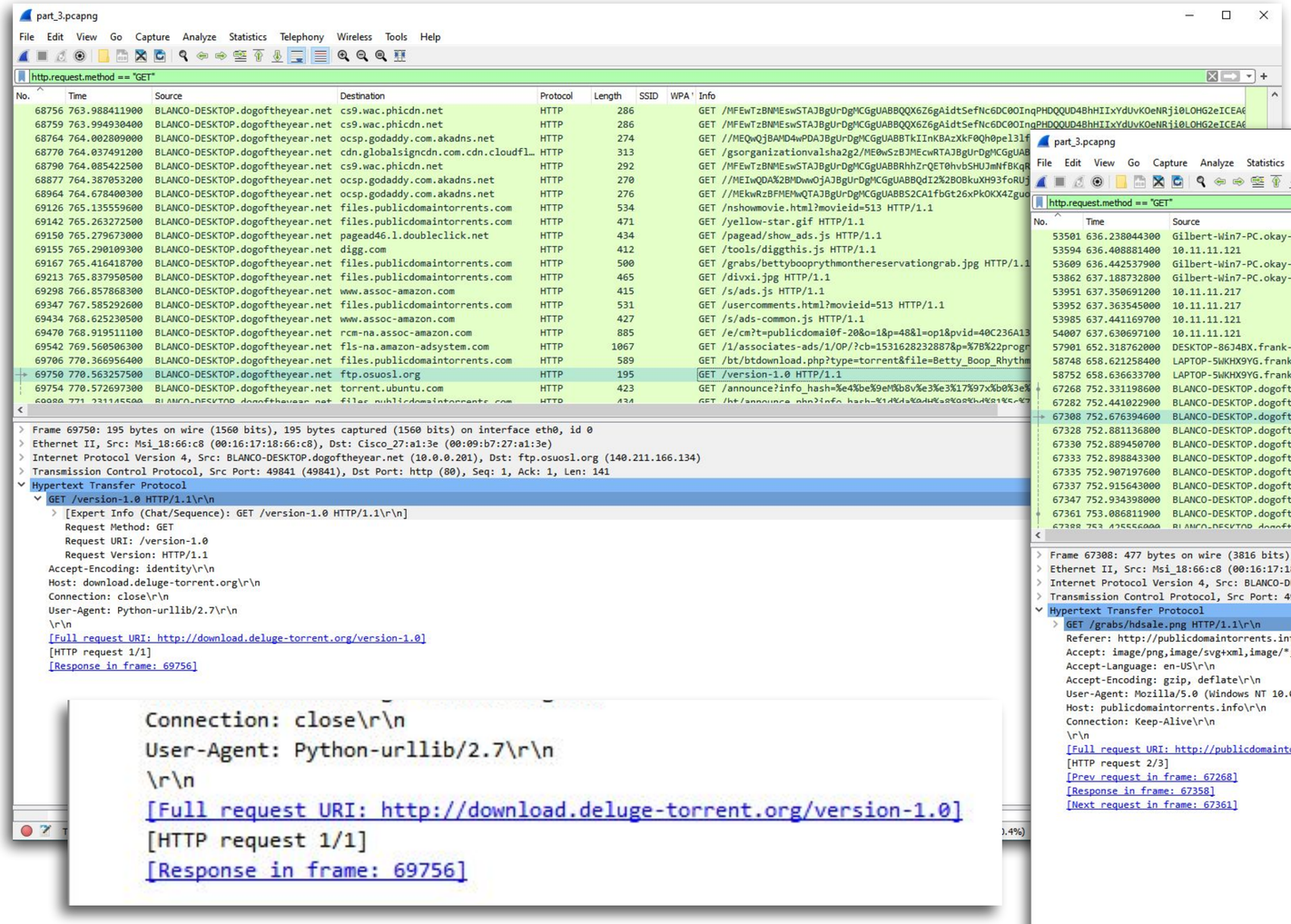


Uploading a File (Example)

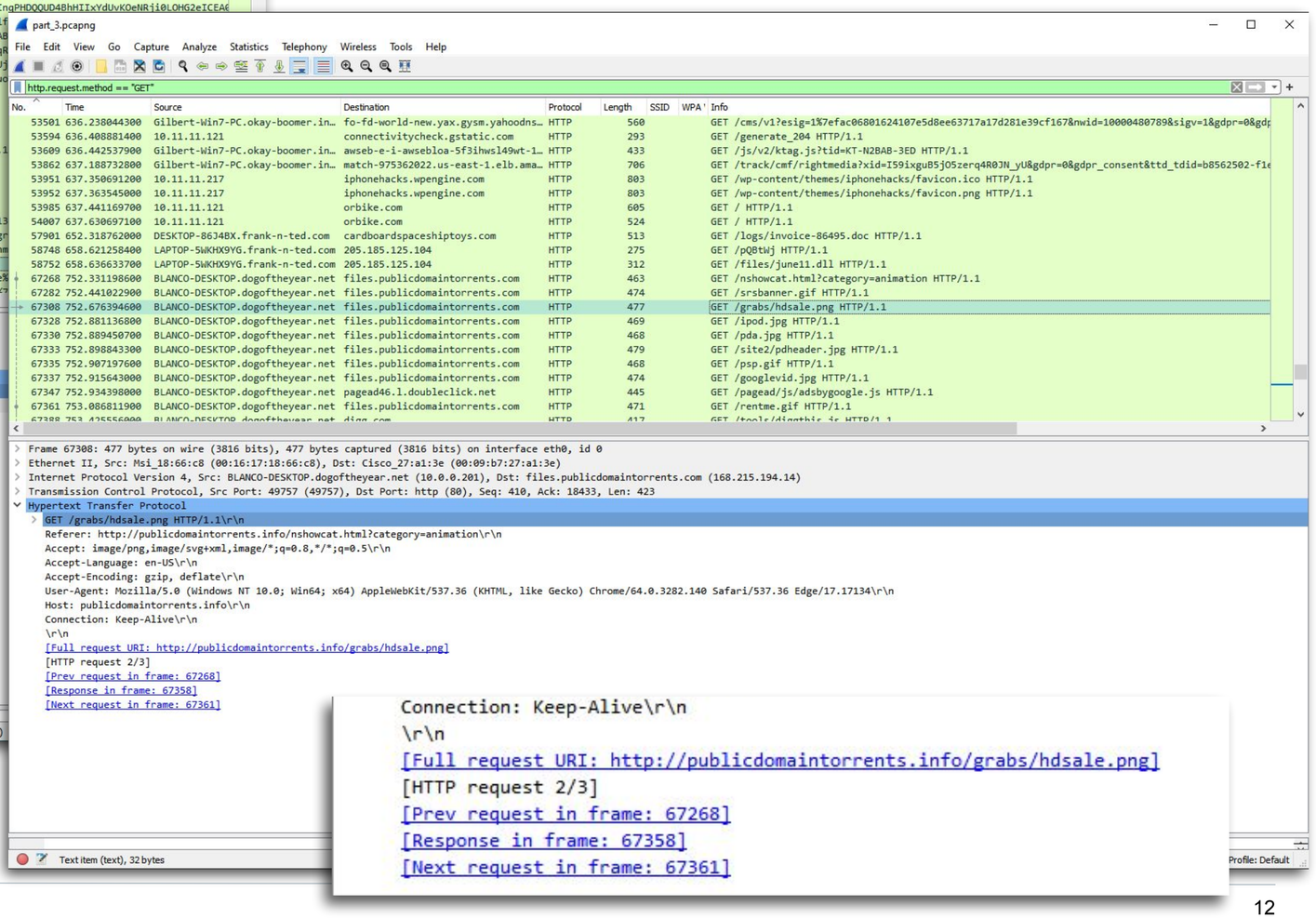


Web Browsing - Interesting Files

Torrent Application Download



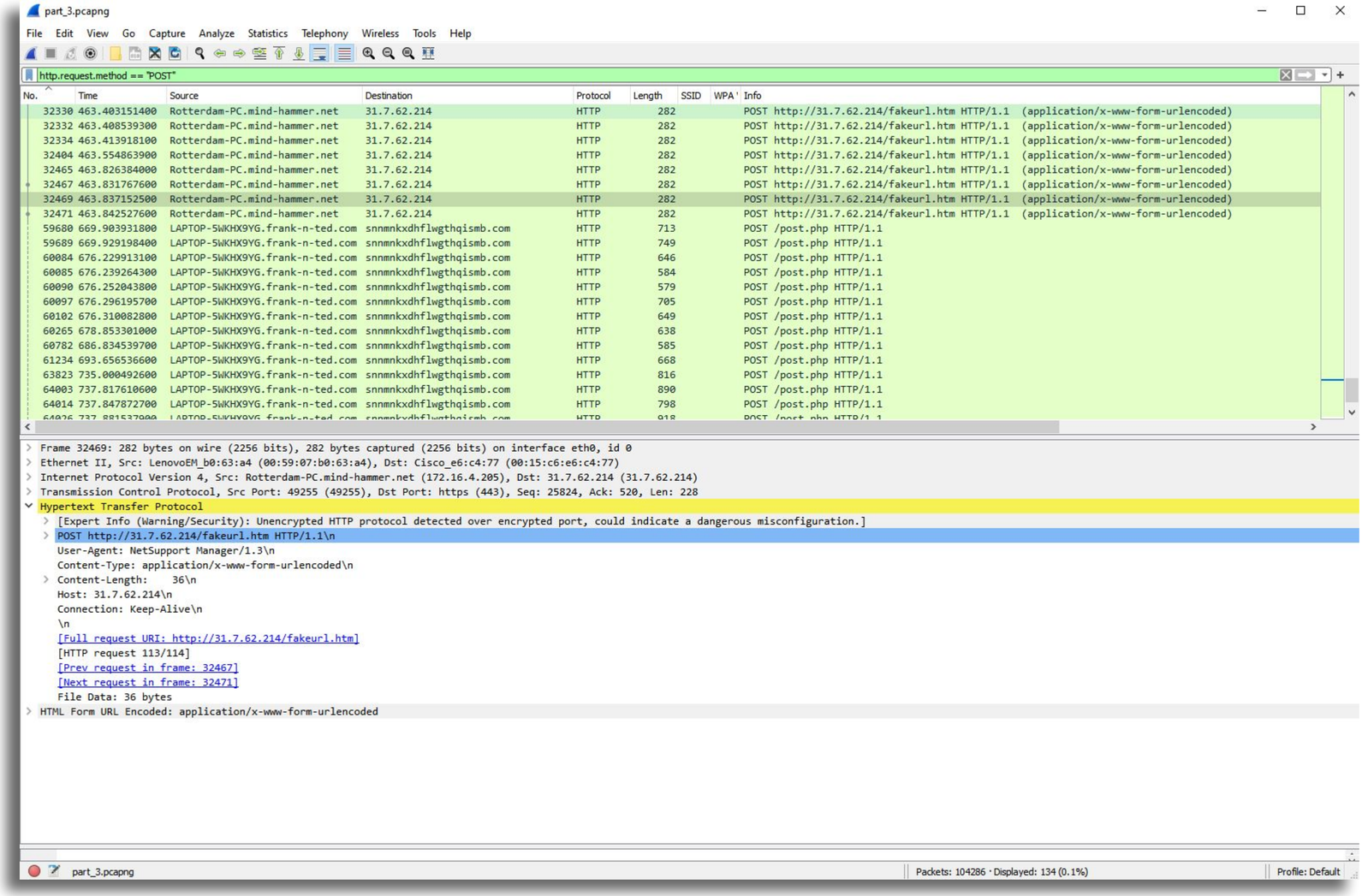
A file downloaded request from a Torrent Site



HTTP POST Request Method - Interesting Traffic

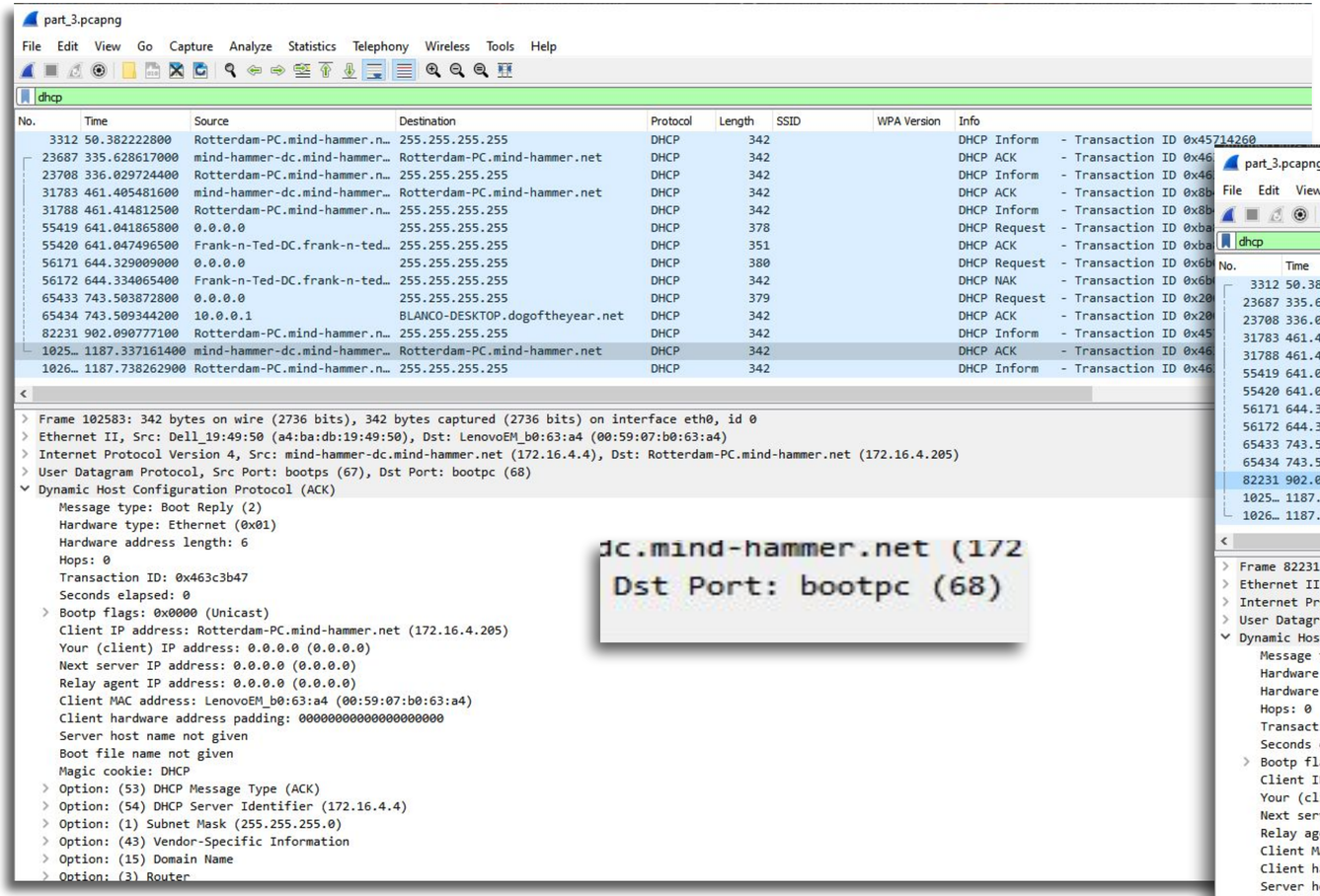
A post request method using secure HTTP connection

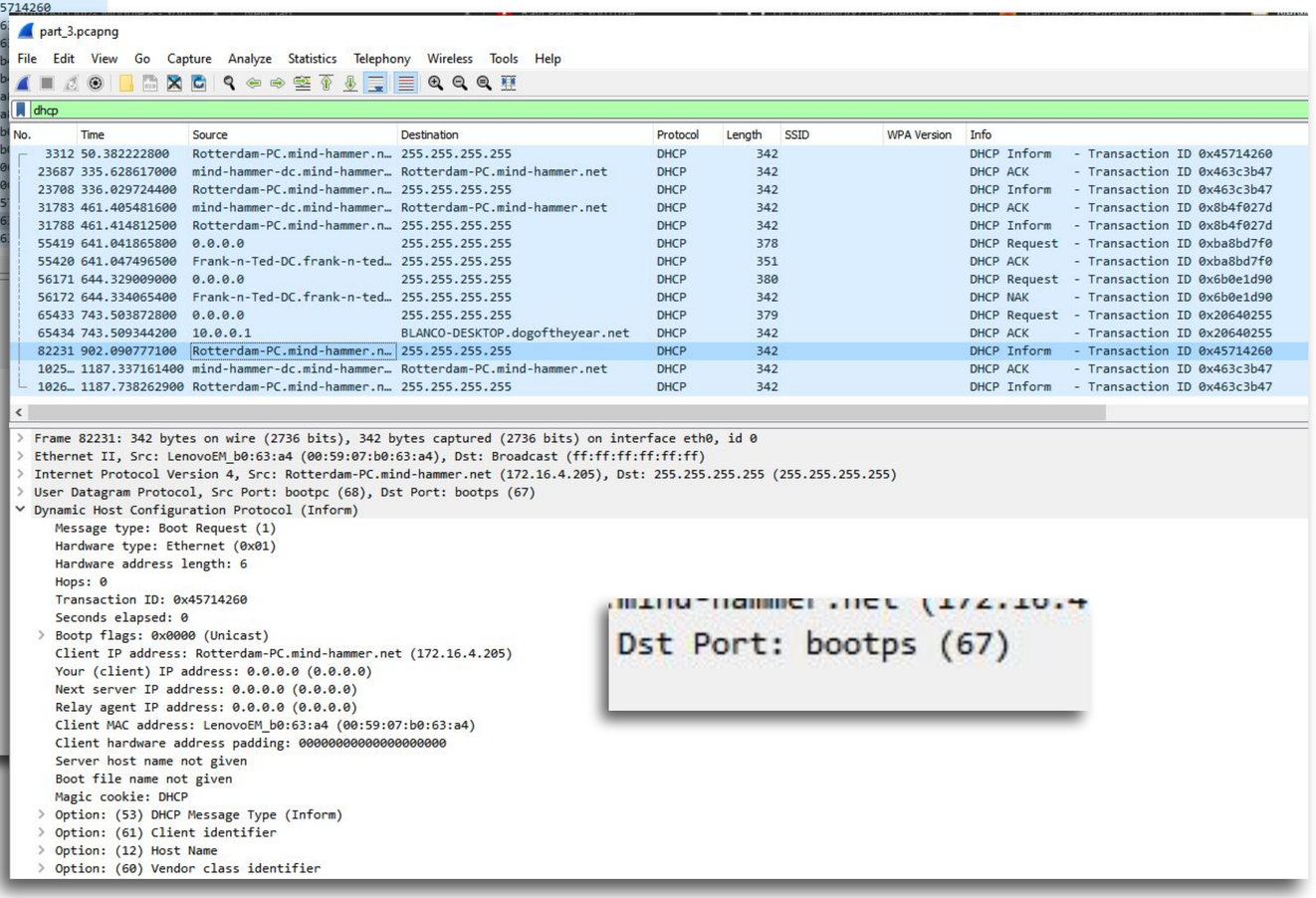
- What kind of traffic did you observe? Which protocol(s)?
  - The warning indicates that “Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous configuration”
  - The POST request Method is using a secure HTTP protocol TCP Port 443
  - There are multiple traffic found on the same request.



DHCP Request

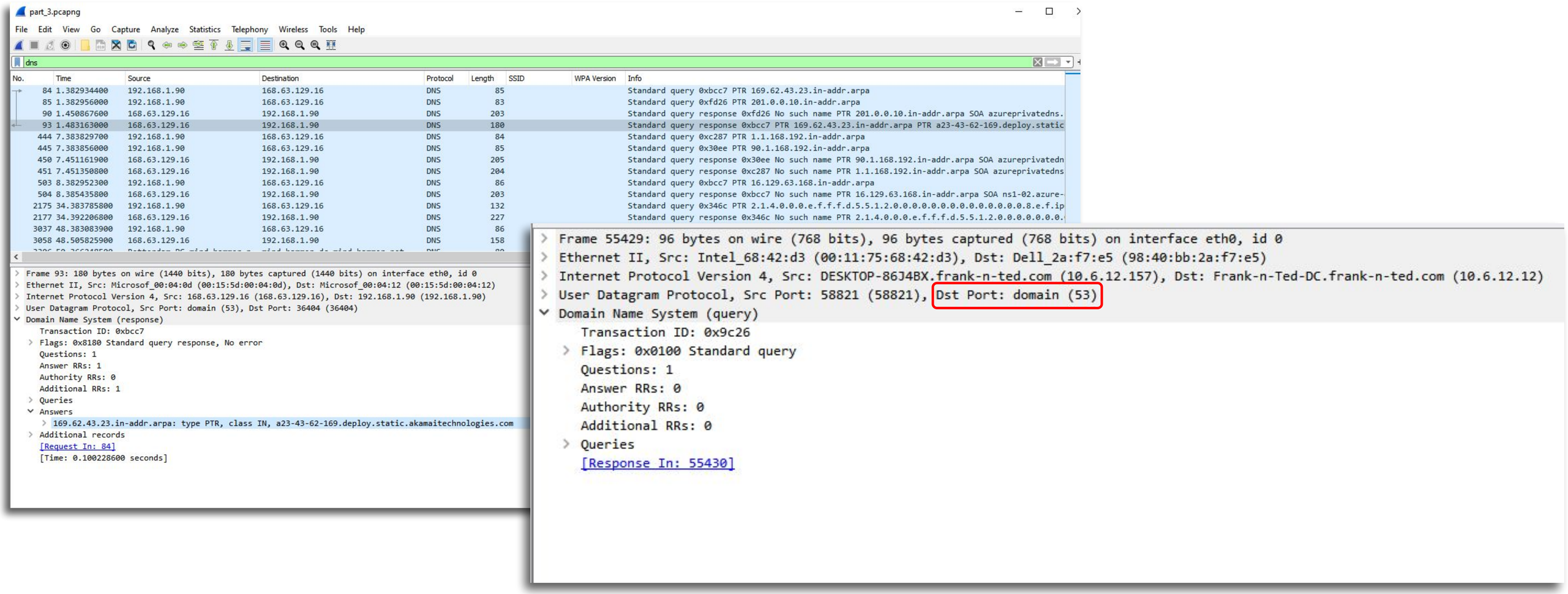
DHCP Protocol using UDP Port 67 and 68





DNS Queries / Interesting DNS Query

DNS Queries using UDP Port 53

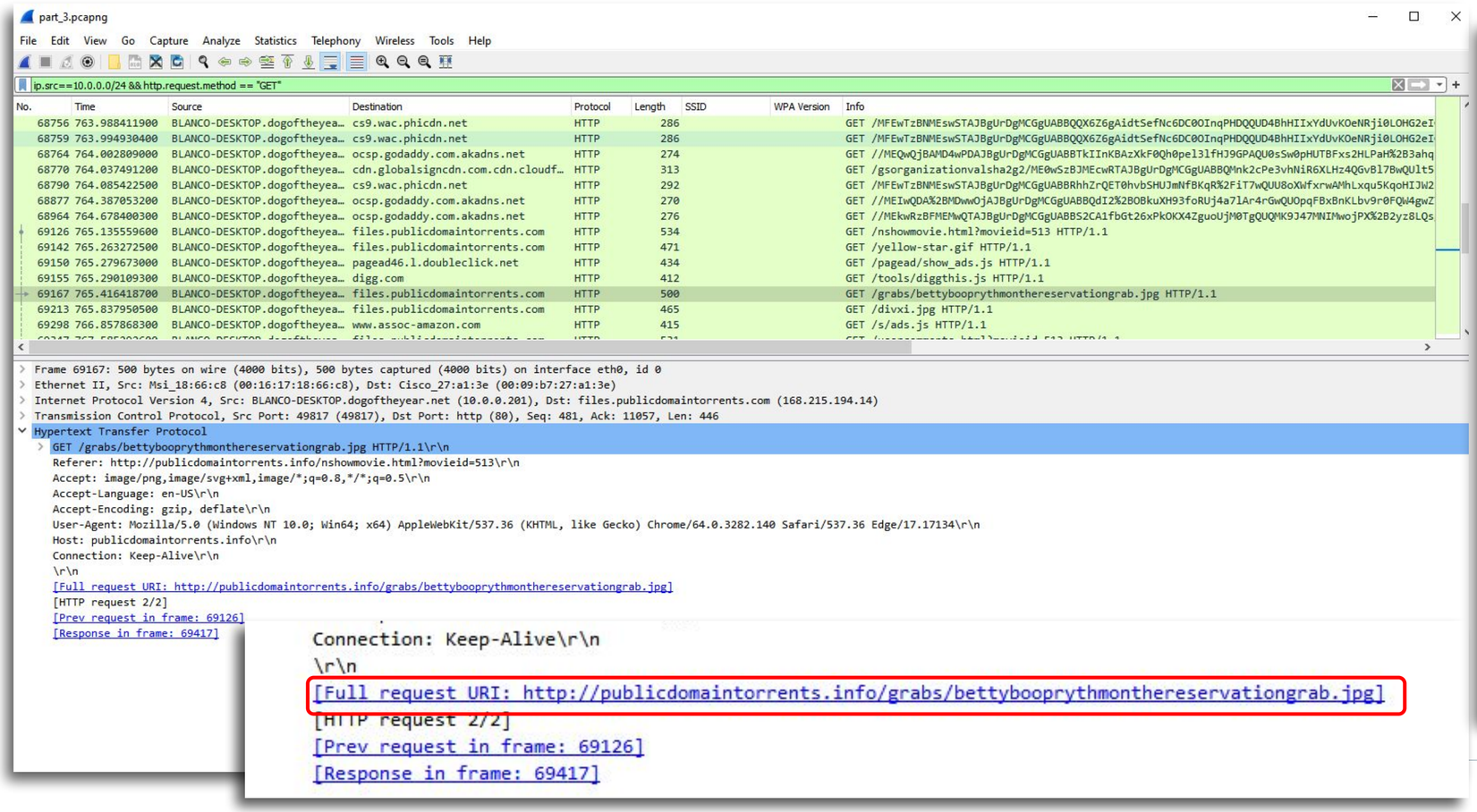


Malicious Activity

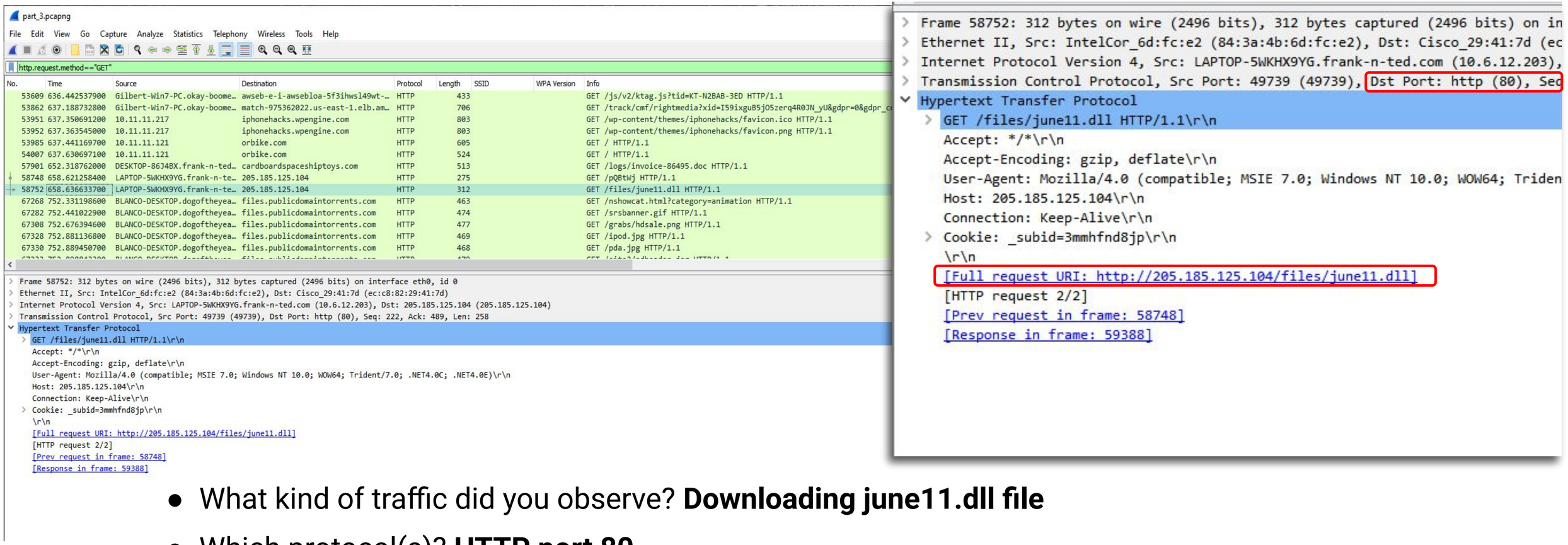
Torrenting copyright material

- What kind of traffic did you observe? **Downloading jpg from Torrent site**
- Which protocol(s)? **HTTP port 80**
- What, specifically, was the user doing? Which site were they browsing? Etc.

  http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrap.jpg



Malware download



- What kind of traffic did you observe? **Downloading june11.dll file**
- Which protocol(s)? **HTTP port 80**
- What, specifically,
- was the user doing?

Which site were they browsing?

http://205.185.125.104/files/june11.dll

The End