

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

By: Leo Katz

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



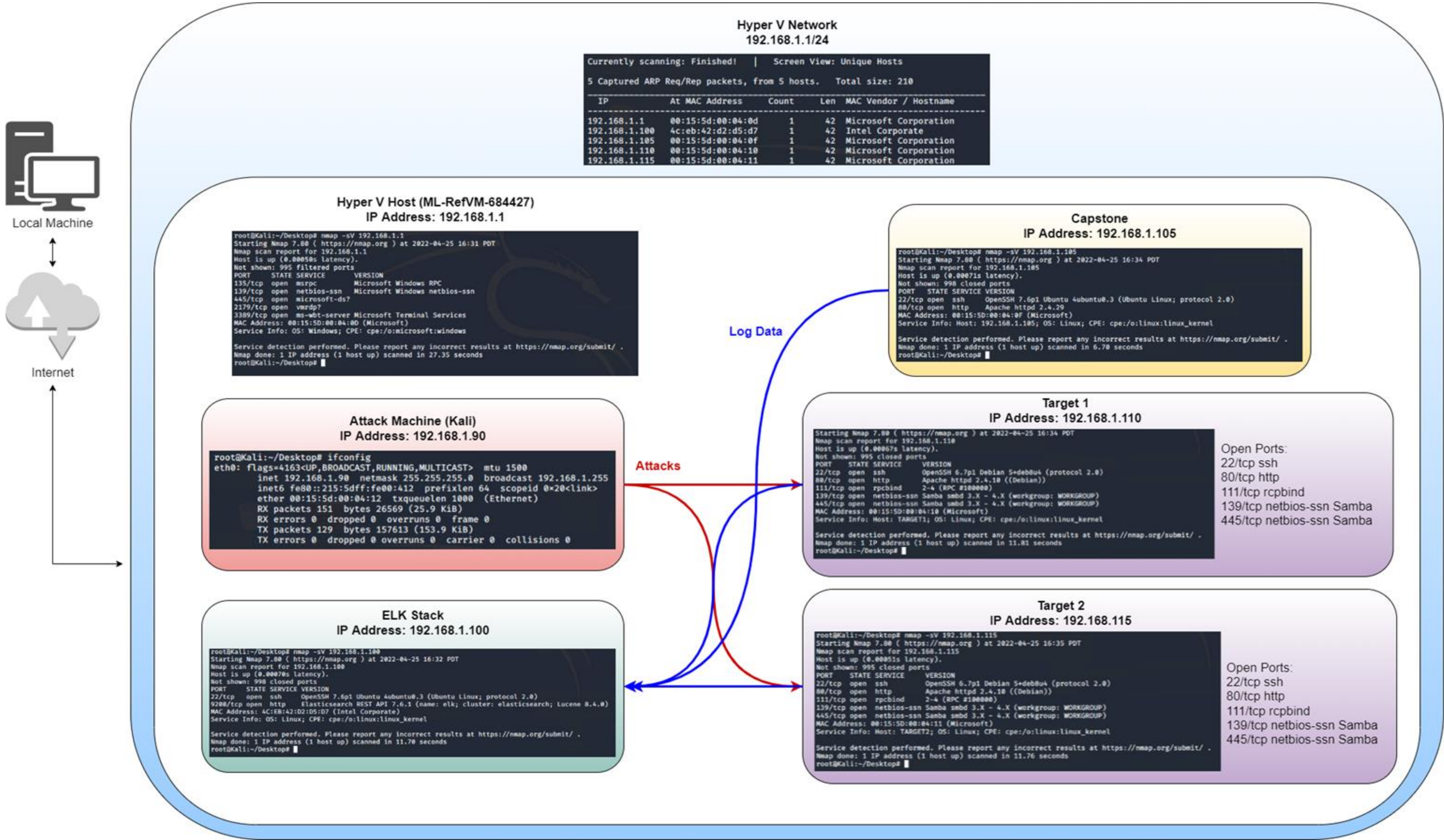
Normal Activity



Malicious Activity

Network Topology & Critical Vulnerabilities

Network Topology



Network

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

Machines

IPv4: 192.168.1.90
OS: Debian Kali 5.4.0
Hostname: Kali

IPv4: 192.168.1.110
OS: Debian GNU/Linux 8
Hostname: Target 1

IPv4: 192.168.1.115
OS: Debian GNU/Linux 8
Hostname: Target 2

IPv4: 192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Network Mapping & User Enumeration	Nmap was used to discover open ports.	Able to discover open ports and craft attacks against them.
Weak Passwords	A weak password was found just by guesswork.	This allowed SSH into the web server.
MySQL Credentials	Attackers were able to find a file with login information for the MySQL database.	Able to use the login information to gain access to the database.
MySQL Data Exfiltration	Attackers were able to find password hashes for all users.	Hashes can be cracked with tools such as John the Ripper—as long as they are not salted.
Unsalted Password Hashes	Stored password hashes were not salted with random characters.	The hashes were not salted, so another account was compromised.
Misconfiguration of Privileges	Steven’s account had sudo privileges for python.	Able to utilize Steven’s python privileges in order to escalate to root access.

Critical Vulnerabilities: Target 2

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

Vulnerability	Description	Impact
Network Mapping & URL Enumeration	Nmap was used to discover open ports, Nikto and Gobuster were used to list URLs.	Able to discover open ports, craft attacks, and find hidden directories.
Exposed Directory & Data	Plaintext information used to locate a hidden directory.	Reveal non-listed directories for vulnerabilities.
Remote Code Execution Vulnerability	Exploiting PHPMailer with a reverse shell.	Gain backdoor access into the target machine.
Weak Passwords	A weak password was found just by guesswork.	This allowed 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)	1. 172.16.4.205 2. 185.243.115.84 3. 5.101.51.151 4. 10.6.12.203 5. 166.62.111.64	Machines that sent the most traffic.
Most Common Protocols	1. TCP 2. TLS 3. HTTP	Three most common protocols on the network.
# of Unique IP Addresses	810 IPv4	Count of observed IP addresses.
Subnets	10.11.11.1/24, 10.6.12.1/24, 13.107.5.1/24, 172.217.0.0/16	Observed subnet ranges.
# of Malware Species	Trojan (june11.dll)	Number of malware binaries identified in traffic.

Behavioral Analysis

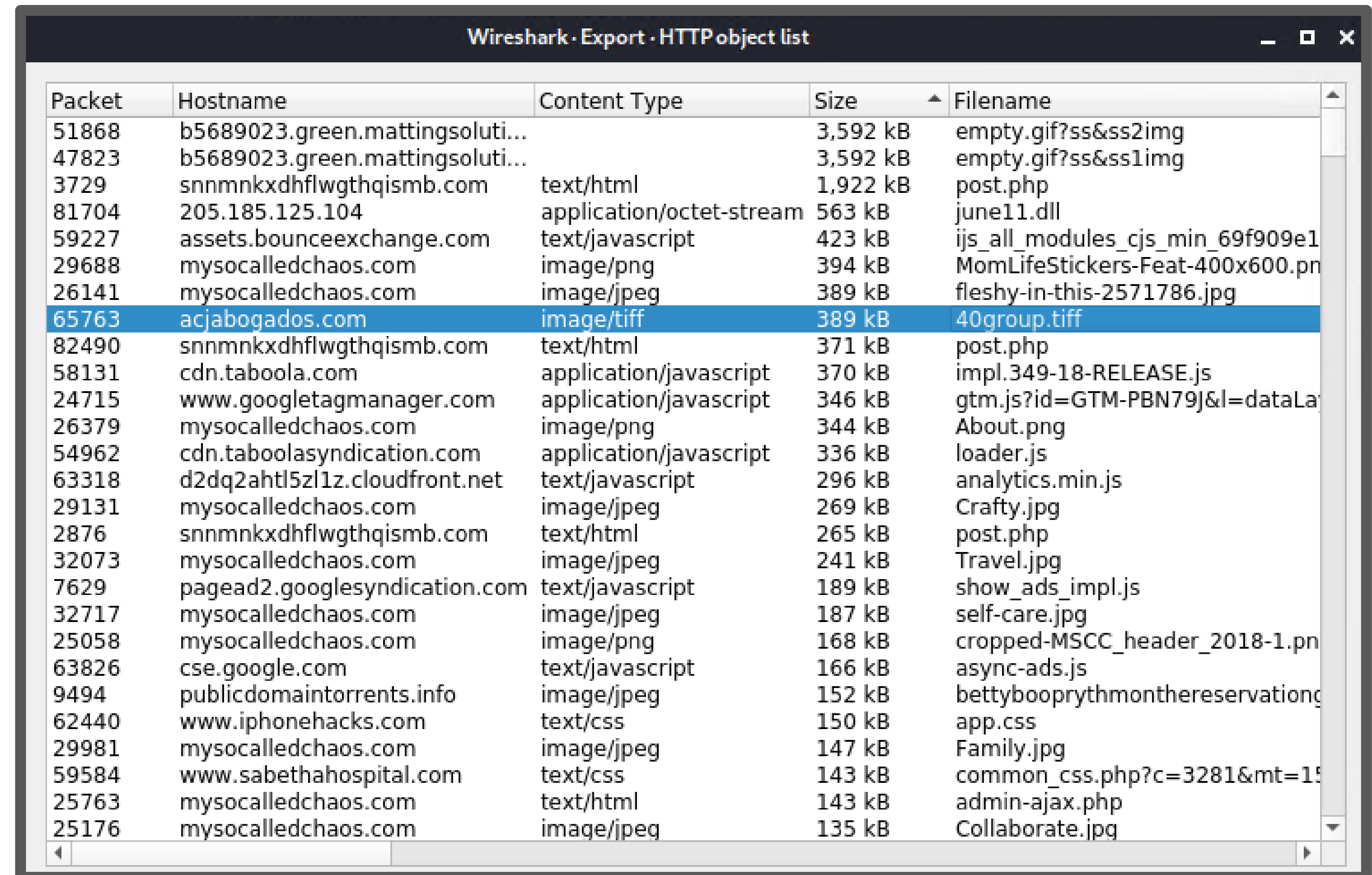
Purpose of Traffic on the Network

“Normal” Activity

- Web browsing
- Skype calls
- Website APIs
- Normal file transfers

Suspicious Activity

- Malware
- Spyware
- Illegal Downloads



Packet	Hostname	Content Type	Size	Filename
51868	b5689023.green.mattingssoluti...		3,592 kB	empty.gif?ss&ss2img
47823	b5689023.green.mattingssoluti...		3,592 kB	empty.gif?ss&ss1img
3729	snnmnkxdhflwgthqismb.com	text/html	1,922 kB	post.php
81704	205.185.125.104	application/octet-stream	563 kB	june11.dll
59227	assets.bounceexchange.com	text/javascript	423 kB	ijs_all_modules_cjs_min_69f909e1
29688	mysocalledchaos.com	image/png	394 kB	MomLifeStickers-Feat-400x600.pn
26141	mysocalledchaos.com	image/jpeg	389 kB	fleshy-in-this-2571786.jpg
65763	acjabogados.com	image/tiff	389 kB	40group.tiff
82490	snnmnkxdhflwgthqismb.com	text/html	371 kB	post.php
58131	cdn.taboola.com	application/javascript	370 kB	impl.349-18-RELEASE.js
24715	www.googletagmanager.com	application/javascript	346 kB	gtm.js?id=GTM-PBN79J&l=dataLa
26379	mysocalledchaos.com	image/png	344 kB	About.png
54962	cdn.taboolasyndication.com	application/javascript	336 kB	loader.js
63318	d2dq2ahtl5zl1z.cloudfront.net	text/javascript	296 kB	analytics.min.js
29131	mysocalledchaos.com	image/jpeg	269 kB	Crafty.jpg
2876	snnmnkxdhflwgthqismb.com	text/html	265 kB	post.php
32073	mysocalledchaos.com	image/jpeg	241 kB	Travel.jpg
7629	pagead2.googlesyndication.com	text/javascript	189 kB	show_ads_impl.js
32717	mysocalledchaos.com	image/jpeg	187 kB	self-care.jpg
25058	mysocalledchaos.com	image/png	168 kB	cropped-MSCC_header_2018-1.pn
63826	cse.google.com	text/javascript	166 kB	async-ads.js
9494	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationc
62440	www.iphonehacks.com	text/css	150 kB	app.css
29981	mysocalledchaos.com	image/jpeg	147 kB	Family.jpg
59584	www.sabethahospital.com	text/css	143 kB	common_css.php?c=3281&mt=15
25763	mysocalledchaos.com	text/html	143 kB	admin-ajax.php
25176	mysocalledchaos.com	image/jpeg	135 kB	Collaborate.jpg



Normal Activity

Standard Web Traffic

Types of Traffic & Protocols

- Vast majority of traffic was TCP
 - Kerberos
 - Data
 - VSS Monitoring Ethernet trailer
- BitTorrent
- Hypertext Transfer Protocol
 - JavaScript Object Notation
 - Line-based text data
 - Images–JPEG, PNG, GIF

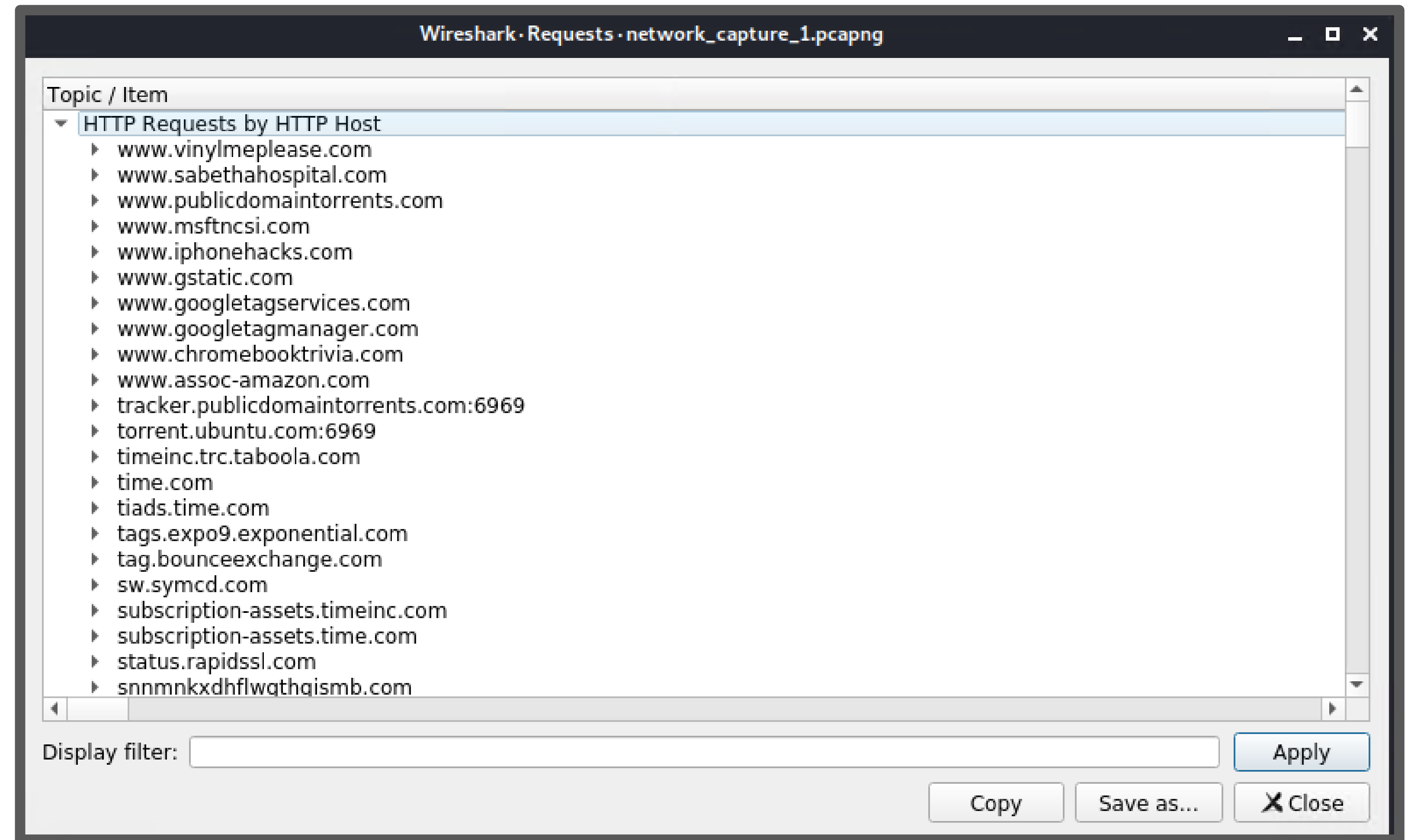
Protocol	Percent Packets	Packets	Percent Bytes	B
Multicast Domain Name System	0.1	104	0.0	1
Simple Service Discovery Protocol	0.1	112	0.0	1
Connectionless Lightweight Directory Access Protocol	0.2	158	0.0	3
NetBIOS Name Service	0.5	511	0.0	3
ADwin configuration protocol	0.7	687	0.1	7
Domain Name System	4.2	4018	0.4	3
Data	7.6	7191	4.6	3
▼ Transmission Control Protocol	86.2	82048	90.9	7
Malformed Packet	0.0	13	0.0	0
Kerberos	0.3	284	0.4	3
Data	0.3	288	0.8	6
VSS Monitoring Ethernet trailer	0.6	585	0.0	1
▼ Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.7	638	0.2	1
Local Security Authority	0.0	8	0.0	1
Microsoft Network Logon	0.0	42	0.0	1
SAMR (pidl)	0.0	45	0.0	2
DCE/RPC Endpoint Mapper	0.1	92	0.0	1
DRSUAPI	0.3	252	0.0	3
Lightweight Directory Access Protocol	0.7	679	0.4	3
BitTorrent	0.9	877	0.1	5
▼ NetBIOS Session Service	0.9	886	0.3	2
SMB (Server Message Block Protocol)	0.0	22	0.0	2
SMB2 (Server Message Block Protocol version 2)	1.0	914	0.3	2
▼ Hypertext Transfer Protocol	4.8	4594	60.0	5
eXtensible Markup Language	0.0	3	0.0	2
Malformed Packet	0.0	4	0.0	0
Compuserve GIF	0.0	13	0.0	1
Online Certificate Status Protocol	0.0	23	0.0	2
Portable Network Graphics	0.0	38	9.9	8
JPEG File Interchange Format	0.0	41	2.6	2
Media Type	0.1	112	4.0	3
HTML Form URL Encoded	0.1	120	0.0	2
Line-based text data	0.1	132	8.0	6
JavaScript Object Notation	1.6	1529	36.9	3
Transport Layer Security	11.2	10637	14.8	1

No display filter

Standard Web Traffic

User Activity & Sites Visited

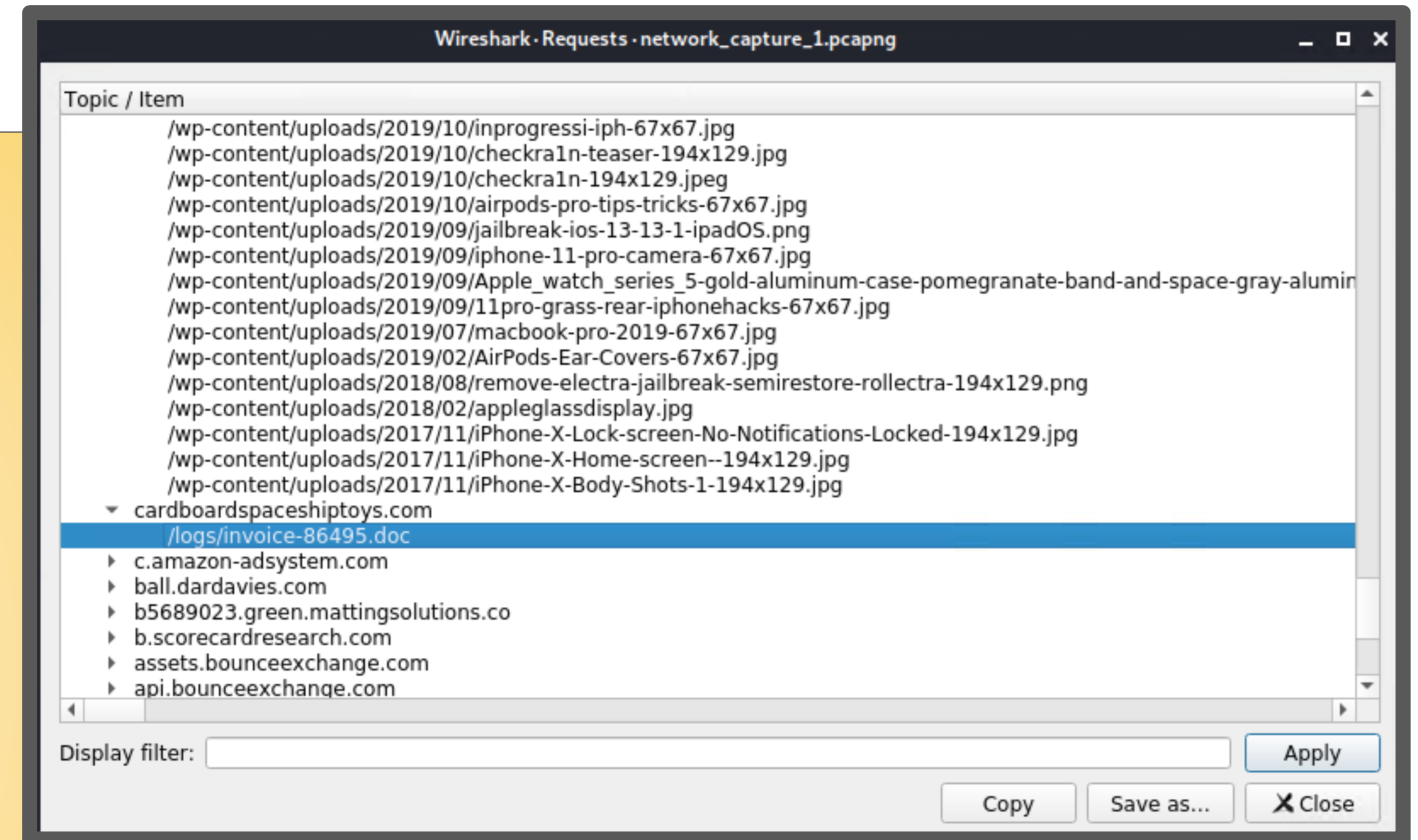
- Common sites
 - time.com
 - instagram.com
- Wordpress sites
 - iphonehacks.com
 - mysocalledchaos.com
- Uncommon sites
 - vinylmeplease.com
 - sabethahospital.com
 - dogoftheyear.net



Standard Web Traffic

Interesting Files

- post.php from snnmnkxdhflwgthqismb.com
 - Large html/text file
- 40group.tiff from acjabogados.com
 - Lossless image format
- invoice-86495.doc from cardboardspaceshiptoy.com
 - Financial details?
 - Social engineering?
- ijs_all_modules_cjs_min_69f909e1f154dad67bb582362cdca3b2.js
- impl.349-18-RELEASE.js



Malicious Activity

Malware

- Two thieves created a web server on the corporate network
 - HTTP & TCP traffic
- Browsing Frank-n-Ted-DC.frank-n-ted.com
- Downloaded “june11.dll”
 - Dynamic link library
 - Contains code, used by more than one program at a time
- This file is actually a Trojan Horse
 - Most often called Trojan.Mint.Zamg.O
 - Ransomware
 - Buffer overflow
 - Encrypt data
 - Hide network activity
 - Lock accounts or devices

80059

822.432672300

DESKTOP-86J4BX.frank-n-ted.com

cardboardspaceship

81044

828.735165700

LAPTOP-5WKHX9YG.frank-n-ted.com

205.185.125.104

81048

828.750543100

LAPTOP-5WKHX9YG.frank-n-ted.com

205.185.125.104

Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80)

Hypertext Transfer Protocol

GET /files/june11.dll HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]

[GET /files/june11.dll HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /files/june11.dll

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; .NET4.0 E) Host: 205.185.125.104\r\n

VirusTotal - File - d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

https://www.virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

GoogleIpdate.exe

invalid-signature overlay pedll signed spreader

50

/ 69

Community Score

50 security vendors and 1 sandbox flagged this file as malicious

549.84 KB

2022-04-18 23:52:42 UTC

12 days ago

DLL

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

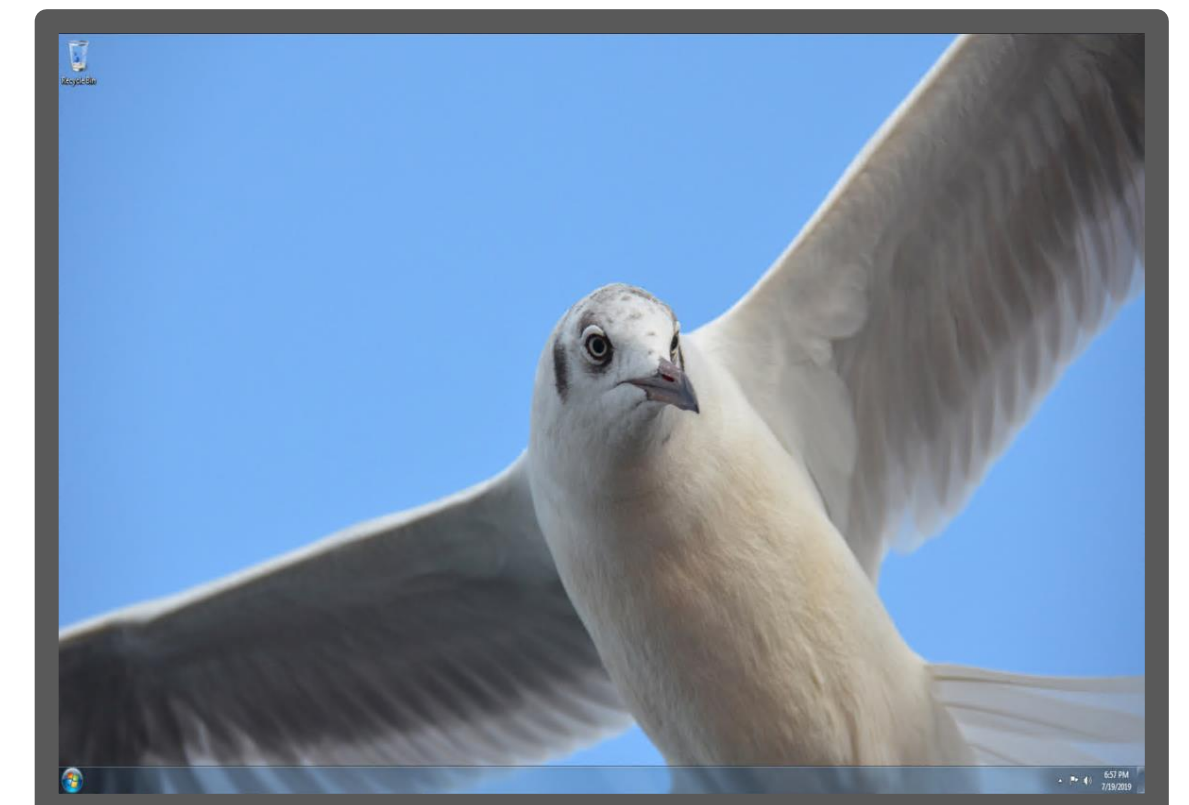
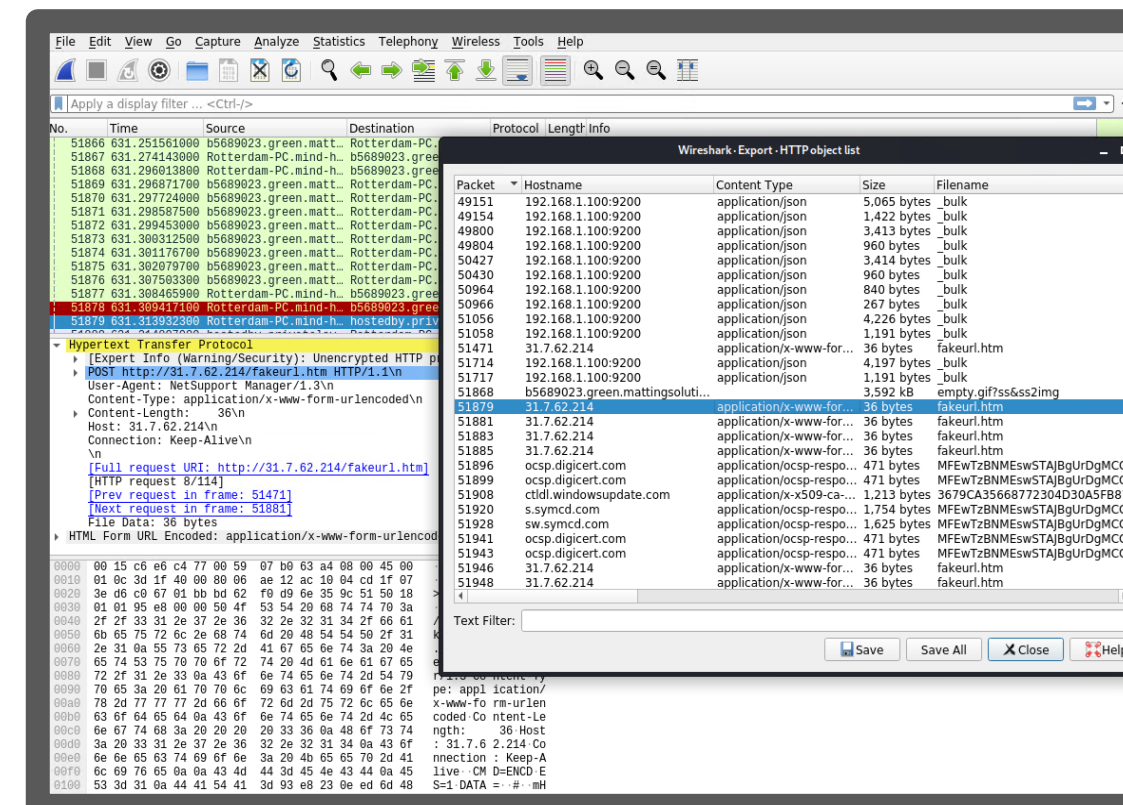
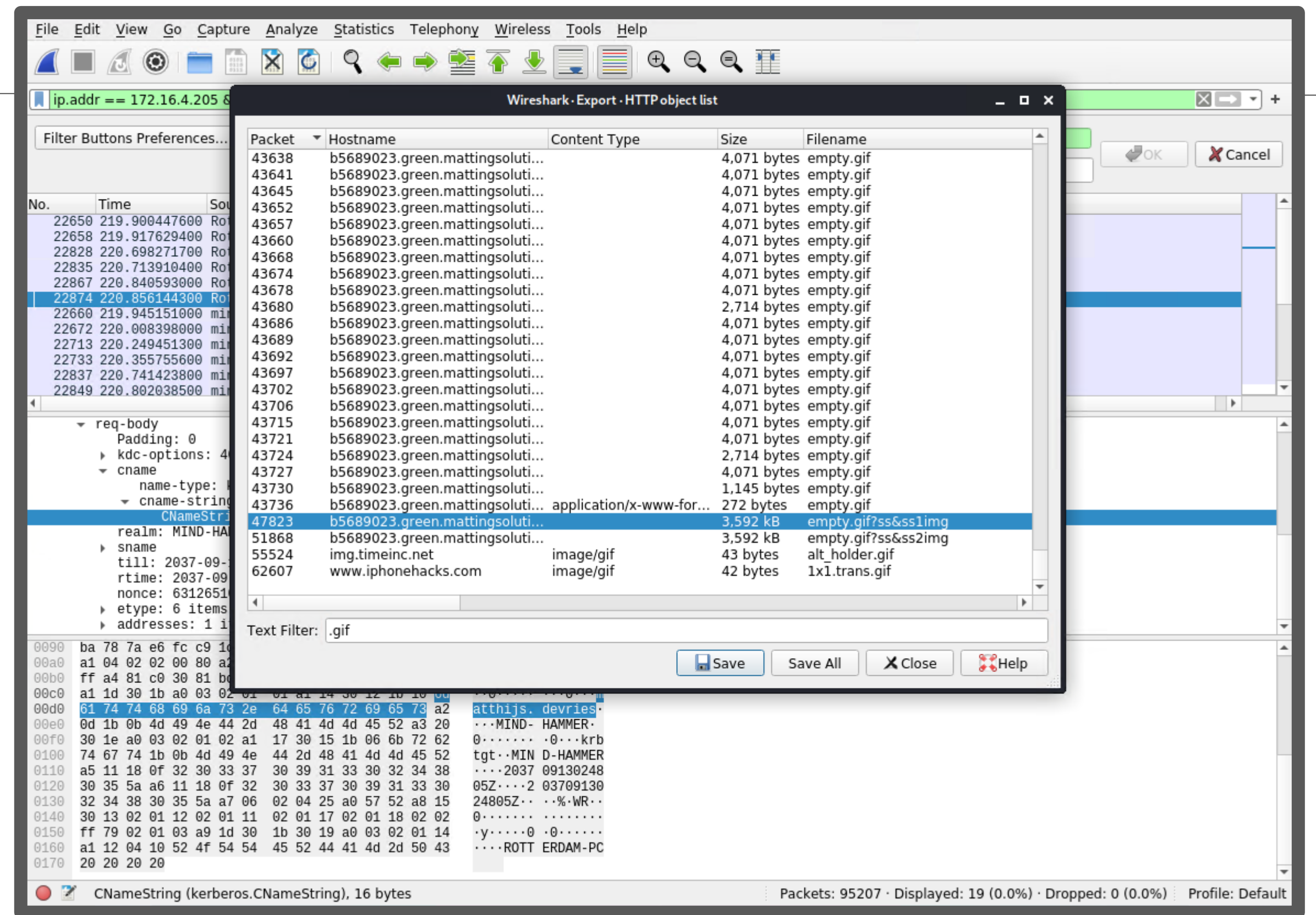
Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	GrayWare/Win32.Kryptik.ehls	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	Gen:NN.ZedlaF.34606.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)

15

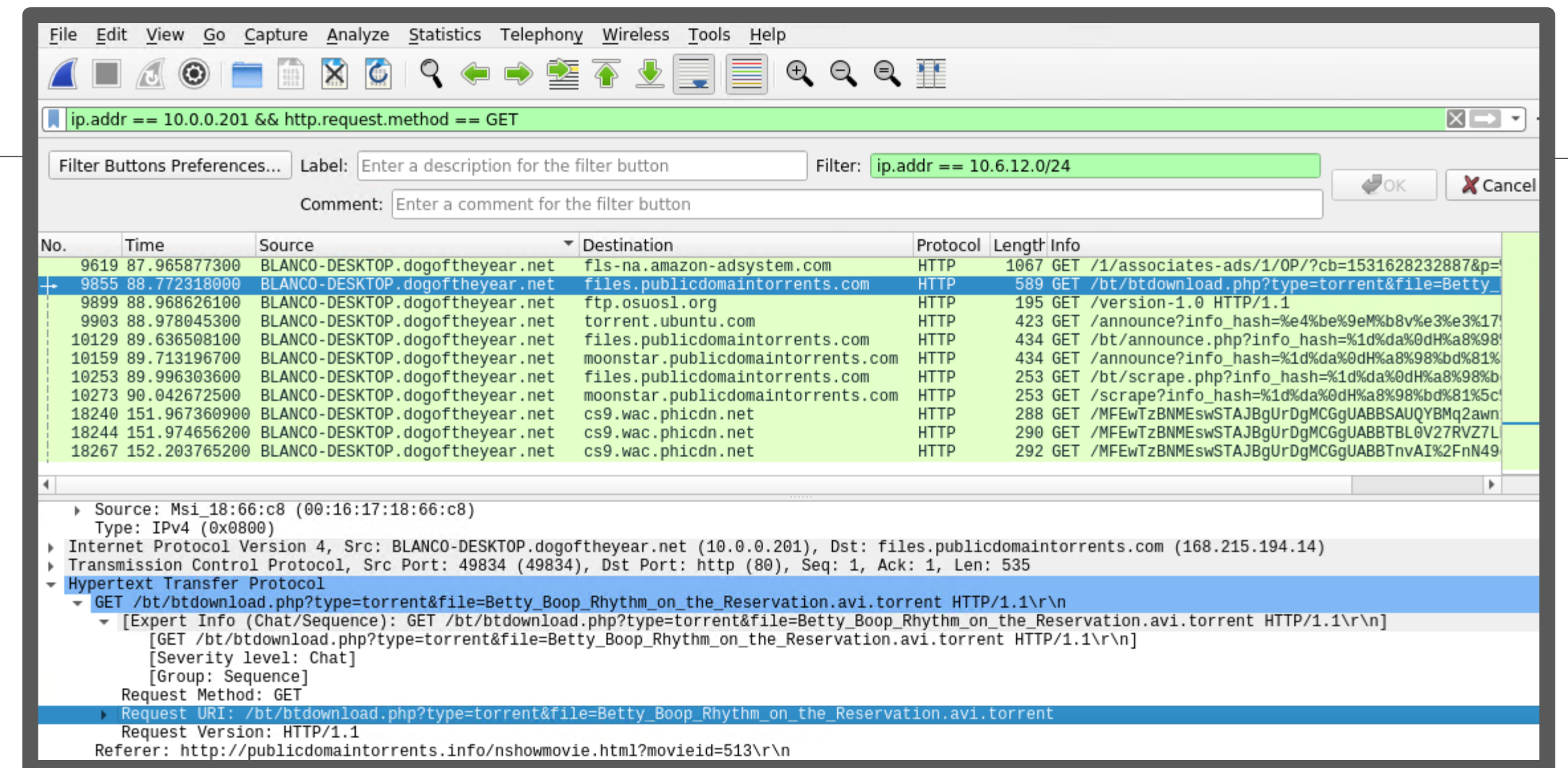
Spyware

- The Security team has received reports of an infected Windows host on the network
 - IP Address: 172.16.4.205
 - Username “matthijs.devries”
- Traffic to and from the host was HTTP & TCP
- Host was conversing with
 - “b5689023.green.mattingsolutions.co”
 - Keep alive to 31.7.62.214/fakeurl.htm
- Discovered a screenshot of the host’s desktop
 - Spyware, Trojan, or even Keylogger



Illegal Downloads

- The Security team has received reports of torrenting on the network
 - Decentralized peer-to-peer file sharing
 - Copyright infringement
 - IP Address: 10.0.0.201
 - Username “elmer.blanco”
- The user browsed “publicdomaintorrents.com”
- The user downloaded
“Betty_Boop_Rhythm_on_the_Reservation.avi.torrent”
- Though the short itself is public domain,
the character herself is currently under copyright





The End