Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

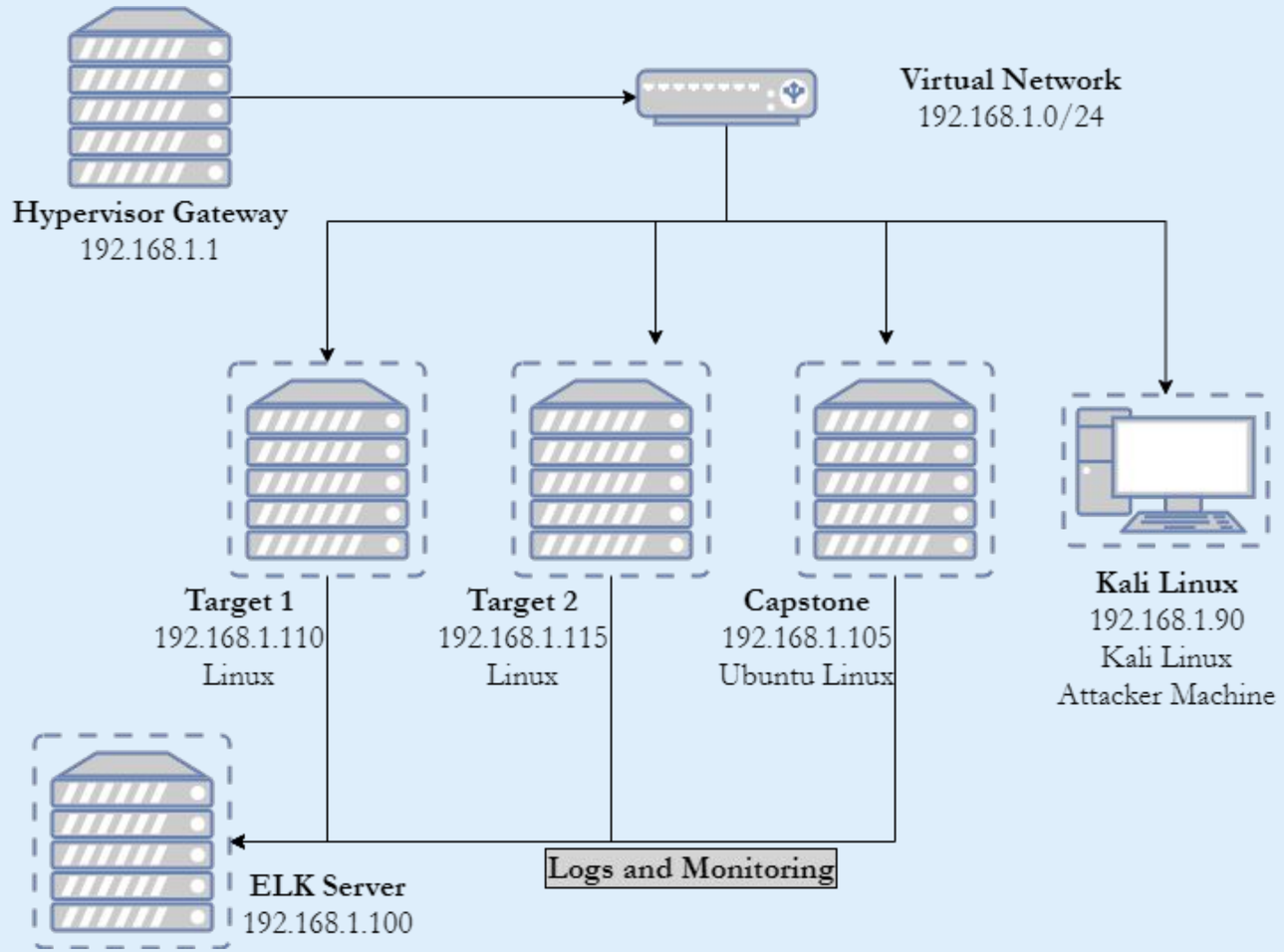
Liam, Shane, Isaac, Graham

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: Debian Kali 5.4.0
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu Linux 18.04
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu Linux 18.04
Hostname: Capstone

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

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 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	Packets / Bytes TCP 88.5% / 89.6% UDP 11.0% / 0.1%	Three most common protocols on the network.
# of Unique IP Addresses	808 IPv4	Count of observed IP addresses.
Subnets	10.0.0.0/24 10.6.12.0/24 172.16.4.0/24	Observed subnet ranges.
# of Malware Species	1 - june11.dll (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

- Browsing the web
- Watching Youtube

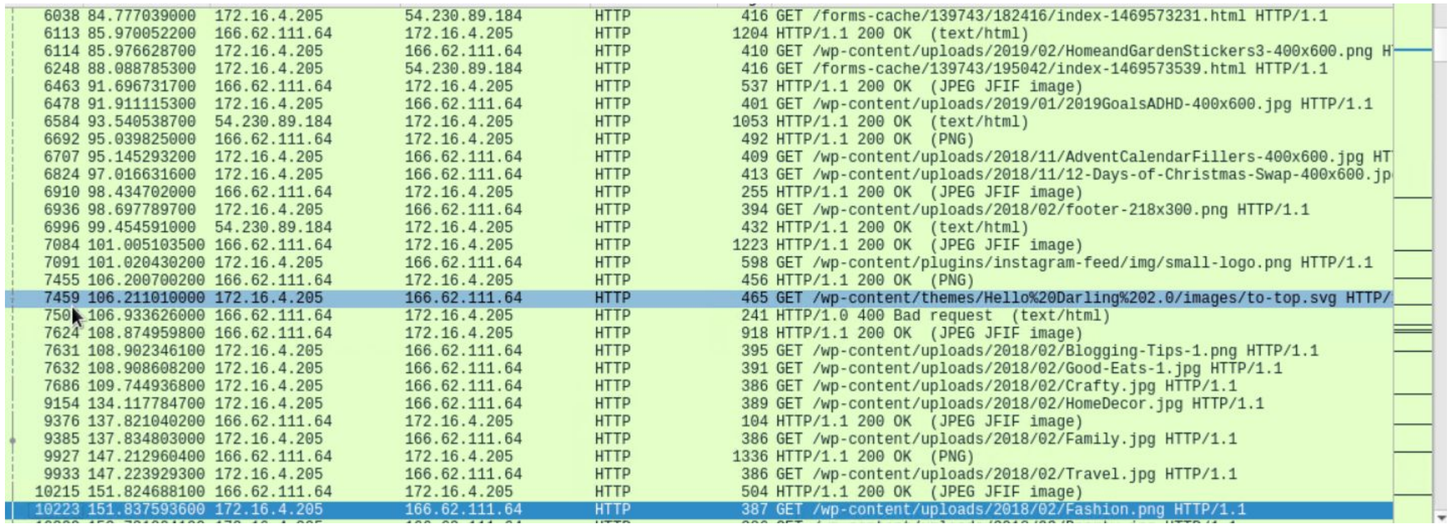
Suspicious Activity

- Malware Infection
- Illegal file downloads

Normal Activity

Browsing the Web

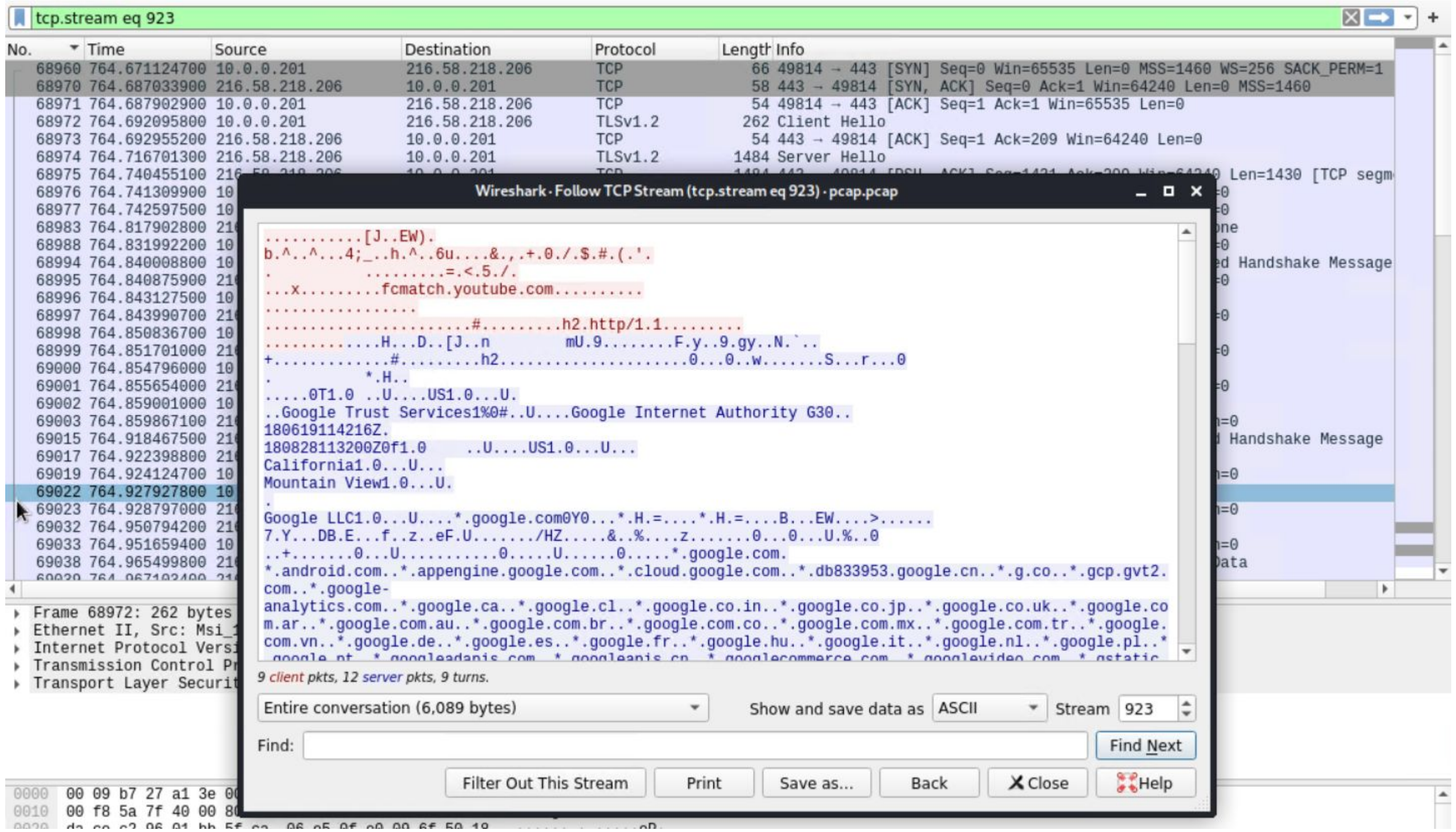
- Normal usage, browsing a wordpress framework based website.
- Normal use of HTTP



6038	84.777039000	172.16.4.205	54.230.89.184	HTTP	416	GET /forms-cache/139743/182416/index-1469573231.html HTTP/1.1
6113	85.970052200	166.62.111.64	172.16.4.205	HTTP	1204	HTTP/1.1 200 OK (text/html)
6114	85.976628700	172.16.4.205	166.62.111.64	HTTP	410	GET /wp-content/uploads/2019/02/HomeandGardenStickers3-400x600.png H
6248	88.088785300	172.16.4.205	54.230.89.184	HTTP	416	GET /forms-cache/139743/195042/index-1469573539.html HTTP/1.1
6463	91.696731700	166.62.111.64	172.16.4.205	HTTP	537	HTTP/1.1 200 OK (JPEG JFIF image)
6478	91.911115300	172.16.4.205	166.62.111.64	HTTP	401	GET /wp-content/uploads/2019/01/2019GoalsADHD-400x600.jpg HTTP/1.1
6584	93.540538700	54.230.89.184	172.16.4.205	HTTP	1053	HTTP/1.1 200 OK (text/html)
6692	95.039825000	166.62.111.64	172.16.4.205	HTTP	492	HTTP/1.1 200 OK (PNG)
6707	95.145293200	172.16.4.205	166.62.111.64	HTTP	409	GET /wp-content/uploads/2018/11/AdventCalendarFillers-400x600.jpg HT
6824	97.016631600	172.16.4.205	166.62.111.64	HTTP	413	GET /wp-content/uploads/2018/11/12-Days-of-Christmas-Swap-400x600.jp
6910	98.434702000	166.62.111.64	172.16.4.205	HTTP	255	HTTP/1.1 200 OK (JPEG JFIF image)
6936	98.697789700	172.16.4.205	166.62.111.64	HTTP	394	GET /wp-content/uploads/2018/02/footer-218x300.png HTTP/1.1
6996	99.454591000	54.230.89.184	172.16.4.205	HTTP	432	HTTP/1.1 200 OK (text/html)
7084	101.005103500	166.62.111.64	172.16.4.205	HTTP	1223	HTTP/1.1 200 OK (JPEG JFIF image)
7091	101.020430200	172.16.4.205	166.62.111.64	HTTP	598	GET /wp-content/plugins/instagram-feed/img/small-logo.png HTTP/1.1
7455	106.200700200	166.62.111.64	172.16.4.205	HTTP	456	HTTP/1.1 200 OK (PNG)
7459	106.211010000	172.16.4.205	166.62.111.64	HTTP	465	GET /wp-content/themes/Hello%20Darling%202.0/images/to-top.svg HTTP/
750	106.933626000	166.62.111.64	172.16.4.205	HTTP	241	HTTP/1.0 400 Bad request (text/html)
7624	108.874959800	166.62.111.64	172.16.4.205	HTTP	918	HTTP/1.1 200 OK (JPEG JFIF image)
7631	108.902346100	172.16.4.205	166.62.111.64	HTTP	395	GET /wp-content/uploads/2018/02/Blogging-Tips-1.png HTTP/1.1
7632	108.908608200	172.16.4.205	166.62.111.64	HTTP	391	GET /wp-content/uploads/2018/02/Good-Eats-1.jpg HTTP/1.1
7686	109.744936800	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Crafty.jpg HTTP/1.1
9154	134.117784700	172.16.4.205	166.62.111.64	HTTP	389	GET /wp-content/uploads/2018/02/HomeDecor.jpg HTTP/1.1
9376	137.821040200	166.62.111.64	172.16.4.205	HTTP	104	HTTP/1.1 200 OK (JPEG JFIF image)
9385	137.834803000	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Family.jpg HTTP/1.1
9927	147.212960400	166.62.111.64	172.16.4.205	HTTP	1336	HTTP/1.1 200 OK (PNG)
9933	147.223929300	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Travel.jpg HTTP/1.1
10215	151.824688100	166.62.111.64	172.16.4.205	HTTP	504	HTTP/1.1 200 OK (JPEG JFIF image)
10223	151.837593600	172.16.4.205	166.62.111.64	HTTP	387	GET /wp-content/uploads/2018/02/Fashion.png HTTP/1.1

Watching Youtube

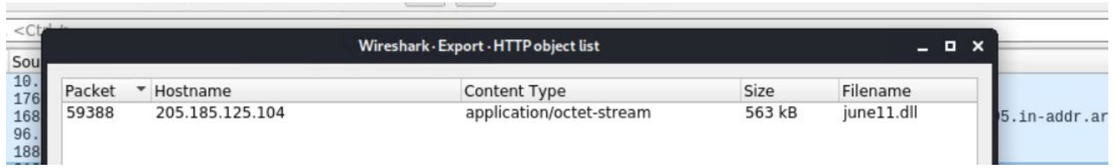
- TCP and TLS traffic to YouTube.com

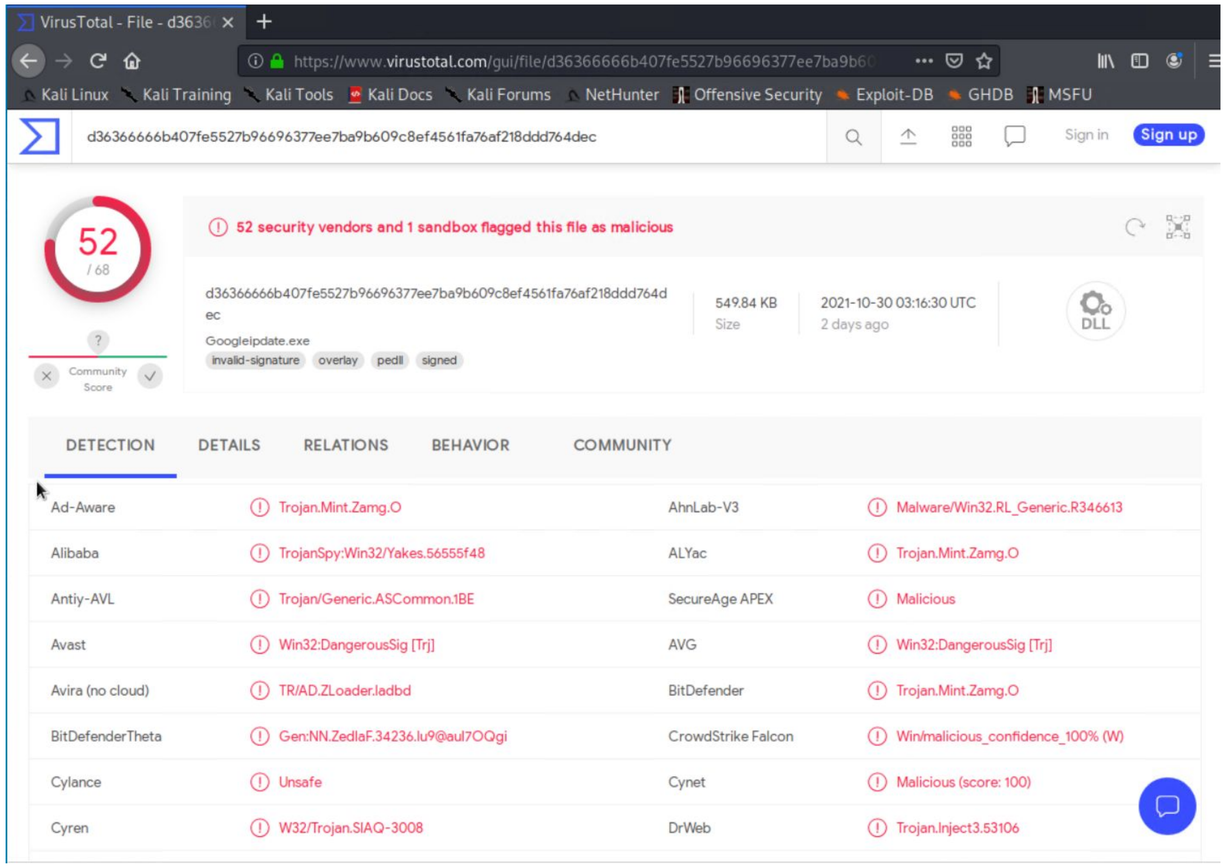


Malicious Activity

Malware Infection

- Malicious file download “june11.dll”

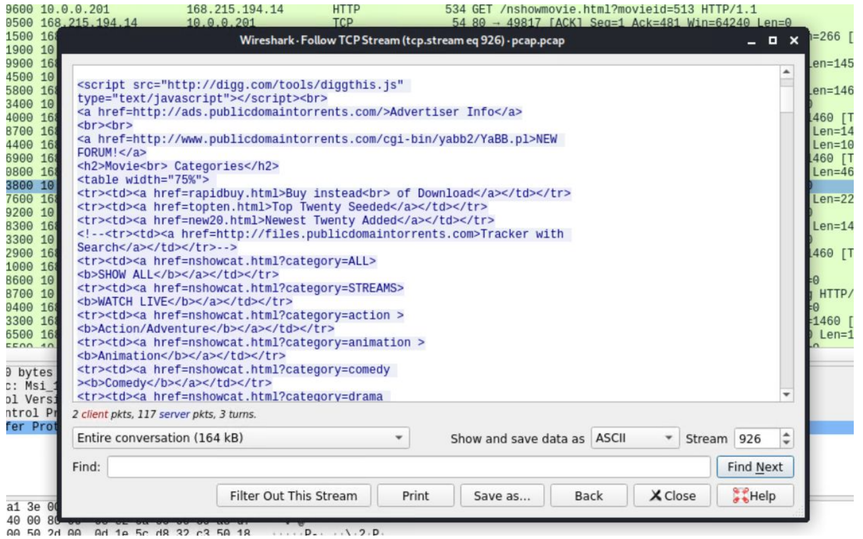


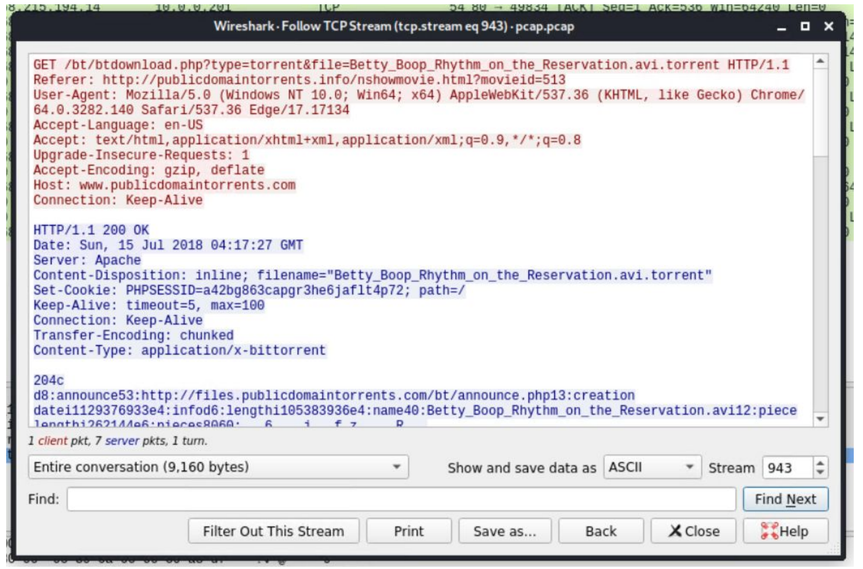


Illegal File Downloads

- Browsing for copyright material on public bittorrent tracker
- Downloading and fetching torrent data

No.	Time	Source	Destination	Protocol	Length	Info
69962	771.188649000	10.0.0.201	62.210.200.57	BitTorrent	122	Handshake
69984	771.237608300	62.210.200.57	10.0.0.201	BitTorrent	242	Handshake Extended
69985	771.249874200	10.0.0.201	62.210.200.57	BitTorrent	766	Extended Bitfield, Len:0x1cb Port
69991	771.262422900	10.0.0.201	61.245.142.233	BitTorrent	122	Handshake
70023	771.349215200	62.210.200.57	10.0.0.201	BitTorrent	513	Bitfield, Len:0x1cb
70146	771.640256500	61.245.142.233	10.0.0.201	BitTorrent	122	Handshake
70147	771.646483900	10.0.0.201	61.245.142.233	BitTorrent	397	Extended Have All Allowed Fast, Piece (Idx:0xf5) Allowed Fast, Pi
70163	771.676909400	10.0.0.201	82.102.24.163	BitTorrent	122	Handshake
70172	771.693627900	82.102.24.163	10.0.0.201	BitTorrent	242	Handshake Extended
70174	771.705913800	10.0.0.201	82.102.24.163	BitTorrent	766	Extended Bitfield, Len:0x1cb Port
70189	771.748350200	61.245.142.233	10.0.0.201	BitTorrent	361	Extended Have All Port Extended
70198	771.770384100	82.102.24.163	10.0.0.201	BitTorrent	513	Bitfield, Len:0x1cb
70218	771.797941500	10.0.0.201	23.82.53.139	BitTorrent	122	Handshake
70224	771.811840100	23.82.53.139	10.0.0.201	BitTorrent	242	Handshake Extended
70225	771.824090500	10.0.0.201	23.82.53.139	BitTorrent	764	Extended Bitfield, Len:0x1cb Port
70233	771.849697900	23.82.53.139	10.0.0.201	BitTorrent	513	Bitfield, Len:0x1cb
70254	771.897834100	10.0.0.201	96.237.60.19	BitTorrent	122	Handshake
70280	771.961740600	96.237.60.19	10.0.0.201	BitTorrent	122	Handshake
70281	771.968101100	10.0.0.201	96.237.60.19	BitTorrent	395	Extended Have All Allowed Fast, Piece (Idx:0xa7f) Allowed Fast, P
70283	771.972078300	96.237.60.19	10.0.0.201	BitTorrent	197	Extended Have All Port
70288	771.982319100	10.0.0.201	91.160.64.33	BitTorrent	122	Handshake
70295	771.991831400	91.160.64.33	10.0.0.201	BitTorrent	122	Handshake
70296	771.998158300	10.0.0.201	91.160.64.33	BitTorrent	395	Extended Have All Allowed Fast, Piece (Idx:0x4e7) Allowed Fast, P
70304	772.016563600	91.160.64.33	10.0.0.201	BitTorrent	289	Extended Have All Port Extended
70315	772.031395800	10.0.0.201	85.17.122.98	BitTorrent	122	Handshake
70320	772.048179300	85.17.122.98	10.0.0.201	BitTorrent	457	Handshake Extended Have All Allowed Fast, Piece (Idx:0x2bb) Allo
70321	772.054508200	10.0.0.201	85.17.122.98	BitTorrent	395	Extended Have All Allowed Fast, Piece (Idx:0xd8c) Allowed Fast, P
70335	772.073112800	10.0.0.201	79.197.60.22	BitTorrent	122	Handshake
70347	772.092472800	10.0.0.201	104.62.139.198	BitTorrent	122	Handshake





The End