

# Network Analysis

## Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

**Frank-n-Ted-DC.frank-n-ted.com**

No.	Time	Source	Destination	Protocol	Length	Info
55506	641.352727000	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	88 → 49676 [ACK] Seq=229 Ack=247 Win=2102272 Len=0
55507	641.353592500	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	88 → 49676 [RST, ACK] Seq=229 Ack=247 Win=0 Len=0
55508	641.354643900	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.frank-n-ted.com	TCP	66	49677 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
55509	641.355699700	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.frank-n-ted.com	TCP	66	88 → 49677 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
55510	641.356564200	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.frank-n-ted.com	TCP	54	49677 → 88 [ACK] Seq=1 Ack=1 Win=262656 Len=0
55511	641.362632800	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.frank-n-ted.com	KRB5	379	AS-REQ
55514	641.386867900	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.frank-n-ted.com	TCP	1514	88 → 49677 [ACK] Seq=1 Ack=326 Win=2102272 Len=1460 [TCP se
55515	641.391140900	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.frank-n-ted.com	KRB5	267	AS-REP
55516	641.392000100	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.frank-n-ted.com	TCP	54	49677 → 88 [ACK] Seq=326 Ack=1674 Win=262656 Len=0
55517	641.392856000	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.frank-n-ted.com	TCP	54	49677 → 88 [FIN, ACK] Seq=326 Ack=1674 Win=262656 Len=0
55518	641.393721200	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	88 → 49677 [ACK] Seq=1674 Ack=327 Win=2102272 Len=0
55519	641.394585400	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	88 → 49677 [RST, ACK] Seq=1674 Ack=327 Win=0 Len=0
55520	641.395647400	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.frank-n-ted.com	TCP	66	49678 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK

Frame 55520: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0  
Ethernet II, Src: Intel\_68:42:d3 (00:11:75:68:42:d3), Dst: Dell\_2a:f7:e5 (98:40:bb:2a:f7:e5)  
Internet Protocol Version 4, Src: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)  
Transmission Control Protocol, Src Port: 49678, Dst Port: 88, Seq: 0, Len: 0

2. What is the IP address of the Domain Controller (DC) of the AD network?

**IP Address = 10.6.12.157**

(can be see in screenshot for #1)

3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

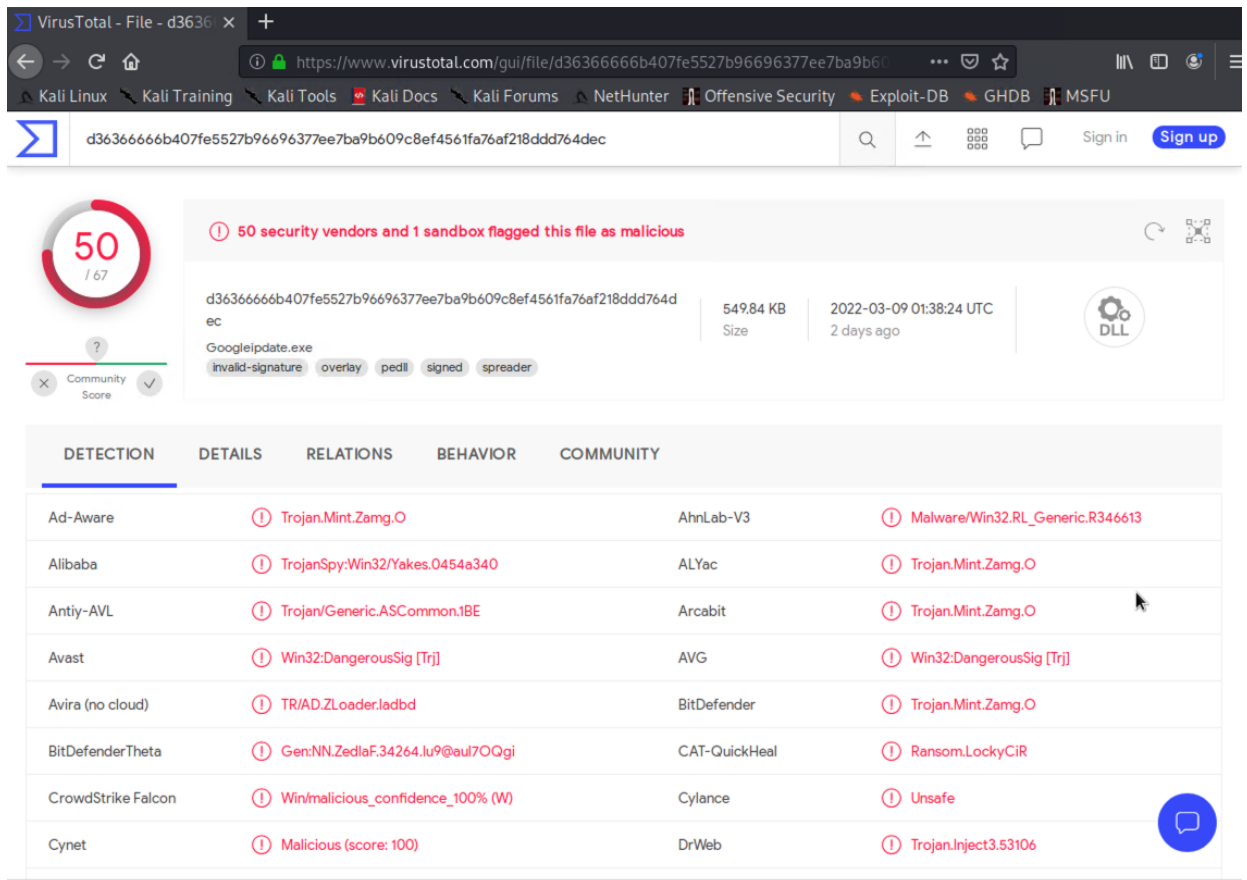
**File = june11.dll**

The image shows a Wireshark network traffic capture. The top pane displays a list of packets, with packet 59388 selected. The middle pane shows the details of the selected packet, which is an HTTP GET request for /files/june11.dll. The bottom pane shows the raw packet data in hexadecimal and ASCII. A 'Wireshark - Export - HTTP object list' dialog box is open, displaying a list of objects from the selected packet. The list includes various files and scripts, with 'june11.dll' highlighted.

Packet	Hostname	Content Type	Size	Filename
51657	insight.adsrvr.org		0 bytes	7adv=dwxytaak
53206	load.sumome.com	text/javascript	2,192 bytes	/
53624	resources.xg4ken.com	text/plain	11 kB	ktag.js?tid=KT-
53866	match.adsrvr.org	text/html	363 bytes	rightmedia?xid
53966	www.iphonhacks.com	image/x-icon	1,150 bytes	favicon.ico
53967	www.iphonhacks.com	image/png	569 bytes	favicon.png
53994	orbike.com	text/html	41 kB	/
54017	orbike.com	text/html	41 kB	/
57913	cardboardspacehoptoys.com	text/html	241 bytes	invoice-86495.c
59388	205.185.125.104	application/octet-stream	563 kB	june11.dll
59680	snnmnkxdhflwqthqismb.com		395 bytes	post.php
59682	snnmnkxdhflwqthqismb.com	text/html	208 bytes	post.php
59689	snnmnkxdhflwqthqismb.com		431 bytes	post.php
60071	snnmnkxdhflwqthqismb.com	text/html	371 kB	post.php
60084	snnmnkxdhflwqthqismb.com		328 bytes	post.php
60085	snnmnkxdhflwqthqismb.com		266 bytes	post.php
60090	snnmnkxdhflwqthqismb.com		261 bytes	post.php
60097	snnmnkxdhflwqthqismb.com		2,111 bytes	post.php
60102	snnmnkxdhflwqthqismb.com		331 bytes	post.php
60107	snnmnkxdhflwqthqismb.com	text/html	1,791 bytes	post.php
60265	snnmnkxdhflwqthqismb.com		320 bytes	post.php
60376	snnmnkxdhflwqthqismb.com	text/html	75 kB	post.php
60775	snnmnkxdhflwqthqismb.com	text/html	64 bytes	post.php
60782	snnmnkxdhflwqthqismb.com		267 bytes	post.php
60835	snnmnkxdhflwqthqismb.com	text/html	217 kB	post.php
60879	snnmnkxdhflwqthqismb.com	text/html	216 kB	post.php
61234	snnmnkxdhflwqthqismb.com		350 bytes	post.php

4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

The malware is classified as a **Trojan (Trojan.Mint.Zamg.O)**



The screenshot shows the VirusTotal file analysis page for the file `d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`. The file is identified as `Googleipdate.exe` (549.84 KB, 2022-03-09 01:38:24 UTC). It has been flagged as malicious by 50 security vendors and 1 sandbox. The file is classified as a Trojan (Trojan.Mint.Zamg.O). The file is also identified as a DLL.

**DETECTION**

Detection	Detection	Detection	Detection
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	Trojan/Generic.ASCommon.1BE	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34264.lu9@aui7OQgi	CAT-QuickHeal	Ransom.LockyCiR
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DrWeb	Trojan.Inject.3.53106

# Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:
  - Host name: **Rotterdam-PC**
  - IP address: **172.16.4.205**
  - MAC address: **00:59:07:b0:63:a4**

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (Frame 3197), which is a Kerberos AS-REP message.

No.	Time	Source	Destination	Protocol	Length	Info
3197	49.831293000	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	204	AS-REP
3209	49.894459400	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	219	TGS-REP
3250	50.135544700	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	158	TGS-REP
3270	50.241859400	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	84	TGS-REP
3378	50.627492100	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	204	AS-REP
3390	50.688223400	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	130	TGS-REP
3417	50.770347900	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	242	AS-REP
3428	50.829698200	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	150	TGS-REP
3440	50.894680000	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	273	TGS-REP
14045	207.906378300	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	206	TGS-REP
14056	207.963495200	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	72	TGS-REP
31819	461.582020800	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	206	TGS-REP
32201	462.933512000	mind-hammer-dc.mind...	Rotterdam-PC.mind-hammer.net	KRB5	84	TGS-REP

Frame 3197: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface eth0, id 0

Ethernet II, Src: Dell\_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)

- Destination: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)  
Address: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)  
... .. = LG bit: Globally unique address (factory default)  
... .. = IG bit: Individual address (unicast)
- Source: Dell\_19:49:50 (a4:ba:db:19:49:50)  
Address: Dell\_19:49:50 (a4:ba:db:19:49:50)  
... .. = LG bit: Globally unique address (factory default)  
... .. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: mind-hammer-dc.mind-hammer.net (172.16.4.4), Dst: Rotterdam-PC.mind-hammer.net (172.16.4.205)
- Transmission Control Protocol, Src Port: 88, Dst Port: 49164, Seq: 1461, Ack: 324, Len: 150
- [2 Reassembled TCP Segments (1619 bytes): #3196(1460), #3197(150)]
- Kerberos

2. What is the username of the Windows user whose computer is infected?

Username = **matthijs.devries**

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
3187	49.786544600	Rotterdam-PC.mind-h...	mind-hammer-dc.mind-hammer.net	KRB5	297	AS-REQ
3195	49.803720100	Rotterdam-PC.mind-h...	mind-hammer-dc.mind-hammer.net	KRB5	377	AS-REQ
3369	50.584361200	Rotterdam-PC.mind-h...	mind-hammer-dc.mind-hammer.net	KRB5	301	AS-REQ
3376	50.599992500	Rotterdam-PC.mind-h...	mind-hammer-dc.mind-hammer.net	KRB5	381	AS-REQ
3408	50.726684900	Rotterdam-PC.mind-h...	mind-hammer-dc.mind-hammer.net	KRB5	292	AS-REQ
3415	50.742235400	Rotterdam-PC.mind-h...	mind-hammer-dc.mind-hammer.net	KRB5	372	AS-REQ

..0. .... = disable-transited-check: False  
...1 .... = renewable-ok: True  
....0... = enc-tkt-in-key: False  
....0... = unused29: False  
....0... = renew: False  
....0... = validate: False

▼ cname  
name-type: KRB5-NT-PRINCIPAL (1)  
▼ cname-string: 1 item  
CNameString: matthijs.devries  
realm: MIND-HAMMER  
▼ sname  
name-type: KRB5-NT-SRV-INST (2)  
▶ sname-string: 2 items  
till: 2037-09-13 02:48:05 (UTC)

0030 01 00 48 a5 00 00 00 00 00 ea 6a 81 e7 30 81 e4 ..H....j..0..  
0040 a1 03 02 01 05 a2 03 02 01 0a a3 15 30 13 30 11 .....0.0..  
0050 a1 04 02 02 00 80 a2 09 04 07 30 05 a0 03 01 01 .....0.....  
0060 ff a4 81 c0 30 81 bd a0 07 03 05 00 40 81 00 10 .....0.....  
0070 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 00 ..0.....0...  
0080 01 74 74 68 69 6a 73 2e 64 65 76 72 69 65 73 a2 matthijs.devries  
0090 0d 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 a3 20 ...MIND- HAMMER  
00a0 30 1e a0 03 02 01 02 a1 17 30 15 1b 06 6b 72 62 0.....0...krb

3. What are the IP addresses used in the actual infection traffic?

IP addresses = **172.16.4.205** and **185.243.115.84**

These IP addresses has the highest packet count and can be traced to infection.

Wireshark - Conversations - pcap.pcap

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bit/s B → A
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611	77 k	126 k
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762	1,109	1,355
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	124 k	4,652	6,920 k	0.000000	900.2057	491 k	13 k
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648	3,492 k	47.425979	854.0467		
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	669.890730	67.9985		
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	571.917522	66.7937		

# Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with IP address 10.0.0.201:
  - MAC address: **00:16:17:18:66:c8**
  - Windows username: **elmer.blanco**
  - OS version: **BLANCO-DESKTOP**

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.0.201 and kerberos.CNameString

Title: Destination Type: Custom Fields: Enter a field ... Occurrence: 0 OK Cancel

No.	Time	Source	Destination	Protocol	Length	Info
65798	745.008607500	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	227	TGS-REP
65827	745.174120600	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	293	TGS-REP
65839	745.233051500	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	114	TGS-REP
66970	751.007645200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogoftheyear.net	KRB5	302	AS-REQ
66978	751.024207500	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogoftheyear.net	KRB5	382	AS-REQ
66980	751.052436500	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	250	AS-REP
66992	751.115116900	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	199	TGS-REP
67036	751.190289600	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogoftheyear.net	KRB5	290	AS-REQ
67044	751.205833000	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogoftheyear.net	KRB5	370	AS-REQ
67046	751.233860000	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	237	AS-REP
67058	751.294737700	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	175	TGS-REP
67080	751.379585100	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogoftheyear.net	KRB5	303	TGS-REP

kdc-options: 40810010

name

name-type: KRB5-NT-PRINCIPAL (1)

name-string: 1 item

CNameString: elmer.blanco

realm: DOGOFtheyear

sname

till: 2037-09-13 02:48:05 (UTC)

rtime: 2037-09-13 02:48:05 (UTC)

nonce: 634194387

etype: 6 items

addresses: 1 item BLANCO-DESKTOP<20>

HostAddress BLANCO-DESKTOP<20>

addr-type: nETBIOS (20)

NetBIOS Name: BLANCO-DESKTOP<20> (Server service)

2. Which torrent file did the user download?

Torrent file = **Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent**

pcap.pcap					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
ip.addr==10.0.0.201 and (http.request.uri contains ".torrent")					
Title:	Destination	Type:	Custom	Fields:	Enter a field ...
No.	Time	Source	Destination	Protocol	Length Info
69706	770.366956400	BLANCO-DESKTOP.dogo...	files.publicdomaintorrents.com	HTTP	589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_t

Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
Ethernet II, Src: Msi 18:66:c8 (00:16:17:18:66:c8), Dst: Cisco 27:a1:3e (00:09:b7:27:a1:3e)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
Transmission Control Protocol, Src Port: 49834, Dst Port: 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
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
<Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n>
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
<User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n>
Accept-Language: en-US\r\n
<Accept-Language: en-US\r\n>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
<Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n>
Upgrade-Insecure-Requests: 1\r\n