

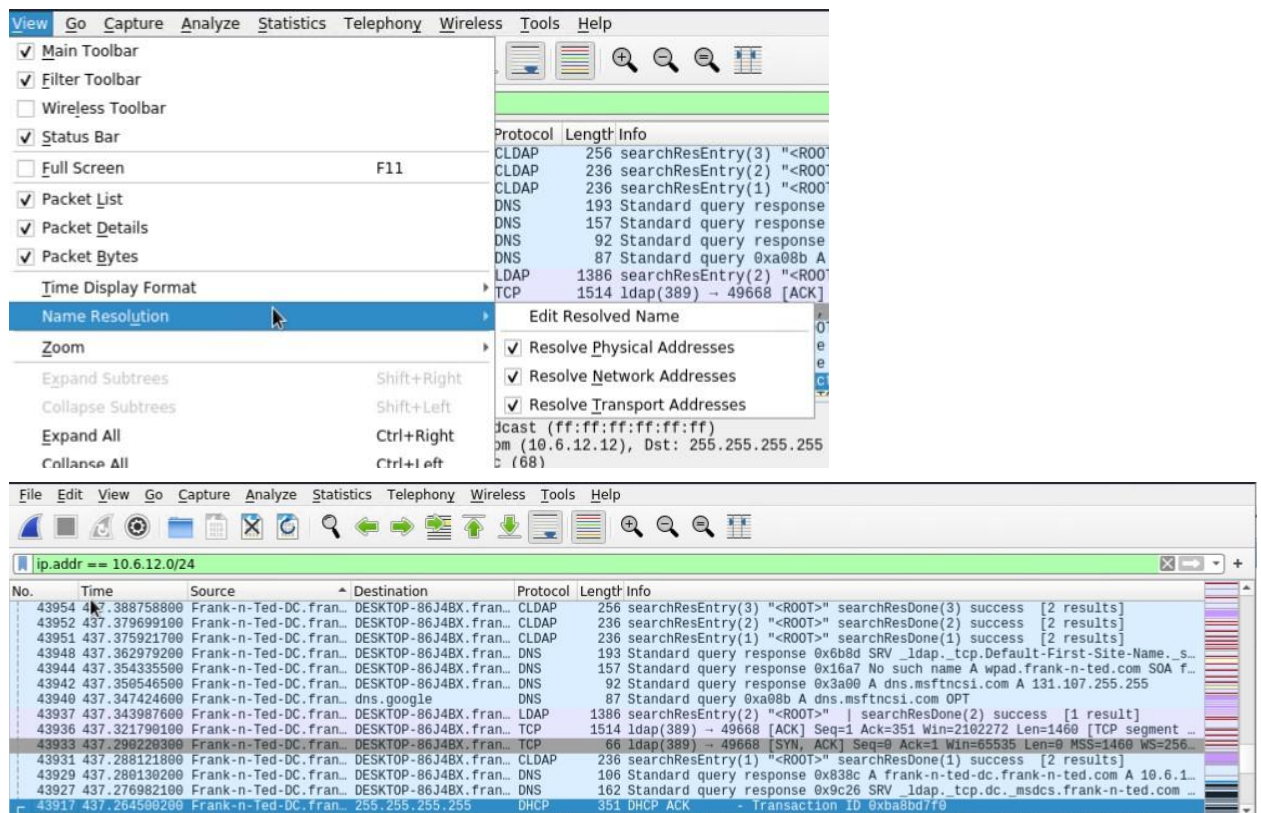
# Network Forensic Analysis Report

## Time Thieves

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



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

10.6.12.12

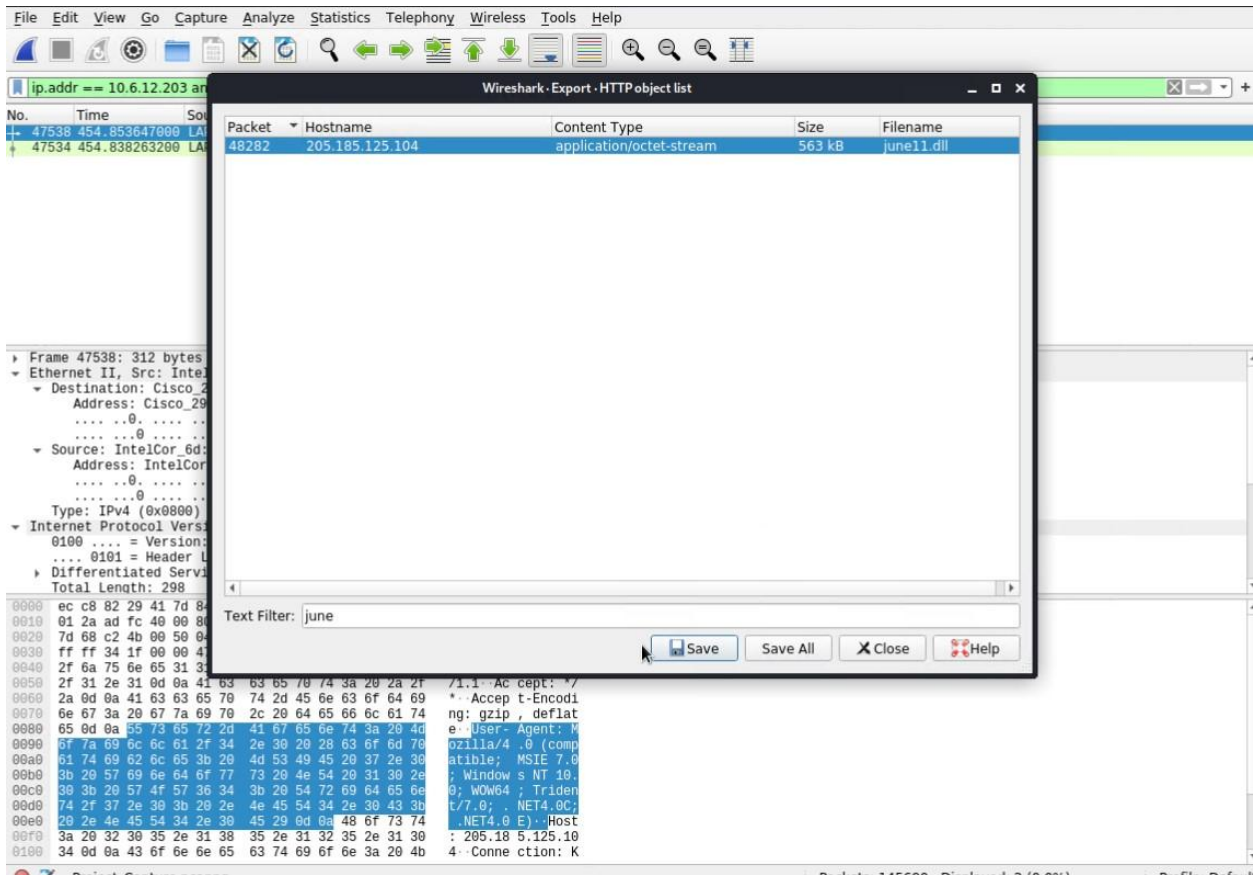
```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 337
    Identification: 0x3880 (14464)
  ▶ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xeb0a [validation disabled]
    [Header checksum status: Unverified]
    Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
    Destination: 255.255.255.255 (255.255.255.255)
  ▶ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
  ▶ Dynamic Host Configuration Protocol (ACK)
```

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

june11.dll

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 10.6.12.203 and http.request.method == GET						
No.	Time	Source	Destination	Protocol	Length	Info
47538	454.853647090	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
47534	454.838263200	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	275	GET /pQ8twj HTTP/1.1

```
▶ Frame 47538: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
▼ Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
  ▼ Destination: Cisco_29:41:7d (ec:c8:82:29:41:7d)
    Address: Cisco_29:41:7d (ec:c8:82:29:41:7d)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
    Address: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 298
```



4. Upload the file to [VirusTotal.com](https://www.virustotal.com).

VirusTotal - File - d3636666b407fe5527b96696377ee7ba9b6c

https://www.virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b6c

d3636666b407fe5527b96696377ee7ba9b6c9cf4561fa76af218ddd764dec

51 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b6c9cf4561fa76af218ddd764dec

GoogleUpdate.exe

Invalid signature (oversig pedt signed)

549.84 KB

2021-11-23 09:06:52 UTC

19 hours ago

DL

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32_RL_Generic.R346613	
Alibaba	Trojan.Spy.Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O	
Antiy-AVL	Trojan.Generic.ASCcommon.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	
BitDefender Theta	Gen:NN.ZedfaF.34294.lu9@au7OQgi	CrowdStrike Falcon	Win/malicious_confidence_100% (W)	
Cylance	Unsafe	Cynet	Malicious (score: 100)	
DrWeb	Trojan.Inject3.53106	eGambit	Unsafe.AI_Score_98%	

5. What kind of malware is this classified as?

trojan.malware

## Vulnerable Windows Machine

- Find the following information about the infected Windows machine:
  - Host name: Rotterdam-PC.mind-hammer.net
  - IP address: 172.16.4.205
  - MAC address: LenovoEM\_b0:64:a4 (00:59:07:b0:63:a4)
- What is the username of the Windows user whose computer is infected?

ip.addr == 172.16.4.205 and kerberos.CNameString							
No.	Time	Source	Destination	CNameString	Protocol	Length	Info
72274	698.061139300	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-h...	ROTTERDAM-PC\$	KRB5	158	TGS-REP
72294	698.167456100	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-h...	ROTTERDAM-PC\$	KRB5	84	TGS-REP
72389	698.509927200	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	ROTTERDAM-PC\$	KRB5	301	AS-REQ
72396	698.525556000	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	ROTTERDAM-PC\$	KRB5	381	AS-REQ
72398	698.553076800	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-h...	ROTTERDAM-PC\$	KRB5	204	AS-REP
72410	698.613694700	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-h...	ROTTERDAM-PC\$	KRB5	130	TGS-REP
72428	698.652244000	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	matthijs.devries	KRB5	292	AS-REQ
72435	698.667803600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	matthijs.devries	KRB5	372	AS-REQ
72437	698.695922300	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-h...	matthijs.devries	KRB5	242	AS-REP
72448	698.755261900	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-h...	matthijs.devries	KRB5	150	TGS-REP
72460	698.820252400	mind-hammer-dc.mind-hammer...	Rotterdam-PC.mind-h...	matthijs.devries	KRB5	273	TGS-REP
72211	697.712101900	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	rotterdam-pc\$	KRB5	297	AS-REQ
72219	697.729292600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	rotterdam-pc\$	KRB5	377	AS-REQ

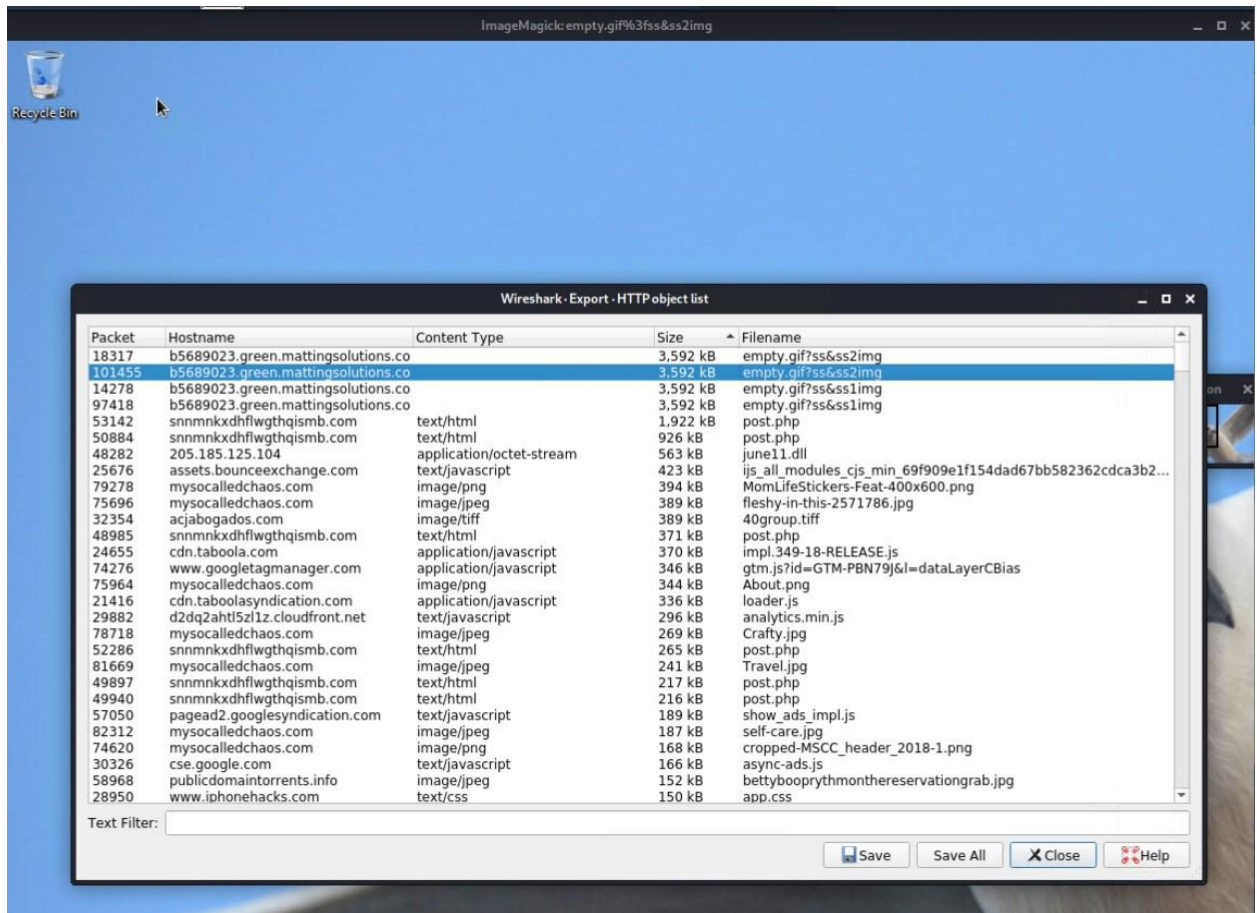
matthijs.devries

- What are the IP addresses used in the actual infection traffic? 185.243.115.84

Wireshark - Conversations - Project_Capture.pcapng											
Ethernet · 85		IPv4 · 881		IPv6 · 9		TCP · 1040		UDP · 1817			
Address A	Address B	Packets	Bytes	Packets	Bytes	Packets	Bytes	Packets	Bytes	Rel Start	Duration
172.16.4.205	185.243.115.84	36,151	32 M	19,338	15 M	16,813	16 M	0.000000	1109.1211	114 k	
5.101.51.151	10.6.12.203	8,652	8,493 k	6,524	8,355 k	2,128	137 k	466.107741	919.7071	72 k	
192.168.1.90	192.168.1.100	8,628	40 M	5,616	39 M	3,012	840 k	3.581061	1430.5809	222 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	699.086815	149.9677	422 k	
10.11.11.200	151.101.50.208	6,540	4,441 k	3,226	224 k	3,314	4,217 k	368.134531	918.5023	1,959	
10.0.0.201	64.187.66.143	5,723	4,245 k	2,632	170 k	3,091	4,074 k	567.877136	867.4994	1,576	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	629.516789	66.9059	8,605	



4. As a bonus, retrieve the desktop background of the Windows host.



## Illegal Downloads

1. Find the following information about the machine with IP address 10.0.0.201:
  - o MAC address: Msi\_18:66:c8 (00:16:17:18.66:c8)
  - o Windows username: elmer.blanco

- OS version: Windows NT 10.0

ip.addr == 10.0.0.201 and http

No.	Time	Source	Destination	CNameString	Protocol
56696	549.303839800	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56693	549.291564400	files.publicdomaintorrents...	BLANCO-DESKTOP.dogo...		HTTP
56682	549.151426400	BLANCO-DESKTOP.dogoftheyear...	pagead46.1.doublecl...		HTTP
56672	549.132665600	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56670	549.124226300	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56668	549.115872800	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56665	549.106466100	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56663	549.098144300	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56662	549.090663200	files.publicdomaintorrents...	BLANCO-DESKTOP.dogo...		HTTP
56643	548.893408900	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56641	548.884944100	files.publicdomaintorrents...	BLANCO-DESKTOP.dogo...		HTTP
56608	548.658042200	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP
56594	548.550704900	BLANCO-DESKTOP.dogoftheyear...	files.publicdomaint...		HTTP

TCP payload (414 bytes)

Hypertext Transfer Protocol

GET /psp.gif HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /psp.gif HTTP/1.1\r\n]

Request Method: GET

Request URI: /psp.gif

Request Version: HTTP/1.1

Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\r\n

Accept: image/png,image/svg+xml,image/\*;q=0.8,\*/\*;q=0.5\r\n

Accept-Language: en-US\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.120 Safari/537.36\r\n

Host: publicdomaintorrents.info\r\n

Connection: Keep-Alive\r\n

\r\n

Full request URI: http://publicdomaintorrents.info/psp.gif

OS	Version	Product
Windows 10	10.0.19041.37	Home Single Language, Home China, Home, Pro, Pro Education, Pro for Workstations, <sup>[38]</sup> Enterprise, Education, Windows 10 S, IoT Core, Mobile, Mobile Enterprise <sup>[39][40]</sup>
Windows Server 2016		Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server
Windows Server 2019		Essentials, Standard, Datacenter, Multipoint Premium Server, Hyper-V Server
Windows Server 2022		
Windows 11		Home Single Language, Home China, Home, Pro, Pro Education, Pro for Workstations, SE

## 2. Which torrent file did the user download?

Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent

