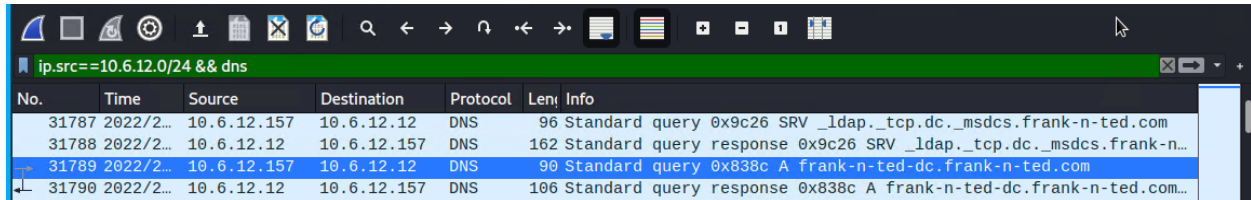


Network Forensic Analysis Report

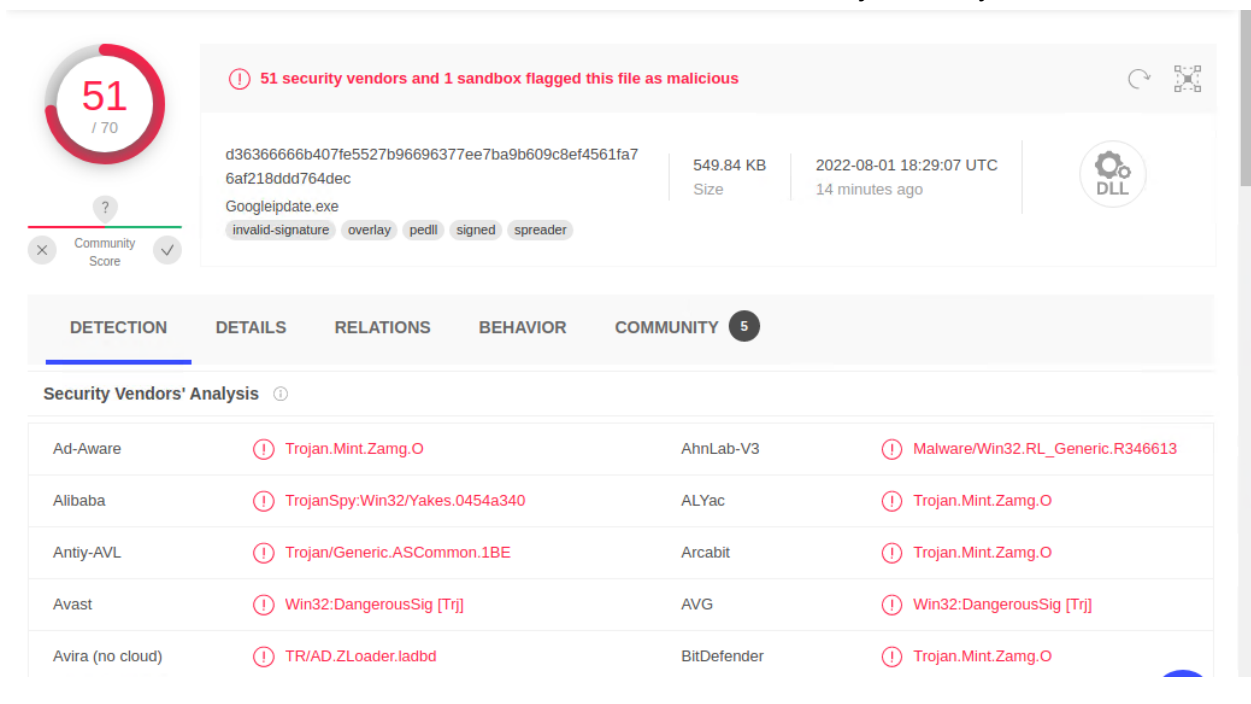
Time Thieves

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



No.	Time	Source	Destination	Protocol	Length	Info
31787	2022/2...	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
31788	2022/2...	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n...
31789	2022/2...	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
31790	2022/2...	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com...

1. What is the domain name of the users' custom site? **frank-n-ted.com**
2. What is the IP address of the Domain Controller (DC) of the AD network? **10.6.12.12**
3. What is the name of the malware downloaded to the 10.6.12.203 machine? **june11.dll**
 - o Once you have found the file, export it to your Kali machine's desktop.
4. Upload the file to [VirusTotal.com](https://www.virustotal.com).
5. What kind of malware is this classified as? Looks like a Trojan mostly



51 / 70

51 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa7
6af218ddd764dec
Googleipdate.exe
invalid-signature overlay pedll signed spreader

549.84 KB
Size

2022-08-01 18:29:07 UTC
14 minutes ago

DLL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

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	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

Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:

- Host name **ROTTERDAM-PC**
- IP address **172.16.4.4**
- MAC address **00:59:07:b0:63:a4**

Filter: `ip.src==172.16.4.205 && nbns`

No.	Time	Source	Destination	Protocol	Length	Info
3172	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<80>
3173	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3174	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3228	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3229	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3230	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<80>
3295	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<80>
3296	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3297	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3363	2020/182...	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>

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

This website offered Windows user account from from Kerberos traffic

<https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/>

So, the username is: **matthijs.devries**

Filter: `ip.src==172.16.4.205 && kerberos.CNameString`

No.	Time	Source	Destination	Protocol	Len	Info
60230	2022/213...	172.16.4.205	172.16.4.4	KRB5	301	AS-REQ
60237	2022/213...	172.16.4.205	172.16.4.4	KRB5	381	AS-REQ
60269	2022/213...	172.16.4.205	172.16.4.4	KRB5	292	AS-REQ
60280	2022/213...	172.16.4.205	172.16.4.4	KRB5	372	AS-REQ

Expanded packet 60280 (KRB5):

- name-type: KRB5-NT-PRINCIPAL (1)
- name-string: 1 item
 - CNameString: **matthijs.devries** (highlighted with a red arrow)
- realm: MIND-HAMMER

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

Filter: `Ethernet II >> IPv4 >> 879`

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.4.205	185.243.115.84	24,448	22 M	13,982	13 M	10,466	8,647 k	0.000000	948.6
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	538.605569	149.9
192.168.1.90	192.168.1.100	6,625	30 M	4,228	30 M	2,397	642 k	8.185460	1092.4
10.11.11.200	151.101.50.208	6,516	4,440 k	3,214	224 k	3,302	4,215 k	207.653280	887.6

185.243.115.84

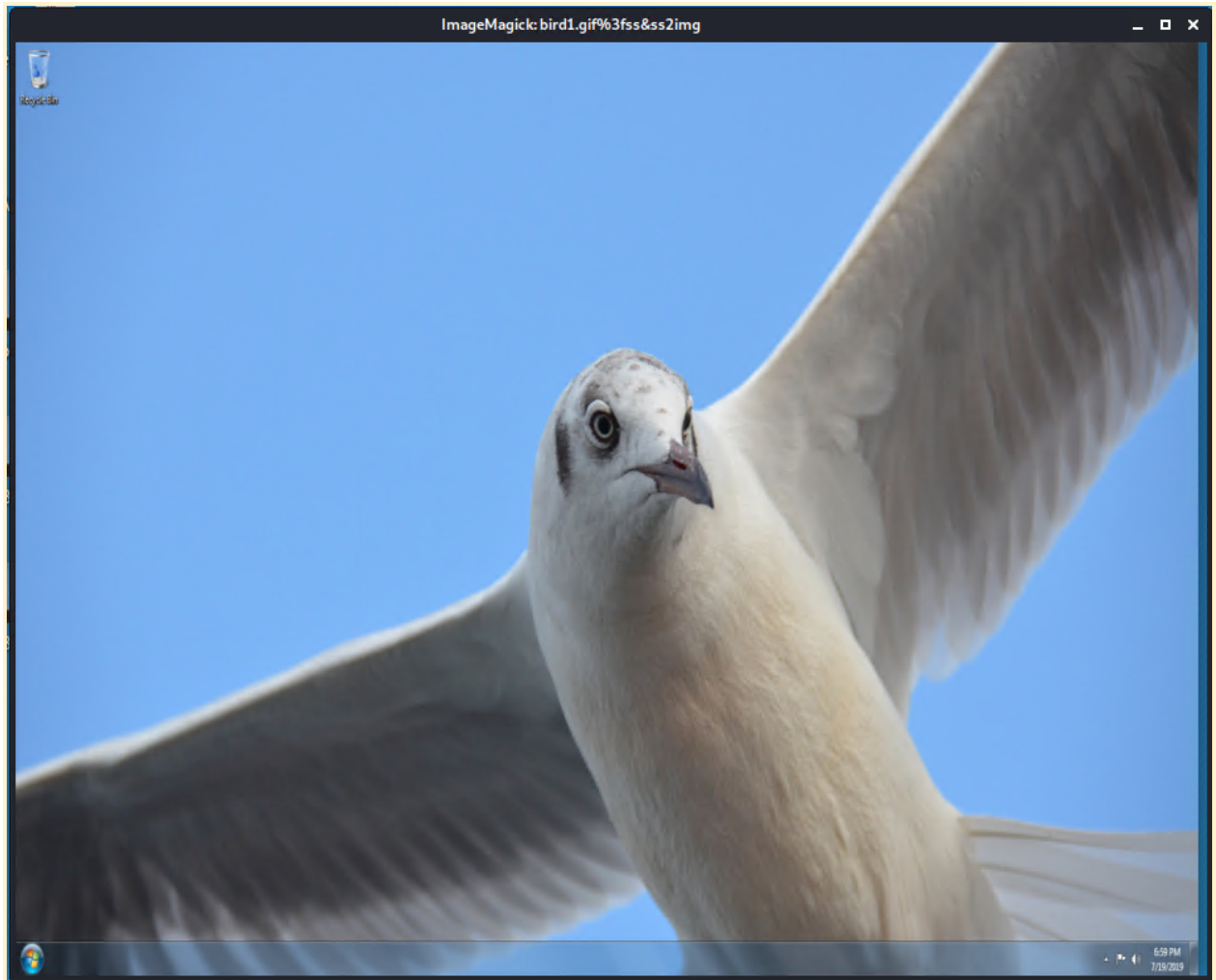
4. As a bonus, retrieve the desktop background of the Windows host.
Hackertarget.com gives a cheatsheet on finding an image, There were only a few files that were worth considering because of the size of the files. This one actually looks like a screenshot of a desktop

Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
9857	img.timeinc.net	application/javascript	16 kB	MobileCompatibility.js
9875	img.timeinc.net	image/gif	43 bytes	alt_holder.gif
9823	img.timeinc.net	application/javascript	10 kB	articles.js
11425	img.timeinc.net	image/png	2,238 bytes	btn_photos.png
9763	img.timeinc.net	text/css	7,350 bytes	channel.css
85359	b5689023.green.mattingssolutions.co		3,592 kB	empty.gif?ss&ss1img
1	b5689023.green.mattingssolutions.co		1,151 bytes	empty.gif?ss&ss2img
2	b5689023.green.mattingssolutions.co		1,357 bytes	empty.gif?ss&ss3img

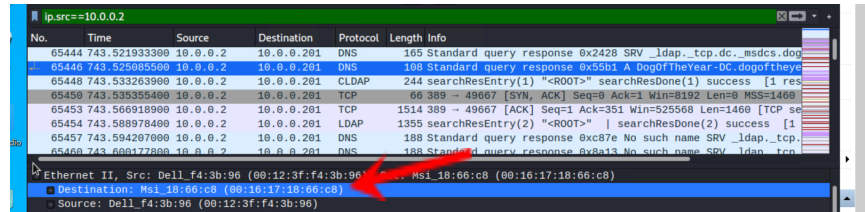
Text Filter: img

Help Save All Close Save



Illegal Downloads

- Find the following information about the machine with IP address 10.0.0.201:
MAC address 00:16:16:18:66:c8



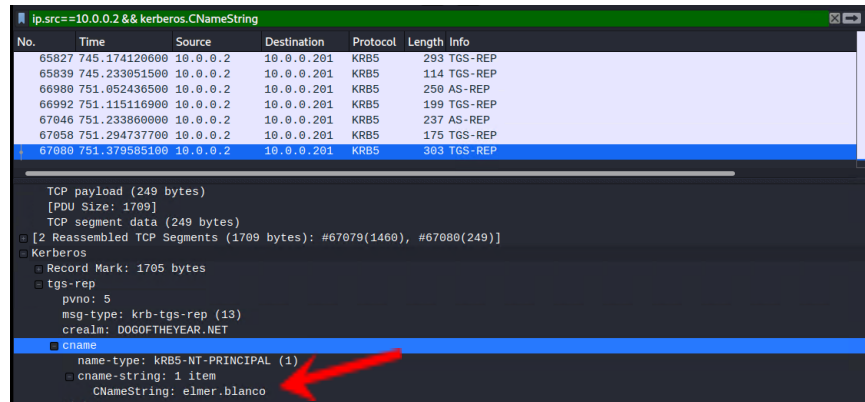
No.	Time	Source	Destination	Protocol	Length	Info
65444	743.521933300	10.0.0.2	10.0.0.201	DNS	105	Standard query response 0x2428 SRV _ldap._tcp.dc._msdcs.dog...
65446	743.525065500	10.0.0.2	10.0.0.201	DNS	108	Standard query response 0x55b1 A DogOfTheYear-DC.dogoftheye...
65448	743.533263900	10.0.0.2	10.0.0.201	LDAP	244	searchResEntry(1) "<CROOT>" searchResDone(1) success [1 res...
65450	743.535355400	10.0.0.2	10.0.0.201	TCP	66	389 -> 49667 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460...
65453	743.566918900	10.0.0.2	10.0.0.201	TCP	1514	389 -> 49667 [ACK] Seq=1 Ack=351 Win=525568 Len=1460 [TCP se...
65454	743.588978400	10.0.0.2	10.0.0.201	LDAP	1355	searchResEntry(2) "<CROOT>" searchResDone(2) success [1...
65457	743.594297000	10.0.0.2	10.0.0.201	DNS	188	Standard query response 0xc87e No such name SRV _ldap._tcp...
65460	743.601777000	10.0.0.2	10.0.0.201	DNS	188	Standard query response 0xb13 No such name SRV _ldap._tcp...

Ethernet II, Src: Dell_F4:3b:96 (00:12:3f:f4:3b:96), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)

Destination: Msi_18:66:c8 (00:16:17:18:66:c8)

Source: Dell_F4:3b:96 (00:12:3f:f4:3b:96)

- Windows username elmer.blanco



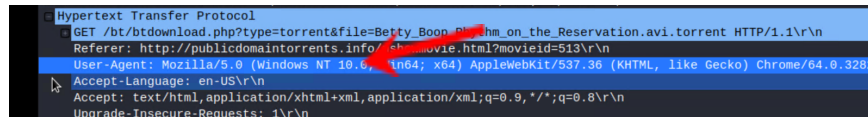
No.	Time	Source	Destination	Protocol	Length	Info
65827	745.174120600	10.0.0.2	10.0.0.201	KRBS	293	TGS-REP
65839	745.233051500	10.0.0.2	10.0.0.201	KRBS	114	TGS-REP
66980	751.052436500	10.0.0.2	10.0.0.201	KRBS	250	AS-REP
66992	751.115116900	10.0.0.2	10.0.0.201	KRBS	199	TGS-REP
67046	751.233860000	10.0.0.2	10.0.0.201	KRBS	237	AS-REP
67058	751.294737700	10.0.0.2	10.0.0.201	KRBS	175	TGS-REP
67080	751.379585100	10.0.0.2	10.0.0.201	KRBS	303	TGS-REP

TCP payload (249 bytes)
[PDU Size: 1709]
TCP segment data (249 bytes)
[2 Reassembled TCP Segments (1709 bytes): #67079(1460), #67080(249)]

Kerberos

- Record Mark: 1705 bytes
- tgs-rep
- pwno: 5
- msg-type: krb-tgs-rep (13)
- crealm: DOGOFtheyear.NET
- cname
 - name-type: KRBS-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: elmer.blanco

- OS version Window NT 10.0



Source	Destination	Protocol	Length	Info
10.0.0.201	72.21.202.62	HTTP	885	GET /e/cm?t=publicdoma10f-20&o=1&p=48&l=op1&pvid=40C236A13FD0066&ref-url=ht...
10.0.0.201	52.94.233...	HTTP	1067	GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7BN22program%22%3AN%22%22%2C...
10.0.0.201	168.215.19...	HTTP	589	GET /bt/btdownload.php?type=torent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

Hypertext Transfer Protocol

GET /bt/btdownload.php?type=torent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n

Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n

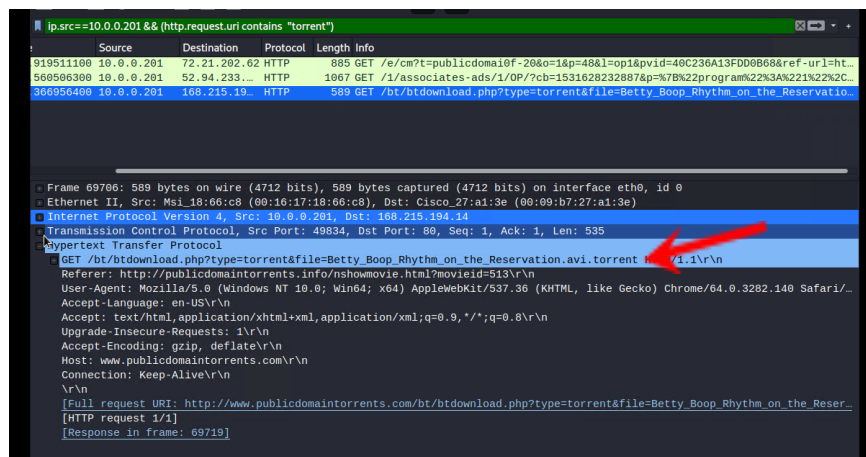
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.148 Safari/537.36\r\n

Accept-Language: en-US\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

- Which torrent file did the user download?
Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



Source	Destination	Protocol	Length	Info
10.0.0.201	72.21.202.62	HTTP	885	GET /e/cm?t=publicdoma10f-20&o=1&p=48&l=op1&pvid=40C236A13FD0066&ref-url=ht...
10.0.0.201	52.94.233...	HTTP	1067	GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7BN22program%22%3AN%22%22%2C...
10.0.0.201	168.215.19...	HTTP	589	GET /bt/btdownload.php?type=torent&file=Betty_Boop_Rhythm_on_the_Reservation...

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: 10.0.0.201, Dst: 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=torent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\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/64.0.3282.148 Safari/537.36\r\n

Accept-Language: en-US\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

Accept-Encoding: gzip, deflate\r\n

Host: www.publicdomaintorrents.com\r\n

Connection: Keep-Alive\r\n

V\r\n

[Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torent&file=Betty_Boop_Rhythm_on_the_Reser...]

[HTTP request 1/1]

[Response in frame: 69710]