Network Analysis

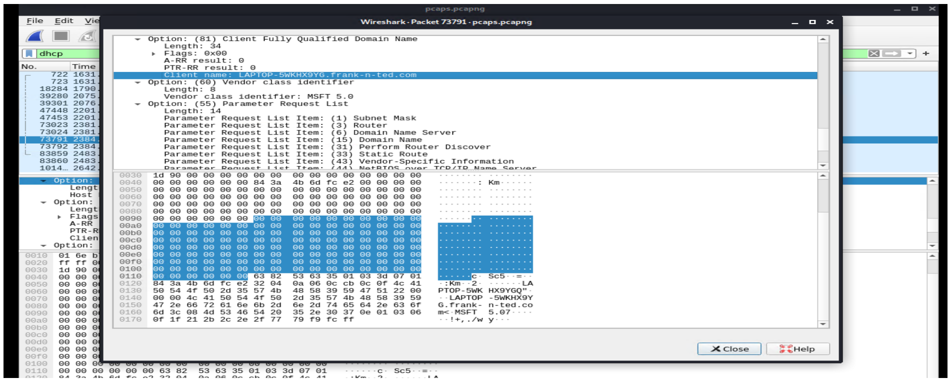
Time Thieves

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?
   -The domain name is frank-n-ted.com

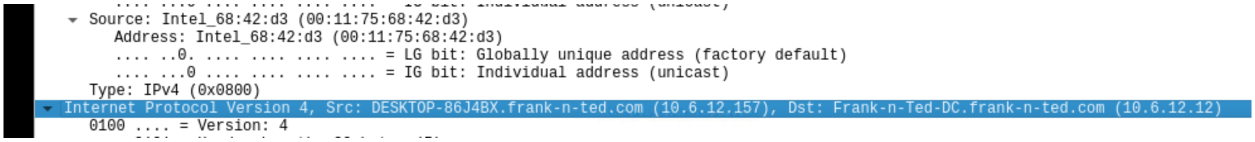


```
    Option: (81) Client Fully Qualified Domain Name
        Length: 34
      ▸ Flags: 0x00
        A-RR result: 0
        PTR-RR result: 0
        Client name: LAPTOP-5WKHX9YG.frank-n-ted.com
    Option: (60) Vendor class identifier
        Length: 8
        Vendor class identifier: MSFT 5.0
    Option: (55) Parameter Request List
        Length: 14
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (3) Router
        Parameter Request List Item: (6) Domain Name Server
        Parameter Request List Item: (15) Domain Name
        Parameter Request List Item: (31) Perform Router Discover
        Parameter Request List Item: (33) Static Route
        Parameter Request List Item: (43) Vendor-Specific Information
        Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
```

```
0030  1d 90 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 84 3a  4b 6d fc e2 00 00 00 00   ·······: Km······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  84 3a 4b 6d fc e2 32 04  0a 06 0c cb 0c 0f 4c 41   ·:Km··2· ······LA
0130  50 54 4f 50 2d 35 57 4b  48 58 39 59 47 51 22 00   PTOP-5WK HX9YGQ"·
0140  00 00 4c 41 50 54 4f 50  2d 35 57 4b 48 58 39 59   ··LAPTOP -5WKHX9Y
0150  47 2e 66 72 61 6e 6b 2d  6e 2d 74 65 64 2e 63 6f   G.frank- n-ted.co
0160  6d 3c 08 4d 53 46 54 20  35 2e 30 37 0e 01 03 06   m<·MSFT  5.07····
0170  0f 1f 21 2b 2c 2e 2f 77  79 f9 fc ff               ··!+,./w y···
```

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

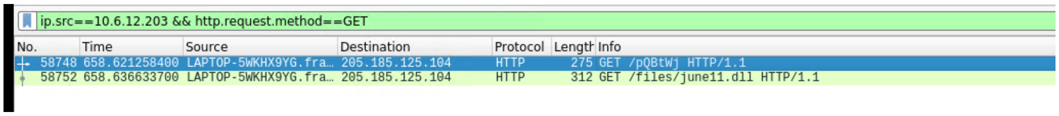
   -The IP for desktop is 10.6.12.157 and DC IP is 10.6.12.12



```
  ▾ Source: Intel_68:42:d3 (00:11:75:68:42:d3)
        Address: Intel_68:42:d3 (00:11:75:68:42:d3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ 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)
    0100 .... = Version: 4
```

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.

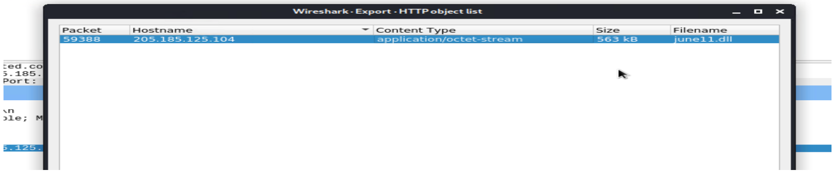
   -The name of the malware file: june11.dll



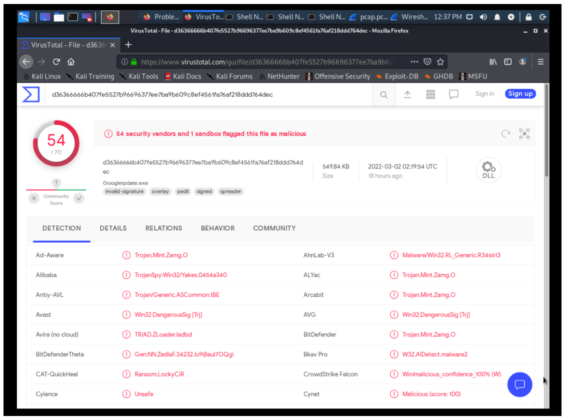
```
ip.src==10.6.12.203 && http.request.method==GET

No.    Time           Source                 Destination      Protocol  Length Info
58748  658.621258400  LAPTOP-5WKHX9YG.fra…  205.185.125.104  HTTP      275 GET /pQBtWj HTTP/1.1
58752  658.636633700  LAPTOP-5WKHX9YG.fra…  205.185.125.104  HTTP      312 GET /files/june11.dll HTTP/1.1
```

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

   -Malware type: Trojan



Packet	Hostname	Content Type	Size	Filename
59388	205.185.125.104	application/octet-stream	563 kB	june11.dll



Proble…
VirusTo…
Shell N…
Shell N…
Shell N…
pcap.pc…
Wiresh…
12:37 PM
VirusTotal - File - d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec - Mozilla Firefox
VirusTotal - File - d3636
https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b60
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Sign in
Sign up

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

54 / 70

54 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Googleipdate.exe
invalid-signature overlay pedll signed spreader

549.84 KB Size

2022-03-02 02:19:54 UTC 18 hours ago

DLL

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.34232.lu9@aul7OQgi	Bkav Pro	W32.AIDetect.malware2
CAT-QuickHeal	Ransom.LockyCiR	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)