Final Engagement

Attack, Defense, and Analysis of a Vulnerable Network

Table of Contents

This document contains the following sections:

01 **Network Topology & Critical Vulnerabilities**

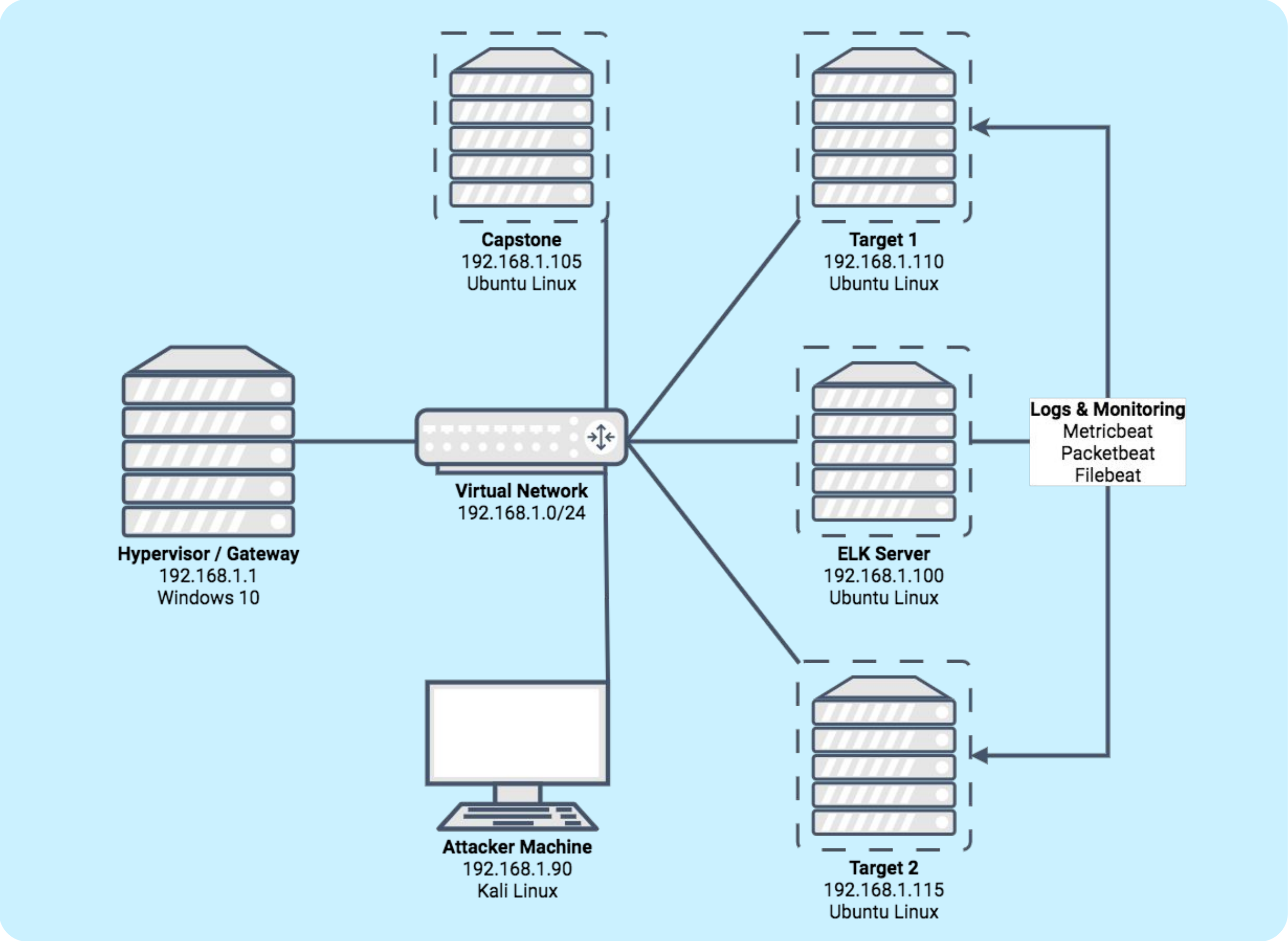
02 **Traffic Profile**

03 **Normal Activity**

04 **Malicious Activity**

Network Topology & Critical Vulnerabilities

Network Topology



Network

Address Range:	192.168.1.0-255
Netmask:	255.255.255.0
Gateway:	192.168.1.1

Machines

IPV4:	192.168.1.1
OS:	Windows 10
Hostname:	ML-RefVm-684427
IPV4:	192.168.1.100
OS:	Ubuntu Linux
Hostname:	ELK
IPV4:	192.168.1.110
OS:	Debian Linux
Hostname:	TARGET1
IPV4:	192.168.1.115
OS:	Debian Linux
Hostname:	TARGET2

Critical Vulnerabilities: Target 1

Our assessment uncovered the following vulnerabilities in **Target 1**

Vulnerability	Description	Impact
Directory Enumeration	In a enumeration attack;a directory listing is inappropriately exposed, this yielding potentially sensitive information to hackers	Exposing the contents of a directory can lead to an attacker gaining access to source code or useful info to devise exploits.
Weak password	Password is incredibly easy to guess	Anyone can easily gain access to Target 1 which is supposed to be protected
Python with sudo permissions	Sudo is prone to a security-bypass vulnerability that could lead to arbitrary code execution. This is due to an error in the application when handling environment variables	A local attacker with the ability to run Python scripts can exploit this vulnerability to gain access to an interactive Python prompt. The attacker may then execute arbitrary code with elevated privileges, facilitating the complete compromise of affected computers.

Critical Vulnerabilities: Target 1 Cont.

Our assessment uncovered the following vulnerabilities in **Target 1**

Vulnerability	Description	Impact
CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	A remote attacker could use this vulnerability to circumvent basic authentication on `httpd`
CVE-2017-7494	Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.	An authenticated attacker with write access can upload arbitrary code to the samba share, this code will will run as root.
Sensitive data publicly available	Sensitive information publicly available when looking at the source code of the web page	Flag 1 was obtainable by looking at the source code of `service.html` page

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network

Feature	Value	Description
Top Talkers (IP Addresses)	192.168.1.90, 192.168.1.100, 172.16.4.205, 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	TCP, HTTP, TLS	Three most common protocols on the network.
# of Unique IP Addresses	818	Count of observed IP addresses.
Subnets	10.6.12.0/24, 10.0.0.0/8, 172.16.4.0/24	Observed subnet ranges.
# of Malware Species	2	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

- **Active Directory Authentication**
- **Accessing SMB Shares**
- **Participating in Video Conferences**

Suspicious Activity

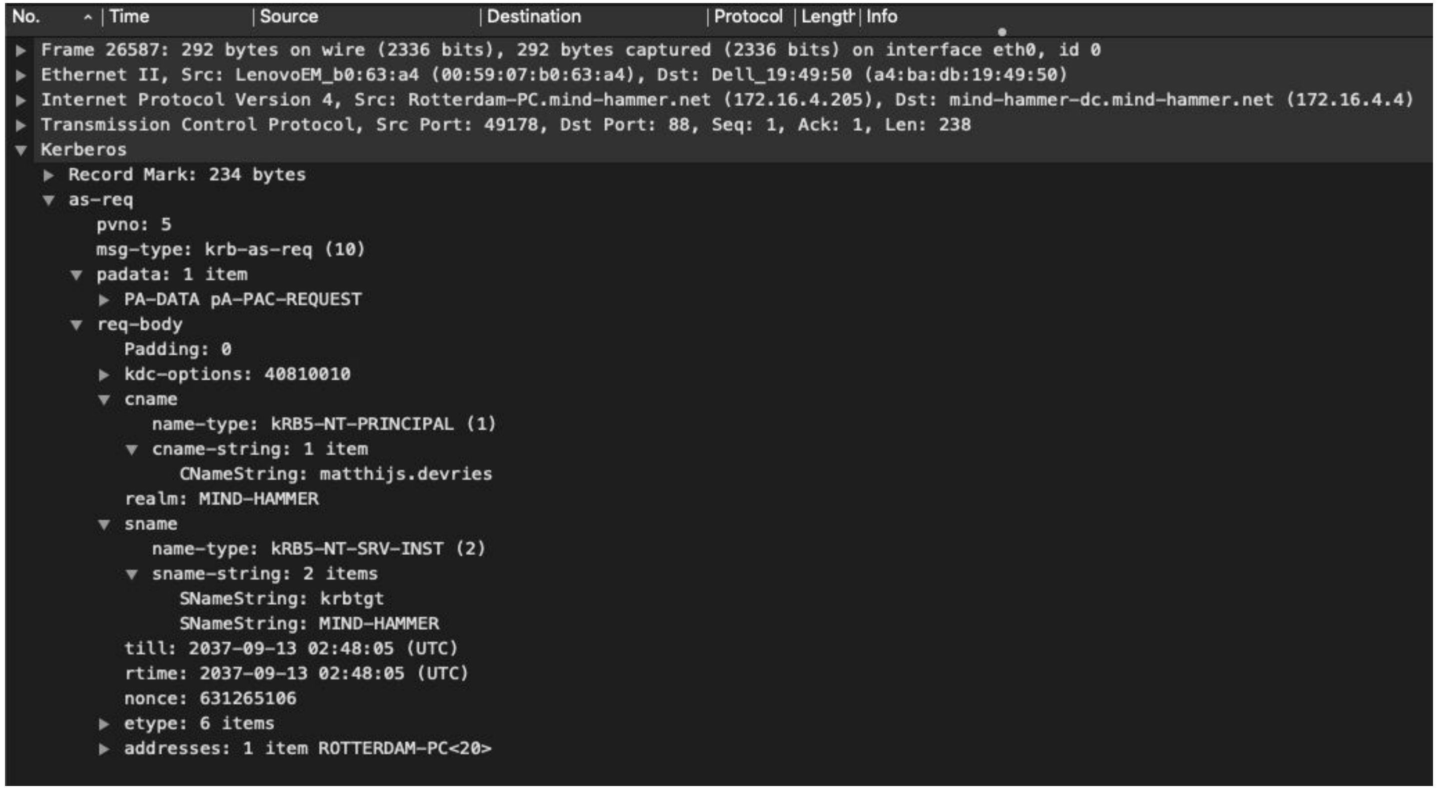
- **Watching YouTube**
- **Downloading Copyrighted BitTorrents**
- **Downloading Malware**

Normal Activity

Active Directory Authentication

Summarize the Following:

- We observed Kerberos activity on port 88, specifically Kerberos / Active Directory Authentication Requests.
- The users were requesting Kerberos tickets to authenticate to the Active Directory realm, in order to access the Active Directory files, shares, and other data needed for work.

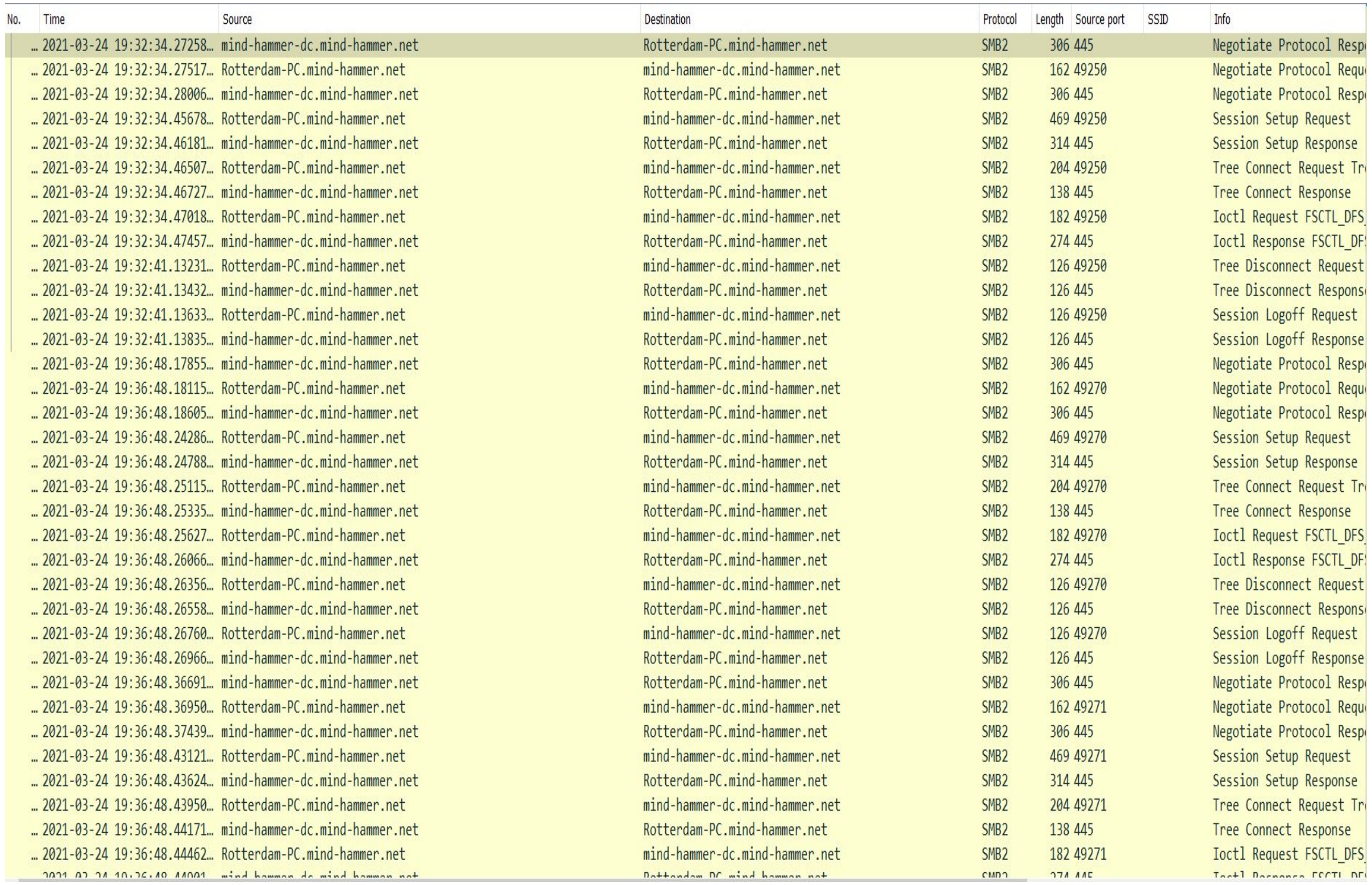


```
▶ Frame 26587: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits) on interface eth0, id 0
▶ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell_19:49:50 (a4:ba:db:19:49:50)
▶ Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: mind-hammer-dc.mind-hammer.net (172.16.4.4)
▶ Transmission Control Protocol, Src Port: 49178, Dst Port: 88, Seq: 1, Ack: 1, Len: 238
▼ Kerberos
  ▶ Record Mark: 234 bytes
  ▼ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▼ padata: 1 item
      ▶ PA-DATA pA-PAC-REQUEST
    ▼ req-body
        Padding: 0
      ▶ kdc-options: 40810010
      ▼ 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
            SNameString: krbtgt
            SNameString: MIND-HAMMER
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 631265106
      ▶ etype: 6 items
      ▶ addresses: 1 item ROTTERDAM-PC<20>
```

Accessing SMB2 Shares

Summarize the Following:

- We can see roughly 100 file shares within the sebnet 172.16.4.0/24
- Though file sharing is encrypted, this is regular activity we'll see in any professional environment

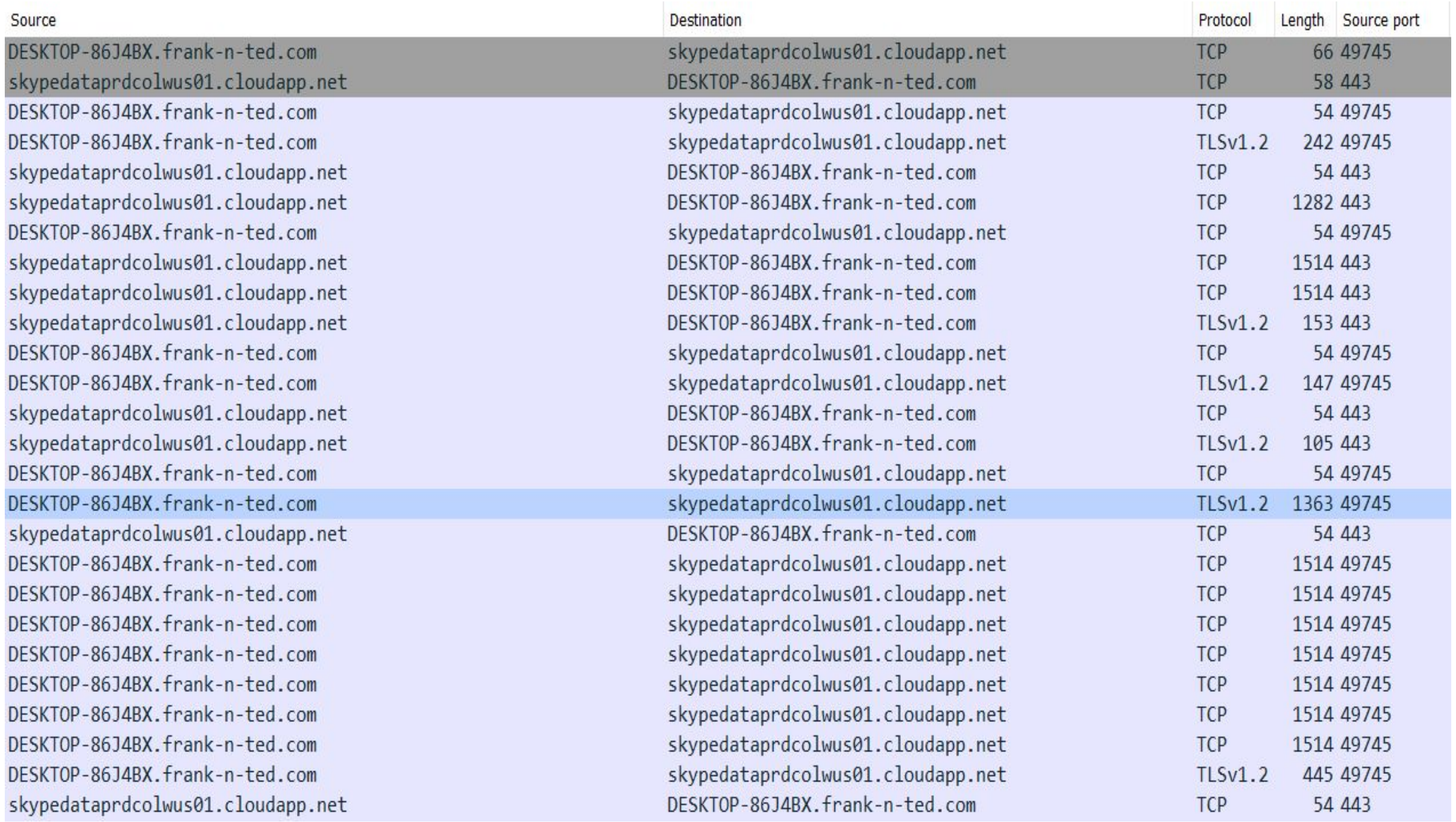


No.	Time	Source	Destination	Protocol	Length	Source port	SSID	Info
…	2021-03-24 19:32:34.27258…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	306	445		Negotiate Protocol Resp
…	2021-03-24 19:32:34.27517…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	162	49250		Negotiate Protocol Requ
…	2021-03-24 19:32:34.28006…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	306	445		Negotiate Protocol Resp
…	2021-03-24 19:32:34.45678…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	469	49250		Session Setup Request
…	2021-03-24 19:32:34.46181…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	314	445		Session Setup Response
…	2021-03-24 19:32:34.46507…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	204	49250		Tree Connect Request Tr
…	2021-03-24 19:32:34.46727…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	138	445		Tree Connect Response
…	2021-03-24 19:32:34.47018…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	182	49250		Ioctl Request FSCTL_DFS_
…	2021-03-24 19:32:34.47457…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	274	445		Ioctl Response FSCTL_DF
…	2021-03-24 19:32:41.13231…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	126	49250		Tree Disconnect Request
…	2021-03-24 19:32:41.13432…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	126	445		Tree Disconnect Respons
…	2021-03-24 19:32:41.13633…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	126	49250		Session Logoff Request
…	2021-03-24 19:32:41.13835…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	126	445		Session Logoff Response
…	2021-03-24 19:36:48.17855…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	306	445		Negotiate Protocol Resp
…	2021-03-24 19:36:48.18115…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	162	49270		Negotiate Protocol Requ
…	2021-03-24 19:36:48.18605…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	306	445		Negotiate Protocol Resp
…	2021-03-24 19:36:48.24286…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	469	49270		Session Setup Request
…	2021-03-24 19:36:48.24788…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	314	445		Session Setup Response
…	2021-03-24 19:36:48.25115…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	204	49270		Tree Connect Request Tr
…	2021-03-24 19:36:48.25335…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	138	445		Tree Connect Response
…	2021-03-24 19:36:48.25627…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	182	49270		Ioctl Request FSCTL_DFS_
…	2021-03-24 19:36:48.26066…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	274	445		Ioctl Response FSCTL_DF
…	2021-03-24 19:36:48.26356…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	126	49270		Tree Disconnect Request
…	2021-03-24 19:36:48.26558…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	126	445		Tree Disconnect Respons
…	2021-03-24 19:36:48.26760…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	126	49270		Session Logoff Request
…	2021-03-24 19:36:48.26966…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	126	445		Session Logoff Response
…	2021-03-24 19:36:48.36691…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	306	445		Negotiate Protocol Resp
…	2021-03-24 19:36:48.36950…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	162	49271		Negotiate Protocol Requ
…	2021-03-24 19:36:48.37439…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	306	445		Negotiate Protocol Resp
…	2021-03-24 19:36:48.43121…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	469	49271		Session Setup Request
…	2021-03-24 19:36:48.43624…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	314	445		Session Setup Response
…	2021-03-24 19:36:48.43950…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	204	49271		Tree Connect Request Tr
…	2021-03-24 19:36:48.44171…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	138	445		Tree Connect Response
…	2021-03-24 19:36:48.44462…	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	182	49271		Ioctl Request FSCTL_DFS_
…	2021-03-24 19:36:48.44901…	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	SMB2	274	445		Ioctl Response FSCTL_DF

Participating in Video Conferences

Summarize the Following:

- We found traffic for a skype conference which uses encrypted channels
- We see here the user first accessed windows events then proceeded to connect to skype
- Since it’s apparent the user is using other Microsoft products and applications, we can surmise that Skype is how they perform their regular video conferencing



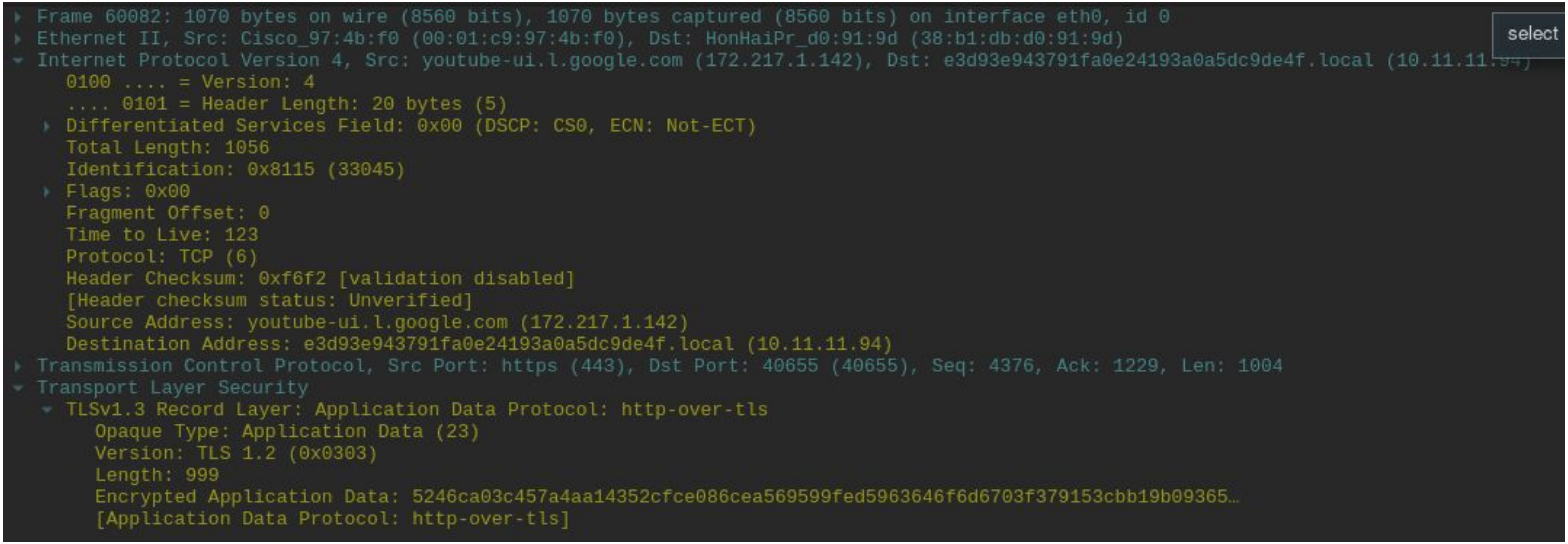
Source	Destination	Protocol	Length	Source port
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	66	49745
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	58	443
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	54	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TLSv1.2	242	49745
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	443
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	1282	443
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	54	49745
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	1514	443
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	1514	443
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TLSv1.2	153	443
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	54	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TLSv1.2	147	49745
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	443
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TLSv1.2	105	443
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	54	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TLSv1.2	1363	49745
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	443
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	1514	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	1514	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	1514	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	1514	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	1514	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	1514	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TCP	1514	49745
DESKTOP-86J4BX.frank-n-ted.com	skypedataprdcolwus01.cloudapp.net	TLSv1.2	445	49745
skypedataprdcolwus01.cloudapp.net	DESKTOP-86J4BX.frank-n-ted.com	TCP	54	443

Malicious Activity

Watching YouTube

Summarize the Following:

- We observed users watching YouTube videos while at work
- Since YouTube uses TLS for data transmission we cannot view the data as it is encrypted.

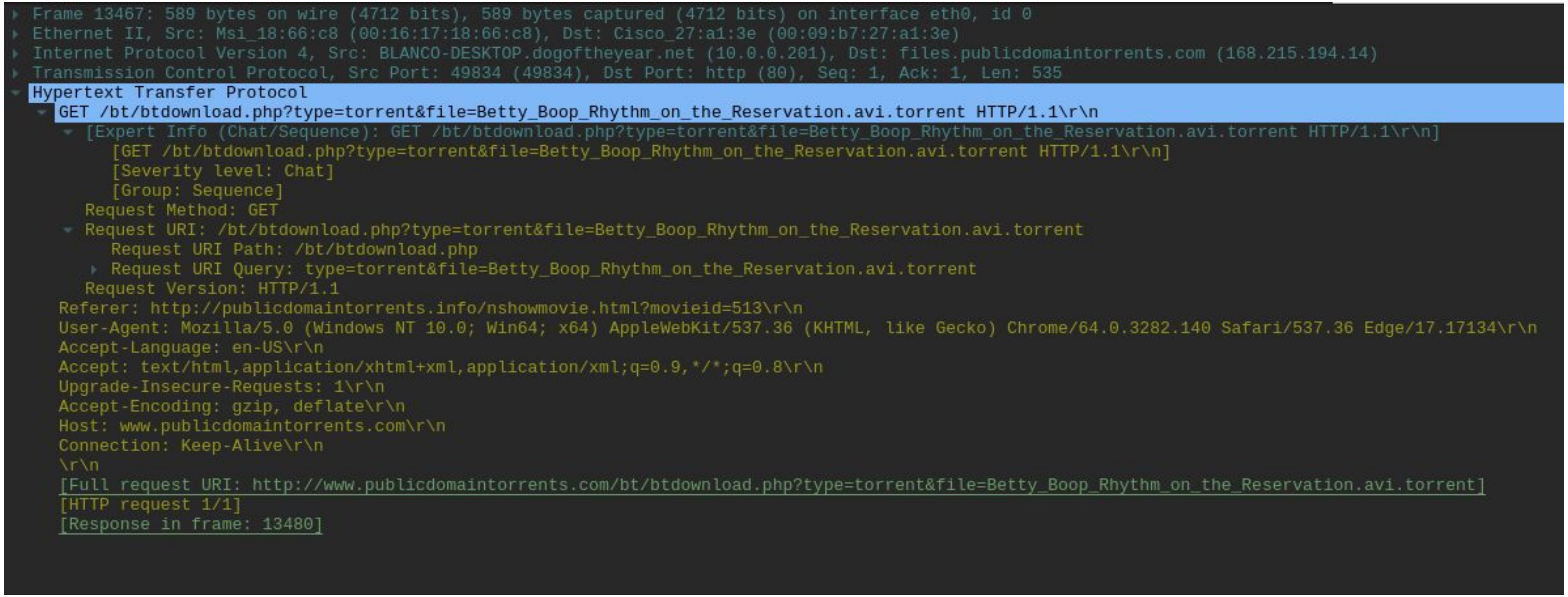


```
▸ Frame 60082: 1070 bytes on wire (8560 bits), 1070 bytes captured (8560 bits) on interface eth0, id 0
▸ Ethernet II, Src: Cisco_97:4b:f0 (00:01:c9:97:4b:f0), Dst: HonHaiPr_d0:91:9d (38:b1:db:d0:91:9d)
▾ Internet Protocol Version 4, Src: youtube-ui.l.google.com (172.217.1.142), Dst: e3d93e943791fa0e24193a0a5dc9de4f.local (10.11.11.94)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1056
    Identification: 0x8115 (33045)
  ▸ Flags: 0x00
    Fragment Offset: 0
    Time to Live: 123
    Protocol: TCP (6)
    Header Checksum: 0xf6f2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: youtube-ui.l.google.com (172.217.1.142)
    Destination Address: e3d93e943791fa0e24193a0a5dc9de4f.local (10.11.11.94)
▸ Transmission Control Protocol, Src Port: https (443), Dst Port: 40655 (40655), Seq: 4376, Ack: 1229, Len: 1004
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 999
      Encrypted Application Data: 5246ca03c457a4aa14352cfce086cea569599fed5963646f6d6703f379153cbb19b09365…
      [Application Data Protocol: http-over-tls]
```

Downloading Copyrighted BitTorrents

Summarize the Following:

- We observed an `HTTP GET` method that downloaded a torrent file.
- The user was downloaded a torrent file for a copyrighted movie, Betty Boop Rhythm on the Reservation

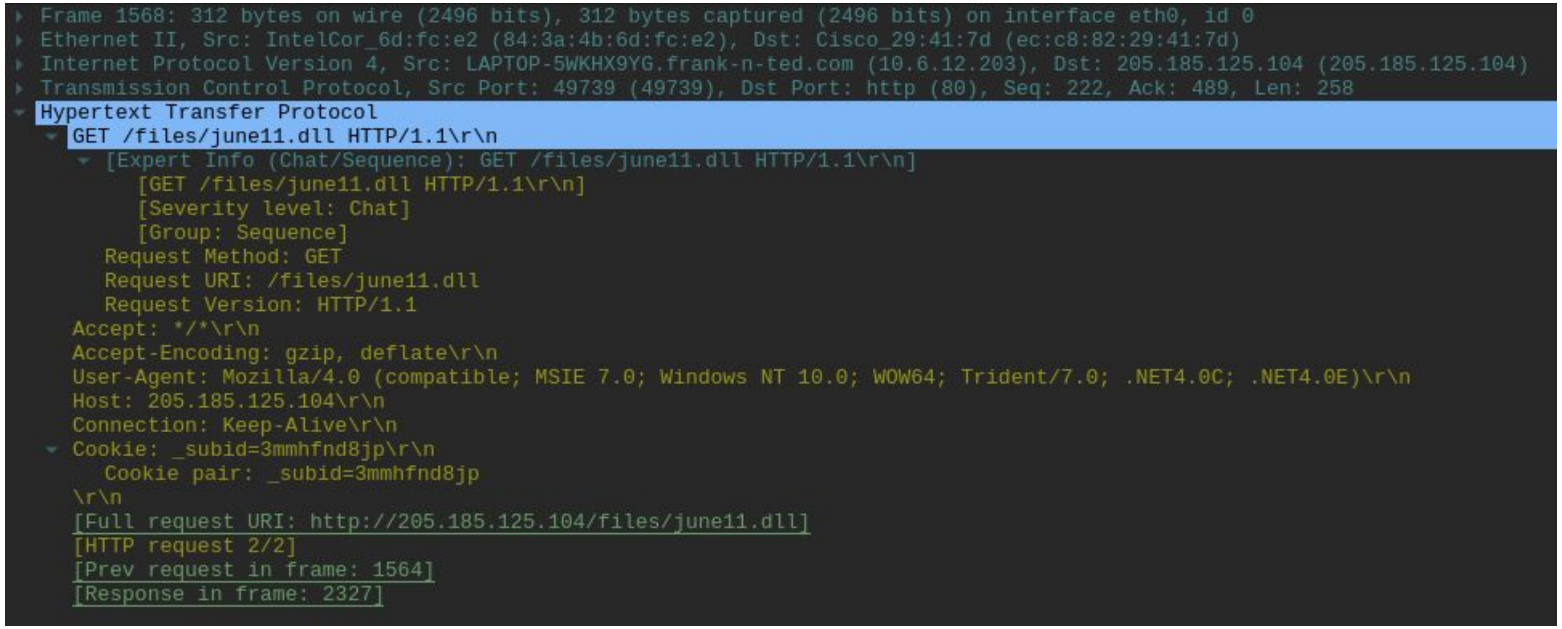


```
Frame 13467: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (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
    [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
      Request URI Path: /bt/btdownload.php
      Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
    Request Version: HTTP/1.1
  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
  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
  \r\n
  [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
  [HTTP request 1/1]
  [Response in frame: 13480]
```

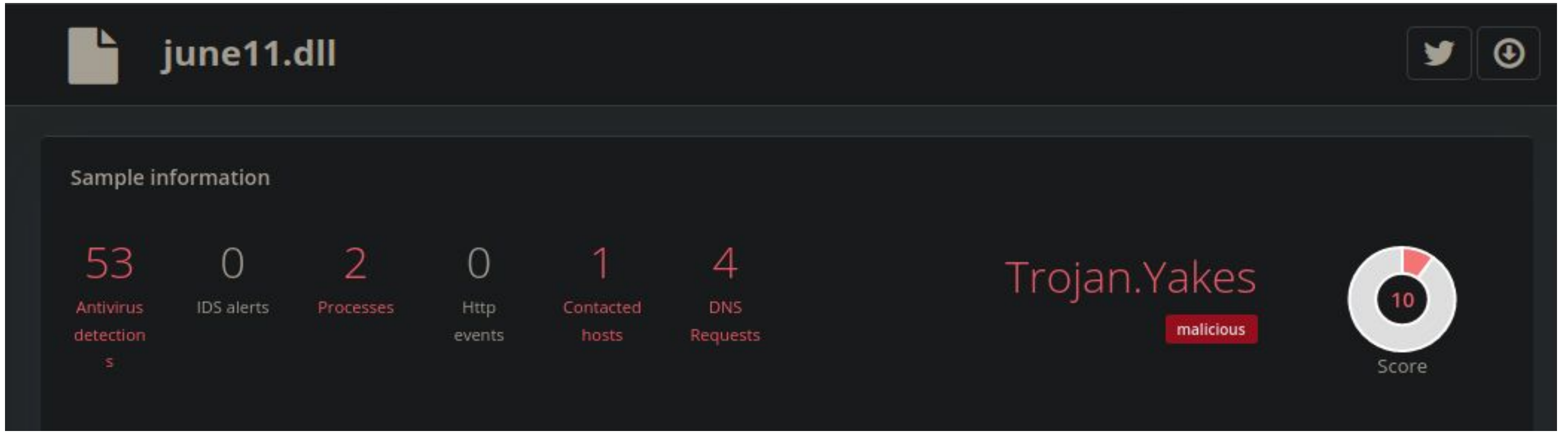
Downloading Malware

Summarize the Following:

- We observed an `HTTP GET` method that downloaded a file.
- A user on the custom domain `frank-n-ted.com` downloaded a trojan ‘`june11.dll`’
- The ‘`june11.dll’ file was found to be malicious by various different anti-virus software.`



```
▸ Frame 1568: 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)
▸ Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
▸ Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 222, Ack: 489, Len: 258
▾ Hypertext Transfer Protocol
  ▾ GET /files/june11.dll HTTP/1.1\r\n
    ▾ [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
        [GET /files/june11.dll HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /files/june11.dll
      Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
    Host: 205.185.125.104\r\n
    Connection: Keep-Alive\r\n
  ▾ Cookie: _subid=3mmhfnd8jp\r\n
      Cookie pair: _subid=3mmhfnd8jp
    \r\n
    [Full request URI: http://205.185.125.104/files/june11.dll]
    [HTTP request 2/2]
    [Prev request in frame: 1564]
    [Response in frame: 2327]
```



june11.dll

Sample information

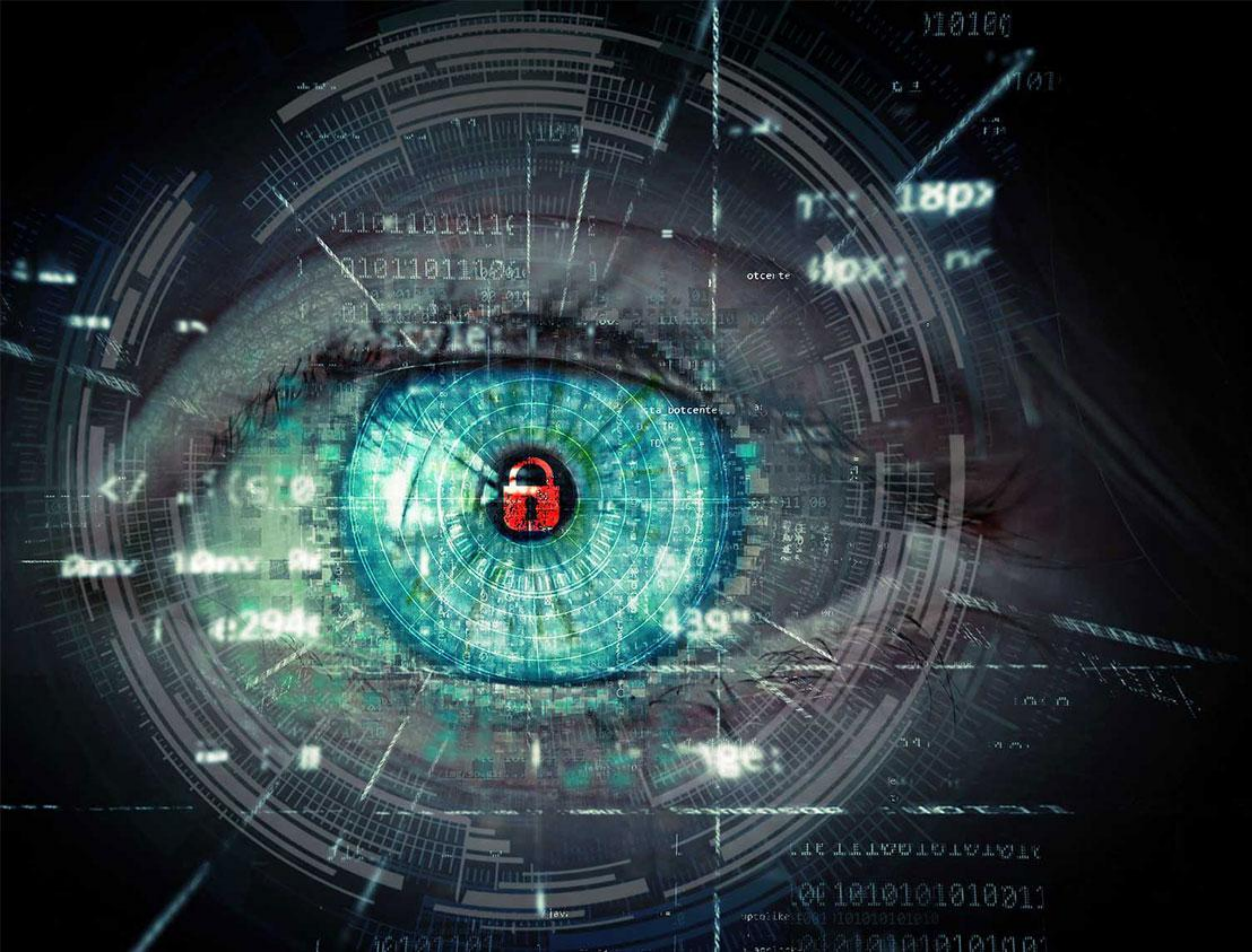
53	0	2	0	1	4
Antivirus detections	IDS alerts	Processes	Http events	Contacted hosts	DNS Requests

Trojan.Yakes

malicious

10

Score



Fín