Final Engagement

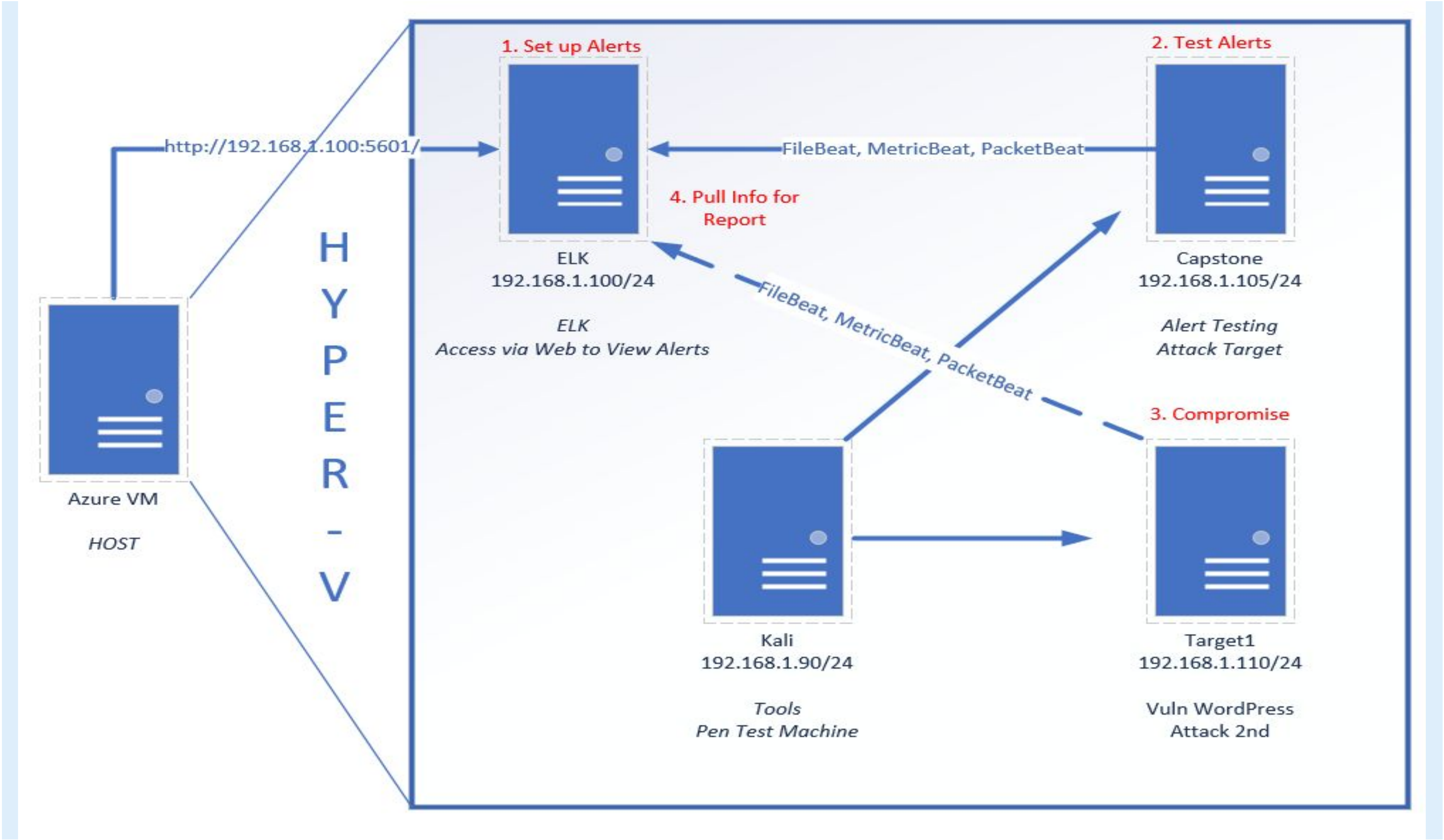
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Critical Vulnerabilities

Our assessment uncovered the following critical vulnerabilities in the network.

Vulnerability	Description	Impact
A05:2021 – Security Misconfiguration	Ports 22, 80, 111, 139, 445 were open and unfiltered	Allowed full service scan and later SSH access
A07:2021 – Identification and Authentication Failures	User had a simple guessable password	Gained SSH access
Password Plaintext Storage	MySQL database password and login were stored in plaintext file with no access controls	Gained access to database with website content and password hashes
A01:2021 – Broken Access Control	User had sudo privileges to run python	Gained unlimited root access from unauthorized user account

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	10.11.11.94, 10.11.11.179	Machines that sent the most traffic.
Most Common Protocols	TCP, TLS 1.2, HTTP	Three most common protocols on the network.
# of Unique IP Addresses	808	Count of observed IP addresses.
Subnets	10.0.0.0/24, 10.6.12.0/24, 10.11.11.0/24, 192.168.1.0/24, 172.16.4.0/24	Observed subnet ranges.
# of Malware Species	1	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

- Web Browsing
- Watching Youtube

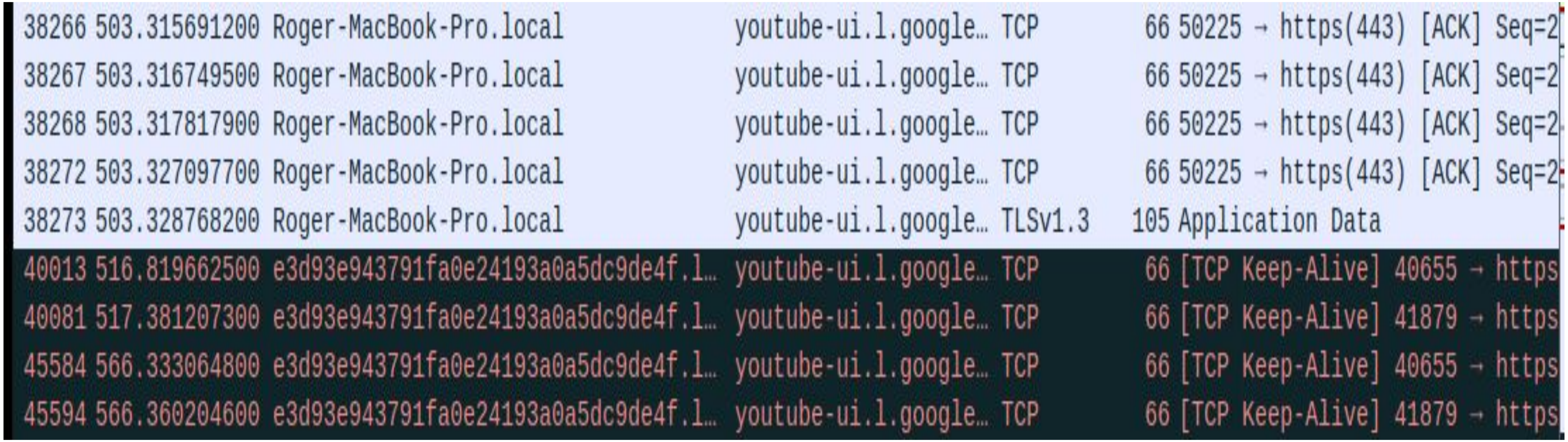
Suspicious Activity

- Private Active Directory
- Company workstation getting infected
- Illegal Downloads using Torrents

Normal Activity

Time Thieves - Youtube watchers

- TCP, TLSv1.3 protocols are used by time thieves
- Roger-MacBook-Pro.local was watching Youtube on their working hours in the office
  - Youtube

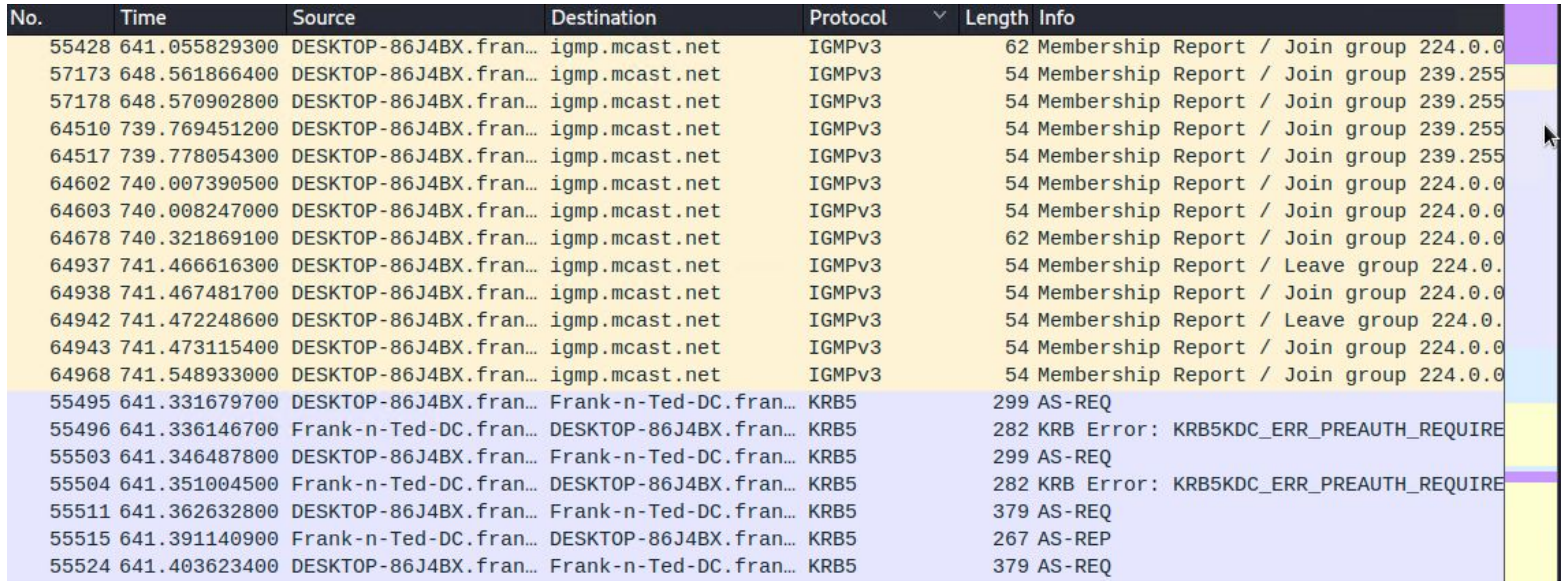


```
38266 503.315691200 Roger-MacBook-Pro.local              youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=2
38267 503.316749500 Roger-MacBook-Pro.local              youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=2
38268 503.317817900 Roger-MacBook-Pro.local              youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=2
38272 503.327097700 Roger-MacBook-Pro.local              youtube-ui.l.google… TCP        66 50225 → https(443) [ACK] Seq=2
38273 503.328768200 Roger-MacBook-Pro.local              youtube-ui.l.google… TLSv1.3   105 Application Data
40013 516.819662500 e3d93e943791fa0e24193a0a5dc9de4f.l… youtube-ui.l.google… TCP        66 [TCP Keep-Alive] 40655 → https
40081 517.381207300 e3d93e943791fa0e24193a0a5dc9de4f.l… youtube-ui.l.google… TCP        66 [TCP Keep-Alive] 41879 → https
45584 566.333064800 e3d93e943791fa0e24193a0a5dc9de4f.l… youtube-ui.l.google… TCP        66 [TCP Keep-Alive] 40655 → https
45594 566.360204600 e3d93e943791fa0e24193a0a5dc9de4f.l… youtube-ui.l.google… TCP        66 [TCP Keep-Alive] 41879 → https
```

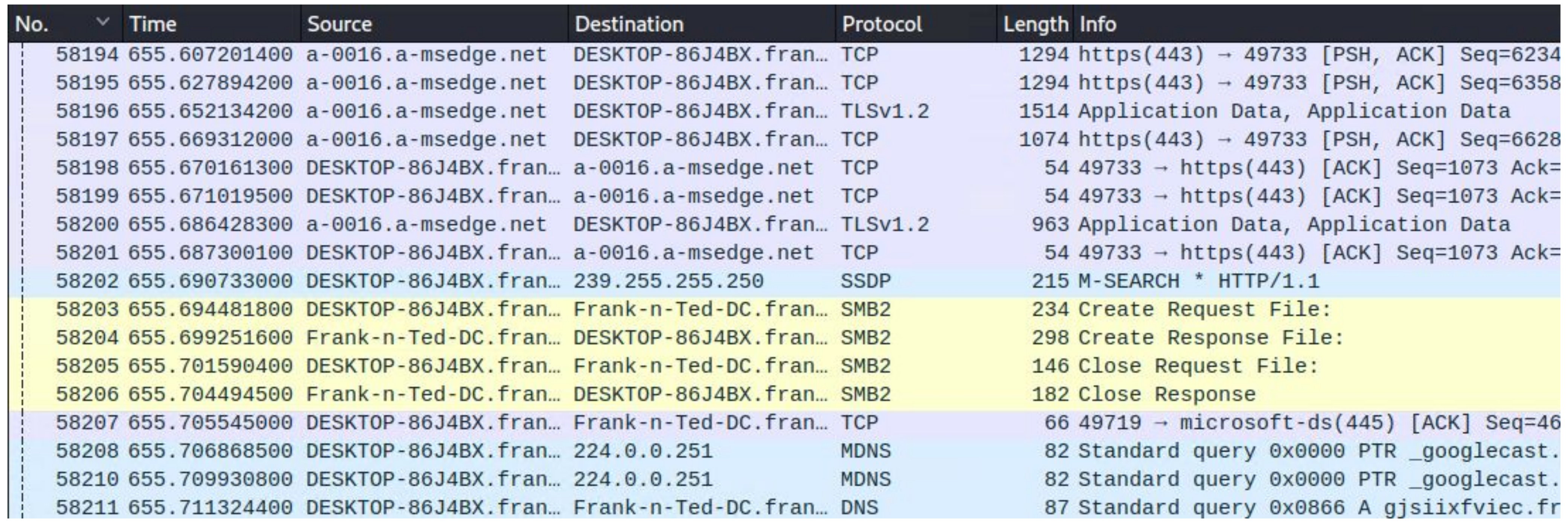
Malicious Activity

Time Thieves - Private Active Directory Network

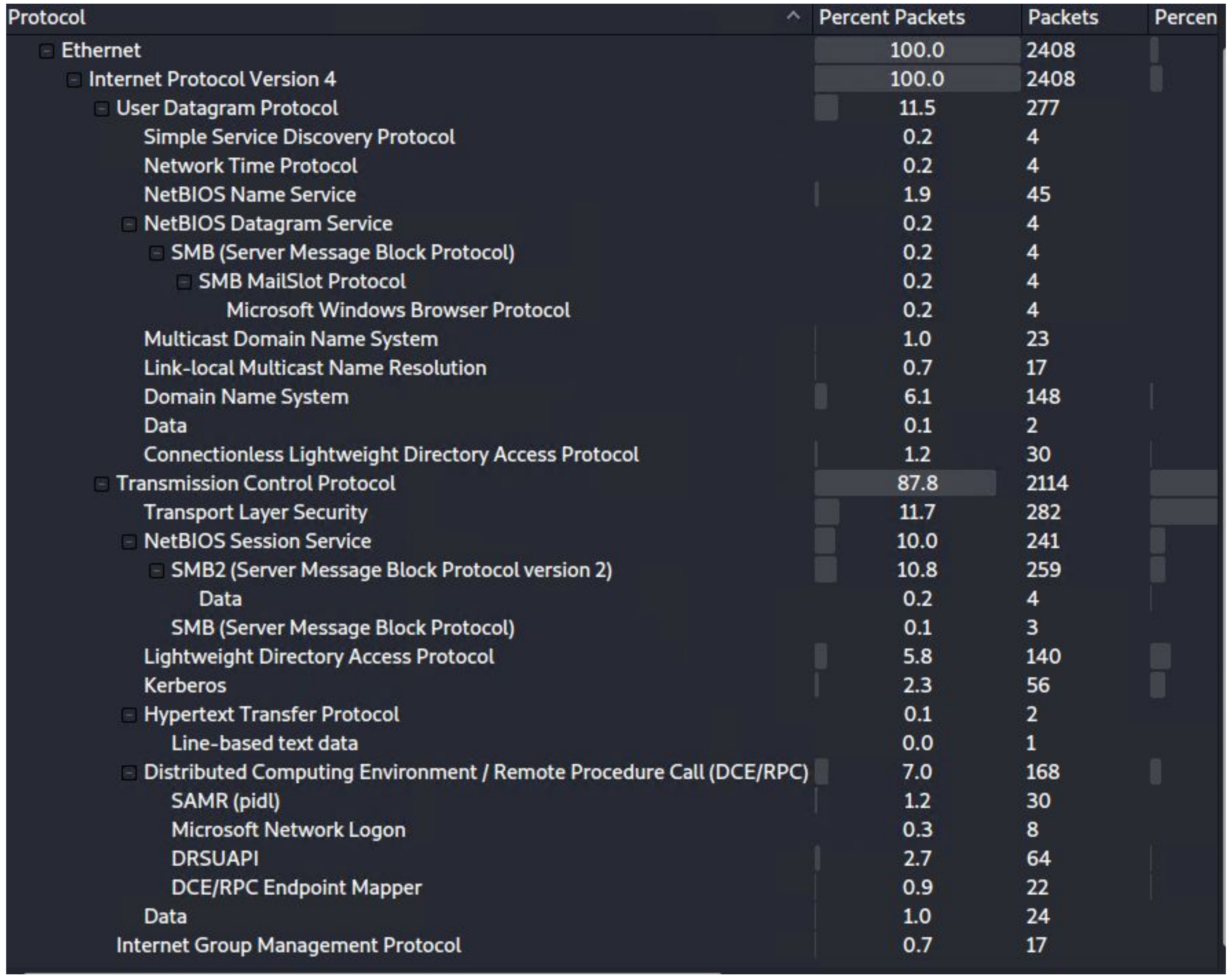
- TCP, CLDAP, LDAP, DNS, NBNS, DCERPC, EPM, DRSUAPI, KRB5, MDNS, NTP, RPC_NETLOGON, SAMR, SMB2, TLSv1.2, TLSv1.3, IGMPv3, SSDP, UDP protocols were used from or to the AD
- They have set up their own Active Directory Network using corporate resources



```
No.    Time          Source                Destination           Protocol    Length Info
 55428 641.055829300 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          62 Membership Report / Join group 224.0.0
 57173 648.561866400 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 239.255
 57178 648.570902800 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 239.255
 64510 739.769451200 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 239.255
 64517 739.778054300 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 239.255
 64602 740.007390500 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 224.0.0
 64603 740.008247000 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 224.0.0
 64678 740.321869100 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          62 Membership Report / Join group 224.0.0
 64937 741.466616300 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Leave group 224.0.
 64938 741.467481700 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 224.0.0
 64942 741.472248600 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Leave group 224.0.
 64943 741.473115400 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 224.0.0
 64968 741.548933000 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3          54 Membership Report / Join group 224.0.0
 55495 641.331679700 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… KRB5           299 AS-REQ
 55496 641.336146700 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… KRB5           282 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRE
 55503 641.346487800 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… KRB5           299 AS-REQ
 55504 641.351004500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… KRB5           282 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRE
 55511 641.362632800 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… KRB5           379 AS-REQ
 55515 641.391140900 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… KRB5           267 AS-REP
 55524 641.403623400 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… KRB5           379 AS-REQ
```



```
No.    Time          Source                Destination           Protocol    Length Info
 58194 655.607201400 a-0016.a-msedge.net  DESKTOP-86J4BX.fran… TCP           1294 https(443) → 49733 [PSH, ACK] Seq=6234
 58195 655.627894200 a-0016.a-msedge.net  DESKTOP-86J4BX.fran… TCP           1294 https(443) → 49733 [PSH, ACK] Seq=6358
 58196 655.652134200 a-0016.a-msedge.net  DESKTOP-86J4BX.fran… TLSv1.2       1514 Application Data, Application Data
 58197 655.669312000 a-0016.a-msedge.net  DESKTOP-86J4BX.fran… TCP           1074 https(443) → 49733 [PSH, ACK] Seq=6628
 58198 655.670161300 DESKTOP-86J4BX.fran… a-0016.a-msedge.net  TCP             54 49733 → https(443) [ACK] Seq=1073 Ack=
 58199 655.671019500 DESKTOP-86J4BX.fran… a-0016.a-msedge.net  TCP             54 49733 → https(443) [ACK] Seq=1073 Ack=
 58200 655.686428300 a-0016.a-msedge.net  DESKTOP-86J4BX.fran… TLSv1.2        963 Application Data, Application Data
 58201 655.687300100 DESKTOP-86J4BX.fran… a-0016.a-msedge.net  TCP             54 49733 → https(443) [ACK] Seq=1073 Ack=
 58202 655.690733000 DESKTOP-86J4BX.fran… 239.255.255.250      SSDP           215 M-SEARCH * HTTP/1.1
 58203 655.694481800 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… SMB2           234 Create Request File:
 58204 655.699251600 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… SMB2           298 Create Response File:
 58205 655.701590400 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… SMB2           146 Close Request File:
 58206 655.704494500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… SMB2           182 Close Response
 58207 655.705545000 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… TCP             66 49719 → microsoft-ds(445) [ACK] Seq=46
 58208 655.706868500 DESKTOP-86J4BX.fran… 224.0.0.251          MDNS            82 Standard query 0x0000 PTR _googlecast.
 58210 655.709930800 DESKTOP-86J4BX.fran… 224.0.0.251          MDNS            82 Standard query 0x0000 PTR _googlecast.
 58211 655.711324400 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… DNS             87 Standard query 0x0866 A gjsiixfviec.fr
```

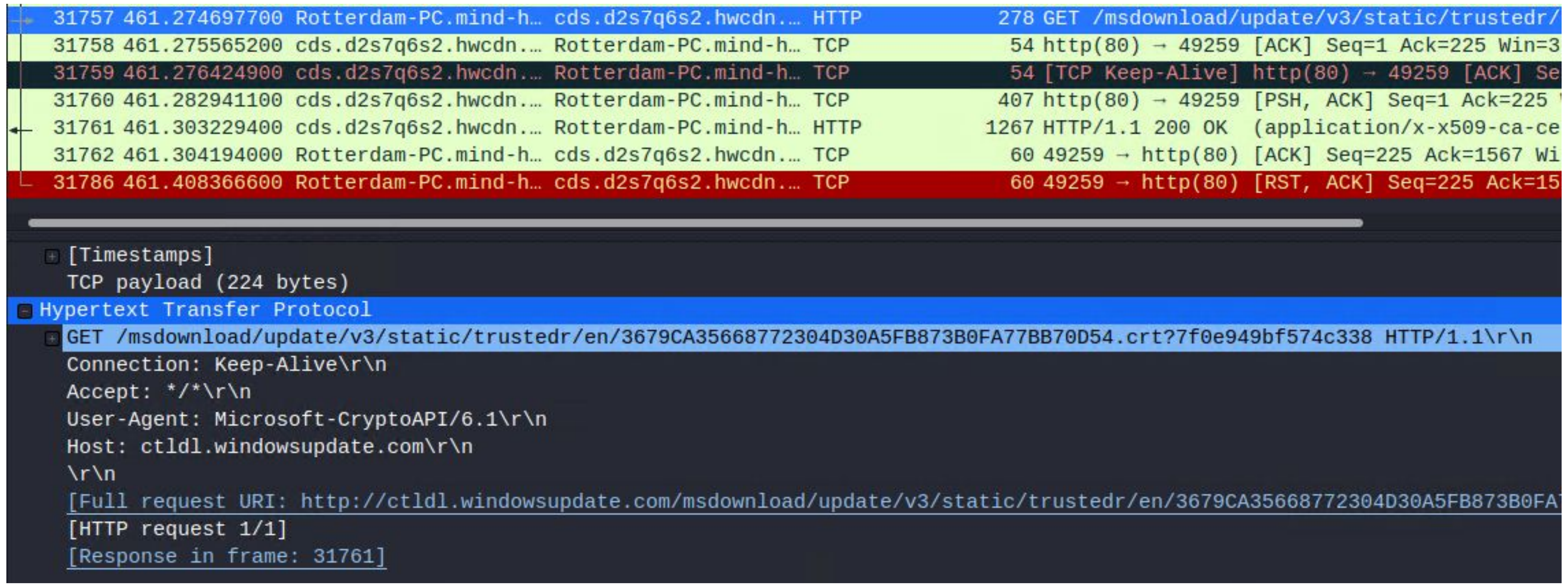


```
Protocol                                                                  Percent Packets  Packets  Percen
 Ethernet                                                                          100.0     2408
   Internet Protocol Version 4                                                     100.0     2408
     User Datagram Protocol                                                         11.5      277
       Simple Service Discovery Protocol                                             0.2        4
       Network Time Protocol                                                         0.2        4
       NetBIOS Name Service                                                          1.9       45
       NetBIOS Datagram Service                                                      0.2        4
         SMB (Server Message Block Protocol)                                         0.2        4
           SMB MailSlot Protocol                                                     0.2        4
             Microsoft Windows Browser Protocol                                      0.2        4
       Multicast Domain Name System                                                  1.0       23
       Link-local Multicast Name Resolution                                          0.7       17
       Domain Name System                                                            6.1      148
       Data                                                                          0.1        2
       Connectionless Lightweight Directory Access Protocol                          1.2       30
     Transmission Control Protocol                                                  87.8     2114
       Transport Layer Security                                                     11.7      282
       NetBIOS Session Service                                                      10.0      241
         SMB2 (Server Message Block Protocol version 2)                             10.8      259
           Data                                                                      0.2        4
         SMB (Server Message Block Protocol)                                         0.1        3
       Lightweight Directory Access Protocol                                         5.8      140
       Kerberos                                                                      2.3       56
       Hypertext Transfer Protocol                                                   0.1        2
         Line-based text data                                                        0.0        1
       Distributed Computing Environment / Remote Procedure Call (DCE/RPC)           7.0      168
         SAMR (pidl)                                                                 1.2       30
         Microsoft Network Logon                                                     0.3        8
         DRSUAPI                                                                     2.7       64
         DCE/RPC Endpoint Mapper                                                     0.9       22
       Data                                                                          1.0       24
     Internet Group Management Protocol                                              0.7       17
```

Vulnerable Windows Machines - Illegal Downloads

Summarize the following:

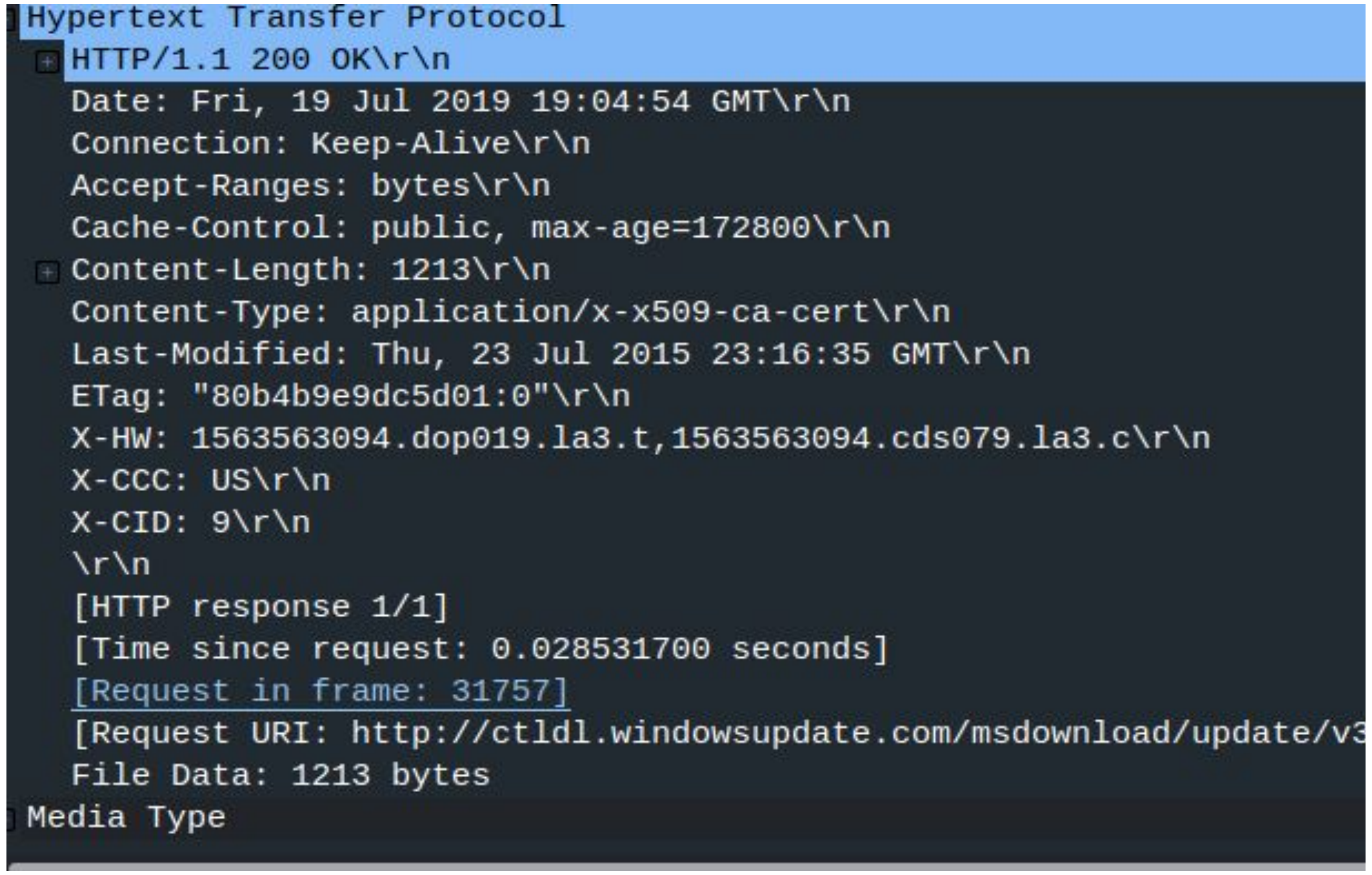
- Traffic observed involved the following culprit:
  - IP address: 172.16.5.205
  - MAC address: 00:59:07:b0:63:a4
  - Host name: rotterdam-PC.mindhammer.net
  - User name of infected machine: matthijs.devries



```
31757 461.274697700 Rotterdam-PC.mind-h… cds.d2s7q6s2.hwcdn.… HTTP        278 GET /msdownload/update/v3/static/trustedr/
31758 461.275565200 cds.d2s7q6s2.hwcdn.… Rotterdam-PC.mind-h… TCP          54 http(80) → 49259 [ACK] Seq=1 Ack=225 Win=3
31759 461.276424900 cds.d2s7q6s2.hwcdn.… Rotterdam-PC.mind-h… TCP          54 [TCP Keep-Alive] http(80) → 49259 [ACK] Se
31760 461.282941100 cds.d2s7q6s2.hwcdn.… Rotterdam-PC.mind-h… TCP         407 http(80) → 49259 [PSH, ACK] Seq=1 Ack=225
31761 461.303229400 cds.d2s7q6s2.hwcdn.… Rotterdam-PC.mind-h… HTTP       1267 HTTP/1.1 200 OK  (application/x-x509-ca-ce
31762 461.304194000 Rotterdam-PC.mind-h… cds.d2s7q6s2.hwcdn.… TCP          60 49259 → http(80) [ACK] Seq=225 Ack=1567 Wi
31786 461.408366600 Rotterdam-PC.mind-h… cds.d2s7q6s2.hwcdn.… TCP          60 49259 → http(80) [RST, ACK] Seq=225 Ack=15

  [Timestamps]
  TCP payload (224 bytes)
Hypertext Transfer Protocol
  GET /msdownload/update/v3/static/trustedr/en/3679CA35668772304D30A5FB873B0FA77BB70D54.crt?7f0e949bf574c338 HTTP/1.1\r\n
  Connection: Keep-Alive\r\n
  Accept: */*\r\n
  User-Agent: Microsoft-CryptoAPI/6.1\r\n
  Host: ctldl.windowsupdate.com\r\n
  \r\n
  [Full request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/3679CA35668772304D30A5FB873B0FA
  [HTTP request 1/1]
  [Response in frame: 31761]
```

- matthijs.devries machine with IP address of “172.16.4.205” downloaded Trojan malware

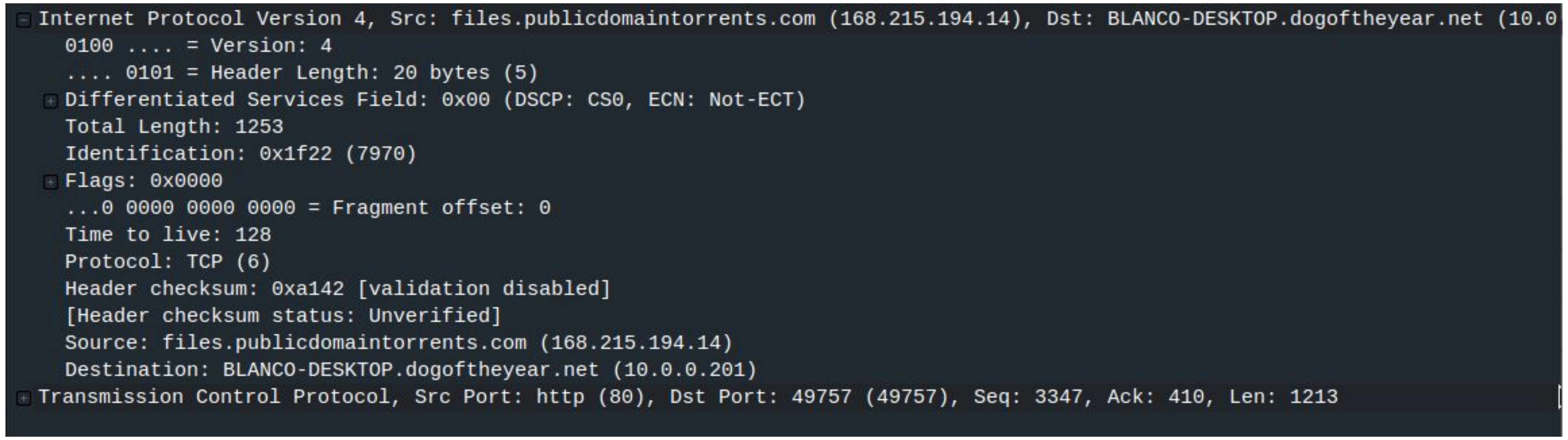


```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 19 Jul 2019 19:04:54 GMT\r\n
  Connection: Keep-Alive\r\n
  Accept-Ranges: bytes\r\n
  Cache-Control: public, max-age=172800\r\n
  Content-Length: 1213\r\n
  Content-Type: application/x-x509-ca-cert\r\n
  Last-Modified: Thu, 23 Jul 2015 23:16:35 GMT\r\n
  ETag: "80b4b9e9dc5d01:0"\r\n
  X-HW: 1563563094.dop019.la3.t,1563563094.cds079.la3.c\r\n
  X-CCC: US\r\n
  X-CID: 9\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.028531700 seconds]
  [Request in frame: 31757]
  [Request URI: http://ctldl.windowsupdate.com/msdownload/update/v3
  File Data: 1213 bytes
Media Type
```

Illegal Downloads - torrents

Summarize the following:

- Traffic observed involved the following culprit:
  - IP address: 10.0.0.201
  - MAC address: 00:16:17:18:66:c8
  - Windows username: elmer.banco
  - OS version: Windows 10 NT 10.0
- The user was browsing a website called dogoftheyear.net and downloaded a file called “Betty_Boop_Rythm_on_the_Reservation.avi”



```
⊟ Internet Protocol Version 4, Src: files.publicdomaintorrents.com (168.215.194.14), Dst: BLANCO-DESKTOP.dogoftheyear.net (10.0
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ⊞ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1253
    Identification: 0x1f22 (7970)
  ⊞ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xa142 [validation disabled]
    [Header checksum status: Unverified]
    Source: files.publicdomaintorrents.com (168.215.194.14)
    Destination: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49757 (49757), Seq: 3347, Ack: 410, Len: 1213
```

The End