Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

[Start of Network Analysis]

Table of Contents

This document contains the following resources:

Traffic Profile

Normal Activity

Malicious Activity

Traffic Profile

Traffic Profile

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 - (44.36%) 185.243.115.84 - (27.87%) 10.0.0.201 - (24.96%) 166.62.111.64 - (12.34%)	Machines that sent the most traffic.

Most Common Protocols	TCP(86%)-TLS(8.4) HTTP(3.6)
	UDP(14%)-NETBIOS data(9.5)
		Three most common protocols on the network.

# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	192.168.1.0/24	Observed subnet ranges.
# of Malware Species	55	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

- Using working related websites; Akamai, google-analytics, double-click
- Some personal traffic: amazon, sky, youtube

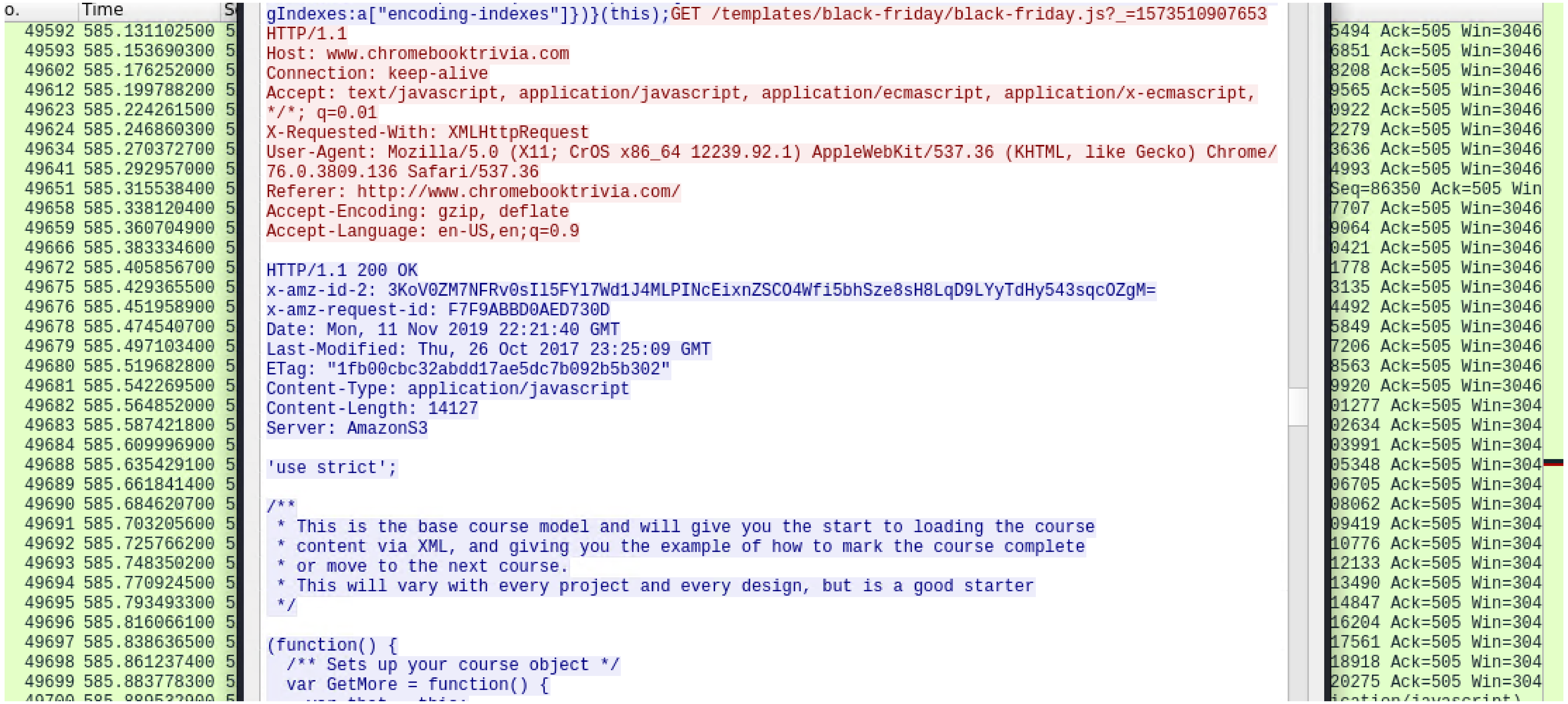
Suspicious Activity

- Sending malware, set up an unauthorized Active Directory

Normal Activity

Normal Professional Use

- TCP and HTTP traffic
- This user was looking for templates for a web page for a black friday sale
- Include a description of any interesting files.



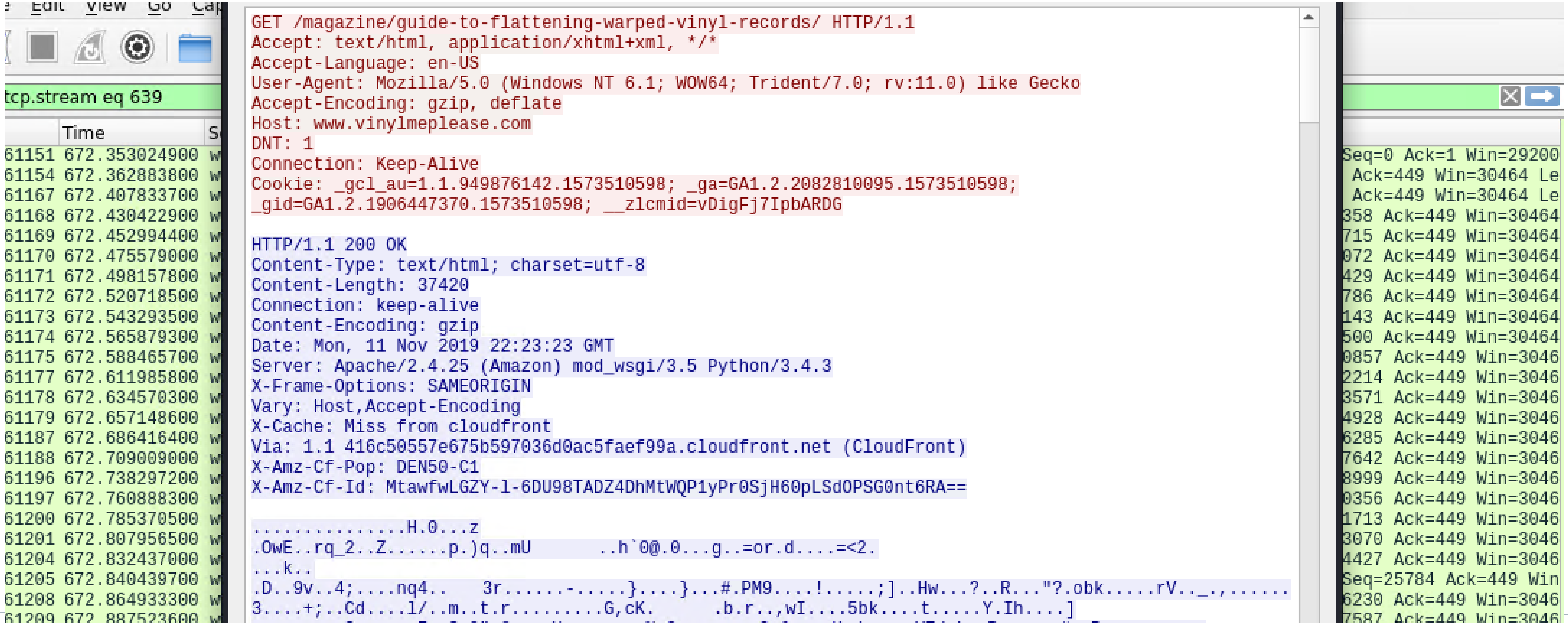
```
o.     Time          S
 49592 585.131102500 5
 49593 585.153690300 5
 49602 585.176252000 5
 49612 585.199788200 5
 49623 585.224261500 5
 49624 585.246860300 5
 49634 585.270372700 5
 49641 585.292957000 5
 49651 585.315538400 5
 49658 585.338120400 5
 49659 585.360704900 5
 49666 585.383334600 5
 49672 585.405856700 5
 49675 585.429365500 5
 49676 585.451958900 5
 49678 585.474540700 5
 49679 585.497103400 5
 49680 585.519682800 5
 49681 585.542269500 5
 49682 585.564852000 5
 49683 585.587421800 5
 49684 585.609996900 5
 49688 585.635429100 5
 49689 585.661841400 5
 49690 585.684620700 5
 49691 585.703205600 5
 49692 585.725766200 5
 49693 585.748350200 5
 49694 585.770924500 5
 49695 585.793493300 5
 49696 585.816066100 5
 49697 585.838636500 5
 49698 585.861237400 5
 49699 585.883778300 5
```

```
gIndexes:a["encoding-indexes"]})}(this);GET /templates/black-friday/black-friday.js?_=1573510907653
HTTP/1.1
Host: www.chromebooktrivia.com
Connection: keep-alive
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript,
*/*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
76.0.3809.136 Safari/537.36
Referer: http://www.chromebooktrivia.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
x-amz-id-2: 3KoV0ZM7NFRv0sIl5FYl7Wd1J4MLPINcEixnZSCO4Wfi5bhSze8sH8LqD9LYyTdHy543sqcOZgM=
x-amz-request-id: F7F9ABBD0AED730D
Date: Mon, 11 Nov 2019 22:21:40 GMT
Last-Modified: Thu, 26 Oct 2017 23:25:09 GMT
ETag: "1fb00cbc32abdd17ae5dc7b092b5b302"
Content-Type: application/javascript
Content-Length: 14127
Server: AmazonS3

'use strict';

/**
 * This is the base course model and will give you the start to loading the course
 * content via XML, and giving you the example of how to mark the course complete
 * or move to the next course.
 * This will vary with every project and every design, but is a good starter
 */

(function() {
  /** Sets up your course object */
  var GetMore = function() {
```

```
5494 Ack=505 Win=3046
6851 Ack=505 Win=3046
8208 Ack=505 Win=3046
9565 Ack=505 Win=3046
0922 Ack=505 Win=3046
2279 Ack=505 Win=3046
3636 Ack=505 Win=3046
4993 Ack=505 Win=3046
Seq=86350 Ack=505 Win
7707 Ack=505 Win=3046
9064 Ack=505 Win=3046
0421 Ack=505 Win=3046
1778 Ack=505 Win=3046
3135 Ack=505 Win=3046
4492 Ack=505 Win=3046
5849 Ack=505 Win=3046
7206 Ack=505 Win=3046
8563 Ack=505 Win=3046
9920 Ack=505 Win=3046
01277 Ack=505 Win=304
02634 Ack=505 Win=304
03991 Ack=505 Win=304
05348 Ack=505 Win=304
06705 Ack=505 Win=304
08062 Ack=505 Win=304
09419 Ack=505 Win=304
10776 Ack=505 Win=304
12133 Ack=505 Win=304
13490 Ack=505 Win=304
14847 Ack=505 Win=304
16204 Ack=505 Win=304
17561 Ack=505 Win=304
18918 Ack=505 Win=304
20275 Ack=505 Win=304
```

Normal Personal Use:

- TCP and HTTP
- Looking up how to flatten warped vinyl records



```
tcp.stream eq 639
```

```
61151 672.353024900 w
61154 672.362883800 w
61167 672.407833700 w
61168 672.430422900 w
61169 672.452994400 w
61170 672.475579000 w
61171 672.498157800 w
61172 672.520718500 w
61173 672.543293500 w
61174 672.565879300 w
61175 672.588465700 w
61177 672.611985800 w
61178 672.634570300 w
61179 672.657148600 w
61187 672.686416400 w
61188 672.709009000 w
61196 672.738297200 w
61197 672.760888300 w
61200 672.785370500 w
61201 672.807956500 w
61204 672.832437000 w
61205 672.840439700 w
61208 672.864933300 w
61209 672.887523600 w
```

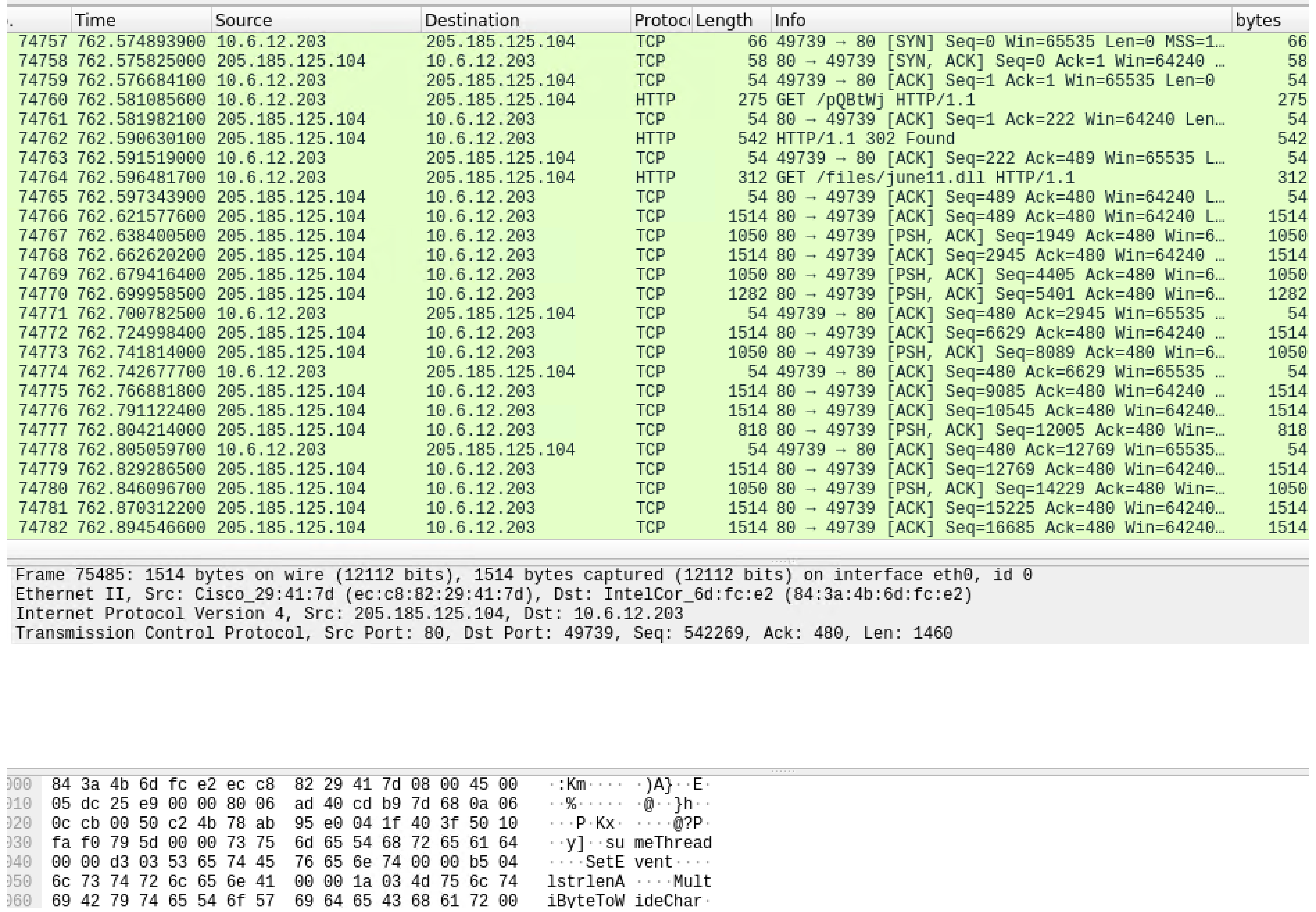
```
GET /magazine/guide-to-flattening-warped-vinyl-records/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.vinylmeplease.com
DNT: 1
Connection: Keep-Alive
Cookie: _gcl_au=1.1.949876142.1573510598; _ga=GA1.2.2082810095.1573510598;
_gid=GA1.2.1906447370.1573510598; __zlcmid=vDigFj7IpbARDG

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 37420
Connection: keep-alive
Content-Encoding: gzip
Date: Mon, 11 Nov 2019 22:23:23 GMT
Server: Apache/2.4.25 (Amazon) mod_wsgi/3.5 Python/3.4.3
X-Frame-Options: SAMEORIGIN
Vary: Host,Accept-Encoding
X-Cache: Miss from cloudfront
Via: 1.1 416c50557e675b597036d0ac5faef99a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: DEN50-C1
X-Amz-Cf-Id: MtawfwLGZY-l-6DU98TADZ4DhMtWQP1yPr0SjH60pLSdOPSG0nt6RA==

...............H.0...z
.OwE..rq_2..Z......p.)q..mU       ..h`0@.0...g..=or.d....=<2.
...k..
.D..9v..4;....nq4..   3r......-.....}....}...#.PM9....!.....;]..Hw...?..R..."?.obk.....rV.._.,......
3....+;..Cd....l/..m..t.r.........G,cK.      .b.r..,wI....5bk....t.....Y.Ih....]
```

```
Seq=0 Ack=1 Win=29200
 Ack=449 Win=30464 Le
 Ack=449 Win=30464 Le
358 Ack=449 Win=30464
715 Ack=449 Win=30464
072 Ack=449 Win=30464
429 Ack=449 Win=30464
786 Ack=449 Win=30464
143 Ack=449 Win=30464
500 Ack=449 Win=30464
0857 Ack=449 Win=3046
2214 Ack=449 Win=3046
3571 Ack=449 Win=3046
4928 Ack=449 Win=3046
6285 Ack=449 Win=3046
7642 Ack=449 Win=3046
8999 Ack=449 Win=3046
0356 Ack=449 Win=3046
1713 Ack=449 Win=3046
3070 Ack=449 Win=3046
4427 Ack=449 Win=3046
Seq=25784 Ack=449 Win
6230 Ack=449 Win=3046
7587 Ack=449 Win=3046
```

Malicious Activity

Download Unverified Software

- Given that the malware was downloaded off the internet we see a mostly TCP and HTTP packets
- The IP the hosted the file is 205.185.125.104 and it was not able to resolve a name.
- june11.dll contains 55 malware binaries including those that affect the kernel, change registry keys, and create processes.



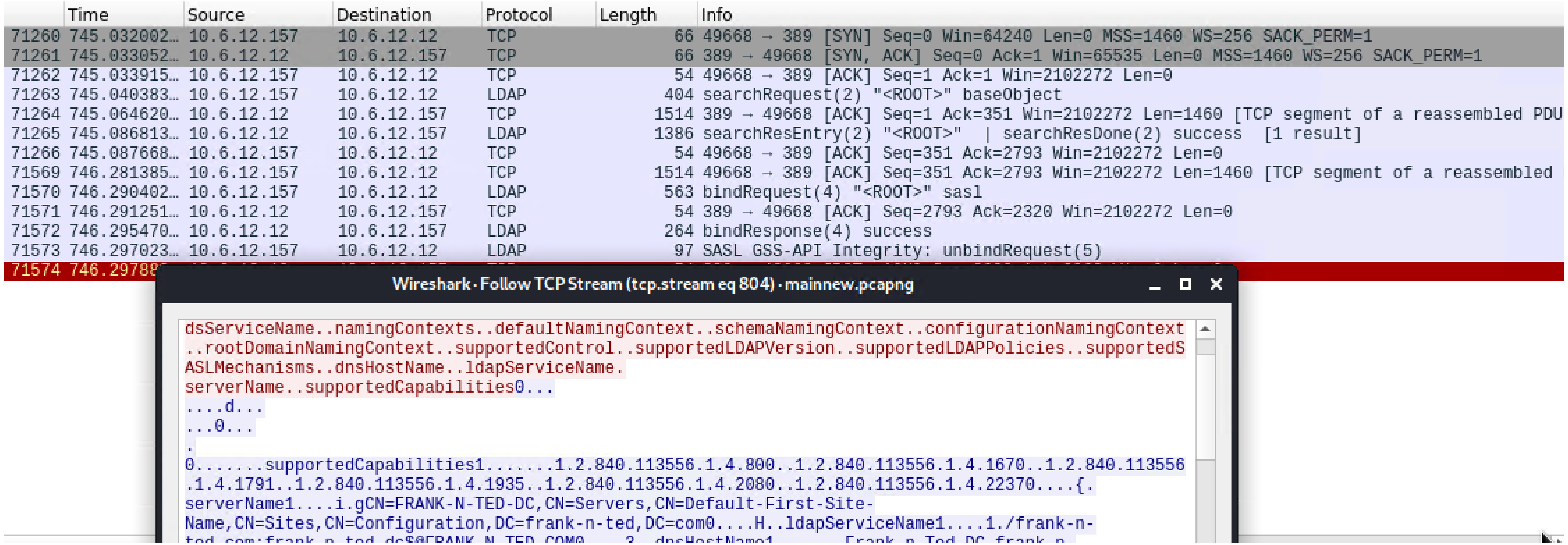
```
.      Time         Source          Destination     Protoc Length Info                                                bytes
 74757 762.574893900 10.6.12.203     205.185.125.104 TCP        66 49739 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1…         66
 74758 762.575825000 205.185.125.104 10.6.12.203     TCP        58 80 → 49739 [SYN, ACK] Seq=0 Ack=1 Win=64240 …         58
 74759 762.576684100 10.6.12.203     205.185.125.104 TCP        54 49739 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0          54
 74760 762.581085600 10.6.12.203     205.185.125.104 HTTP      275 GET /pQBtWj HTTP/1.1                                 275
 74761 762.581982100 205.185.125.104 10.6.12.203     TCP        54 80 → 49739 [ACK] Seq=1 Ack=222 Win=64240 Len…         54
 74762 762.590630100 205.185.125.104 10.6.12.203     HTTP      542 HTTP/1.1 302 Found                                   542
 74763 762.591519000 10.6.12.203     205.185.125.104 TCP        54 49739 → 80 [ACK] Seq=222 Ack=489 Win=65535 L…         54
 74764 762.596481700 10.6.12.203     205.185.125.104 HTTP      312 GET /files/june11.dll HTTP/1.1                       312
 74765 762.597343900 205.185.125.104 10.6.12.203     TCP        54 80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 L…         54
 74766 762.621577600 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 L…       1514
 74767 762.638400500 205.185.125.104 10.6.12.203     TCP      1050 80 → 49739 [PSH, ACK] Seq=1949 Ack=480 Win=6…       1050
 74768 762.662620200 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=2945 Ack=480 Win=64240 …       1514
 74769 762.679416400 205.185.125.104 10.6.12.203     TCP      1050 80 → 49739 [PSH, ACK] Seq=4405 Ack=480 Win=6…       1050
 74770 762.699958500 205.185.125.104 10.6.12.203     TCP      1282 80 → 49739 [PSH, ACK] Seq=5401 Ack=480 Win=6…       1282
 74771 762.700782500 10.6.12.203     205.185.125.104 TCP        54 49739 → 80 [ACK] Seq=480 Ack=2945 Win=65535 …         54
 74772 762.724998400 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=6629 Ack=480 Win=64240 …       1514
 74773 762.741814000 205.185.125.104 10.6.12.203     TCP      1050 80 → 49739 [PSH, ACK] Seq=8089 Ack=480 Win=6…       1050
 74774 762.742677700 10.6.12.203     205.185.125.104 TCP        54 49739 → 80 [ACK] Seq=480 Ack=6629 Win=65535 …         54
 74775 762.766881800 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=9085 Ack=480 Win=64240 …       1514
 74776 762.791122400 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=10545 Ack=480 Win=64240…       1514
 74777 762.804214000 205.185.125.104 10.6.12.203     TCP       818 80 → 49739 [PSH, ACK] Seq=12005 Ack=480 Win=…        818
 74778 762.805059700 10.6.12.203     205.185.125.104 TCP        54 49739 → 80 [ACK] Seq=480 Ack=12769 Win=65535…         54
 74779 762.829286500 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=12769 Ack=480 Win=64240…       1514
 74780 762.846096700 205.185.125.104 10.6.12.203     TCP      1050 80 → 49739 [PSH, ACK] Seq=14229 Ack=480 Win=…       1050
 74781 762.870312200 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=15225 Ack=480 Win=64240…       1514
 74782 762.894546600 205.185.125.104 10.6.12.203     TCP      1514 80 → 49739 [ACK] Seq=16685 Ack=480 Win=64240…       1514
```

```
Frame 75485: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0, id 0
Ethernet II, Src: Cisco_29:41:7d (ec:c8:82:29:41:7d), Dst: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
Internet Protocol Version 4, Src: 205.185.125.104, Dst: 10.6.12.203
Transmission Control Protocol, Src Port: 80, Dst Port: 49739, Seq: 542269, Ack: 480, Len: 1460
```

```
000  84 3a 4b 6d fc e2 ec c8  82 29 41 7d 08 00 45 00   ·:Km····  ·)A}··E·
010  05 dc 25 e9 00 00 80 06  ad 40 cd b9 7d 68 0a 06   ··%·····  ·@··}h··
020  0c cb 00 50 c2 4b 78 ab  95 e0 04 1f 40 3f 50 10   ···P·Kx·  ····@?P·
030  fa f0 79 5d 00 00 73 75  6d 65 54 68 72 65 61 64   ··y]··su meThread
040  00 00 d3 03 53 65 74 45  76 65 6e 74 00 00 b5 04   ····SetE vent····
050  6c 73 74 72 6c 65 6e 41  00 00 1a 03 4d 75 6c 74   lstrlenA ····Mult
060  69 42 79 74 65 54 6f 57  69 64 65 43 68 61 72 00   iByteToW ideChar·
```

Establishing an Unauthorized Active Directory Network

- Most commonly we see TCP followed by LDAP
- We can see that a bind request as root was sent to the Domain Controller



```
      Time           Source        Destination    Protocol    Length  Info
71260 745.032002… 10.6.12.157   10.6.12.12     TCP             66 49668 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
71261 745.033052… 10.6.12.12    10.6.12.157    TCP             66 389 → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
71262 745.033915… 10.6.12.157   10.6.12.12     TCP             54 49668 → 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
71263 745.040383… 10.6.12.157   10.6.12.12     LDAP           404 searchRequest(2) "<ROOT>" baseObject
71264 745.064620… 10.6.12.12    10.6.12.157    TCP           1514 389 → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a reassembled PDU
71265 745.086813… 10.6.12.12    10.6.12.157    LDAP          1386 searchResEntry(2) "<ROOT>"  | searchResDone(2) success  [1 result]
71266 745.087668… 10.6.12.157   10.6.12.12     TCP             54 49668 → 389 [ACK] Seq=351 Ack=2793 Win=2102272 Len=0
71569 746.281385… 10.6.12.157   10.6.12.12     TCP           1514 49668 → 389 [ACK] Seq=351 Ack=2793 Win=2102272 Len=1460 [TCP segment of a reassembled
71570 746.290402… 10.6.12.157   10.6.12.12     LDAP           563 bindRequest(4) "<ROOT>" sasl
71571 746.291251… 10.6.12.12    10.6.12.157    TCP             54 389 → 49668 [ACK] Seq=2793 Ack=2320 Win=2102272 Len=0
71572 746.295470… 10.6.12.12    10.6.12.157    LDAP           264 bindResponse(4) success
71573 746.297023… 10.6.12.157   10.6.12.12     LDAP            97 SASL GSS-API Integrity: unbindRequest(5)
71574 746.29788
```

Wireshark · Follow TCP Stream (tcp.stream eq 804) · mainnew.pcapng

```
dsServiceName..namingContexts..defaultNamingContext..schemaNamingContext..configurationNamingContext
..rootDomainNamingContext..supportedControl..supportedLDAPVersion..supportedLDAPPolicies..supportedS
ASLMechanisms..dnsHostName..ldapServiceName.
serverName..supportedCapabilities0...
....d...
...0...
.
0.......supportedCapabilities1.......1.2.840.113556.1.4.800..1.2.840.113556.1.4.1670..1.2.840.113556
.1.4.1791..1.2.840.113556.1.4.1935..1.2.840.113556.1.4.2080..1.2.840.113556.1.4.22370....{.
serverName1....i.gCN=FRANK-N-TED-DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=frank-n-ted,DC=com0....H..ldapServiceName1....1./frank-n-
ted.com:frank-n-ted-dc$@FRANK-N-TED.COM0....3..dnsHostName1........Frank-n-Ted-DC.frank-n-
```

The End