# Signature-based Detection

## Using Network Timing


Josh Pyorre, Nov, 2022

DEEPSEC


**Previously:**

zscaler

MANDIANT

NASA

# A few things first

I’m not a scientist

Also not a mathematician

More like an artist who likes to brute force through a problem using Python (Security Researcher)


DEEPSEC

| Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|
| 2022-11-09 15:38:57.233046 | 3.237.73.239 | 192.168.1.79 | TCP | 1506 | 443 → 57853 [ACK] Seq=161142 Ack=8959 Win=56704 Len=1440 TSval=34 |
| 2022-11-09 15:38:57.233047 | 3.237.73.239 | 192.168.1.79 | TCP | 1506 | 443 → 57853 [ACK] Seq=162582 Ack=8959 Win=56704 Len=1440 TSval=34 |
| 2022-11-09 15:38:57.233047 | 3.237.73.239 | 192.168.1.79 | TCP | 1506 | 443 → 57853 [ACK] Seq=164022 Ack=8959 Win=56704 Len=1440 TSval=34 |
| 2022-11-09 15:38:57.233048 | 3.237.73.239 | 192.168.1.79 | TCP | 1506 | 443 → 57853 [ACK] Seq=165462 Ack=8959 Win=56704 Len=1440 TSval=34 |
| 2022-11-09 15:38:57.233049 | 3.237.73.239 | 192.168.1.79 | TCP | 1506 | 443 → 57853 [ACK] Seq=166902 Ack=8959 Win=56704 Len=1440 TSval=34 |
| 2022-11-09 15:38:57.233102 | 192.168.1.79 | 3.237.73.239 | TCP | 66 | 57853 → 443 [ACK] Seq=8959 Ack=168342 Win=122432 Len=0 TSval=3629 |
| 2022-11-09 15:38:57.233118 | 192.168.1.79 | 3.237.73.239 | TCP | 66 | [TCP Window Update] 57853 → 443 [ACK] Seq=8959 Ack=168342 Win=131 |
| 2022-11-09 15:38:57.308865 | 3.237.73.239 | 192.168.1.79 | TCP | 1506 | 443 → 57853 [ACK] Seq=168342 Ack=8959 Win=56704 Len=1440 TSval=34 |
| 2022-11-09 15:38:57.308866 | 3.237.73.239 | 192.168.1.79 | TCP | 1506 | 443 → 57853 [ACK] Seq=169782 Ack=8959 Win=56704 Len=1440 TSval=34 |
| 2022-11-09 15:38:57.309201 | 192.168.1.79 | 3.237.73.239 | TCP | 66 | 57853 → 443 [ACK] Seq=8959 Ack=171222 Win=316800 Len=0 TSval=3629 |
| 2022-11-09 15:38:57.311057 | 3.237.73.239 | 192.168.1.79 | TLSv1… | 1207 | Application Data, Application Data |

**(Slide contains a video of streaming traffic)**

**Notes for the viewer: analyzing network traffic requires skills and can be prone to errors. It can also be tedious and time-consuming. If you're looking at your network traffic, it's difficult to find bad activity. However, we have tools to reduce that - IDS, various network analysis tools.**

```
byte
Src: SonyInte_6b:06:97 (00:e4:21:6b
ocol Version 4, Src: 192.168.1.9, D
Protocol, Src Port: 5353, Dst Port
ain Name System (response)
```

```
0010  00 68 97 4e 00 00 ff 11  81 89 c0 a8 01 09 e0 00   ·h·N···· ····· ·····
0020  00 fb 14 e9 14 e9 00 54  62 db 00 00 84 00 00 00   ·····T b·····
0030  00 01 00 00 00 00 09 5f  73 65 72 76 69 63 65 73   ·····_ services
0040  07 5f 64 6e 73 2d 73 64  04 5f 75 64 70 05 6c 6f   ·_dns-sd ·_udp·lo
0050  63 61 6c 00 00 0c 00 01  00 00 11 94 00 18 10 5f   cal····· ·····_
0060  73 70 6f 74 69 66 79 2d  63 6f 6e 6e 65 63 74 04   spotify- connect·
0070  5f 74 63 70 c0 23                                  _tcp·#
```

DEEPSEC

```
POST /wp-includes/fonts/Review/Home/ HTTP/1.1
jpeg, application/xaml+xml, application/x-ms-xbap, appl
application, application/vnd.ms-excel, application/msword, */*
Referer: http://triangularllc.com/wp-includes/fonts/Review/Home/
Accept-Language: en-us
Us
Co
Ac
Ho
Co
Connection: Keep-Alive
Cache-Control: no-cache

hidCflag=&Email=johnharmathon&Passwd=%2544q439%26%26&signIn=Sign+in&rmShown=1HTTP/1.1 200 OK
Date: Mon, 28 Sep 2015 17:38:32 GMT
Server: Apache/2.2.31 (Unix) mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited/1.4
X-Powered-By: PHP/5.4.45
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

**Notes for the viewer: How do you find the one bad thing in all that traffic?**

Notes for the viewer: Building context while leading into the topic. Let’s talk about Attribution

# Attribution

**Notes for the viewer:**
**If we see a suspicious URL in our network, what does it mean?**

URLhaus by ABUSE.ch

Browse API Feeds Statistics About

| | |
|---|---|
| **URL:** | http://www.angloextrema.com.br/assets/mQVRrHu7o0eJXxTFu/ |
| **URL Status:** | Online |
| **Host:** | www.angloextrema.com.br |
| **Date added:** | 2022-11-02 22:03:12 UTC |
| **Threat:** | Malware download |
| **Tags:** | dll emotet epoch4 heodo |

Emotet

Epoch4

HASH for the dropper

16
/ 71

?

Community Score

16 security vendors and no sandboxes flagged this file as malicious

87af3c9a35d995a70e8f771dd9f10111e7507535fcda3c44635c9007b0e21903

64bits assembly pedll

629.50 KB
Size

2022-11-02 22:26:30 UTC
10 minutes ago

DLL

DETECTION DETAILS RELATIONS CONTENT TELEMETRY COMMUNITY

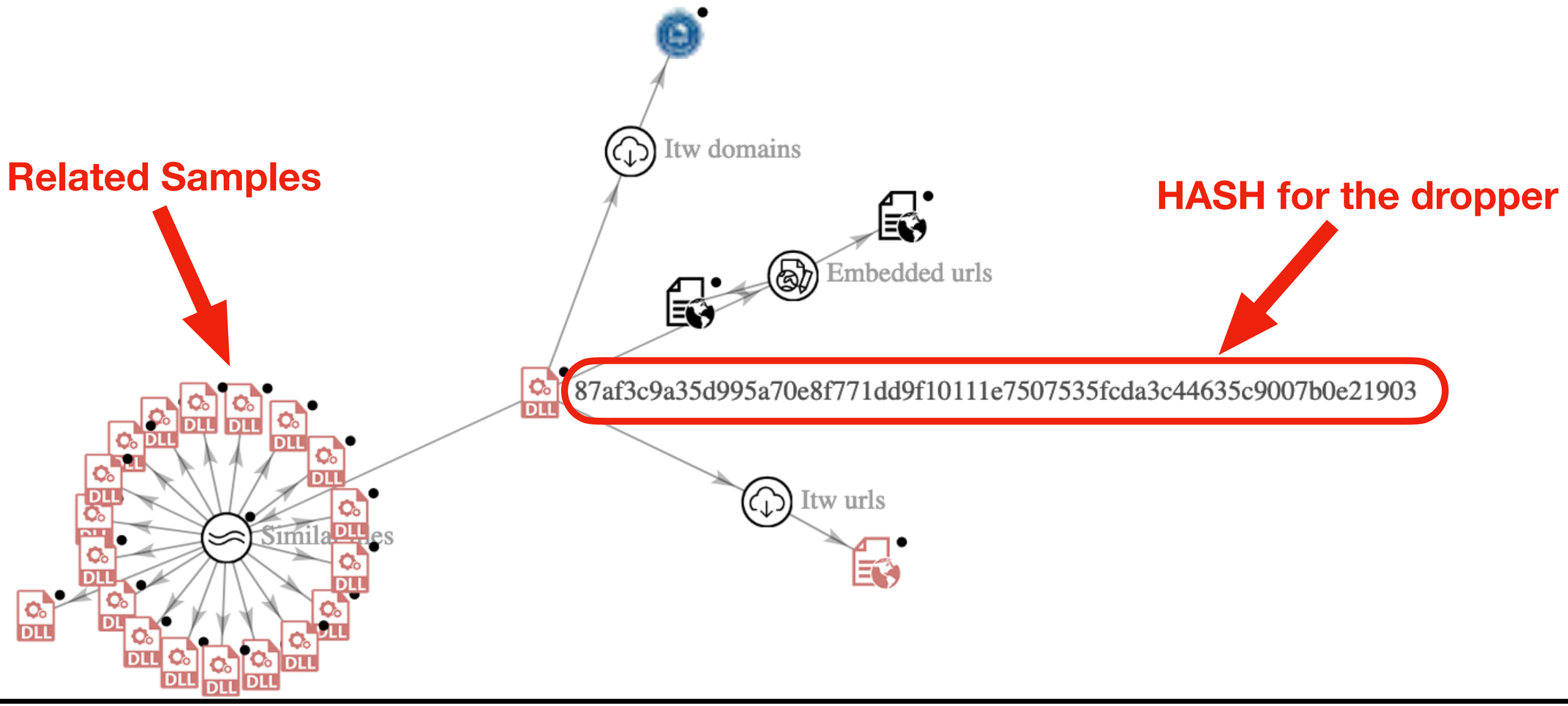
ITW Urls (1)

| Scanned | Detections | Status | URL |
|---|---|---|---|
| 2022-11-02 | 5 / 90 | 200 | http://www.angloextrema.com.br/assets/mQVRrHu7o0eJXxTFu/ |

URL

Notes for the viewer:
When that URL leads to a suspicious file, what is that file?

DEEPS




**Notes for the viewer:**
**We can look at the file and find relationships with other similar files**

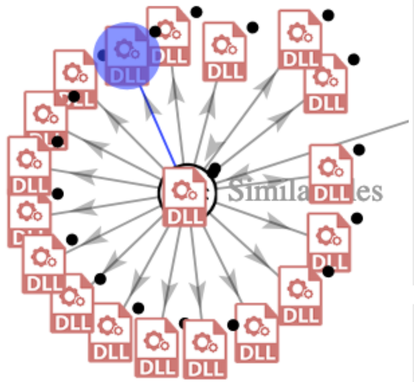
## Basic Properties

| | |
|---|---|
| Type | Win32 DLL |
| Size | 629.50 kB |
| First Seen | 2022-11-02 22:22:52 |
| Last Seen | 2022-11-02 22:22:52 |
| Submissions | 1 |
| File Name | payload_1.bin |

## Relations

| | |
|---|---|
| Embedded urls | 2 |
| Similar files | 168 |

Expand using new intelligence search



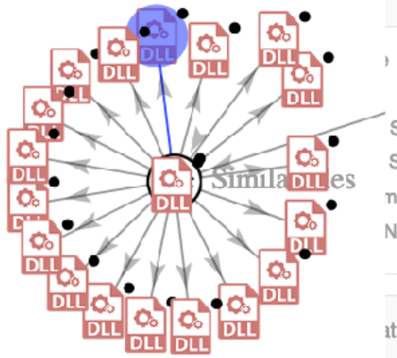

## Basic Properties

| | |
|---|---|
| Type | Win32 DLL |
| Size | 629.50 kB |
| First Seen | 2022-11-02 22:25:08 |
| Last Seen | 2022-11-02 22:25:08 |
| Submissions | 1 |
| File Name | 5728b804df714f928d30432a571830ba.virus |

## Relations

| | |
|---|---|
| Embedded urls | 2 |
| Similar files | 168 |

Expand using new intelligence search




## Basic Properties

| | |
|---|---|
| Type | Win32 DLL |
| Size | 629.50 kB |
| First Seen | 2022-11-02 22:10:27 |
| Last Seen | 2022-11-02 22:10:27 |
| Submissions | 1 |
| File Name | payload_1.bin |

## Relations

| | |
|---|---|
| Embedded urls | 2 |
| Similar files | 168 |

Expand using new intelligence search

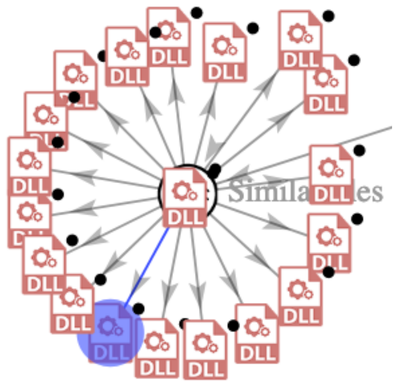
## Basic Properties

| | |
|---|---|
| Type | Win32 DLL |
| Size | 629.50 kB |
| First Seen | 2022-11-02 22:25:11 |
| Last Seen | 2022-11-02 22:25:11 |
| Submissions | 1 |
| File Name | 49d1ac29fa559b4b9c6a54c700beaba9.virus |

## Relations

| | |
|---|---|
| Embedded urls | 2 |
| Similar files | 168 |

Expand using new intelligence search



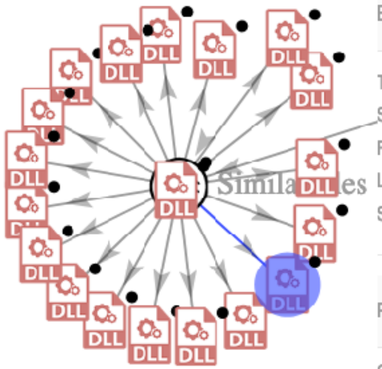

## Basic Properties

| | |
|---|---|
| Type | Win32 DLL |
| Size | 629.50 kB |
| First Seen | 2022-11-02 22:26:30 |
| Last Seen | 2022-11-02 22:26:30 |
| Submissions | 1 |

## Relations

| | |
|---|---|
| Embedded urls | 2 |
| Itw domains | 1 |
| Itw urls | 1 |
| Similar files | 168 |

Expand using new intelligence search



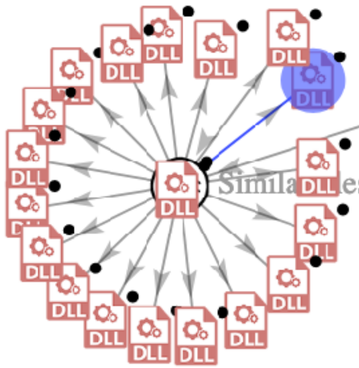

## Basic Properties

| | |
|---|---|
| Type | Win32 DLL |
| Size | 629.50 kB |
| First Seen | 2022-11-02 22:13:50 |
| Last Seen | 2022-11-02 22:13:50 |
| Submissions | 1 |

## Relations

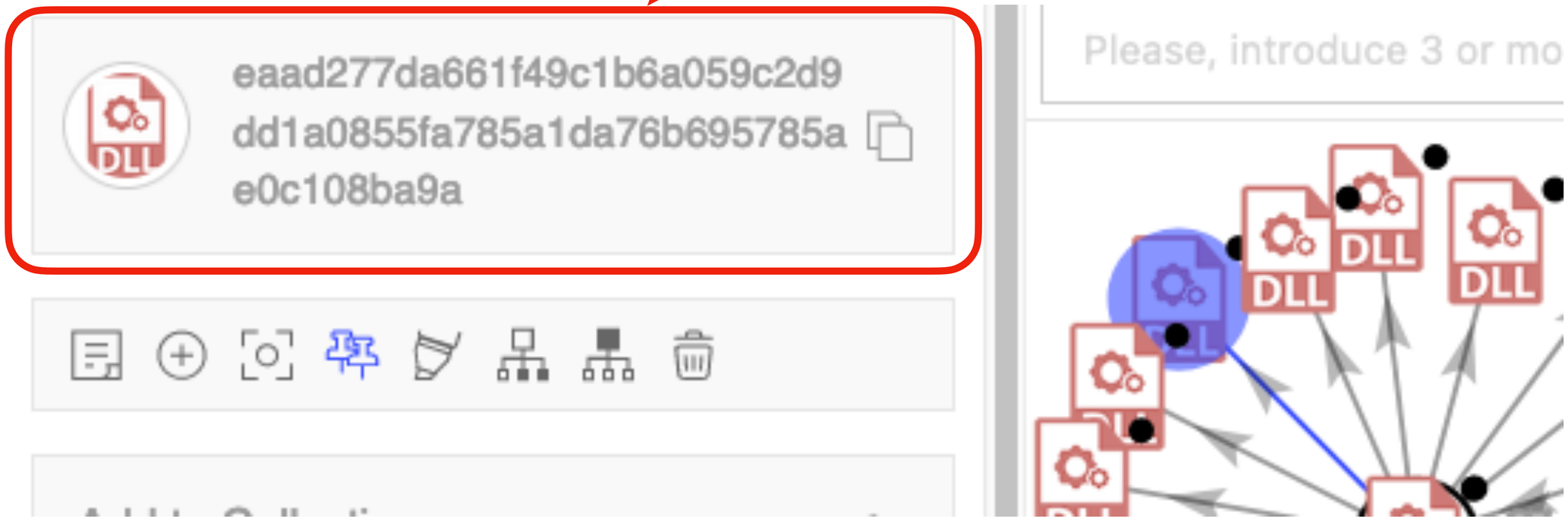
| | |
|---|---|
| Collections | 1 |
| Embedded urls | 2 |
| Similar files | 168 |

Expand using new intelligence search



**Notes for the viewer:**
**We can look at the file and find relationships with other similar files**

Copy the HASH for one of the files




**Notes for the viewer:**
**We can continue looking using various third party tools to find other relationships, attributing to a campaign**

## Associated Artifacts

The following artifacts may have been incomplete or missing information about behavioral indicators and network connections.

| SHA256 Signature | Magic Type | AV Result |
|---|---|---|
| b5a9530302ceab6a1193dcda7a6b68e9e32ae90513285b38... | PE32+ executable (GUI) x86-64 | |
| ac3f645023b0a826a8dfdf01610cc9ebd6dfcec6a06ba8f3151... | MS Windows Vista Event Log | |
| bbb7404419f91f82cedfec915931a9339f04165b27d8878d63... | PE32+ executable (GUI) x86-64 | |
| 9b7ac0309609983d0cc06a7d4872d68f0c33d865b4abf8e29... | data | |
| 9117986e2928133190cbaa2ab698d6280ff9bffd0e17e43ca7... | PE32+ executable (GUI) x86-64 | |
| 3b633bb92eb56e06c8d60d8f6328aa835be63a5a8e1abf2d3... | MS Windows Vista Event Log | |
| b0bc89e94585c3bf6e1123ac27c4e66c04f6400487b3fe57d9... | data | |
| d03e31bf532aadfa780081cd2f387ac2519543379de231b5d... | MS Windows Vista Event Log | |
| cda618f08b4bf7099206ff6cc85156a69e2744c1bb7157c798... | MS Windows Vista Event Log | |

1 - 9 of 9

**Notes for the viewer:**
**We can continue looking using various third party tools to find other relationships, attributing to a campaign**

DEEPSEC

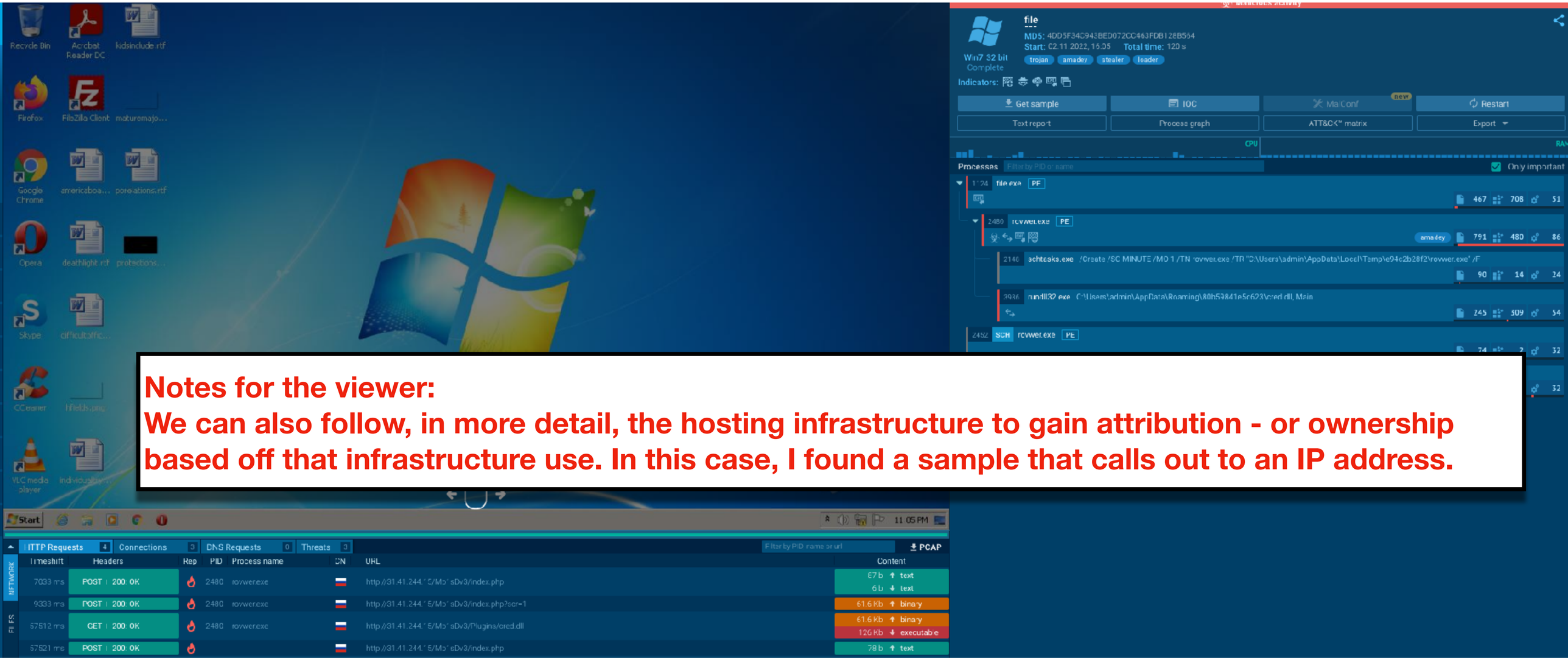
# Compromised websites

http://www.angloextrema.com.br/assets/mQVRrHu7o0eJXxTFu/

http://alvaovillagecamping.pt/wp-content/Ra9iwOPb6uLf/

| | | | |
|---|---|---|---|
| 2022-11-02 22:03:11 | http://alvaovillagecamping.pt/wp-content/Ra9iwOPb6uLf/ | Online | dll emotet epoch4 heodo |
| 2022-11-02 21:51:07 | http://wordpress.xinmoshiwang.com/list/cRIH9Bd/ | Online | dll emotet epoch5 heodo |
| 2022-11-02 21:50:20 | http://ruitaiwz.com/wp-admin/sV1NeVxLDiHJ1xm/ | Online | dll emotet epoch5 heodo |
| 2022-11-02 21:50:15 | http://voinet.ca/cgi-bin/RXDWHpi8dHHZf8/ | Offline | dll emotet epoch5 heodo |
| 2022-11-02 21:50:15 | http://cultura.educad.pe/wp-content/A86I7QxwuEZV/ | Online | dll emotet epoch5 heodo |
| 2022-11-02 17:35:41 | https://atlantia.sca.org/php_fragments/D8Nwm2F80BL4s/ | Offline | dll emotet epoch4 heodo |
| 2022-11-02 17:35:13 | https://amorecuidados.com.br/wp-admin/t3D/ | Offline | dll emotet epoch4 heodo |
| 2022-11-02 17:35:13 | http://thuybaohuy.com/wp-content/u3MJwXSP9tmiaTCyZD/ | Online | dll emotet epoch4 heodo |
| 2022-11-02 09:53:06 | http://sat7ate.com/wordpress/ZAf5j4MG8Hwnig/ | Online | dll emotet epoch5 heodo |

**Notes for the viewer:**
**We can continue looking using various third party tools to find other relationships (URLs in this case), attributing to a campaign**




**Notes for the viewer:**
**We can also follow, in more detail, the hosting infrastructure to gain attribution - or ownership based off that infrastructure use. In this case, I found a sample that calls out to an IP address.**

**Notes for the viewer:**
**We can also follow, in more detail, the hosting infrastructure to gain attribution - or ownership based off that infrastructure use. In this case, I found a sample that calls out to an IP address.**

http://31.41.244.15/Mb1sDv3/index.php

http://31.41.244.15/Mb1sDv3/index.php?scr=1

http://31.41.244.15/Mb1sDv3/Plugins/cred.dll

http://31.41.244.15/Mb1sDv3/index.php

31.41.244.15 INVESTIGATE BACK TO TOP

DNS Resolution | Autonomous Systems | Associated Samples | Recent Detections

| Threat Score | SHA256 Signature | AV Result | File Type | First Seen |
|---|---|---|---|---|
| 95 | 18dc2f794315142579f1e66b13dea4e23ff1c515892b8d079b... | malicious, (RDML:ZHvxJU985AcNY... gen,(high,[Trj],win /malicious_confidence_1... Downloader.Win32.Deym... [Trj],ML.Attribute.HighCon... gen,Trojan.Malware.3009... /GenKryptik.ETEM!tr,Dete... /Kryptik.HUW.gen!Eldorad... Downloader.Win32.Deym... /PE-A,Trojan.Win32.Save.a,Su... (W),Generic.Malware,W3... (score:,Trojan.MalPack.G... | PE32 executable (GUI) Intel 80386 | 11/02/2022 |
| 95 | cb31e10b9290209208fe012f4e3e48348efbe31f9e46c4b073... | [Trj], suspicious,Trojan.Malwar... QV,PWSX-gen,W32 /Kryptik.HWT.gen!Eldorad... Cryptor.2LA.gen,Static,Tr... /Sabsik.FL.B!ml, (W),Generic.Malware,W3... (score:,Mal/Generic-S,Trojan.MalPack.GS,Mali... /GenKryptik.FBYO!tr,malic... | PE32 executable (GUI) Intel 80386 | 11/02/2022 |
| | | Generic.Malware,W32.AI... (score:,Trojan.MalPack.G... 9976466,confidence),mal... (high,[Trj],win /malicious_confidence_1... gen,AI,100),Malicious,VH... | | |

**Notes for the viewer:**
**We can then look at that IP using third party services or other intelligence to find additional relationships.**

DEEPSEC

18dc2f794315142579f1e66b13dea4e23ff1c515892b8d079b149dca9db0b625

INVESTIGATE

BACK TO TOP

| Destination | URLs | Security Categories |
|---|---|---|
| 31.41.244.15 | 3 | |
| Destination<br>http://31.41.244.15/Mb1sDv3/Plugins/cred64.dll<br>http://31.41.244.15/Mb1sDv3/index.php<br>http://31.41.244.15/Mb1sDv3/index.php?scr=1 | | |

1 - 1 of 1

cb31e10b9290209208fe012f4e3e48348efbe31f9e46c4b0739e4b92af2ea206

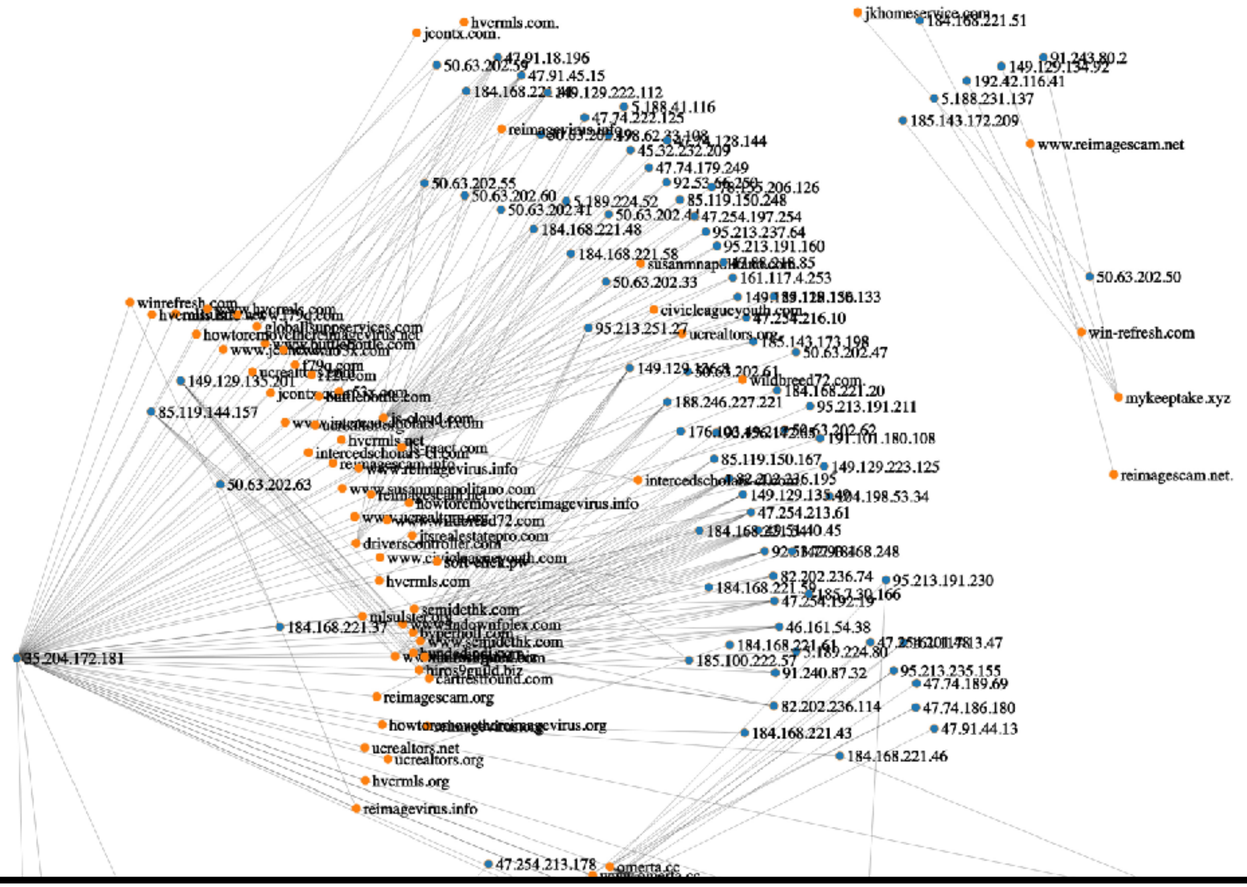
INVESTIGATE

BACK TO TOP

## Network Connections

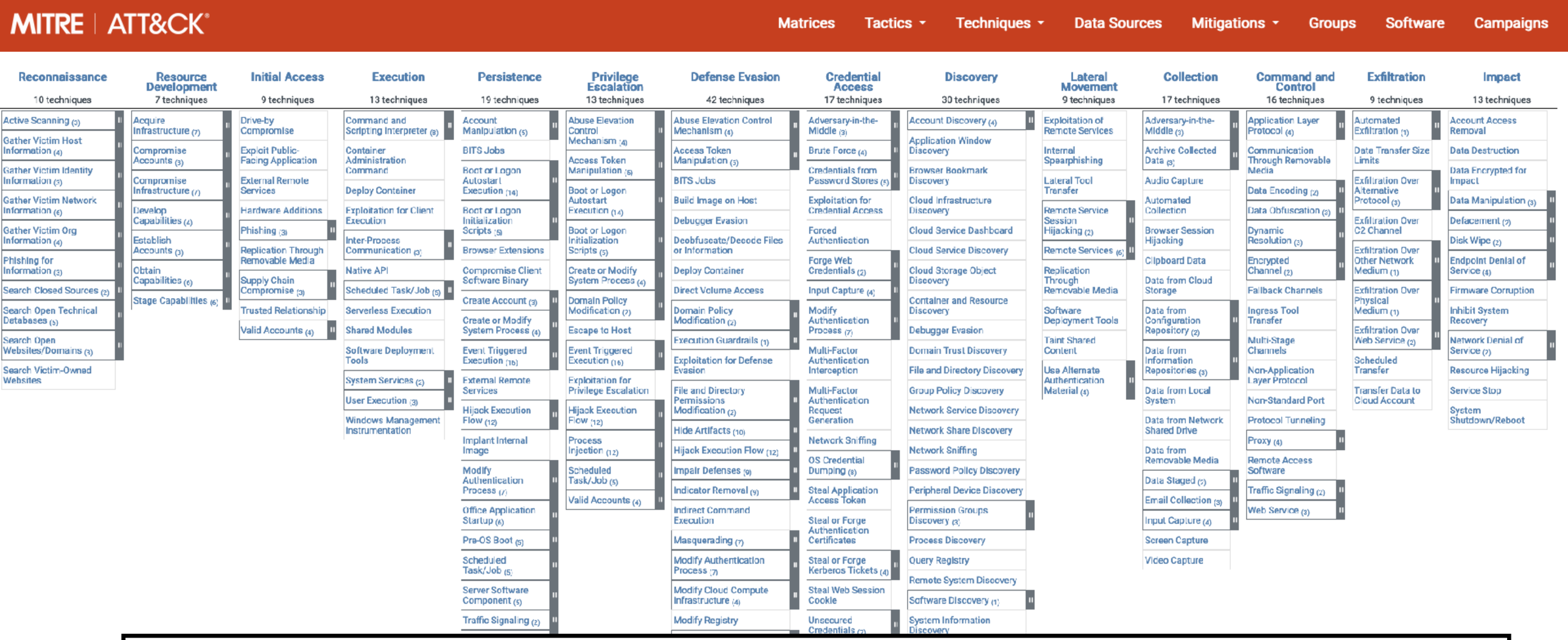
| Destination | URLs | Security Categories |
|---|---|---|
| 31.41.244.15 | 3 | |
| Destination<br>http://31.41.244.15/Mb1sDv3/Plugins/cred64.dll<br>http://31.41.244.15/Mb1sDv3/index.php<br>http://31.41.244.15/Mb1sDv3/index.php?scr=1 | | |

**Notes for the viewer:**
**We can then look at that IP using third party services or other intelligence to find additional relationships.**




**Notes for the viewer:**
**And we can map those relationships if needed to get an even clearer picture of attribution.**

DEEPSEC




**Notes for the viewer:**
**The MITRE ATT&CK Framework is a well-known method of tracking attribution across multiple levels of a malware or attack campaign.**

# APT29

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).[1][2] They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.[3][4][5][6]

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.[7][8] Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.[9][10][11][12][13]

ID: G0016

Associated Groups: IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Contributors: Daniyal Naeem, BT Security; Matt Brenton, Zurich Insurance Group; Katie Nickels, Red Canary

Version: 3.1

Created: 31 May 2017

Last Modified: 11 July 2022

Version Permalink

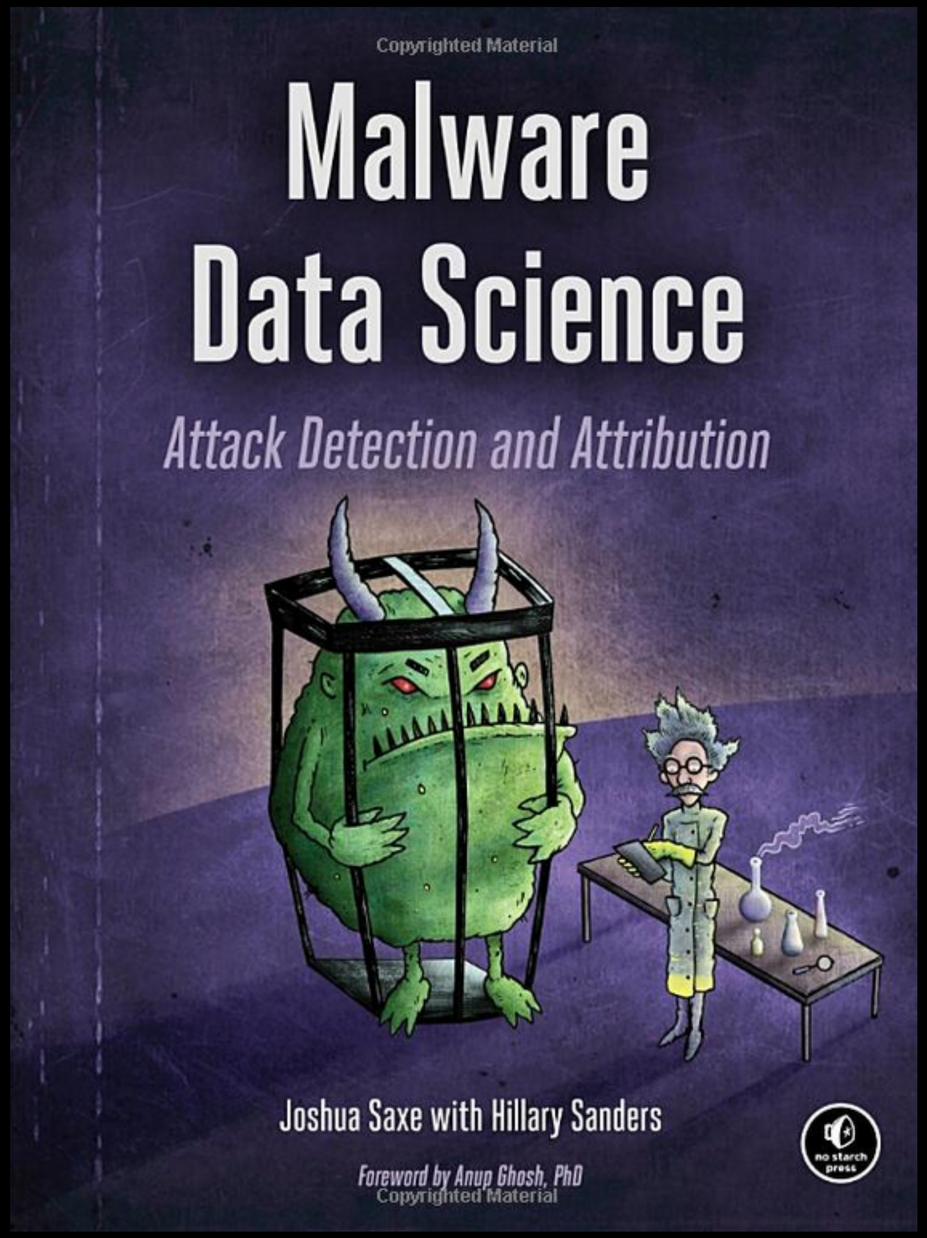
**Notes for the viewer:**
**The MITRE ATT&CK Framework can be used to trace tactics and techniques to various known threat actors.**

## Techniques Used

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1548 | .002 | Abuse Elevation Control Mechanism: Bypass User Account Control | APT29 has bypassed UAC.[24] |
| Enterprise | T1087 | | Account Discovery | APT29 obtained a list of users and their roles from an Exchange server using `Get-ManagementRoleAssignment`.[12] |
| | | .002 | Domain Account | APT29 has used PowerShell to discover domain accounts by executing `Get-ADUser` and `Get-DGroupMember`.[17][14] |
| | | .004 | Cloud Account | APT29 has conducted enumeration of Azure AD accounts.[25] |
| Enterprise | T1098 | .001 | Account Manipulation: Additional Cloud Credentials | APT29 has added credentials to OAuth Applications and Service Principals.[26][17] |
| | | .002 | Account Manipulation: Additional Email Delegate Permissions | APT29 added their own devices as allowed IDs for active sync using `Set-CASMailbox`, allowing it to obtain copies of additional permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals.[12] |
| | | .003 | Account Manipulation: Additional Cloud Roles | APT29 has granted `company administrator` privileges to a newly created service principal.[17] |
| | | .005 | Account Manipulation: Device Registration | APT29 registered devices in order to enable mailbox syncing via the `Set-CASMailbox` command.[12] |
| Enterprise | T1583 | .001 | Acquire Infrastructure: Domains | APT29 has acquired C2 domains, sometimes through resellers.[10][27][18] |
| | | .006 | Acquire Infrastructure: Web Services | APT29 has registered algorithmically generated Twitter handles that are used for C2 by malware, such as HAMMERT |
| | | | Registry Run Keys / Startup Folder | |

**Notes for the viewer:**
**The MITRE ATT&CK Framework can be used to trace tactics and techniques to various known threat actors.**

There are books about doing this kind of thing



# Levels of Attribution

Threat Actors

APT Groups

Individuals

governments

Etc…

Campaigns

Malware

Ransom

Spam

Extortion

State

Financial

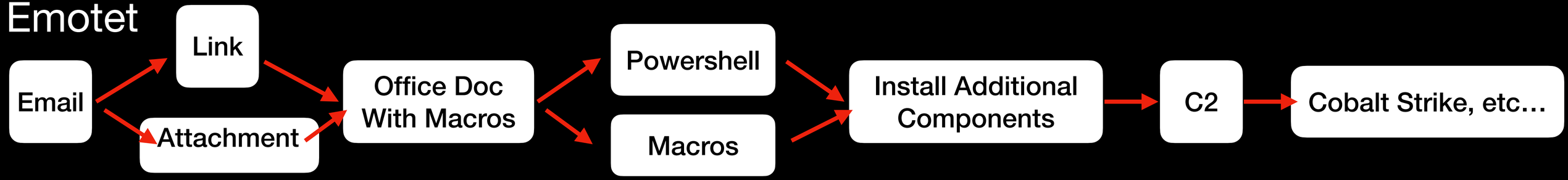
**Notes for the viewer:**
**Attribution is up to you. Are you interested in what group is targeting your network? Or maybe you just want to know if that URL is related to some malware family. Or maybe you simply want to know what is happening in your network and that's enough.**

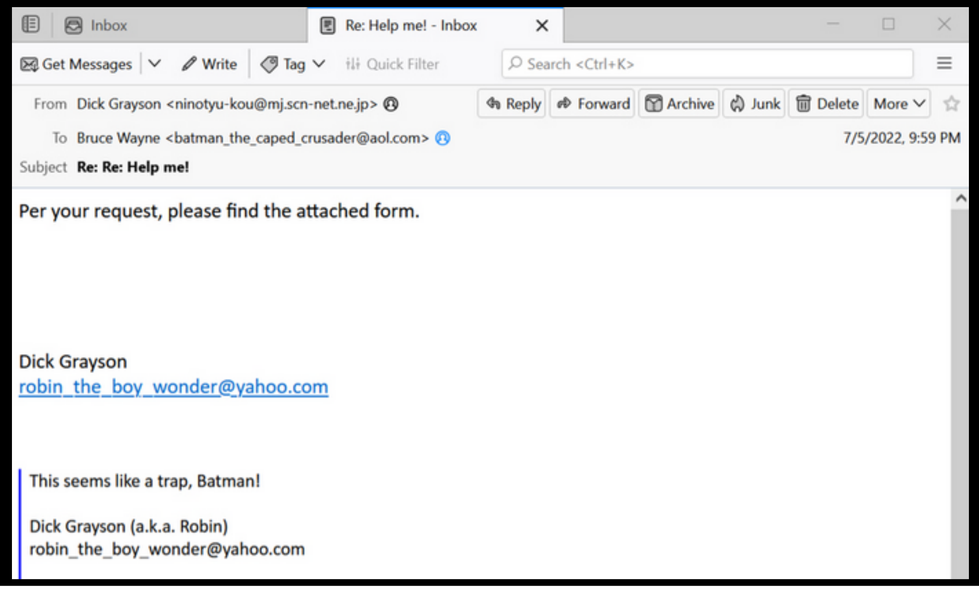
…Or just what's in your network

**Notes for the viewer:**
**A quick summary of the common path of infection on a system, before we get into a bunch of PCAP analysis.**

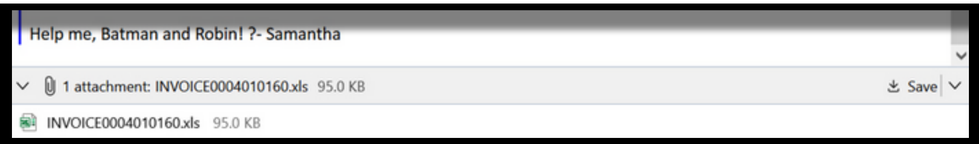
# The Infection Chain

# Emotet



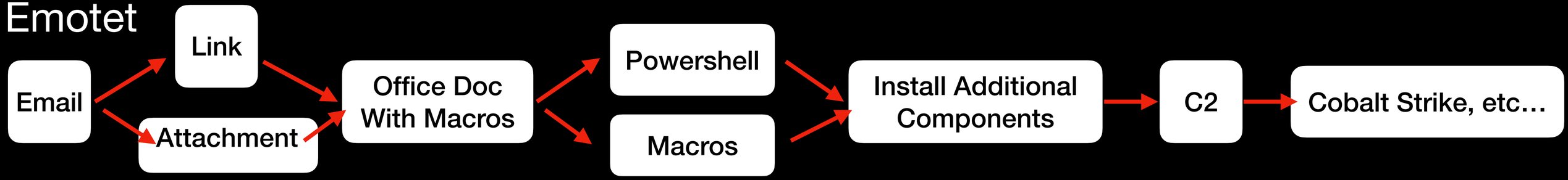

**Notes for the viewer:**
**Using Emotet as an example: Comes in as email, leading to a URL to download additional components, and typically ending up in Cobalt Strike and Ransomware infection.**

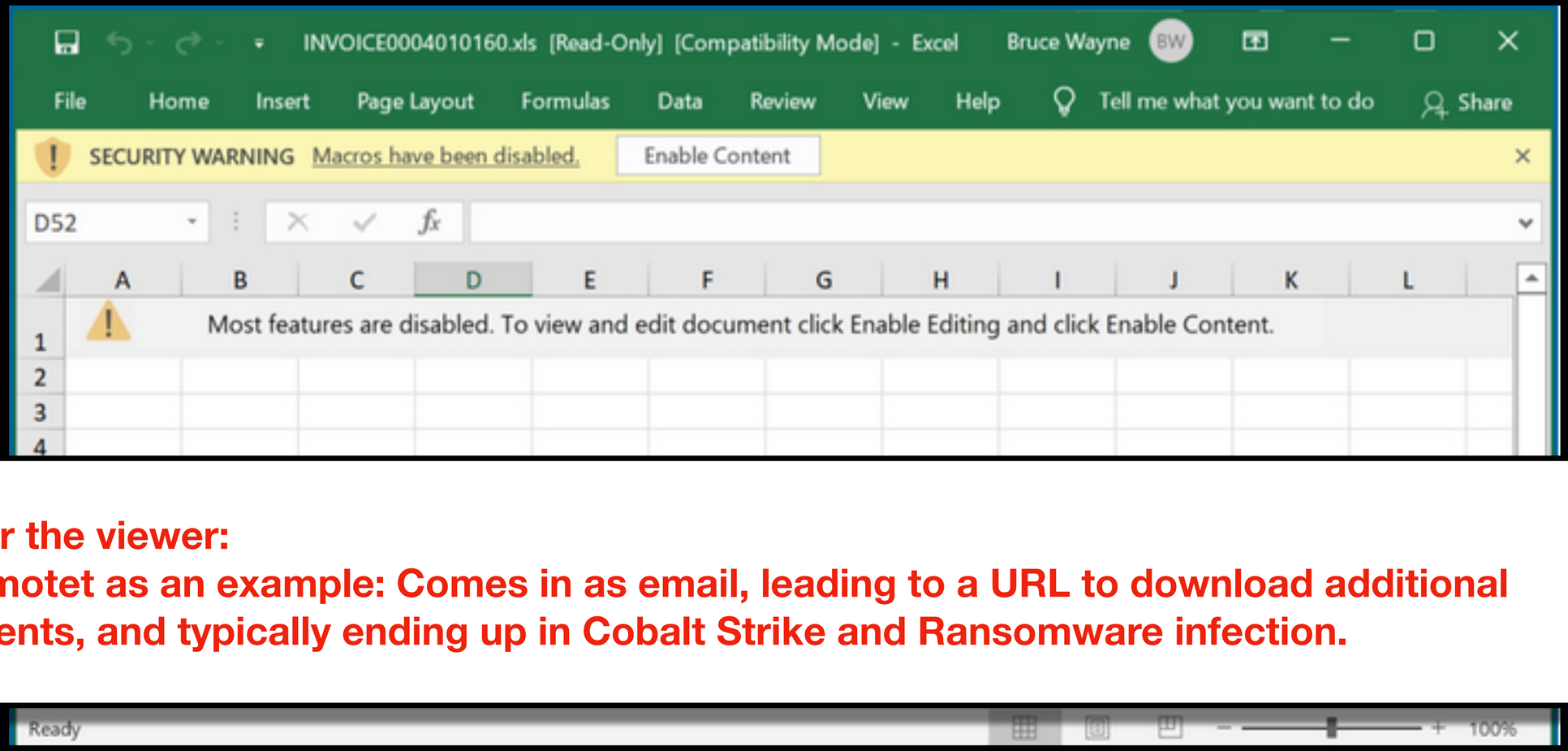



DEEPSEC

Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/

# Emotet



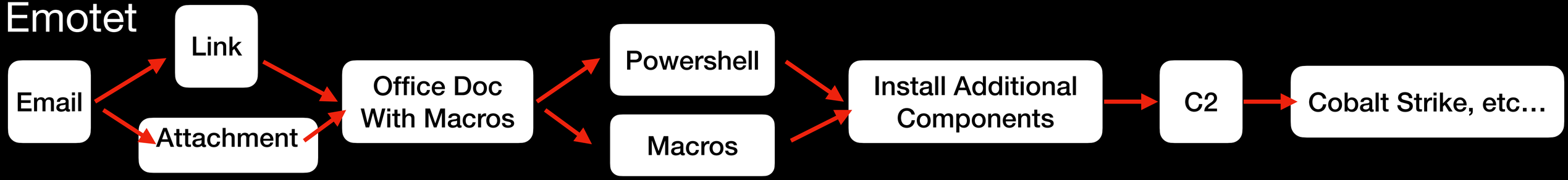



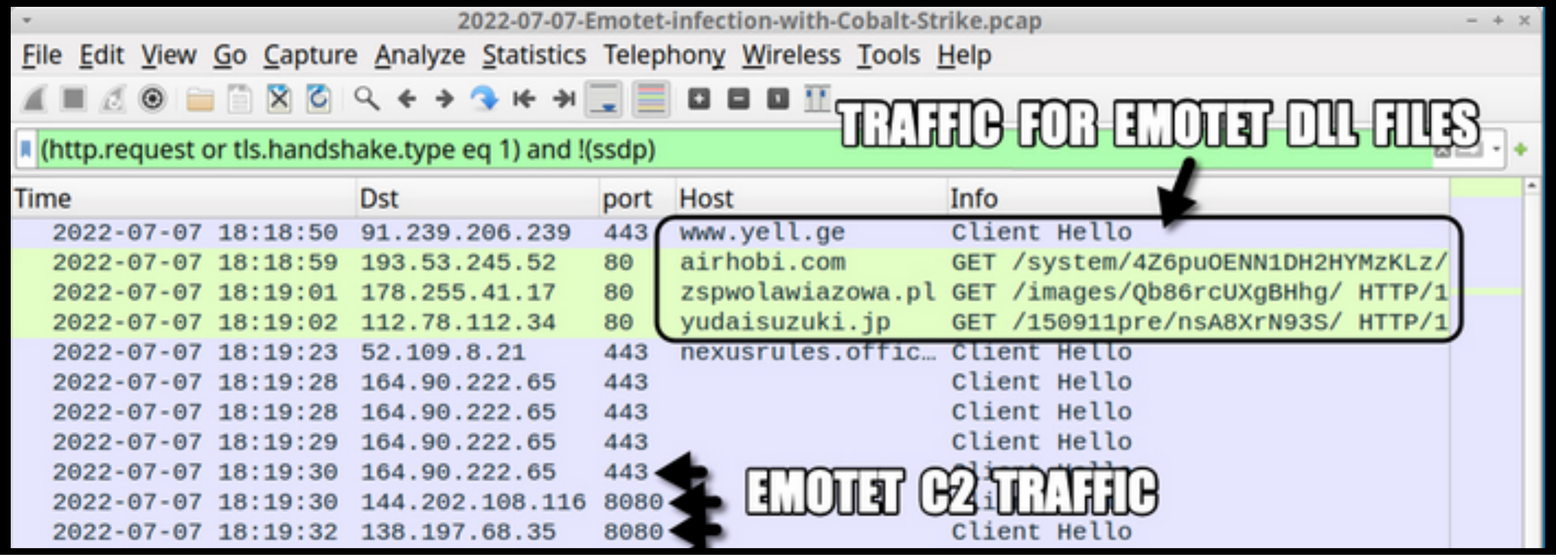

**Notes for the viewer:**
**Using Emotet as an example: Comes in as email, leading to a URL to download additional components, and typically ending up in Cobalt Strike and Ransomware infection.**

DEEPSEC

Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/

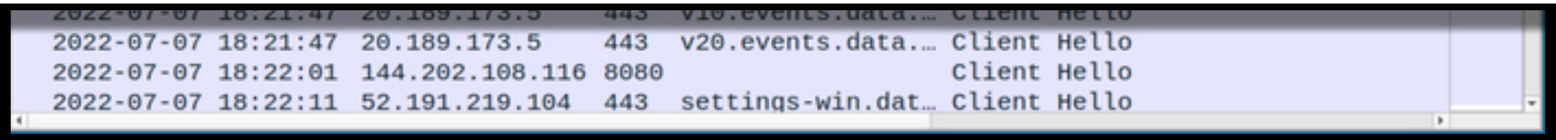
# Emotet




| Time | Dst | port | Host | Info |
|---|---|---|---|---|
| 2022-07-07 18:18:50 | 91.239.206.239 | 443 | www.yell.ge | Client Hello |
| 2022-07-07 18:18:59 | 193.53.245.52 | 80 | airhobi.com | GET /system/4Z6puOENN1DH2HYMzKLz/ |
| 2022-07-07 18:19:01 | 178.255.41.17 | 80 | zspwolawiazowa.pl | GET /images/Qb86rcUXgBHhg/ HTTP/1 |
| 2022-07-07 18:19:02 | 112.78.112.34 | 80 | yudaisuzuki.jp | GET /150911pre/nsA8XrN93S/ HTTP/1 |
| 2022-07-07 18:19:23 | 52.109.8.21 | 443 | nexusrules.offic… | Client Hello |
| 2022-07-07 18:19:28 | 164.90.222.65 | 443 | | Client Hello |
| 2022-07-07 18:19:28 | 164.90.222.65 | 443 | | Client Hello |
| 2022-07-07 18:19:29 | 164.90.222.65 | 443 | | Client Hello |
| 2022-07-07 18:19:30 | 164.90.222.65 | 443 | | |
| 2022-07-07 18:19:30 | 144.202.108.116 | 8080 | | |
| 2022-07-07 18:19:32 | 138.197.68.35 | 8080 | | Client Hello |

**Notes for the viewer:**
**Once traffic starts, you typically see a second-stage download over HTTP (although it might be over SSL), and then C2 communication over SSL**

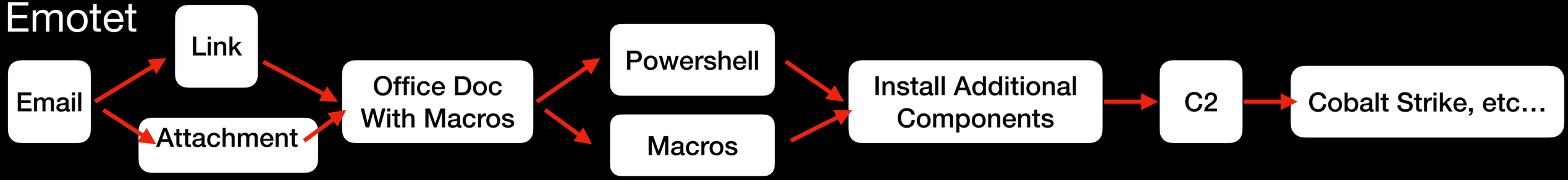


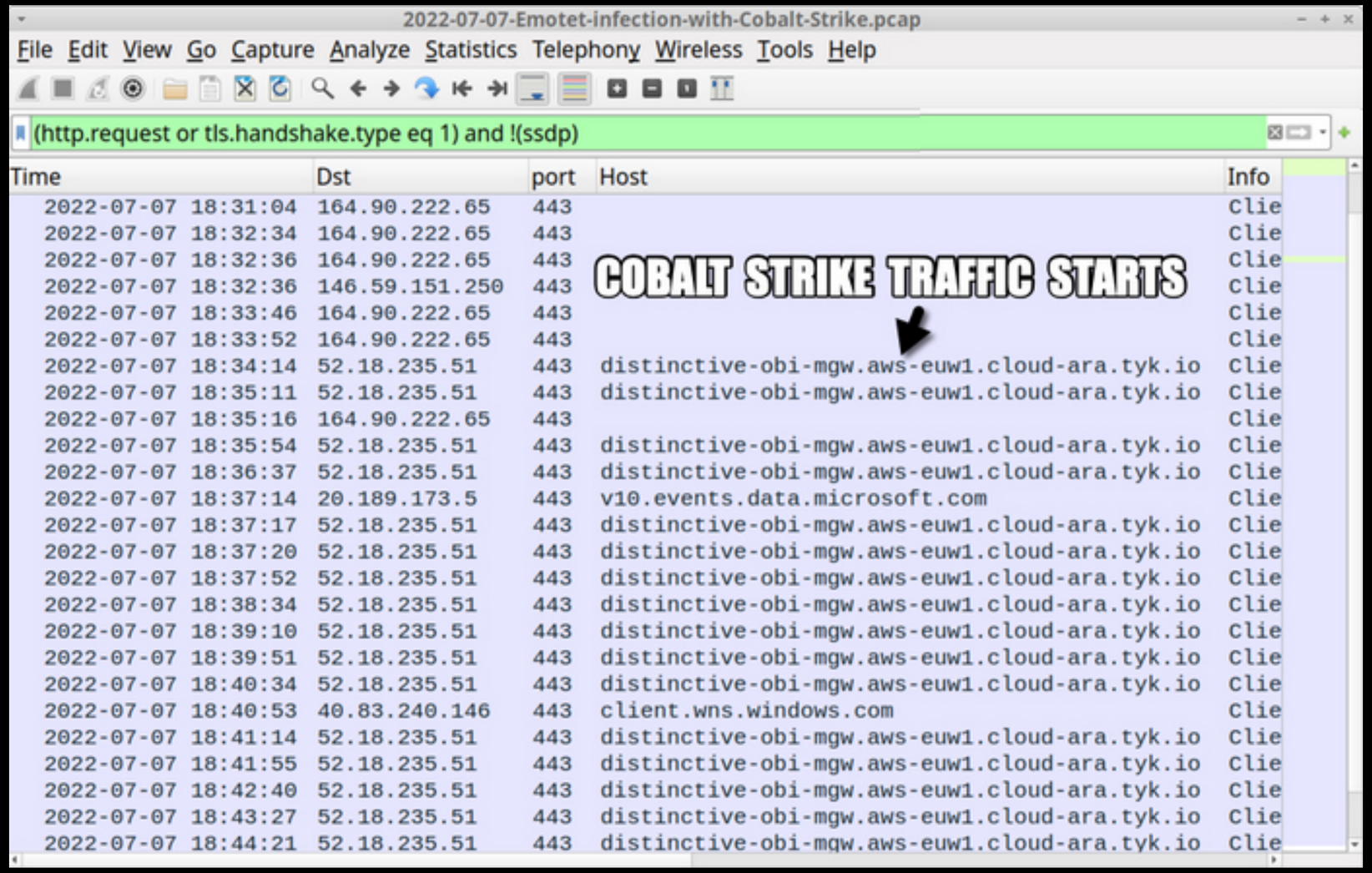
| | | | | |
|---|---|---|---|---|
| 2022-07-07 18:21:47 | 20.189.173.5 | 443 | v20.events.data.… | Client Hello |
| 2022-07-07 18:22:01 | 144.202.108.116 | 8080 | | Client Hello |
| 2022-07-07 18:22:11 | 52.191.219.104 | 443 | settings-win.dat… | Client Hello |

DEEPSEC

Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/

# Emotet




| Time | Dst | port | Host | Info |
|---|---|---|---|---|
| 2022-07-07 18:31:04 | 164.90.222.65 | 443 | | Clie |
| 2022-07-07 18:32:34 | 164.90.222.65 | 443 | | Clie |
| 2022-07-07 18:32:36 | 164.90.222.65 | 443 | | Clie |
| 2022-07-07 18:32:36 | 146.59.151.250 | 443 | | Clie |
| 2022-07-07 18:33:46 | 164.90.222.65 | 443 | | Clie |
| 2022-07-07 18:33:52 | 164.90.222.65 | 443 | | Clie |
| 2022-07-07 18:34:14 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:35:11 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:35:16 | 164.90.222.65 | 443 | | Clie |
| 2022-07-07 18:35:54 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:36:37 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:37:14 | 20.189.173.5 | 443 | v10.events.data.microsoft.com | Clie |
| 2022-07-07 18:37:17 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:37:20 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:37:52 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:38:34 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:39:10 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:39:51 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:40:34 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:40:53 | 40.83.240.146 | 443 | client.wns.windows.com | Clie |
| 2022-07-07 18:41:14 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:41:55 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:42:40 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:43:27 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |
| 2022-07-07 18:44:21 | 52.18.235.51 | 443 | distinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io | Clie |

DEEPSEC

Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/

# Common Signature Detection Methods

**Notes for the viewer:**
**Let’s cover the most common signature-based detection methods**

# IDS Rules

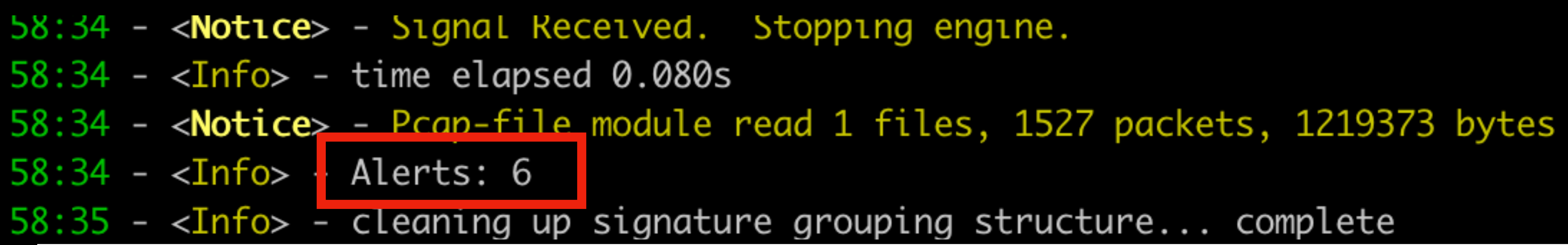
josh@research: ~ (ssh)

josh@ids: ~ (ssh)

```
josh@ids:~$ sudo suricata -c /etc/suricata/suricata.yaml -r ~/2020-09-30-Emotet-infection-with-Trickbot_POST.pcap  -v
```

**This is a video showing:**
**A PCAP file is replayed through Suricata IDS. The PCAP contains network traffic associated with Emotet C2 traffic. The video shows an IDS rule catching the C2 activity.**

DEEPSEC



```
58:34 - <Notice> - Signal Received.  Stopping engine.
58:34 - <Info> - time elapsed 0.080s
58:34 - <Notice> - Pcap-file module read 1 files, 1527 packets, 1219373 bytes
58:34 - <Info> - Alerts: 6
58:35 - <Info> - cleaning up signature grouping structure... complete
```

**Notes for the Viewer:**
**Here is a close up of Suricata running and catching the C2 activity.**

```
09/30/                                                                                                                 y: 1]
{TCP}
09/30/2020-16:50:21.950965  [**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 10.9.30.101:64263 -> 80.87.201.221:7080
09/30/2020-16:50:25.861050  [**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 10.9.30.101:64263 -> 80.87.201.221:7080
09/30/2020-16:50:28.057649  [**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 10.9.30.101:64263 -> 80.87.201.221:7080
09/30/2020-16:50:29.657596  [**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 10.9.30.101:64263 -> 80.87.201.221:7080
09/30/2020-16:50:34.181486  [**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priority: 1]
{TCP} 10.9.30.101:64263 -> 80.87.201.221:7080
```

```
alert http $HOME_NET any -> $EXTERNAL_NET [7080,8080,443,80,4143,995,21,50000,20,8090,8443,990,22]
(msg:"ET MALWARE Win32/Emotet CnC Activity (POST) M10";
flow:established,to_server; content:"POST"; http.uri; content:!"."; content:!"&"; content:!"-";
http.user_agent; content:"Mozilla/5.0 (Windows NT 6.";
startswith; content:"|3b 20|"; distance:1; within:2;
http.request_body; content:!".zip"; content:!".png"; content:!".jp"; content:!".exe";
content:"--|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|";
fast_pattern; http.content_len; byte_test:0,<,8000,0,string,dec; byte_test:0,>,500,0,string,dec;
http.header_names; content:"|0d 0a|User-Agent|0d 0a|Accept|0d 0a|Accept-Language|0d 0a|Accept-Encoding|0d 0a|"; startswith; content:"Referer|0d 0a|"; distance:0;
reference:md5,ba2e4a231652f8a492feb937b1e96e71; classtype:trojan-activity; sid:2030868; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_09_14, deployment Perimeter, signature_severity Major
2020_09_14;)
```

ne 9, Column 1 Tab Size: 4

**Notes for the Viewer:**
**The top text is the rule that captured the C2 activity, and the bottom is the PCAP.**

```
17
18
19
20
21
22
23
24
25
26  2020-09-30 09:50:17.953918  10.9.30.101
27  2020-09-30 09:50:17.954608  trafcj.fvds.r
28  2020-09-30 09:50:17.954734  10.9.30.101
29  2020-09-30 09:50:17.958959  trafcj.fvds.r
```

```
Frame 8: 478 bytes on wire (3824 bits), 478 by
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:
Internet Protocol Version 4, Src: 10.9.30.101
Transmission Control Protocol, Src Port: 64263
[5 Reassembled TCP Segments (5457 bytes): #3(6
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: mult
```

```
Host: 80.87.201.221:7080
Content-Length: 4804
Cache-Control: no-cache


--------------------UZ9rmC1SsoZVjPcS5Vu
Content-Disposition: form-data; name="emdseqxxlbwpxzof"; filename="rhyjvabjbzq"
Content-Type: application/octet-stream

?.V..P.we.0.t...n..)y....... ..0c.
.`.._..`.=$x.........x..V+....&F.%....{.3<..*...5oOx... S,..[..|9..&.          ...i....a.....
5.a..r.........."$,....y...a:k.i<....N..!..V...........C....eB.....C.E......{.8..=._*0.........,..XT...?dz...z(}
~...q.Ns.,.Q.i+....|...ti...J..E.v...&5...L|.]+.#..5..B.mQJC..9v.E.7....y.[.$'
/y.Mp..FHF.5.%........%
...V(.J.....9.Q*c...C`....0.....l...Z.&.S...3.....;......V+x.R..
.......%v.L@..L.{Z.......././/..f.k.1...2..!...q.0v....(g....n..90R,CV|..7.+T.R..a=."..\..T,;......
2....*g.&...W.....d..CH.)..w:%...bjE.b..
z.q\.ao.`...%z..c{...C........W.....~IdC.},.[...Q.9......$%.......p.....3'....P.+.3...f..b..\<..?.2.k.K..Yi.E
k......R".3......*...N.'.2.H&0@M.:...v_e.#.....z.\(.>.....
--------------------
UZ9rmC1SsoZVjPcS5Vu--.......................................................................................
.......................................................................................................
```

DEEPSEC


**Notes for the Viewer:**
**The IDS rule looks for POST**

DEEPSEC

```
alert http $HOME_NET any -> $EXTERNAL_NET [7080,8080,443,80,4143,995,21,50000,20,8090,8443,990,22]
(msg:"ET MALWARE Win32/Emotet CnC Activity (POST) M10";
flow:established,to_server; content:"POST"; http.uri; content:!"."; content:!"&"; content:!"-";
http.user_agent; content:"Mozilla/5.0 (Windows NT 6.";
http.header_names; content:"|0d 0a|User-Agent|0d 0a|Accept|0d 0a|Accept-Language|0d 0a|Accept-Encoding|0d 0a|"; startswith; content:"Referer|0d 0a|"; distance:0;
reference:md5,ba2e4a231652f8a492feb937b1e96e71; classtype:trojan-activity; sid:2030868; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_09_14, deployment Perimeter, signature_severity Major
2020_09_14;)
```

```
http.user_agent; content:"Mozilla/5.0 (Windows NT 6.";
```

```
17  2020-09-30 09:50:17.591672  trafcj.fvds.r
18  2020-09-30 09:50:17.591752  10.9.30.101
22  2020-09-30 09:50:17.614494  10.9.30.101
23  2020-09-30 09:50:17.823782  trafcj.fvds.r
24  2020-09-30 09:50:17.823992  10.9.30.101
25  2020-09-30 09:50:17.953767  trafcj.fvds.r
26  2020-09-30 09:50:17.953918  10.9.30.101
27  2020-09-30 09:50:17.954608  trafcj.fvds.r
28  2020-09-30 09:50:17.954734  10.9.30.101
29  2020-09-30 09:50:17.958959  trafcj.fvds.r
```

```
POST /pIXPXFus4dL9VHy/Ae4QuOOcWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:75.0) Gecko/20100101 Firefox
```

```
DNT: 1
Connection: keep-alive
Referer: 80.87.201.221/pIXPXFus4dL9VHy/Ae4QuOOcWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----------------UZ9rmC1SsoZVjPcS5Vu
Host: 80.87.201.221:7080
Content-Length: 4804
Cache-Control: no-cache
```

**Notes for the Viewer:**
**And it looks for the user agent**

DEEPSEC

# YARA Rules

**Notes for the Viewer:**
**Another method of signature-based detection.**

yara

The pattern matching swiss knife for malware researchers (and everyone else)

## { } YARA in a nutshell

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
```

**Notes for the Viewer:**
**YARA rules are typically used to find data within static files, like HTML or binaries**

https://github.com/kevthehermit/YaraPcap

# yaraPCAP

Yara Scanner For IMAP Feeds and saved Streams

###What it does:

- Reads a PCAP File and Extracts Http Streams.
- gzip deflates any compressed streams
- Scans every file with yara
- writes a report.txt
- optionally saves matching files to a Dir

###Usage

**Notes for the Viewer:**
**I found a project that uses YARA against network traffic.**

- Yara / PyYara
- TCPFlow 1.3 - https://github.com/simsong/tcpflow
- For windows edit the Script to point to your copy of the tcpflow binary. Line 29

DEEPSEC

- Write a YARA rule:

```
rule emotet : post {
meta:
  author = "Josh Pyorre"
  date = "2022-09-21"
  description = "Emotet"
strings:
  $type="POST"
  $user_agent="Mozilla/5.0 (Windows NT 6."
  $content="--|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"
  $referer="Referer|0d 0a|"
condition:
  ($user_agent) and ($type) and ($content) and ($referer)
}
```

**Notes for the Viewer:**
**I created a YARA rule based off the IDS rule to capture the Emotet C2 traffic shown in the Suricata example.**

```
jpyorre@evol YaraPcap %
```

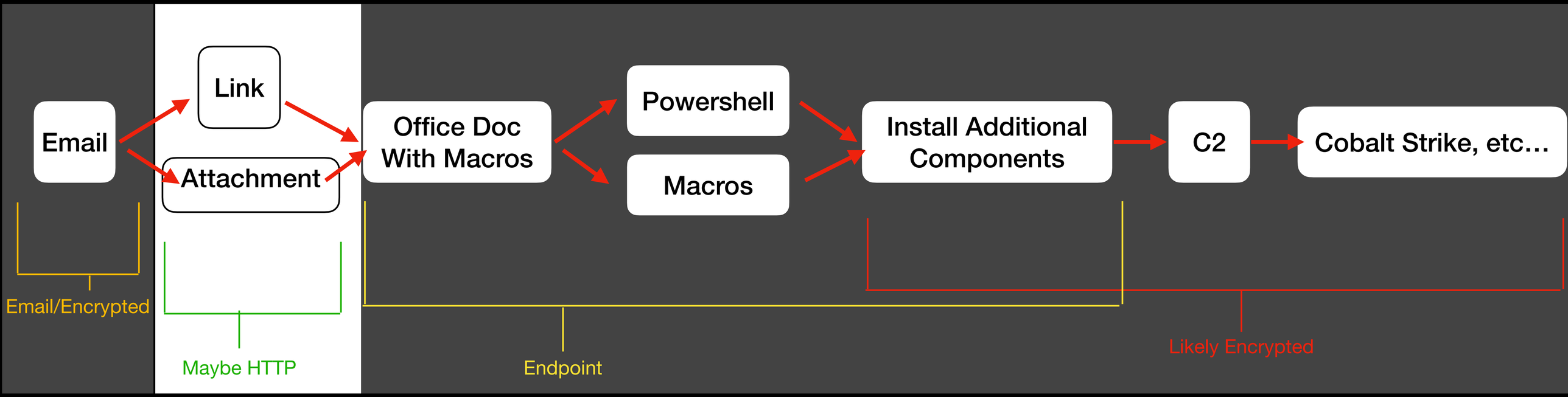
**This is a video showing:**
**The same PCAP file is replayed through YARAPCAP. The video shows the YARA rule catching the C2 activity.**

~~Visibility~~

SSL

Notes for the Viewer:
One more piece of context: Visibility is difficult because most traffic is SSL

# Emotet




**Notes for the Viewer:**
**With SSL, you are most likely to see only the initial second-stage GET request over HTTP (maybe)**

# IcedID Dropper -> Cobalt Strike

| | | | | | | |
|---|---|---|---|---|---|---|
| 27721 | 2022-08-10 04:17:47.753017 | 172.93.98.170 | 10.8.9.101 | TCP | 58 | 80 → 58697 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 |
| 27722 | 2022-08-10 04:17:47.753188 | 10.8.9.101 | 172.93.98.170 | TCP | 54 | 58697 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 27723 | 2022-08-10 04:17:47.753357 | 10.8.9.101 | 172.93.98.170 | HTTP | 132 | GET /download/a2.dll HTTP/1.1 |

Wireshark · Follow HTTP Stream (tcp.stream eq 1020) · 2022-08-09-IcedID-part-2-with-Cobalt-Strike.pcap

```
GET /download/a2.dll HTTP/1.1
Connection: Keep-Alive
Host: 172.93.98.170

HTTP/1.1 200 OK
Date: Wed, 10 Aug 2022 11:17:48 GMT
Server: Microsoft-IIS/8.5
Content-Type: application/octet-stream
Cache-Control: max-age=1
```

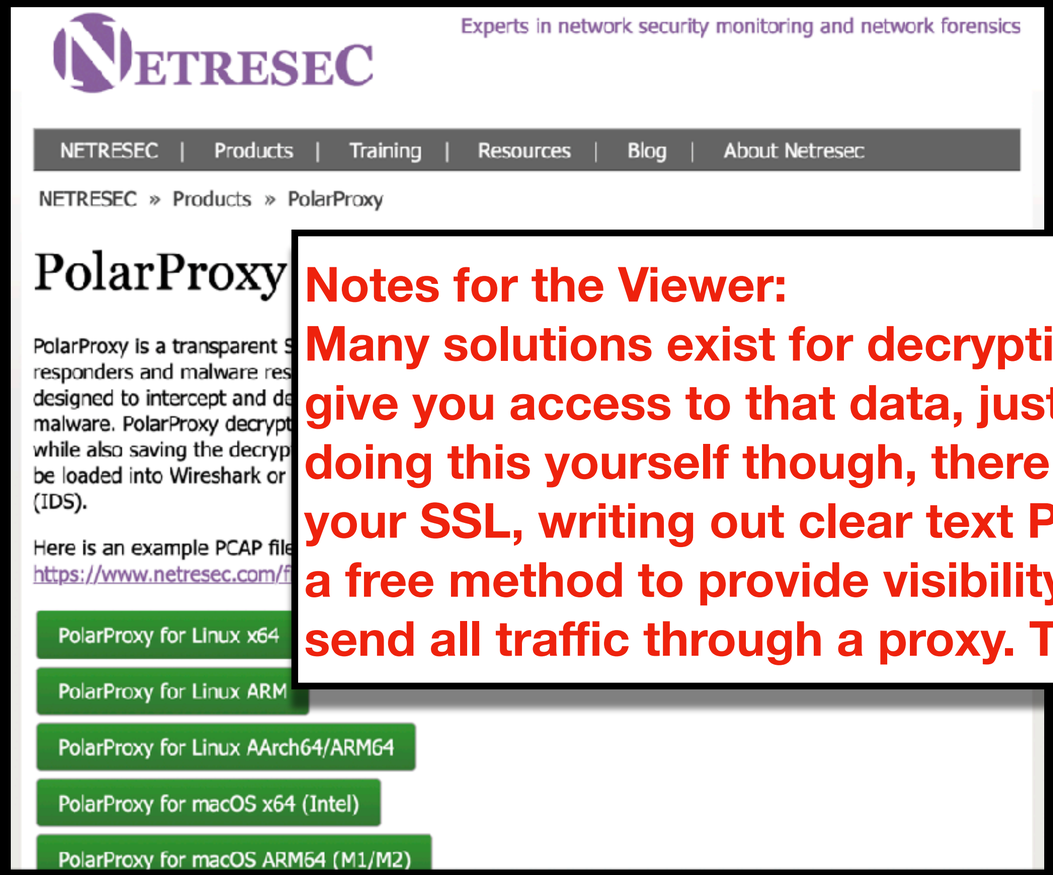
**Notes for the Viewer:**
**With SSL, you are most likely to see only the initial second-stage GET request over HTTP (maybe)**

DEEPSEC

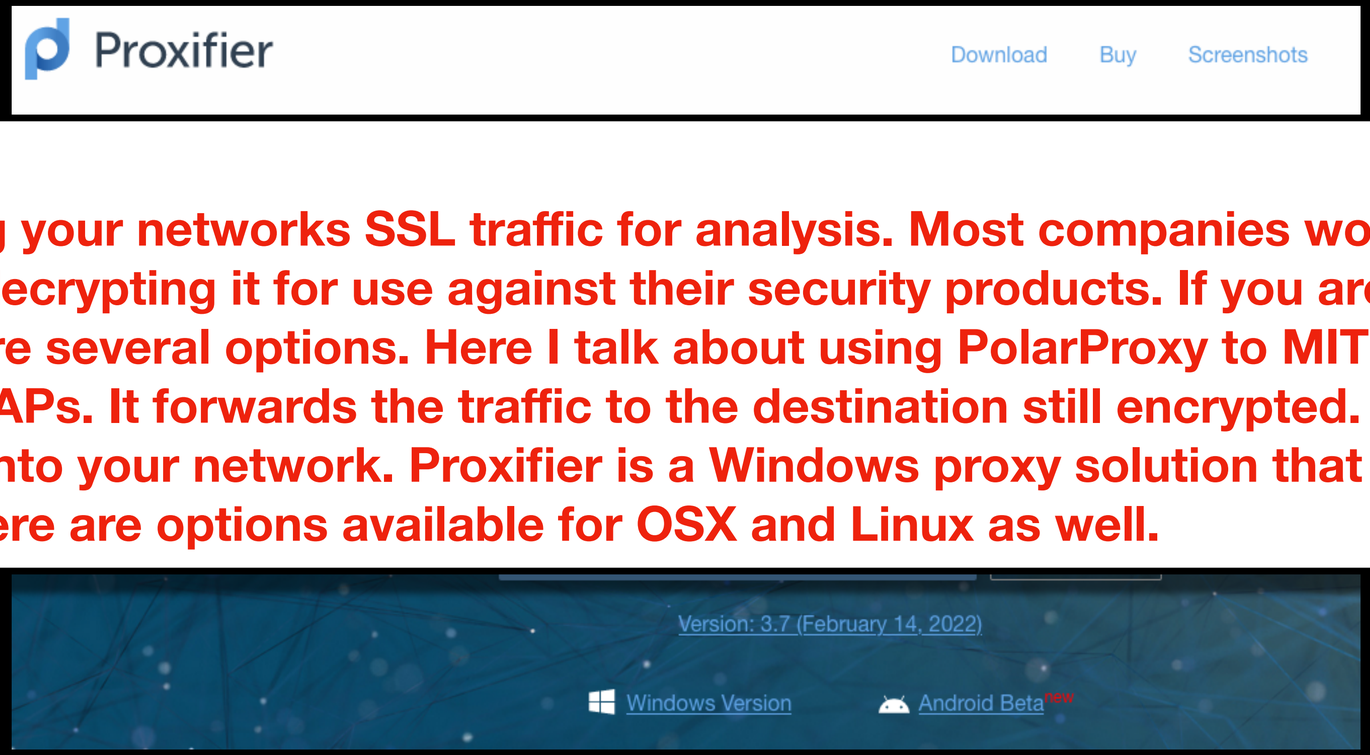
# IcedID Dropper -> Cobalt Strike

| | | | | | | |
|---|---|---|---|---|---|---|
| 30047 | 2022-08-10 04:17:49.014657 | 172.93.98.170 | 10.8.9.101 | HTTP | 714 | HTTP/1.1 200 OK |
| 30048 | 2022-08-10 04:17:49.014680 | 10.8.9.101 | 172.93.98.170 | TCP | 54 | 58697 → 80 [ACK] Seq=79 Ack=2134239 Win=63580 Len=0 |
| 30049 | 2022-08-10 04:17:49.015324 | 10.8.9.101 | 172.93.98.170 | TCP | 54 | 58697 → 80 [FIN, ACK] Seq=79 Ack=2134239 Win=63580 Len=0 |
| 30050 | 2022-08-10 04:17:49.015349 | 172.93.98.170 | 10.8.9.101 | TCP | 54 | 80 → 58697 [ACK] Seq=2134239 Ack=80 Win=64239 Len=0 |
| 30051 | 2022-08-10 04:17:49.151010 | 213.227.154.169 | 10.8.9.101 | TLSv1… | 220 | Change Cipher Spec, Application Data, Application Data |
| 30052 | 2022-08-10 04:17:49.151105 | 10.8.9.101 | 213.227.154.169 | TCP | 54 | 58699 → 443 [ACK] Seq=365 Ack=300 Win=65535 Len=0 |
| 30053 | 2022-08-10 04:17:49.151485 | 10.8.9.101 | 213.227.154.169 | TLSv1… | 134 | Change Cipher Spec, Application Data |
| 30054 | 2022-08-10 04:17:49.151553 | 213.227.154.169 | 10.8.9.101 | TCP | 54 | 443 → 58699 [ACK] Seq=300 Ack=445 Win=64240 Len=0 |
| 30055 | 2022-08-10 04:17:49.151944 | 10.8.9.101 | 213.227.154.169 | TLSv1… | 579 | Application Data |
| 30056 | 2022-08-10 04:17:49.151972 | 213.227.154.169 | 10.8.9.101 | TCP | 54 | 443 → 58699 [ACK] Seq=300 Ack=970 Win=64240 Len=0 |
| 30057 | 2022-08-10 04:17:49.172055 | 213.227.154.169 | 10.8.9.101 | TLSv1… | 1376 | Application Data, Application Data, Application Data, Application Data |
| 30058 | 2022-08-10 04:17:49.172118 | 10.8.9.101 | 213.227.154.169 | TCP | 54 | 58698 → 443 [ACK] Seq=970 Ack=1711 Win=65535 Len=0 |

**Notes for the Viewer:**
**With SSL, you are most likely to see only the initial second-stage GET request over HTTP (maybe)**




https://www.netresec.com/?page=PolarProxy



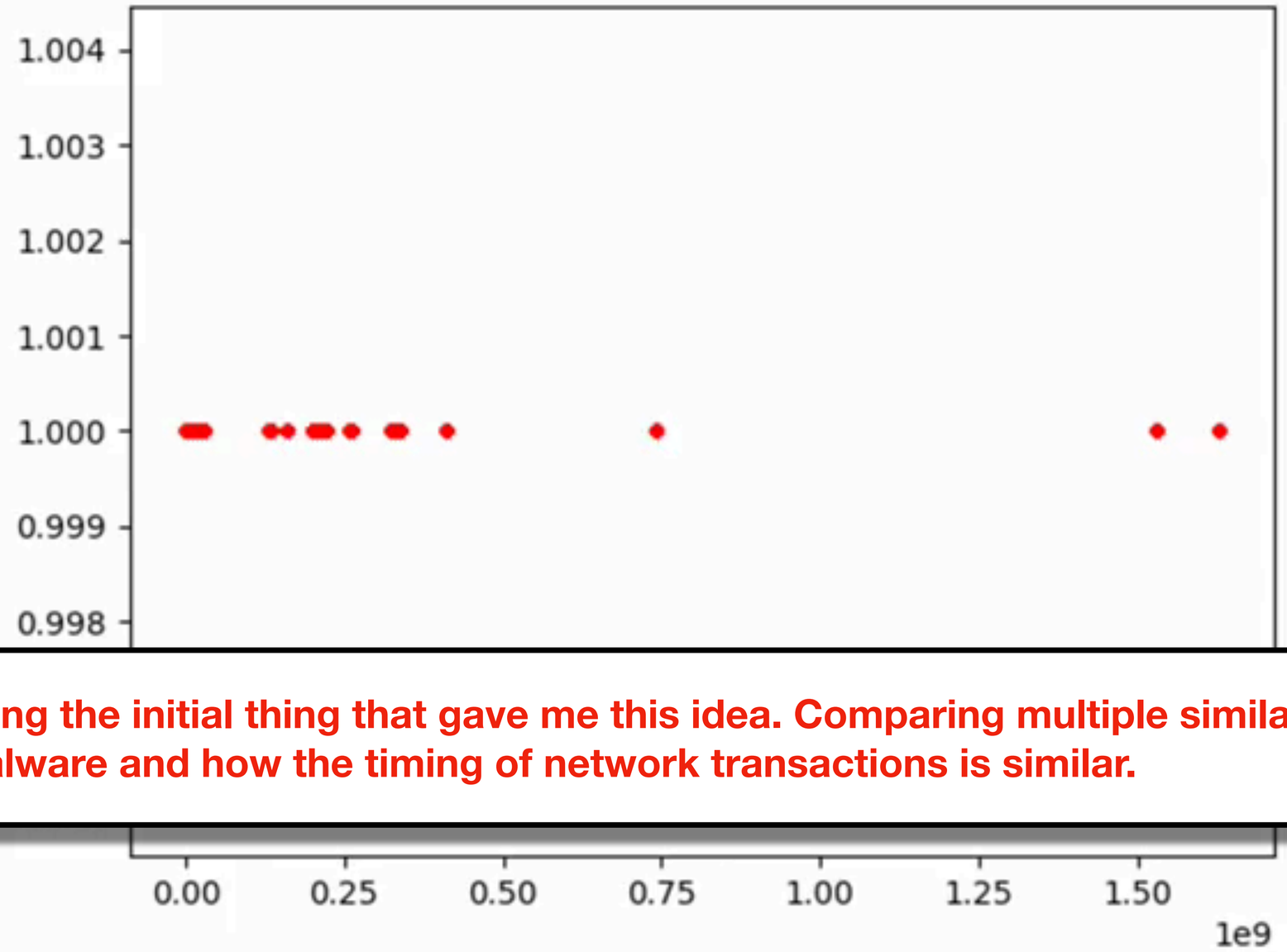

https://www.netresec.com/?page=PolarProxy

**Notes for the Viewer:**

**Many solutions exist for decrypting your networks SSL traffic for analysis. Most companies won't give you access to that data, just decrypting it for use against their security products. If you are doing this yourself though, there are several options. Here I talk about using PolarProxy to MITM your SSL, writing out clear text PCAPs. It forwards the traffic to the destination still encrypted. It's a free method to provide visibility into your network. Proxifier is a Windows proxy solution that wil send all traffic through a proxy. There are options available for OSX and Linux as well.**

# Can we build a signature Using network Timing?

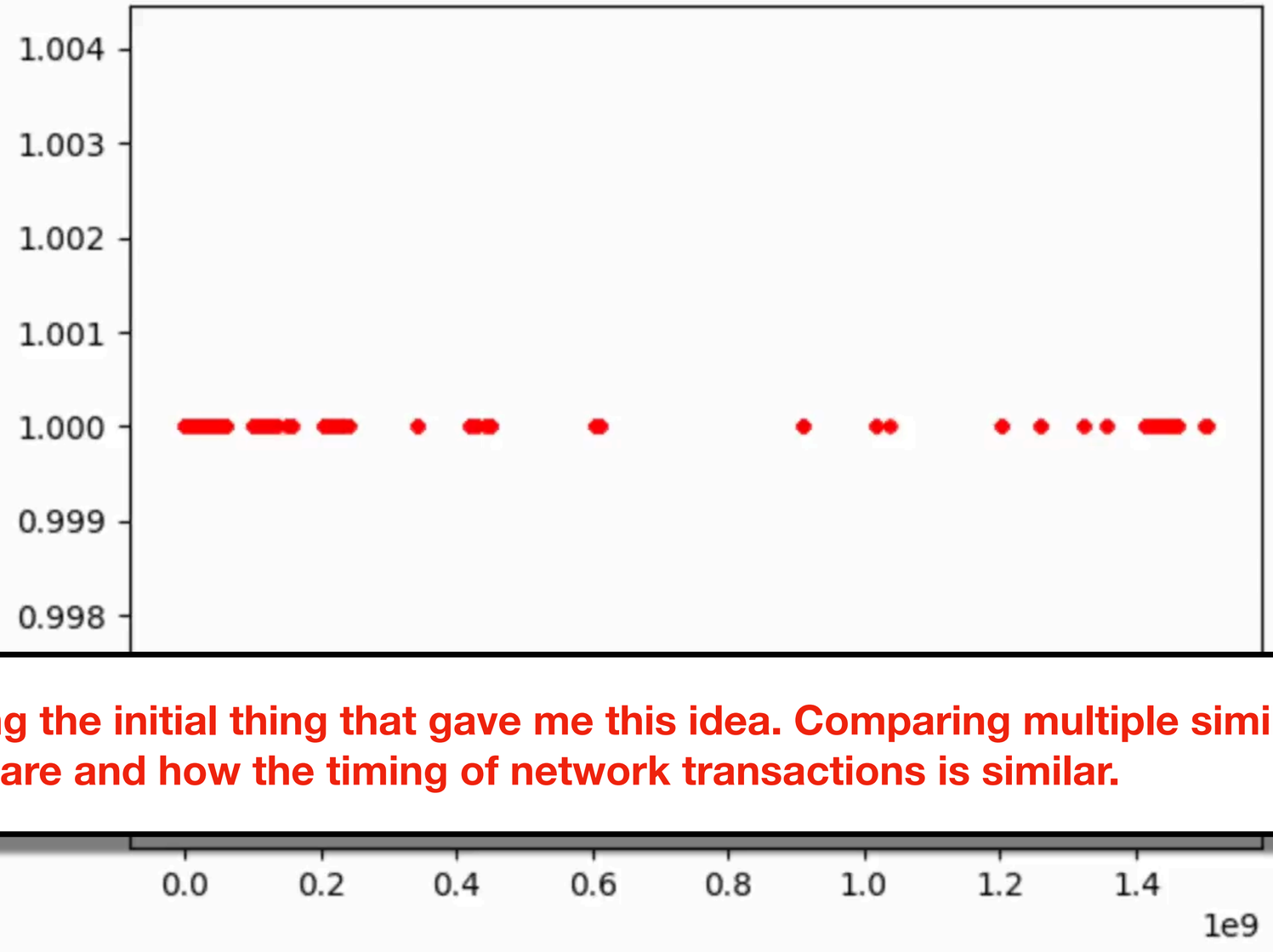
2018-06-28-Hancitor-malspam-infection-traffi.png Open with Preview




**Video showing the initial thing that gave me this idea. Comparing multiple similar PCAPs for Hancitor malware and how the timing of network transactions is similar.**

DEEPSEC

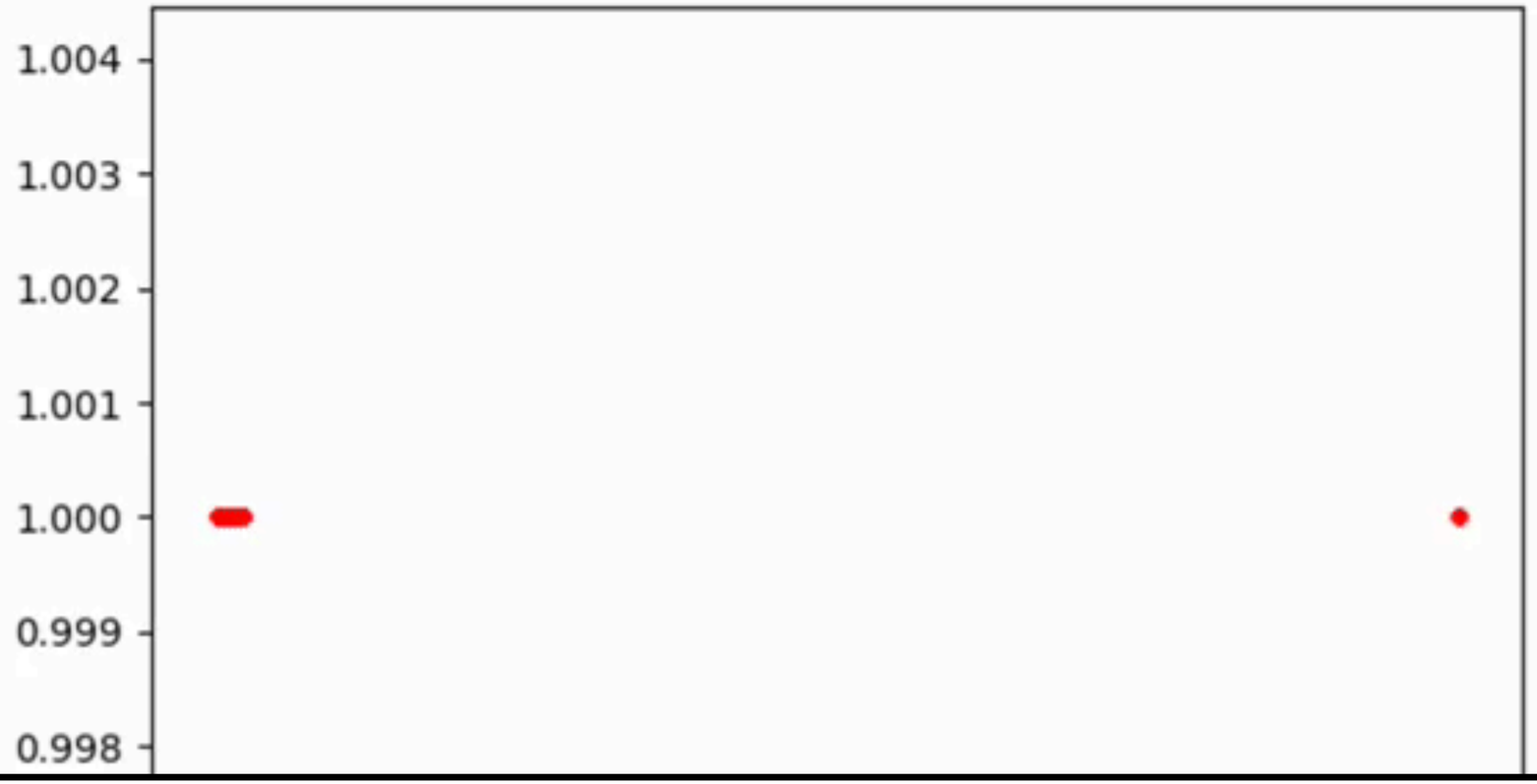
2018-06-05-Emotet-malspam-infection-traffi.png Open with Preview



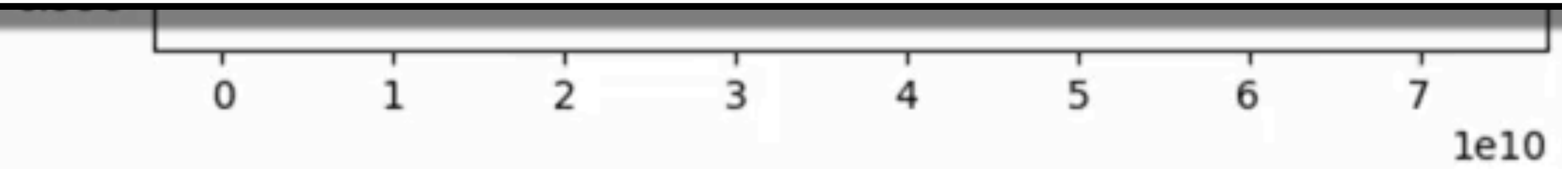

**Video showing the initial thing that gave me this idea. Comparing multiple similar PCAPs for Emotet malware and how the timing of network transactions is similar.**

DEEPSEC

2018-06-14-Emotet-infection-traffic-with-Trickbot.png Open with Preview




**Video showing the initial thing that gave me this idea. Comparing multiple similar PCAPs for Trickbot malware and how the timing of network transactions is similar.**




DEEPSEC

# Finding Patterns

**Notes for the Viewer:**
**Beginning the process of trying to find patterns that can be used to create a signature.**

# Dropper Downloads

**Notes for the Viewer:**
**We'll start by looking at dropper downloads.**

2052 transactions

| Protoc | Leng | Info |
|---|---|---|
| TCP | 66 | 63087 → http(80) [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| TCP | 58 | http(80) → 63087 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| TCP | 54 | 63087 → http(80) [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| HTTP | 133 | GET /download/msb.exe HTTP/1.1 |
| TCP | 54 | http(80) → 63087 [ACK] Seq=1 Ack=80 Win=64240 Len=0 |
| TCP | 275 | http(80) → 63087 [PSH, ACK] Seq=1 Ack=80 Win=64240 Len=221 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=222 Ack=80 Win=64240 Len=1460 [T |
| TCP | 1346 | http(80) → 63087 [PSH, ACK] Seq=1682 Ack=80 Win=64240 Len=1 |
| TCP | 54 | 63087 → http(80) [ACK] Seq=80 Ack=2974 Win=64240 Len=0 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=2974 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=4434 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=5894 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1178 | http(80) → 63087 [PSH, ACK] Seq=7354 Ack=80 Win=64240 Len=1 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=8478 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=9938 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1262 | http(80) → 63087 [PSH, ACK] Seq=11398 Ack=80 Win=64240 Len= |
| TCP | 54 | 63087 → http(80) [ACK] Seq=80 Ack=12606 Win=64240 Len=0 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=12606 Ack=80 Win=64240 Len=1460 |
| TCP | 1346 | http(80) → 63087 [PSH, ACK] Seq=14066 Ack=80 Win=64240 Len= |
| TCP | 54 | 63087 → http(80) [ACK] Seq=80 Ack=15358 Win=64240 Len=0 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=15358 Ack=80 Win=64240 Len=1460 |
| TCP | 1346 | http(80) → 63087 [PSH, ACK] Seq=16818 Ack=80 Win=64240 Len= |

Wireshark · Follow TCP Stream (tcp.st

```
GET /download/msb.exe HTTP/1.1
Connection: Keep-Alive
Host: 209.222.98.13

HTTP/1.1 200 OK
Date: Mon, 25 Jul 2022 19:56:38 GMT
Server: Microsoft-IIS/8.5
Content-Type: application/octet-stream
Cache-Control: max-age=1
Connection: keep-alive
X-Powered-By: ASP.NET
Content-Length: 2134016

MZ.......................@.......................
program cannot be run in DOS mode.
```

Two Separate
icedID Downloads

Similar Transactions

1107 transactions

| Protoc | Leng | Info |
|---|---|---|
| TCP | 66 | 50462 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER |
| TCP | 58 | http(80) → 50462 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| TCP | 54 | 50462 → http(80) [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| HTTP | 135 | GET /download/sys.exe HTTP/1.1 |
| TCP | 54 | http(80) → 50462 [ACK] Seq=1 Ack=82 Win=64240 Len=0 |
| TCP | 274 | http(80) → 50462 [PSH, ACK] Seq=1 Ack=82 Win=64240 Len=220 [TCP segme |
| TCP | 1442 | http(80) → 50462 [PSH, ACK] Seq=221 Ack=82 Win=64240 Len=1388 [TCP se |
| TCP | 54 | 50462 |
| TCP | 1442 | http( |
| TCP | 1442 | http( |
| TCP | 54 | 50462 |
| TCP | 1442 | http( |
| TCP | 1442 | http( |
| TCP | 54 | 50462 |
| TCP | 1442 | http( |
| TCP | 1442 | http( |
| TCP | 1442 | http( |
| TCP | 54 | 50462 |

Wireshark · Follow TCP Stream (tcp.stream eq 0) ·

```
GET /download/sys.exe HTTP/1.1
Connection: Keep-Alive
Host: 104.238.220.131

HTTP/1.1 200 OK
Date: Mon, 8 Aug 2022 21:27:00 GMT
Server: Microsoft-IIS/8.5
Content-Type: application/octet-stream
```

| | | |
|---|---|---|
| TCP | 1514 | http( |
| TCP | 1370 | http( |

```
MZ.......................@.......................
program cannot be run in DOS mode.
```

**Notes for the Viewer: Two similar PCAPs**

DEEPSEC

2052 transactions

| Protoc | Leng | Info |
|---|---|---|
| TCP | 66 | 63087 → http(80) [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| TCP | 58 | http(80) → 63087 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| TCP | 54 | 63087 → http(80) [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| HTTP | 133 | GET /download/msb.exe HTTP/1.1 |
| TCP | 54 | http(80) → 63087 [ACK] Seq=1 Ack=80 Win=64240 Len=0 |
| TCP | 275 | http(80) → 63087 [PSH, ACK] Seq=1 Ack=80 Win=64240 Len=221 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=222 Ack=80 Win=64240 Len=1460 [T |
| TCP | 1346 | http(80) → 63087 [PSH, ACK] Seq=1682 Ack=80 Win=64240 Len=1 |
| TCP | 54 | 63087 → http(80) [ACK] Seq=80 Ack=2974 Win=64240 Len=0 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=2974 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=4434 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=5894 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1178 | http(80) → 63087 [PSH, ACK] Seq=7354 Ack=80 Win=64240 Len=1 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=8478 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=9938 Ack=80 Win=64240 Len=1460 [ |
| TCP | 1262 | http(80) → 63087 [PSH, ACK] Seq=11398 Ack=80 Win=64240 Len= |
| TCP | 54 | 63087 → http(80) [ACK] Seq=80 Ack=12606 Win=64240 Len=0 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=12606 Ack=80 Win=64240 Len=1460 |
| TCP | 1346 | http(80) → 63087 [PSH, ACK] Seq=14066 Ack=80 Win=64240 Len= |
| TCP | 54 | 63087 → http(80) [ACK] Seq=80 Ack=15358 Win=64240 Len=0 |
| TCP | 1514 | http(80) → 63087 [ACK] Seq=15358 Ack=80 Win=64240 Len=1460 |
| TCP | 1346 | http(80) → 63087 [PSH, ACK] Seq=16818 Ack=80 Win=64240 Len= |

Wireshark · Follow TCP Stream (tcp.st

```
GET /download/msb.exe HTTP/1.1
Connection: Keep-Alive
Host: 209.222.98.13

HTTP/1.1 200 OK
Date: Mon, 25 Jul 2022 19:56:38 GMT
Server: Microsoft-IIS/8.5
Content-Type: application/octet-stream
Cache-Control: max-age=1
Connection: keep-alive
X-Powered-By: ASP.NET
Content-Length: 2134016

MZ.......................@.......................
program cannot be run in DOS mode.
```

Similar byte lengths

1107 transactions

| Protoc | Leng | Info |
|---|---|---|
| TCP | 66 | 50462 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER |
| TCP | 58 | http(80) → 50462 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| TCP | 54 | 50462 → http(80) [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| HTTP | 135 | GET /download/sys.exe HTTP/1.1 |
| TCP | 54 | http(80) → 50462 [ACK] Seq=1 Ack=82 Win=64240 Len=0 |
| TCP | 274 | http(80) → 50462 [PSH, ACK] Seq=1 Ack=82 Win=64240 Len=220 [TCP segme |
| TCP | 1442 | http(80) → 50462 [PSH, ACK] Seq=221 Ack=82 Win=64240 Len=1388 [TCP se |
| TCP | 54 | 50462 |
| TCP | 1442 | http |
| TCP | 1442 | http |
| TCP | 54 | 50462 |
| TCP | 1442 | http |
| TCP | 1442 | http |
| TCP | 54 | 50462 |
| TCP | 1442 | http |
| TCP | 1442 | http |
| TCP | 1442 | http |
| TCP | 54 | 50462 |

Wireshark · Follow TCP Stream (tcp.stream eq 0) ·

```
GET /download/sys.exe HTTP/1.1
Connection: Keep-Alive
Host: 104.238.220.131

HTTP/1.1 200 OK
Date: Mon, 8 Aug 2022 21:27:00 GMT
Server: Microsoft-IIS/8.5
Content-Type: application/octet-stream
```

**Notes for the Viewer: They have similar byte lengths**

| | | |
|---|---|---|
| TCP | 1514 | http |
| TCP | 1370 | http |

```
MZ.......................@.......................
program cannot be run in DOS mode.
```

DEEPSEC

2052 transactions

```
Difference in microseconds: 93622 (12:56:39.441422 - 12:56:39.535044)
Difference in microseconds: 98 (12:56:39.535044 - 12:56:39.535142)
Difference in microseconds: 159 (12:56:39.535142 - 12:56:39.535301)
Difference in microseconds: 56 (12:56:39.535301 - 12:56:39.535357)
Difference in microseconds: 92677 (12:56:39.535357 - 12:56:39.628034)
Difference in microseconds: 1444 (12:56:39.628034 - 12:56:39.629478)
Difference in microseconds: 21 (12:56:39.629478 - 12:56:39.629499)
```

Similar timing, at least in the beginning
(The GET request)

1107 transactions

```
Difference in microseconds: 58480 (14:27:00.681914 - 14:27:00.740394)
Difference in microseconds: 82 (14:27:00.740394 - 14:27:00.740476)
Difference in microseconds: 180 (14:27:00.740476 - 14:27:00.740656)
Difference in microseconds: 50 (14:27:00.740656 - 14:27:00.740706)
Difference in microseconds: 62994 (14:27:00.740706 - 14:27:00.803700)
Difference in microseconds: 3189 (14:27:00.803700 - 14:27:00.806889)
Difference in microseconds: 92 (14:27:00.806889 - 14:27:00.806981)
```

**Notes for the Viewer: Looking at the time in between transactions, there are some similarities**

DEEPSEC

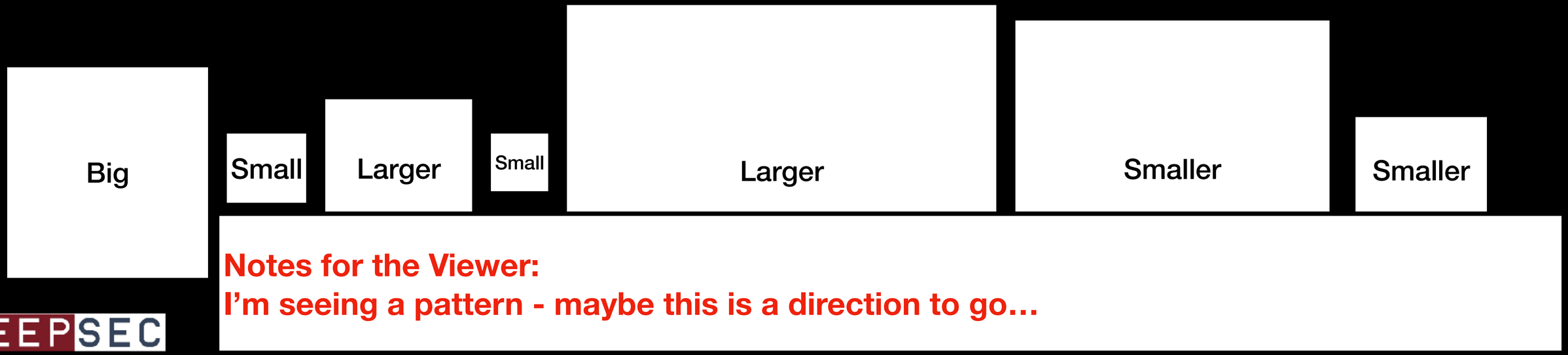
2052 transactions

```
Difference in microseconds: 93622 (12:56:39.441422 - 12:56:39.535044)
Difference in microseconds: 98 (12:56:39.535044 - 12:56:39.535142)
Difference in microseconds: 159 (12:56:39.535142 - 12:56:39.535301)
Difference in microseconds: 56 (12:56:39.535301 - 12:56:39.535357)
Difference in microseconds: 92677 (12:56:39.535357 - 12:56:39.628034)
Difference in microseconds: 1444 (12:56:39.628034 - 12:56:39.629478)
Difference in microseconds: 21 (12:56:39.629478 - 12:56:39.629499)
```

Similar timing, at least in the beginning
(The GET request)

1107 transactions

```
Difference in microseconds: 58480 (14:27:00.681914 - 14:27:00.740394)
Difference in microseconds: 82 (14:27:00.740394 - 14:27:00.740476)
Difference in microseconds: 180 (14:27:00.740476 - 14:27:00.740656)
Difference in microseconds: 50 (14:27:00.740656 - 14:27:00.740706)
Difference in microseconds: 62994 (14:27:00.740706 - 14:27:00.803700)
Difference in microseconds: 3189 (14:27:00.803700 - 14:27:00.806889)
Difference in microseconds: 92 (14:27:00.806889 - 14:27:00.806981)
```



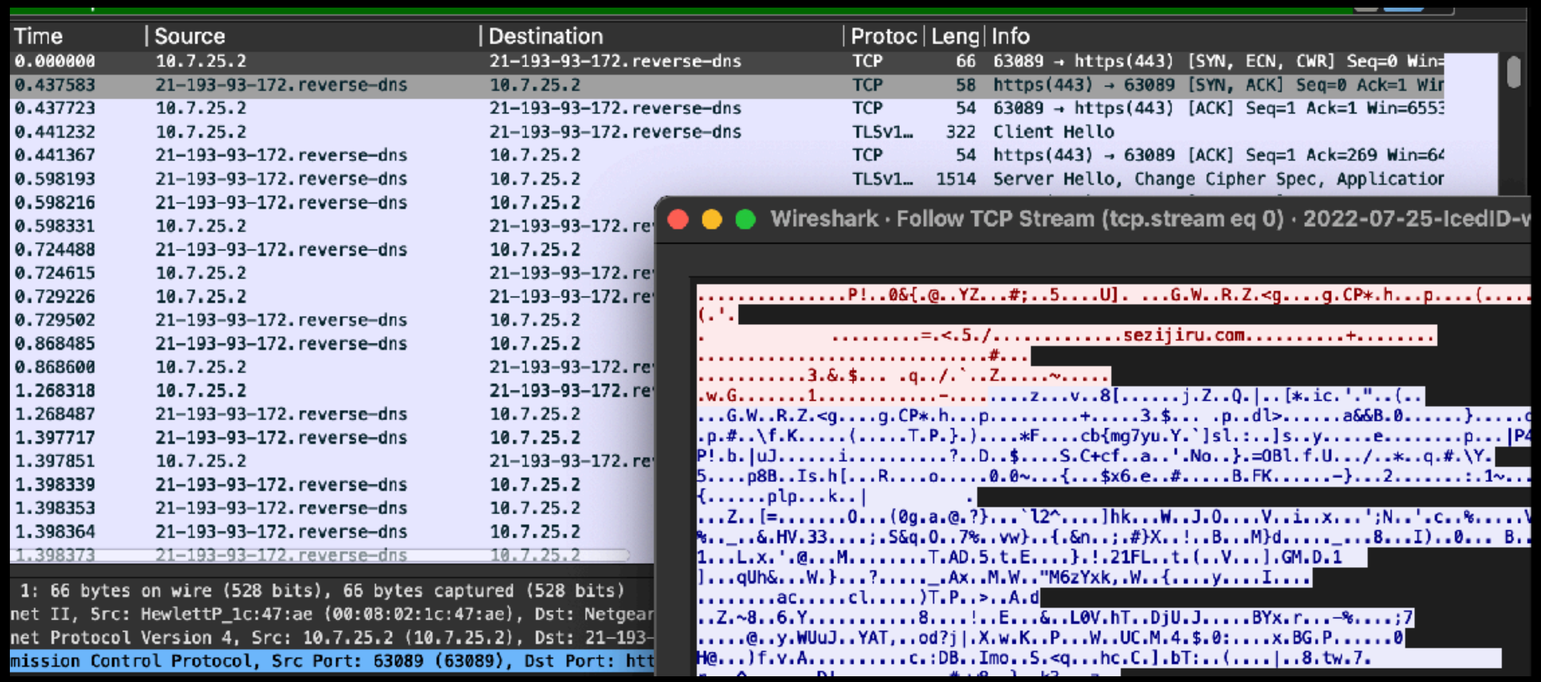

**Notes for the Viewer:**
**I'm seeing a pattern - maybe this is a direction to go…**

DEEPSEC

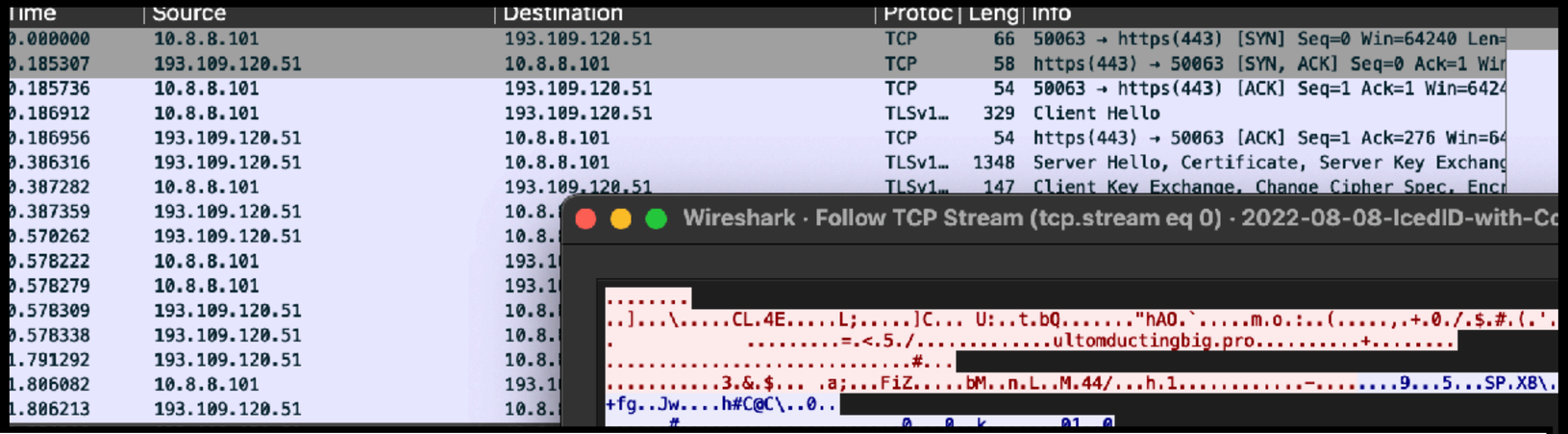
# Beaconing

**Notes for the Viewer:**
**Let’s look at C2 beaconing**

Cobalt Strike Beaconing, Sample 1




Cobalt Strike Beaconing, Sample 2




**Notes for the Viewer:**
**Two similar PCAPs with CobaltStrike beaconing**

DEEPSEC

Cobalt Strike Beaconing, Sample 1

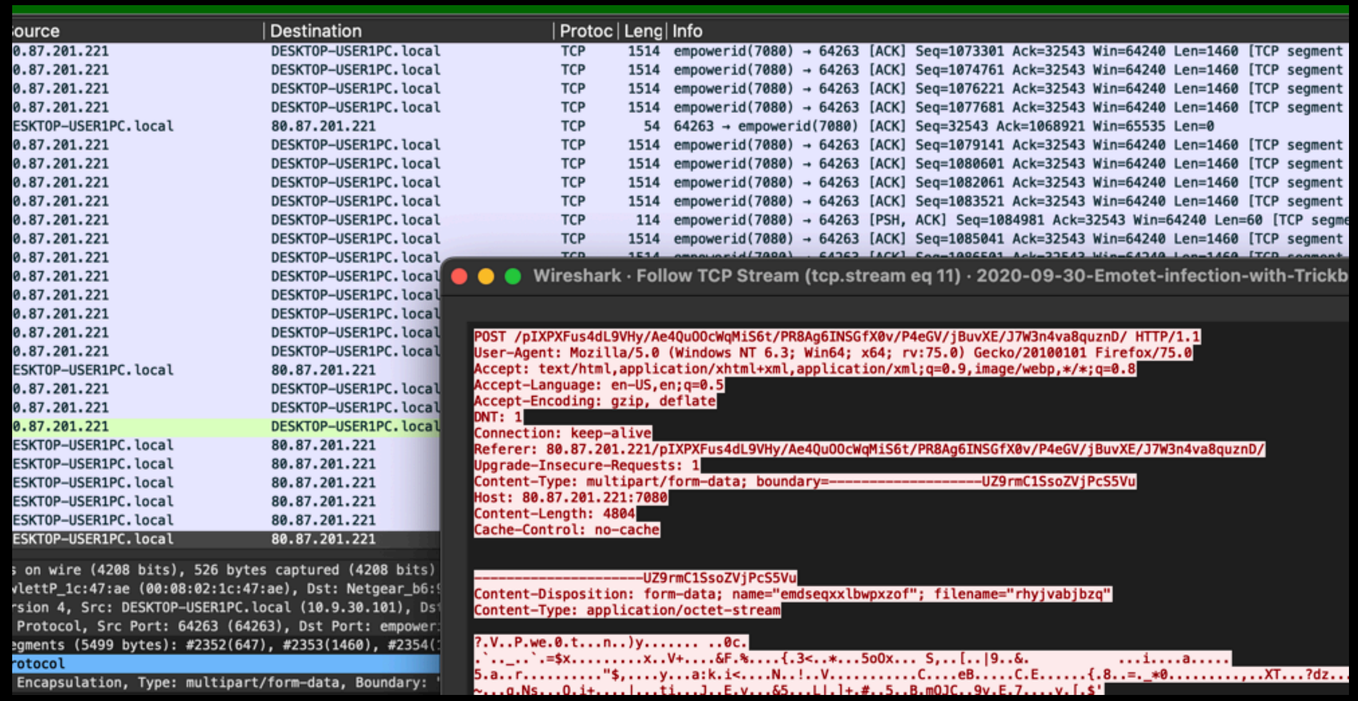
```
279 Packets
Difference in microseconds: 437583 (12:56:54.546469 - 12:56:54.984052)
Difference in microseconds: 140 (12:56:54.984052 - 12:56:54.984192)
Difference in microseconds: 3509 (12:56:54.984192 - 12:56:54.987701)
Difference in microseconds: 135 (12:56:54.987701 - 12:56:54.987836)
Difference in microseconds: 156826 (12:56:54.987836 - 12:56:55.144662)
Difference in microseconds: 23 (12:56:55.144662 - 12:56:55.144685)
Difference in microseconds: 115 (12:56:55.144685 - 12:56:55.144800)
Difference in microseconds: 126157 (12:56:55.144800 - 12:56:55.270957)
Difference in microseconds: 127 (12:56:55.270957 - 12:56:55.271084)
```

**Notes for the Viewer: Looking at the time in between transactions, there are some similarities**

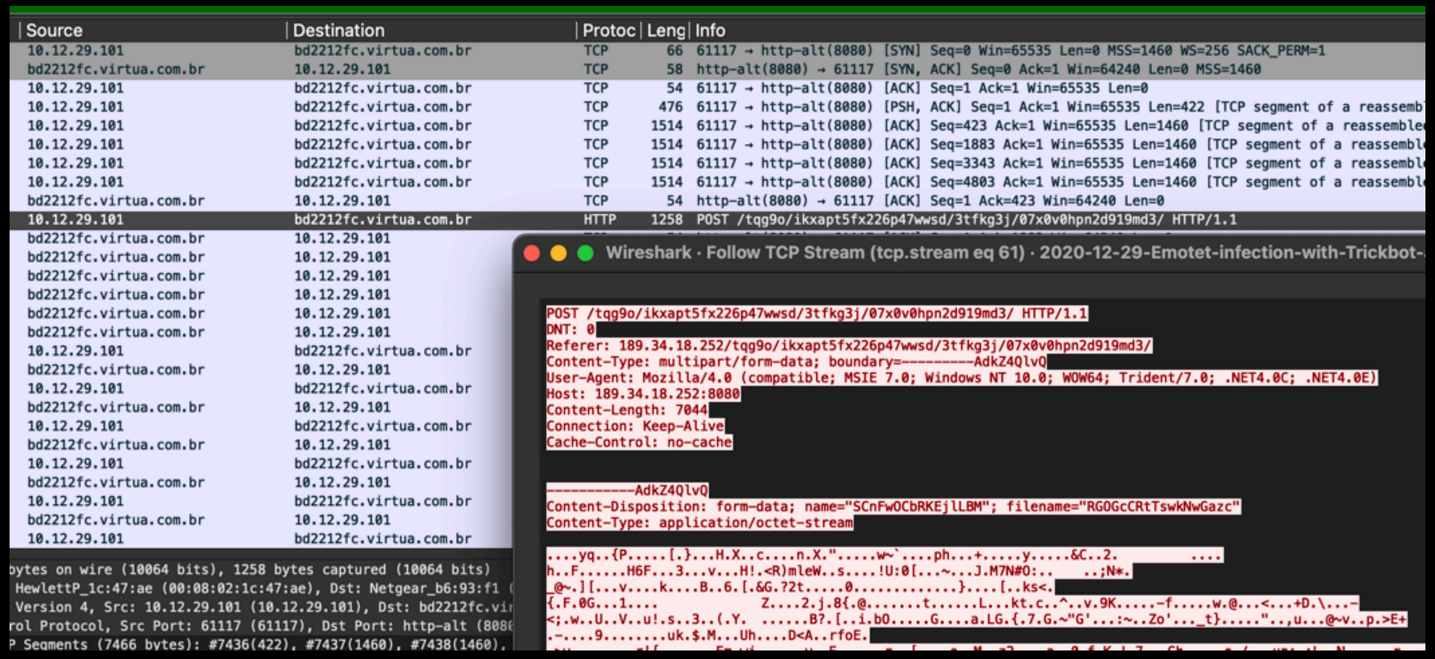
Cobalt Strike Beaconing, Sample 2

```
24 Packets
Difference in microseconds: 185307 (13:15:56.474085 - 13:15:56.659392)
Difference in microseconds: 429 (13:15:56.659392 - 13:15:56.659821)
Difference in microseconds: 1176 (13:15:56.659821 - 13:15:56.660997)
Difference in microseconds: 44 (13:15:56.660997 - 13:15:56.661041)
Difference in microseconds: 199360 (13:15:56.661041 - 13:15:56.860401)
Difference in microseconds: 966 (13:15:56.860401 - 13:15:56.861367)
Difference in microseconds: 77 (13:15:56.861367 - 13:15:56.861444)
Difference in microseconds: 182903 (13:15:56.861444 - 13:15:57.044347)
Difference in microseconds: 7960 (13:15:57.044347 - 13:15:57.052307)
```

Emotet and Trickbot beacon 1:




Emotet and Trickbot beacon 2:




DEEPSEC

Emotet and Trickbot beacon 1:

```
1527 Total Packets
Difference in microseconds: 285959 (09:50:16.520476 - 09:50:16.806435)
Difference in microseconds: 522 (09:50:16.806435 - 09:50:16.806957)
Difference in microseconds: 91 (09:50:16.806957 - 09:50:16.807048)
Difference in microseconds: 137 (09:50:16.807048 - 09:50:16.807185)
Difference in microseconds: 10 (09:50:16.807185 - 09:50:16.807195)
Difference in microseconds: 5 (09:50:16.807195 - 09:50:16.807200)
Difference in microseconds: 4 (09:50:16.807200 - 09:50:16.807204)
Difference in microseconds: 74 (09:50:16.807204 - 09:50:16.807278)
Difference in microseconds: 62 (09:50:16.807278 - 09:50:16.807340)
Difference in microseconds: 40 (09:50:16.807340 - 09:50:16.807380)
Difference in microseconds: 39 (09:50:16.807380 - 09:50:16.807419)
Difference in microseconds: 783370 (09:50:16.807419 - 09:50:17.590789)
Difference in microseconds: 177 (09:50:17.590789 - 09:50:17.590966)
```

Emotet and Trickbot beacon 2:

```
5493 Total Packets
Difference in microseconds: 249919 (10:19:19.476849 - 10:19:19.726768)
Difference in microseconds: 192 (10:19:19.726768 - 10:19:19.726960)
Difference in microseconds: 363 (10:19:19.726960 - 10:19:19.727323)
Difference in microseconds: 99 (10:19:19.727323 - 10:19:19.727422)
Difference in microseconds: 14 (10:19:19.727422 - 10:19:19.727436)
Difference in microseconds: 7 (10:19:19.727436 - 10:19:19.727443)
Difference in microseconds: 6 (10:19:19.727443 - 10:19:19.727449)
Difference in microseconds: 7 (10:19:19.727449 - 10:19:19.727456)
Difference in microseconds: 2 (10:19:19.727456 - 10:19:19.727458)
Difference in microseconds: 70 (10:19:19.727458 - 10:19:19.727528)
Difference in microseconds: 52 (10:19:19.727528 - 10:19:19.727580)
Difference in microseconds: 45 (10:19:19.727580 - 10:19:19.727625)
Difference in microseconds: 55 (10:19:19.727625 - 10:19:19.727680)
```

**Notes for the Viewer: Looking at the time in between transactions, there are some similarities**

# Benign vs Malicious

**Notes for the Viewer:**
**What if we add in some benign network traffic?**

# Benign .exe Download

| Time | Source | Destination |
|---|---|---|
| .000000 | evol.lan | li744-28.members.linode.com |
| .048434 | li744-28.members.linode.com | evol.lan |
| .048696 | evol.lan | li744-28.members.linode.com |
| .048807 | evol.lan | li744-28.members.linode.com |
| .054736 | li744-28.members.linode.com | |
| .193391 | li744-28.members.linode.com | |
| .193707 | evol.lan | |
| .195468 | li744-28.members.linode.com | |
| .195616 | evol.lan | |
| .196584 | li744-28.members.linode.com | |
| .196586 | li744-28.members.linode.com | |
| .196649 | evol.lan | |
| .196763 | evol.lan | |
| .497034 | li744-28.members.linode.com | |

Appearance

6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bi
et II, Src: GLTechno_18:d6:06 (94:83:c4:18:d6:06), Dst: Apple_09:
et Protocol Version 4, Src: li744-28.members.linode.com (23.239.2
ission Control Protocol, Src Port: http (80), Dst Port: 55278 (55

Wireshark · Follow TCP Stream (tcp.stream eq 0) · benign_exe_download.pcap

```
GET /existential.exe HTTP/1.1
Host: samplevault.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:103.0) Gecko/20100101 Firefox/
103.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

HTTP/1.1 200 OK
Date: Wed, 24 Aug 2022 18:58:19 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 24 Aug 2022 18:55:28 GMT
ETag: "1800-5e701397c408b"
Accept-Ranges: bytes
Content-Length: 6144
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdos-program

MZ......................@.......................................        .!..L.!This
```

**Notes for the Viewer:**
**This is a download of a small .exe that is benign, but was created to be used in testing to look like a potential dropper download.**

DEEPSEC

# Benign .exe Vs Malicious Dropper Download

Benign:

```
14 packets
Difference in microseconds: 48434 (11:58:19.135349 - 11:58:19.183783)
Difference in microseconds: 262 (11:58:19.183783 - 11:58:19.184045)
Difference in microseconds: 111 (11:58:19.184045 - 11:58:19.184156)
Difference in microseconds: 5929 (11:58:19.184156 - 11:58:19.190085)
Difference in microseconds: 138655 (11:58:19.190085 - 11:58:19.328740)
Difference in microseconds: 316 (11:58:19.328740 - 11:58:19.329056)
Difference in microseconds: 1761 (11:58:19.329056 - 11:58:19.330817)
Difference in microseconds: 148 (11:58:19.330817 - 11:58:19.330965)
Difference in microseconds: 968 (11:58:19.330965 - 11:58:19.331933)
Difference in microseconds: 2 (11:58:19.331933 - 11:58:19.331935)
Difference in microseconds: 63 (11:58:19.331935 - 11:58:19.331998)
Difference in microseconds: 114 (11:58:19.331998 - 11:58:19.332112)
Difference in microseconds: 300271 (11:58:19.332112 - 11:58:20.632383)
```

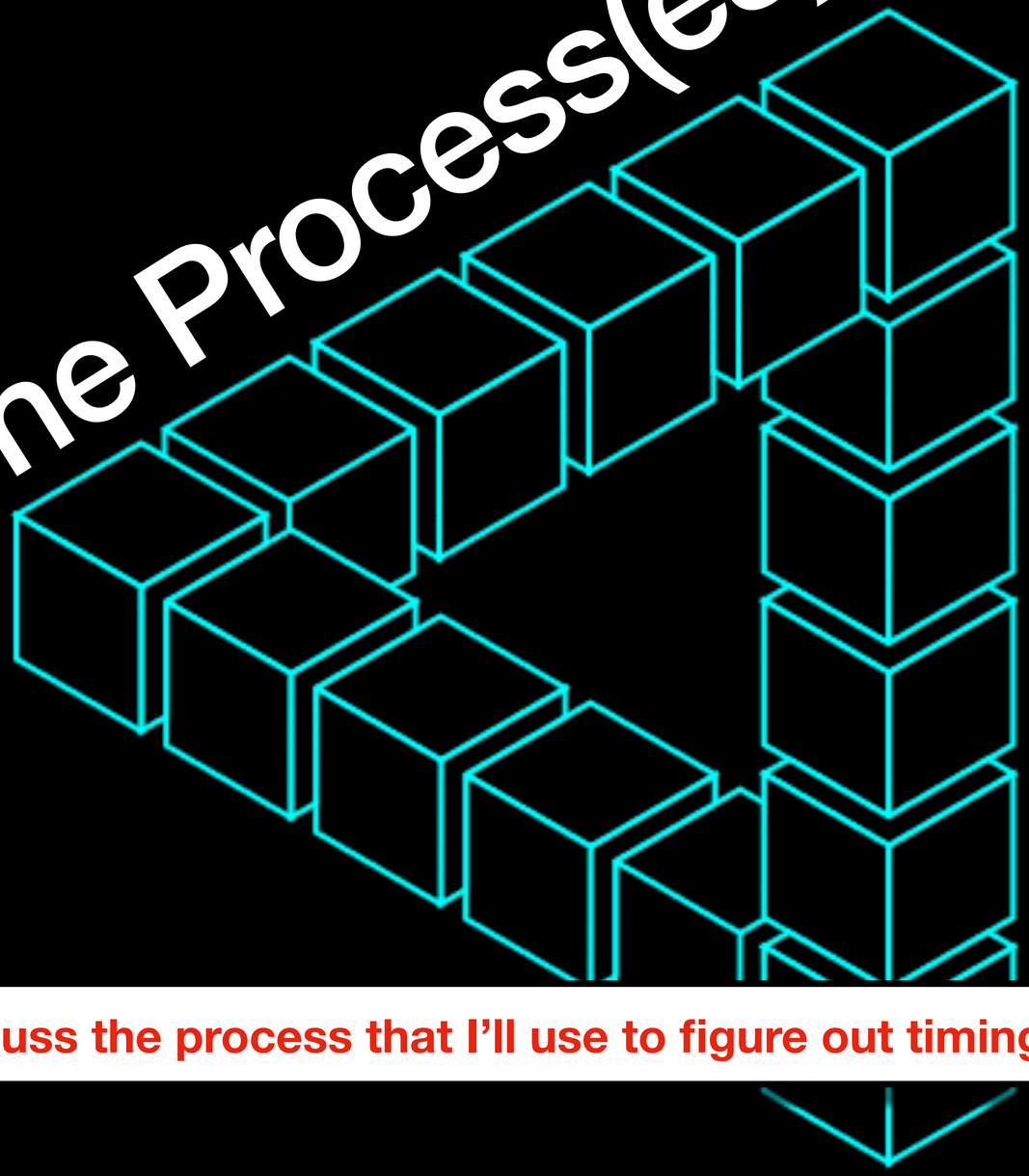
**Notes for the Viewer: The similarities break down earlier in the network traffic.**

Malicious:

```
Difference in microseconds: 93622 (12:56:39.441422 - 12:56:39.535044)
Difference in microseconds: 98 (12:56:39.535044 - 12:56:39.535142)
Difference in microseconds: 159 (12:56:39.535142 - 12:56:39.535301)
Difference in microseconds: 56 (12:56:39.535301 - 12:56:39.535357)
Difference in microseconds: 92677 (12:56:39.535357 - 12:56:39.628034)
Difference in microseconds: 1444 (12:56:39.628034 - 12:56:39.629478)
Difference in microseconds: 21 (12:56:39.629478 - 12:56:39.629499)
```

DEEPSEC

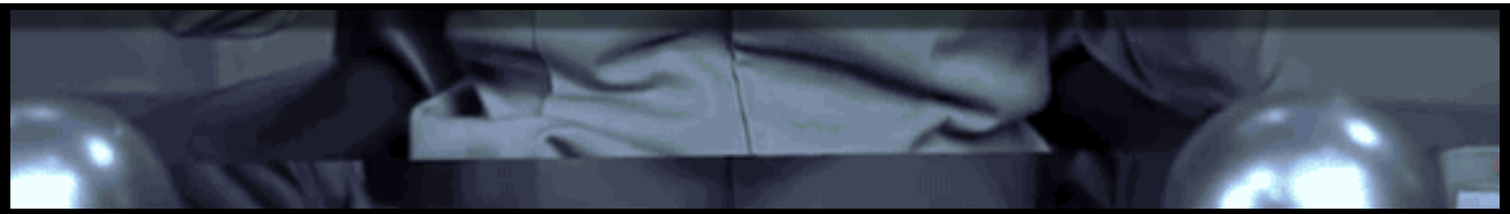
# The Process(es)



Notes for the Viewer: Let’s discuss the process that I’ll use to figure out timing and build a signature.

# Challenges

**Notes for the Viewer:**
**There are a few challenges in the process.**



DEEPSEC

# Finding the Part I'm Interested in…

2022-04-25-Emotet-epoch4-infection-with-spambot-traffic.pcap

Apply a display filter … <⌘/>

| No. | Time | Source | Destination | Protoc | Leng | Info |
|---|---|---|---|---|---|---|
| 1 | 2022-04-25 09:49:34.889906 | 0.0.0.0 | 255.255.255.255 | DHCP | 344 | DHCP Discover - Transaction ID 0x4f27af50 |
| 2 | 2022-04-25 09:49:34.895369 | 10.4.25.1 | 10.4.25.101 | DHCP | 344 | DHCP Offer - Transaction ID 0x4f27af50 |
| 3 | 2022-04-25 09:49:34.896160 | 0.0.0.0 | 255.255.255.255 | DHCP | 394 | DHCP Request - Transaction ID 0x4f27af50 |
| 4 | 2022-04-25 09:49:34.900425 | 10.4.25.1 | 10.4.25.101 | DHCP | 349 | DHCP ACK - Transaction ID 0x4f27af50 |
| 5 | 2022-04-25 09:49:34.911631 | 10.4.25.101 | 224.0.0.22 | IGMPv3 | 60 | Membership Report / Join group 224.0.0.251 for any sources |
| 6 | 2022-04-25 09:49:34.911712 | 10.4.25.101 | 224.0.0.22 | IGMPv3 | 60 | Membership Report / Join group 224.0.0.252 for any sources |
| 7 | 2022-04-25 09:49:34.911767 | HewlettP_1c:47:ae | Broadcast | ARP | 60 | Who has 10.4.25.4? Tell 10.4.25.101 |
| 8 | 2022-04-25 09:49:34.911925 | Dell_c2:09:6a | HewlettP_1c:47:ae | ARP | 60 | 10.4.25.4 is at a4:1f:72:c2:09:6a |
| 9 | 2022-04-25 09:49:34.911953 | 10.4.25.101 | 10.4.25.4 | DNS | 88 | Standard query 0x6eaa A wpad.formulaonefigurines.com |
| 10 | 2022-04-25 09:49:34.912225 | 10.4.25.4 | 10.4.25.101 | DNS | 173 | Standard query response 0x6eaa No such name A wpad.formulaonefigurines.com SOA formulafigs-dc.formulaone |
| 11 | 2022-04-25 09:49:34.913950 | 10.4.25.101 | 224.0.0.22 | IGMPv3 | 60 | Membership Report / Leave group 224.0.0.252 |
| 12 | 2022-04-25 09:49:34.914033 | 10.4.25.101 | 224.0.0.22 | IGMPv3 | 60 | Membership Report / Join group 224.0.0.252 for any sources |
| 13 | 2022-04-25 09:49:34.914384 | 10.4.25.101 | 10.4.25.4 | DNS | 75 | Standard query 0xdfc9 A wpad.mshome.net |
| 14 | 2022-04-25 09:49:34.915872 | 10.4.25.101 | 224.0.0.251 | MDNS | 81 | Standard query 0x0000 ANY DESKTOP-J95JQDS.local, "QM" question |
| 15 | 2022-04-25 09:49:34.916236 | 10.4.25.101 | 224.0.0.252 | LLMNR | 75 | Standard query 0x26f0 ANY DESKTOP-J95JQDS |
| 16 | 2022-04-25 09:49:34.918028 | 10.4.25.101 | 224.0.0.251 | MDNS | 91 | Standard query response 0x0000 A 10.4.25.101 |
| 17 | 2022-04-25 09:49:34.918923 | 10.4.25.101 | 10.4.25.4 | DNS | 135 | Standard query 0xbce1 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.formulaonefigurines.com |
| 18 | 2022-04-25 09:49:34.919368 | 10.4.25.4 | 10.4.25.101 | DNS | 209 | Standard query response 0xbce1 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.formulaonefigurin |
| 19 | 2022-04-25 09:49:34.920641 | 10.4.25.101 | 10.4.25.4 | DNS | 98 | Standard query 0xbd16 A formulafigs-dc.formulaonefigurines.com |
| 20 | 2022-04-25 09:49:34.920879 | 10.4.25.4 | 10.4.25.101 | DNS | 114 | Standard query response 0xbd16 A formulafigs-dc.formulaonefigurines.com A 10.4.25.4 |
| 21 | 2022-04-25 09:49:34.921510 | 10.4.25.101 | 10.4.25.4 | DNS | 104 | Standard query 0x4b25 SRV _ldap._tcp.dc._msdcs.formulaonefigurines.com |
| 22 | 2022-04-25 09:49:34.921838 | 10.4.25.4 | 10.4.25.101 | DNS | 178 | Standard query response 0x4b25 SRV _ldap._tcp.dc._msdcs.formulaonefigurines.com SRV 0 100 389 formulafig |
| 23 | 2022-04-25 09:49:34.923638 | 10.4.25.101 | 10.4.25.4 | DNS | 146 | Standard query 0xf474 SRV _ldap._tcp.e100423e-bd3f-477e-ae13-62deff7ad5f1.domains._msdcs.formulaonefigur |
| 24 | 2022-04-25 09:49:34.924026 | 10.4.25.4 | 10.4.25.101 | DNS | 220 | Standard query response 0xf474 SRV _ldap._tcp.e100423e-bd3f-477e-ae13-62deff7ad5f1.domains._msdcs.formul |
| 25 | 2022-04-25 09:49:34.926645 | 10.4.25.101 | 10.4.25.4 | DNS | 125 | Standard query 0x72eb SRV _ldap._tcp.Default-First-Site-Name._sites.formulaonefigurines.com |
| 26 | 2022-04-25 09:49:34.926925 | 10.4.25.4 | 10.4.25.101 | DNS | 199 | Standard query response 0x72eb SRV _ldap._tcp.Default-First-Site-Name._sites.formulaonefigurines.com SRV |

> Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)

**Notes for the Viewer:**

**Challenge 1: Finding the bad thing I'm interested in and isolating it.**

DEEPSEC

# Acquiring Relevant Threat Traffic

https://www.malware-traffic-analysis.net/2022/index.html

MALWARE-TRAFFIC-ANALYSIS.NET

[ 2013 ] - [ 2014 ] - [ 2015 ] - [ 2016 ] - [ 2017 ] - [ 2018 ] - [ 2019 ] - [ 2020 ] - [ 2021 ] - [ 2022 ]

- 2022-10-10 -- Qakbot (Qbot) infection with Cobalt Strike
- 2022-10- okbot) --> Cobalt Strike

Notes for the Viewer:
Challenge 2: Acquiring the relevant traffic, as in what's relevant to the risks in my network? What's current? Etc… this website, as well as others can be very useful in accomplishing this.

- 2022-09- obalt Strike
- 2022-09- Cobalt Strike
- 2022-09- rom Brazil malspam
- 2022-09- om scans/probes hitting a web server

08- rike

Open Link in New Private Window
Bookmark Link...
Save Link As...
Save Link to Pocket
Copy Link

DEEPSEC

# Once I have a Viable PCAP

| | |
|---|---|
| 2022-10-06-IcedID-and-Cobalt-Strike-malware-and-artifacts | Today at 23:01 |
| [redacted]-file-10.06.2022.html | Today at 23:01 |
| 2022-10-06-gzip-binary-from-didociskal.com.bin | Today at 23:01 |
| 2022-10-06-IOCs-for-IcedID-with-Cobalt-Strike.txt | Today at 23:01 |
| 2022-10-06-scheduled-task-for-IcedID.txt | Today at 23:01 |
| d755ab64-50f8-4faa-bd40-559682f92698.zip | Today at 23:01 |
| 2022-10-06-IcedID-with-Cobalt-Strike-santized-and-carved.pcap | |
| license.dat | Today at 23:01 |
| step_64.dat | Today at 23:01 |
| 2022-10-06-IcedID-with-Cobalt-Strike-santized-and-carved.pcap | Today at 23:01 |
| 2022-10-06-IOCs-for-IcedID-with-Cobalt-Strike | Today at 23:01 |
| 2022-10-06-IOCs-for-IcedID-with-Cobalt-Strike.txt | Today at 23:01 |
| description.txt | Today at 23:01 |

**Notes for the Viewer:**
**I've finally got a PCAP file that contains just a portion of the bad traffic I want to build a signature from.**

DEEPSEC

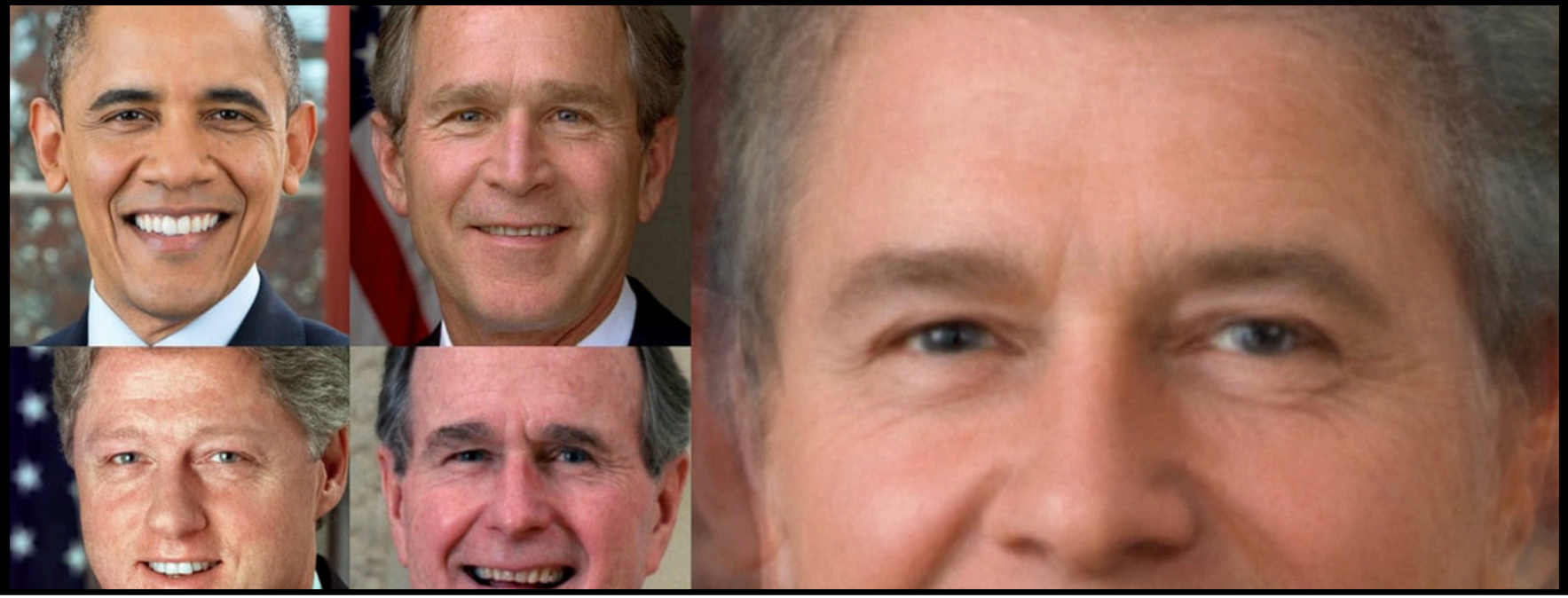
# Isolated Trickbot POST from a larger PCAP

*TrickBot 1*

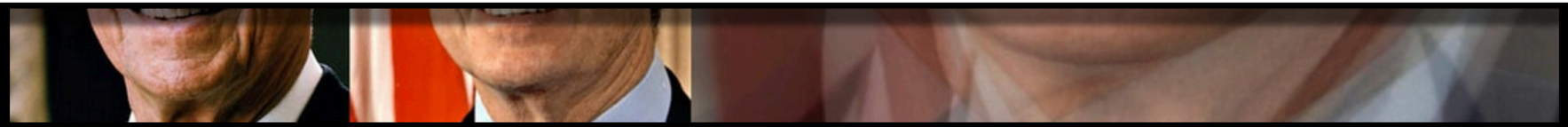
| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 0.000247 | 10.9.30.101 | 80.87.201.221 | HTTP | 478 | POST /pIXPXFus4dL9VHy/Ae4QuOOcWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/ HTTP/1.1 |
| 78 | 1.699744 | 80.87.201.221 | 10.9.30.101 | HTTP | 396 | HTTP/1.1 200 OK (text/html) |
| 83 | 1.706418 | 10.9.30.101 | 80.87.201.221 | HTTP | 478 | POST /HZn5Um1RGxgZ4AC5/BW8yR5/RHTBz5XxAFoC/ivnOvfar/Xq6HEyvjsyv0U/ HTTP/1.1 |
| 321 | 4.434370 | 80.87.201.221 | 10.9.30.101 | HTTP | 311 | HTTP/1.1 200 OK (text/html) |
| 326 | 4.442984 | 10.9.30.101 | 80.87.201.221 | HTTP | 478 | POST /CICnqOruETzlLi/Bd5APHiVCt4zWEU/KDsFyce3t5NTCuNWc/ HTTP/1.1 |
| 343 | 5.289803 | 80.87.201.221 | 10.9.30.101 | HTTP | 220 | HTTP/1.1 200 OK (text/html) |
| 348 | 5.299435 | 10.9.30.101 | 80.87.201.221 | HTTP | 478 | POST /hucUozNM1/kIARs4tFzz2LgSrAenQ/kqcmV0gVM6g/btrh6lz8jsMOF8/ HTTP/1.1 |
| 459 | 10.289254 | 80.87.201.221 | 10.9.30.101 | HTTP | 1369 | HTTP/1.1 200 OK (text/html) |
| 464 | 10.295713 | 10.9.30.101 | 80.87.201.221 | HTTP | 494 | POST /B1GC6eAbxy4DL71le/A5lrsR/ZTF0jhiNTGWIuSShlZR/lZJh2BIiq2hRZ5/lrq6gLJguipxQCN/P1yEI/ HTTP/1.1 |
| 577 | 12.092188 | 80.87.201.221 | 10.9.30.101 | HTTP | 663 | HTTP/1.1 200 OK (text/html) |
| 582 | 12.099466 | 10.9.30.101 | 80.87.201.221 | HTTP | 494 | POST /vlddDI/QAmLy/zGRph9CuZ3/ HTTP/1.1 |
| 834 | 15.375483 | 80.87.201.221 | 10.9.30.101 | HTTP | 444 | HTTP/1.1 200 OK (text/html) |
| 839 | 15.388285 | 10.9.30.101 | 80.87.201.221 | HTTP | 526 | POST /duJg5C1/xFUO1X4gXH/DmmM6AOJa4mihFadzyh/LnSnCuyOO2TpiJ/oHTysVuVbyi422DaAg/422SlS/ HTTP/1.1 |

**Notes for the Viewer:**
**I've finally got a PCAP file that contains just a portion of the bad traffic I want to build a signature from. I'm not worried about having multiple POSTs. It doesn't have to be perfect. I just don't want 'clean' traffic in there.**

# Averages



**Notes for the Viewer:**
**We've looked at the time in between network transactions - now let's try getting the average of all of those times. The idea is that some PCAP files will contain possibly thousands of transactions while others contain maybe only a few.**



# Calculate time in between transactions

```
Time between queries:
Difference in microseconds: 228 (09:50:16.806957 - 09:50:16.807185)
Difference in microseconds: 10 (09:50:16.807185 - 09:50:16.807195)
Difference in microseconds: 5 (09:50:16.807195 - 09:50:16.807200)
Difference in microseconds: 4 (09:50:16.807200 - 09:50:16.807204)
Difference in microseconds: 783585 (09:50:16.807204 - 09:50:17.590789)
Difference in microseconds: 738 (09:50:17.590789 - 09:50:17.591527)
Difference in microseconds: 145 (09:50:17.591527 - 09:50:17.591672)
Difference in microseconds: 21950 (09:50:17.591672 - 09:50:17.613622)
Difference in microseconds: 738 (09:50:17.613622 - 09:50:17.614360)
Difference in microseconds: 209422 (09:50:17.614360 - 09:50:17.823782)
Difference in microseconds: 129985 (09:50:17.823782 - 09:50:17.953767)
Difference in microseconds: 841 (09:50:17.953767 - 09:50:17.954608)
Difference in microseconds: 4351 (09:50:17.954608 - 09:50:17.958959)
```

**Notes for the Viewer:**

**1: Get the microseconds between transactions.**

```
Difference in microseconds: 102 (09:50:17.975335 - 09:50:17.975437)
Difference in microseconds: 67007 (09:50:17.975437 - 09:50:18.042444)
Difference in microseconds: 11647 (09:50:18.042444 - 09:50:18.054091)
```

```
Total Queries: 840
```

DEEPSEC

# Get all the Microseconds of those times

```
[228, 10, 5, 4, 783585, 738, 145, 21950, 738, 209422, 129985, 841, 4351, 851, 15150, 190, 185, 102, 67007, 11647, 12485, 146142, 123, 355, 175, 30, 237, 771, 62, 266,
745, 98, 142, 2384, 702, 135, 196, 44370, 629, 57793, 749, 11, 222, 130906, 942, 7216, 695, 301, 25, 811, 146, 7885, 898, 159, 87, 345, 18, 20649, 119, 271, 8, 337, 13
23, 824, 227, 14, 773, 6888, 718, 148, 239, 23, 251, 152, 167, 216, 7, 6583, 72, 9, 4, 6, 707215, 791, 102, 35053, 120, 153, 153, 121, 13125, 46462, 719, 133, 16071, 7
43, 100, 22161, 17049, 750, 3613, 810, 101, 13979, 16223, 90, 3719, 825, 176, 39487, 698, 168, 407973, 809, 102, 200, 89, 169, 191, 172, 160, 186, 152, 184, 155, 114,
159, 163, 174, 164, 214, 104, 222, 168, 114, 133, 279, 167, 94, 162, 209, 88, 165, 177, 207, 105, 2936, 134, 182, 100, 165, 153, 149, 194, 143, 169, 182, 151, 150, 202
, 149, 168, 174, 139, 464, 21, 354030, 9, 233, 206, 255, 16, 43, 278, 121, 137, 229, 78, 206, 184, 171, 151, 152, 76, 276, 184, 152, 146, 182, 98, 224, 135, 189, 150,
159, 156, 193, 145, 179, 1407, 157, 144, 170, 166, 160, 183, 126, 184, 187778, 704, 187, 9450, 722, 107, 219, 100, 171, 157, 161, 771, 173, 170, 1201, 154, 190, 122, 1
98, 1288, 169, 765, 162, 1975, 153, 176, 19183, 55, 287, 40, 220, 126, 107, 290, 177, 13, 269, 168, 170, 73113, 594, 194, 44, 183, 216, 105, 933, 107, 34837, 728, 139,
 37418, 829, 154, 62151, 178, 67, 24524, 793, 114, 45977, 765, 1709, 22937, 697, 132, 39130, 767, 137, 27822, 723, 139, 51946, 95, 54, 8008, 838, 58, 6265, 771, 147, 4
6732, 1662, 167, 14968, 796, 157, 49576, 84, 170, 14163, 851, 13586, 7895, 9605, 841, 20327, 122, 138, 21636, 704, 75, 123528, 144, 102, 179, 292, 8, 1297, 194, 80, 8,
 8492, 96, 15, 7, 4, 700859, 753, 101, 37864, 791, 115, 92451, 15, 118, 10629, 727, 58, 1838, 125, 197, 170, 8, 9506, 105, 9, 6, 6, 754535, 24, 17, 36, 405, 158, 23, 1
63, 8, 262, 306764, 60, 18, 517, 21, 142, 29, 24, 328, 7, 166, 244, 304642, 8, 21, 509, 22, 155, 7, 74, 203, 153, 144, 230, 194, 184, 155, 97, 184, 184, 314520, 10, 8,
 338, 21, 183, 116, 118, 217, 172, 124, 178, 164, 279, 19, 187, 199, 49, 276, 152, 155, 170, 147, 72, 285, 153, 145, 165, 151, 171, 168, 150, 168, 292482, 38, 23, 264,
 18, 200, 229, 21, 231, 227, 49, 229, 164, 139, 59, 235, 147, 159, 177, 162, 158, 155, 201, 170, 108, 232, 153, 140, 184, 149, 165, 189, 132, 1247, 157, 134, 178, 167,
 6337, 77, 14, 16, 15, 954626, 91, 215, 19916, 646, 186, 45735, 259, 10200, 693, 972, 115, 19967, 816, 64, 355884, 2902, 85, 91, 298, 233, 10, 2887, 56, 257, 10, 271,
205, 11, 230, 221, 768, 158, 774, 170, 868, 61, 14336, 45, 143, 373, 12, 44, 246, 185, 168, 138, 13935, 47, 230, 213, 19, 230, 187, 192, 10, 382, 11, 163, 210, 3671, 7
26, 131, 31349, 823, 58, 30361, 91, 202, 3197, 814, 188, 26773, 605, 172, 99948, 12, 182, 106, 249, 70, 340, 23, 256, 8, 261, 159, 278, 34, 169, 16559, 730, 137, 16474
, 716, 191, 27928, 91, 174, 15332, 81, 246, 19381, 692, 203, 10125, 761, 9049, 4184, 125, 253, 19288, 29, 7078, 146, 33, 12, 9, 750988, 87, 178, 18970, 63, 213, 38524,
, 9, 10, 7, 66, 11, 26, 8, 7, 9, 10, 20, 10, 7, 12637, 128, 7, 27, 3, 985891]
```

**Notes for the Viewer:**
**2: and put them in a list**

DEEPSEC

# Get all the Microseconds of those times


**Notes for the Viewer:**
**This list is the entire length of the PCAP.**

DEEPSEC

# Find the Average

```
sum_of_trickbot1 = sum(trickbot1)
average_of_microseconds_trickbot1 = sum_of_trickbot1 / len(trickbot1)
```

14748.719904648391

**Notes for the Viewer:**
**3: Calculate the average of all of those microseconds.**

# Again with Another PCAP

```
Time between queries:
Difference in microseconds: 228 (09:50:16.806957 - 09:50:16.807185)
Difference in microseconds: 10 (09:50:16.807185 - 09:50:16.807195)
Difference in microseconds: 5 (09:50:16.807195 - 09:50:16.807200)
Difference in microseconds: 4 (09:50:16.807200 - 09:50:16.807204)
Difference in microseconds: 783585 (09:50:16.807204 - 09:50:17.590789)
Difference in microseconds: 738 (09:50:17.590789 - 09:50:17.591527)
Difference in microseconds: 145 (09:50:17.591527 - 09:50:17.591672)
Difference in microseconds: 21950 (09:50:17.591672 - 09:50:17.613622)
Difference in microseconds: 738 (09:50:17.613622 - 09:50:17.614360)
Difference in microseconds: 209422 (09:50:17.614360 - 09:50:17.823782)
Difference in microseconds: 129985 (09:50:17.823782 - 09:50:17.953767)
Difference in microseconds: 841 (09:50:17.953767 - 09:50:17.954608)
Difference in microseconds: 4351 (09:50:17.954608 - 09:50:17.958959)
Difference in microseconds: 851 (09:50:17.958959 - 09:50:17.959810)
Difference in microseconds: 15150 (09:50:17.959810 - 09:50:17.974960)
Difference in microseconds: 190 (09:50:17.974960 - 09:50:17.975150)
Difference in microseconds: 185 (09:50:17.975150 - 09:50:17.975335)
Difference in microseconds: 102 (09:50:17.975335 - 09:50:17.975437)
Difference in microseconds: 67007 (09:50:17.975437 - 09:50:18.042444)
Difference in microseconds: 11647 (09:50:18.042444 - 09:50:18.054091)
```

# Isolated Trickbot POST

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 6 | 0.000135 | 10.12.29.101 | 189.34.18.252 | HTTP | 1258 | POST /tqg9o/ikxapt5fx226p47wwsd/3tfkg3j/07x0v0hpn2d919md3/ HTTP/1.1 |
| 1101 | 16.946285 | 189.34.18.252 | 10.12.29.101 | HTTP | 1015 | HTTP/1.1 200 OK (text/html) |
| 1106 | 16.959638 | 10.12.29.101 | 189.34.18.252 | HTTP | 1486 | POST /xomdq50t/se7srsiitec3m/f54e1juni4kuk7fjb/t99r946mvo/4okinw5f6ydnhll/ HTTP/1.1 |
| 2224 | 33.285627 | 189.34.18.252 | 10.12.29.101 | HTTP | 609 | HTTP/1.1 200 OK (text/html) |
| 2230 | 33.302493 | 10.12.29.101 | 189.34.18.252 | HTTP | 1018 | POST /bkynd5lifqfsi52b/uv7prprsl/3sppbt6b5vy7kmzb3/v5djoxr/4ffc8gdir/ HTTP/1.1 |
| 2415 | 38.493605 | 189.34.18.252 | 10.12.29.101 | HTTP | 157 | HTTP/1.1 200 OK (text/html) |
| 2421 | 38.502688 | 10.12.29.101 | 189.34.18.252 | HTTP | 74 | POST /wjg8qaqd7v5a1963ris/3une6mc1wpq/p701bp/2rue8040hzdt4/f8jppv/o1yjc7bglajqueh4/ HTTP/1.1 |
| 2665 | 42.838930 | 189.34.18.252 | 10.12.29.101 | HTTP | 563 | HTTP/1.1 200 OK (text/html) |
| 2671 | 42.852352 | 10.12.29.101 | 189.34.18.252 | HTTP | 1370 | POST /n74ib0xs4u/gwu50m6qpx2j2emq/hq2xxkl10fvht/ HTTP/1.1 |
| 2897 | 48.905648 | 189.34.18.252 | 10.12.29.101 | HTTP | 288 | HTTP/1.1 200 OK (text/html) |
| 2903 | 48.917313 | 10.12.29.101 | 189.34.18.252 | HTTP | 1290 | POST /jpksx0k4h/x6w356jvwlgq7x/fjgjxvec/df1fu0by8pfkm/rifmu7/msrdq8wu/ HTTP/1.1 |
| 2905 | 49.827338 | 189.34.18.252 | 10.12.29.101 | HTTP | 1042 | HTTP/1.1 200 OK (text/html) |

Total Queries: 2905

# PCAP 1:

TrickBot 1 (20200930_trickbotpost.pcap)

Total Queries: 840

# PCAP 2:

TrickBot 2 (20201229_trickbotpost.pcap)

Total Queries: 2905

**Notes for the Viewer:**
**Compare two similar PCAPs, both with a very different number of total transactions (I called them queries for some reason)**

## PCAP 1:

TrickBot 1 (20200930_trickbotpost.pcap)

Total Queries: 840

Average: 14748.719904648391

## PCAP 2:

TrickBot 2 (20201229_trickbotpost.pcap)

Total Queries: 2905

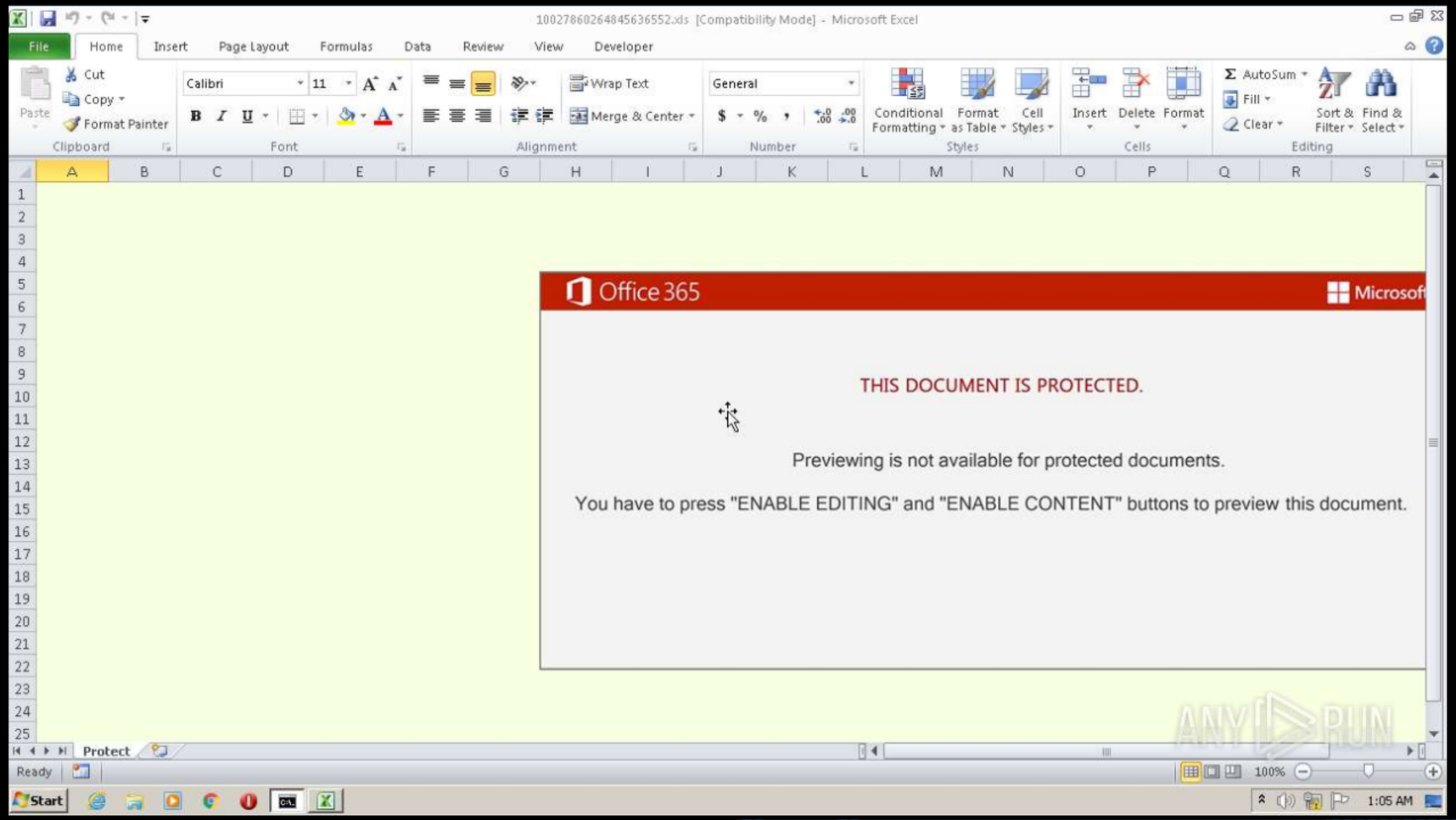
Average: 16125.116391184572

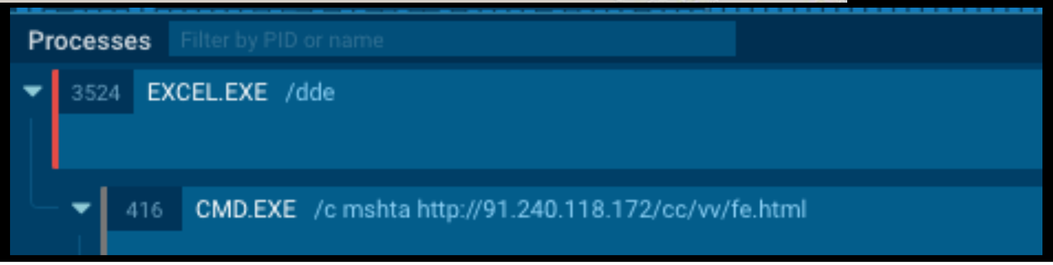
**Notes for the Viewer:**
**The average is not close out of context with other data that we'll see in a the next few slides, but for now they're somewhat close…**

DEE

# Emotet GET requests

**Notes for the Viewer:**
**Trying with Emotet GET requests**




**Notes for the Viewer:**
**I took a bunch of Emotet samples from the same campaign.**

8559dde7-764a-47ab-844e-9e1881a99e9a.pcap
Average between queries: 144,443
Total Queries: 16

76efeed5-e608-49de-81f6-4f5356c4641a.pcap
Average between queries: 9,747
Total Queries: 5450

ad85a-cebc-4425-b428-7a1707d8d80e.pcap
Average between queries: 5,574
Total Queries: 5

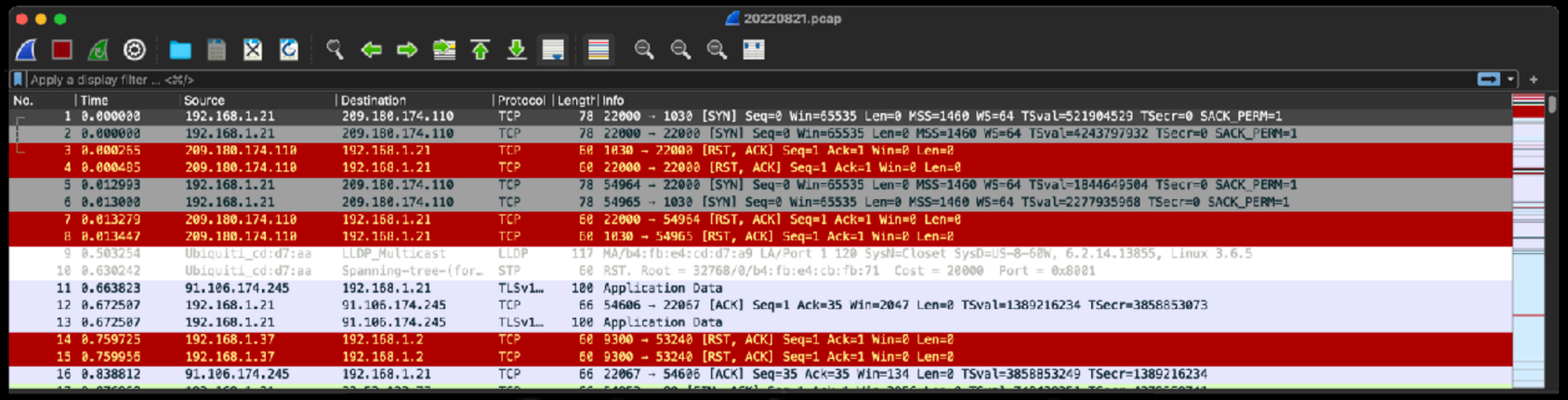
d74dfa64-f9bc-4696-b4f3-a66f329e0b27.pcap
Average between queries: 3,804
Total Queries: 3425

**Notes for the Viewer:**
**I took a bunch of Emotet samples from the same campaign. Some are close, while the first isn't.**

# Compare Against Random Traffic

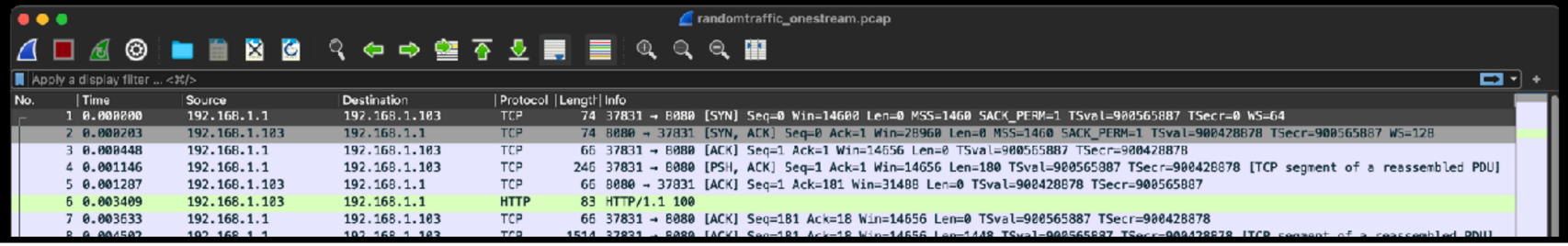
**Notes for the Viewer:**
**Let’s put some random traffic in the mix**

# Multiple Flows of Random Traffic

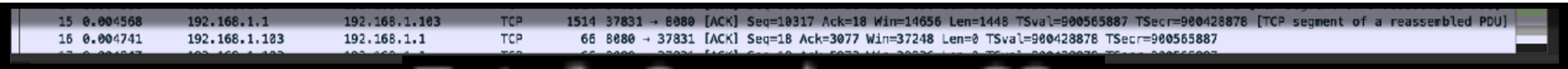



Total Queries: 779

# One Flow from this Traffic




**Notes for the Viewer: Use a full PCAP with many network flows, and also take one flow from that PCAP to use.**




Total Queries: 32

DEEPSEC

```
14748.719904648391:     Trickbot POST 1
16125.116391184572:     Trickbot POST 2
8356.612903225807:      Random Traffic, one stream
72144.2343387471:       Random Traffic, full stream
```

**Notes for the Viewer:**
**The two Trickbot averages of times in between look a lot closer now to each other than they do with the random traffic. Maybe this is a good direction to go?**

DEEPSEC

Find a sample of something I know is bad:

https://www.malware-traffic-analysis.net/2022/04/25/index.html

MALWARE-TRAFFIC-ANALYSIS.NET

## 2022-04-25 (MONDAY) - EMOTET EPOCH 4 ACTIVITY (LNK FILES)

REFERENCE:

- **https://twitter.com/Cryptolaemus1/status/1517634855940632576**

ASSOCIATED FILES:

- **2022-04-25-IOCs-for-Emotet-epoch4.txt.zip** 2.3 kB (2,302 bytes)
- **2022-04-25-Emotet-epoch4-malspam-10-examples.zip** 46.0 kB (45,961 bytes)
- **2022-04-25-Emotet-epoch4-attachments.zip** 37.0 kB (37,037 bytes)
- **2022-04-25-Emotet-epoch4-infection-with-spambot-traffic.pcap.zip** 8.5 MB (8,495,143 bytes)
- **2022-04-25-Emotet-epoch4-malware-and-artifacts.zip** 299 kB (298,940 bytes)

**Notes for the Viewer:**
**Trying again with another sample to see I get similar results. This time a GET request for Emotet.**



https://www.malware-traffic-analysis.net/2022/04/25/index.html

| Time | Dst | port | Host | Info |
|---|---|---|---|---|
| 2022-04-25 16:50:14 | 77.105.36.156 | 80 | filmmogzivota.rs | GET /SprvAssets/gDR/ HTTP/1.1 |
| 2022-04-25 16:51:07 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:51:09 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:51:34 | 49.231.16.102 | 8080 | | Client Hello |
| 2022-04-25 16:51:36 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:51:58 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:52:00 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:52:01 | 93.104.209.56 | 8080 | | Client Hello |
| 2022-04-25 16:52:23 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:52:46 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:52:49 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:52:49 | 131.100.24.199 | 7080 | | Client Hello |
| 2022-04-25 16:53:15 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:53:40 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:53:43 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:53:43 | 51.210.176.76 | 443 | | Client Hello |
| 2022-04-25 16:54:08 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:54:36 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:54:37 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:54:39 | 49.231.16.102 | 8080 | | Client Hello |
| 2022-04-25 16:55:04 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:55:31 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:55:33 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:56:02 | 138.197.147.101 | 443 | | Client Hello |
| 2022-04-25 16:56:05 | 138.197.147.101 | 443 | | Client Hello |

EMOTET DLL

EMOTET C2 TRAFFIC

**Notes for the Viewer:**
**Trying again with another sample to see I get similar results. This time a GET request for Emotet.**



https://www.malware-traffic-analysis.net/2022/04/25/index.html

```
TCP        66  49797 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

Wireshark · Follow TCP Stream (tcp.stream eq 21) · 2022-04-25-Emotet-epoch4-infection-with-spamb

```
GET /SpryAssets/gDR/ HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: vBKbaQgjyvRRbcgfvlsc
Host: filmmogzivota.rs

HTTP/1.1 200 OK
Date: Mon, 25 Apr 2022 16:49:52 GMT
Server: Apache
X-Powered-By: PHP/5.6.40
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 25 Apr 2022 16:49:52 GMT
Content-Disposition: attachment; filename="TfBXbg6gEAqeHioMEKOtCAAn73.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 6266d1304df16=1650905392; expires=Mon, 25-Apr-2022 16:50:52 GMT; Max-Age=60; path=/
Last-Modified: Mon, 25 Apr 2022 16:49:52 GMT
Content-Length: 543744
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload

MZ.......................@.......................................          .!..L.!This program cannot be run
in DOS mode.
```

**Notes for the Viewer:**
**Take the whole PCAP, and just grab the part I want (the flow containing the GET request)**

# Another PCAP with similar activity

```
GET /video/6JvA8/ HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: gandhitoday.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 20 Apr 2022 21:33:04 GMT
Server: Apache
X-Powered-By: PHP/5.6.40
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Wed, 20 Apr 2022 21:33:04 GMT
Content-Disposition: attachment; filename="EGh7x6aKN3ILP.dll"
Content-Transfer-Encoding: binary
```

**Notes for the Viewer:**
**Grab the part I want (the flow containing the GET request) from a similar, but different PCAP**

```
MZ.......................@.......................................        .!..L.!This program cannot be run
in DOS mode.
```

*2022-04-20-Emotet-epoch4-infection-with-spambot-traffic.pcap*

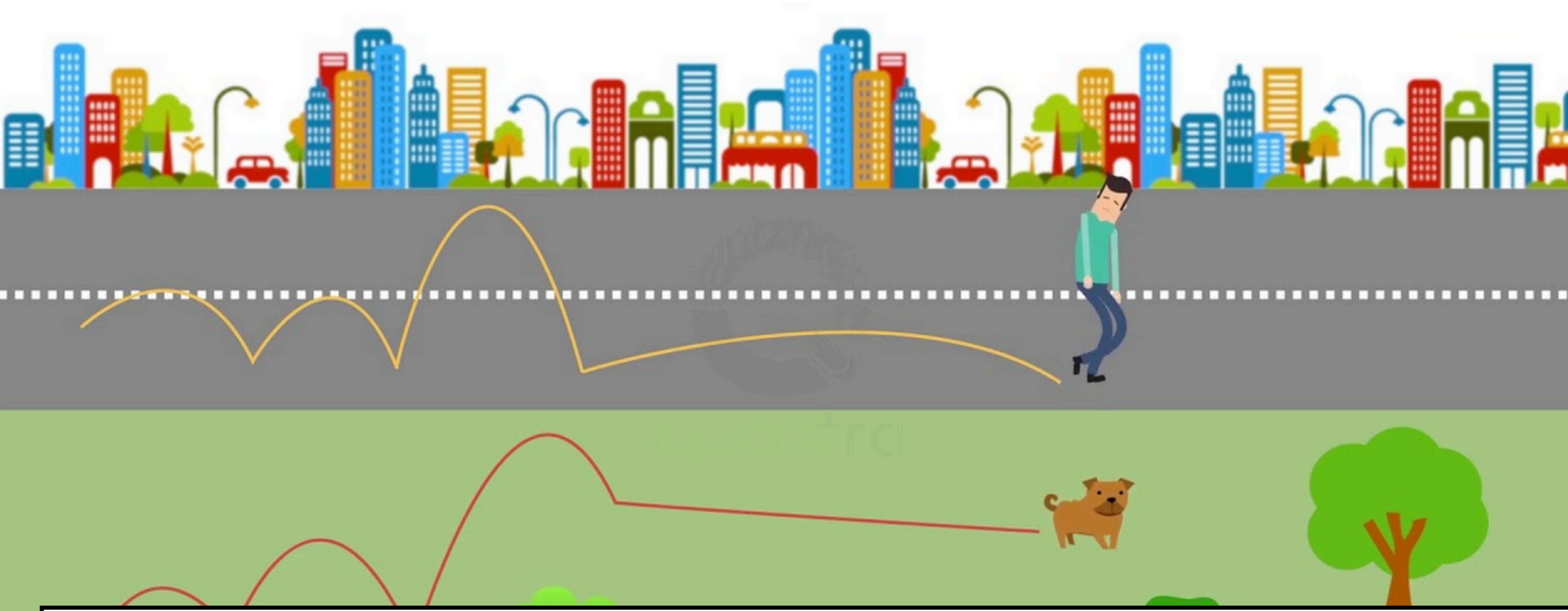
# The GET request: Not Really Matching

```
2022-04-20-Emotet-epoch4-dll_download_0.cap
    Average beteen queries: 8598.687198067633
    Total Queries: 829
##############
1 Flows in 2022-04-20-Emotet-epoch4-dll_download.pcap
##############
```

```
2022-04-25-Emotet-epoch4-dll_download_0.cap
    Average beteen queries: 3529.211367673179
    Total Queries: 564
##############
1 Flows in 2022-04-25-Emotet-epoch4-dll_download.pcap
##############
```

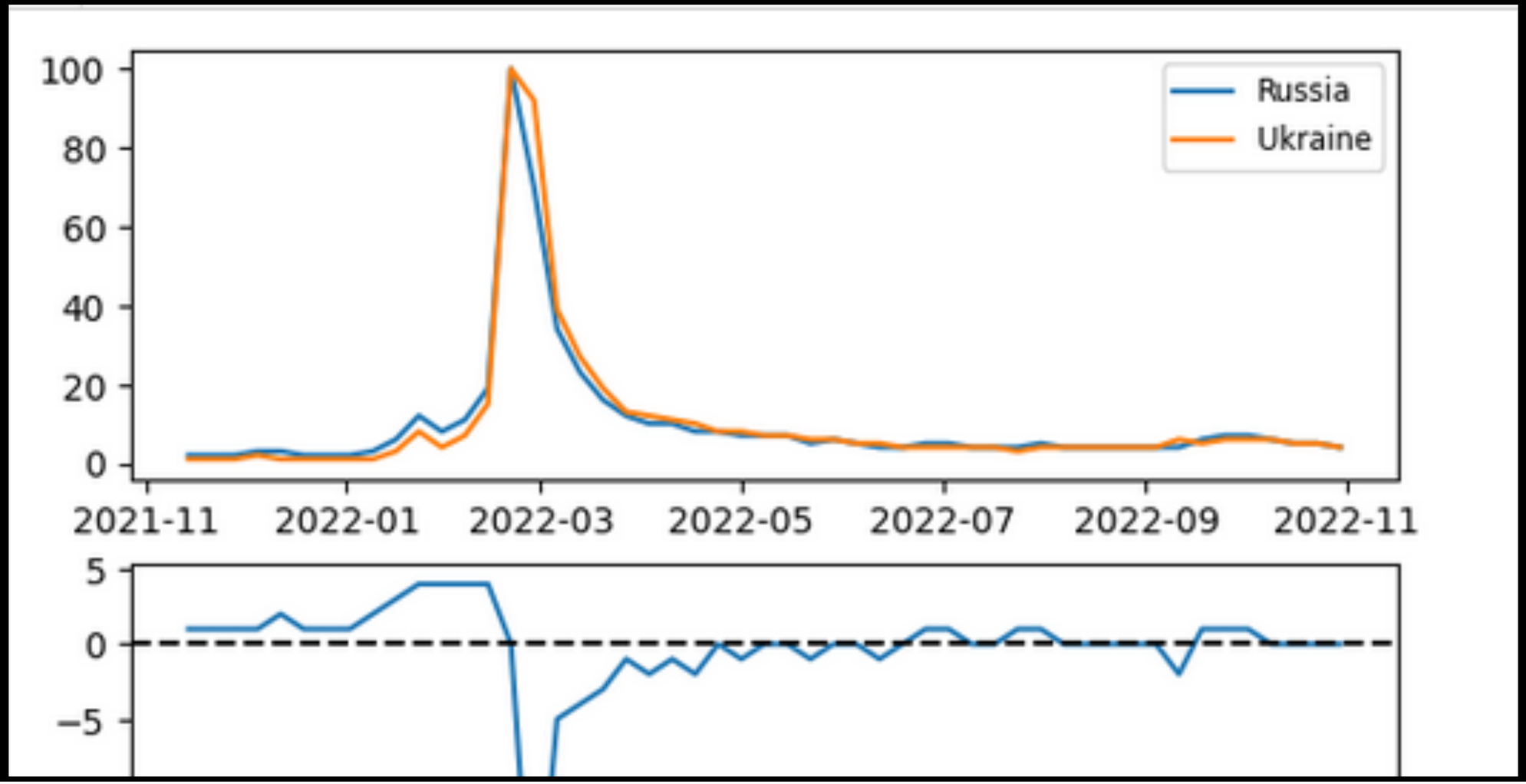
**Notes for the Viewer:**
**They aren't matching very well this time. Maybe this isn't the best direction**

# Cointegration



**Notes for the Viewer: New attempt, Cointegration. The idea behind it:**

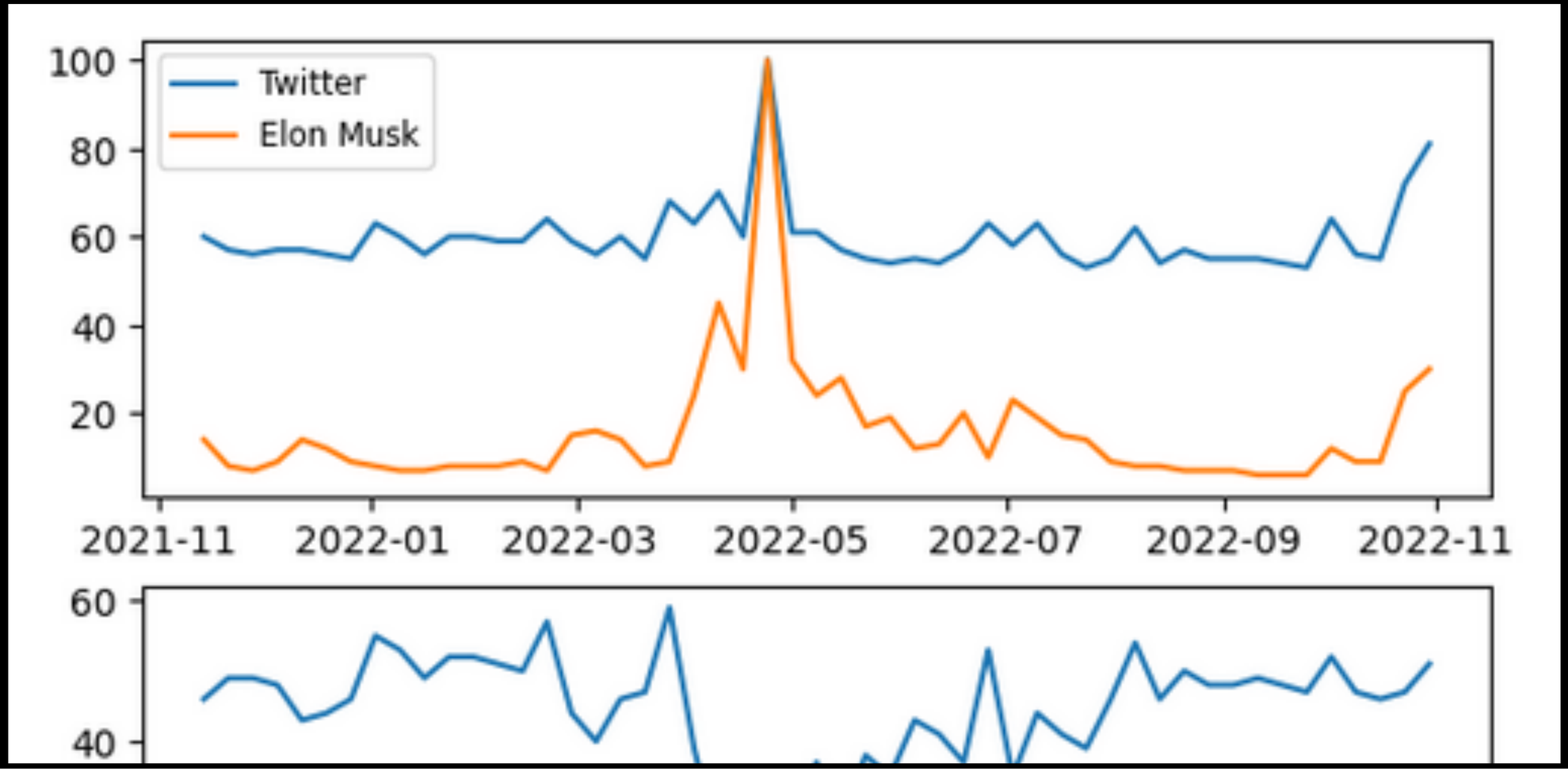
**Drunk guy and a dog are walking the same direction. They look like they might be together. That's correlation, but then if they start to drift apart, maybe they aren't together. So their timeline looks to be the same, but if they aren't going the same direction, they aren't cointegrated. If they do continue walking together, eventually it can be assumed that they are together, aka cointegrated.**



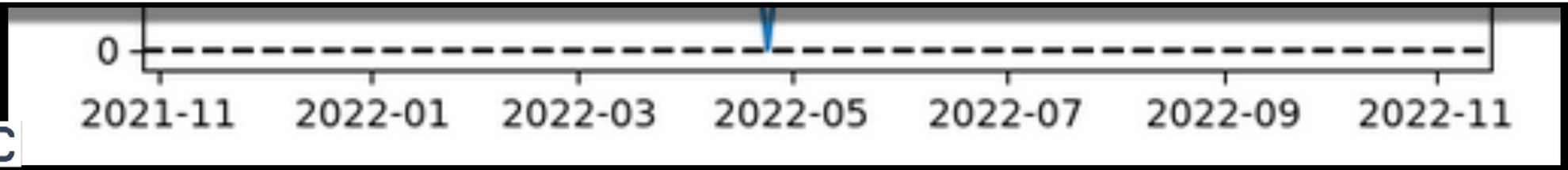

**Notes for the Viewer: Conintegration example #1, just to understand.**
**Google searches over one year for 'Russia' and 'Ukraine'. They look like they're together. The bottom graph (called 'the spread') primarily stays on 0, showing they are also cointegrating. So the searches correlate AND cointegrate**

2021-11 2022-01 2022-03 2022-05 2022-07 2022-09 2022-11

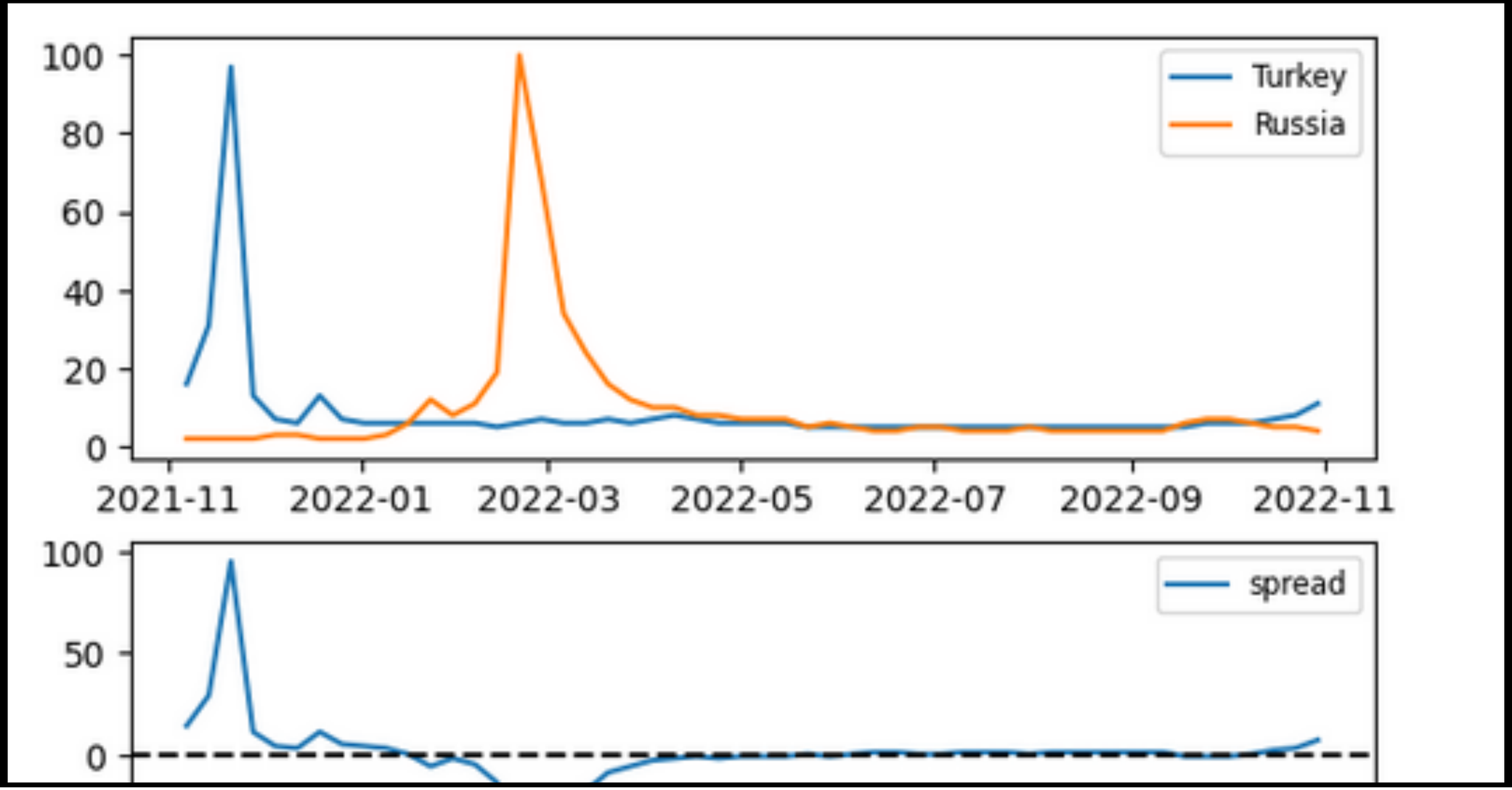
DEEPSEC




**Notes for the Viewer: Conintegration example #2, just to understand.**
**Google searches over one year for ‘Twitter’ and ‘Elon Musk’. They look like they correlate, but the spread doesn’t quite show a relationship since it’s not primarily staying on 0. So the searches correlate but do not cointegrate**

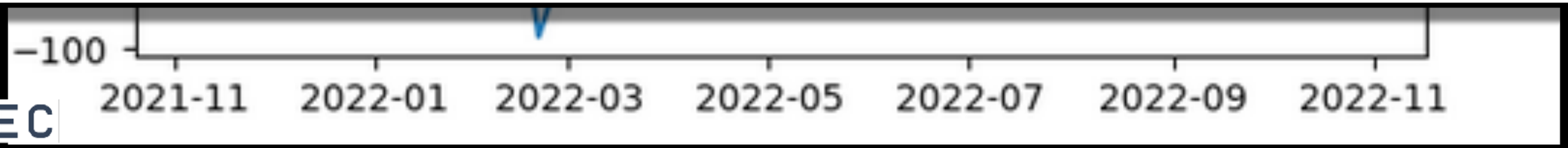



DEEPSEC

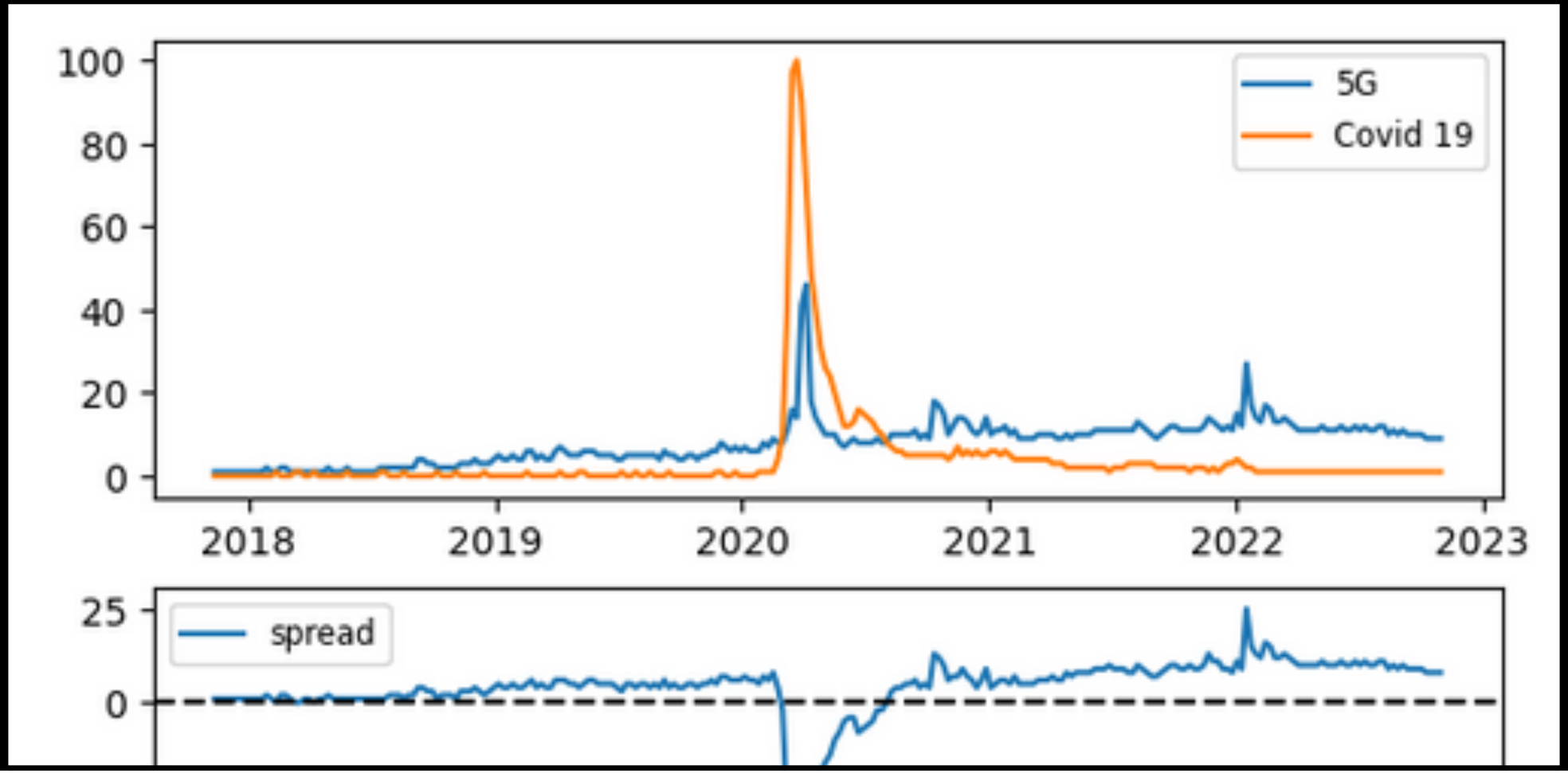



**Notes for the Viewer: Cointegration example #3, just to understand.**

**Google searches over one year for 'Turkey' and 'Russia'. They don't look like they're lining up, suggesting no correlation. The spread however primarily stays on 0, showing they are cointegrating. So the timelines are similar/matching.**

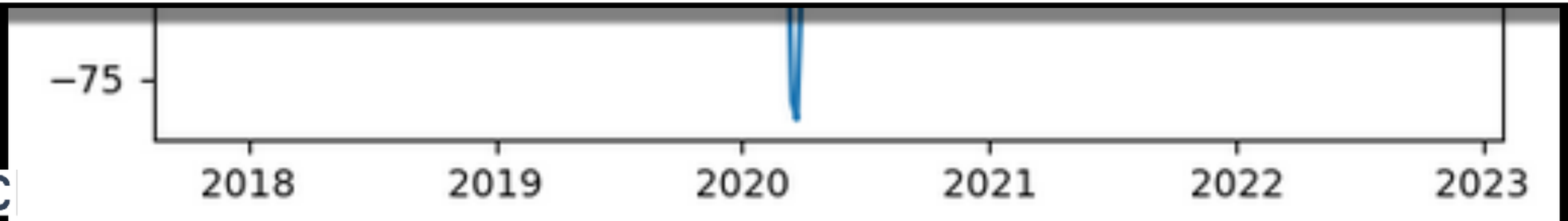



DEEPSEC




**Notes for the Viewer: Conintegration example #4, just to understand.**

**Google searches over one year for ‘5G’ and ‘Covid 19’. Timelines line up and the spread stays on 0. Unfortunately, google searches for 5G and Covid 19 cointegrate and correlate.**

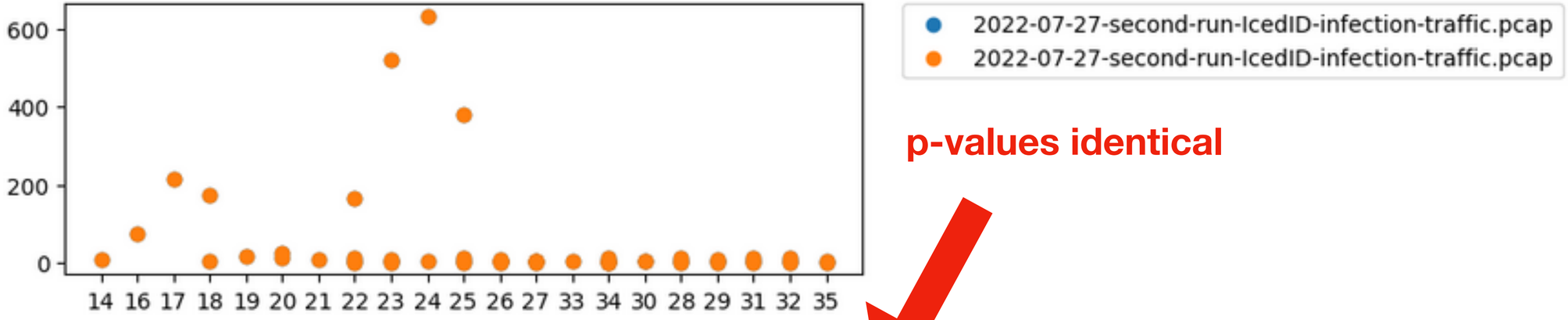



DEEPSEC

Two identical PCAP files
They should cointegrate

# Identical PCAP files: 100% Cointegration

```
file1='2022-07-27-second-run-IcedID-infection-traffic.pcap'
file2='2022-07-27-second-run-IcedID-infection-traffic.pcap'
```

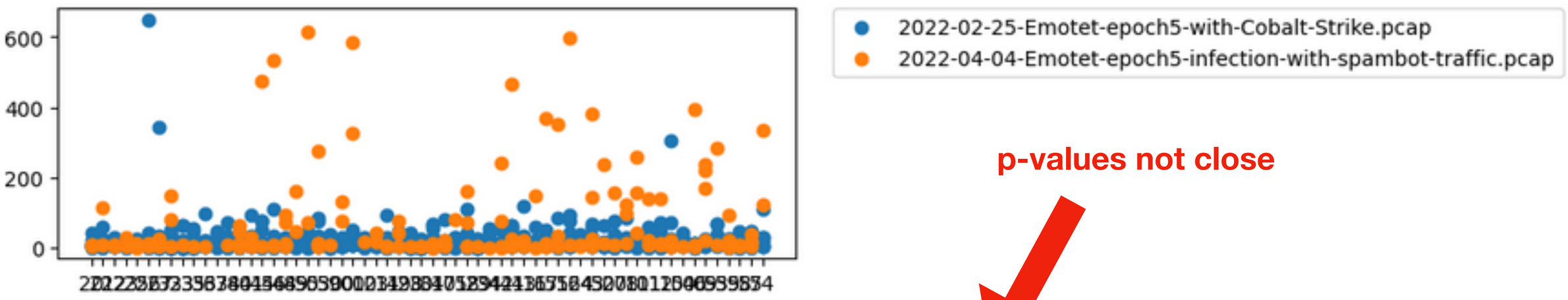



**p-values identical**

```
p-value for file1:  0.06304175482717005
p-value for file2:  0.06304175482717005
```

Two different PCAP files
They should not cointegrate

# Two different PCAP files: No Cointegration




p-values not close

```
p-value for file1:  8.217878712201338e-09
p-value for file2:  0.3893690552236816
```

**Notes for the Viewer:**
**Two pcaps that seem similar, but are actually following different timelines. They likely won't cointegrate. There is likely too much going on in these since they are full packet captures with all the flows.**

But now there’s a method to start finding similarities

Two different PCAP files
With similar traffic

# Two PCAP files: Similar Traffic

.stream eq 2

| | Time | Source | Destination | Protoc | Le |
|---|---|---|---|---|---|
| 21 | 0.350055 | 192.168.100.102 | 93.184.220.29 | HTTP | 2 |
| 22 | 0.362456 | 93.184.220.29 | 192.168.100.102 | TCP | 12 |
| 23 | 0.362496 | 93.184.220.29 | 192.168.100.102 | TCP | 2 |
| 24 | 0.362522 | 93.184.220.29 | 192.168.100.102 | OCSP | 3 |
| 25 | 0.407985 | 192.168.100.102 | 93.184.220.29 | HTTP | 2 |
| 26 | 0.439880 | 93.184.220.29 | 192.168.100.102 | OCSP | 5 |

```
GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: ocsp.digicert.com

HTTP/1.1 200 OK
Accept-Ranges: bytes
Age: 4679
Cache-Control: 'max-age=158059'
Content-Type: application/ocsp-response
Date: Mon, 19 Sep 2022 03:49:48 GMT
Last-Modified: Mon, 19 Sep 2022 02:31:49 GMT
Server: ECS (amb/6B86)
X-Cache: HIT
Content-Length: 1507
```

tcp.stream eq 0

| | Time | Source | Destination | Protoc | Ler |
|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.100.205 | 93.184.221.240 | HTTP | 34 |
| 3 | 0.060479 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 4 | 0.060520 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 5 | 0.060537 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 6 | 0.061314 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 7 | 0.062094 | 93.184.221.240 | 192.168.100.205 | HTTP | 39 |
| 24 | 9.347911 | 192.168.100.205 | 93.184.221.240 | HTTP | 24 |
| 25 | 9.390606 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 26 | 9. | | | | |
| 27 | 9. | | | | |
| 28 | 9. | | | | |
| 29 | 9. | | | | |
| 30 | 9. | | | | |
| 31 | 9. | | | | |
| 32 | 9. | | | | |
| | | 3.184.221.240 | 192.168.100.205 | TCP | 126 |
| | | 3.184.221.240 | 192.168.100.205 | TCP | 126 |

```
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5858daff14fe131d HTTP/1.1
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Tue, 15 Sep 2020 17:59:10 GMT
If-None-Match: "06b9ae9898bd61:0"
User-Agent: Microsoft-CryptoAPI/6.1
Host: ctldl.windowsupdate.com

HTTP/1.1 200 OK
Accept-Ranges: bytes
Age: 803
Cache-Control: public,max-age=900
```

```
X-Powered-By: ASP.NET
Content-Length: 4817
```

**Notes for the Viewer:**
**two separate PCAPs that are doing similar activity. It's benign - just GET requests to Microsoft domains**

DEEPSEC

# Two PCAP files: Similar Traffic

Transactions per Second

7 Time Items

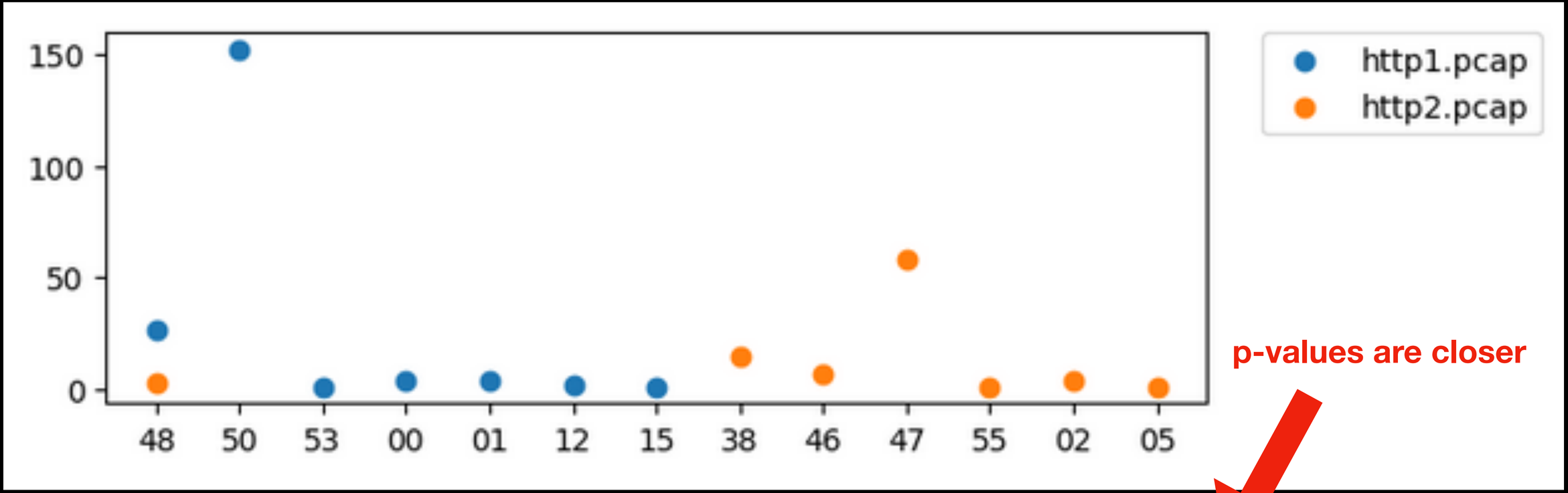
| | http1.pcap |
|---|---|
| 48 | 26 |
| 50 | 152 |
| 53 | 1 |
| 00 | 4 |
| 01 | 4 |
| 12 | 2 |
| 15 | 1) |

7 Time Items

| | http2.pcap |
|---|---|
| 38 | 14 |
| 46 | 7 |
| 47 | 58 |
| 48 | 3 |
| 55 | 1 |
| 02 | 4 |
| 05 | 1) |

DEEPSEC

# Two PCAP files: Similar Traffic




p-values are closer

```
p-value for file1:  0.25540542612601075
p-value for file2:  0.17851805162874884
```

DEEPSEC

# Problems with Cointegration

# Problems with Cointegration: The Time Value

```
file1='http1.pcap'
file2='2022-07-27-second-run-IcedID-infection-traffic.pcap'
```

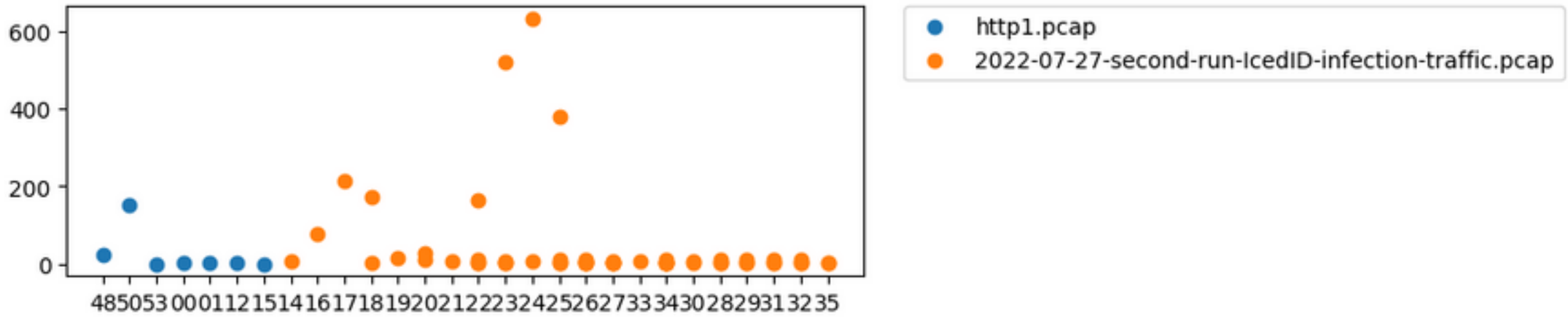
| | http1.pcap |
|---|---|
| 48 | 26 |
| 50 | 152 |
| 53 | 1 |
| 00 | 4 |
| 01 | 4 |
| 12 | 2 |
| 15 | 1) |

| | 2022-07-27-second-run-IcedID-infection-traffic.pcap |
|---|---|
| 14 | 7 |
| 16 | 76 |
| 17 | 213 |
| 18 | 174 |
| 18 | 3 |
| 19 | 16 |
| 20 | 27 |
| 21 | 7 |
| 22 | 164 |
| 23 | 519 |
| 24 | 632 |
| 25 | 378 |
| 26 | 5 |
| 27 | 2 |
| 33 | 6 |
| 34 | 2 |
| 26 | 6 |
| 27 | 6 |
| 30 | 6 |
| 34 | 4 |
| 27 | 3 |
| 20 | 13 |
| 22 | 2 |
| 22 | 4 |
| 22 | 13 |
| 23 | 2 |
| 23 | 4 |
| 23 | 7 |
| 24 | 6 |
| 25 | 2 |
| 25 | 4 |
| 25 | 13 |
| 29 | 10 |
| 30 | 3 |
| 31 | 2 |

**Notes for the Viewer:**
**Two time-series of different lengths - I can't use them. I tried normalizing by calculating percentages, but that didn't quite work because then it's not enough data points to do the cointegration tests.**

# Problems with Cointegration: The Time Value

```
file1='http1.pcap'
file2='2022-07-27-second-run-IcedID-infection-traffic.pcap'
```




```
p-value for file1:  0.25540542612601075
p-value for file2:  0.06304175482717005
```

**Notes for the Viewer:**

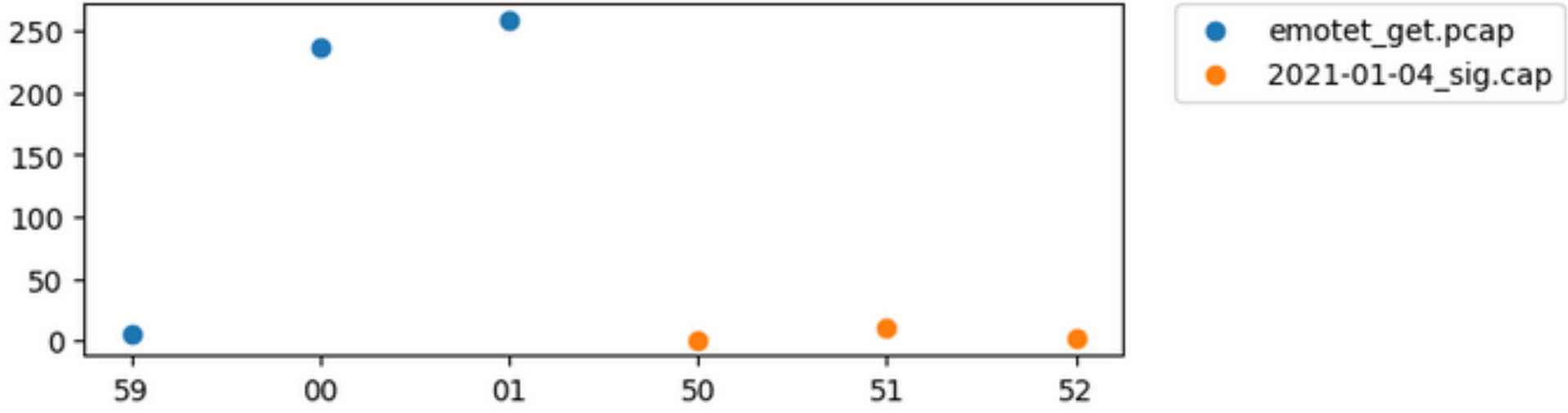
**We can run the cointegration test on the timelines, but it's a bit messed up using seconds for the time. And having drastically different timeline lengths can cause some confusion. Here though, you can see that the p-value's don't match, so at least we have that.**

# Short Sample Size

# Problems with Cointegration: Short Sample Size

```
file1='emotet_get.pcap'
file2='2021-01-04_sig.cap'
```

| | emotet_get.pcap | | 2021-01-04_sig.cap |
|---|---|---|---|
| 59 | 5 | 50 | 1 |
| 00 | 237 | 51 | 10 |
| 01 | 259) | 52 | 2) |



# Problems with Cointegration: Short Sample Size

```
file1='emotet_get.pcap'
file2='2021-01-04_sig.cap'
```

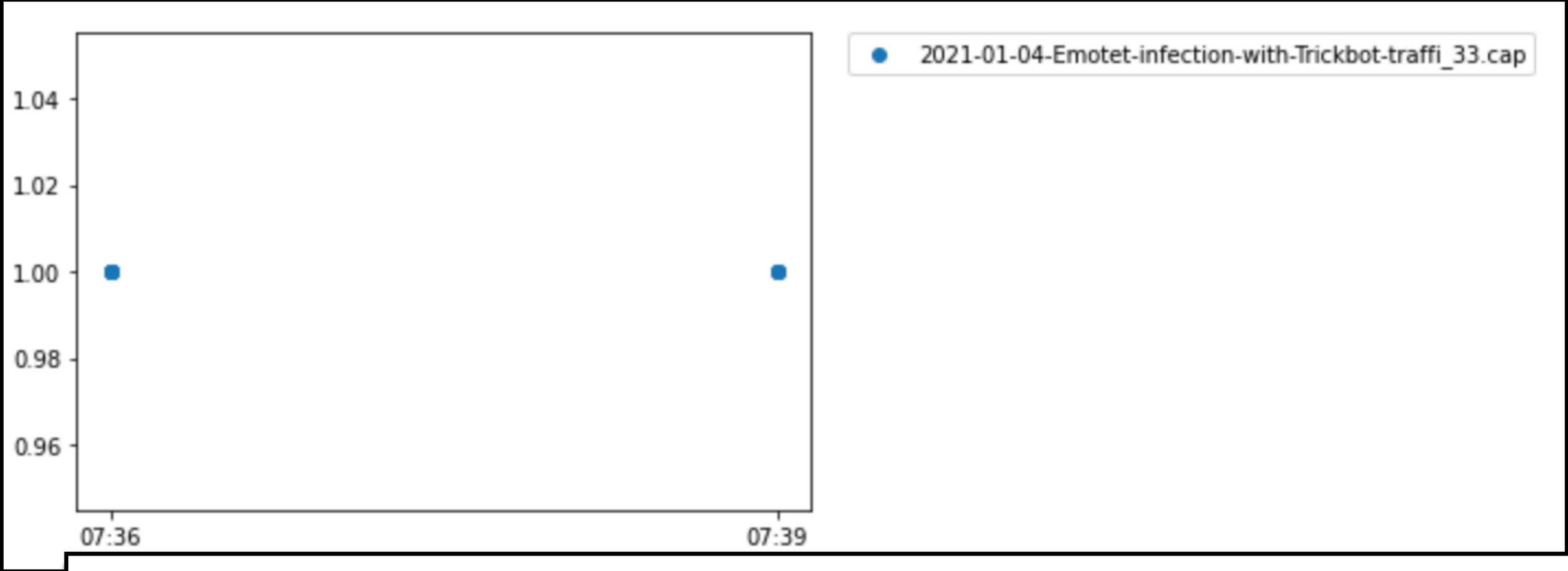
```
# Compute ADF for the two PCAPs:
result_f1 = adfuller(df_f1[file1])
print("p-value for file1: ",result_f1[1])

result_f2 = adfuller(df_f2[file2])
print("p-value for file2: ",result_f2[1])

```

```
ValueError: sample size is too short to use selected regression component
```

# Time Resolution

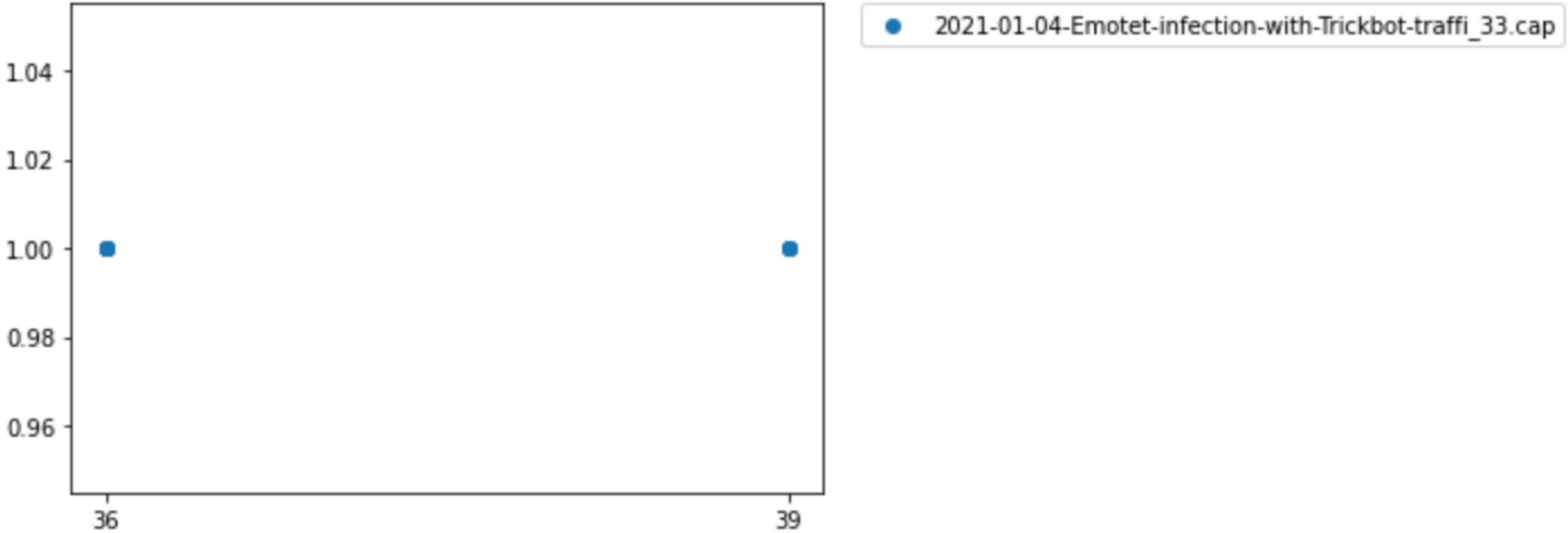
**Notes for the Viewer:**
**It’s important to consider what resolution to look at (Minutes, seconds, microseconds)**

# At the ‘Minutes’ Resolution



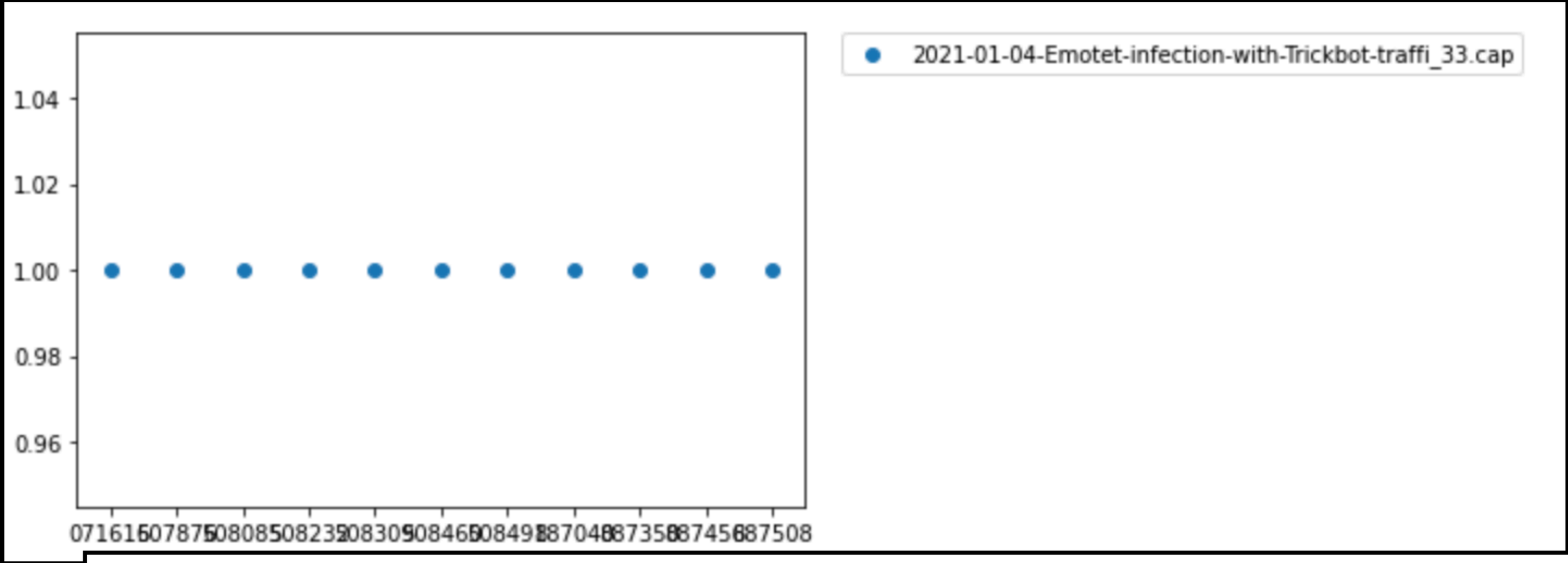

**Notes for the Viewer:**
**It’s important to consider what resolution to look at (Minutes, seconds, microseconds)**

# At the ‘seconds’ Resolution




**Notes for the Viewer:**
**It’s important to consider what resolution to look at (Minutes, seconds, microseconds)**

# At the ‘microseconds’ Resolution




**Notes for the Viewer:**
**It’s important to consider what resolution to look at (Minutes, seconds, microseconds)**

# Normalize

**Notes for the Viewer:**
**It helps to normalize the times**

# Normalized: Time a Transaction Occurred

```
for i in when_transactions_happened:
    print(i['date'],i['count'])
```

```
2021-01-04-Emotet-infection-with-Trickbot-traffi_33.cap
2000-01-01T00:00:00.071616+00:00 1
2000-01-01T00:00:00.507876+00:00 1
2000-01-01T00:00:00.508085+00:00 1
2000-01-01T00:00:00.508232+00:00 1
2000-01-01T00:00:00.508309+00:00 1
2000-01-01T00:00:00.508460+00:00 1
2000-01-01T00:00:00.508491+00:00 1
2000-01-01T00:00:00.887040+00:00 1
```

**Notes for the Viewer:**
**I rewrote the time to 2000-01-01, 00:00 to normalize**

```
2000-01-01T00:00:00.887508+00:00 1
```

DEEPSEC

# Normalized: Time Between Transactions

```python
for i in full_timeline_from_zero:
    print(i)
```

```
2021-01-04-Emotet-infection-with-Trickbot-traffi_33.cap
2000-01-01T00:00:00+00:00
2000-01-01T00:00:00.436260+00:00
2000-01-01T00:00:00.436469+00:00
2000-01-01T00:00:00.436616+00:00
2000-01-01T00:00:00.436693+00:00
2000-01-01T00:00:00.436844+00:00
2000-01-01T00:00:00.436875+00:00
2000-01-01T00:00:00.815424+00:00
2000-01-01T00:00:00.815734+00:00
2000-01-01T00:00:00.815840+00:00
```

**Notes for the Viewer:**
**And then calculated the times in between starting from that normalized start time.**

# Combo of the two

start at zero → 2000-01-01T00:00:00+00:00

2000-01-01T00:00:00.071616+00:00 1 ← Transaction 1

436,260 ms between → 2000-01-01T00:00:00.436260+00:00

2000-01-01T00:00:00.507876+00:00 1 ← Transaction 2

436469 ms between → 2000-01-01T00:00:00.436469+00:00

2000-01-01T00:00:00.508085+00:00 1 ← Transaction 3

436616 ms between → 2000-01-01T00:00:00.436616+00:00

2000-01-01T00:00:00.508232+00:00 1 ← Transaction 4

436693 ms between → 2000-01-01T00:00:00.436693+00:00

2000-01-01T00:00:00.508309+00:00 1 ← Transaction 5

436844 ms between → 2000-01-01T00:00:00.436844+00:00

2000-01-01T00:00:00.508460+00:00 1 ← Transaction 6

436875 ms between → 2000-01-01T00:00:00.436875+00:00

2000-01-01T00:00:00.508491+00:00 1 ← Transaction 7

815424 ms between → 2000-01-01T00:00:00.815424+00:00

2000-01-01T00:00:00.887040+00:00 1 ← Transaction 8

815734 ms between → 2000-01-01T00:00:00.815734+00:00

2000-01-01T00:00:00.887350+00:00 1 ← Transaction 9

815840 ms between → 2000-01-01T00:00:00.815840+00:00

2000-01-01T00:00:00.887456+00:00 1 ← Transaction 10

815892 ms between → 2000-01-01T00:00:00.815892+00:00

2000-01-01T00:00:00.887508+00:00 1 ← Transaction 11

# Signature Creation

**Notes for the Viewer:**
**Now we'll take various parts of what's already been shown to start developing a signature that can be applied to find specific network traffic**

# 1: Separate all the flows

Ethernet · 4 | IPv4 · 120 | IPv6 | TCP · 353 | UDP · 230

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration |
|---|---|---|---|---|---|---|---|---|---|
| 0.0.0.0 | 255.255.255.255 | 2 | 684 bytes | 2 | 684 bytes | 0 | 0 bytes | 0.000000 | 0.0009 |
| 192.168.1.1 | 192.168.1.221 | 437 | 45.674 KiB | 219 | 28.996 KiB | 218 | 16.678 KiB | 0.000699 | 318.9567 |
| 192.168.1.1 | 255.255.255.255 | 1 | 322 bytes | 1 | 322 bytes | 0 | 0 bytes | 3.539167 | 0.0000 |
| 192.168.1.221 | 13.33.61.67 | 51 | 15.988 KiB | 24 | 3.360 KiB | 27 | 12.628 KiB | 149.666647 | 131.3836 |
| 192.168.1.221 | 13.77.161.179 | 6 | 354 bytes | 4 | 228 bytes | 2 | 126 bytes | 51.449515 | 0.2600 |
| 192.168.1.221 | 34.240.211.33 | 33 | 4.615 KiB | 16 | 3.353 KiB | 17 | 1.263 KiB | 179.483259 | 6.8793 |
| 192.168.1.221 | 37.1.217.172 | 23 | 2.514 KiB | 12 | 1.164 KiB | 11 | 1.350 KiB | 138.918247 | 55.9948 |
| 192.168.1.221 | 40.129.73.242 | 209 | 26.277 KiB | 101 | 17.888 KiB | 108 | 8.390 KiB | 285.111452 | 37.1815 |
| 192.168.1.221 | 43.231.4.7 | 11 | 1.065 KiB | 5 | 407 bytes | 6 | 684 bytes | 57.005241 | 2.0630 |
| 192.168.1.221 | 46.4.52.109 | 310 | 192.089 KiB | 184 | 177.391 KiB | 126 | 14.698 KiB | 122.451040 | 207.7845 |
| 192.168.1.221 | 46.28.66.2 | 143 | 32.562 KiB | 65 | 21.941 KiB | 78 | 10.620 KiB | 122.212165 | 208.9215 |
| 192.168.1.221 | 46.137.75.217 | 33 | 4.514 KiB | 16 | 3.251 KiB | 17 | 1.263 KiB | 266.025045 | 4.6886 |
| 192.168.1.221 | 46.226.52.104 | 33 | 4.553 KiB | 16 | 3.290 KiB | 17 | 1.263 KiB | 196.090463 | 4.8636 |
| 192.168.1.221 | 47.43.18.9 | 1,021 | 150.433 KiB | 495 | 110.665 KiB | 526 | 39.768 KiB | 124.075039 | 198.1918 |
| 192.168.1.221 | 52.41.212.0 | 97 | 35.338 KiB | 45 | 8.518 KiB | 52 | 26.820 KiB | 266.660879 | 30.5686 |
| 192.168.1.221 | 52.88.19.91 | 25 | 8.874 KiB | 12 | 2.169 KiB | 13 | 6.705 KiB | 303.694859 | 16.1514 |
| 192.168.1.221 | 52.166.201.127 | 37 | 4.795 KiB | 18 | 3.411 KiB | 19 | 1.384 KiB | 260.521988 | 10.4123 |
| 192.168.1.221 | 54.86.81.5 | 68 | 9.460 KiB | 33 | 6.771 KiB | 35 | 2.689 KiB | 231.930751 | 35.3727 |
| 192.168.1.221 | 54.192.39.68 | 18 | 6.889 KiB | 8 | 863 bytes | 10 | 6.046 KiB | 312.234250 | 10.2297 |
| 192.168.1.221 | 62.8.140.122 | 33 | 4.539 KiB | 16 | 3.276 KiB | 17 | 1.263 KiB | 263.193602 | 8.5101 |
| 192.168.1.221 | 62.24.139.42 | 35 | 4.843 KiB | 17 | 3.416 KiB | 18 | 1.427 KiB | 136.258808 | 7.1211 |
| 192.168.1.221 | 62.149.178.10 | 33 | 4.577 KiB | 16 | 3.314 KiB | 17 | 1.263 KiB | 258.802042 | 3.7648 |
| 192.168.1.221 | 62.159.91.51 | 33 | 4.541 KiB | 16 | 3.278 KiB | 17 | 1.263 KiB | 200.543042 | 10.9354 |
| 192.168.1.221 | 62.159.95.227 | 33 | 4.565 KiB | 16 | 3.303 KiB | 17 | 1.263 KiB | 189.483022 | 8.7831 |
| 192.168.1.221 | 62.159.186.4 | 35 | 4.759 KiB | 17 | 3.332 KiB | 18 | 1.427 KiB | 156.463835 | 13.3246 |
| 192.168.1.221 | 62.181.145.234 | 33 | 4.589 KiB | 16 | 3.326 KiB | 17 | 1.263 KiB | 248.451866 | 10.6580 |
| 192.168.1.221 | 67.195.204.72 | 1,582 | 208.074 KiB | 767 | 145.880 KiB | 815 | 62.194 KiB | 105.789059 | 198.3949 |
| 192.168.1.221 | 67.195.204.75 | 444 | 58.940 KiB | 216 | 40.893 KiB | 228 | 18.048 KiB | 191.941130 | 79.4995 |
| 1.221 | 67.195.204.79 | 254 | 31.027 KiB | 120 | 20.489 KiB | 134 | 10.538 KiB | 290.918861 | 39.8501 |
| 1.221 | 67.195.228.111 | 19 | 1.470 KiB | 6 | 425 bytes | 13 | 1.055 KiB | [illegible] | [illegible] |

DEEPSEC

# 2: Operate against each flow individually

- 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_20221017-143616.txt
- 2022-02-25-Emotet-epoch5-spambot-traffic-snippet.pcap
- flowoutputs
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_0.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_1.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_2.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_3.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_4.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_5.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_6.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_7.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_8.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_9.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_10.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_11.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_12.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_13.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_14.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_15.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_16.cap
  - 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_17.cap

# 2: Operate against each flow individually

```
1: 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_20221017-143616.txt
2: 2022-02-25-Emotet-epoch5-spambot-traffic-snippet.pcap
       Average beteen queries: 14135.07467057101
       Total Queries: 1367
3: 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_15.cap
       Average beteen queries: 8049.0
       Total Queries: 3
4: 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_14.cap
       Average beteen queries: 73373.6
       Total Queries: 11
5: 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_16.cap
       Average beteen queries: 133663.0588235294
       Total Queries: 18
6: 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_17.cap
       Average beteen queries: 150335.16666666666
       Total Queries: 25
7: 2022-02-25-Emotet-epoch5-spambot-traffic-snippet_13.cap
       Average beteen queries: 59165.142857142855
       Total Queries: 36
```

DEEPSEC

# Calculate Percentages

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 2022-03-29 07:17:49.109583 | 10.3.29.101 | 104.161.127.22 | HTTP | 500 | GET /wp-content/Elw3kPvOsZxM5/ HTTP/1.1 |
| 2 | 2022-03-29 07:17:49.313841 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=1 Ack=447 Win=6 |
| 3 | 2022-03-29 07:17:49.313918 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=1362 Ack=447 Wi |
| 4 | 2022-03-29 07:17:49.314270 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=2723 Ack=447 Wi |
| 5 | 2022-03-29 07:17:49.314494 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=4084 Ack=447 Wi |
| 6 | 2022-03-29 07:17:49.314711 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=5445 Ack=447 Wi |
| 7 | 2022-03-29 07:17:49.314939 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=6806 Ack=447 Wi |
| 8 | 2022-03-29 07:17:49.315151 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=8167 Ack=447 Wi |
| 9 | 2022-03-29 07:17:49.315647 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=9528 Ack=447 Wi |
| 10 | 2022-03-29 07:17:49.315893 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=10889 Ack=447 W |
| 11 | 2022-03-29 07:17:49.316113 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=12250 Ack=447 W |
| 12 | 2022-03-29 07:17:49.431163 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=13611 Ack=447 W |
| 13 | 2022-03-29 07:17:49.431384 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=14972 Ack=447 W |
| 14 | 2022-03-29 07:17:49.431724 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=16333 Ack=447 W |
| 15 | 2022-03-29 07:17:49.431975 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=17694 Ack=447 W |
| 16 | 2022-03-29 07:17:49.441210 | 104.161.127.22 | 10.3.29.101 | TCP | 1415 | 80 → 56309 [PSH, ACK] Seq=19055 Ack=447 W |

| | | | | | | |
|---|---|---|---|---|---|---|
| 568 | 2022-03-29 07:18:34.204988 | 74.124.193.14 | 10.3.29.101 | TCP | 1415 | 80 → 56321 [PSH, ACK] Seq=583870 Ack=214 Win=64240 Len=1361 [TCP |
| 569 | 2022-03-29 07:18:34.206474 | 74.124.193.14 | 10.3.29.101 | TCP | 1415 | 80 → 56321 [PSH, ACK] Seq=585231 Ack=214 Win=64240 Len=1361 [TCP |
| 570 | 2022-03-29 07:18:34.206708 | 74.124.193.14 | 10.3.29.101 | TCP | 1415 | 80 → 56321 [PSH, ACK] Seq=586592 Ack=214 Win=64240 Len=1361 [TCP |
| 571 | 2022-03-29 07:18:34.206929 | 74.124.193.14 | 10.3.29.101 | TCP | 1415 | 80 → 56321 [PSH, ACK] Seq=587953 Ack=214 Win=64240 Len=1361 [TCP |
| 572 | 2022-03-29 07:18:34.207125 | 74.124.193.14 | 10.3.29.101 | HTTP | 1117 | HTTP/1.1 200 OK (application/x-msdownload) |

**Notes for the Viewer:**

**network traffic is not all the same. Here, I'm looking at two PCAPs. A lot more transactions in one. Also a lot of 0 time in between traffic. Not super useful. One PCAP has 572 packets**

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2022-04-20 14:33:18.628513 | 10.4.20.102 | 107.161.178.210 | HTTP | 279 | GET /video/6JvA8/ HTTP/1.1 |
| 2 | 2022-04-20 14:33:59.595290 | 10.4.20.102 | 49.231.16.102 | TCP | 1434 | 54331 → 8080 [ACK] Seq=1 Ack=1 Win=1024 Len=1380 |
| 3 | 2022-04-20 14:33:59.595358 | 10.4.20.102 | 49.231.16.102 | TCP | 1434 | 54331 → 8080 [ACK] Seq=1381 Ack=1 Win=1024 Len=1380 |
| 4 | 2022-04-20 14:33:59.595430 | 10.4.20.102 | 49.231.16.102 | TCP | 926 | 54331 → 8080 [PSH, ACK] Seq=2761 Ack=1 Win=1024 Len=872 |
| 5 | 2022-04-20 14:37:57.405290 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | 54360 → 8080 [ACK] Seq=1 Ack=1 Win=1024 Len=1388 |
| 6 | 2022-04-20 14:37:57.552709 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=8329 Ack=1 |
| 7 | 2022-04-20 14:37:57.552873 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | 54360 → 8080 [PSH, ACK] Seq=9717 Ack=1 Win=1024 Len=1388 |
| 8 | 2022-04-20 14:37:57.559324 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=19433 Ack= |
| 9 | 2022-04-20 14:37:57.701945 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=44417 Ack= |
| 10 | 2022-04-20 14:37:57.708372 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=68013 Ack= |
| 11 | 2022-04-20 14:37:57.713906 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=77729 Ack= |
| 12 | 2022-04-20 14:37:57.714774 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=87445 Ack= |
| 13 | 2022-04-20 14:37:57.714847 | 10.4.20.102 | 176.31.163.17 | TCP | 1442 | 54360 → 8080 [ACK] Seq=88833 Ack=1 Win=1024 Len=1388 |
| 43 | 2022-04-20 15:13:38.193545 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=244808 Ack=1 Win |
| 44 | 2022-04-20 15:13:38.200169 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=257300 Ack=1 Win |
| 45 | 2022-04-20 15:13:38.269912 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=265385 Ack=1 Win |
| 46 | 2022-04-20 15:13:38.302228 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=273713 Ack=1 Win |
| 47 | 2022-04-20 15:13:38.366600 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=279022 Ack=1 Win |
| 48 | 2022-04-20 15:13:38.367030 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=284574 Ack=1 Win |
| 49 | 2022-04-20 15:13:38.436687 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=298211 Ack=1 Win |
| 50 | 2022-04-20 15:13:38.450193 | 45.55.63.166 | 10.4.20.102 | TCP | 1442 | [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=303763 Ack=1 Win |
| 51 | 2022-04-20 15:13:38.524592 | 45.55.63.166 | 10.4.20.102 | TCP | 1199 | [TCP Previous segment not captured] 8080 → 54383 [PSH, ACK] Seq=324340 Ack= |
| 52 | 2022-04-20 15:13:38.552988 | 45.55.63.166 | 10.4.20.102 | TCP | 1137 | [TCP Previous segment not captured] 8080 → 54383 [PSH, ACK] Seq=333813 Ack= |

**Notes for the Viewer:**
**The other PCAP has 52 packets**

DEEPSEC

```
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]
4
992316552291476588
pyorre@scavpn-056 extractflows % python3 signature_generation.py epoch4/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_http.pcap
7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 1, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 10, 11, 8, 6, 7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0,
, 0, 0,
, 0, 0,
, 0, 0
```

**Notes for the Viewer:**

**Here, I'm looking at two PCAPs. A lot more transactions in one. Also a lot of 0 time in between traffic. Not super useful.**

```
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]
4
992316552291476588
pyorre@scavpn-056 extractflows % python3 signature_generation.py epoch4/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_http.pcap
7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 1, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 10, 11, 8, 6, 7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0,
, 0, 0,
, 0, 0,
, 0, 0
```

**Notes for the Viewer:**
**Here, I'm looking at two PCAPs. A lot more transactions in one. Also a lot of 0 time in between traffic. Not super useful.**

Similar traffic Times

Similar traffic Times

[13, 0, 1, 0, 0, 7, 0, 0, 5, 0, 0, 7, 1, 0, 1, 0, 6, 0, 0, 15, 0, 0, 8, 0, 0, 14, 0, 0, 0, 0, 1, 0, 0, 0, 0, 9, 0, 0, 0, 0, 13]

[6, 0, 12, 0, 0, 8, 0, 0, 7, 0, 0, 7, 1, 9, 1, 0, 0, 0, 6, 0, 0, 16, 0, 0, 9, 0, 0, 0, 0, 12, 0, 0, 0, 0, 4, 0, 0, 0, 0, 3]

A little off

**Notes for the Viewer:**
**One interesting thing in these percentages of the time in between packets as they relate to the total time of the whole flow is that they are fairly similar, despite being different. Maybe it's because this is SSL and it's just following the pattern of SSL traffic, which might be similar no matter what kind of flow it's on.**

DEEPSEC

# Add a little chaos

2022-03-29-Emotet-epoch4-with-Cobalt-Strike_http.pcap Today at 22:53 810 KB

[16, 14, 2, 2, 2, 2, 8, 5, 2, 10, 5, 5, 9, 1, 1, 2, 3, 3, 1, 1, 1, 1, 1]

2022-04-20-Emotet-epoch4-infection-with-spambot-traffic_http.pcap Today at 22:55 72 KB

[7, 4, 3, 1, 4, 4, 4, 3, 10, 11, 8, 6, 7, 4, 4, 3, 3, 2, 1, 2, 1]

# By Rounding things

**Notes for the Viewer:**
**I want to work with integers, not floats because I want the comparison to be a little 'looser' - so I'm converting to ints and rounding them.**

# 2022-07-07-Emotet-infection-with-Cobalt-Strike:

```
emotet20220707/1_emotet_get/1_emotet_get.pcap:
Percent of each time in between toward the total: [2, 46, 2, 1, 12, 3, 4, 1, 13, 3, 5, 2]

emotet20220707/2_emotet_c2/2_emotet_c2.pcap:
Percent of each time in between toward the total: [2, 16, 1, 6, 2, 1, 1, 1, 2, 1, 3, 38]

emotet20220707/3_cobaltstriketraffic/3_cobaltstriketraffic.pcap:
Percent of each time in between toward the total: [1, 19, 25, 16, 19, 19, 2]
```

**Notes for the Viewer:**
**They are sometimes just below or above 100, but that's because I round them.**

# Now we can find exact matches

# Which isn’t really Useful

DEEPSEC

# Percentages and Distance

## Levenshtein Distance

**Notes for the Viewer:**
**I need my search to be even more ‘loose’/less precise. So now I’m exploring Levenshtein Distance. This is typically used for word searches.**

# Levenshtein Distance

| | | | | | |
|---|---|---|---|---|---|
| K | I | T | T | E | N |
| S | I | T | T | E | N |

substitution
K with S

| | | | | | |
|---|---|---|---|---|---|
| K | I | T | T | E | N |
| S | I | T | T | I | N |

substitution
E with I

| | | | | | | |
|---|---|---|---|---|---|---|
| K | I | T | T | E | N | |
| S | I | T | T | I | N | G |

insertion G

**Notes for the Viewer:**
**Levenshtein Distance is typically used for word searches - how many changes between two words shows how close they are.**

# GET REQUESTS

```
emotet20220707/1_emotet_get/1_emotet_get.pcap:
Percent of each time in between toward the total: [2, 46, 2, 1, 12, 3, 4, 1, 13, 3, 5, 2]
```

signatures.json

```
{
    "emotetGET_20220707":[2, 46, 2, 1, 12, 3, 4, 1, 13, 3, 5, 2],
}
```

**Notes for the Viewer:**
**Before applying Levenshtein Distance, let's make a static signature. Start by putting the percentages into a text file to be read by the test_signature script**

# Check Signature Against the PCAP it was created from

```
jpyorre@Joshs-MacBook-Pro test_signatures % python3 test_signature.py 1_emotet_ge
t.pcap
[{'filename': 'flowoutputs/1_emotet_get_0.cap', 'percent of times in between': [2
, 46, 2, 1, 12, 3, 4, 1, 13, 3, 5, 2]}]
ratio: flowoutputs/1_emotet_get_0.cap: emotetGET_20220707, 100
partial_ratio: flowoutputs/1_emotet_get_0.cap: emotetGET_20220707, 100
jpyorre@Joshs-MacBook-Pro test_signatures %
```

**Notes for the Viewer:**
**Still from a video showing the process of detecting an exact match (no Levenshtein - just a perfect match of percentage signature to percentages in a PCAP.**

DEEPSEC

# What about a similar bad PCAP?

**Notes for the Viewer:**
**We need to try it on something that is not exactly the same.**

1_emotet_get.pcap

Apply a display filter ... <⌘/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 2022-07-07 11:18:59.829216 | 10.7.7.101 | 193.53.245.52 | TCP | 66 | 57305 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2 | 2022-07-07 11:18:59.859796 | 193.53.245.52 | 10.7.7.101 | TCP | 58 | 80 → 57305 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 3 | 2022-07-07 11:18:59.860058 | 10.7.7.101 | 193.53.245.52 | TCP | 54 | 57305 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 4 | 2022-07-07 11:18:59.860336 | 10.7.7.101 | 193.53.245.52 | HTTP | 291 | GET /system/4Z6pu0ENN1DH2HYMzKLz/ HTTP/1.1 |
| 5 | 2022-07-07 11:18:59.860479 | 193.53.245.52 | 10.7.7.101 | TCP | 54 | 80 → 57305 [ACK] Seq=1 Ack=238 Win=64240 Len=0 |
| 6 | 2022-07- | | | TCP | 804 | 80 → 57305 [PSH, ACK] Seq=1 Ack=238 Win=64240 Len=750 [TCP segment of a reassembled PDU] |
| 7 | 2022-07- | | | TCP | 1514 | 80 → 57305 [ACK] Seq=751 Ack=238 Win=64240 Len=1460 [TCP segment of a reassembled PDU] |
| 8 | 2022-07- | | | TCP | 1074 | 80 → 57305 [PSH, ACK] Seq=2211 Ack=238 Win=64240 Len=1020 [TCP segment of a reassembled PDU] |
| 9 | 2022-07- | | | | | ed PDU] |
| 10 | 2022-07-07 11:19:00.454899 | 193.5 | | | | d PDU] |
| 11 | 2022-07-07 11:19:00.454902 | 10.7. | | | | |
| 12 | 2022-07-07 11:19:00.454986 | 193.5 | | | | ed PDU] |
| 13 | 2022-07-07 11:19:00.455140 | 10.7.7.101 | 193.53.245.52 | TCP | 54 | 57305 → 80 [ACK] Seq=238 Ack=6087 Win=65535 Len=0 |
| 14 | 2022-07-07 11:19:00.455651 | 193.53.245.52 | 10.7.7.101 | TCP | 1294 | 80 → 57305 [PSH, ACK] Seq=6087 Ack=238 Win=64240 Len=1240 [TCP segment of a reassembled PDU] |
| 15 | 2022-07-07 11:19:00.455739 | 193.53.245.52 | 10.7.7.101 | TCP | 1514 | 80 → 57305 [ACK] Seq=7327 Ack=238 Win=64240 Len=1460 [TCP segment of a reassembled PDU] |

# Our Signature PCAP

```
"emotetGET_20220707":[2, 46, 2, 1, 12, 3, 4, 1, 13, 3, 5, 2]
```

> Frame 4: 291 bytes on wire (2328 bits
> Ethernet II, Src: IntelCor_58:ad:6c (
> Internet Protocol Version 4, Src: 10.
> Transmission Control Protocol, Sr
> Hypertext Transfer Protocol

```
0000  00 04 4d 11 a7 08 a0 a8  cd 58 ad 6c 08 00 45 00   ··M····· ·X·l··E·
0010  01 15 f2 e2 40 00 80 06  3f 2a 0a 07 07 65 c1 35   ····@··· ?*···e·5
0020  f5 34 df d9 00 50 b6 61  b7 33 bf 8b 8a 32 50 18   ·4···P·a ·3···2P·
0030  ff ff a2 31 00 00 47 45  54 20 2f 73 79 73 74 65   ···1··GE T /syste
```

2022-08-08_exe_download-IcedID-with-Cobalt-Strike.pcap

Apply a display filter ... <⌘/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 2022-08-08 14:27:00.681914 | 10.8.8.101 | 104.238.220.131 | TCP | 66 | 50462 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2 | 2022-08-08 14:27:00.740394 | 104.238.220.131 | 10.8.8.101 | TCP | 58 | 80 → 50462 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 3 | 2022-08-08 14:27:00.740476 | 10.8.8.101 | 104.238.220.131 | TCP | 54 | 50462 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 4 | 2022-08-08 14:27:00.740656 | 10.8.8.101 | 104.238.220.131 | HTTP | 135 | GET /download/sys.exe HTTP/1.1 |
| 5 | 2022-08-08 14:27:00.740706 | 104.238.220.131 | 10.8.8.101 | TCP | 54 | 80 → 50462 [ACK] Seq=1 Ack=82 Win=64240 Len=0 |
| 6 | 2022-08-08 14:27:00.803700 | 104.238.220.131 | 10.8.8.101 | TCP | 274 | 80 → 50462 [PSH, ACK] Seq=1 Ack=82 Win=64240 Len=220 [TCP segment of a reassembled PDU] |
| 7 | 2022-08-08 14:27:00.806889 | 104.238.220.131 | 10.8.8.101 | TCP | 1442 | 80 → 50462 [PSH, ACK] Seq=221 Ack=82 Win=64240 Len=1388 [TCP segment of a reassembled PDU] |
| 8 | 2022-08-08 14:27:00.806981 | 10.8.8.101 | 104.238.220.131 | TCP | 54 | 50462 → 80 [ACK] Seq=82 Ack=1609 Win=64240 Len=0 |
| 9 | 2022-08-08 14:27:00.810051 | 104.238.220.131 | | | | Ack=82 Win=64240 Len=1388 [TCP segment of a reassembled PDU] |
| 10 | 2022-08-08 14:27:00.813267 | 104.238.220.131 | | | | Ack=82 Win=64240 Len=1388 [TCP segment of a reassembled PDU] |
| 11 | 2022-08-08 14:27:00.813309 | 10.8.8.101 | | | | 5 Win=64240 Len=0 |
| 12 | 2022-08-08 14:27:00.816458 | 104.238.220.131 | | | | Ack=82 Win=64240 Len=1388 [TCP segment of a reassembled PDU] |
| 13 | 2022-08-08 14:27:00.827539 | 104.238.220.131 | 10.8.8.101 | TCP | 1442 | 80 → 50462 [PSH, ACK] Seq=5773 Ack=82 Win=64240 Len=1388 [TCP segment of a reassembled PDU] |
| 14 | 2022-08-08 14:27:00.827588 | 10.8.8.101 | 104.238.220.131 | TCP | 54 | 50462 → 80 [ACK] Seq=82 Ack=7161 Win=64240 Len=0 |
| 15 | 2022-08-08 14:27:00.827608 | 104.238.220.131 | 10.8.8.101 | TCP | 1442 | 80 → 50462 [PSH, ACK] Seq=7161 Ack=82 Win=64240 Len=1388 [TCP segment of a reassembled PDU] |

# Our Suspicious PCAP

> Frame 4: 135 bytes on wire (1080 bits
> Ethernet II, Src: HewlettP_1c:47:ae (
> Internet Protocol Version 4, Src: 10.
> Transmission Control Protocol, Src Pc
> Hypertext Transfer Protocol

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*····· ··G···E·
0010  00 79 52 0a 40 00 80 06  50 96 0a 08 08 65 68 ee   ·yR·@··· P····eh·
0020  dc 83 c5 1e 00 50 c9 d2  cb 46 2e fa 11 d7 50 18   ·····P·· ·F····P·
0030  fa f0 eb 27 00 00 47 45  54 20 2f 64 6f 77 6e 6c   ···'··GE T /downl
0040  6f 61 64 2f 73 79 73 2e  65 78 65 20 48 54 54 50   oad/sys. exe HTTP
0050  2f 31 2e 31 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   /1.1··Co nnection
0060  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 48 6f   : Keep-A live··Ho
0070  73 74 3a 20 31 30 34 2e  32 33 38 2e 32 32 30 2e   st: 104. 238.220.
0080  31 33 31 0d 0a 0d 0a                               131····
```

DEEPSEC

# Check Signature Against similar bad PCAP

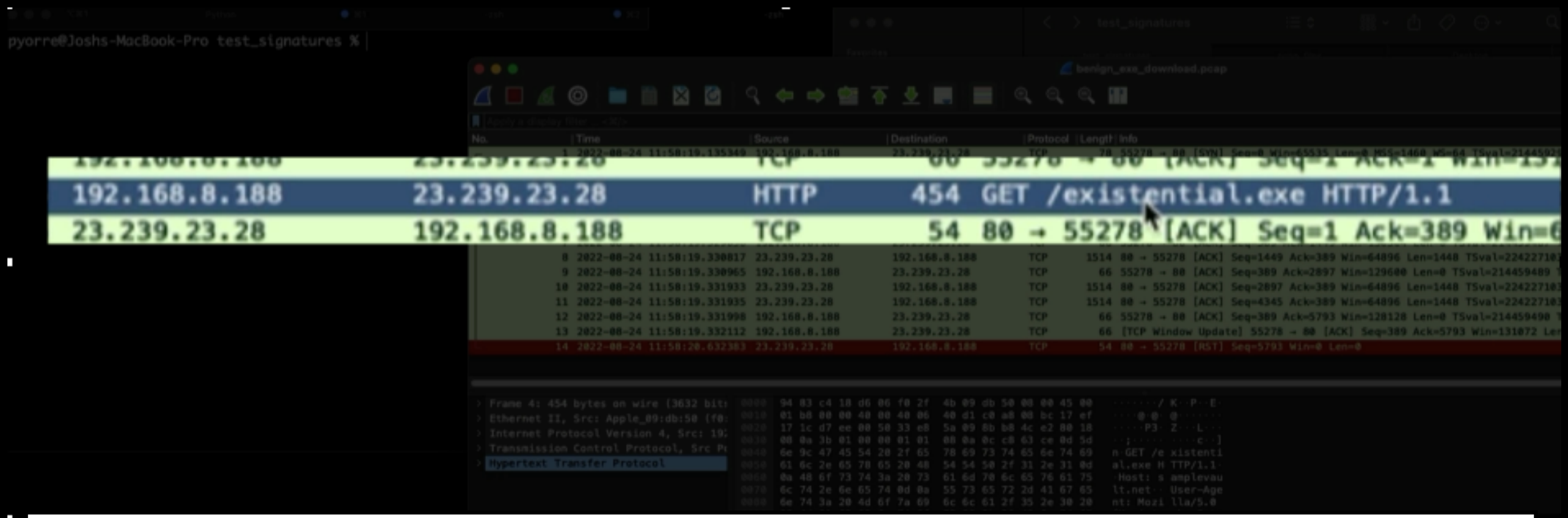
```
{'filename': 'flowoutputs/2022-08-08_exe_download-IcedID-with-Cobalt-Strike_0.cap', 'percent of times in betw
n': [3, 4, 1, 2, 1, 2, 2, 1, 1, 1, 1, 8, 1, 1, 1, 1, 2, 1, 1, 2, 2, 1, 8, 3, 3, 3, 1, 1, 1, 1, 4, 1]}]
atio: flowoutputs/2022-08-08_exe_download-IcedID-with-Cobalt-Strike_0.cap: emotetGET_20220707, 47
artial_ratio: flowoutputs/2022-08-08_exe_download-IcedID-with-Cobalt-Strike_0.cap: emotetGET_20220707, 74
pyorre@Joshs-MacBook-Pro test_signatures %
```

**Notes for the Viewer:**
**Still from a video of signature and using Levenshtein Distance to compare two similar PCAPs. The percentages are different, but we have a partial ratio that is somewhat close, suggesting a relationship.**

DEEPSEC

# What about a similar benign PCAP?

# Check Signature Against similar benign PCAP




**Notes for the Viewer:**
**Using a benign .exe download that is designed to look like a malware dropper**

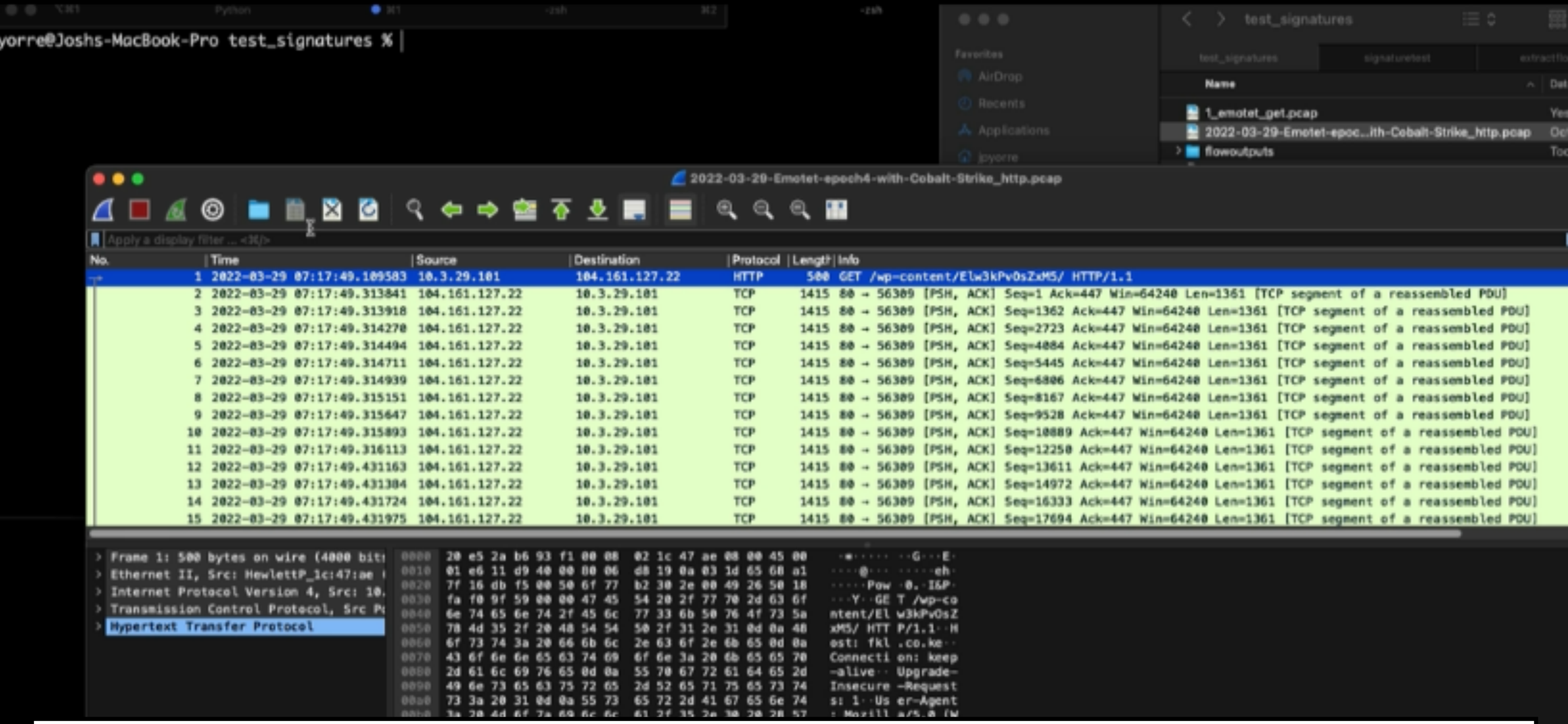
DEEPSEC

# Check Signature Against similar benign PCAP

```
pyorre@Joshs-MacBook-Pro test_signatures % python3 test_signature.py benign_exe_download.pcap
{'filename': 'flowoutputs/benign_exe_download_0.cap', 'percent of times in between': [10, 1, 28]}]
atio: flowoutputs/benign_exe_download_0.cap: emotetGET_20220707, 36
artial_ratio: flowoutputs/benign_exe_download_0.cap: emotetGET_20220707, 57
pyorre@Joshs-MacBook-Pro test_signatures %
```

**Notes for the Viewer:**
**It doesn’t match too well to the emotet dropper download, which is good!**

# Multiple Flows in a PCAP



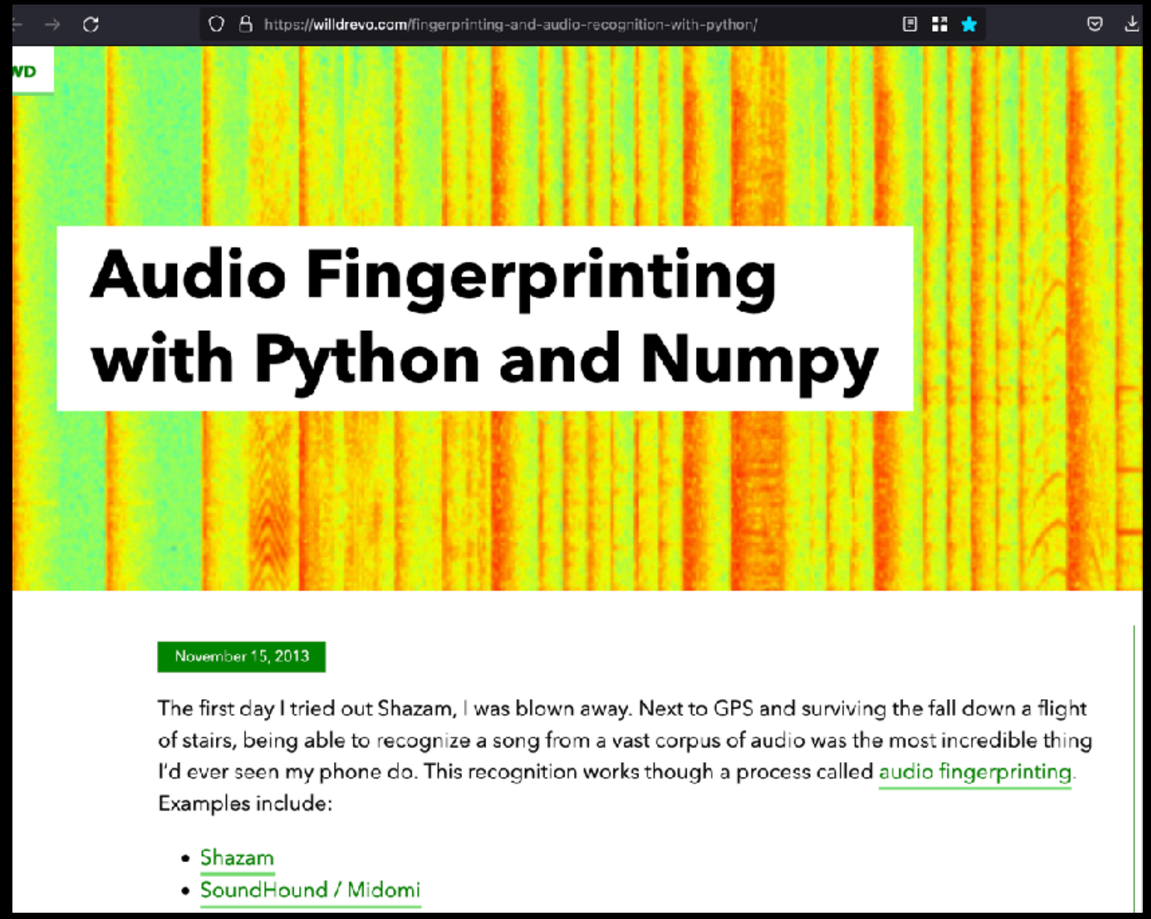

**Notes for the Viewer:**
**Running a PCAP containing a GET request for an Emotet dropper to a compromised wordpress account.**

```
jpyorre@Joshs-MacBook-Pro test_signatures % python3 test_signature.py 2022-03-29-Emotet-epoch4-with-Cobalt-Strike_http.pcap
[{'filename': 'flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_1.cap', 'percent of times in between': []}, {'filename': 'flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_0.cap', 'percent of times in
ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_1.cap: emotetGET_20220707, 0
partial_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_1.cap: emotetGET_20220707, 0
ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_0.cap: emotetGET_20220707, 68
partial_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_0.cap: emotetGET_20220707, 72
ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_2.cap: emotetGET_20220707, 0
partial_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_2.cap: emotetGET_20220707, 0
ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_3.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike_htt_3.cap: emotetGET_20220707, 74
jpyorre@Joshs-MacBook-Pro test_signatures %
```

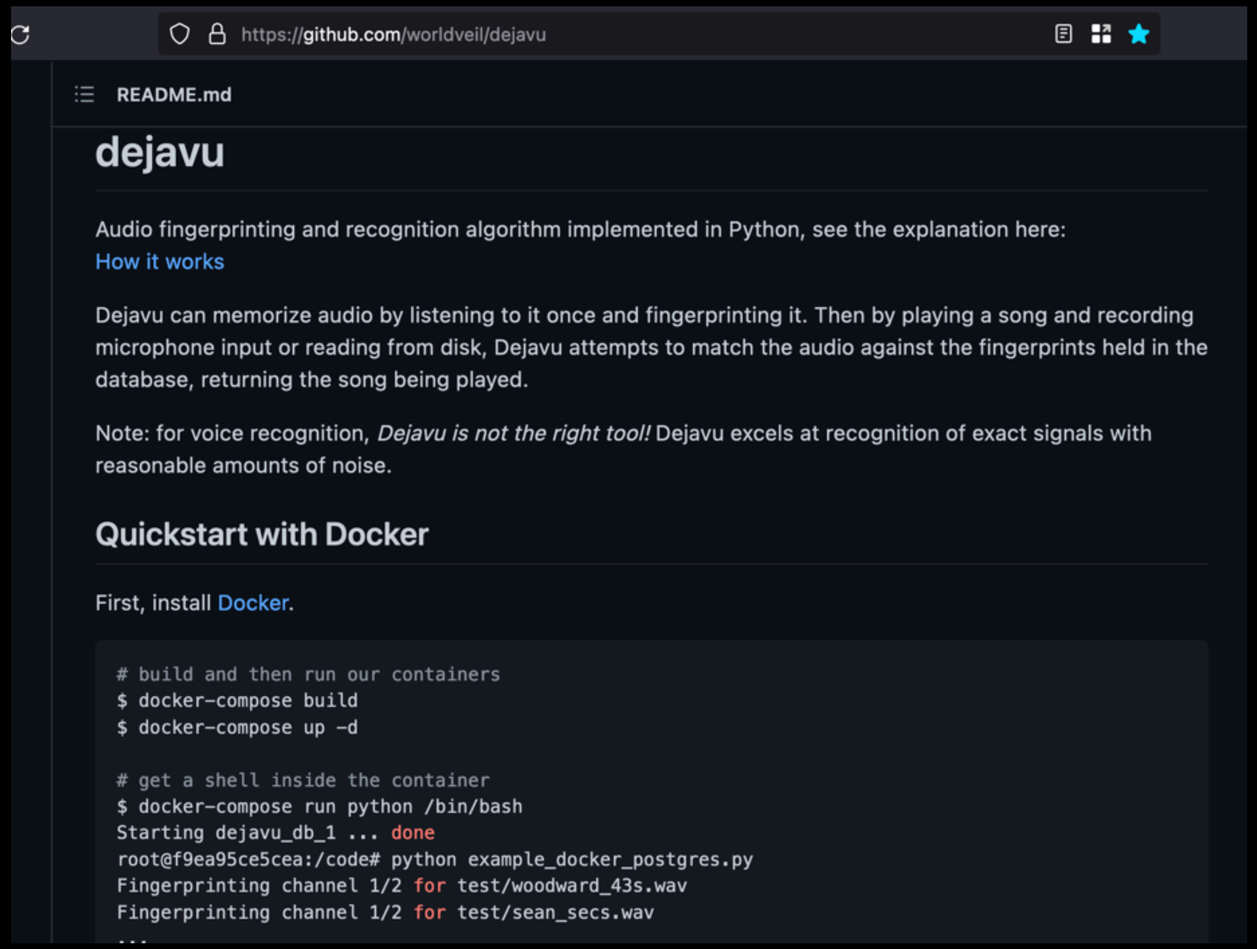
**Notes for the Viewer:**
**Each flow is separated from the PCAP and the signature is run against them, one at a time. Higher matches are shown. The PCAPs with partial ratios of 72 and 74 are a match for Emotet Dropper downloads**

# Audio?

**Notes for the Viewer:**
**This image shows that music is another thing I do, and security is a creative process. Just to think outside the box, can we convert time to audio and use something to identify it, much like the app ‘Shazam’ is used to identify a song by listening to part of it?**

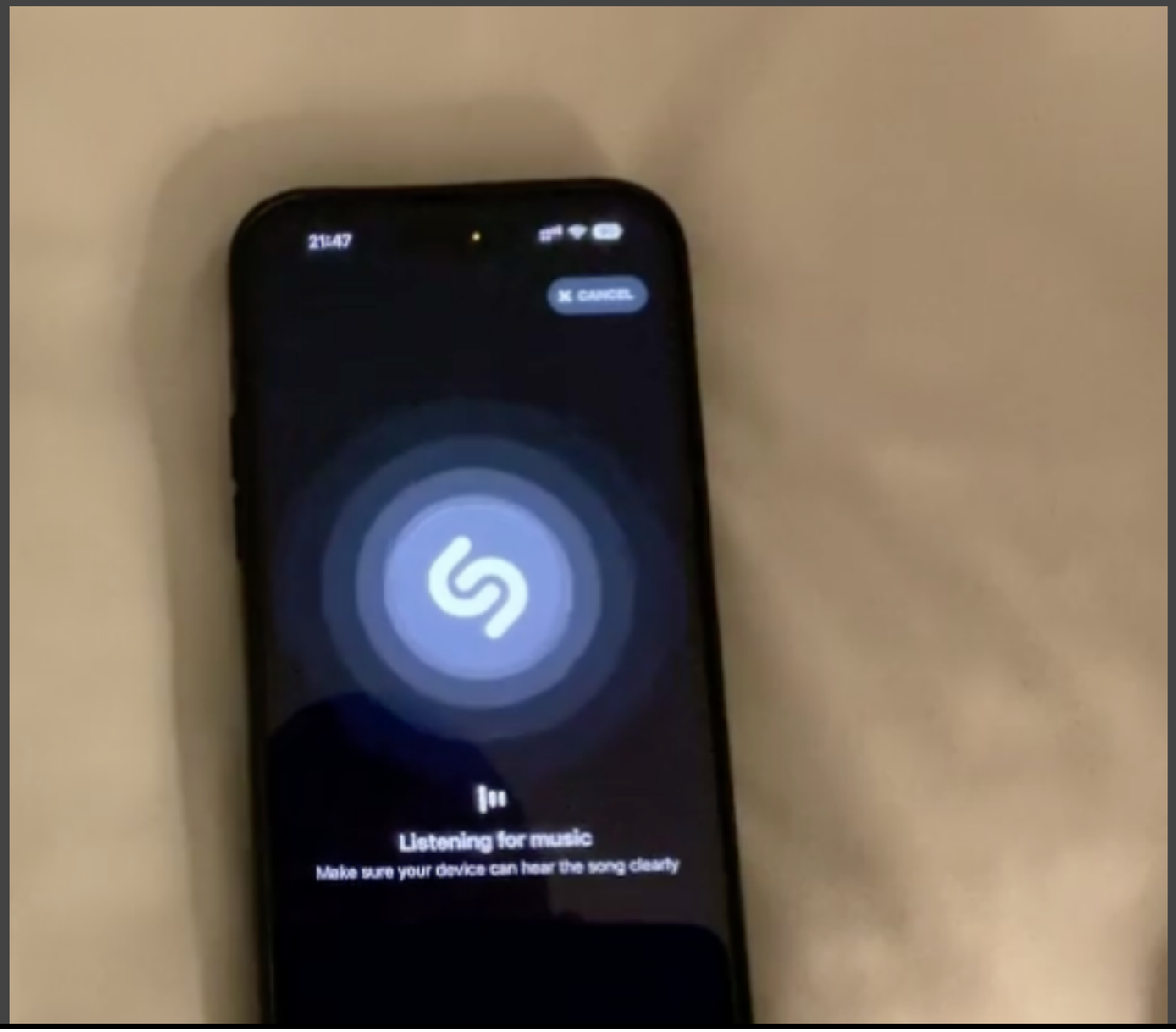



https://willdrevo.com/fingerprinting-and-audio-recognition-with-python/

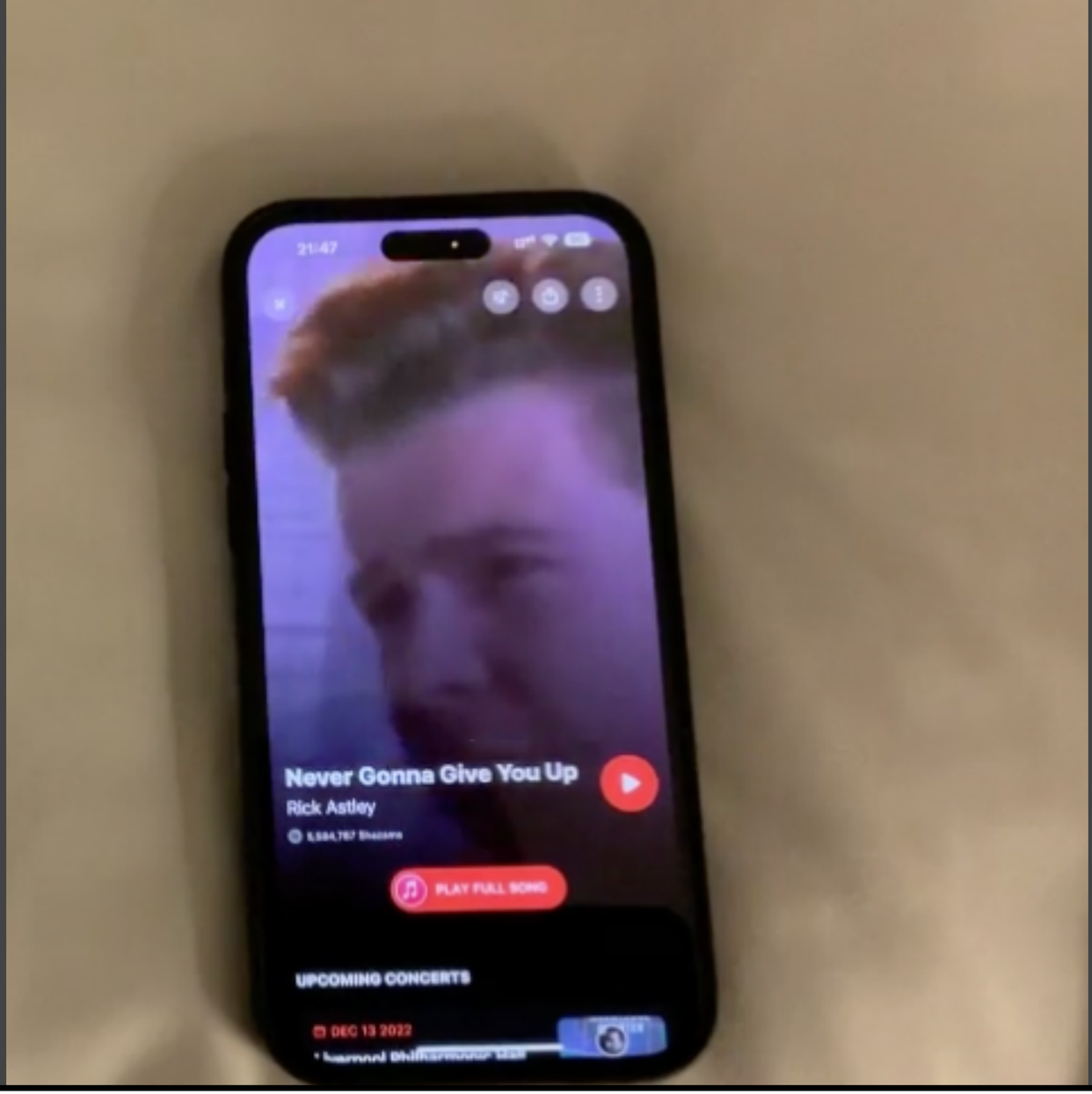



https://github.com/worldveil/dejavu

**Notes for the Viewer:**
**I found a great post about fingerprinting audio, along with a framework I could modify/play with.**




**Notes for the Viewer:**
**Stills from a video showing how Shazam identifies music.**




**Notes for the Viewer:**
**Stills from a video showing how Shazam identifies music.**

```
33, 72, 77, 62, 348, 6047, 75, 3054, 72, 3861, 71, 164, 70, 2817, 69, 75, 2966, 71, 168, 85, 50, 2753, 69, 120, 140, 2788, 119,
46, 4388, 70, 3035, 118, 71, 87, 2842, 118, 69, 109, 2825, 118, 72, 149, 8415, 117, 69, 130, 126, 2653, 120, 120, 134, 117, 123,
78, 2506, 71, 165, 63, 2820, 69, 75, 2963, 123, 35, 9215, 122, 8780, 76, 3032, 58, 30018, 123, 2909, 69, 129, 86, 2826, 71, 118
, 2920, 66, 69, 19514, 118, 34, 2947, 69, 170, 10638, 122, 8939, 112, 2974, 71, 122, 3651, 119, 33, 2968, 72, 3034, 68, 165, 48,
2821, 71, 164, 81, 127, 2702, 71, 117, 2915, 118, 72, 127, 55, 2752, 72, 121, 2915, 121, 66, 130, 120, 24, 144, 7685, 124, 2962
, 68, 121, 129, 128, 123, 122, 175, 7102, 68, 121, 141, 2783, 122, 72, 126, 117, 130, 123, 169, 6882, 103, 74, 8857, 58, 4909, 1
18, 71, 149, 2737, 170, 34, 2953, 121, 28123, 70, 9852, 118, 10003, 78, 13889, 69, 79, 14458, 122, 2928, 73, 10876, 52, 10914, 7
4, 3018, 73, 6807, 71, 6927, 75, 4953, 123, 2984, 120, 2976, 71, 3031, 118, 34, 2962, 87, 2973, 27, 111, 100, 2910, 76, 3025, 11
9, 41, 2944, 75, 3025, 71, 165, 49, 2951, 72, 3012, 118, 71, 181, 2756, 120, 6602, 68, 121, 145, 2790, 109, 35, 4619, 69, 120, 9
3, 2833, 118, 72, 127, 118, 216, 2478, 133, 2967, 119, 4494, 74, 1766, 13189, 145, 8882, 72, 3026, 73, 11744, 121, 13932, 72, 49
56, 74, 8923, 71, 165, 45, 2834, 71, 194, 54, 52, 2753, 118, 69, 96, 2835, 122, 33, 8594, 118, 32, 2971, 71, 164, 84, 174, 68, 2
1, 106, 118, 124, 124, 173, 71, 128, 84, 1685, 69, 120, 177, 35, 2729, 118, 72, 127, 60, 8047, 72, 164, 71, 2804, 69, 118, 82, 2
851, 71, 168, 73, 2809, 69, 118, 132, 165, 76, 185, 34, 2372, 73, 8540, 119, 47, 2949, 71, 164, 50, 2834, 70, 165, 84, 114, 2695
, 68, 118, 133, 42, 2770, 118, 34, 8289, 72, 12838, 122, 2978, 120, 21792, 72, 3014, 121, 10742, 119, 33, 13984, 74, 3009, 124,
12744, 76, 4968, 72, 11883, 121, 3881, 202, 7797, 72, 11847, 122, 12975, 122, 15887, 121, 10802, 72, 10932, 120, 10934, 78, 1488
5, 72, 9921, 121, 8857, 122, 7816, 118, 7892, 123, 5906, 125, 4948, 90, 7917, 92, 9839, 121, 6847, 117, 6926, 119, 6912, 74, 693
4, 77, 12963, 121, 10815, 72, 13903, 74, 4935, 75, 3028, 71, 3800, 120, 5879, 121, 6884, 70, 13945, 74, 10916, 131, 2812, 232, 9
388, 221, 3750, 158523, 102, 518, 8392, 52958, 120072, 2775, 88, 716, 2824, 175514, 155465, 113794, 84, 60724, 223924, 46940, 15
542, 124961, 93668, 179892, 500224, 170839, 172608, 130, 327996, 177188, 4764, 70169, 102, 552, 82322, 16174, 76, 6003, 72854, 9
1, 834, 125699, 522332, 133, 11213, 75, 2723, 67, 165, 48, 2743, 68, 117, 105, 2820, 118, 112, 2894, 63, 56736, 130, 2741, 117,
59, 86, 2738, 71, 140, 2888, 118, 68, 102, 2819, 118, 72, 168, 2766, 80, 78, 14312, 77, 3009, 69, 118, 99, 2776, 117, 121, 32860
, 79, 3029, 77, 67, 2714, 79, 3010, 71, 171, 74, 173, 2529, 73, 68, 2968, 119, 71, 107, 2821, 79, 3021, 71, 172, 67, 81, 2738, 6
3, 121, 150, 2784, 118, 71, 187, 77, 2672, 71, 122, 2919, 119, 34, 2922, 140, 2993, 118, 71, 181, 88, 2669, 70, 75, 2963, 119, 3
```

**Notes for the Viewer:**

**I take the microseconds in between and make them a frequency in an audio file using wavio and pydub**

```
58, 42, 2439, 113, 645, 2354, 149, 535, 11752, 135, 60, 13047, 3099, 42, 69, 3056, 1408, 184, 11131, 3099, 59, 5197, 3364, 48, 1
76, 18, 91, 42758, 3741, 68, 111, 2507, 58, 5880, 2265, 2251
```

**wavio 0.0.4**

```
pip install wavio
```

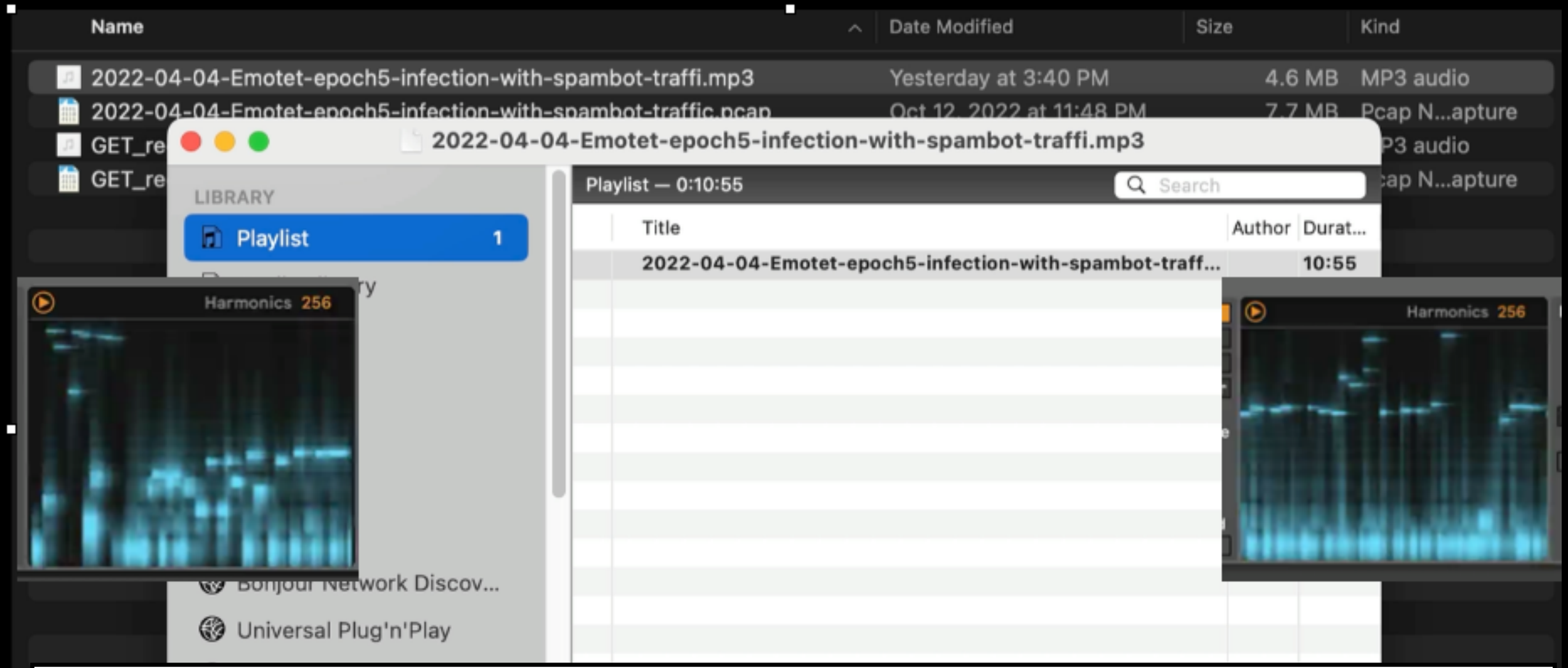
https://github.com/WarrenWeckesser/wavio

**pydub 0.25.1**

```
pip install pydub
```

http://pydub.com/

DEEPSEC




**Notes for the Viewer:**
**Still from a video: Here's what it sounds like when I convert the microseconds in between to different frequencies, each played for .02 seconds. The windows: Spectrum analysis for each file**

# Same Malware Sample/ Different Environments

**Notes for the Viewer:**
**Let's see what happens when malware is run in different environments, where bandwidth might make the timing differ. Will we still see a signature match?**

https://bazaar.abuse.ch/sample/ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa

MALWARE bazaar by ABUSE.ch

Browse | Upload | Hunting | API | Export | Statistics | FAQ | About | Login

Browse / Malware sample

# MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

## Database Entry

AgentTesla

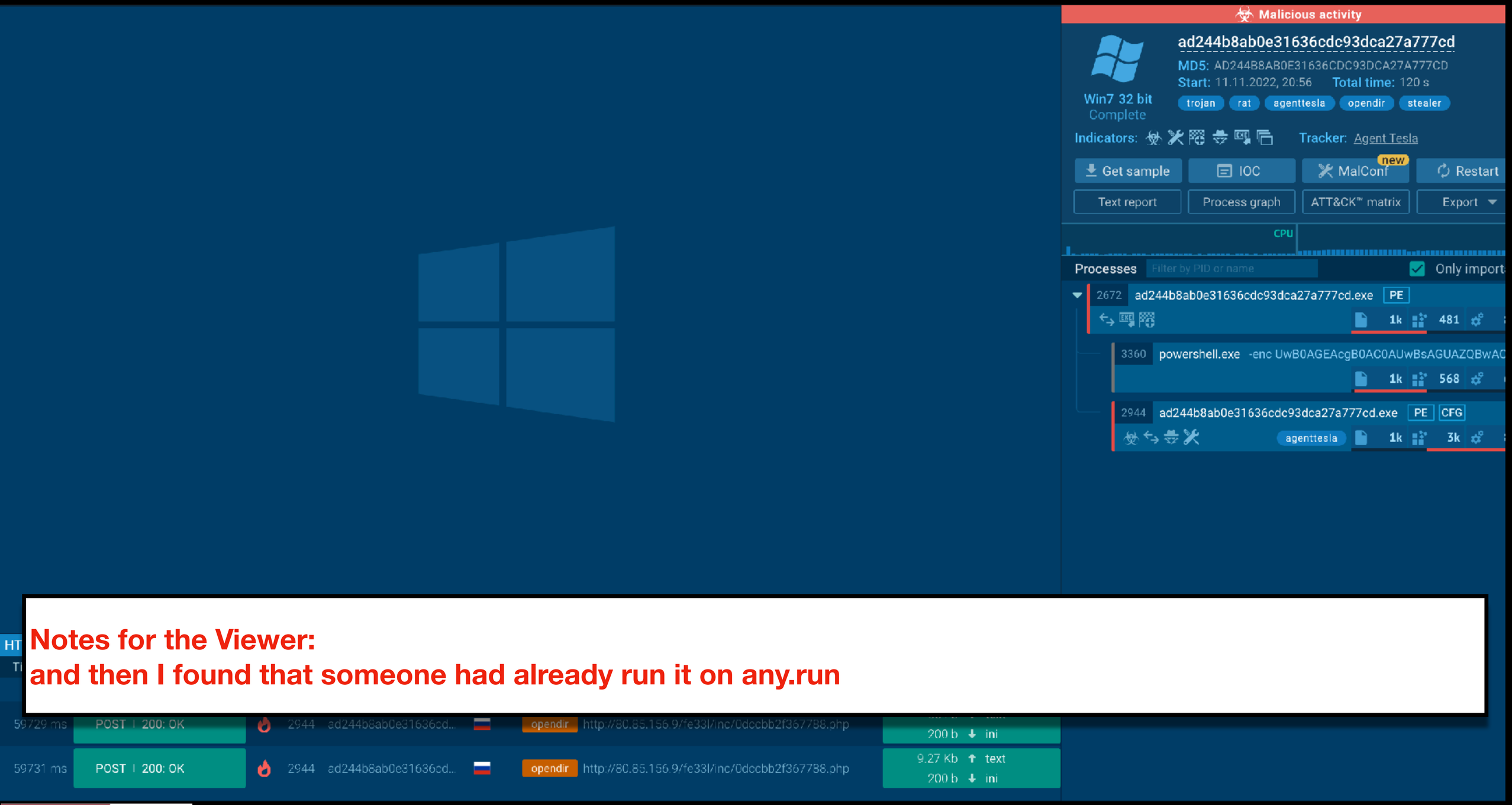
Vendor detections: **17**

**Notes for the Viewer:**
**I went on malwarebazaar and found a copy of Agent Tesla**

Intelligence 17 | IOCs | YARA 3 | File information | Comments 1 | Actions

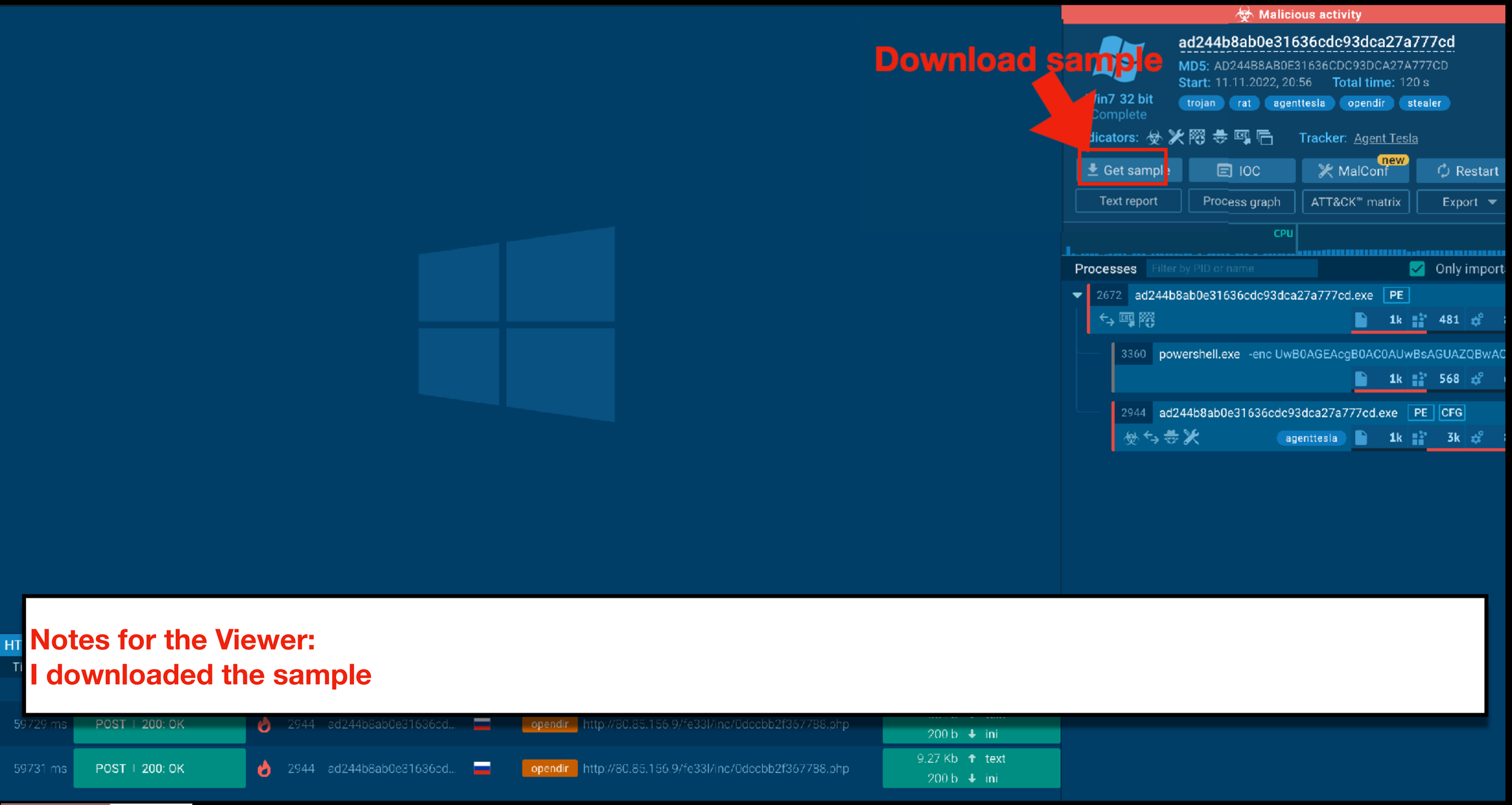
| | |
|---|---|
| **SHA256 hash:** | ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f |

DEEPSEC




**Notes for the Viewer:**
**and then I found that someone had already run it on any.run**

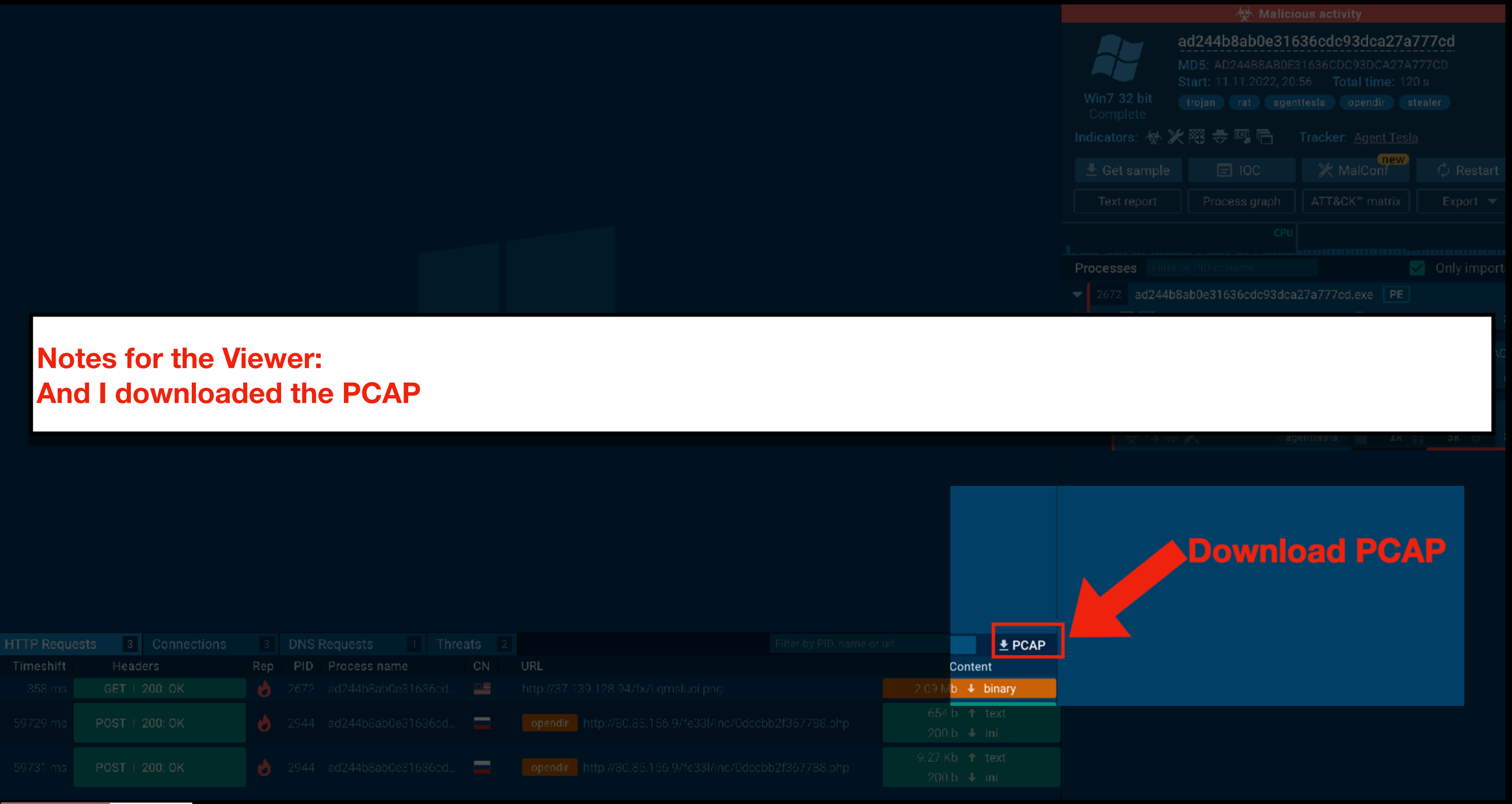
DEEPSEC mple/ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f/ → https://app.any.run/tasks/e9aeecd4-dd3f-4cf1-8275-9d505c1c3631/#




**Notes for the Viewer:**
**I downloaded the sample**

DEEPSEC mple/ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f/ → https://app.any.run/tasks/e9aeecd4-dd3f-4cf1-8275-9d505c1c3631/#

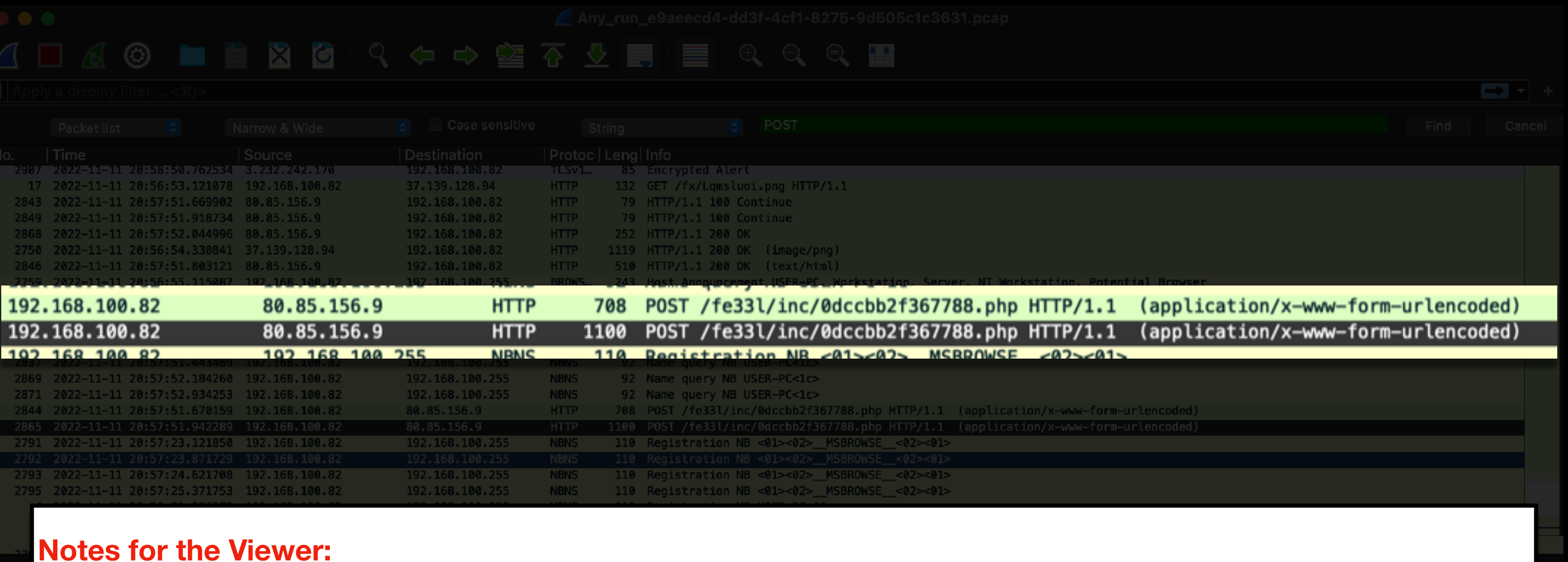
**Notes for the Viewer:**
**And I downloaded the PCAP**




DEEPSEC mple/ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f/ → https://app.any.run/tasks/e9aeecd4-dd3f-4cf1-8275-9d505c1c3631/#

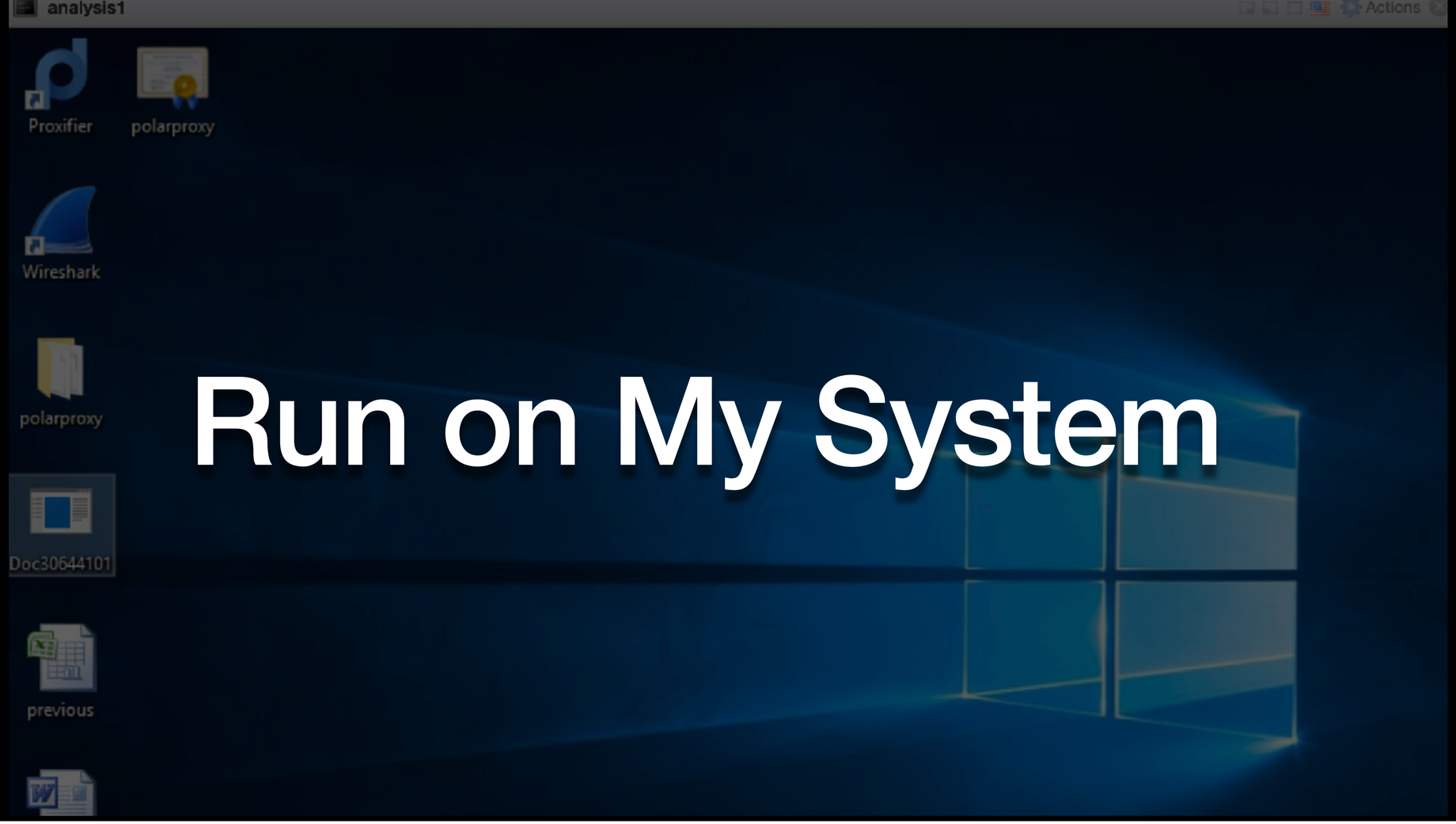
# any.run: 192.168.100.82 -> 80.85.156.9

POST /fe33l/inc/0dccbb2f367788.php




**Notes for the Viewer:**
**Here is just the traffic from that machine to any hosts**

DEEPSEC




# Run on My System

**Notes for the Viewer:**
**I then ran the same malware sample on my own malware analysis system for about 5 minutes while collecting the traffic on my gateway**

DEEPSEC

# Me: 192.168.1.99 -> 80.85.156.9

POST /fe33l/inc/0dccbb2f367788.php

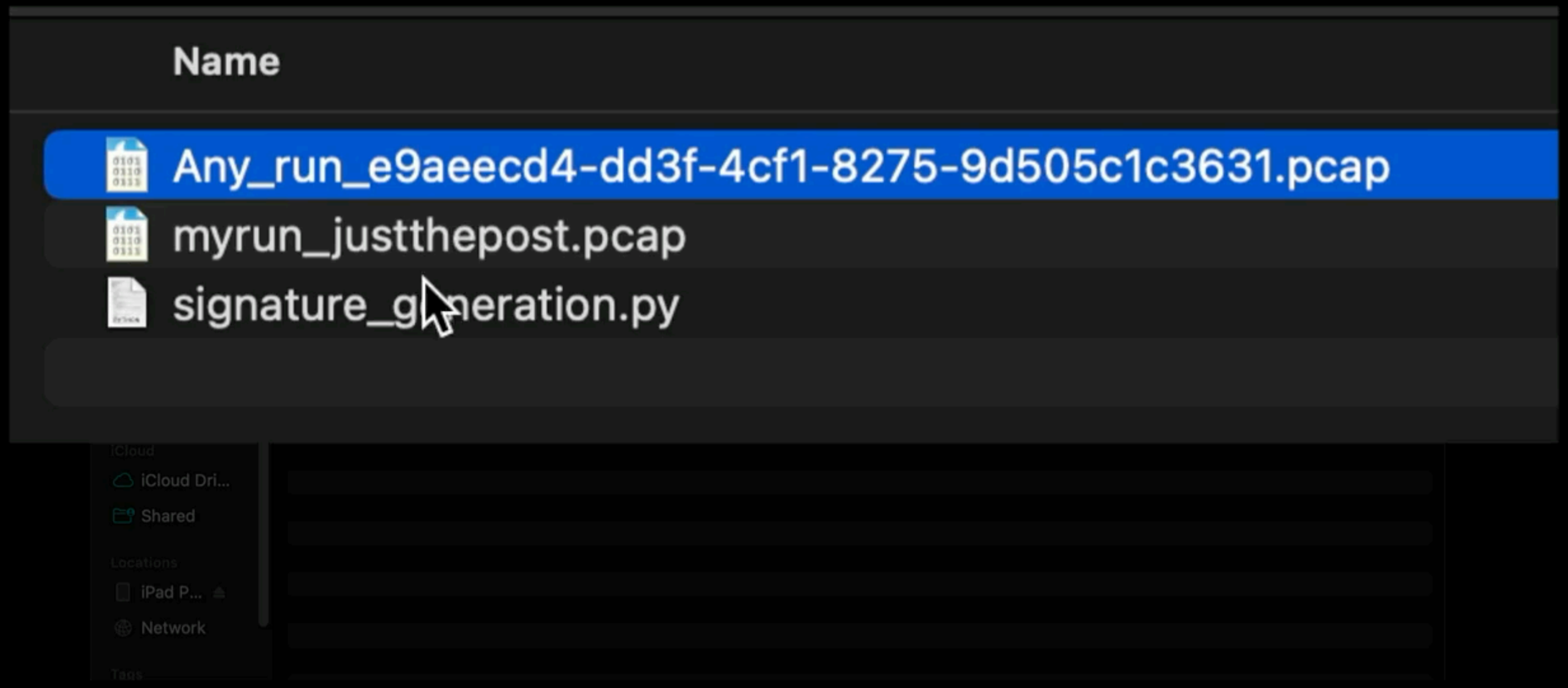
Apply a display filter ... <⌘/>

| No. | Time | Source | Destination | Protoc | Leng | Info |
|---|---|---|---|---|---|---|
| 16 | 2022-11-12 00:16:41.052871 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=3181 Win=132096 Len=0 |
| 17 | 2022-11-12 00:16:41.053645 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=6085 Win=132096 Len=0 |
| 18 | 2022-11-12 00:16:41.054304 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=10441 Win=132096 Len=0 |
| 19 | 2022-11-12 00:16:41.054829 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=11893 Win=132096 Len=0 |
| 20 | 2022-11-12 00:16:41.055996 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=14797 Win=132096 Len=0 |
| 21 | 2022-11-12 00:16:41.056680 | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=14797 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU] |
| 22 | 2022-11-12 00:16:41.056680 | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=16249 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU] |
| 23 | 2022-11-12 00:16:41.056680 | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=17701 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU] |
| 24 | 2022-11-12 00:16:41.056680 | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=19153 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU] |
| 25 | 2022-11-12 00:16:41.056680 | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=20605 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU] |
| 26 | 2022-11-12 00:16:41.056726 | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=22057 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU] |
| | | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=26413 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled |
| | | 192.168.1.99 | 80.85.156.9 | TCP | 1506 | 49719 → 80 [ACK] Seq=27865 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled |
| | | 192.168.1.99 | 80.85.156.9 | HTTP | 178 | POST /fe33l/inc/0dccbb2f367788.php HTTP/1.1 (application/x-www-form-urlencoded) |
| | | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=20605 Win=132096 Len=0 |
| | | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=26413 Win=132096 Len=0 |
| 34 | 2022-11-12 00:16:41.284304 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=26 Ack=29441 Win=132096 Len=0 |
| 35 | 2022-11-12 00:16:41.349047 | 80.85.156.9 | 192.168.1.99 | HTTP | 308 | HTTP/1.1 200 OK |
| 36 | 2022-11-12 00:16:41.403414 | 192.168.1.99 | 80.85.156.9 | TCP | 60 | 49719 → 80 [ACK] Seq=29441 Ack=280 Win=262400 Len=0 |
| 37 | 2022-11-12 00:16:46.838844 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [FIN, ACK] Seq=280 Ack=29441 Win=132096 Len=0 |
| 38 | 2022-11-12 00:16:46.843653 | 192.168.1.99 | 80.85.156.9 | TCP | 60 | 49719 → 80 [ACK] Seq=29441 Ack=281 Win=262400 Len=0 |
| 39 | 2022-11-12 00:18:21.353694 | 192.168.1.99 | 80.85.156.9 | TCP | 60 | 49719 → 80 [FIN, ACK] Seq=29441 Ack=281 Win=262400 Len=0 |
| 40 | 2022-11-12 00:18:21.578559 | 80.85.156.9 | 192.168.1.99 | TCP | 60 | 80 → 49719 [ACK] Seq=281 Ack=29442 Win=132096 Len=0 |

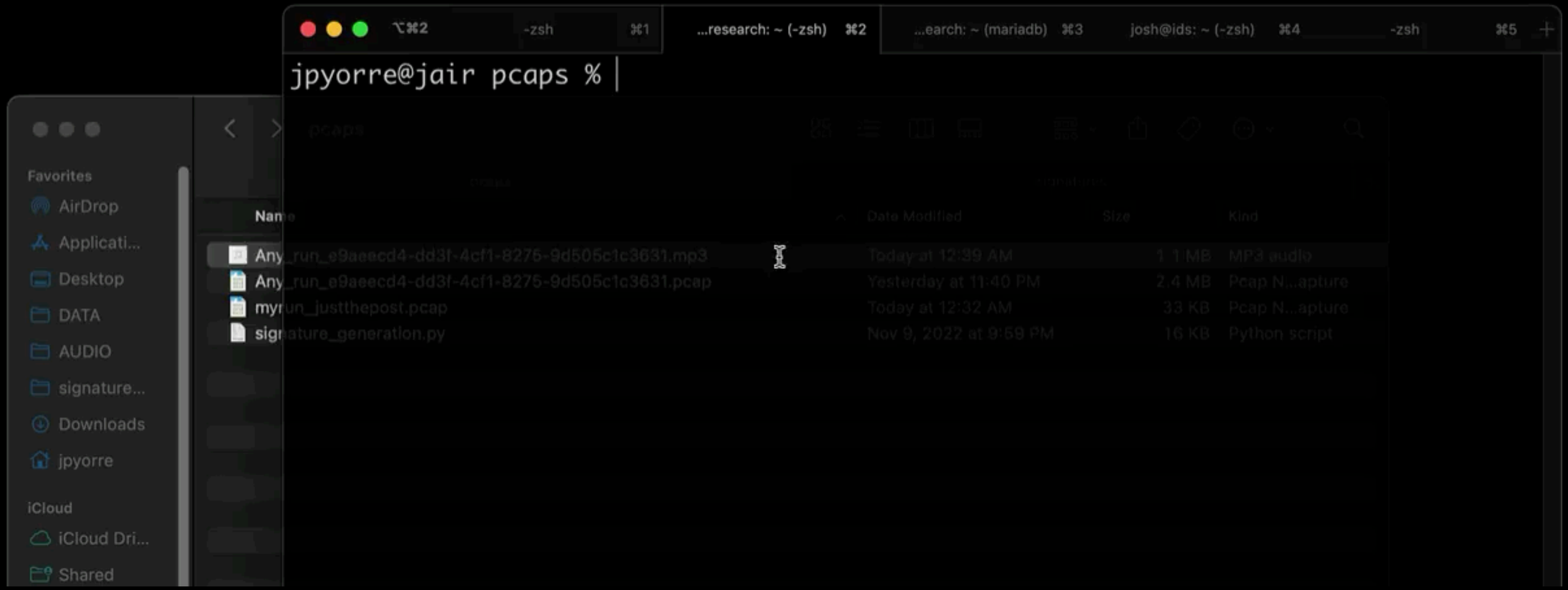
**Notes for the Viewer:**
**Seeing the same type of traffic**

# Shazam it!

# Create an audio file from the any.run PCAP



# Create an audio file from my PCAP



# Identify Threat (AKA Shazam it)

```
jpyorre@jair dejavu % python3 dejavu.py --recognize file ~/Desktop/pcaps/myrun_justthepost.mp3
{'total_time': 0.010400772094726562, 'fingerprint_time': 0.0063121318817138 67, 'query_time': 0.00281691551
2084961, 'align_time': 0.0012142658233642578, 'results': [{'song_id': 1, 'song_name': b'Any_run_e9aeecd4-d
d3f-4cf1-8275-9d505c1c3631', 'input_total_hashes': 518, 'fingerprinted_hashes_in_db': 33606, 'hashes_match
ed_in_input': 22, 'input_confidence': 0.04, 'fingerprinted_confidence': 0.0, 'offset': 257, 'offset_second
s': 11.93506, 'file_sha1': b'73847241D576F998CF526A15E9002D5517737BAA'}]}
```

**Notes for the Viewer:**
**Video still after running the mp3 file through the audio recognition script and it identifies the ‘song’ it’s a part of.**

# Same, but signature method based off percentages

**Notes for the Viewer:**
**Repeating this process, but using the quicker and more practical signature method we've been building during this presentation.**

```
jpyorre@jair 2_signature_generation %
```

2_signature_generation

Favorites
- AirDrop
- Applicati...
- Desktop
- DATA
- AUDIO
- signature...
- Downloads
- jpyorre

iCloud
- iCloud Dri...
- Shared

2_signature_generation | signatures

| Name | Date Modified | Size | Kind |
|---|---|---|---|
| anyrun_justthepost.pcap | Today at 12:31 AM | 14 KB | Pcap N...apture |
| my_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631.pcap | Today at 12:26 AM | 2.4 MB | Pcap N...apture |
| signature_generation.py | Today at 1:12 AM | 16 KB | Python script |

Tags
- Red
- Orange

**Notes for the Viewer:**
**Video Still: We have both PCAPs, one from the any.run analysis and one from my own.**

DEEPSEC

```
jpyorre@jair 2_signature_generation % python3 signature_generation.py anyrun_jus
tthepost.pcap
[11407, 150, 139, 12029, 132776, 257, 11133, 121829, 37241, 11690, 66682, 215, 2
2, 8, 10996, 25, 128, 17, 6, 5, 4, 11938, 25, 12, 10, 126, 18, 11006, 25, 91676,
 201768, 312995, 181]
jpyorre@jair 2_signature_generation %
```

**Notes for the Viewer:**
**Video Still: We generate a signature from a PCAP that has just the POST data from Agent Tesla**

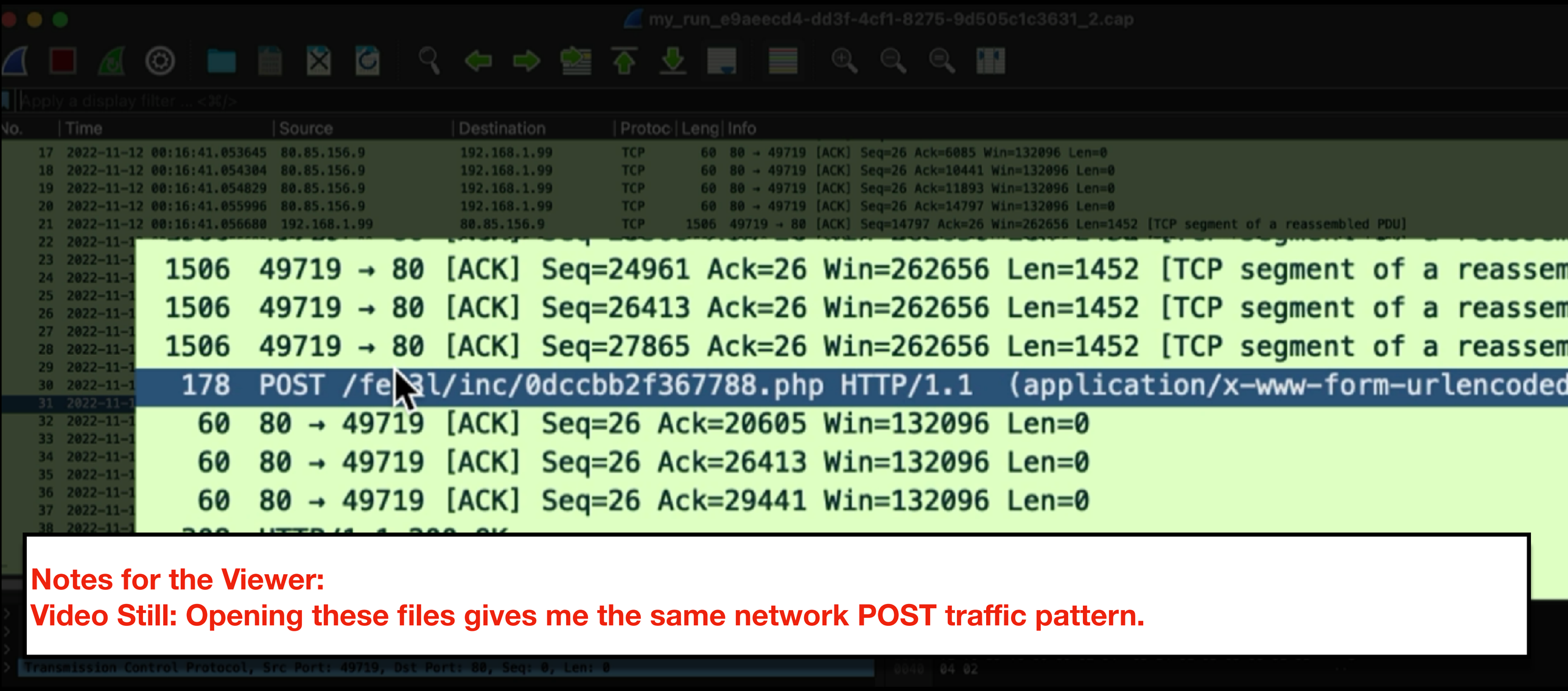
signatures.json

```
{
    "Agent Tesla POST":[11407, 150, 139, 12029, 132776, 257, 11133, 121829, 37241, 11690, 66682, 215, 22,
        8, 10996, 25, 128, 17, 6, 5, 4, 11938, 25, 12, 10, 126, 18, 11006, 25, 91676, 201768, 312995,
        181]
}
```

**Notes for the Viewer:**
**Video Still: and we put that signature in our signatures.json file.**

```
jpyorre@jair 2_signature_generation % python3 test_signature.py my_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631.pcap
[5, 5, 4, 5, 5, 4, 4, 4, 1, 2, 1, 2, 22]
[5, 2, 5, 5, 3, 2, 5, 4, 63]
'my_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631_0.cap: Agent Tesla POST, 65
'my_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631_1.cap: Agent Tesla POST, 64
'my_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631_2.cap: Agent Tesla POST, 60
```

**Notes for the Viewer:**
**Video Still: Then we run the detection and get back some partial ratios for each flow in the larger PCAP from the malware run on my system.**




**Notes for the Viewer:**
**Video Still: Opening these files gives me the same network POST traffic pattern.**

DEEPSEC

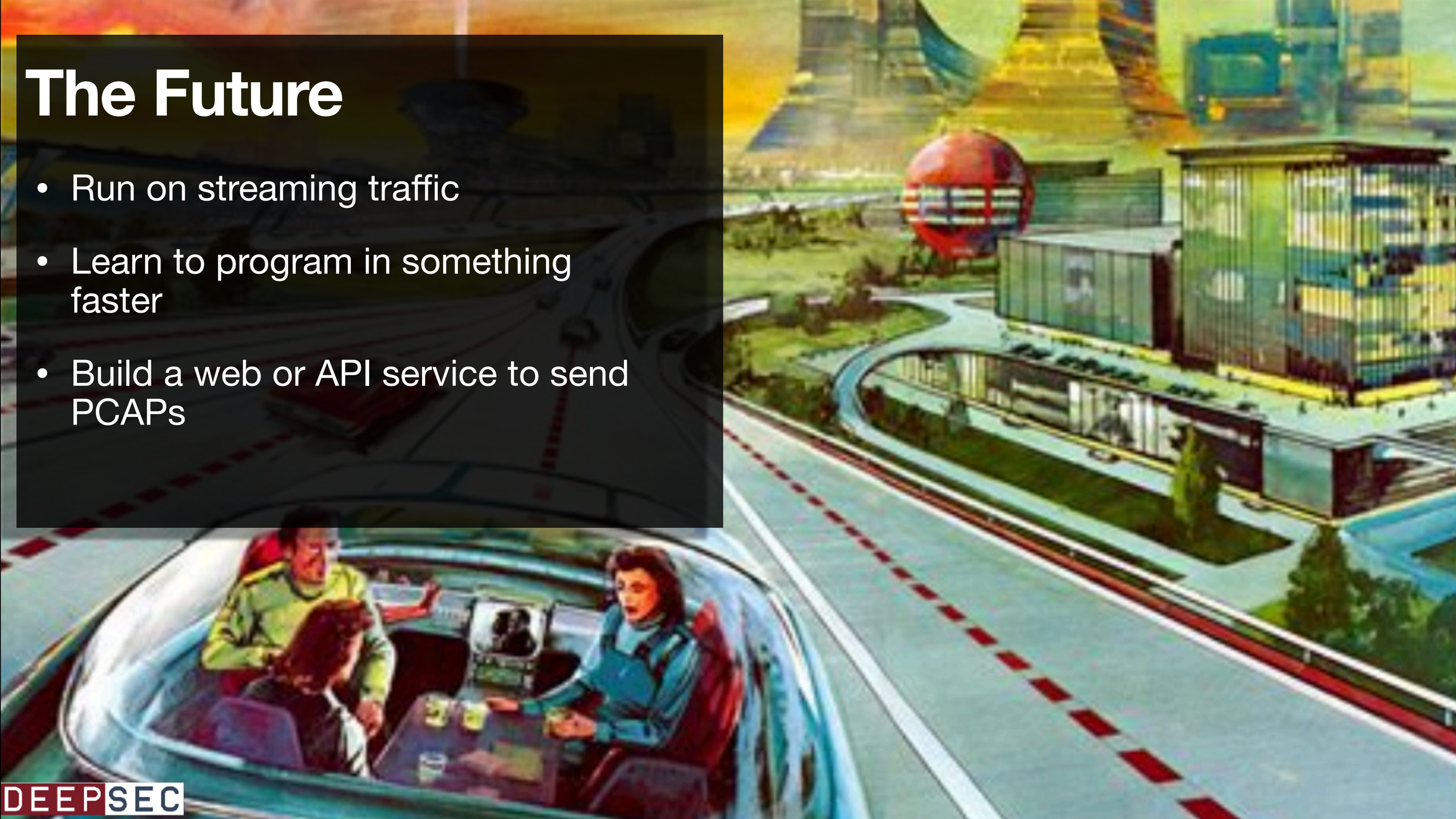
# Going Further

- Using Third Party API's
  - Domain/IP Reputation & Relationships
  - Analysis of Components within the PCAPs

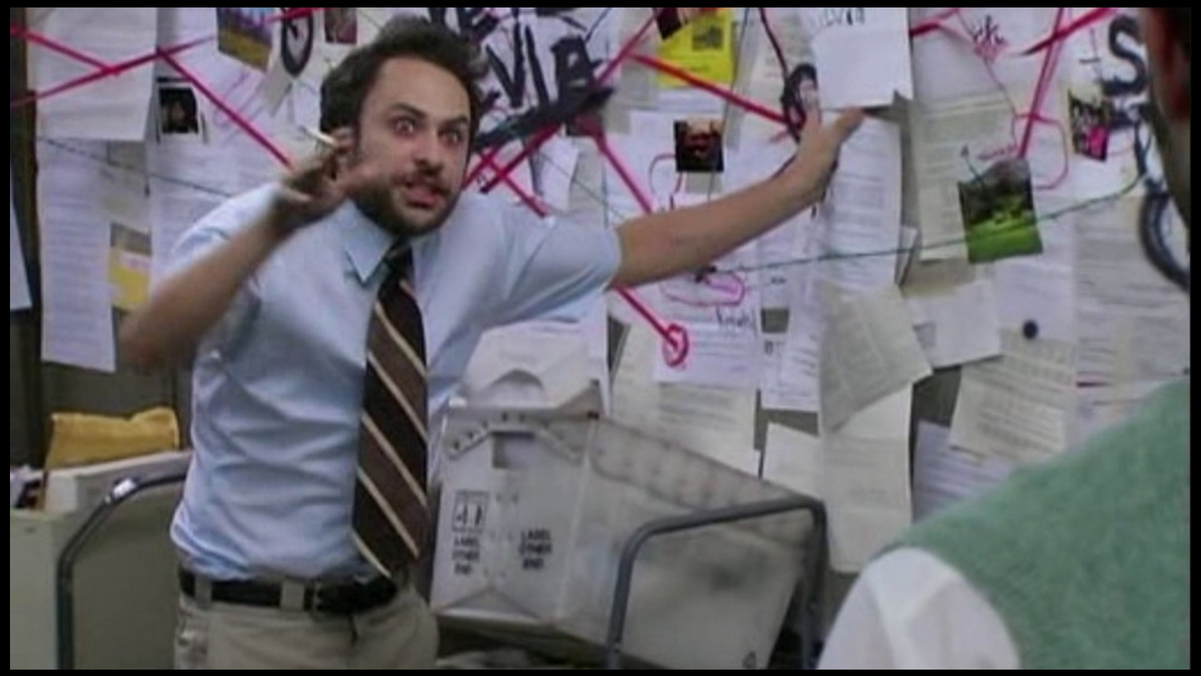
DEEPSEC

# The Future

- Run on streaming traffic
- Learn to program in something faster
- Build a web or API service to send PCAPs



# Code



https://github.com/jpyorre/

Website:
https://pyosec.com

Twitter:
@joshpyorre

Mastodon:
@joshpyorre@infosec.exchange

DEEPSEC