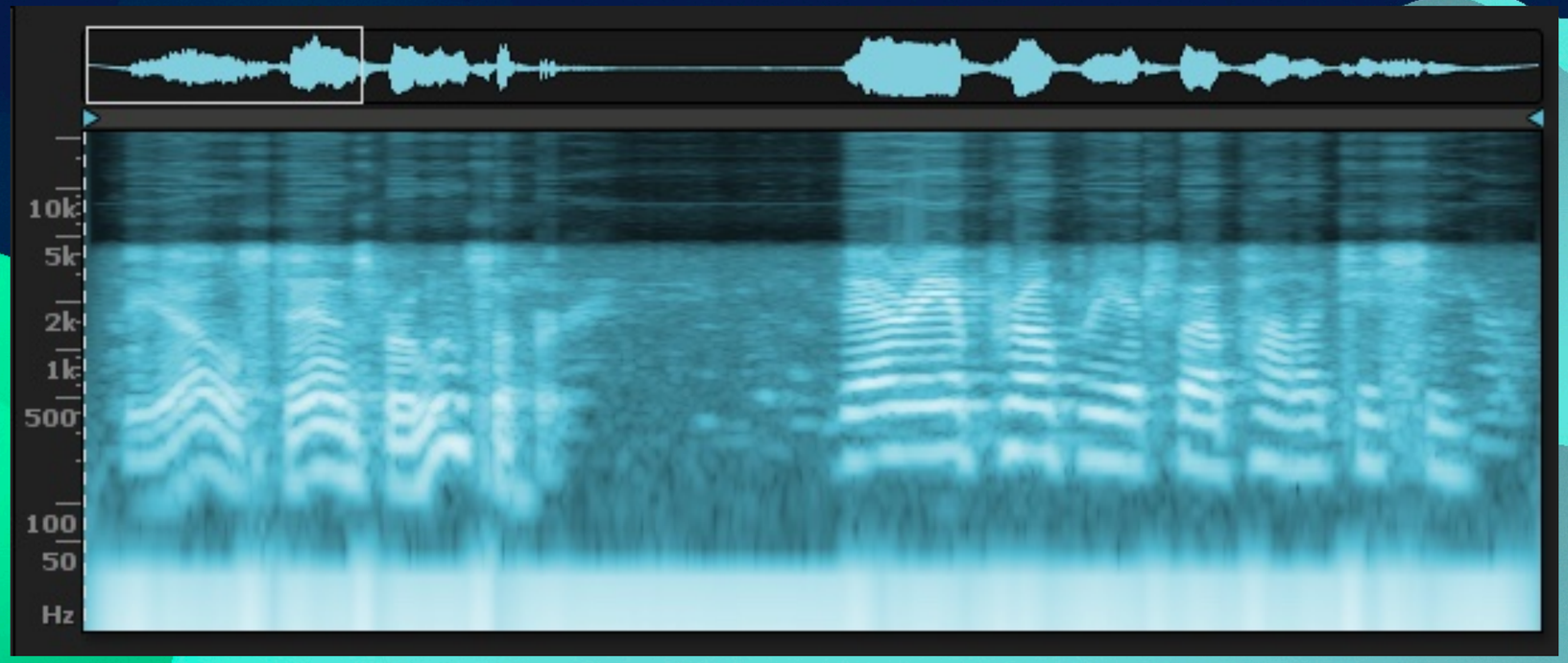
# Signature-based Detection

## Using Network Timing

Josh Pyorre




Defcon Packet Hacking Village, 2024

# JOSH PYORRE Security Researcher




Talos

**Previously:**

zscaler

CISCO Umbrella

OpenDNS

MANDIANT

NASA

# Attribution

Slide Notes

Investigation into an incident often involves getting Attribution, or finding out who created malicious code, compromised a network, stole data, etc..

Slide Notes

# The process of getting Attribution might follow the following procedures: Grab the delivery/dropper URL

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/ |

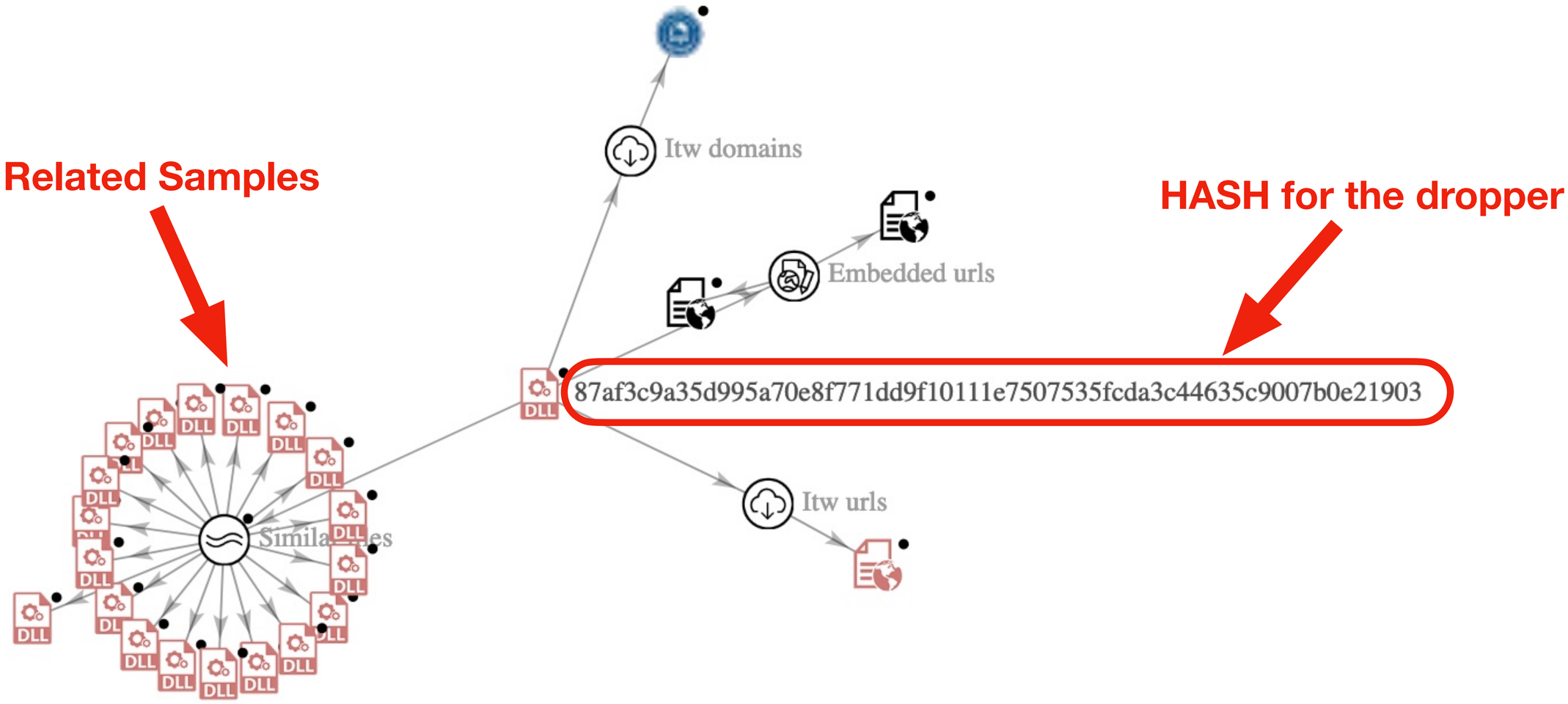
URL

Slide Notes

Get the hash of the file

Slide Notes

# Find related samples



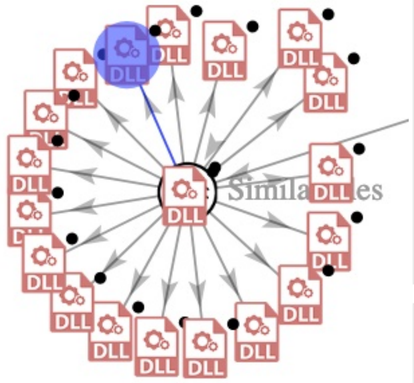
Basic Properties

| | |
|---|---|
| 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



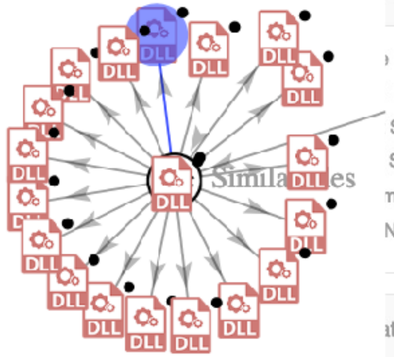
Basic Properties

| | |
|---|---|
| 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



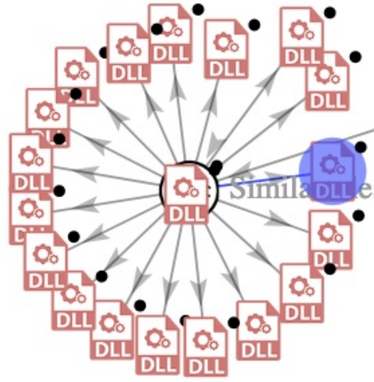
ic Properties

| | |
|---|---|
| | Win32 DLL |
| | 629.50 kB |
| Seen | 2022-11-02 22:10:27 |
| Seen | 2022-11-02 22:10:27 |
| nissions | 1 |
| Name | payload_1.bin |

ations

| | |
|---|---|
| edded urls | 2 |
| lar files | 168 |

and using new intelligence search



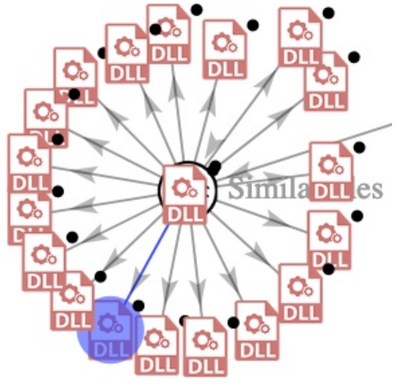
Basic Properties

| | |
|---|---|
| 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



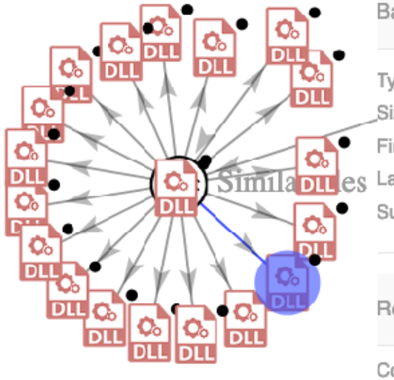
Basic Properties

| | |
|---|---|
| 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



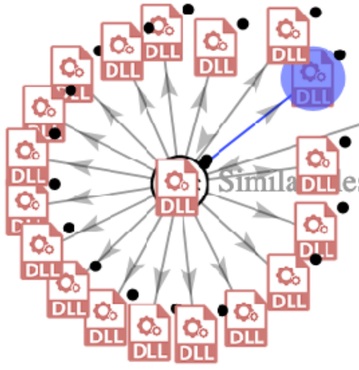
Basic Properties

| | |
|---|---|
| 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 |

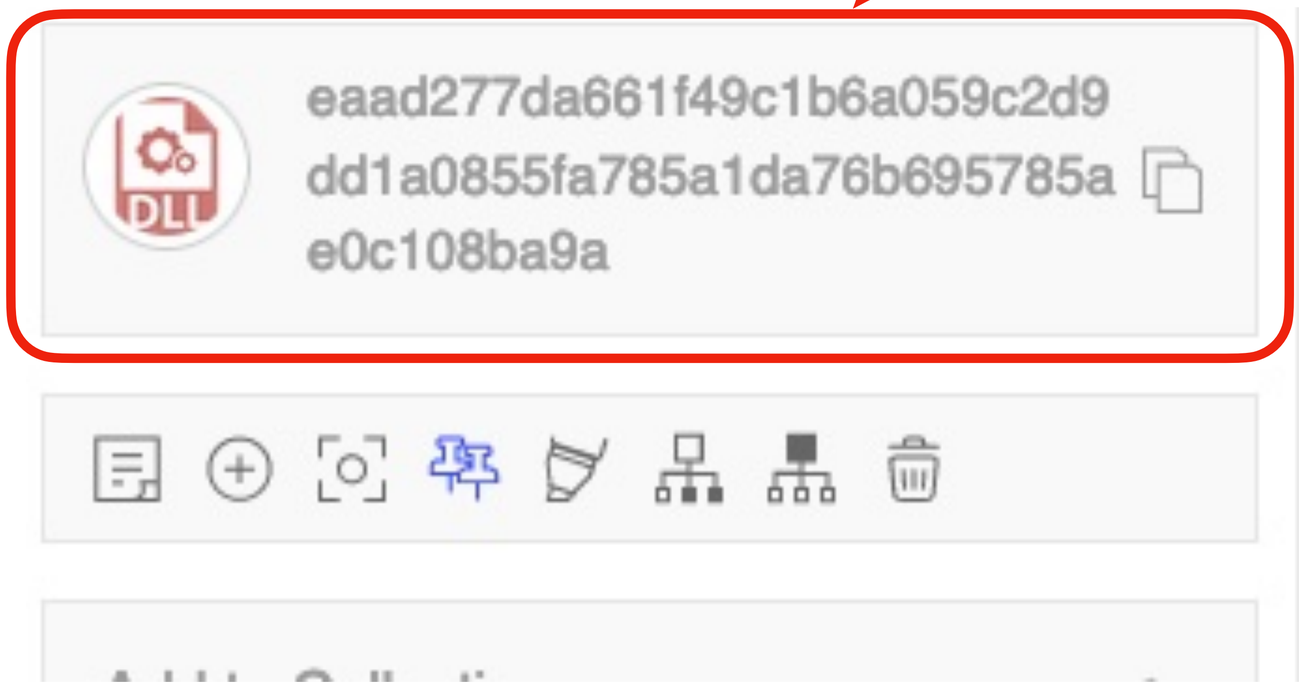
Expand using new intelligence search

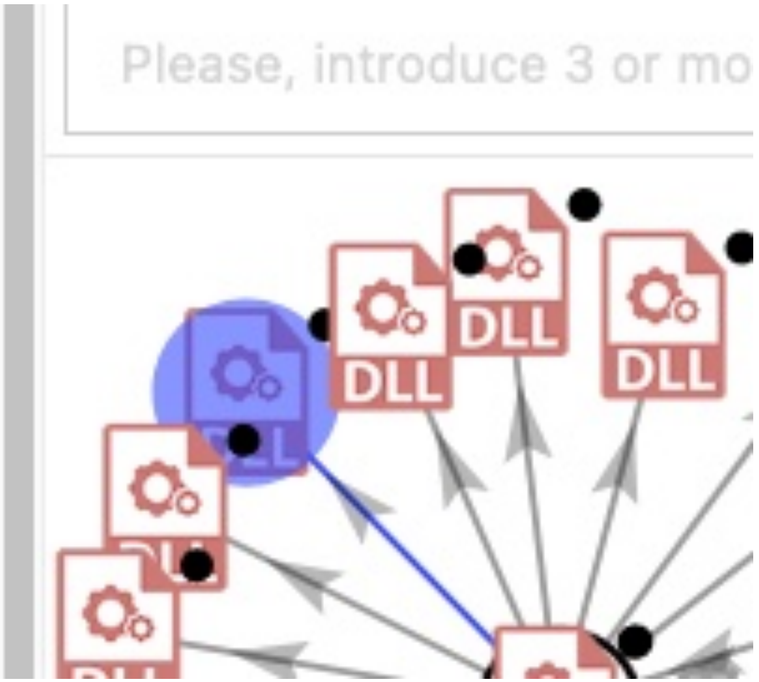


Slide Notes

Look at first and last seen dates, number of embedded URLs, etc…

Copy the HASH for one of the files




Slide Notes

Looking further at the network infrastructure - grabbing the hash for one file

Slide Notes

# Using other sources, find additional, related samples

## Associated Artifacts

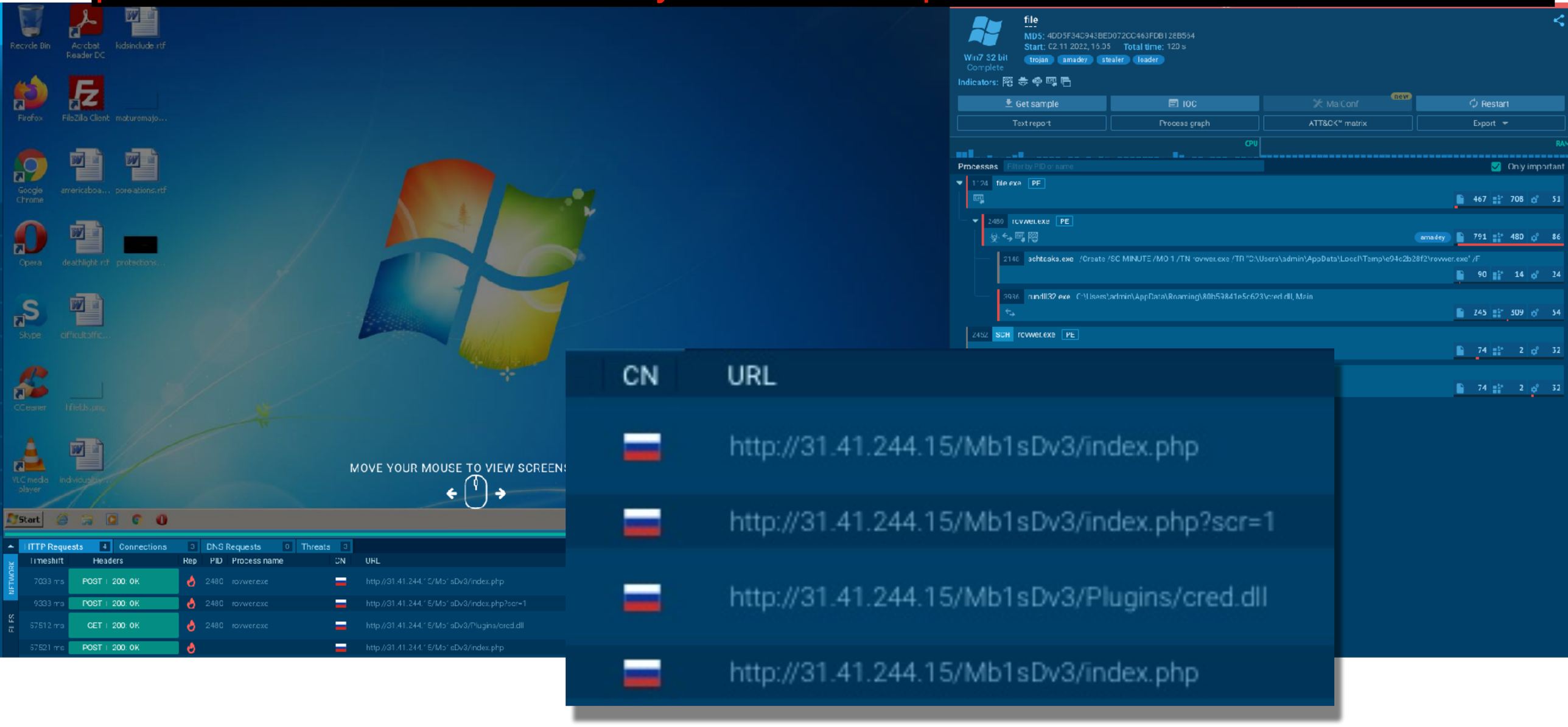
The following artifacts may have been incomplete or missing information about behavioral indicators and network connections.

| 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

Slide Notes

# Other ways to start with attribution: Running a sample in a sandbox. This was a public submission found on any.run. The sample calls out to this IP



Slide Notes

31.41.244.15 INVESTIGATE BACK TO TOP

We can keep following the trail to find additional samples associated with this IP

| 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... 9976466,confidence),UD... (high,[Trj],win /malicious_confidence_1... gen,AI,100),Generic.mg.... (RDML:cqO9EngCGGmT... | PE32 executable (GUI) Intel 80386 | 11/02/2022 |
| | | (W), Generic.Malware,W32.AI... (score:,Trojan.MalPack.G... 9976466,confidence),mal... (high,[Trj],win /malicious_confidence_1... gen,AI,100),Malicious,VH... | | |

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

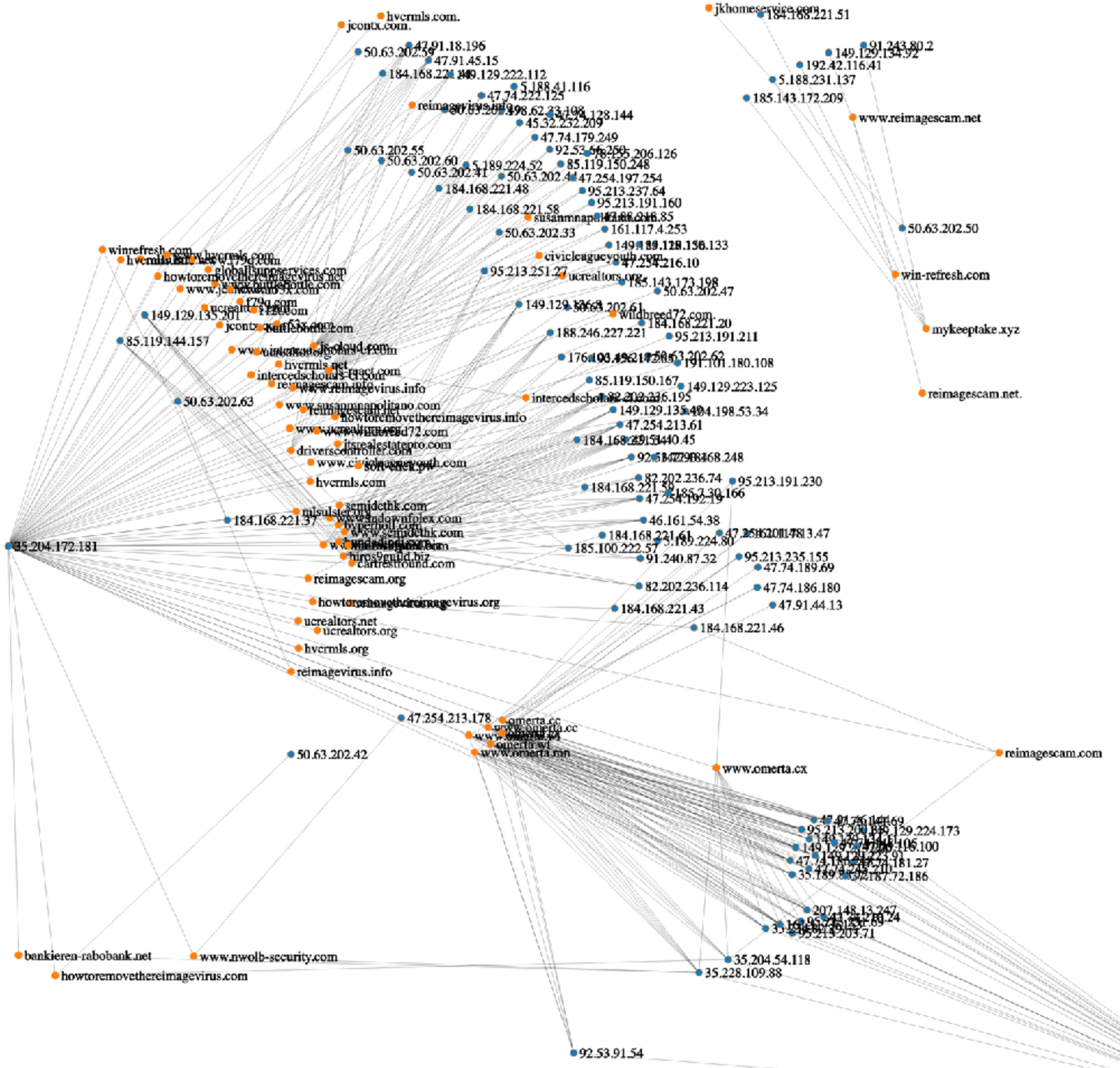
## Network Connections

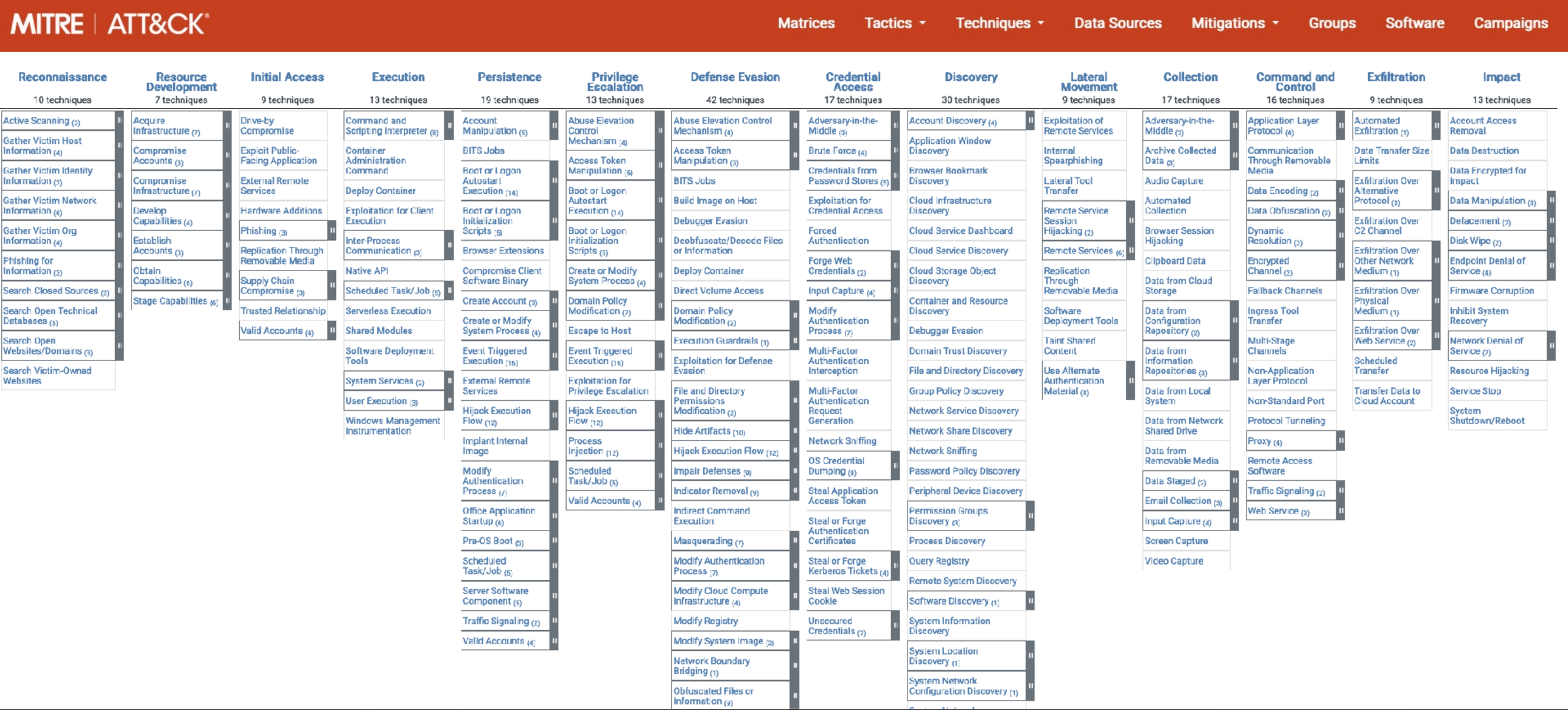
| Destination | URLs | Security Categories |
|---|---|---|
| 31.41.244.15 | 3 | |
| Destination<br>http://31.41.244.15/Mb1sDv3/Plugins/cred64.dll<br>http://31.41.244.15/Mb1sDv3/index.php<br>http://31.41.244.15/Mb1sDv3/index.php?scr=1 | | |

1 - 1 of 1

Slide Notes

# Relate IP's and domains with others

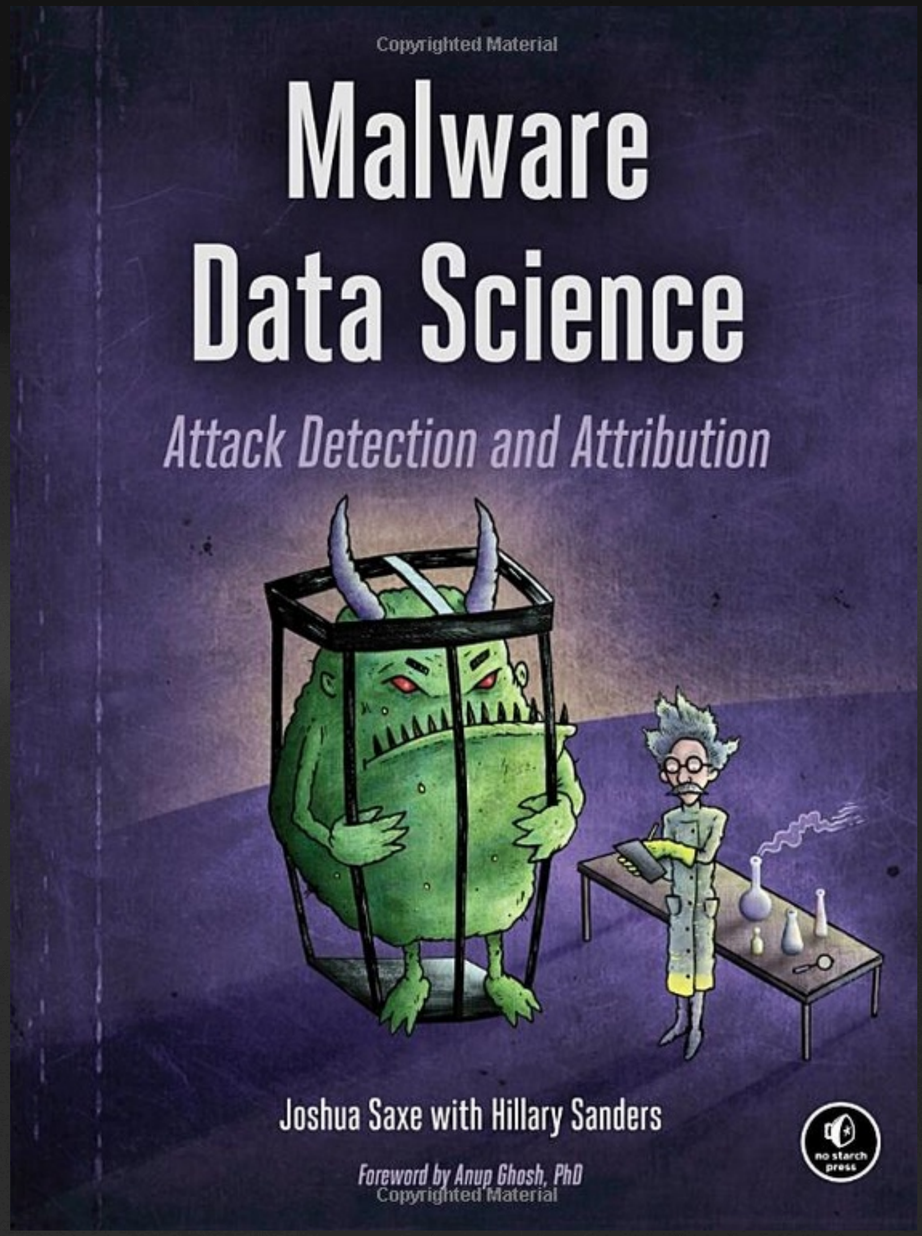





Slide Notes

MITRE ATT&CK is a framework for attribution

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

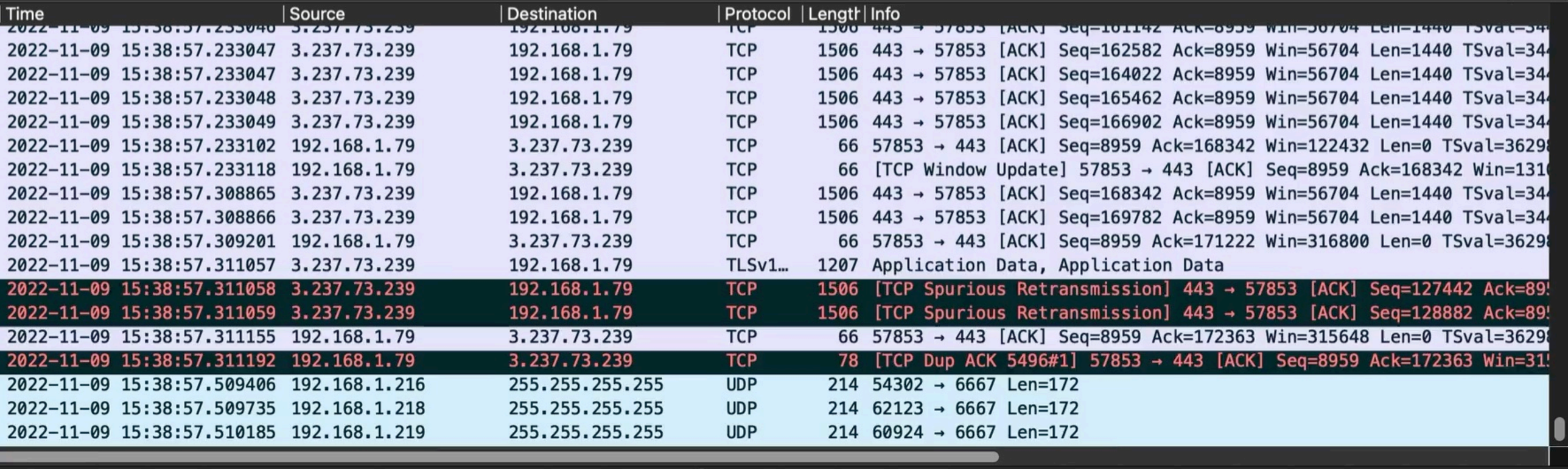
Etc…

…Or just what's in your network

Slide Notes

What kind of Attribution are you interested in? For this talk, we are looking for similar malware variants or malicious activity.


The Problem:
How do we find
bad things in the network?




Slide Notes

Analyzing network traffic requires skills and can be prone to errors. It can also be tedious and time-consuming.

```
POST /wp-includes/fonts/Review/Home/ HTTP/1.1
[illegible]pjpeg, 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
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: triangularllc.com
Content-Length: 77
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
```

Slide Notes

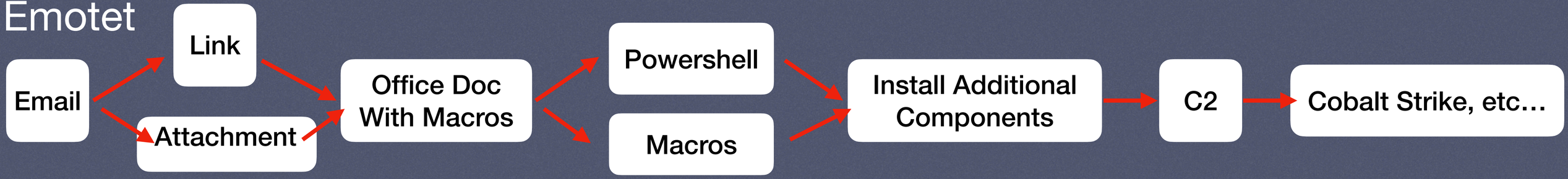
How do you find this kind of thing in lots of traffic?

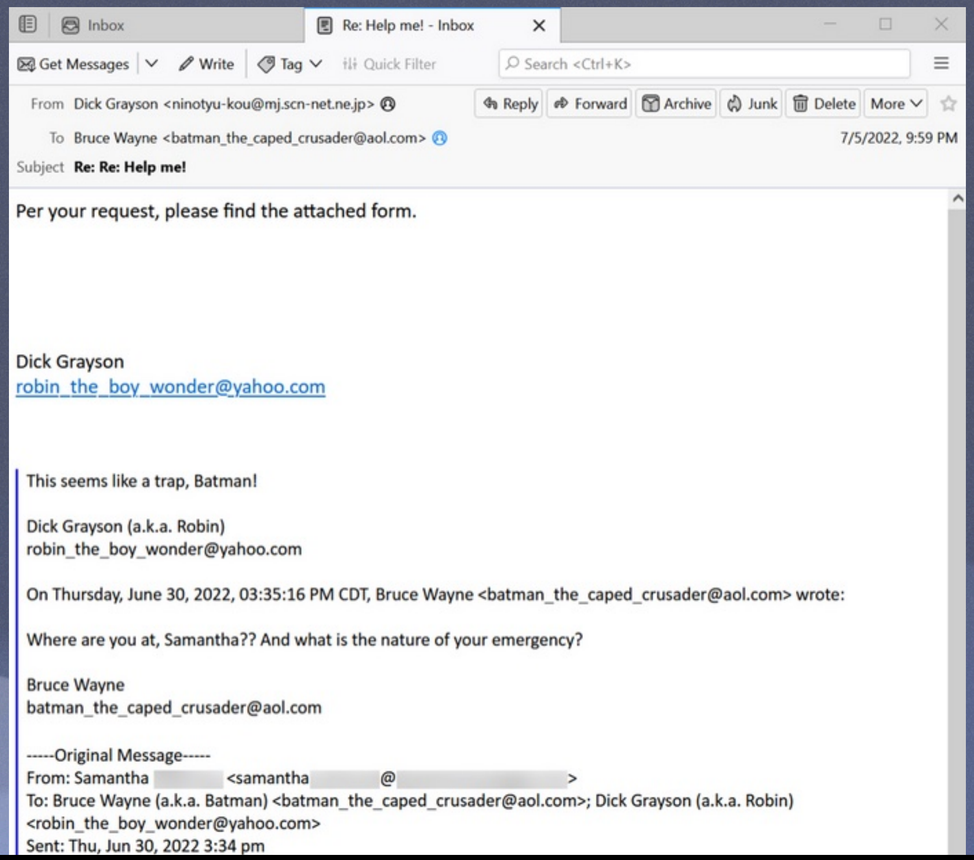
Slide Notes

A quick talk about the infection chain and where to watch for activity within it

# The Infection Chain

# Emotet



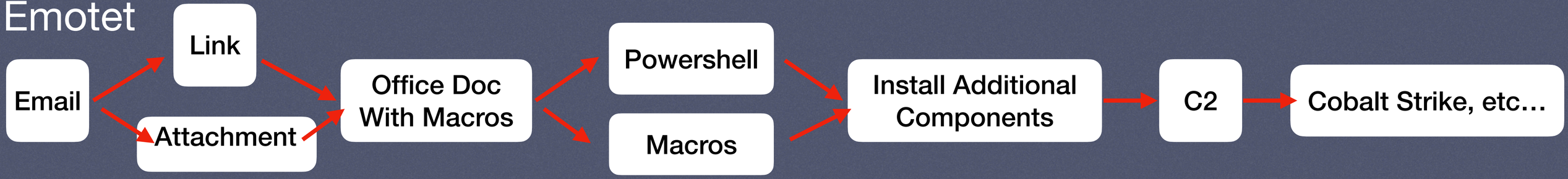


Inbox
Re: Help me! - Inbox
Get Messages
Write
Tag
Quick Filter
Search <Ctrl+K>
From Dick Grayson <ninotyu-kou@mj.scn-net.ne.jp>
Reply
Forward
Archive
Junk
Delete
More
To Bruce Wayne <batman_the_caped_crusader@aol.com>
7/5/2022, 9:59 PM
Subject Re: Re: Help me!
Per your request, please find the attached form.
Dick Grayson
robin_the_boy_wonder@yahoo.com
This seems like a trap, Batman!
Dick Grayson (a.k.a. Robin)
robin_the_boy_wonder@yahoo.com
On Thursday, June 30, 2022, 03:35:16 PM CDT, Bruce Wayne <batman_the_caped_crusader@aol.com> wrote:
Where are you at, Samantha?? And what is the nature of your emergency?
Bruce Wayne
batman_the_caped_crusader@aol.com
-----Original Message-----
From: Samantha <samantha @ >
To: Bruce Wayne (a.k.a. Batman) <batman_the_caped_crusader@aol.com>; Dick Grayson (a.k.a. Robin) <robin_the_boy_wonder@yahoo.com>
Sent: Thu, Jun 30, 2022 3:34 pm

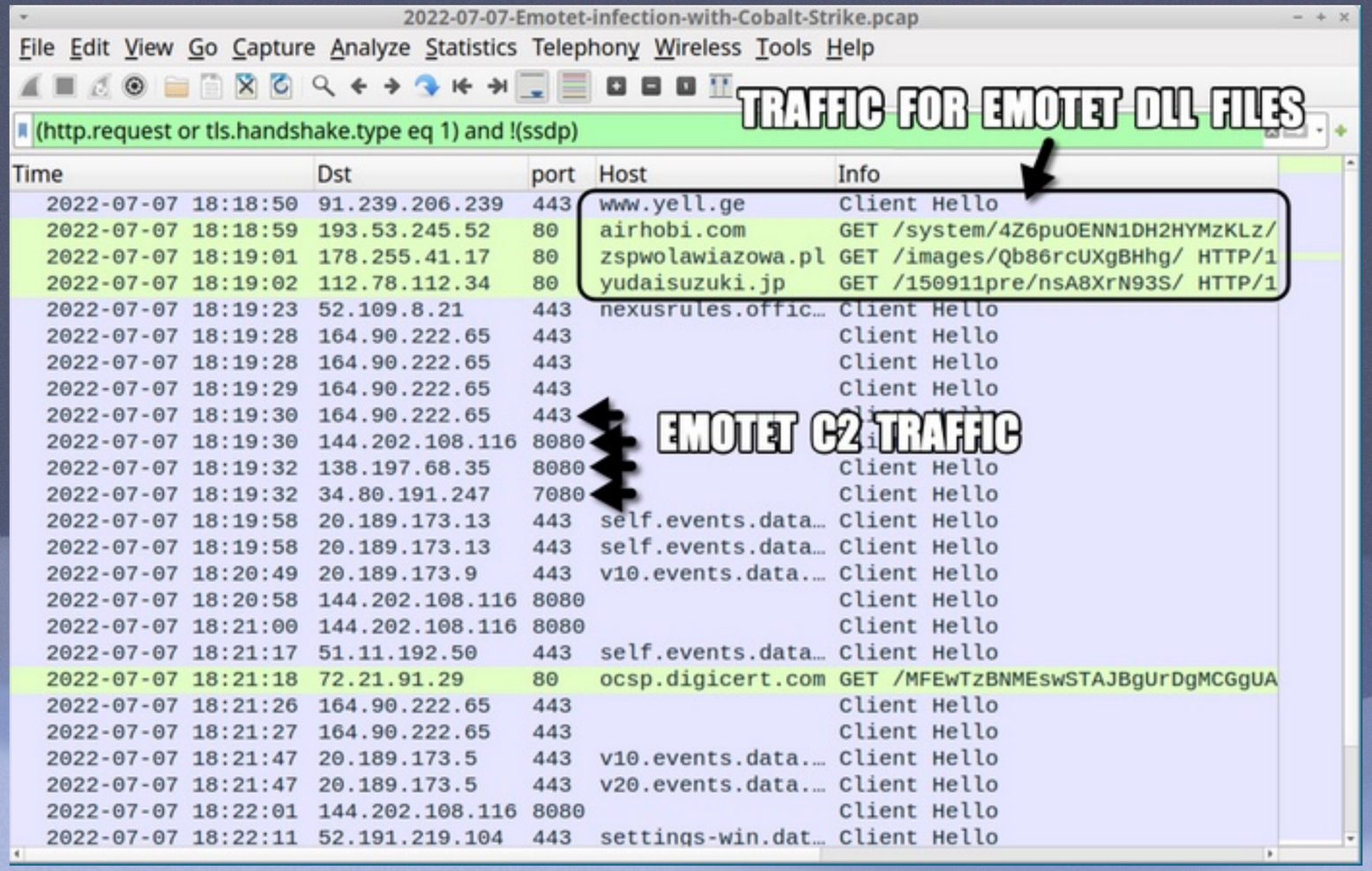
Slide Notes

Emotet is old, but good to use an example in many of the instances here. Most malware lifecycles follow the same as this.

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

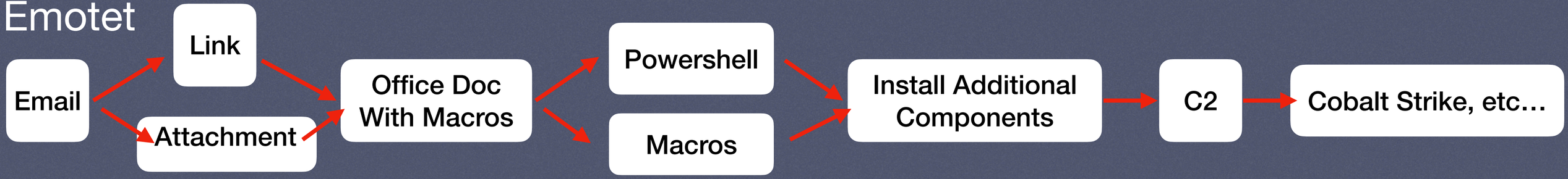
# Emotet




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

# Emotet




2022-07-07-Emotet-infection-with-Cobalt-Strike.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.type eq 1) and !(ssdp)

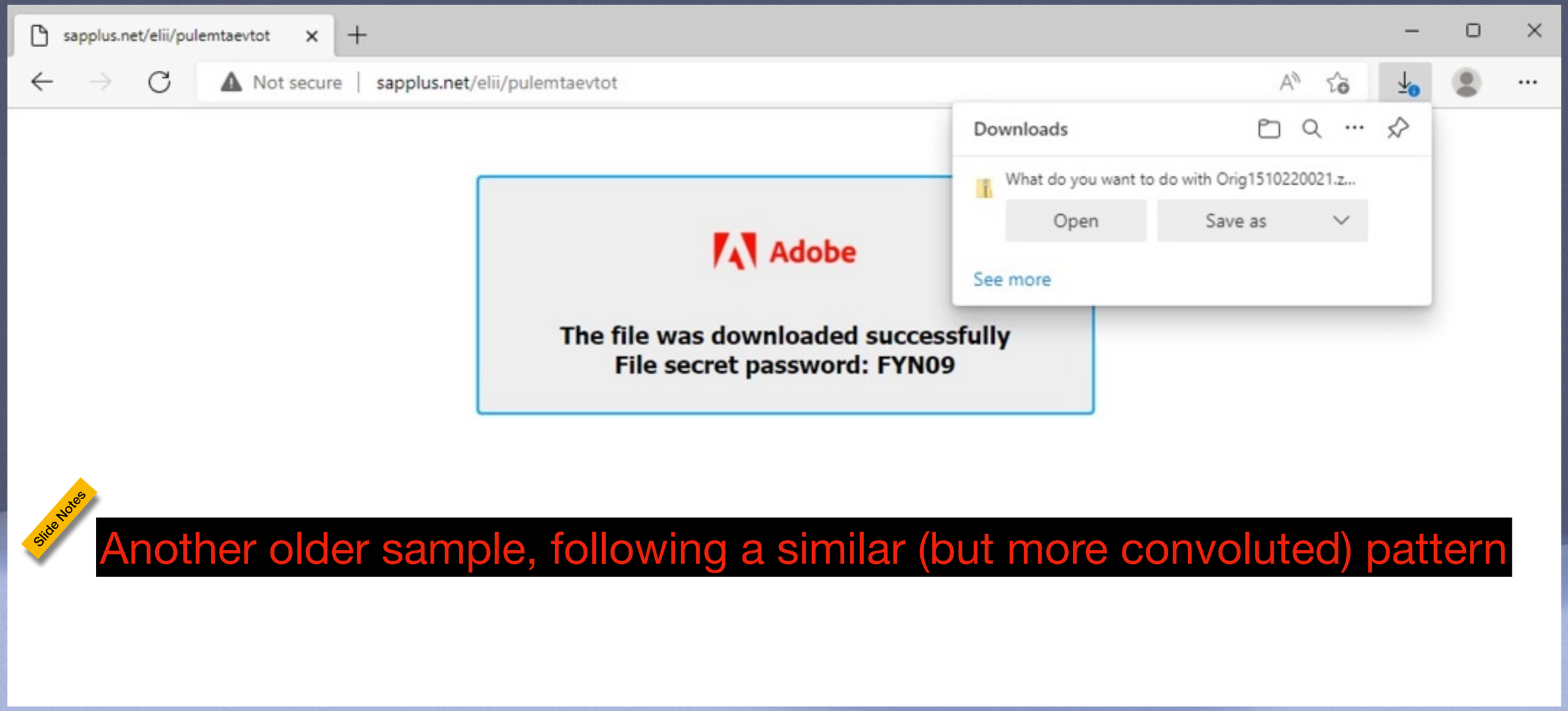
COBALT STRIKE TRAFFIC STARTS

| 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 |

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

# Qakbot

Email → Link → Password-Protected zip → ISO → Windows Shortcut → Install DLL → Qakbot C2



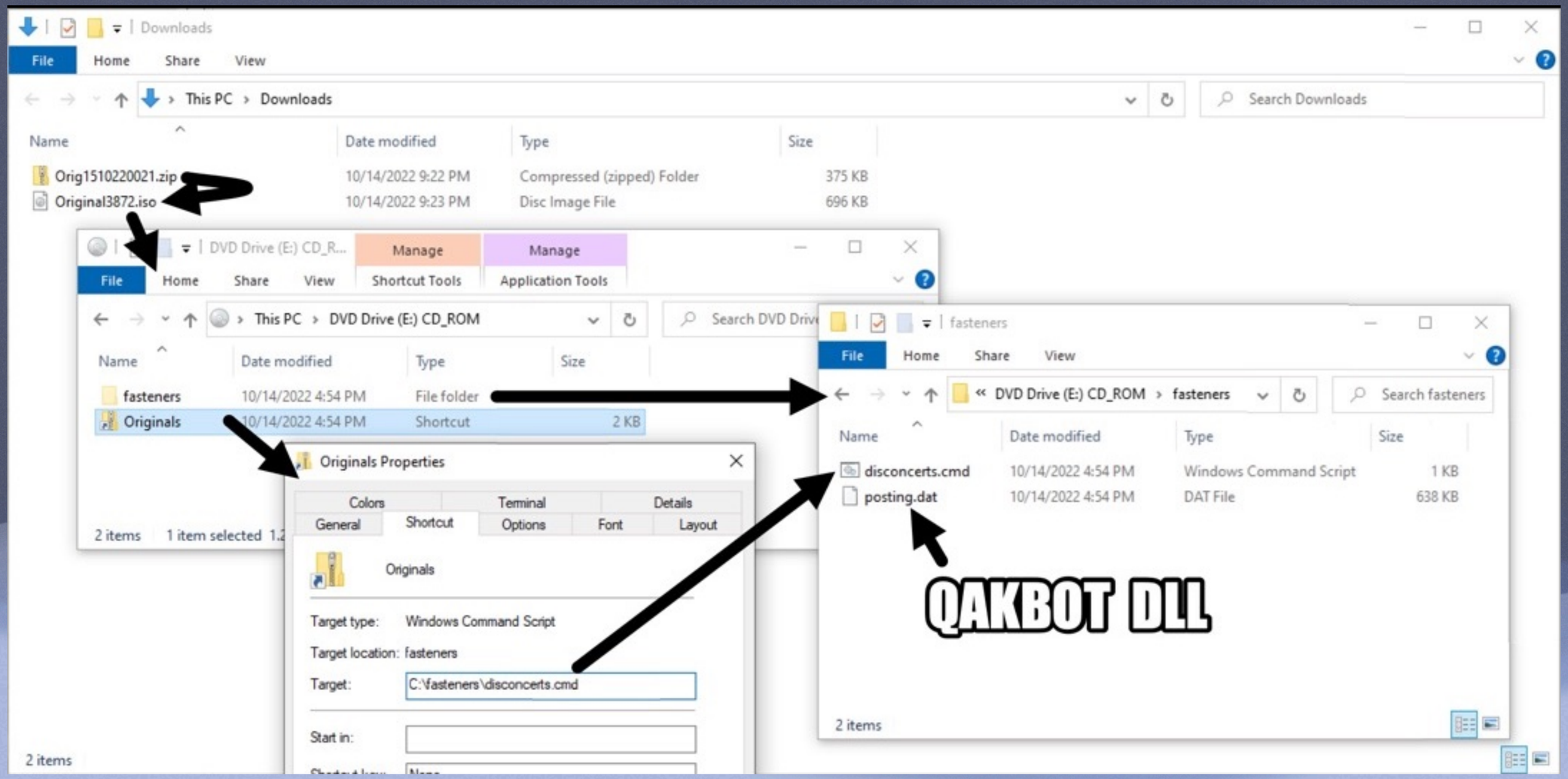

Slide Notes

Another older sample, following a similar (but more convoluted) pattern

Images from: https://www.malware-traffic-analysis.net/2022/10/14/index.html

# Qakbot

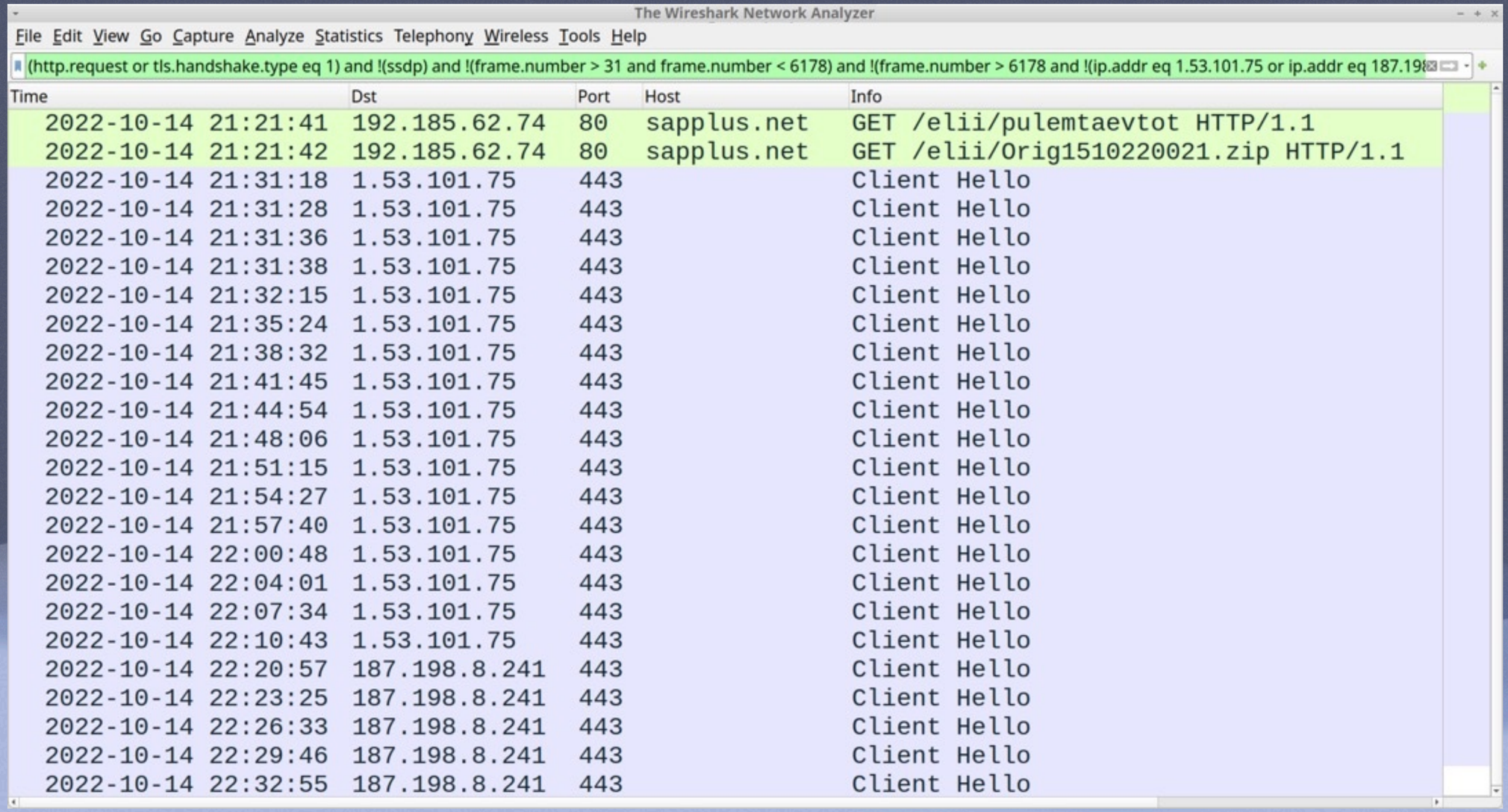
Email → Link → Password-Protected zip → ISO → Windows Shortcut → Install DLL → Qakbot C2




Images from: https://www.malware-traffic-analysis.net/2022/10/14/index.html

# Qakbot

Email → Link → Password-Protected zip → ISO → Windows Shortcut → Install DLL → Qakbot C2




| Time | Dst | Port | Host | Info |
|---|---|---|---|---|
| 2022-10-14 21:21:41 | 192.185.62.74 | 80 | sapplus.net | GET /elii/pulemtaevtot HTTP/1.1 |
| 2022-10-14 21:21:42 | 192.185.62.74 | 80 | sapplus.net | GET /elii/Orig1510220021.zip HTTP/1.1 |
| 2022-10-14 21:31:18 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:31:28 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:31:36 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:31:38 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:32:15 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:35:24 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:38:32 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:41:45 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:44:54 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:48:06 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:51:15 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:54:27 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 21:57:40 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 22:00:48 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 22:04:01 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 22:07:34 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 22:10:43 | 1.53.101.75 | 443 | | Client Hello |
| 2022-10-14 22:20:57 | 187.198.8.241 | 443 | | Client Hello |
| 2022-10-14 22:23:25 | 187.198.8.241 | 443 | | Client Hello |
| 2022-10-14 22:26:33 | 187.198.8.241 | 443 | | Client Hello |
| 2022-10-14 22:29:46 | 187.198.8.241 | 443 | | Client Hello |
| 2022-10-14 22:32:55 | 187.198.8.241 | 443 | | Client Hello |

Images from: https://www.malware-traffic-analysis.net/2022/10/14/index.html

# Signature Detection Methods

Slide Notes

There are methods for detecting malicious activity - let’s talk about a couple

Slide Notes

Probably the most well-known:

# IDS Rules

```
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 Majo
2020_09_14;)
```

ne 9, Column 1 Tab Size: 4

```
 17  2020-09-30 09:50:17.591672  trafcj.fvds.r
 18  2020-09-30 09:50:17.591752  10.9.30.101
 19  2020-09-30 09:50:17.613622  trafcj.fvds.r
 20  2020-09-30 09:50:17.613751  10.9.30.101
 21  2020-09-30 09:50:17.614360  trafcj.fvds.r
 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
```

```
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
```

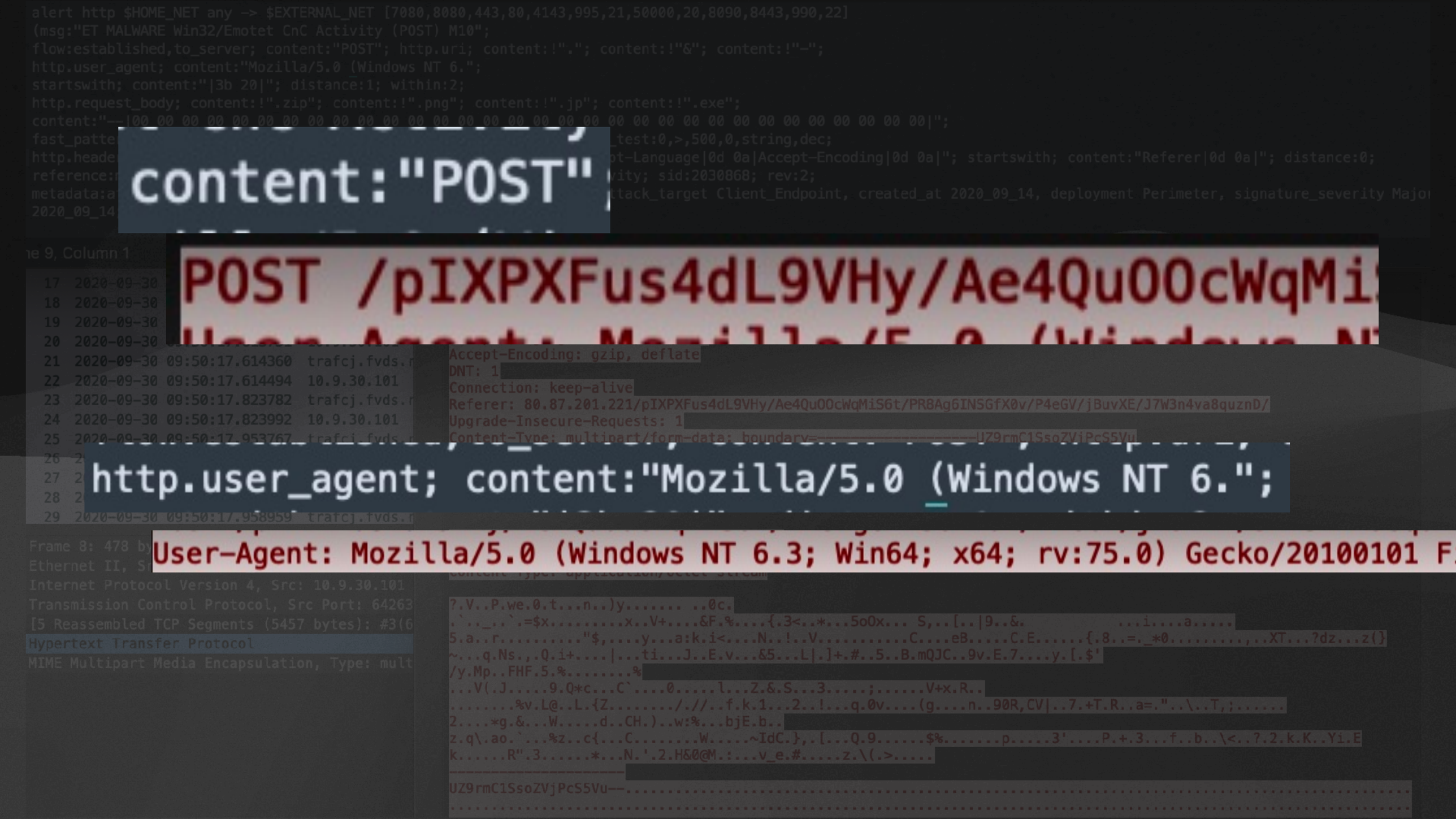
```
POST /pIXPXFus4dL9VHy/Ae4QuOOcWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
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


----------------------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,;.....
.Yi.E
----------------------
UZ9rmC1SsoZVjPcS5Vu--.....
.....
```

Slide Notes

IDS rules (top) are created to catch specific network traffic (seen below)


content:"POST"
POST /pIXPXFus4dL9VHy/Ae4QuOOcWqMi
http.user_agent; content:"Mozilla/5.0 (Windows NT 6.";
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:75.0) Gecko/20100101 F

Slide Notes

Notes

```
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
```

```
09/30/2020-16:50:17.590966  [**] [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
09/30/2020-16:50:21.950965  [**] [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
```

Slide Notes

YARA rules are not typically used against network traffic. YARA is useful to find strings or certain other encoded data in binary and text-related files.

# YARA Rules

Slide Notes

# YARA rules are simple to write and read:

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}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

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

- Simple report "python yaraPcap.py -r sampleReport.txt sample.yar sample.pcap"
- Save Matching Files "python yaraPcap.py -s SampleDir sample.yar sample.pcap"

###Requirements

- Python
- For windows edit the Script to point to your copy of the tcpflow binary. Line 29

Slide Notes

Others have done work on analyzing network traffic with YARA. This tool is used to run a PCAP file against YARA

```
class YaraPcapProcessor:
    def __init__(self, pcap, rules):
        self.pcap = pcap
        self.rules = rules

    def process_pcap(self, tmpDir):
        shutil.copyfile(self.pcap, os.path.join(tmpDir, "raw.pcap"))
        retcode = subprocess.call(f"(cd {tmpDir} && {tcpFlowPath} -a -r raw.pcap)", shell=T
        if retcode != 0:
            raise subprocess.CalledProcessError(retcode, tcpFlowPath)
        return tmpDir

    def yara_scan(self, scanfile, yara_rules):
        matches = []
        if os.path.getsize(scanfile) > 0:
            for match in yara_rules.match(scanfile):
                matches.append({"name": match.rule, "meta": match.meta})
        return matches

    def main(self):
        tmpDir = tempfile.mkdtemp()
        try:
            self.process_pcap(tmpDir)
            yara_rules = yara.compile(self.rules)
                    for item in results:
                        line = "Signature Name: {}</br>Author: {}</br>Date: {}".format(item
                        results_uniqued.append(line)
            return results_uniqued
        finally:
            shutil.rmtree(tmpDir)
```

Slide

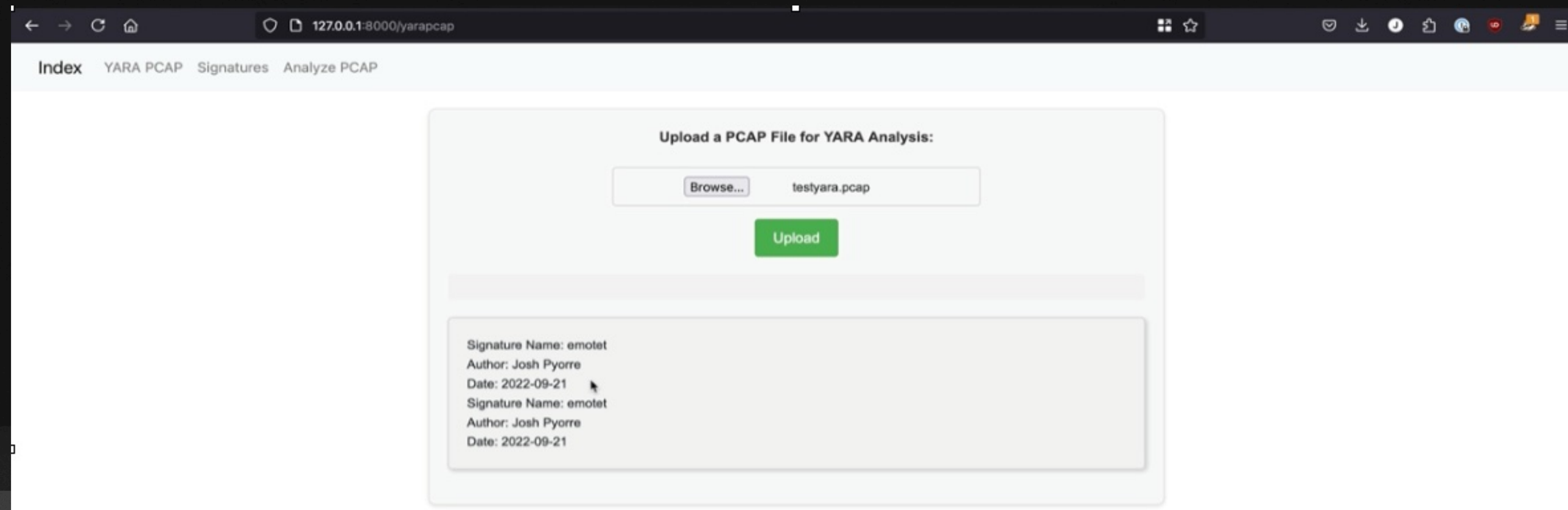
I modified YARApcap to fit the needs of this presentation and added my modification to the code (at the end)

# The IDS rule:

```
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 Majo
2020_09_14;)
```

# Becomes a YARA rule:

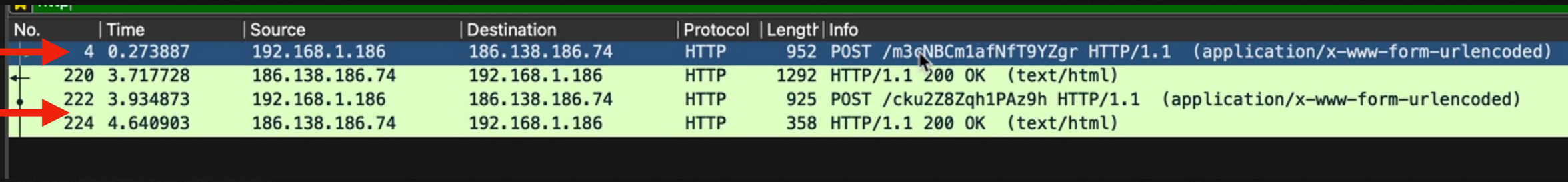
```
rule emotet : post {
meta:
  author = "Josh Pyorre"
  date = "2022-09-21"
  description = "Emotet"
strings:
  $type="POST"
  $user_agent="Mozilla/5.0 (Windows NT 6."
  $content="--|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"
  $referer="Referer|0d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




Slide Notes

Video of the web app I made demonstrating running YARA against a PCAP

1:
2:



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 4 | 0.273887 | 192.168.1.186 | 186.138.186.74 | HTTP | 952 | POST /m3cNBCm1afNfT9YZgr HTTP/1.1 (application/x-www-form-urlencoded) |
| 220 | 3.717728 | 186.138.186.74 | 192.168.1.186 | HTTP | 1292 | HTTP/1.1 200 OK (text/html) |
| 222 | 3.934873 | 192.168.1.186 | 186.138.186.74 | HTTP | 925 | POST /cku2Z8Zqh1PAz9h HTTP/1.1 (application/x-www-form-urlencoded) |
| 224 | 4.640903 | 186.138.186.74 | 192.168.1.186 | HTTP | 358 | HTTP/1.1 200 OK (text/html) |

Slide Notes

The POST happens twice in the PCAP, so two alerts are generated

1:

Signature Name: emotet
Author: Josh Pyorre
Date: 2022-09-21

2:

Signature Name: emotet
Author: Josh Pyorre
Date: 2022-09-21

Slide Notes

# Not all traffic is in the clear…

~~Visibility~~

Slide Notes

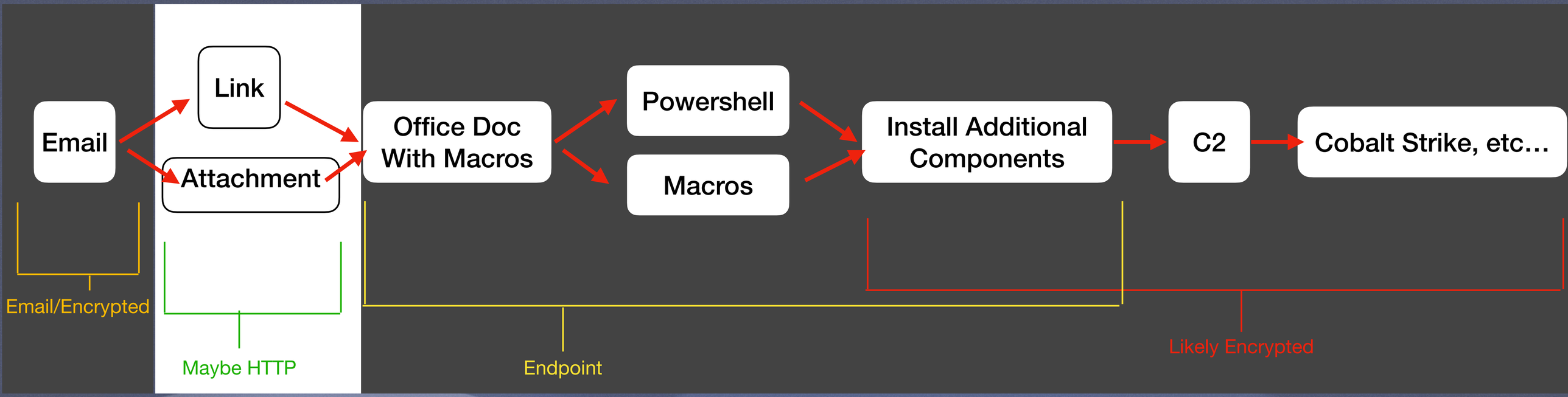
Actually, most is over SSL

# SSL

# Emotet

Slide Notes

Looking at the attack chain, our visibility is limited to only a few areas



# IcedID Dropper -> Cobalt Strike

| | | | | | | |
|---|---|---|---|---|---|---|
| 27771 | 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 |
| 277 | 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 |
| 27 | 2022-08-10 04:17:47.753357 | 10.8.9.101 | 172.93.98.170 | HTTP | 132 | GET /download/a2.dll HTTP/1.1 |

The GET here is over HTTP, but that is often not the case with easy to get SSL certs

```
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
Connection: keep-alive
X-Powered-By: ASP.NET
Content-Length: 2134016

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

$.......u+..1J.X1J.X1J.X%!.Y$J.X%!.Y?J.X%!.Y.J.X%!.Y2J.X1J.XWJ.XW%EX9J.X.>.Y.J.X.>.Y!J.X.>.Y;J.X.>.Y>J.X.>.Y6J.X.
3.Y.J.X.>.Y0J.X.>.Y0J.XRich1J.X........PE..d...v<.b.........."
```

# IcedID Dropper -> Cobalt Strike

Slide

Shortly after the clear traffic, encrypted traffic begins and we've lost visibility into the transactions.

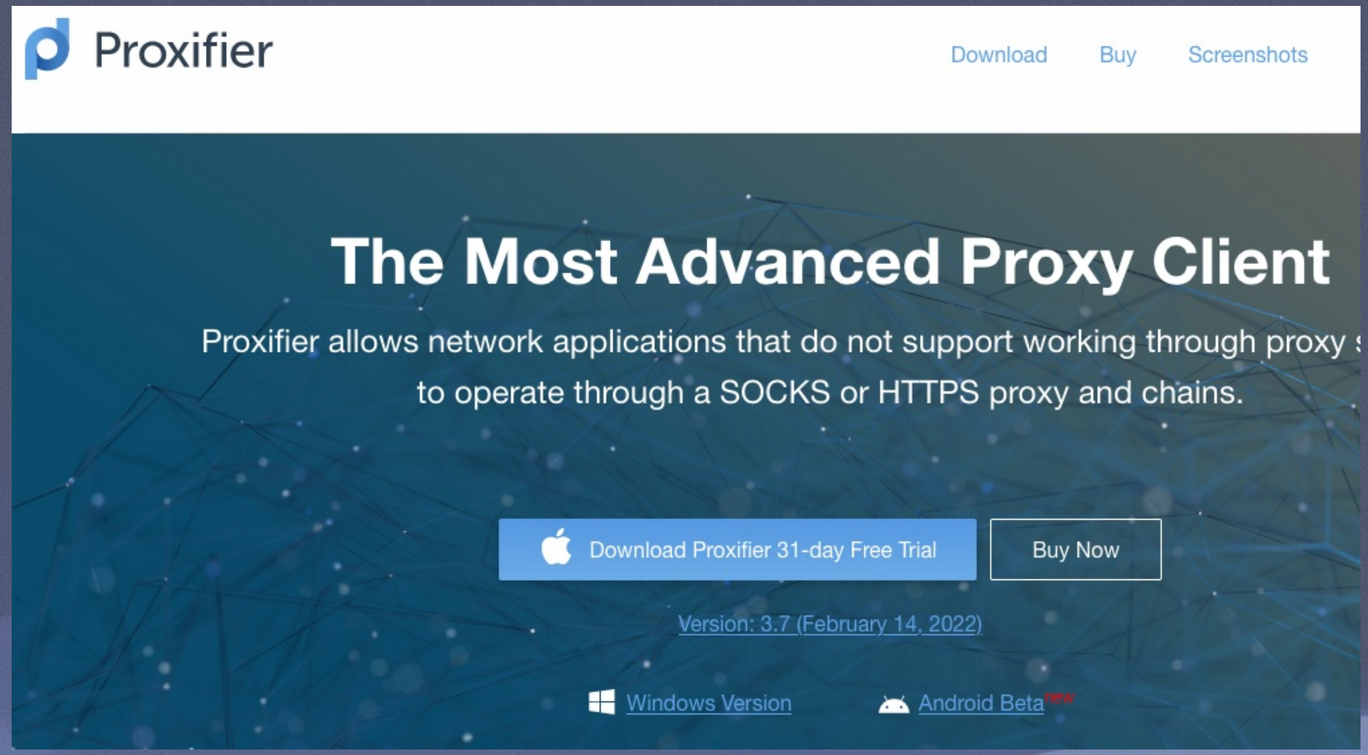
| | | | | | | |
|---|---|---|---|---|---|---|
| 30047 | 2022-08-10 04:17:49.014657 | 172.93.98.170 | 10.8.9.101 | HTTP | 714 | HTTP/1.1 200 OK |
| 30048 | 2022-08-10 04:17:49.014680 | 10.8.9.101 | 172.93.98.170 | TCP | 54 | 58697 → 80 [ACK] Seq=79 Ack=2134239 Win=63580 Len=0 |
| 30049 | 2022-08-10 04:17:49.015324 | 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 |

Slide Notes

# There are open source tools to decrypt SSL on your network tap




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




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

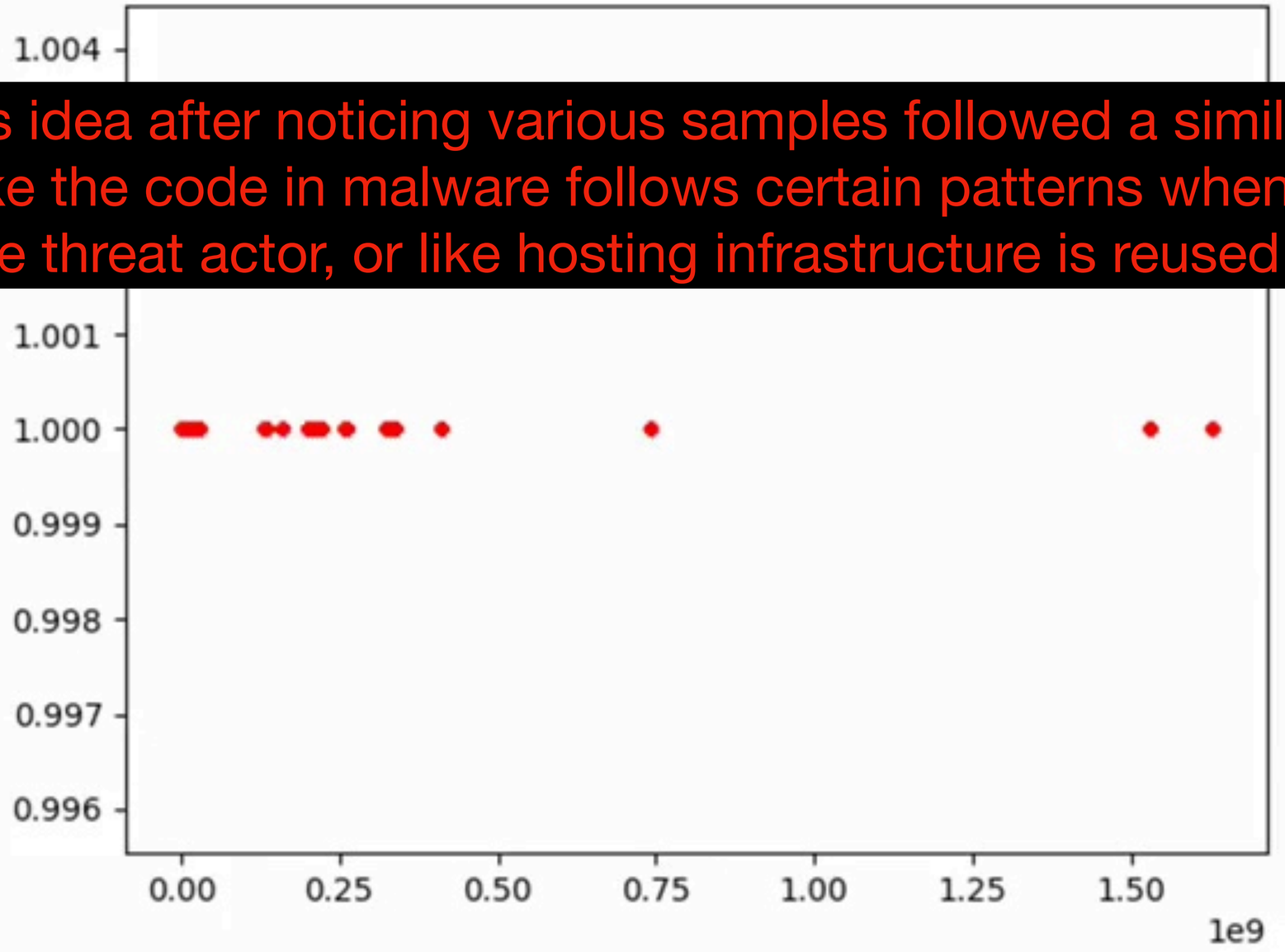
# Can we build a signature Using network Timing?

Slide Notes

Let’s talk about building signatures based on the timing in between network transactions

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

# Network Transactions of Hancitor Samples

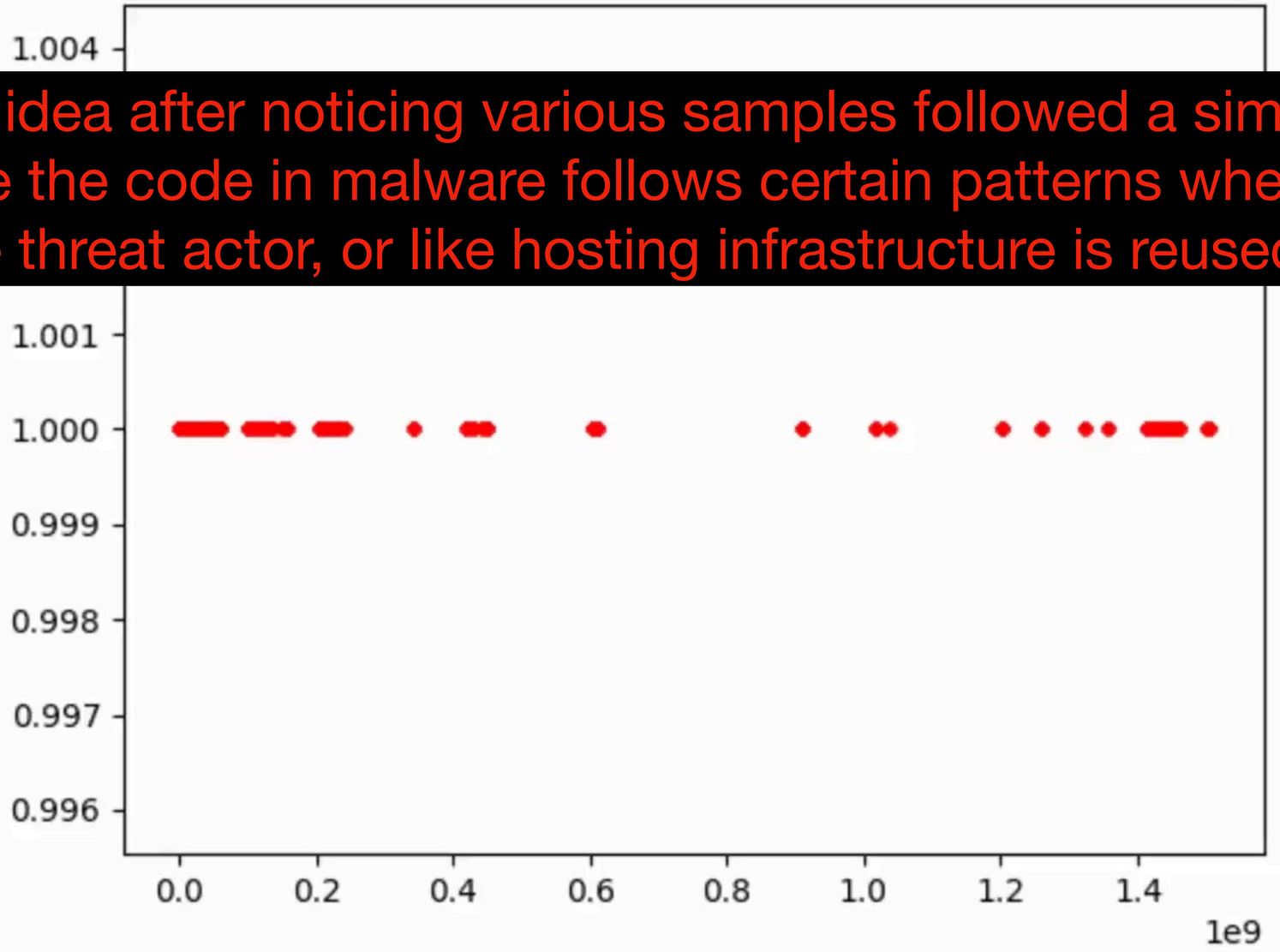



Slide Notes

I got this idea after noticing various samples followed a similar pattern, much like the code in malware follows certain patterns when created by the same threat actor, or like hosting infrastructure is reused

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

# Network Transactions of Emotet Samples

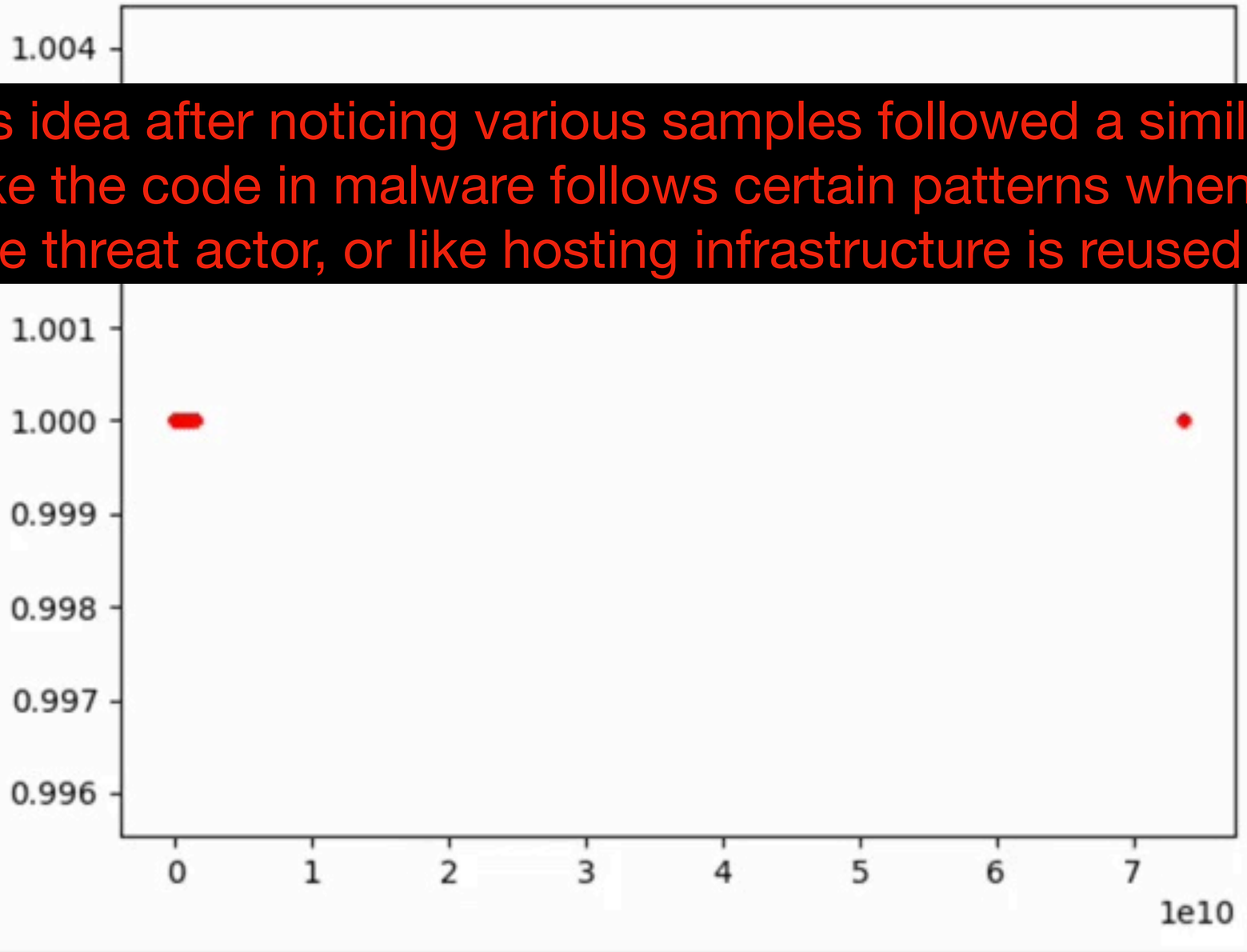



Slide Notes

I got this idea after noticing various samples followed a similar pattern, much like the code in malware follows certain patterns when created by the same threat actor, or like hosting infrastructure is reused

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

# Network Transactions of Trickbot Samples




Slide Notes

I got this idea after noticing various samples followed a similar pattern, much like the code in malware follows certain patterns when created by the same threat actor, or like hosting infrastructure is reused

Slide Notes

Starting with attempting to find patterns in network traffic

# Finding Patterns

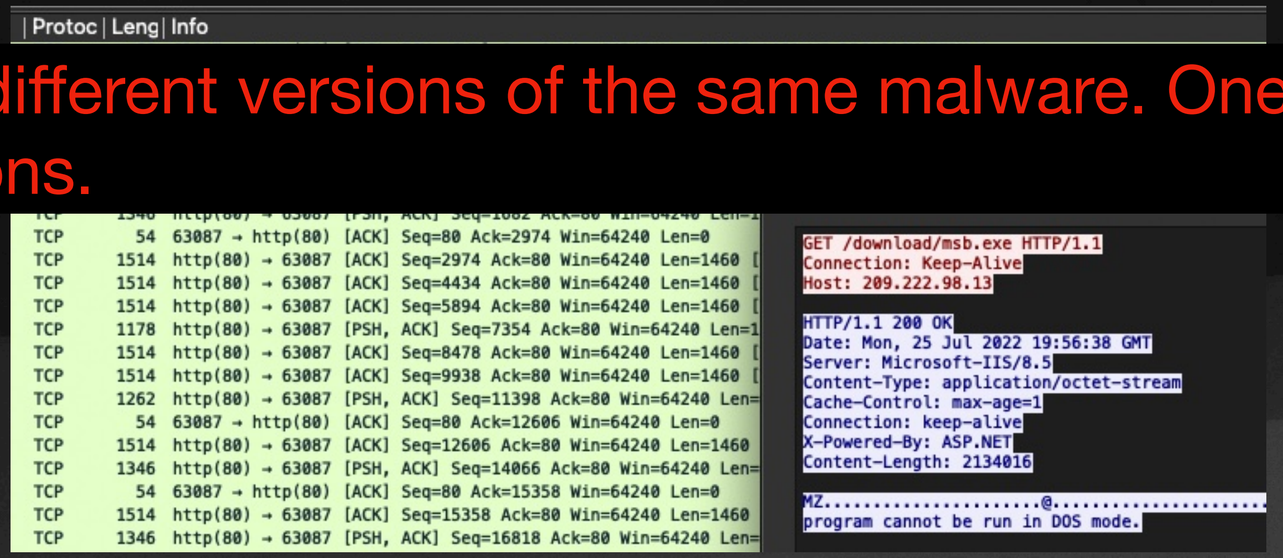
# Dropper Downloads

# Two Separate icedID Downloads

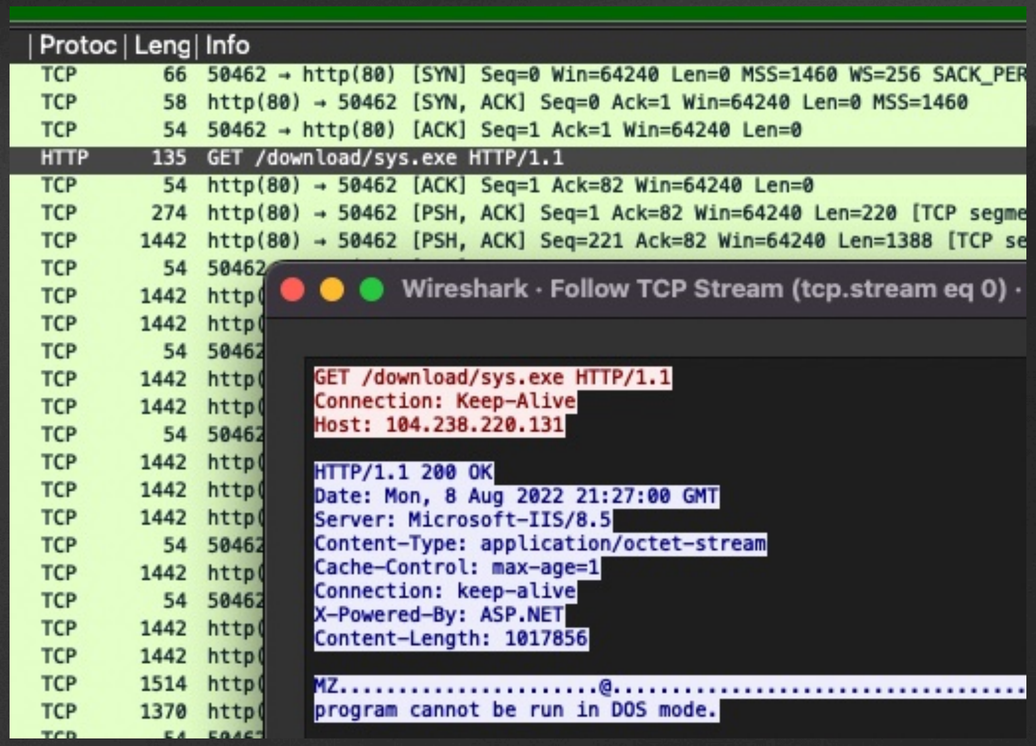
Slide Notes

Two PCAPs from different versions of the same malware. One has twice as many network transactions.

2052 transactions




1107 transactions



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

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)
```

Slide Notes

Looking at the time in between the transactions.

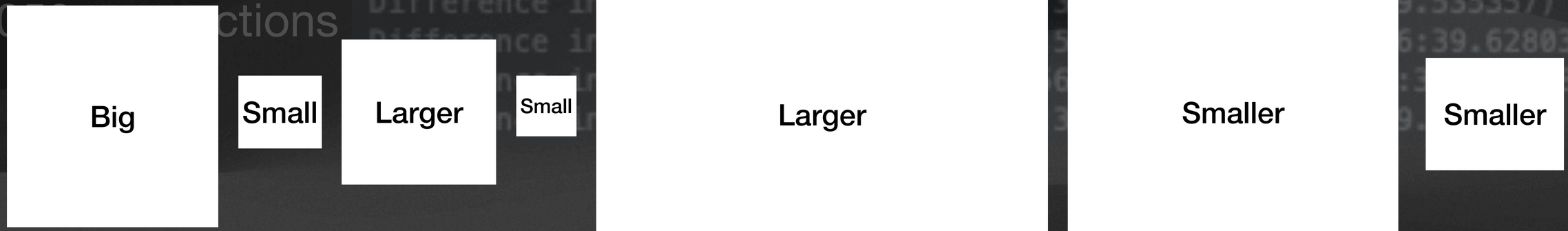
1107 transactions

```
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)
```

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

Slide Notes

There does seem to be a relationship between them. But is this just how networks operate, or is it how this malware operates? Does network latency affect this?




1107 transactions

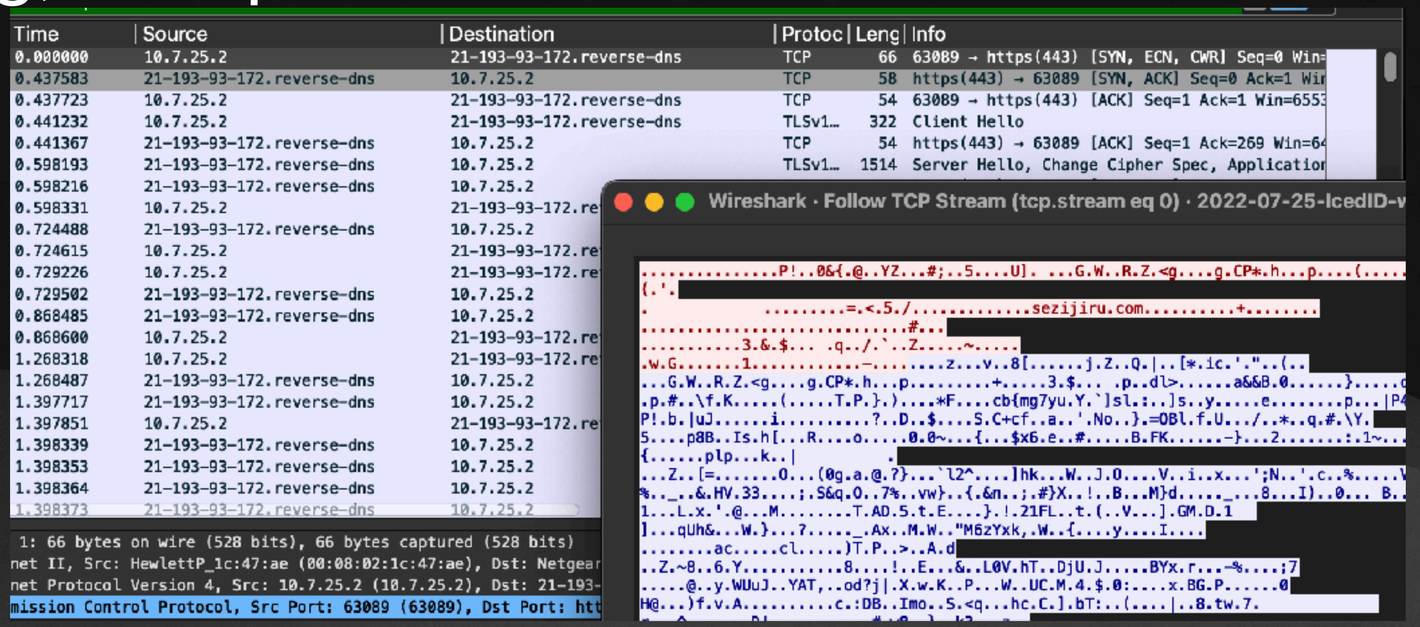
Difference in microseconds: 82 (14:27:00.740394 - 14:27:00.740476)
Difference in microseconds: 180 (14:27:00.740476 - 14:27:00.740656)
Difference in microseconds: 50 (14:27:00.740656 - 14:27:00.740706)
Difference in microseconds: 62994 (14:27:00.740706 - 14:27:00.803700)
Difference in microseconds: 3189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

Slide Notes

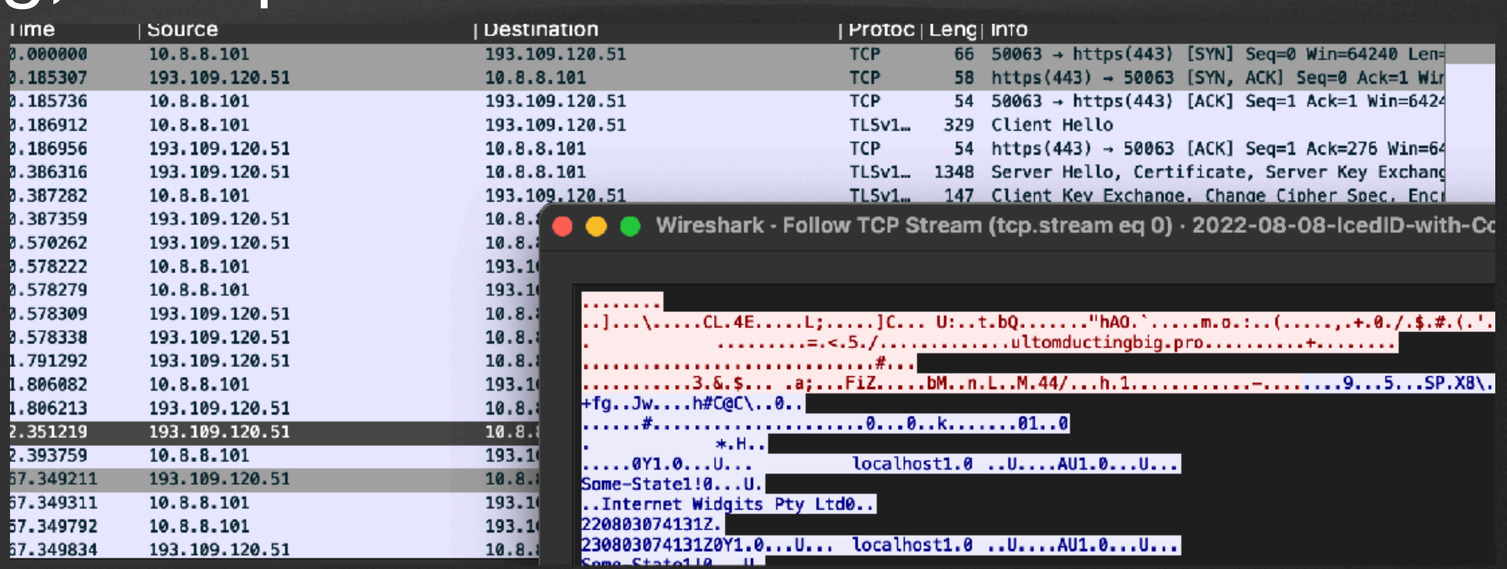
We’ll look at different traffic to try to answer some of the previous questions

# Beaconing

# Cobalt Strike Beaconing, Sample 1




# Cobalt Strike Beaconing, Sample 2



# 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)
```

Slide Notes

Seeing the same kind of timing. Maybe still just how networks work, but there may similarities for each malware…

# 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:

```
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)
```

Slide Notes

Seeing the same kind of timing. Maybe still just how networks work, but there ma
similarities for each malware…

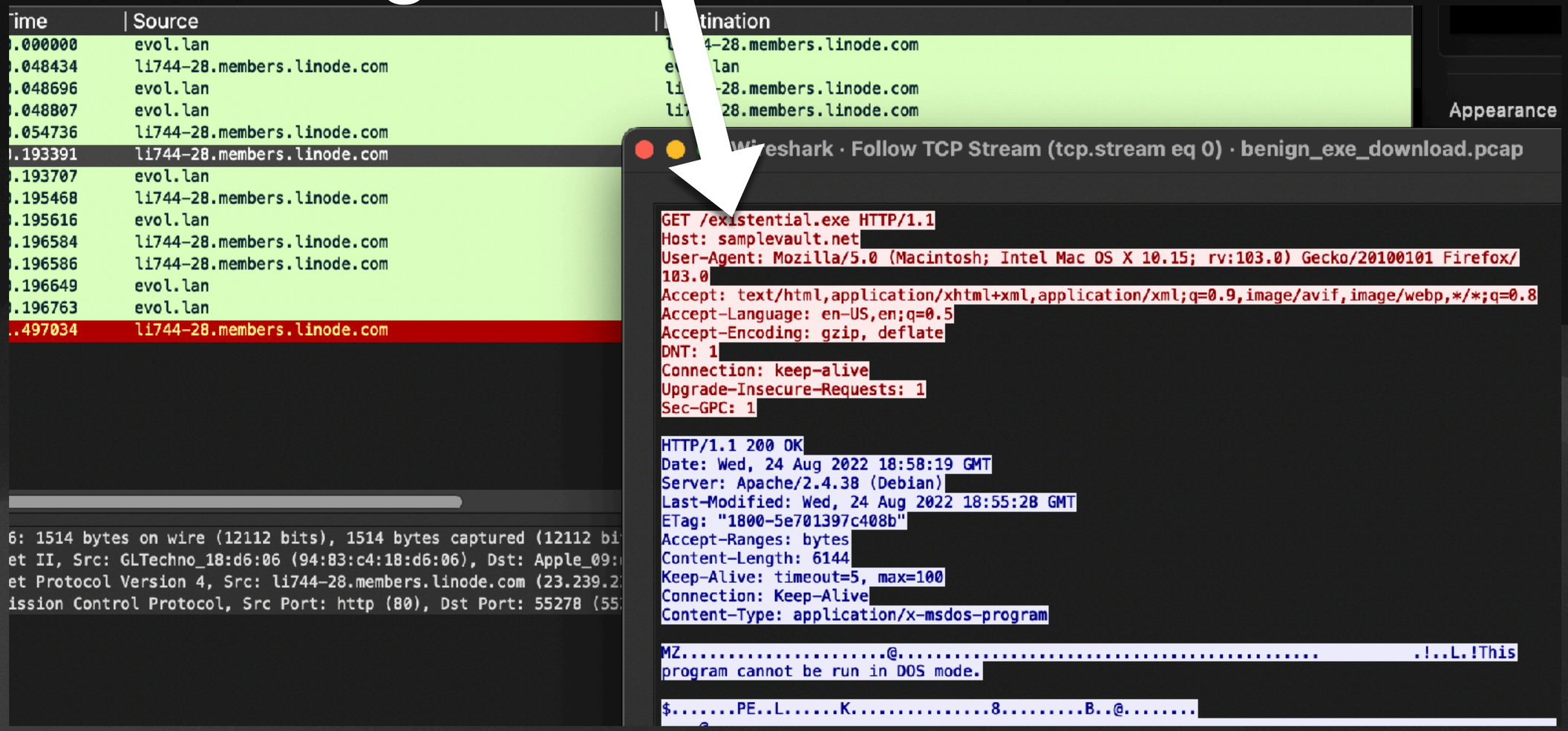
# Emotet and Trickbot beacon 2:

```
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)
```

Let’s look at one malicious and one benign to see if it’s just how networks operate

# Benign vs Malicious

# Benign .exe Download




Slide Notes

This was a download of a benign .exe file that's designed to look like a malicious dropper.

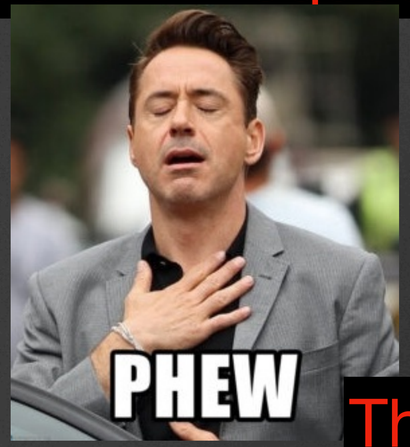
# Benign .exe Vs Malicious Dropper Download

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)
```

Slide Notes

The two GET requests look very different in their network timing…




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)
```

The talk can continue

Slide Notes

The main processes that will be used going forward:

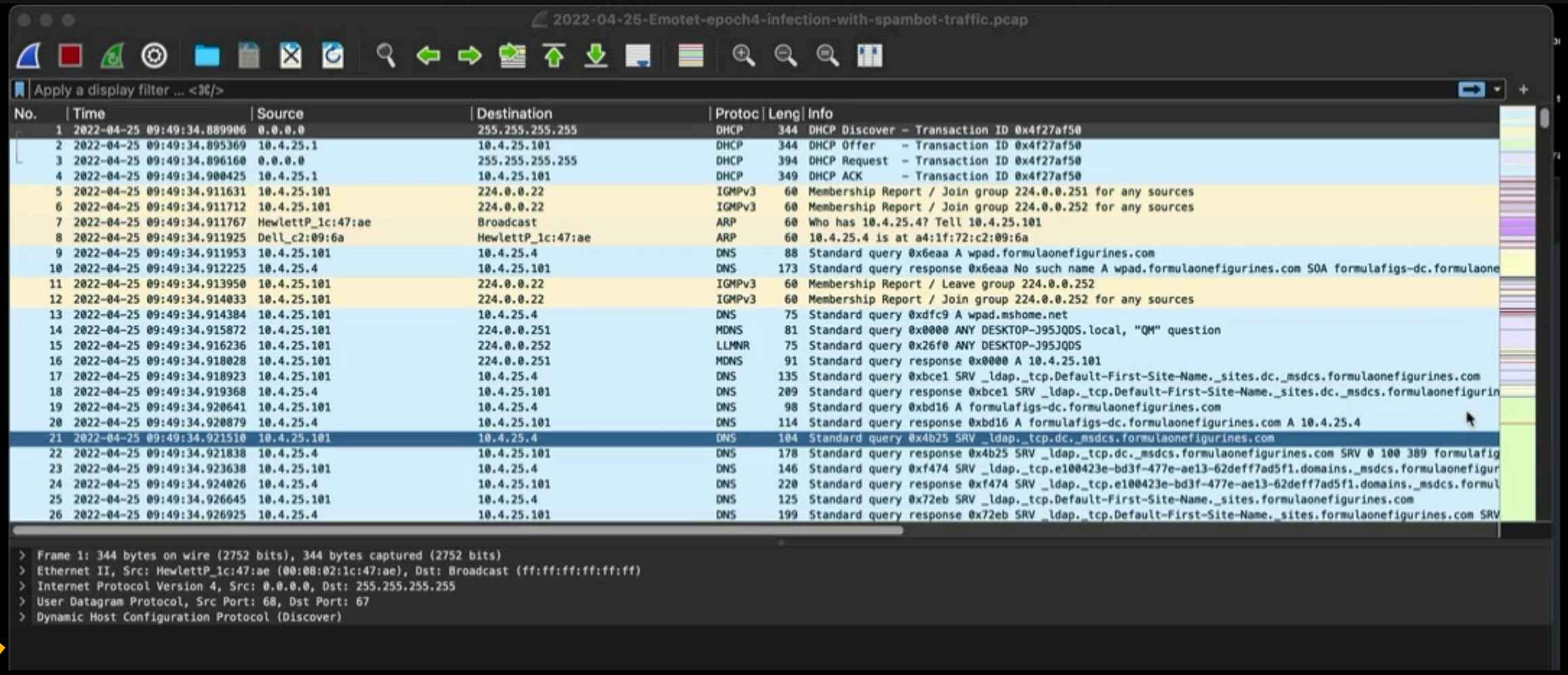
# The Process(es)

**Averages**
**Levenshtein Distance**
**Fuzzyness**

# Challenges



# Finding the Part I'm Interested in…




Slide Notes

When you open a PCAP, it's busy. We need to get just the traffic we're interested in.

# Averages

# Isolated Trickbot POST 840 Queries

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 | [illegible] | [illegible] | [illegible] | POST [illegible]/Iiq2hRZ5/lrq6gLJguipxQCN/P1yEI/ HTTP/1.1 |
| 577 | 12.092188 | 80.87.201.221 | 1 | | | |
| 582 | 12.099466 | 10.9.30.101 | 8 | | | |
| 834 | 15.375483 | 80.87.201.221 | 1 | | | |
| 839 | 15.388285 | 10.9.30.101 | 8 | | | jJ/oHTvsVuVbyi422DaAg/422SlS/ HTTP/1.1 |
| 840 | 17.374176 | 80.87.201.221 | 1 | | | |

```
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)
Difference in microseconds: 12485 (09:50:18.054091 - 09:50:18.066576)
```

# Calculate time in between transactions

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 | [illegible] | [illegible] | [illegible] | [illegible]iq2hRZ5/lrq6gLJguipxQCN/P1yEI/ HTTP/1.1 |
| 577 | 12.092188 | 80.87.201.221 | [illegible] | | | |
| 582 | 12.099466 | 10.9.30.101 | [illegible] | | | |
| 834 | 15.375483 | 80.87.201.221 | [illegible] | | | |
| 839 | 15.388285 | 10.9.30.101 | [illegible] | | | jJ/oHTvsVuVbyi422DaAg/422SlS/ HTTP/1.1 |
| 840 | 17.374176 | 80.87.201.221 | [illegible] | | | |

```
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)
Difference in microseconds: 12485 (09:50:18.054091 - 09:50:18.066576)
```

# Get all the Microseconds of those times



# Find the Average

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

Average Time Between Queries = 12,748

# Another PCAP: Isolated Trickbot POST

2,905 Queries

| 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) |

```
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)
```

**PCAP 1:**
TrickBot 1 (20200930_trickbotpost.pcap)

Total Queries: 840
Average: 14,748

**PCAP 2:**
TrickBot 2 (20201229_trickbotpost.pcap)

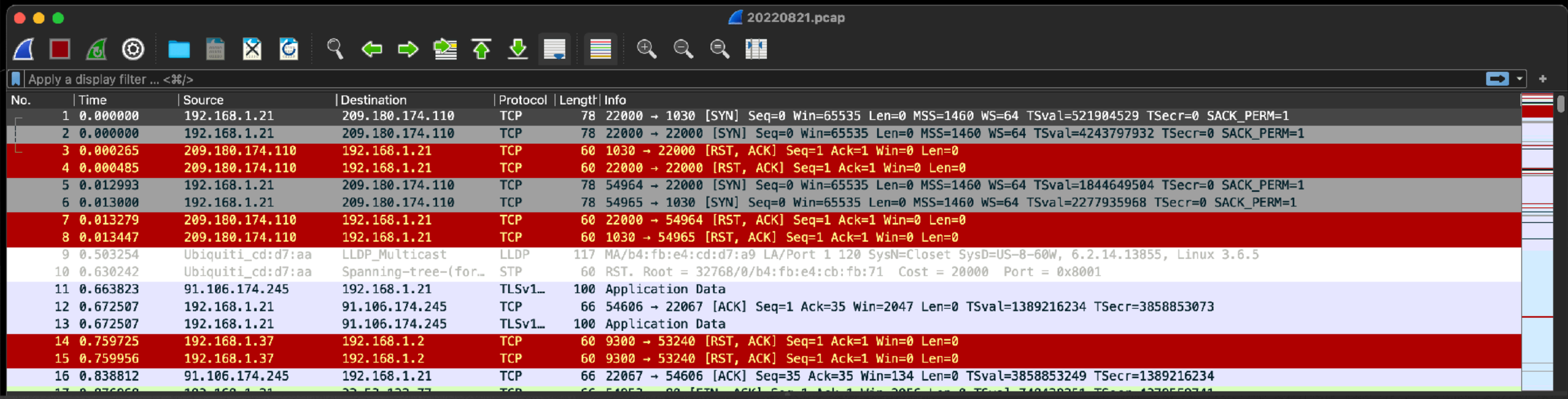
Total Queries: 2905
Average: 16,125

Slide Notes

Very different number of queries. Can we find any similarities?
The averages are a bit close. This is with no boundary detection (I’m not worried about how many packets there are)

# Compare Against Random Traffic

# Multiple Flows of Random Traffic




# Total Queries: 779

# One Flow from that Random Traffic

randomtraffic_onestream.pcap

Apply a display filter ... <⌘/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.1.1 | 192.168.1.103 | TCP | 74 | 37831 → 8080 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=900565887 TSecr=0 WS=64 |
| 2 | 0.000203 | 192.168.1.103 | 192.168.1.1 | TCP | 74 | 8080 → 37831 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=900428878 TSecr=900565887 WS=128 |
| 3 | 0.000448 | 192.168.1.1 | 192.168.1.103 | TCP | 66 | 37831 → 8080 [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=900565887 TSecr=900428878 |
| 4 | 0.001146 | 192.168.1.1 | 192.168.1.103 | TCP | 246 | 37831 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=14656 Len=180 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 5 | 0.001287 | 192.168.1.103 | 192.168.1.1 | TCP | 66 | 8080 → 37831 [ACK] Seq=1 Ack=181 Win=31488 Len=0 TSval=900428878 TSecr=900565887 |
| 6 | 0.003409 | 192.168.1.103 | 192.168.1.1 | HTTP | 83 | HTTP/1.1 100 |
| 7 | 0.003633 | 192.168.1.1 | 192.168.1.103 | TCP | 66 | 37831 → 8080 [ACK] Seq=181 Ack=18 Win=14656 Len=0 TSval=900565887 TSecr=900428878 |
| 8 | 0.004502 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=181 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 9 | 0.004531 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=1629 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 10 | 0.004532 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=3077 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 11 | 0.004532 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=4525 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 12 | 0.004532 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=5973 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 13 | 0.004532 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=7421 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 14 | 0.004568 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=8869 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 15 | 0.004568 | 192.168.1.1 | 192.168.1.103 | TCP | 1514 | 37831 → 8080 [ACK] Seq=10317 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr=900428878 [TCP segment of a reassembled PDU] |
| 16 | 0.004741 | 192.168.1.103 | 192.168.1.1 | TCP | 66 | 8080 → 37831 [ACK] Seq=18 Ack=3077 Win=37248 Len=0 TSval=900428878 TSecr=900565887 |

# Total Queries: 32

Slide Notes

While relatively different from each other, they're more similar to each other than they are to random similar traffic. This also shows that averages could potentially be applied to a full PCAP and a piece of the PCAP to get things that are close.

14,748: Trickbot POST 1
16,125: Trickbot POST 2
8,356: Random Traffic, one stream
72,144: Random Traffic, full stream

# Cointegration

Slide Notes

Cointegration tells you that, although two series move independently, the average distance between them remains relatively constant.

*Is the drunk guy walking with the dog or are they just walking in the same direction for a while?*



Not cointegrating

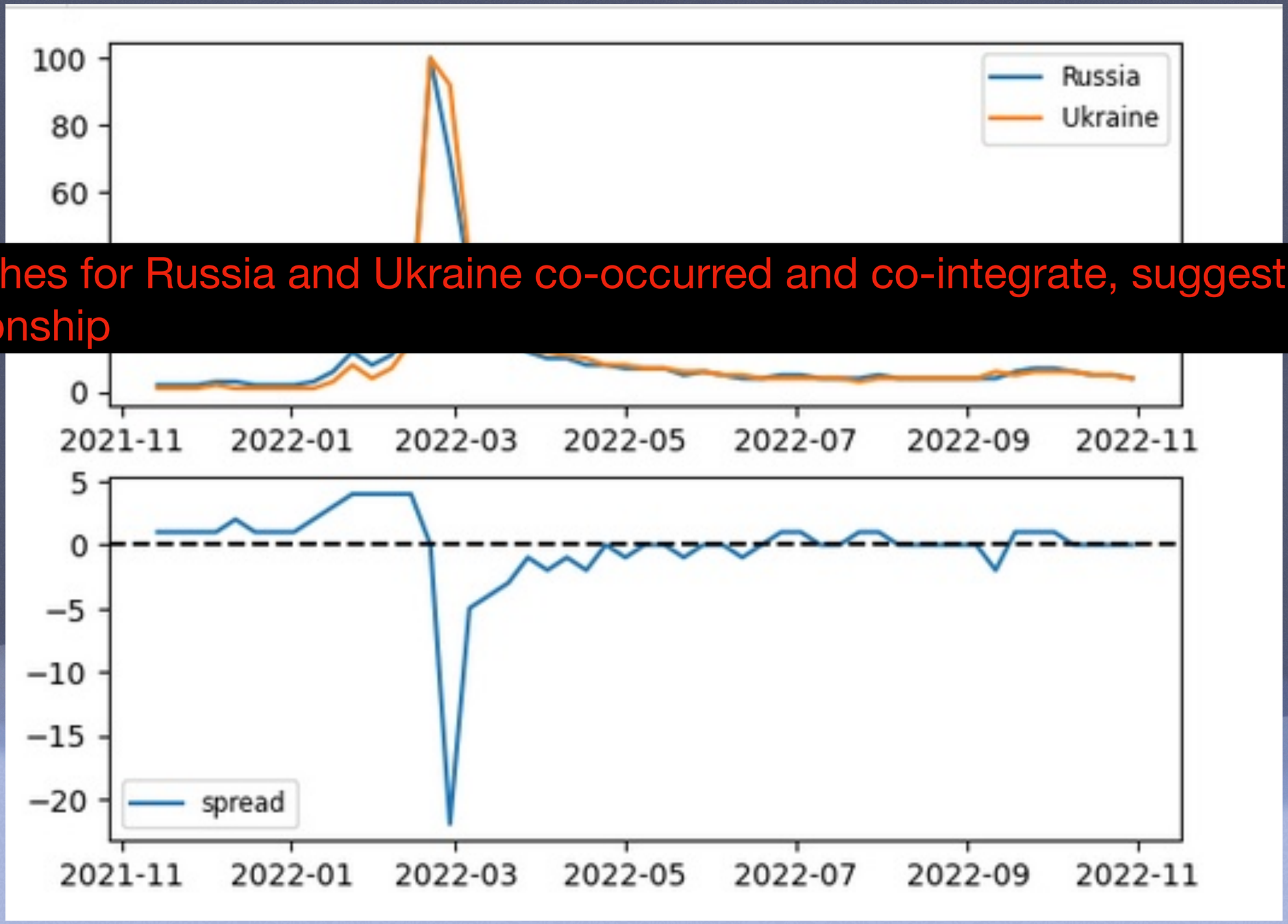
Cooccurring

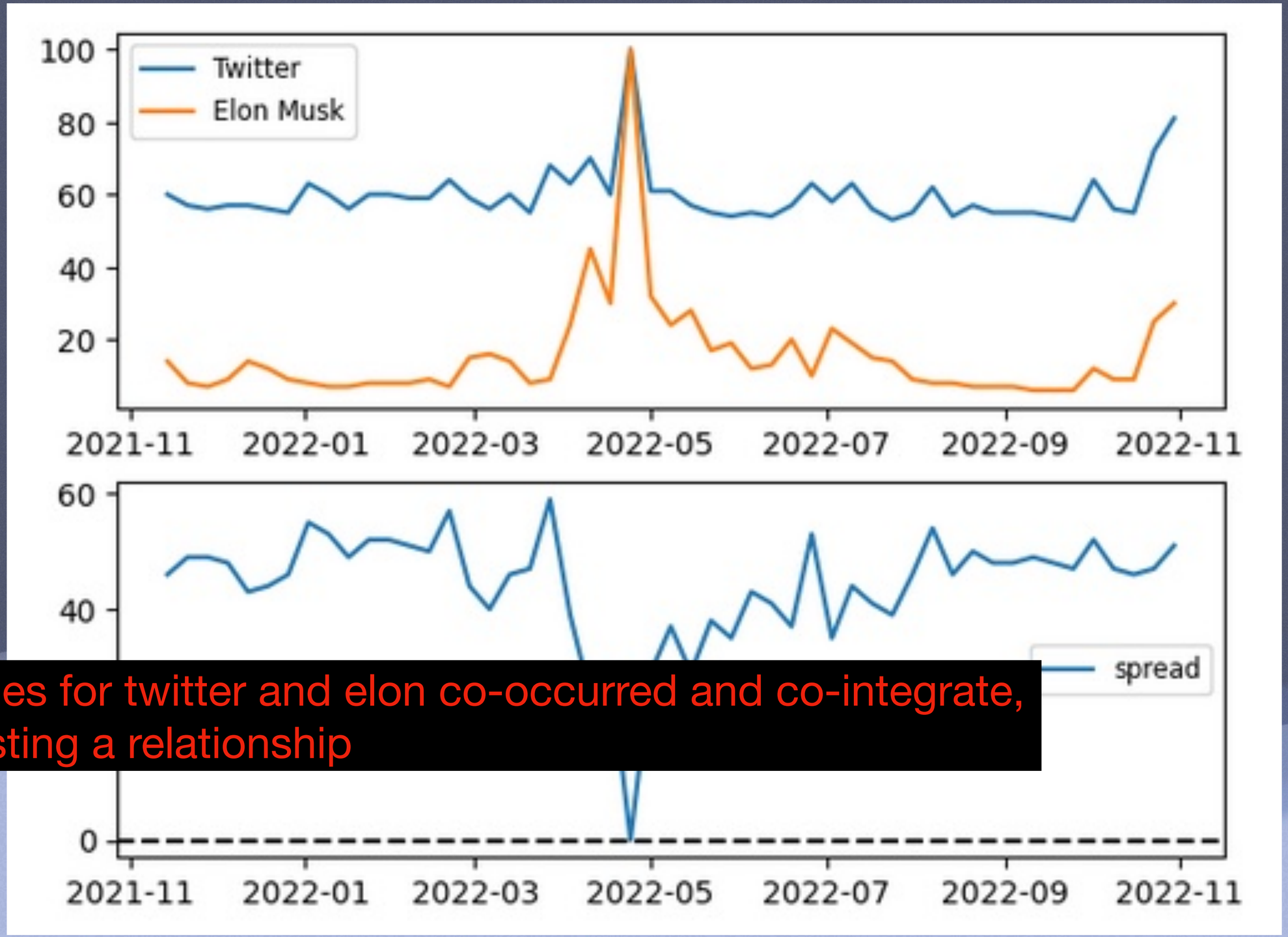
Not cointegrating



Slide Notes

Searches for Russia and Ukraine co-occurred and co-integrate, suggesting a relationship






Slide Notes

Searches for twitter and elon co-occurred and co-integrate, suggesting a relationship

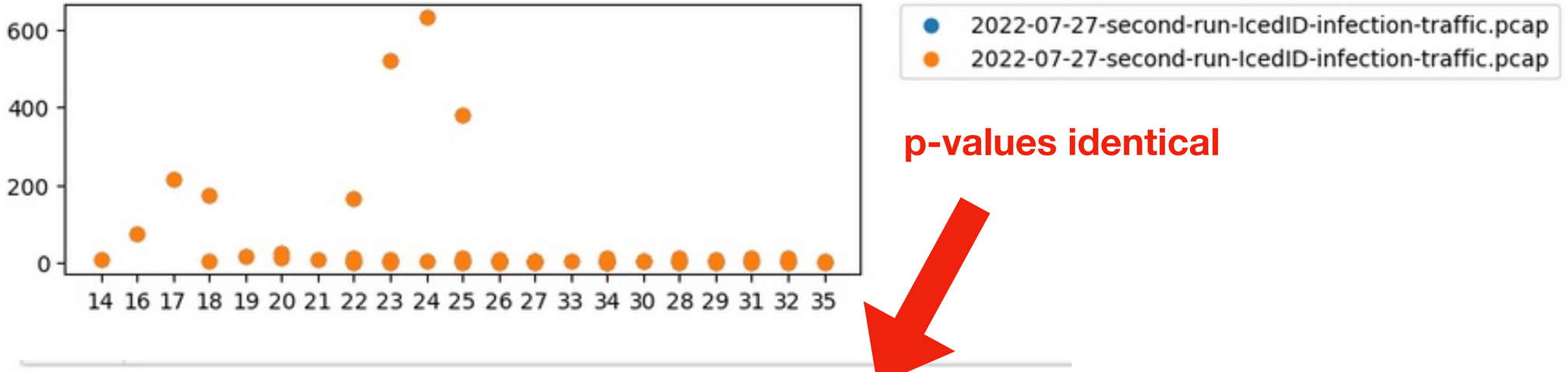
Two identical PCAP files
They should cointegrate

# Identical PCAP files: 100% Cointegration

Slide Notes

Identical will obviously be identical. Just want to see what that looks like

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

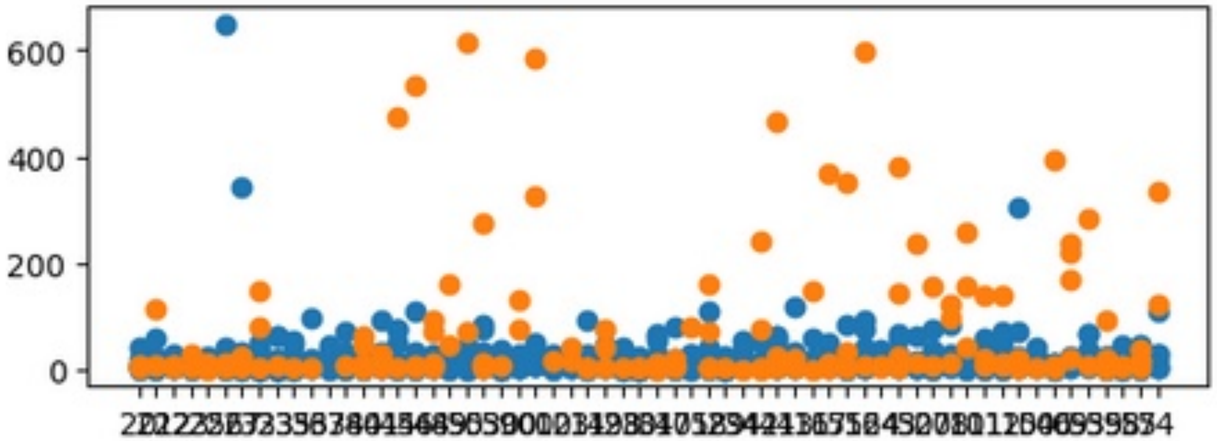



**p-values identical**

```
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
```

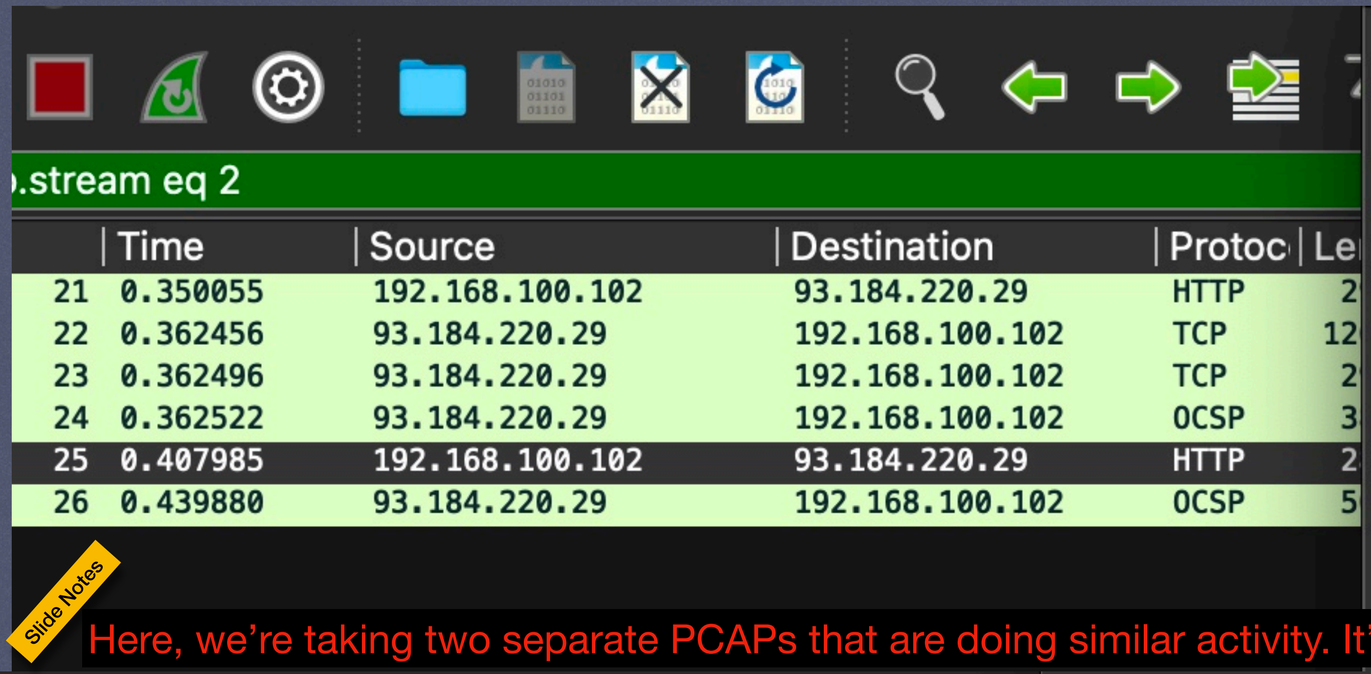
Slide Notes

Two pcaps that seem similar, but are actually following different timelines. They likely won't cointegrate. There is 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

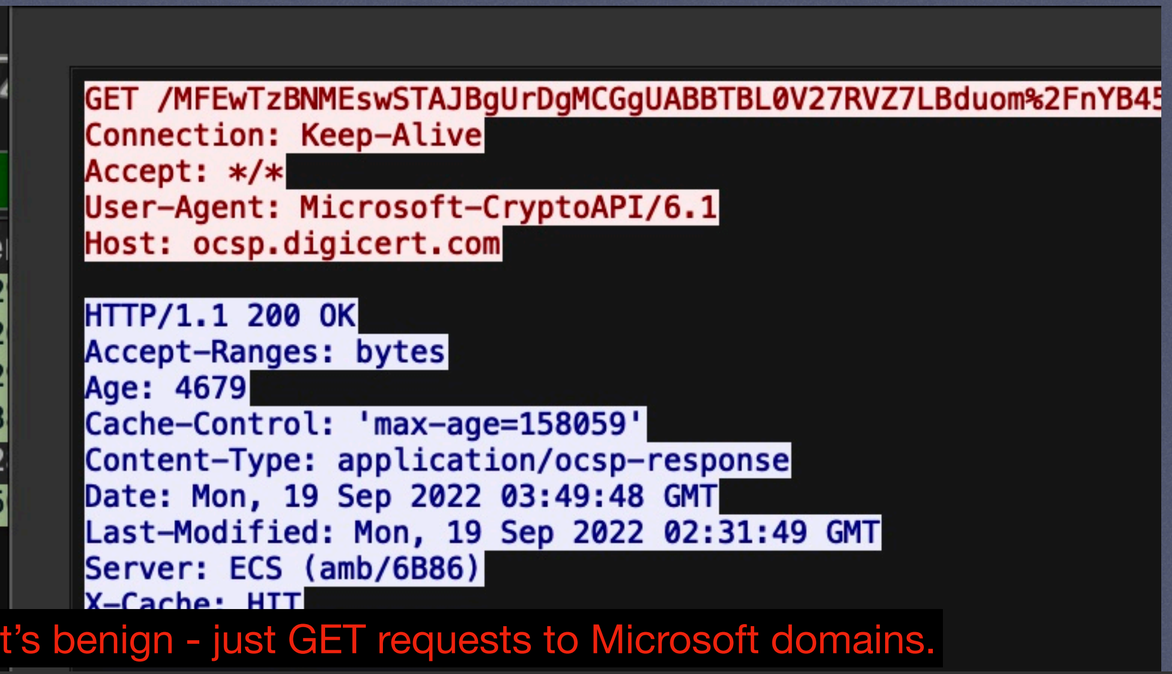
# Two different PCAP files
# With similar traffic

# 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 |

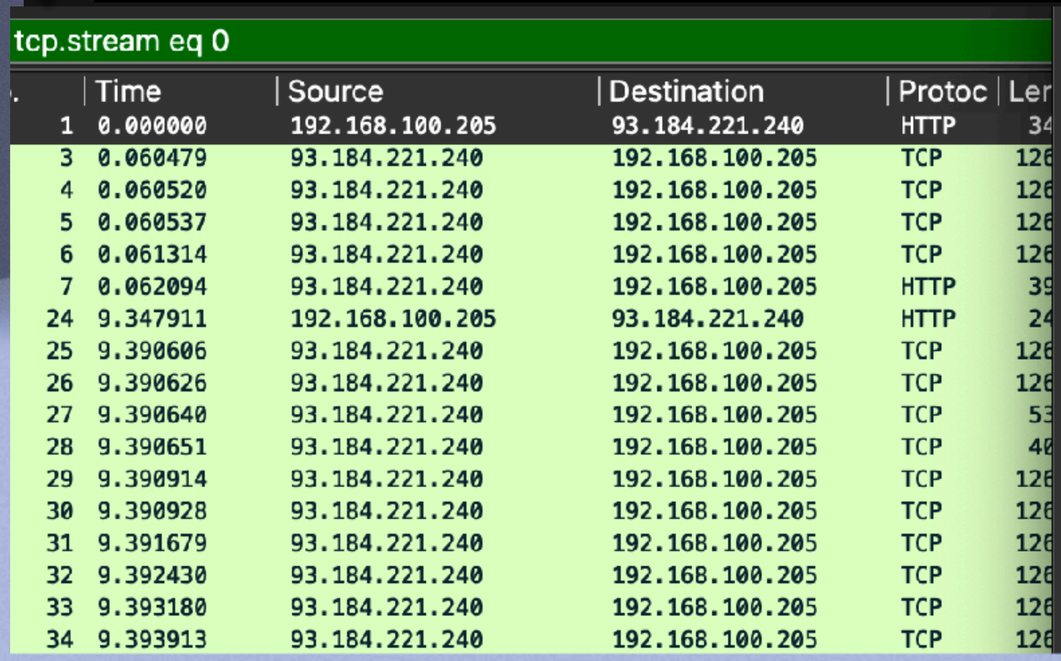


```
GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: ocsp.digicert.com

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
```

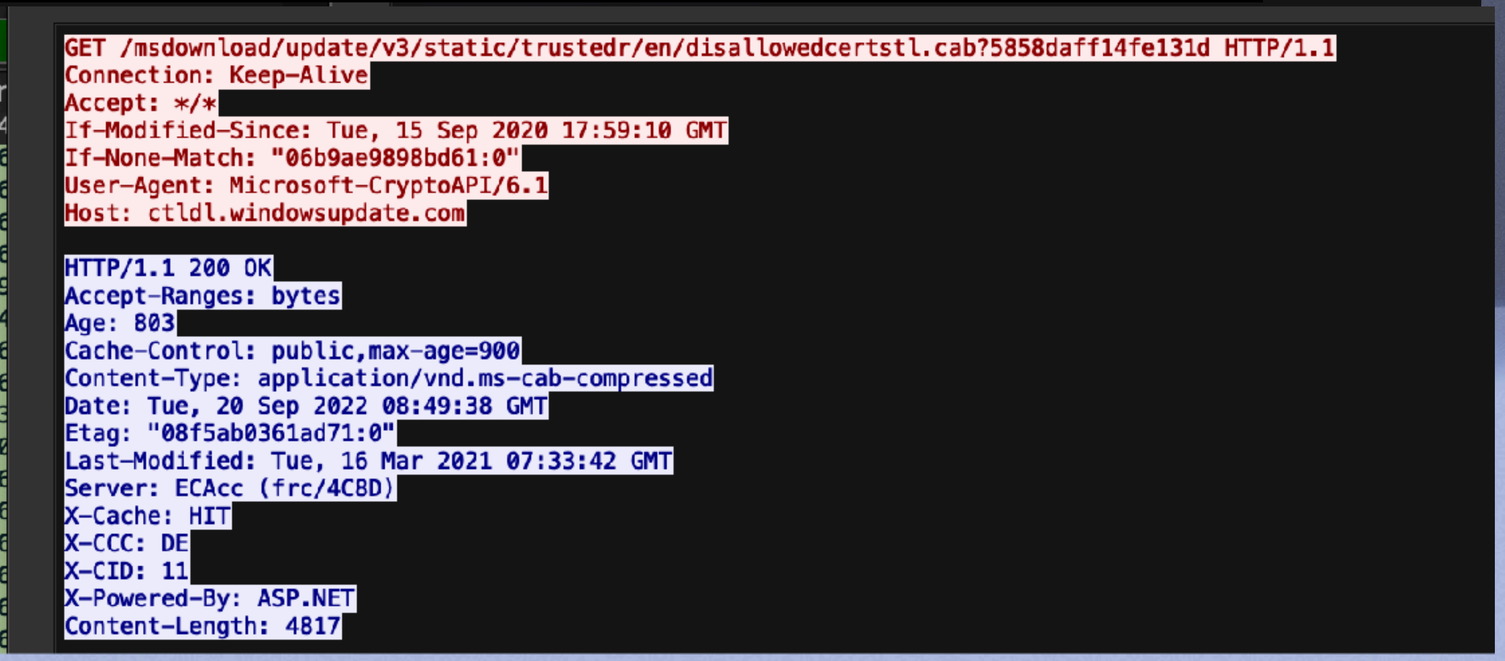
Slide Notes

Here, we're taking two separate PCAPs that are doing similar activity. It's benign - just GET requests to Microsoft domains.



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 | 9.390626 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 27 | 9.390640 | 93.184.221.240 | 192.168.100.205 | TCP | 53 |
| 28 | 9.390651 | 93.184.221.240 | 192.168.100.205 | TCP | 40 |
| 29 | 9.390914 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 30 | 9.390928 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 31 | 9.391679 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 32 | 9.392430 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 33 | 9.393180 | 93.184.221.240 | 192.168.100.205 | TCP | 126 |
| 34 | 9.393913 | 93.184.221.240 | 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
Content-Type: application/vnd.ms-cab-compressed
Date: Tue, 20 Sep 2022 08:49:38 GMT
Etag: "08f5ab0361ad71:0"
Last-Modified: Tue, 16 Mar 2021 07:33:42 GMT
Server: ECAcc (frc/4CBD)
X-Cache: HIT
X-CCC: DE
X-CID: 11
X-Powered-By: ASP.NET
Content-Length: 4817
```

# Two PCAP files: Similar Traffic

Transactions per Second

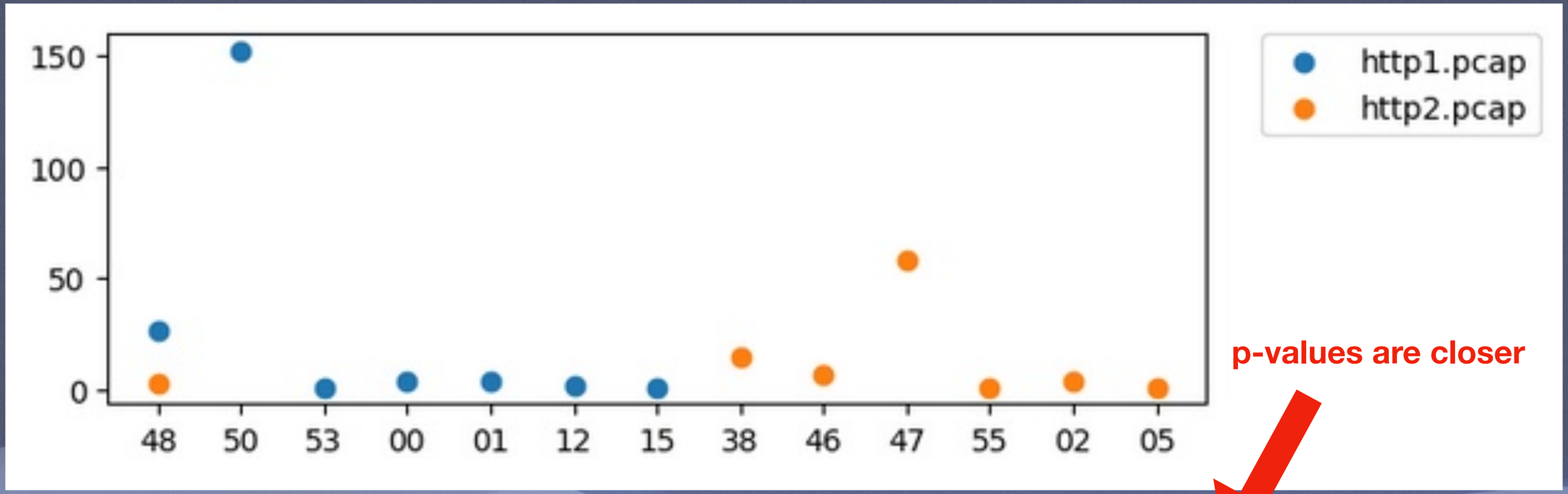
7 Time Items

| 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) |

# Two PCAP files: Similar Traffic




p-values are closer

```
p-value for file1:  0.2554054261260107 5
p-value for file2:  0.1785180516287488 4
```

# Problems with Cointegration

# Problems with Cointegration: The Time Value

```
1 file1='http1.pcap'
2 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) |

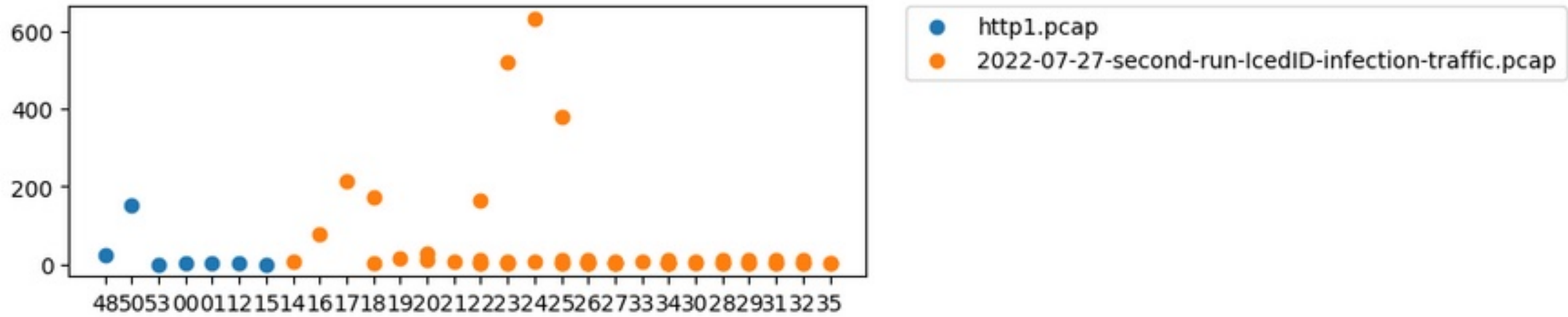
| | 2022-07-27-second-run-IcedID-infection-traffic.pcap |
|---|---|
| 14 | 7 |
| 16 | 76 |
| 17 | 213 |
| 18 | 174 |
| 18 | 3 |
| 19 | 16 |
| 20 | 27 |
| 21 | 7 |
| 22 | 164 |
| 23 | 519 |
| 24 | 632 |
| 25 | 378 |
| 26 | 5 |
| 27 | 2 |
| 33 | 6 |
| 34 | 2 |
| 26 | 6 |
| 27 | 6 |
| 30 | 6 |
| 34 | 4 |
| 27 | 3 |
| 20 | 13 |
| 22 | 2 |
| 22 | 4 |
| 22 | 13 |
| 23 | 2 |
| 23 | 4 |
| 23 | 7 |
| 24 | 6 |
| 25 | 2 |
| 25 | 4 |
| 25 | 13 |
| | 2 |
| | 4 |
| | 10 |
| | 3 |
| 28 | 2 |
| 28 | 4 |
| 28 | 13 |
| 29 | 2 |
| 29 | 4 |
| 29 | 10 |
| 30 | 3 |
| 31 | 2 |

Slide Notes

If the lengths are different, it won't work

# Problems with Cointegration: The Time Value

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

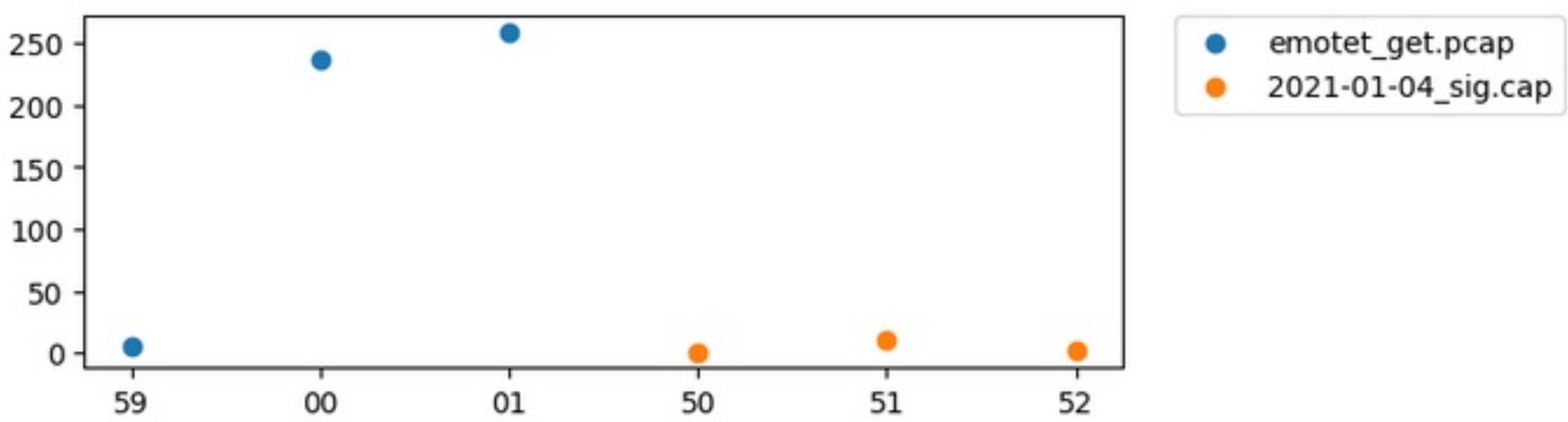



```
p-value for file1:  0.25540542612601075
p-value for file2:  0.06304175482717005
```

# Problems with Cointegration: Short Sample Size

```
1 file1='emotet_get.pcap'
2 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

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

```
1  # Compute ADF for the two PCAPs:
2  result_f1 = adfuller(df_f1[file1])
3  print("p-value for file1: ",result_f1[1])
4
5  result_f2 = adfuller(df_f2[file2])
6  print("p-value for file2: ",result_f2[1])
7
```



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

Slide Notes

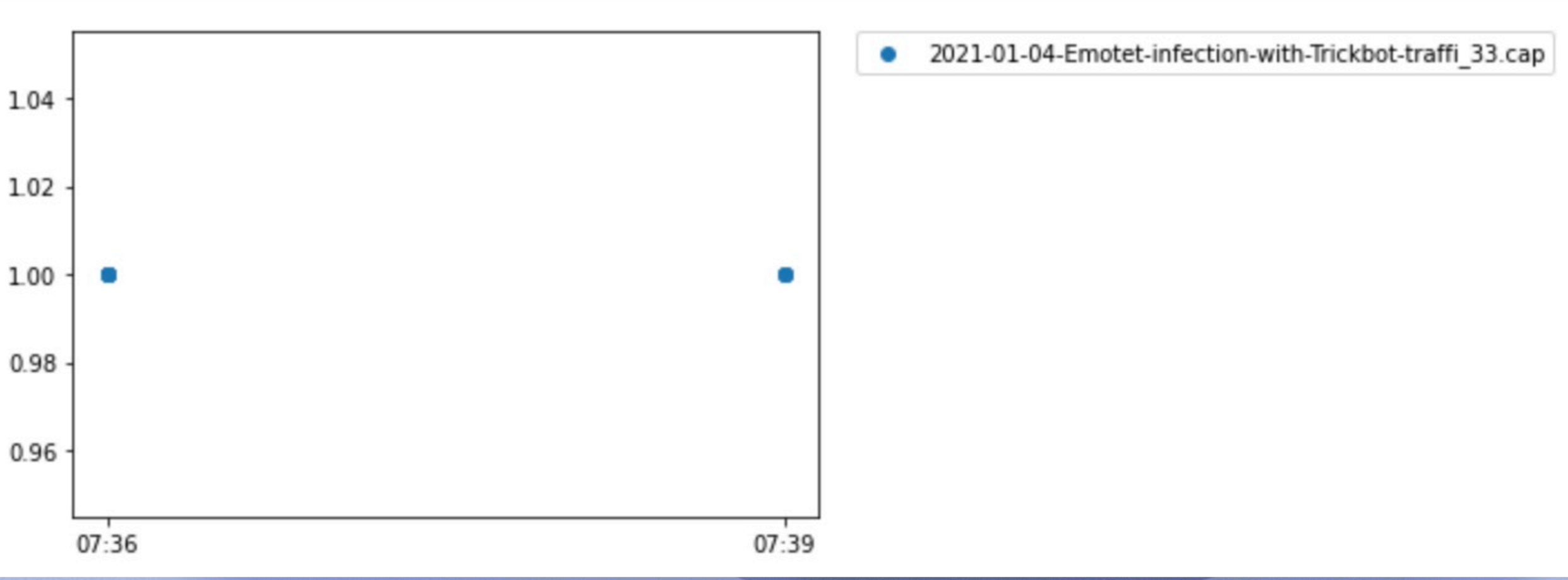
To consider: What is the best measurement of time to look at?

# Time Resolution

# At the ‘Minutes’ Resolution

Slide Notes

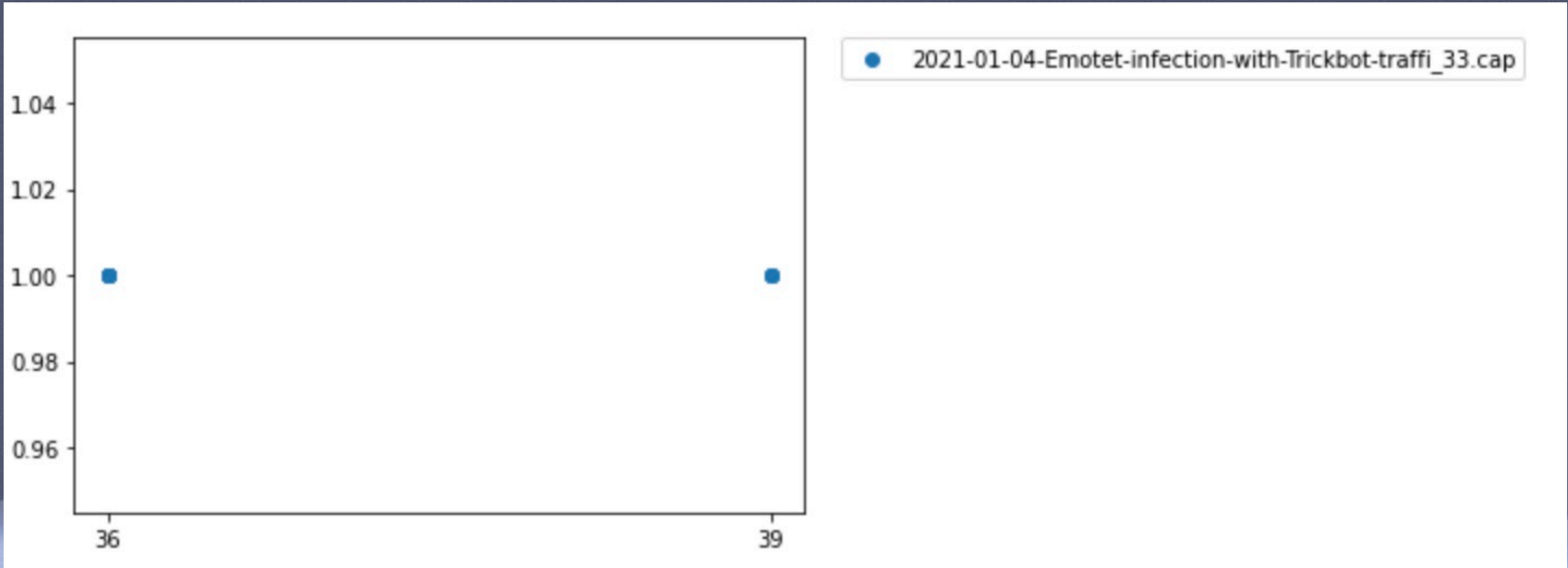
Minutes is too long



# At the ‘seconds’ Resolution

Slide Notes

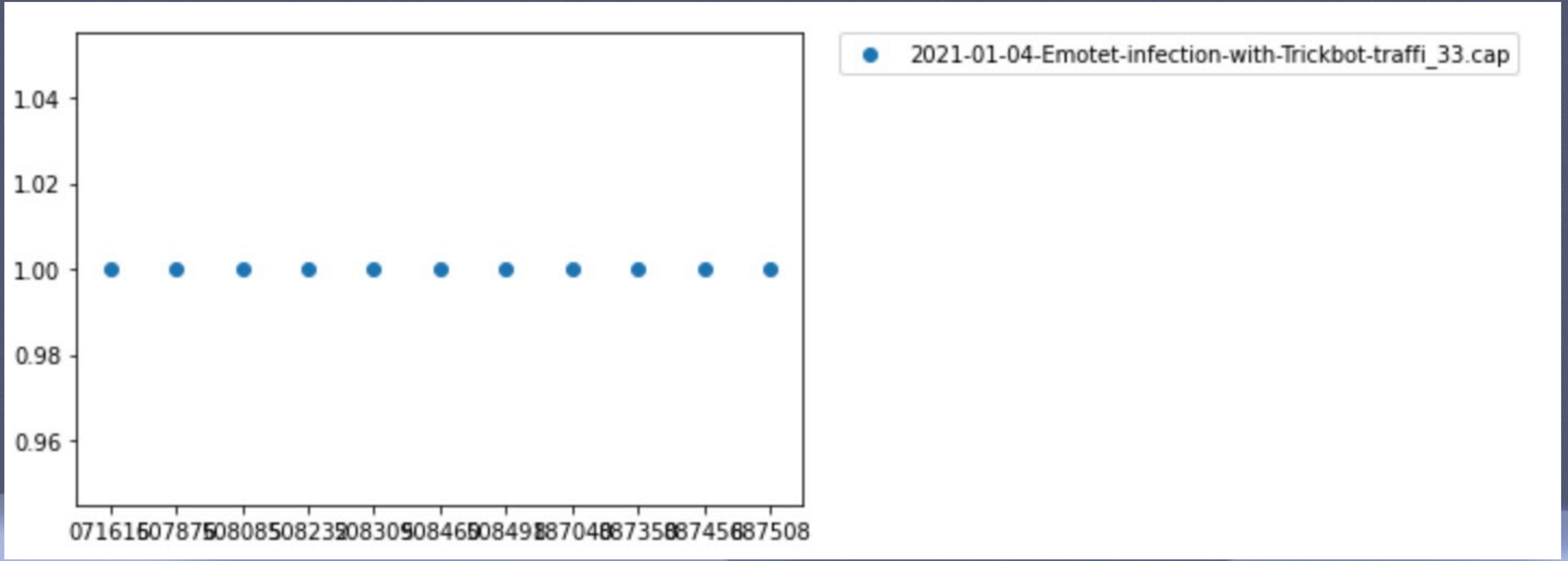
Seconds is also too long



# At the ‘microseconds’ Resolution

Slide Notes

Microseconds is better



Slide Notes

The time may need to be normalized, this explores that option.

# Normalize

# Normalized: Time a Transaction Occurred

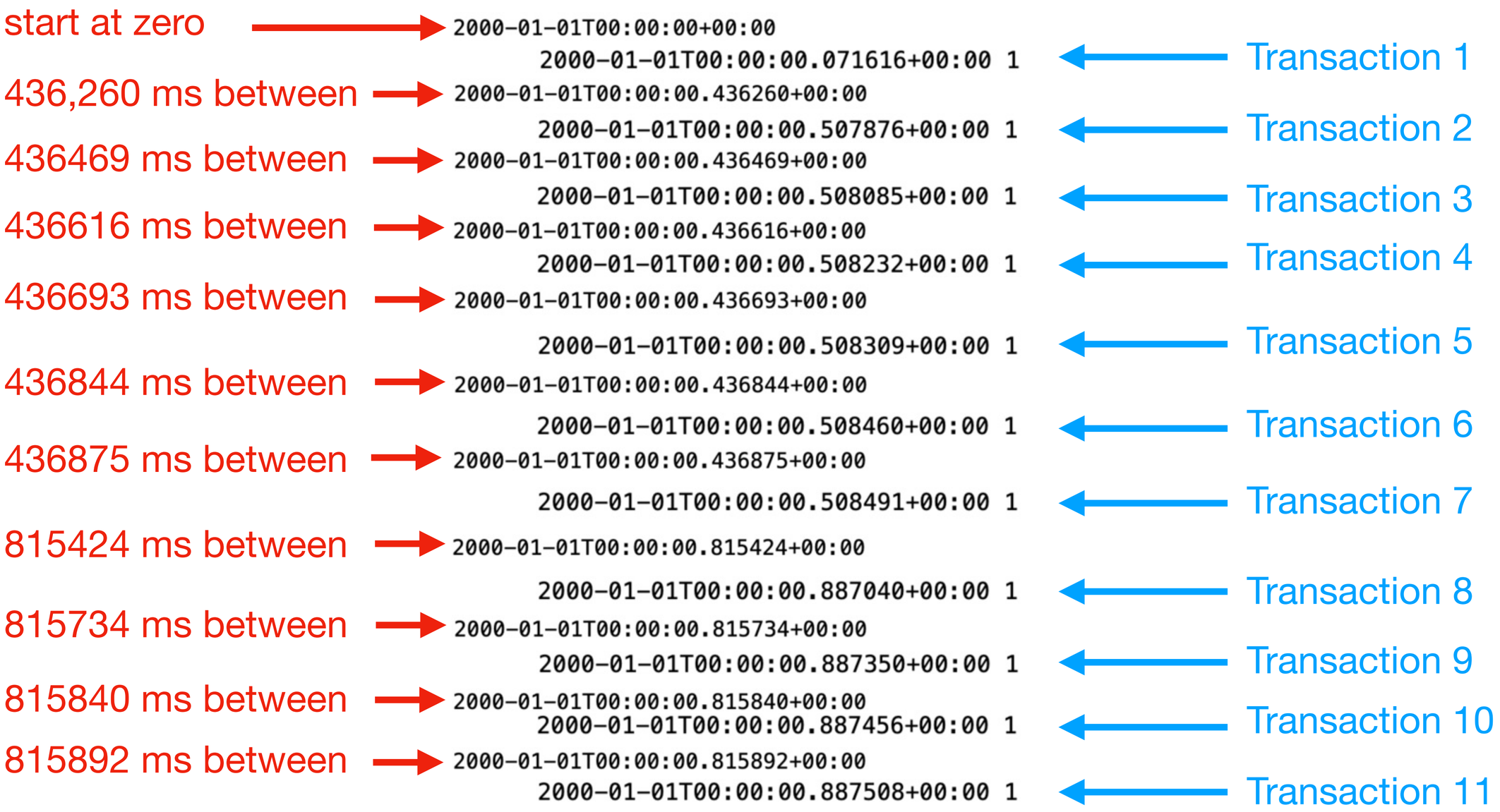
```
for i in when_transactions_happened:
    print(i['date'],i['count'])
```

```
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
2000-01-01T00:00:00.508491+00:00 1
2000-01-01T00:00:00.887040+00:00 1
2000-01-01T00:00:00.887350+00:00 1
2000-01-01T00:00:00.887456+00:00 1
2000-01-01T00:00:00.887508+00:00 1
```

Slide Notes

Setting all the transactions to start at the same time

# Combo of the two



# Signature Creation

Slide Notes

The flows need to be separated/isolated. If given a PCAP, take all flows and work on them individually

# Separate Flows

# Lots of Flows

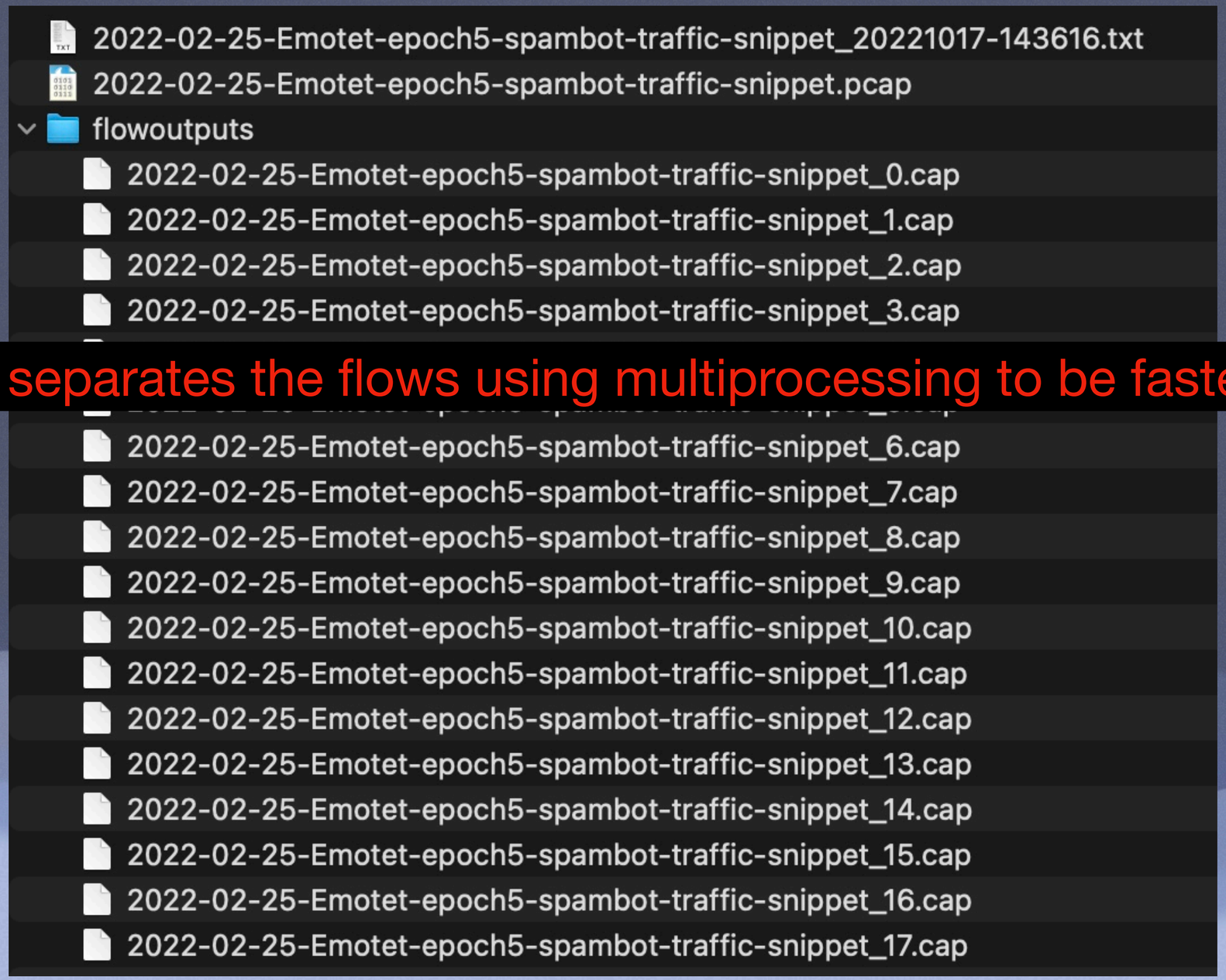
Ethernet · 4 | IPv4 · 120 | IPv6 | TCP · 353 | UDP · 230

| 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 |
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | 1.350 KiB | 138.918247 | 55.9948 |
| 192.[illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | 8.390 KiB | 285.111452 | 37.1815 |
| 192.[illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | 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 |
| 192.168.1.221 | 67.195.204.79 | 254 | 31.027 KiB | 120 | 20.489 KiB | 134 | 10.538 KiB | 290.918861 | 39.8501 |
| 192.168.1.221 | 67.195.228.111 | 19 | 1.470 KiB | 6 | 425 bytes | 13 | 1.055 KiB | 310.861517 | 10.8436 |

Slide Notes

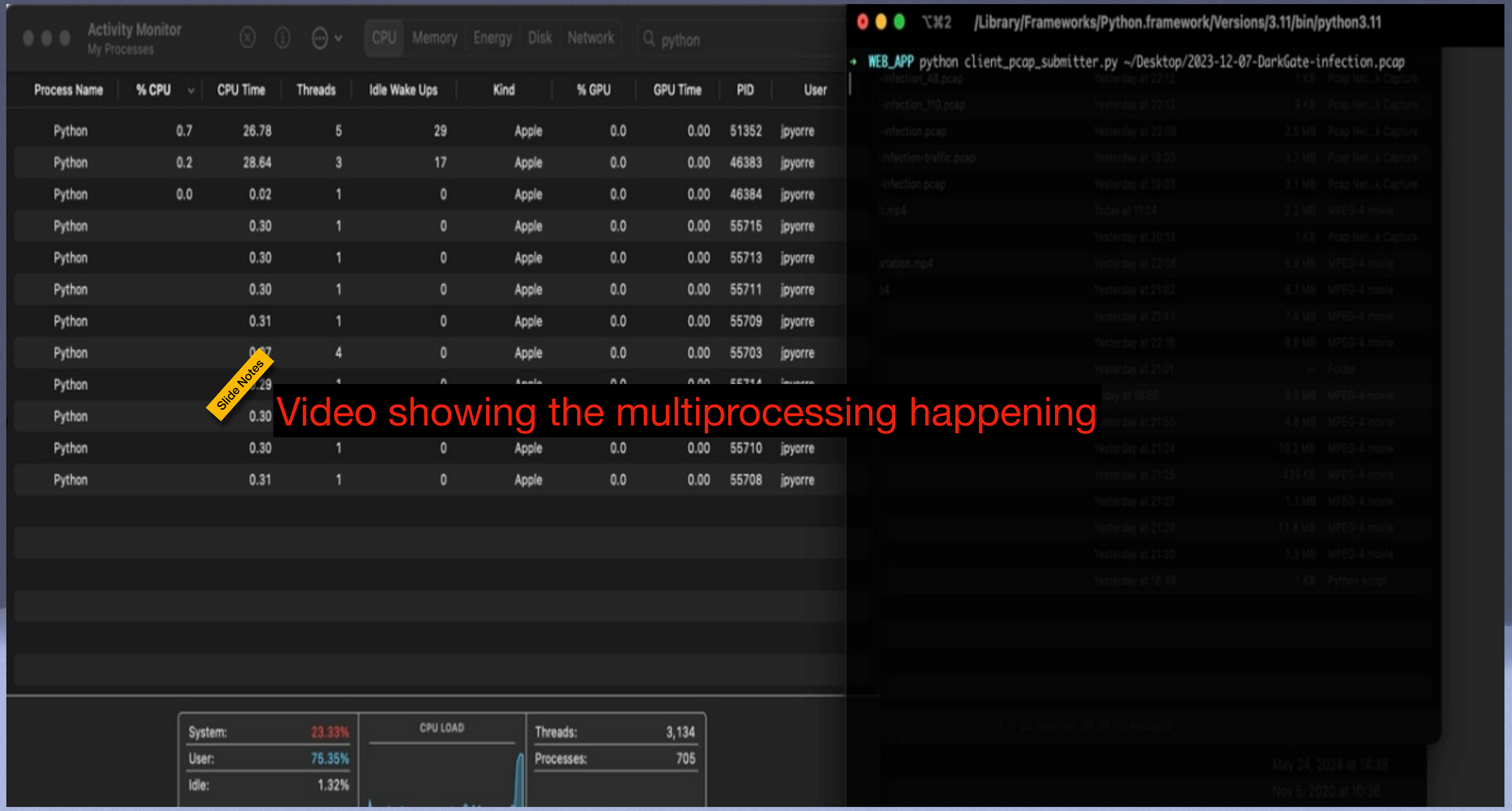
There are lots of flows at once going over the wire/air

# Operate against each flow individually




Slide Notes

My code separates the flows using multiprocessing to be faster


Activity Monitor
My Processes
CPU
Memory
Energy
Disk
Network
python
Process Name
% CPU
CPU Time
Threads
Idle Wake Ups
Kind
% GPU
GPU Time
PID
User
Python 0.7 26.78 5 29 Apple 0.0 0.00 51352 jpyorre
Python 0.2 28.64 3 17 Apple 0.0 0.00 46383 jpyorre
Python 0.0 0.02 1 0 Apple 0.0 0.00 46384 jpyorre
Python 0.30 1 0 Apple 0.0 0.00 55715 jpyorre
Python 0.30 1 0 Apple 0.0 0.00 55713 jpyorre
Python 0.30 1 0 Apple 0.0 0.00 55711 jpyorre
Python 0.31 1 0 Apple 0.0 0.00 55709 jpyorre
Python 4 0 Apple 0.0 0.00 55703 jpyorre
Python 0.30 1 0 Apple 0.0 0.00 55710 jpyorre
Python 0.31 1 0 Apple 0.0 0.00 55708 jpyorre
Slide Notes
Video showing the multiprocessing happening
/Library/Frameworks/Python.framework/Versions/3.11/bin/python3.11
WEB_APP python client_pcap_submitter.py ~/Desktop/2023-12-07-DarkGate-infection.pcap
System: 23.33%
User: 75.35%
Idle: 1.32%
CPU LOAD
Threads: 3,134
Processes: 705

# 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
    Average beteen queries: 14135.07467057101
    Total Queries: 1367
2022-02-25-Emotet-epoch5-spambot-traffic-snippet_15.cap
    Average beteen queries: 8049.0
    Total Queries: 3
2022-02-25-Emotet-epoch5-spambot-traffic-snippet_14.cap
    Average beteen queries: 73373.6
    Total Queries: 11
2022-02-25-Emotet-epoch5-spambot-traffic-snippet_16.cap
    Average beteen queries: 133663.0588235294
    Total Queries: 18
2022-02-25-Emotet-epoch5-spambot-traffic-snippet_17.cap
    Average beteen queries: 150335.16666666666
    Total Queries: 25
2022-02-25-Emotet-epoch5-spambot-traffic-snippet_13.cap
    Average beteen queries: 59165.142857142855
    Total Queries: 36
```

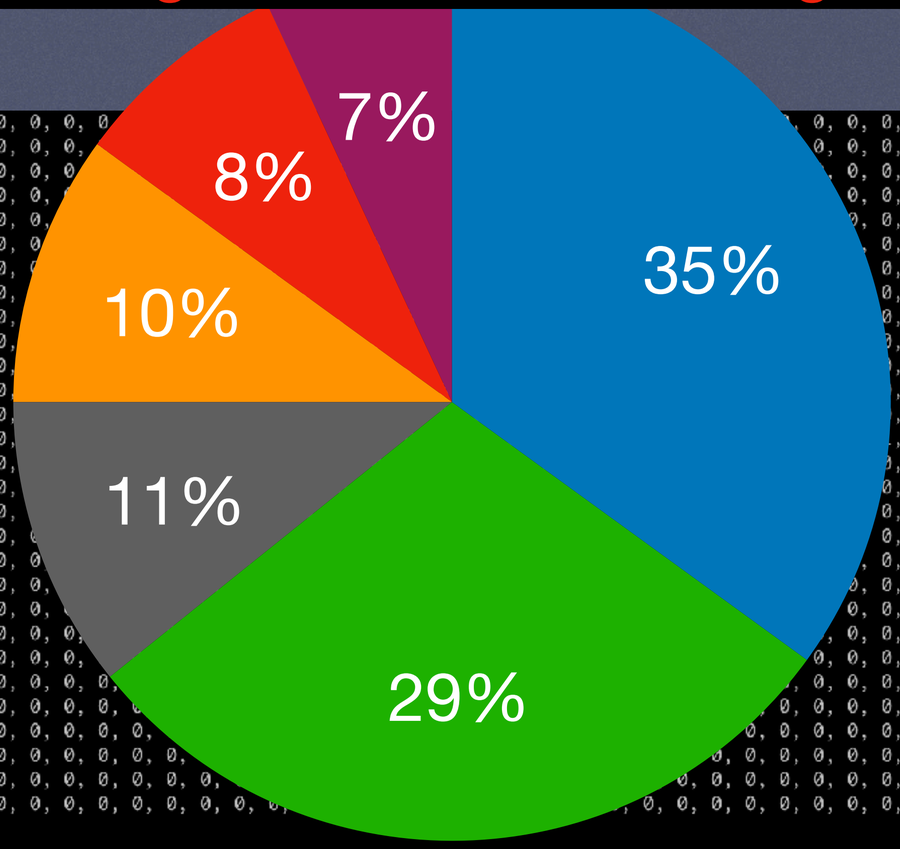
Slide Notes

Working with the microseconds is too specific. I abstract them by turning them into percentages of the entire network transaction

# Calculate Percentages

Slide Notes

# Percentages end up having a lot of zeros. We'll get rid of those.





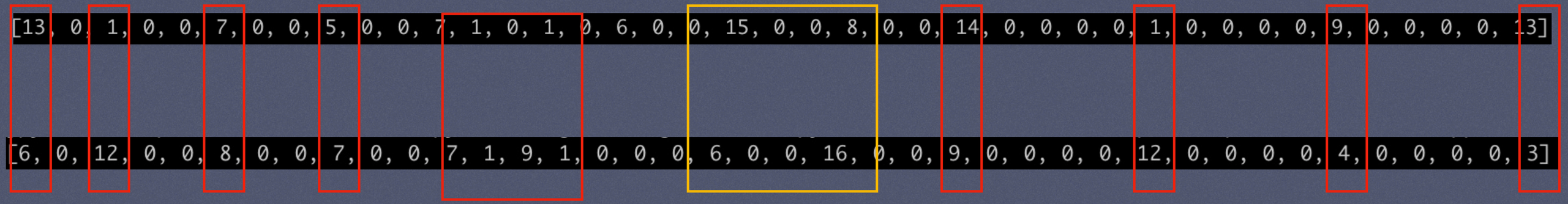
0, 0, 0, 

Slide Notes

# Just a quick look - seeing similarities using percentages

**Similar traffic Times**

**Similar traffic Times**

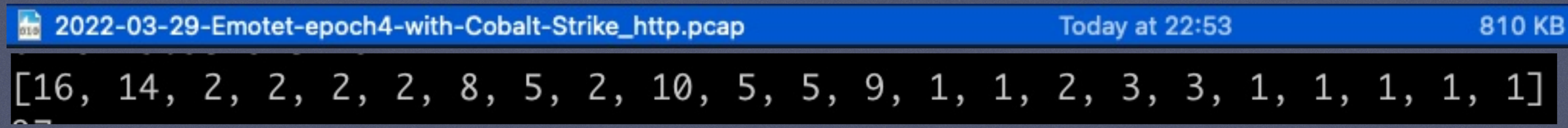


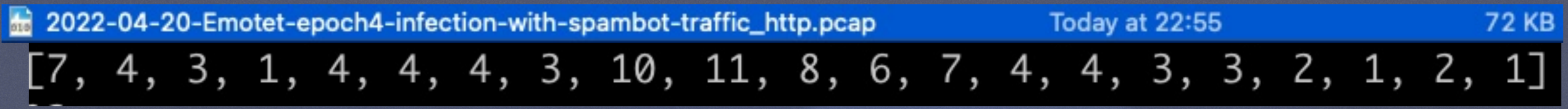

**A little off**

Slide Notes

Get rid of floats. I only want integers

# Add a little chaos




# By Rounding things

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

Slide Notes

Starting to get to something that I can call a signature

```
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]
```

# Now we can find exact matches

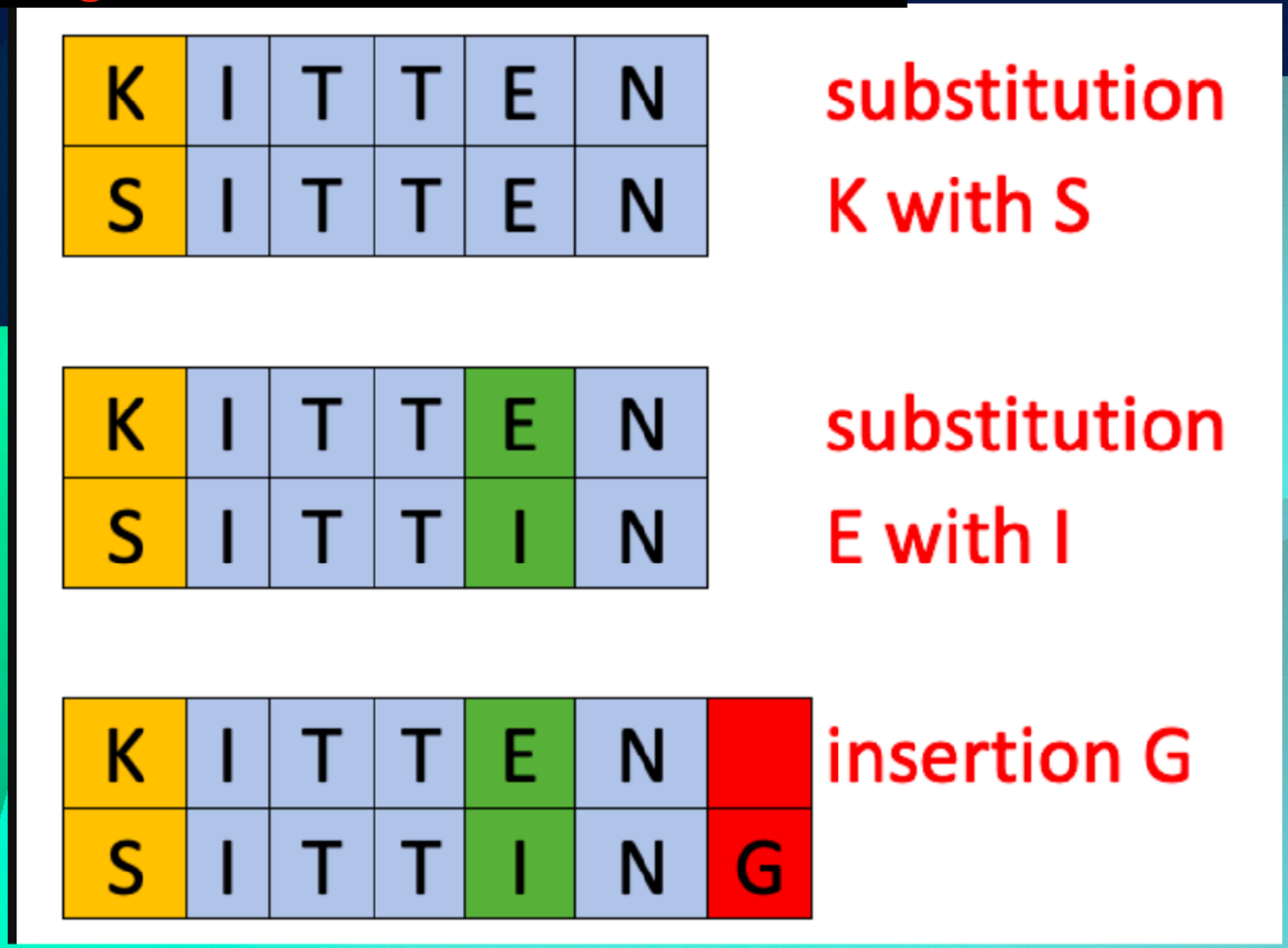


**Not really Useful**

# Levenshtein Distance

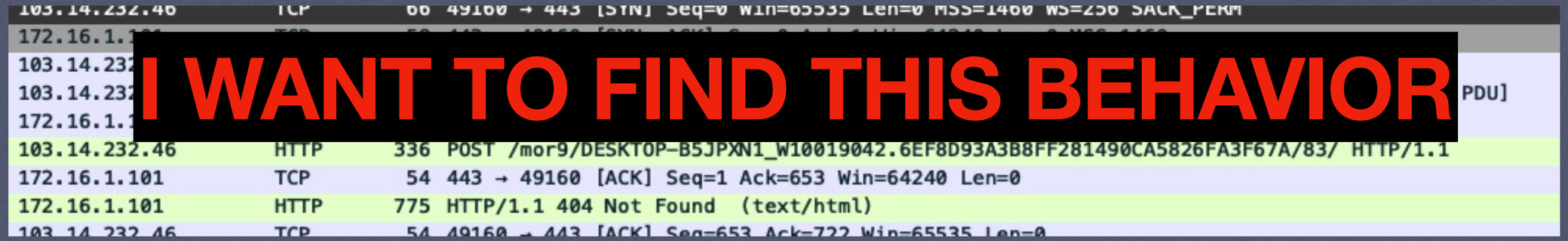
Slide Notes

I need something to find different, but similar.

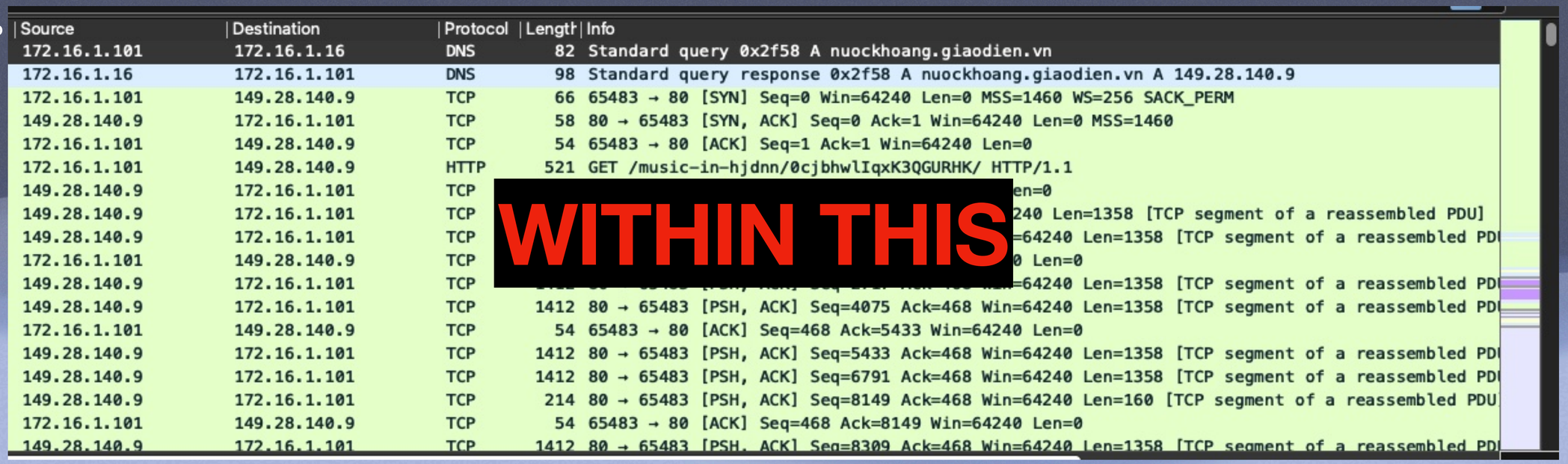


| | | |
|---|---|---|
| 2021-01-04_sig.cap | Oct 14, 2022 at 22:51 | 2 KB |
| 2021-01-04-Emotet-infection-with-Trickbot-traffic.pcap | Oct 12, 2022 at 23:46 | 5.4 MB |

Signature




Large PCAP



# Create Signature

```
2020-12-29-Emotet-infection-with-Trickbot-and-spambot-activity_POST.pcap:
Percent of each time in between toward the total: [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 2,
1, 1, 2, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 2, 2, 2]
```

```
{
    "emotetGET_20220707":[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
        1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 2, 1, 1, 2, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 2, 2, 2]
}
```

Slide Notes

Finding the exact match - number represents probability of a match. It is never 100 unless its exact and there is no real good area to decide the threshold.

```
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_47.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_20.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_37.cap: emotetGET_20220707, 73
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_23.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_22.cap: emotetGET_20220707, 57
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_2.cap: emotetGET_20220707, 57
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_36.cap: emotetGET_20220707, 75
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_32.cap: emotetGET_20220707, 56
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_6.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_26.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_27.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_33.cap: emotetGET_20220707, 62
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_7.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_19.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_25.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_5.cap: emotetGET_20220707, 45
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_31.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_4.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_30.cap: emotetGET_20220707, 56
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_24.cap: emotetGET_20220707, 71
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_18.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_15.cap: emotetGET_20220707, 57
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_9.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_29.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_28.cap: emotetGET_20220707, 57
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_8.cap: emotetGET_20220707, 52
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_14.cap: emotetGET_20220707, 57
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_16.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_17.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_13.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_12.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_38.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_10.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_11.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_39.cap: emotetGET_20220707, 58
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_49.cap: emotetGET_20220707, 50
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_48.cap: emotetGET_20220707, 67
```

Slide Notes

The search needs to be fuzzier

# Fuzzyness



https://github.com/seatgeek/thefuzz

README.rst

*Used to be called Fuzzy Wuzzy, which is way cooler in my opinion*

# TheFuzz

Fuzzy string matching like a boss. It uses Levenshtein Distance to calculate the differences between sequences in a simple-to-use package.

Slide Notes

Introducing fuzzy ratio to loosen up the search, now I can find a number that separates the hits from the misses.

```
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_43.cap: emotetGET_20220707, 75
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_41.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_44.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_46.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_52.cap: emotetGET_20220707, 100
MATCH: emotetGET_20220707, in flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_52.cap
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_37.cap: emotetGET_20220707, 73
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_36.cap: emotetGET_20220707, 75
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_27.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_33.cap: emotetGET_20220707, 62
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_4.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_24.cap: emotetGET_20220707, 71
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_48.cap: emotetGET_20220707, 67
jpyorre@Joshs-MacBook-Pro 3_signature_testing %
```

Slide Notes

# above 75 fuzzy ratio seems to match here

```
jpyorre@Joshs-MacBook-Pro 3_signature_testing % python3 test_signature.py 2021-01-04-Emotet-infection-with-Trickbot-traffi
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_43.cap: emotetGET_20220707, 75
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_41.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_44.cap:
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_46.cap:
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_52.cap: emotetGET_20220707, 100
MATCH: emotetGET_20220707, in flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_52.cap
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_37.cap: emotetGET_20220707, 73
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_36.cap: emotetGET_20220707, 75
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_27.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_33.cap: emotetGET_20220707, 62
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_4.cap: emotetGET_20220707, 67
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_24.cap: emotetGET_20220707, 71
partial_ratio: flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_48.cap: emotetGET_20220707, 67
jpyorre@Joshs-MacBook-Pro 3_signature_testing %
```

Signature made from this flow:

# EXACT MATCH

Slide Notes

One of the highest

```
flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_36.cap: emotetGET_20220707, 75
```

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 172.16.1.101 | 103.14.232.46 | TCP | 66 | 65527 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 103.14.232.46 | 172.16.1.101 | TCP | 58 | 443 → 65527 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65527 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 172.16.1.101 | 103.14.232.46 | TCP | 424 | 65527 → 443 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=370 [TCP segment o |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65527 [ACK] Seq=1 Ack=371 Win=64240 Len=0 |
| 172.16.1.101 | 103.14.232.46 | HTTP | 336 | POST /mor9/DESKTOP-B5JPXN1_W10019042.6EF8D93A3B8FF281490CA5826FA3F6 |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65527 [ACK] Seq=1 Ack=653 Win=64240 Len=0 |
| 103.14.232.46 | 172.16.1.101 | HTTP | 775 | HTTP/1.1 404 Not Found (text/html) |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65527 → 443 [ACK] Seq=653 Ack=722 Win=65535 Len=0 |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65527 → 443 [FIN, ACK] Seq=653 Ack=722 Win=65535 Len=0 |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65527 [ACK] Seq=722 Ack=654 Win=64239 Len=0 |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65527 [FIN, PSH, ACK] Seq=722 Ack=654 Win=64239 Len=0 |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65527 → 443 [ACK] Seq=654 Ack=723 Win=65535 Len=0 |

# ANOTHER EXACT MATCH

```
flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_43.cap: emotetGET_20220707, 75
```

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 172.16.1.101 | 103.14.232.46 | TCP | 66 | 65534 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PE |
| 103.14.232.46 | 172.16.1.101 | TCP | 58 | 443 → 65534 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65534 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 172.16.1.101 | 103.14.232.46 | TCP | 424 | 65534 → 443 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=370 [TCP segme |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65534 [ACK] Seq=1 Ack=371 Win=64240 Len=0 |
| 172.16.1.101 | 103.14.232.46 | HTTP | 336 | POST /mor9/DESKTOP-B5JPXN1_W10019042.6EF8D93A3B8FF281490CA5826F |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65534 [ACK] Seq=1 Ack=653 Win=64240 Len=0 |
| 103.14.232.46 | 172.16.1.101 | HTTP | 775 | HTTP/1.1 404 Not Found  (text/html) |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65534 → 443 [ACK] Seq=653 Ack=722 Win=65535 Len=0 |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65534 → 443 [FIN, ACK] Seq=653 Ack=722 Win=65535 Len=0 |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65534 [ACK] Seq=722 Ack=654 Win=64239 Len=0 |
| 103.14.232.46 | 172.16.1.101 | TCP | 54 | 443 → 65534 [FIN, PSH, ACK] Seq=722 Ack=654 Win=64239 Len=0 |
| 172.16.1.101 | 103.14.232.46 | TCP | 54 | 65534 → 443 [ACK] Seq=654 Ack=723 Win=65535 Len=0 |

# NO MATCH

Slide Notes

A little less and it starts to fall away

```
flowoutputs/2021-01-04-Emotet-infection-with-Trickbot-traffi_46.cap: emotetGET_20220707, 67
```

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 172.16.1.101 | 185.188.6.10 | TCP | 66 | 49154 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 172.16.1.101 | 185.188.6.10 | TCP | 66 | [TCP Retransmission] [TCP Port numbers reused] 49154 → 443 [SYN] Se |
| 172.16.1.101 | 185.188.6.10 | TCP | 66 | [TCP Retransmission] [TCP Port numbers reused] 49154 → 443 [SYN] Se |
| 172.16.1.101 | 185.188.6.10 | TCP | 66 | [TCP Retransmission] [TCP Port numbers reused] 49154 → 443 [SYN] Se |
| 172.16.1.101 | 185.188.6.10 | TCP | 66 | [TCP Retransmission] [TCP Port numbers reused] 49154 → 443 [SYN] Se |
| 185.188.6.10 | 172.16.1.101 | TCP | 54 | 443 → 49154 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0 |

Slide Notes

Create signatures using both to improve detection

# New signature, different PCAP

# Make a signature out of this

MALWARE-TRAFFIC-ANALYSIS.NET

## 2022-02-10 (THURSDAY) - EMOTET EPOCH 5 INFECTION WITH COBALT STRIKE

REFERENCE:

- **https://twitter.com/Unit42_Intel/status/1492160514109149193**

ASSOCIATED FILES:

- **2022-02-10-IOCs-for-Emotet-epoch5-infection-with-Cobalt-Strike.txt.zip** 2.2 kB
- **2022-02-10-Emotet-epoch5-malspam-0207-UTC.eml.zip** 88.3 kB (88,261 bytes)
- **2022-02-10-Emotet-epoch5-infection-with-Cobalt-Strike.pcap.zip** 11.1 MB (11
- **2022-02-10-Emotet-epoch5-and-Cobalt-Stike-malware-and-artifacts.zip** 506.2 k

NOTES:

- All zip archives on this site are password-protected. If you don't know the password

**Click here** to return to the main page.

Copyright © 2022 | Ma

tcp.stream eq 1

| o. | Time | Source | Destination |
|---|---|---|---|
| 12 | 2022-02-10 16:58:08.776470 | 10.2.10.101 | 66.175.58.9 |
| 13 | 2022-02-10 16:58:08.879231 | 66.175.58.9 | 10.2.10.101 |
| 14 | 2022-02-10 16:58:08.879339 | 10.2.10.101 | 66.175.58.9 |
| 15 | 2022-02-10 16:58:08.879507 | 10.2.10.101 | 66.175.58.9 |
| 16 | 2022-02-10 16:58:08.879541 | 66.175.58.9 | 10.2.10.101 |
| 17 | 2022-02-10 16:58:09.009401 | 66.175.58.9 | 10.2.10.101 |
| 18 | 2022-02-10 16:58:09.009610 | 66.175.58.9 | 10.2.10.101 |
| 19 | 2022-02-10 16:58:09.009668 | 10.2.10.101 | 66.175.58.9 |
| 20 | 2022-02-10 16:58:09.009695 | 66.175.58.9 | 10.2.10.101 |
| 21 | 2022-02-10 16:58:09.057344 | 10.2.10.101 | 66.175.58.9 |
| 22 | 2022-02-10 16:58:09.124524 | 66.175.58.9 | 10.2.10.101 |
| 23 | 2022-02-10 16:58:09.124606 | 66.175.58.9 | 10.2.10.101 |
| 24 | 2022-02-10 16:58:09.124677 | 10.2.10.101 | 66.175.58.9 |
| 25 | 2022-02-10 16:58:09.125997 | 66.175.58.9 | 10.2.10.101 |
| 26 | 2022-02-10 16:58:09.126150 | 66.175.58.9 | 10.2.10.101 |
| 27 | 2022-02-10 16:58:09.126195 | 10.2.10.101 | 66.175.58.9 |
| 28 | 2022-02-10 16:58:09.126296 | 66.175.58.9 | 10.2.10.101 |
| 29 | 2022-02-10 16:58:09.183286 | 10.2.10.101 | 66.175.58.9 |
| 30 | 2022-02-10 16:58:09.242685 | 66.175.58.9 | 10.2.10.101 |
| 31 | 2022-02-10 16:58:09.242762 | 66.175.58.9 | 10.2.10.101 |
| 32 | 2022-02-10 16:58:09.242878 | 10.2.10.101 | 66.175.58.9 |
| 33 | 2022-02-10 16:58:09.244385 | 66.175.58.9 | 10.2.10.101 |
| 34 | 2022-02-10 16:58:09.244472 | 66.175.58.9 | 10.2.10.101 |
| 35 | 2022-02-10 16:58:09.244533 | 10.2.10.101 | 66.175.58.9 |

Frame 15: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93

Wireshark · Follow TCP Stream (tcp.stream eq 1) · 2022

```
GET /NATE_05_22_2009/BI710N4cQ6R3/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPow
Host: tempral.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 10 Feb 2022 15:58:09 GMT
Content-Type: application/x-msdownload
Content-Length: 560128
Connection: keep-alive
Set-Cookie: 620536110685a=1644508689; expires=Thu, 10-Feb-2022 15:59:09
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Thu, 10 Feb 2022 15:58:09 GMT
Expires: Thu, 10 Feb 2022 15:58:09 GMT
Content-Disposition: attachment; filename="WteY.dll"
Content-Transfer-Encoding: binary

MZ.....@.....
```

Current signatures:


```
{
 "2022-02-10-Emotet-epoch5-infection-with-Cobalt-Strike_for_signature_20230308-121157": [
  3,
  4,
  1,
  2,
  2,
  2,
  1,
  2,
  2,
  1,
  2,
  1,
  1,
  2,
  3,
  3,
  1,
  3,
  3,
  3,
  3,
  3,
  3,
  3,
  3,
  1,
  1,
  1,
  1,
  2,
  1,
  2,
  1,
  1,
  1,
```

# Download some other PCAP




## 2022-07-05 (TUESDAY) - QUICK POST: EMOTET

NOTES:

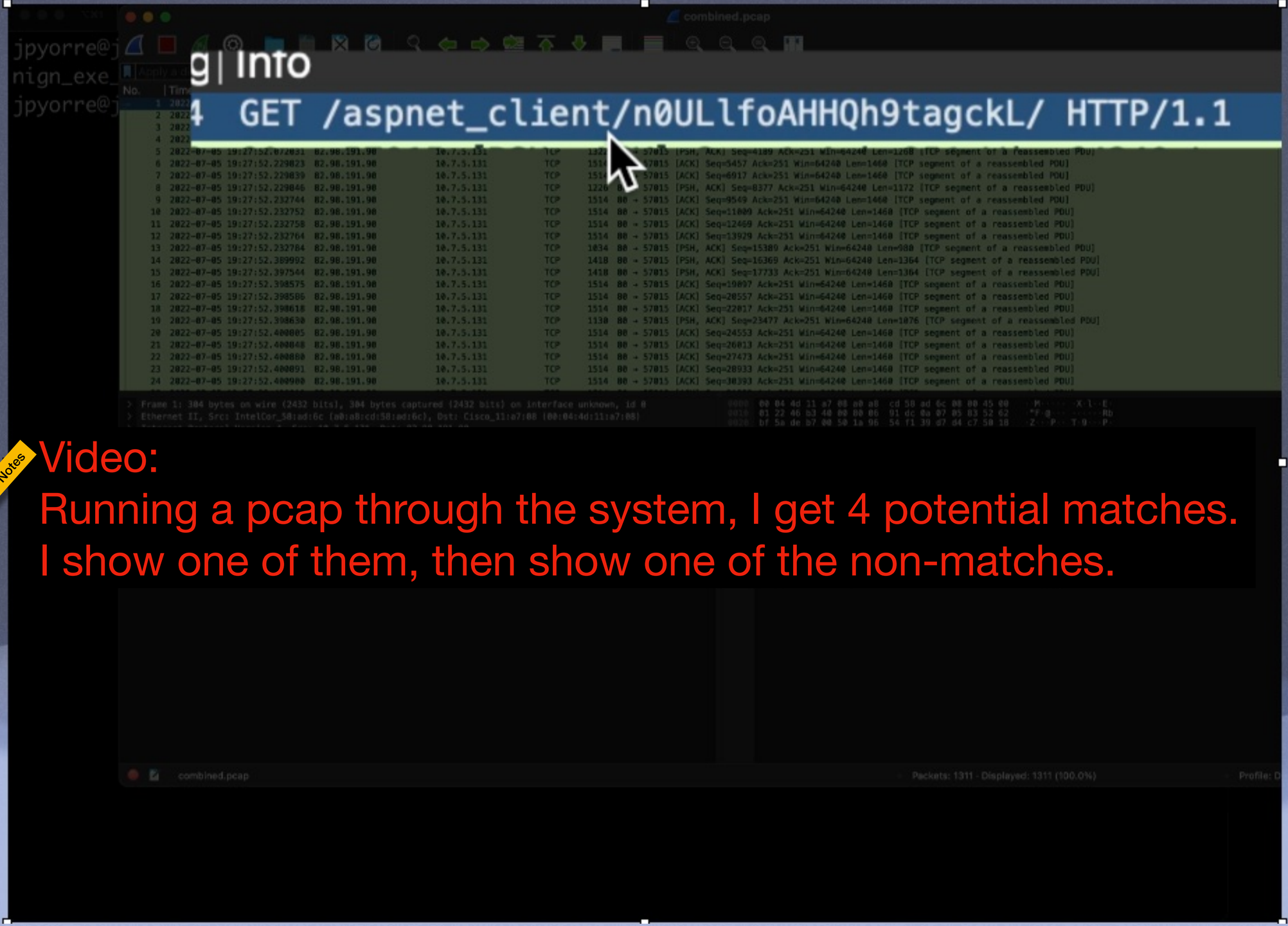
- Zip files are password-protected. If you don't know the password, see the "about" page of this website.

ASSOCIATED FILES:

- **2022-06-27-thru-07-05-Emotet-malspam-10-examples.zip** 465 kB (465,348 bytes)
- **2022-07-05-Emotet-epoch4-infection-with-spambot-traffic.pcap.zip** 19.9 MB (19,892,904 bytes)

**Click here** to return to the main page.

**Copyright © 2022 | Malware-Traffic-Analysis.net**




Slide Notes

Video:

Running a pcap through the system, I get 4 potential matches.

I show one of them, then show one of the non-matches.

Signatures

127.0.0.1:5000/analyzepcap

Total TCP flows: 1
Total UDP flows: 0
Total IPs: 2
Data for flow: (('10.7.5.131', 57038), ('217.79.180.211', 8080))
Total Bytes: 1514
Average Bytes: 1514.0
Total Duration: 0.0
Filename: combined_4.cap"
Percenta

Slide Notes

Video:
Running a pcap through the system, I get 4 potential matches.
I show one of them, then show one of the non-matches.
Starting to show it in web app form

2, 1, 4, 1]

**Total TCP flows:** 1
**Total UDP flows:** 0
**Total IPs:** 2
**Data for flow:** (('192.168.8.188', 55278), ('23.239.23.28', 80))
**Total Bytes:** 7100
**Average Bytes:** 507.14285714285717
**Total Duration:** 1.4970340728759766
**Filename:** combined_11.cap"
**Percentages of time in between:** [10, 1, 28]

## Signature:

```
GET /NATE_05_22_2009/BI710N4cQ6R3/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1320
Host: tempral.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 10 Feb 2022 15:58:09 GMT
Content-Type: application/x-msdownload
Content-Length: 560128
Connection: keep-alive
Set-Cookie: 620536110685a=1644508689; expires=Thu, 10-Feb-2022 15:59:09 GMT; Max-Age=60; path=/
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Thu, 10 Feb 2022 15:58:09 GMT
Expires: Thu, 10 Feb 2022 15:58:09 GMT
Content-Disposition: attachment; filename="WteY.dll"
Content-Transfer-Encoding: binary

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

## Matching Flow:

```
GET /aspnet_client/n0ULlfoAHHQh9tagckL/ 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: zonainformatica.es
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 525824
Content-Type: application/x-msdownload
Expires: Tue, 05 Jul 2022 17:27:51 GMT
Last-Modified: Tue, 05 Jul 2022 17:27:51 GMT
Server: Microsoft-IIS/8.0
X-Powered-By: PHP/7.3.0
Set-Cookie: 62c47497a0e2a=1657042071; expires=Tue, 05-Jul-2022 17:28:51 GMT; Max-Age=60; path=/
Content-Disposition: attachment; filename="2IGMMjM233lxT.dll"
Content-Transfer-Encoding: binary
X-Powered-By: ASP.NET
Date: Tue, 05 Jul 2022 17:27:51 GMT

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

Slide Notes

Sometimes, the threshold need to be tuned…

# TUNING

Slide Notes

# The threshold can be set in the code (at the top of the script)

```
9   from multiprocessing import Pool
10  from Levenshtein import distance as levenshtein_distance
11
12  threshold = 60 # Adjust this value as needed
13  levenshtein_threshold = 1  # Adjust this value as needed
14  signature_file = 'signatures/networkrules/signatures.json'
15  pcap_directory = 'static/analysis/flowoutputs'
16
```

Slide Notes

# Tuning with Darkgate activity, first PCAP




## 2023-11-30 (THURSDAY) - DARKGATE ACTIVITY

NOTICE:

- Of note, the zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

REFERENCES:

- **https://www.linkedin.com/posts/unit42_darkgate-timelythreatintel-malwaretraffic-activity-7136107640379637760-F4OH**
- **https://twitter.com/Unit42_Intel/status/1730342021628400092**

ASSOCIATED FILES:

- **2023-11-30-IOCs-for-DarkGate-activity.txt.zip** 1.9 kB (1,896 bytes)
- **2023-11-30-DarkGate-infection-traffic.pcap.zip** 1.7 MB (1,697,331 bytes)
- **2023-11-30-DarkGate-malware-and-artifacts.zip** 2.9 MB (2,915,603 bytes)

Slide Notes

# Tuning with Darkgate activity, second PCAP




## 2023-12-07 (THURSDAY): DARKGATE ACTIVITY

NOTICE:

- Of note, the zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

REFERENCE:

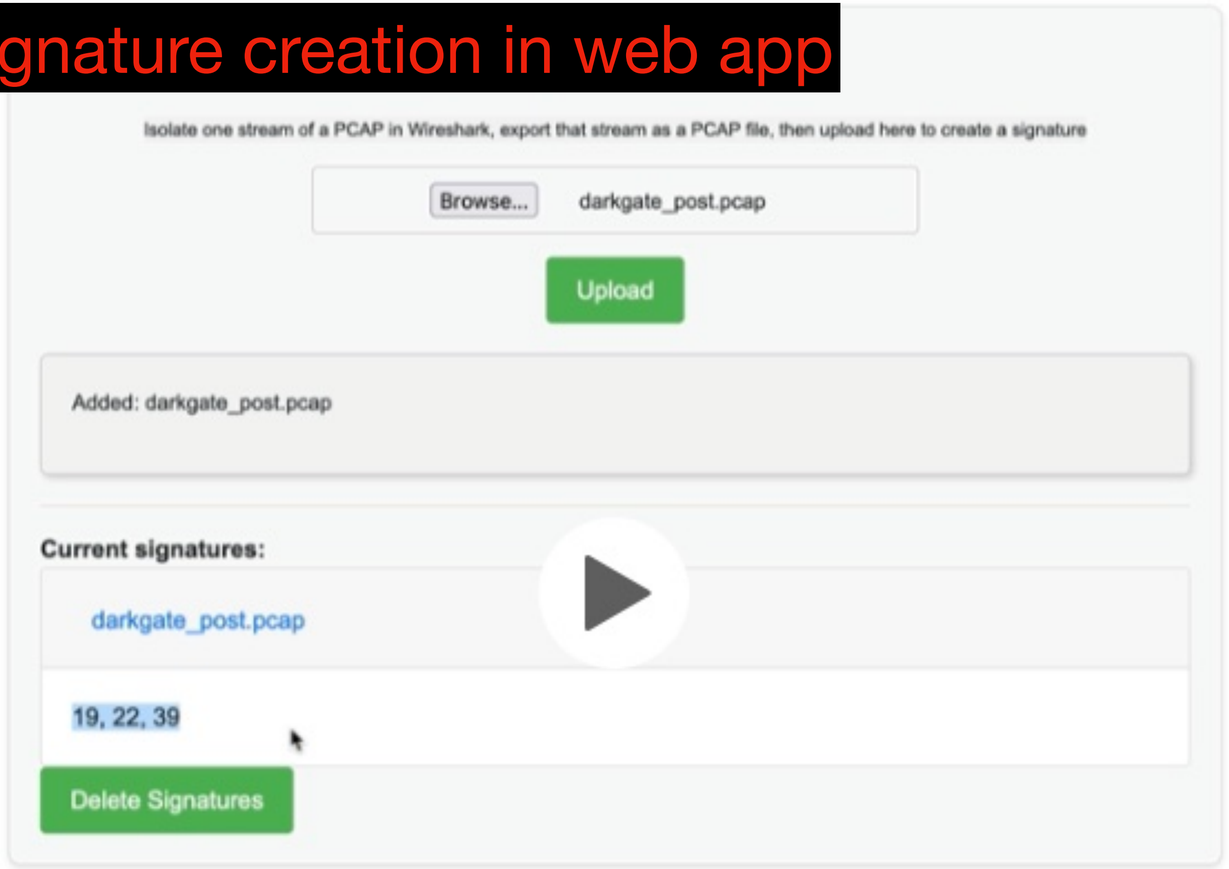
- **https://www.linkedin.com/posts/unit42_darkgate-timelythreatintel-threatintelligence-activity-7138645787709767680-mgL_/**
- **https://twitter.com/Unit42_Intel/status/1732857094167023618**

ASSOCIATED FILES:

- **2023-12-07-IOCs-for-DarkGate-infection.txt.zip** 2.4 kB (2,431 bytes)
- **2023-12-07-DarkGate-infection.pcap.zip** 2.8 MB (2,789,892 bytes)
- **2023-12-07-DarkGate-malware-and-artifacts.zip** 2.7 MB (2,690,277 bytes)

Slide Notes

# Video showing signature creation in web app



Upload a PCAP file to check against signatures:

Browse... 2023-11-30-DarkGate-infection-traffic.pcap

Upload

Slide Notes

Video showing matches and non-matches (used to tune the threshold)

- **File:** 2023-11-30-DarkGate-infection-traffi_2.pcap
  **Signature Name:** darkgate_post.pcap
  **Ratio:** 100%
  **Levenshtein Distance:** 0
  **Signature Percentages:** 19,22,39

**No matches on any of the following flows:**

- 2023-11-30-DarkGate-infection-traffi_22.pcap: Ratio: 75%
  **Levenshtein Distance:** 4
- 2023-11-30-DarkGate-infection-traffi_7.pcap: Ratio: 75%
  **Levenshtein Distance:** 3
- 2023-11-30-DarkGate-infection-traffi_38.pcap: Ratio: 75%
  **Levenshtein Distance:** 3
- 2023-11-30-DarkGate-infection-traffi_42.pcap: Ratio: 75%
  **Levenshtein Distance:** 3
- 2023-11-30-DarkGate-infection-traffi_58.pcap: Ratio: 75%
  **Levenshtein Distance:** 3
- 2023-11-30-DarkGate-infection-traffi_31.pcap: Ratio: 75%
  **Levenshtein Distance:** 4
- 2023-11-30-DarkGate-infection-traffi_8.pcap: Ratio: 75%
  **Levenshtein Distance:** 3
- 2023-11-30-DarkGate-infection-traffi_18.pcap: Ratio: 67%
  **Levenshtein Distance:** 4
- 2023-11-30-DarkGate-infection-traffi_14.pcap: Ratio: 67%
  **Levenshtein Distance:** 4
- 2023-11-30-DarkGate-infection-traffi_54.pcap: Ratio: 67%
  **Levenshtein Distance:** 5

- 2023-11-30-DarkGate-infection-traffi_41.pcap: Ratio: 67%

  **Levenshtein Distance:** 5
- 2023-11-30-DarkGate-infection-traffi_52.pcap: Ratio: 64%

  **Levenshtein Distance:** 4

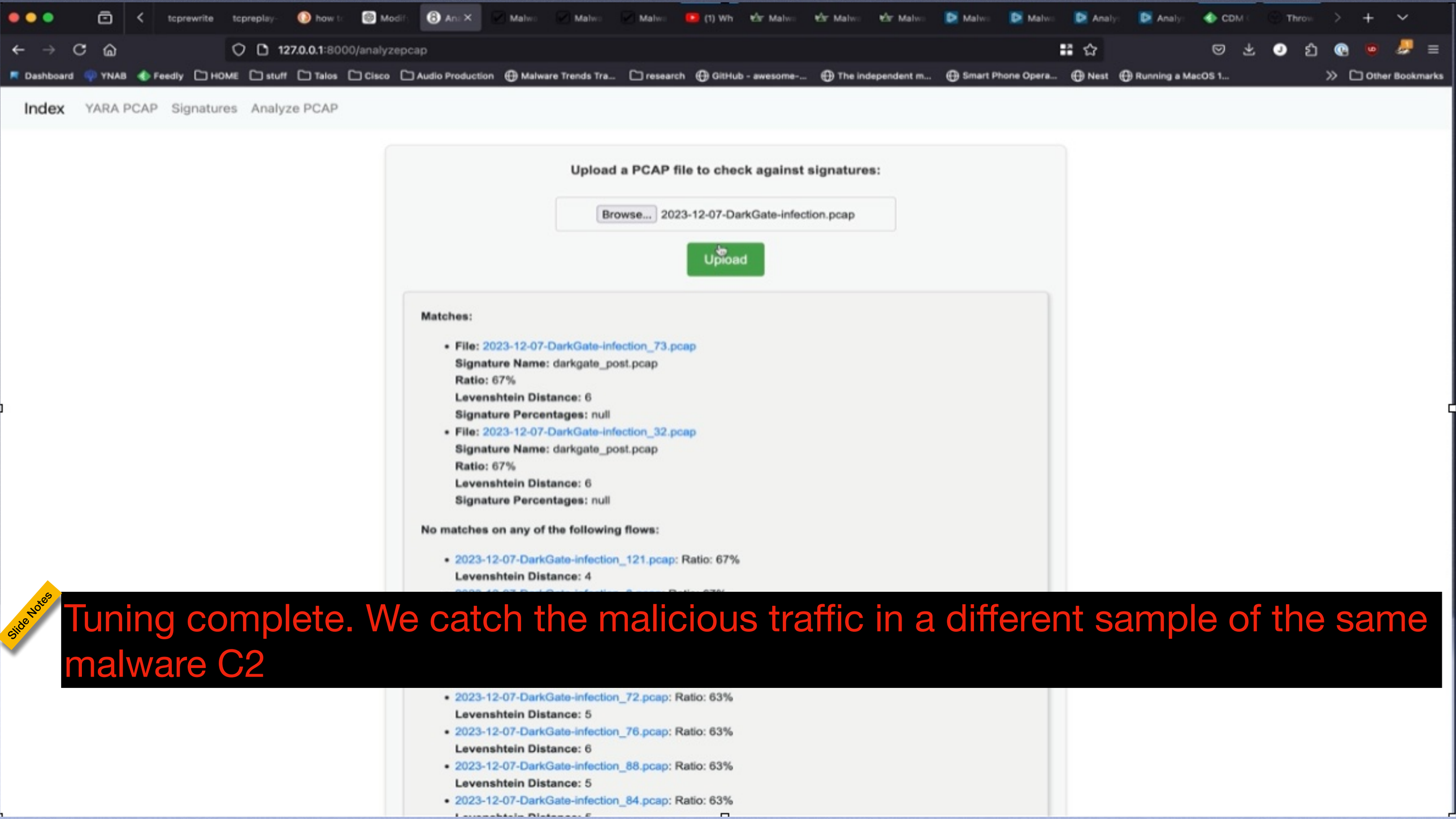
| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 10.11.30.101 | 158.160.77.234 | TCP | 66 | 50305 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2 |
| 2 | 0.176015 | 158.160.77.234 | 10.11.30.101 | TCP | 66 | 80 → 50305 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS |
| 3 | 0.176165 | 10.11.30.101 | 158.160.77.234 | TCP | 60 | 50305 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 4 | 0.176372 | 10.11.30.101 | 158.160.77.234 | HTTP | 416 | POST / HTTP/1.0 |
| 5 | 0.349008 | 158.160.77.234 | 10.11.30.101 | TCP | 60 | 80 → 50305 [ACK] Seq=1 Ack=363 Win=64128 Len=0 |
| 6 | 0.759576 | 158.160.77.234 | 10.11.30.101 | HTTP | 195 | HTTP/1.1 200 OK (text/html) |
| 7 | 0.759576 | 158.160.77.234 | 10.11.30.101 | TCP | 60 | 80 → 50305 [FIN, ACK] Seq=142 Ack=363 Win=64128 Len= |
| 8 | 0.759741 | 10.11.30.101 | 158.160.77.234 | TCP | 60 | 50305 → 80 [ACK] Seq=363 Ack=143 Win=131072 Len=0 |
| 9 | 0.759943 | 10.11.30.101 | 158.160.77.234 | TCP | 60 | 50305 → 80 [FIN, ACK] Seq=363 Ack=143 Win=131072 Len= |
| 10 | 0.964047 | 158.160.77.234 | 10.11.30.101 | TCP | 60 | 80 → 50305 [ACK] Seq=143 Ack=364 Win=64128 Len=0 |

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 10.11.30.101 | 64.190.113.222 | TCP | 66 | 50329 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 2 | 1.012402 | 10.11.30.101 | 64.190.113.222 | TCP | 66 | [TCP Retransmission] 50329 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK |
| 3 | 3.012324 | 10.11.30.101 | 64.190.113.222 | TCP | 66 | [TCP Retransmission] 50329 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK |
| 4 | 7.012146 | 10.11.30.101 | 64.190.113.222 | TCP | 66 | [TCP Retransmission] 50329 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK |
| 5 | 15.027398 | 10.11.30.101 | 64.190.113.222 | TCP | 66 | [TCP Retransmission] 50329 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK |

Slide Notes

Picking the threshold - somewhere between 64% and 67%, with a Levenshtein distance of less than 5

```
threshold = 65 # Adjust this value as needed
levenshtein_threshold = 5  # Adjust this value as needed
```


127.0.0.1:8000/analyzepcap
Index
YARA PCAP
Signatures
Analyze PCAP
Upload a PCAP file to check against signatures:
Browse...
2023-12-07-DarkGate-infection.pcap
Upload
Matches:
File: 2023-12-07-DarkGate-infection_73.pcap
Signature Name: darkgate_post.pcap
Ratio: 67%
Levenshtein Distance: 6
Signature Percentages: null
File: 2023-12-07-DarkGate-infection_32.pcap
Signature Name: darkgate_post.pcap
Ratio: 67%
Levenshtein Distance: 6
Signature Percentages: null
No matches on any of the following flows:
2023-12-07-DarkGate-infection_121.pcap: Ratio: 67%
Levenshtein Distance: 4
2023-12-07-DarkGate-infection_72.pcap: Ratio: 63%
Levenshtein Distance: 5
2023-12-07-DarkGate-infection_76.pcap: Ratio: 63%
Levenshtein Distance: 6
2023-12-07-DarkGate-infection_88.pcap: Ratio: 63%
Levenshtein Distance: 5
2023-12-07-DarkGate-infection_84.pcap: Ratio: 63%
Slide Notes
Tuning complete. We catch the malicious traffic in a different sample of the same malware C2

Slide Notes

# Tried again from a malware version that is a month older than the signature




## 2023-10-04 (WEDNESDAY) - DAKRGATE MALWARE INFECTION

NOTICE:

- Of note, the zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

ASSOCIATED FILES:

- **2023-10-04-DarkGate-IOCs.txt.zip** 1.6 kB (1,618 bytes)
- **2023-10-04-DarkGate-infection.pcap.zip** 1.3 MB (1,255,503 bytes)
- **2023-10-04-DarkGate-malware.zip** 6.1 MB (6,124,952 bytes)

Index YARA PCAP Signatures Analyze PCAP

**Upload a PCAP file to check against signatures:**

Browse... 2023-10-04-DarkGate-infection.pcap

Upload

**Matches:**

- **File:** 2023-10-04-DarkGate-infection_48.pcap
  **Signature Name:** darkgate_post.pcap
  **Ratio:** 62%
  **Levenshtein Distance:** 4
  **Signature Percentages:** null
- **File:** 2023-10-04-DarkGate-infection_25.pcap
  **Signature Name:** darkgate_post.pcap

Slide Notes

Tried again from a malware version that is a month older than the signature - found matches

**Ratio:** 62%
**Levenshtein Distance:** 4
**Signature Percentages:** null
- **File:** 2023-10-04-DarkGate-infection_188.pcap
  **Signature Name:** darkgate_post.pcap
  **Ratio:** 62%
  **Levenshtein Distance:** 4
  **Signature Percentages:** null
- **File:** 2023-10-04-DarkGate-infection_44.pcap
  **Signature Name:** darkgate_post.pcap
  **Ratio:** 62%
  **Levenshtein Distance:** 4
  **Signature Percentages:** null
- **File:** 2023-10-04-DarkGate-infection_9.pcap
  **Signature Name:** darkgate_post.pcap
  **Ratio:** 62%

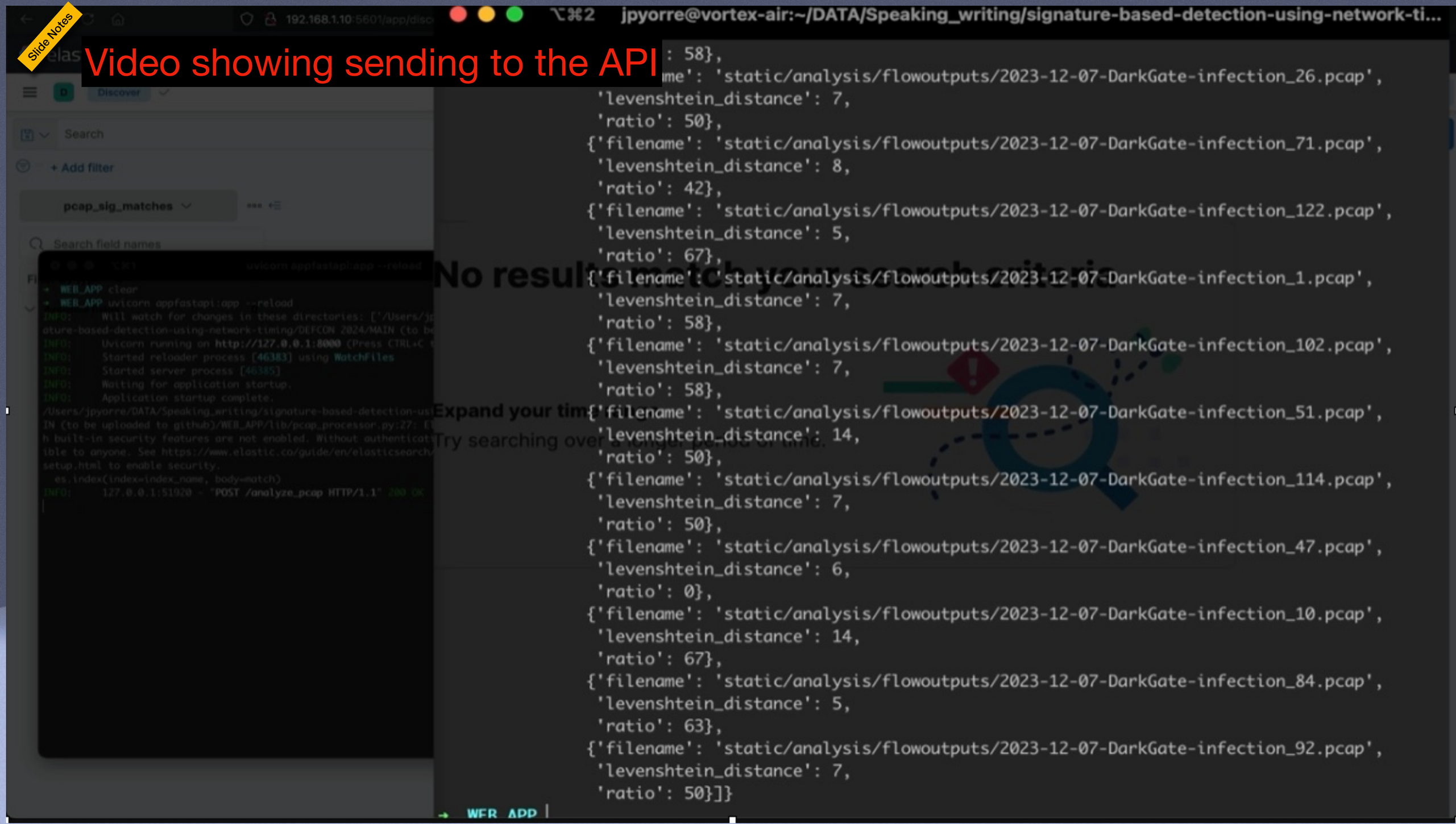
Slide Notes

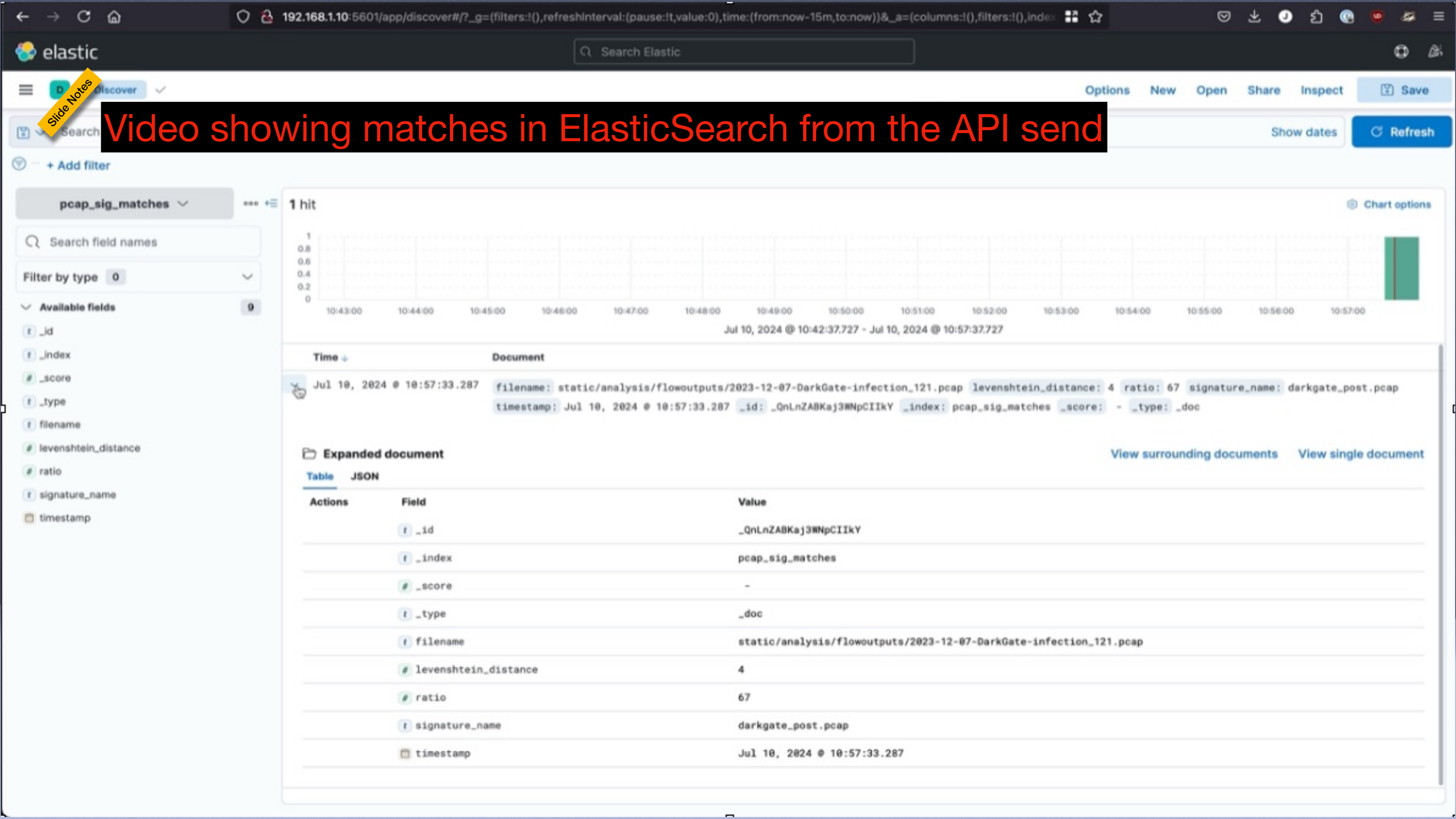
Web app is cool, but can we run it on streaming network traffic?

# API & SIEM

Slide Notes

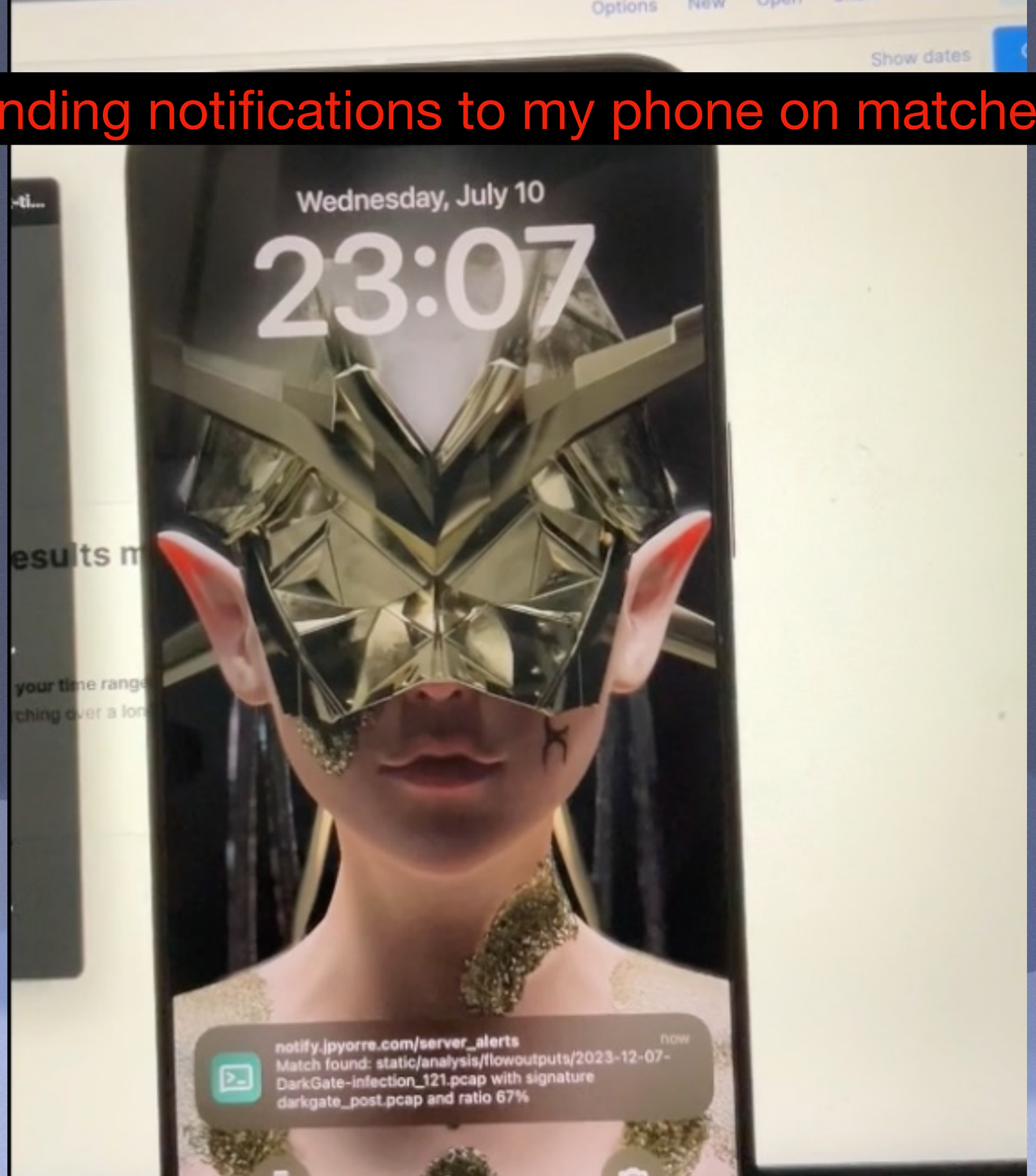
# Video showing sending to the API




192.168.1.10:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(),filters:!(),index
elastic
Search Elastic
Discover
Options
New
Open
Share
Inspect
Save
Slide Notes
Video showing matches in ElasticSearch from the API send
Search
Show dates
Refresh
+ Add filter
pcap_sig_matches
Search field names
Filter by type 0
Available fields 9
_id
_index
_score
_type
filename
levenshtein_distance
ratio
signature_name
timestamp
1 hit
Chart options
1
0.8
0.6
0.4
0.2
0
10:43:00
10:44:00
10:45:00
10:46:00
10:47:00
10:48:00
10:49:00
10:50:00
10:51:00
10:52:00
10:53:00
10:54:00
10:55:00
10:56:00
10:57:00
Jul 10, 2024 @ 10:42:37.727 - Jul 10, 2024 @ 10:57:37.727
Time
Document
Jul 10, 2024 @ 10:57:33.287
filename: static/analysis/flowoutputs/2023-12-07-DarkGate-infection_121.pcap levenshtein_distance: 4 ratio: 67 signature_name: darkgate_post.pcap
timestamp: Jul 10, 2024 @ 10:57:33.287 _id: _QnLnZABKaj3WNpCIIkY _index: pcap_sig_matches _score: - _type: _doc
Expanded document
View surrounding documents
View single document
Table
JSON
Actions
Field
Value
_id
_QnLnZABKaj3WNpCIIkY
_index
pcap_sig_matches
_score
-
_type
_doc
filename
static/analysis/flowoutputs/2023-12-07-DarkGate-infection_121.pcap
levenshtein_distance
4
ratio
67
signature_name
darkgate_post.pcap
timestamp
Jul 10, 2024 @ 10:57:33.287

Slide Notes

# Video showing sending notifications to my phone on matches



Slide Notes

I’m also a musician, so let’s do something non-practical related to music

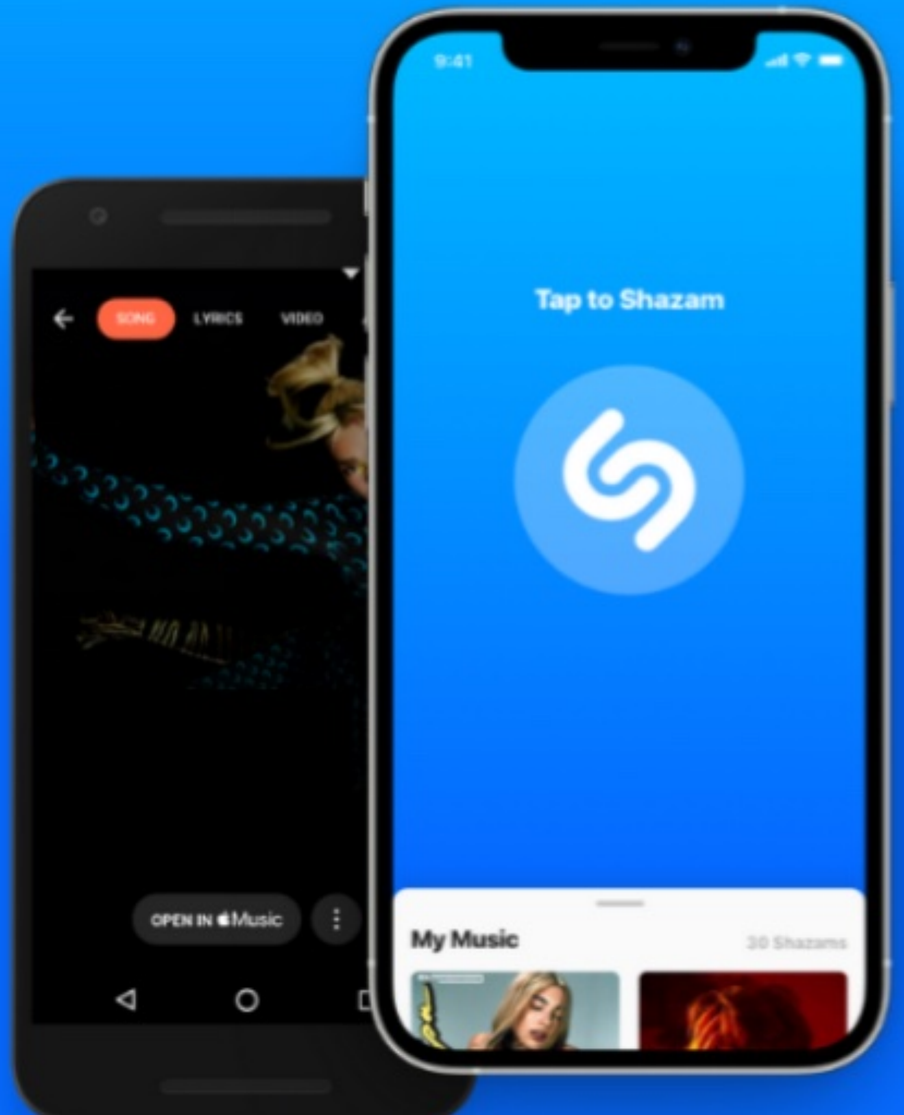


# Art is how we decorate space, music is how we decorate time.

—Jean-Michel Basquiat

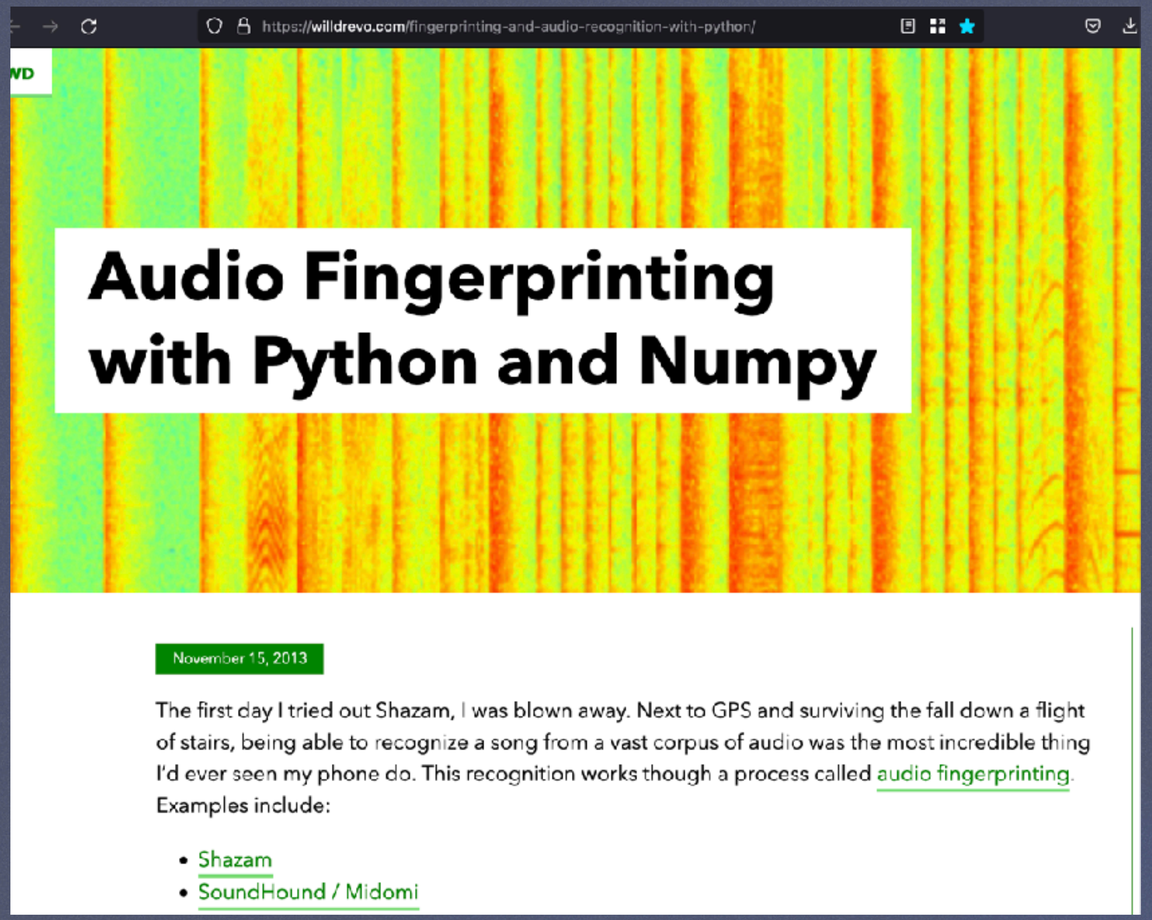
Slide Notes

# Can we “shazam” malware traffic?

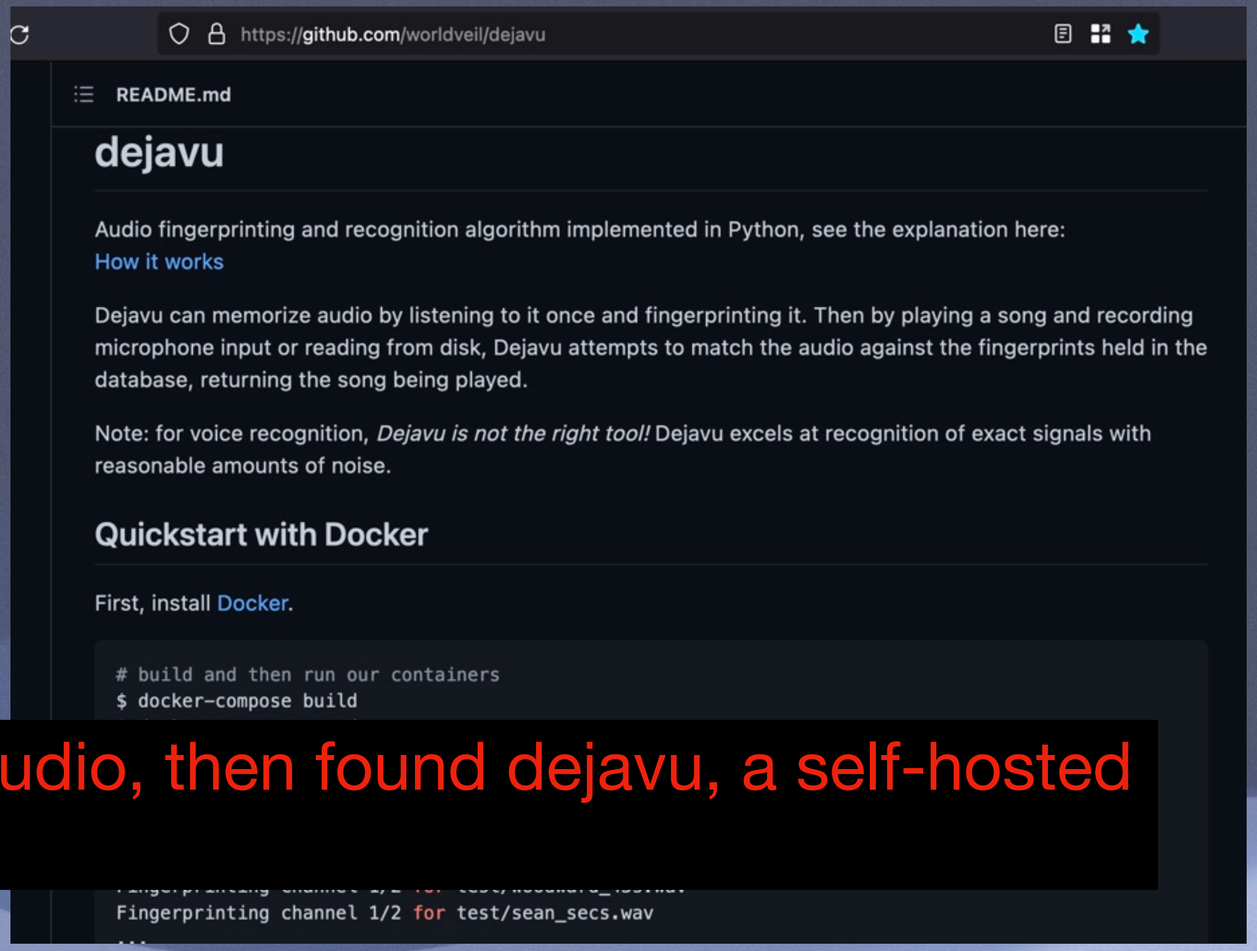



## Name songs in seconds

Find music, concerts and more with Shazam




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



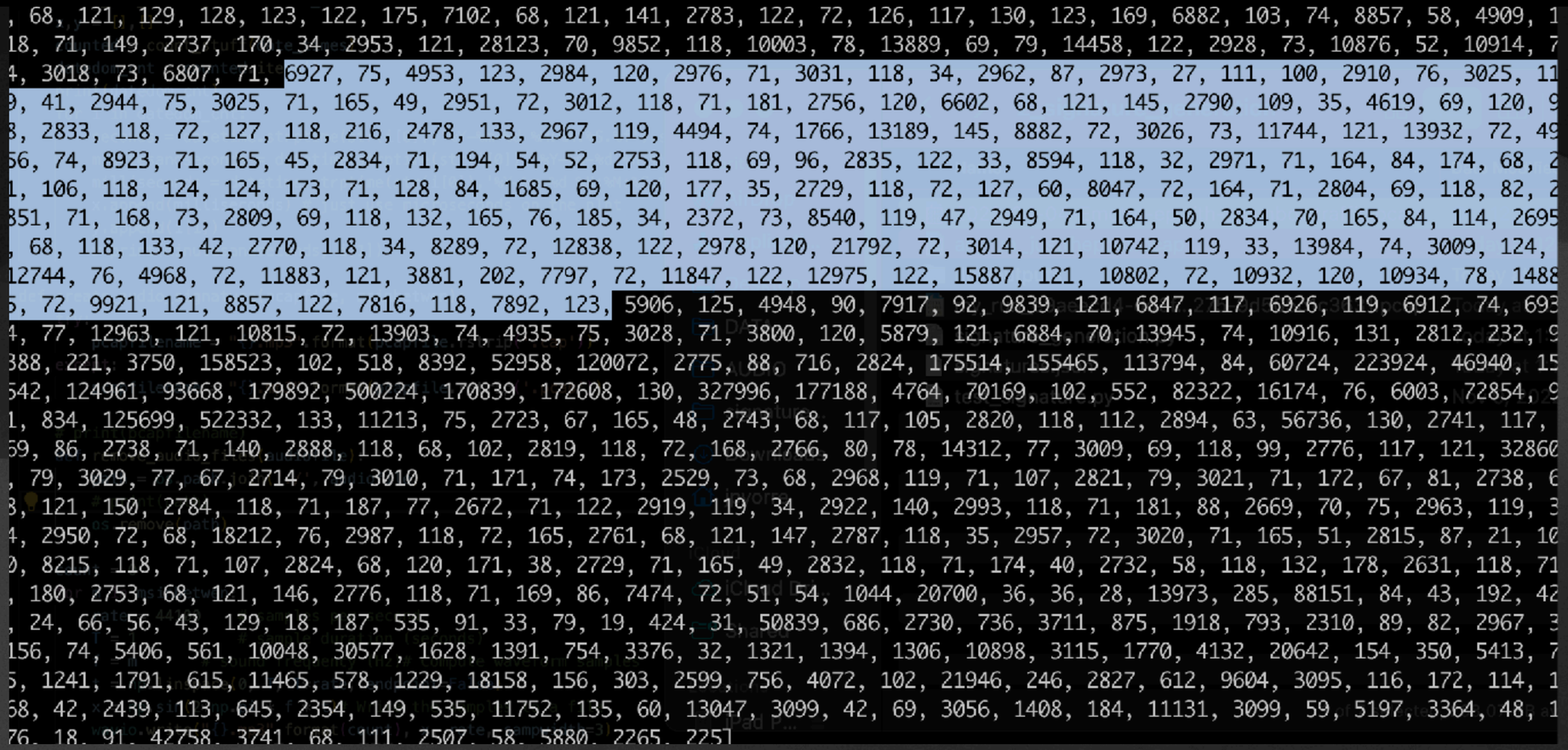

https://github.com/worldveil/dejavu

Slide Notes

Found articles about fingerprinting audio, then found dejavu, a self-hosted Shazam-like platform

Slide Notes

# Take those transactions times and treat them like frequency, or musical pitch.
# High numbers == high sound
# Low numbers == low sound




**wavio 0.0.4**

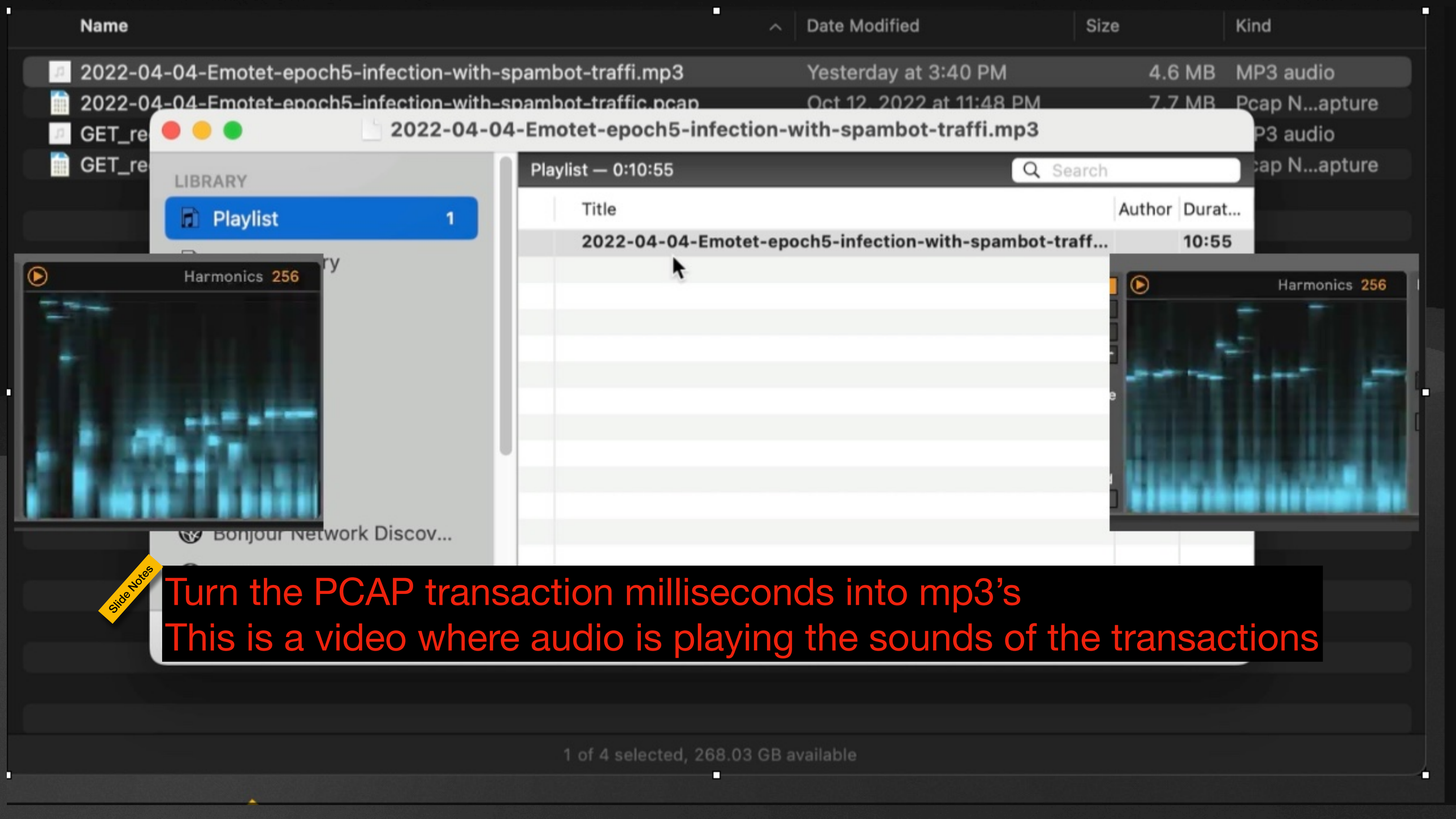
```
pip install wavio
```

https://github.com/WarrenWeckesser/wavio

**pydub 0.25.1**

```
pip install pydub
```

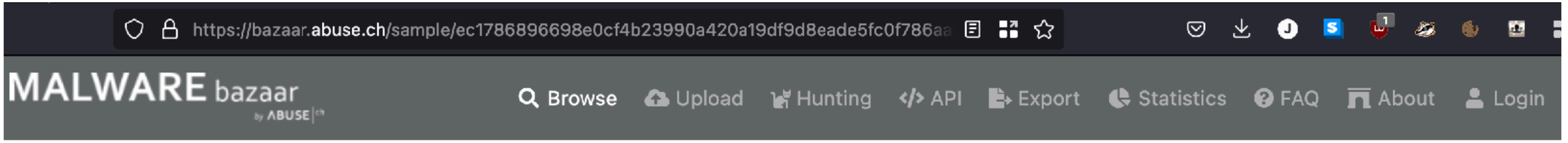
http://pydub.com/


Name
Date Modified
Size
Kind
2022-04-04-Emotet-epoch5-infection-with-spambot-traffi.mp3
Yesterday at 3:40 PM
4.6 MB
MP3 audio
2022-04-04-Emotet-epoch5-infection-with-spambot-traffic.pcap
Oct 12, 2022 at 11:48 PM
7.7 MB
Pcap N...apture
GET_re
P3 audio
GET_re
ap N...apture
2022-04-04-Emotet-epoch5-infection-with-spambot-traffi.mp3
LIBRARY
Playlist
1
Playlist — 0:10:55
Search
Title
Author
Durat...
2022-04-04-Emotet-epoch5-infection-with-spambot-traff...
10:55
Harmonics 256
Harmonics 256
Bonjour Network Discov...
Slide Notes
Turn the PCAP transaction milliseconds into mp3's
This is a video where audio is playing the sounds of the transactions
1 of 4 selected, 268.03 GB available

Slide Notes

Try running this process using the same malware, but from different environments (to answer the question: Does bandwidth or network latency affect detection?

# Same Malware Sample/ Different Environments




Slide Notes

Browse / Malware sample

I went on malwarebazaar and found a copy of Agent Tesla (it's old….sorry)

# 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

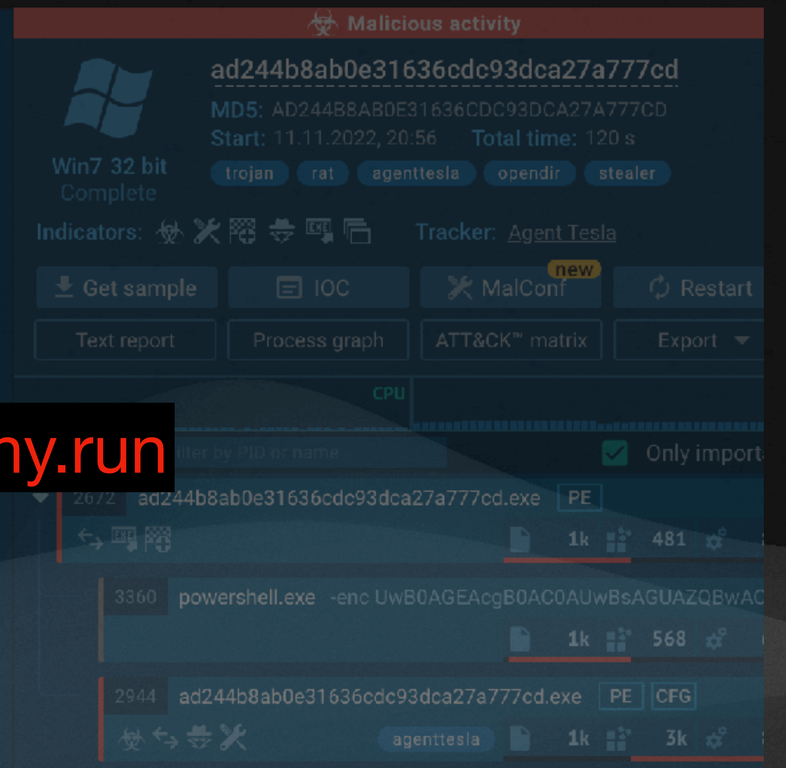
Vendor detections: **17**

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

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

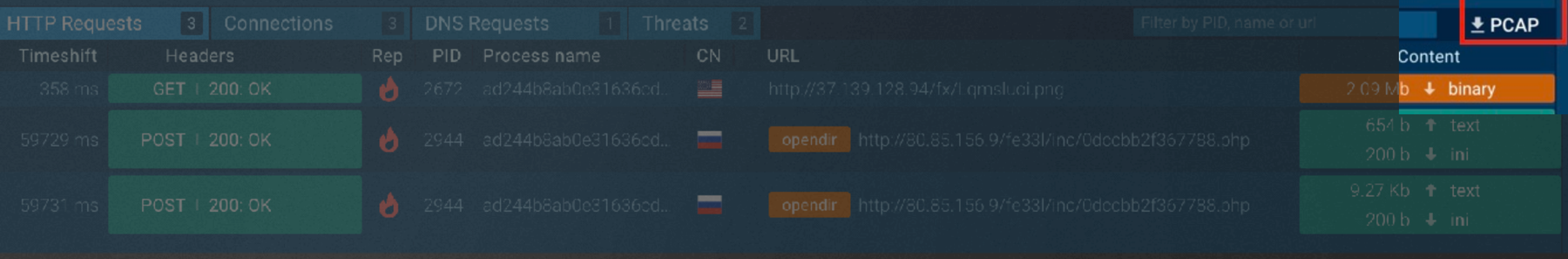
Slide Notes

# and then I found that someone had already run it on any.run





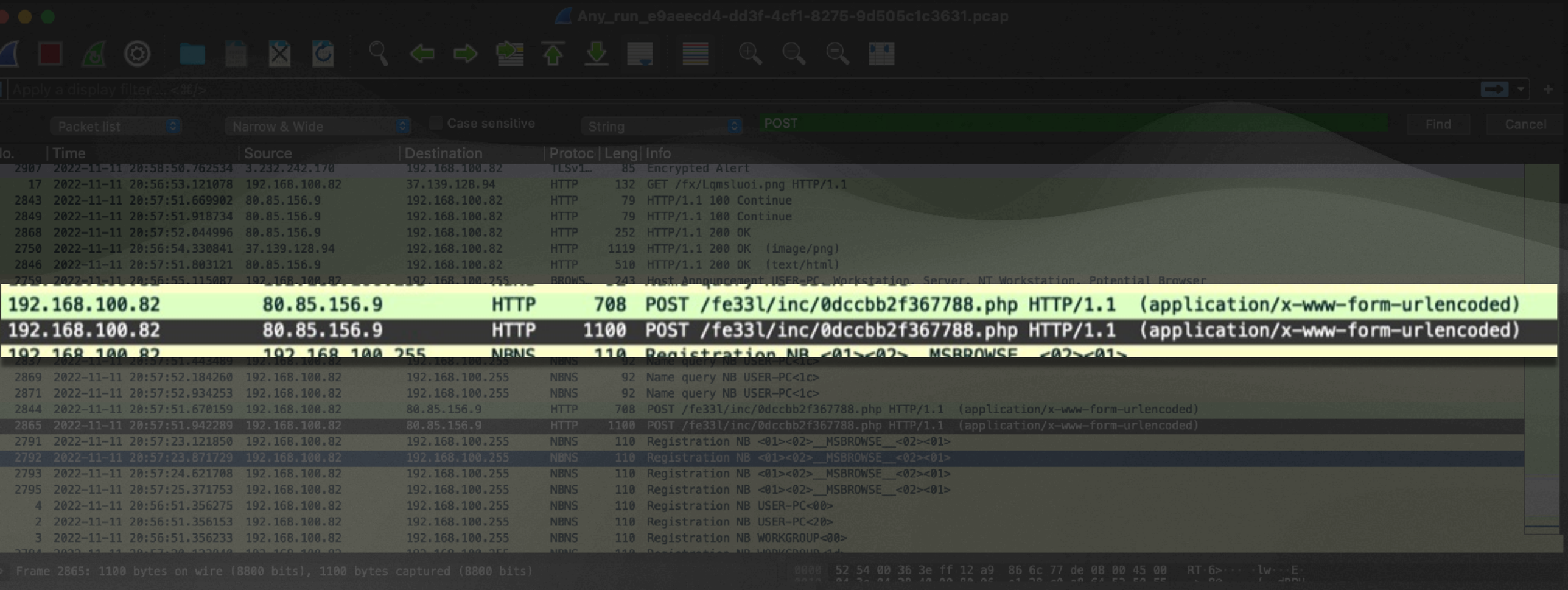





https://bazaar.abuse.ch/sample/ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f/ → https://app.any.run/tasks/e9aeecd4-dd3f-4cf1-8275-9d505c1c3631/#

# any.run: 192.168.100.82 -> 80.85.156.9

POST /fe33l/inc/0dccbb2f367788.php



Slide Notes

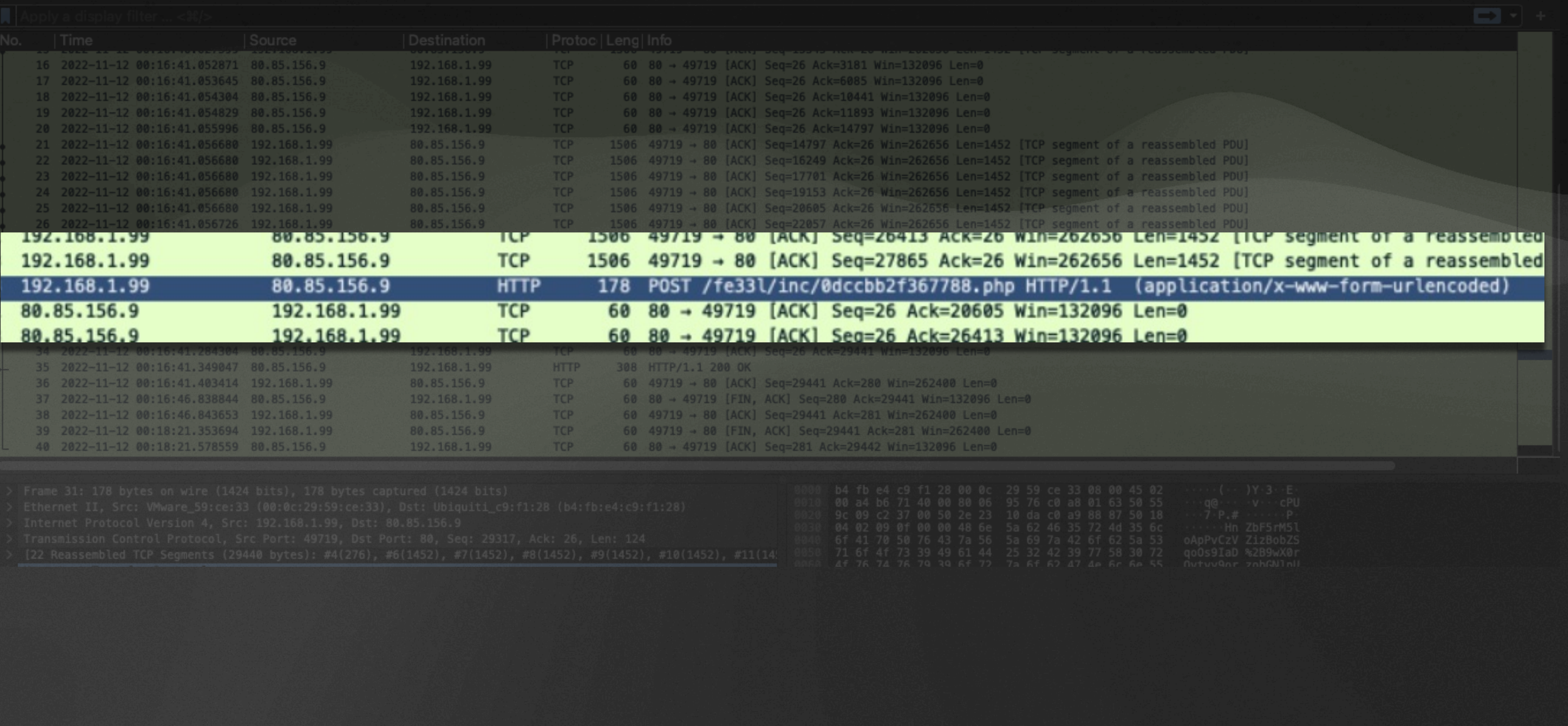
Also ran it on my own malware analysis system




# Run on My System

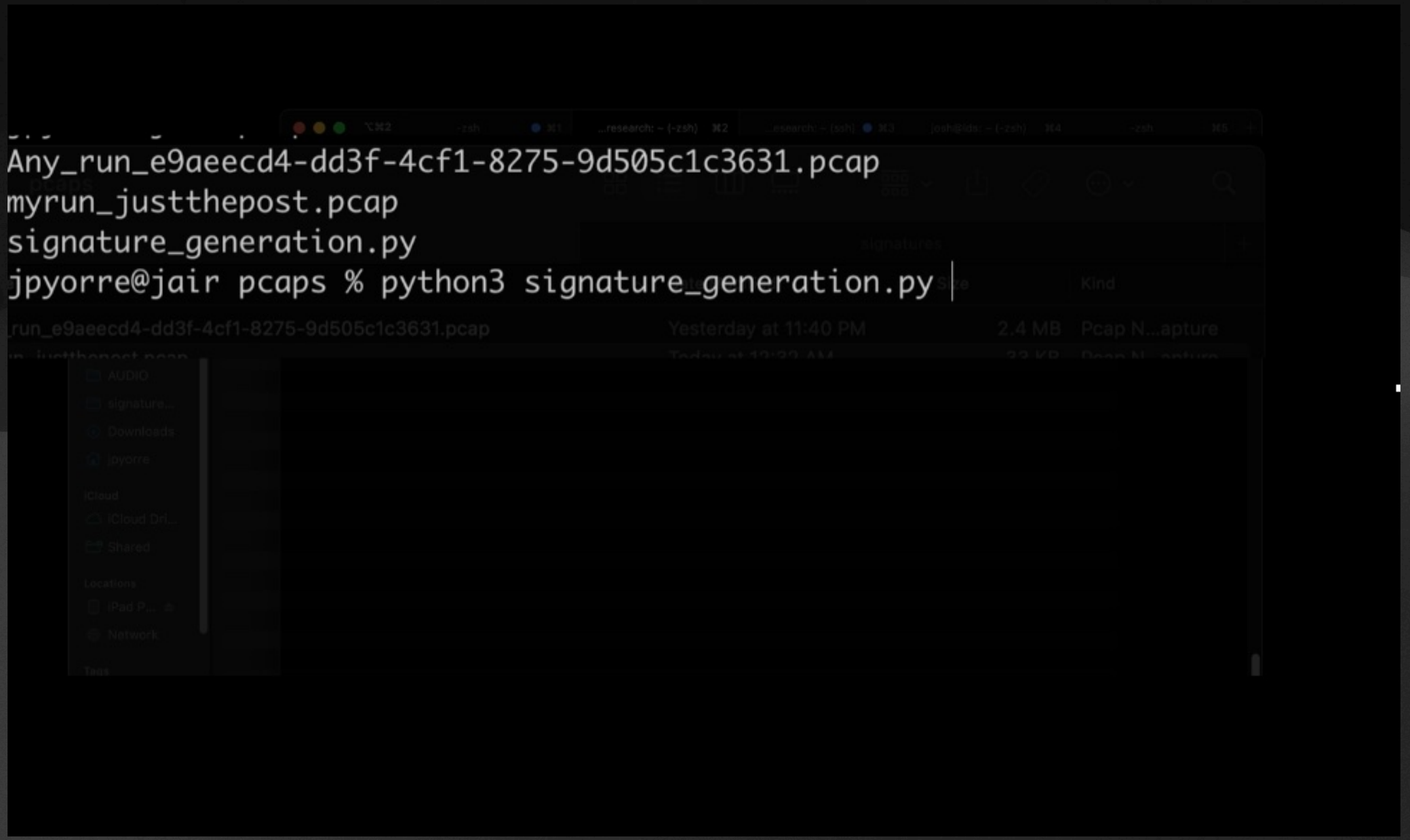
# Me: 192.168.1.99 -> 80.85.156.9

POST /fe33l/inc/0dccbb2f367788.php

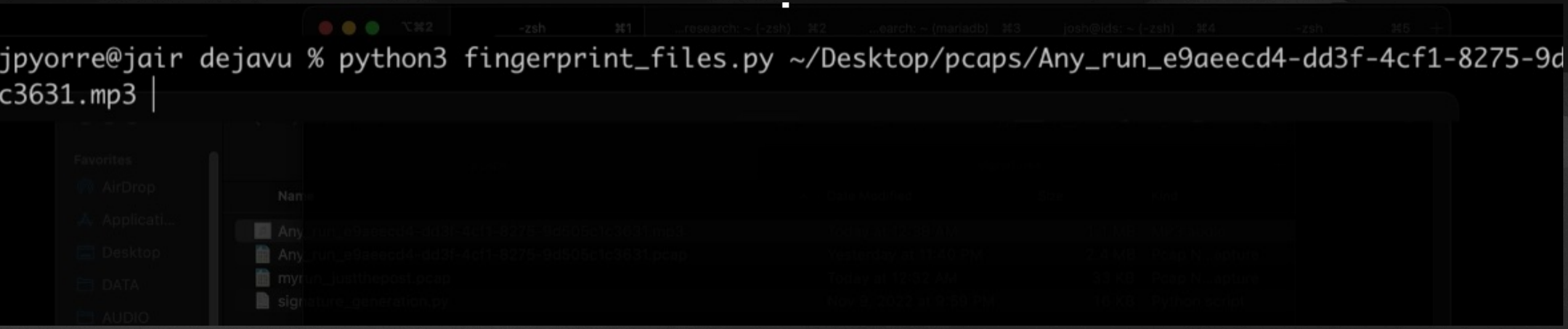


# Shazam it!

# Create an audio file from the any.run PCAP



# Create a Fingerprint from the any.run PCAP (now audio)



# Create an audio file from my PCAP

```
jpyorre@jair pcaps % ls
Any_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631.mp3
Any_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631.pcap
myrun_justthepost.pcap
signature_generation.py
```

# 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': 0.00121426582336425 78, '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'}]}
```

Slide Notes

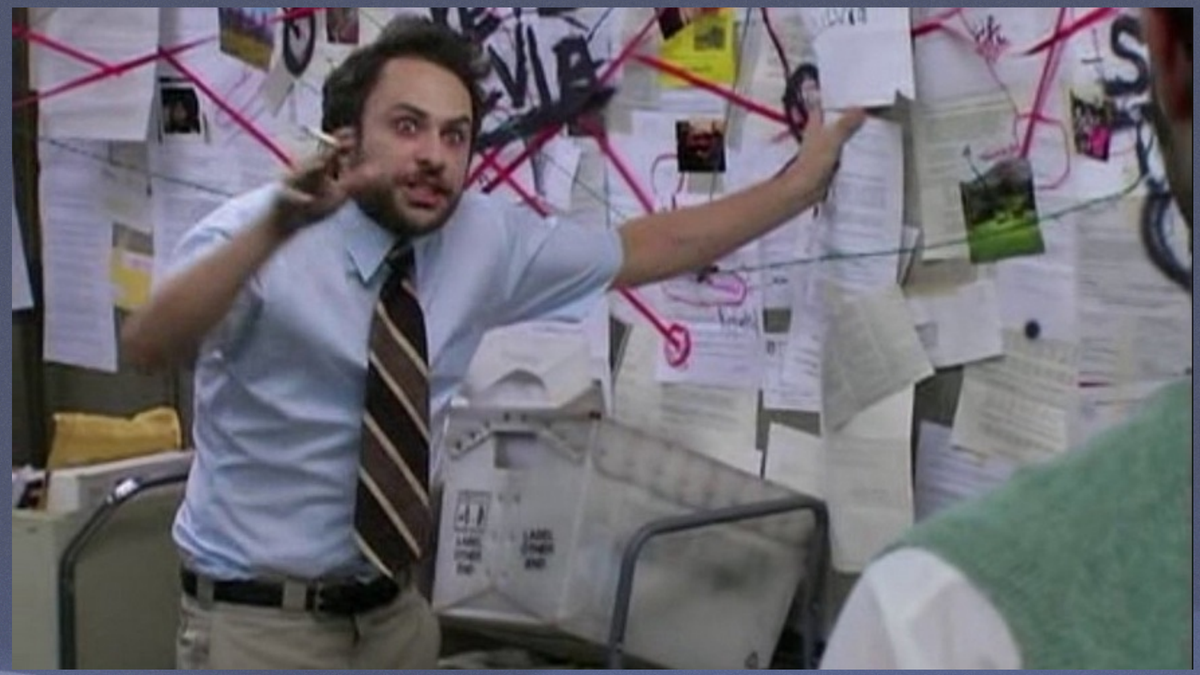
Video of the process

# Going Further

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



# Code



https://github.com/jpyorre/transaction_time_networksignatures

Website:
https://pyosec.com

Twitter (meh):
@joshpyorre

Mastodon (I don't even have the app installed):
@joshpyorre@infosec.exchange