# 100 Security Tools - more or less

## Tools you use every day, or at least you should be!

by Josh Galvez - aka Zevlag

# Josh Galvez

## zevlag

- Offensive Security Operator at LogMeIn
- In the Security industry for 15 years
- DEFCON 25 Black Badge
- DEFCON 29 Black Badge
- SAINTCON 2014 Black Badge



Network
digitalblasphemy.com

# Nmap

## Network Mapper

```
[zevlag@Z314 ~ % nmap -v -A webplay.hackerschallenge.org                                ]
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-20 22:59 MDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:59
Completed NSE at 22:59, 0.00s elapsed
Initiating NSE at 22:59
Completed NSE at 22:59, 0.00s elapsed
Initiating NSE at 22:59
Completed NSE at 22:59, 0.00s elapsed
Initiating Ping Scan at 22:59
Scanning webplay.hackerschallenge.org (54.212.225.228) [2 ports]
Completed Ping Scan at 22:59, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:59
Completed Parallel DNS resolution of 1 host. at 22:59, 0.17s elapsed
Initiating Connect Scan at 22:59
Scanning webplay.hackerschallenge.org (54.212.225.228) [1000 ports]
Discovered open port 22/tcp on 54.212.225.228
Completed Connect Scan at 23:00, 9.22s elapsed (1000 total ports)
Initiating Service scan at 23:00
Scanning 1 service on webplay.hackerschallenge.org (54.212.225.228)
Completed Service scan at 23:00, 0.11s elapsed (1 service on 1 host)
NSE: Script scanning 54.212.225.228.
Initiating NSE at 23:00
Completed NSE at 23:00, 1.22s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Nmap scan report for webplay.hackerschallenge.org (54.212.225.228)
Host is up (0.041s latency).
rDNS record for 54.212.225.228: ec2-54-212-225-228.us-west-2.compute.amazonaws.com
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE    SERVICE      VERSION
22/tcp  open     ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 2b:39:30:00:08:64:5d:8a:2a:4f:07:7f:ae:f0:89:c9 (RSA)
|   256 f3:42:d3:d8:fd:d5:6c:91:a6:e5:5f:1e:19:96:e8:58 (ECDSA)
|_  256 c0:98:c1:81:c0:62:86:a4:42:d7:24:91:d5:24:e5:b1 (ED25519)
25/tcp  filtered smtp
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
587/tcp filtered submission
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
```

# Nmap

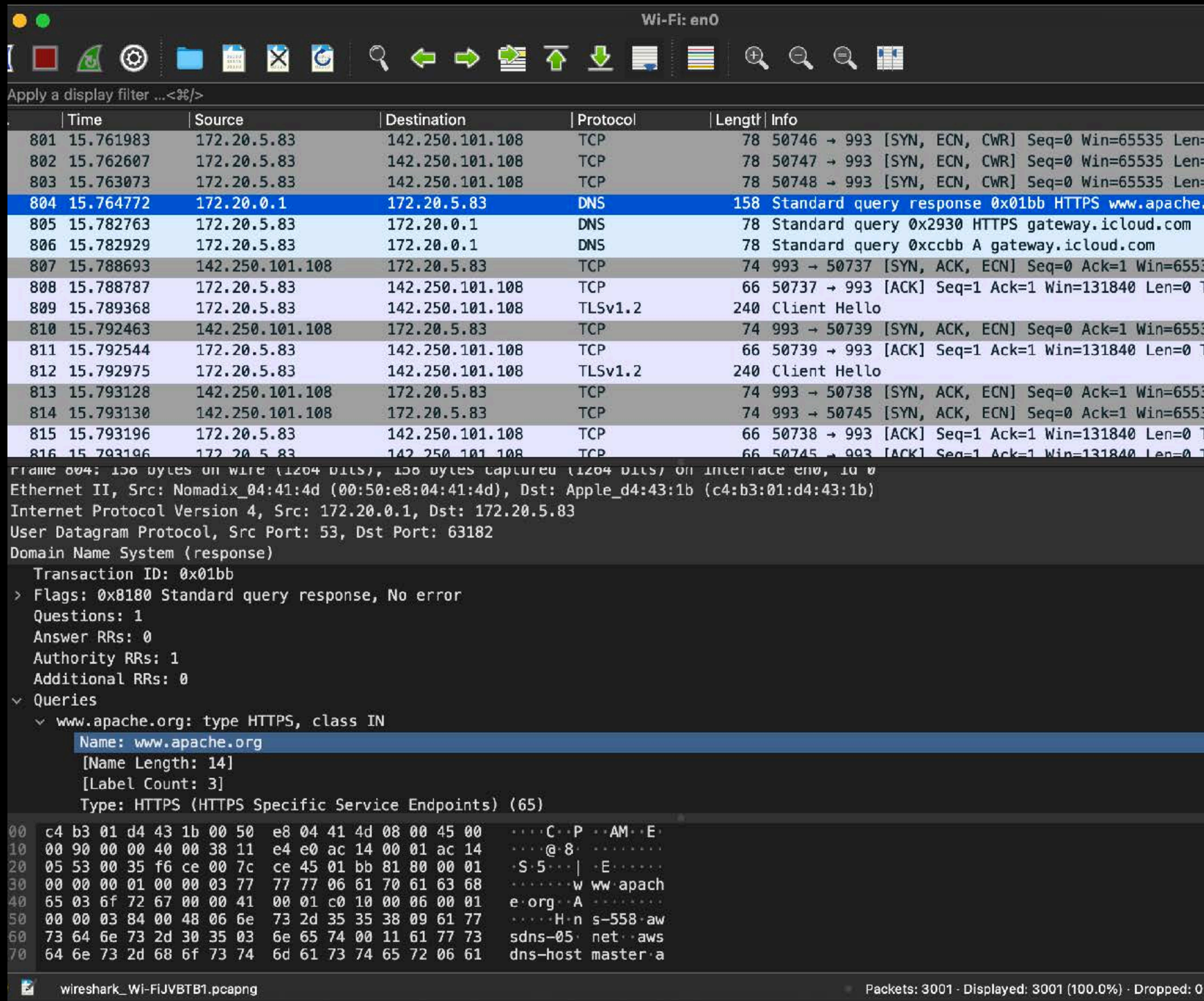
Scan for active IP's:
nmap -sn 192.168.0.0/24

Scan for Operating Systems:
nmap -O 192.168.0.164

Scan it all, and do it fast:
nmap -T4 -A 192.168.0.0/24

Be More Verbose:
nmap -v

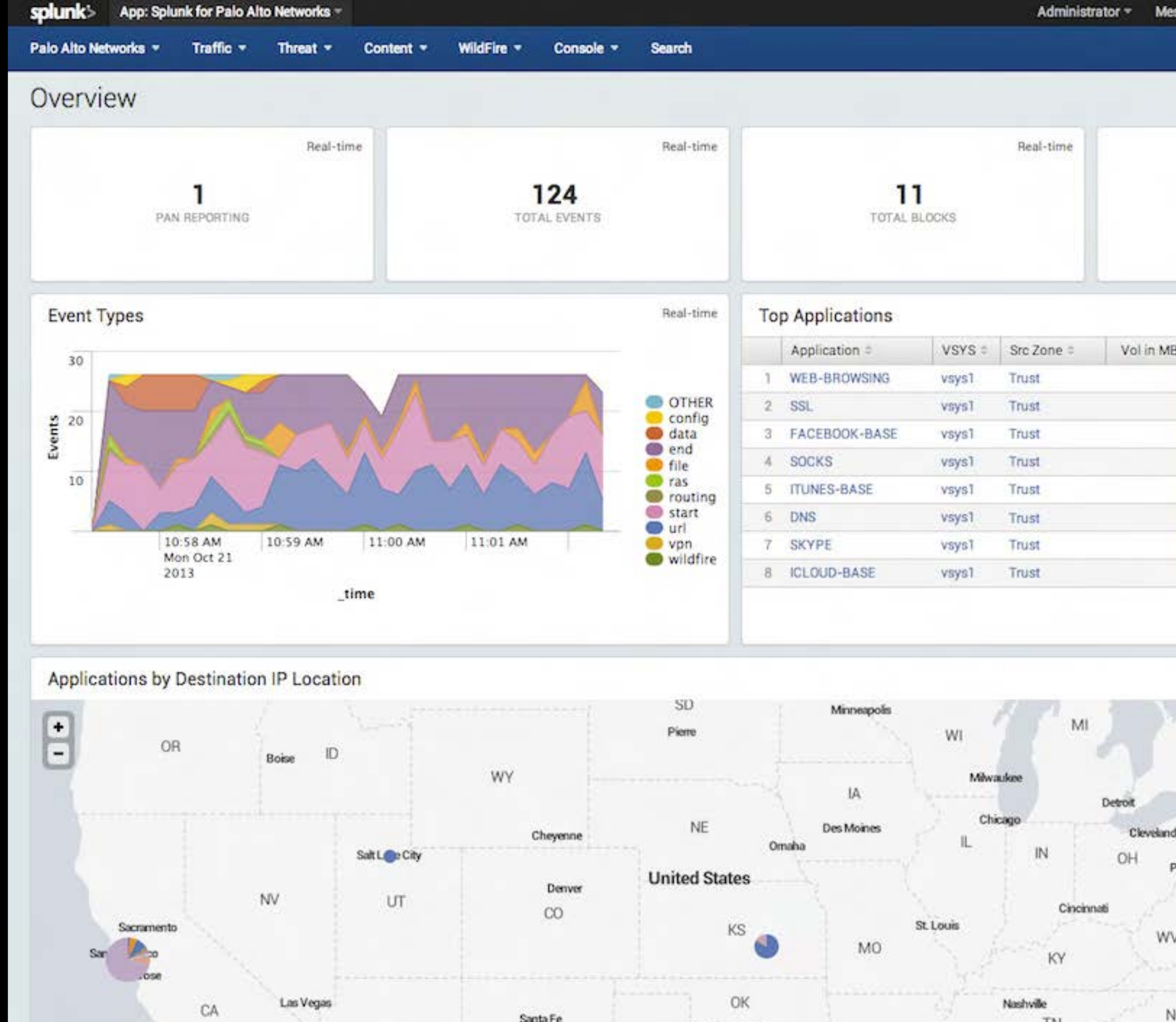
# Wireshark


Wi-Fi: en0
Apply a display filter ...<⌘/>
No. Time Source Destination Protocol Length Info
801 15.761983 172.20.5.83 142.250.101.108 TCP 78 50746 → 993 [SYN, ECN, CWR] Seq=0 Win=65535 Len=
802 15.762607 172.20.5.83 142.250.101.108 TCP 78 50747 → 993 [SYN, ECN, CWR] Seq=0 Win=65535 Len=
803 15.763073 172.20.5.83 142.250.101.108 TCP 78 50748 → 993 [SYN, ECN, CWR] Seq=0 Win=65535 Len=
804 15.764772 172.20.0.1 172.20.5.83 DNS 158 Standard query response 0x01bb HTTPS www.apache.
805 15.782763 172.20.5.83 172.20.0.1 DNS 78 Standard query 0x2930 HTTPS gateway.icloud.com
806 15.782929 172.20.5.83 172.20.0.1 DNS 78 Standard query 0xccbb A gateway.icloud.com
807 15.788693 142.250.101.108 172.20.5.83 TCP 74 993 → 50737 [SYN, ACK, ECN] Seq=0 Ack=1 Win=655
808 15.788787 172.20.5.83 142.250.101.108 TCP 66 50737 → 993 [ACK] Seq=1 Ack=1 Win=131840 Len=0
809 15.789368 172.20.5.83 142.250.101.108 TLSv1.2 240 Client Hello
810 15.792463 142.250.101.108 172.20.5.83 TCP 74 993 → 50739 [SYN, ACK, ECN] Seq=0 Ack=1 Win=655
811 15.792544 172.20.5.83 142.250.101.108 TCP 66 50739 → 993 [ACK] Seq=1 Ack=1 Win=131840 Len=0
812 15.792975 172.20.5.83 142.250.101.108 TLSv1.2 240 Client Hello
813 15.793128 142.250.101.108 172.20.5.83 TCP 74 993 → 50738 [SYN, ACK, ECN] Seq=0 Ack=1 Win=655
814 15.793130 142.250.101.108 172.20.5.83 TCP 74 993 → 50745 [SYN, ACK, ECN] Seq=0 Ack=1 Win=655
815 15.793196 172.20.5.83 142.250.101.108 TCP 66 50738 → 993 [ACK] Seq=1 Ack=1 Win=131840 Len=0
Ethernet II, Src: Nomadix_04:41:4d (00:50:e8:04:41:4d), Dst: Apple_d4:43:1b (c4:b3:01:d4:43:1b)
Internet Protocol Version 4, Src: 172.20.0.1, Dst: 172.20.5.83
User Datagram Protocol, Src Port: 53, Dst Port: 63182
Domain Name System (response)
Transaction ID: 0x01bb
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
www.apache.org: type HTTPS, class IN
Name: www.apache.org
[Name Length: 14]
[Label Count: 3]
Type: HTTPS (HTTPS Specific Service Endpoints) (65)
c4 b3 01 d4 43 1b 00 50 e8 04 41 4d 08 00 45 00
00 90 00 00 40 00 38 11 e4 e0 ac 14 00 01 ac 14
05 53 00 35 f6 ce 00 7c ce 45 01 bb 81 80 00 01
00 00 00 01 00 00 03 77 77 77 06 61 70 61 63 68
65 03 6f 72 67 00 00 41 00 01 c0 10 00 06 00 01
00 00 03 84 00 48 06 6e 73 2d 35 35 38 09 61 77
73 64 6e 73 2d 30 35 03 6e 65 74 00 11 61 77 73
64 6e 73 2d 68 6f 73 74 6d 61 73 74 65 72 06 61
wireshark_Wi-FiJVBTB1.pcapng
Packets: 3001 · Displayed: 3001 (100.0%) · Dropped: 0


Defensive
digitalblasphemy.com

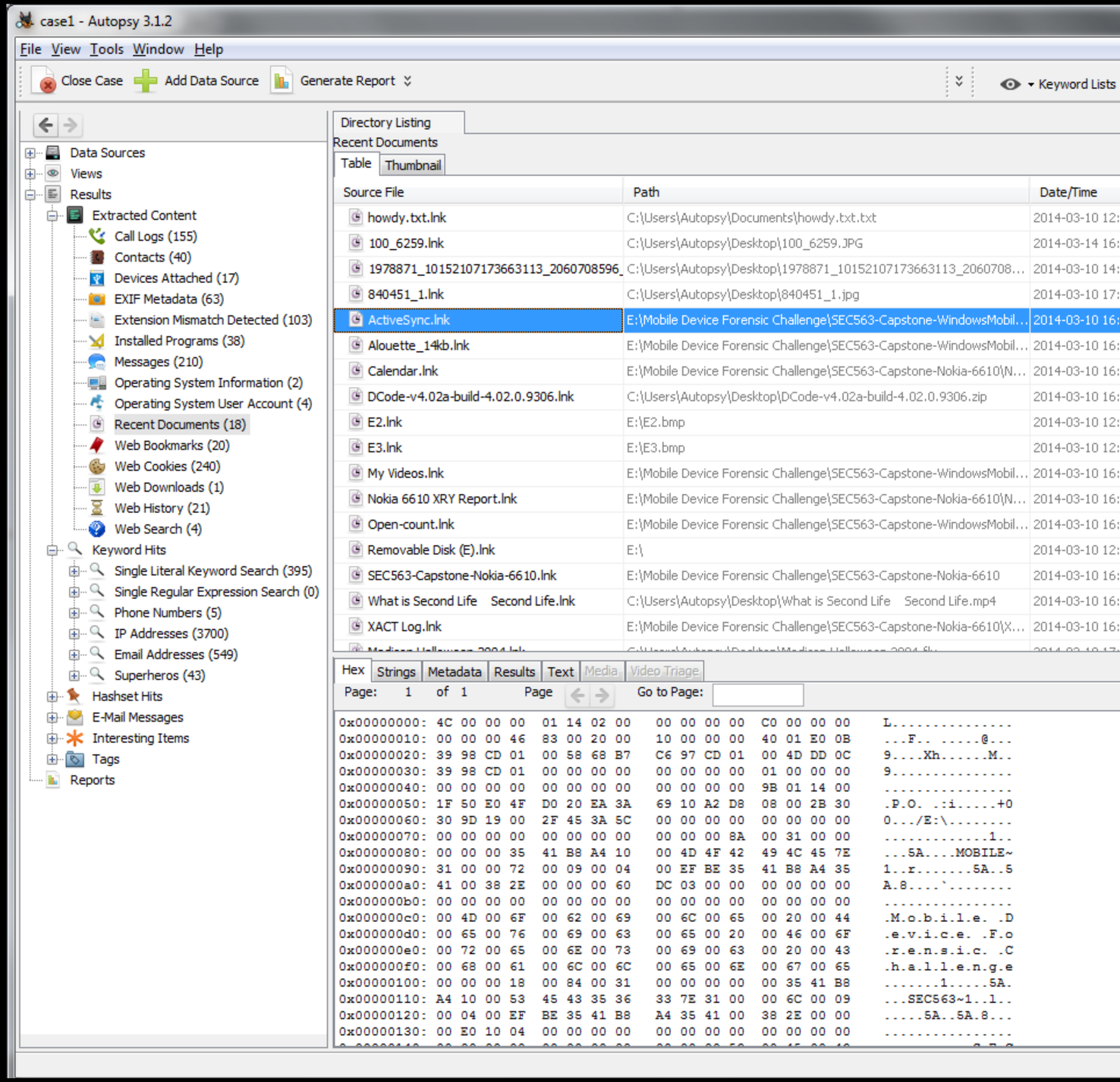
# Splunk

## Centralized Logging



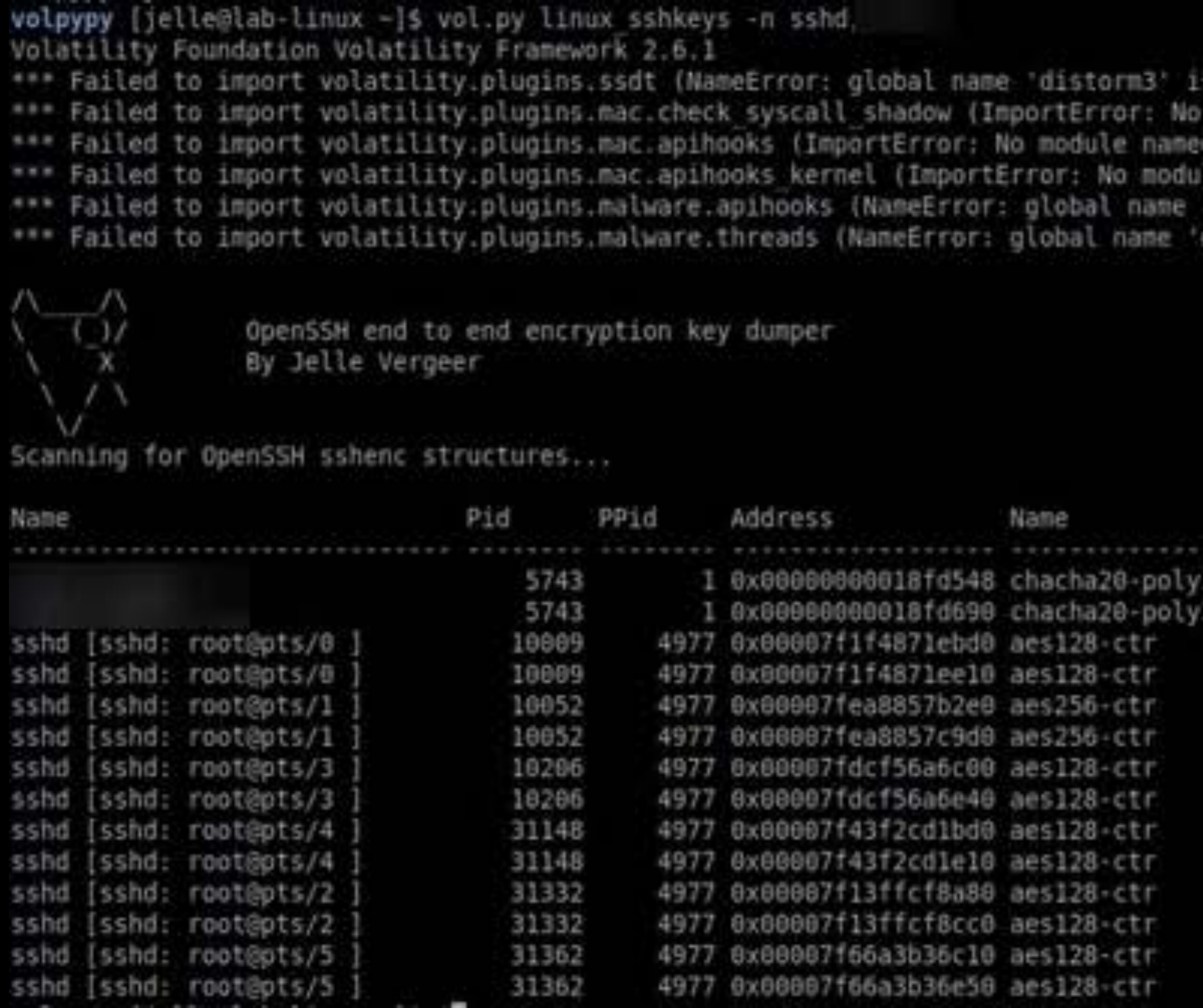
# Autopsy

## Digital forensics platform



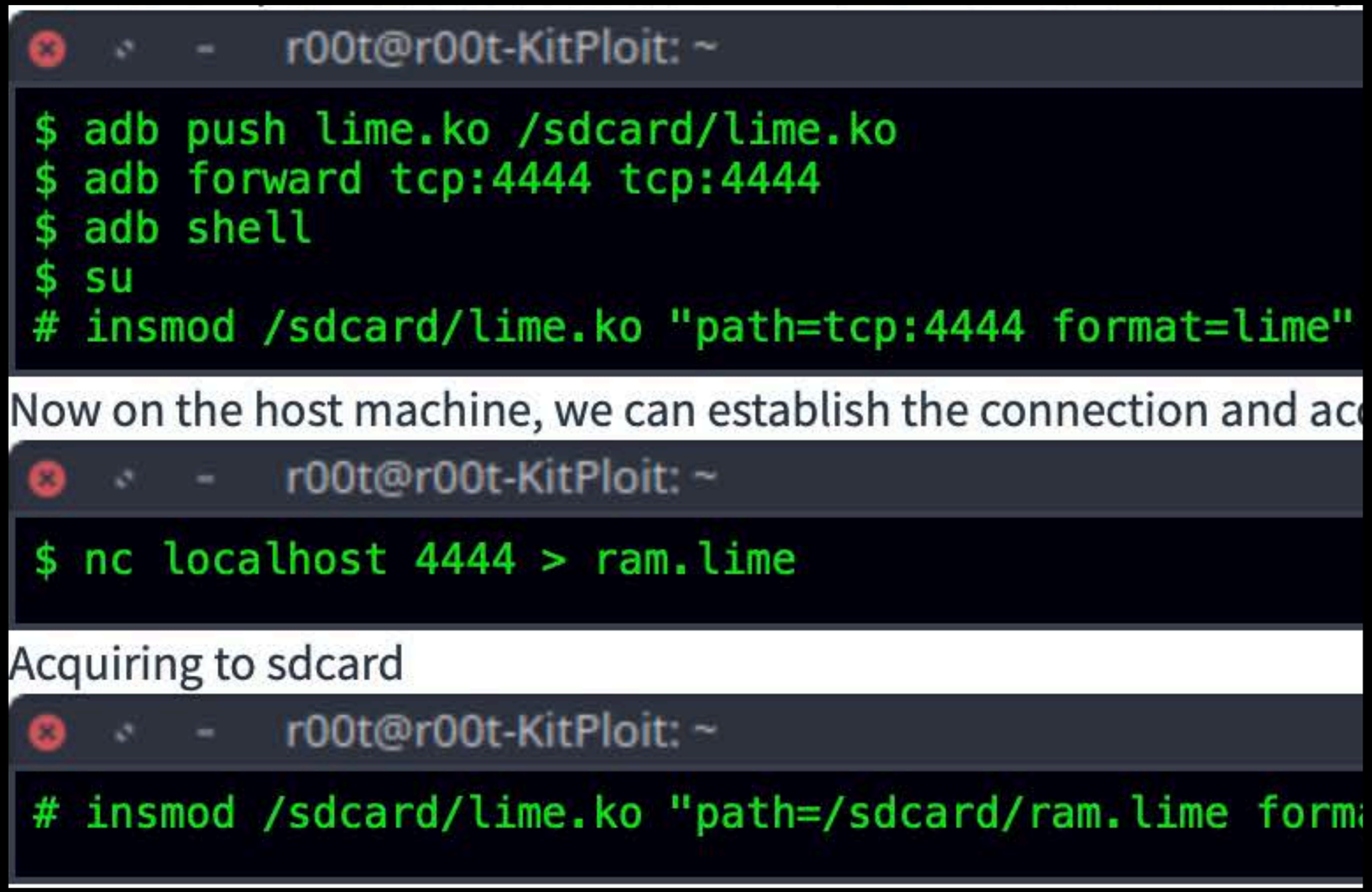
# Volatility

## Memory Forensics



# LiME

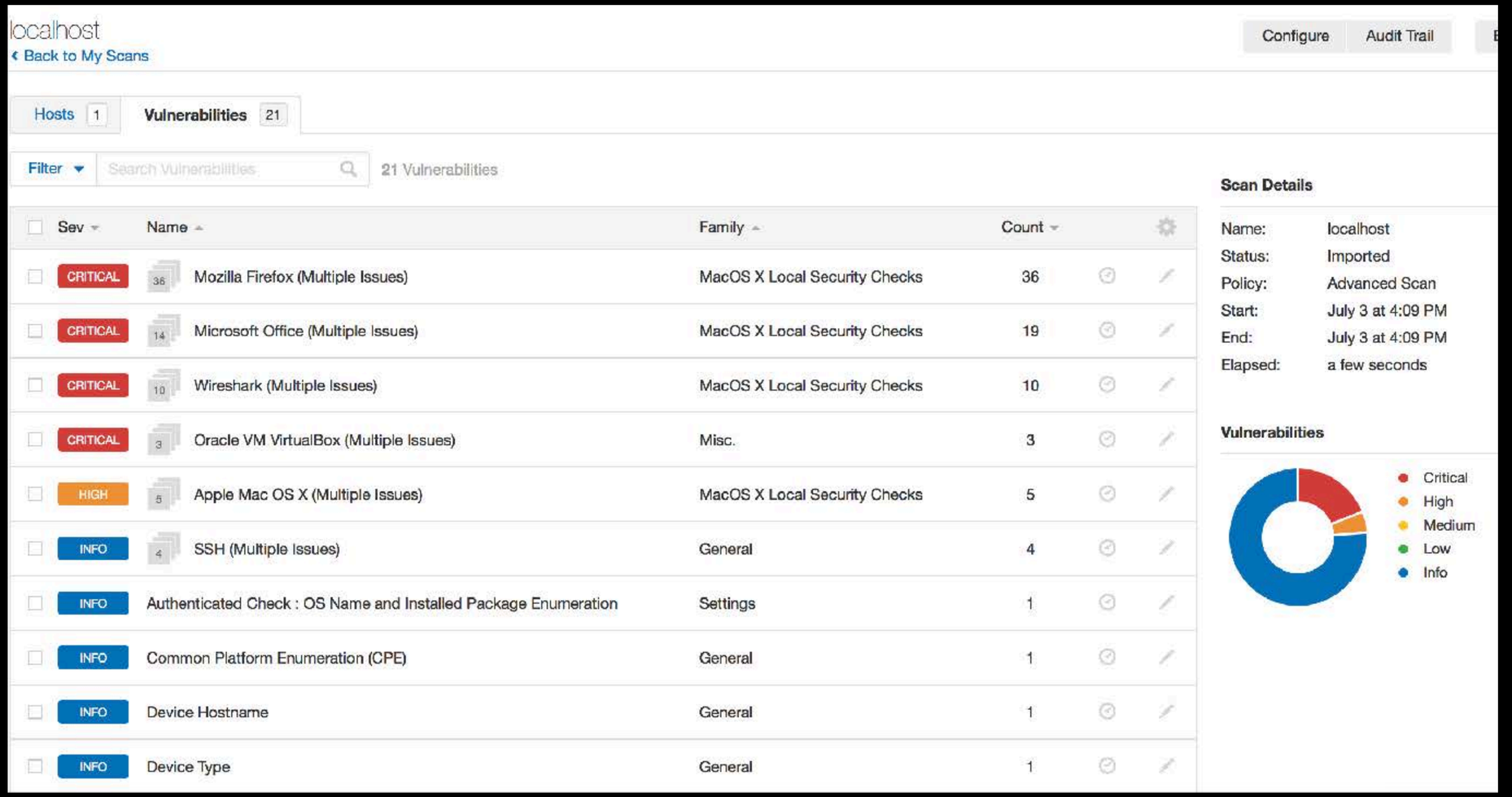
## Linux Memory Extractor



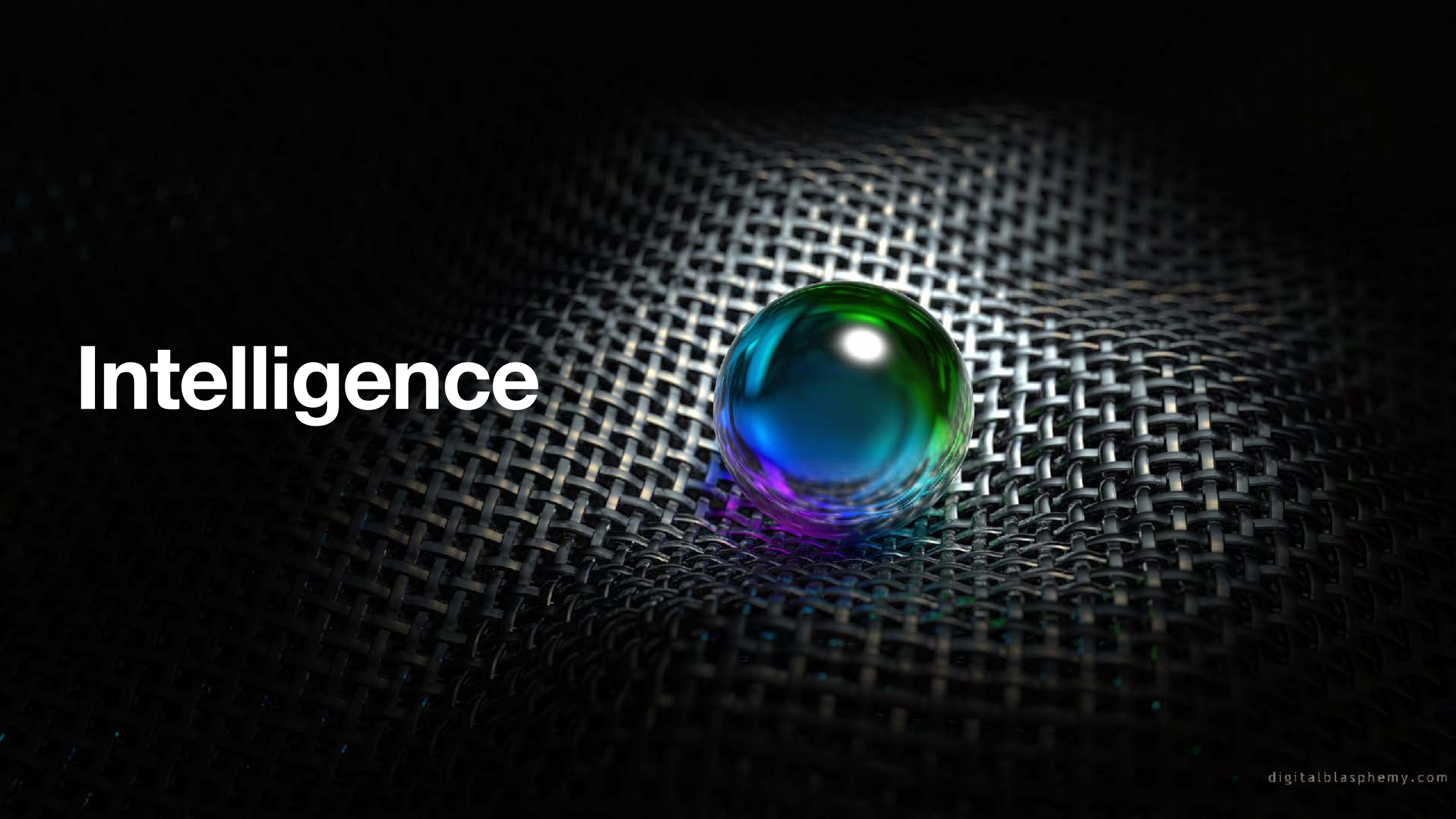
# WinPmem

## Windows Memory Extractor

# Nessus
## Vulnerability Assessment



# Intelligence



# Shodan

SHODAN | Explore | Downloads | Pricing | enphase-envoy

TOTAL RESULTS

997

TOP COUNTRIES

| | |
|---|---|
| United States | 723 |
| Netherlands | 104 |
| Canada | 45 |
| Belgium | 32 |
| France | 25 |

More...

TOP ORGANIZATIONS

| | |
|---|---|
| Charter Communications Inc | 348 |
| CPE Customers NL | 35 |
| AT&T Corp. | 27 |
| Hawaiian Telcom Services Company, Inc. | 21 |
| Comcast Cable Communications, Inc. | 15 |

More...

View Report | Download Results | Historical Trend | View

**New Service:** Keep track of what you have connected to the Internet

**67.213.99.243**

host-67-213-99-243.public.eastlink.ca

Amtelecom Cable Inc

Canada, Aylmer

```
mDNS:
  services:
    80/tcp enphase-envoy:
      txtvers=1
      protovers=3.7.31
      serialnum=121049456542
      Name=envoy
      Address=67.213.99.243
  answers:
    PTR:
      _enphase-envoy._tcp.local
```

**136.26.94.86**

136-26-94-86.cab.webpass.net

Webpass Inc.

United States, San Diego

```
mDNS:
  services:
    80/tcp enphase-envoy:
      txtvers=1
      protovers=5.0.55
      serialnum=121920036082
      Name=envoy
      Address=136.26.94.86 2604:5500:50cb:0:12ce:
  answers:
    PTR:
      _enphase-envoy._tcp.local
```

**76.14.61.121**

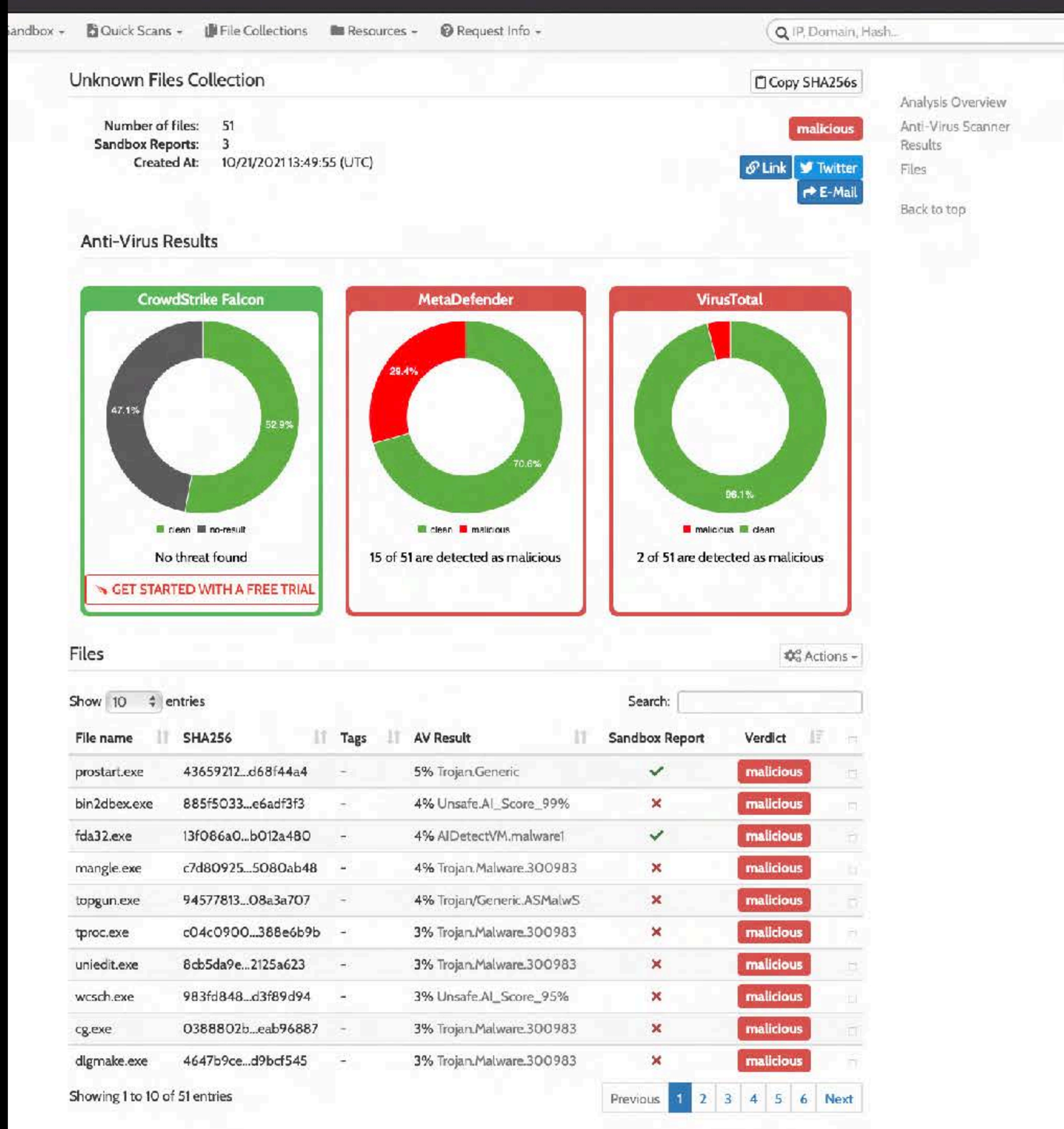
76-14-61-121.sf-cable.astound.net

Wave Broadband

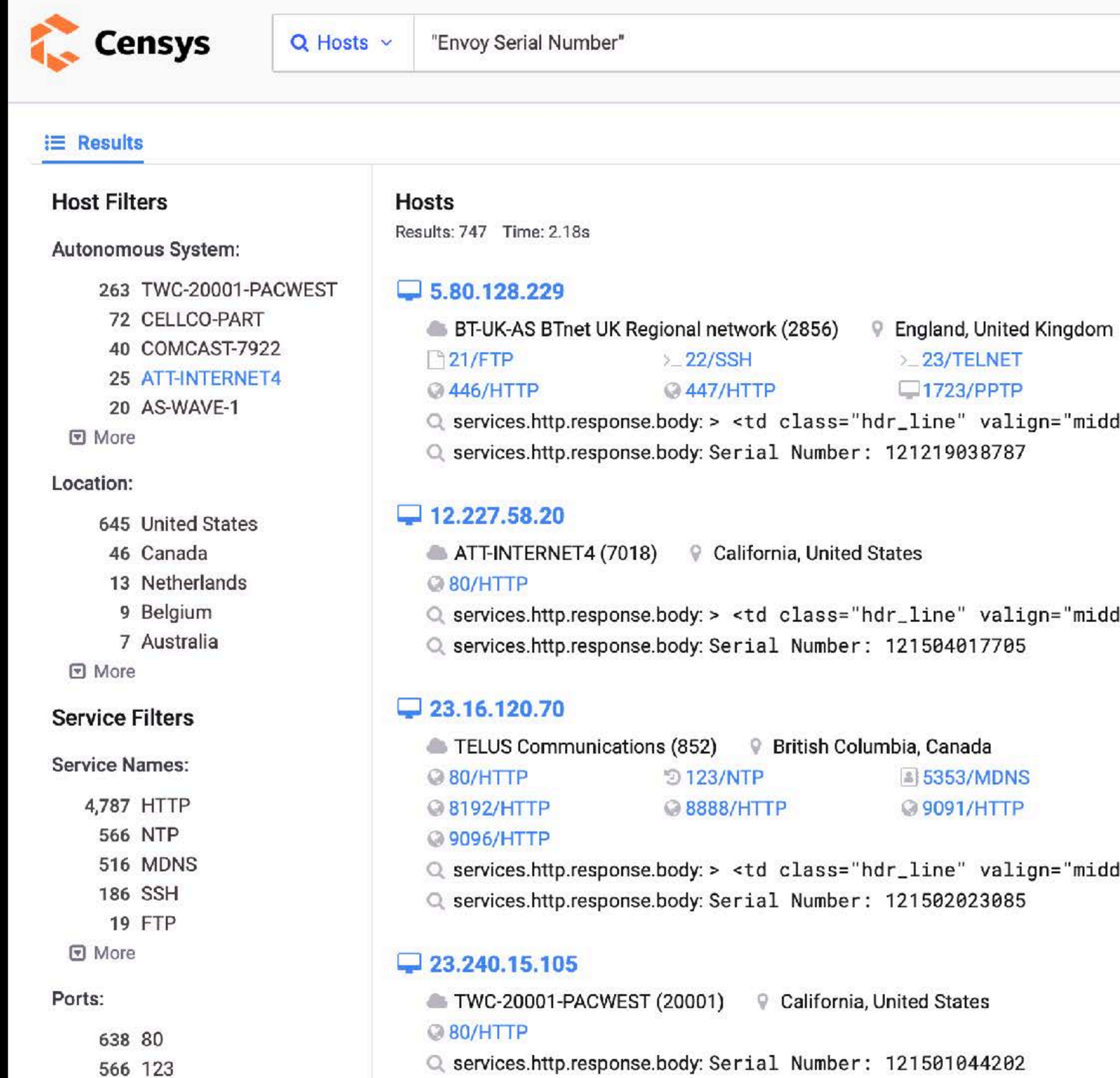
United States, Walnut Creek

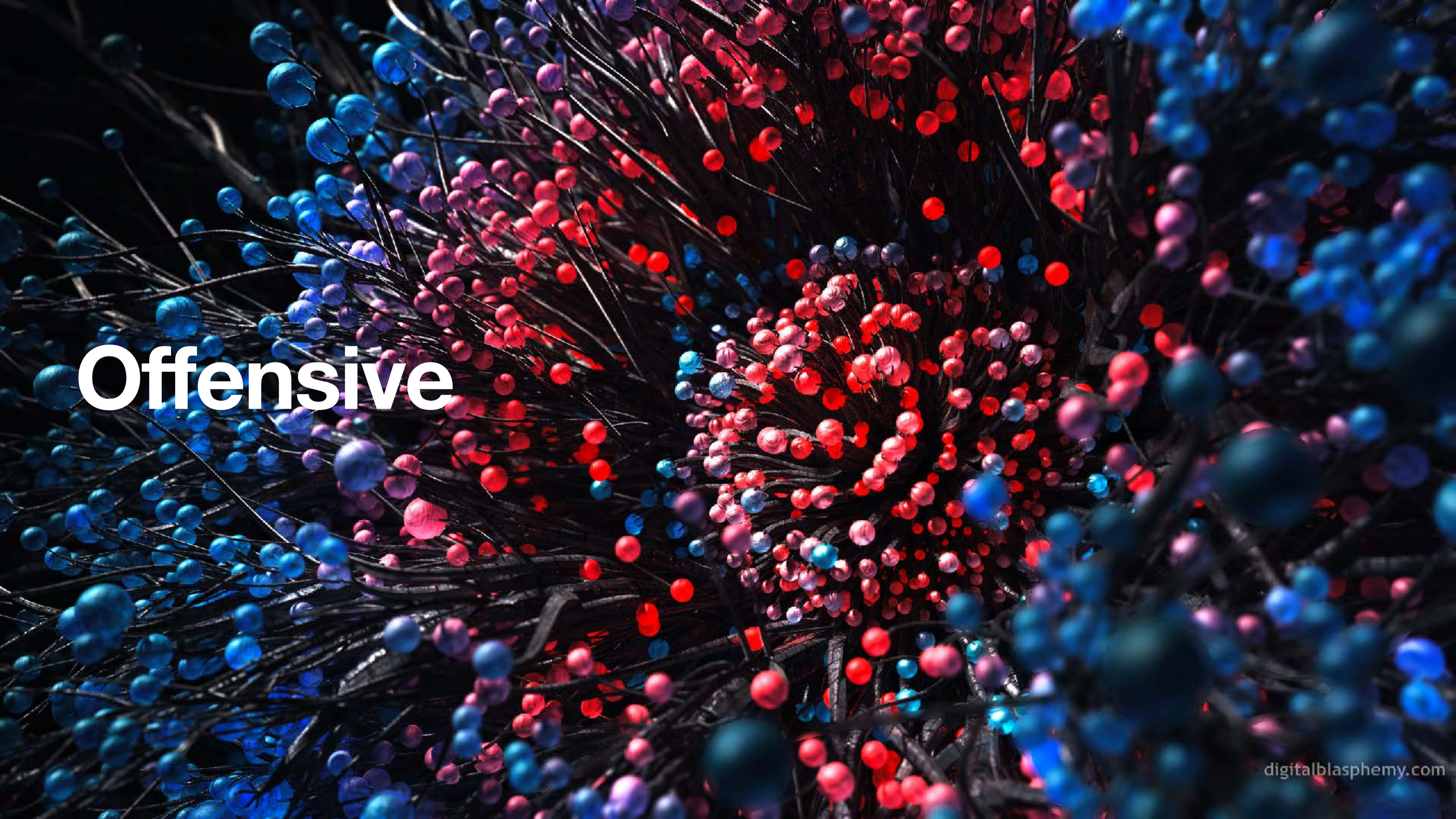
```
mDNS:
  services:
    80/tcp enphase-envoy:
      txtvers=1
      protovers=3.17.3
      serialnum=121345000892
      Name=envoy-00069
```

# hybrid-analysis.com



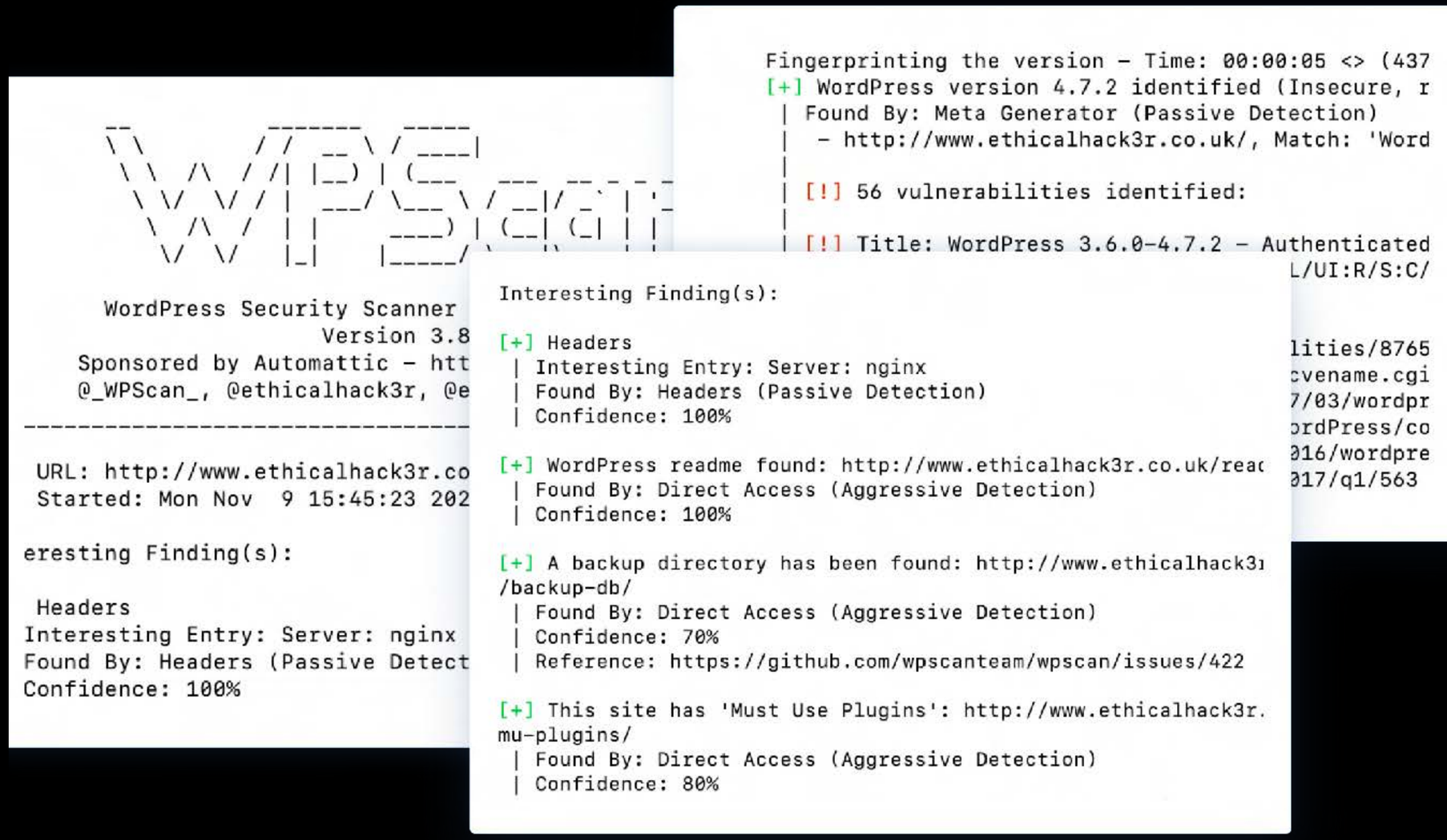
# censys.io


Censys
Hosts
"Envoy Serial Number"
Results
Host Filters
Autonomous System:
263 TWC-20001-PACWEST
72 CELLCO-PART
40 COMCAST-7922
25 ATT-INTERNET4
20 AS-WAVE-1
More
Location:
645 United States
46 Canada
13 Netherlands
9 Belgium
7 Australia
More
Service Filters
Service Names:
4,787 HTTP
566 NTP
516 MDNS
186 SSH
19 FTP
More
Ports:
638 80
566 123
Hosts
Results: 747 Time: 2.18s
5.80.128.229
BT-UK-AS BTnet UK Regional network (2856)
England, United Kingdom
21/FTP
22/SSH
23/TELNET
446/HTTP
447/HTTP
1723/PPTP
services.http.response.body: > <td class="hdr_line" valign="midd
services.http.response.body: Serial Number: 121219038787
12.227.58.20
ATT-INTERNET4 (7018)
California, United States
80/HTTP
services.http.response.body: > <td class="hdr_line" valign="midd
services.http.response.body: Serial Number: 121504017705
23.16.120.70
TELUS Communications (852)
British Columbia, Canada
80/HTTP
123/NTP
5353/MDNS
8192/HTTP
8888/HTTP
9091/HTTP
9096/HTTP
services.http.response.body: > <td class="hdr_line" valign="midd
services.http.response.body: Serial Number: 121502023085
23.240.15.105
TWC-20001-PACWEST (20001)
California, United States
80/HTTP
services.http.response.body: Serial Number: 121501044202


Offensive
digitalblasphemy.com

# WPScan

## WordPress Security Scanner



# Nikto

## Web Server Scanner

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.131.85.78
+ Target Hostname:    zevlag.com
+ Target Port:        80
+ Start Time:         2021-11-18 10:04:37 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.43 (FreeBSD) OpenSSL/1.0.2s-freebsd PHP/5.6.32
+ Retrieved x-powered-by header: PHP/5.6.32
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
 some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
f the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /favicon.ico, field
+ OSVDB-39272: favicon.ico file identifies this server as: Wordpress
+ Web Server returns a valid response with junk HTTP methods, this may caus
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable
+ /error_log: PHP include error may indicate local or remote file inclusion
+ OSVDB-3092: /error_log: This might be interesting...
+ OSVDB-3268: /logs/: Directory indexing found.
+ OSVDB-3092: /logs/: This might be interesting...
+ OSVDB-3268: /temp/: Directory indexing found.
+ OSVDB-3092: /temp/: This might be interesting...
+ OSVDB-3233: /a/: May be Kebi Web Mail administration menu.
+ OSVDB-3268: /mc/: Directory indexing found.
+ OSVDB-3092: /mc/: This might be interesting... potential country code (Mo
+ OSVDB-3092: /tl/: This might be interesting... potential country code (Ti
```

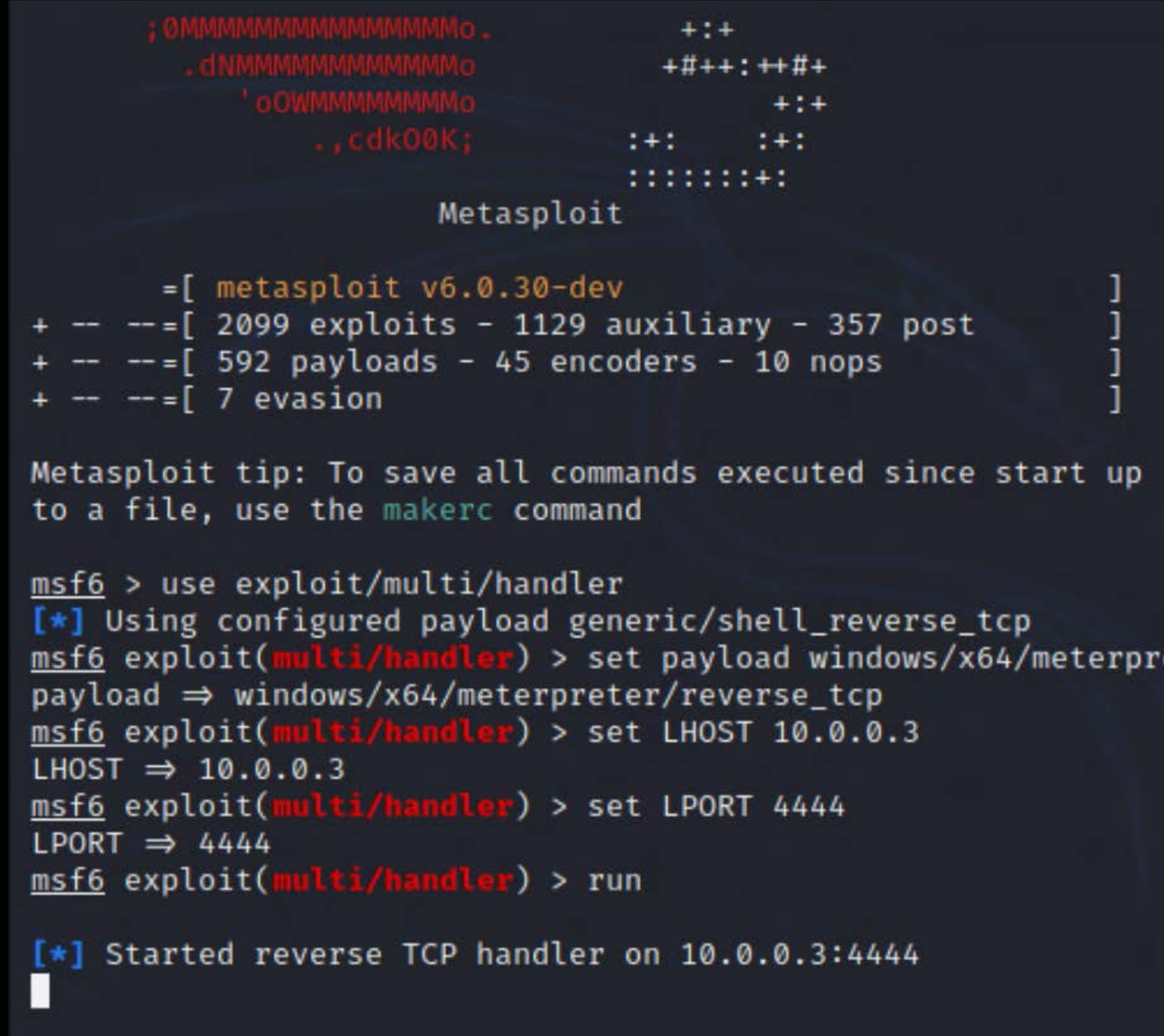
# hashcat

## Password Cracker

```
hashcat (v6.2.1) starting...

CUDA API (CUDA 11.3)
====================
* Device #1: NVIDIA GeForce RTX 2080 Ti, 10137/11264 MB, 68MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1100 MB

e983672a03adcc9767b24584338eb378:00:hashcat

Session..........: hashcat
Status...........: Cracked
Hash.Name........: SolarWinds Serv-U
Hash.Target......: e983672a03adcc9767b24584338eb378:00
Time.Started.....: Sun May 23 11:43:13 2021 (1 sec)
Time.Estimated...: Sun May 23 11:43:14 2021 (0 secs)
Guess.Mask.......: ?a?a?a?a?a?at [7]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 24620.9 MH/s (32.19ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 31606272000/735091890625 (4.30%)
Rejected.........: 0/31606272000 (0.00%)
Restore.Point....: 0/857375 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:35840-36864 Iteration:0-1024
Candidates.#1....: 4{,erat -> cyr ~}t
Hardware.Mon.#1..: Temp: 62c Fan: 31% Util:100% Core:1920MHz Mem:7000MHz Bus:16

Started: Sun May 23 11:43:12 2021
Stopped: Sun May 23 11:43:15 2021
```

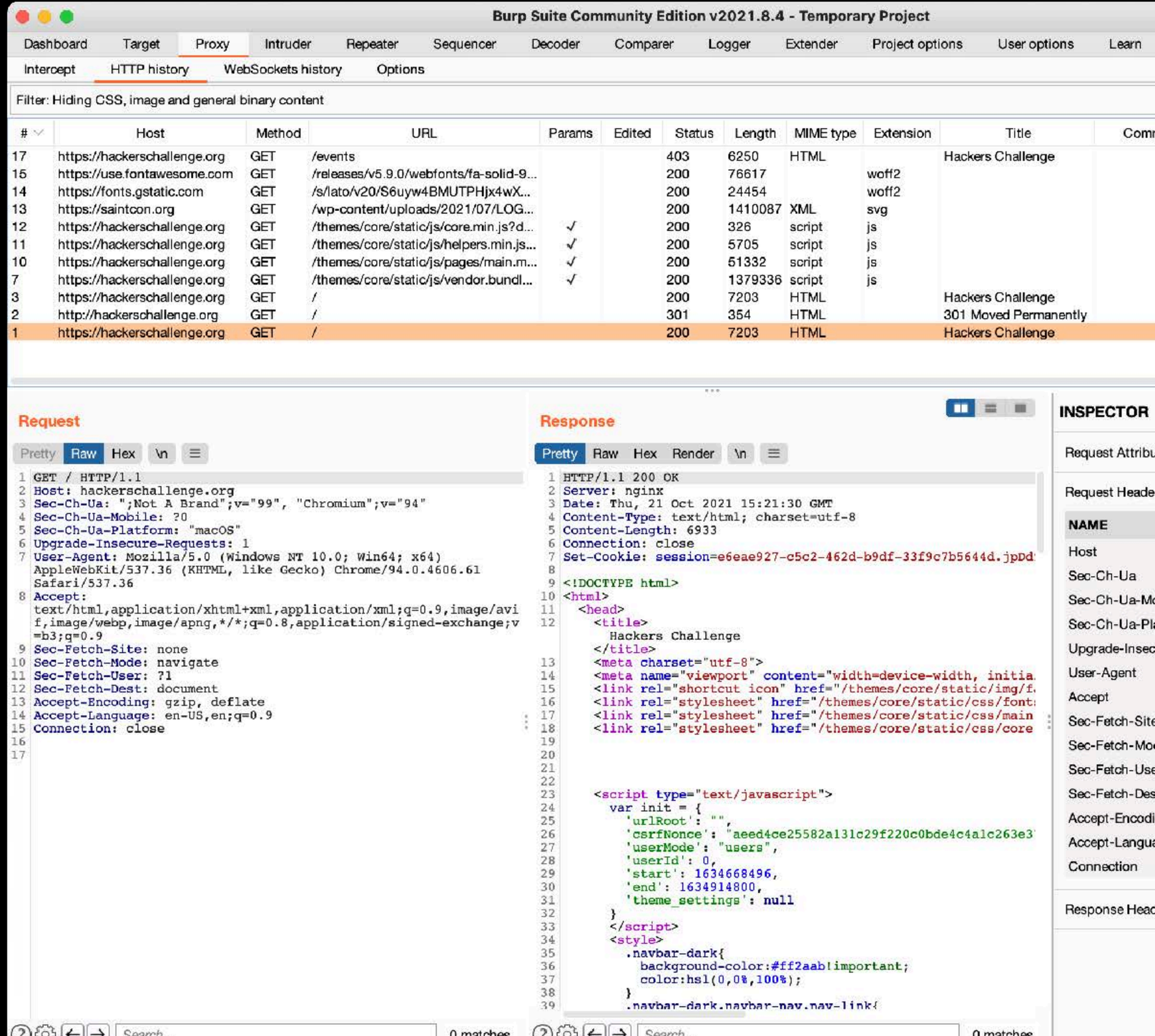
# Metasploit

## Swiss Army knife of Expoitation

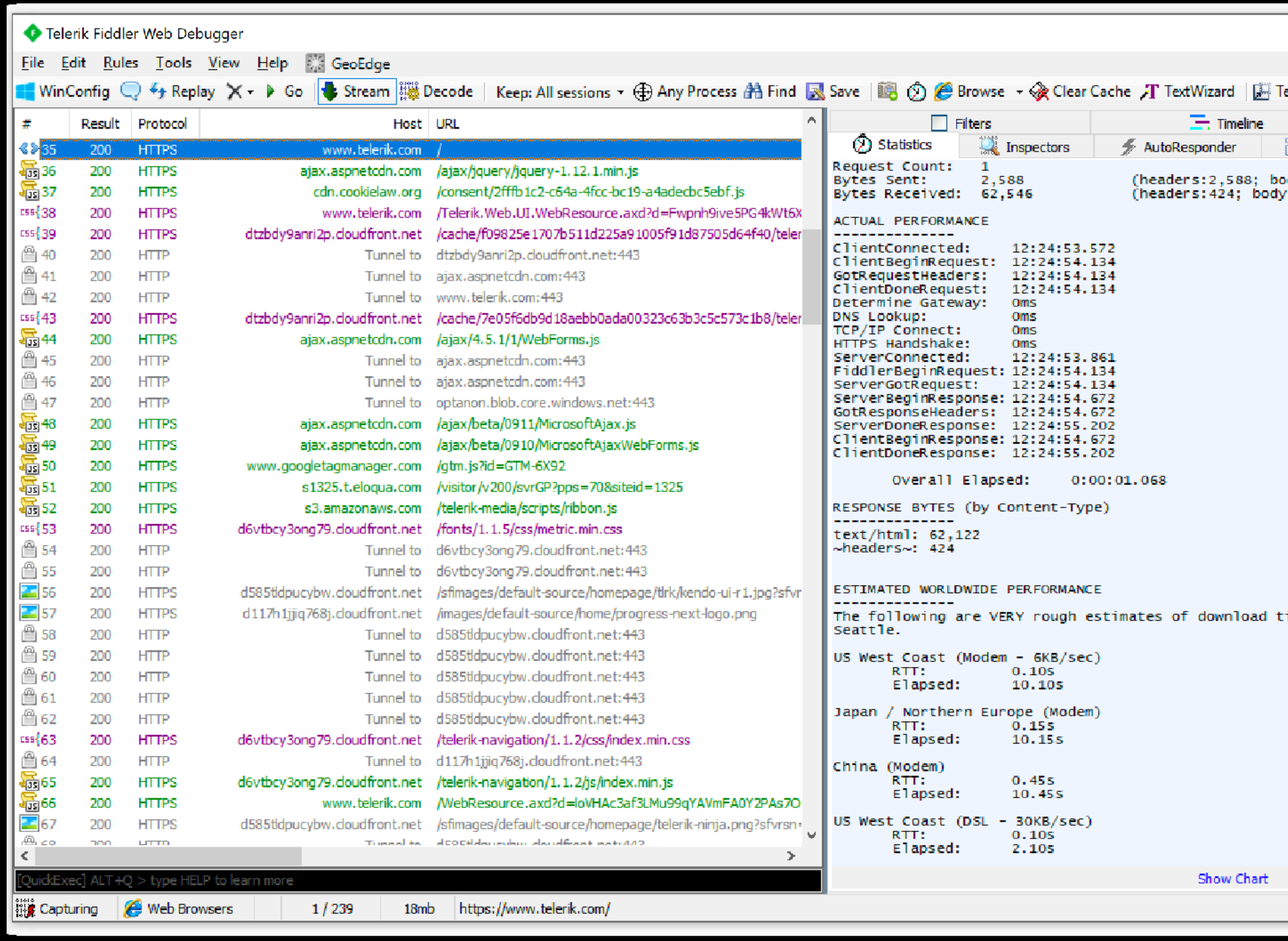


# Burp Suite

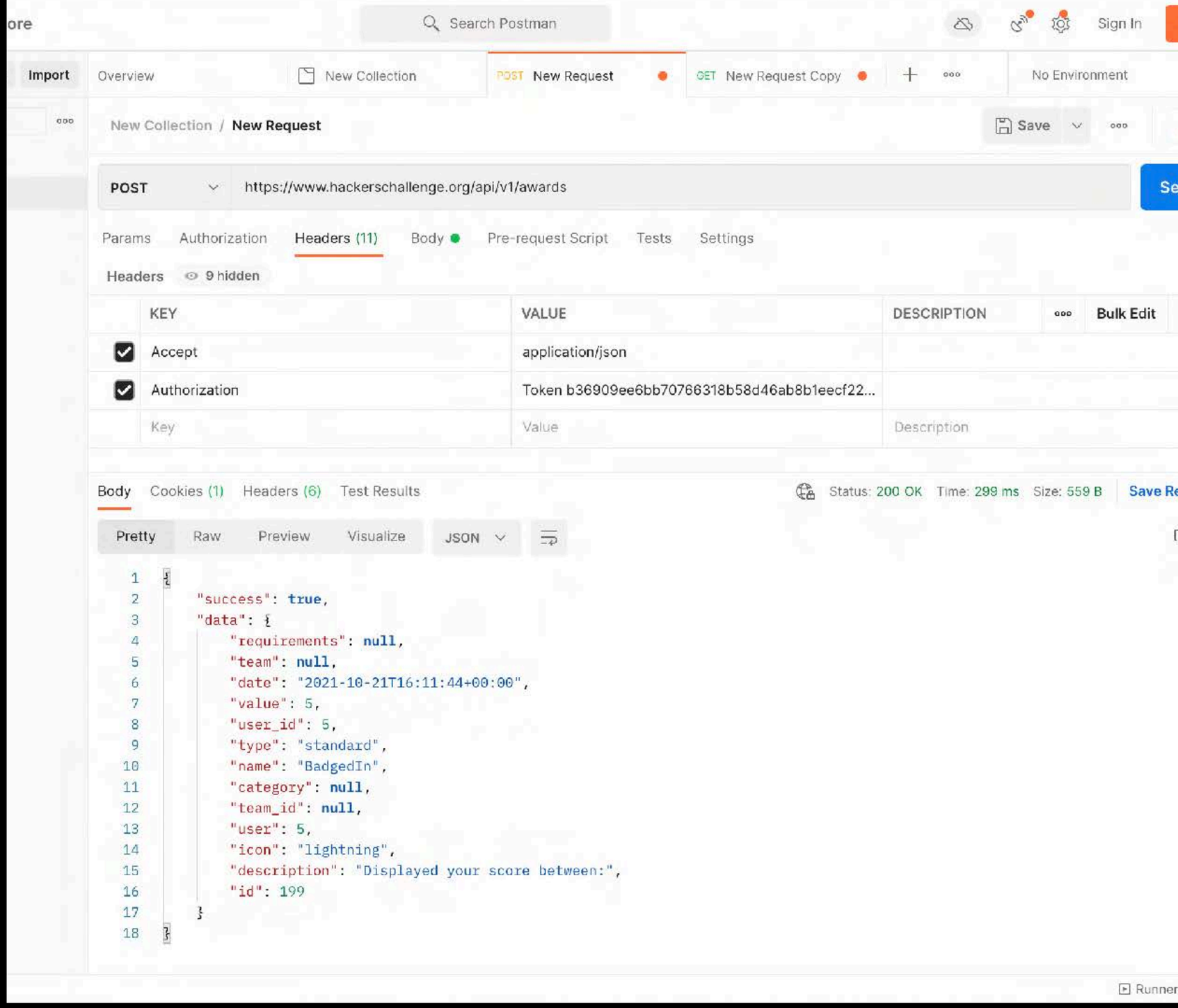
## Ultimate MITM Proxy
## And attack suite



# Fiddler

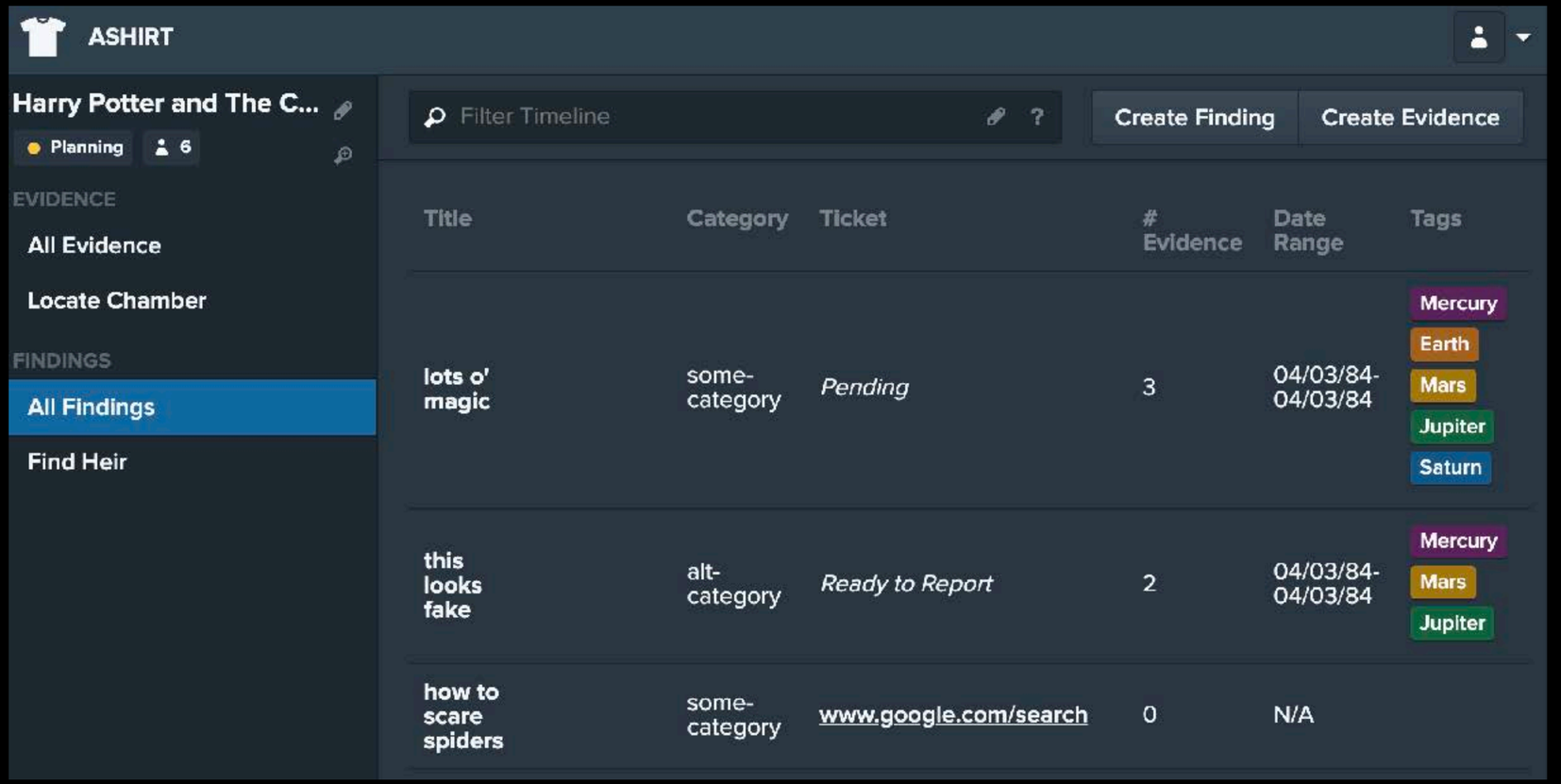

Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard
# Result Protocol Host URL
35 200 HTTPS www.telerik.com /
36 200 HTTPS ajax.aspnetcdn.com /ajax/jquery/jquery-1.12.1.min.js
37 200 HTTPS cdn.cookielaw.org /consent/2fffb1c2-c64a-4fcc-bc19-a4adecbc5ebf.js
38 200 HTTPS www.telerik.com /Telerik.Web.UI.WebResource.axd?d=Fwpnh9ive5PG4kWt6X
39 200 HTTPS dtzbdy9anri2p.cloudfront.net /cache/f09825e1707b511d225a91005f91d87505d64f40/teler
40 200 HTTP Tunnel to dtzbdy9anri2p.cloudfront.net:443
41 200 HTTP Tunnel to ajax.aspnetcdn.com:443
42 200 HTTP Tunnel to www.telerik.com:443
43 200 HTTPS dtzbdy9anri2p.cloudfront.net /cache/7e05f6db9d18aebb0ada00323c63b3c5c573c1b8/teler
44 200 HTTPS ajax.aspnetcdn.com /ajax/4.5.1/1/WebForms.js
45 200 HTTP Tunnel to ajax.aspnetcdn.com:443
46 200 HTTP Tunnel to ajax.aspnetcdn.com:443
47 200 HTTP Tunnel to optanon.blob.core.windows.net:443
48 200 HTTPS ajax.aspnetcdn.com /ajax/beta/0911/MicrosoftAjax.js
49 200 HTTPS ajax.aspnetcdn.com /ajax/beta/0910/MicrosoftAjaxWebForms.js
50 200 HTTPS www.googletagmanager.com /gtm.js?id=GTM-6X92
51 200 HTTPS s1325.t.eloqua.com /visitor/v200/svrGP?pps=70&siteid=1325
52 200 HTTPS s3.amazonaws.com /telerik-media/scripts/ribbon.js
53 200 HTTPS d6vtbcy3ong79.cloudfront.net /fonts/1.1.5/css/metric.min.css
54 200 HTTP Tunnel to d6vtbcy3ong79.cloudfront.net:443
55 200 HTTP Tunnel to d6vtbcy3ong79.cloudfront.net:443
56 200 HTTPS d585tldpucybw.cloudfront.net /sfimages/default-source/homepage/tlrk/kendo-ui-r1.jpg?sfvr
57 200 HTTPS d117h1jjiq768j.cloudfront.net /images/default-source/home/progress-next-logo.png
58 200 HTTP Tunnel to d585tldpucybw.cloudfront.net:443
59 200 HTTP Tunnel to d585tldpucybw.cloudfront.net:443
60 200 HTTP Tunnel to d585tldpucybw.cloudfront.net:443
61 200 HTTP Tunnel to d585tldpucybw.cloudfront.net:443
62 200 HTTP Tunnel to d585tldpucybw.cloudfront.net:443
63 200 HTTPS d6vtbcy3ong79.cloudfront.net /telerik-navigation/1.1.2/css/index.min.css
64 200 HTTP Tunnel to d117h1jjiq768j.cloudfront.net:443
65 200 HTTPS d6vtbcy3ong79.cloudfront.net /telerik-navigation/1.1.2/js/index.min.js
66 200 HTTPS www.telerik.com /WebResource.axd?d=loVHAc3af3LMu99qYAVmFA0Y2PAs7O
67 200 HTTPS d585tldpucybw.cloudfront.net /sfimages/default-source/homepage/telerik-ninja.png?sfvrsn=
Filters Timeline
Statistics Inspectors AutoResponder
Request Count: 1
Bytes Sent: 2,588 (headers:2,588; bo
Bytes Received: 62,546 (headers:424; body
ACTUAL PERFORMANCE
ClientConnected: 12:24:53.572
ClientBeginRequest: 12:24:54.134
GotRequestHeaders: 12:24:54.134
ClientDoneRequest: 12:24:54.134
Determine Gateway: 0ms
DNS Lookup: 0ms
TCP/IP Connect: 0ms
HTTPS Handshake: 0ms
ServerConnected: 12:24:53.861
FiddlerBeginRequest: 12:24:54.134
ServerGotRequest: 12:24:54.134
ServerBeginResponse: 12:24:54.672
GotResponseHeaders: 12:24:54.672
ServerDoneResponse: 12:24:55.202
ClientBeginResponse: 12:24:54.672
ClientDoneResponse: 12:24:55.202
Overall Elapsed: 0:00:01.068
RESPONSE BYTES (by Content-Type)
text/html: 62,122
~headers~: 424
ESTIMATED WORLDWIDE PERFORMANCE
The following are VERY rough estimates of download t
Seattle.
US West Coast (Modem - 6KB/sec)
RTT: 0.10s
Elapsed: 10.10s
Japan / Northern Europe (Modem)
RTT: 0.15s
Elapsed: 10.15s
China (Modem)
RTT: 0.45s
Elapsed: 10.45s
US West Coast (DSL - 30KB/sec)
RTT: 0.10s
Elapsed: 2.10s
Show Chart
[QuickExec] ALT+Q > type HELP to learn more
Capturing Web Browsers 1 / 239 18mb https://www.telerik.com/

# Postman

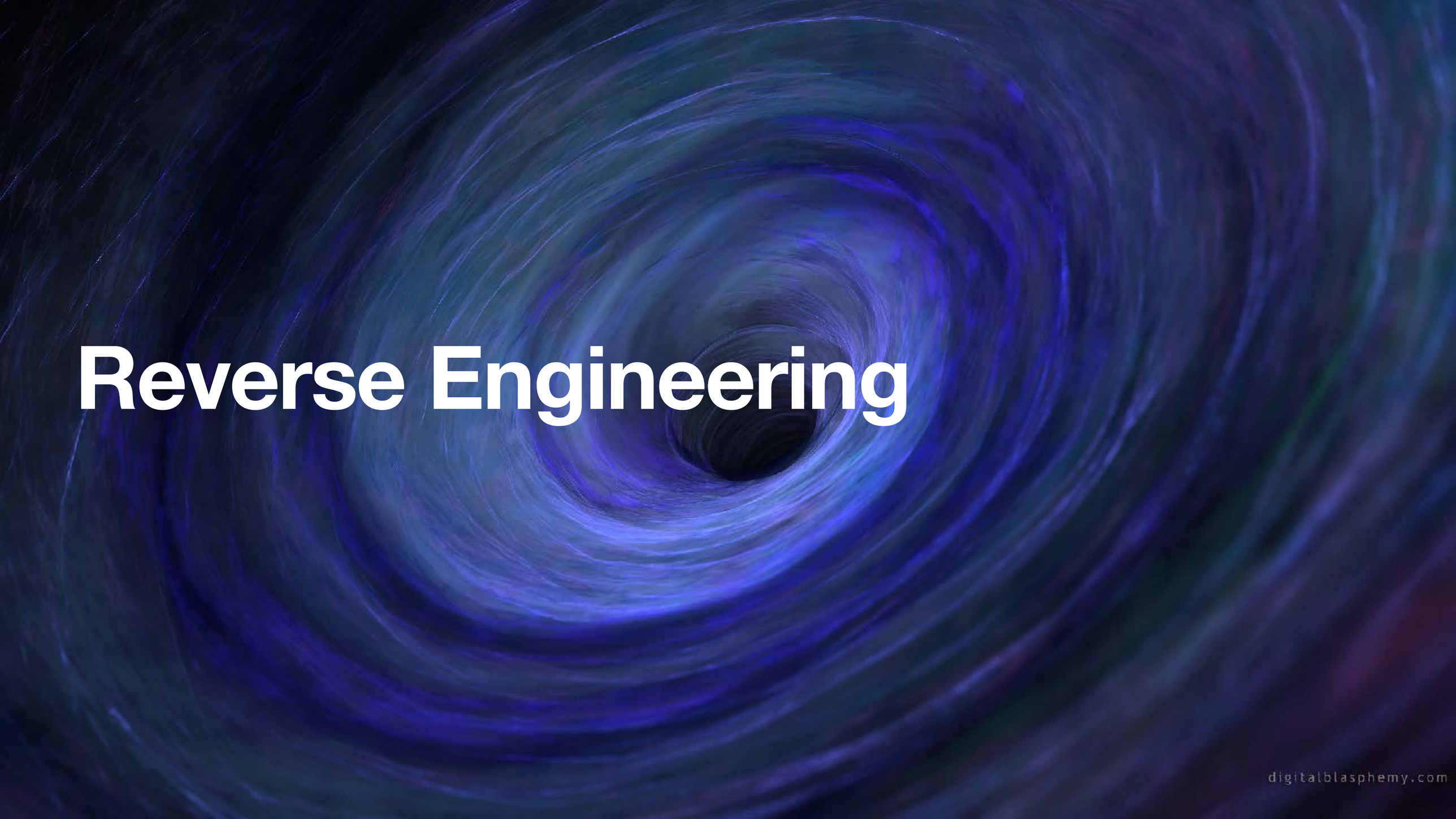

Search Postman
Sign In
Import
Overview
New Collection
POST New Request
GET New Request Copy
No Environment
New Collection / New Request
Save
POST
https://www.hackerschallenge.org/api/v1/awards
Params
Authorization
Headers (11)
Body
Pre-request Script
Tests
Settings
Headers
9 hidden
KEY
VALUE
DESCRIPTION
Bulk Edit
Accept
application/json
Authorization
Token b36909ee6bb70766318b58d46ab8b1eecf22...
Key
Value
Description
Body
Cookies (1)
Headers (6)
Test Results
Status: 200 OK
Time: 299 ms
Size: 559 B
Pretty
Raw
Preview
Visualize
JSON
{
"success": true,
"data": {
"requirements": null,
"team": null,
"date": "2021-10-21T16:11:44+00:00",
"value": 5,
"user_id": 5,
"type": "standard",
"name": "BadgedIn",
"category": null,
"team_id": null,
"user": 5,
"icon": "lightning",
"description": "Displayed your score between:",
"id": 199
}
}
Runner

# ashirt

https://github.com/theparanoids/ashirt-server/

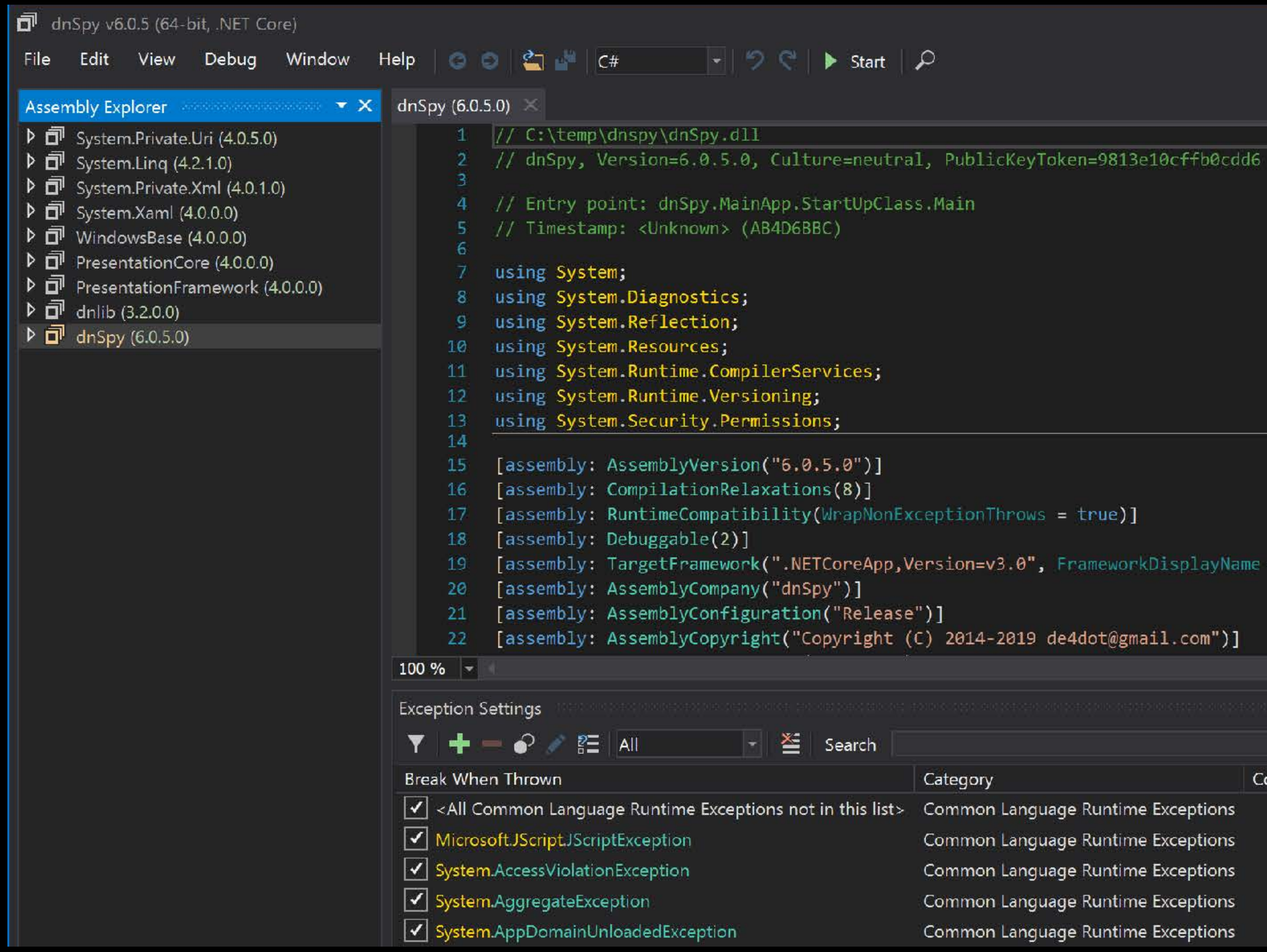


# Reverse Engineering

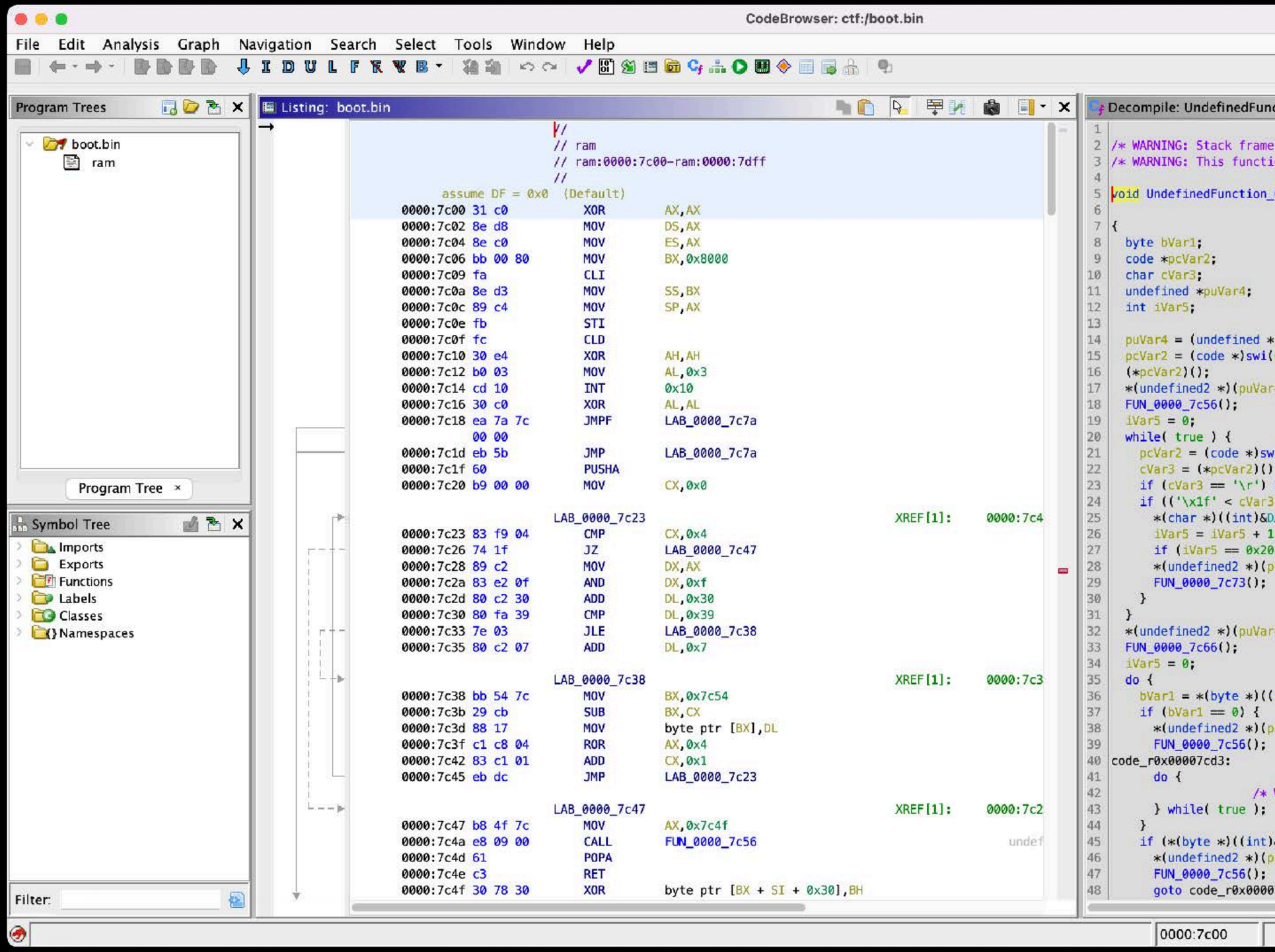


# dnSpy

## A Decompiler for .NET

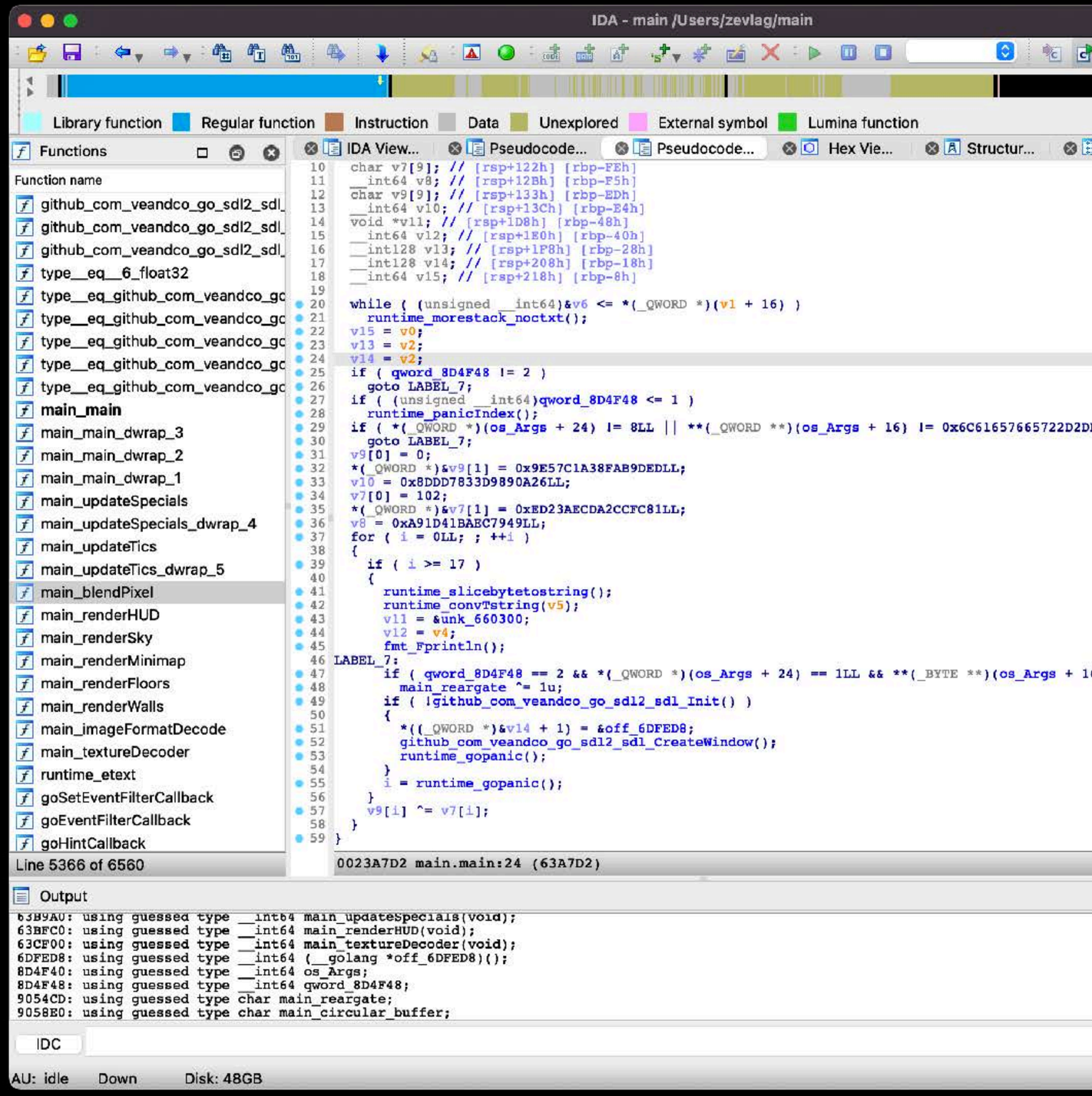


# Ghidra

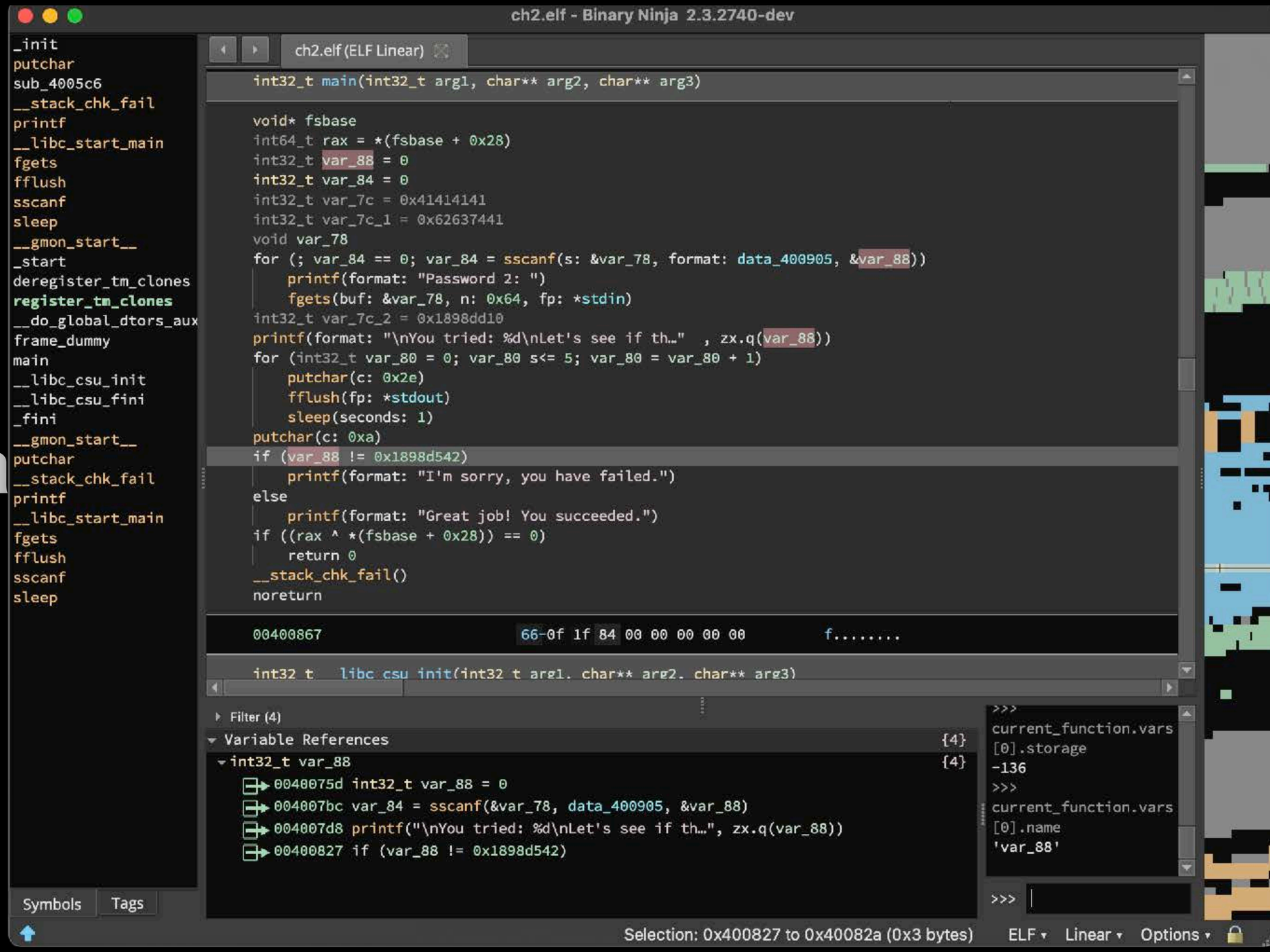

CodeBrowser: ctf:/boot.bin
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
boot.bin
ram
Program Tree
Symbol Tree
Imports
Exports
Functions
Labels
Classes
Namespaces
Filter:
Listing: boot.bin
//
// ram
// ram:0000:7c00-ram:0000:7dff
//
assume DF = 0x0 (Default)
0000:7c00 31 c0 XOR AX,AX
0000:7c02 8e d8 MOV DS,AX
0000:7c04 8e c0 MOV ES,AX
0000:7c06 bb 00 80 MOV BX,0x8000
0000:7c09 fa CLI
0000:7c0a 8e d3 MOV SS,BX
0000:7c0c 89 c4 MOV SP,AX
0000:7c0e fb STI
0000:7c0f fc CLD
0000:7c10 30 e4 XOR AH,AH
0000:7c12 b0 03 MOV AL,0x3
0000:7c14 cd 10 INT 0x10
0000:7c16 30 c0 XOR AL,AL
0000:7c18 ea 7a 7c 00 00 JMPF LAB_0000_7c7a
0000:7c1d eb 5b JMP LAB_0000_7c7a
0000:7c1f 60 PUSHA
0000:7c20 b9 00 00 MOV CX,0x0
LAB_0000_7c23 XREF[1]: 0000:7c4
0000:7c23 83 f9 04 CMP CX,0x4
0000:7c26 74 1f JZ LAB_0000_7c47
0000:7c28 89 c2 MOV DX,AX
0000:7c2a 83 e2 0f AND DX,0xf
0000:7c2d 80 c2 30 ADD DL,0x30
0000:7c30 80 fa 39 CMP DL,0x39
0000:7c33 7e 03 JLE LAB_0000_7c38
0000:7c35 80 c2 07 ADD DL,0x7
LAB_0000_7c38 XREF[1]: 0000:7c3
0000:7c38 bb 54 7c MOV BX,0x7c54
0000:7c3b 29 cb SUB BX,CX
0000:7c3d 88 17 MOV byte ptr [BX],DL
0000:7c3f c1 c8 04 ROR AX,0x4
0000:7c42 83 c1 01 ADD CX,0x1
0000:7c45 eb dc JMP LAB_0000_7c23
LAB_0000_7c47 XREF[1]: 0000:7c2
0000:7c47 b8 4f 7c MOV AX,0x7c4f
0000:7c4a e8 09 00 CALL FUN_0000_7c56
0000:7c4d 61 POPA
0000:7c4e c3 RET
0000:7c4f 30 78 30 XOR byte ptr [BX + SI + 0x30],BH
Decompile: UndefinedFunc
/* WARNING: Stack frame
/* WARNING: This functi
void UndefinedFunction_
{
byte bVar1;
code *pcVar2;
char cVar3;
undefined *puVar4;
int iVar5;
puVar4 = (undefined *
pcVar2 = (code *)swi(
(*pcVar2)();
*(undefined2 *)(puVar
FUN_0000_7c56();
iVar5 = 0;
while( true ) {
pcVar2 = (code *)sw
cVar3 = (*pcVar2)()
if (cVar3 == '\r')
if ('\x1f' < cVar3
*(char *)((int)&D
iVar5 = iVar5 + 1
if (iVar5 == 0x20
*(undefined2 *)(p
FUN_0000_7c73();
}
}
*(undefined2 *)(puVar
FUN_0000_7c66();
iVar5 = 0;
do {
bVar1 = *(byte *)((
if (bVar1 == 0) {
*(undefined2 *)(p
FUN_0000_7c56();
code_r0x00007cd3:
do {
/*
} while( true );
}
if (*(byte *)((int)
*(undefined2 *)(p
FUN_0000_7c56();
goto code_r0x0000
0000:7c00

# IDA

## Free Version is quite capable with cloud decompiler



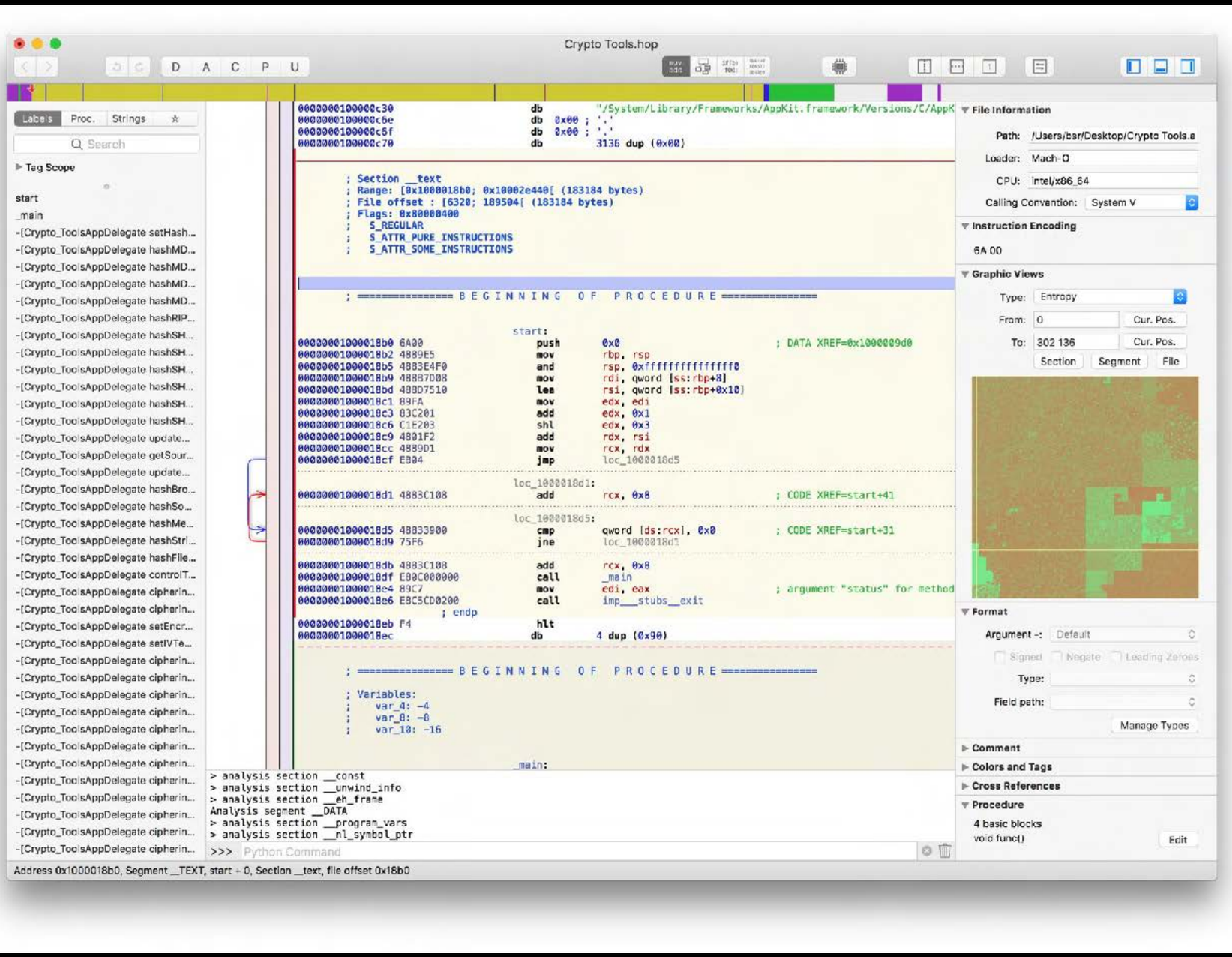
# Binary Ninja



# Hopper

## MacOS Decompiler

## Objective C




Everything Else
digitalblasphemy.com

# SQL

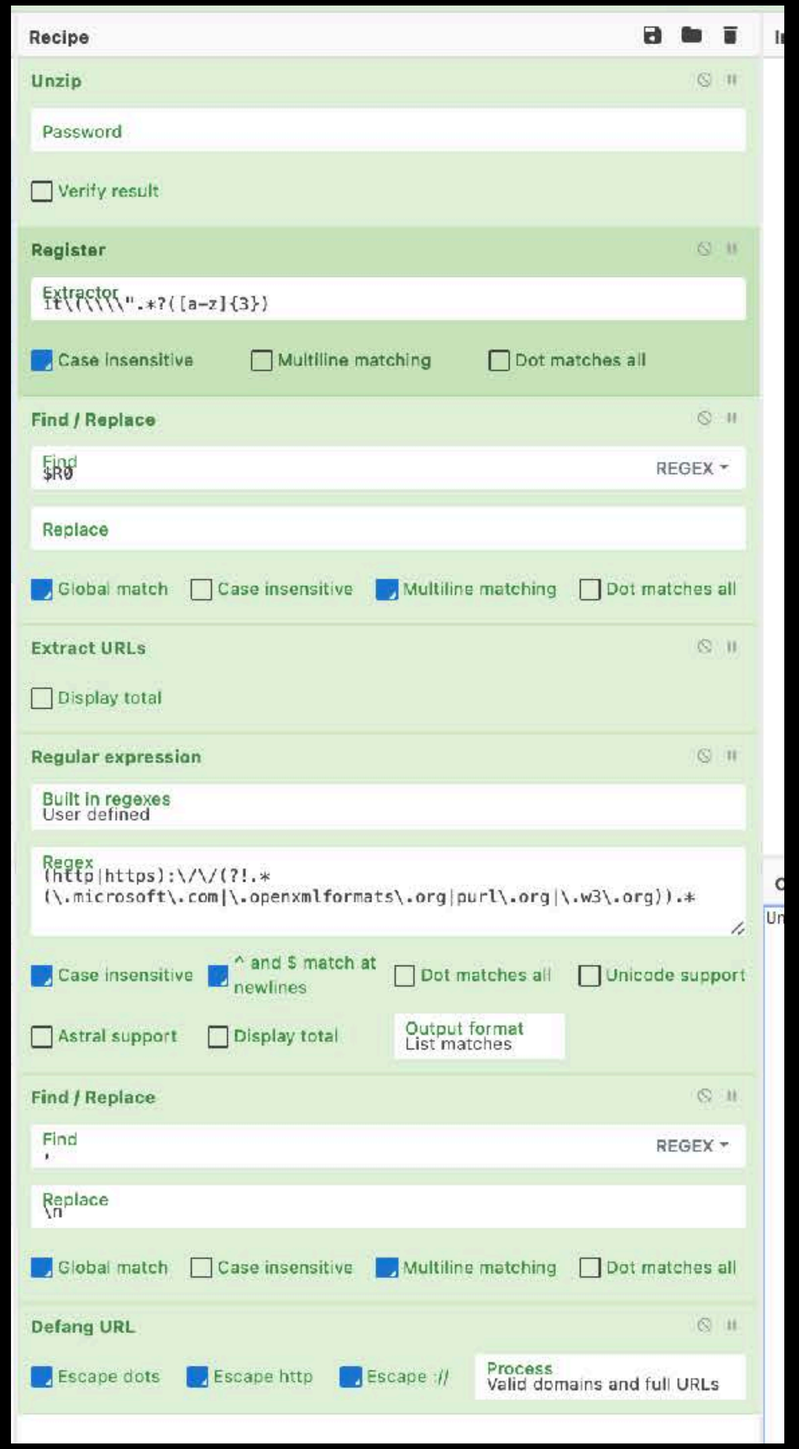
**Structured Query Language**

```
SELECT incidents.*,
       sub.incidents AS incidents_that_day
  FROM tutorial.sf_crime_incidents_2014_01 incidents
  JOIN ( SELECT date,
           COUNT(incidnt_num) AS incidents
            FROM tutorial.sf_crime_incidents_2014_01
           GROUP BY 1
       ) sub
    ON incidents.date = sub.date
 ORDER BY sub.incidents DESC, time
```

# Excel

# CyberChef

https://github.com/mattnotmax/cyberchef-recipes




base64

```
iVBORw0KGgoAAAANSUhEUgAAB8IAAAEICAYAAAAk3j7UAAAMaGlDQ1BJQ0MgUHJ
vZmlsZQAASImVVwdUU8kanltSSWiBCEgJvQnSq5QQWgABqYKNkAQSSgwJQcVeFh
VcKyKKFV0Vsa2ugKwFsZdFsPfFgoqyLuqiKCpvQgK67ivn/efMnS/f/
PO3O5M7A4BWL08qzUO1AciXFMoSIkJYY9PSWaQOQAYYoAIHYMXjy6Xs+PgYAGWw
/7u8uwEQZX/VSWnrn+P/
VXQFQjkfAGQ8xJkCOT8f4iYA8PV8qawQAKKSt5xSKFXiORDryWCAEJcrcbYK71T
iTBU+MqCTlMCBuBUAMo3Hk2UDoHkP
….
66Xq3zNYrlSzbC4Erivzhf/
fasc8GD3npvti+uAZ7ZFTtrn3XQSXnWGHb1TJmveBMWZ1Kfo9/04yDD2w85d/
gw9T7n3B98OP4//tE11adQOR8AAAAASUVORK5CYII=
```

# curl / wget

**curl Protocols:**

DICT
FILE
FTP(S)
GOPHER(S)
HTTP(S)
IMAP(S)
LDAP(S)
MQTT
POP3(S)
RTMP(S)
RTSP
SCP
SFTP
SMB(S)
SMTP(S)
TELNET
TFTP

**wget Features:**

Recursive download

# jq

## JSON data manipulation

```
zevlag@Z314 ~ % cat users.json | jq '.data[]'
{
  "pos": 1,
  "account_id": 100,
  "account_url": "/users/100",
  "account_type": "user",
  "oauth_id": null,
  "name": "phaktor",
  "score": 0
}
{
  "pos": 2,
  "account_id": 6,
  "account_url": "/users/6",
  "account_type": "user",
  "oauth_id": null,
  "name": "Santiago",
  "score": 0
}
{
  "pos": 3,
  "account_id": 78,
  "account_url": "/users/78",
  "account_type": "user",
  "oauth_id": null,
  "name": "Legoclones",
  "score": 0
}
{
  "pos": 4,
  "account_id": 69,
  "account_url": "/users/69",
  "account_type": "user",
  "oauth_id": null,
  "name": "cha0swir3",
  "score": 0
}
```

# WSL

Windows
Subsytem
Linux

# proxychains

hooks network functions
and redirects to a proxy

Vmware

Virtualbox

QEMU

# grep

https://beyondgrep.com/feature-comparison/

vscode

Notepad++

Sublime Text

BBEdit

# Collections

# Kali

# CommandoVM

**Windows-based security distribution for penetration testing and red teaming**

COMMANDOVM

COMPLETE MANDIANT OFFENSIVE VM

# flareVM

**Windows-based security distribution for malware analysis, incident response**

# And Finally

# Play Capture The Flag

# Be Curious

Why?

How?