NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

THAILAND CYBER TOP TALENT

HUAWEI

Thailand Cyber Top Talent 2023

นาย ปรมินทร์ ช่วงมณี (พี่มินทร์)

CERT Manger, TB-CERT

ผู้บรรยาย

นาย ปรมินทร์ ช่วงมณี (พี่มินทร์)

การศึกษา

- Master's Degree : Management & Strategy
- Bachelor's degree: Computer Science

ตำแหน่ง

- ผู้จัดการ (CERT Manger) ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)
- พนักงานเจ้าหน้าที่ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- Hack The Box (HTB) Ambassador

HACKTHEBOX www.meetup.com/hack-the-box-meetup-thailand/

YouTube www.youtube.com/@hackatmin

ภาพกิจกรรมของ TB-CERT

หัวข้อบรรยาย

1. ทักษะและยุทธวิธี
2. เตรียมความพร้อมทักษะด้านต่างๆ
    - Web Application
    - Cryptography
    - Reverse engineering
    - Digital Forensics
    - Network Analysis

ภาพรวมบรรยาย

ทักษะและยุทธวิธี

David Beckham

ตำแหน่ง: ปีกขวา

ทักษะ: Free Kick, Corner, Crossing

Steven Gerrard

ตำแหน่ง: “เดอะแบก” เป็นกัปตัน มิดฟิลด์ตัวรับ, มิดฟิลด์ตัวรุก, ปีกขวา, แบ็กขวา

ทักษะ: Leadership, Tanker, Free Kick, Crossing

ทักษะและยุทธวิธี

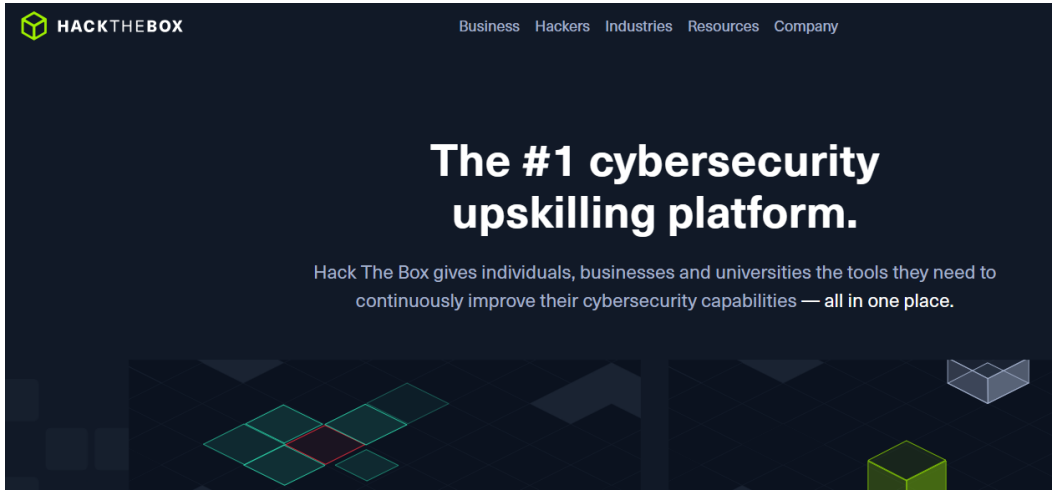
คำถาม

1. น้องๆ คิดว่าทักษะคืออะไร
2. น้องๆ จะสร้างทักษะขึ้นได้อย่างไร

ทักษะและยุทธวิธี

ช่องทางการฝึกทักษะเพิ่มเติม

https://app.hackthebox.com/



https://tryhackme.com/

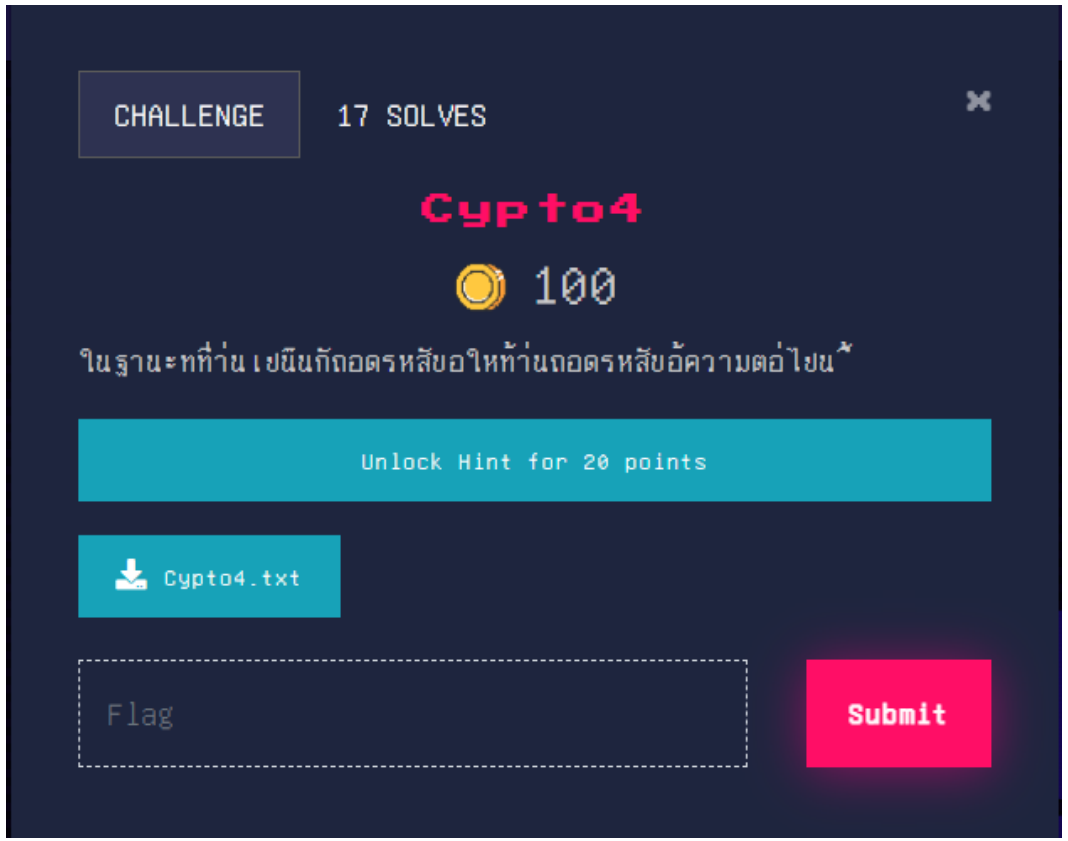
ทักษะและยุทธวิธี

กำหนดยุทธวิธี การแข่ง

1. เข้าใจกฎกติกา ข้อห้าม
2. เข้าใจเกณฑ์การตัดสิน และการให้คะแนน (Fixed & Dynamic)
3. จัดแบ่งตามความถนัด
4. ทักษะที่ต้องฝึกเพิ่ม
5. ทดแทนตำแหน่งการเล่น
6. เปิดเกมเร็ว ดึงเกมช้า หลอกล่อ

ทักษะและยุทธวิธี

จุดสังเกตุบนระบบแข่ง

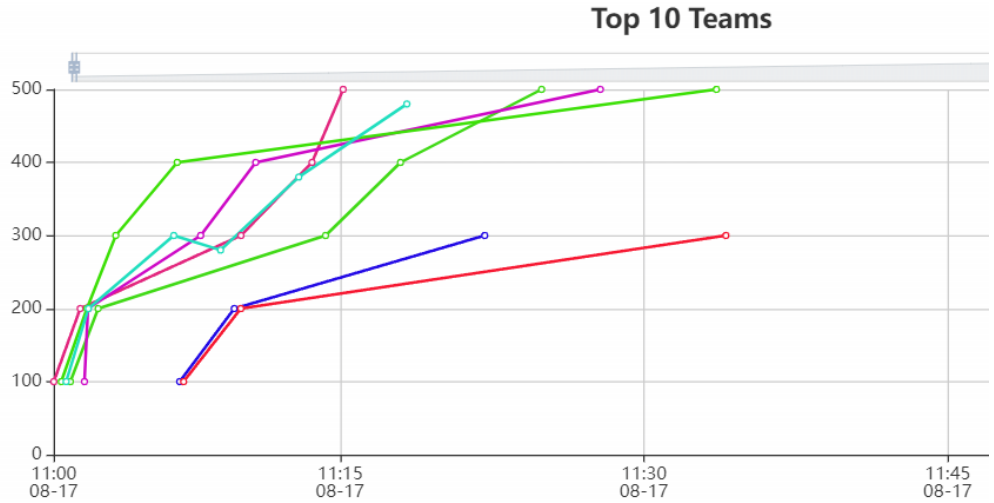


1. จำนวนคะแนนจะสะท้อนความยาก (ในกรณี Fixed score)
2. หมั่นสังเกตุจำนวนทีมที่ Solves
3. พิจารณาตัดสินในใช้ Hint (ถ้าจำเป็น) แต่คะแนนจะถูกลบ

หมายเหตุ จำลองหน้าจอ ระบบจริงจะมีหน้าจอที่แตกต่าง

ทักษะและยุทธวิธี

จุดสังเกตุบนระบบแข่ง



4. สังเกตุทีมกลุ่มคะแนนใกล้เคียงกับทีมเรา แก้ไขโจทย์ประเภทอะไร ชื่อโจทย์อะไร

5. สังเกตุกลุ่ม Top5

Place	Team	Score
1	[redacted]	1100
2		1100
3		1100
4		1100
5		1100
6		1100
7		1100

Solves

Challenge	Value	Time
Network2	100	August 17th, 2:40:48 PM
Reverse2	100	August 17th, 2:40:03 PM
Network1	100	August 17th, 2:38:37 PM
Forensic1	100	August 17th, 2:30:28 PM
Reverse3	100	August 17th, 2:27:04 PM
Reverse1	100	August 17th, 2:25:42 PM
Cypto3	100	August 17th, 11:15:09 AM

หมายเหตุ จำลองหน้าจอ ระบบจริงจะมีหน้าจอที่แตกต่าง

ทักษะและยุทธวิธี

คำถาม (คุยกันในทีม)

1. มียุทธวิธีในการแข่งไว้แล้วหรือยัง
2. วางยุทธวิธีในการแข่งอย่างไร

Introduction

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

THAILAND CYBER TOP TALENT

HUAWEI

Thailand Cyber Top Talent 2023

การแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย จัดโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ร่วมกับบริษัท หัวเว่ย เทคโนโลยี่ (ประเทศไทย) จำกัด โดยมุ่งหวังให้นักเรียน นิสิต นักศึกษา และประชาชนทั่วไปที่เข้าร่วมการแข่งขันได้ เรียนรู้ พัฒนาทักษะ และประสบการณ์ เพื่อให้กลายเป็นบุคลากรที่มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์และเป็นการสร้างแรงงานออกสู่ตลาดแรงงานในอนาคต อีกทั้งเป็นการช่วยเพิ่มความตระหนักรับรู้เกี่ยวกับภัยคุกคามทางด้านไซเบอร์ให้กับบุคคลทั่วไปมากขึ้น และผู้ที่ได้รางวัลชนะเลิศยังมีสิทธิเป็นตัวแทนประเทศไทยไปแข่งขันในรายการ Cyber SEA Game 2023

Introduction

รูปแบบและกติกาการแข่งขัน

การแข่งขันจะแบ่งเป็น 3 ระดับ

ระดับมัธยมศึกษา เป็นนักเรียนระดับมัธยมศึกษาตอนต้น ตอนปลาย หรือเทียบเท่า สังกัดโรงเรียนหรือสถาบันในประเทศไทย

ระดับอุดมศึกษา เป็นนักศึกษาในระดับอุดมศึกษา หรือเทียบเท่า สังกัดมหาวิทยาลัยหรือสถาบันในประเทศไทย อายุไม่เกิน 30 ปีบริบูรณ์ ณ วันที่ลงทะเบียนสมัคร

ระดับประชาชนทั่วไป เป็นหน่วยงาน CII หน่วยงานภาครัฐ ภาคเอกชน และประชาชนทั่วไปสัญชาติไทย

รูปแบบการแข่งขัน แบ่งเป็น 2 รอบ

- **รอบที่ 1 รอบคัดเลือก** เป็นการแข่ง Capture the Flag ในรูปแบบ Jeopardy คือผู้เข้าแข่งขันสามารถเลือกโจทย์ในหัวข้อใดทำก่อนก็ได้ คะแนนของโจทย์แต่ละหัวข้อจะไม่เท่ากัน ขึ้นอยู่กับระดับความยากง่ายของโจทย์
- **รอบที่ 2 รอบชิงชนะเลิศ** เป็นการแข่ง Capture the Flag ในรูปแบบ Attack the virtual World คือผู้เข้าแข่งขันต้องหาคำตอบจากเครื่องแม่ข่าย เครื่องผู้ใช้งาน และอุปกรณ์เครือข่ายต่าง ๆ ที่อยู่ในระบบจำลอง ด้วยการโจมตีจากภายนอก และต้องหาคำตอบจากร่องลอยในเครื่องแม่ข่ายที่ถูกโจมตี

Introduction

รอบคัดเลือก

เป็นการแข่ง Capture the Flag ในรูปแบบ Jeopardy คือผู้เข้าแข่งขันสามารถเลือกโจทย์ในหัวข้อใดทำก่อนก็ได้ คะแนนของโจทย์แต่ละหัวข้อจะไม่เท่ากัน ขึ้นอยู่กับระดับความยากง่ายของโจทย์ ในรูปแบบออนไลน์ โดยมีหัวข้อต่าง ๆ ดังนี้

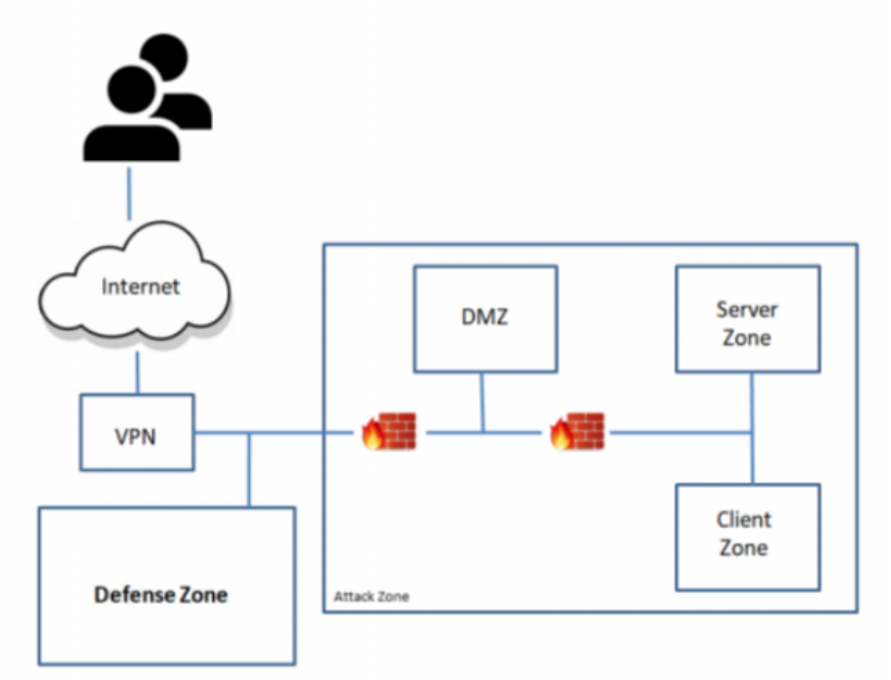
- Web Application
- Digital Forensic
- Reverse Engineering & Pwnable
- Network Security
- Mobile Security
- Programming
- Cryptography

ระยะเวลาการแข่งขัน : วันเสาร์ที่ 16 กันยายน 2566 เวลา 09:00 – 16:00 น. (รวมเวลา 7 ชั่วโมง) UPDATE!

Introduction

รอบชิงชนะเลิศ

เป็นการแข่งขัน CTF Jeopardy ในรูปแบบ Attack the virtual World โดยผู้เข้าแข่งขันต้องหาคำตอบจากเครื่องแม่ข่าย เครื่องผู้ใช้งาน และอุปกรณ์เครือข่ายต่าง ๆ ที่อยู่ในระบบจำลอง ด้วยการโจมตีจากภายนอก และต้องหาคำตอบจากร่องลอยในเครื่องแม่ข่ายที่ถูกโจมตี



รูปภาพ Diagram : การแข่งขัน CTF Jeopardy ในรูปแบบ Attack the virtual World

ระยะเวลาการแข่งขัน : วันเสาร์ที่ 30 กันยายน 2566 เวลา 09:00 – 16:00 น. (รวมเวลา 7 ชั่วโมง) UPDATE!

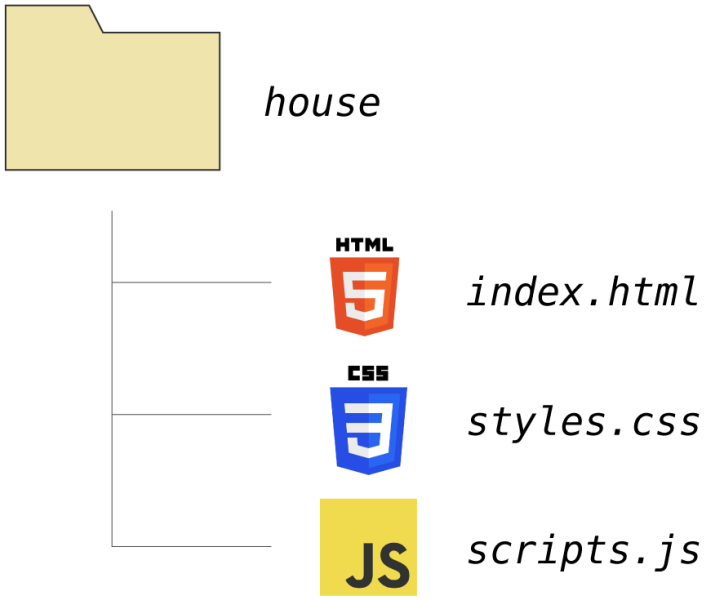
เกณฑ์การตัดสิน : ทีมที่ทำคะแนนได้สูงสุดและส่งคำตอบเร็วที่สุด

Web Application

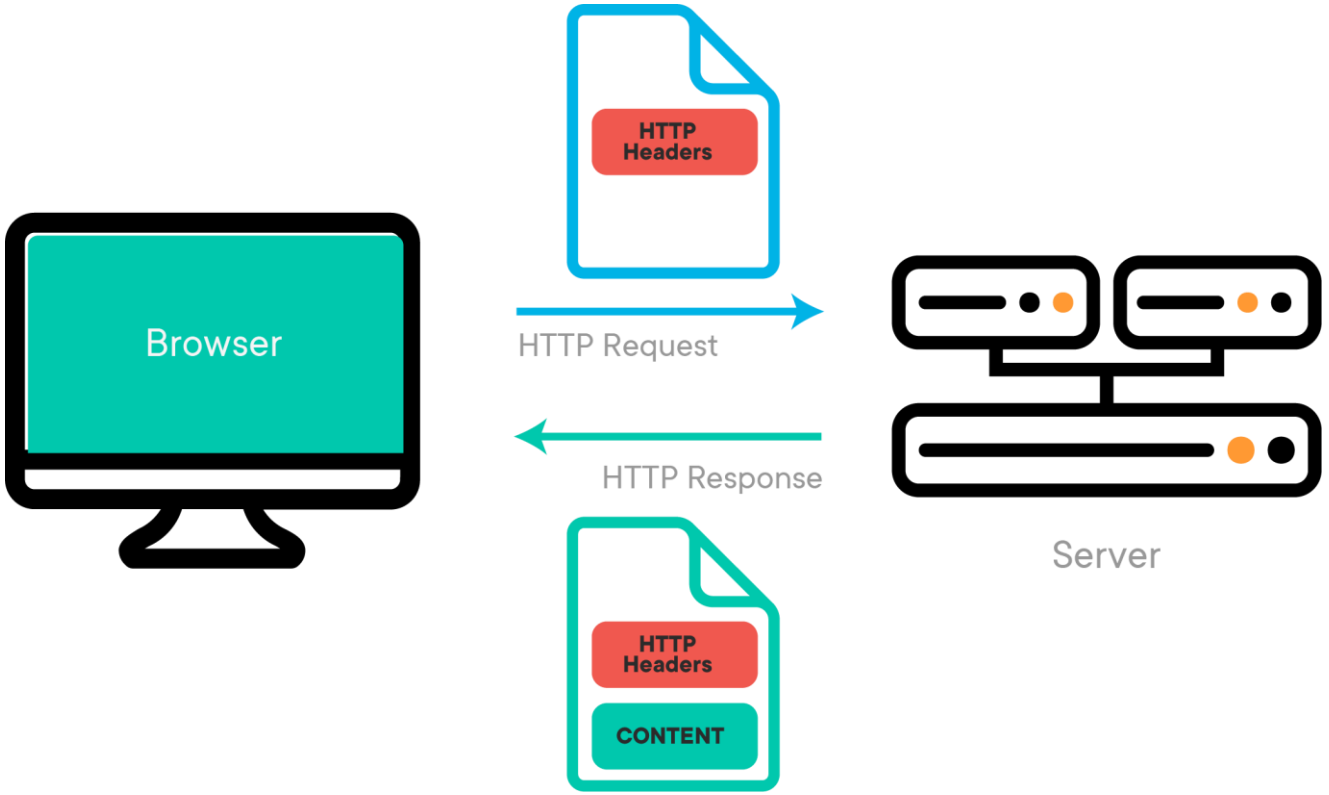
Web Application is application software that is accessed using a web browser. Web applications are delivered on the World Wide Web to users with an active network connection.[Wikipedia]

Web Application

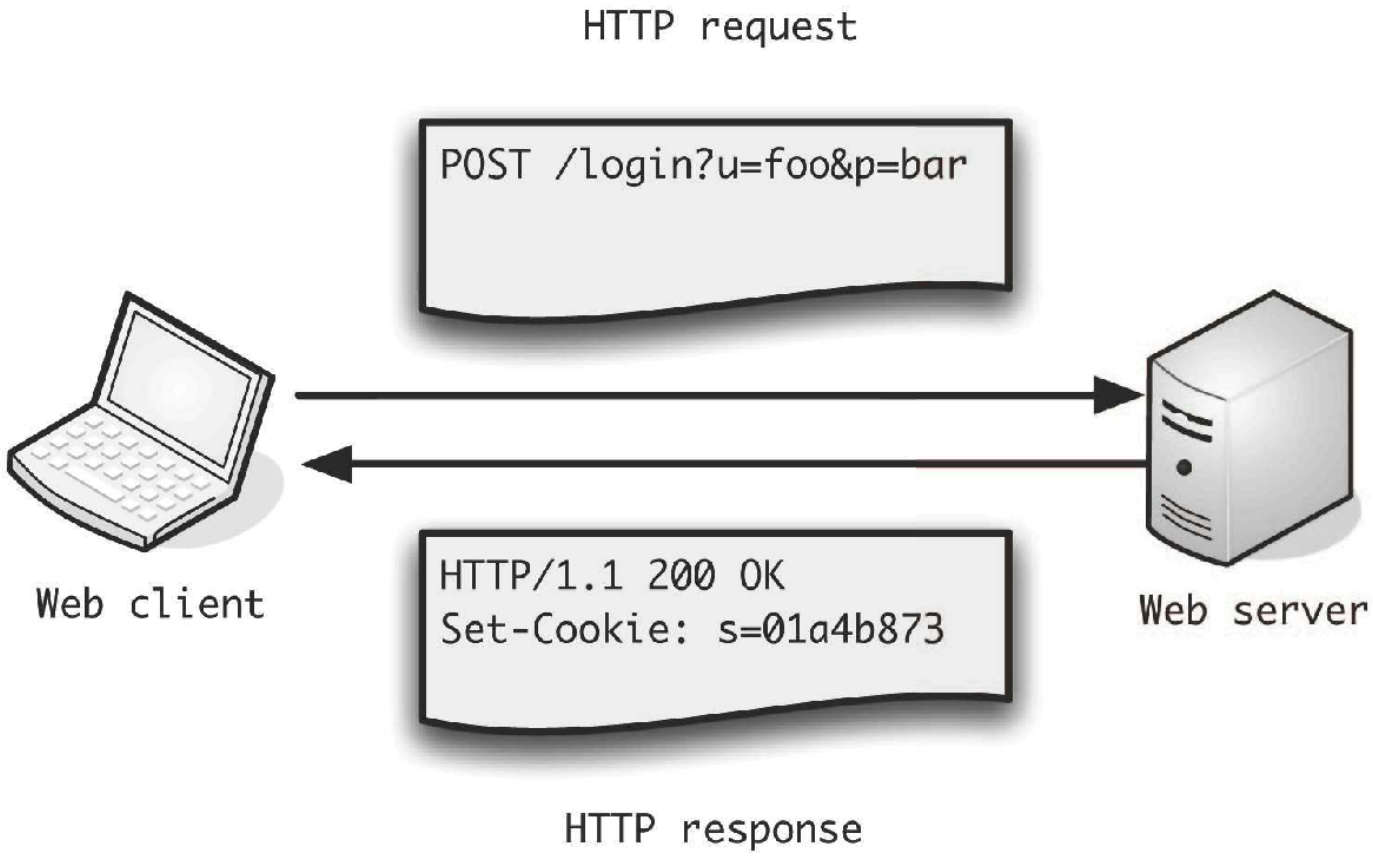
Web application ?



Web Application

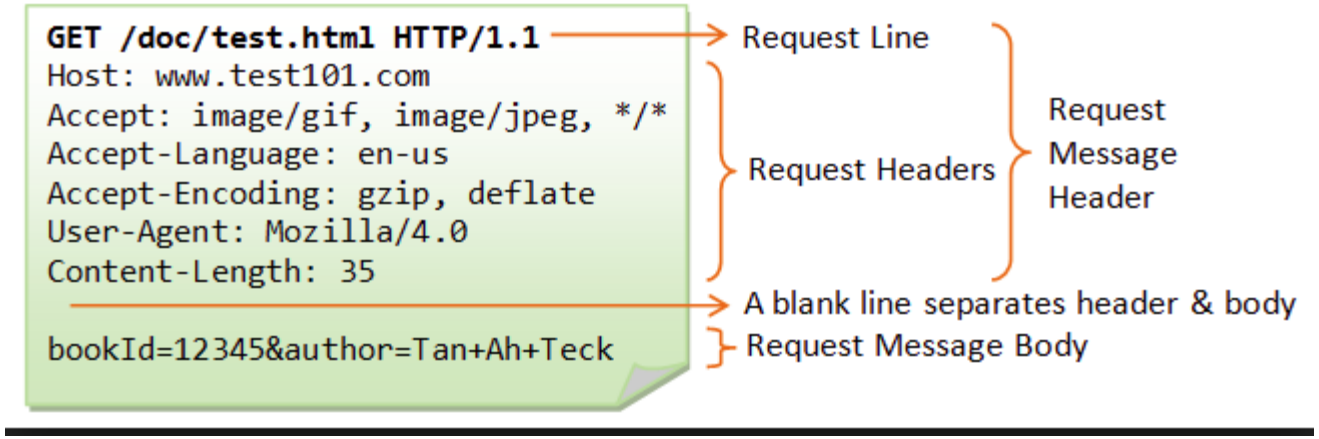


Web Application



Web Application

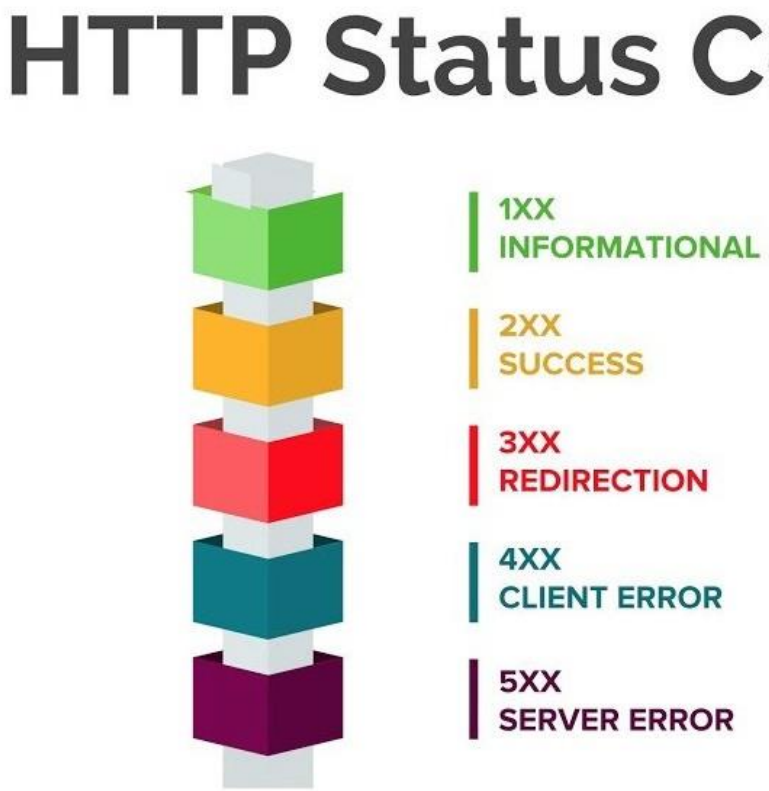
HTTP Request



GET	HTTP/1.1 MUST IMPLEMENT THIS METHOD
HEAD	INSPECT RESOURCE HEADERS
PUT	DEPOSIT DATA ON SERVER – INVERSE OF GET
POST	SEND INPUT DATA FOR PROCESSING
PATCH	PARTIALLY MODIFY A RESOURCE
TRACE	ECHO BACK RECEIVED MESSAGE
OPTIONS	SERVER CAPABILITIES
DELETE	DELETE A RESOURCE – NOT GUARANTEED

Web Application

HTTP Response



1XX Informational	
100	Continue
101	Switching Protocols
102	Processing

2XX Success	
200	OK
201	Created
202	Accepted
203	Non-authoritative Information
204	No Content
205	Reset Content
206	Partial Content
207	Multi-Status
208	Already Reported
226	IM Used

3XX Redirectional	
300	Multiple Choices
301	Moved Permanently
302	Found
303	See Other
304	Not Modified
305	Use Proxy
307	Temporary Redirect
308	Permanent Redirect

4XX Client Error	
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout

4XX Client Error Continued	
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Payload Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Requested Range Not Satisfiable
417	Expectation Failed
418	I'm a teapot
421	Misdirected Request
422	Unprocessable Entity
423	Locked
424	Failed Dependency
426	Upgrade Required
428	Precondition Required
429	Too Many Requests
431	Request Header Fields Too Large
444	Connection Closed Without Response
451	Unavailable For Legal Reasons
499	Client Closed Request

5XX Server Error	
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not Supported
506	Variant Also Negotiates
507	Insufficient Storage
508	Loop Detected
510	Not Extended
511	Network Authentication Required
599	Network Connect Timeout Error

Web Application

BURPSUITE

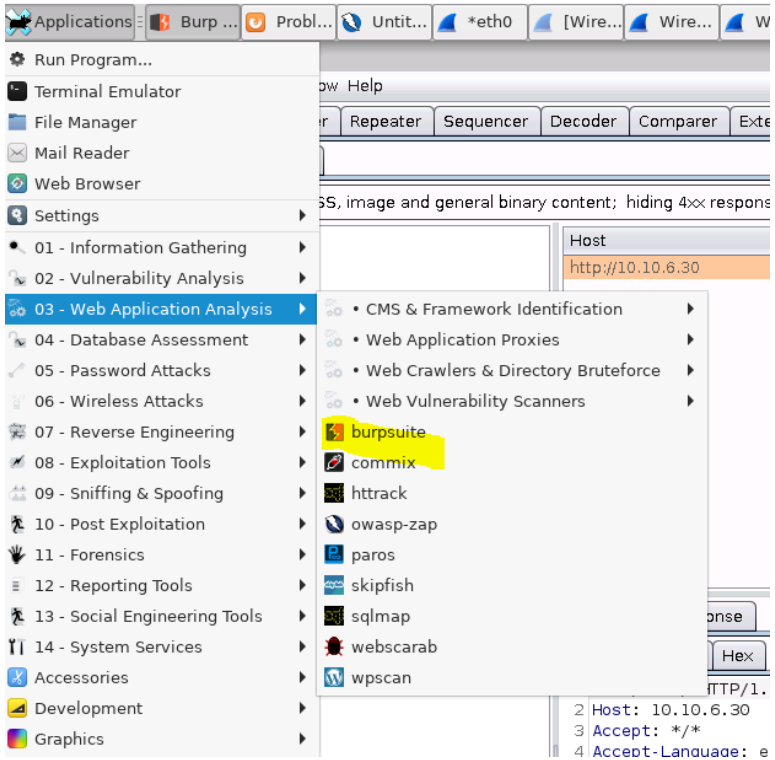
- **Site Map**
- HTTP History
- Scope
- Intercepter
- Repeater
- Intruder
- Spider
- Scanner
- BApp Store

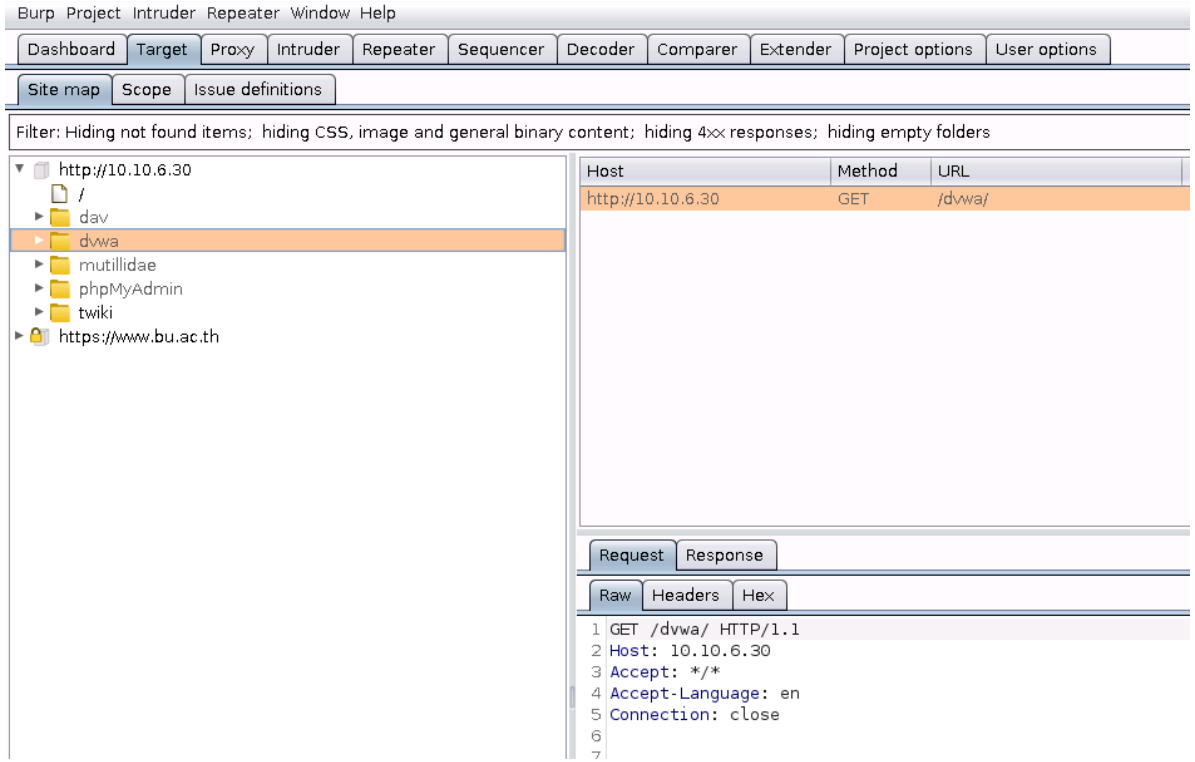
ZAP

- **Site Tree**
- History
- Context
- Break
- Request Editor
- Fuzzer
- Spider
- Active Scan
- Add On Marketplace

Web Application

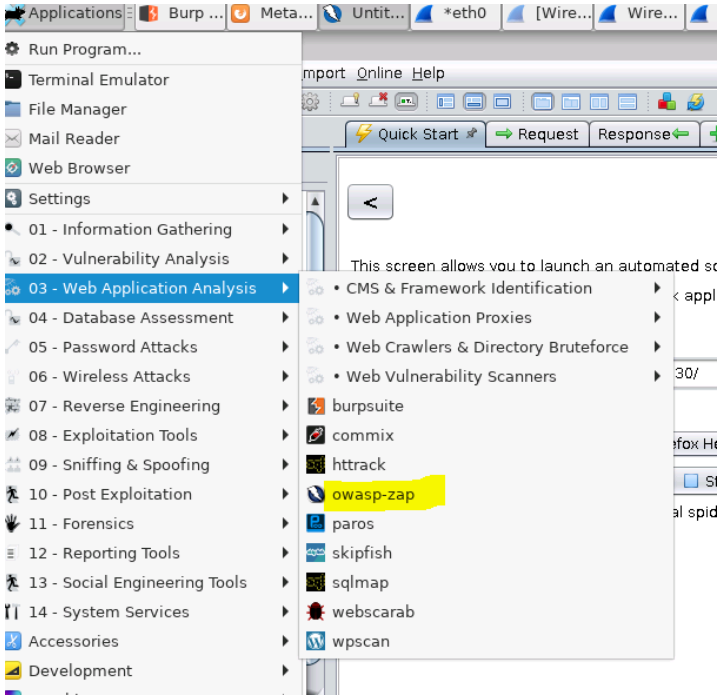
- Menu → 03 Web Application Analysis → burpsuit

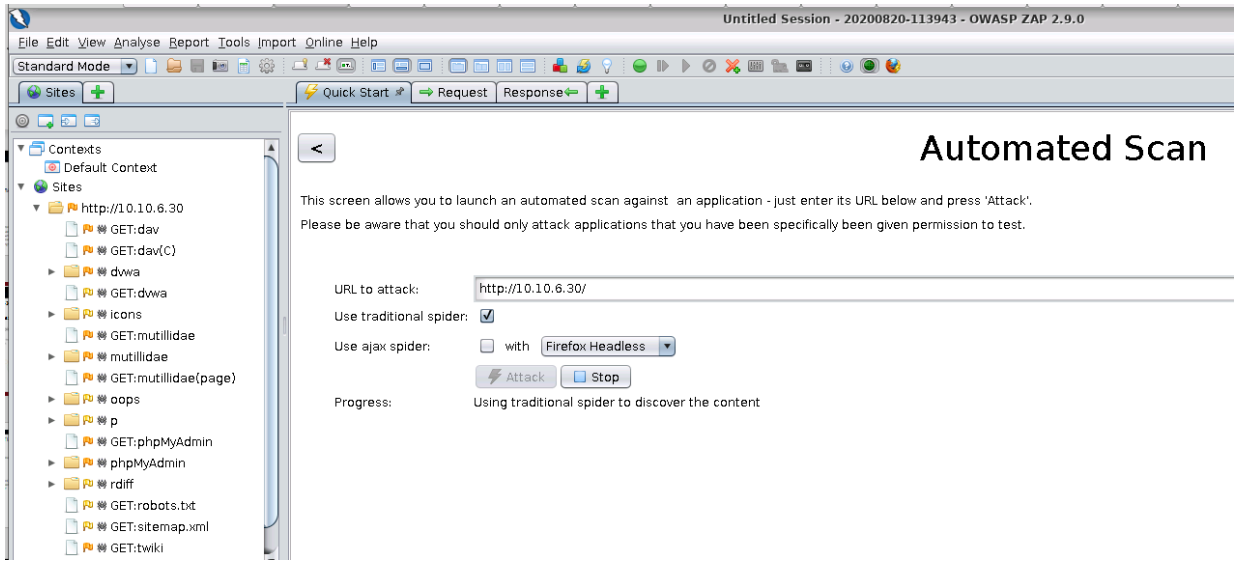




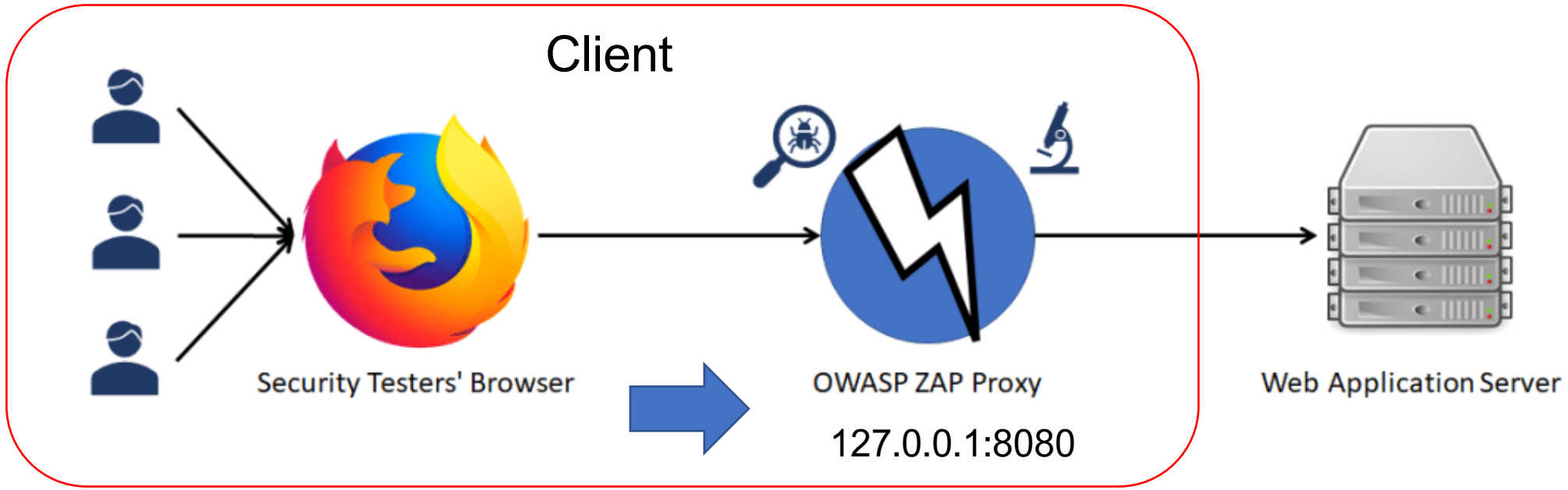
Web Application

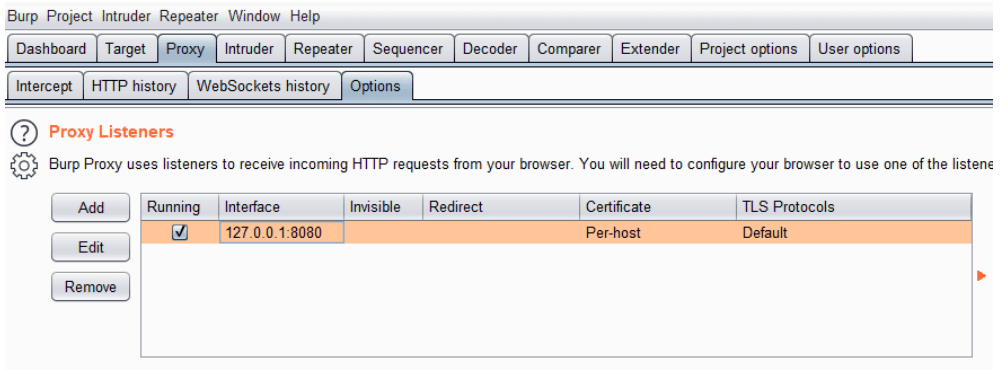
- Menu → 03 Web Application Analysis → OWASP-Zap





Web Application

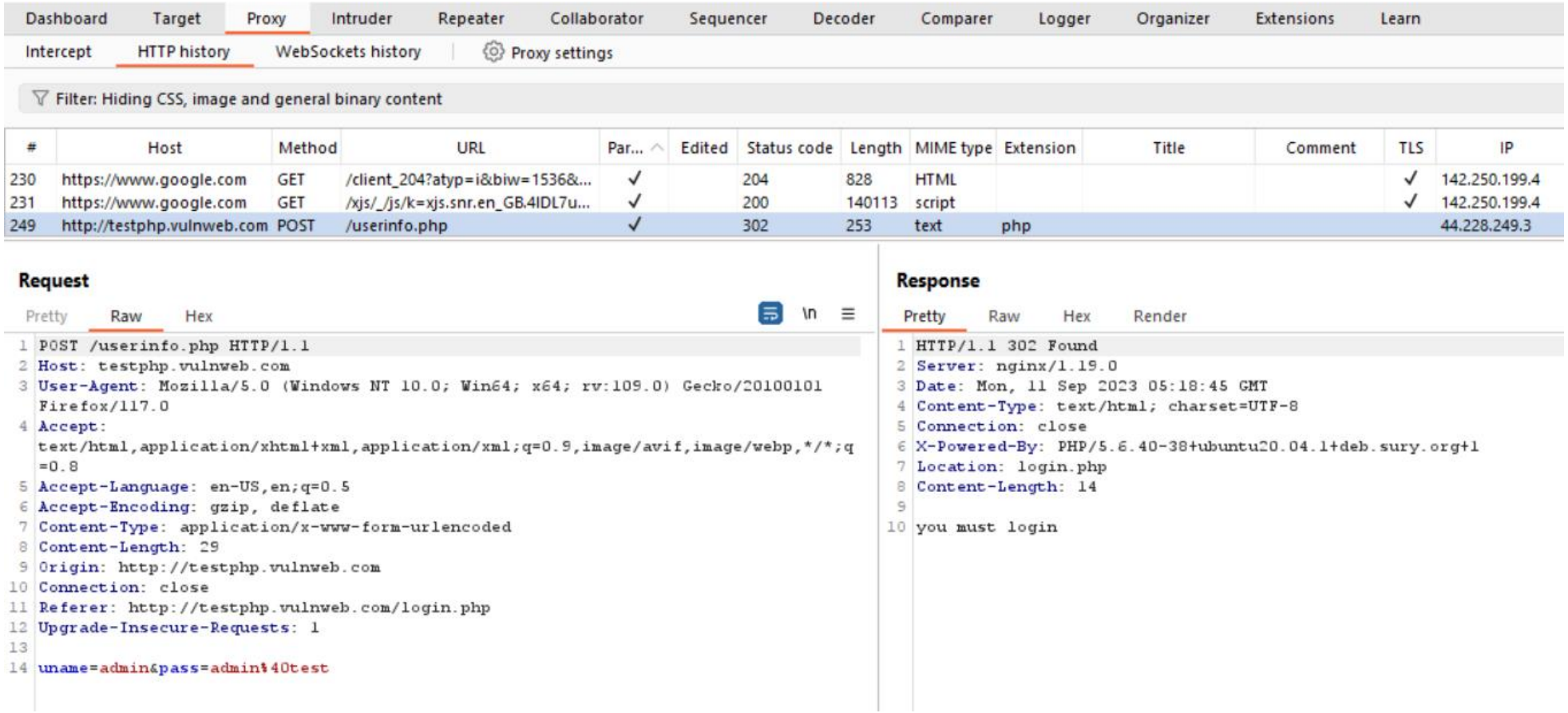




Tip: ให้ระวังเรื่อง Port ที่ใช้งานอยู่

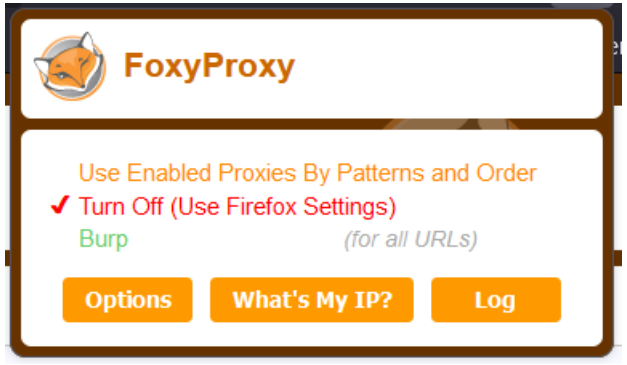
Web Application

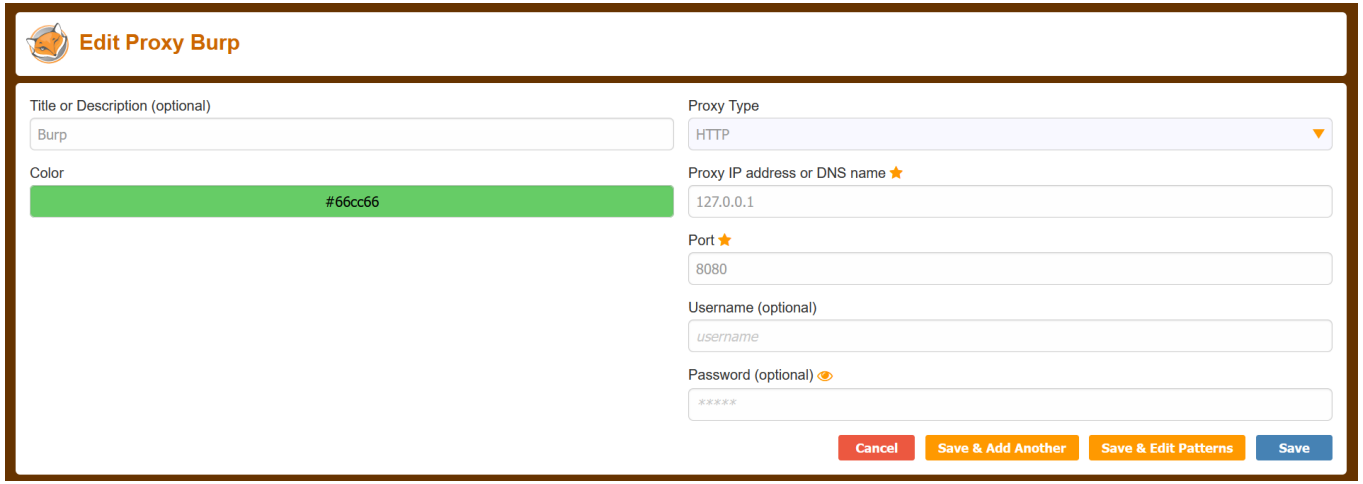
ตรวจสอบการเข้าใช้งาน ดูค่า HTTP request/response ผ่านเมนู HTTP history



Web Application

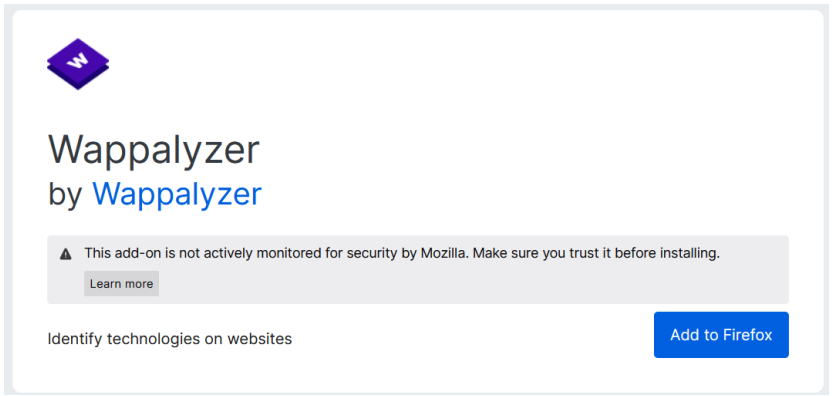
Useful extensions : FoxyProxy

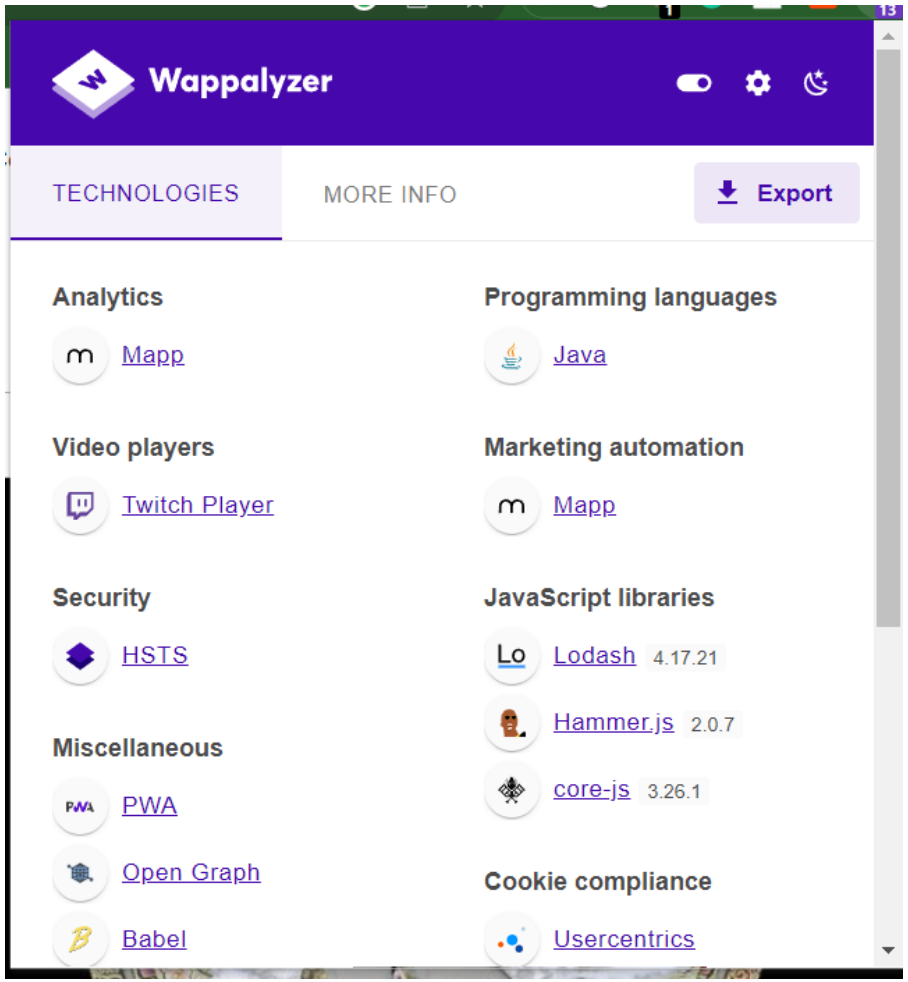




Web Application

Useful extensions : Wappanlyzer

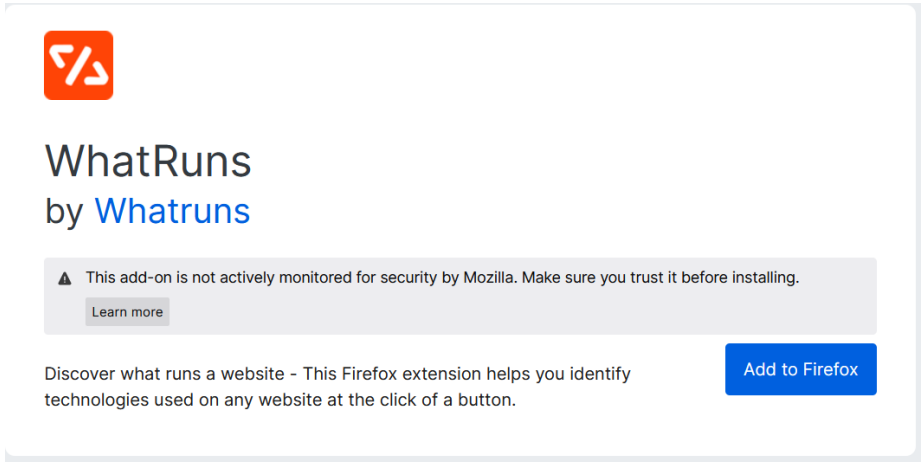


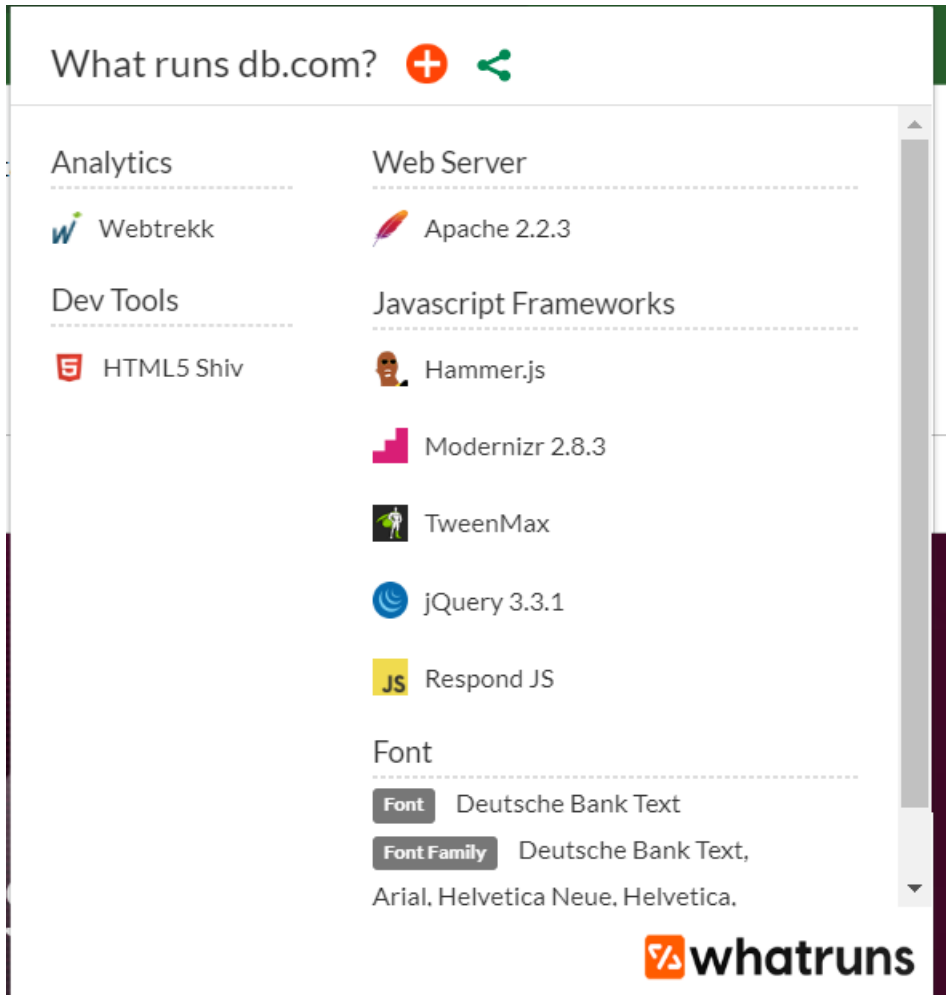


Tip: บางครั้งต่าง Web browser (Chrome, Firefox) อาจจะแสดงค่าต่างกันเล็กน้อย ดังนั้นควร Cross-check เสมอ

Web Application

Useful extensions : whatruns



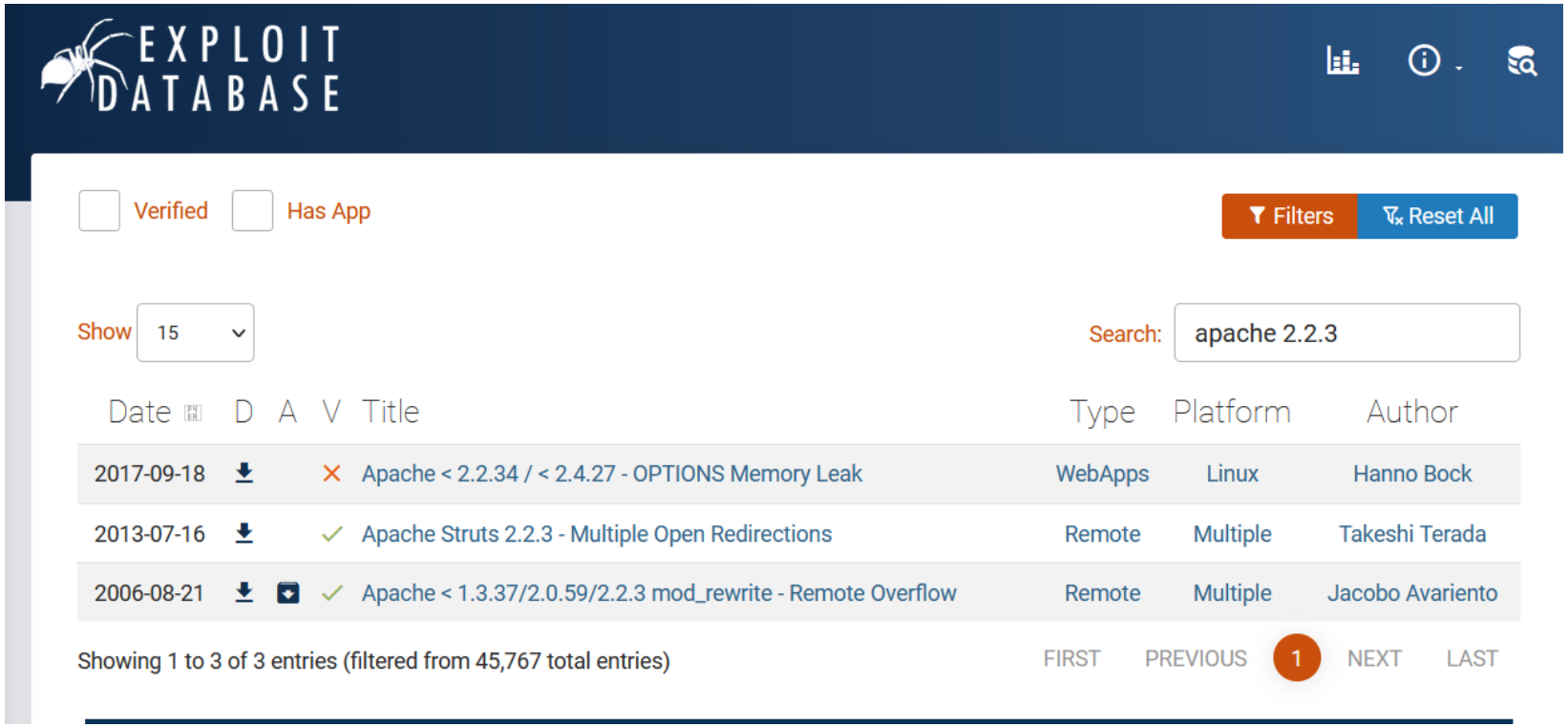


Tip: บางครั้งต่าง Web browser (Chrome, Firefox) อาจจะแสดงค่าต่างกันเล็กน้อย ดังนั้นควร Cross-check เสมอ

Web Application

Search public exploit code

- https://www.exploit-db.com/



Web Application

Search web directory and file extension

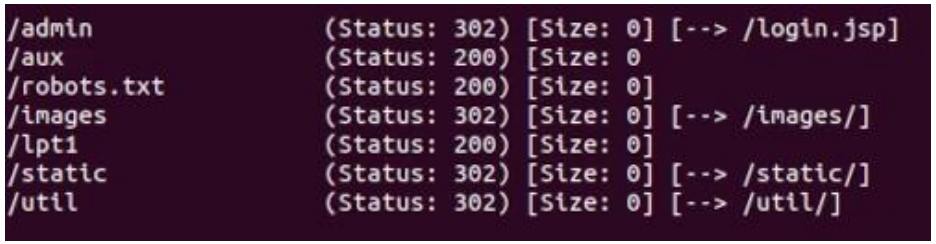
- Gobuster quick directory busting

  #gobuster dir -u target -w /usr/share/seclists/Discovery/Web_Content/common.txt -t 80 -a Linux

- Gobuster search with file extension

  #gobuster dir -u target -w /usr/share/seclists/Discovery/Web_Content/common.txt -t 80 -x .txt,.php

  #gobuster dir -u target -w /usr/share/seclists/Discovery/Web_Content/common.txt -t 80 -x .asp,aspx

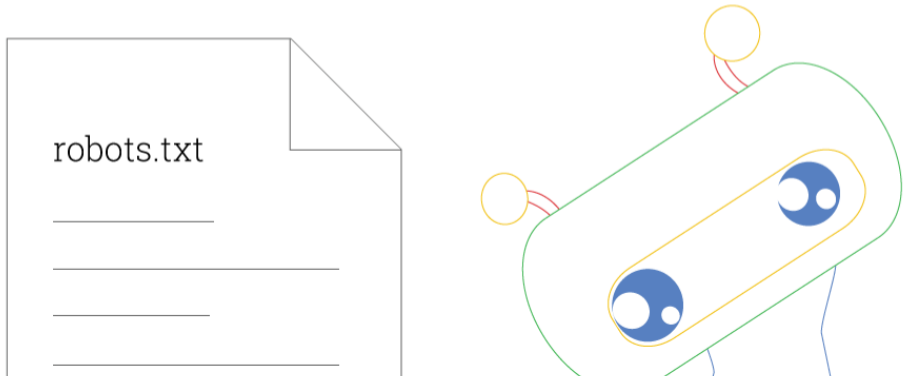


Web Application

- `www.yourwebsite.com/robots.txt`

Search engine spiders

The first thing a search engine spider like Googlebot looks at when it is visiting a page is the robots.txt file.



Allow full access

```
User-agent: *
Disallow:
```

Block all access

```
User-agent: *
Disallow: /
```

Block one folder

```
User-agent: *
Disallow: /folder/
```

Block one file

```
User-agent: *
Disallow: /file.html
```


Web Application

Useful wordlist : /usr/share/wordlists/

Wordlists Usage Examples

```
root@kali:~# ls -lh /usr/share/wordlists/
total 51M
lrwxrwxrwx 1 root root  25 Jan  3 13:59 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root  30 Jan  3 13:59 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root  35 Jan  3 13:59 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root  41 Jan  3 13:59 fasttrack.txt -> /usr/share/set/src/fasttrack/wor
lrwxrwxrwx 1 root root  45 Jan  3 13:59 fern-wifi -> /usr/share/fern-wifi-cracker/extras/
lrwxrwxrwx 1 root root  46 Jan  3 13:59 metasploit -> /usr/share/metasploit-framework/dat
lrwxrwxrwx 1 root root  41 Jan  3 13:59 nmap.lst -> /usr/share/nmap/nselib/data/passwords
-rw-r--r-- 1 root root 51M Mar  3  2013 rockyou.txt.gz
lrwxrwxrwx 1 root root  34 Jan  3 13:59 sqlmap.txt -> /usr/share/sqlmap/txt/wordlist.txt
lrwxrwxrwx 1 root root  25 Jan  3 13:59 wfuzz -> /usr/share/wfuzz/wordlist
root@kali:~#
root@kali:~# gunzip /usr/share/wordlists/rockyou.txt.gz
root@kali:~#
root@kali:~# wc -l /usr/share/wordlists/rockyou.txt; ls -lah /usr/share/wordlists/rockyou
14344392 /usr/share/wordlists/rockyou.txt
-rw-r--r-- 1 root root 134M Mar  3  2013 /usr/share/wordlists/rockyou.txt
root@kali:~#
```


Web Application

Powerful wordlist : seclists

seclists

SecLists is a collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many more.

The goal is to enable a security tester to pull this repo onto a new testing box and have access to every type of list that may be needed.

Installed size: `1.63 GB`
How to install: `sudo apt install seclists`

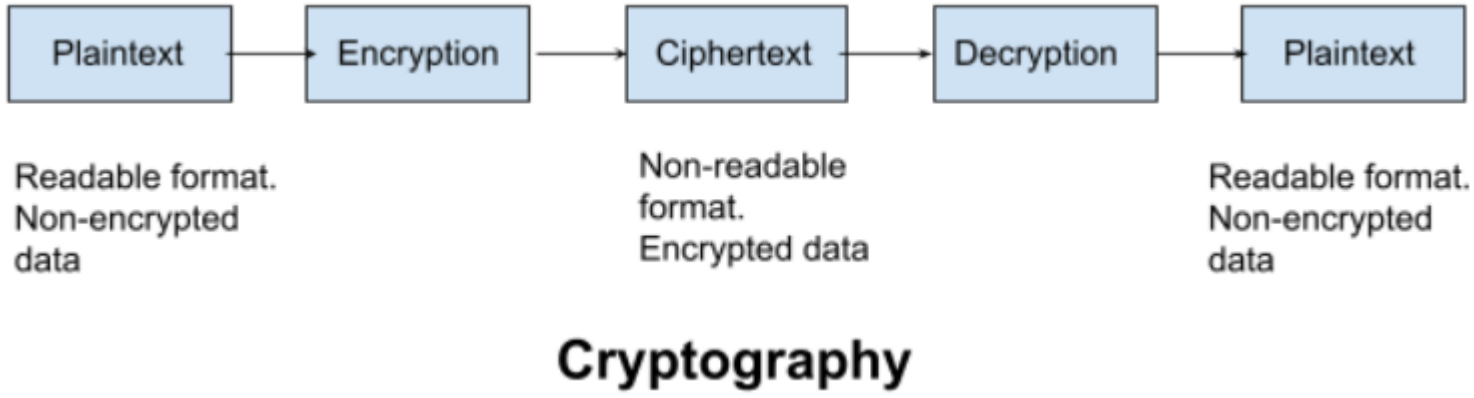
```
root@kali:~# seclists -h

> seclists ~ Collection of multiple types of security lists

/usr/share/seclists
|-- Discovery
|-- Fuzzing
|-- IOCs
|-- Miscellaneous
|-- Passwords
|-- Pattern-Matching
|-- Payloads
|-- Usernames
`-- Web-Shells
```

Cryptography

Cryptography is the process of encryption or decryption of messages and data.



Cryptography

Cryptography

จูเลียส ซีซาร์ (Julius Caesar)

อดีตผู้เผด็จการโรมัน

กาอิอุส ยูลิอุส ไกซาร์ หรือ จูเลียส ซีซาร์ เป็นรัฐบุรุษ แม่ทัพ และผู้ประพันธ์ร้อยแก้วอันเลื่องชื่อชาวโรมัน เขามีบทบาทสำคัญในเหตุการณ์อันนำไปสู่การสิ้นสุดสาธารณรัฐโรมันและความเจริญของจักรวรรดิโรมัน ใน 60 ปีก่อน ค.ศ. วิกิพีเดีย

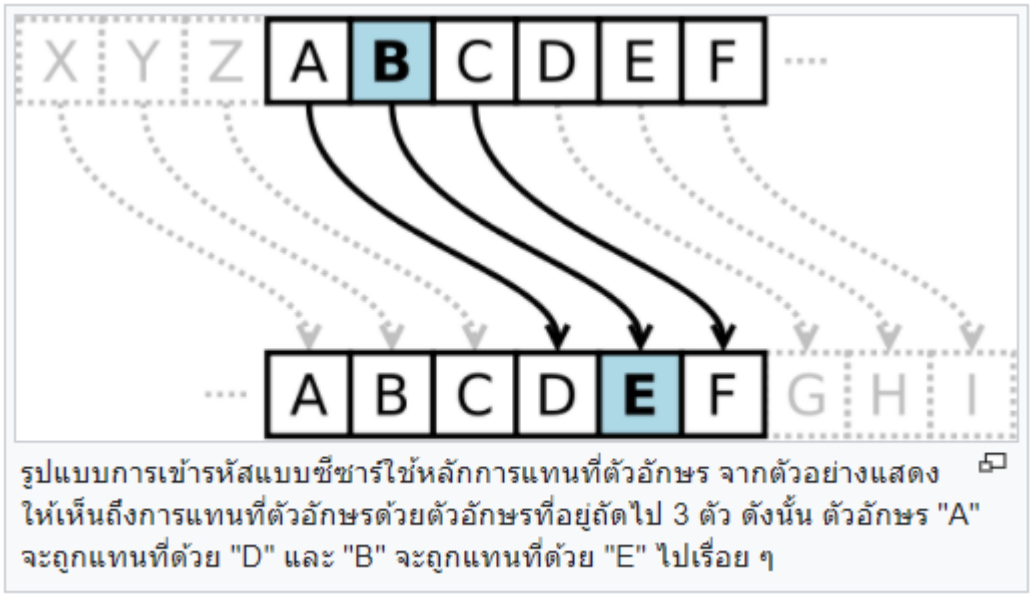
เกิด: 12 กรกฎาคม พ.ศ. 444, โรม, อิตาลี

ถูกลอบสังหาร: 15 มีนาคม พ.ศ. 500, Largo di Torre Argentina, โรม, อิตาลี

ภาพยนตร์: Caesar the Conqueror

คู่สมรส: คอร์เนเลีย (สมรส พ.ศ. 460), ป็อมเปยา (สมรส พ.ศ. 477), กัลปูร์นิอา (สมรส พ.ศ. 485–พ.ศ. 500)

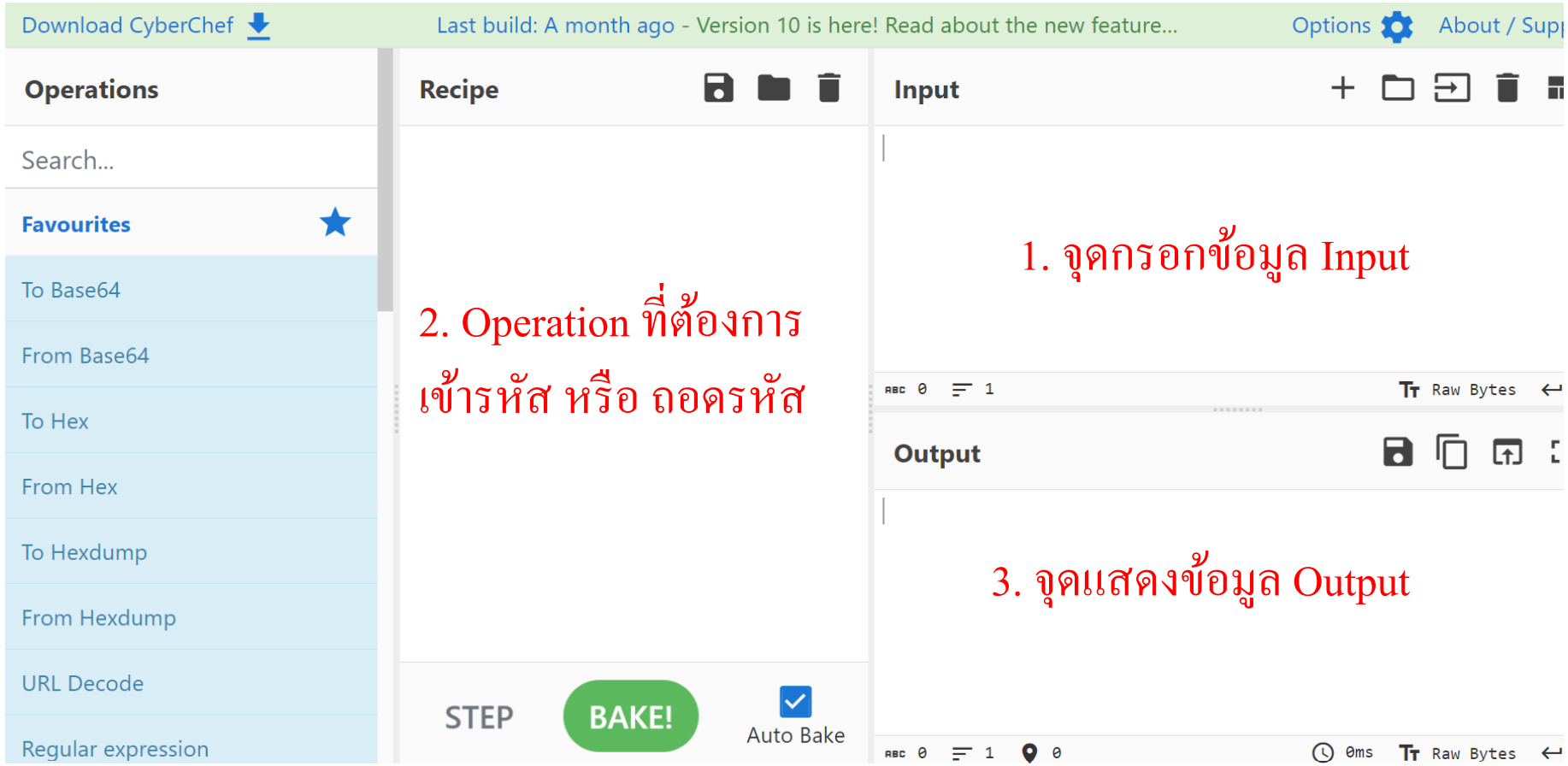
บุตร: จักรพรรดิเอากุสตุส, ทอเลมีที่ 15 ซีซาเรียน, จูเลีย ซีซาริส



รูปแบบการเข้ารหัสแบบซีซาร์ใช้หลักการแทนที่ตัวอักษร จากตัวอย่างแสดงให้เห็นถึงการแทนที่ตัวอักษรด้วยตัวอักษรที่อยู่ถัดไป 3 ตัว ดังนั้น ตัวอักษร "A" จะถูกแทนที่ด้วย "D" และ "B" จะถูกแทนที่ด้วย "E" ไปเรื่อย ๆ

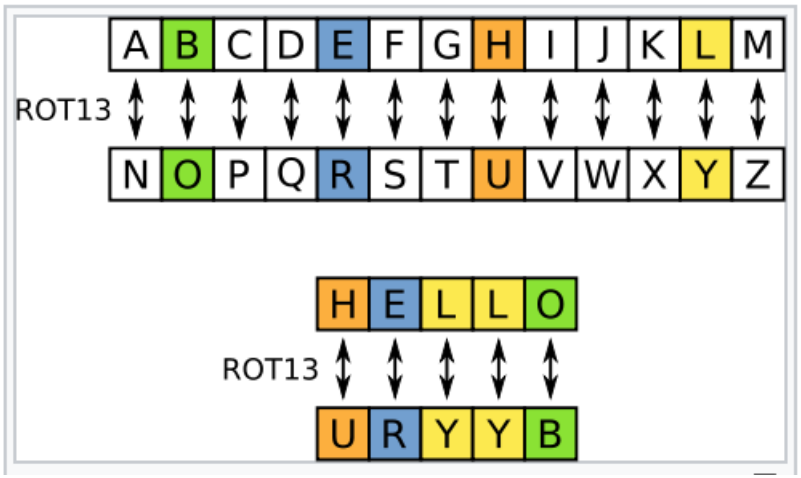
Cryptography

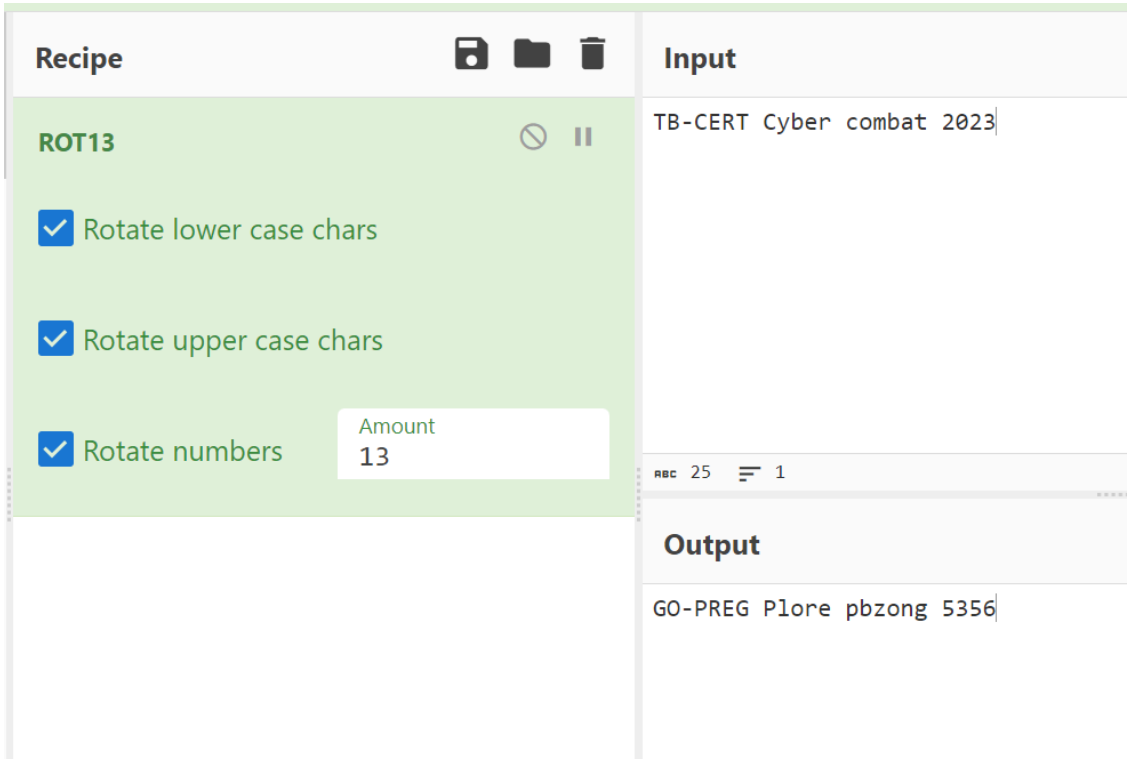
Tool: CyberChef
https://gchq.github.io



Cryptography

- **ROT13** ("**rotate by 13 places**", sometimes hyphenated **ROT-13**) is a simple letter substitution cipher that replaces a letter with the 13th letter after it, in the alphabet. ROT13 is a special case of the Caesar cipher which was developed in ancient Rome.



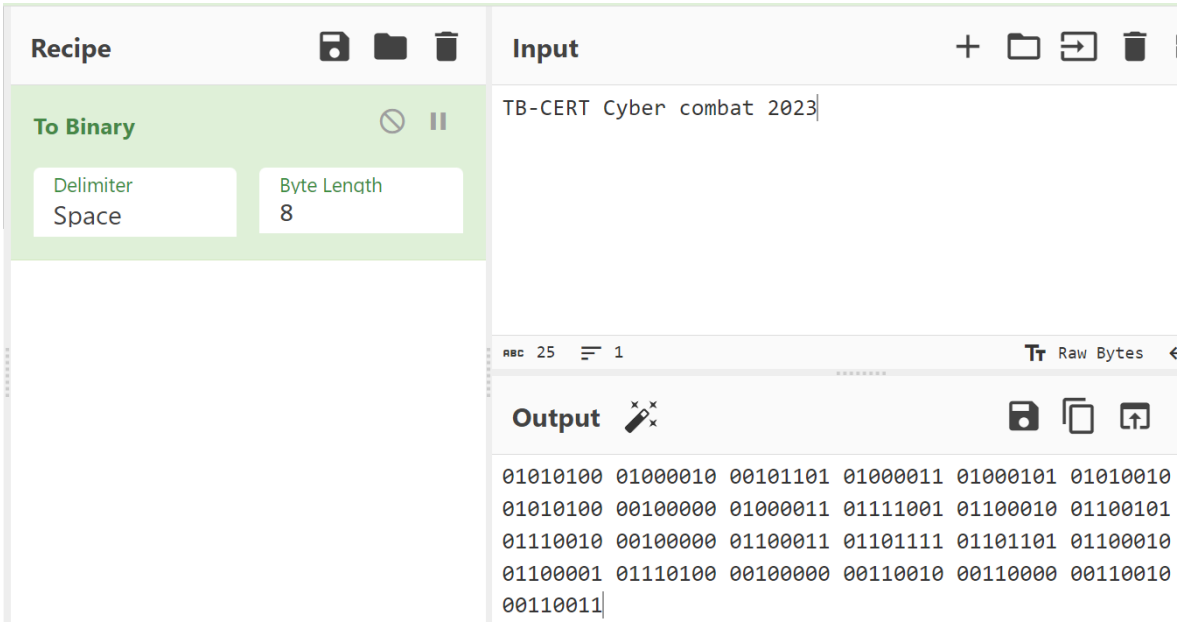


Cryptography

- **Binary** is a number expressed in the base-2 numeral system or binary numeral system, a method of mathematical expression which uses only two symbols: typically **"0"** and **"1"**

Binary Code

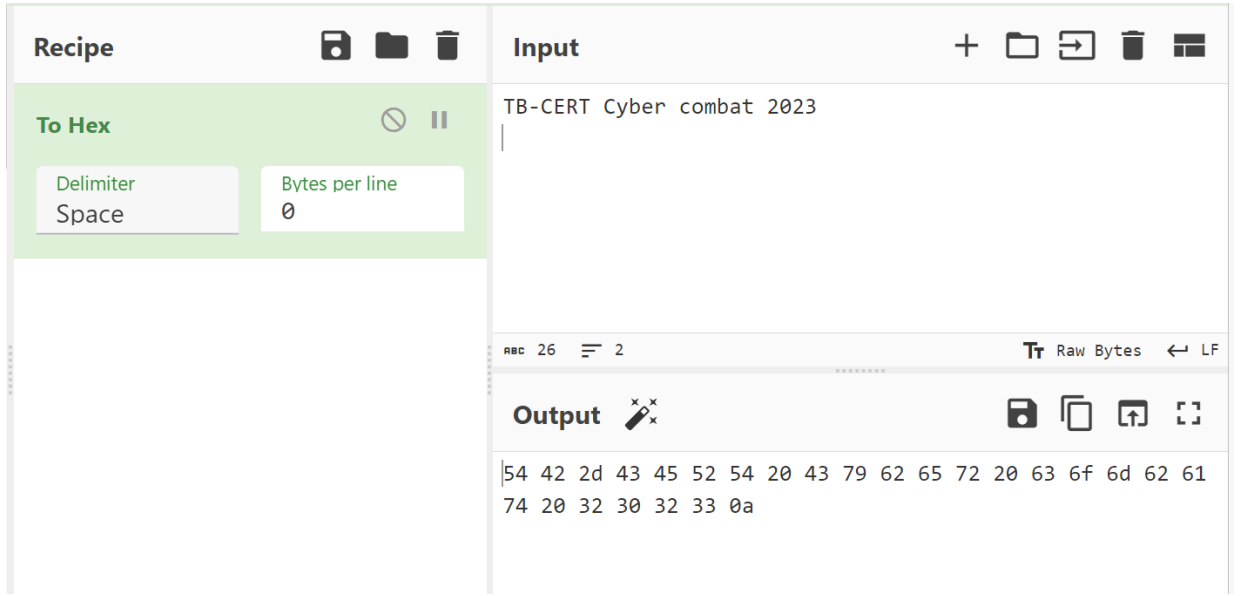
A	100 0001	H	100 1000	O	100 1111	V	101 0110
B	100 0010	I	100 1001	P	101 0000	W	101 0111
C	100 0011	J	100 1010	Q	101 0001	X	101 1000
D	100 0100	K	100 1011	R	101 1010	Y	101 1001
E	100 0101	L	100 1100	S	101 0011	Z	101 1010
F	100 0110	M	100 1101	T	101 0100	a	110 0001
G	100 0111	N	100 1110	U	101 0101	b	110 0010



Cryptography

- **Hex** is a numeral system made up of 16 symbols (base 16). Hexadecimal uses the decimal numbers and six extra symbols. 0,1,2,3,4,5,6,7,8,9, A, B, C, D, E and F.

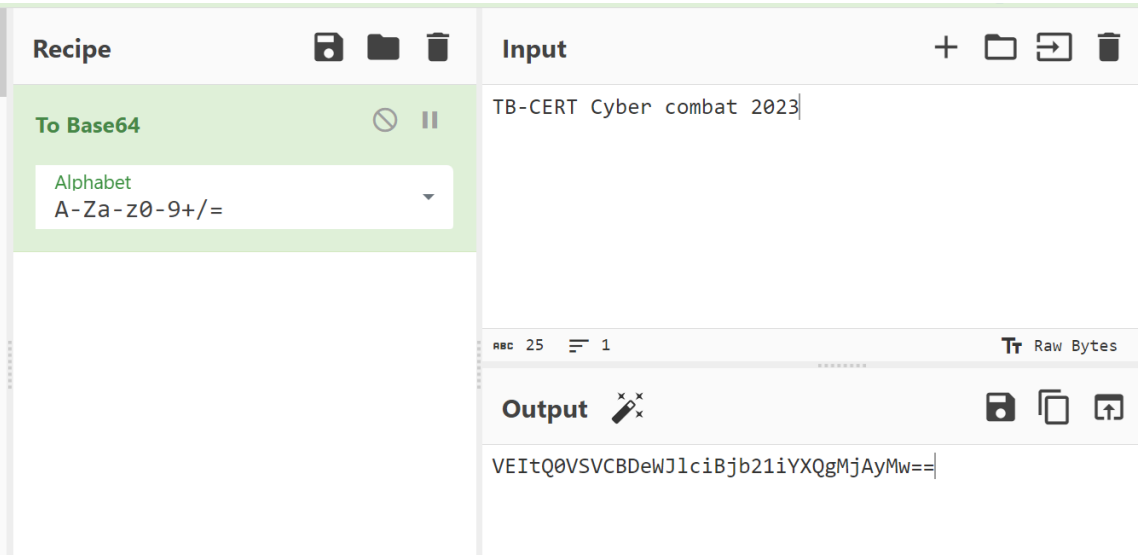
Hex	Binary	Octal	Decimal
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
A	1010	12	10
B	1011	13	11
C	1100	14	12
D	1101	15	13
E	1110	16	14
F	1111	17	15



Cryptography

- **Base64** is designed to carry data stored in binary formats across channels that only reliably support text content. Base64 is particularly prevalent on the World Wide Web where one of its uses is the ability to embed image files or sending e-mail attachments.

Source	**Text (ASCII)**	**M**							**a**																				
	Octets	77 (0x4d)							97 (0x61)																				
Bits		0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0										
Base64 encoded	**Sextets**	19							22						4					Padding									
	Character	**T**							**W**						**E**					**=**									
	Octets	84 (0x54)							87 (0x57)						69 (0x45)					61 (0x3D)									



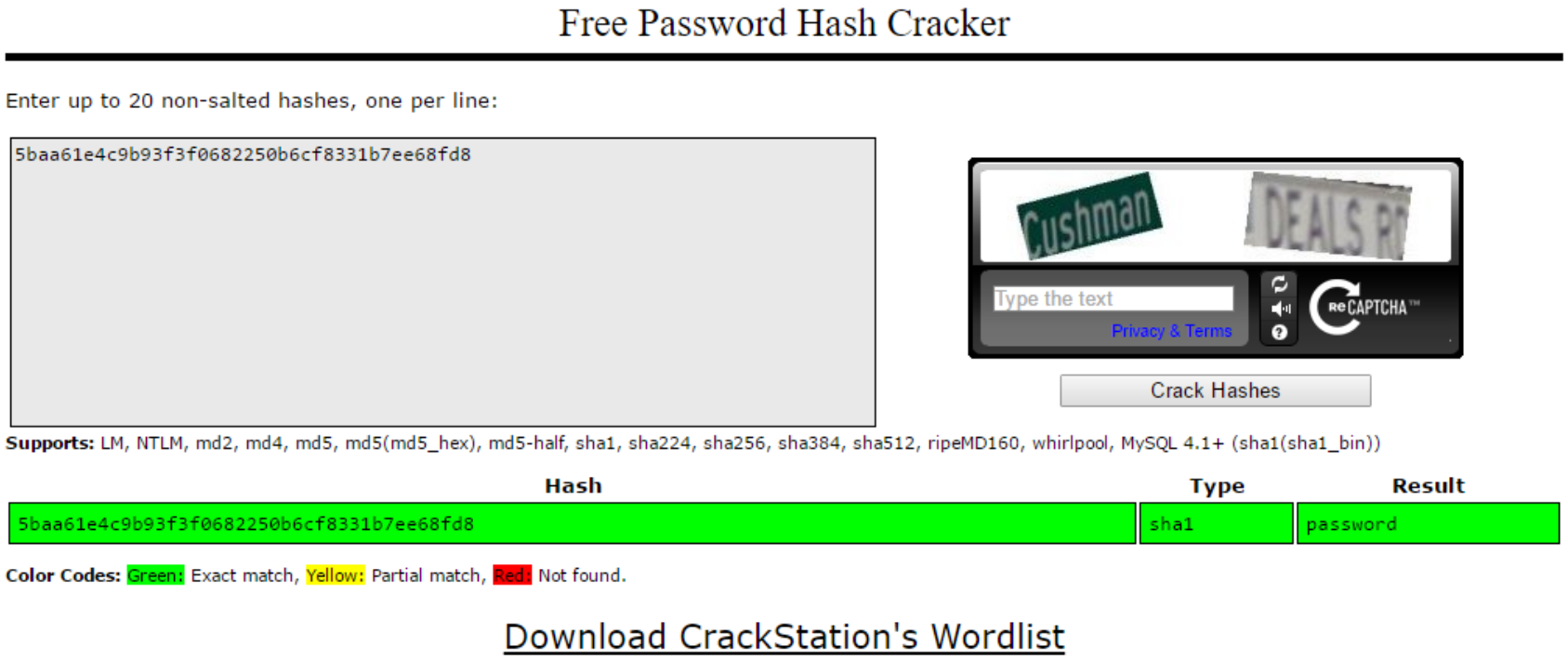
Cryptography

- **HASH** is any function that can be used to map data of arbitrary size to fixed-size values, though there are some hash functions that support variable length output.

Cryptography

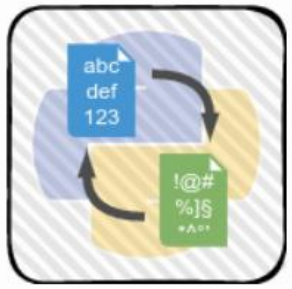
Tool: Crack Station
https://crackstation.net

- **HASH sha1** is a hash function which takes an input and produces a 160-bit hash value known as a message digest



Cryptography

Tool: Crack Station
Install: sudo pip install codext



CodExt Tweet

Encode/decode anything.

CodExt is a (Python2-3 compatible) library that extends the native codecs library (namely for adding new custom encodings and character mappings) and provides 120+ new codecs, hence its name combining CODecs EXTension. It also features a guess mode for decoding multiple layers of encoding and CLI tools for convenience.

Example:

```
┌──(kali㉿atmin)-[~]
└─$ echo -en "KZCUS5CRGBLFGVSDIJGWEM22NREUOVRSLJMEUNLCGI2WY====" | codext decode base32 base64
TB-CERT Love everyone

┌──(kali㉿atmin)-[~]
└─$
```

Cryptography

Morse code is a method used in telecommunication to encode text characters as standardized sequences of two different signal durations, called dots and dashes, or dits and dahs.

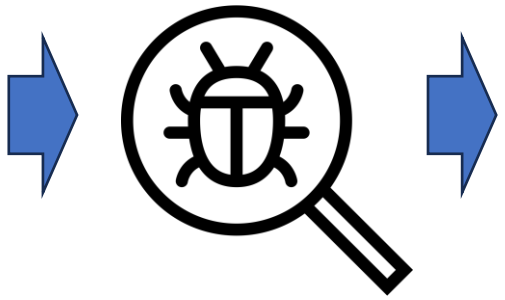
Online Tools
https://morsedecoder.com/
https://www.morsecode-translator.com
https://morsecode.world/international/decoder/audio-decoder-adaptive.html

Reverse engineering

Reverse Engineering is typically the process of taking a compiled (machine code, bytecode) program and converting it back into a more human readable format.

Executable or binary file

- PE File (.exe or .dll)
- ELF File (elf)
- APK File (apk)
- .NET File (exe)

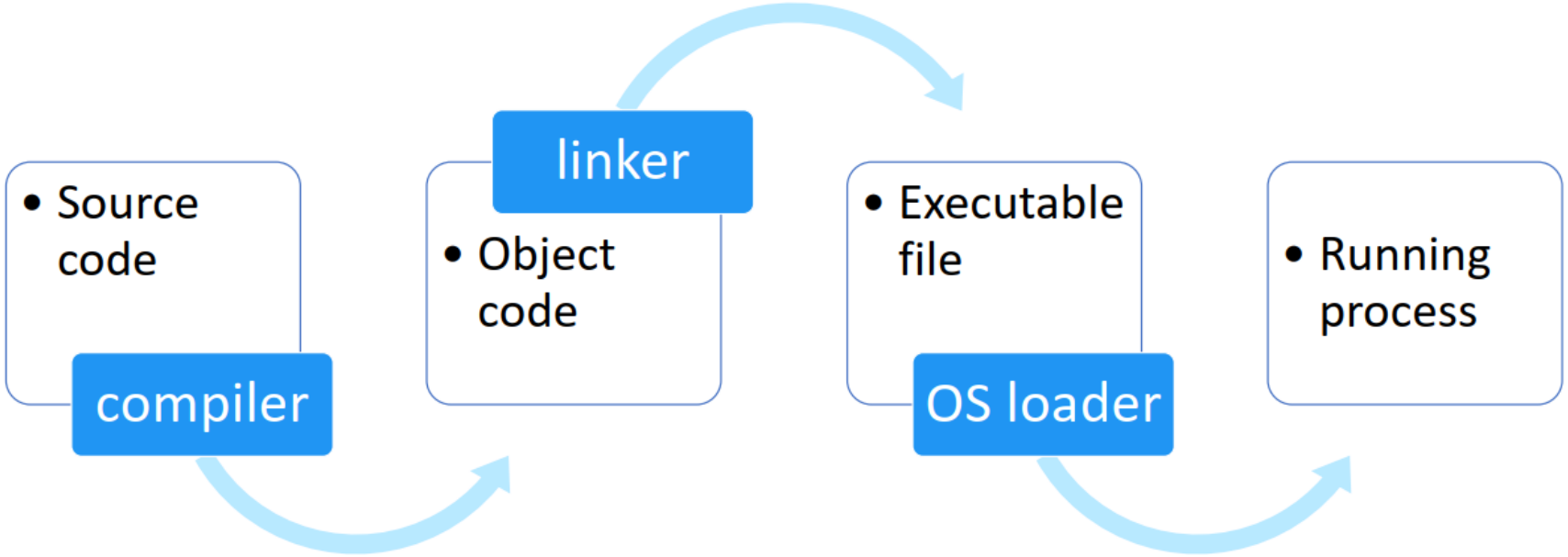


Human readable

- Assembly / Machine Code
- The High-level Programming Language (C, Java)

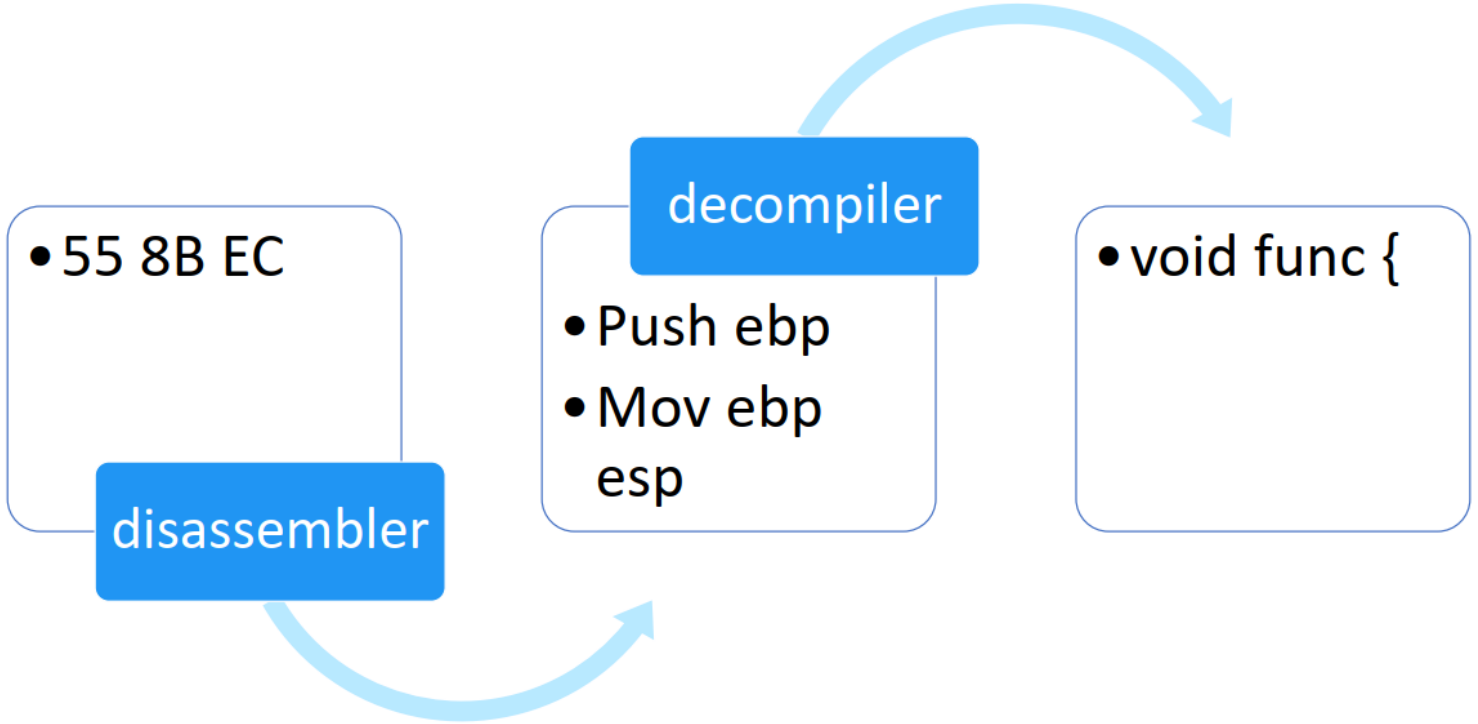
Reverse engineering

Programming cycle



Reverse engineering

Reverse engineering cycle



Reverse engineering

Tool: file
Built-in tool on Kali Linux

file - determine file type

```
┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ file pass_test
pass_test: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),
5055295c4ff1855b83f271caa5, for GNU/Linux 3.2.0, not stripped

┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ file pass_test.c
pass_test.c: C source, ASCII text
```

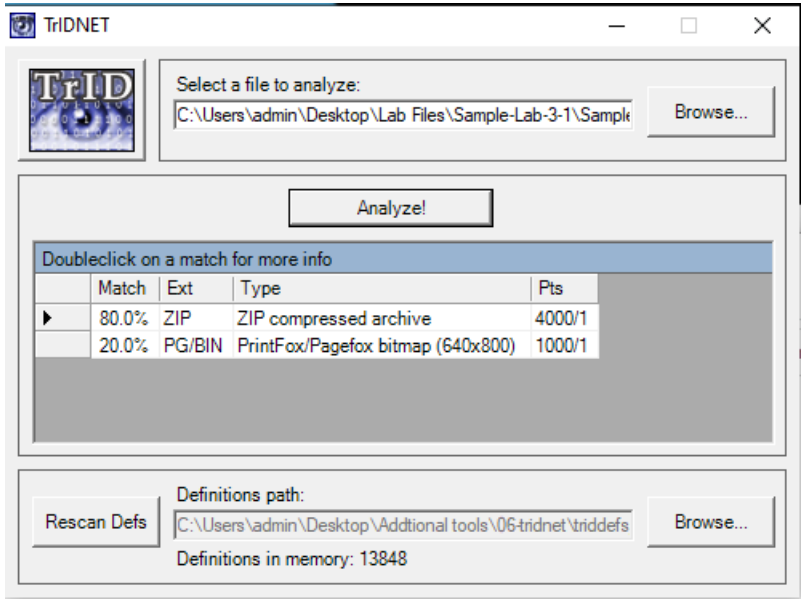
Reverse engineering

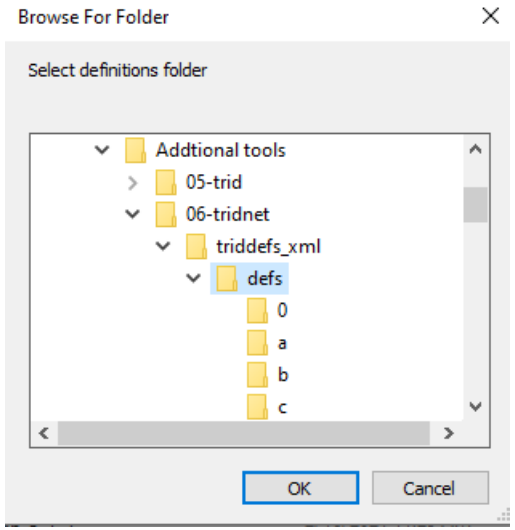
Tool: TrIDNet is an utility designed to identify file types from their binary signatures.
Install: https://mark0.net/soft-tridnet-e.html

TrIDNet - determine file type

Download

.NET	TrIDNet v1.95, 32KB ZIP - (PGP sig)
	TrID XML defs, 1910KB 7z (7-Zip archive with 16462 definitions, 13/08/23)





Reverse engineering

Tool: String
Built-in tool on Kali Linux

strings - print the sequences of printable characters in files

Open with strings

```
┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ strings pass_test
/lib64/ld-linux-x86-64.so.2
PU)\O
putchar
__libc_start_main
__cxa_finalize
syscall
libc.so.6
GLIBC_2.34
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
/etc/passwd
;*3$"
GCC: (Debian 11.2.0-13) 11.2.0
Scrt1.o
```

Open with cat

```
┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ cat pass_test
@@@@◆▒▒▒PP◆◆   ◆◆◆-◆=◆=PX◆-◆=◆=◆888 XXXDDS◆td888
start_main__cxa_finalizesyscalllibc.so.6GLIBC_2.3
◆/H◆◆t◆◆H◆◆◆5◆/◆%◆/@◆%◆/h◆◆◆◆◆◆%◆/h◆◆◆◆◆◆%◆/f◆1◆I
+UH◆=◆.H◆◆t
          H◆=◆.◆)◆◆◆◆d◆◆◆◆◆.]◆◆◆◆◆◆w◆◆◆UH◆◆H◆◆◆H


]$"D◆◆◆\y◆◆◆bA◆C
@2
◆◆▒◆◆◆◆o◆◆◆
◆
 ▒◆?0 ◆ ▒◆◆◆◆◆◆o0◆◆◆o◆◆◆o ◆◆◆o◆=6F▒@GCC: (Debian

t1.o__abi_tagcrtstuff.cderegister_tm_clones__do_g
s_test.c__FRAME_END___DYNAMIC__GNU_EH_FRAME_HDR_G
ta_startsyscall@GLIBC_2.2.5__gmon_start____dso_ha
```


Reverse engineering

Portable Executable (PE)

- The Portable Executable (PE) format is a file format for executables, object code, DLLs and others used in 32-bit and 64-bit versions of Windows operating systems. The PE format is a data structure that encapsulates the information necessary for the Windows OS loader to manage the wrapped executable code.

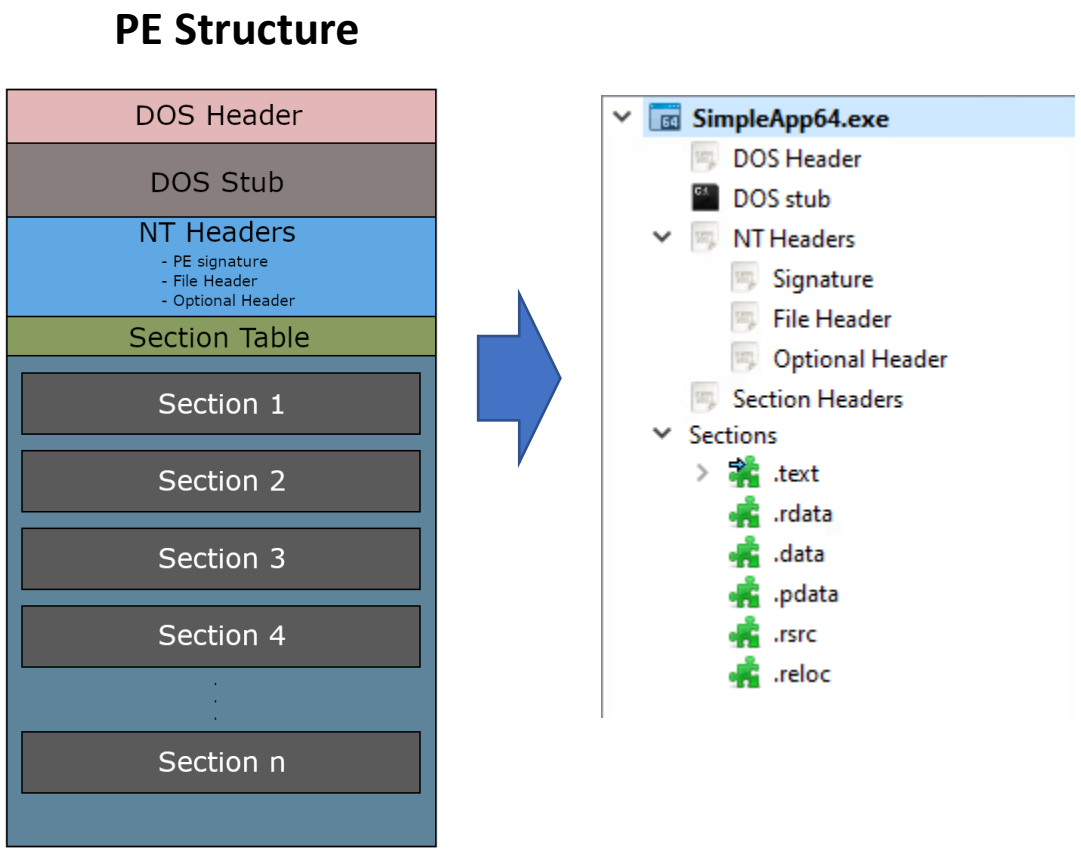
Portable Executable

Filename extension	.acm , .ax , .cpl , .dll , .drv , .efi , .exe , .mui , .ocx , .scr , .sys , .tsp

Refer: https://en.wikipedia.org/wiki/Portable_Executable

Reverse engineering

Portable Executable (PE)



Refer: https://0xrick.github.io/win-internals/pe2/

Reverse engineering

Magic number: 4D 5A

Offset	0	1	2	3	4	5
00000000	4D	5A	90	00	03	00
00000010	B8	00	00	00	00	00
00000020	00	00	00	00	00	00
00000030	00	00	00	00	00	00

Portable Executable (PE)

DOS Header

- Every PE file starts with a 64-bytes-long structure called the DOS header, it's what makes the PE file an MS-DOS executable.

DOS Stub

- After the DOS header comes the DOS stub which is a small MS-DOS 2.0 compatible executable that just prints an error message saying "This program cannot be run in DOS mode" when the program is run in DOS mode.

NT Headers

- The NT Headers part contains three main parts:
  - PE signature: A 4-byte signature that identifies the file as a PE file.
  - File Header: A standard COFF File Header. It holds some information about the PE file.
  - Optional Header: The most important header of the NT Headers, its name is the Optional Header because some files like object files don't have it, however it's required for image files (files like .exe files). This header provides important information to the OS loader.

Refer: https://0xrick.github.io/win-internals/pe2/

Reverse engineering

Portable Executable (PE)

Section Table

- The section table follows the Optional Header immediately, it is an array of Image Section Headers, there's a section header for every section in the PE file.
- Each header contains information about the section it refers to.

Sections

- Sections are where the actual contents of the file are stored, these include things like data and resources that the program uses, and also the actual code of the program, there are several sections each one with its own purpose.

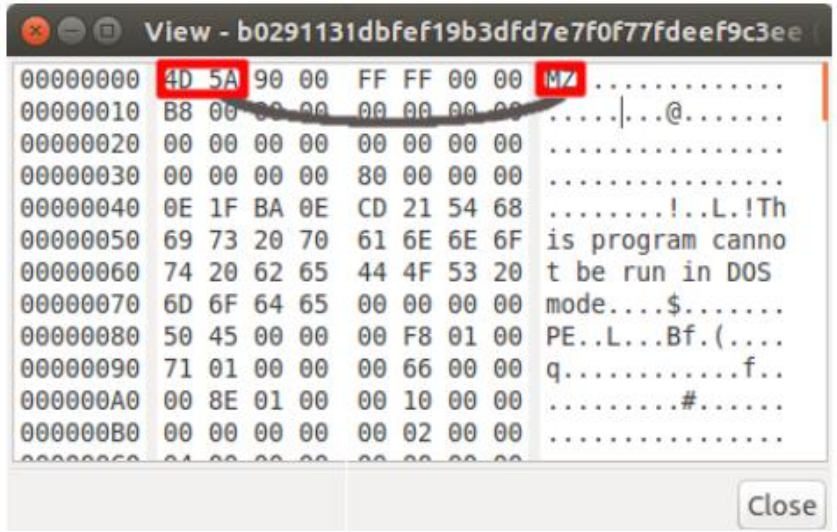
Refer: https://0xrick.github.io/win-internals/pe2/

Reverse engineering

Portable Executable (PE)

History 101

While at Microsoft, Mark Zbikowski developed the MS-DOS executable file format to start with his initials, MZ. These letters translate in hexadecimal to 4D5A. When header inspection of a file a malware analyst commonly checks the first two bytes for this value to qualify that the file is an executable.

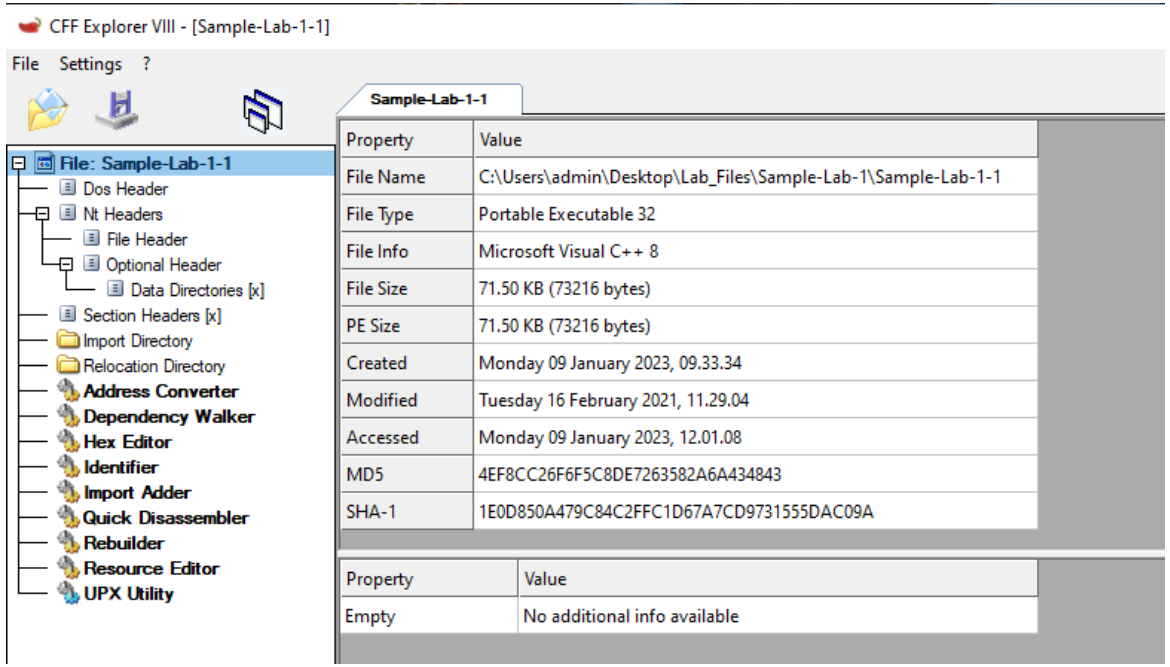


Refer: http://4d5asecurity.com/why-4d5a

Reverse engineering

Tool: CFF Explorer
Install: https://ntcore.com/?page_id=388

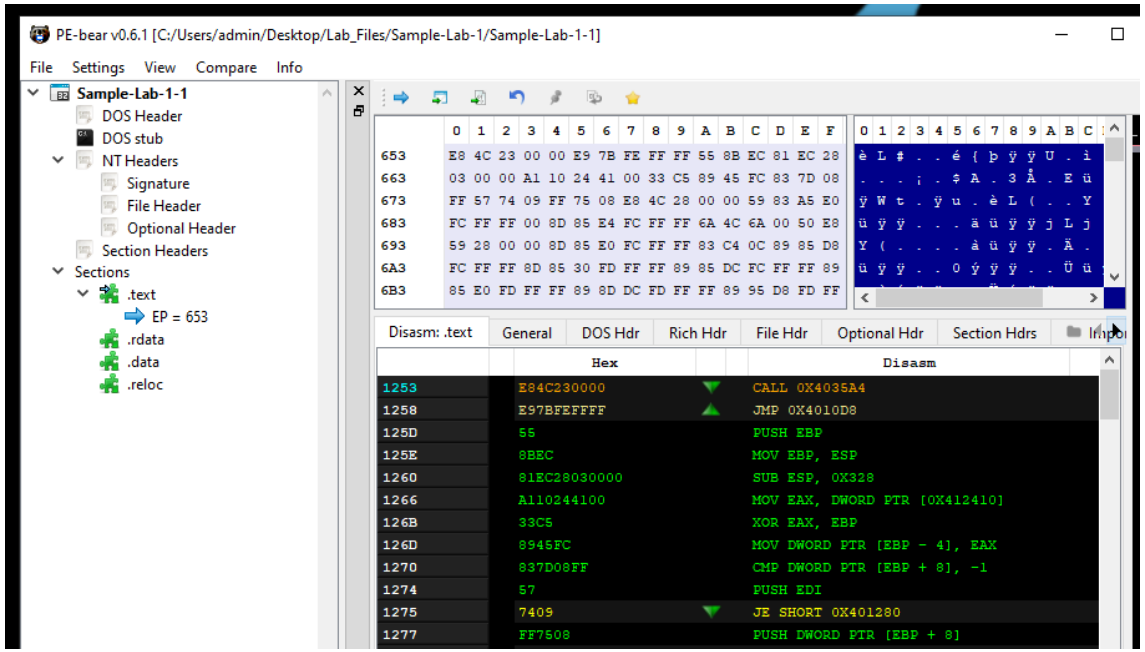
CFF Explorer - was designed to make PE editing as easy as possible, This application includes a series of tools which might help not only reverse engineers but also programmers.



Reverse engineering

Tool: PE-bear
Install: https://github.com/hasherezade/pe-bear/releases

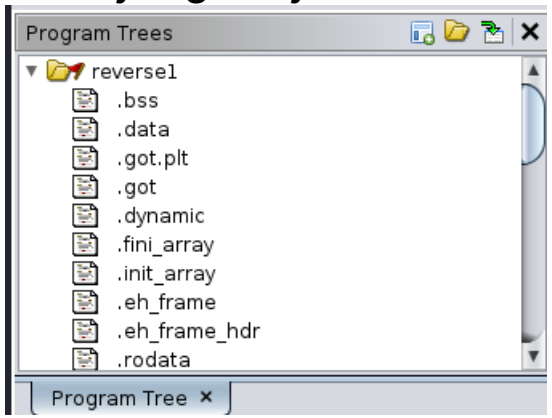
PE-bear is a multiplatform reversing tool for PE files. Its objective is to deliver fast and flexible “first view” for malware analyst

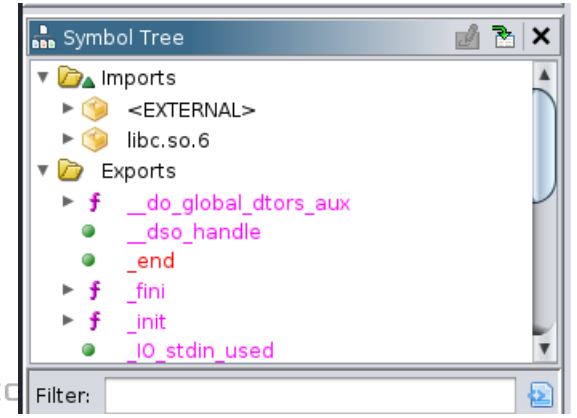


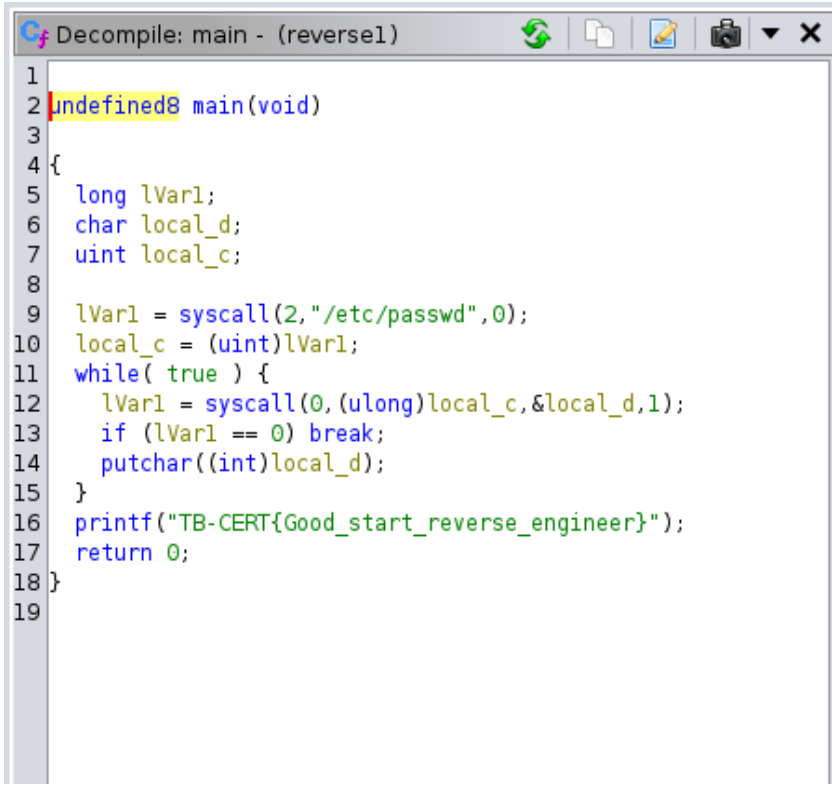
Reverse engineering

Tool: Ghidra
Install: sudo apt install ghidra

This package contains a software reverse engineering (SRE) framework created and maintained by the National Security Agency Research Directorate.

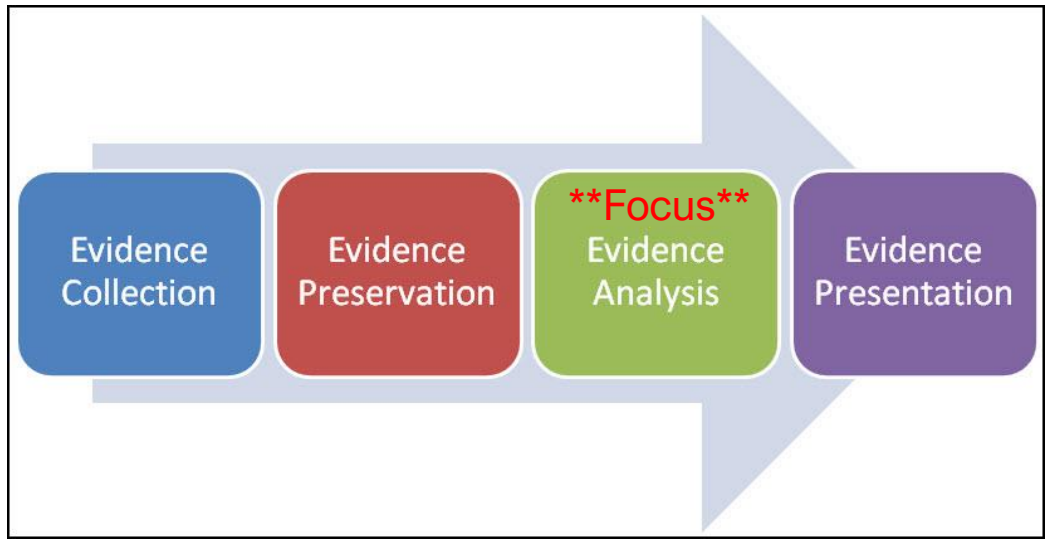






Digital Forensics

Digital forensics is the analysis and investigation of digital data, and digital forensics can take many forms, from analyzing an entire hard drive or individual files to investigating computer network traffic



Digital Forensics

Tool: file
Built-in tool on Kali Linux

file - determine file type

```
┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ file pass_test
pass_test: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),
5055295c4ff1855b83f271caa5, for GNU/Linux 3.2.0, not stripped

┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ file pass_test.c
pass_test.c: C source, ASCII text
```

Digital Forensics

Tool: String
Built-in tool on Kali Linux

strings - print the sequences of printable characters in files

Open with strings

```
┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ strings pass_test
/lib64/ld-linux-x86-64.so.2
PU)\O
putchar
__libc_start_main
__cxa_finalize
syscall
libc.so.6
GLIBC_2.34
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
/etc/passwd
;*3$"
GCC: (Debian 11.2.0-13) 11.2.0
Scrt1.o
```

Open with cat

```
┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ cat pass_test
@@@@◆▒▒▒PP◆◆   ◆◆◆-◆=◆=PX◆-◆=◆=◆888 XXXDDS◆td888
start_main__cxa_finalizesyscalllibc.so.6GLIBC_2.3
◆/H◆◆t◆◆H◆◆◆5◆/◆%◆/@◆%◆/h◆◆◆◆◆◆%◆/h◆◆◆◆◆◆%◆/f◆1◆I
+UH◆=◆.H◆◆t
          H◆=◆.◆)◆◆◆◆d◆◆◆◆◆.]◆◆◆◆◆◆w◆◆◆UH◆◆H◆◆◆H



]$"D◆◆◆\y◆◆◆bA◆C
@2
◆◆▒◆◆◆◆o◆◆◆
◆
 ▒◆?0 ◆ ▒◆◆◆◆◆◆o0◆◆◆o◆◆◆o ◆◆◆o◆=6F▒@GCC: (Debian

t1.o__abi_tagcrtstuff.cderegister_tm_clones__do_g
s_test.c__FRAME_END___DYNAMIC__GNU_EH_FRAME_HDR_G
ta_startsyscall@GLIBC_2.2.5__gmon_start____dso_ha
```


Digital Forensics

Tool: ExifTool
Install: sudo apt-get install libimage-exiftool-perl

exiftool for reading and writing meta information in a wide variety of files, including the maker note information of many digital cameras

```
┌──(kali㉿atmin)-[~/Downloads/tb-cert]
└─$ exiftool Logo.png
ExifTool Version Number         : 12.64
File Name                       : Logo.png
Directory                       : .
File Size                       : 6.8 kB
File Modification Date/Time     : 2023:08:14 08:26:59-07:00
File Access Date/Time           : 2023:08:14 08:27:49-07:00
File Inode Change Date/Time     : 2023:08:14 08:26:59-07:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 283
Image Height                    : 159
Bit Depth                       : 8
Color Type                      : Palette
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Palette                         : (Binary data 291 bytes, use -b option to extract)
Image Size                      : 283×159
Megapixels                      : 0.045
```

Digital Forensics

Tool: Foremost
Install: sudo apt install foremost

Foremost is a forensic program to recover lost files based on their headers, footers, and internal data structures.

Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive.

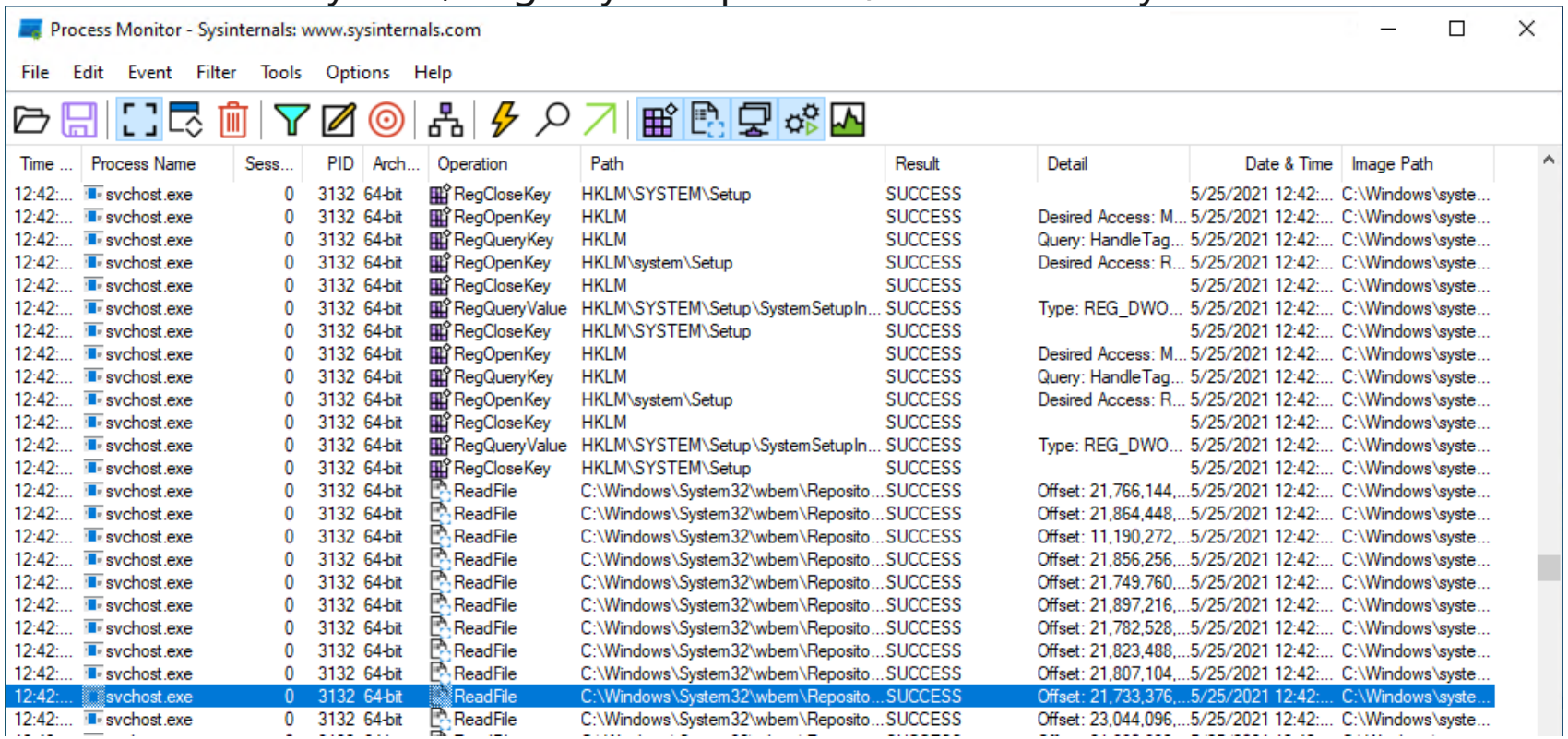
```
root@kali:~# foremost -t doc,jpg,pdf,xls -i image.dd
Processing: image.dd
|*|
root@kali:~# ls output/
audit.txt  jpg  pdf
```

Digital Forensics

Tool: Process Monitor

Install: https://download.sysinternals.com/files/ProcessMonitor.zip

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.

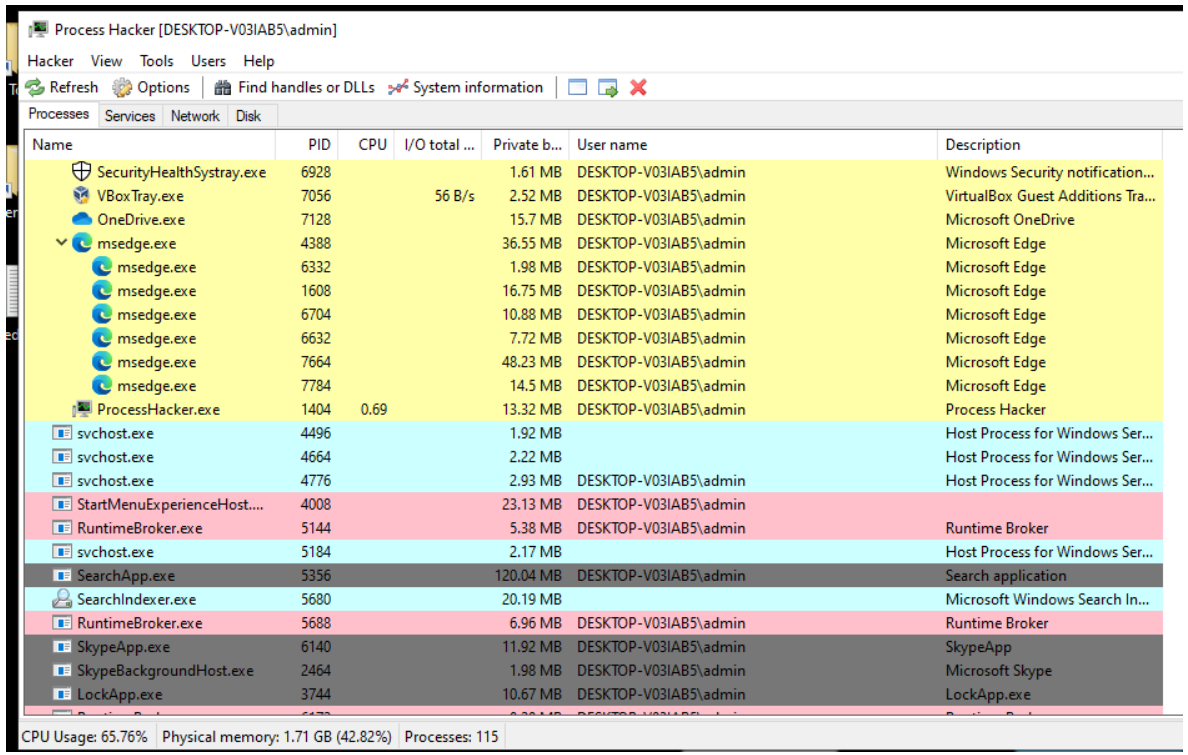


Time ...	Process Name	Sess...	PID	Arch...	Operation	Path	Result	Detail	Date & Time	Image Path
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM	SUCCESS	Desired Access: M...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM	SUCCESS		5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM	SUCCESS	Desired Access: M...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM	SUCCESS		5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,766,144,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,864,448,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 11,190,272,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,856,256,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,749,760,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,897,216,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,782,528,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,823,488,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,807,104,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 21,733,376,...	5/25/2021 12:42:...	C:\Windows\syste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Reposito...	SUCCESS	Offset: 23,044,096,...	5/25/2021 12:42:...	C:\Windows\syste...

Digital Forensics

Tool: Process Hacker
Install: https://processhacker.sourceforge.io/downloads.php

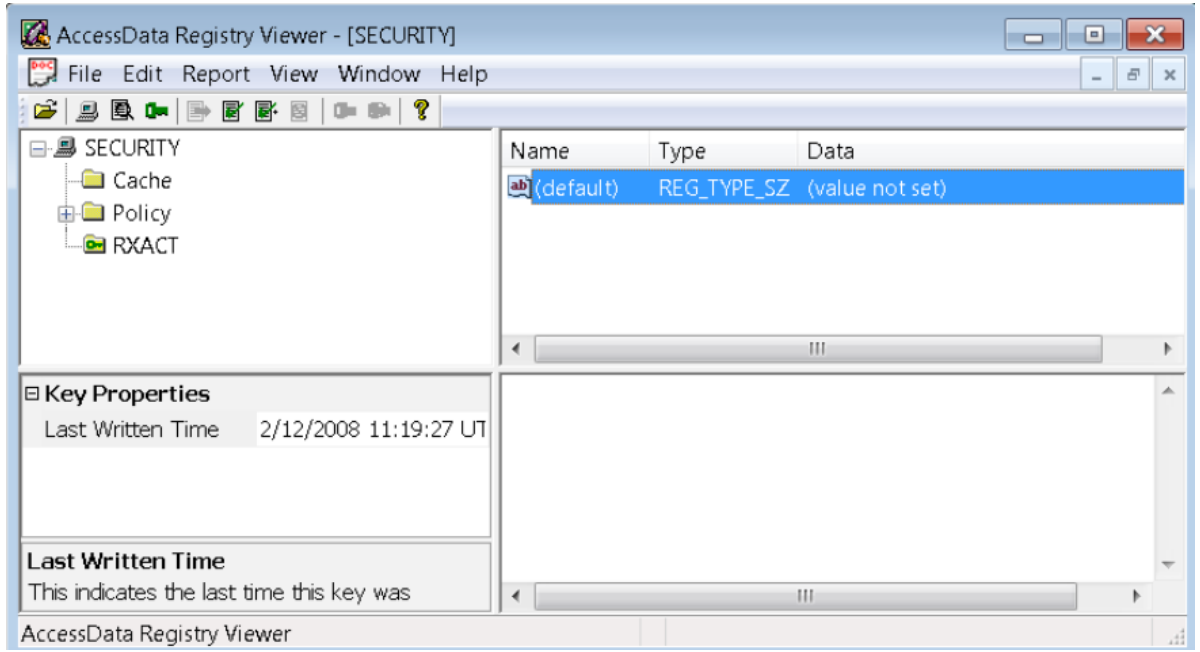
Process Hacker is a free, powerful, multi-purpose tool that helps you monitor system resources, debug software and detect malware.

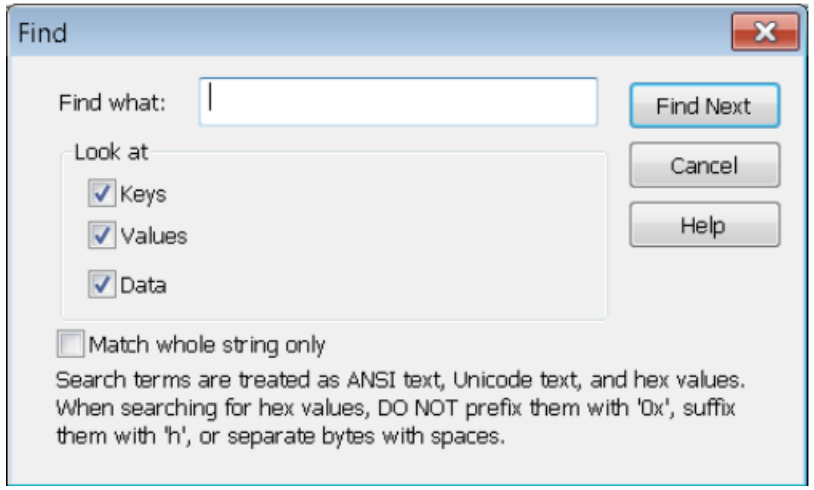


Digital Forensics

Registry Viewers

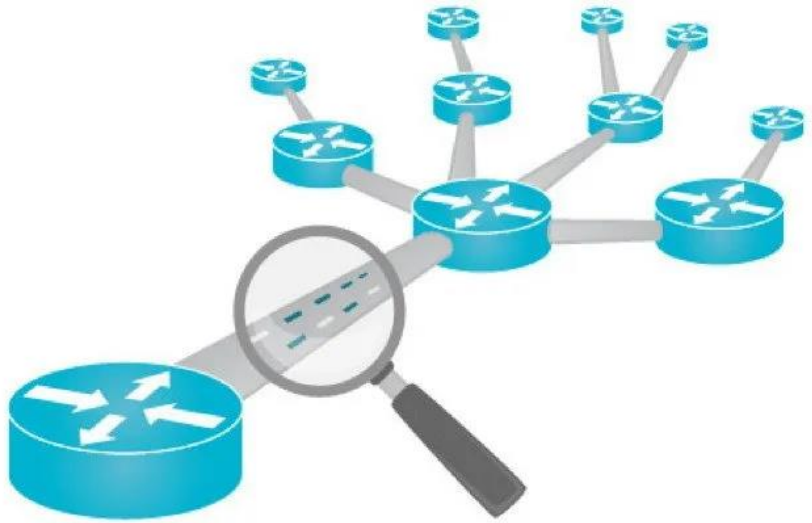
- RegistryViewer – Used to view windows registries
- https://www.exterro.com/ftk-product-downloads/registry-viewer-2-0-0





Network Analysis

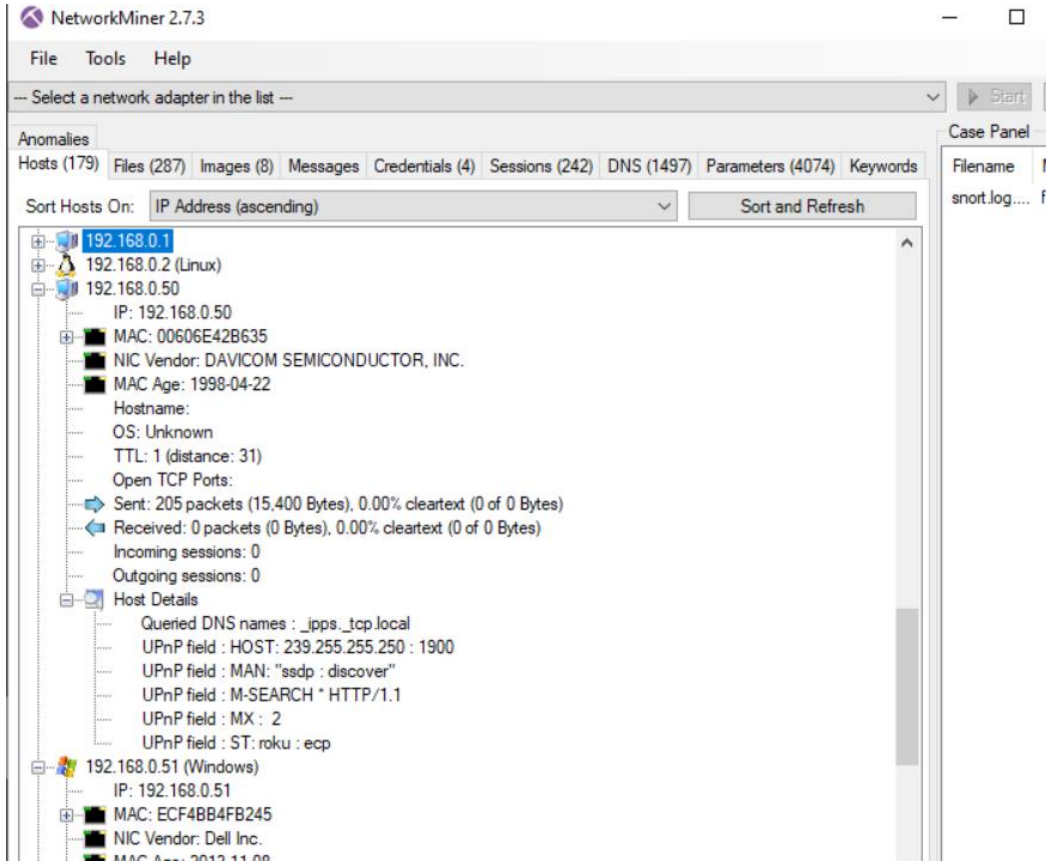
Network analysis is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.



Network Analysis

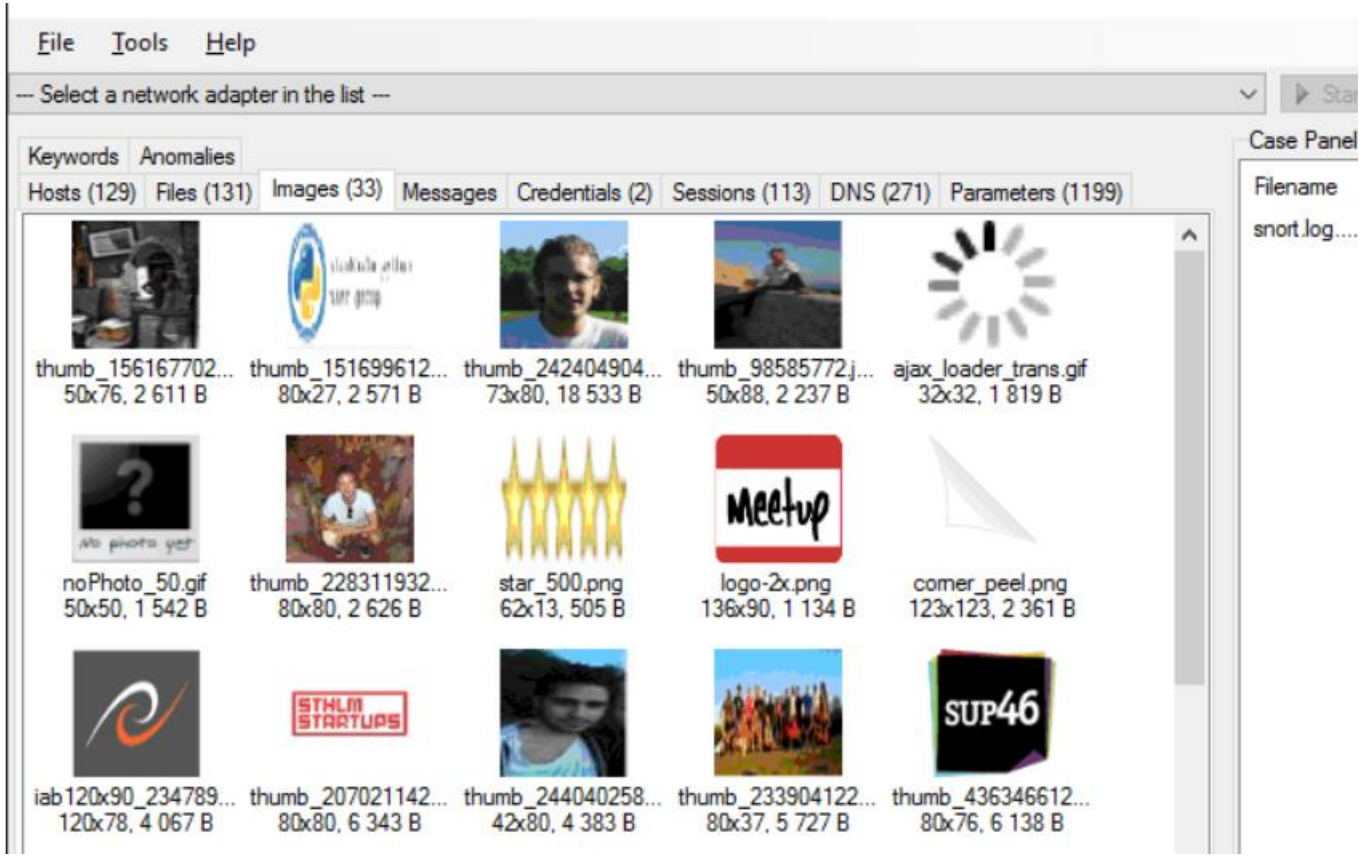
Tool: NetworkMinner

Install: https://www.netresec.com/?page=NetworkMiner



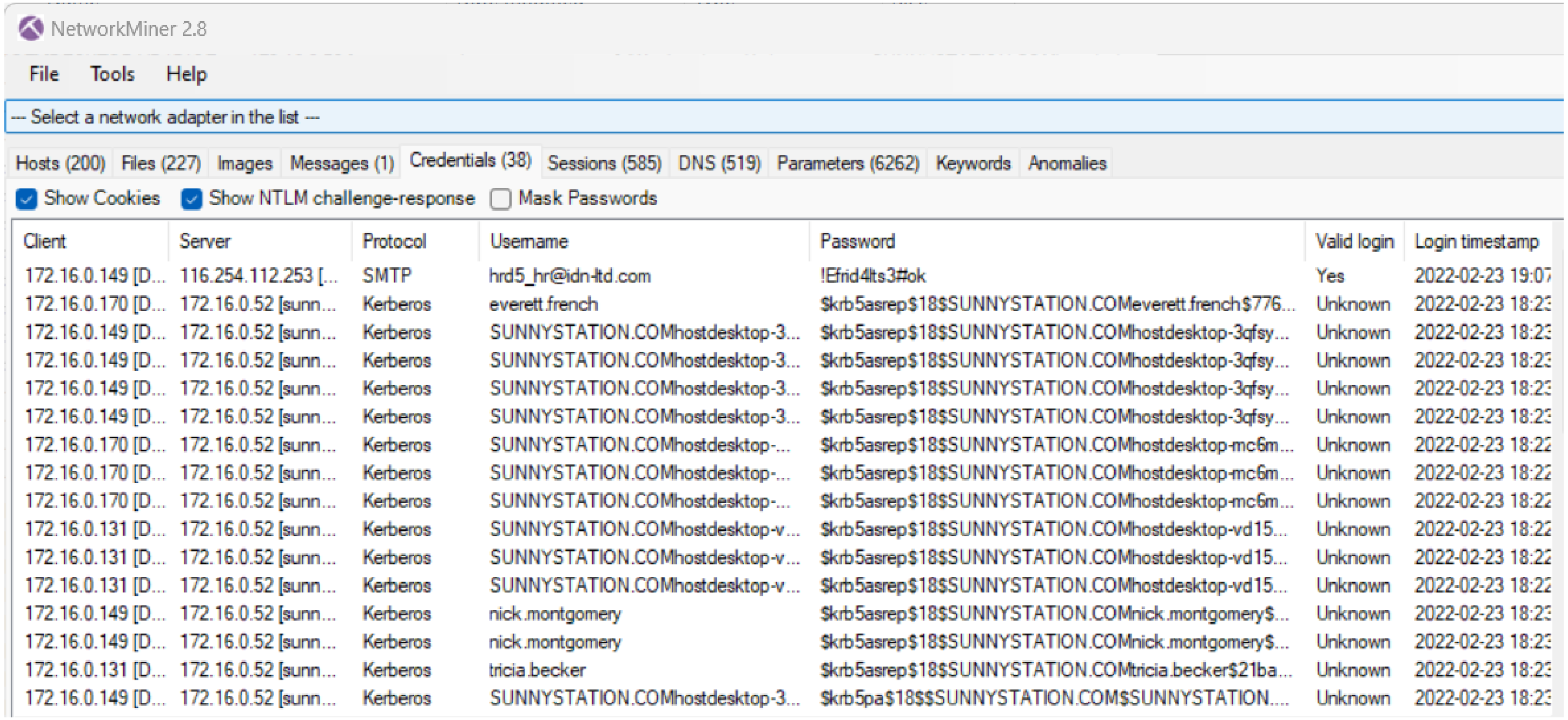
Network Analysis

Tool: NetworkMinner
Install: https://www.netresec.com/?page=NetworkMiner



Network Analysis

Tool: NetworkMinner
Install: https://www.netresec.com/?page=NetworkMiner

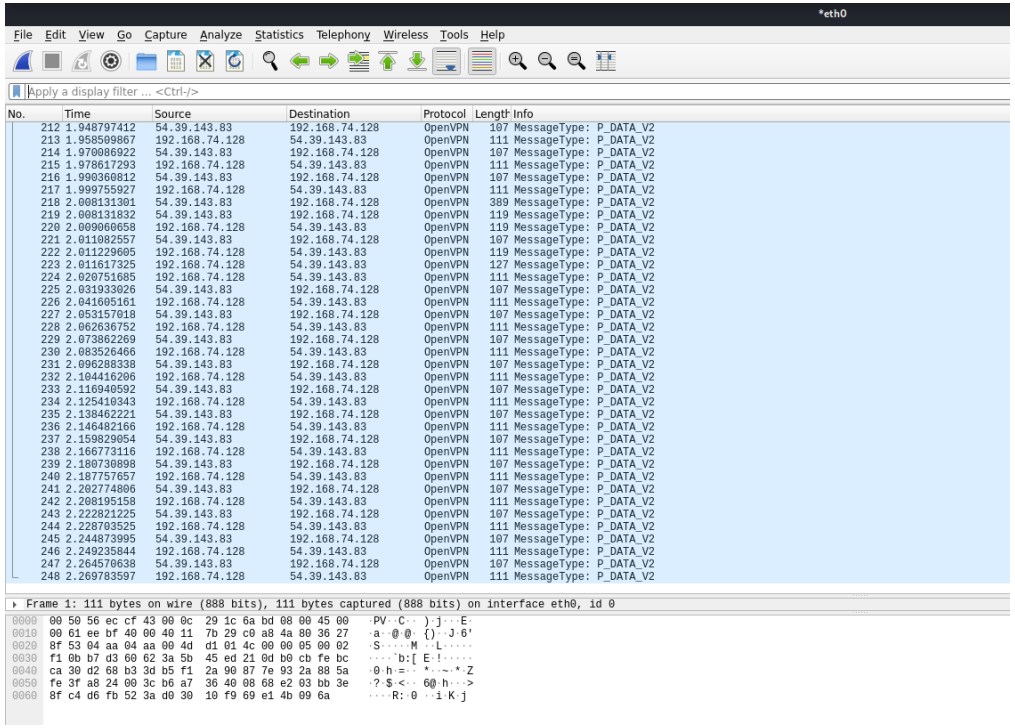


Client	Server	Protocol	Username	Password	Valid login	Login timestamp
172.16.0.149 [D...	116.254.112.253 [...	SMTP	hrd5_hr@idn-ltd.com	!Efrid4lts3#ok	Yes	2022-02-23 19:07
172.16.0.170 [D...	172.16.0.52 [sunn...	Kerberos	everett.french	$krb5asrep$18$SUNNYSTATION.COMeverett.french$776...	Unknown	2022-02-23 18:23
172.16.0.149 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-3...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-3qfsy...	Unknown	2022-02-23 18:23
172.16.0.149 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-3...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-3qfsy...	Unknown	2022-02-23 18:23
172.16.0.149 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-3...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-3qfsy...	Unknown	2022-02-23 18:23
172.16.0.149 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-3...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-3qfsy...	Unknown	2022-02-23 18:23
172.16.0.170 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-mc6m...	Unknown	2022-02-23 18:22
172.16.0.170 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-mc6m...	Unknown	2022-02-23 18:22
172.16.0.170 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-mc6m...	Unknown	2022-02-23 18:22
172.16.0.131 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-v...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-vd15...	Unknown	2022-02-23 18:22
172.16.0.131 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-v...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-vd15...	Unknown	2022-02-23 18:22
172.16.0.131 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-v...	$krb5asrep$18$SUNNYSTATION.COMhostdesktop-vd15...	Unknown	2022-02-23 18:22
172.16.0.149 [D...	172.16.0.52 [sunn...	Kerberos	nick.montgomery	$krb5asrep$18$SUNNYSTATION.COMnick.montgomery$...	Unknown	2022-02-23 18:23
172.16.0.149 [D...	172.16.0.52 [sunn...	Kerberos	nick.montgomery	$krb5asrep$18$SUNNYSTATION.COMnick.montgomery$...	Unknown	2022-02-23 18:23
172.16.0.131 [D...	172.16.0.52 [sunn...	Kerberos	tricia.becker	$krb5asrep$18$SUNNYSTATION.COMtricia.becker$21ba...	Unknown	2022-02-23 18:23
172.16.0.149 [D...	172.16.0.52 [sunn...	Kerberos	SUNNYSTATION.COMhostdesktop-3...	$krb5pa$18$$SUNNYSTATION.COM$SUNNYSTATION....	Unknown	2022-02-23 18:23

Network Analysis

Tool: WireShark
Built-in tool on Kali Linux

- Menu -> 09 Sniffing & Spoofing -> wireshark



Network Analysis

Tool: WireShark
Built-in tool on Kali Linux

Useful filters

Usage	Filter syntax
Wireshark Filter by IP	ip.addr == 10.10.50.1
Filter by Destination IP	ip.dest == 10.10.50.1
Filter by Source IP	ip.src == 10.10.50.1
Filter by IP range	ip.addr >= 10.10.50.1 and ip.addr <= 10.10.50.100
Filter by Multiple Ips	ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100
Filter out IP address	!(ip.addr == 10.10.50.1)
Filter subnet	ip.addr == 10.10.50.1/24
Filter by port	tcp.port == 25
Filter by destination port	tcp.dstport == 23
Filter by ip address and port	ip.addr == 10.10.50.1 and Tcp.port == 25

Network Analysis

Tool: WireShark
Built-in tool on Kali Linux

Useful filters

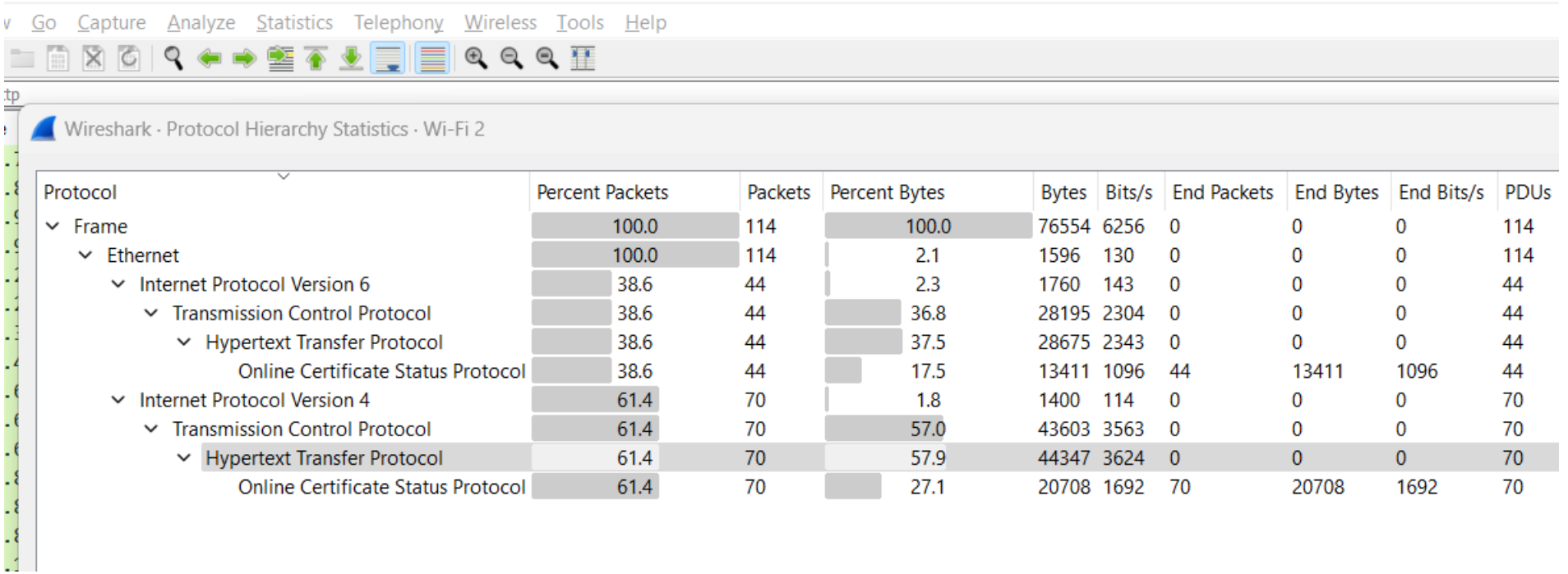
Usage	Filter syntax
Filter by URL	http.host == “host name”
Filter by time stamp	frame.time >= “June 02, 2019 18:04:00”
Filter SYN flag	tcp.flags.syn == 1
	tcp.flags.syn == 1 and tcp.flags.ack == 0
Wireshark Beacon Filter	wlan.fc.type_subtype = 0x08
Wireshark broadcast filter	eth.dst == ff:ff:ff:ff:ff:ff
Wireshark multicast filter	(eth.dst[0] & 1)
Host name filter	ip.host = hostname
MAC address filter	eth.addr == 00:70:f4:23:18:c4
RST flag filter	tcp.flags.reset == 1

Network Analysis

Tool: WireShark
Built-in tool on Kali Linux

Useful functions

Protocol Hierarchy (Statistics-> Protocol Hierarchy)



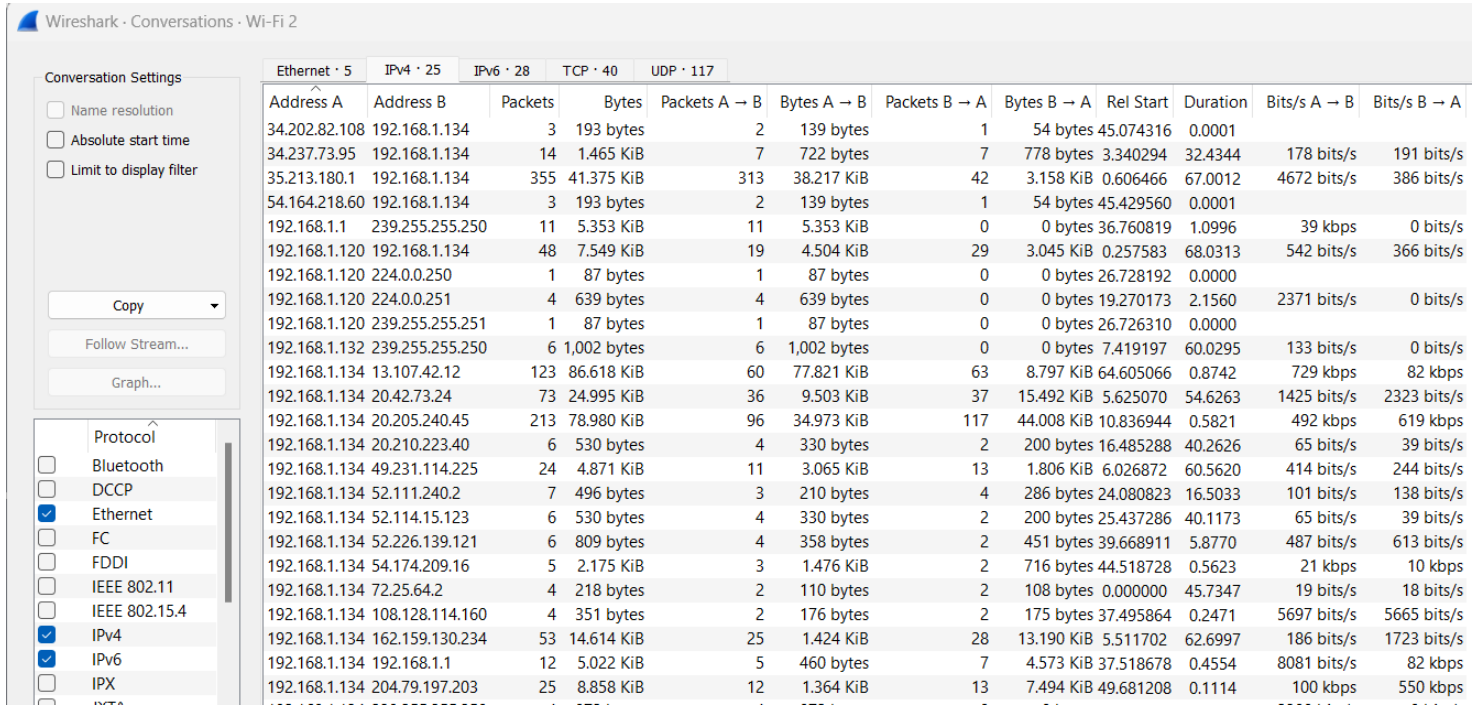
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	114	100.0	76554	6256	0	0	0	114
Ethernet	100.0	114	2.1	1596	130	0	0	0	114
Internet Protocol Version 6	38.6	44	2.3	1760	143	0	0	0	44
Transmission Control Protocol	38.6	44	36.8	28195	2304	0	0	0	44
Hypertext Transfer Protocol	38.6	44	37.5	28675	2343	0	0	0	44
Online Certificate Status Protocol	38.6	44	17.5	13411	1096	44	13411	1096	44
Internet Protocol Version 4	61.4	70	1.8	1400	114	0	0	0	70
Transmission Control Protocol	61.4	70	57.0	43603	3563	0	0	0	70
Hypertext Transfer Protocol	61.4	70	57.9	44347	3624	0	0	0	70
Online Certificate Status Protocol	61.4	70	27.1	20708	1692	70	20708	1692	70

Network Analysis

Tool: WireShark
Built-in tool on Kali Linux

Useful functions

Conversations (Statistics-> Conversations)



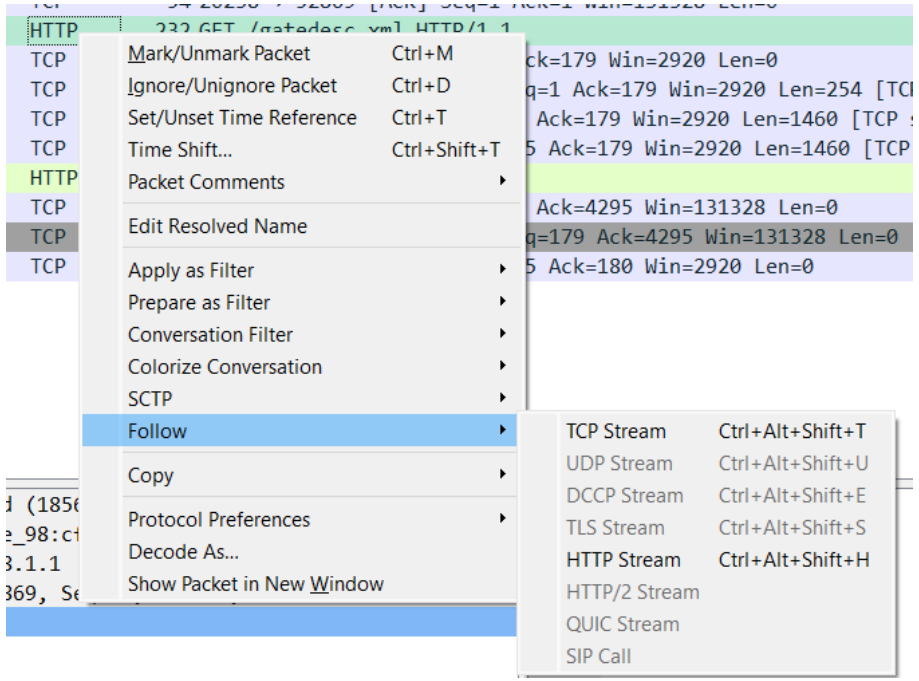
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
34.202.82.108	192.168.1.134	3	193 bytes	2	139 bytes	1	54 bytes	45.074316	0.0001		
34.237.73.95	192.168.1.134	14	1.465 KiB	7	722 bytes	7	778 bytes	3.340294	32.4344	178 bits/s	191 bits/s
35.213.180.1	192.168.1.134	355	41.375 KiB	313	38.217 KiB	42	3.158 KiB	0.606466	67.0012	4672 bits/s	386 bits/s
54.164.218.60	192.168.1.134	3	193 bytes	2	139 bytes	1	54 bytes	45.429560	0.0001		
192.168.1.1	239.255.255.250	11	5.353 KiB	11	5.353 KiB	0	0 bytes	36.760819	1.0996	39 kbps	0 bits/s
192.168.1.120	192.168.1.134	48	7.549 KiB	19	4.504 KiB	29	3.045 KiB	0.257583	68.0313	542 bits/s	366 bits/s
192.168.1.120	224.0.0.250	1	87 bytes	1	87 bytes	0	0 bytes	26.728192	0.0000		
192.168.1.120	224.0.0.251	4	639 bytes	4	639 bytes	0	0 bytes	19.270173	2.1560	2371 bits/s	0 bits/s
192.168.1.120	239.255.255.251	1	87 bytes	1	87 bytes	0	0 bytes	26.726310	0.0000		
192.168.1.132	239.255.255.250	6	1,002 bytes	6	1,002 bytes	0	0 bytes	7.419197	60.0295	133 bits/s	0 bits/s
192.168.1.134	13.107.42.12	123	86.618 KiB	60	77.821 KiB	63	8.797 KiB	64.605066	0.8742	729 kbps	82 kbps
192.168.1.134	20.42.73.24	73	24.995 KiB	36	9.503 KiB	37	15.492 KiB	5.625070	54.6263	1425 bits/s	2323 bits/s
192.168.1.134	20.205.240.45	213	78.980 KiB	96	34.973 KiB	117	44.008 KiB	10.836944	0.5821	492 kbps	619 kbps
192.168.1.134	20.210.223.40	6	530 bytes	4	330 bytes	2	200 bytes	16.485288	40.2626	65 bits/s	39 bits/s
192.168.1.134	49.231.114.225	24	4.871 KiB	11	3.065 KiB	13	1.806 KiB	6.026872	60.5620	414 bits/s	244 bits/s
192.168.1.134	52.111.240.2	7	496 bytes	3	210 bytes	4	286 bytes	24.080823	16.5033	101 bits/s	138 bits/s
192.168.1.134	52.114.15.123	6	530 bytes	4	330 bytes	2	200 bytes	25.437286	40.1173	65 bits/s	39 bits/s
192.168.1.134	52.226.139.121	6	809 bytes	4	358 bytes	2	451 bytes	39.668911	5.8770	487 bits/s	613 bits/s
192.168.1.134	54.174.209.16	5	2.175 KiB	3	1.476 KiB	2	716 bytes	44.518728	0.5623	21 kbps	10 kbps
192.168.1.134	72.25.64.2	4	218 bytes	2	110 bytes	2	108 bytes	0.000000	45.7347	19 bits/s	18 bits/s
192.168.1.134	108.128.114.160	4	351 bytes	2	176 bytes	2	175 bytes	37.495864	0.2471	5697 bits/s	5665 bits/s
192.168.1.134	162.159.130.234	53	14.614 KiB	25	1.424 KiB	28	13.190 KiB	5.511702	62.6997	186 bits/s	1723 bits/s
192.168.1.134	192.168.1.1	12	5.022 KiB	5	460 bytes	7	4.573 KiB	37.518678	0.4554	8081 bits/s	82 kbps
192.168.1.134	204.79.197.203	25	8.858 KiB	12	1.364 KiB	13	7.494 KiB	49.681208	0.1114	100 kbps	550 kbps

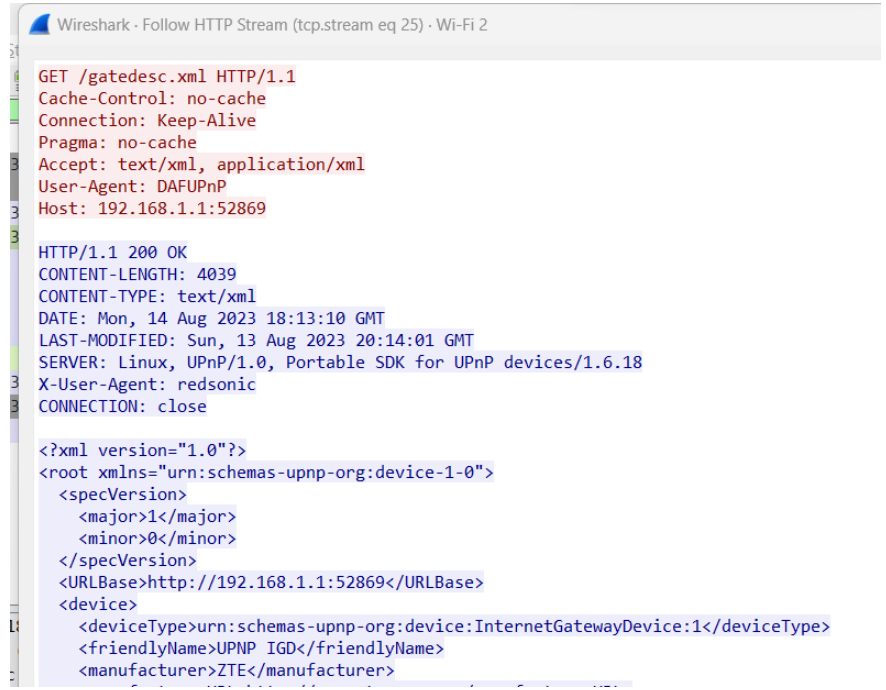
Network Analysis

Tool: WireShark
Built-in tool on Kali Linux

Useful functions

Follow TCP and HTTP Steam (Right-Click)





Key Takeaway

ซ้อม ซ้อม ซ้อม!!!

(Practice makes perfect)

thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
merci
obrigado
bedankt
dziękuję
спасибо
Баярлалаа
рахмат
sukriya
kop khun krap
go raibh maith agat
mochchakkeram
arigatō
grazie
dakujem
takk
terima kasih
감사합니다
ありがとう
мерси
tapadh leat
hvala
mauruuru
sagolun
dank je
mersi
barka
welalin
tack
spas
mahalo
paldies
grazzi
misaotra
matondo
blagodaram
vinaka
faafetai lava
kiitos
dankie
dhanyavad
nandri
nanni
enkosi
bayarlalaa
gracie
koszonom
chnorakaloutioun
gratias ago
gracies
sulpay
taiku
djiere dieuf
tau
mamnun
хвала
asante
manana
obrigada
murakoze
tenki
trugarez
shukriya
merce
dhanyavadagalu
diolch
ευχαριστώ
xièxie
rahmet
tanemirt
najis tuke
kam sah hamnida
didi madobo
mesi
dekuji
sobodi
rahmat
akun
dankon
aciū
kia ora

CYBER
COMBAT