



Thailand Cyber Top Talent 2023

นาย ประมินทร์ ช่างมณี (พีมินทร์)
CERT Manager, TB-CERT



ผู้บรรยาย

นาย ปรมินทร์ ช่างมณี (พีมินทร์)
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

 TB-CERT Thailand Banking Sector CERT	 SOSECURE	 McAiden IT SELECT LAB	 Secure-D CENTER
วันที่ 11 กันยายน 2566 เวลา 17.00 น. - 19.00 น.	วันที่ 12 กันยายน 2566 เวลา 17.00 น. - 19.00 น.	วันที่ 13 กันยายน 2566 เวลา 17.00 น. - 19.00 น.	วันที่ 14 กันยายน 2566 เวลา 17.00 น. - 19.00 น.
โดย TB-CERT	โดย SOSECURE	โดย McAiden และ IT SELECT LAB	โดย Secure-D Center
หัวข้อ “การเตรียมทักษะ และยุทธวิธีในการแข่ง”	หัวข้อ “Mini Capture the flag ”	หัวข้อ “Mobile Malware Reverse Engineering - Ox1: The Begining”	หัวข้อ “Threat Hunting”



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

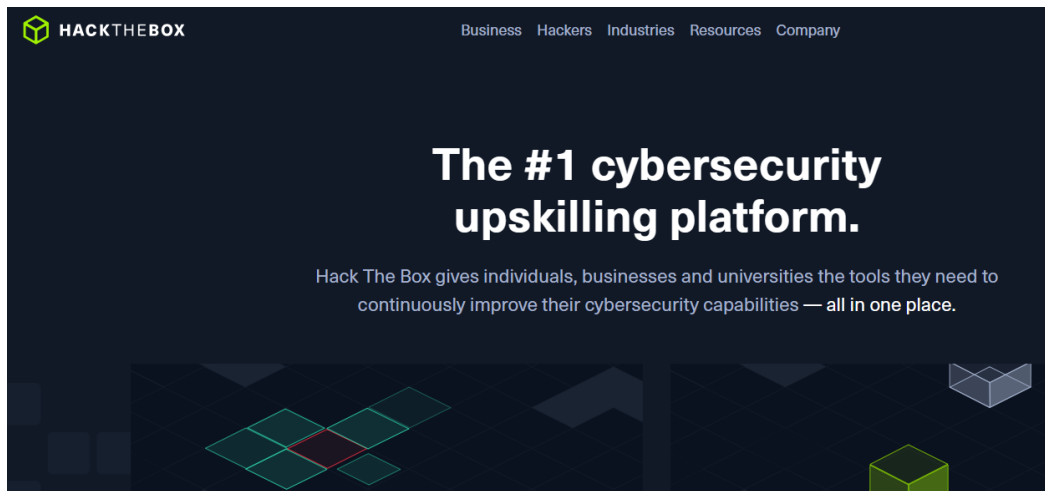
1. น้องๆ คิดว่าทักษะคืออะไร
2. น้องๆ จะสร้างทักษะขึ้นได้อย่างไร



ทักษะและยุทธวิธี

ช่องทางการฝึกทักษะเพิ่มเติม

<https://app.hackthebox.com/>



<https://tryhackme.com/>



ทักษะและยุทธวิธี



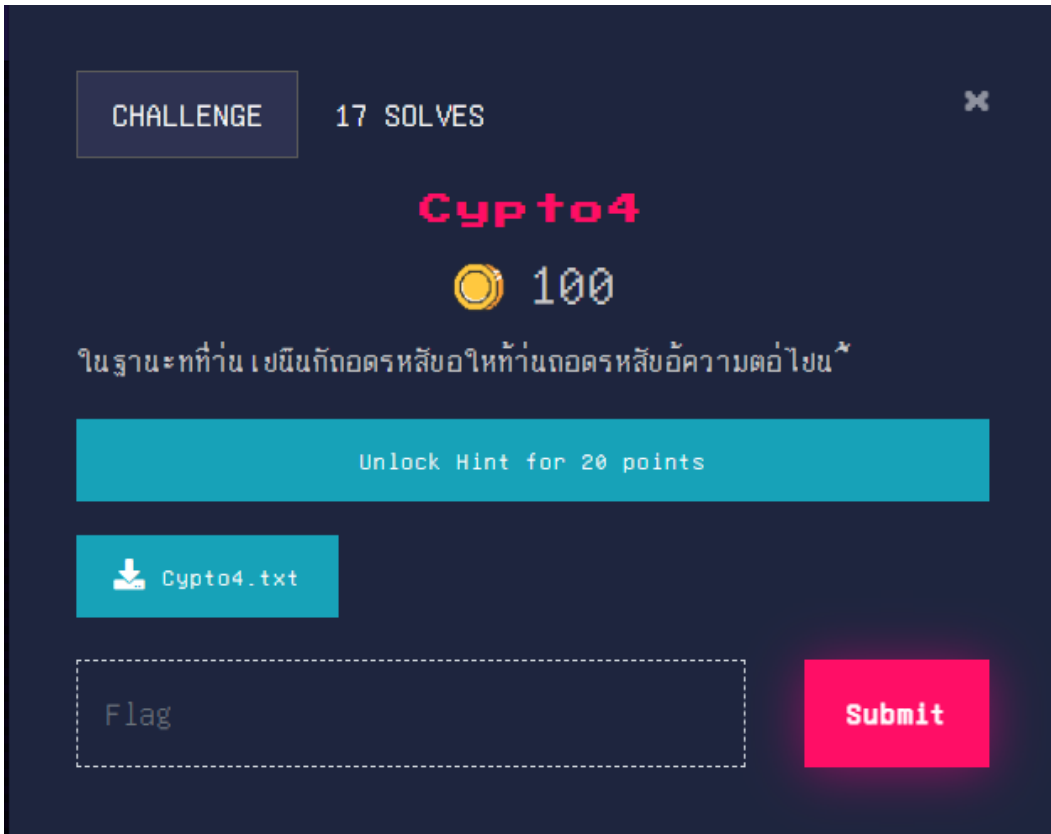
กำหนดยุทธวิธี การแข่ง

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



ทักษะและยุทธวิธี

จุดสังเกตระบบแข่ง

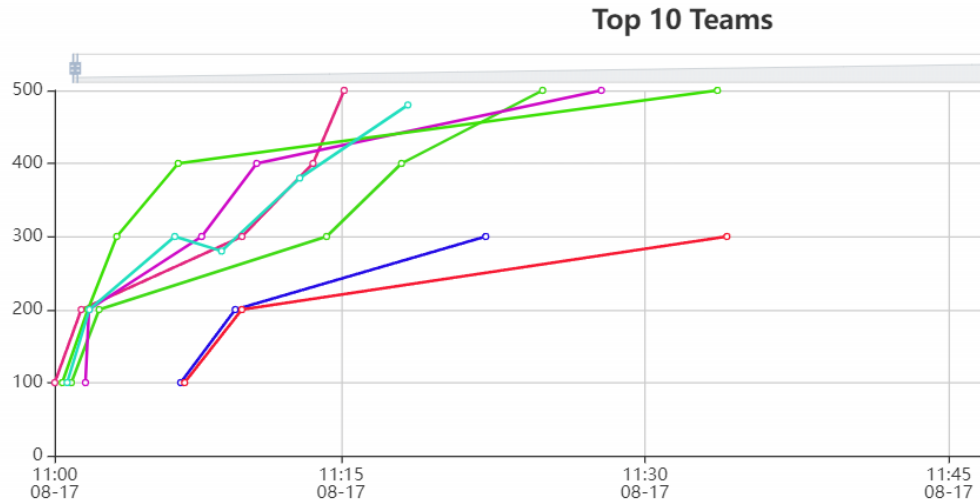


1. จำนวนคะแนนจะสะท้อนความยาก (ในกรณี Fixed score)
2. หมดสังเกตจำนวนทีมที่ Solves
3. พิจารณาตัดสินใจในใช้ Hint (ถ้าจำเป็น) แต่คะแนนจะถูกลบ



ทักษะและยุทธวิธี

จุดสังเกตบนระบบแข่ง



4. สังเกตทีมกลุ่มคะแนนใกล้เคียงกับทีมเรา
แก้ไขโจทย์ประเภทอะไร ชื่อโจทย์อะไร
5. สังเกตกลุ่ม Top5

Place	Team	Score
1		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
Crypto3	100	August 17th, 11:15:09 AM



ทักษะและยุทธวิธี

คำถาม (คุยกันในทีม)

1. มียุทธวิธีในการแข่งไว้แล้วหรือยัง
2. วางยุทธวิธีในการแข่งอย่างไร



Introduction



Thailand Cyber Top Talent 2023

การแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย จัดโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ร่วมกับบริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย) จำกัด โดยมุ่งหวังให้นักเรียน นิสิต นักศึกษา และประชาชนทั่วไป ที่เข้าร่วมการแข่งขันได้ เรียนรู้ พัฒนาทักษะ และประสบการณ์ เพื่อให้กลายเป็นบุคลากรที่มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์และเป็นการสร้างแรงงานออกสู่ตลาดแรงงานในอนาคต อีกทั้งเป็นการช่วยเพิ่มความตระหนักรู้เกี่ยวกับภัยคุกคามทางด้านไซเบอร์ให้กับบุคคลทั่วไปมากขึ้น 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 และต้องหาคำตอบจากร่องรอยในเครื่องแม่ข่ายที่ถูกโจมตี



Introduction

รอบคัดเลือก

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

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

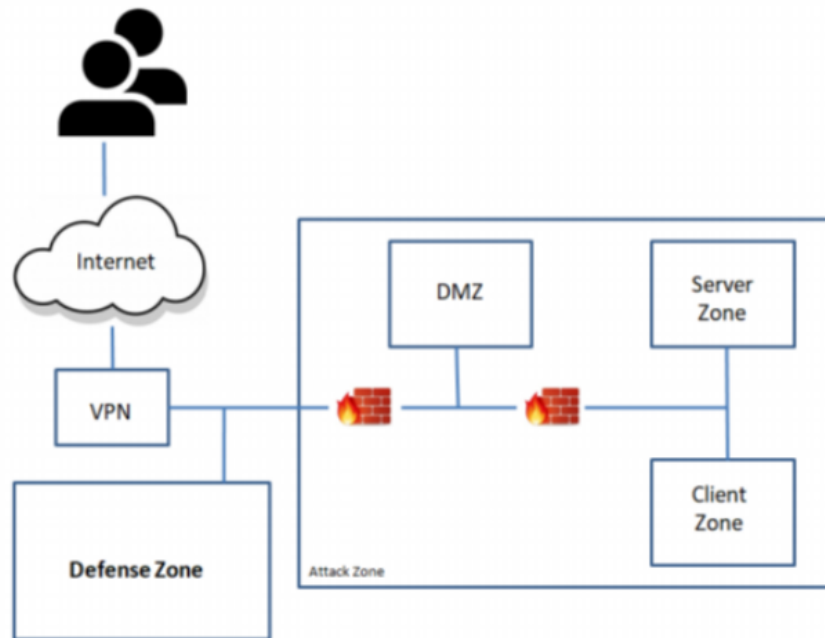
ระยะเวลาการแข่งขัน : วันเสาร์ที่ 16 กันยายน 2566 เวลา 09:00 – 16:00 น. (รวมเวลา 7 ชั่วโมง) **UPDATE!**



Introduction

รอบชิงชนะเลิศ

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



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



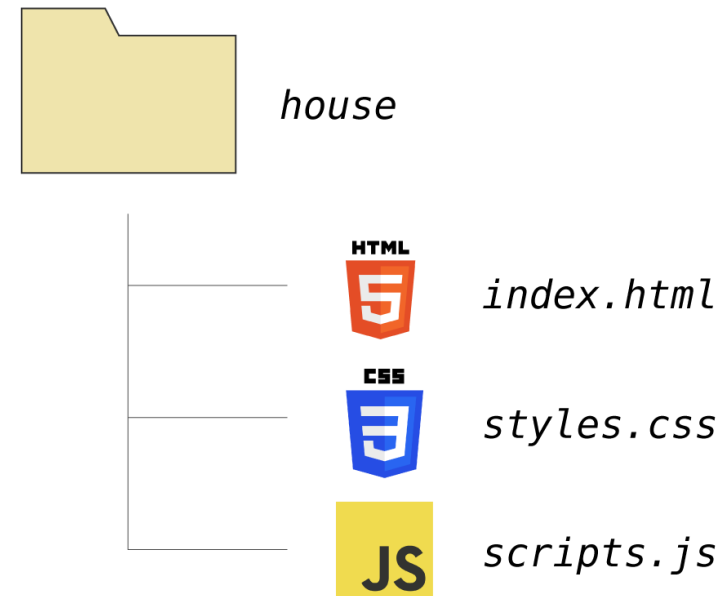
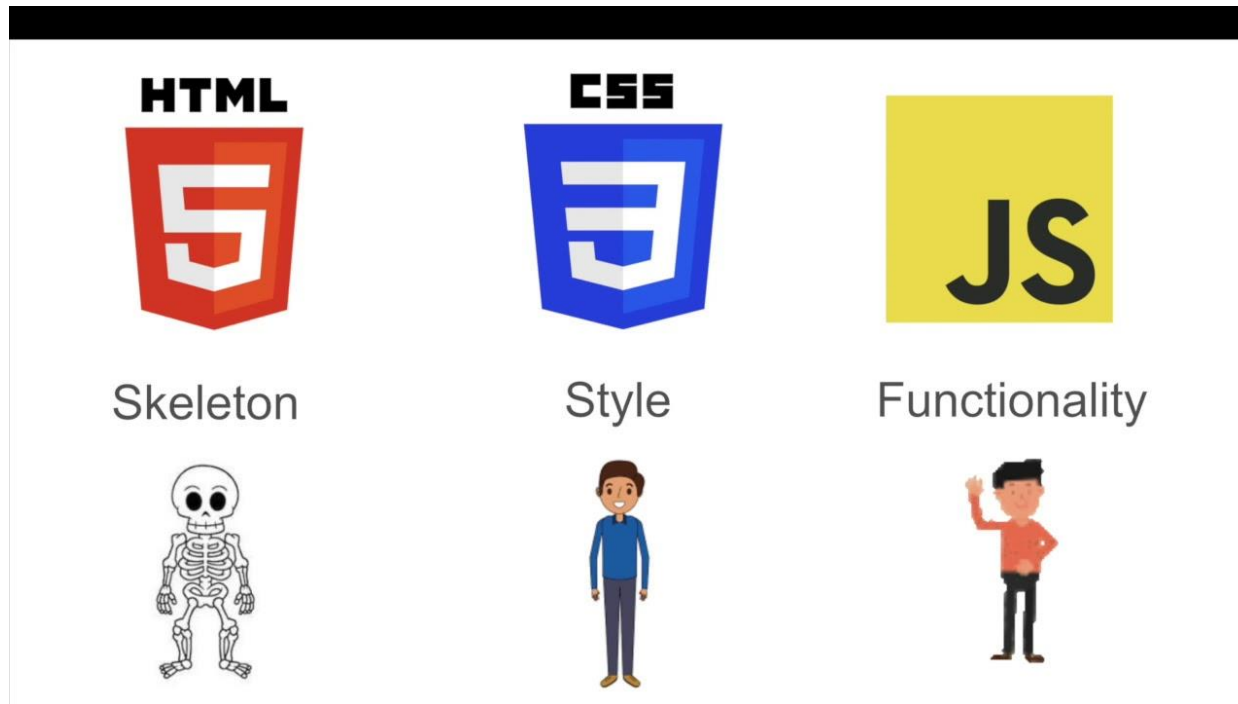
Web Application

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]

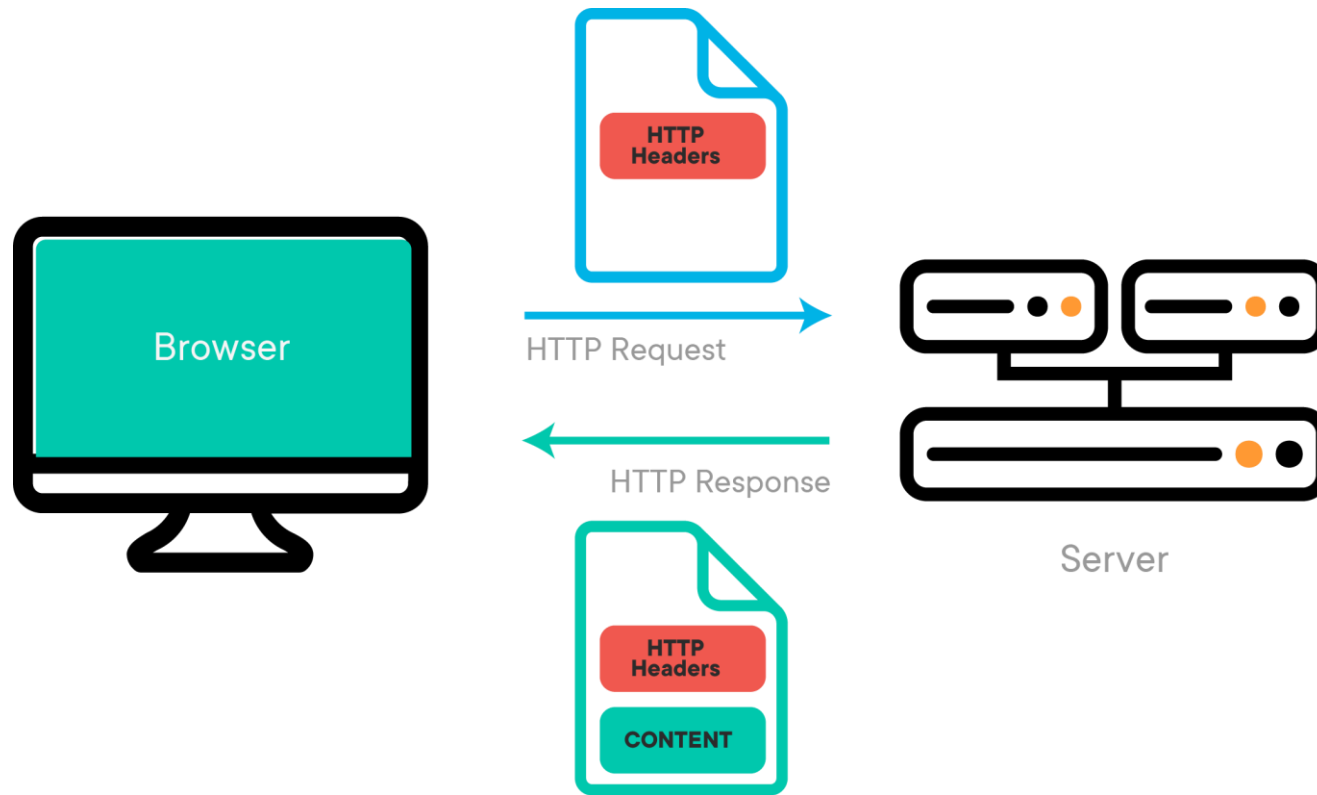


Web Application

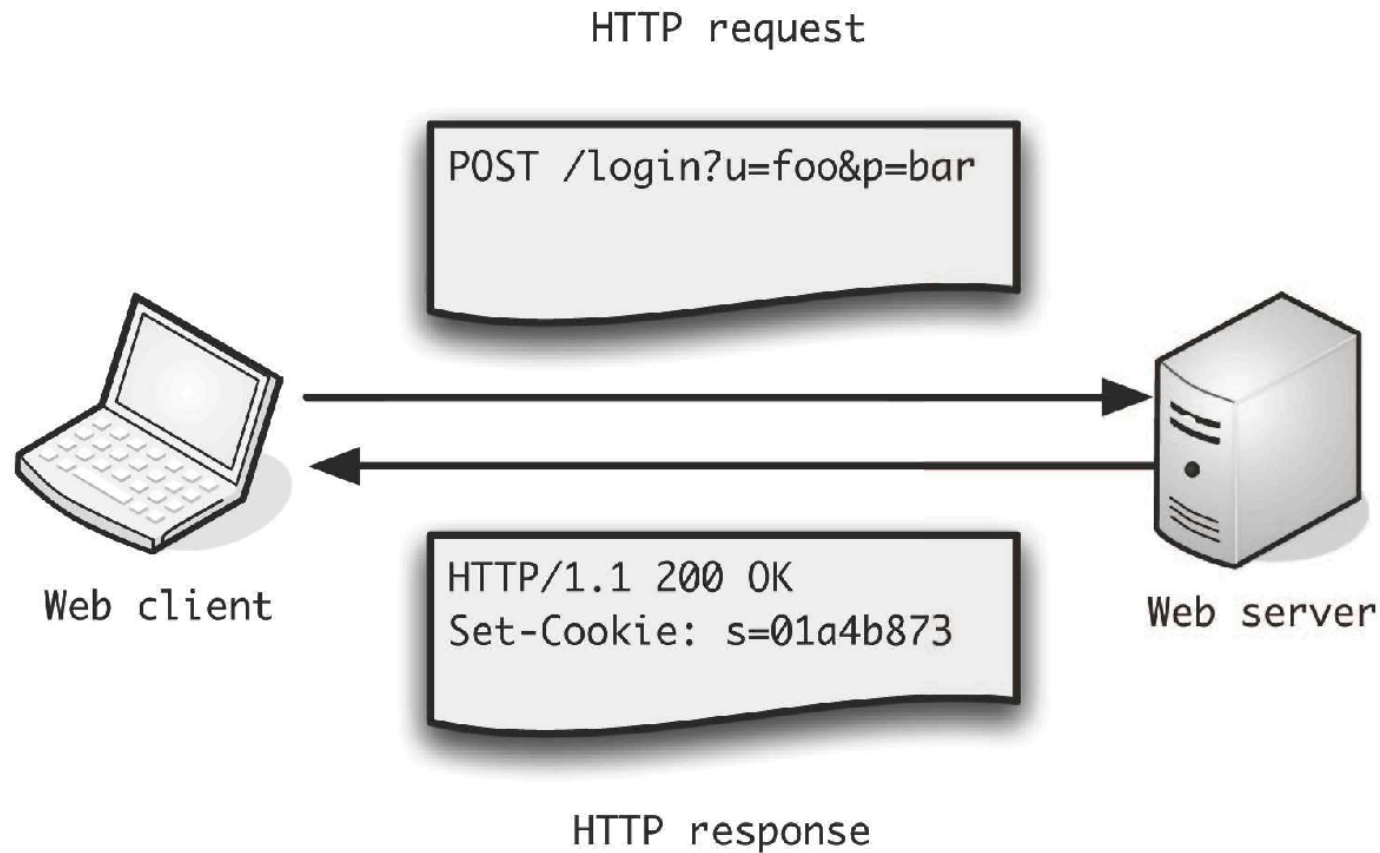
Web application ?



Web Application



Web Application



Web Application

HTTP Request

```
GET /doc/test.html HTTP/1.1
Host: www.test101.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Content-Length: 35

bookId=12345&author=Tan+Ah+Teck
```

Diagram illustrating the structure of an HTTP Request:

- Request Line:** GET /doc/test.html HTTP/1.1
- Request Headers:** Host: www.test101.com, Accept: image/gif, image/jpeg, */*, Accept-Language: en-us, Accept-Encoding: gzip, deflate, User-Agent: Mozilla/4.0, Content-Length: 35
- Request Message Header:** (Grouped with Request Headers)
- A blank line separates header & body**
- Request Message Body:** bookId=12345&author=Tan+Ah+Teck

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

HTTP Status Codes



**1XX
INFORMATIONAL**

**2XX
SUCCESS**

**3XX
REDIRECTION**

**4XX
CLIENT ERROR**

**5XX
SERVER ERROR**

1XX Informational		4XX Client Error Continued	
100	Continue	409	Conflict
101	Switching Protocols	410	Gone
102	Processing	411	Length Required
2XX Success		412	Precondition Failed
200	OK	413	Payload Too Large
201	Created	414	Request-URI Too Long
202	Accepted	415	Unsupported Media Type
203	Non-authoritative Information	416	Requested Range Not Satisfiable
204	No Content	417	Expectation Failed
205	Reset Content	418	I'm a teapot
206	Partial Content	421	Misdirected Request
207	Multi-Status	422	Unprocessable Entity
208	Already Reported	423	Locked
226	IM Used	424	Failed Dependency
3XX Redirection		426	Upgrade Required
300	Multiple Choices	428	Precondition Required
301	Moved Permanently	429	Too Many Requests
302	Found	431	Request Header Fields Too Large
303	See Other	444	Connection Closed Without Response
304	Not Modified	451	Unavailable For Legal Reasons
305	Use Proxy	499	Client Closed Request
307	Temporary Redirect	5XX Server Error	
308	Permanent Redirect	500	Internal Server Error
4XX Client Error		501	Not Implemented
400	Bad Request	502	Bad Gateway
401	Unauthorized	503	Service Unavailable
402	Payment Required	504	Gateway Timeout
403	Forbidden	505	HTTP Version Not Supported
404	Not Found	506	Variant Also Negotiates
405	Method Not Allowed	507	Insufficient Storage
406	Not Acceptable	508	Loop Detected
407	Proxy Authentication Required	510	Not Extended
408	Request Timeout	511	Network Authentication Required
		599	Network Connect Timeout Error



Web Application



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



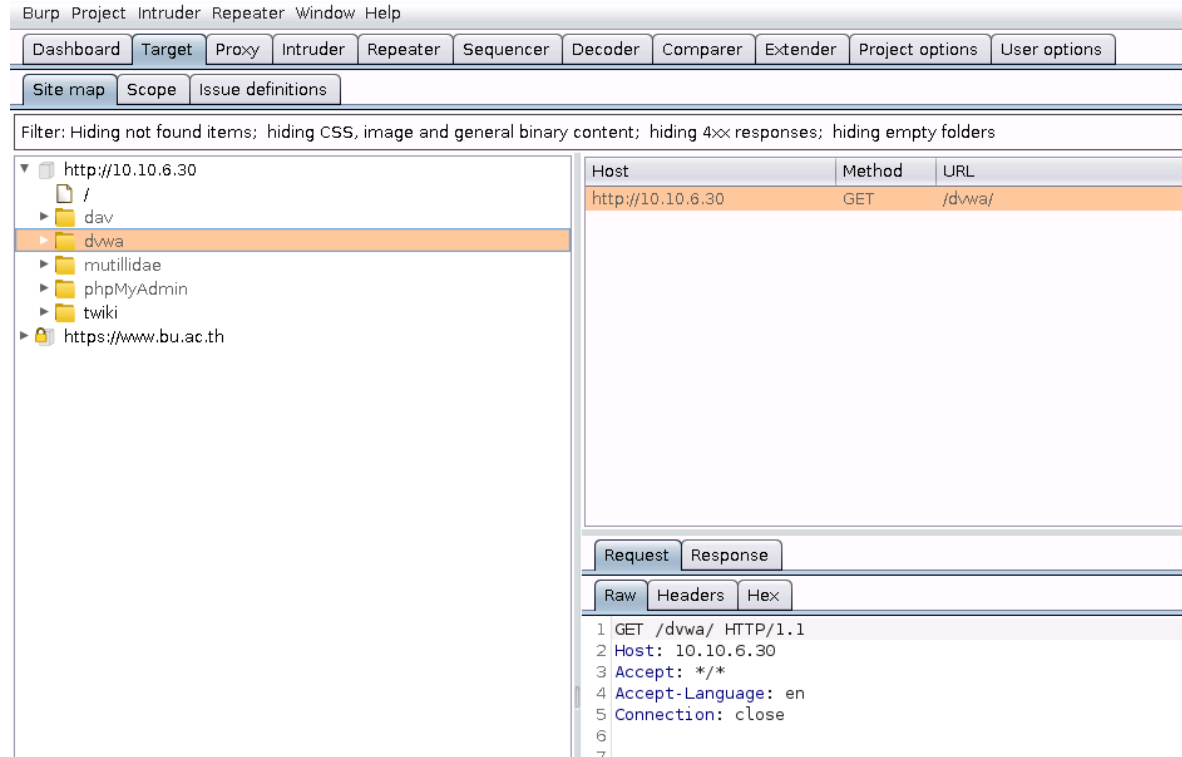
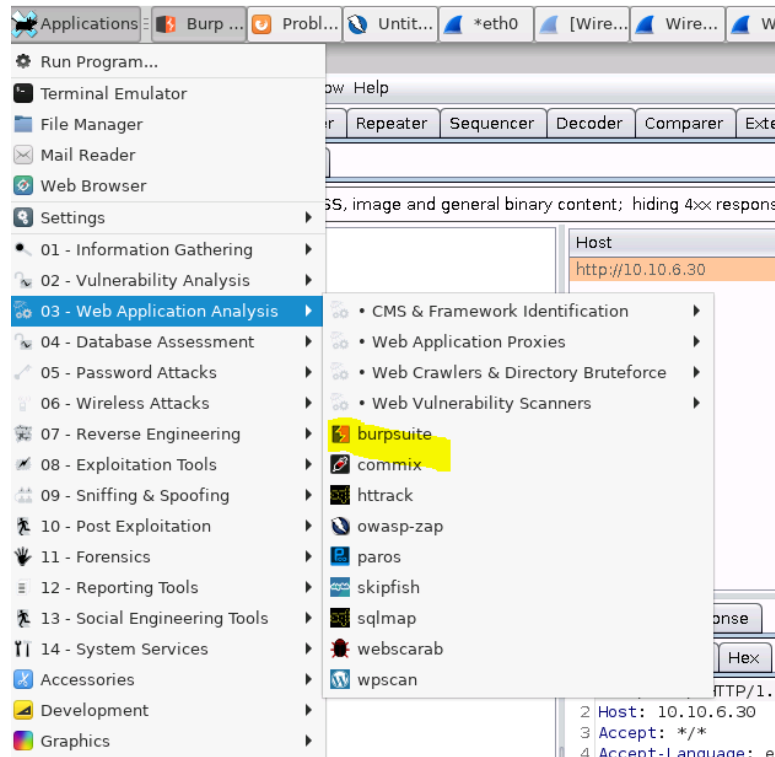
ZAP

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



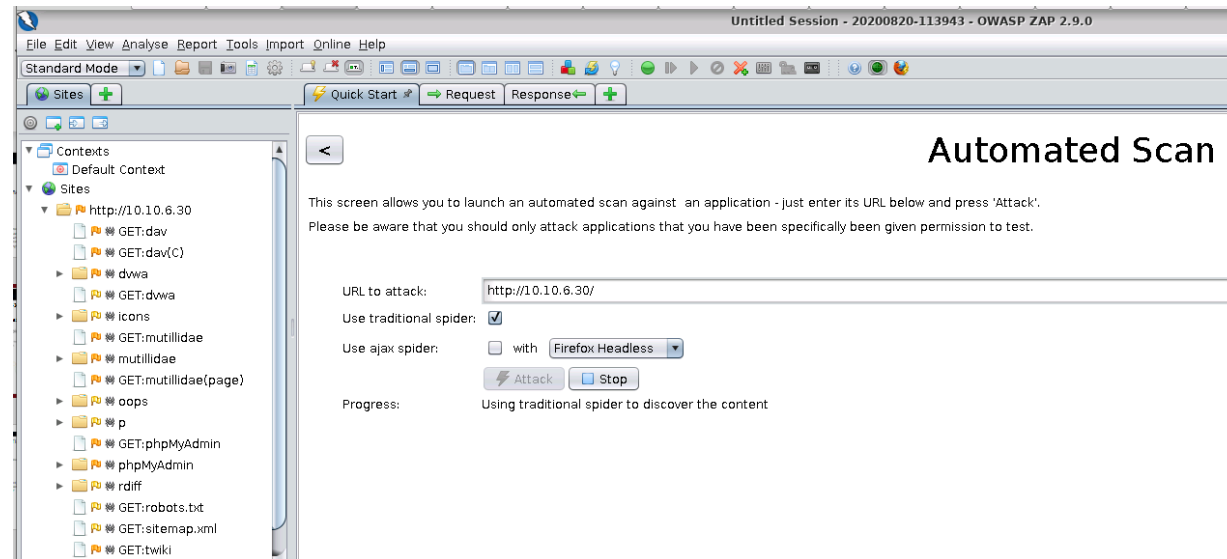
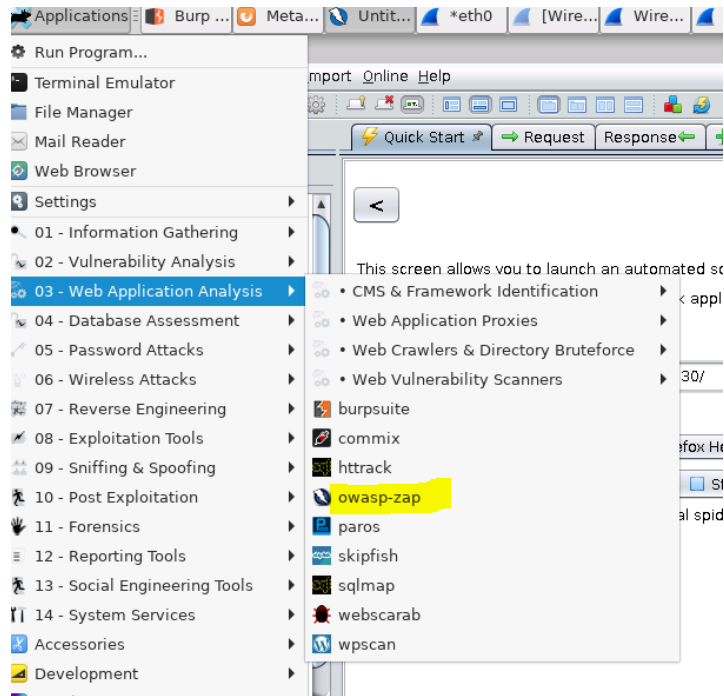
Web Application

- Menu → 03 Web Application Analysis → burpsuit

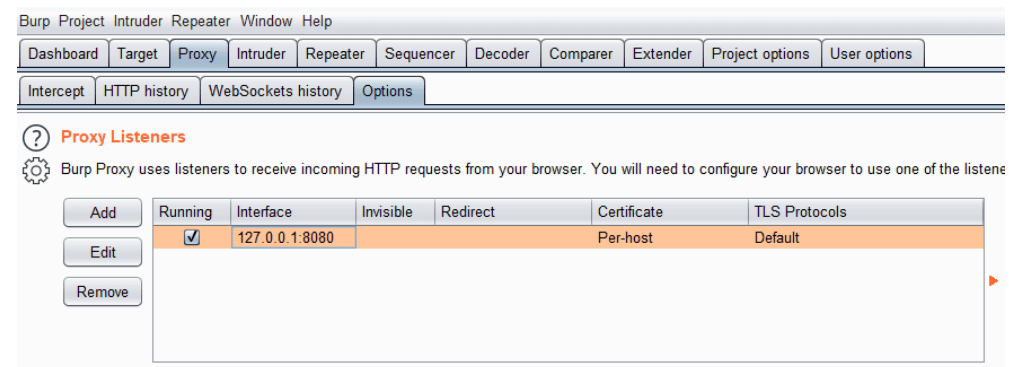
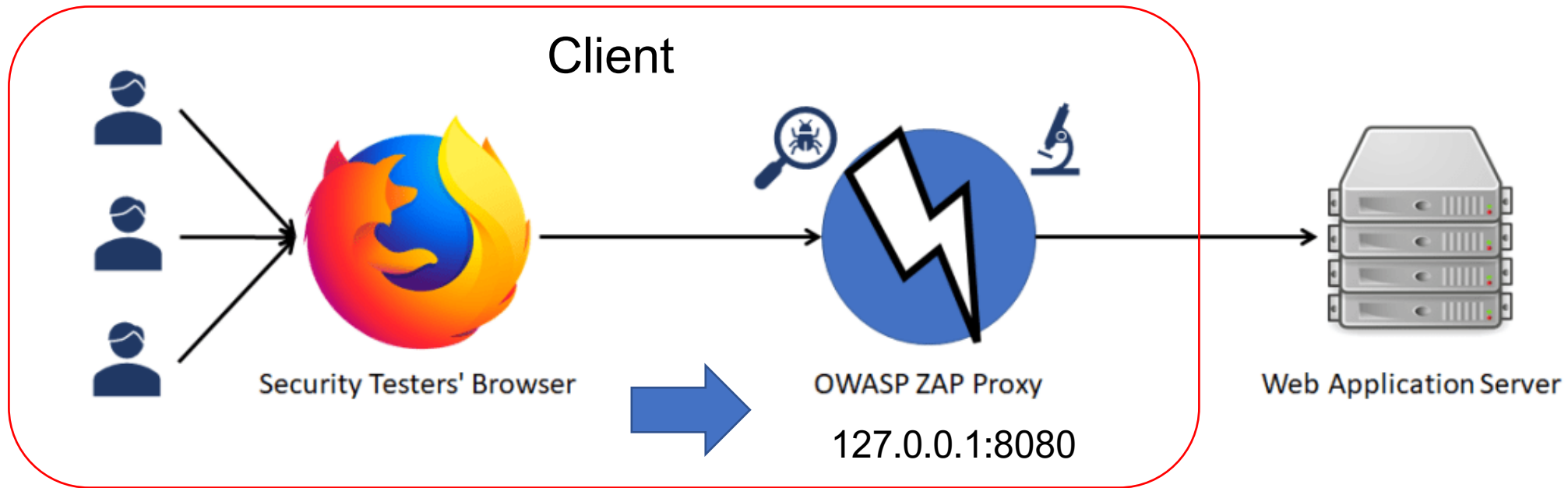


Web Application

- Menu → 03 Web Application Analysis → OWASP-Zap



Web Application



Tip: ให้ระวังเรื่อง Port ที่ใช้งานอยู่



Web Application

ตรวจสอบการเข้าใช้งาน ดูค่า HTTP request/response ผ่านเมนู HTTP history

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Par...	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
230	https://www.google.com	GET	/client_204?atyp=i&biw=1536&...	✓		204	828	HTML				✓	142.250.199.4
231	https://www.google.com	GET	/xjs/_/js/k=xjs.snr.en_GB.4IDL7u...	✓		200	140113	script				✓	142.250.199.4
249	http://testphp.vulnweb.com	POST	/userinfo.php	✓		302	253	text	php				44.228.249.3

Request

PrettyRawHex

1 POST /userinfo.php HTTP/1.1

2 Host: testphp.vulnweb.com

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 29

9 Origin: http://testphp.vulnweb.com

10 Connection: close

11 Referer: http://testphp.vulnweb.com/login.php

12 Upgrade-Insecure-Requests: 1

13

14 uname=admin&pass=admin%40test

Response

PrettyRawHexRender

1 HTTP/1.1 302 Found

2 Server: nginx/1.19.0

3 Date: Mon, 11 Sep 2023 05:18:45 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: close

6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

7 Location: login.php

8 Content-Length: 14

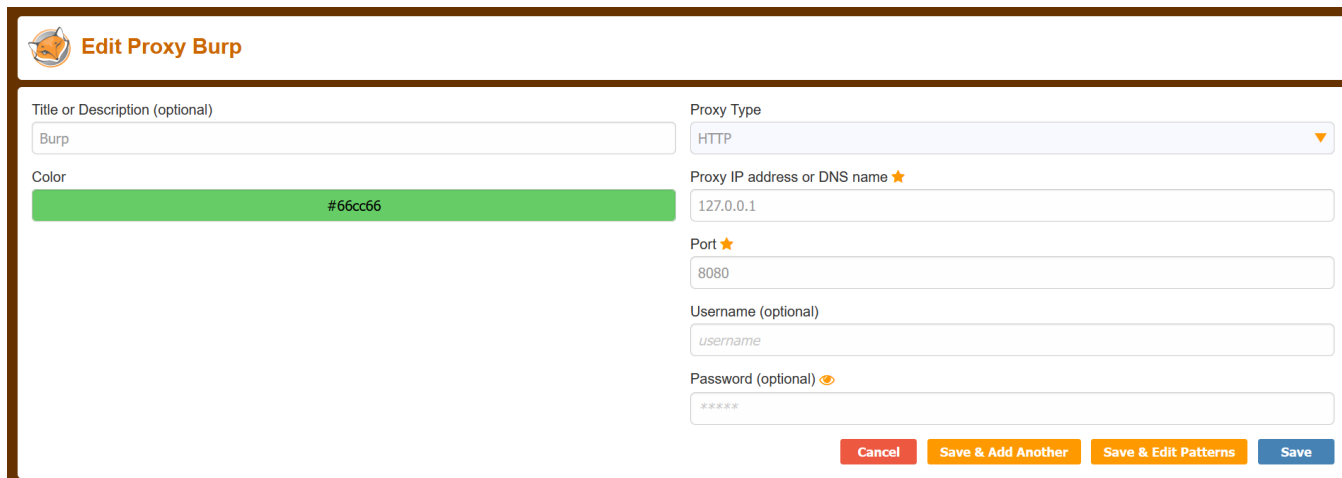
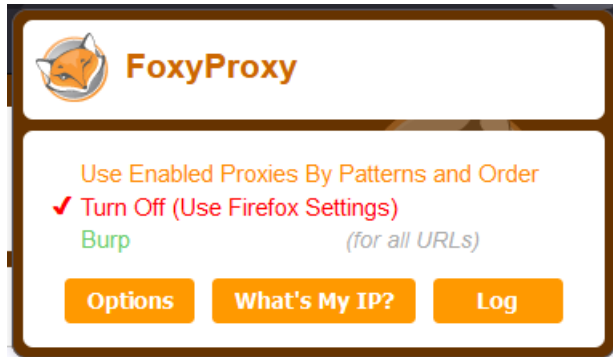
9

10 you must login



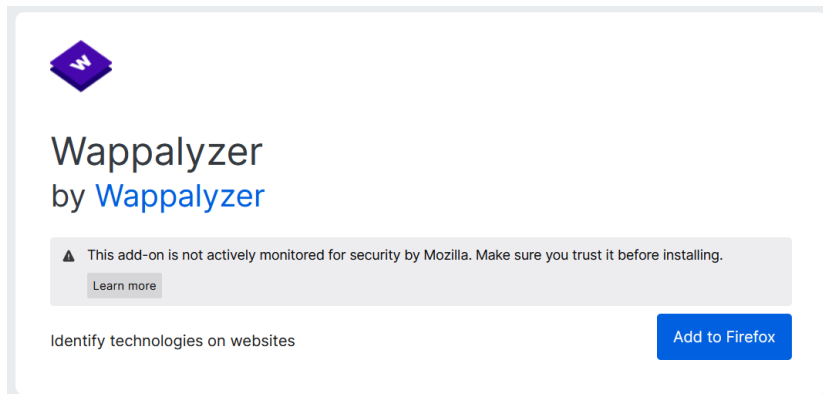
Web Application

Useful extensions : FoxyProxy

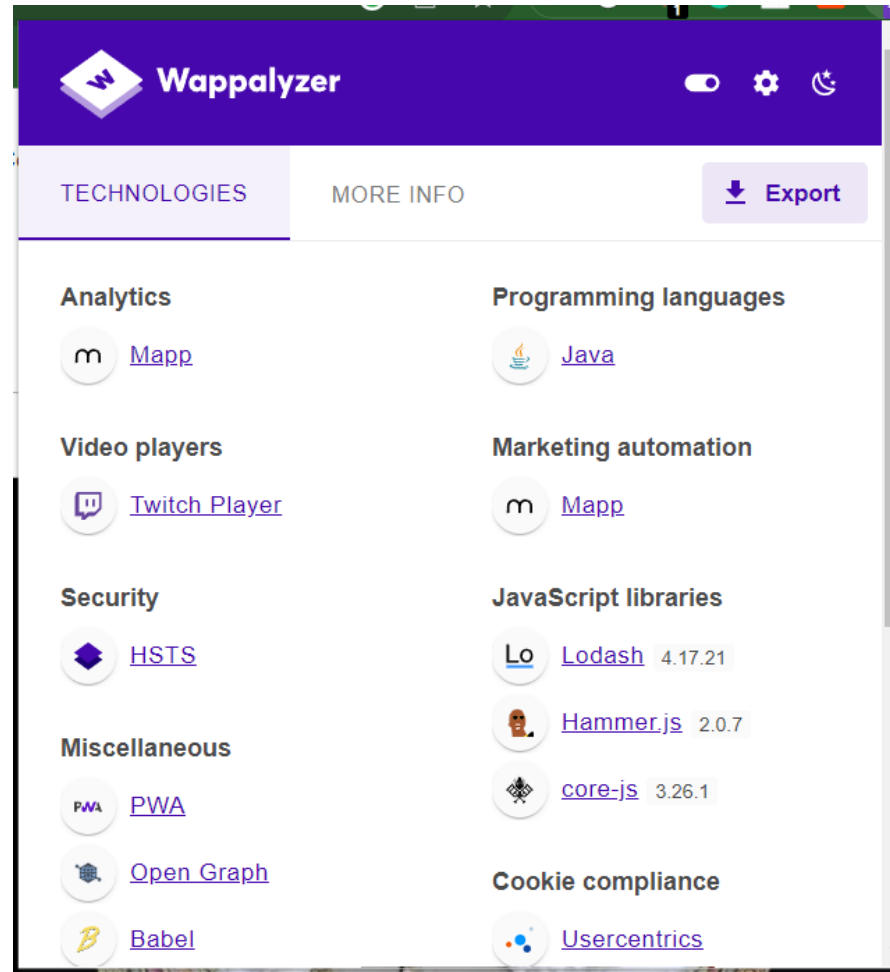
The image shows the "Edit Proxy Burp" form. The form has a header with the FoxyProxy logo and the title "Edit Proxy Burp". Below the header, there are two columns of input fields. The left column contains a "Title or Description (optional)" field with the value "Burp", and a "Color" field with a green color swatch and the hex code "#66cc66". The right column contains a "Proxy Type" dropdown menu with "HTTP" selected, a "Proxy IP address or DNS name" field with the value "127.0.0.1", a "Port" field with the value "8080", a "Username (optional)" field with the value "username", and a "Password (optional)" field with a masked password. At the bottom of the form, there are four buttons: "Cancel", "Save & Add Another", "Save & Edit Patterns", and "Save".

Web Application

Useful extensions : Wappalyzer



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



Web Application

Useful extensions : whatruns



WhatRuns
by [Whatruns](#)

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.
[Learn more](#)

Discover what runs a website - This Firefox extension helps you identify technologies used on any website at the click of a button.

[Add to Firefox](#)

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

What runs db.com?  

Analytics	Web Server
 Webtrekk	 Apache 2.2.3
Dev Tools	Javascript Frameworks
 HTML5 Shiv	 Hammer.js
	 Modernizr 2.8.3
	 TweenMax
	 jQuery 3.3.1
	 Respond JS
	Font
	Font Deutsche Bank Text
	Font Family Deutsche Bank Text, Arial, Helvetica Neue, Helvetica.

 **whatruns**



Web Application

Search public exploit code

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



The screenshot shows the Exploit Database website interface. The header includes the logo and navigation icons. Below the header, there are filters for 'Verified' and 'Has App', a 'Show 15' dropdown, and a search bar containing 'apache 2.2.3'. The search results are displayed in a table with columns: Date, D, A, V, Title, Type, Platform, and Author. Three results are shown, filtered from a total of 45,767 entries. The first result is for 'Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak' by Hanno Bock. The second is 'Apache Struts 2.2.3 - Multiple Open Redirections' by Takeshi Terada. The third is 'Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow' by Jacobo Avariento. The page number '1' is highlighted in the pagination controls.

Date	D	A	V	Title	Type	Platform	Author
2017-09-18	📄	✗		Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak	WebApps	Linux	Hanno Bock
2013-07-16	📄	✓		Apache Struts 2.2.3 - Multiple Open Redirections	Remote	Multiple	Takeshi Terada
2006-08-21	📄	✓	📄	Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow	Remote	Multiple	Jacobo Avariento

Showing 1 to 3 of 3 entries (filtered from 45,767 total entries)

Pagination: FIRST PREVIOUS 1 NEXT LAST



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
```

```
kali@H
File Actions Edit View Help
(kali@HackAtMin)-[~]
$ gobuster dir -u http://10.10.10.245/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php

/admin      (Status: 302) [Size: 0] [--> /login.jsp]
/aux        (Status: 200) [Size: 0]
/robots.txt (Status: 200) [Size: 0]
/images     (Status: 302) [Size: 0] [--> /images/]
/lpt1       (Status: 200) [Size: 0]
/static     (Status: 302) [Size: 0] [--> /static/]
/util       (Status: 302) [Size: 0] [--> /util/]
```

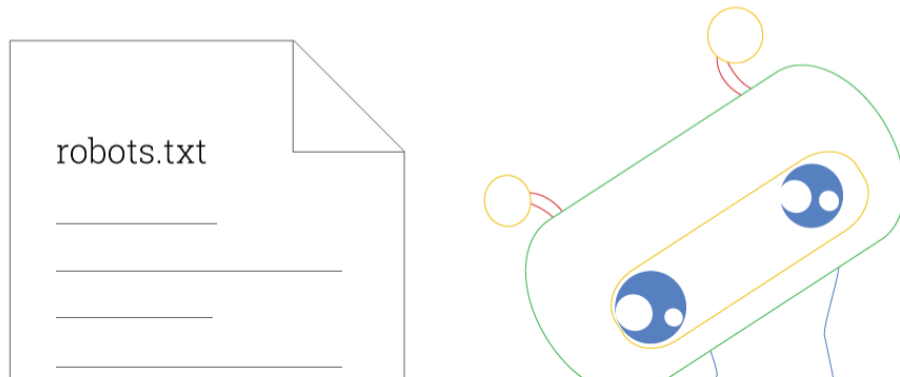


Web Application

- `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
```

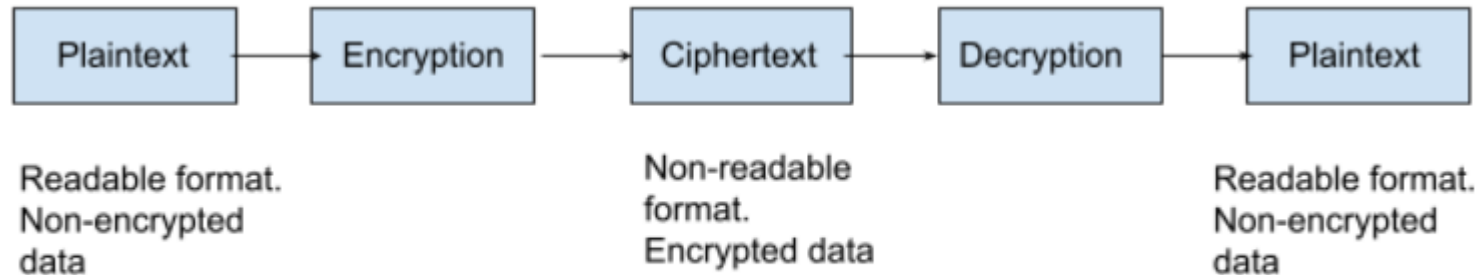
```
|-- Usernames
```

```
`-- Web-Shells
```



Cryptography

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



Cryptography



Cryptography

จูเลียส ซีซาร์
(Julius Caesar)

อดีตผู้เผด็จการโรมัน



กาอึส ยูลิอุส ไกซาร์ หรือ จูเลียส ซีซาร์ เป็นรัฐบุรุษ แม่ทัพ และผู้ประพันธ์ร้อยแก้วอันเลื่องชื่อชาวโรมัน เขามีบทบาทสำคัญในเหตุการณ์อันนำไปสู่การสิ้นสุดสาธารณรัฐโรมันและความเจริญของจักรวรรดิโรมัน ใน 60 ปีก่อน ค.ศ. [วิกิพีเดีย](#)

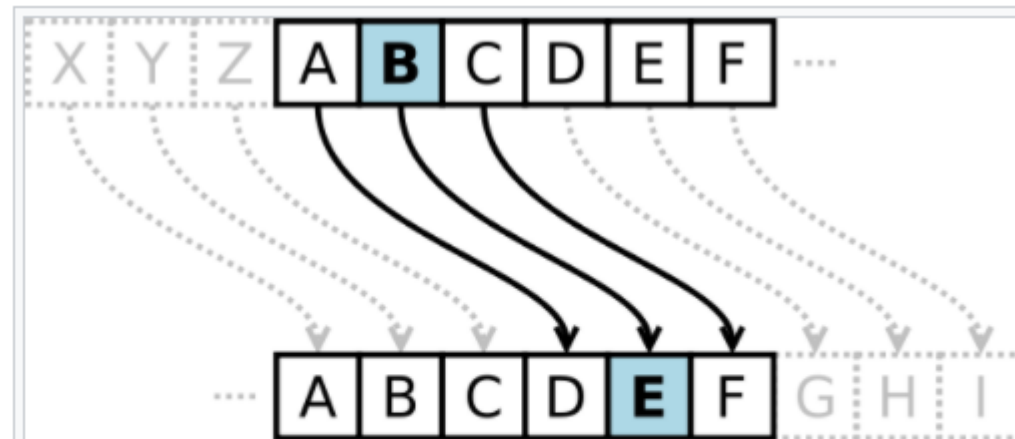
เกิด: 12 กรกฎาคม พ.ศ. 444, โรม, อิตาลี

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), กัลปूरินิอา (สมรส พ.ศ. 485–พ.ศ. 500)

บุตร: จักรพรรดิเอากุสตุส, ทอเลมีที่ 15 ซีซาร์เรียน, จูเลีย ซีซาร์ริส



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



Cryptography

Tool: CyberChef

<https://gchq.github.io>

Download CyberChef  Last build: A month ago - Version 10 is here! Read about the new feature... Options  About / Support

Operations

Search...

Favourites 

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Recipe   

2. Operation ที่ต้องการ
เข้ารหัส หรือ ถอดรหัส

STEP   Auto Bake

Input     

1. จุดกรอกข้อมูล Input

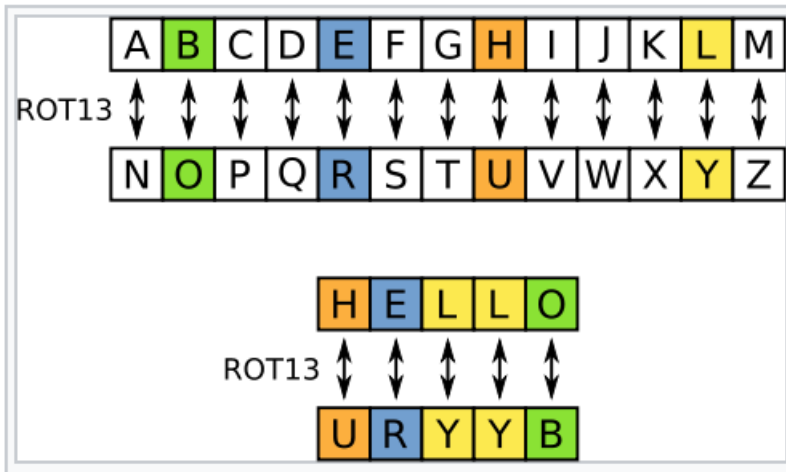
Output    

3. จุดแสดงข้อมูล Output



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.



Recipe	Input
ROT13	TB-CERT Cyber combat 2023
☒ Rotate lower case chars	
☒ Rotate upper case chars	
☒ Rotate numbers	
Amount 13	
	abc 25 1
	Output
	GO-PREG Plore pbzong 5356



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

Recipe

To Binary

Delimiter
Space

Byte Length
8

Input

TB-CERT Cyber combat 2023

Output

01010100 01000010 00101101 01000011 01000101 01010010
01010100 00100000 01000011 01111001 01100010 01100101
01110010 00100000 01100011 01101111 01101101 01100010
01100001 01110100 00100000 00110010 00110000 00110010
00110011



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

Recipe

To Hex

Delimiter
Space

Bytes per line
0

Input

TB-CERT Cyber combat 2023

Output

54 42 2d 43 45 52 54 20 43 79 62 65 72 20 63 6f 6d 62 61
74 20 32 30 32 33 0a



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.

Hashing



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

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin))

Hash	Type	Result
5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	sha1	password

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

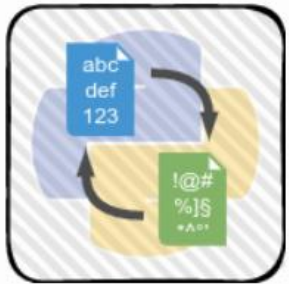
[Download CrackStation's Wordlist](#)



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 "KZCUS5CRGBLFGVSDIJGWEM22NREU0VRSLJMEUNLCGI2WY==" | 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.

Morse Translator and Decoder

A	B	C	D	E	F	G
.._	..._	..._.	.._.	. .	..._.	..._.
H	I	J	K	L	M	N
....	.. .	.._.	..._.	.._.	_ .	.._.
O	P	Q	R	S	T	
_ .	..._.	..._.	.._.		_ .	
U	V	W	X	Y	Z	
_ .	..._.	..._.	..._.	..._.	..._.	
1	2	3	4	5		
_ .	..._.	..._.				
6	7	8	9	0		
....		..._.				

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)



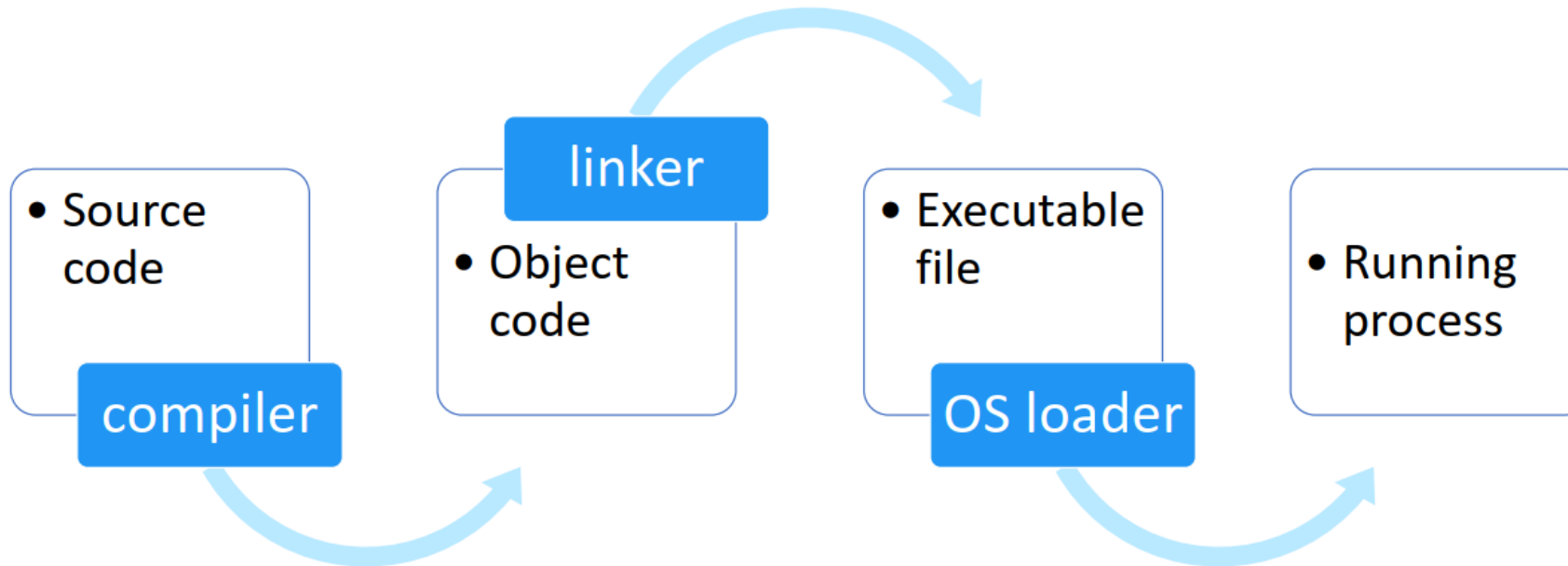
Human readable

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



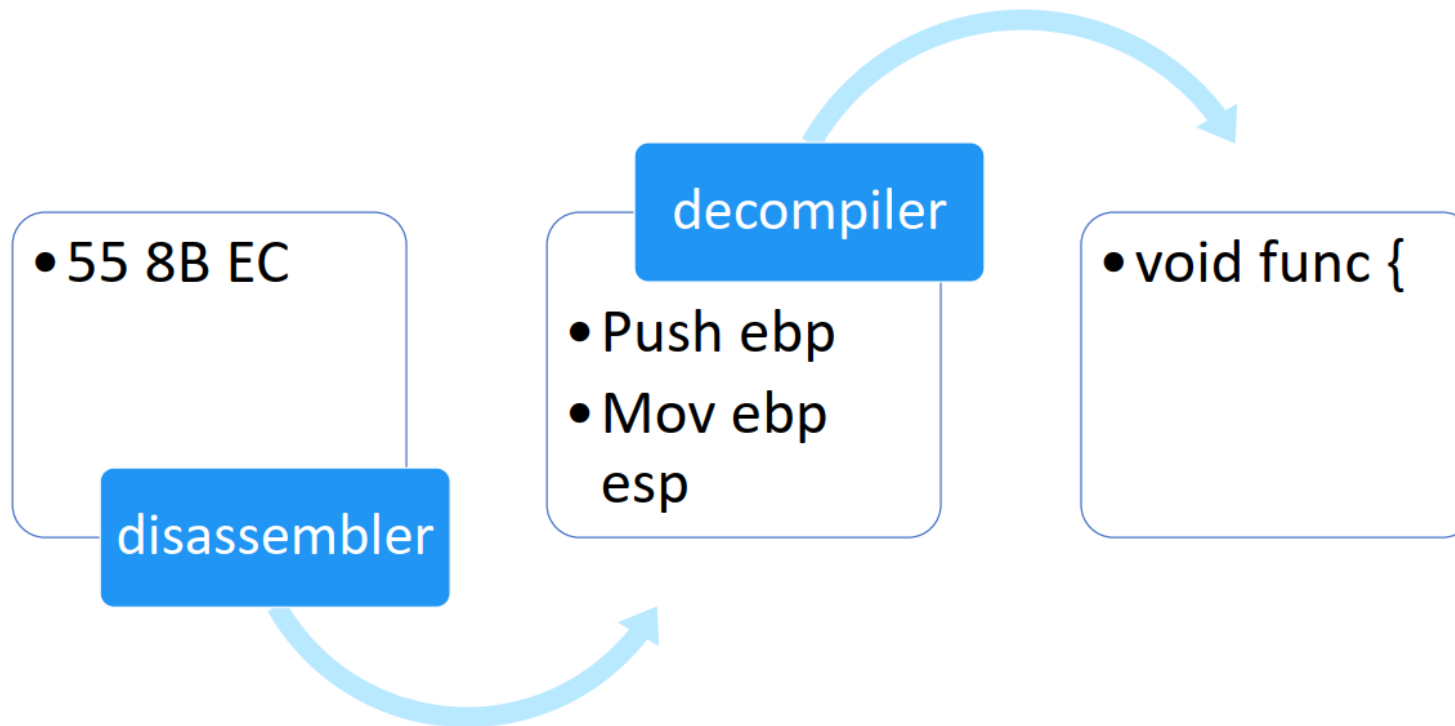
Reverse engineering

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

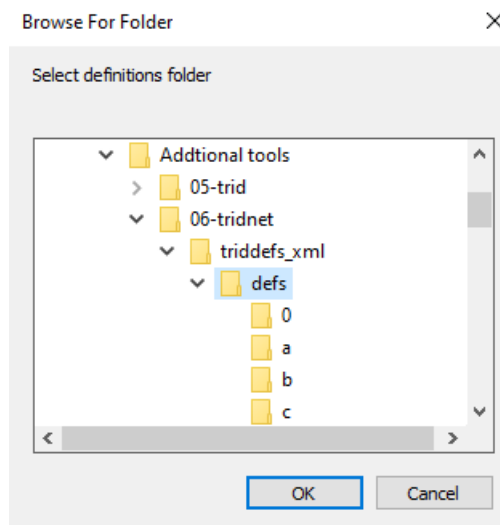
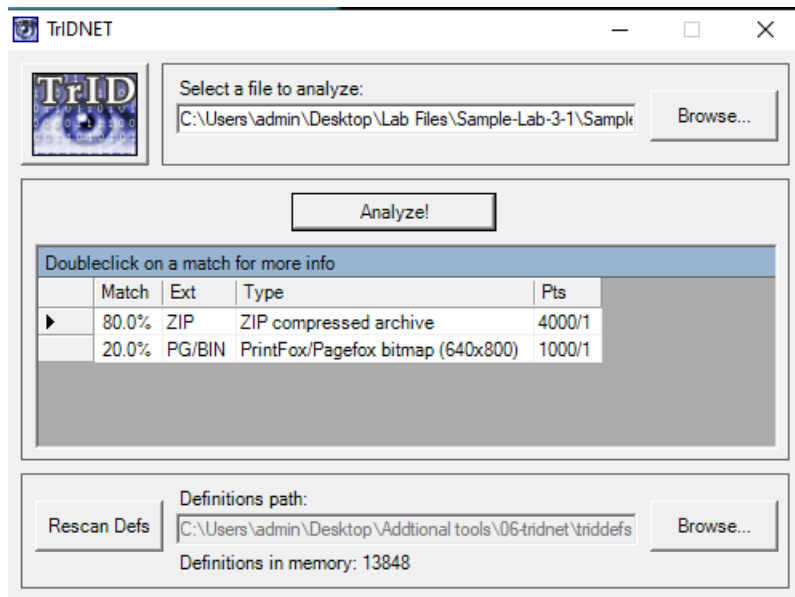
Tool: TrIDNet is an utility designed to identify file types from their binary signatures.

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)



Built-in tool on Kali Linux

strings - print the sequences of printable characters in files

Open with cat

```
(kali@atmin)-[~/Downloads/tb-cert]
$ cat pass_test
PP      PX888 XXXDDS888
start_main__cxa_finalize$syscallslib.so.6GLIBC_2.3
/HtH5/%/@%/h%/h%/f1I
+UH=.Ht
        H=.)d.]wUHHH
Fire
]$"D\ybA C
02
o o o o o
?0  o o o o o o o 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

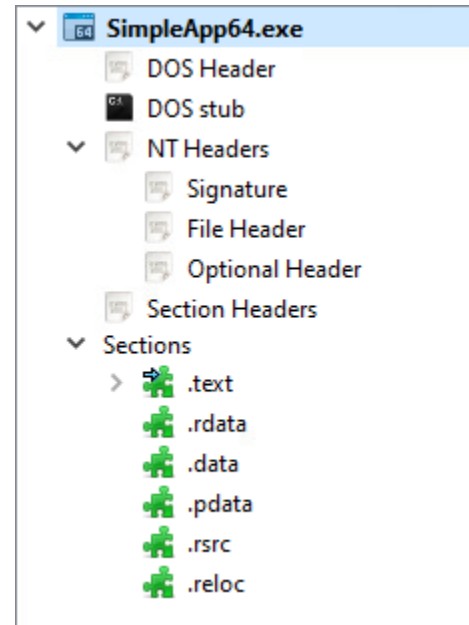
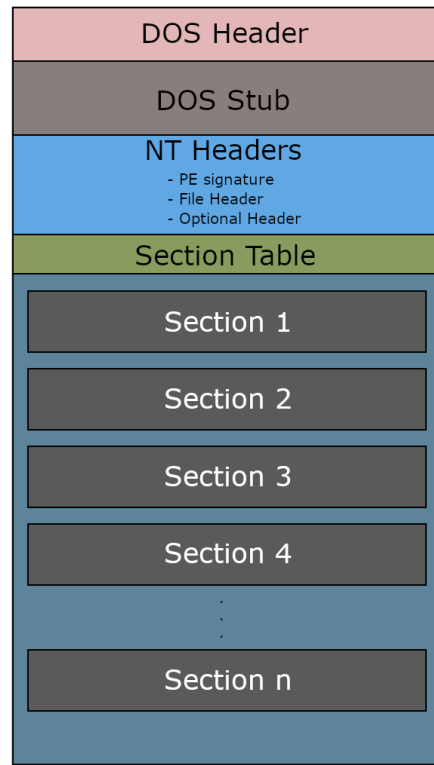
.acm	, .ax	, .cpl	, .dll	,
.drv	, .efi	, .exe	, .mui	,
.ocx	, .scr	, .sys	, .tsp	



Reverse engineering

Portable Executable (PE)

PE Structure



Reverse engineering



Portable Executable (PE)

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

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.



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.

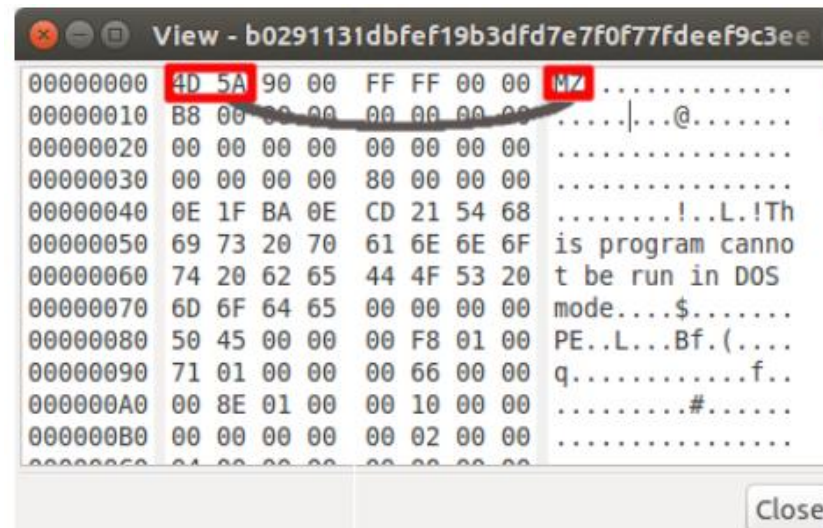


Reverse engineering

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.

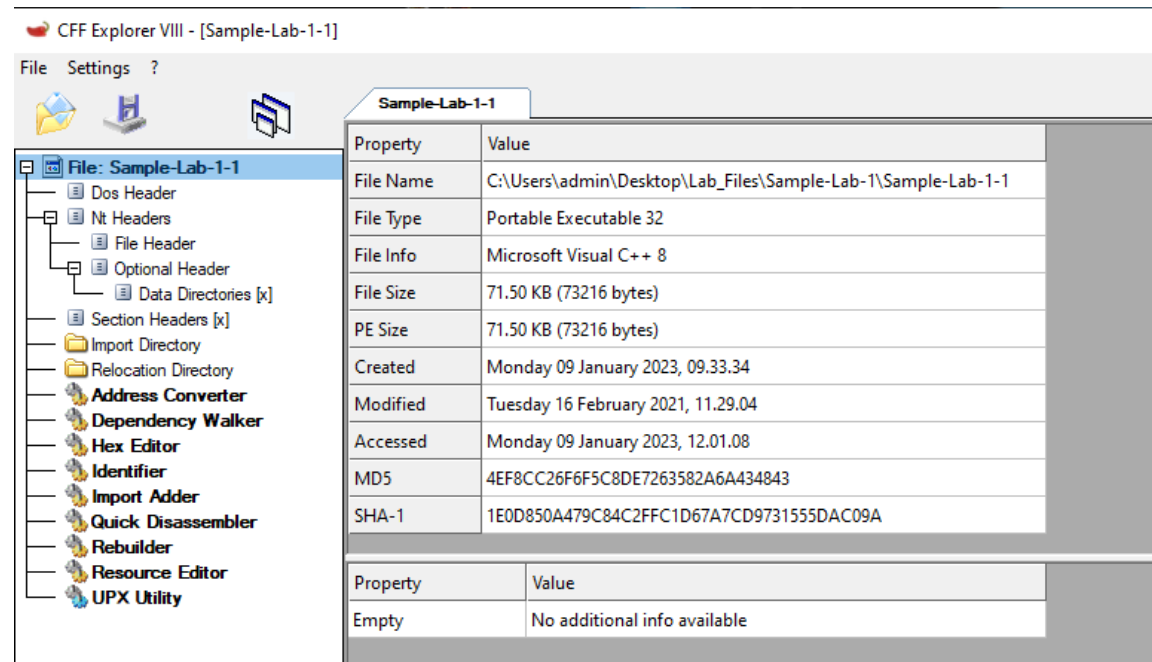


Reverse engineering

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.

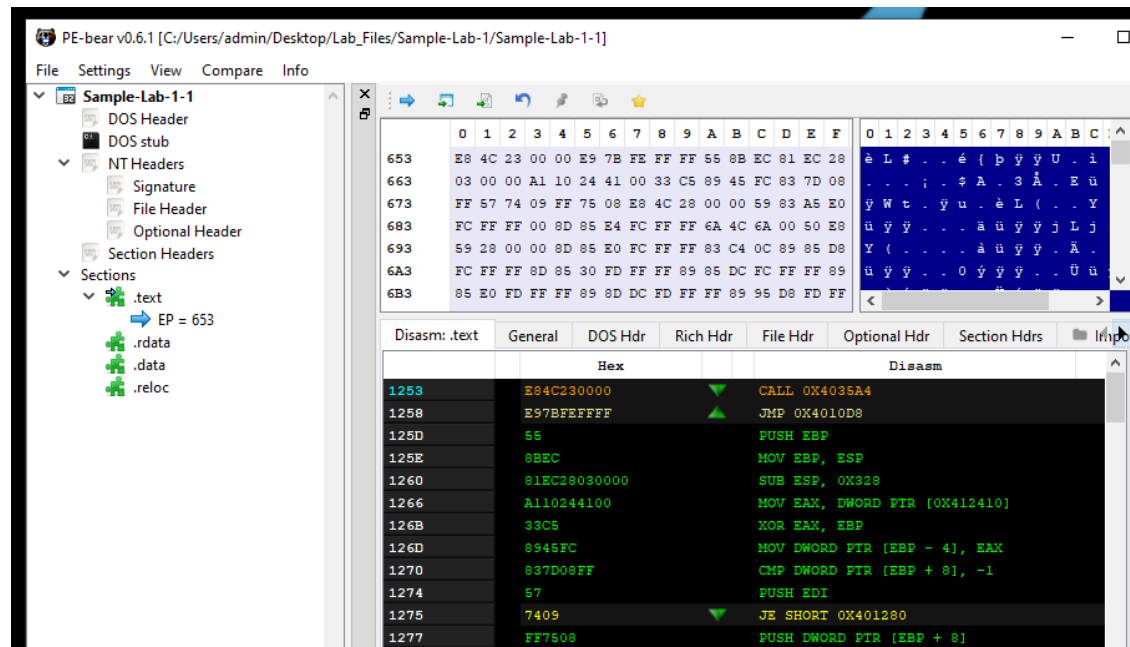


Reverse engineering

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

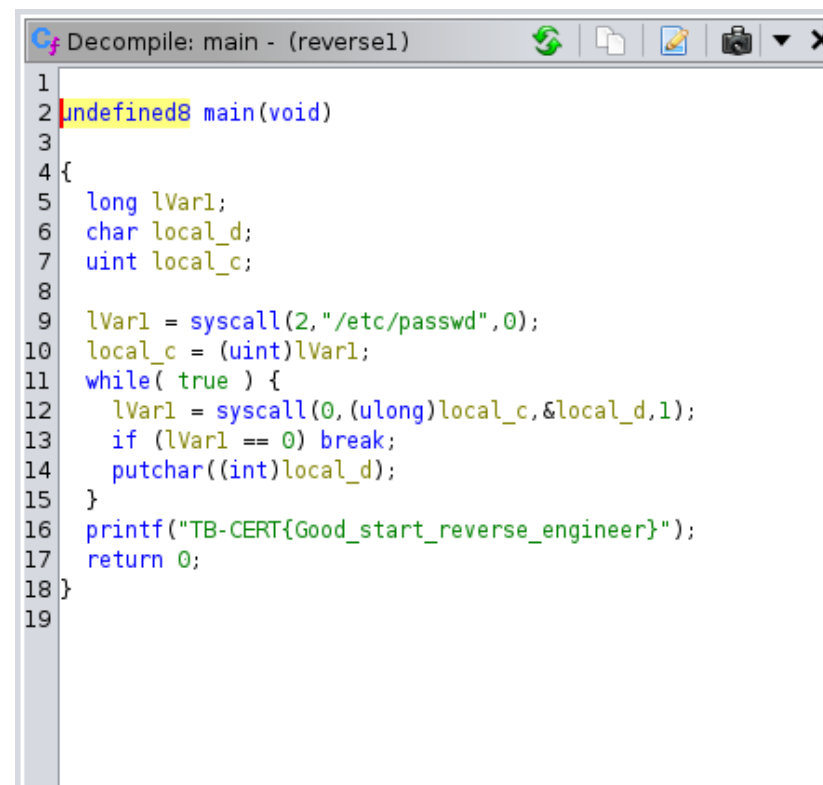
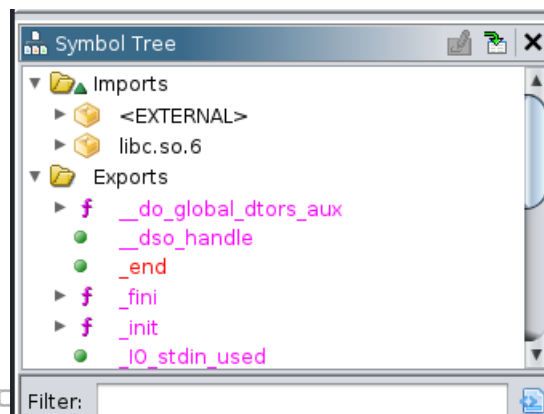
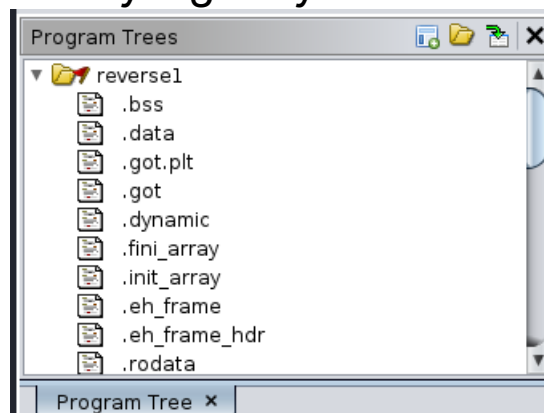


Reverse engineering

Tool: Ghidra

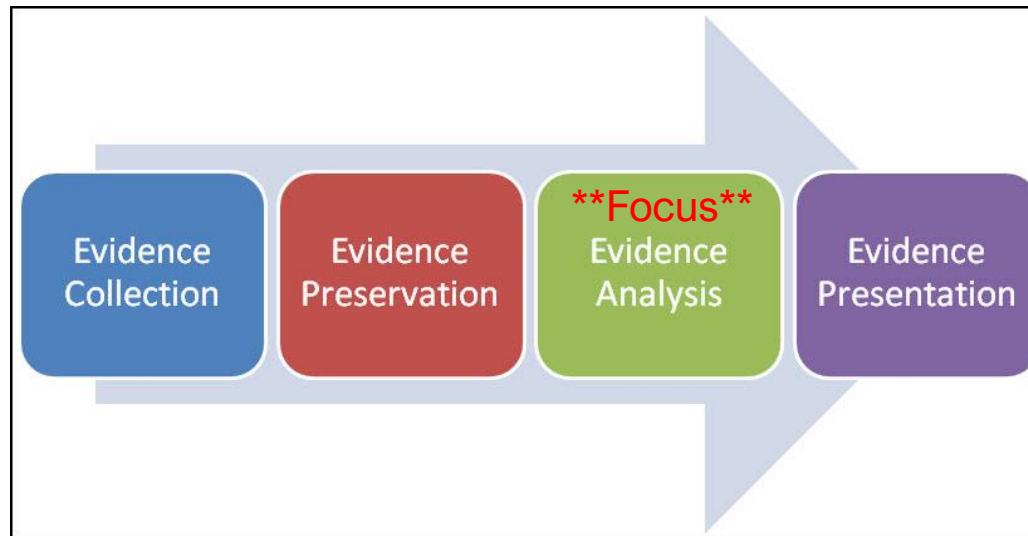
Install: `sudo apt install ghidra`

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
```



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)\0
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      PX888 XXXDDS888
start_main__cxa_finalizesyscalllibc.so.6GLIBC_2.3
/HtH5/%/@%/h%%/h%%/f1I
+UH=.Ht
        H=.)d.]wUHHeH
Fire
]$"DyybA^C
@2
o
?0 oooooo0ooo 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                  : 283x159
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
```

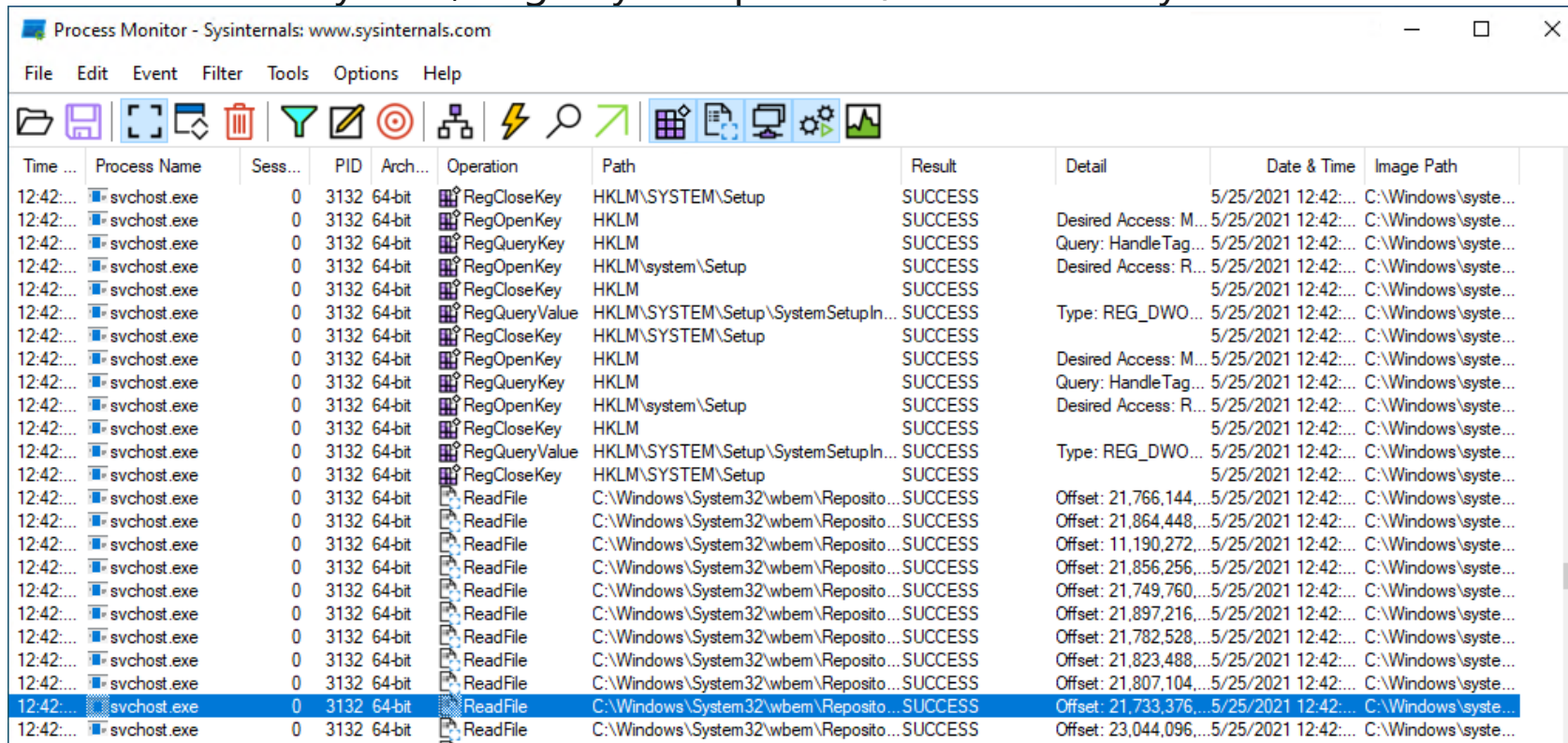


Digital Forensics

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\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM	SUCCESS	Desired Access: M...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM	SUCCESS	Desired Access: M...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS		5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,766,144...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,864,448...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 11,190,272...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,856,256...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,749,760...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,897,216...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,782,528...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,823,488...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,807,104...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 21,733,376...	5/25/2021 12:42:...	C:\Windows\sysste...
12:42:...	svchost.exe	0	3132	64-bit	ReadFile	C:\Windows\System32\wbem\Repository...	SUCCESS	Offset: 23,044,096...	5/25/2021 12:42:...	C:\Windows\sysste...

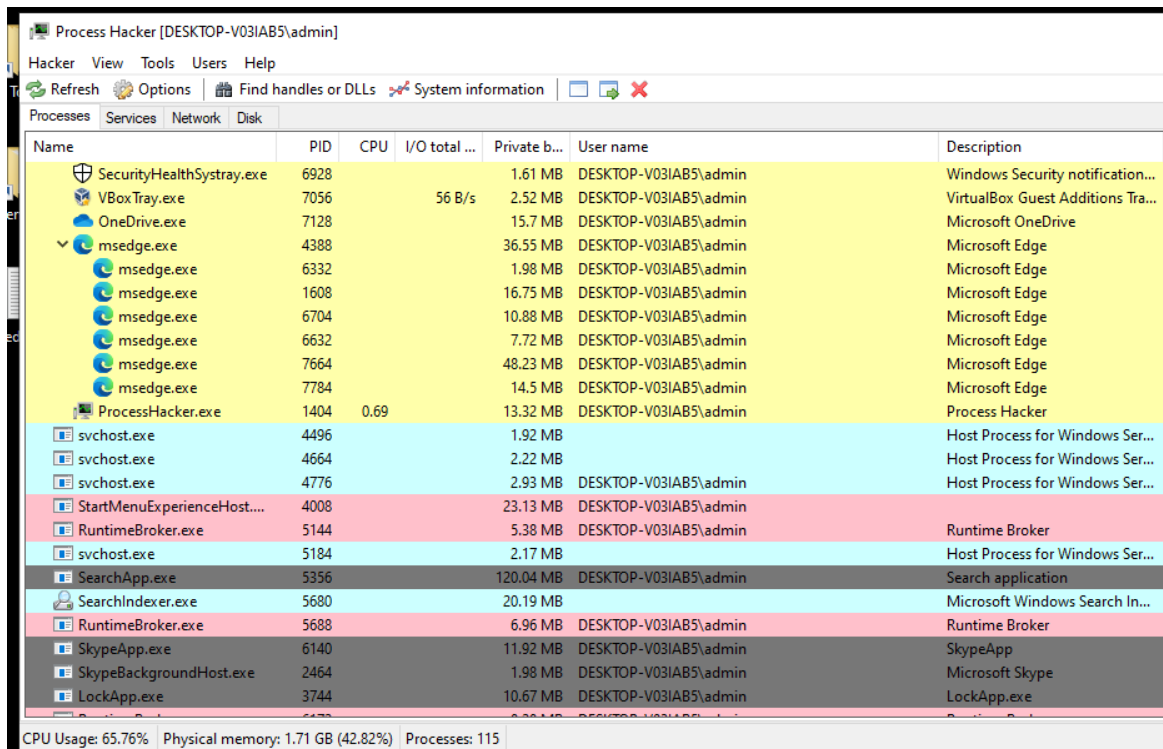


Digital Forensics

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.



The screenshot shows the Process Hacker application window. The title bar reads 'Process Hacker [DESKTOP-V03IAB5\admin]'. The menu bar includes 'Hacker', 'View', 'Tools', 'Users', and 'Help'. Below the menu is a toolbar with icons for 'Refresh', 'Options', 'Find handles or DLLs', and 'System information'. The main window has tabs for 'Processes', 'Services', 'Network', and 'Disk', with 'Processes' selected. A table lists running processes with columns for Name, PID, CPU, I/O total, Private b..., User name, and Description. The status bar at the bottom shows 'CPU Usage: 65.76%', 'Physical memory: 1.71 GB (42.82%)', and 'Processes: 115'.

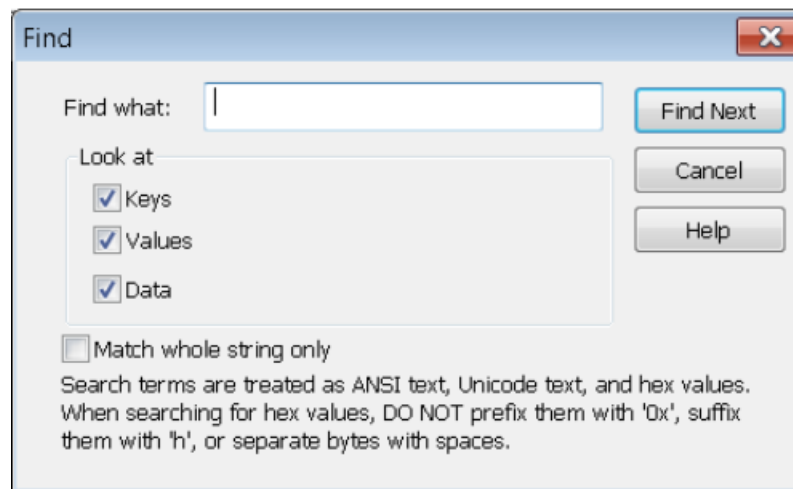
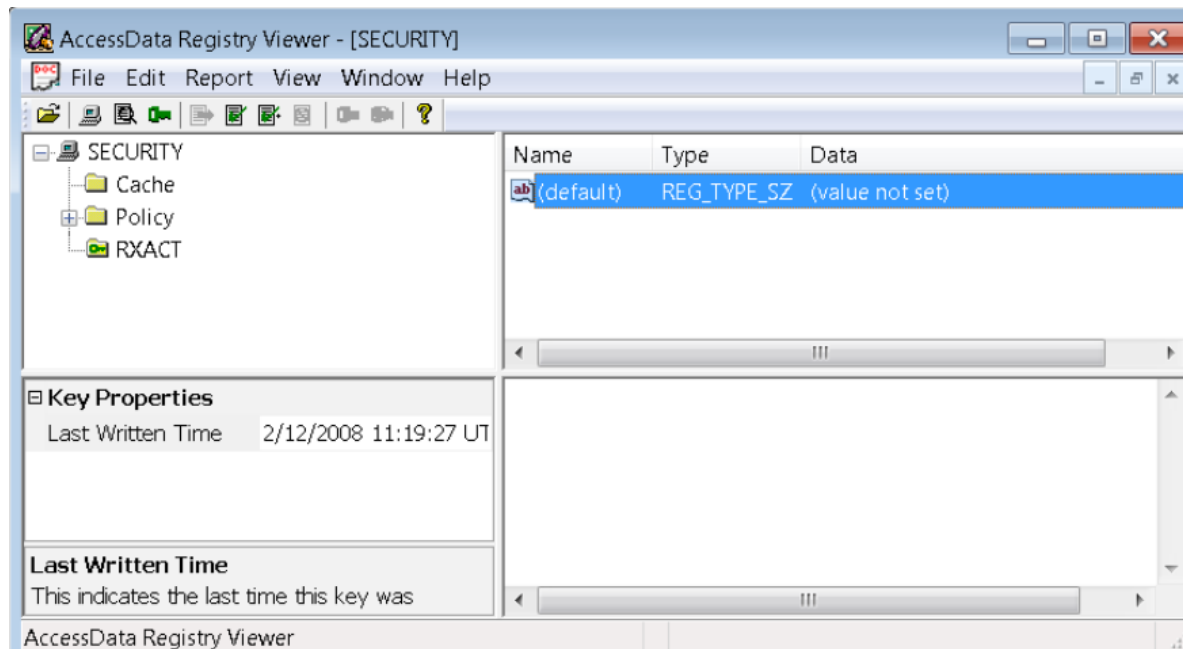
Name	PID	CPU	I/O total ...	Private b...	User name	Description
SecurityHealthSystray.exe	6928			1.61 MB	DESKTOP-V03IAB5\admin	Windows Security notification...
VBoxTray.exe	7056		56 B/s	2.52 MB	DESKTOP-V03IAB5\admin	VirtualBox Guest Additions Tra...
OneDrive.exe	7128			15.7 MB	DESKTOP-V03IAB5\admin	Microsoft OneDrive
msedge.exe	4388			36.55 MB	DESKTOP-V03IAB5\admin	Microsoft Edge
msedge.exe	6332			1.98 MB	DESKTOP-V03IAB5\admin	Microsoft Edge
msedge.exe	1608			16.75 MB	DESKTOP-V03IAB5\admin	Microsoft Edge
msedge.exe	6704			10.88 MB	DESKTOP-V03IAB5\admin	Microsoft Edge
msedge.exe	6632			7.72 MB	DESKTOP-V03IAB5\admin	Microsoft Edge
msedge.exe	7664			48.23 MB	DESKTOP-V03IAB5\admin	Microsoft Edge
msedge.exe	7784			14.5 MB	DESKTOP-V03IAB5\admin	Microsoft Edge
ProcessHacker.exe	1404	0.69		13.32 MB	DESKTOP-V03IAB5\admin	Process Hacker
svchost.exe	4496			1.92 MB		Host Process for Windows Ser...
svchost.exe	4664			2.22 MB		Host Process for Windows Ser...
svchost.exe	4776			2.93 MB	DESKTOP-V03IAB5\admin	Host Process for Windows Ser...
StartMenuExperienceHost.exe	4008			23.13 MB	DESKTOP-V03IAB5\admin	
RuntimeBroker.exe	5144			5.38 MB	DESKTOP-V03IAB5\admin	Runtime Broker
svchost.exe	5184			2.17 MB		Host Process for Windows Ser...
SearchApp.exe	5356			120.04 MB	DESKTOP-V03IAB5\admin	Search application
SearchIndexer.exe	5680			20.19 MB		Microsoft Windows Search In...
RuntimeBroker.exe	5688			6.96 MB	DESKTOP-V03IAB5\admin	Runtime Broker
SkypeApp.exe	6140			11.92 MB	DESKTOP-V03IAB5\admin	SkypeApp
SkypeBackgroundHost.exe	2464			1.98 MB	DESKTOP-V03IAB5\admin	Microsoft Skype
LockApp.exe	3744			10.67 MB	DESKTOP-V03IAB5\admin	LockApp.exe



Digital Forensics

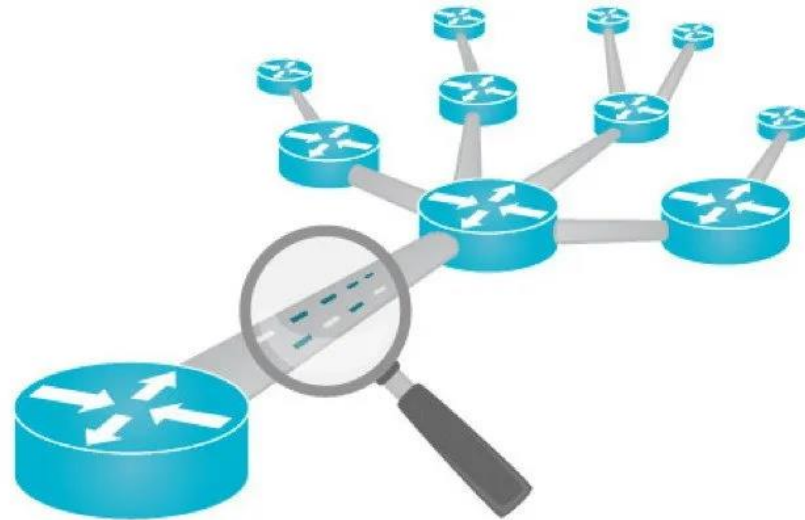
Registry Viewers

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



Network Analysis

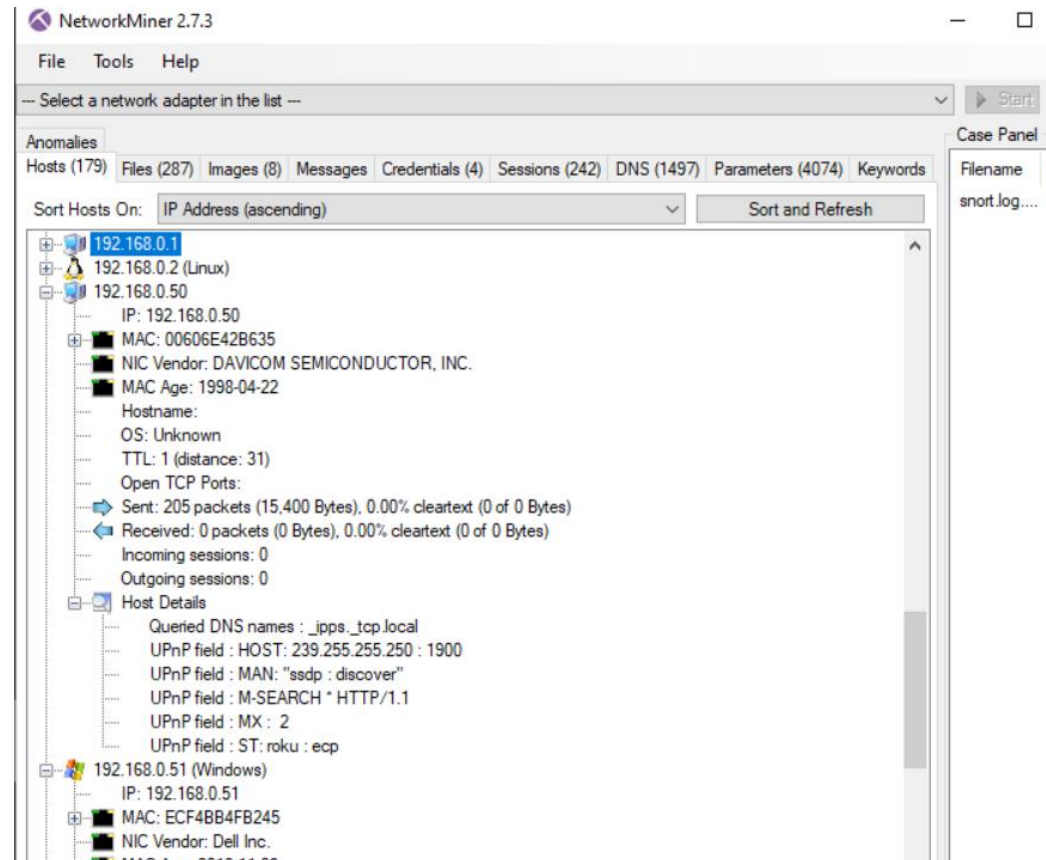
Network analysis is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.



Network Analysis

Tool: NetworkMiner

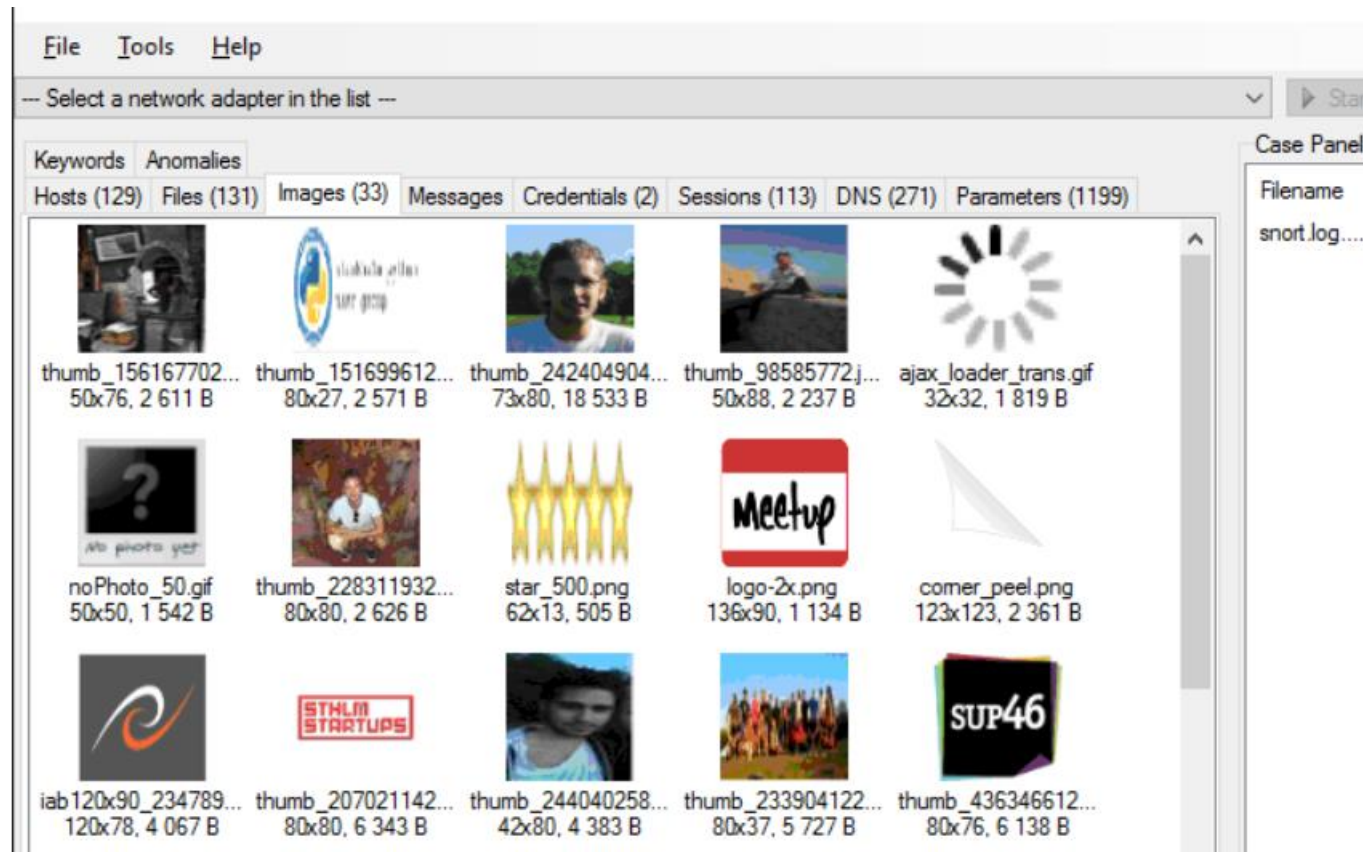
Install: <https://www.netresec.com/?page=NetworkMiner>



Network Analysis

Tool: NetworkMiner

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



Network Analysis

Tool: NetworkMiner

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

NetworkMiner 2.8

File Tools Help

-- Select a network adapter in the list --

Hosts (200) Files (227) Images Messages (1) Credentials (38) Sessions (585) DNS (519) Parameters (6262) Keywords Anomalies

☒ Show Cookies ☒ Show NTLM challenge-response ☐ Mask Passwords

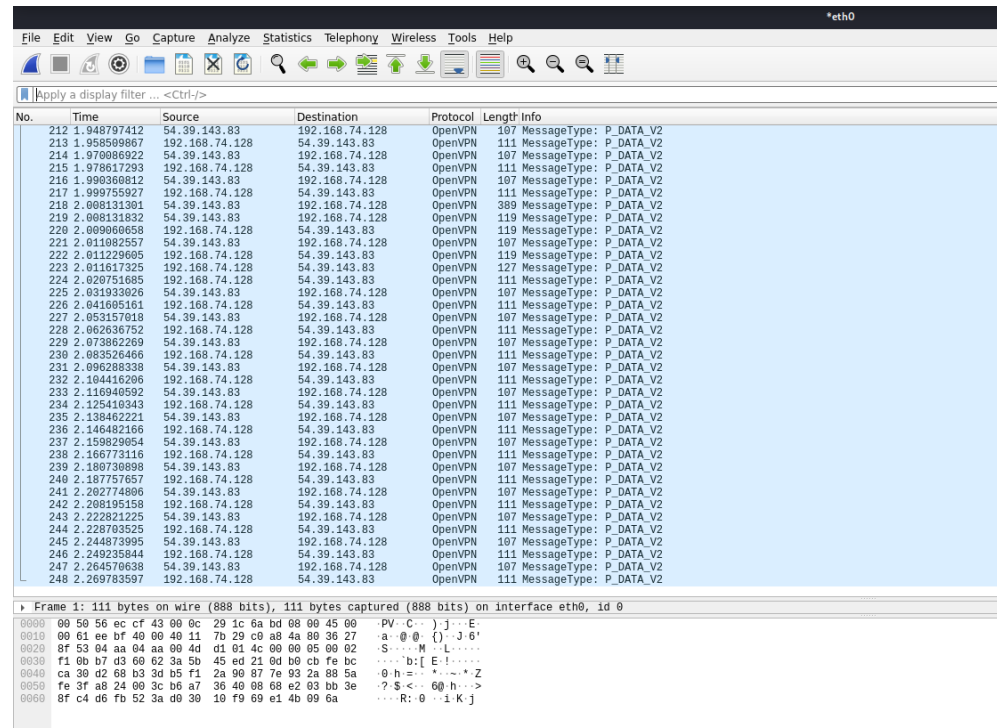
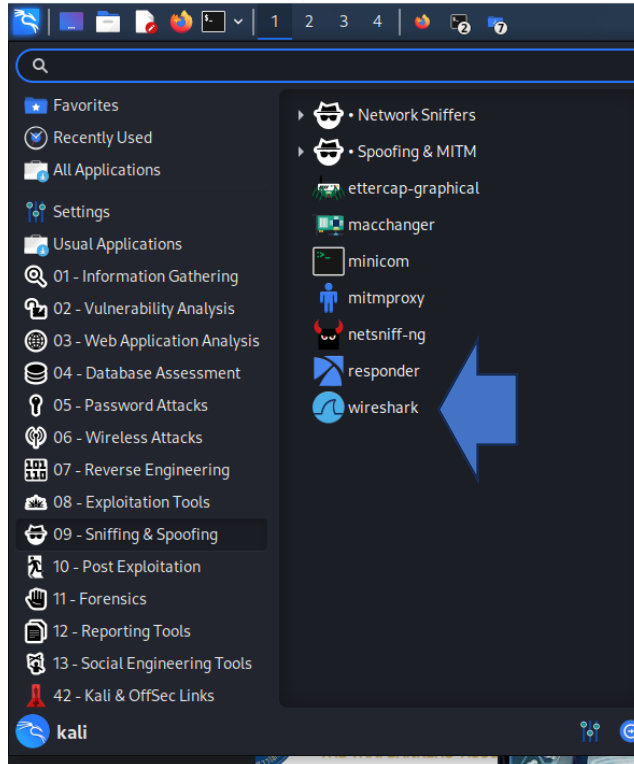
Client	Server	Protocol	Username	Password	Valid login	Login timestamp
172.16.0.149 [D...	116.254.112.253 [...	SMTP	hrd5_hr@idn-ltd.com	!Efrid4lts3#ok	Yes	2022-02-23 19:07
172.16.0.170 [D...	172.16.0.52 [sunn...	Kerberos	everett.french	\$krb5asrep\$18\$SUNNYSTATION.COMeverett.french\$776...	Unknown	2022-02-23 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	<code>ip.addr == 10.10.50.1</code>
Filter by Destination IP	<code>ip.dest == 10.10.50.1</code>
Filter by Source IP	<code>ip.src == 10.10.50.1</code>
Filter by IP range	<code>ip.addr >= 10.10.50.1 and ip.addr <= 10.10.50.100</code>
Filter by Multiple Ips	<code>ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100</code>
Filter out IP address	<code>!(ip.addr == 10.10.50.1)</code>
Filter subnet	<code>ip.addr == 10.10.50.1/24</code>
Filter by port	<code>tcp.port == 25</code>
Filter by destination port	<code>tcp.dstport == 23</code>
Filter by ip address and port	<code>ip.addr == 10.10.50.1 and Tcp.port == 25</code>



Network Analysis

Tool: WireShark

Built-in tool on Kali Linux

Useful filters

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

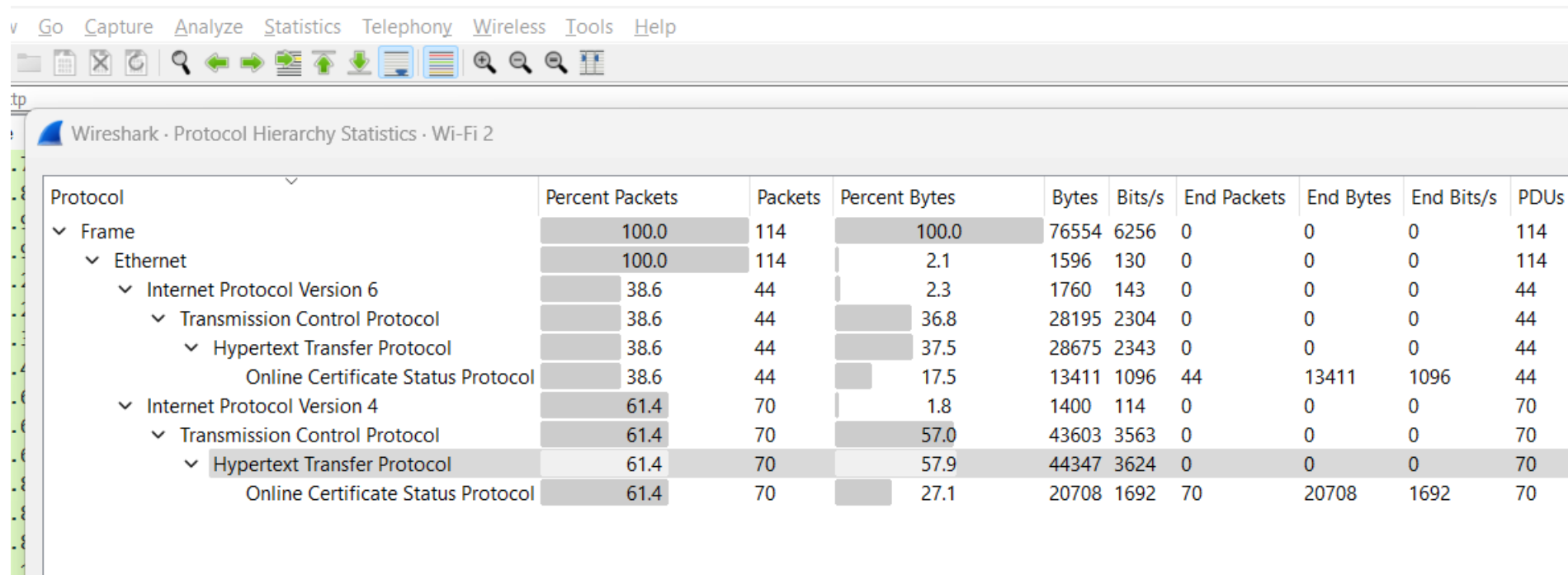


Network Analysis

Tool: WireShark
Built-in tool on Kali Linux

Useful functions

Protocol Hierarchy (Statistics-> Protocol Hierarchy)



The screenshot shows the Wireshark Protocol Hierarchy Statistics window for a capture named 'Wi-Fi 2'. The window displays a tree view of protocols on the left and a corresponding table of statistics on the right. The table includes columns for Protocol, Percent Packets, Packets, Percent Bytes, Bytes, Bits/s, End Packets, End Bytes, End Bits/s, and PDUs. The hierarchy starts with 'Frame' (100.0% packets, 114 total), which branches into 'Ethernet' (100.0% packets, 114 total). 'Ethernet' further branches into 'Internet Protocol Version 6' (38.6% packets, 44 total) and 'Internet Protocol Version 4' (61.4% packets, 70 total). 'IPV6' branches into 'Transmission Control Protocol' (38.6% packets, 44 total) and 'Hypertext Transfer Protocol' (38.6% packets, 44 total). 'TCP' branches into 'Online Certificate Status Protocol' (38.6% packets, 44 total) and 'Hypertext Transfer Protocol' (38.6% packets, 44 total). 'HTTP' branches into 'Online Certificate Status Protocol' (38.6% packets, 44 total) and 'Hypertext Transfer Protocol' (38.6% packets, 44 total). 'IPV4' branches into 'Transmission Control Protocol' (61.4% packets, 70 total) and 'Hypertext Transfer Protocol' (61.4% packets, 70 total). 'TCP' branches into 'Online Certificate Status Protocol' (61.4% packets, 70 total) and 'Hypertext Transfer Protocol' (61.4% packets, 70 total). 'HTTP' branches into 'Online Certificate Status Protocol' (61.4% packets, 70 total) and 'Hypertext Transfer Protocol' (61.4% packets, 70 total).

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)

Wireshark · Conversations · Wi-Fi 2											
Conversation Settings											
☐ Name resolution ☐ Absolute start time ☐ Limit to display filter											
Copy											
Follow Stream...											
Graph...											
Protocol											
☐ Bluetooth											
☐ DCCP											
☒ Ethernet											
☐ FC											
☐ FDDI											
☐ IEEE 802.11											
☐ IEEE 802.15.4											
☒ IPv4											
☒ IPv6											
☐ IPX											
TCP · 40											
UDP · 117											
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

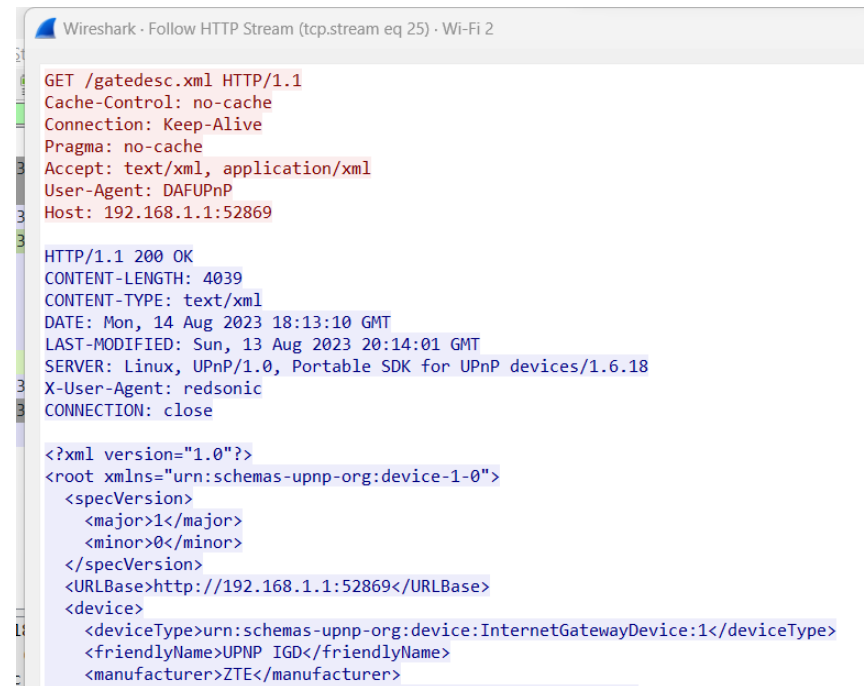
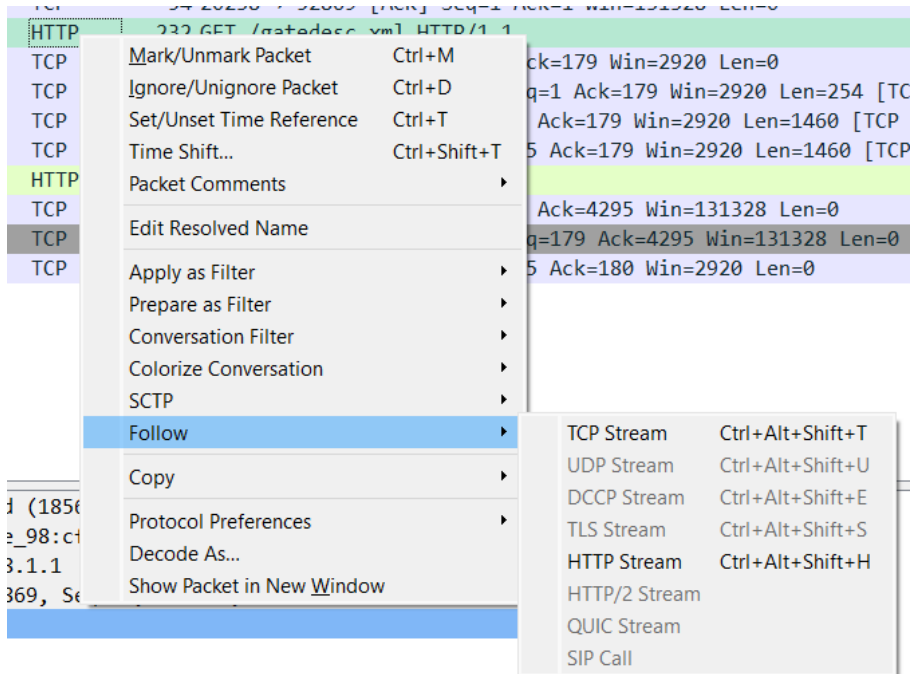


Network Analysis

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)



