



Forensics

List of Content

Apa itu Forensic dalam cybersecurity dan ctf?

Steganography

Metadata

Wireshark

List of Content

File Carving

Hex Editors dan File Formats

Challenges Latihan/Tambahan

***Apa itu Forensic dalam
cybersecurity dan ctf?***

Forensik digital dalam konteks profesional, keterampilan ini menjadi tulang punggung dari tim Incident Response (IR). Ketika sebuah perusahaan mengalami pelanggaran data atau serangan siber, analis forensik bertugas untuk membedah insiden tersebut

Dalam kompetisi Capture The Flag (CTF), kategori "Forensik" berfungsi sebagai simulasi dari tugas-tugas investigatif ini. Kategori ini bertujuan untuk membikin peserta menganalisis file statis—seperti gambar, rekaman audio, dokumen, atau rekaman lalu lintas jaringan—untuk menemukan sebuah "flag" atau informasi rahasia.

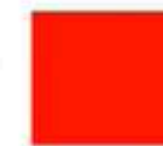
Steganografi

Steganografi

Steganografi adalah teknik menyembunyikan informasi rahasia di dalam file biasa seperti gambar atau audio. Dalam tantangan CTF, Anda akan diberi sebuah file dan harus membongkarnya untuk menemukan flag yang disamarkan di dalamnya, seringkali tanpa petunjuk apa pun.



Original Image: 10100



10010000 10001101 01010001

Hidden Message: 101001

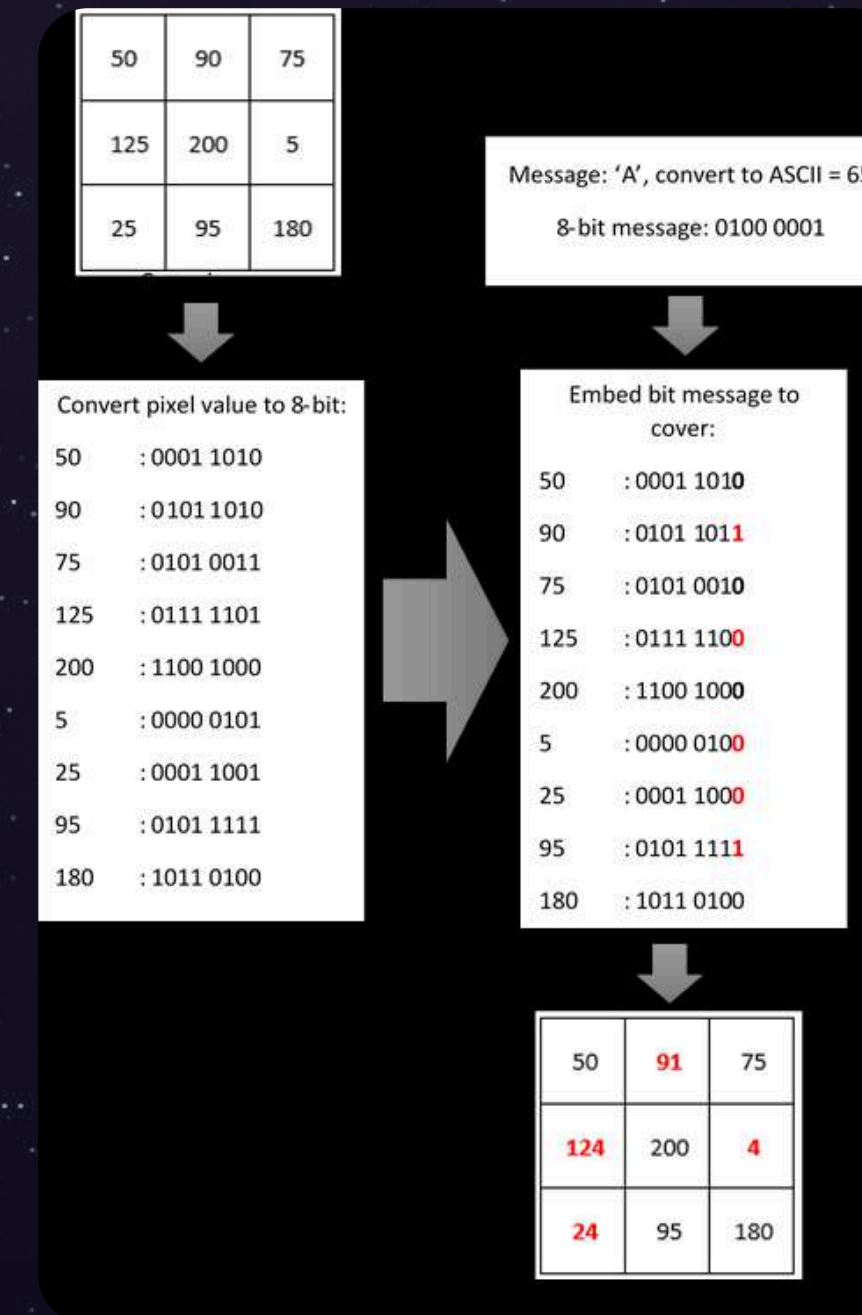


100100001 10001100 010100001

Least Significant Bit (LSB)

LSB, atau Least Significant Bit, adalah bit terakhir (paling kanan) dalam representasi biner dari sebuah angka. Mengubah bit ini hanya akan menyebabkan perubahan yang sangat kecil pada nilai angka tersebut, sehingga seringkali tidak terlihat perbedaannya.

- Setiap piksel gambar terdiri dari kombinasi warna RGB (Merah, Hijau, Biru).
- Tiap saluran warna (R, G, B) memiliki 8 bit data, dan bit terakhirnya disebut LSB (Least Significant Bit).
- Data rahasia disembunyikan dengan cara mengubah LSB pada setiap saluran warna di tiap piksel.
- Artinya, 1 piksel dapat menyimpan 3 bit data rahasia tanpa mengubah tampilan gambar secara kasat mata.
- Pesan (teks) yang akan disembunyikan diubah dulu menjadi kode biner, lalu disisipkan ke LSB piksel secara berurutan.



Tools

- StegSolve: Analisis lapisan dan properti gambar.
- zsteg: Deteksi data tersembunyi dengan cepat dalam file PNG atau BMP.
- binwalk: Ekstrak file tertanam dari file biner.
- strings: Cari teks yang dapat dibaca di dalam file.
- ExifTool: Ekstrak metadata.
- Steghide: Tanam dan ekstrak data dari gambar/audio.

Hands On

Example 1 (Showcase):

picoCTF 2018: husky.png

[https://github.com/Shazaw/
OmahTIAcademy_Hands_On_Practice_Cysec/blob/main/
Class2%20-%20Forensics/steganography/husky.png](https://github.com/Shazaw/OmahTIAcademy_Hands_On_Practice_Cysec/blob/main/Class2%20-%20Forensics/steganography/husky.png)

Example 2:

PicoCTF: St3g0

<https://play.picoctf.org/practice/challenge/305> (or in github)

Metadata

Metadata

Metadata adalah data tentang data. Berbagai jenis file memiliki metadata yang berbeda. Sebagai contoh, metadata pada foto dapat mencakup tanggal, informasi kamera, lokasi GPS, komentar, dll. Untuk musik, metadata dapat mencakup judul, penulis, nomor trek, dan album. Challenge CTF seringkali mengharuskan kalian untuk mencari petunjuk khusus dalam metadata suatu file (terutama file media).


```
.....+-----+
Tag                |Value
+-----+-----+
Manufacturer       |Apple
Model              |iPhone 4
Orientation        |Right-top
X-Resolution       |72
Y-Resolution       |72
Resolution Unit    |Inch
Software           |4.2.1
Date and Time      |2010:12:27 11:17:34
YCbCr Positioning  |Centered
Compression        |JPEG compression
X-Resolution       |72
Y-Resolution       |72
Resolution Unit    |Inch
Exposure Time      |1/4300 sec.
F-Number           |f/2.8
Exposure Program   |Normal program
ISO Speed Ratings   |80
Exif Version       |Exif Version 2.21
Date and Time (Orig)|2010:12:27 11:17:34
Date and Time (Digit)|2010:12:27 11:17:34
Components Configura|Y Cb Cr
Shutter Speed      |12.07 EV (1/4300 sec.)
Aperture           |2.97 EV (f/2.8)
Metering Mode      |Average
Flash              |Flash did not fire, auto mode
Focal Length       |3.9 mm
Subject Area       |Within rectangle (width 699, height 696) around (x,y) = (1
FlashPixVersion    |FlashPix Version 1.0
Color Space        |sRGB
Pixel X Dimension  |2592
Pixel Y Dimension  |1936
Sensing Method     |One-chip color area sensor
Exposure Mode      |Auto exposure
White Balance       |Auto white balance
Scene Capture Type  |Standard
Sharpness          |Hard
North or South Latit|N
Latitude           |21. 7.68.  0
East or West Longitu|W
Longitude          |86. 45.00.  0
Altitude Reference  |Sea level
Altitude           |22.427
GPS Time (Atomic Clo|17:17:33.26
GPS Image Direction |T
GPS Image Direction |122.544
+-----+-----+
XIF data contains a thumbnail (9932 bytes).
```


Tools

- Exiftool: Sebuah tool di linux yang kita bisa memakai untuk melihat metadata. Tool ini juga bisa dipakai untuk mengubah isi metadata dari suatu file
- Cyberchef: Sering kali orang menyembunyikan informasi secara enkripsi di dalam metadata

Hands On

Example 1 (Showcase):

cat.jpeg:

https://github.com/Shazaw/OmahTIAcademy_Hands_On_Practice_Cysec/blob/main/Class2%20-%20Forensics/Metadata/cat.jpeg

Example 2:

PicoCTF: Information

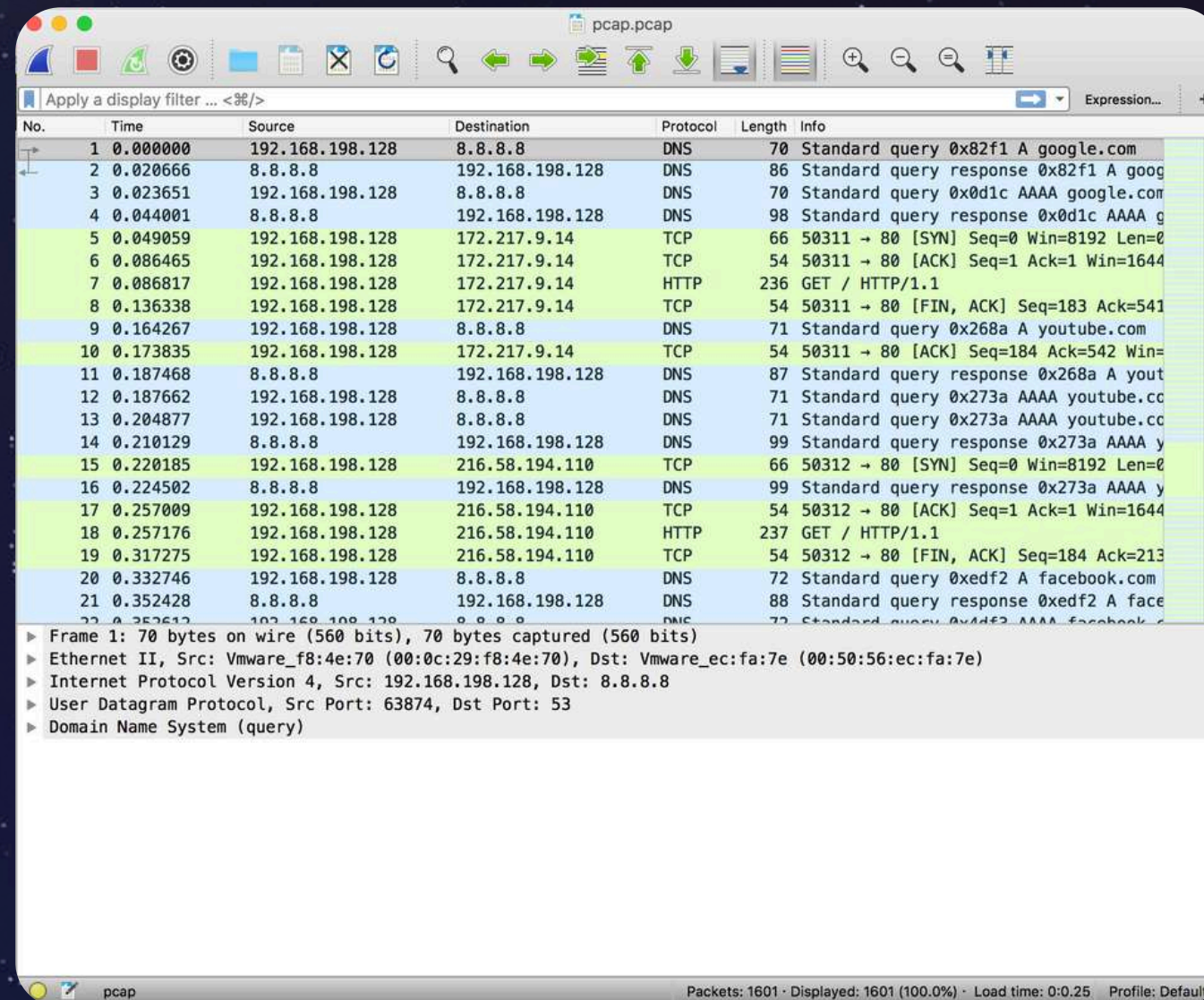
<https://play.picoctf.org/practice/challenge/186> (or in github)

Wireshark

Wireshark

Wireshark adalah penganalisa network traffic. Ia berfungsi untuk menangkap dan menampilkan data yang bergerak di jaringan secara detail. Semua aktivitas online, mulai dari membuka situs web hingga mengirim pesan, dipecah menjadi paket-paket data yang bisa diperiksa oleh Wireshark. Challenge CTF seringkali memberikan file rekaman lalu lintas (.pcap) dan mengharuskan kalian untuk menganalisisnya, mencari petunjuk seperti password, file yang ditransfer, atau flag yang tersembunyi di dalam percakapan jaringan.

Gambaran Network Traffic di Wireshark:



pcap.pcap

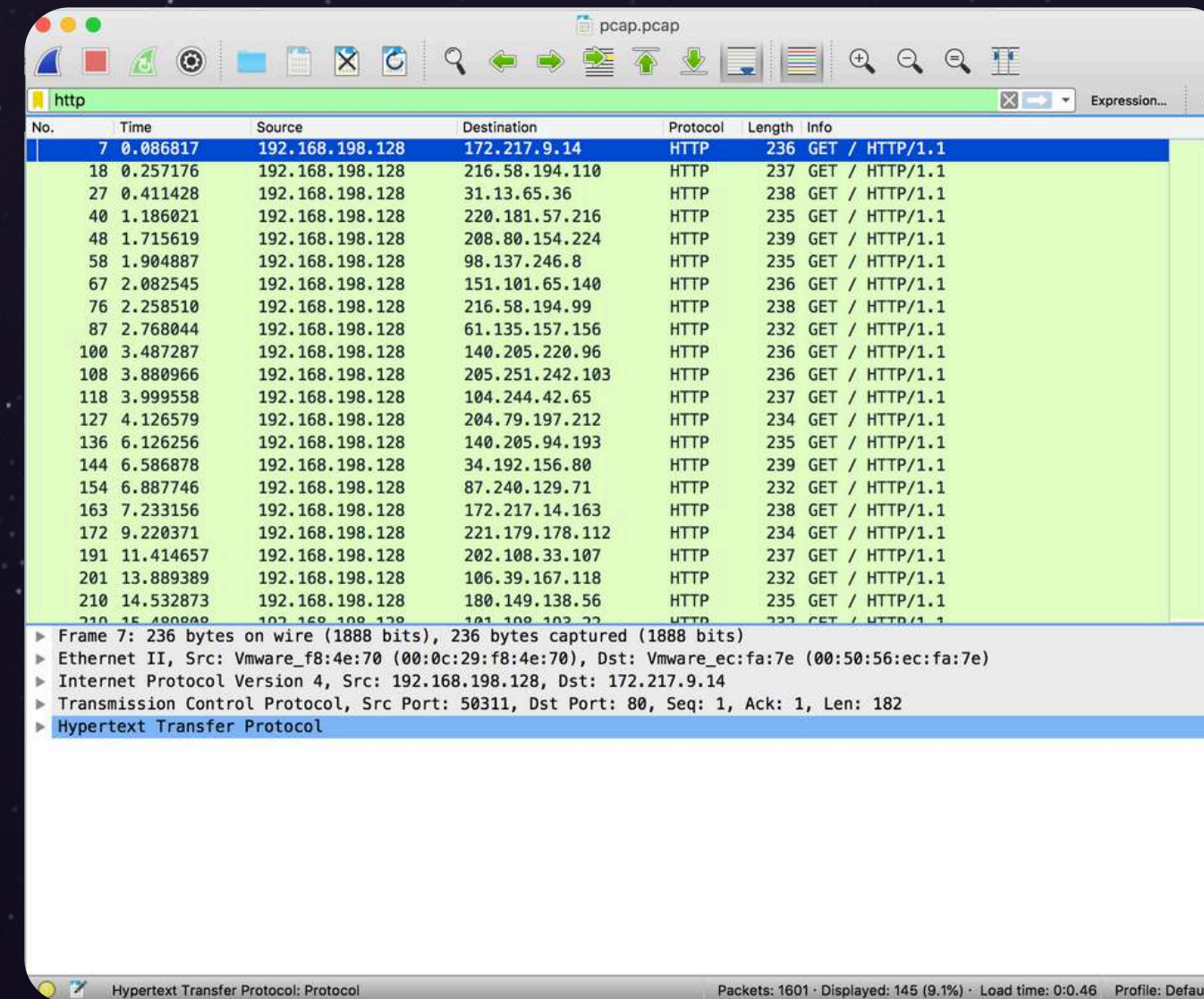
Apply a display filter ... <=>/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.198.128	8.8.8.8	DNS	70	Standard query 0x82f1 A google.com
2	0.020666	8.8.8.8	192.168.198.128	DNS	86	Standard query response 0x82f1 A goog
3	0.023651	192.168.198.128	8.8.8.8	DNS	70	Standard query 0x0d1c AAAA google.com
4	0.044001	8.8.8.8	192.168.198.128	DNS	98	Standard query response 0x0d1c AAAA g
5	0.049059	192.168.198.128	172.217.9.14	TCP	66	50311 → 80 [SYN] Seq=0 Win=8192 Len=0
6	0.086465	192.168.198.128	172.217.9.14	TCP	54	50311 → 80 [ACK] Seq=1 Ack=1 Win=1644
7	0.086817	192.168.198.128	172.217.9.14	HTTP	236	GET / HTTP/1.1
8	0.136338	192.168.198.128	172.217.9.14	TCP	54	50311 → 80 [FIN, ACK] Seq=183 Ack=541
9	0.164267	192.168.198.128	8.8.8.8	DNS	71	Standard query 0x268a A youtube.com
10	0.173835	192.168.198.128	172.217.9.14	TCP	54	50311 → 80 [ACK] Seq=184 Ack=542 Win=
11	0.187468	8.8.8.8	192.168.198.128	DNS	87	Standard query response 0x268a A yout
12	0.187662	192.168.198.128	8.8.8.8	DNS	71	Standard query 0x273a AAAA youtube.cc
13	0.204877	192.168.198.128	8.8.8.8	DNS	71	Standard query 0x273a AAAA youtube.cc
14	0.210129	8.8.8.8	192.168.198.128	DNS	99	Standard query response 0x273a AAAA y
15	0.220185	192.168.198.128	216.58.194.110	TCP	66	50312 → 80 [SYN] Seq=0 Win=8192 Len=0
16	0.224502	8.8.8.8	192.168.198.128	DNS	99	Standard query response 0x273a AAAA y
17	0.257009	192.168.198.128	216.58.194.110	TCP	54	50312 → 80 [ACK] Seq=1 Ack=1 Win=1644
18	0.257176	192.168.198.128	216.58.194.110	HTTP	237	GET / HTTP/1.1
19	0.317275	192.168.198.128	216.58.194.110	TCP	54	50312 → 80 [FIN, ACK] Seq=184 Ack=213
20	0.332746	192.168.198.128	8.8.8.8	DNS	72	Standard query 0xedf2 A facebook.com
21	0.352428	8.8.8.8	192.168.198.128	DNS	88	Standard query response 0xedf2 A face

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: Vmware_f8:4e:70 (00:0c:29:f8:4e:70), Dst: Vmware_ec:fa:7e (00:50:56:ec:fa:7e)
Internet Protocol Version 4, Src: 192.168.198.128, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 63874, Dst Port: 53
Domain Name System (query)

pcap Packets: 1601 · Displayed: 1601 (100.0%) · Load time: 0:0.25 Profile: Default

Filter http di wireshark:



pcap.pcap

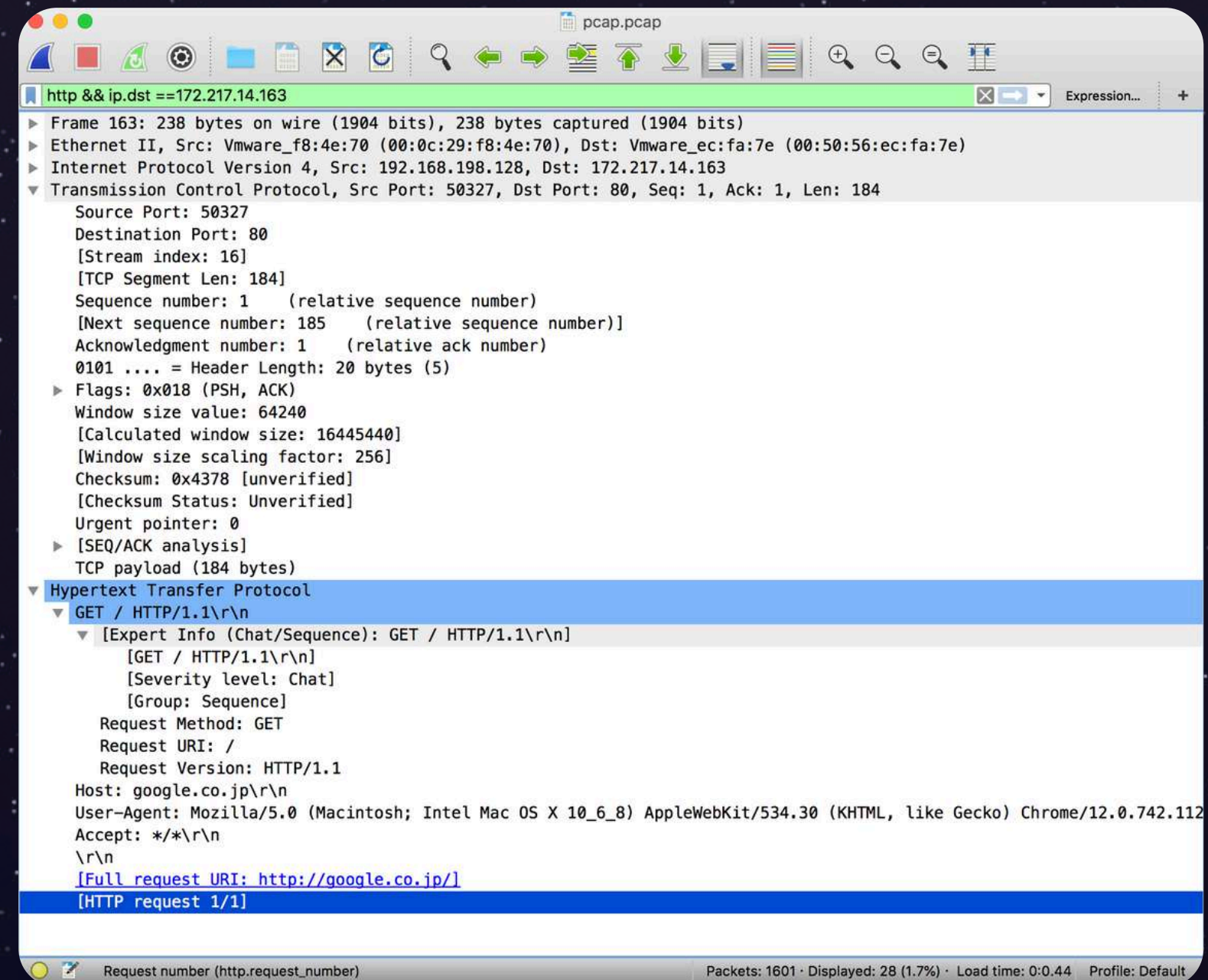
http Expression...

No.	Time	Source	Destination	Protocol	Length	Info
7	0.086817	192.168.198.128	172.217.9.14	HTTP	236	GET / HTTP/1.1
18	0.257176	192.168.198.128	216.58.194.110	HTTP	237	GET / HTTP/1.1
27	0.411428	192.168.198.128	31.13.65.36	HTTP	238	GET / HTTP/1.1
40	1.186021	192.168.198.128	220.181.57.216	HTTP	235	GET / HTTP/1.1
48	1.715619	192.168.198.128	208.80.154.224	HTTP	239	GET / HTTP/1.1
58	1.904887	192.168.198.128	98.137.246.8	HTTP	235	GET / HTTP/1.1
67	2.082545	192.168.198.128	151.101.65.140	HTTP	236	GET / HTTP/1.1
76	2.258510	192.168.198.128	216.58.194.99	HTTP	238	GET / HTTP/1.1
87	2.768044	192.168.198.128	61.135.157.156	HTTP	232	GET / HTTP/1.1
100	3.487287	192.168.198.128	140.205.220.96	HTTP	236	GET / HTTP/1.1
108	3.880966	192.168.198.128	205.251.242.103	HTTP	236	GET / HTTP/1.1
118	3.999558	192.168.198.128	104.244.42.65	HTTP	237	GET / HTTP/1.1
127	4.126579	192.168.198.128	204.79.197.212	HTTP	234	GET / HTTP/1.1
136	6.126256	192.168.198.128	140.205.94.193	HTTP	235	GET / HTTP/1.1
144	6.586878	192.168.198.128	34.192.156.80	HTTP	239	GET / HTTP/1.1
154	6.887746	192.168.198.128	87.240.129.71	HTTP	232	GET / HTTP/1.1
163	7.233156	192.168.198.128	172.217.14.163	HTTP	238	GET / HTTP/1.1
172	9.220371	192.168.198.128	221.179.178.112	HTTP	234	GET / HTTP/1.1
191	11.414657	192.168.198.128	202.108.33.107	HTTP	237	GET / HTTP/1.1
201	13.889389	192.168.198.128	106.39.167.118	HTTP	232	GET / HTTP/1.1
210	14.532873	192.168.198.128	180.149.138.56	HTTP	235	GET / HTTP/1.1

Frame 7: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits)
Ethernet II, Src: Vmware_f8:4e:70 (00:0c:29:f8:4e:70), Dst: Vmware_ec:fa:7e (00:50:56:ec:fa:7e)
Internet Protocol Version 4, Src: 192.168.198.128, Dst: 172.217.9.14
Transmission Control Protocol, Src Port: 50311, Dst Port: 80, Seq: 1, Ack: 1, Len: 182
Hypertext Transfer Protocol

Hypertext Transfer Protocol: Protocol Packets: 1601 · Displayed: 145 (9.1%) · Load time: 0:0.46 Profile: Default

Konten terpenting di dalam network traffic, seperti transfer protocol, host, destination dan, source:



Tools

- Wireshark: Ini tool utama yang kita gunakan untuk melihat dan menganalisis network traffic
- Tshark: versi CLI dari wireshark dan dipake untuk kerjaan otomatisasi analisis network traffic
- Cyberchef: Banyak data yang kita temukan di dalam network traffic harus di decode

Hands On

Example 1 (Showcase):

PicoCTF: Wireshark doo doooo do doo...

<https://play.picoctf.org/practice/challenge/115> (or in github)

Example 2:

PicoCTF: shark on wire 1

<https://play.picoctf.org/practice/challenge/30> (or in github)

File Carving

Dalam tantangan forensik CTF dan firmware sistem tertanam, sering ditemukan file yang disembunyikan di dalam file lain. Hal ini terutama umum pada sistem dengan struktur file yang sederhana atau datar. Proses untuk menemukan dan mengekstrak file tersembunyi ini disebut filecarving. Dua alat populer untuk tugas ini adalah Binwalk dan Foremost, yang sangat berguna untuk menganalisis firmware dan memulihkan file yang tertanam.

Contoh dari file di dalam file:

```
(mshazaw@kali)-[~/OmahTIAcademy/Examples/Class2/FileCarving]
$ binwalk -e dolls.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
272492	0x4286C	Zip archive data, at least v2.0 to extract, compressed size: 378956, uncompressed size: 383938, name: base_images/2_c.jpg

WARNING: One or more files failed to extract: either no utility was found or it's unimplemented

Contoh dari file yang kepanjangan,
dan kita terpaksa memakai tools
file carving untuk mencari flag di
dalam .txt ini

And here, over the portals of my fort, I shall cut in the stone
the word which is to be my beacon and my banner. The word which
will not die, should we all perish in battle. The word which can
never die on this earth, for it is the heart of it and the
meaning and the glory.

The sacred word:

EGO

```
(mshazaw@kali)-[~/OmahTIAcademy/Examples/Class2/FileCarving]
$ wc -l anthem.flag.txt
2146 anthem.flag.txt
```


Tools

- strings: Mencari teks yang dapat dibaca di dalam file.
- foremost: Mengekstrak jenis file tertentu berdasarkan header dan footer-nya.
- binwalk: Menganalisis file binary untuk mencari data atau file yang tersemat di dalamnya.
- photorec: Memulihkan file yang terhapus dari hard drive atau kartu memori.

Hands On

Example 1 (Showcase):

PicoCTF: Matroyshka Doll

<https://play.picoctf.org/practice/challenge/129> (or in github)

Example 2:

PicoCTF: Lookey here

<https://play.picoctf.org/practice/challenge/279> (or in github)

Hex Editors dan File Formats

File Signatures

File signatures (also known as File Magic Numbers) adalah bytes dalam file yang digunakan untuk mengidentifikasi format file tersebut. Umumnya panjangnya 2-4 bytes, dan dapat ditemukan di awal file.

```
(mshazaw@kali)-[~/OmahTIAcademy/Examples/Class2/Steganography]
$ xxd husky.png | head -n 10
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG.....IHDR
00000010: 0000 085c 0000 08b8 0806 0000 00e7 1624  ... \.....$
00000020: ee00 0020 0049 4441 5478 5e94 bd4f 8b24  ... .IDATx^..0.$
00000030: 5b96 edb7 d3ca ca9e e338 8e13 2497 a206  [...8.. $ ...
00000040: 8f87 06e2 0d1e fd09 c443 68a0 9106 6fa2  ....Ch ... o.
00000050: af2e 9a46 1445 71b9 2449 1038 2ec7 f1f6  ... F.Eq.$I.8....
00000060: b6b2 14bf b5d6 36b3 c85b dd48 7989 1b91  ....6.. [.Hy ...
00000070: 9111 ee66 c7ce d97f d65e 7bed 2fff f47f  ... f.....^{/ ...
00000080: fea7 1f7f f8fb 8ffa b154 7de1 7f7f 5faa  ....T} ... _
00000090: 961f b5cc 3fea c78f 2fb5 0c43 d55c f563  ....? ... / ..C.\.c
```


PNG Files

Bagian pertama dalam file PNG (setiap file juga sama), terdapat tanda tangan (signature). Tanda tangan adalah bagian yang menunjukkan jenis file tertentu. Biasanya, kita melihat ekstensi file untuk mengidentifikasi jenis file tersebut. Namun, ekstensi file dapat dipalsukan menjadi apa saja tanpa merusak file, sementara tanda tangan file tidak bisa. Misalnya, aku dapat mengganti nama file gambar menjadi 'image.zip' dan file gambar tersebut masih dapat dibuka. Namun, ketika aku mengubah tanda tangan file menjadi hal lain, file tersebut tidak dapat dibuka. Untuk melihat header file PNG, kita dapat menggunakan editor hexadesimal dan memeriksa baris pertama.

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 PNG.....IHDR
```


Setiap chunk terdiri dari 4 bagian, yaitu panjang data chunk, jenis chunk, data chunk, dan CRC.

→ Bagian pertama adalah panjang data chunk, yang memiliki 4 byte dan menunjukkan berapa banyak byte yang terdapat dalam data chunk.

→ Bagian kedua adalah jenis chunk, yang juga memiliki 4 byte. Bagian ini menunjukkan apakah chunk tersebut adalah IHDR, IDAT, atau IEND.

→ Bagian ketiga adalah data chunk. Bagian ini berisi data dari chunk tersebut. Ukuran bagian ini akan ditulis di bagian pertama chunk yang saya sebutkan sebelumnya.

→ Dan terakhir, kita memiliki CRC yang juga berukuran 4 byte.

Size of chunk data	Chunk type	Chunk data	CRC
4 bytes	4 bytes	The size is based on what stated in 'size of chunk data' part	4 bytes

89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
00 00 06 6A 00 00 04 47 08 02 00 00 00 7C 8B AB ...J...G.....|<<

IHDR:

Blok yang berisi informasi gambar seperti lebar, tinggi, ukuran byte warna, jenis warna, kompresi, filter, dan metode enkapsulasi.

Width	Height	Size of colour byte	Colour type	Compression method	Filter method	Enlacement method
4 bytes	4 bytes	1 byte	1 byte	1 byte	1 byte	1 byte

```

89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
00 00 06 6A 00 00 04 47 08 02 00 00 00 7C 8B AB ...j...G.....|<«
78 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 x....sRGB.®î.é..
  
```


IDAT:

Berisi byte-byte yang akan ditampilkan atau dirender di layar. Sama seperti IHDR chunk, IDAT juga memiliki 4 bagian. Perbedaannya adalah ukuran data chunk IDAT lebih besar.

52 24 F0 00 00 FF A5 49 44 41 54 78 5E EC BD 3F R\$6..y IDATx^i4?

4 byte sebelum IDAT (jenis chunk) merupakan bagian “ukuran data chunk”, sehingga berisi ukuran data chunk. Nilai tersebut menunjukkan bahwa IDAT ini memiliki ukuran data 0xFFA5, sedangkan IHDR hanya memiliki 0x0D.

IEND:

Bagian terakhir dalam file PNG adalah IEND. Kalau kalian membuka file PNG menggunakan hex editor, kalian akan menemukan IEND berada di bagian bawah. Seperti biasa, sama seperti bagian-bagian lainnya, IEND terdiri dari 4 bagian.

Size of chunk data	Type of chunk	Chunk data	CRC
00 00 00 00	49 45 4E 44	null	AE 42 60 82

Tools

- > xxd: Melihat hexdump dari files dan file signatures-nya
- > pngcheck: Melihat apakah file tersebut mempunyai masalah dan apa yang harus di fix untuk menghilangkan masalah tersebut
- > hexedit: Mengedit hexdump ke values yang diinginkan untuk mengubah file-nya

Hands On

Example 1 (Showcase):

Github: OmahTIAcademy1.png

[https://github.com/Shazaw/
OmahTIAcademy_Hands_On_Practice_Cysec/tree/main/
Class2%20-%20Forensics/HexEditor/OmahTIAcademy1.png](https://github.com/Shazaw/OmahTIAcademy_Hands_On_Practice_Cysec/tree/main/Class2%20-%20Forensics/HexEditor/OmahTIAcademy1.png)

Example 2:

Github: OmahTIAcademy2.png

[https://github.com/Shazaw/
OmahTIAcademy_Hands_On_Practice_Cysec/tree/main/
Class2%20-%20Forensics/HexEditor/OmahTIAcademy2.png](https://github.com/Shazaw/OmahTIAcademy_Hands_On_Practice_Cysec/tree/main/Class2%20-%20Forensics/HexEditor/OmahTIAcademy2.png)

Materials

Buat semua materi dan practice questions:
https://github.com/Shazaw/OmahTIAcademy_Hands_On_Practice_Cysec

Terima Kasih All