#CátedrasCiber

Módulo I: Introducción y Criptografía

23/10/2024

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

Entidad colaboradora:
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Información del curso

1. Horario de clase.
2. Material básico necesario.
3. Módulos del curso.
4. Plataformas que vamos a utilizar.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Horario y enlaces

- 23 Octubre – 20 Noviembre (5 sesiones).
- Los miércoles de 17:00 a 19:00 (excepto el último).
- Online: Se anunciará el enlace de la sesión por correo cada semana y si no la web estará actualizada.
- Se grabarán las sesiones para aquellos que no puedan venir.
- Información: https://catedra-uc-incibe.github.io/curso-ctf/

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

¿Qué es necesario para participar?

- VirtualBox, para usar KaliLive.
- Ganas de aprender.

- ¿Conocimientos básicos en algún lenguaje de programación?
- ¿Conocimientos básicos de Linux y/o terminal?
- ¿Soltura utilizando los buscadores (Google, Bing, DuckDuckGo...)?

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Módulos del curso

- Módulo I: Introducción y Criptografía.
- Módulo II: Análisis Forense y Esteganografía.
- Módulo III: Ataques a servidores y Explotación web.
- Módulo IV: Reversing y Explotación de binarios.

Las sesiones serán teórico-prácticas con retos durante la sesión y más retos después de la sesión, el propósito es aprender a usar las herramientas y aplicar el conocimiento.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Plataforma de retos del curso

https://ctf-catedra-incibe.numa.host/

Credenciales en correo de bienvenida

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Plataformas recomendadas

Pico CTF: https://picoctf.org/

OverTheWire: https://overthewire.org/wargames/

TryHackMe: https://tryhackme.com/

HackTheBox: https://www.hackthebox.eu/

Atenea: https://atenea.ccn-cert.cni.es/home

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Certificados

Certificado de superación: Asistencia a 4 clases + participación.

Certificado de asistencia: En otro caso que se demuestre participación.

¿Posibilidad de créditos?

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

¿Cómo interactuar?

Levantamos manos de teams.

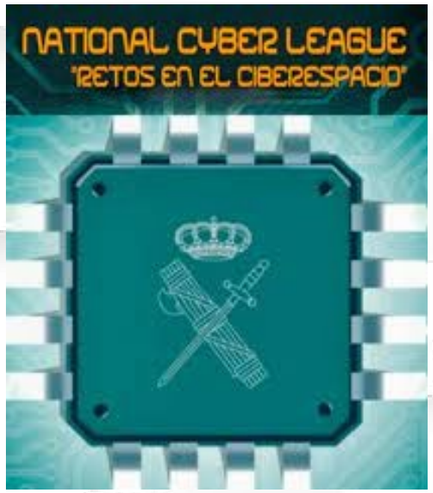
Las sesiones se grabarán, por lo que tendremos el grupo de Telegram disponible para dudas.

El propósito es aprender, no solo competir.

Y responder al correo en copia a todossssss

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Experiencia de los Docentes



Facebook Bug Bounty

BIT UP

SEEK & HACK

Qynamon

HackOn 2025

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

JNIC
Jornadas Nacionales de Investigación en Ciberseguridad

EUROPEAN CYBER SECURITY CHALLENGE

grafo RESEARCH

Universidad Rey Juan Carlos

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Módulo I: Introducción y Criptografía

Índice del módulo

1. ¿Qué es un CTF?
    ¿Qué tipos de retos se encuentran en los CTF?
    Conceptos básicos: encuentra la bandera.
2. Criptografía y codificaciones básicas.
    Representación de los datos.
    Codificaciones y cifrados.
    Otros cifrados (XOR, Dcodefr...).
    Hashes (MD5, SHA1, SHA256).
3. OSINT.
    OSINT Básico.
    IMINT.
    HUMINT.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

¿Qué es un CTF?

CTF = Capture The Flag (Captura la Bandera)

- Competición de hacking, en la que ponemos a prueba nuestras habilidades resolviendo retos de ciberseguridad en un tiempo limitado, con el objetivo de sumar puntos.
- Por equipos o individual.

1. Elige un reto.
2. Resuélvelo lo antes posible.
3. Introduce la flag y obtén puntos.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

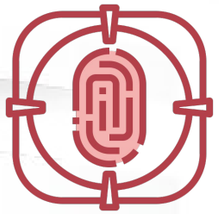
Tipos de CTF

- Existen 3 tipos principales de competiciones CTF:

1. Jeopardy: retos de distintas categorías a resolver en un tiempo limitado.
2. Ataque – Defensa: 2 equipos, 2 redes y servicios vulnerables en cada red. Ambos equipos deben atacar a los servicios del contrincante a la vez que defienden los suyos.
3. Boot2root: máquinas creadas con fallos de seguridad que se deben explotar para convertirse en superusuario (root).
4. Mezcla.

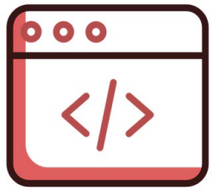
Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Categorías



Forense

Investigaciones sobre incidentes informáticos.

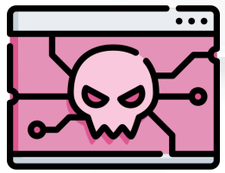


Web

Búsqueda y explotación de vulnerabilidades en aplicaciones web.

Criptografía

Descifrado de mensajes ilegibles a simple vista.



Reversing

Análisis del código de programas y ejecutables.

OSINT

Recolección de datos a través de fuentes públicas de información.

Esteganografía

Técnica que oculta mensajes o archivos dentro de otros.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía básica

Representación de los datos

Es esencial entender que nos podemos encontrar los datos con diferentes formatos. Sin embargo, su significado será el mismo. Las formas más comunes son:

ASCII

Relaciona caracteres con números. A cada carácter le corresponde un valor de la tabla ASCII.

Hexadecimal

Utiliza base 16 como representación de los datos. En caracteres toma como referencia el valor ASCII

ASCII	Símbolo
96	`
97	a
98	b
99	c
100	d
101	e
102	f
103	g
104	h
105	i
106	j
107	k
108	l
109	m
110	n
111	o

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Representación de los datos

Es esencial entender que nos podemos encontrar los datos con diferentes formatos. Sin embargo, su significado será el mismo. Las formas más comunes son:

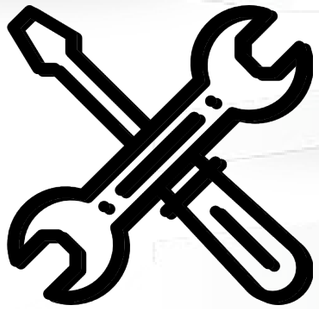
Binario

Es la representación más básica.
Tan solo utiliza dos valores: 1 y 0.

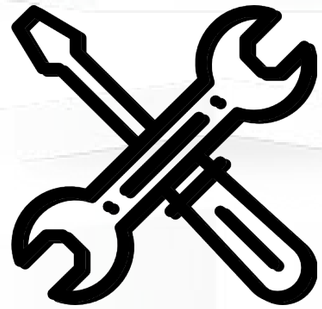
DECIMAL	BINARIO	HEXADECIMAL
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Representación de los datos



https://gchq.github.io/CyberChef/
https://www.dcode.fr/



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Codificaciones y cifrados

Algunas de las maneras más comunes de ocultar información son mediante codificaciones y cifrados. Esto consiste en utilizar una única clave para cifrar y descifrar la información. Por lo tanto, siendo el cifrado reversible.

Codificaciones

- Representan la misma información de diferentes maneras.
- Es reversible.
- Algunos ejemplos son Base64, Base32 o ASCII.

Cifrados

- Ocultan la información mediante claves, normalmente secretas, y un conjunto de operaciones.
- Es reversible.
- Algunos ejemplos son ROT-N/César o Vigenère.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Codificación BASE64

BASE64

Es un sistema de numeración posicional que usa 64 caracteres como base. Sirve para representar cualquier información en binario como texto. Se suele identificar rápidamente por su estructura (en general, suelen acabar en ==)

Texto original

CTF{Esto es un texto en Base64. También existen otras como Base32, Base58 o Base85, por ejemplo}

Texto en Base64

Q1RGe0VzdG8gZXMgdW4gdGV4dG8gZW4gQmFzZTY0LiBUYW1iaelu IGV4aXN0ZW4gb3RyYXMgY29tbyBCYXNlMzIsIEJhc2U1OCBvIEJhc2U4NSwgcG9yIGVqZW1wbG99Cg==

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Cifrado ROT-N

ROT-N

Es un tipo particular de cifrado en el que los caracteres se desplazan N posiciones. Por ello, N será nuestra clave secreta que ayudará a cifrar y descifrar el texto. Además de conocer la clave, deberemos conocer el diccionario que se usa.

Texto original

CTF{El rot solo va a modificar las letras, pero no las llaves}

abcdefghijklmnopqrstuvwxyz

Texto en ROT 13

PGS{Ry ebg fbyb in n zbqvsvpne ynf yrgenf, creb ab ynf yynirf}

nopqrstuvwxyzabcdefghijklm

Cifrado de César

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Cifrado Vigenère

Vigenère

Se basa en una tabla con dos entradas. Una será la clave y la otra el texto a cifrar. Iremos sustituyendo en el texto carácter a carácter con ayuda de la tabla y la clave. La clave será la misma para cifrar y descifrar.

Texto original

CTF{Mi clave de cifrado es Chachipiruli}

Texto en Vigenère

EAF{Op kaimy om epfthld mj Wsieoirpzjtz}

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Cifrado Vigenère

ENTRADA CLAVE \ ENTRADA TEXTO PLANO	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

C T F { M i c l a v e d e c i f r a d o e s C h a c h i p i r u l i }
C H A { c h i p i r u l i C h a c h i p i r u l i C h a c h i p i r l }
E A F { O p k a i m y o m e p f t h l d m j W s i e o i r p z j t z }

Texto original

CTF{Mi clave de cifrado es Chachipiruli}

Texto en Vigenère

EAF{Op kaimy om epfthld mj Wsieoirpzjtz}

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Otros cifrados

XOR

Consiste en cifrar siguiendo unas **reglas matemáticas** y una **clave secreta**. Como la **longitud** de la **clave** suele ser **menor al texto**, se repetirá **cíclicamente**. Todos los caracteres se pasarán a binario y se operará con ellos. Reglas:

1. **Conmutativa:** `A xor B = B xor A`
2. **Asociativa:** `(A xor B) xor C = A xor (B xor C)`
3. **Autoinversa:** `(A xor B) xor B = A`

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Otros cifrados

XOR

Propiedad autoinversa del XOR podremos descifrar

```
(A xor B) xor B = A
```

Texto en claro: A
Texto cifrado: (A xor K)

Clave: Texto xor Cifrado
Clave: A xor (A xor K)= K

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

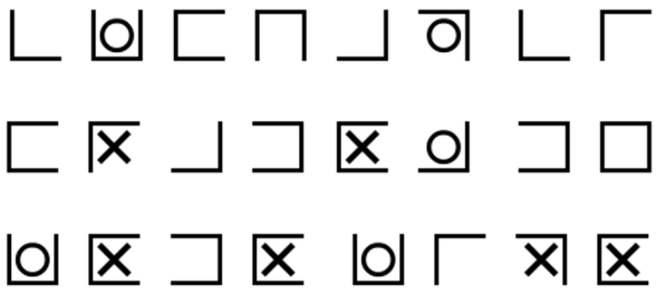
Otras codificaciones

Tic Tac Toe

Texto original

CTF{Hay cifrados de todo tipo}

Texto en Tic-Tac-Toe

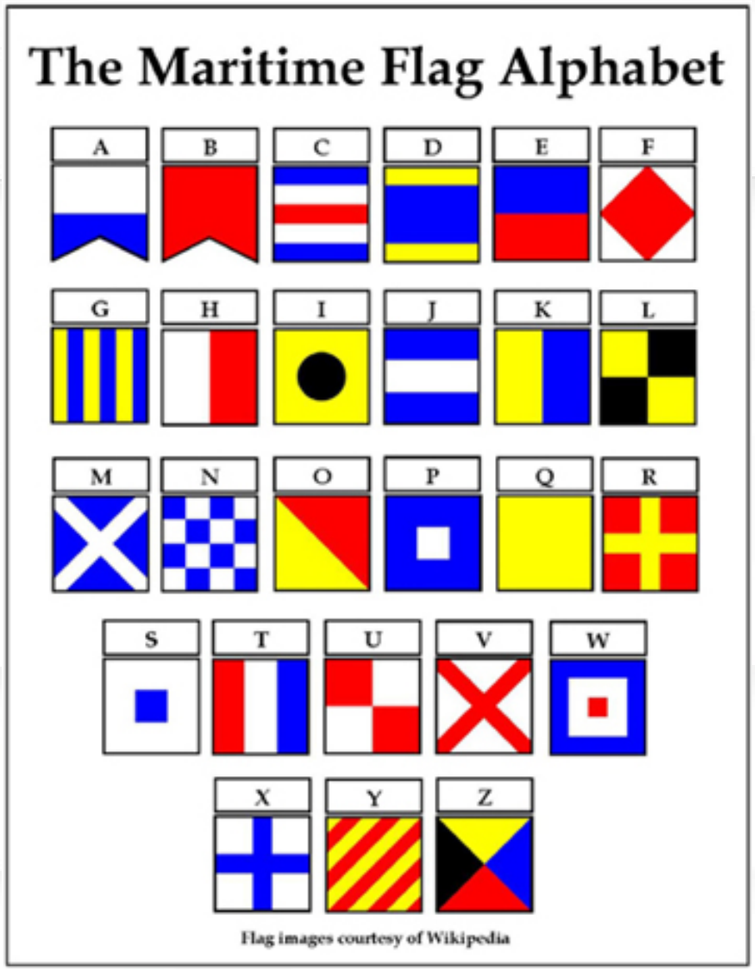


DCode.fr: https://www.dcode.fr/chiffre-tic-tac-toe

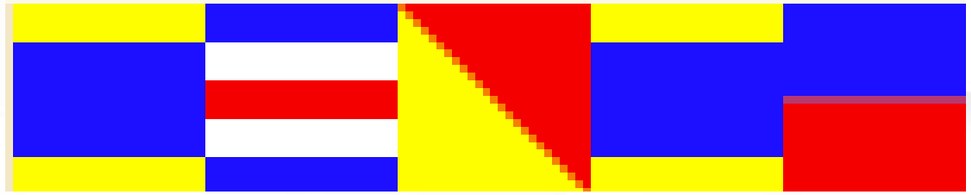
Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Otras codificaciones

Sustitución con banderas marítimas



Texto original: DCODE



https://www.dcode.fr/maritime-signals-code

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Ejercicios propuestos

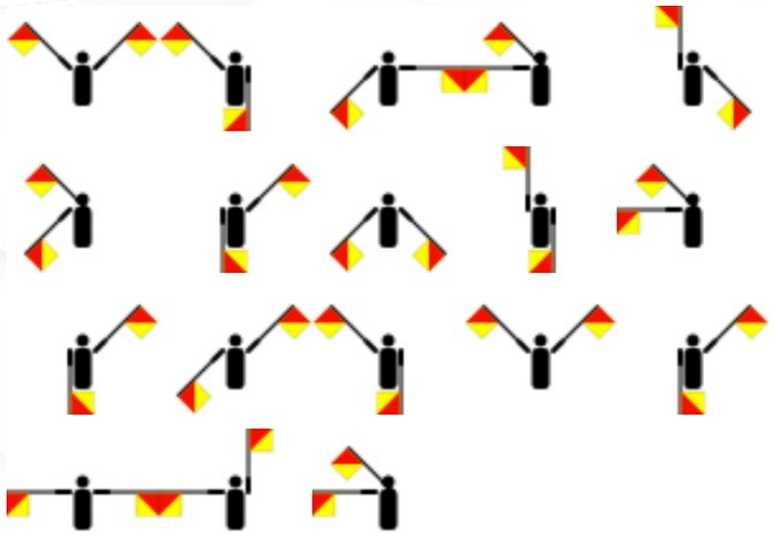
EJ 1: VUN7TXV5IGJpZW4sIHZlbyBxdWUgc2FiZXMgaWRlbnRpZmljYXIgdW4gYmFzZTY0fQ==

EJ 2: YG{Rs xshsw psw VSX wsr 57}

EJ 3: D1ETr0RtqzIwMKZtoT9mVUEyrUEiplOyp3EuovOwnJMlLJEiplOgLKZtMTHtqJ5uVUMyra0=

EJ 4: CTF{. ... - --- . ... -.-. --- -.. .. --. --- -- --- .-. ... .}

EJ 5:

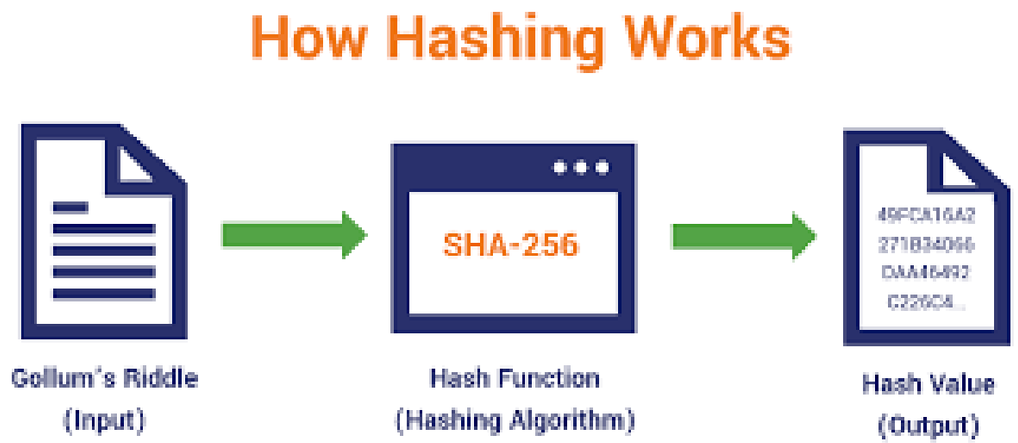


Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes

¿Qué es un hash?

- Es una función matemática o criptográfica, resume la información.
- Da como resultado una cadena de caracteres de longitud fija (digest), independientemente de la longitud entrada.
- Es irreversible. Una vez aplicada no se puede obtener el valor inicial.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

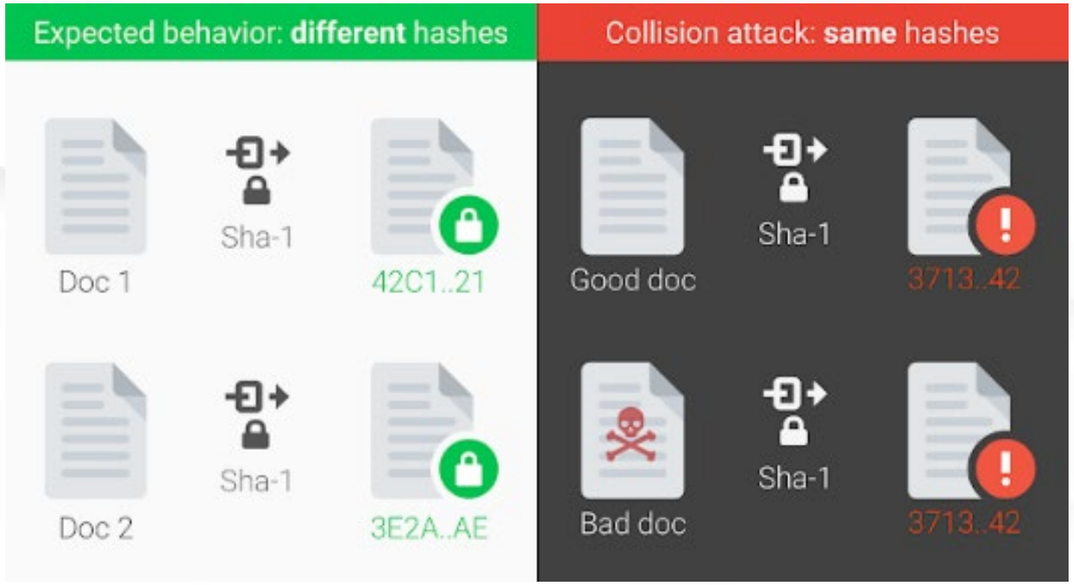
Criptografía - Hashes

- Lo que sí puede hacerse es pre-computar cadenas típicas, dado que una función hash devolverá el mismo resultado para la misma cadena (es determinista).
- Conociendo la función utilizada podemos realizar ataques de fuerza bruta sobre los hashes, de forma que, si en nuestro diccionario se encuentra la palabra *hasheada*, sabremos qué esconde el hash.
- Es importante destacar que esto NO ES LO MISMO QUE REVERTIR EL CÁLCULO.
- Intentar adivinar un hash de una palabra de longitud mayor que 8 es computacionalmente muy costoso.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes

- Existen determinadas funciones hash cuyo uso no se recomienda
  - MD5
  - SHA1
- Aunque la probabilidad es muy baja, podrían existir colisiones



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes

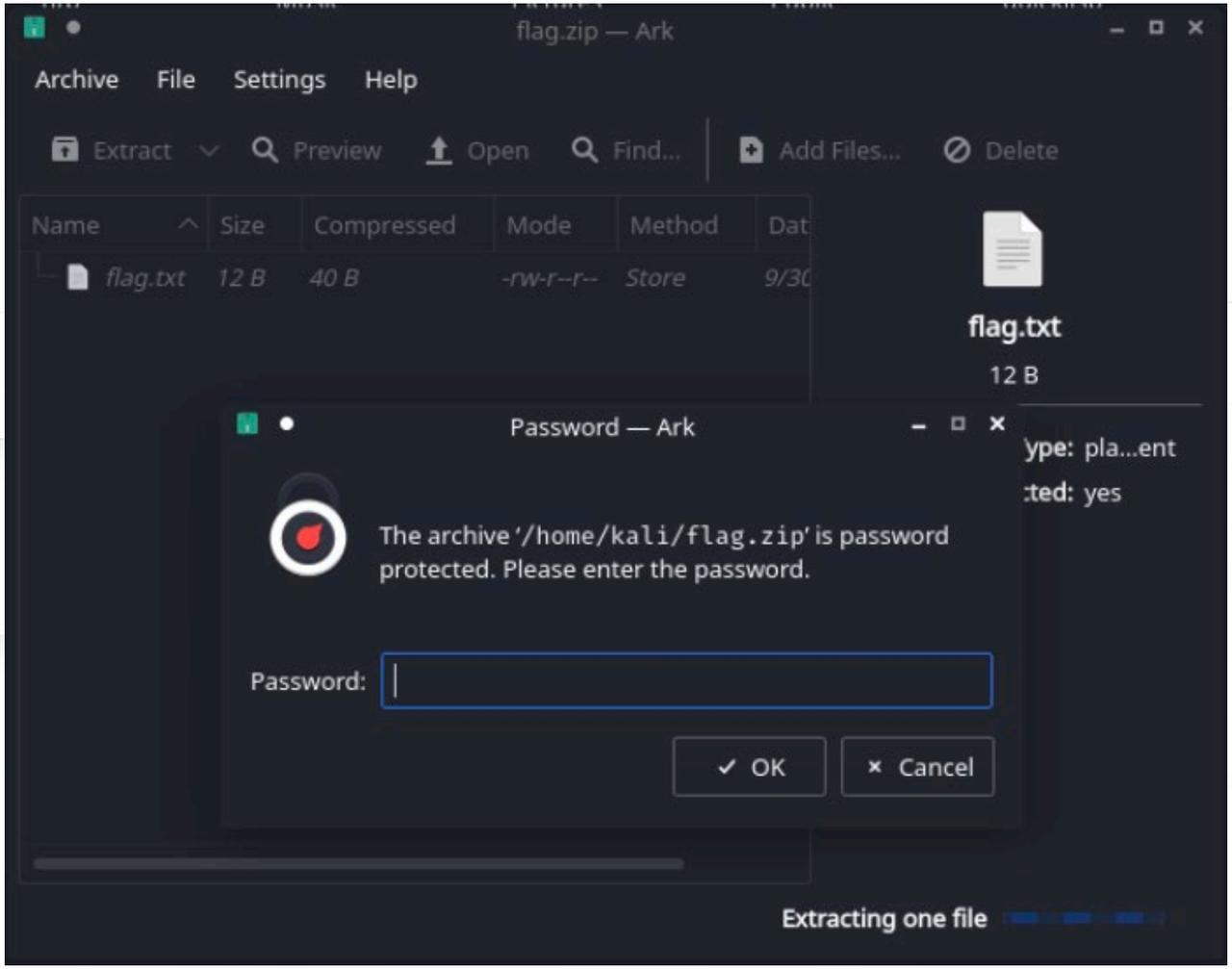
- Cada fichero se puede resumir con un valor hash.
- Existen herramientas que, dada una lista de hashes, nos automatizan el proceso de obtener un valor que genere dicho hash.
- Esto permite obtener la contraseña de ficheros cifrados.

hashcat

advanced
password
recovery

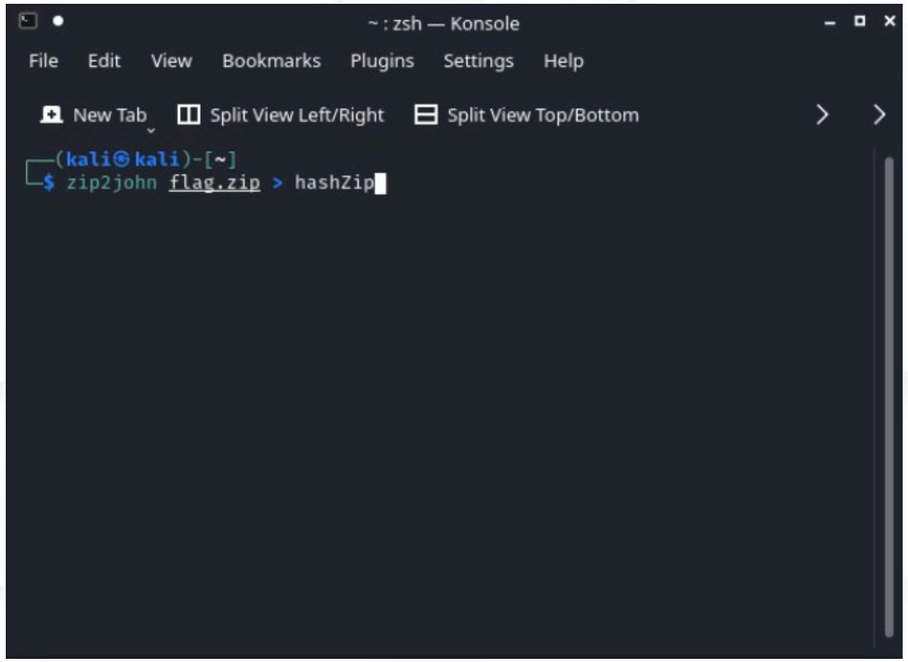
Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

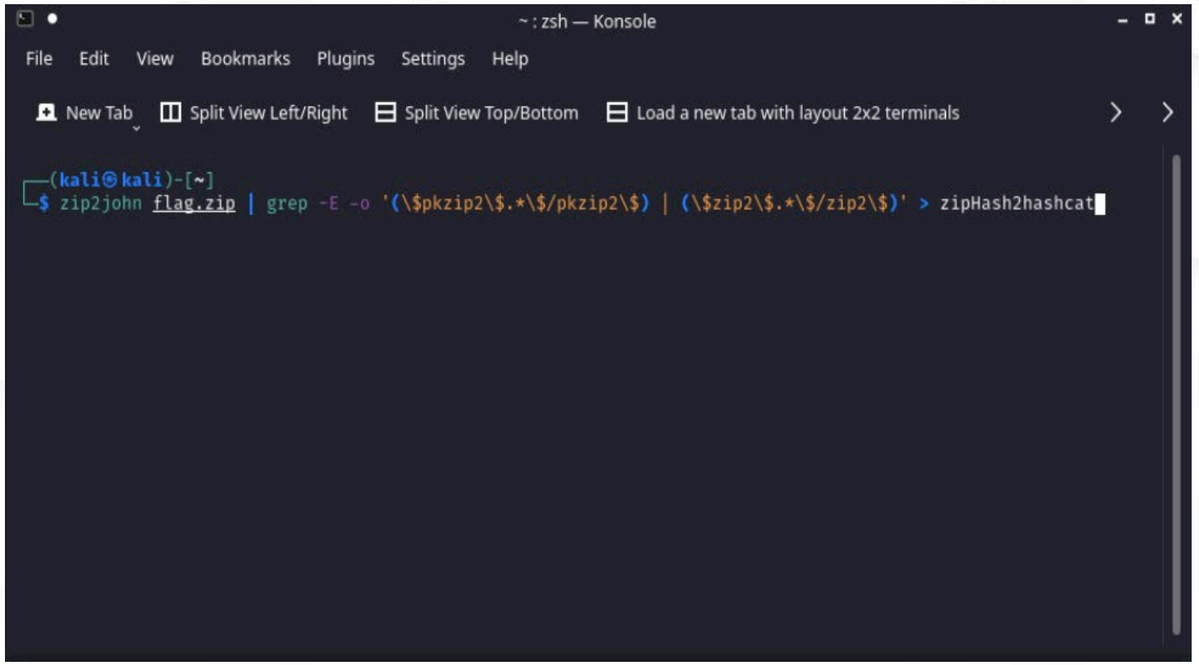
Criptografía - Hashes



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes





Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes


```
~ : zsh — Konsole
File  Edit  View  Bookmarks  Plugins  Settings  Help
New Tab  Split View Left/Right  Split View Top/Bottom

┌──(kali㉿kali)-[~]
└─$ john hashZip --wordlist=wordlists.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 16 needed for performance.
hola1234         (flag.zip/flag.txt)
1g 0:00:00:00 DONE (2021-09-30 16:55) 100.0g/s 100.0p/s 100.0c/s 100.0C/s hola1234
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~]
└─$ john hashZip --show
flag.zip/flag.txt:hola1234:flag.txt:flag.zip:flag.zip

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$
```

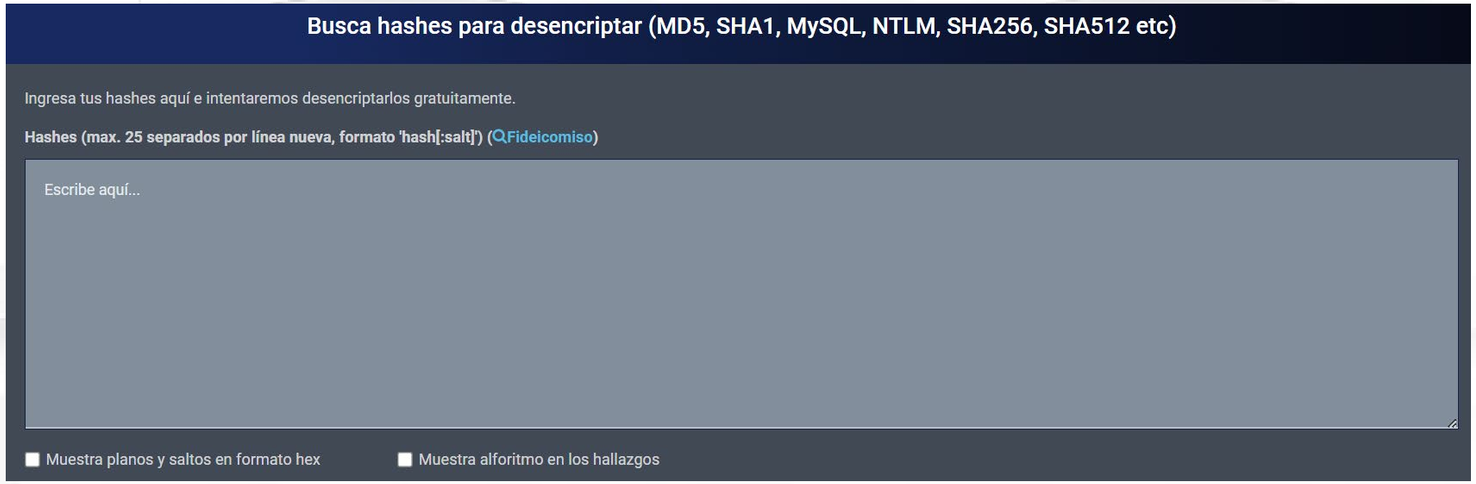
```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 13600 zipHash2hashcat ./wordlists.txt
hashcat (v6.1.1) starting ...
```

```
Session..........: hashcat
Status...........: Cracked
Hash.Name........: WinZip
Hash.Target......: $zip2$*0*3*0*f819c01513f1f5018f4e73128d711b52*8d6c* ... /zip2$
Time.Started.....: Thu Sep 30 16:59:35 2021 (0 secs)
Time.Estimated...: Thu Sep 30 16:59:35 2021 (0 secs)
Guess.Base.......: File (./wordlists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:        3 H/s (1.66ms) @ Accel:64 Loops:999 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 1/1 (100.00%)
Rejected.........: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-999
Candidates.#1....: hola1234 -> hola1234

Started: Thu Sep 30 16:58:55 2021
Stopped: Thu Sep 30 16:59:37 2021

┌──(kali㉿kali)-[~]
└─$ hashcat -m 13600 zipHash2hashcat --show
$zip2$*0*3*0*f819c01513f1f5018f4e73128d711b52*8d6c*c*327662bd488eec34fe3ad3fa*4b36073395bdba927dda*$/zip2$:hola1234

┌──(kali㉿kali)-[~]
└─$
```

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes

https://crackstation.net/



https://hashes.com/es/decrypt/hash &
https://hashes.com/en/tools/hash_identifier

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes

Dado los siguientes hashes extraídos de una base de datos, ¿podrías conocer el secreto?

1. 7a1a3d2146e0ab5340c0b96d4192112e
2. 317bd5baefa35ec490b328a7b5a44b3d50e410bc
3. e840ff16ef44f8b2fefdad3f4a77104d36d21726
4. 8979b983ddf689e074c399a20f49cb85f129d9d4
5. ad40a5b8f4c288ded741f1951d735d19b8ecf794

Reemplaza el resultado de cada hash formando una Flag tal que: UC{1_2_3_4_5}.

Cada palabra, contiene letras mayúsculas y números del 0 al 9.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Criptografía - Hashes

Como atacantes, esto nos viene bastante bien, dado que podemos intentar encontrar colisiones que nos favorezcan

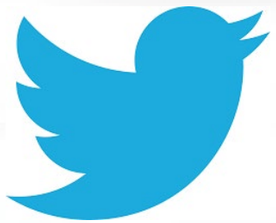
Como defensores, debemos utilizar siempre funciones hash seguras

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

OSINT

OSINT

- Se trata de descubrir información de fuentes abiertas (*Open Source Intelligence*).
- Normalmente, tirando del hilo llegaremos a la flag.
- Hay muchas formas de dar la información en estos retos.





Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

OSINT

- Habrá ocasiones que las páginas web que queremos visitar ya no están disponibles
- ¿Significa que han desaparecido de Internet?
- Recuerda que Internet, normalmente, es para siempre.

WayBackMachine: http://archive.org/

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

OSINT – Problema común

Tengo un amigo que acaba de empezar a jugar al CS:GO y se cree que es un pro player. Tanto que en algunas de sus redes sociales se hace llamar Pr0g4m3rCSG0. Incluso le ha dado por grabar vídeos con sus kills.

El otro día se dejó su cuenta abierta en mi PC y escondí una flag en su contenido, además de hacer alguna publicación en su nombre. ¿Puedes recuperar la flag?

https://www.tracelabs.org/blog/searchparty-ctf-2024-01

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

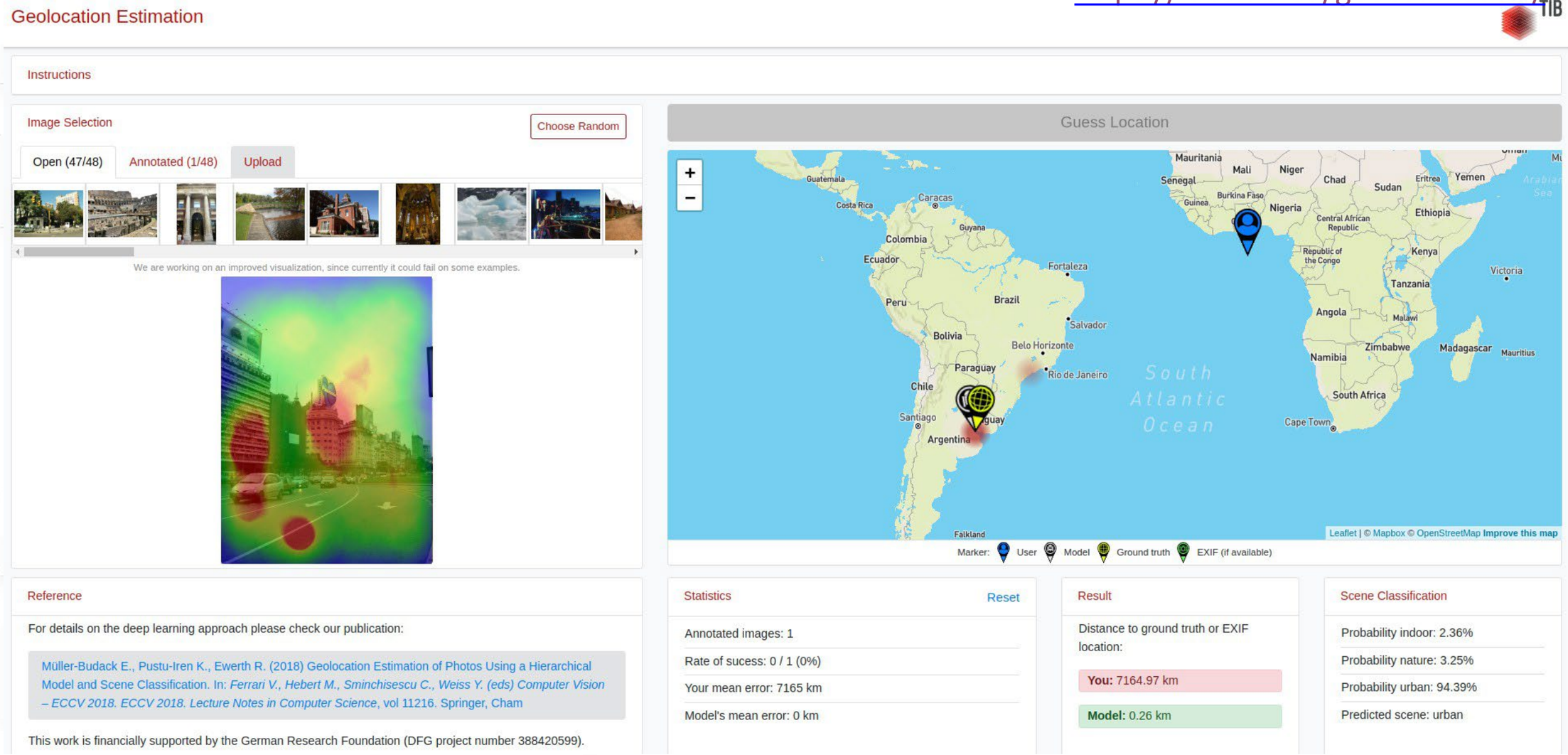
IMINT – Problema común

- Otras veces la información no es tan clara.
- Pueden darnos una imagen de la que partir para encontrar otra información:
  - En qué ciudad/calle/país/lugar se hizo la imagen.
  - Obtener información de una persona a partir de la imagen.
  - Encontrar un número de vuelo, número de teléfono, etc.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

OSINT - Herramientas

https://labs.tib.eu/geoestimation/



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

OSINT - Herramientas

- Google imágenes
- TinEye (https://tineye.com/)
- Yandex (https://yandex.com/)
- Google Lens
- Otros buscadores
  - DuckDuckGo,Bing…

Yandex

TinEye

Google Lens

DuckDuckGo

Microsoft Bing

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

HUMINT

Otro de los casos más comunes es que nos den (o encontremos durante nuestra investigación) algún dato personal de nuestro objetivo.

Tenemos entonces que empezar a utilizar otros mecanismos:

- Si es un mail: cuentas asociadas(https://tools.epieos.com), leaks asociados a esas cuentas (https://haveibeenpwned.com/)...
- Si es un número de teléfono: cuentas asociadas en RRSS, herramientas abiertas
- Si es un nombre: LinkedIn, Freelancer, TripAdvisor... redes donde se utiliza el nombre real
- Si es un usuario: redes sociales/plataformas como Twitter, Github, Instagram...
- https://github.com/sherlock-project/sherlock

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

OSINT - Retos

1. El marqués del castillo
2. El monumento
3. Stego is love, stego is life

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

HERRAMIENTAS

- https://osintframework.com/
- Histórico Web: http://archive.org/
- Localización Imágenes: https://labs.tib.eu/geoestimation/
- Imágenes: Google imágenes, TinEye (https://tineye.com/), Yandex (https://yandex.com/), Google Lens...
- Emails: https://tools.epieos.com , https://haveibeenpwned.com/
- Usuarios: Redes sociales, https://github.com/sherlock-project/sherlock

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

#CátedrasCiber

Módulo I: Introducción y Criptografía

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

Entidad colaboradora:
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria