POWERED BY iSEC

IA vs Cybsec → Aliados o rivales?

IA vs BESTIA

KNOWHOW SECURITY
SABEMOS QUE HACER

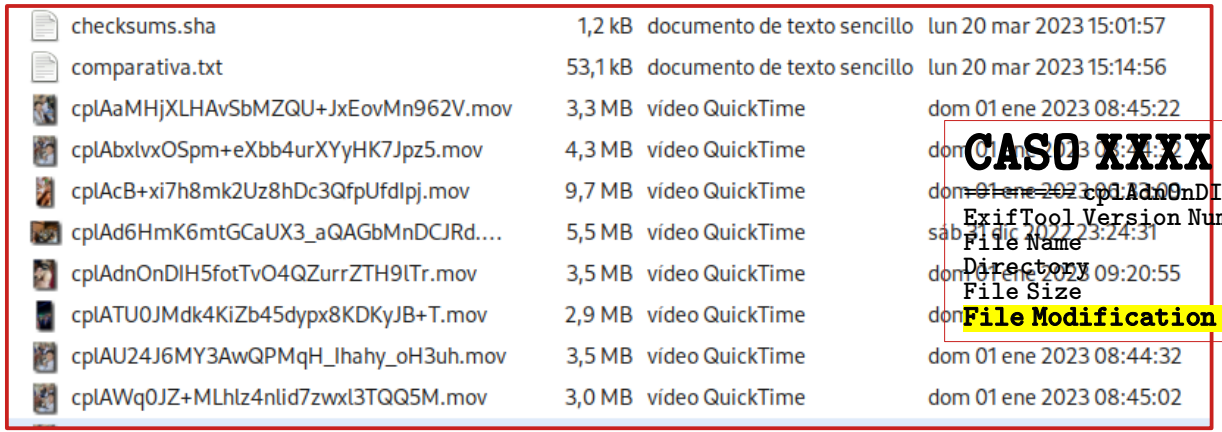
Analicemos una hipotética pelea entre IA vs Hombre

- Sería algo así como Robot vs Bestia
- Obviamente “la bestia“ seríamos nosotros
- 1er Round USO DE IA EN UNA CAUSA DE HOMICIDIO

1er Round USO DE IA EN UNA CAUSA DE HOMICIDIO

KNOWHOW SECURITY
SABEMOS QUE HACER

¿se imagina una persona analógica (supuestamente ignorante de la tecnología) modificar metadatos de un video para usar de coartada en un femicidio?...



checksums.sha	1,2 kB	documento de texto sencillo	lun 20 mar 2023 15:01:57
comparativa.txt	53,1 kB	documento de texto sencillo	lun 20 mar 2023 15:14:56
cplAaMHjXLHAvSbMZQU+JxEovMn962V.mov	3,3 MB	vídeo QuickTime	dom 01 ene 2023 08:45:22
cplAbxlvxOSpm+eXbb4urXYyHK7Jpz5.mov	4,3 MB	vídeo QuickTime	dom 01 ene 2023 08:23:23
cplAcB+xi7h8mk2Uz8hDc3QfpUfdlpj.mov	9,7 MB	vídeo QuickTime	dom 01 ene 2023 08:33:00
cplAd6HmK6mtGCaUX3_aQAGbMnDCJRd....	5,5 MB	vídeo QuickTime	sáb 31 dic 2022 23:24:31
cplAdnOnDIH5fotTvO4QZurrZTH9lTr.mov	3,5 MB	vídeo QuickTime	dom 01 ene 2023 09:20:55
cplATU0JMdk4KiZb45dypx8KDKyJB+T.mov	2,9 MB	vídeo QuickTime	dom 01 ene 2023 08:23:23
cplAU24J6MY3AwQPMqH_Ihahy_oH3uh.mov	3,5 MB	vídeo QuickTime	dom 01 ene 2023 08:44:32
cplAWq0JZ+MLhlz4nlid7zwxl3TQQ5M.mov	3,0 MB	vídeo QuickTime	dom 01 ene 2023 08:45:02

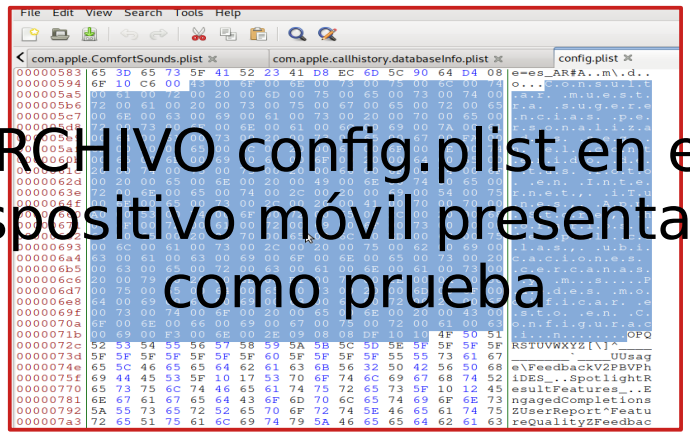
CASO XXXX → MODIFICACIÓN DE METADATOS

```
cplAdnOnDIH5fotTvO4QZurrZTH9lTr.mov
ExifTool Version Number         : 12.16
File Name                       : cplAdnOnDIH5fotTvO4QZurrZTH9lTr.mov
Directory                       : .
File Size                       : 3.3 MiB
File Modification Date/Time     : 2023:01:01 09:20:55-03:00
```

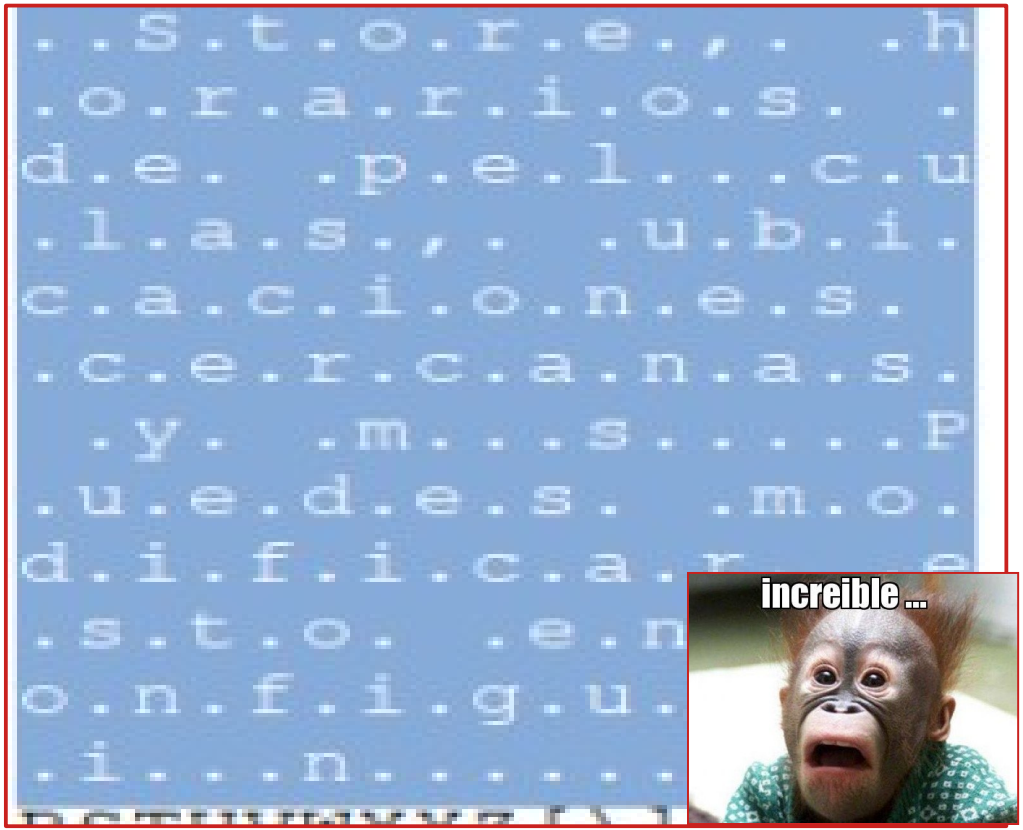
1er Round USO DE IA EN UNA CAUSA DE HOMICIDIO

KNOWHOW SECURITY
SABEMOS QUE HACER

resulta que los móviles ya habían pasado por varias pericias + software forense + algoritmos de búsqueda + …



ARCHIVO config.plist en el dispositivo móvil presentado como prueba



1er Round USO DE IA EN UNA CAUSA DE HOMICIDIO

KNOWHOW SECURITY
SABEMOS QUE HACER

- IA → adquisición de evidencia y procesamiento de datos
- BESTIA (yo) → interpretación de la escena del crimen (principio de reconstrucción histórica del hecho)

Celular Apple_iPhone 11 de [redacted]

El archivo "config.plist" guardó la última búsqueda realizada en la aplicación de configuración general (es el renglón al lado de la lupa), lo que se buscó fue: **"consultar-muestra-sugerencias-personalizadas-segn-el-contenido-de-tus-fotos-en-internet", "iTunes", "AppStore", "horarios-de-pel-culas", "ubicaciones-cercanas-y-m-5-puedes-modificar-esto-en-configuraci-on"**

NOTA → antes de llamar a emergencias en el celular de [redacted] se estaban preparando actividades para modificar los metadatos de los archivos y otras configuraciones

IA vs BESTIA

KNOWHOW SECURITY
SABEMOS QUE HACER

Analicemos una hipotética pelea entre IA vs Hombre

- ¿Cómo le fue a la IA contra la “viveza criolla” o “saber popular“????
- 2do Round USO DE IA EN UNO DE LOS PRIMEROS CHATBOT → Tai.ai (Twitter by Microsoft)

2do Round USO DE IA EN UNO DE LOS PRIMEROS CHATBOT POPULARES → Tai.ai

KNOWHOW SECURITY
SABEMOS QUE HACER

- IA → bot de conversación de inteligencia artificial
- BESTIA (nosotros) → chatbot poisoning que alteró el algoritmo de aprendizaje

Home / Innovation / Artificial Intelligence

Microsoft's Tay AI chatbot goes offline after being taught to be a racist

The internet teaches Microsoft a lesson in the dangers of artificial intelligence and public interaction.

IA vs BESTIA

KNOWHOW SECURITY
SABEMOS QUE HACER

Analicemos una hipotética pelea entre IA vs Hombre

- Mejor hagamos un enfrentamiento „EN VIVO“
- FINAL ROUND

3er Round Preguntémosle su opinión

KNOWHOW SECURITY
SABEMOS QUE HACER

Preguntémosle a ella misma a ver que opina:

- usar AI en ciberseguridad es bueno?
- https://chatgpt.com/

„Sin embargo, es importante tener en cuenta que la Ai no es una solución mágica y debe ser parte de una estrategia de ciberseguridad integral que incluya medidas preventivas, defensivas y de respuesta…“

- AI → Es inocente, nunca jugó al mortal kombat
- BESTIA (NOSOTROS) → Soy tu mejor solución!!!

KNOWHOW SECURITY
SABEMOS QUE HACER

IA vs Cybsec → Aliados o rivales?

IA A MÍ NO ME DURA NI DOS ROUNDS!!

KNOWHOW SECURITY
SABEMOS QUE HACER

“La Pelea del Siglo” entre Muhammad Ali y Joe Frazier

https://knowhowsec.com/

KNOWHOW SECURITY
SABEMOS QUE HACER

Red Team Dōjō

Web Security Dōjō

Phishing Attack Dōjō

Enhance awareness against risks

Entrenamiento intensivo en todas las modalidades del ataque de Phishing, incluye

MUCHAS GRACIAS

POWERED BY iSEC

powered by KnowHow Security Labs ® - CeVila - christian.vila@knowhowsec.com