RedRoom CTF Workshop – Forensics

27/11/25

ORIGINAL POWERPOINT BY: MONIQUE CORNALL

PRESENTED BY: LINDSAY COUDERT

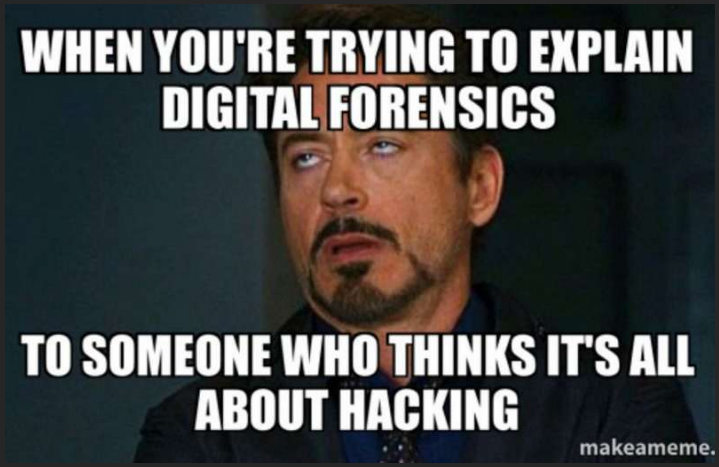
What is Digital Forensics

- Process of investigating and analysing data stored in electronic devices to find evidence of a crime
- Skills:

Critical Thinking

Analysis

Curiosity


WHEN YOU'RE TRYING TO EXPLAIN DIGITAL FORENSICS
TO SOMEONE WHO THINKS IT'S ALL ABOUT HACKING
makeameme.

Types of Forensics found in CTFs

- Network traffic analysis
- Picture analysis (steganography)
- Filesystem analysis
- Audio analysis
- Data & Broken files
- Memory analysis

Network Forensics

TOOLS: WIRESHARK, TCPDUMP, NETWORKMINER

FILE: .PCAP .PCAPNG

Network Forensics
- Approach

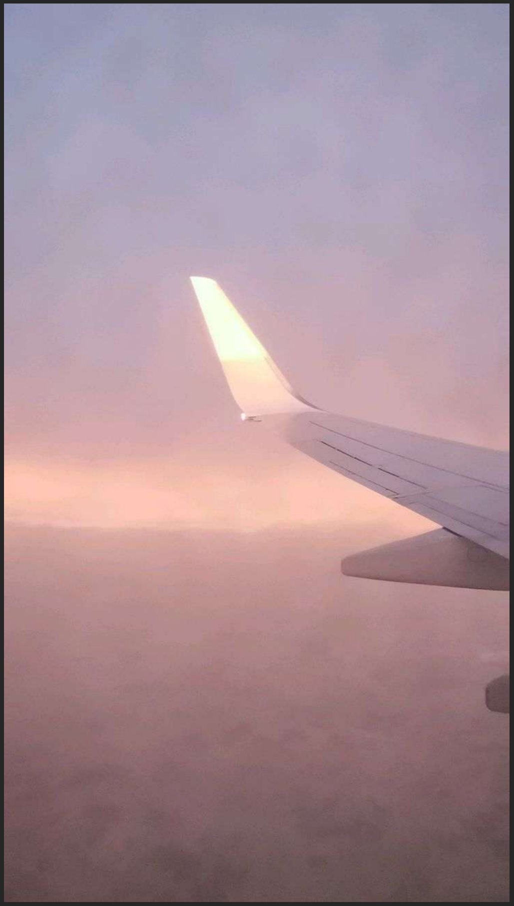
- Look at strings
- Follow streams

  Right click a packet → Follow → Stream decided
- Export objects

  File → Exports Object → HTTP

Network Forensics - Challenges

- Packets Primer
- wireshark doo doo…
- DoS’ed out



Picture Analysis

- Metadata

  Additional information about the image, that gets stored with the image file

  (Comments, Author, Date and Time, camera type, date modified)

  Tools: exiftool and metadata2go

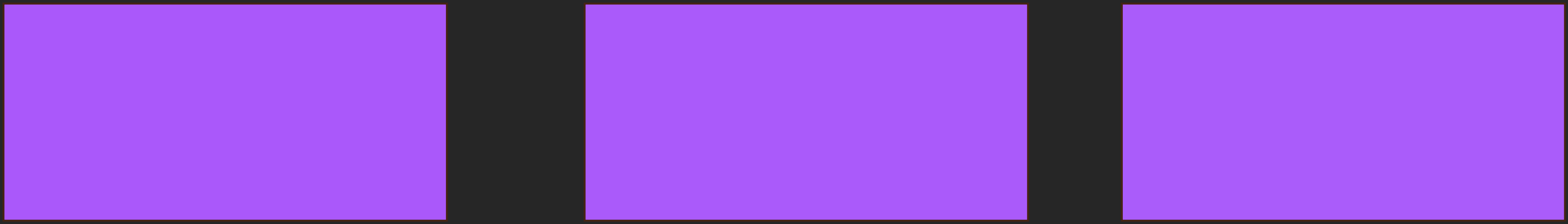
- Steganography

  Practise of hiding information within other information/content

  Files, messages, images

  Tools: steghide, zsteg, cat/strings

Picture Analysis - Steganography



170, 88, 250	170, 90, 250	170, 92, 250
X	Z	\

Picture Analysis - Approach

- Look at the metadata – Any additional information that could be a clue?

  File type is also a good indicator to understand what you are dealing with

- Analyse the image on a base level

  Does the image itself leave any clues?

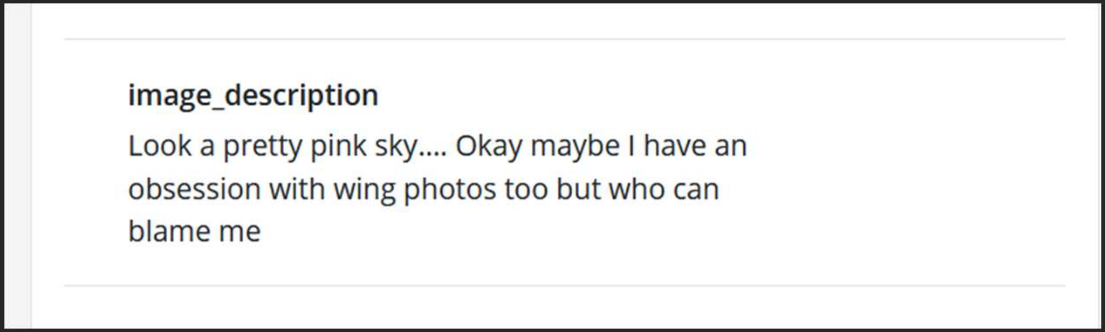
- Look into the image raw code

  cat, strings, hex editor, etc

- Are there any hidden files in the image?

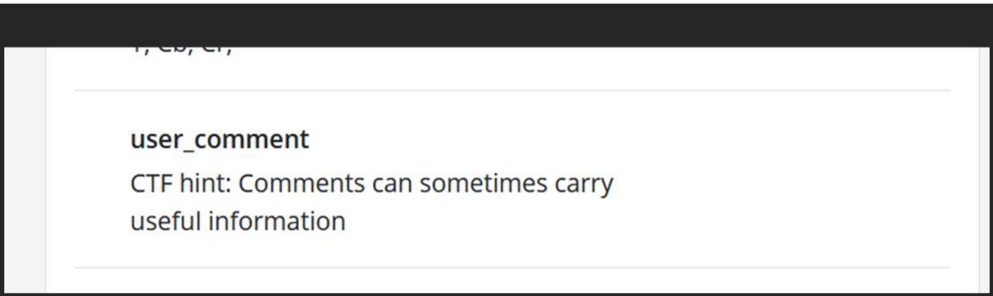
  Certain image types act as folders

Metadata Finds useful in CTFS



image_description

Look a pretty pink sky…. Okay maybe I have an obsession with wing photos too but who can blame me



Y, Cb, Cr,

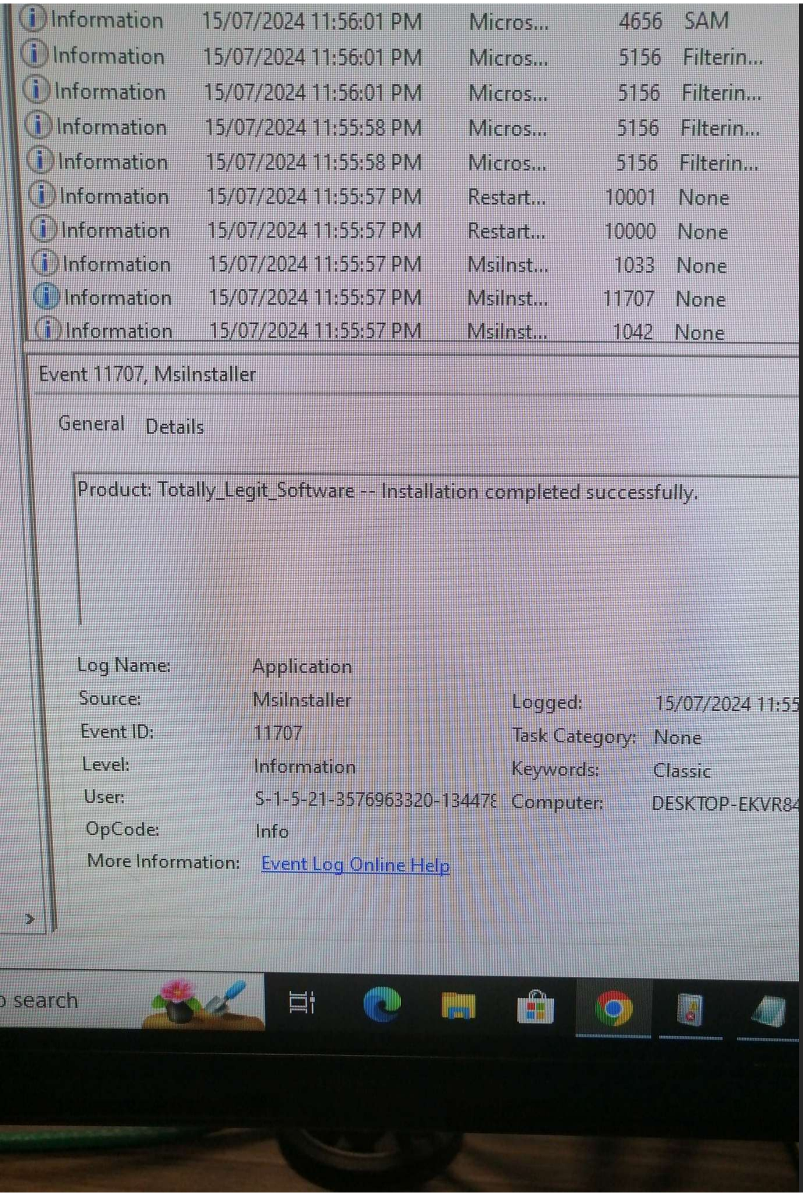
user_comment

CTF hint: Comments can sometimes carry useful information

Using that comment – we are going to go back and visit the metadata of the photo of the wing from earlier and see if we can find something else

OS Forensics

TOOLS: AUTOPSY, EVENT LOGS, REGISTRY,



```
Information   15/07/2024 11:56:01 PM   Micros...    4656   SAM
Information   15/07/2024 11:56:01 PM   Micros...    5156   Filterin...
Information   15/07/2024 11:56:01 PM   Micros...    5156   Filterin...
Information   15/07/2024 11:55:58 PM   Micros...    5156   Filterin...
Information   15/07/2024 11:55:58 PM   Micros...    5156   Filterin...
Information   15/07/2024 11:55:57 PM   Restart...  10001   None
Information   15/07/2024 11:55:57 PM   Restart...  10000   None
Information   15/07/2024 11:55:57 PM   MsiInst...   1033   None
Information   15/07/2024 11:55:57 PM   MsiInst...  11707   None
Information   15/07/2024 11:55:57 PM   MsiInst...   1042   None
```

Event 11707, MsiInstaller

Product: Totally_Legit_Software -- Installation completed successfully.

Log Name: Application

Source: MsiInstaller Logged: 15/07/2024 11:55

Event ID: 11707 Task Category: None

Level: Information Keywords: Classic

User: S-1-5-21-3576963320-134478 Computer: DESKTOP-EKVR84

OpCode: Info

More Information: Event Log Online Help

What Can Security Logs tell us

- Tracks Activities – User logins/logouts file access and system changes
- Identify anomalies –login fails or suspicious program execution
- It allows for the investigator to build an event timeline

Consolidation

- Variety of types of forensics
- Network forensics: wireshark, understanding protocols
- Picture analysis: steganography, metadata

  Exiftool, strings, grep, zsteg
- Broken files: file signatures & hex editor

- Extra Challenges: WebNet1, c0rrupt
- TryHackMe: Intro to Digital Forensics, Windows Forensics, Memory Forensics, etc.

Happy Hunting!