HALMSTAD UNIVERSITY

DFRWS EU 2024 Workshop: Python toolbox for mobile forensics

Johan Wallengren
Halmstad University

Hello! 👋

- My name is Johan Wallengren
- Research Engineer @ Halmstad University
- Operations Developer & Digital Forensic Expert
  @ Swedish Police – National Forensic Centre

@j_wallengren

@johwal@infosec.exchange

Johan Wallengren

Today! 🗓️

- Simple Toolbox for using Python with extracted data from mobile phones
- On a very basic level, we will learn to:
  - Handle zip-files
  - Handle sqlite-databases
  - Handle plist files
  - Handle protobufs
- We will then assemble everything to build a simple script to access one artefact.

What you need? ✌️

- A good mood 😉
- In the beginning, you need the zip-file:
  - “exerciseFiles.zip”
  - Go ahead and unpack it!
- You need a Python IDE
  - I recommend PyCharm (Community edition)
- At the end of the workshop, we are going to use:
  - “Magnet CTF 2022 iOS subset minimal.zip” (≈1,4 GB)

https://tinyurl.com/DFRWSPYTHON

https://github.com/joh-wal/DFRWS2024

What you need? ✌️ part 2

- We are going to use the following packages:
  - zipfile
  - gzip
  - plistlib / biplist*
  - sqlite3
  - blackboxprotobuf*
  - NSKeyedUnArchiver*

- * Needs to be installed – not part of the standard library
  - Don't panic! 🫨 I will show you how.

Lastly what you need to know

- I will go slow, but this is no basic Python workshop
- I am no Python Expert
  - I often write code that is easier to read than the more advanced syntax
- This is a ”code-along”. Stop me if I go to fast!