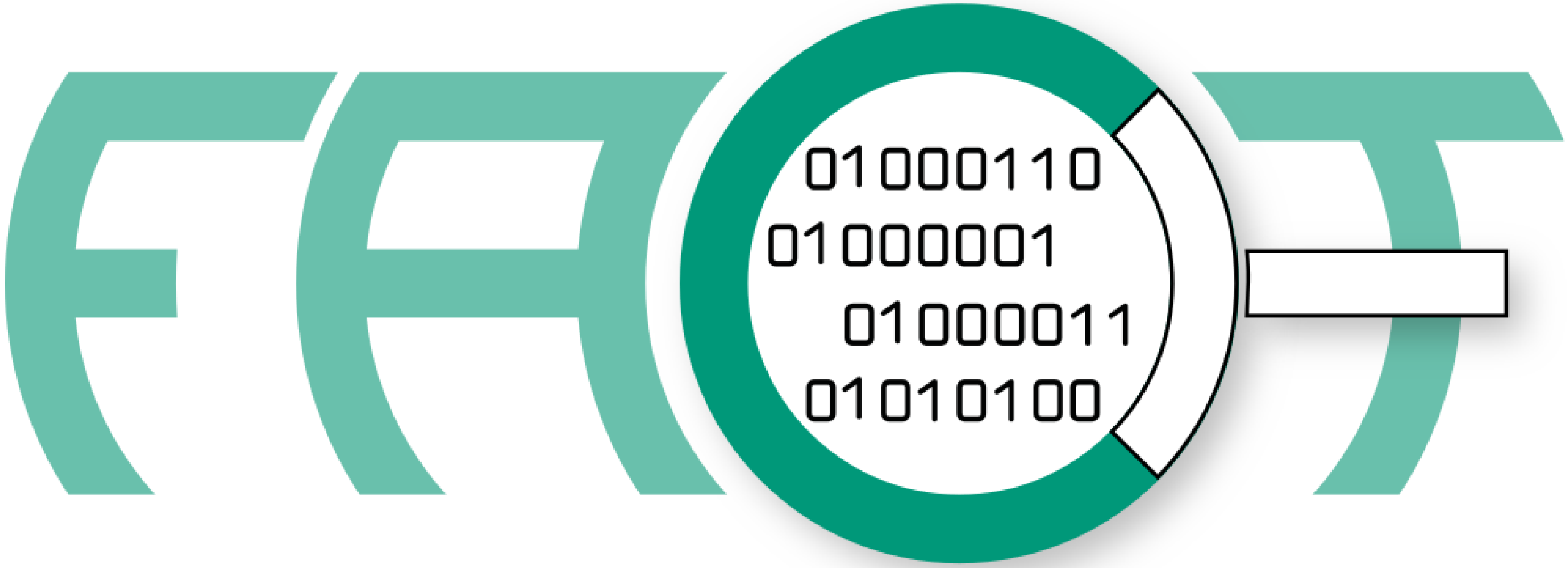
ENTER FACT

BOOST YOUR FIRMWARE SECURITY ANALYSIS WITH AUTOMATION, VISUALIZATION, AND CROSS REFERENCING

Peter Weidenbach @weidenba1

Johannes vom Dorp @jovomdorp

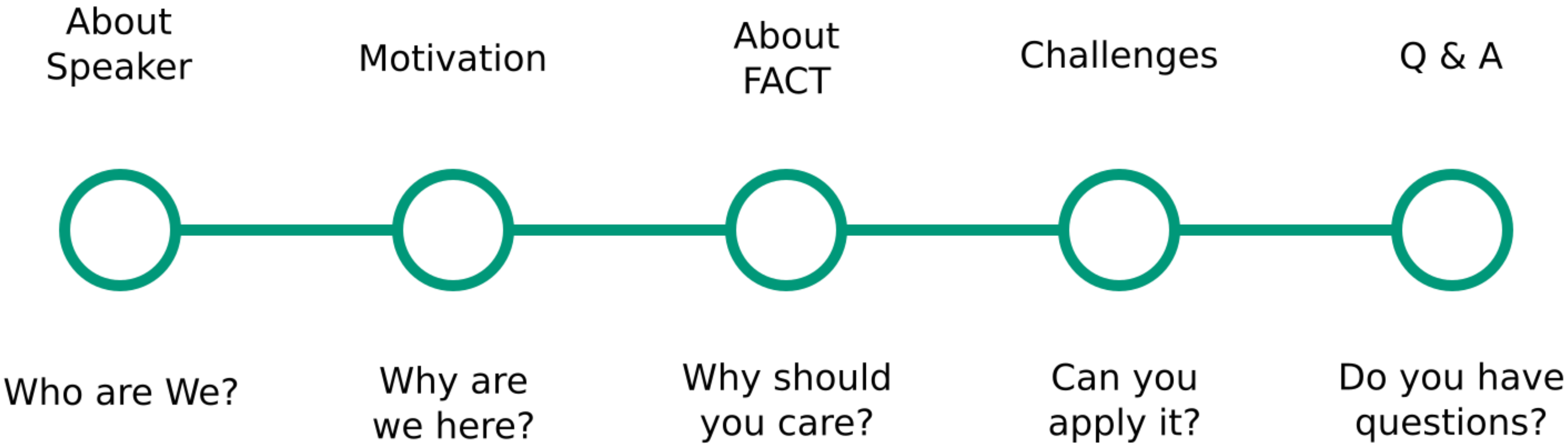
@FAandCTool



FIRMWARE ANALYSIS AND COMPARISON TOOL

Fraunhofer
FKIE

AGENDA



About Speaker
Who are We?

Motivation
Why are we here?

About FACT
Why should you care?

Challenges
Can you apply it?

Q & A
Do you have questions?

About Speaker

Who are we?

- Currently researchers at Fraunhofer FKIE in Bonn, Germany
  - PW: Graduated 2013 as Dipl.Ing. in Computer Science
  - JvD: Graduated 2016 as M.Sc. in Computer Science
- Started doing hardware related work around 2014
- In 2015 wrote first LOCs for FACT (f.k.a. FAF)
- Relevant publications
  - Xerox Printer Ransomware Whitepaper 2016
  - FACT @ HW.io 2017
- Awesome Embedded and IoT Security List
  - https://github.com/fkie-cad/awesome-embedded-and-iot-security

Motivation

Why are we here?

- Spread the word
  - FACT was open sourced in 2017 after 2 years development
  - Tool presentations at hardwear.io, BlackHat Arsenal, Pass the Salt
  - Currently at ~ 340 Stars on GitHub
  - There is room to grow
- Interact with community to get feedback / improve on use cases
  - Show use and see what‘s not intuitive
  - Where is improvement needed?

About FACT

Why should you care?

Typical firmware analysis process

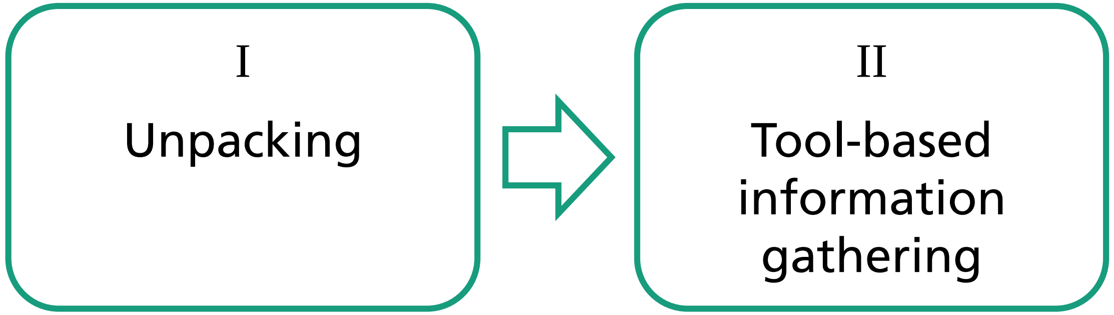
I

Unpacking

About FACT

Why should you care?

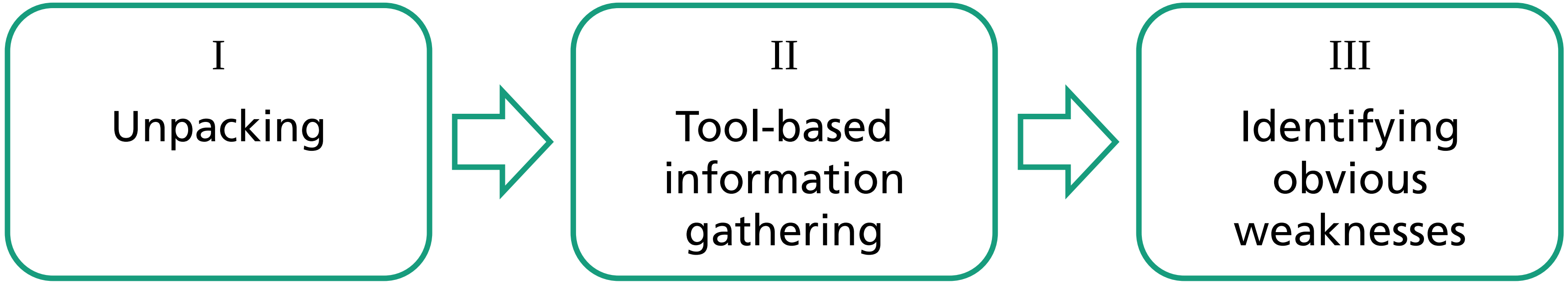
Typical firmware analysis process



About FACT

Why should you care?

Typical firmware analysis process



I

Unpacking

II

Tool-based information gathering

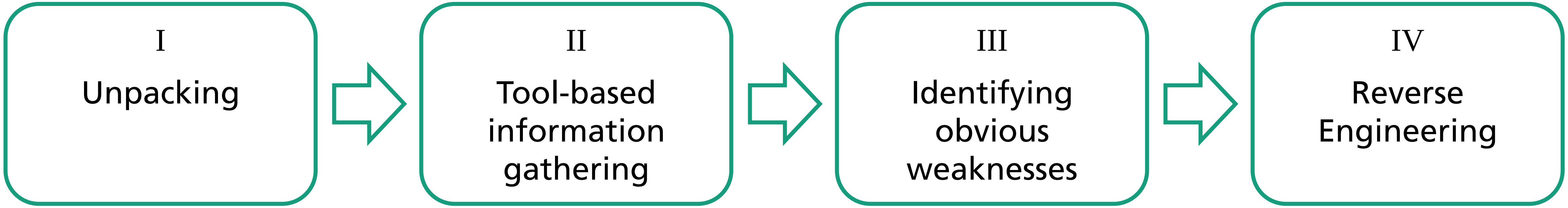
III

Identifying obvious weaknesses

About FACT

Why should you care?

Typical firmware analysis process


I
Unpacking

II
Tool-based information gathering

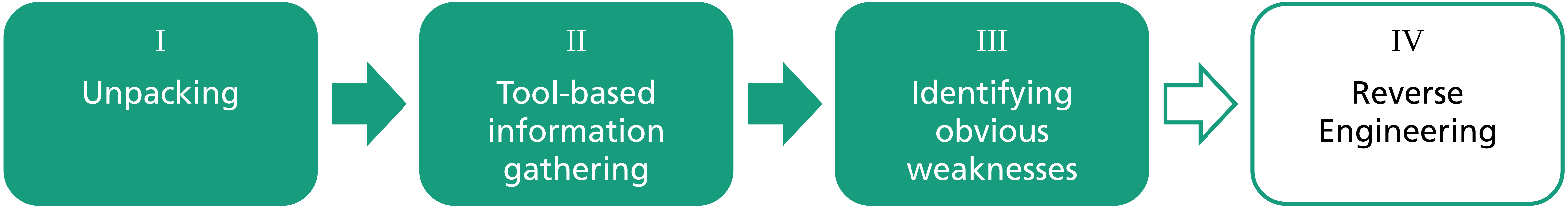
III
Identifying obvious weaknesses

IV
Reverse Engineering

About FACT

Why should you care?

Firmware analysis process with FACT



I
Unpacking

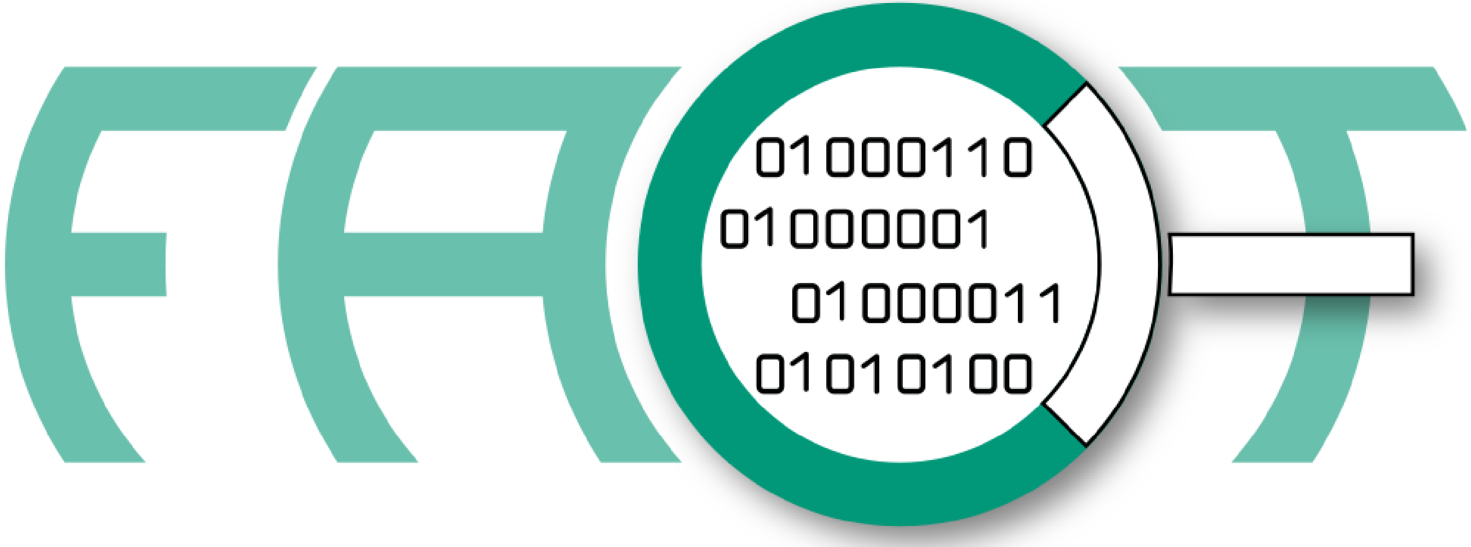
II
Tool-based information gathering

III
Identifying obvious weaknesses

IV
Reverse Engineering

About FACT

Why should you care?

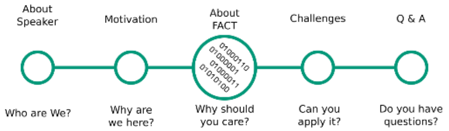


Firmware Analysis and Comparison Tool

https://github.com/fkie-cad/FACT_core

About FACT

Why should you care?



DEMO

FACT Demo System

- SSIDs:
  - FACT-A
  - FACT-B
  - FACT-C
- Password: FK13!R0ck5
- FACT-Server: https://192.168.5.1

Challenges

Extraction

- Find firmware image for TP-Link TL-WR810N
- Which kind of files are contained (fs, executable, library, text ..)
- Is the firmware extracted correctly
  - Would it be possible to repack it with standard tools?
- Compare extraction of image for Ubiquity UniFi AP

Challenges

Xerox Case Study

- Background
    - 2013: D. Heiland: „From Patched to Pwned“ (Xerox WorkCentre 5632)
        - Firmware signature tool inside the firmware itself (dlm_toolkit)
        - Firmware update via print job on jetdirect port

Challenges

Pattern Matching

- Have a look at dlm_maker executable in “Xerox WorkCentre 5632”
- Write a yara rule identifying dlm_maker executeable.
- What other Firmware samples might be affected by the same issue?

Challenges

Xerox Case Study (ctnd.)

- Background
  - 2013: D. Heiland: „From Patched to Pwned“ (Xerox WorkCentre 5632)
    - Firmware signature tool inside the firmware itself (dlm_toolkit)
    - Firmware update via print job on jetdirect port
  - 2016: P. Weidenbach: „Pwn Xerox Printers (again…)“ (Xerox Phaser 6700)
    - Few minutes to get the exploit working again after Xerox fixed the issue

Challenges

Firmware Compare 1

- Compare “Xerox Phaser 6700” firmware versions
- How did Xerox fix the issue?
- What to do to get the exploit working again?

Challenges

Firmware Compare 2

- Compare „D-Link DWR-932“ firmware versions 2.02 und 2.03
- Version 2.02 contains an open ssh port with hardcoded password
- Did the vendor fix the issue with the patches in version 2.03?

Challenges

Quick reversing

- Firmware “Unknown IOT Device” contains the **unknown.elf**
- On which architecture does it run?
- Find out as much as possible of what it does
  - You can use (e.g.)
    - elf analysis
    - exploit mitigations
    - radare2 integration

radare2 cheat sheet (script tab)

- Run single command by dropping it in place of “?V”

  → `r2.cmd("?V", log);`

  - `s <0x????>` - Go to address
  - `s/ <string>` - Search and jump to string

Challenges

Owning

- Analyze firmware version 4.0.42 for Ubiquity UniFi AP
  - Look for software, configurations, etc.
  - Do you find issues?
- Try using issues to make connection to device
- What can you do now?

Challenges

Reproducing Vulnerability

- Search online for CVE-2013-0714
  - What is it about?
  - Can you find affected devices in the database?

Challenges

Low level analysis

- Look at Firmware image Jetter JetControl 647
  - What kind of OS do you guess it implements? (UNIX, RTOS, NONE)
  - Can you find included software?
  - Can you identify/guess the OS?

Thanks and Q & A

Do you have questions?

@FAandCTool

@weidenba1

@jovomdorp

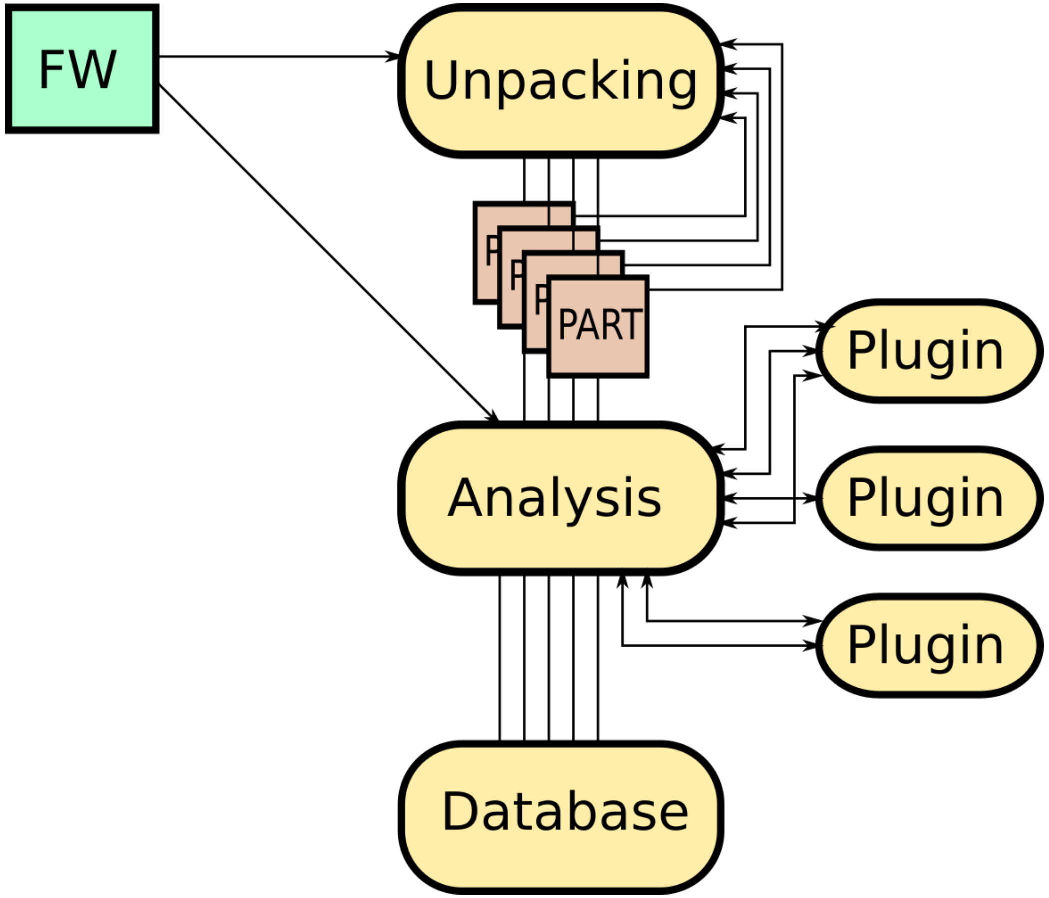
Thanks for your attention !!

Don‘t spare the hard hitting questions

About FACT

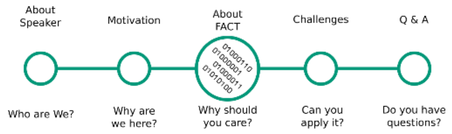
Why should you care?

- FACT architecture
  - Multilayered automated extraction
  - Purpose-driven analysis scheduling
  - Storage for querying, visualization

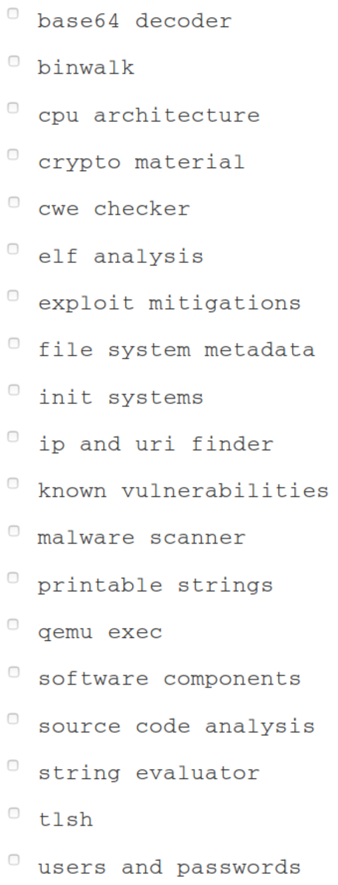


About FACT

Why should you care?



- Some useful analysis plugins
  - Linux-style FW
    - elf analysis (behavior tagging)
    - exploit mitigations (nx, canary, relro etc.)
    - cwe checker
    - source code analysis
  - Arbitrary FW
    - binwalk (yes, that binwalk)
    - crypto material
    - software components
    - (known vulnerabilities)



□ base64 decoder
□ binwalk
□ cpu architecture
□ crypto material
□ cwe checker
□ elf analysis
□ exploit mitigations
□ file system metadata
□ init systems
□ ip and uri finder
□ known vulnerabilities
□ malware scanner
□ printable strings
□ qemu exec
□ software components
□ source code analysis
□ string evaluator
□ tlsh
□ users and passwords

About FACT

Why should you care?

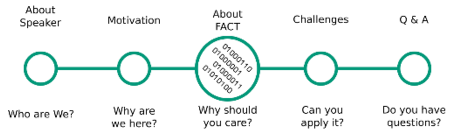
- Interfacing
  - Web UI
    - (Mostly) intuitive click-and-see interface
    - Full functionality exposed
    - Use for analysis, monitoring, querying, statistics
  - REST API
    - Most functionality exposed
    - Use for automation, repetitive tasks, integration

https://localhost/about

{ REST }

About FACT

Why should you care?



- Input for RE
  - Quick first observations with r2 integration
  - Addresses of potential vulnerabilities
  - Information on behaviour of unknown binaries
  - …
- Input for future analysis
  - Queryable database containing all analysis results
  - Compare feature for finding commonalities / changes
  - Cross referencing vulnerabilities using yara rules
  - …