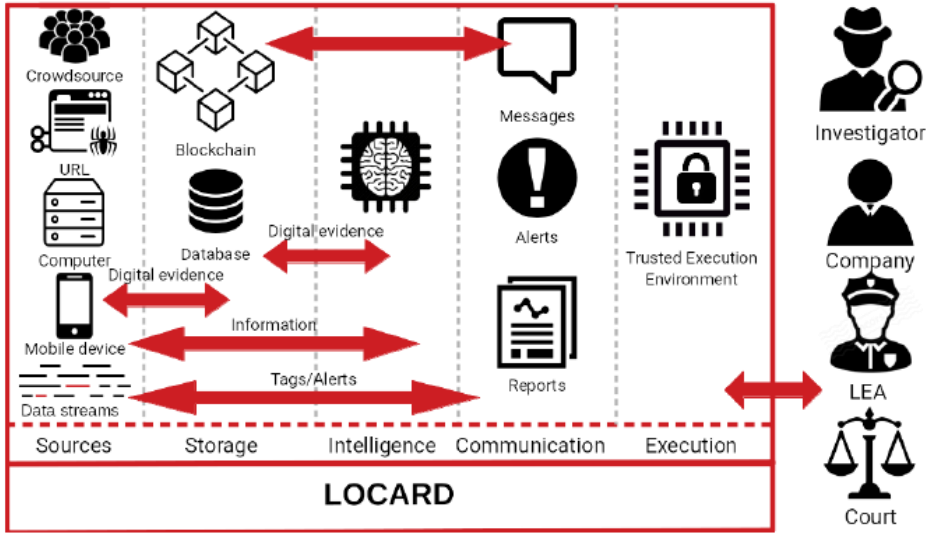
# LOCARD

(Lawful evidence collecting and continuity platform development)
an EU-wide automated case management for cybercrime.

This project has received financial support
from the European Union Horizon 2020
Program under grant agreement no. 832735

https://locard.eu

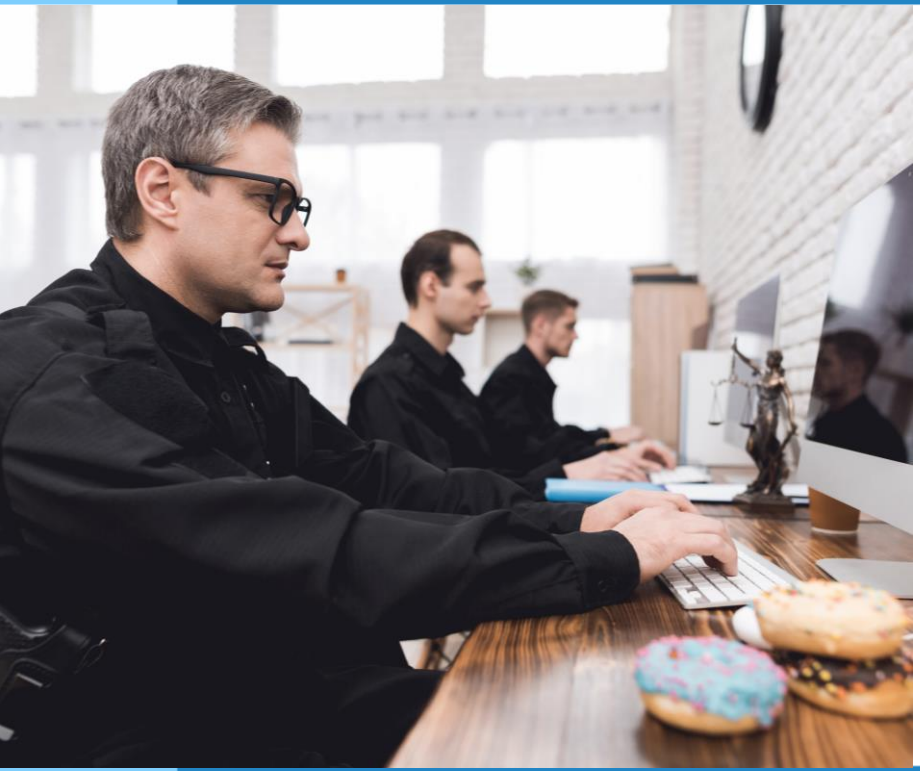
# What is LOCARD?
# EU-wide automated cybercrime case management




LOCARD will provide a holistic platform for chain of custody assurance along the forensic workflow and a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain.

This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

# Cross-Border & Latest Technology Applicability



- Legal frameworks in all relevant national levels as well at EU level will be analysed to identify and develop proper mechanisms to facilitate cross-jurisdictional use of digital evidence, enhancing LEAs' capabilities especially in cases when time is crucial (e.g. Child abuse, TV stream piracy, data exfiltration, cyber bullying).
- Suitable identity management and access control methodology to meet the requirements of LOCARD and all its stakeholders.
- Evidence collectors for latest technology.

This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

# LOCARD Consortium

















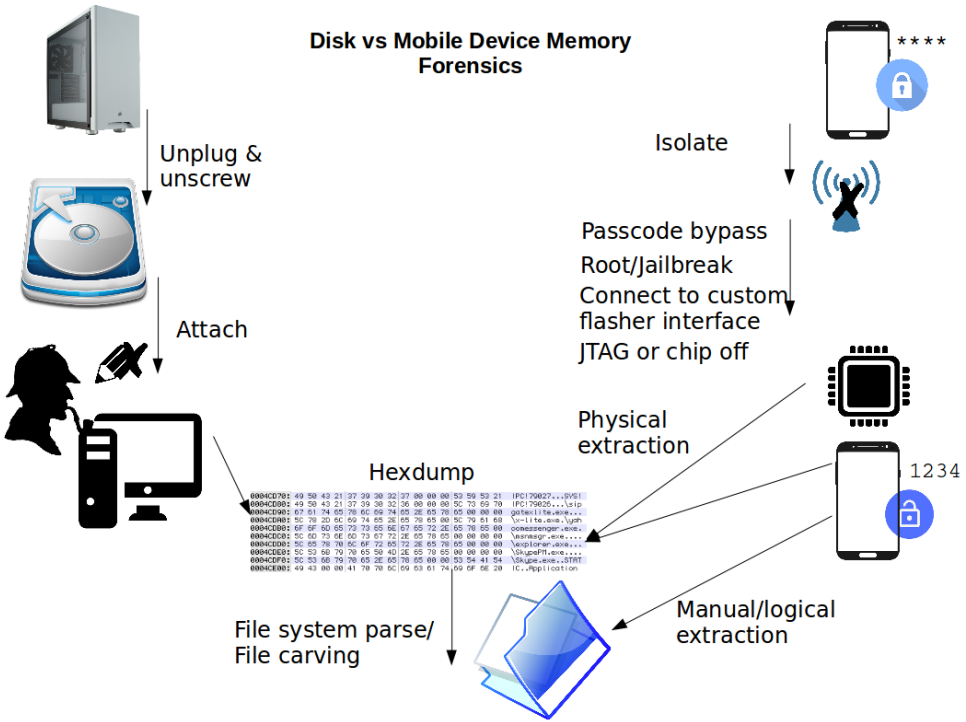
Hochschule für den öffentlichen Dienst in Bayern

| | |
|---|---|
| Start Date | 1st May 2019 |
| Duration | 36 months |
| Call | H2020-SU-SEC-2018-2019-2020 |
| Topic | SU-FCT02-2018-2019-2020 |
| Budget | 6,843,385.00€ |

This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

# Mobile device forensics

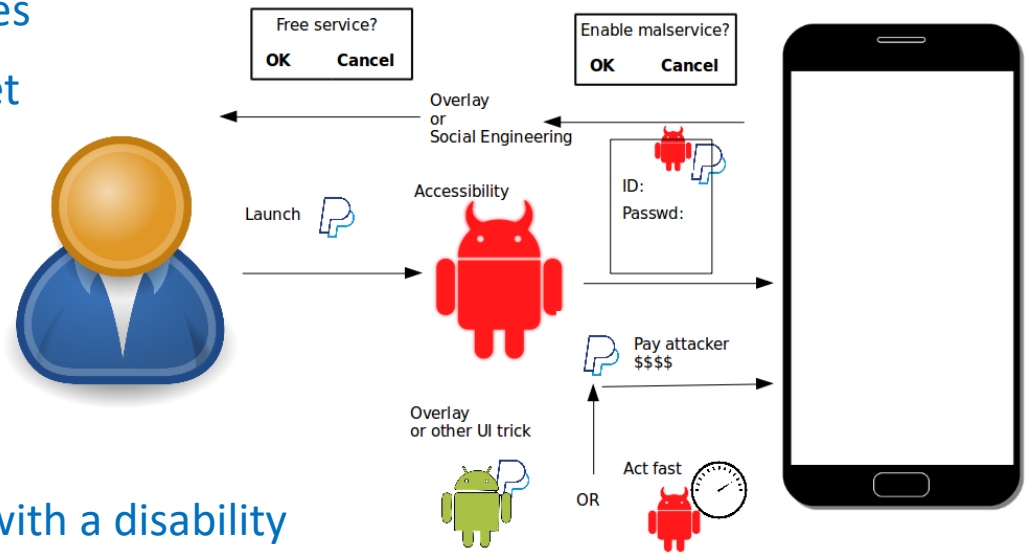
- Technical challenges
- for tool developers
- and investigators alike




This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

# Incident handling i

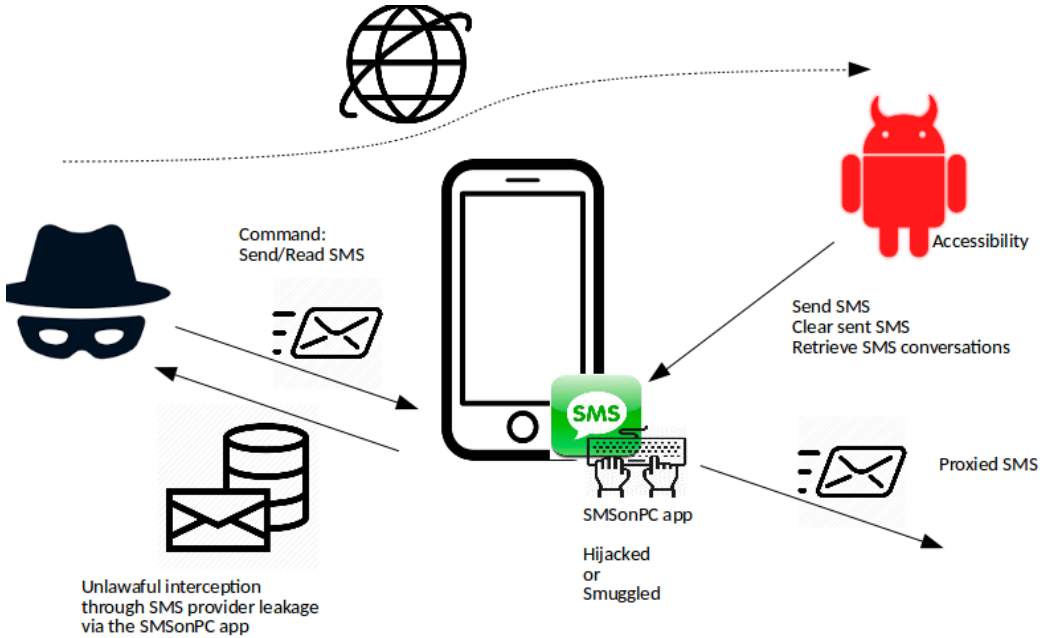
- Digitally investigating security breaches
- Where cyber and physical crimes meet
  - Spying or covert communication
- Android design vulnerabilities
  - Accessibility & overlays
- Overlays increased restrictions
- Accessibility is now a pandora's box
  - Accessibility goes beyond users with a disability
  - Accessibility are trojans on the rise




This project has received financial support
from the European Union Horizon 2020
Program under grant agreement no. 832735

# Incident handling ii

- Messaging hijacking: Long-term stealth
- Appstore detection
  - What is correct usage of accessibility services?
  - Sandbox evasion
- Anti-malware
  - What if messaging app is white-listed? – Living-off-the-land
- Malware analysis
  - What if there is no sample yet?




This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

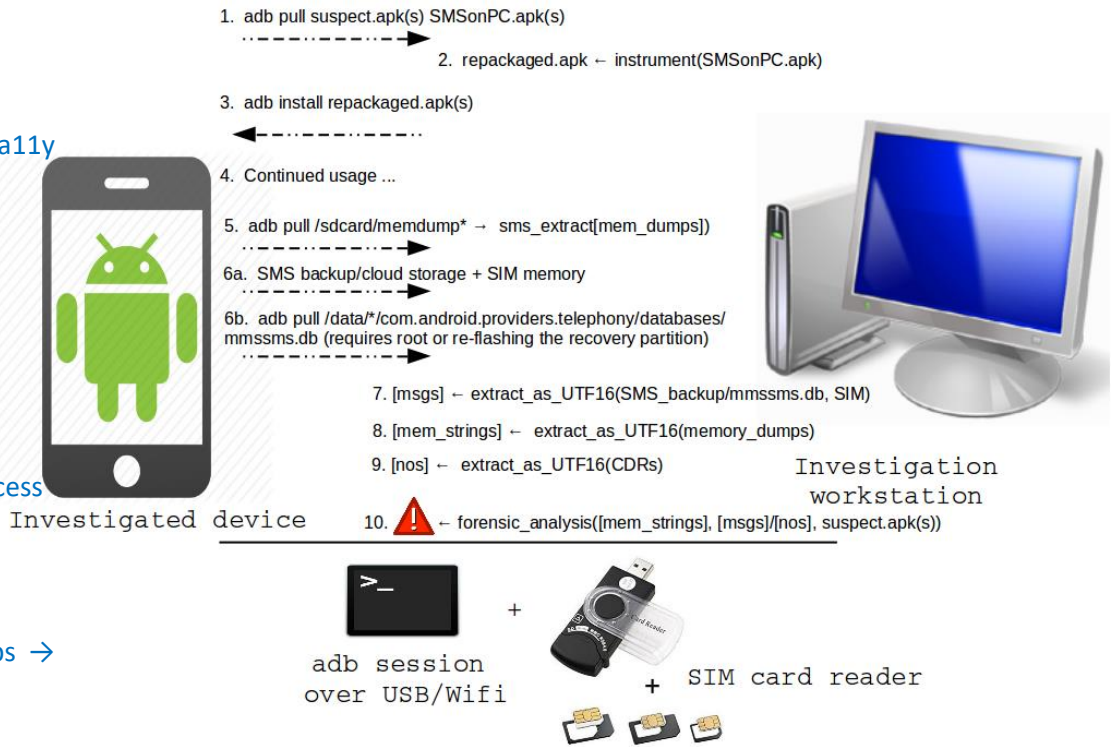
# Android memory forensics i

- Crime proxy: deleted sent messages for stealth
- Unlawful interception: No recording of message read accesses
- Root problem: No SMS send/read SMS flow tracking and recording
- Recover from just-in-time memory dumps


This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

# Android memory forensics ii

- Full flow tracking vs event-driven in-memory artifact collection,
- any SMS send/read flows coupled with draw-on-top and a11y activities should be regarded as suspicious
- Artifacts:
  - Dalvik heap of SMSonPC apps
  - Native heap of phone process (requires device rooting)
  - Should contain originating/stolen sms messages
- Triggers inside candidate target SMSonPC apps:
  - Send/read SMS
  - Native method calls (if native heap of phone process is collected)
- Smali-level patching approach in prototype
  - User, not system, apps
- No user consent for i)CDR nos; ii)msgs found inside dumps → SMS hijack : to be ascertained by fully reversing suspect malware




This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

# A novel *experimental* concept

- ***JIT-MF***: Just-in-time Memory Forensics (for Android)
  - Event-driven collection of evidence from volatile memory
  - For acquisition, it requires an amount of forensic readiness to be applied to the device in question;
  - with DBI earmarked as a core enabler technology for dumping ephemeral evidence in a timely manner before it gets overwritten; and
  - which overall carries the challenge of keeping runtime overheads and storage requirements for dumps minimal.
  - For the analysis stage, it requires preparatory work that goes beyond knowledge of file-systems, file formats, and long-lived kernel memory data structures.
  - Rather, it has to tap into more specific data structures, possibly ones custom-designed for individual applications.
- for Advanced Threat Protection (ATP) / End-point Detect and Recover (EDR) / Forensic Record-and-Replay

This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735

# Thank You

Mark Vella
Principal Investigator
mark.vella@um.edu.mt

L-Università ta' Malta

Constantinos Patsakis
Coordinator
info@locard.eu
https://locard.eu

LOCARD

This project has received financial support from the European Union Horizon 2020 Program under grant agreement no. 832735