POLITIET

Cyber Crime Fighting

Keynote BSides 2023

Oslo 19th of September

By Steffen E. Thorkildsen

NCIS / NC3

(KRIPOS)

POLITIET

Keynote

- Length: 45 minutes.
- In this keynote, the National Cyber Crime Centre (NC3) at NCIS Norway will present how they fight and prevent cybercrime. With a historical perspective on how technologies have given both opportunities and challenges, we will learn more about methods, cases and plans on how to stay relevant also in the future!
- Keywords: *cyber crime*, *digital forensics*, *incident response*, *international collaboration*, *innovation*, *research and development*, *how to stay relevant* and *some lessons learned*.

POLITIET

About me

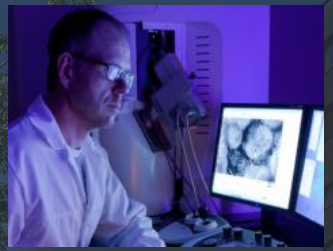
- Head of Section at the National Cyber Crime Centre (NC3) in Norway, which is part of the National Criminal Investigation Service (NCIS).
- 25+ years working experience with digital forensics, cyber security, serious crime investigations and developing organizational capability for tackling modern IT challenges
- Academic and R&D background and interests involves programming, reverse engineering, exploitation, machine learning, cyber security and related topics.

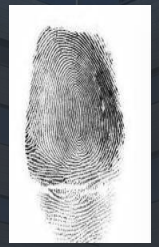
POLITIET

POLITIET

The National Criminal Investigation Service (NCIS)

Special Agency for Fighting Organized and Serious Crime

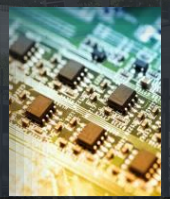


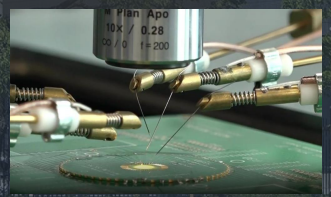


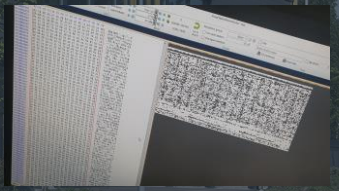











POLITIET

The National Cyber Crime Centre (NC3) at NCIS

Prevent, detect and combat threats and crime in cyberspace.

Our mission:

The NC3 will provide robust national capacity to combat cybercrime and online child sexual abuse. The centre will further contribute to increased awareness and knowledge about the causes of crime in a digital society, capacity to preserve digital evidence, and by developing the professional skills of the local police, develop the police's total capability to combat cybercrime. This will contribute to uphold the public's trust in the police, the public's safety and legal protection.

POLITIET

TICAT

Triage, Incident Coordination and Tasking Section

CIS

Cyber Investigation Support Section

DFS

Digital Forensics Section

HTC

High-tech Crime Section

ICAC

Internet Crime Against Children Section

OPO

Online Police Section

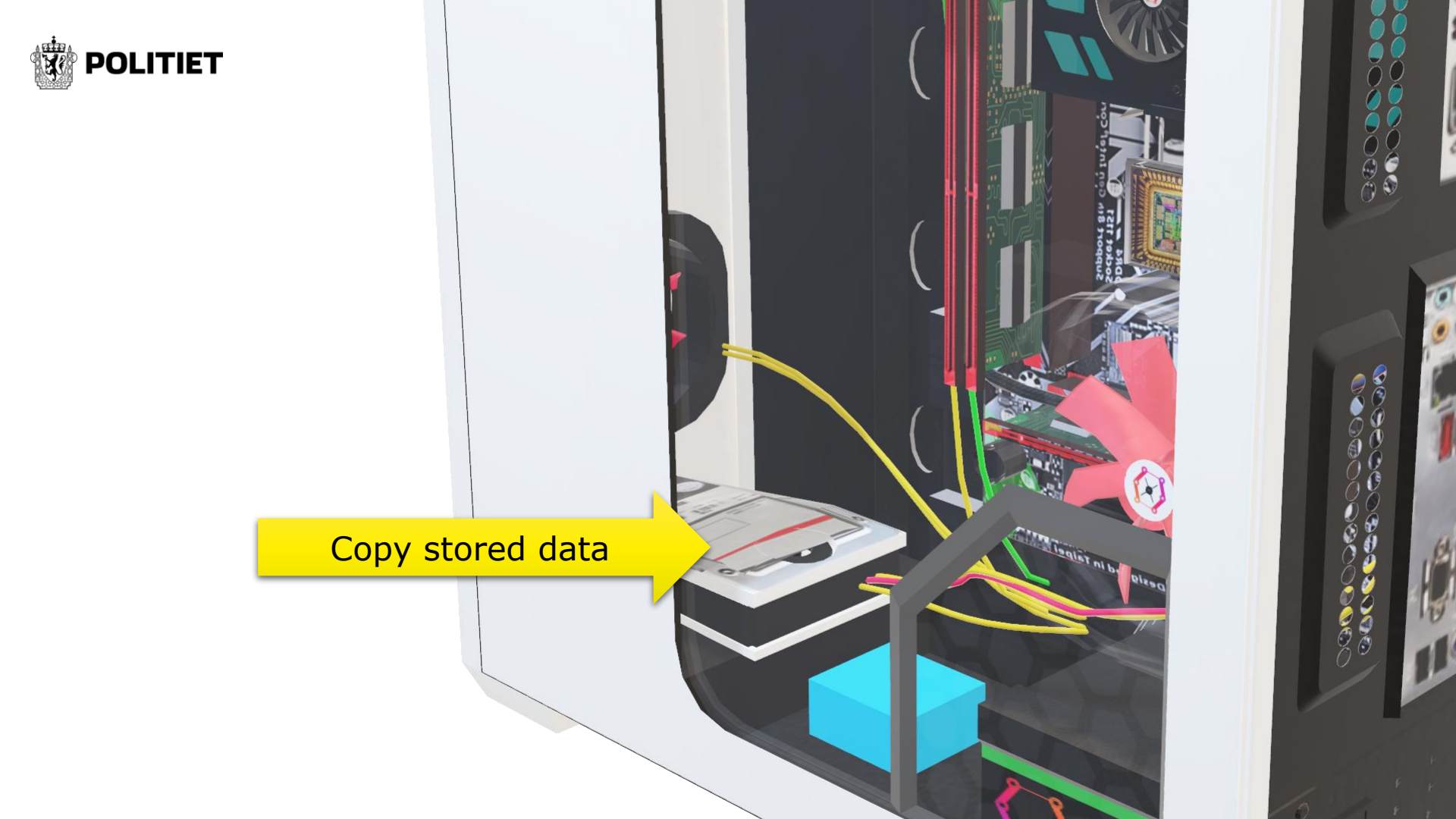
POLITIET

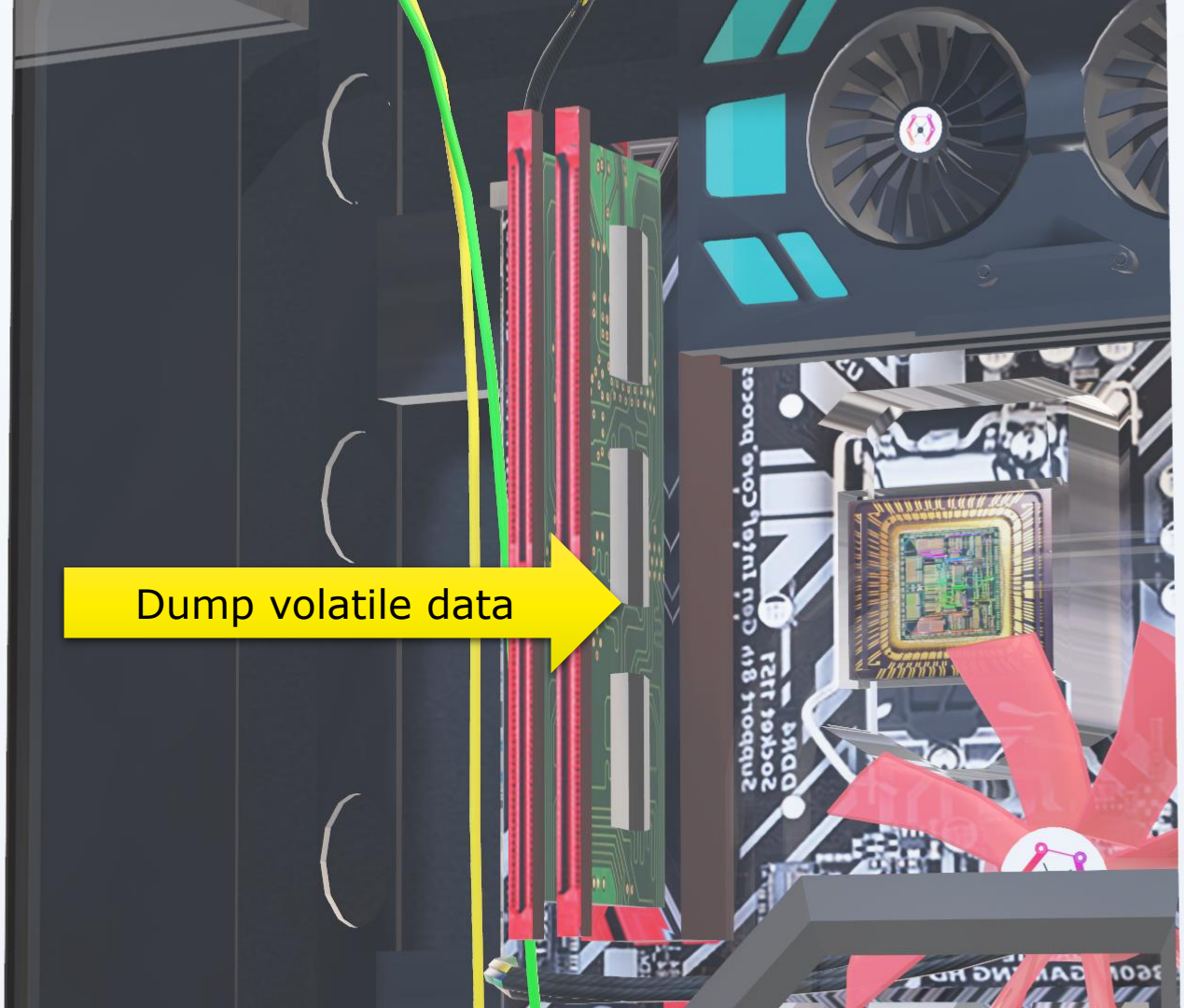
Digital Forensics

- Order of Volatility
- Chain-of-custody
- Traceability
- Integrity
- Reproduceable
- Forensicially Soundness
- ...

(Trial court is our exam)

POLITIET

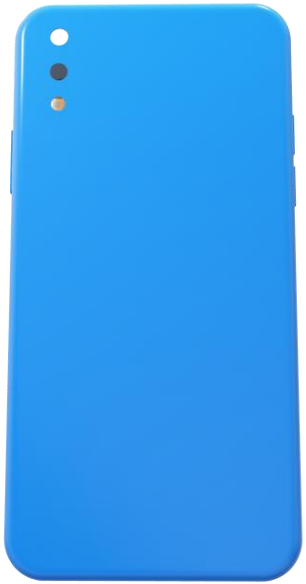



Dump volatile data

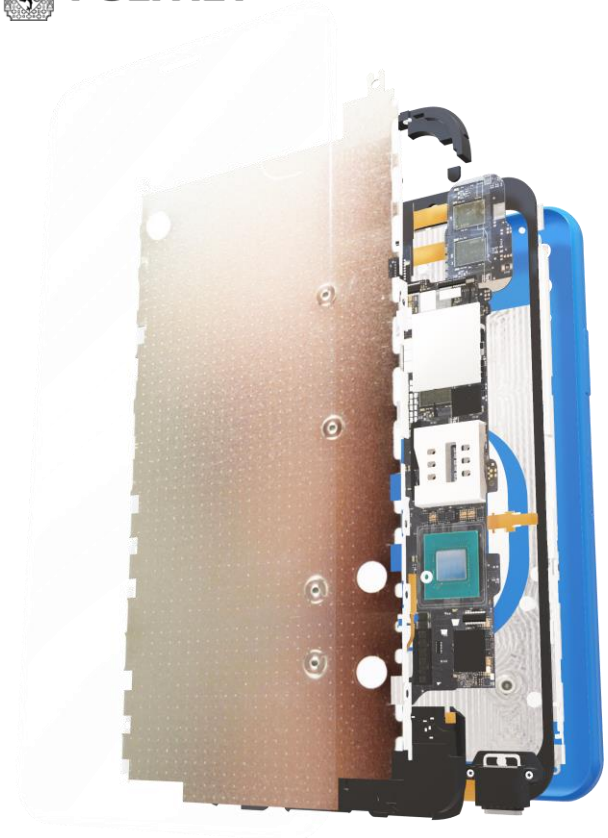
POLITIET

Mobile Phone Acquisition

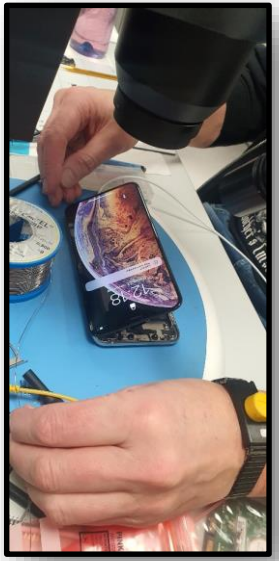
- Level 1: Manual Extraction
- Level 2: Logical Extraction
- Level 3: Hex Dumping / JTAG
- Level 4: Chip-off
- Level 5: Micro Read
- Level 6: …

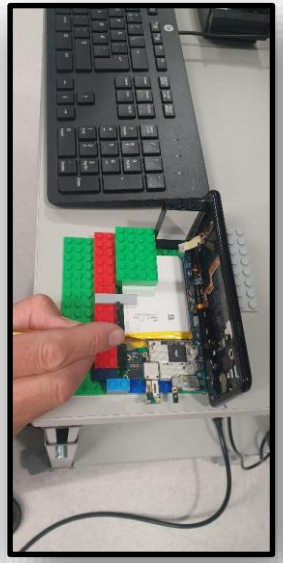


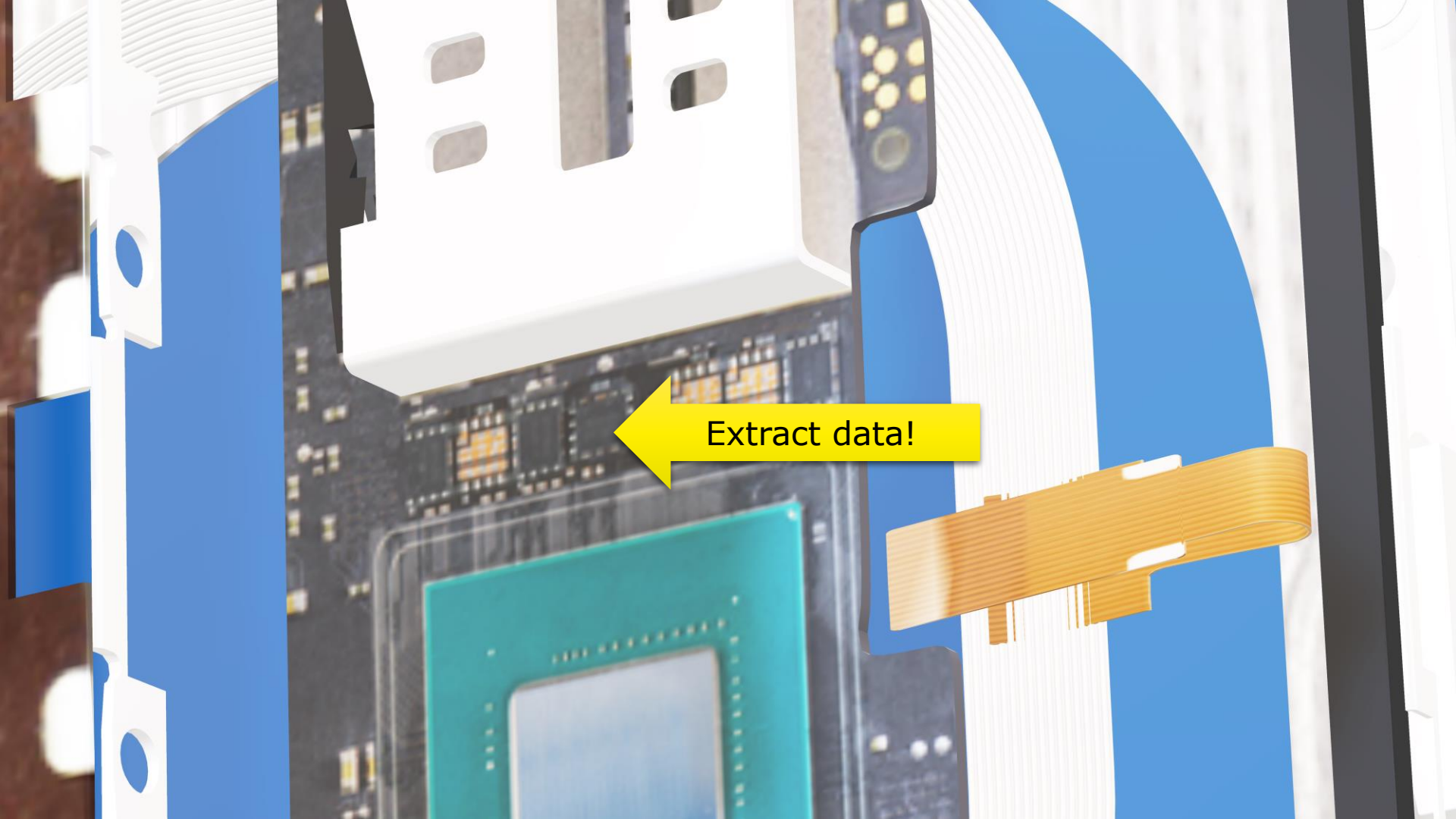
POLITIET



Creative ways to access the inside components!

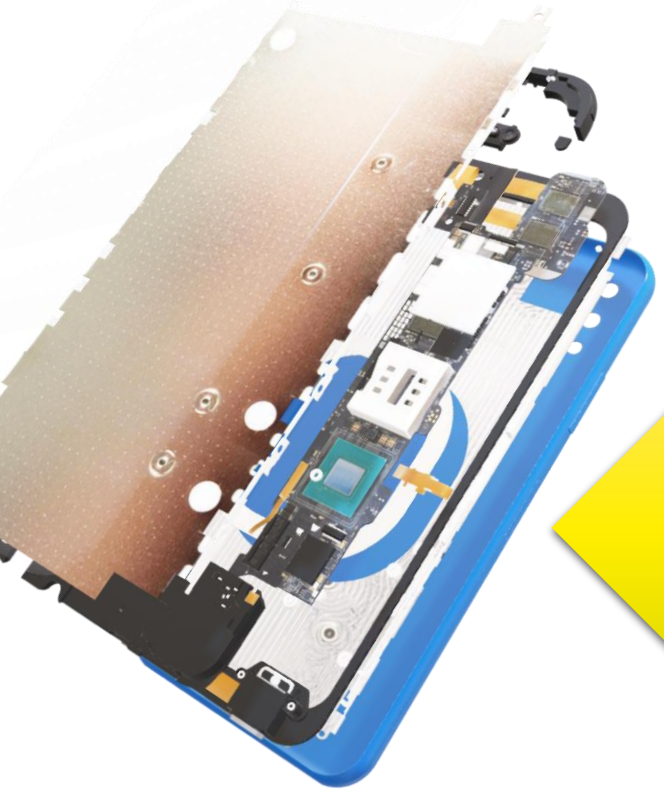


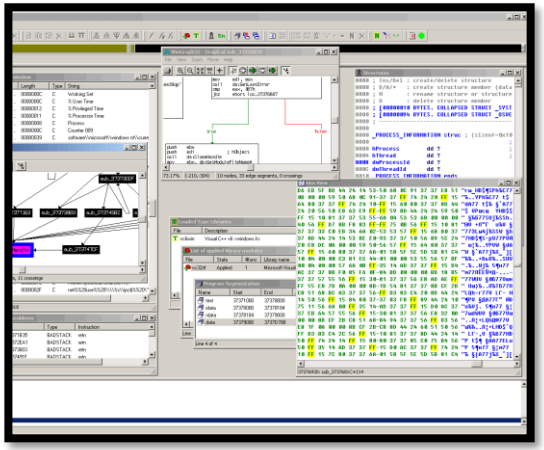


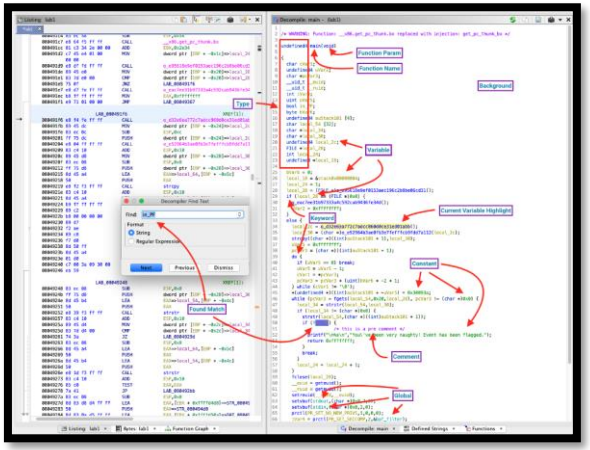

Extract data!


Extract data!

POLITIET







Reverse and analyze the code!

(Jump over the fence or find the way through the hole!)

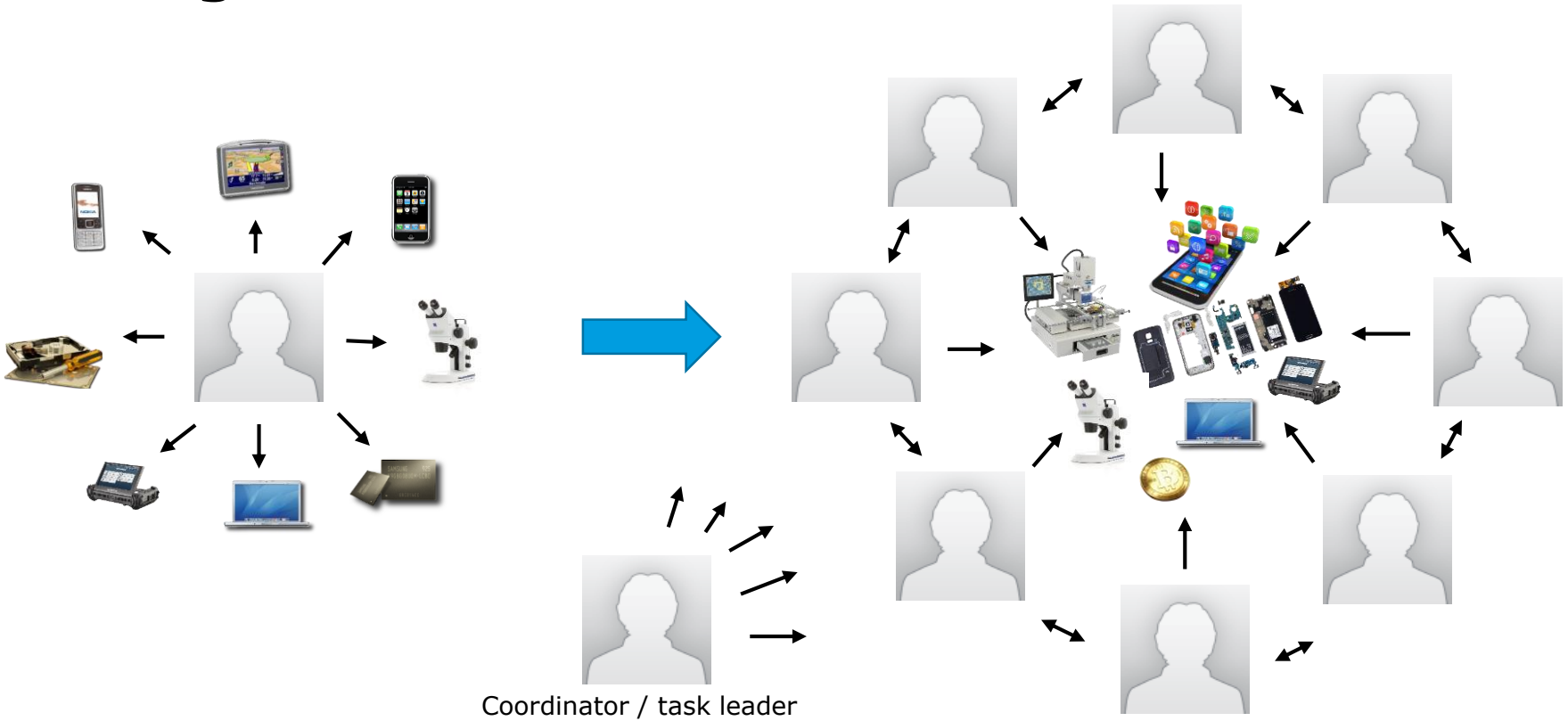
POLITIET

Computer Forensics

- Live Forensics vs Incident Response
- A lot of available tools
- Combine with other police methods for evidence collection and data seizure
- Work together with targeted business, ICT, …

POLITIET

Change of how we work



Coordinator / task leader

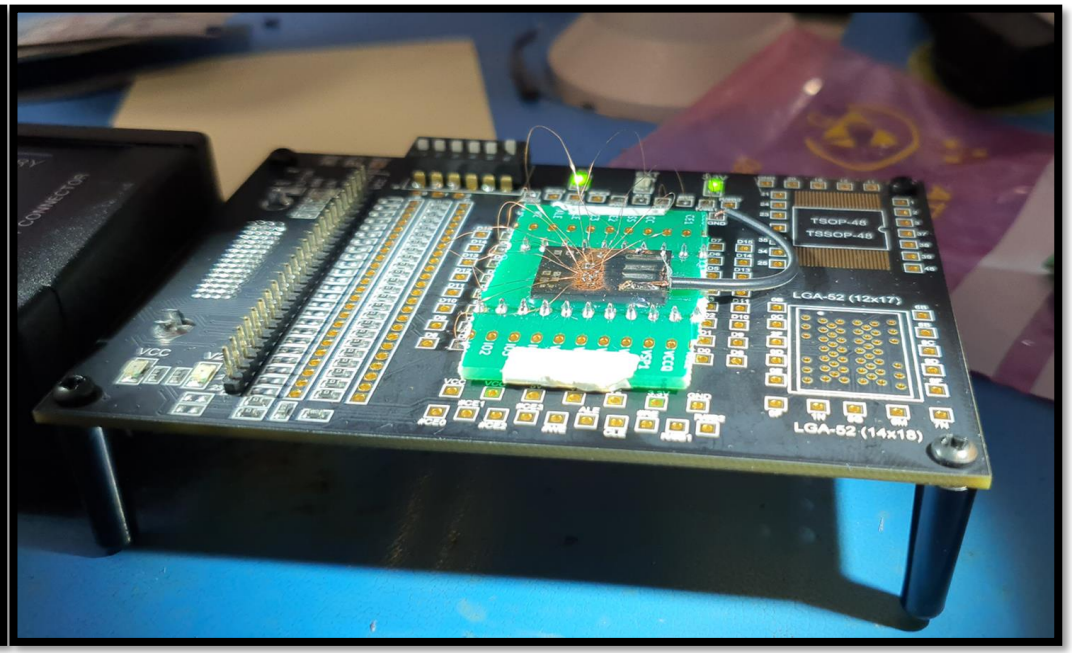
POLITIET

Ok, fancy animations ☺, but how does it look for real?

POLITIET

Data Recovery and Extraction

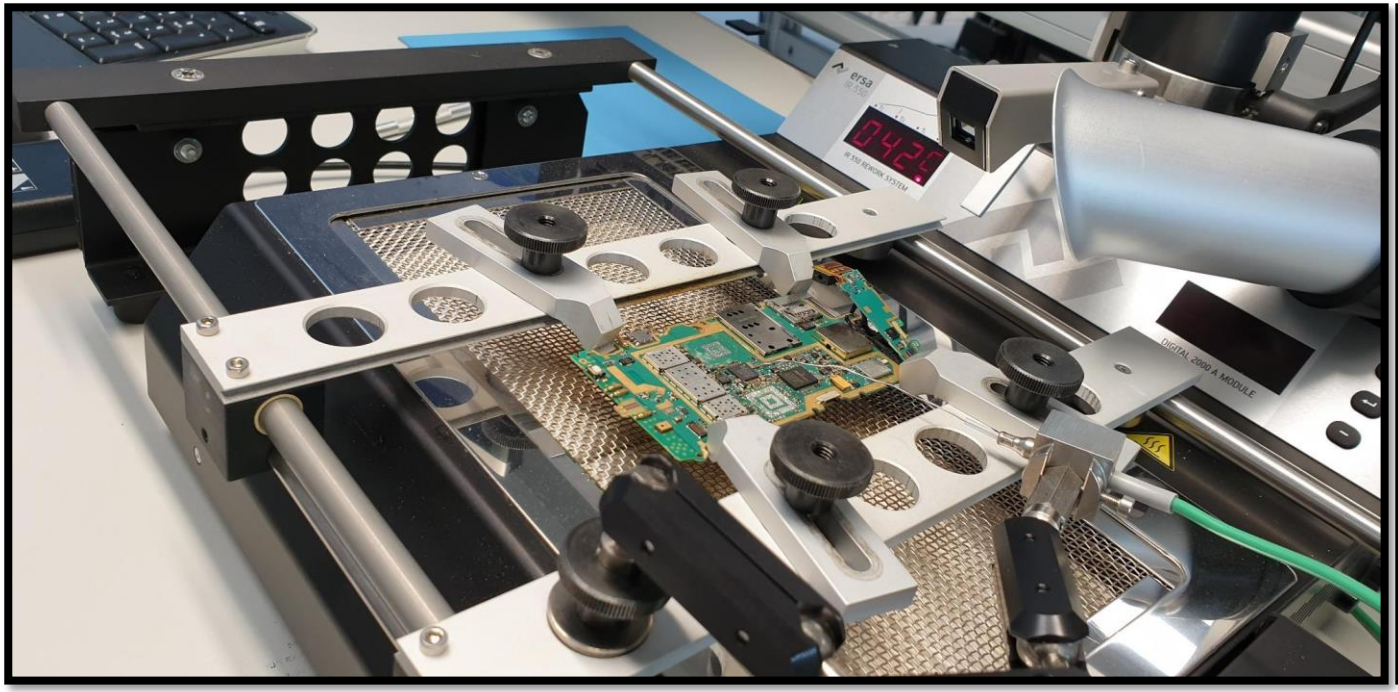
(storage devices, pcbs, chips, …)

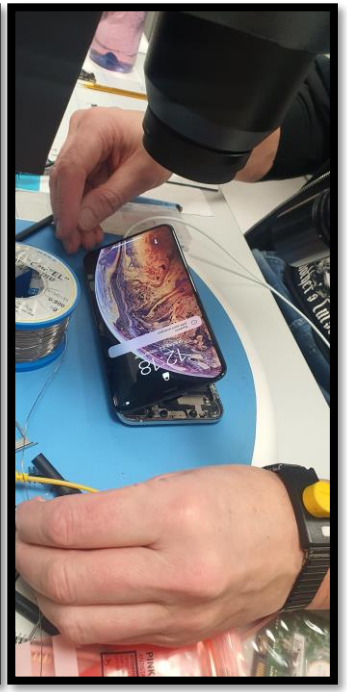


POLITIET

Data Recovery and Extraction

(storage devices, pcbs, chips, …)

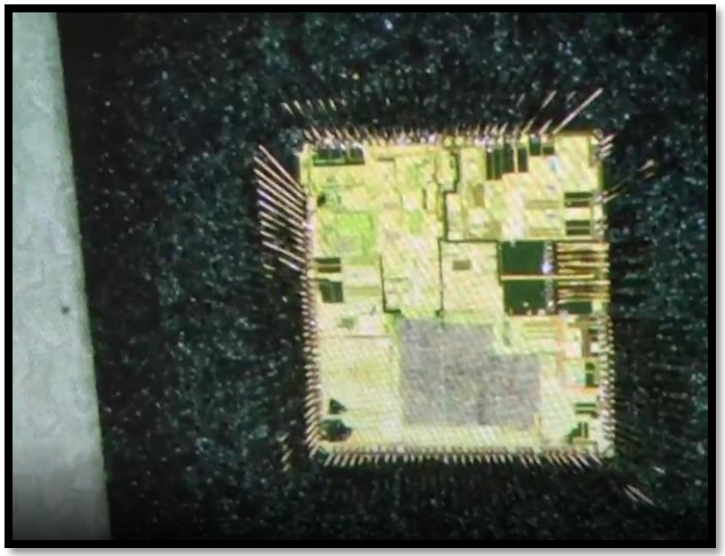


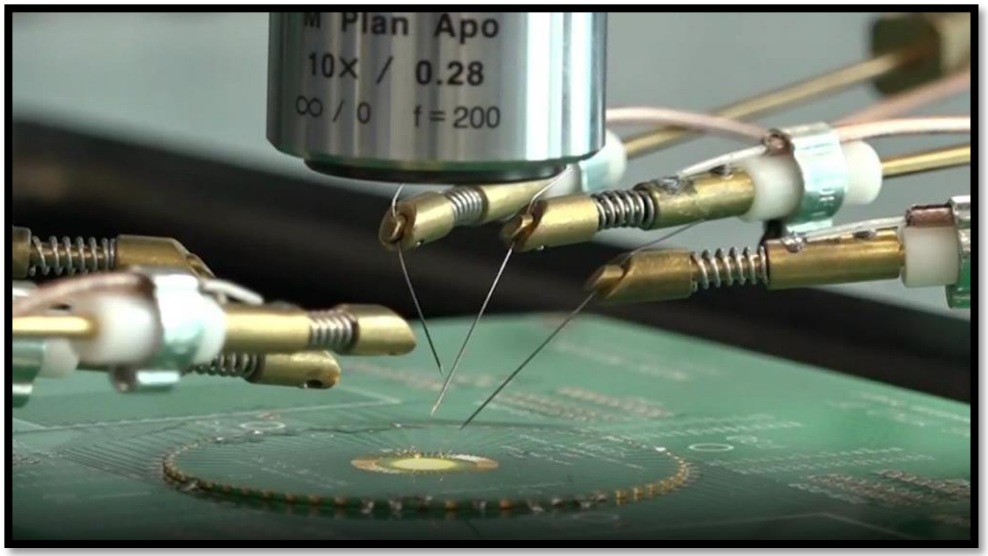


POLITIET

Data Recovery and Extraction

(storage devices, pcbs, chips, …)

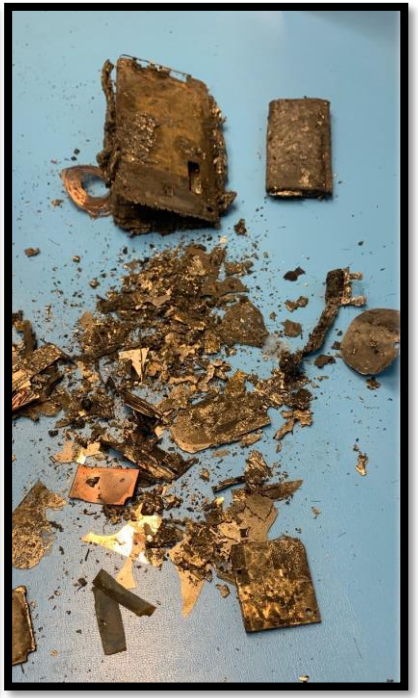




POLITIET

Data Recovery from non-functional hardware

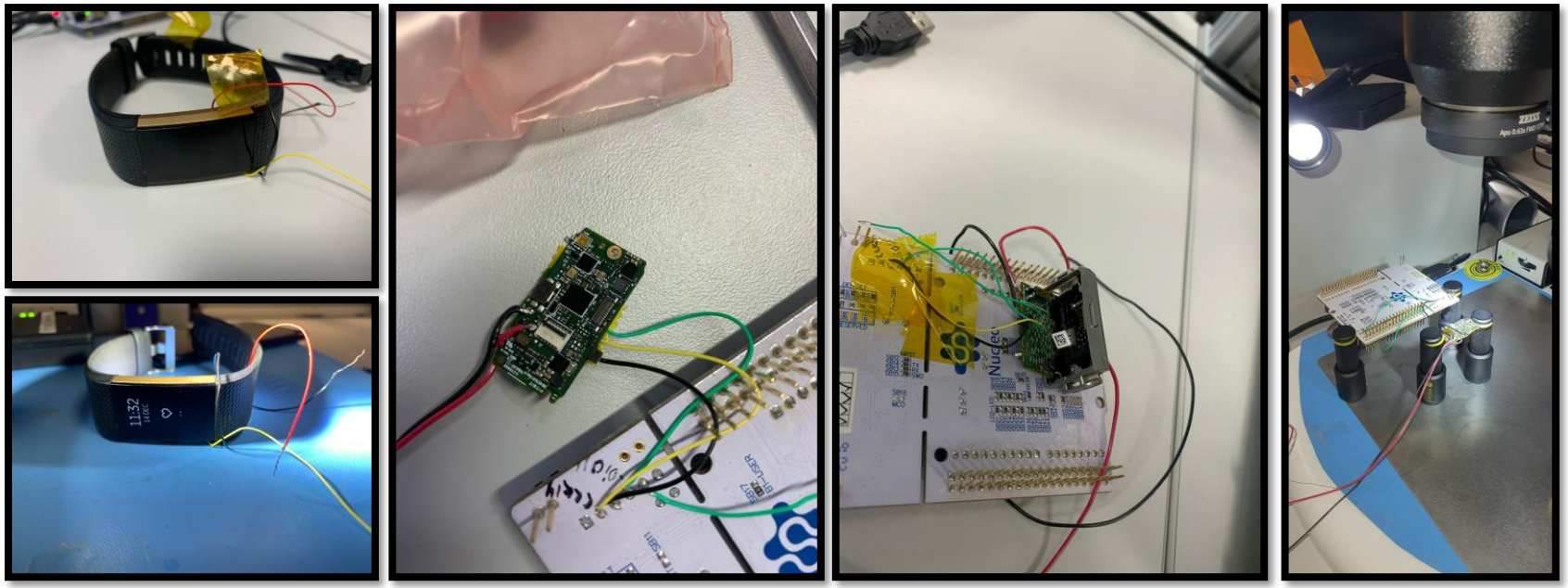
(Cause of damages: fire, water, fluids, collisions, …)



POLITIET

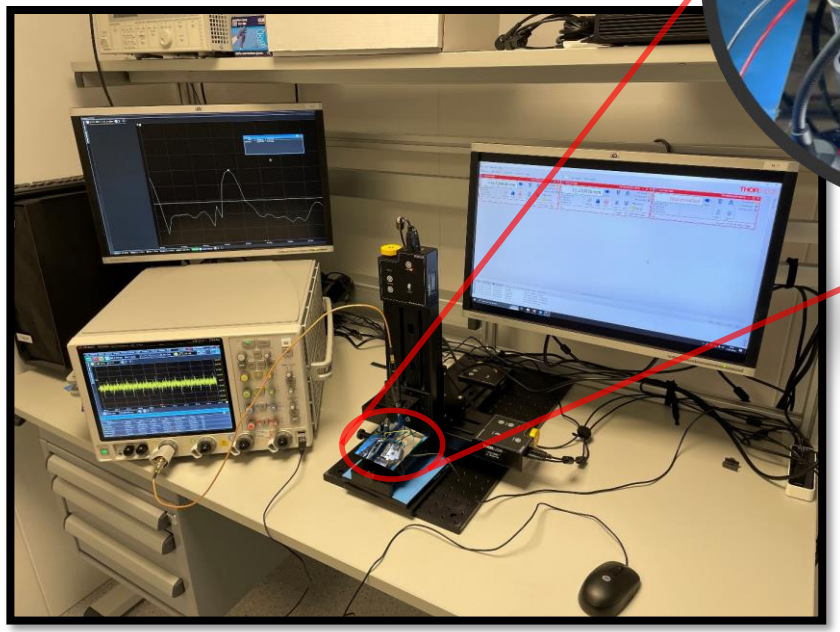
Reverse Engineering for Digital Forensics Purposes

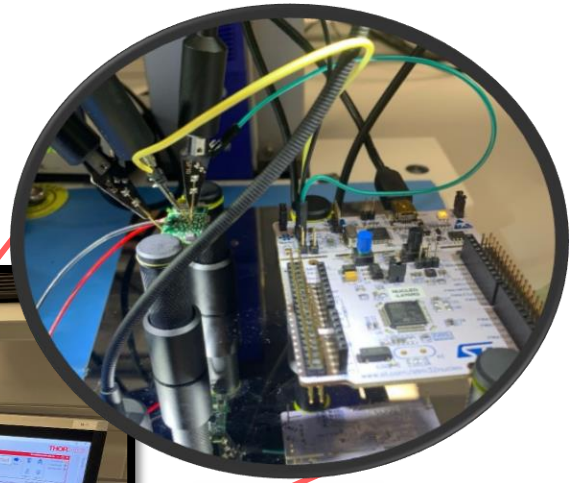
(health data, geomap coords, bt, profiling, …)



POLITIET

Ex: Lab Setup for SCA, …





POLITIET

Attack vectors; three ways to access data

Through **internet**

Through **software**

Through **hardware**

POLITIET

It is all about finding vulnerabilities in technology…

POLITIET

…and develop new methods/ways to defeat **security and protection mechanisms**, in order to do data aquistition and follow the traces online…

POLITIET

R&D, Innovation, Collaboration and partnerships

POLITIET

European Commission

European R&D programmes for funding

- **Horizon Europe** (was Horizon 2020) is the EU's key funding programme for research and innovation.
- Period: 2021 – 2027
- Budget: EUR 95.5 billion

- **Internal Security Fund** (was EU-ISF-Police) will contribute to reach high level of security in EU, in particular by preventing and combating terrorism, radicalisation, serious and organised crime and cybercrime […]
- Period: 2021 - 2027
- Budget: EUR 1.93 billion

POLITIET

EXFILES

EXtract **F**orensic **I**nformation for **L**EAs from **E**ncrypted **S**martphones

- Financed by Horizon 2020. Project budget of EUR 7 million over 3 years
- Aim: Develop new forensic models and methods for accessing data by bypassing security features in modern mobile phones; Non-invasive, semi-invasive and full invasive attacks. (Side channel attacks (SCA), fault injection techniques, secure boot bypassing, blackbox functions, …)
- 3 private companies, 5 academics and 5 LE agencies
- Website: https://exfiles.eu (with downloadable results)
- Status: Completed in oktober 2023!

POLITIET

OVERCLOCK

Operational **V**anguard: using **E**ncryption **R**esearch for **C**riminal **LOCK**down

- Financed by EU Internal Security Fund – Police (EU-ISFP)
- Project budget of EUR 4 million over 3 years
- Aim: Combat encrypted communication platforms used in organized crime and give police investigators access to decrypted data
- 4 LE agencies
- Status: Completes in September 2024

Bundeskriminalamt

Netherlands Forensic Institute
Ministry of Justice and Security

POLITIET
KRIPOS

POLITIET

ForRES

Forensic **R**everse **E**ngineering of **S**ilicon chips

- Financed by EU Internal Security Fund – Police (EU-ISFP)
- Project budget of EUR 4 million over 2 years
- Aim: Perform fully invasive operations on leading-edge semiconductor devices develop necessary tools and methods to attack the hardware chain of trust and advance the capability of extracting user data from highly integrated devices.
- 3 LE agencies and 1 research institute (CSIC)
- Website: https://forres.eu
- Status: Just started this week ;-)

Bundeskriminalamt

Netherlands Forensic Institute
Ministry of Justice and Security

CSIC

POLITIET
KRIPOS

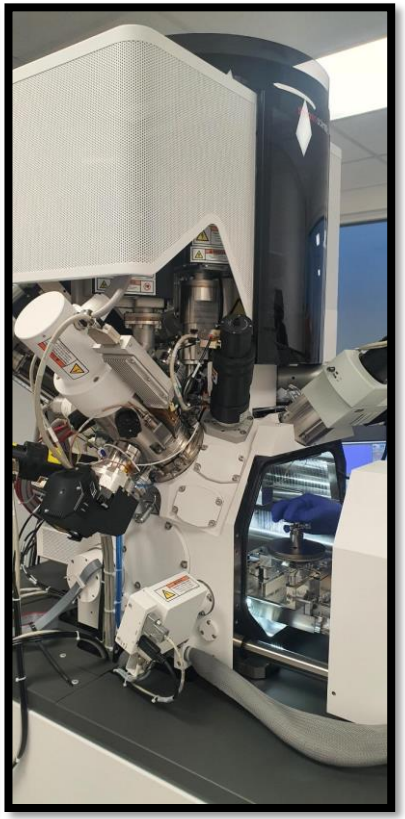
POLITIET

Nanotech Lab

Capability for nanotechnology research to support digital forensics and R&D

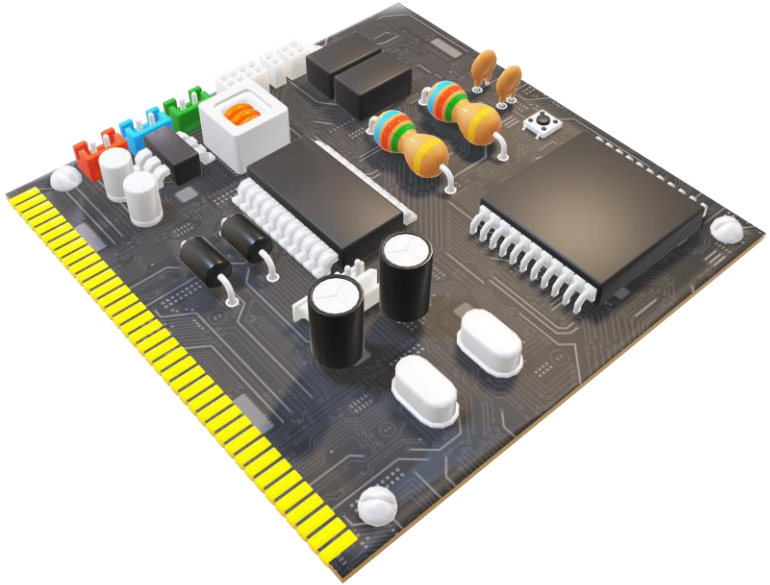
- Inspection and manipulation directly on the silicium in electronic components:
- Equipment: lapping machines, ultracollimator, plasma chamber, Scanning Electron Microscope/Focused Ion Beam (SEM/FIB), 3D CT-scanner, micro mill, and so forth…
- Challenging, but neccessary!

POLITIET

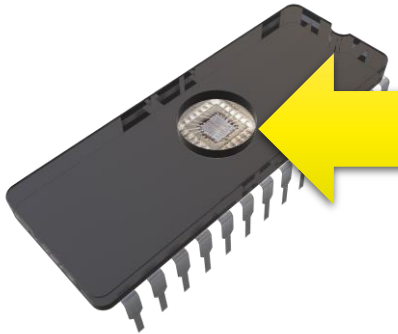


POLITIET

Example

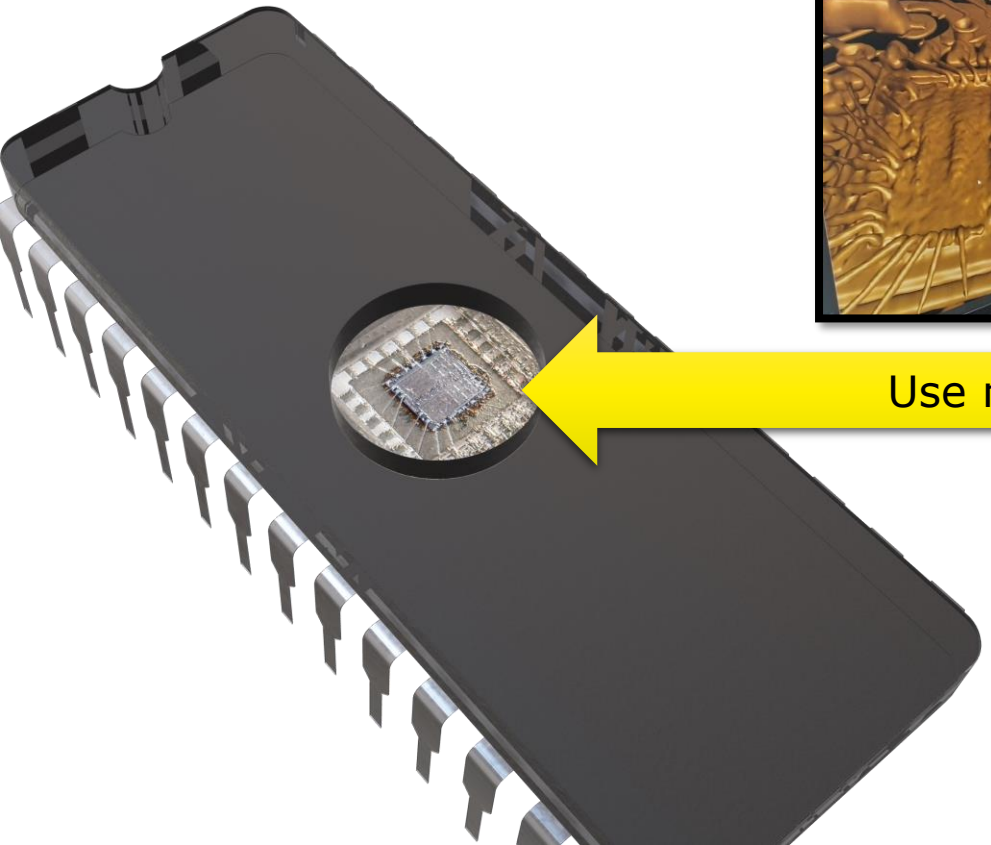


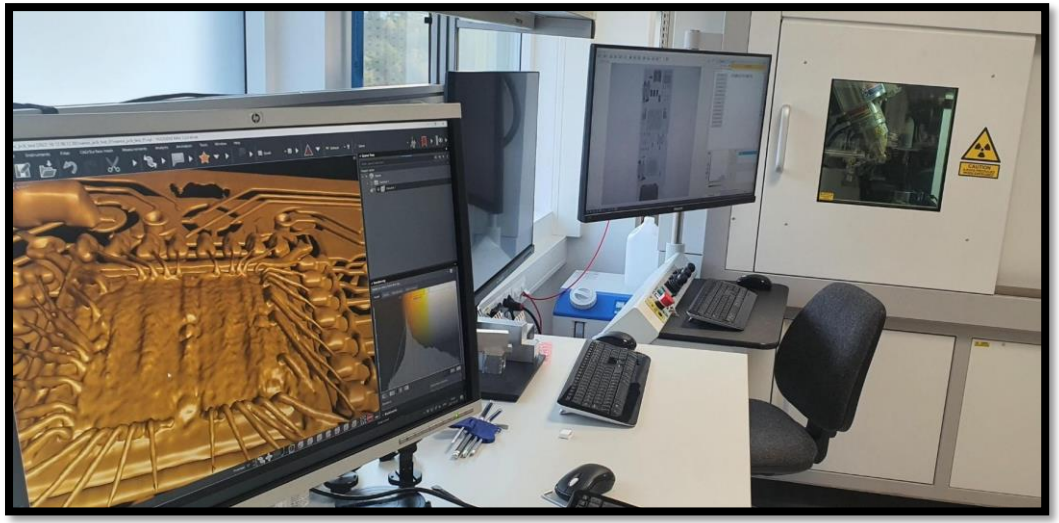
POLITIET



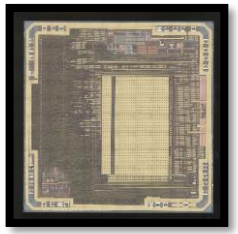
Use micromill to remove material

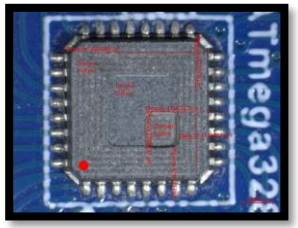
POLITIET

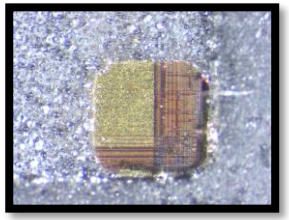




Use nano tools to investigate!



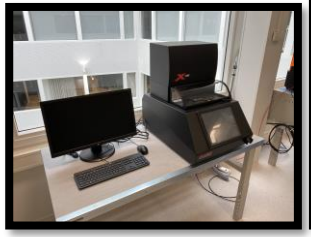




POLITIET

Other instruments used in the projects and lab

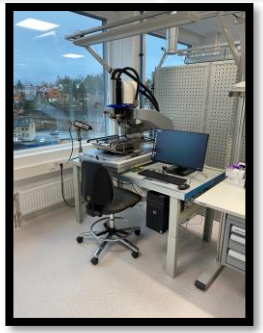
Micro mill



Faraday room

SEM/FIB

3D CT scanner



soldering

CNC router

POLITIET

Ransomware Case Examples

POLITIET

TICAT

Triage, Incident Coordination and Tasking Section

CIS

Cyber Investigation Support Section

DFS

Digital Forensics Section

HTC

High-tech Crime Section

ICAC

Internet Crime Against Children Section

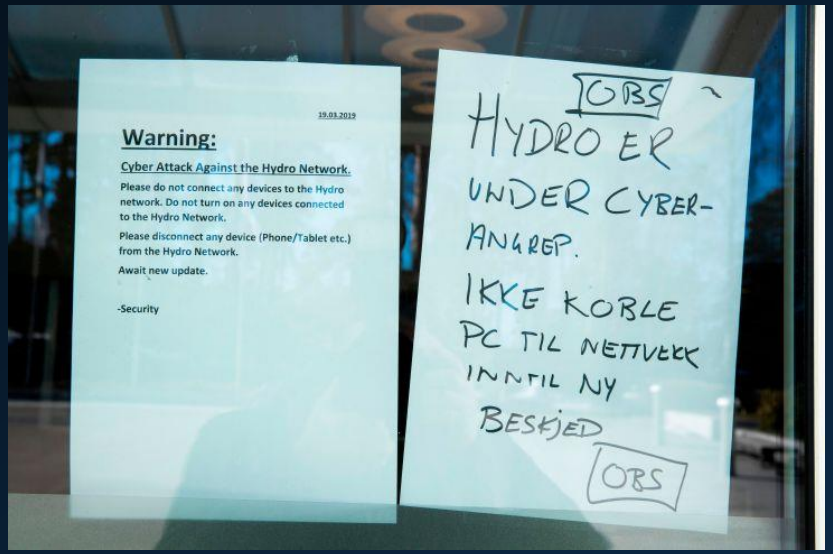
OPO

Online Police Section

POLITIET

The Cyber Attack on Norsk Hydro ASA

- 18th of March 2019 at 23:00 ransomware LockerGoga was detected
- The attack affected the production worldwide
- Almost all factories and production lines had to be isolated and put on manual control.
- The Police was notified 19th of March, received information and started data acquisition, …



POLITIET

International Cooperation

- The police must know about the cases - they must be reported!
- The Hague (Europol and Eurojust)
- Identify perpetrators, initiate criminal prosecution and prevent neew attacks.
- NCIS (NC3) has organized and coordinated the cooperation.

POLITIET

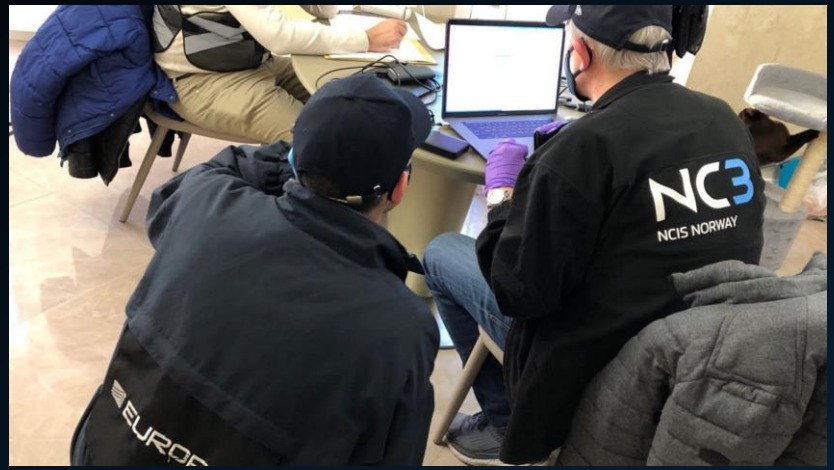
Technical and tactical Investigation

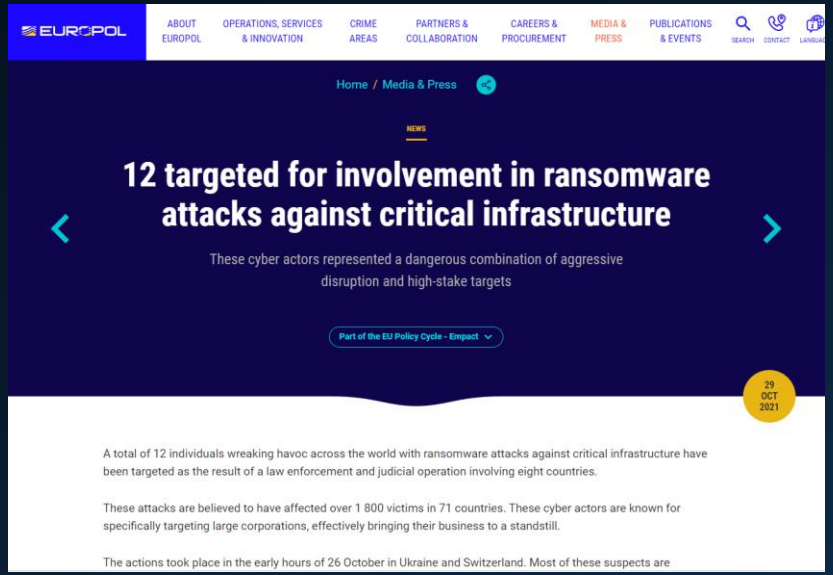
Our main focus:

- Collect information
- Follow the leads from the C2 servers (Command & Control)
- The money trails
- Prevent new attacks
- Identify perpetrators
- Ukraine – a hot spot!

POLITIET

International Operation




EUROPOL

ABOUT EUROPOL | OPERATIONS, SERVICES & INNOVATION | CRIME AREAS | PARTNERS & COLLABORATION | CAREERS & PROCUREMENT | MEDIA & PRESS | PUBLICATIONS & EVENTS | SEARCH | CONTACT | LANGUAGE

Home / Media & Press

NEWS

12 targeted for involvement in ransomware attacks against critical infrastructure

These cyber actors represented a dangerous combination of aggressive disruption and high-stake targets

Part of the EU Policy Cycle - Empact

29 OCT 2021

A total of 12 individuals wreaking havoc across the world with ransomware attacks against critical infrastructure have been targeted as the result of a law enforcement and judicial operation involving eight countries.

These attacks are believed to have affected over 1 800 victims in 71 countries. These cyber actors are known for specifically targeting large corporations, effectively bringing their business to a standstill.

The actions took place in the early hours of 26 October in Ukraine and Switzerland. Most of these suspects are

POLITIET

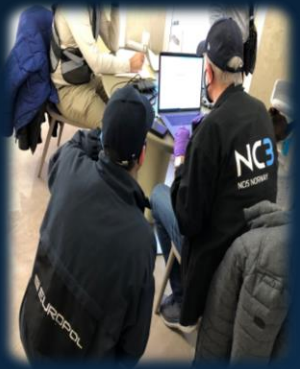
Decrypting the Data

- During investigation we found the keys for LockerGoga and MegaCortex
- Decryption key to Hydro's data derived from decryption software at seized computer
- Put together script handed over to Hydro so they could decrypt their data
- Later, on 16th sept 2022, keys and software were published on https://www.nomoreransom.org/

POLITIET

Experiences from the investigation

- Investigating cyber crime is time consuming
- Good collaboration with targeted company is importar
- International cooperation is required
- Combating cyber crime actually works:
  - We know how it happened
  - We know how dit it
  - We have individuals in custody and still seeking
  - We found the decryption keys



POLITIET

Other International Investigations

- **Hive ransomware as a Service**
- NC3 assists local police with investigations of companies and public services hit by Hive ransomware
- NC3 is helping with analyzing seisured infrastructure and data after takedown

POLITIET

Thirteen Lessons from Cyber Crime Fighting

POLITIET

#1 Balance innovation and production

Rapid development of new techniques is impossible if the same group of people have to manage these techniques.

The ability to simultaneously explore and exploit, enables us to adapt over time. Finding the balance is difficult, but necessary to stay relevant and in business! It is a two-sided dilemma with limited amount of resources:

1) Case production using known techniques
2) Innovatively find new techniques for tomorrow's case production

POLITIET

#2 You're only as relevant as your latest discovery

New techniques are like fresh produce; at some point they will go bad and become irrelevant. Sharing new information is the key to obtaining new information.

You have to bring something to the table, to get something from the table.
Important to have ability to prioritize long-term resource allocation to R&D for new discoveries.

POLITIET

#3 It's good to have friends

When everyone is working to solve the same challenges, a joint, international effort is the only sensible solution.

Fighting cyber crime often means fighting a high tech, organized, criminal activity across borders with unequal legislation, resources and regulation. Effective cyber crime fighting requires collaborative role clarification to balance incident response handling versus investigation, speedy information sharing, utilize each others country legislation, mutual cross-border overview synchronization of each others investigative activity.

POLITIET

#4 Big data is here to stay

The amount of data to be acquired, filtered, analysed and transferred will only increase.

More complex data analysis required. Law Enforcement needs data scientists!
Existence of the Big Data challenge confirms/hints a paradigm shift for Law Enforcement.
Big data boosts life to *Smart Policing* strategies and a data-driven approach for fighting crime becomes the future.

POLITIET

#5 The technological evolution will determine your focus areas

In order to stay ahead in the game of cyber crime, you have to continuously research and develop new methods, techniques and knowledge.

The number of data carriers, data volume size, database origins is rapidly increasing. Distributed storage, encrypted storage, in cloud storage.
Internet-of-things (IoT) are everywhere and give unexpected networks of attack vectors as they are installed in local (home) networks, usually have poor security components and often are available online or are connected to external servers.
As electronical chips and components and constantly miniaturized, data extraction instruments in digital forensics laboratories need to be upgraded to keep up the race!
The technological evolution pushes competence specialization, and cyber crime fighting becomes multi-disciplinary task as investigation and incident response handling must be perfectly balanced!
To stay ahead, it will cost you!

POLITIET

#6 Encryption is (mostly) bad for law enforcement

Encryption makes data harder to obtain, however once decrypted, the data may prove extremely valuable.

Criminals talk openly on encrypted platforms and consider them safe.
For Law Enforcement, it's expensive to defeat security mechanisms and do data extraction on proprietary platforms
Lawful Interception is less useful as end-to-end encryption is common.
Computer surveillance ("interception at source") is quite advanced, expensive and challenging in many ways due to its' operational and tactical nature along with the tech component.
Traditional data acquisition is no longer a trivial pursuit.
The use of undercover / covert operations increases and become more relevant in serious cyber crime fighting.

POLITIET

#7 Zero-days are hard currency

Finding an exploit and weaponizing an exploit will provide you with an extremely useful and attractive solution.

Commercial tools are not always up-to-date, and many are expensive.
Hunting zero-days, pushes crime fighting into a multi disciplinary merging game mixing information security, digital investigation, reverse engineering and exploitation, and so on, …

POLITIET

#8 The best defence is a good offence

Researching and reverse engineering a system to find vulnerabilities could prove to be time and money well spent.

Disruptive actions to become a valid police strategy. Too many criminals to fit in jail.

POLITIET

#9 Burn bridges in the right order

There is usually more than one way to solve a problem. Make sure you don't close the door on one approach before considering potential consequences.

Stay true to long term goals, don't be too short sighted.
Save takedown for the big(gest) fish.
Know the order of volatility.

POLITIET

#10 Don't ignore outreach and prevention

Sometimes a non-technical solution is the best solution in a cost/benefit perspective.

Outreach and prevention activity. Too many criminals to jail!
Partnerships with other sectors, private companies and academia.
Collaboration with regulators and legislators internationally.

POLITIET

#11 Invest in bright minds

Provide a work environment where creativity can prosper.

Advanced digital forensics and digital investigations require skills which are few in supply and high in demand.
Fighting complex cyber crime requires smart police officers.
The infosec pond is small and there are many parties fishing in it. If you cannot compete on salary, you can compete with the freedom to pursue ideas and less invoicing.

POLITIET

#12 Respect the value of your own data

Algorithms are fed with data in a data-driven world.

Respect, understand and protect!
Don't underestimate consequence of data compromise.

POLITIET

#13 Artificial Intelligence (AI) is (also) here to stay!

The reward is a function of regulation / legislation, understanding and actual application.

New possibilities for Law Enforcement
New possibilities for criminals
The Matrix is one step closer!

POLITIET

Cyber Crime Fighting

Keynote BSides 2023

THANKS FOR LISTENING