Final Conference Post-Event Report & Exploitation Overview

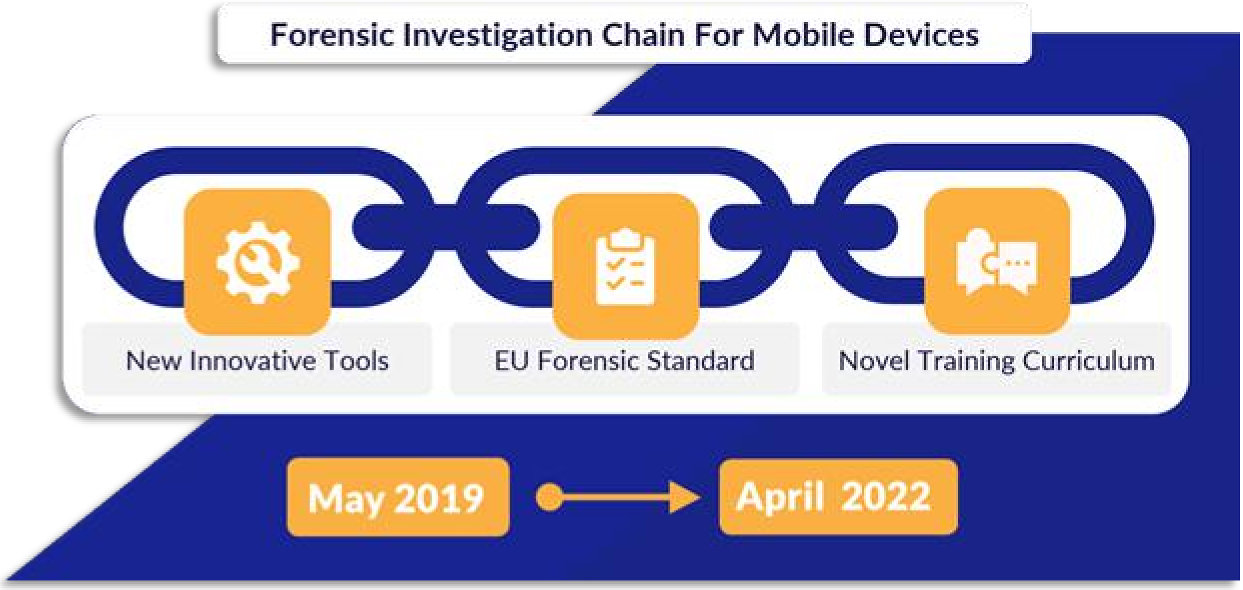
27 - 29 April 2022

FORMOBILE

• FROM MOBILE PHONES TO COURT •

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

Table of Contents


Forensic Investigation Chain For Mobile Devices
New Innovative Tools
EU Forensic Standard
Novel Training Curriculum
May 2019
April 2022

Executive Summary

The FORMOBILE Final Conference was held from the 27th to the 29th of April 2022, in The Hague, Netherlands. This was a concluding event for the 3-year EU-funded project in which the key results and actions conducted by the 19 partners from 15 countries were presented, along with a celebration of the Consortium's achievements throughout the project's duration. Thanks to the commendable support of our host, the Netherlands Forensics Institute (NFI) and Consortium partners, the conference went according to plan.

Objectives

The objectives of the Final Conference were to:

- **Discuss the tasks related to closing the project**
- **Disseminate FORMOBILE's results**
- **Reach practitioners specialised in the mobile forensics domain**
- **Ensure the project outcomes will be exploited**
- **Celebrate closing the project**

Annex

To view the event participant guide, click **here**.

Visit FORMOBILE on github **here**.

Event Overview

The FORMOBILE Final Conference served as a platform to showcase the innovative tools intended for Law Enforcement Agencies that were developed within the project and activities carried out by each of the Work Packages (1-6). The event was organised in a hybrid fashion with 60 attendees joining in person (a maximum capacity of 80 registrants) and 36 online.

The conference commenced with opening and keynote speeches from the NFI Scientific Director, Annemieke de Vries, DG Home Policy Officer, Nada Milisavljevic, and the FORMOBILE Project Coordinator, Dirk Pawlaszczyk offering their congratulations to all project partners for the milestones achieved.

An overview of **before and after the FORMOBILE project** was shared by the Project Initiator, Christian Hummert, and the Project Coordinator giving an insight into the changes in the focus of digital forensics from computers to mobiles and presently further changing to embedded systems for example in cars.

Picture: BuabengFelix, Licence:CC-BY-SA4.0

Picture: Mbrickn, Licence: CC-BY-SA4.0

Picture: Damian B Oh, Licence: CC-BY-SA4.0

Some challenges that were highlighted related to mobile forensics include the use of mobile phones to communicate, coordinate, organise and execute illegal activities, mobile phones as a unique challenge for law enforcement agencies (LEAs) due to the volume and variants in circulation, and the need for LEAs to access, decode and use the data as evidence - in a safe, trustworthy and reliable manner, while the relevant fundamental rights are appropriately taken into account.

These challenges were the foundation for the FORMOBILE project that aimed to create an end-to-end mobile forensic investigation chain, to improve digital safety in the EU.

Before and After FORMOBILE

Challenges

Mobile phones are a unique challenge for law enforcement agencies (LEAs) due to the volume and variants in circulation. They are also analysed differently from other devices such as PCs and Laptops, meaning the investigation requires a separate forensic process.

Smart devices are widely used in society by most citizens. criminals are also using mobile phones to communicate, coordinate, organise and execute illegal activities.

LEAs have ways to; access, decode and use the data as evidence - in a safe, trustworthy and reliable manner, while the relevant fundamental rights are appropriately taken into account.

Smartphone-Related Facts

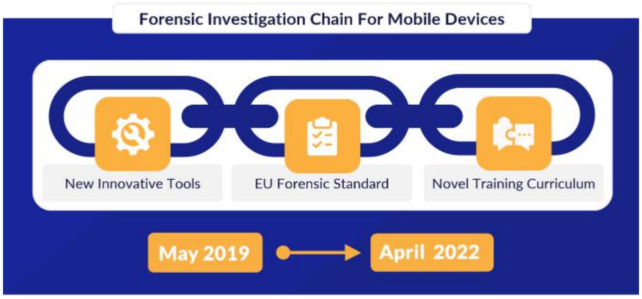
85% Crime Investigation includes Mobile Data

65% EU Citizens prefer Smartphones to access Internet (2017)

85% of all photos taken in the EU are made using Smartphones (2017)

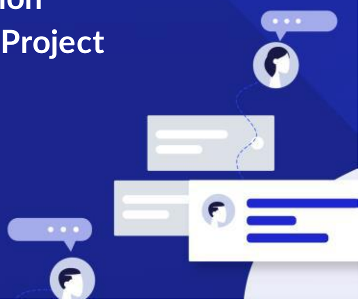
Solution - FORMOBILE

An EU project aiming to create an end-to-end mobile forensic investigation chain, taking evidence from the mobile phone and presenting it in court.


Forensic Investigation Chain For Mobile Devices
New Innovative Tools
EU Forensic Standard
Novel Training Curriculum
May 2019
April 2022

FORMOBILE Highlights

1. 19 Partners
2. 15 Countries
3. €7 Million
4. 3 Year Project



Project Benefits & Results

FORMOBILE explored the use of mobile phones as a means of communication between criminals and terrorists, which would ultimately benefit the project's target groups: **Security Practitioners**, **Research Groups** and **EU Citizens**.

Policy Benefit

FORMOBILE relates to EU strategies and policies, and holds potential to add value to them:

- Security Union Strategy
- European Agenda on Security
- EU Strategy to tackle organised crime

Scientific Benefit

FORMOBILE builds upon and relates to EU projects from previous calls namely I-LEAD, CASE and Evidence. It has established close connections to EU projects from the same call, namely ROXANNE, LOCARD and EXFILES - exchanging knowledge and experiences.

Economic & Competitive Benefit

FORMOBILE strengthens the digital sovereignty of the EU. Tools for mobile examination within the EU include two main players. Cellebrite – the Israeli provider and MSAB located in Sweden. Important results of the FORMOBILE project will be exploited by MSAB. This will strengthen the European mobile forensics market and make the main EU player more competitive.
FORMOBILE will contribute significantly to the qualification of young researchers within the EU by allowing them to finish a PhD–work within the project.

Technological Benefit

The expertise obtained in developing the eMMC and UFS emulator will facilitate the development of emulators of new chip technologies in the future.
This new technology will strengthen the abilities of the EU economy in the fields of hardware development especially for disruptive technologies like the IoT.

Political Benefit

Regarding capabilities to respond to major cyberattacks, FORMOBILE supports with the strengthened forensic acquisition and analysis tools, as well as with training for the LEAs.

- Development of the CWA explicitly supports LEA and judiciary cooperation.
- Most tools will be integrated into MSAB tool kit making results available for European LEAs.
- Results – easy-to-use tools, CWA, LEA training, legal and ethical transfer efforts – support LEA's and judiciary's transformation to the digital age.

Ring Trials Experience

Ralf Zimmermann from ZITiS shared a presentation of WP1's activities, which included the collection of LEA requirements that were foundational to the standards and testing methods, agreements and tools developed - providing a basis for the subsequent WPs. During the session, two ring trial participants shared their experiences on the effectiveness of the FORMOBILE results. The work package comprised 4 tasks and the feedback on how each contributed is shared below:

Task 1.1 Specification of end user requirements

T1.1 allowed us to collect the requirements of LEAs, which emphasised the importance of the FORMOBILE ambitions and served as the base for the subsequent WPs.

Task 1.2 Evaluation of current status in mobile forensics

T1.2 showed that the FORMOBILE goals are highly relevant in a practical environment aiming at closing some of the gaps in the current mobile forensic workflow.

Task 1.3 Developing methodologies to test the project results

T1.3 involved extensive communication and collaboration with LEAs and technical WPs, which led to the realistic scenario for 2nd ring trial helping to ensure that the results are useful in practice.

Task 1.4 Validation of the FORMOBILE results

T1.4 showed that the FORMOBILE results are highly relevant and practical. By taking into account LEA's technical requirements and by applying the methods developed in T1.3, the setup of the ring trial ensured a realistic test case that covered all aspects of the FORMOBILE project.

Ring Trial Participant Testimonials

"Close collaboration of all members involved in the ring trial is important to define the purpose of the ring trial from the outset." - Steve Collins,
Home Office (UK)

*"...Docendo discimus
By teaching, we learn..."* - Bruno Teixeira,
Portuguese Judicial Police

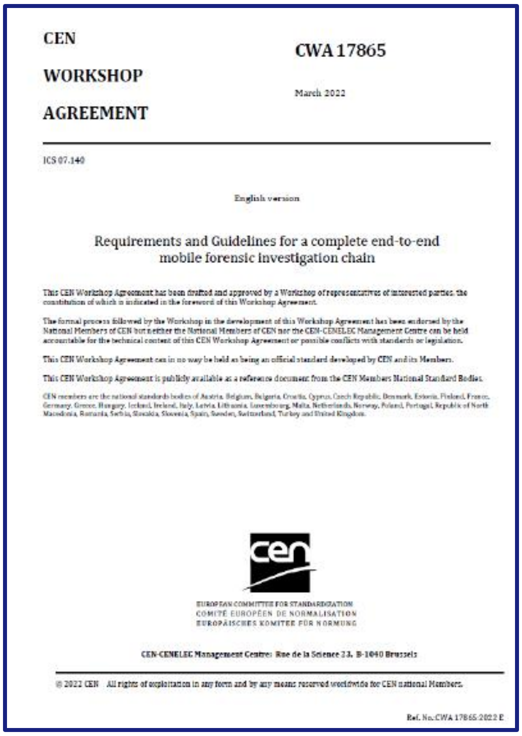
Standards

One of the main results of FORMOBILE, the new CEN Workshop Agreement (CWA) on mobile devices was presented in the session led by WP3 leader, Karl Grün, and CWA expert Christian Hummert.

CWA 17865:2022, Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain

This Standard comes highly-regarded as:

- It was designed to address the needs of LEAs and others involved in mobile forensics.
- It was developed by peers, e.g. LEAs, tool providers, research, NGOs, legal and ethical advisors, etc.
- It was validated to ensure it is fit for use.



CEN
WORKSHOP
AGREEMENT

CWA 17865

March 2022

ICS 07.140

English version

Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2022 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No.:CWA 17865:2022 E

The CWA focuses on the personnel, tools, processes and legal and ethical framework specific for mobile forensics. It was developed in an open, transparent, inclusive multi-stakeholder-process with 56 experts from 30 organisations.

Before publication, the CWA:

- Was subject to an open commenting phase.
- Was validated by FORMOBILE, e.g. is the text clear, understandable, requirements implementable, etc.
- Was assessed from a legal and ethical perspective.

Applying the CWA 17865 leads to

- **Enhanced confidence** in the evidence using digital forensic methods;
- **Robust, verified and validated results** of mobile forensics presented in court;
- **Improved quality** of the evaluation results obtained by means of mobile forensics;
- **Harmonised methods** of mobile forensics between institutions;
- **Better international cooperation** in fighting cross-border crime.

The CWA:

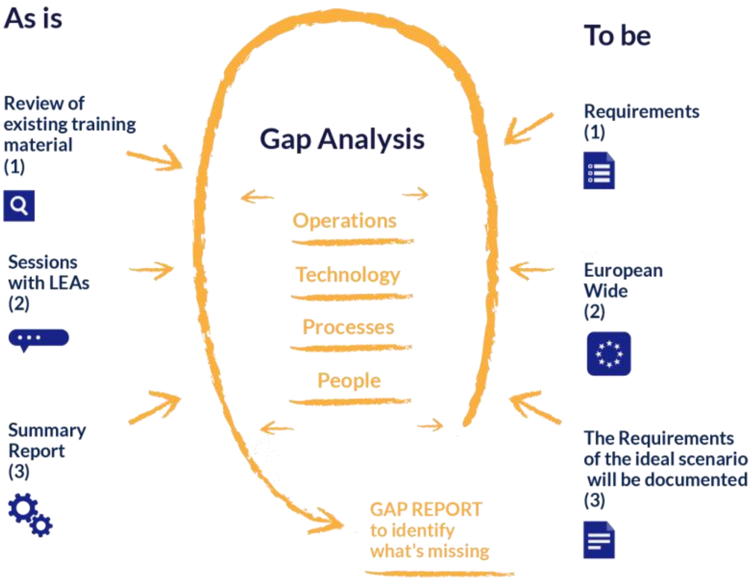
- **Refers to existing standards such as ISO/IEC 17025, ISO/IEC 27041ff,**
- **Supports the implementation of EU law, in particular**
  - Directive 2012/13/EU on the right to information in criminal proceedings,
  - Directive 2014/41/EU regarding the European Investigation Order in criminal matters,
  - Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings,
  - Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data,
  - Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
  - Convention on Cybercrime
- **Offers a collection of building blocks covering different aspects of mobile forensics allowing for adjustments based on national laws and regulations as well as internal rules and codes of conduct.**
- **Allows LEAs from different countries to accommodate their available technical solutions, at the same time offering a standardised collection of procedures and requirements.**

In addition, the CWA provides practical guidelines

- A Good Practice Guide for Mobile Forensic Tool Selection
- Mobile Forensic Tool – Checklist for Selection
- Mobile Forensic Tool – Risk Register
- Six Steps to Successful Mobile Validation
- Forensic Information Report Template
- Governance implications of the use of Artificial Intelligence in mobile forensics

Training

Measuring The Gap

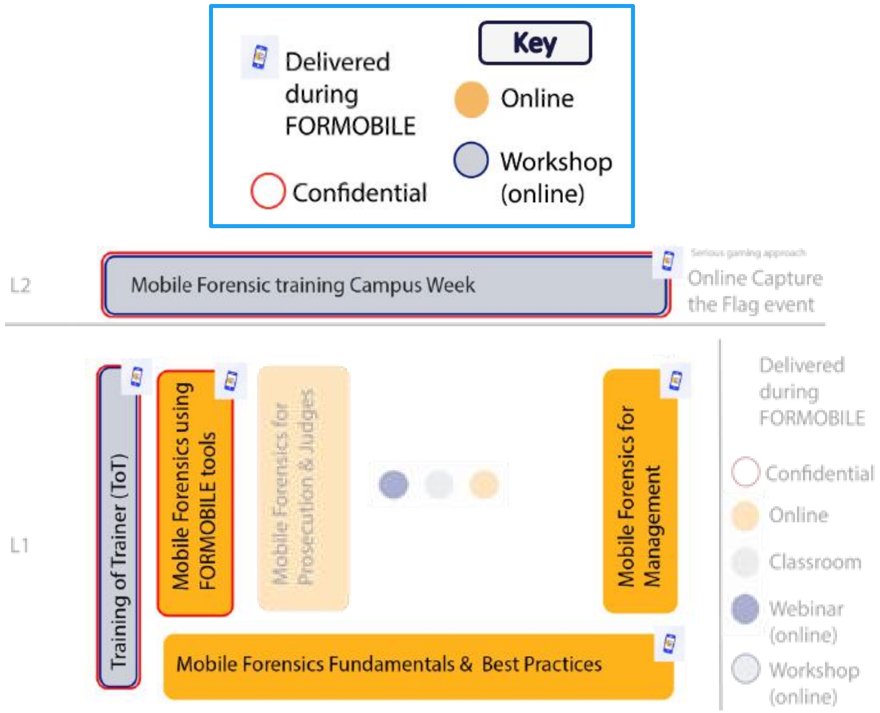

As is
Review of existing training material (1)
Sessions with LEAs (2)
Summary Report (3)
Gap Analysis
Operations
Technology
Processes
People
GAP REPORT to identify what's missing
To be
Requirements (1)
European Wide (2)
The Requirements of the ideal scenario will be documented (3)

Novel Training

To maximise the success of the FORMOBILE project, it is imperative that the LEAs and associated agencies receive the best training possible on the new tools and standard implemented.

A dedicated training team combined research and needs analysis to create a new curriculum concerning the key requirements in the mobile investigation chain.

What was delivered?


Key
Delivered during FORMOBILE
Online
Workshop (online)
Confidential
L2
Mobile Forensic training Campus Week
Serious gaming approach
Online Capture the Flag event
L1
Training of Trainer (ToT)
Mobile Forensics using FORMOBILE tools
Mobile Forensics for Prosecution & Judges
Mobile Forensics for Management
Mobile Forensics Fundamentals & Best Practices
Delivered during FORMOBILE
Confidential
Online
Classroom
Webinar (online)
Workshop (online)

4 Pilot of e-Learning Courses and Online Workshops

Pilot e-learning courses between December 2021 and February 2022 for applicants to the FORMOBILE training.

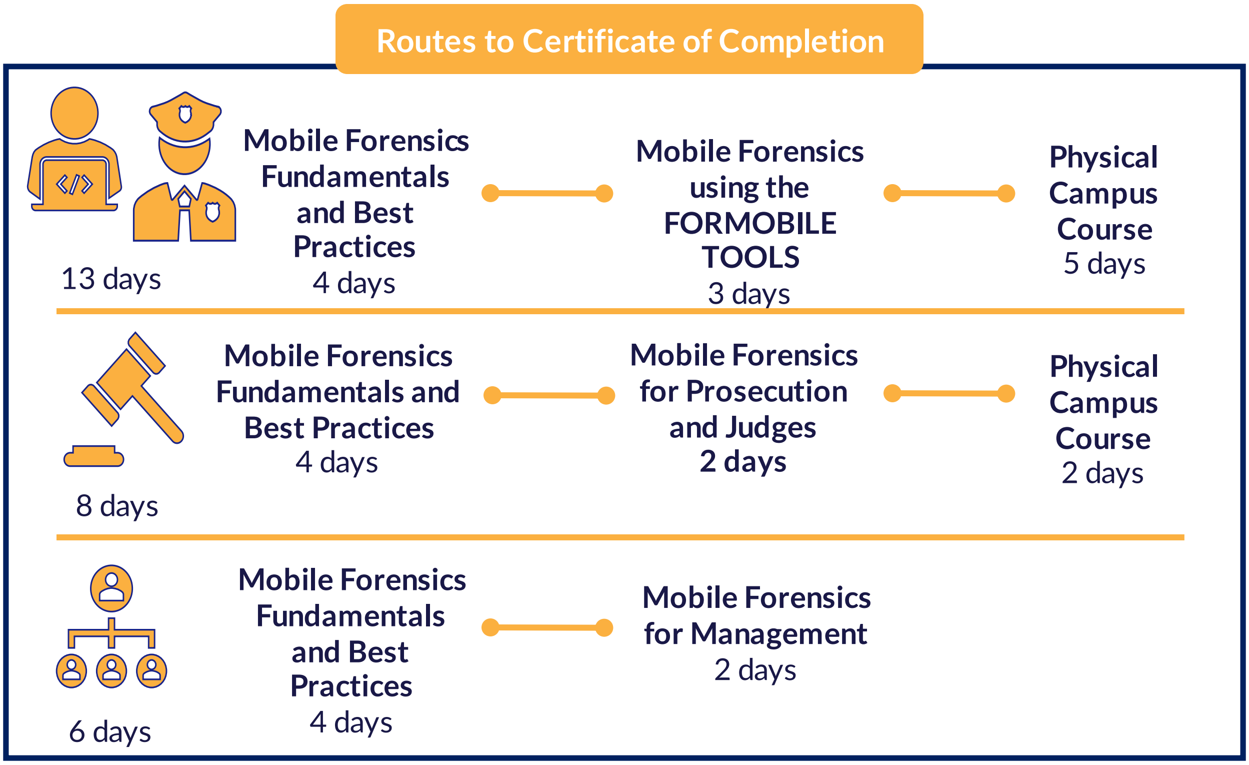
Pilot train the trainer model which includes M1TOT (Jan'22), trainer involvement in the CTF design, development and facilitation of a CTF event (Feb'22).

Pilot CTF event held in February 2022 with available participants.

Pre- and Post-learning evaluations for all e-learning pilot courses.

Feedback from participants for courses via email and/or evaluation forms.

During the **Training** session, Georgina Humphries, WP7 Leader, Harry Manifavas, FORTH, and Guiseppe Di Franscesco, ECTEG shared some highlights on the efforts that were carried out within the project to create a novel curriculum for LEA, develop training materials and establish a relationship that will continue to deliver training materials for LEAs following the project.



Routes to Certificate of Completion

13 days	**Mobile Forensics Fundamentals and Best Practices** 4 days	**Mobile Forensics using the FORMOBILE TOOLS** 3 days	**Physical Campus Course** 5 days
8 days	**Mobile Forensics Fundamentals and Best Practices** 4 days	**Mobile Forensics for Prosecution and Judges** **2 days**	**Physical Campus Course** 2 days
6 days	**Mobile Forensics Fundamentals and Best Practices** 4 days	**Mobile Forensics for Management** 2 days	

1 Fundamental and Best Practices of Mobile Forensics

2 Mobile Forensics for Management

3 Mobile Forensics for Judges and Prosecution

The **European Cybercrime Training and Education Group (ECTEG),** will build from the foundations of the work completed in FORMOBILE through their dedicated project – MobiFor. Please reach ECTEG to explore opportunities for accessing course materials and trainings.

Find out more - contact@ecteg.eu

Exploitation of the Training Materials

Synergy built with ECTEG

- MoU signed for the collaboration between FORMOBILE and ECTEG
- ECTEG to explore content in the FORMOBILE curriculum can be hosted for LEAs (adhering to Export controls etc.)
- ECTEG to consider content that can be further developed based on topics outlined in D7.1
- funding for LE to attend highly specialised labs after the end of the project at NFI via ECTEG funding
- ECTEG to **explore FORMOBILE content** in the **MobiFor** curriculum for LEAs (adhering to Export controls etc.)
- ECTEG to consider **content** that can be **further developed** based on topics outlined in D7.1
- ***Annual Specialised Workshops for Forensics Labs*** to be continued at the **NFI** with ECTEG's support

Legal Findings Panel

A panel was held on Legal topics with sister projects. Denitsa Khozhura the WP2 leader and a Researcher and Consultant in the area of fundamental rights and electronic governance, moderated the session. The panel was opened with the speakers Ashwinee Kumar, a Lawyer and Research Analyst at LOCARD, Joshua Hughes, a Research Analyst at Trilateral Research and a member of ROXANNE, and Dr Uwe Ewald, a Lawyer, Analyst and certified expert in Digital Forensics serving on the FORMOBILE Advisory Board, engaging in an insightful debate centred around the following 5 questions:

1 How do you respond to sceptics saying that the AI Act could 'kill' innovation, in particular in the security domain?

2 In your view what should be the approach of the legislator in balancing biometrics' processing for public security vs. preserving individuals' privacy and freedom of discrimination?

3 According to you, how the regulation of AI use in law enforcement activities will influence the modus operandi of criminals?

4 Would the safeguards introduced by AI Act be enough to ensure fundamental rights when applying AI in forensics analyses?

5 How will the AI Act influence research activities in the future?

FORMOBILE Tools

The FORMOBILE tools session on Day 2 was opened up by FORMOBILE Security Officer, Mike Dickinson, MSAB. The aim of the session was to demonstrate 11 out of the 12 tools that were developed in the **Work Packages 4-6** throughout the project’s lifespan.

WP4

- RAMxTRACTOR
- CLOUDxTRACT
- CLONEaQUIRE

WP5

- eMMC emulator
- RAMdCODER
- Antiforensic System
- Dump Decoder

WP6

- Semantic Analyser
- Malware Analysis Platform
- FORMOBILE Visualiser
- Dump Analysis Tool

WP4: Decoding Mobile Data

Task 4.1 RAMxTRACT

Enlarging the mobile phone attack surface: Method for selecting promising peripheral interface; tool for recording communication on internal channels; tool for inserting malicious packets into recorded communications; tool for analysing phone driver software in order to find vulnerabilities and exploit them.

Task 4.2 CLOUDxTRACT

A set of modular python scripts to extract data from cloud services. Full integration into MSAB's XRY tool for easy use. Forensic features like logging and hashing and reminders for legal restrictions.

Task 4.3 CLONEaCQUIRE

Acquire data from counterfeit (cloned) phones, like fake iPhones, Samsungs etc. These phones often confuse first responders because they behave differently than their real counterparts. Now 400+ counterfeit phones have been added to XRY support, including visual aid in recognising them.

Task 4.4 Data importer

Ways to import new data sources (Cloud, RAM) into the XRY tool, so common analysis methods become available for these images.

WP5: Decoding Mobile Data

Task 5.1 eMMC Emulator

A full-fledged eMMC Emulator for restoring a mobile device to a previous state and facilitating the reverse engineering of its low-level components and operation. The eMMC Emulator combined with case-specific software tools may result in the extraction of forensic information from more advanced mobile devices.

Task 5.2 Live forensics to gain passkeys

A software tool for reverse engineering in-RAM process memory. The tool automatically decodes internal RAM structures to help find passwords, cryptographic keys, credentials (e.g. for cloud-stored data) and other forensically relevant data.

Task 5.3 Detection and bypassing antiforensics

A tool that checks all lines of a USB connections between a forensic system and a mobile device for active defence mechanisms. The tool protects the analysis system from any potential damage. It also indicates the connection status, for further decision-making criteria and additional processing.

Task 5.4 Development of novel decoding tools

A software tool for the decoding of file systems and file formats with support of new apps and maintaining existing apps' support. Supported file systems and file formats are documented in D5.5 File Format Handbook.

WP6: Analysis of mobile data

Task 6.1 Semantic analysis

The content analysis of mobile data covers the analysis and evaluation of multiple artefacts, like text, images, audio and video. The Joint Semantic Analyzer (JoSemA) uses machine learning techniques to analyze each data type and integrates all retrieved information into one complete knowledge map.

Task 6.2 Malware analysis

The main function of Z-A^{3}L, the Automated Android Analysis Lab of ZITiS, is the analysis of Android applications for malicious functions and characterisation based on static properties and the behaviour shown during execution.

Task 6.3 FORMOBILE Visualizer

One problem of the analysis of big data is to find value in the mass amount of data. Visualization is the main tool to overcome this problem. The FORMOBILE Visualizer brings a set of visual tools to get an understanding of who is participating in a call, which app was used, what was communicated, and when.

Task 6.4 Development of novel analysis tools

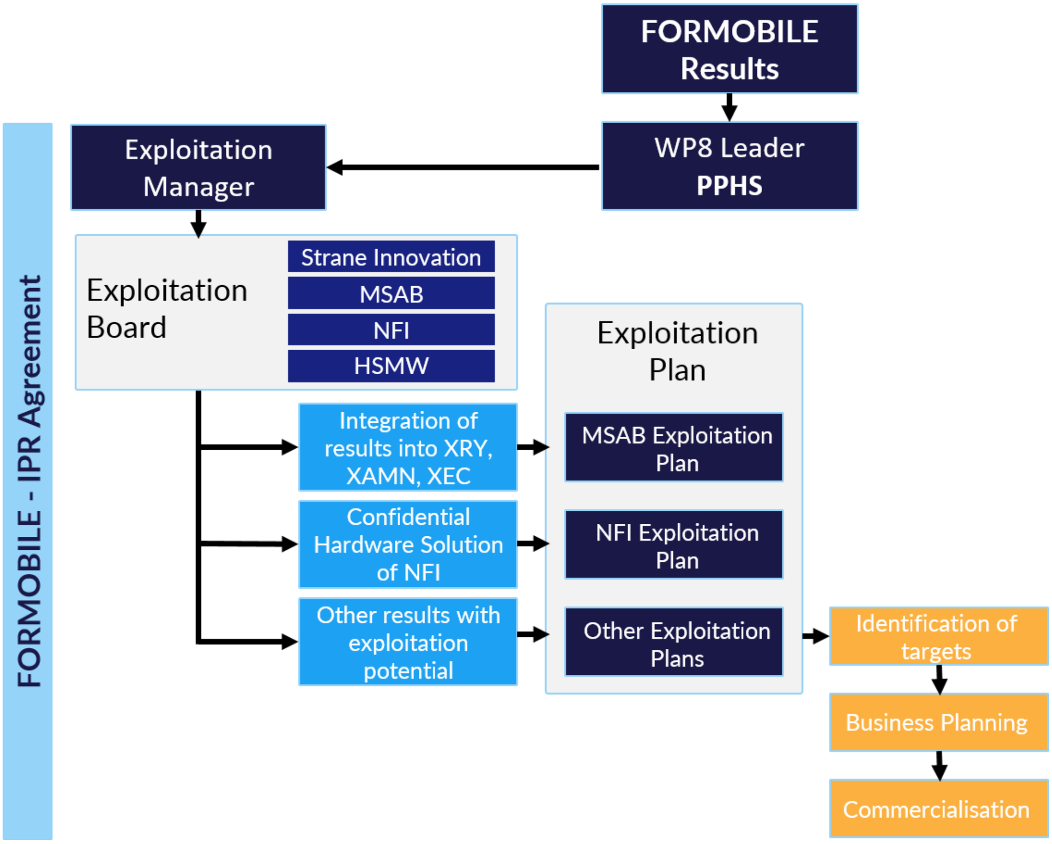
The aim of this task has been to integrate the results of the other tasks, create answers from the data, and make the data available for use in other systems as well as for producing a report of the analysis that can be used in court.

FORMOBILE Legacy

As a conclusion to the project's Final Conference, the Exploitation Board namely Coert Klaver, NFI, Dirk Pawlaszczyk, HSMW, and Mike Dickinson, MSAB, gave a summary of ways in which the FORMOBILE outcomes, training and tools can further be utilised beyond the project's completion.

Three main exploitation routes in FORMOBILE:

1. MSAB is the main exploitation partner and will integrate most results within its XRY, XAMN or XEC solutions
2. NFI exploits its tools for highly specialised forensic laboratories
3. HSMW will continue to improve the tools developed in the project and will make their tools freely available to LEAs.



Conclusion

The FORMOBILE Final Conference was quite memorable not only because of the milestones and achievements that have been realised, but also because of the relationships that have sprouted out of our engagements.

A note of thanks to all the FORMOBILE partners, the PMO, event speakers, invited guests, LEAs, the communication and dissemination team and the host NFI who made this Final Conference a success!

The FORMOBILE project results will be made available on partners' media channels: MSAB, Netherlands Forensic Institute (NFI), Hochschule MITTWEIDA UNIVERSITY OF APPLIED SCIENCES, ZITiS, ECTEG, and the Europol Innovation Lab. Additionally, the CYCLOPES - Cybercrime Law Enforcement Practitioners' Network and ENLETS communities provide brilliant platforms for all relevant stakeholders to remain engaged!

To find out more about the tools developed within WPs 4-6:

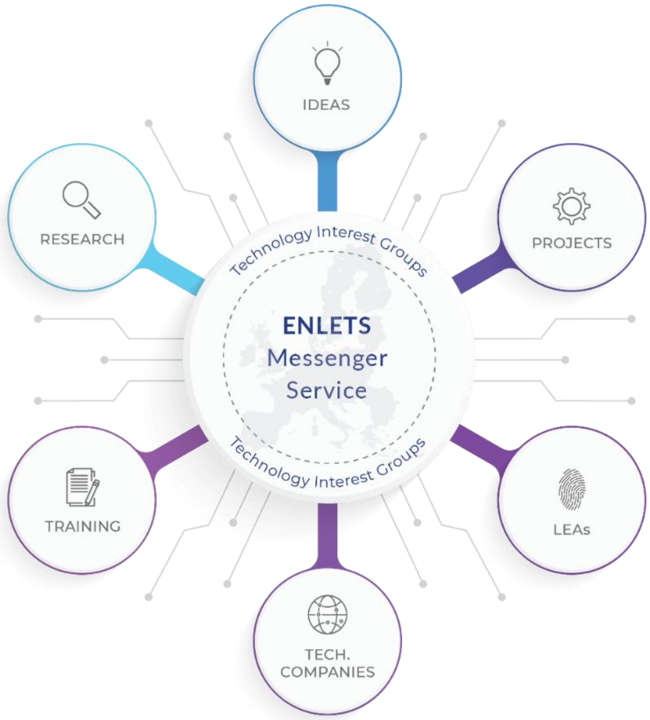
Tools	Notes	Contact
RAMxTRACTOR	Confidential tool for specialists.	Coert Klaver c.klaver@nfi.minvenj.nl
CLOUDxTRACT	Part of MSAB's XRY suite but will be provided to EUROPOL as an open-source solution.	Prof. Dr Dirk Pawlaszczyk pawlaszc@hs-mittweida.de
CLONEaQUIRE	Part of MSAB's XRY Suite. The solution is available and will be further developed by MSAB.	Mike Dickinson mike.dickinson@msab.com
eMMC emulator	Confidential tool for specialists.	Coert Klaver c.klaver@nfi.minvenj.nl
RAMdCODER	Confidential tool for specialists.	Mike Dickinson mike.dickinson@msab.com
Antiforensic System	Plans to make it part of the standard MSAB XRY kit.	Mike Dickinson mike.dickinson@msab.com
Dump Decoder	Part of MSAB's XRY suite, will be improved and developed by MSAB.	Mike Dickinson mike.dickinson@msab.com
Semantic Analyser	A tool with huge potential but requires continued development – managed by Hochschule Mittweida.	Prof. Dr Dirk Pawlaszczyk pawlaszc@hs-mittweida.de
Malware Analysis Platform	A standalone tool that is under development.	Andreas Richl Andreas.Richl@ZITiS.bund.de
FORMOBILE Visualiser	Part of MSAB's XAMN platform. The solution will be improved and developed continuously.	Mike Dickinson mike.dickinson@msab.com
Dump Analysis Tool	Part of MSAB's XAMN platform. The solution will be improved and developed continuously.	Mike Dickinson mike.dickinson@msab.com

Continued Dialogue

Interested LEAs can connect through the European Network of Law Enforcement Technology Services, ENLETS.

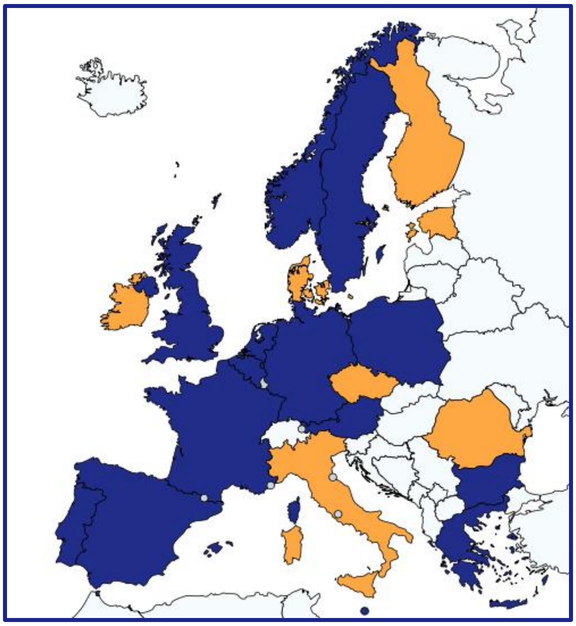
The free solution provides a safe, encrypted chat experience through a dedicated mobile application and web browser service.

GET ACCESS



FORMOBILE Consortium

HOCHSCHULE MITTWEIDA University of Applied Sciences
Nederlands Forensisch Instituut Ministerie van Justitie en Veiligheid
MSAB
AUSTRIAN STANDARDS
ZITiS
Home Office
POLICIA NACIONAL
POLICJA
TIMELEX
TUDelft Delft University of Technology
UNIVERSITY OF PATRAS
POLITIHØGSKOLEN
FORTH
Strane Innovation
LAW AND INTERNET FOUNDATION
POLISH PLATFORM FOR HOMELAND SECURITY



🟦 Consortium Partners

🟧 Contribution from other countries

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800