Work Package 1 Questionnaire
Definition of law enforcement agencies
REQUIREMENTS on mobile forensics

Introduction:

The EU is a connected society. Mobile phones are used to continuously share information, files and images. Thankfully much of this communication is ordinary. However, criminals and terrorists use the same channels for communication. The project FORMOBILE will focus on the requirements of law enforcement agencies (LEA) in mobile forensics.

Mobile phones are a unique challenge for LEAs due to the number and variants in circulation. They are also analyzed differently in another way than devices such as PCs and Laptops, meaning the investigation requires a separate process. It is imperative that LEAs have ways to access, decode and use the data as evidence - in a safe, trustworthy and reliable manner.

We collect the requirements of LEAs to provide the base for a standardized process all over Europe as well as tools and applications therefor. During this process, the input from the LEAs is essential to ensure that the results are useful in practice.

Therefore, we need your help today. Please fill out the following form to provide the information we need to build tools making your daily work easier, more comfortable and safer.

Editing instructions:

Hereinafter you find questions related to (1) your law enforcement agency, (2) your range of services, (3) your technical equipment, (4) your intern processes and (5) your requirements and needs. The last point is the most important one for us. We would like to know *what you need* to build the tools and describe processes *you can really use* purposefully.

It will take some time to fill out that questionnaire. Please feel free to ask different persons in your agency for information: the administration department, technicians, engineers, field staff or wherever you find the most appropriate information to reflect how your agency deals with data on mobile phones and what you need to work even more effectively.

So please don't hesitate to ask for assistance. Please ensure that every department working on this questionnaire is listed in the following table. We will not ask for names, but please track the persons working on this form for yourself in case we will contact you for further information.

Departments working on this questionnaire

Data protection declaration:

The entire information you provide are highly confidential. There will be no unauthorized publication of your data. All information is only used within the FORMOBILE project to define and validate tools and processes to deal with data on mobile phones in criminal investigations.

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

Law Enforcement Agency - Background information		
1	Country	
2	Agency: Name	
3	Agency: Number of employees (all)	
4	Number of technicians in your agency handling mobile forensic tools	
5	Is your agency represented on a European Network of Practitioners that is dedicated to digital forensic issues?	o no o yes o unknown
6	If you answered "yes" to the last question: Please provide the name of the network:	
7	Is your agency a member of any online community / forums dedicated to digital forensics?	o no o yes o unknown
8	If you answered "yes" to the last question: Please provide the website address of the organizing body:	
9	Please rate the level of your forensic laboratory:	o First responder: The first contact with the evidence regularly occurs with so-called first responders. These are in general officers of local police departments. They can realize a first examination with standard tools and solve common cases. o Common forensic laboratories: If the first responders fail in the examination, the traces are passed to forensic laboratories that are more specialized. Such laboratories are usually resident to the offices of the federal police. These groups have more specialized tools and can solve more complicated cases. o Highly specialized forensic laboratories: In the case of the most complicated, technically highly sophisticated traces, the evidence will be passed onto highly specialized forensic laboratories. Most of the EU member states maintain only one or two of these laboratories.
	Expertise	
10	Does your agency have employees (police officers, personnel, etc.) that are dedicated to working only in the field of digital forensic investigations?	o no o yes o unknown
11	If you answered "yes" to the last question: Are any of your dedicated staff on a digital forensics "register of experts"?	o no o yes o unknown
12	If you answered "yes" to the last question: Please provide details of the expert register:	

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

	Collaborations / Knowledge Exchange	
13	Does your agency work on cases in digital forensics within your agency? [single choice]	o yes, we solve digital forensic cases on our own o yes, we try to solve digital forensic cases on our own, but we can ask other agencies for support o no, all of the digital forensic cases go directly to another agency / institution / etc.
14	Does your agency have any kind of cooperation to solve cases in digital forensics? (e.g., technical labs, other agencies, etc.)	o no o yes o unknown
15	If you answered "yes" to the last question: Which kind(s) of cooperation does your agency have to solve digital forensic cases? [multiple choice]	o other agencies national o other agencies international o state laboratories national o state laboratories international o other state institutions national o other state institutions international o private laboratories national o private laboratories international o other private institutions national o other private institutions international o academic or research institutes national o academic or research institutes international o other
16	Does your agency share knowledge on digital forensic related issues with other law enforcement agencies?	o no o yes o unknown
17	If you answered "yes" to the last question: Please name the agencies:	o I'm unable to share this information
18	If you answered "yes" to the last question: Please provide details of the knowledge sharing platform that is used:	
19	In your opinion, how important is it to share ideas and information with colleagues *within your country* with regard to digital forensic issues? (1 = not important – 10 = extremely important)	**1** O O O O O O O O O O **10**
20	In your opinion, how important is it to share ideas and information with colleagues *across the EU* with regards digital forensic issues? (1 = not important – 10 = extremely important)	**1** O O O O O O O O O O **10**
21	Has your agency been consulted in defining requirements for any standardization related work within the field of digital forensic?	o no o yes o unknown

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

22	If you answered “yes” to the last question: Please provide details of the work carried out with regard to standardization:	
23	Has your agency been consulted with regard to procurement within the field of digital forensic?	o no o yes o unknown
24	If you answered “yes” to the last question: Please provide details of the work carried out with regard towards procurement:	

Law Enforcement Agency - Processes and procedures - *at the crime scene*		
	ONLY for first responders: Please answer this section only if you answered question 9 (level of your forensic laboratory) with “first responder”. Could you please describe the following process: Mobile phones at crime scenes - how are they seized?	
25	When / Where does your seizure process start?	o at the crime scene o in the office o in the lab
26	Are additional items seized? (e.g., cables, memory cards, SIM cards)	o no o yes o unknown
27	Is biometric data seized from the device (e.g., to connect persons to the device)?	o no o yes o unknown
28	How is the seizure process documented? [multiple choice]	o video o dictaphone o pictures o writing
29	How is the device protected when under transport (integrity, confidentiality)?	
30	Is the mobile phone bagged and tagged by default?	o no o yes o unknown
31	If you answered “yes” to the last question: Please describe the chain of custody you follow:	
32	Do you follow a process to protect the integrity of the data?	o no o yes o unknown
33	If you answered “yes” to the last question: Please describe the process:	
34	Is the mobile phone attached to a power bank or other power sources by default?	o no o yes o unknown

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

35	Is the mobile device disconnected from all networks?	o no o yes o unknown	
36	If you answered “no” to the last question: Please describe in which cases they are not disconnected from the networks:		
37	Did you encounter with remote deletion of a mobile phone that has not been disconnected from the network?	o no o yes o unknown	
38	Are you permitted to leave the device online with open network access, allowing new incoming calls or other communications?	o no o yes o unknown	
39	If the device is unlocked during seizure, how is this access preserved until data acquisition?		
40	Do you document any / all changes to the phone?	o no o yes o unknown	
41	Are you looking for passwords, phone backups, access token on computers/tablets/etc. at the crime scene?	o no o yes o unknown	
42	Do you have standard (suspect) interview questions related to mobile acquisition on-scene for:	PIN	o no o yes o unknown
43		PUK	o no o yes o unknown
44		Unlock pattern	o no o yes o unknown
45		Unlock password	o no o yes o unknown
46		Accounts and passwords	o no o yes o unknown
47		Fingerprint access	o no o yes o unknown
48		Face access	o no o yes o unknown

Law Enforcement Agency - Processes and procedures - *in general*

Please describe in the following questions the process your agency follows when you encounter mobile devices (e.g., national / agency standards).

49	Where does the first mobile forensic step take place (e.g., at a crime scene, in your lab, in an external lab)?	

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

50	"Who" brings the mobile phone into your agency / department (e.g., police men, other agencies / departments)?	
51	Which department takes care of the mobile phone first?	
52	Which department starts the analysis process (e.g., extracting data)?	
53	Where do you send mobile phones if you reached your limits in analyzing data within the department you just described?	
54	Which department writes the final report on the acquired mobile phone data?	
55	Is the process, you just described, congruent to the standards within your agency / national / European standards?	o no o yes
56	If you answered "no" to the last question: Please provide details on the differences of the case work compared to the intended process of the standard:	
57	Do you think the process you described in questions 56 – 61 is the best way to analyze mobile phone data?	o no o yes o unknown
58	If you answered "no" to the last question: Please provide details of what could be improved:	
59	Do you follow any national or international standards / documents (e.g., NIST Special Publication 800-101, ISO17025)?	
60	Do the standards you follow have any influence of your work in the field of mobile forensics?	o no, o yes,
61	Do the standards you follow leads to court-proof evidence?	o no, o yes,
62	Are there *safety specifications* (within your agency) that hinder you while working in the field of mobile forensics?	o no o yes
63	If you answered "yes" to the last question: Please provide details of what hinders you:	
64	Are there *legal regulations* (including ethics aspects in your country) that hinder you while working in the field of mobile forensics?	o no o yes
65	If you answered "yes" to the last question: Please provide details of what hinders you:	

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

Law Enforcement Agency - Technical equipment		
66	Please name the special-purpose mobile forensic **software** you can use and have an active license for (e.g., software of manufacturers like MSAB, Cellebrite, …):	
	In the following questions please describe the special-purpose mobile forensic **hardware** you can use in your agency / department:	
67	Grayshift GrayKey	o we don't have o we have, but we don't use o we have and we use
68	Cellbrite UFED Ultimate	o we don't have o we have, but we don't use o we have and we use
69	NFI Memory Toolkit	o we don't have o we have, but we don't use o we have and we use
70	General-purpose lab instruments (e.g., oscil-loscope, probe-station, rework-station)	o we don't have o we have, but we don't use o we have and we use
71	Other (please name)	
	In the following questions please describe the special purpose mobile forensic **capabilities** you use to analyze mobile phone data:	
72	Wet chemical etching	o no o yes
73	Chip preparation	o no o yes
74	Chip-off	o no o yes
75	Password guessing	o no o yes
76	Non-invasive attacks (e.g., side channel)	o no o yes
77	Semi-invasive attacks (e.g., fault attacks)	o no o yes
78	Fully-invasive attacks (e.g., fuse extraction, circuit edit)	o no o yes
79	Other (please name)	
80	How often do you receive / buy forensic software updates / new software?	o every month o every six month o once a year o as often as we need
81	How often do you receive / buy hardware updates / new hardware you need for working in the field of mobile forensics?	o every month o every six month o once a year o as often as we need
82	If you could freely choose, which additional hard-ware / software would you use?	

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

Law Enforcement Agency - Scope of services		
83	Please describe a few typical cases in mobile forensics in your agency:	
84	Please describe a few extremely rare cases in mobile forensic in your agency:	
85	During the last two years: Did you have cases with mobile phones you could not analyze?	o yes, because we did nott have the hardware tools o yes, because we did not have the software tools o yes, because we did not have the skills / knowledge o no, so far we solved every task
86	If you answered “yes” to the last question: Please name the mobile phones (manufacturer and operating system) you were not able to analyze:	
87	Please describe the typical / common problems you encountered:	
88	Please describe rare / unusual problems you encountered:	
89	Which mobile phones (manufacturer and operating system) are the most common you work with?	
90	Do you analyze additional apps, which are not covered by the standard forensic tools (e.g., by using self-written scripts)?	o no o yes

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

Law Enforcement Agency - Competencies

91	Please describe the team members who work with mobile phones in your agency (e.g., technicians, specialists for digital forensics, police officers with passion for digital devices)	
	Please rate the competencies (of your whole team) for the following processes on the scale (1 = low – 10 = high) in:	
92	Data collection	**1** O O O O O O O O O O **10**
93	Sharing data	**1** O O O O O O O O O O **10**
94	Encryption	**1** O O O O O O O O O O **10**
95	Artificial intelligence	**1** O O O O O O O O O O **10**
96	Digital forensic tools	**1** O O O O O O O O O O **10**
97	RAM acquisition	**1** O O O O O O O O O O **10**
98	Cloud data extraction	**1** O O O O O O O O O O **10**
99	Acquisition of mobile clones	**1** O O O O O O O O O O **10**
100	eMMC / UFS emulation	**1** O O O O O O O O O O **10**
101	RAM-decoding	**1** O O O O O O O O O O **10**
102	Anti-forensics detection	**1** O O O O O O O O O O **10**
103	Data visualization	**1** O O O O O O O O O O **10**
104	Semantic analysis	**1** O O O O O O O O O O **10**
105	Malware analysis	**1** O O O O O O O O O O **10**
106	How do you deal with mobile phones you are unable to analyze? Please describe the process:	
107	How is your mobile forensic staff trained?	o higher education (university, university of applied sciences) o vocational education o structured training o training on the job o by passion for digital forensics (individually)
	If you are able to **share any success** of your agency in the field of mobile forensics, could you please describe briefly …	
108	(1) the case:	o I'm unable to share this information

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

109	(2) what went quite well:	
110	(3) what do you think was important for this success (e.g., teamwork, technology):	
	If you are able to **share any failure** of your agency in the field of mobile forensics, could you please describe briefly …	
111	(1) the case:	o I'm unable to share this information
112	(2) what went quite badly:	
113	(3) what do you think was the reason for this failures, e.g., missing teamwork, old technology, missing competencies, problems with commercial products, solutions and workarounds,…	

Law Enforcement Agency - Requirements and needs

What do you think you would need to perform better even better when dealing with mobile forensics: (1 = irrelevant – 10 = very important)

114	Theoretical training for mobile forensics	**1** o o o o o o o o o o **10**
115	Hand-on training for mobile forensics	**1** o o o o o o o o o o **10**
116	Service points to send in all that mobile forensic stuff (and get expert reports back)	**1** o o o o o o o o o o **10**
117	Better technical equipment (hardware)	**1** o o o o o o o o o o **10**
118	Better technical equipment (software)	**1** o o o o o o o o o o **10**
119	Better internal processes	**1** o o o o o o o o o o **10**
120	Additional generic staff	**1** o o o o o o o o o o **10**
121	Additional specialized staff	**1** o o o o o o o o o o **10**
122	Access to physical classroom training	**1** o o o o o o o o o o **10**
123	Access to online training	**1** o o o o o o o o o o **10**
124	Certification in mobile forensics	**1** o o o o o o o o o o **10**

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

125	Other (please name)	

	Other	
126	Is there anything else you want to tell us? About this questionnaire, the project, anything else we didn't think about?	

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

Thank you very much for the time you spent on filling out this form. We are sure that was a heavy workload on top of your regular work. We want you to know that the results are used to make your daily work with mobile forensics easier and better to handle. Based on your results, we develop software and trainings for your needs.

Thank you for being part of the project FORMOBILE.

For questions regarding the questionnaire, please contact:

Dr. Susanne Heininger
WP 1 – Project Manager
Research Manager
Central Office for Information Security in the Security Sector (ZITiS)
e-mail: susanne.heininger@zitis.bund.de
phone: +49 (0) 89 / 6080 679 6251

Andreas Richl
Head of Projects Cryptanalysis
Central Office for Information Security in the Security Sector (ZITiS)
e-mail: andreas.richl@zitis.bund.de
phone: +49 (0) 89 / 6080 679 6228

Dr. Ralf Zimmermann
WP 1 – Leader
Head of Research Cryptanalysis
Central Office for Information Security in the Security Sector (ZITiS)
e-mail: ralf.zimmermann@zitis.bund.de
phone: +49 (0) 89 / 6080 679 6108

More about the FORMOBILE project:

www.formobile-project.eu

Linkedin – Formobile-project

Twitter – @Formobile2019

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