# Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition

Alexios Mylonas, Vasilis Meletiadis, Bill Tsoumas, Lilian Mitrou, Dimitris Gritzalis

# Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition

Alexios Mylonas[1], Vasilis Meletiadis[1], Bill Tsoumas[1], Lilian Mitrou[1,2], Dimitris Gritzalis[1]

[1]Information Security and Critical Infrastructure Protection Research Laboratory
Dept. of Informatics, Athens University of Economics and Business (AUEB)
76 Patission Ave., Athens, GR-10434 Greece
{amylonas,meletiadisv,bts, dgrit}@aueb.gr

[2]Dept. of Information & Communication Systems Engineering,
University of the Aegean, Samos 83200, Greece
l.mitrou@aegean.gr

**Abstract.** Smartphones constantly interweave into everyday life, as they accompany individuals in different contexts. Smartphones include a combination of heterogeneous data sources, which can prove essential when combating crime. In this paper we examine potential evidence that may be collected from smartphones. We also examine the available connection channels for evidence transfer during a forensic investigation. We propose a Proactive Smartphone Investigation Scheme that focuses on ad hoc acquisition of smartphone evidence. We also, take into consideration the legal implications of the proposed scheme, as it is essential that the scheme includes prevention mechanisms, so as to protect individuals from misuse by investigators or malicious entities.

**Keywords:** Smartphones, Forensics, Digital Evidence.

## 1 Introduction

Smartphones, as ubiquitous devices, merge with a person's everyday life. As a recent report[1] points out, smartphone sales outnumbered these of feature phones, thus, acquiring a significant user base. Smartphones are characterized by mobility, context-awareness, and diversity on the data sources that they integrate.

In a crime investigation context, the aforementioned characteristics can be used for forensic purposes, not only after a crime, but even proactively. For instance, in some crimes, which the in place legal and regulatory context regards as 'severe' (e.g. crimes against public or the state, pedophilia, etc.), proactive acquisition of smartphone data may be required. Currently, in a Lawful Interception (LI) of cell phones, Law Enforcement Agencies engage via the carrier's infrastructure, the intercep-

[1] International Data Corporation (IDC). Smartphones Outstrip Feature Phones for First Time in Western Europe as Android Sees Strong Growth in 2Q11, September 2011.

tion of specific data, such as phone calls, messaging services, and network data traffic [3]. The need for direct and in-time access to forensics data is also present in other technological contexts.

In the organizational context, Grobler et al. [5] refer to proactivity, as "creating or controlling a situation rather just responding to it". They stress that a Proactive Digital Forensics (ProDF) as a process, ensures the facilitation of the investigation in a successful and cost-effective manner for enterprise systems. ProDF refers, for example, to the deployment of *forensic readiness* processes [15], which aim to maximize an environment's ability to collect credible digital evidence and, at the same time, minimize the forensics cost during incident response. These processes incorporate tools and techniques for active/live forensics that acquire volatile data for detecting criminal activity [14].

In traditional, i.e. post mortem, forensics the need for *forensic triage* [9], [13] emerges. Forensic triage refers to the notion of *on-site forensics*, which allows an investigator to directly assess a crime scene. Assessment is feasible for a subset of the available digital evidence. Consequently, delays on results, stemming from time-consuming processes in the forensics lab, are avoided. Furthermore, in on-going crime investigations, forensic triage can assist an investigator to determine critical issues, such as subjects in immediate need or the suspect's call activity [17], and act as appropriate. Also, mobile live memory forensic techniques focus on the acquisition of volatile data, which reside in device's memory [16].

In this paper, we examine the technological aspects of proactive smartphone digital forensics. A smartphone can provide additional information, which exceeds communication data. The multitude, variety and 'context awareness' of smartphone data may constitute crime evidence beyond the scope of current LI systems, both in technical and legal terms. Thus, we propose a Proactive Smartphone Investigation Scheme that incorporates misuse avoidance of proactive evidence collection.

The paper is organized as follows. In Section 2, a taxonomy of smartphone evidence and evidence transport channels is presented. Section 3 proposes an Investigation Scheme for proactive smartphone forensics. Section 4 discusses legal considerations for proactive evidence acquisition on smartphones. Section 5 concludes the paper.

## 2 Smartphone Evidence

Smartphones host a plethora of heterogeneous data generated from hardware or software sources. This section associates smartphone data sources with evidence types and then correlates these sources with smartphone evidence transport channels. These associations will be used in the sequel for smartphone ad hoc evidence acquisition.

### 2.1 Smartphone Evidence Taxonomy

In order to associate smartphone data to evidence types, a data-oriented analysis was followed. The analysis used a smartphone data taxonomy presented in [12]. Data are categorized, with respect to their source, as: a) *Messaging Data*, i.e. the content and

metadata (e.g. sender, delivery time, etc.) from messaging services (e.g. Short Message Service (SMS), email etc.), b) *Device data*, i.e. data that are stored in the device storage media and are not related to any application (e.g. multimedia files, software and hardware identifiers etc.), c) *(U)SIM Card Data*, that reside in a (Universal) Subscriber Identity Module, such as IMSI[2] and MSIN[3], d) *Usage History Data*, i.e. user logs (e.g. call logs, browsing history, etc.) and system logs kept for monitoring and debugging, e) *Application Data*, i.e. permanent or temporal data that are used during application execution (e.g. flat files, databases, etc.), f) *Sensor Data*, which are created by sensors that are found in most devices (e.g. camera, microphone, GPS), motion sensors (accelerometer, gyroscope), or environment sensors (magnetometer, proximity, light, temperature, etc.) and g) *User Input Data*, i.e. data from keystrokes, gestures, etc., which are processed on the fly, or stored in a keyboard cache for performance reasons.

The above mentioned data sources were organized in *a taxonomy* of *evidence types*, which derived from a set of questions - i.e. {*who, where, when, what, why, how*} [20]. These questions are being used in digital forensics literature [6], [8], [1] for evidence examination and analysis, as well as for evidence presentation in courts of law.

- *Identity Evidence*. Data identify subjects that are part of an event.
- *Location Evidence*. Data define the approximate or exact location, where an event takes place.
- *Time Evidence*. Data can be used to infer the time that an event takes place.
- *Context Evidence*. Data provide adequate context, such as user actions and activities for an event description [7], or the event nature.
- *Motivation Evidence*. Data can be used to determine event motivation.
- *Means Evidence*. Data describe the way that an event took place, or the mean that were used.

Even if we both assume that smartphone data are generated in a deterministic and undisturbed way and their acquisition is always feasible, this does not necessarily mean that evidence will always be present. Hence, we use three levels of association of *direct* relationship between a data source and an evidence type, namely: a) *Strong Correlation* to represent that data sources always (or in most cases) provide potential evidence, b) *Weak Correlation* to represent that data sources may provide potential evidence according to their state, and c) *No Correlation* to represent lack of relationship between a data source and evidence type. In this point we note that motivation evidence may be deduced *indirectly* via the combination of the other evidence types.

The rest of this section presents the correlation of the evidence types with the data sources.

- *Messaging Data*. Both traditional messaging services (e.g. SMS) and modern ones, e.g. email, often constitute potential evidence. Specifically, external communication data reveal the subjects and the communication time and, as a result, this source is strongly correlated with time and identity evidence. In addition, the

[2] The International Mobile Subscriber Identity (IMSI) identifies the subscriber to the network.
[3] Mobile Subscriber Identification Number (MSIN) is the 10-digit phone subscriber number.

communication content may reveal location evidence, motive evidence, etc., therefore this source is weakly correlated with them as well.

- *Device Data*. Data such as system identifiers (e.g. IMEI) can be used to determine a subject from the provider's records, therefore a strong correlation with identity evidence exists. File system metadata can be used to determine time (e.g. file access time). Hence, a strong correlation with time evidence exists. Data created by the user (e.g. multimedia) may reveal motive or means evidence. In addition, device data may include sensor data as metadata (e.g. in geo-tagging). This provides a weak correlation with location, context, motivation or means of an incident.
- *(U)SIM Card Data* includes identifiers (e.g. ICCID[4], IMSI, etc.) that uniquely identify a device owner, thus, a strong correlation exists. Other data that may be stored in this source (e.g. contact entries, SMS and LAI[5]) [8] can be used to deduce the rest evidence types, and, in this case a weak correlation exists.
- *Usage History Data* can infer the event time and the means used by a digital incident, or they can even reconstruct user events, thus implying a strong correlation with the respective evidence types. Furthermore, under certain circumstances, the wireless connection history (i.e. access point MAC logs) may be used to infer the device location[6], implying a weak correlation with this evidence type. Finally, Bluetooth pairing logs can be used to infer whether the user is in a crowded area and, in some cases, identify subject evidence via the device Bluetooth id.
- *Application Data*. In some cases, private application data stored on the device may lead to potential evidence about an event and, thus, weak associations with the corresponding evidence exist. For instance: a) cached maps in navigation applications determine location evidence, b) cached social networking application data can be used to infer all the other evidence types depending on their content, etc.
- *Sensor Data* provide weak correlations with all evidence types, since they can be used to infer the device context. For instance, a microphone can be remotely enabled [12] and harvest speech data related to all evidence types. Nonetheless, in the case of location evidences, the correlation is strong due to the popularity and location accuracy of GPS sensors. .
- *User Input Data* can be used to identify a subject via keystroke analysis and, as a result, a weak correlation with this evidence type exists. Often, the keystroke cache content may reveal other evidence types, thus, a weak correlation with them exists.

Table 1 depicts the correlations between data sources and potential evidence types, where: (✓) stands for strong correlation, (~) for weak and (✘) for no correlation.

Finally, the above evidence types can be combined to form evidence chains when they include valid timestamps. For instance, call logs combined with cached data of a navigation application can be used to reveal or confirm a subject's alibi.

---

[4] Integrated Circuit Card ID (ICCID) is the serial number of the (U)SIM card.

[5] Simply put the Location Area Identity (LAI) identifies the cell where the device is in and as a result can be used to get an approximation of device location.

[6] Via public mapping of MAC addresses to GPS coordinates, such as http://samy.pl/mapxss/

**Table 1.** Correlation between evidence types and data sources

| Data sources \ Evidence Types | Identity | Location | Time | Context | Motivation | Means |
|---|---|---|---|---|---|---|
| Messaging Data | ✓ | ~ | ✓ | ~ | ~ | ~ |
| Device data | ✓ | ~ | ✓ | ~ | ~ | ~ |
| (U)SIM Card Data | ✓ | ~ | ~ | ~ | ~ | ~ |
| Usage History Data | ✘ | ~ | ✓ | ~ | ✘ | ✓ |
| Application Data | ~ | ~ | ~ | ~ | ~ | ~ |
| Sensor Data | ~ | ✓ | ~ | ~ | ~ | ~ |
| User Input Data | ~ | ~ | ~ | ~ | ~ | ~ |

### 2.2 Evidence Transport Channels

Smartphones can use four data transport channels (or interfaces) that provide different transport services. This section discusses their ability to support evidence transfer during a proactive forensic investigation.

1. *GSM Messaging interface* (e.g. SMS, etc.) provides a remote channel appropriate for small volume data transfers, which is nearly always available. Apart from the restriction in volume, another refers to cost. Increased cost a) may limit the messaging service availability, thus, large data may not be transferrable and b) may alert suspects, who thoroughly check their carrier bills in the case a proactive investigation taking place.
2. *Personal Area Network (PAN) interface* (e.g. Bluetooth, IrDA, etc.) provides a cost free, ad hoc, remote data channel, appropriate if the data collector is in the smartphone's proximity. By not relying on any base station existence, it avoids network monitoring mechanisms, such as Intrusion Detection System (IDS). Furthermore, as this channel requires no cost, it is stealthier than others. Potential shortcomings are: a) distance constraint between the device and the collector, which increases attack complexity (e.g. Bluetooth range is 10 meters), b) the average transfer speed and c) the requirement for a pairing bypass without alerting the smartphone user.
3. *WLAN interface* (e.g. Wi-Fi) provides a fast, remote channel that is appropriate for any data volume often without a cost. Due to the general popularity of Wi-Fi, availability is considered high. A shortcoming is that data transfer speed and availability rely on the distance from a base station. This distance, though, is considerably larger than the PAN's requirement, thus, it does not add considerable complexity on evidence collection.
4. *Cellular network (CN) interface* provides a data transport channel of variable speed, which is dependent on the supported carrier network technology (e.g. GPRS, HSDPA, etc). A CN channel is not restrained by the antenna range. It provides greater mobility than any of the aforementioned channels, since the smartphone may travel through cells. Nonetheless, this channel is not considered suitable for large data volume, as: a) it suffers from connection drops, b) the network speed may vary as the user moves inside a cell or visits others, and c) this channel use has considerable cost, and thus it may be discovered by the owner.

Table 2 summarizes each channel's ability to effectively transfer each source data volume (hereto referred as 'volume'). For the association notation three symbols were used, i.e.: 1. (?) transfers small subset of the data source, 2. (~) transfers most data in this data source and 3. (✓) can transfer source type. Obviously, the WLAN channel is able to transfer all data sources. The rest of the associations are listed below:

- *Messaging data* are not volume intense, thus, they can be transferred by all channels.
- *Device data* include data with different volume requirements, ranging from small files to high definition videos. Hence, the GSMMe channel can only convey a subset of this source, whereas PAN and CN can convey, in general, this data source. Nonetheless, the latter are limited by time and transfer cost respectively.
- *(U)SIM Card Data* is not volume demanding, and can be transferred by all channels.
- *Application Data* volume requirements range from few Kbytes up to hundreds of Mbytes. As a result, PAN and CN (provided that available quota exist) are able to transfer this data type. GSMMe can only transfer application data that are not volume intense.
- *Usage History Data* are not always volume demanding (e.g. recent call logs) and, hence, can be transferred by GSMMe. Nonetheless, this data type includes OS logs, which are data volume intense and are transferable by PANs and CNs (if available bandwidth quota exists).
- Similarly to *Usage History Data*, *Sensor* data can be a) either not volume intense (e.g. GPS coordinates) and, thus, transferrable by GSMMe, or b) volume intense (e.g. accelerometer data) that can be transferred by PAN and CN.
- *User Input Data* volume requirements range from a few Bytes, which are transferable even by GSMMe, up to several Mbytes (e.g. keystroke dictionaries) that are transferable by PANs and CNs.

**Table 2.** Correlation between transport channels and data sources

| Transport channel / Data type | GSMMe | PAN | WLAN | CN |
|---|---|---|---|---|
| Messaging Data | ✓ | ✓ | ✓ | ✓ |
| Device data | **?** | ~ | ✓ | ~ |
| (U)SIM Card Data | ✓ | ✓ | ✓ | ✓ |
| Application Data | **?** | ✓ | ✓ | ~ |
| Usage History Data | **?** | ✓ | ✓ | ~ |
| Sensor Data | **?** | ✓ | ✓ | ~ |
| User Input Data | **?** | ✓ | ✓ | ✓ |

## 3 Proactive Smartphone Forensics Investigation

This section focuses on proactive forensics, where ad hoc acquisition of smartphone evidence takes place. A proactive smartphone forensics investigation may take place

for the investigation of crimes considered 'severe' by the legal and regulatory context in place (e.g. crimes against public or the state, pedophilia, etc.). In such cases, the creation and defence of an investigation hypothesis[7] may use the aforementioned associations of smartphone sources with transport channels and evidence types. In this context, an investigation scheme is presented and outlined.

### 3.1 Proactive Smartphone Forensics Scheme

The proposed scheme consists of three entities (Fig. 1), namely: a) subject(s) carrying out a proactive smartphone forensic investigation (hereinafter 'investigator'), b) an Independent Authority (IA), and c) the investigation's subject(s) (hereinafter 'suspect').

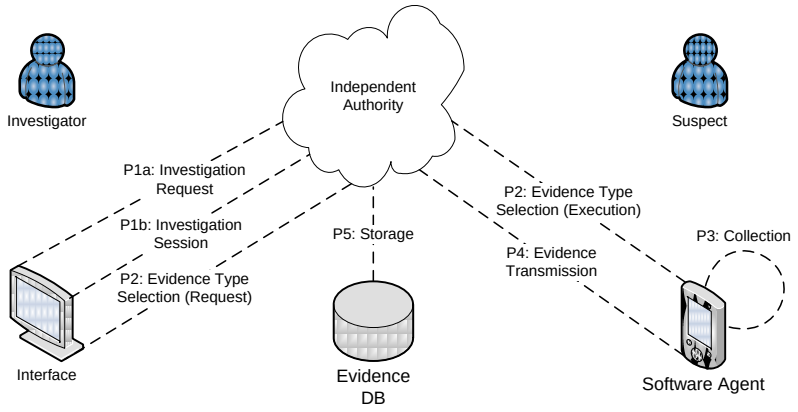


**Fig. 1.** Proactive Smartphone Forensics Scheme

As depicted in Fig. 1, the *IA* is the scheme's corner stone, as it: a) controls evidence collection from the Software Agent (SA) that resides in the suspect's smartphone, b) handles evidence storage for a time period compliant with existing laws and regulations, and c) authorizes investigator's requests for a proactive forensic investigation against individuals.

This architecture was selected so as to hinder investigators, or other individuals, from misusing the evidence collection mechanism for profiling and intelligence gathering reasons (see Section 4).

Hence, it is assumed that the IA allows a proactive digital forensic investigation to take place only in suspected 'severe' crimes. It is also assumed that the IA maintains a database, where evidence data are stored and protected, in terms of forensic soundness and confidentiality.

The *investigator's* role in this scheme is to create a hypothesis, i.e. collect adequate evidence suitable for use in courts of law. An investigator may request from the IA authorization for a proactive smartphone forensics investigation to take place when: a)

[7] Hypothesis is a report based on the examination and the analysis of collected evidence that are admissible to court.

other mechanisms for data collection are either incapable to gather the required data (e.g. cases where the suspect's context is required), or they collect data of reduced accuracy, inadequate for evidence presentation in a court of law (e.g. the location accuracy of the GPS sensor is greater than the approximate location provided by the cell phone provider), and b) the suspected crime is considered 'severe' by laws and regulations.

In this scheme, it is assumed that a Software Agent (SA), controlled by the IA, is present in the *suspect's* smartphone. Also, the IA has the capability to commence the collection of evidence types from selected smartphone sources. The scheme's architecture is depicted in Fig. 1, while its processes are described in the following section.

### 3.2 Scheme Processes

The proposed scheme consists of six building blocks - processes, namely: 1) *investigation engagement*, 2) *evidence type selection*, 3) *evidence collection*, 4) *evidence transmission*, 5) *evidence storage* and 6) *investigation completion*.

The first process takes place once per suspect investigation, while the remaining processes are iterative and incremental. The last process (*Process 6: Investigation Completion*) is completed when the investigation's requirements are satisfied, i.e. the hypothesis can be created and its validity can be defended in the courts of law, or when the IA's granted permission becomes invalid. The other processes are described in detail in the sequel.

**Process 1: Investigation Engagement**. It consists of two sub processes that define an investigation's details:

- *Process 1.1: Investigation Request (IR).* This is the formal request of investigation authorization, addressed to the IA. The request contains a definition of investigation specific parameters, such as: a) the investigator who creates the hypothesis, b) the suspects(s), c) the nature of the examined crime, d) the expected investigation period, e) the required data sources that will be collected as potential evidence, and f) the required channels for evidence transmission.
- *Process 1.2: Investigation Session*. Once an Investigation Request is submitted to the IA, a non-automated process determines the investigation's permission level upon the suspect's smartphone. This permission level is determined by the IR details and the evaluation criteria of each IA, which are dependent on the regulatory context. If the IR is accepted, an investigation session is provided to the investigator that is used for the following processes.

**Process 2: Evidence Type Selection.** This process is initiated after the investigation engagement process. It refers to the selection of evidence types and the corresponding transport channels by the investigator. This selection is carried out based on the two associations presented previously: (1) between smartphone data and digital evidences, and (2) between smartphone data and transport channels. For instance, an investigator may compile a configuration request for the SA evidence collection process. This configuration request specifies the desired data sources (e.g. motion sensors data) and transport channels (e.g. WLAN), and it is forwarded to the IA. Then, the IA

executes the request by acquiring evidence from the SA, only if the configuration request parameters are conformant with the current investigation session permission level. In this way, misuse of evidence collection is avoided. Finally, this activity takes place every time the investigator makes a new request for potential evidence in the context of the same investigation session.

**Process 3: Evidence Collection.** It is triggered every time the SA configuration is altered. Based on configuration attributes (i.e. data source, transfer channel, interception period and duration, etc.) the SA harvests potential evidence, applies integrity mechanisms and forwards them to the evidence transmission process.

**Process 4: Evidence Transmission.** The transmission of evidence takes place, when the collection process ends. It is assumed that an Evidence Transmission Protocol (ETP) is applied between IA and SA. This ETP must include messages for the collection of all smartphone data sources and support the various smartphone transport channels. Furthermore, the ETP must impose security properties, such as message authenticity, integrity, liveness, and confidentiality.

**Process 5: Evidence Storage.** It refers to the storage of potential evidence that is received from the SA in the IA's infrastructure. The preservation of potential evidence in the forensics database must ensure their forensic soundness via employing integrity mechanisms, as well as, their confidentiality. The stored evidence is bound to be revisited during an investigation, so as to be further examined and analyzed before being presented in court. Thus, limited access (e.g. read-only) is provided to the investigator via an interface.

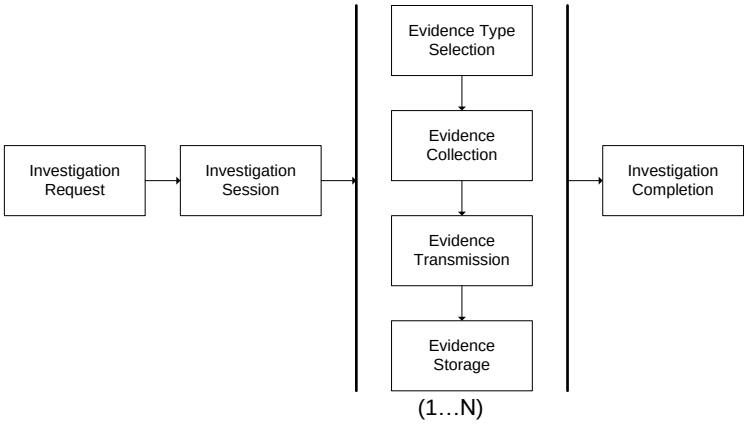


**Fig. 2.** Processes of the Investigation Scheme

## 4 Legal Considerations

A smartphone combines the features of a cell phone along with PC-like functionalities. It permits access to saved and sent messages and files and provides tools for accessing data not presently stored on the device.

Even if some Courts (like the Fifth Circuit) do not recognize any conceptual differences between searching a person's body and searching electronic equipment that this person possesses or carries with him, a smartphone stores and reveals apparently and tremendously more information, thereby providing law enforcement with access to information that a person would never carry in her pocket [4].

A smartphone itself, alone or in its technical networking, can contain personal data to such a degree and in such diversity that it may provide a revealing picture of her personality, and/or facilitate insight even into the core area of private life of a person. With the increasing use of such devices for every kind of communications, including social networking, the importance of digital evidence gathering is increasing as well. A smartphone offers law enforcement authorities "a window into their suspect" not only via hard evidences but also through the character and habit information it may provide [11].

Accessing, searching, and using as evidence the data communicated, accessed or stored by a smartphone, poses new challenges to courts and legislators that are far reaching and go far beyond the secrecy of telecommunications. Neither regulatory regimes concerning the monitoring and recording of communication content, nor rules providing for the retention of external communications data (traffic data) is deemed appropriate and/or sufficient to deal with evidence acquisition for smartphone forensics, as interception refers to the surveillance of a communication taking place between communication partners.

Sensor data or User Input Data could be deemed as biometric data, enabling the collecting of sensitive data and the profiling of the person concerned. Different legal standards and requirements apply to the lawful interception of communications by law enforcement authorities than to the recovery of data stored on a smartphone.

Especially if the data provided by such a device are remotely searched or are not presently stored with the confines of the device, it appears that the acquisition evidence appears to be comparable to a search of premises [19]. The need for review of existing regulatory concepts and converged regulatory regimes in order to face modern converged communication and IT systems in a consistent way is obvious.

The German Constitutional Court has recently (2008) placed strict limits upon the ability law enforcement authorities to remotely access computers, PDAs and mobile phones. The Court has specified the rights to "informational self-determination" and "absolute protection of the core area of the private conduct of life" and has lifted "security and integrity of information systems" as a fundamental right of the user, expressing a right to the unhampered development of her personality in the information era [18]. On the other side it is not clear if the Fourth Amendment of the US Constitution affords reasonable expectation of privacy and protection against unreasonable searches and seizures to a person who uses a smartphone.

Evidence acquisition and surveillance in the digital world need to be adapted to keep pace with technological progress. Legislators have to constantly struggle to keep up with technology and to new risks and challenges. The proposed smartphone investigation scheme is valuable for combating crime and security threats through proactiveness.

Proactive, routine data and preservation reflects the transformation from the traditional constitutional model of gathering conclusive evidence of wrongdoing of suspect individuals toward a model of intelligence gathering where information is collected at random on all users [10].

Both legislators and IT-designers should take care to prevent the deployment of technology that treats all users as potential criminals or suspects without any cause [2].

Therefore, the proposed proactive forensic investigation scheme has been conceived and designed with protective mechanisms in place that hinder investigators or other malicious individuals, from misusing it, and, in a way that allows the acquisition and preservation of data, without infringing fundamental rights.

## 5 Conclusions

Proactive digital forensics is, per se, an interdisciplinary task, requiring the cooperation of computer and law scientists. In this paper, we examined the technological aspects of proactive smartphone digital forensics.

We studied associations between the smartphone data sources and evidence types, as well as the available connection channels in order to deliver potential evidence from a smartphone.

Then, a proactive smartphone forensics scheme was developed. By using this scheme, the appropriate person can collect smartphone data that are essential for combating 'severe' crimes.

We also examined the current legal and regulatory framework concerning ad hoc data acquisition from smartphones. We stressed that even though our proposed investigation scheme can be an essential tool in combating specific types of crime, its application and legality lies clearly with the presence of strong protection mechanisms that ensure its lawful use. Otherwise, this scheme could be used as a tool for profiling or intelligence gathering, thus violating fundamental rights of individuals.

Future work will include the implementation of the proposed scheme with a focus on the Software Agent and the Evidence Transmission Protocol. We also plan to evaluate the implementation performance in real world scenarios, explore alternative misuse avoidance mechanisms and add stealthiness techniques to the agent. Finally, we plan to elaborate more on the proposed taxonomies by identifying subgroups in each smartphone data source and their respective correlations.

**Acknowledgements**

This research has been co-funded by the European Union (ESF) and Greek national funds, through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (Program HERACLEITUS II: Investing in knowledge society through the European Social Fund).

The authors would like to thank Marianthi Theoharidou (AUEB) for her valuable contribution.

## References


1. Blackwell, C.: An Investigative Framework for Incident Analysis. In: Peterson, G., Shenoi, S. (eds.) Advances in Digital Forensics, Part VII, pp. 23-34, Springer (2011)
2. Brown, I.: Regulation of Converged Communications Surveillance. In: Nyeland D., Goold B. (eds.) New Directions in Surveillance and Privacy, pp. 39-73, Willan (2009)
3. European Telecommunications Standards Institute (ETSI): Lawful Interception; Requirements of Law Enforcement Agencies. Technical Specification 101: 331 (2009)
4. Gershowitz, A.: The iPhone meets the Fourth Amendment. Available at http://works .bepress.com/adam_gershowitz/3 (2008)
5. Grobler, C., Louwrens, C., Von Solms, S.: A Multi-component View of Digital Forensics. In: Aleksy, M., Ghernaouti-Helie, S., Quirchmayr, G. International Conference on Availability Reliability and Security (ARES '10), pp. 647-652 (2010)
6. Ieong, S. C. R.: FORZA – Digital forensics investigation framework that incorporate legal issues. Digital Investigation, 3 (Suppl. 1), 29-36 (2006)
7. Lane, N., Miluzzo, E., Ly, H., Peebles, D., Choudhury, T., Campbell, A.: A survey of mobile phone sensing. IEEE Communications Magazine, 48(9), 140-150 (2010)
8. Jansen, W., Ayers, R.: Guidelines on cell phone forensics. NIST Special Publication 800: 101 (2007)
9. Mislan, R.P., Casey, E., Kessler, G.C.: The growing need for on-scene triage of mobile devices. Digital Investigation, 6(3-4), 112-124 (2010)
10. Mitrou L.: Data Retention: a Pandora Box for Rights and Liberties?. In Acquisti, A., De Capitani di Vimercati, S., Gritzalis, S., Lambrinoudakis, C. (eds.), Digital Privacy: Theory, Technologies and Practices, pp. 410-433. Auerbach Publications (2008)
11. Morrissey, S.: IOS Forensic Analysis: for IPhone, IPad and IPod Touch. Apress (2010)
12. Mylonas, A.: Smartphone spying tools. M.Sc. Thesis, Royal Holloway, University of London (2008)
13. Rogers, M., Goldman, J., Mislan, R., Wedge, T., Debrota, S.: Computer forensics field triage process model. In: Proceeding of the Conference on Digital Forensics Security and Law. pp. 27--40 (2006)
14. Sutherland, I., Evans, J., Tryfonas, T., Blyth, A.: Acquiring Volatile Operating System Data Tools and Techniques. SIGOPS Operating System Review., 42(3), 6-73 (2008)
15. Tan, J.: Forensic readiness. @ Stake Technical Report (2001)
16. Thing, V., Ng, K.-Y., Chang, E.-C.: Live memory forensics of mobile phones. Digital Investigation, 7 (Suppl. 1), 74-82 (2010)
17. Walls, J.: Forensic Triage for Mobile Phones with DEC0DE. USENIX Security Symposium (2011)
18. Wiebe, A.: The new Fundamental Right to IT Security - First evaluation and comparative view at the U.S., Datenschutz und Datensicherheit, pp. 713-716 (2008)
19. Wiebke, A.: Agents, Trojans and tags: The next generation of investigators. International Review of Law, Computers & Technology, 23(1-2), 99-108 (2009)
20. Zachman, J. A.: A framework for information systems architecture. IBM Systems Journal, 26(3), 276--292 (1987)