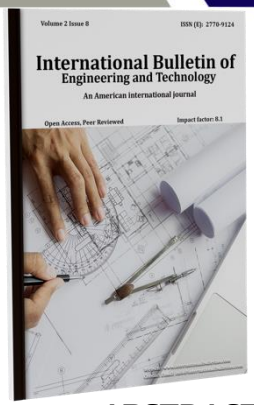

MOBILE FORENSICS - METHODS AND TOOLS APPLIED IN EXPERT EXAMINATION OF MOBILE DEVICES

Gadjiyev Xagani Mokhubbat ogly
Law Enforcement Academy of the Republic of Uzbekistan
Head of the Specialized Center for Digital Research
xagani89@gmail.com
https://doi.org/10.5281/zenodo.13944880

ABSTRACT: This article examines the genesis of methods and techniques for mobile device forensics, and how this field emerged as a distinct area from computer forensics. It provides a list of commercial tools widely used by forensic experts in mobile device investigations and their advantages. The process and sequence of actions an expert takes during the stage of obtaining digital evidence from mobile devices is also discussed.

KEYWORDS: mobile devices, commercial tools, software, object identification, Faraday cage, data collection, analysis.

INTRODUCTION: Currently, mobile phones are one of the technical means most frequently used for illegal purposes. They serve not only as carriers of forensically significant information but also as the subject and instrument of crime

The emergence of mobile device forensics as a distinct field from computer forensics occurred in the late 1990s - early 2000s and was associated with the increasing role of mobile phones in the commission and, consequently, investigation of crimes. With the growing availability and prevalence of mobile phones, along with improvements in their functionality and the number of supported platforms, there was an increased need to develop methods for conducting forensic examinations in general and extracting data from mobile devices in particular. [1]

Analysis of expert practice shows that over 75% in 2020 and over 85% in 2021 of the total number of digital storage devices received by the digital forensics laboratory of the Main Forensic Center of the Ministry of Internal Affairs of the Republic of Uzbekistan were mobile devices.

At the same time, there has been an increase in the number of mobile devices examined in 2022 by 150% compared to 2021. This dynamic is explained by the fact that modern humans are virtually inseparable from a complex of technical devices, which they either carry with them (mobile phones, smartphones, tablet computers and other gadgets) or regularly access (social networks, internet resources).

In the early days of mobile device forensics methods and techniques, specialists used the same approaches as in traditional forensics. Phone content analysis was performed directly through the screen, and important information was photographed. Over time, commercial tools emerged that allowed for recovering the memory of mobile devices with minimal loss, and then studying and analyzing them.

Commercial tools are hardware-software complexes and software widely used in the practical activities of forensic experts in conducting mobile device investigations.

A wide range of solutions for mobile device investigation is offered by companies such as Cellebrite UFED, Final Data (final mobile forensic), HANCOM GMD (md next, md read), XRAY, Oxygen Forensic (Mobile Forensic), Meya Pico, Elcomsoft and others.

Let's consider the universal hardware-software complex UFED 4PC. This complex allows for extracting, decoding and analyzing digital data obtained from mobile devices on an existing PC or laptop. [2]

The complex provides access to tens of thousands of mobile devices, is not difficult to use, has a good interface, and does not require constant technical support. UFED Physical Analyzer processes and analyzes data in real-time, creates compliant reports that can be attached to the expert's conclusion and case materials.

Software from Korean manufacturers Final Data (final mobile forensic), HANCOM GMD (md next, md read) have a very wide range of capabilities in solving tasks in mobile device research. Data extraction using these tools from Samsung, LG, Sky, Huawei, and other mobile phones is positively evaluated. Data processing and analysis are excellently performed with the ability to play recovered files with graphic images and audiovisual data even when the file structure is damaged.

Analysis of the available scientific literature showed that the process of obtaining digital evidence from mobile devices includes seven stages: [3]

1. Presentation of the object for examination. At this stage, the investigative body (inquiry body, court) prepares a resolution on the appointment of an examination, which subsequently enters the expert institution along with the object of study. It is necessary to note the importance of preliminary agreement on the questions posed to the expert for resolution. In addition, it is necessary to make sure that there is no damage to the packaging of the object, as well as the correspondence of the objects presented for examination to those indicated in the resolution on the appointment of the examination.

2. Object identification. The expert entrusted with the examination, after preliminarily photographing the packaging, extracts the object received for study from it. The device extracted from the package is compared with the device specified in the resolution on the appointment of the examination. The manufacturer, model and serial number of the device, IMEI, as well as other features that individualize it (color, body type, damage, etc.) are recorded. The presence of SIM cards and memory cards in the body of the mobile device is established.

3. Preparation for the study. The information necessary for this stage has already been collected by the expert during the identification of the object. Having obtained information about the manufacturer and model, the forensic expert must select the appropriate cable, software necessary for conducting the study, including drivers necessary for the interaction of the mobile device with the expert's workstation.

4. Isolation of the object. Most mobile devices interact with cellular networks and others through Bluetooth, IR port and Wi-Fi module. At this stage, the expert isolates the device from all these networks. This avoids making changes to the data stored in the device's memory, for example, by incoming calls, SMS messages, etc. In addition, some devices support remote access, which the suspect can use to destroy digital evidence, so it is necessary to switch the phone to airplane mode. For these purposes, a Faraday cage (a device for shielding equipment from external electromagnetic fields) or other packaging with shielding of radio frequency radiation can be used, which can enhance the depletion of the mobile phone battery. [4, p.30]

5. Data extraction. After isolating the mobile device from networks, the expert proceeds to direct data extraction and analysis using the chosen software and (hardware-

software complexes). It should be noted that external storage devices (memory cards) should be examined separately, as there is a possibility of making changes to the data stored on it during the examination of the mobile device. When examining memory cards, it is necessary to apply traditional methods of computer forensics, which allow preserving the examined computer information in its original form.

6. Verification of obtained results. Unfortunately, quite often software products intended for forensic examination of mobile devices do not extract data completely. Therefore, verification of digital evidence obtained during the study is an integral part of forensic examination.

7. Preparation of the conclusion. The conclusion should contain: the date and time of the beginning and end of the study; information about the physical condition of the mobile device, photographs of its appearance, stickers with identifying information, as well as SIM card and memory card (if any); information about the state of the phone in which it was received for examination (on/off); information about the manufacturer, model and other identification data of the device; information about the software used in the production of the examination; information about the methods used in the production of the examination; information about the categories of data found during the study and their content.

The conclusions reached by the expert based on the results of the forensic examination should be brief and unambiguous, corresponding to the questions posed to the expert for resolution.

Foreign practice: In a number of countries, such as the USA, Republic of Korea, China, Japan, Republic of Singapore, the forensic examination known to us, including the examination of mobile devices and digital storage media, does not exist as a separate procedural action with certain time limits for appointment, conduct and conclusion.

Such examination has been replaced by continuous support of the process of detection, disclosure and investigation of crimes by specialists in the field of computer (digital) technologies.

For example, the US Department of Justice proposes the following algorithm for conducting digital investigations, which includes the following stages: [5]

- Identification – detection and determination of the type of incident;
- Preparation – preparation and approval of methods, tools, search warrants, obtaining access rights from management;
- Investigation strategy – collection of legally impeccable evidence and minimization of impact on the victim of the incident;
- Preservation – ensuring the protection and isolation of physical and digital evidence;
- Data collection – description of the scene and copying of digital evidence;
- Examination – search for evidence related to the offense;
- Analysis – determining the significance of evidence, reconstruction of data fragments and presentation of conclusions based on them. The analysis phase can be repeated multiple times until the initial assumption is confirmed;
- Presentation of results – summarizing and presenting the findings of the investigation;
- Return of evidence – ensuring the return of digital and physical evidence to their rightful owner.

In the Republic of Korea, at the National Digital Forensics Center under the Prosecutor General's Office, employees develop not methods of crime investigation and examination, but algorithms for forensic support, i.e., special systems and software that guarantee constant access of the investigation subject to digital analysis. [6]

Algorithms and programs automatically detect and record traces during the commission of various types of crimes through automatic study of malicious program activity, logs, networks, big data. Accordingly, information collection and documentation is carried out not by a person, i.e., a specialist, detective, police officer, prosecutor or investigator, but by specialized software (SW), essentially a digital robot. Based on the analysis of the collected information, the investigation team or detectives receive the necessary data according to a given combination and analysis criteria, which can be used not only for investigating a specific act but also for detecting and preventing crimes in general. [7, p.69]

Despite the fact that the aforementioned models were initially oriented towards working with computer systems, they contain key points that should be considered when working with mobile devices as well.

CONCLUSION: In conclusion, it should be noted that both in foreign practice and in the Republic of Uzbekistan, the process of obtaining digital evidence from mobile devices is carried out through commercial tools, which are hardware-software complexes and software widely used in the practical activities of forensic experts in conducting mobile device investigations. In this regard, it is necessary to constantly develop new types of expert research on mobile devices, establish close cooperation with countries that have rich experience in investigating incidents related to mobile device research, participate in projects for exchanging experience and conduct joint research on developing unified theoretical foundations for this type of examination.

References:

1.Рязанкина Н. Экспертиза мобильных устройств: Принципы и методы // Безопасность информационное обозрение – [Электронный ресурс]. – Режим доступа: http://securityinfowatch.ru/view.php?section=articles&item=565. – Дата доступа: 07.10.2021.

2. Аппаратно-программный комплекс для съема и исследования данных из мобильных устройств UFED 4PC – [Электронный ресурс]. – Режим доступа: http://aimtech.ru/catalog/154. – Дата доступа 07.07.2021

3. Михайлов И. Основы криминалистического исследования мобильных устройств – – [Электронный ресурс]. – Режим доступа: https ://www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv. – Дата доступа: 08.07.2021.

4.ISO/IEC 27037:2012, MOD Государственный стандарт Республики Узбекистан // Методы обеспечения безопасности. Руководящие указания по идентификации, сбору, получению и сохранению цифровых доказательств. – 2017. – С. 30

5. Рязанкина Н. Экспертиза мобильных устройств: Принципы и методы // Безопасность информационное обозрение – [Электронный ресурс]. – Режим доступа: http://securityinfowatch.ru/view.php?section=articles&item=565. – Дата доступа: 08.07.2021.

6. Университет Корё — Korea University — частный исследовательский университет [Электронный ресурс]. – Режим доступа: https://www.unipage. net/ru/korea_university (дата доступа: 09.07.2021).
7.Кучин О.С. Электронная криминалистика: Миф или реальность // Сетевое издание «Академическая мысль». – 2019. №3 (8). – С.69