A STANDARD METHODOLOGY FOR EXAMINING INFORMATION STORED ON MOBILE DEVICES AND THEIR COMPONENTS

Olga Tushkanova

Methodologies and methodological guidelines in forensic science

Methodology – a formalized algorithm of the expert's actions, ensuring the reproducibility and reliability of the results. It includes the stages of preparation, execution and evaluation of results, as well as requirements for the tools and the conditions of the examination

- Methodological guidelines – advisory documents that explain and help apply forensic methodologies, equipment, etc.

Historical background

- …
- Methodological guidelines on the forensic examination of cellular mobile phones in the bodies for control over the trafficking of narcotic drugs and psychotropic substances (2011, FSKN, FOUO);

- Standard methodology for examining information contained in mobile phones (2014, EKC MVD of Russia);

Examining information contained in mobile phones: Standard methodology (2023, EKC MVD of Russia);

- Standard methodology for the forensic examination of information contained in mobile devices and their components (2025, Investigative Committee of Russia)

What's new?

- mobile phones —> mobile devices:
  - keypad mobile phones;
  - smartphones;
  - tablet computers;
  - smartwatches and smart bands

  the section on the objects of examination has been reworked, including the addition of a description of data encryption technologies
- the requirements for the equipment used to conduct the examination have been clarified

Equipment requirements (expert's workstation)

- have various interface and technology connectors, specialized devices (e.g. a Bluetooth adapter, a Wi-Fi adapter, etc.), interface cables for connecting mobile devices, SIM cards, memory cards, etc.;
- have equipment for working with information on storage media;
- have the ability to block registration of mobile devices in cellular networks;
- have the ability to supply power to batteries and to the mobile devices themselves (e.g. a universal power supply unit);
- have the ability to remove memory chips from mobile devices;

Equipment requirements (expert's workstation)

- have the ability to read SIM card memory and to write identifiers to SIM card memory;
- have the ability to decode the user partitions of mobile device memory;
- have SIM cards that are not registered by cellular operators;
- have an ultrasonic bath and drying equipment (optional);

have the ability to search and interpret information obtained from the memory of mobile devices, memory cards and SIM cards;

- have the ability to video-record actions performed by the expert during the examination;
- have the ability to document the examination results and prepare report files.

Recommendations on diagnosing faults in a mobile device and restoring it to working order

- the device does not power on;
- the image on the display is partially or completely absent;

the device does not respond, or responds incorrectly, to the control buttons;

- no response from the device to touchscreen input;

- **no communication with the device through the connection port, including when the device fails to initialize in the operating system of the bench equipment**

What's new?

- the examination procedure has been made more specific and expanded, including:
  - measures ensuring the preservation and integrity of the information contained in the memory of the mobile device and its components (software /hardware, for powered-on or powered-off devices);
  - recommendations on diagnosing faults in a mobile device and restoring it to working order;
  - measures for establishing the password (code) for the device and the PIN and/or PUK codes for the SIM card(s);

Types of motions

- for provision of the password value for access to the mobile device's memory;
- for provision of the PIN and/or PUK code values for access to the SIM card(s) memory;

for the device's user to be present at the forensic examination in order to pass biometric identification

Methods and stages of extracting information from mobile device memory

- methods:
  - low-level extraction (full file system access);
  - extraction of publicly accessible data
- stages:
  - powering the device on/off;
  - photographing/video-recording the screen;
  - connecting the device via a connecting cable or wireless interfaces to the expert's workstation;
  - establishing (initializing) the connection between the mobile device and the expert's workstation;
  - putting the device into a service mode (using test pads and/or the device's buttons);
  - installing an agent program;
  - downgrading the operating system and software version;

What's new?

- the examination procedure has been made more specific and expanded, including:

  measures ensuring the preservation and integrity of the information contained in its memory and components (software /hardware, for powered-on or powered-off devices);

  - recommendations on diagnosing faults in a mobile device and restoring it to working order;
  - measures for establishing the password (code) for the device and the PIN and/or PUK codes for the SIM card(s);

  methods and stages of extracting information from mobile device memory;

  a glossary of key terms and definitions;

  - etc.

What's new?

- the procedure for writing the sought information to rewritable storage media has been regulated:

If the results of the examination are written to a solid-state drive or an external hard disk drive, then the explanatory label and the expert's signature are put on adhesive paper tape attached to a part of the drive that has no identifying features. A corresponding entry is made in the research section of the expert report, stating the identifying features of the storage medium - (make, model, serial number, etc.), the size of the written information in bytes, the cryptographic hash value of the information written to the storage medium

What's new?

- the situation where the objects under examination contain authentication data for cloud services and storage has been resolved:
- establishing the presence of files containing authentication data for cloud services and cloud storage (“tokens”) is a stage of the information examination;

“If the mobile device's memory contains files with authentication data for cloud services (so-called ‘tokens’), internet resources (social networks, email, etc.), immediately send a notice about this to the investigator, attach this information to the expert report and note the possibility of extracting data from cloud services later on, in the course of investigative actions”;

What's new?

- a recommendation has been given on correcting errors in the questions put to the expert:

"if the questions put to the expert contain semantic, stylistic, lexical, syntactic, spelling or similar errors, in the introductory part of the expert report the wording of the questions to be resolved by the expert may be edited, indicating the reasons for making the corresponding changes"

By decision No. 13 of 26.06.2025 of the meeting of the Scientific and Technical Council of the Investigative Committee of the Russian Federation, the Standard methodology for the forensic examination of information contained in mobile devices and their components has been approved and recommended for publication and for distribution for practical use to the forensic units of the Investigative Committee of Russia, the EKC MVD of Russia, the RFTsSE of Russia and the TsST FSB of Russia, as well as for posting on the closed portal of scientific and methodological support

https://sovetnik.sledcom.ru/