Whitepaper

THE POSSIBILITIES OF MOBILE FORENSICS: EXTRACTION, INVESTIGATION, AND CRIME SOLVING

CONTENT

What is Mobile Forensics?

Mobile forensics is the science of recovering digital evidence from mobile devices.

Most people use mobile devices in their daily lives: mobile phones, smartphones, tablets, MP3 players, smartwatches, fitness bracelets, and more. Currently, most mobile devices run on the Android or iOS operating systems.

Mobile devices contain more personal data and other information about their owners than computers and laptops.

They contain the following main types of forensic artefacts: contacts (phone book), calls, text messages, MMS messages, chats, emails, multimedia files (graphics, videos), geolocation data, documents, installed applications, malware, and other artefacts that may point to:

- The presence of malware on a mobile device;
- Unauthorised access to a mobile device;
- Payment orders being sent from the device, data compromise, etc.

In digital forensics, the study of mobile devices is treated as a separate field for the following reasons:

- **Mobile devices have their own hardware solutions, different from those used in computers**
- **They have their own operating systems (Android, iOS, Blackberry OS, Windows Mobile), different from those used on servers, personal computers, and laptops**
- **They have their own system and application software**

Types of Extractions

These methods differ with regard to the amount of recoverable data and the complexity of the work required to extract the information from the mobile device. For different mobile devices (depending on the device hardware architecture, system software, security settings, etc.), one or several data extraction methods can be used.

There are several basic types of data extraction from mobile devices. Conventionally, they can be divided into four groups:

- Logical extraction
- Creating a backup copy of your mobile device
- Retrieving the file system of the mobile device
- Retrieving the physical memory dump of the device

16% OF PEOPLE

over 16 years old have broken their mobile device (most often, a smartphone).

25% OF DAMAGE

to all mobile devices is due to water damage.

10 WEEKS

is the average time after which an iPhone malfunctions after being purchased.

19%

of all damaged mobile devices are dropped in the toilet.

EXTRACTION TYPE	DESCRIPTION OF THE METHOD	EXTRACTED DATA	FEATURES OF THE METHOD
Logical	Only the main types of data explicitly available on the device are extracted from the device (an exception are databases in SQLite format, deleted records of which can be recovered)	It is possible to recover deleted: **Contacts, Calls, Text messages, MMS messages.** And to extract: **Multimedia files (graphics, video), Documents, Geolocation data.**	Using this method, it is possible to establish instances of unauthorised access to data stored on the mobile device and retrieve any sent (and received) text messages regarding payment transactions (e.g. containing a verification code or payment information) made using the mobile device being investigated.
Create a backup copy of the mobile device	Additional artefacts, specific to given device models, can be extracted together with the main artefacts. Extracting certain types of data is possible only with the appropriate operating systems settings. For example, you can view emails on an iPhone, but not export them. Similarly, you cannot extract applications from an iPhone that has not been subject to jailbreaking, which makes it more complicated to detect malware on such devices.	It is possible to recover deleted: **Contacts, Calls, Text messages, MMS messages, Chats*, Emails, if the messages are stored in an SQLite database*.** And to extract: **Multimedia files (graphics, videos), Documents, Geolocation data, Installed applications*.** ** types of data that can only be extracted with the appropriate operating system add-ons*	Using this method, it is possible to establish instances of unauthorised access to data stored on the mobile device and retrieve sent (and received) text messages regarding payment transactions (e.g. containing a verification code or payment information) made using the mobile device being investigated. In certain cases, it is possible to determine the malicious mobile applications that were installed on the mobile device as well as their features.
Retrieve the mobile device file system	When extracting the file system, the maximum number of logical artefacts (including emails, chats, etc.) is extracted. Similarly to logical extraction methods and mobile device backups, it is impossible to restore deleted files using this method.	It is possible to recover deleted: **Contacts, Calls, Text messages, MMS messages, Chats.** And to extract: **Multimedia files (graphics, videos), Documents, Emails, Geolocation data, Installed applications.**	Using this method, it is possible to establish instances of unauthorised access to data stored on the mobile device and retrieve sent (and received) text messages regarding payment transactions (e.g. containing a verification code or payment information) made using the mobile device being investigated. Similarly, it is possible determine the malicious mobile applications that were installed on the mobile device, as well as their features.
Retrieve a physical device dump	This extraction method creates a complete copy of the device's physical memory; it is possible to recover both the maximum number of the different mobile device artefacts and all deleted files.	It is possible to recover deleted: **Contacts, Calls, Text messages, MMS messages, Chats.** And to extract: **Multimedia files (graphics, videos), Documents (including deleted ones), Emails, Geolocation data, Installed applications.**	Using this method, it is possible to establish unauthorised access to data stored on the mobile device and retrieve sent (and received) text messages regarding payment transactions (e.g. containing a verification code or payment information) made using the mobile device being investigated. Moreover, it is possible to determine the malicious mobile applications that were installed on the mobile device and their features, as well as recover deleted files and other artefacts pointing to the occurrence of information security incidents through the use of the device being investigated.

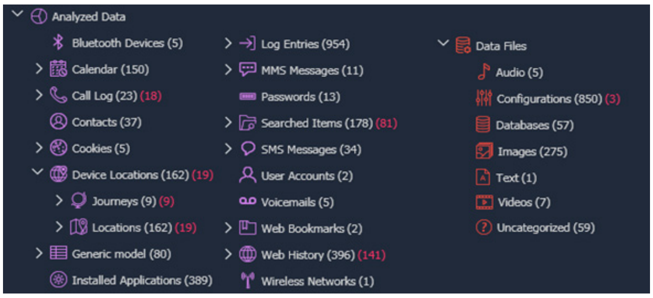
The maximum number of forensic artefacts can therefore be extracted from the device using the method of creating a physical dump of the mobile device. However, this method cannot be used in the case of flagship models of Android devices (starting with Android 6) and iOS devices (starting with versions above 9.3.5). These devices use an additional measure to protect the owner's personal data: encryption, which makes it impossible to recover deleted files and makes it significantly more complicated to retrieve information. Nevertheless, in such cases it is possible to assess what data was stored on the device. This means that if graphic files and videos are deleted, it is impossible to restore the deleted files; it is possible, however, to extract thumbnails of such files from the device's memory and assess the images it contained.

Group-IB Mobile Forensics Services

Retrieval of data from locked devices

A common request made by customers is to retrieve data from a locked device (using the pin code or pattern lock). Group-IB's Computer Forensic Lab specialists are able to extract data from virtually **any device, including encrypted ones.**

Moreover, this service is available for flagship mobile devices running on the Android or iOS operating systems.



- Analyzed Data
  - Bluetooth Devices (5)
  - Calendar (150)
  - Call Log (23) (18)
  - Contacts (37)
  - Cookies (5)
  - Device Locations (162) (19)
    - Journeys (9) (9)
    - Locations (162) (19)
  - Generic model (80)
  - Installed Applications (389)
  - Log Entries (954)
  - MMS Messages (11)
  - Passwords (13)
  - Searched Items (178) (81)
  - SMS Messages (34)
  - User Accounts (2)
  - Voicemails (5)
  - Web Bookmarks (2)
  - Web History (396) (141)
  - Wireless Networks (1)
- Data Files
  - Audio (5)
  - Configurations (850) (3)
  - Databases (57)
  - Images (275)
  - Text (1)
  - Videos (7)
  - Uncategorized (59)

Figure 1. Example of types of data retrieved from a locked iPhone (the red colour indicates the amount of files recovered).

Retrieval of data from damaged devices

Employees of Group-IB's Forensic Laboratory are able to recover data from almost any damaged mobile device. Exceptions include:

- Devices with destroyed or missing memory chips
- Mobile devices running on iOS or Android operating systems with a damaged electronics board
- Other smartphone models

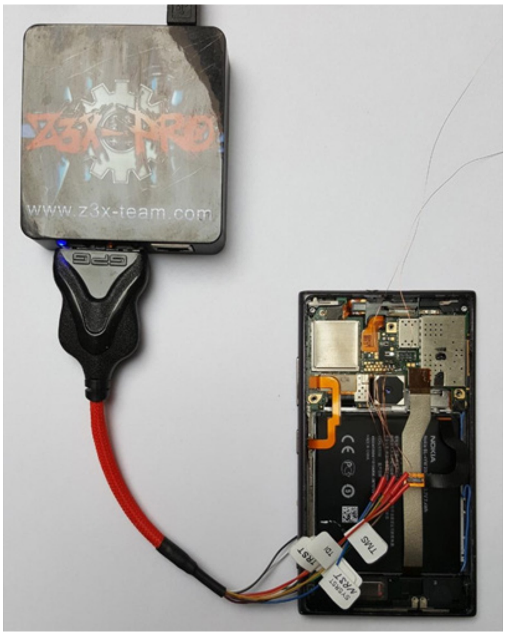


Figure 2. Retrieval of data from a damaged smartphone

Forensic analysis of mobile devices

Forensic analysis of mobile devices makes it possible to extract the maximum possible number of artefacts (depending on the investigation method used).

Law enforcement agencies and private laboratories often do not have the equipment and qualified staff required to ensure that all information is retrieved from the mobile device. As a result, the customer (or law enforcement agency) does not have all the information about the incident and therefore has an incorrect idea of the reasons behind it.

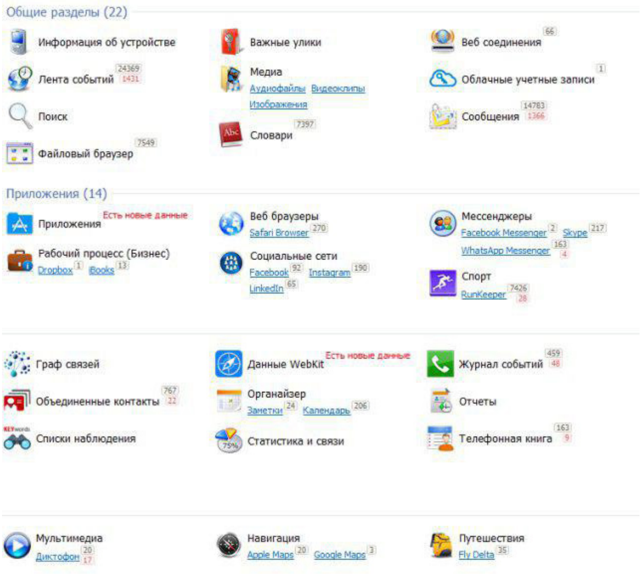


Figure 3. Example of types of data retrieved from a mobile device. The red colour indicates the recovered files for each type of data.

Search for malware and tracking software

Group-IB's Forensic Laboratory experts are able to detect such programs, determine their functions (what information the program collects from the device and where it sends that information), and record instances of unauthorised access to customer data.

A malware program (e.g. a banking trojan) does not need to be authorised as the superuser of a mobile device to operate.

The main sources of infections of mobile devices are:

- Fake applications
- Compromised websites
- Chats and social networks
- Emails
- Close relatives (who might install a monitoring program obtained from an unreliable source, which could infect the device with malware)

Examples of Group-IB cases

Case 1. Cyber fascists, or the 5th Reich

Several private individuals who had experienced unauthorised withdrawals of funds from their bank accounts asked for Group-IB's assistance. While studying their smartphones, a malicious mobile application was discovered that replaced the Google Pay program screen, instead displaying an interface similar to the Google Pay app. The device owners would enter their bank card data (card number, owner's name, expiration date, CVV code) into the appropriate fields of this interface and the information would then be transmitted to the attacker's server.

All the programs had similar features and programming styles. The investigation helped identify hackers who were members of the 5th Reich group; they were subsequently detained by law enforcement officers.

Case 2: Suicide in a military unit

In a military unit, the corpse of a soldier was found; he had committed suicide. The investigation's initial hypothesis was that he had been incited to suicide by his fellow soldiers. It was impossible to access the data stored on the deceased's smartphone as the device was locked with a password. After unlocking the smartphone and extracting data from it, Group-IB experts discovered the cause of the suicide: the soldier had been blackmailed by third parties, who threatened to spread compromising information about him.

Case 3: Investigation into a business partner

One of our customers suspected that his partner was deceiving him about his location at certain times. While investigating the partner's mobile device, our experts discovered a fitness application that was tracking the device location every two seconds. Analysis of the device's movements showed that there were no discrepancies between the partner's claims and the data on his device.

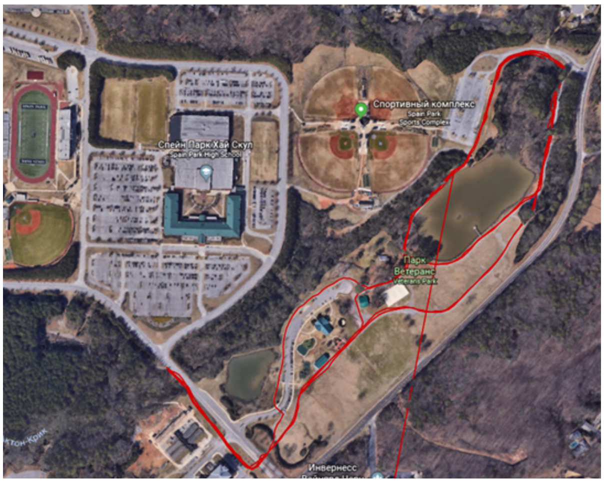


Figure 4. The mobile device's motion data recorded by the fitness app and other geotags extracted from the device memory.

About Group-IB

Group-IB is one of the world's leading developers of solutions for cyber-attack detection and prevention, fraud detection, and protection of intellectual property online.

17 years of hands-on experience	**1,200+** cybercrime investigations worldwide	**$300 mln** was returned to a client company as the result of our efforts	**65, 000+** hours of incident response

Group-IB's security ecosystem provides automated tracking of malicious activities, extraction and analysis of threat data, mapping of adversaries' infrastructure and enrichment of their profiles. Our top-tier experts relentlessly reinforces our technologies with insights "from the battlefield".

Group-IB Products

- **Threat Intelligence & Attribution**
- **Threat Hunting Framework**
- **Fraund Hunting Platform**
- **Digital Risk Protection**

INTERPOL | EUROPOL

Official Europol and Interpol partner

IDC | GARTNER | FORRESTER

Group-IB is ranked among the best Threat Intelligence vendors in the world, according to IDC, Gartner and Forrester

OSCE

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

PREVENTION

- Penetration Testing
- Red Teaming
- Security Assessment
- Incident Response Readiness Assessment (Pre-IR)
- Compromise Assessment
- Compliance Audit

RESPONSE

- Incident Response Retainer
- 24/7 CERT-GIB
- Incident Response

INVESTIGATION

- Digital Forensics
- Investigation
- eDiscovery
- Financial Forensics

EDUCATION

- Incident Responder
- Malware Analyst
- Digital Forensics Analyst
- Threat Hunter

Contact us to learn more

info@group-ib.com **www.group-ib.com**

GROUP-IB