Whitepaper

eDiscovery: Basics, Methods and Techniques of Strategic Digital Evidence Management
eDiscovery

CONTENT

What is eDiscovery? .................................................................................................................. 3

eDiscovery’s primary goals ...................................................................................................... 3

Why is eDiscovery important? .................................................................................................. 4

Model of detection and consolidation of electronic evidence .................................................... 5

Result presentation formats ....................................................................................................... 6

Group-IB eDiscovery cases ...................................................................................................... 8

About Group-IB ........................................................................................................................ 12
What is eDiscovery?

**eDiscovery (Electronic Discovery)** is the process of identifying, consolidating and formatting digital evidence in compliance with legal requirements, analyzing it and presenting in court.

Typical eDiscovery objects include emails, database information, voice-mail messages, chat information from instant messaging programs, image files, video files, and information from social networks.

---

**eDiscovery’s primary goals**

The goal of eDiscovery is to facilitate the cooperation of technical experts who are responsible for the investigation of digital evidence with the client and his lawyers:

1. Technicians ensure that digital evidence is secured so that the opposing side of the lawsuit has no grounds to claim that evidence was somehow altered, planted, or destroyed while it was being obtained, or that it was obtained in violation of procedural rules.

2. The digital evidence being sought is often found in a vast array of poorly structured data from various sources: on company servers, in clouds, databases, archival copies of data, IoT devices, etc. It is almost impossible for an unprepared lawyer to find the required data by working with such sources.

   **Technicians help select only the information that the client or his lawyers are interested in from this mass of data. Thus, they help the company to reduce the time it spends conducting an audit or internal investigation.**

3. Lawyers, judges, and attorneys are not experts on technical terminology. The task of specialists is to explain to them the essence of the processes and methods used to identify, consolidate, format in compliance with legal requirements, and extract digital evidence, as well as the importance of the identified information, in a way that they will understand.
Why is eDiscovery important

Human activity in the modern world, whether we like it or not, gives rise to a huge number of digital traces. In one way or another, these traces can be detected and procedurally consolidated by technical experts for further use by the client or his attorney during court proceedings.

eDiscovery provides secure and instant access to a client’s business information in accordance with a strict access model, with the ability to search, view, and analyze data. It also consolidates identified documents that are relevant to the client’s request, and formats them in compliance with legal requirements.

As part of the eDiscovery process, technicians help to:

- Detect these traces, consolidate and format them in compliance with legal requirements, and analyze them
- Evaluate and prepare the materials for presentation in court
- Develop a model for the correct presentation of the collected digital evidence in court, provide legally valid arguments, and build a line of defense using the identified data and documents
Model of detection and consolidation of electronic evidence

eDiscovery refers to the use of a combination of processes and technologies and includes nine basic steps

**STAGE 1**
Preparatory stage
At this stage, the client’s policies, procedures, and processes of electronic circulation are studied. The range of sources involved in the client’s information processes is determined: workstations, servers, clouds, mobile devices, storage systems, virtual storage, etc.

**STAGE 2**
Identification
At this stage, experts look for sources that could potentially contain data relevant to the client’s request.

**STAGE 3**
Protection of information
After identifying potential information sources, experts conduct procedures to protect information stored on them from accidental or intentional changes, damage, or destruction.

**STAGE 4**
Collection of information
Information is collected from the client’s sources, and the procedures performed are recorded and formatted in compliance with legal requirements. In addition to the most relevant information, there is a collection of metadata, such as creation dates, file sizes, and cryptographic hashes. This data allows us to further confirm that the collected information has not been modified.

**STAGE 5**
Data processing
The processing stage includes the preparation of the collected information for analysis and the performance of such analysis. As a rule, information processing is performed by special forensic software. During processing, files can be extracted from directories and forensic copies, while irrelevant files, system files, and duplicates may be deleted. Information can be converted to a format more convenient for viewing by the client and the client’s lawyers.

**STAGE 6**
Assessment of the results
Specialists in computer forensics, together with the client or his lawyers, analyze the results obtained in order to identify the relevant, non-relevant, and most important results and documents obtained during the previous stage. Artificial intelligence is increasingly being used to speed up such analysis.

**STAGE 7**
Analysis
This stage is a variation of the sixth stage, aimed at a deeper search for content and context in the analyzed information and documents, and includes using search patterns, key topics, and data about people, as well as discussing the obtained results.

**STAGE 8**
Preparation
The documents and information that will be used as potential evidence by the client and his lawyers are identified, and the documents are prepared for the client.

**STAGE 9**
Presentation of results
Presentation of the results of analysis to the client and his lawyers.
Result presentation formats

During the execution of eDiscovery, the results of the work of specialists can be presented in the following formats:

**Graphic format**
Identified files are converted to graphic files, usually in .tiff format.

**Native format**
Files are saved in the format in which they were originally created. For example, a .docx format document is saved as a .docx file; an email contained in an .eml file is saved in the same .eml format, etc.

**Similar format**
Files are extracted or converted to another format, which displays the data as similarly to the native format as possible. This is done because specialized software is required for data display. This also makes it convenient to search for information (with keywords or using special requests).

For example, information from emails is saved in .htm, .mht or .rtf format, and databases are saved as text files or .csv files.

**Paper format**
All electronic evidence found is printed on paper.
Frequent cases

One common type of eDiscovery case is determining the actions taken by an employee preceding dismissal: what documents he deleted or transferred to external drives, and whether he sent confidential company documents to a personal email address.

Even when an employer has complete information about a former employee’s embezzlement of confidential documents constituting company trade secrets (for example, if the employer can get this information from the company’s DLP system), the information still must be consolidated and formatted in compliance with legal requirements to make it possible to press charges against the former employee.

Typical cases in which this service is required are:

- Verifying the content of an individual chat;
- Verifying site content;
- Establishing the fact that an email was sent or received;
- Determining whether a document was edited on a specific computer and determining the history of its editing;
- Tracking the Internet history of a computer or laptop user;
- Establishing a sequence of actions performed by a computer or laptop user.
eDiscovery: Group-IB cases

Case No. 1. “Dishonest worker”

A large industrial robot production company, a market leader with more than 2,000 employees

Situation

The company suspected one of its former employees, who occupied a management position, of stealing information constituting trade secrets – specifically, technical documents for equipment produced, information about regular customers, etc. Suspicion of theft arose from the fact that the former employee created his own company with a similar profile of work, and customers switched to this new company from our client.

The following were submitted for investigation: the former employee’s office laptop and smartphone.

Actions

While working on this case, Group-IB experts discovered digital traces in the devices under investigation, indicating the copying to external USB drives of documents constituting the client’s trade secrets and technical documentation. There were also six instances of the client’s technical documentation being sent from the former employee’s work email address to his personal mailbox, which was located on a free mail server.

Result

Analysis of the former employee’s emails revealed that three emails had been sent from his work email to his personal email, with attachments containing trade secret information. The electronic evidence identified was consolidated and formatted in compliance with legal requirements, which allowed the client company to file a claim in court against the former employee to recover their losses.

Emails sent from the employee’s mailbox to his personal mailbox
Case No. 2. “A dishonest employee of an insurance company”

Client Profile

One of the Top-10 Russian insurance companies, a large company with more than 10 regional offices located throughout the country

Situation

The head office of the insurance company received a statement from a regional division about the reimbursement of a Casco insurance policy due to a car being irreparably damaged in an accident. The cost of compensation was several million rubles. The employee whom the client assigned to investigate the materials produced by the insurance case suspected that the photographs of the car for which payment was issued were fake.

Actions

During the investigation, conducted by an expert from Group-IB, these photos and the insurance agent’s laptop were studied. Studying the timestamps of the files revealed that these photos were taken after the accident had occurred (that is, photos were taken of another car of similar make and color, and the insurance claim itself was backdated).

Result

The evidence collected allowed the insurance company to contact law enforcement authorities regarding the employee’s fraud.
Case No. 3 “Theft of intellectual property”

**Client Profile**
A transnational IT company with more than 8,500 employees, which provides more than 50 services in the Internet space

**Situation**
The company had an incident involving the leakage of confidential data. The client’s DLP (Data Leak Protection) system recorded an instance of information containing the company’s trade secrets being transferred through the network.

**Actions**
A Group-IB expert went to the client and made a copy of the suspect’s HDD, downloaded the DLP logs and interviewed employees. While investigating the HDD and DLP logs, we discovered the following:

An employee, Smith (not his real last name), used cloud storage service Dropbox to store commercially sensitive files. Smith provided his friends with access to this cloud storage, thereby illegally distributing the data.

The correspondence found on the disc made it possible to establish that Smith, together with friends, established a company whose main activity was to provide premises for rent in the Moscow area. Using illegally obtained information, namely ranking algorithms, they promoted their company’s site to first place in search results. Smith and his associates knew at this time that they were breaking the law.

**Result**
In the course of further investigation, experts identified a criminal group that had used the client’s intellectual property for personal gain. This proved Smith’s direct involvement in the transfer to third parties of information constituting a trade secret. Searches were conducted of the defendants, information carriers were seized, and subsequent investigation confirmed and supplemented the initial findings.

As of this writing, Smith has been convicted.
Case No. 4. “Internal investigation”

**Situation**
A group of employees at a large regional bank planned to steal money by imitating a hacker attack. They carried out most of their discussion of preparations for the attempt using corporate email.

**Actions**
Our experts downloaded and analyzed the mail database of the bank’s mail server. During the investigation, the emails sent by these employees were separated out. Big Data techniques allowed all the bank employees involved in the incident to be identified.

**Result**
The evidence discovered was consolidated and formatted in compliance with legal requirements, which allowed the management of the bank to move forward and contact law enforcement agencies.
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.

Group-IB’s 17 years of experience manifest in the cyber threat early detection system — a line of high-tech products for monitoring, detecting, and preventing cyber threats based on the most current cyber intelligence data and in-depth analysis of real hacker attacks.

<table>
<thead>
<tr>
<th>17 years</th>
<th>1,200+</th>
<th>65,000+</th>
<th>500+</th>
</tr>
</thead>
<tbody>
<tr>
<td>of hands-on experience</td>
<td>investigations around the world</td>
<td>hours of incident response</td>
<td>experts and developers</td>
</tr>
</tbody>
</table>

Group-IB Products

- Threat Intelligence & Attribution
- Threat Hunting Framework
- Fraud 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)

Security & Risk Assessment

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

Incident Response & Threat Hunting

- Incident Response Retainer
- CERT-GiB
- Incident Response

Forensics & Investigation

- Digital Forensics
- Financial Forensics Investigation

Education

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

Contact us to learn more about eDiscovery services