5.8. Digital Traces

In criminalistics any changes in the material environment produced as a result of the crime commission are considered as traces. In terms of criminalistics, traces cover the who les cope of the obtained information, which is used to carry out search operations, formulates each and other hypotheses, determine the direction of the investigator's activity. However, the current traditional classification of traces in criminalistics does not cover the types of traces that emerged as a result of new types of crime involving computer (information) technologies.

Digital traces are a new object of criminalistic research, and digital technology as a means of crime and trails-forming object attaches this information significance as a source of evidence. Computer technology, information technology and some software product scan be used as a mean sofcommitting crimes, and subject of criminal offence.

The nature of trails in the crime pattern involving the use of information technology depends on the methods of the crime commission and characteristics of electronic means applied for the criminalistics.

In the last 5-10 years, digital technology has almost completely replaced the analog one. In view of this, law enforcement bodies, nowadays, mostly focus on digital traces.

Digital traces comprise any forensically significant in formation in the digital form. These are material in visible trails, which represent data recorded in the digital form on material carriers.

A digital trace is a system of specific information elements that can be recorded on one or several digital media. The digital traces media can be simultaneously connected to several digital devices integrated into a telecommunications network.

The mechanism of forming digital traces is based on electromagnetic interactions of two or more material objects, each of which is a combination of a digital device (a set of devices) and a control system (a set of software products). Objects that form and perceive trails, as well as the information contained in them (digital traces) have an objective form of existence.

The traces of one objective form of existence of digital information impacting another can be identified, documented and studied only with the help of specific digital devices. In a similar way, an objective form of the existence of trails of the effect of high temperature on the knife blade can be identified and studied only with the help of special metallographic microscopes.

The principal objects that form and perceive digital traces are computer data carriers, integrated microcircuits, microcontrollers, computers and their systems, telecommunications network equipment, digital cameras and dictaphones, devices for reading information from plastic bank cards, mobile phones etc.

Along with recording digital traces related to the crime event, some electronic modules of these items allow experts to establish the place and time of the device making specific traces. For example, with the help of a geolocation system in real time, you can get information about the exact location of a computer, tablet or phone and, accordingly, identify the person who owns it.

Geolocation data can also be used to establish the simultaneous presence of two or more persons in one place, and repeated establishment of such facts indicates the interaction of the person under surveillance with specific people.

Processing digital traces, the following specific features of digital information should be taken into account: the impossibility of its detection, recording and research without the use of digital technology; the absence of an inextricable connection with the material carrier and the possibility of transferring digital information to another medium; dynamism, the ability to instantly change location with modern digital means of communication (e.g. move from one part of the globe to another); the possibility of instant changing and destroying any amount of information (for example, through remote access); identity of the original and all subsequent copies of computer information (regardless of the type of media).

To date, a significant number of effective modern means of searching for digital traces and restoring damaged electronic information have been developed. The most complete evidence base can be formed by means of involving experts in the field of information technology for detecting and recording digital traces.

The traces of destruction, modification, copying of information, blocking the information system are the results of impacting computer information through an external access to it. The traces of such actions remain on digital information carriers and reflect the effects on databases, computer programs, text and other files.

The information can bear the traces of its partial destruction or modification (removal of file names from catalogs, addition or deletion of individual records, physical destruction or demagnetization of digital information carriers, etc.). Traces of an unauthorized access to information can also be found on the Internet, and the hardware (computer, network equipment) used to commit the offence can be identified.

Expert examination of computers and network equipment, operating system protocols, applications, antivirus programs, program code, etc. is carried out to detect such traces.

When examining computer equipment, its could be considered, that the user's time in the network can be established by special log-files (logs). Additional in formation on the type, order and time of connection of the user to the Internet is a convincing proof of an unauthorized access to a certain computer system.

Traces of an unauthorized access to the information contained in the «victim» computer can be found in the operating system log and in specific software products. The computer memory contains backup copies of the created, sent and received files, and also there are files-reports on working with them.

Traces that indicate an unauthorized access to computer information include the following: renaming directories and files, changing the size and contents of files, creating new directories, changing file attributes (for example, author's name, time of creation and editing), etc.

Important information can be obtained by studying the data of electronic correspondence and messaging services (Short Messaging Service). The attributes of e-mail files contain information about the date and time they were sent, the sender's electronic address, the name and address of the Internet provider, and other information. Phone calls from a mobile phone and texts of SMS-messages are automatically recorded and accumulated on the server of the mobile operator. Such digital traces allow us to establish important evidentiary information.

Social networks (for example, Facebook, Twitter, Linkedln, Instagram, etc.), providee-trails in the form of messages and comments left by the individuals under surveillance, the irpersonal data (e.g. email address), photo sand videos, the history of search queries. These tracks also contain information about the time of visiting the site.The user's e-mail address in some cases helps to identify his/her phone number, date of birth, place of work and residence, determine the circle of contact sand interests.

In the last 2-3 years there has been a rapid growth of offences in remote banking services (RBS). RBS is a set of services for remote access of customers to banking services, which allows them to remotely (without a visit to a bank) manage their financial matters using information technology. RBS systems are divided in to the following types: «Client-Bank» system (PC-banking, remote banking, direct banking, home banking); Internet banking; mobile banking. The fraudulent scheme of money theft consists of three main stages: obtaining confidential information about the user (login, password, bank card data, signature keys, etc.), performing financial transactions on behalf of the user using his authorization data and electronic protection keys, receiving financial resources.

For stealing personal (authorization) data from a user of a RBS system, offenders often use special malicious software with additional functions that allow them to completely «self-destruct» after the commission of certain unlawful actions without the possibility of restoring them.

However, digital traces of such misconduct remain. Their identification and research are usually handled by experts in the field of information technology and forensic experts.

Currently, an international system of combating these types of crimes is being actively developed, qualified personnel is combining their efforts, methods for investigating crimes of this category are being worked out, procedures for interaction with international structure sand law enforcement agencies of various countries (in particular, through telecommunication sand systems) are being specified.

A rapid change in the generations of computer hardware and software products (every 3-5 years) calls for fur their research in to the development of the latest information security tools and ways to detect digital traces.

TEXTBOOK OF

CRIMINALISTICS

Volume II: Criminalistic Technique and Tactics

Edited by

Hendryk Malevski

Doctor of Law, Professor
Institute of Statutory Education
Public Security Academy
Mykolas Romeris University
Vilnius, Lithuania

Valery Shepitko

Doctor of Law, Professor
Criminalistics Department
Yaroslav Mudryi National Law University
Kharkiv, Ukraine

ПРАВО

Vilnius
Kharkiv

Pravo Publishing House LLC
80 Chernyshevska str., Kharkiv 61002, Ukraine
e-mail: sales@pravo-izdat.com.ua

Authors: Victoria **Alekseichuk** (Ukraine) – 3.1, 12.2, 16.3; Galina **Avdeeva** (Ukraine) – 1.4, 5.8, 8.5; Rima **Ažubalytė** (Lithuania) – 25.4, 25.5; Eglė **Bilevičiūtė** (Lithuania) – 13.1, 13.3–13.5, 13.7; Vasyl **Bilous** (Ukraine) – 1.3; Ryšardas **Burda** (Lithuania) – 19.2, 19.3; Rafal **Cieśla** (Poland) – 8.4; Andrej **Gorbatkov** (Lithuania) – 4.1–4.10; Gabrielė **Juodkaitė-Granskienė** (Lithuania) – 9.1–9.4, 23.1–23.4, 24.1–24.4, 25.4, 25.5, 26.1–26.3; Janina **Juškevičiūtė** (Lithuania) – 4.1–4.10; Mariietta **Kapustina** (Ukraine) – 3.2, 12.1, 12.3, 16.1; Vidmantas Egidijus **Kurapka** (Lithuania) – 5.1–5.7, 22.1–22.4; Kateryna **Latysh** (Ukraine) – 2.2; Hendryk **Malevski** (Lithuania) – 5.1–5.7, 7.1–7.7, 18.1–18.5; Snieguolė **Matulienė** (Lithuania) – 23.1–23.4, 26.1–26.3; Jozef **Metenko** (Slovakia) – 6.1–6.4; Giedrius **Mozūraitis** (Lithuania) – 24.1–24.4; Oleg **Musiienko** (Ukraine) – 1.2, 15.4; Žaneta **Navickienė** (Lithuania) – 22.1–22.4; Genrikas **Nedveckis** (Lithuania) – 13.1, 13.3–13.5, 13.7; Vilius **Ramanauskas** (Lithuania) – 13.1, 13.3–13.5, 13.7; Iryna **Shepitko** (Ukraine) – 19.10, 25.3; Mykhaylo **Shepitko** (Ukraine) – 2.1, 2.3, 11.2, 17.1–17.3, glossary; Valery **Shepitko** (Ukraine) – 1.1, 1.2, 2.1, 2.3, 8.1–8.3, 11.1–11.3, 13.2, 13.6, 14.1–14.5, 15.1–15.4, 17.1, 17.2, 18.6, 18.7, 19.1, 19.4–19.7, 19.9, 20.1–20.3, 21.1–21.3, 25.1–25.3, glossary; Viktor **Shevchuk** (Ukraine) – 1.5, 10.1–10.3, 16.3; Rasa **Tamošiūnaitė** (Lithuania) – 7.1–7.7; Maciej **Trzciński** (Poland) – 2.4; Renata **Valunė** (Lithuania) – 5.1–5.7, 7.1–7.7; Dmytro **Zatenatskyi** (Ukraine) 5.9, 10.1–10.3, 16.3; Volodymyr **Zhuravel** (Ukraine) – 16.2, 19.8.

Texbook of Criminalistics / editorial board: Prof. Dr. Hendryk Malevski (co-editor-in-chief), Prof. Dr. Valery Shepitko (co-editor-in-chief), Assoc. Prof. Dr. Gabrielė Juodkaitė-Granskienė, Prof. Dr. Vidmantas Egidijus Kurapka, Prof. Dr. Snieguolė Matulienė, Prof. Dr. Mykhaylo Shepitko.

840 p.

Includes name index, subject index, abbreviations, and glossary.

ISBN 978-966-998-568-2

Last digit is a print number: 10 9 8 7 6 5 4 3 2 1

Chapter 5.
FORENSIC INVESTIGATION OF TRACES (TRACEOLOGY)

Chapter 6.
FORENSIC WEAPONS SCIENCE