8.5. Specificity of Working with Digital Documents

Currently, in the investigative and judicial practice, digital documents are increasingly used as sources of evidence, along with paper documents. They differ from traditional documents in the file structure, created with the help of electronic (digital) devices (personal computers, digital photo, video and sound recording equipment, mobile phones, video recorders, video surveillance cameras, etc.) and system or special software.

A digital document is a document with the information recorded in the form of electronic data, including the standard details of the document. Digital documents can acquire the status of physical evidence and serve as forensic objects.

Digital documents comprise individual files or a set of files of various formats (computer programs, databases, etc.). The file format is a way of organizing information elements (bits, bytes) in a file. The type of the digital document file is determined by the document purpose (recording text, graphics, moving images and sound data, etc.) and the characteristics of the computer program, used to create the document.

International organizations and software companies develop standard formats of digital documents. The format (type) of the digital document is indicated by the file extension as a certain sequence of characters added to the file name after the point.

The most frequently used types of digital document files are: * .txt, * .doc, * .docx, * .docm, * .dot, * .odt, * .rtf, * .xlr, * .xls, * .xlsx (text documents and tables); * .pdf, * .djv, * .pps, * .ppsm, * .ppt (combined documents containing text and graphic information); * .tif, * .tiff, * .gif, * jpeg, * jpg, * .jpe, * .wdp, * .hdp (graphic documents and photos); * .mp3, * .mpa, * .ogg, * .wma, * .wav (sound documents) * .flac, * .mp4, * .mkv, * .mpeg, * .avi, * .mpg, * .3gp , * .mov, * .flv. (audiovisual documents). There are standard and

special software products to read through digital documents of various formats, most of which can be downloaded free of charge from online resources.

The use of digital document sand digital signatures is regulated by the legislation on digital document management. The names of official documents (a set of symbols before the dot) must also comply with the law requirements. The structure of the file name of the official digital document consists of the following elements: the country of origin identifier; the identifier of the institution; date of creation of the digital document; the registration index of the digital document; data translation version (original, firstcopy, secondcopy); filename extension. In the filename only Arabic numeral sand «.» (Dot), «-» (hyphen) sign sare used, which separate groups of elements of the filename. The country code of originis a threedigitnumeric code. For example, the code of Ukraine is «804».

A digital document can be created, transmitted, saved, changed by electronic device sand transformed into a visual form. The visual form of a text or graphical digital document displays the information contained there is on the screen (monitor) of the electronic medium and can be reproduced on paper with a printer.

A digital documents a source of judicial evidence can serve both as an object of criminal assault and as a means of achieving criminal purposes.

Digital documents are involved in the criminal process most often as a result of inspection of the scene and electronic equipment, search and seizure of their media, in the course of conducting other investigative actions.

Digital documents can also be provided by the proceedings participants (suspect, accused, defence counsel and others).

In the course of investigative actions in premises with remote access to computer equipment, special attention should be paid to preventing attempts to destroy digital documents by means of a local or global computer network. The simplest and quickest way to protect digital documents stored in the computer's memory from destruction or modification by remote access to it is to disconnect computer equipment from the electrical network.

The work of an investigator (judge) with digital documents is carried out in two stages. At the first stage, the details of the document are analyzed, and at the second stage, the analysis of its contents is performed.

Official digital documents have standard details (attributes), which ensure the documents' legal effect. They include the name of the sending institution, the document type (not indicated in the letters), the date of sending, the document's registration index, the title to the text, the text, the electronic digital signature. The layout and order of standard details of digital documents is determined by law.

Preparation and execution of a text digital document begins with its draft. At the stage of preparation of the draft document, the layout of the mandatory details can be changed or supplemented, depending on the type of document. Whatever structure the digital document might have, all its components should be enclosed in one file. The creation of a digital document is completed by putting an electronic digital signature on the data. It is used to identify the author of the document and to confirm its integrity.

The original digital document is an electronic copy of the document with mandatory details, including - the author or authorized person's digital signature. If the author creates several documents identical in content and details (for example, a digital document and a paper document), each of the documents is an original and has equal legal force. A paper copy of the digital document is certified as provided by the law.

The admissibility of a digital document as evidence can not be disputed solely on the grounds that it is in an electronic form. However, some digital documents can not be used as originals. Such documents include, for example, a certificate of inheritance rights and documents that, according to the law, can only be created in one original copy.

Working with digital documents, it should be borne in mind that sending and transmission of digital documents are carried out electronically using information, telecommunications, information and telecommunications systems or by mailing electronic media, which record the document.

Unless specified otherwise by the sender and the addressee, the date and time after which the sending of the digital document can not be canceled by the sender for technical reasons, are considered the date and time of sending the digital document.

The subjects of digital document management should keep digital documents on electronic data storage devices within the timeframe established by legislation for the relevant paper documents. Unless these requirements can not me met, digital documents must be kept as a paper copy of the document (in the absence of the original of this paper document). Before copying a digital document from an electronic data carrier, its integrity should be verified.

The following requirements are to be met when storing digital documents and working with them: 1) the information contained in digital documents must be unchanged and accessible for its further use; 2) an digital document may be converted into a visual form in the original format, used to create, send or receive it; 3) information on the origin and purpose of the digital document, as well as the date and time of its sending or receiving, should be kept.

An electronic digital signature, which is the result of converting a set of electronic data using special electronic digital signature means, is a type of digital signature. Such means are a system consisting of a software product and a hardware device. The means of electronic digital signature are intended for the generation of keys and the application and / or verification of an electronic digital signature.

The authentication of the personal key is carried out using a public key. The personal key is available only to the owner of the electronic digital signature, and the public key is known to the parties of relations involved in the use of electronic digital signature.

The fact of obtaining a public key and its appurtenance to the signer is confirmed by a public key certificate. Key certificates are issued by authorized bodies in electronic form or as a paper document.

Electronic digital signature by legal status is equivalent to a handwritten signature (seal) under the following conditions: 1) electronic digital signature is verified with the help of reliable digital signature

means; 2) in the course of verification, an enhanced key certificate was used, valid at the time of applying the electronic digital signature; 3) the personal key of the signatory corresponds to the public key specified in the certificate.

When working with incoming digital documents, it should be noted that digital documents are delivered to institutions in accordance with special instructions and regulations regarding the exchange of digital documents (data) between institutions.

The information system of the institution must ensure that incoming and outgoing digital documents are received and sent in accordance with these requirements. All incoming to an institution documents are usually received centrally in the documentation management office. The fact of receiving a digital document is recorded in a special register.

To ensure the security of the institution's information system, the reception and technical inspection of incoming digital documents is carried out with the help of an autonomous (separated from the main information system) hardware-software complex. The requirements for an integrated information security system are determined by special regulatory and legal acts on information security.

The problems of detecting, restoring, establishing authenticity, retrieving documents from the memory of electronic devices and reaserching them are prevalently solved with the involvement of IT experts or specialists.

They help to solve the problems of visualizing (printing out) text and graphic digital documents, reproducing audio and video recordings with the help of special software, restoring destroyed and damaged digital documents, studying attributes of the document file etc.

Attributes of the digital document file contain information on the date of its creation and modification, the date of destroying or copying the document, the author of the document, the place, the means of preparation, the method of production and subsequent processing of the document, etc. in addition, forensic experts will help decipher the encoded in the digital document information, guess a password and retrieve documents from the memory of the electronic device, provided an information security systems have been installed.

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

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; Rafał **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