2.1.1. Digital Forensic Tools

The absence of state's or their geographical borders is a valuable advantage of Digital Forensics, among other directions of forensic science, for searching and collecting digital information. Digital forensics implements computer hardware and software, computer information, network technologies, mobile communications, and cloud technologies. The Internet unites all computer networks based on Transmission Control Protocol.

Plenty of digital information can be explored through the Internet. Digital tools are highly demanded in searching for it and in detecting the authenticity of digital images and other materials.

Digital forensic tools can be divided into:

1) those used to search and collect information that may have potential evidential value for the investigation of crimes on the Internet:

- searching information in social media using hashtags, keywords, geolocation tags,
- public access to photo and video materials researching and providing to the investigation,
- using "big data" analysis technologies (Big Data),
- using programs for the analysis and processing of digital images,
- searching in cloud data storage,
- game systems analysing,
- user account data (usernames, passwords, avatars) observing;

2) those used to search and collect information on physical gadgets and other devices:

- tools that can take information from data storage and store detected encrypted data on other various physical drives,
- electronic devices for analysis (computers, smartphones, flash drives),
- telephone conversations studying,

- encrypted, hidden and/or deleted data searching;

- face recognition systems and their search in relevant databases (e.g. the Clearview AI face recognition application is used to identify potential criminals).

3) those used for the distant crime scene review when the scene area is significant, as well as in cases when the scene area access is dangerous, limited or unavailable at all, especially during a war, armed conflicts and territories occupation:

- satellite images analysing,

- radars and Marine Traffic vessels official monitoring systems.

By their type, digital forensics tools can be divided into:

1) cloud storage forensics;

2) mobile forensics (iOS and android phones, Huawei smartphones (Harmony OS 2.0));

3) examination of Instant Messaging applications which are used for exchanging messages (Line, Blackberry Messenger, iPhone health app, Snapchat, Kik, WeChat, Telegram, WhatsApp, Skype, Viber etc);

4) examination of the Internet of Things (e.g., IoT with biometric information and other personal identities, combining the data from multiple devices with those from other sources for them to be considered with all the information according to the investigation circumstances, events chronology and place, together);

5) network forensics (data traffic observing and traffic log analysis);

6) new devices and apps forensics (Amazon's Alexa, Google Assistant, Apple's Siri etc.);

7) non-phone apps forensics (database forensics, Spotlight, America online instant messaging, drones, volatile memory forensics, Dark net, anti-forensics tools, deleted and fragmented files, images, chip-off forensics, cryptocurrency);

8) digital forensic intelligence and open source intelligence[1].

By components, digital forensics tools are divided into:

- hardware,
- software,
- services.

Depending upon the object, digital forensics tools are divided into:

1) operating system forensics; 2) file system and disc forensics; 3) live memory forensics; 4) web forensics (web browser, web application); 5) email forensics; 6) network forensics; 7) multimedia forensics[2]; 8) desktop forensic tool, 9) live forensic tool, 10) email forensic tool[3].

According to the search object location, digital forensics tools can be classified into working: 1) through the Internet, 2) on technical devices, 3) at the crime scene place.

By display form, digital forensics tools can be: 1) direct (physical) and 2) virtual (online).

Digital forensics tools play a crucial role in collecting information. There were found 62 different tools which were categorized according to digital forensics subfields and only 33 of these tools were found to be publicly available, most of which were not maintained after development (T. Wu, F. Breitinger, S. O'Shaughnessy)[4]. So, it is enough to classify it into groups and it is unnecessary to give digital forensics tools exact examples because they are modified very quickly, and new ones appear.

---

[1] Reedy P. Interpol review of digital evidence 2016-2019. (2020) Forensic Science International: Synergy. Vol. 2, 489–520.

[2] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," in IEEE Access, vol. 10, pp. 11065-11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[3] Barik, K., Abirami, A., Konar, K., Das, S. (2022). Research Perspective on Digital Forensic Tools and Investigation Process. In: Misra, S., Arumugam, C. (eds) Illumination of Artificial Intelligence in Cybersecurity and Forensics. Lecture Notes on Data Engineering and Communications Technologies, vol 109. Springer, Cham. https://doi.org/10.1007/978-3-030-93453-8_4

[4] Tina Wu, Frank Breitinger, Stephen O'Shaughnessy, «Digital forensic tools: Recent advances and enhancing the status quo»ю Forensic Science International: Digital Investigation, Volume 34, 2020, doi: 10.1016/j.fsidi.2020.300999.

2.1.2. Open-Source Intelligence

Digital forensic tools can accumulate plenty of information with evidentiary value, but not in all cases does such information from open data sources can be admitted to be evidence. There can be issues with the installed source of origin and authenticity of such data in some cases. Therefore, Berkeley Protocol on Digital Open-Source Investigations was developed as a Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. The Protocol provides guidance on methodologies and procedures for gathering, analysing, and preserving open-source digital information, that is freely available, in a professional, legal, and ethical manner[5].

In literature, this kind of information is qualified by different terms such as «open-source information» or «open-source research»[6]. In the official NATO Terminology Database, it is called open-source intelligence (OSINT) and defined as «derived from publicly available information, as well as other unclassified information that has limited public distribution or access»[7]. It can be taken from public media, the Internet, and public government data (reports, budgets, press conferences, hearings, and speeches), professional and academic publications, commercial data (commercial imagery, business and financial assessments, and databases), grey literature (unpublished reports and newsletters)[8].

Collected OSINT data should:

1) contain sufficient and necessary information for the investigation's goals directly related to a particular case;

---

[5] Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

[6] Daragh Murray, Yvonne McDermott and K. Alexa Koenig Mapping the Use of Open Source Research in UN Human Rights Investigations. Journal of Human Rights Practice, 2022, 1–28 https://doi.org/10.1093/jhuman/huab059

[7] The official NATO Terminology Database URL: https://nso.nato.int/natoterm/Web.mvc

[8] European Commission. Open-source intelligence. URL: https://data.europa.eu/en/publications/datastories/open-source-intelligence

2) be relevant (reliable) and authentic (fifteen «core» elements (properties) from «Dublin Core Metadata Standard»[9] can be used for description and further evaluation).

A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence identifies the core forensic processes that apply to all forensic disciplines including digital and multimedia evidence: 1) authentication, 2) identification, 3) classification, 4) reconstruction, 5) evaluation[10].

There are six main phases of open-source investigation cycle: 1) online inquiry (discover information), 2) preliminary assessment (determine what to gather), 3) collection (capture digital items from the Internet), 4) preservation (ensure that collected information is stored and retrievable), 5) verification (evaluate the reliability of sources and content), 6) investigative analysis (data consideration and identification of gaps for further investigation)[11].

To sum up, digital forensic stages of collection data can consist of:

1) Plan preparation of searching data: methodology and list of control sources (links),
2) Looking for relevant data and further collection appropriately and securely;
3) Verification, analysis and evaluation of collected data.

[9] Dublin Core Metadata Standard URL: https://www.dublincore.org/specifications/dublin-core/dces/

[10] Nist A Framework for Harmonizing Forensic Science Practices and Digital/ multimedia Evidence, National Institutes of Standards and Testing: Organization of Scientific Area Committees for Forensic Science, 2018. Retrieved from, https://www.nist.gov/sites/default/files/documents/2018/01/10/osac_ ts_0002.pdf.

[11] Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source