OPEN ACCESS Freely available online

ISSN: 2090-2697
Journal of
Forensic Biomechanics

Perspective

Significance of Digital Evidence in Forensics

Malinova Gustav*

Department of Forensic Research and Education, University of Zilina, Zilina, Slovak Republic

DESCRIPTION

Digital forensics is a branch of forensic science dealing with legal evidence found in computers and digital storage media. During the course of the investigation, investigators obtain digital evidence from computers, laptops, and other electronic devices. However, there may be times when a suspect, witness, or someone close to you does not want to work with an investigator to remove digital evidence. As a result, data content has been removed in many studies aimed at generating data from flash memory, hard drives, or other digital storage media. Unfortunately, we cannot guarantee that all deleted data can be restored in such a way. Most of them are partial and in some cases incomplete, so you can't open the file.

Digital evidence, also known as electronic evidence, provides valuable information to forensic research teams. All information present in digital devices is a source of digital evidence. This includes email, text messages, photos, graphics, documents, files, images, video clips, audio clips, databases, internet browsing history and more. Reliance on electronic media and IOT devices increases the risks and vulnerabilities associated with digital devices are also high. For example, cybercriminals can launch malware campaigns by infecting computers with viruses to promote malicious intent. The digital forensic professional can determine the identification and storage of evidence collected during detective diagnosis from digital devices.

Digital forensics basically involves a three-step sequential process of media confiscation, media acquisition, and analysis of the forensic image of the original media. Some of the biggest challenges that forensics may face when collecting evidence are the number of PCs and the widespread use of Internet access, which can add difficulty of the investigation process. Hack tracking tools and software are not immediately available. Lack of physical evidence can complicate the criminal charge process. Large terabytes of storage space can make the research process bulky and difficult, so need to adapt the current situation. For example, technology changes may update certain techniques.

TYPES OF EVIDENCE

Anecdotal evidence

Anecdotal evidence is roughly translated into people's explanations and stories about a particular incident or event. However, such testimony is not valid in court, but can be used as a supporting theory for better understanding or analysis of the situation.

Circumstantial evidence

Circumstantial evidence is evidence that does not come from direct observation of the facts in a case. To draw criminal conclusions, we rely on inferences from a set of facts. This proof is an indirect proof, for example: if an investigator gets an audio clip of someone expressing a desire to commit a crime before execution, some inference can be drawn from the internet search history of the person involved in the crime. However, this is not a direct observation of the crime.

Character evidence

Evidence of personality is considered testimony to support a person's behavior on a particular subject related to that person's personality. Character proof helps to show intent, motivation, or opportunity.

Digital evidence

Today, digital evidence has multiple sources, including email, text messages, hard drives, social media accounts, audio and video files, and smart TVs. Therefore, digital data from electronic media and internet devices has become an important link in solving crime. Digital evidence is of paramount importance in court as establishing the facts are very important. Data or related information from electrical devices comes from two sources.

Volatile or non-persistent: Hard disks and detachable gadgets are some examples of gadgets risky factors which mean that the

Correspondence to: Malinová Gustav, Department of Forensic Research and Education, University of Zilina, Zilina, Slovak Republic, E-mail: gmalinova@gmail.com

Received: 02-Mar-2022, Manuscript No. JFB-22-16062; **Editor assigned:** 04-Mar-2022, Pre QC No. JFB-22-16062 (PQ); **Reviewed:** 18-Mar-2022, QC No. JFB-22-16062; **Revised:** 23-Mar-2022, Manuscript No. JFB-22-16062 (R); **Published:** 30-Mar-2022, DOI: 10.35248/2090-2697.22.13.391.

Citation: Gustav M (2022) Significance of Digital Evidence in Forensics. J Forensic Biomech.13:391.

facts aren't available while they're unplugged from the computer. Further, facts may be intentionally erased or wiped from those gadgets to ruin evidence. Of course, volatile additionally refers to reminiscence that is based on electricity to keep its contents, which include RAM chips. When the electricity is switched off the reminiscence contents are also lost.

Non-volatile which is persistent: Persistent data is permanently stored in memory and its contents are not erased by a power failure such as data stored in flash memory, ROM (read-only memory), CD/DVD, or tape.

CONCLUSION

Forensic investigations are incomplete without digital evidence. Digital data and information stored on electronic devices is associated with E-crime which is the other name for cybercrime. In the age of digitization, Internet-enabled electronic devices such as smart watches, smart TVs, and video game consoles can be an important factor in gathering information to resolve cases. In order to collect digital evidence with cyber security, investigators must follow appropriate steps to catch the perpetrators. Understanding this will help to detect crime scenarios efficiently by following the various phases built into the digital forensic capture process. This can be the crucial evidence collected and used for the right justice in court.