What Is Digital Evidence?

Posted on March 14, 2019

Digital evidence includes information on digital images, voice recordings, audio files, and computers. It is essential in dealing with crimes related to computers and the internet. At the same time, this evidence assists in dealing with other crimes by providing surveillance tapes, crime scene photos, and facial recognition. According to Ashcroft (2001), digital evidence comprises only information held in digital form with some probative value because a formal legal definition is elusive. The typical digital evidence sought in legal cases includes file system data, network traffic capture, network management logs, application logs, audit logs, and systems logs (Sommer, 1998). It also has the capability to provide information concerning the time, place, and manner of an event.

For the purpose of legal proceedings, both at national and international levels, digital evidence is defined as the information stored or transmitted in a digital format that is used in a legal proceeding by a party (Casey, 2011). Several international courts have authenticated the use of digital evidence through external indicators such as the use of multiple evidence and expert testimony (Prosecutor vs. Rutaganda). Digital evidence may raise hearsay concerns for two reasons: firstly, it is detached from its original resource, and secondly, it is not live testimony. Similarly, establishing the provenance of digital evidence at the court requires two testimonies: firstly, the object remained in substantially the same conditions, and secondly, the testimony of continuous possession (Black's Law Dictionary). Furthermore, complete and accurate evidence can only be provided if the proper preservation of the digital evidence is maintained.

Difference Between Physical Evidence And Digital Evidence

In comparison to conventional paper evidence, digital evidence is often considered superior. Firstly, it contains useful data along with details of key dates and history (Janes, 2000). Therefore, it can provide evidence that the defendant might wish not to exist. Secondly, digital evidence is easier to locate and process (Caloyannides, 2001). Also, in comparison to the conventional paper evidence, it provides metadata about itself prior to the fact. Therefore, it tends to provide valuable information related to a crime, including evidence of opportunity, intent, and ability, and it links a defendant to a crime (Flusche, 2001; Janes, 2000).

Several authors contend that conventional paper evidence and digital evidence are two different types of data despite the fact that both of them are required to provide a link between the perpetrator and the offense, linking the victim and the crime, and establishing the commission of an offense (Saferstein, 2000; Carrier et al., 2003). Moreover, it is believed that physical evidence is given credit over the digital data in the digital domain. However, the crime scene investigation methods

show fundamental similarities between the domains. In order to resolve this contention, Carrier et al. (2003) defined conventional and digital evidence in this way: physical evidence includes a computer, computer hardware, and computer peripherals, whereas digital evidence comprises the memory held in these devices.

Therefore, several authors point out that there is no fundamental difference between physical evidence and digital evidence. However, digital evidence is problematic for several reasons, including rapid changes to technology, large datasets, the complexity of the digital domain, and the volatility of digital evidence (Mercuri, 2005; Sommer, 2000). Moreover, the rapid changes in technology are difficult to keep due to the fact that they require technical understanding, which most practitioners, especially legal practitioners, do not have the capability to cope with (Mercuri, 2005; Sommer, 2000).

Emerging Problems In Digital Evidence

Technological advancements have made it easier for the authorities to obtain and store digital evidence. However, this practice faces several challenges at various levels. First of all, the question arises of whether, in order to meet the demands and needs of the current digital times, all global evidence must be transcripted into a digital form. It is an important question because it answers the possibility and extent of the presence of digital evidence in the virtual world, which can be used later in the trial process of criminal cases. Similarly, there are challenges related to the internet activities of the users, i.e., how much and when should they be recorded? Additionally, capturing information from a remote website questions its validity and authenticity due to the suspicions of incitement, fraud, and distribution of illegal information. There is a problem with expertise and its availability as well. However, the context of the issues related to digital evidence changes at the international level.

Digital Evidence And International Criminal Court

Digital evidence poses specific challenges to the International Criminal Court. Here, it is defined as the information stored or transmitted in a digital format that is used in a legal proceeding by a party (Casey, 2011). Thus, it comes in several forms, including emails, audio and video recordings, photographs, social media (e.g., Twitter, Facebook), and blogs. The international court has to learn to respond to its use as digital evidence becomes more prevalent.

The use of digital evidence offers new opportunities and challenges. Using evidence from a video, a satellite intercept, and an email may help establish linkage evidence between the commission of an international crime and the defendant being associated with it. Digital evidence, depending on the technology used, can provide information concerning the time, place, and manner of an event. This information is critical because it supplements the live testimony or viva voce evidence. However, the biggest problem with digital evidence is that it can be altered or degraded. Moreover, it is divorced from its source; for instance, only one perspective of a location at a particular time can be captured in

a picture. Similarly, the tone of voice or the demeanor of the author of an email cannot be captured.

The Authenticity Of Digital Evidence:

The evidentiary considerations of digital evidence at the international level are dependent on the fact that it is accepted as collaborative evidence instead of direct evidence. It is often introduced with other evidence that holds a higher probative value. As a matter of fact, the viva voce evidence is given a higher probative value than the digital evidence. The probative value is assessed through a variety of techniques. Firstly, the authenticity of the data source is assessed. It promotes the integrity of the trial proceedings because it ensures that the tendered evidence establishes what it offers to prove (Prosecutor vs. Popovic et al.). The authenticity of a piece of digital evidence is questioned because it can easily be altered or tampered with.

Moreover, authenticity and reliability are interrelated but distinct concepts. The former ensures that the evidence is in its original form and has not been tampered with or altered, whereas the latter establishes whether the evidence provides what it purports to be. For instance, in 2009, the reliability of video footage captured through the mobile telephone set of a soldier was questioned by the Sri Lankan government. The video allegedly depicted the killings of prisoners in Sri Lanka. The government argued that the killings were staged. Therefore, even if the video was authentic, i.e., it had not been tampered with, altered, or modified, and is thus authentic, its reliability is questioned. The prosecutor has to prove that it is reliable, which means that the killings were not staged and the prisoners were killed in real (Mackey, 2010).

Hearsay Digital Evidence:

Hearsay evidence is generated from outside the direct knowledge of the testifying witnesses (Prosecutor vs. Blagojević & Joki). Digital evidence may raise hearsay concerns for two reasons: firstly, it is detached from its original resource, and secondly, it is not live testimony. However, the International Criminal Court, in comparison to other ad hoc courts, does not have any explicit rule on it (Prosecutor vs. Lubanga). Although it prefers live testimony, the alternatives can be allowed in exceptional circumstances (Rule 67, ICC). One example in this regard can be its admission to anonymous hearsay (Prosecutor vs. Lubanga). Moreover, emails are considered anonymous hearsay evidence because objections arise regarding their authenticity and truthfulness (Prosecutor vs. Lubanga). As per the general rule, it can be admitted only as corroborating other evidence.

The Provenance Of Digital Evidence:

Furthermore, the element of provenance (chain of custody) of the evidence matters at the international level. It is the location and movement of real evidence and the history of the entities that held it in their custody. It covers the time from when it was obtained to the time it was presented

in court (Black's Law Dictionary). Establishing the provenance of digital evidence at the court requires two testimonies: firstly, the object remained in substantially the same conditions, and secondly, the testimony of continuous possession (Black's Law Dictionary). Therefore, a complete history of hosting and possession must be presented with regard to any type of digital evidence at the court. Such information about the electronic evidence is specifically important in determining if the evidence has been tampered with, modified, or altered. Thus, the accuracy of the evidence is assessed by the court on this information (Center for Research Libraries Study 51, 2012). The proof of authorship increases the authenticity level of the digital evidence (Prosecutor vs. Brdanin and Talic). However, there is no consistent definition of authorship in this regard.

Preservation

Digital preservation refers to long-term, error-free storage of digital information, with means for retrieval and interpretation, for the entire time span (Digital Preservation Definition). Complete and accurate evidence can only be provided if the proper preservation of the digital evidence is maintained. Digital evidence can remain an authentic source of testimony for a long period once stored or achieved (Center for Research Libraries Study 147, 2012). For example, during the Gikonda massacre in Rwanda, a journalist used a digital camera to capture footage of the killing of a father and a daughter, among others. The footage was distributed among the world news organizations. It was kept in storage for a long period. Later, this footage was used for the purpose of identifying victims and perpetrators (Center for Research Libraries Study 147, 2012). This usage of the footage helped in promoting awareness among the public regarding the genocide in Rwanda (Center for Research Libraries Study 147, 2012). Currently, the International Criminal Court is working on developing methods for ensuring complete and accurate preservation of digital evidence (Prosecutor vs. Callixte Mbarushimana). The e-Court Protocol is the most relevant example in this regard.

The Government And Digital Evidence

The government has started several projects with the purpose of connecting digital evidence with data collection methods in order to obtain a comprehensive data set that can later be used in dealing with various crime cases. The list includes computer forensic reference data sets, computer forensic tool testing, a national software reference library, and real-time forensic imaging for analog and digital video tapes.

Computer Forensic Reference Data Sets

The National Institute of Standards and Technology is working on creating and establishing computer forensic reference data sets. They are important because the number of crimes is not only continuously increasing but also overwhelming crime laboratories. Therefore, the existence of an

assured and quick way to validate the experience of an examiner and the functionality of the equipment is the need of the hour for managers. The national institute has been working to develop an online resource for managers and computer forensic analysts in order to facilitate their obtaining mock case examples for carrying out an in-house evaluation of equipment calibration and the skills of the examiner.

Computer Forensic Tool Testing

Numerous hardware and software packages that offer forensic capabilities are available in today's digital world. However, these tools must be tested before the courts, and forensic scientists trust these claims. This testing must be done with the purpose of evaluating the tools that are capable of supporting the functions such as collecting, examining, and analyzing as well as court testimony of the digital evidence. The National Institute of Standards and Technology has conducted a number of functional tests on the specific hardware and software that offer forensic capabilities using a unique testing framework. The national institute also provides information regarding the results of these tests on its official website.

National Software Reference Library

It is a digital era. Virtual storage of information is a reality today. Keeping this trend, or calling it a perspective of life, in mind, the researchers and practitioners are working on the establishment of a national software reference library. The other specific reason behind the creation of this library lies in the fact that forensic scientists often have to face a large pile of files on the hard drive after evaluating the computer evidence for a crime. These examiners need assistance, and the best method to assist them lies in the creation of a software reference library. The national institution has evaluated several software programs in this regard. It also provides the results of these evaluations on its official website.

Real-Time Forensic Imaging For Analog And Digital Video Tapes

It is a fact that technological advancements have made it easier for researchers and practitioners from all fields to collect and access data. However, it also indicates the threat of tempering, erasing, recording over, and otherwise modifying of the data. Therefore, forensic scientists must be able to identify any kind of tempering with the digital evidence. Keeping this need in mind, it is critically important for developers to develop high-level, real-time forensic imaging software. It must be a high-resolution imaging system using nano-engineered magnetic imaging methods. Such a system helps to screen and recover data from media that is tampered with or has been damaged.

Conclusion

Digital evidence has the capability to provide information concerning the time, place, and manner of an event. It includes information on digital images, voice recordings, audio files, and computers. In comparison to conventional paper evidence, digital evidence is often considered superior; it can provide evidence that a defendant might wish not to exist and is easier to locate and process. Using evidence from a video, a satellite intercept, and an email may help establish linkage evidence between the commission of an international crime and the defendant being associated with it. However, the process of connecting the digital evidence with the data collection methods in order to obtain a comprehensive data set that can later be used in dealing with various crime cases is the need of the hour. The government's involvement in this regard is appreciable.

Works Cited

Casey, Eoghan. Digital Evidence and Computer Crime. 3rd Ed. 2011.

Prosecutor v. Popovic, et al., Case No. IT-05-88-T. Int'l Crim. Trib. for the Former Yugoslavia Dec. 7, 2007.

Robert Mackey, Video of Sri Lankan Executions Appear Authentic UN Says, Jan. 8, 2010, https://thelede.blogs.nytimes.com/2010/01/08/sri-lanka-atrocity-video-appears-authentic-un-says/ (Accessed: 1st April, 2018).

Prosecutor v. Rutaganda, Case No. ICTR-96-3-T. Int'l Crim. Trib. for Rwanda Feb. 13, 1996.

Prosecutor v. Blagojević & Joki, Case No. IT-02-60-T. Int'l Crim. Trib. for the Former Yugoslavia Jan. 17, 2005.

Prosecutor v. Lubanga, Case No. ICC-01/04-01/06. 107. Mar. 14, 2010.

Rule 167. International Criminal Court. Rules of Evidence and Procedure of the International Criminal Court.

Black's Law Dictionary. 260. 9th Ed. 2009.

Center for Research Libraries. Human Rights Electronic Study 51. 2012. https://www.crl.edu/grn/hradp/electronic-evidence (Accessed: 1st April 2018).

Center for Research Libraries. Human Rights Electronic Study 147. 2012. https://www.crl.edu/grn/hradp/electronic-evidence (Accessed: 1st April 2018).

Prosecutor vs. Brdanin and Talic. Case No. IT-99-36-T. Int'l Crim. Trib. for the Former Yugoslavia, Feb. 15, 2002.

Digital Preservation Definition. U.S. Legal. https://definitions.uslegal.com/d/digital-preservation (Accessed: 1st April 2018).

Prosecutor vs. Callixte Mbarushimana. Case No. ICC-01/04-01/10. Apr. 28, 2011.