Electronic Crimes

The law enforcement agencies and legal entities have realized the importance of computer forensic investigations and the value of information technology experts in investigative procedures. With the coming of electronic crimes, tracing mischievous online doings has become inevitable to protect information. The pursuing of digital activities enables law enforcers to establish relationships between cyberinfrastructures and digitally kept the information to physical confirmation of a criminal action. Computer forensics are important as they allow investigators to unearth premeditated criminal activities to assist in the avoidance of future crimes (Nizami, 2017). The paper will consider forensic procedures for investigation, trends in digital forensics, data reconnaissance activities, methods of using forensic tools, the legal implication to electronic crimes, the implication of new laws to evidence collection, and the procedure of law enforcement reporting.

Forensic Procedures for Investigation

In combating electronic crimes, there are computer forensic procedures that contribute to a thorough and revealing investigation. The first procedure is evidence assessment. It entails the assessment of potential evidence in electronic crime. There is a flawless appreciative of the particulars of the presented event and the organization of the crime. For example, if the investigative agency is tasked with proving that an individual has committed electronic crimes, they will scrutinize through hard drives, emails, and other technological records to retrieve and access any material that can be used as confirmation.

The second step is evidence attainment. This is the direst procedure of a computer forensic investigation (Norwich University, 2017). There is an all-encompassing recording that is required during and after the attainment procedure. Information such as hardware and software specifications has to be recorded and well-kept. During this stage, guidelines that relate to the preservation of the integrity of probable indication apply.

The third step is the examination of the information. To commendably scrutinize on possible information, processes must be followed regarding recovering, replication, and keeping evidence within the suitable databases. The investigators look at information from various databases by using key words and other file retrieval procedures. The files are also analyzed to establish when and where they were created downloaded or uploaded.

Finally, the information collected is documented and reported. The investigators have to keep an accurate record of all investigation related activities such as methods used in the testing of system functionality, retrieving, copying, and storing data (Norwich University, 2017). This is meant to show the integrity of the process followed.

Trends in Digital Forensics

With the increased usage of connected devices, the likelihood of one becoming a victim of electronic crime is increased. With nearly half of the entire world's population interacting each day with electronic devices, there is a continued risk of becoming a victim of cybercrime (Rodriguez, 2020). With an increasing population and evolution of cheaper technology, electronic crimes are likely to increase in the future. This creates new challenges for forensic investigators. Luckily, several emerging technologies are already taking shape and assisting forensic investigators to counter existing electronic crimes. Additionally, the technology will keep evolving in the future meaning that forensic investigators have to keep changing and adapting to the technological changes.

Data Reconnaissance Activities

A reconnaissance attack involves gathering information on a network system negatively. It is done in several ways such as data fishing, trojan, spam mails, social networks, malicious web links, and free applications such as antivirus. It is the longest phase and requires time that may take up months. The cyber thief tries to gain all possible information from the target to understand how it functions through the exploitation of internet explorations, dumpster diving, social engineering, domain management, and non-intrusive network scanning. It is always difficult to ensure adequate security over reconnaissance. There are several ways that information regarding an organization finds its way into the internet. it is always easy to provide information about tidbits which gives a complete understanding of the potential weaknesses that can be used to attack. Making sure that the systems do not leak information to the web such as email addresses can be vital in countering data monitoring.

Methods for Using Forensic Tools

The forensic process is aimed at preserving evidence. The forensic tools consider the acquired data for the information that may be considered unusual, deleted, or hidden. Different methods are utilized at various stages of the investigative process. To preserve the evidence, investigators have to make an exact copy of the original data by using s write blocker to prevent changes in the original data. The common tools include sleuth kit, SIFT, encase, forensic toolkit, and coroner's toolkit. Forensic duplication assists in the retrieving of deleted files that may have been erased to hide evidence. The method uses similar tools as those used in preserving evidence. Removing files assists in eliminating unneeded files to leave those that will be used in the investigation. The method used is known as comparing md5 hashes. The common tools used are forensic toolkit and encase. Web activity reconstruction involves getting web browsing data, cookies, and temporary files. The tools used for the process are encase, browser logs, and forensic toolkit. Live forensics use methods to analyze volatile processes that are loaded in and of the memory. It uses tools such as COFEE, and windows forensic toolchest. To recover hidden files and data decryption and cryptanalysis are used. It uses tools such as frequency analysis, steg detect, password cracking, and steg break.

Legal Implications for Electronic Crimes

Electronic crime regulations include preventive, substantive, and procedural regulations. They outline the standards of acceptable behavior for information technology by establishing legal sanctions. The regulations prevent electronic harm from being perpetrated to people, systems, services, data, and infrastructure. The laws also allow investigation and prosecution for crimes committed electronically. They establish standards of behavior regarding digital technologies as well as criminal procedures all aimed at countering electronic crimes.

New Laws Affect Evidence Collection

New laws have an impact on how forensic investigators collect evidence. The laws bring impact on the procedure and speed with which information is being collected. The laws seek to protect both the suspect and the forensic investigators. The investigators may be barred from secretly reviewing information regarding a suspect. They may be required to document all the undertakings to be used as evidence. This slows down the pace at which evidence is being collected.

Procedures for Law Enforcement Reporting

In the event of electronic crime, one contacts the local law enforcement unit. They should assist in the making up of a formal report and make referrals to other appropriate agencies. The crime should be reported as soon as possible. The Internet Crime Complaint Center will then take up the case and evaluate the complaint and make referrals to the appropriate state, federal, or international agency under whose jurisdiction the issue lies. It is expected that the first responders secure digital evidence at the scene of the electronic crime. The search and seizure practices must be done in the set legal framework to ensure admissibility in the judicial setting.

In conclusion, digital evidence for electronic crimes are highly delicate and need to be addressed appropriately and within the legal framework. Forensic investigators understand the importance that digital evidence has towards preventing or proving an electronic crime. This makes them operate within strict guidelines and procedures. They use various tools that are protected within state and federal regulations.

References

Nizami, S. M. N. (2017). Electronic Crimes and Prevention. *IJECI*, *1*(1), 6-6.

Norwich University, (2017). 5 Steps for Conducting Computer Forensics Investigations. Retrieved from https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations

Rodriguez, E., (2020). Trends in Digital Forensic Science. Retrieved from https://study.com/academy/lesson/trends-in-digital-forensic-science.html