Example of digital forensics how this concept applies to digital crime and digita...

Law, Evidence

DIGITAL FORENSICS: HOW THIS CONCEPT APPLIES TO DIGITAL CRIME AND DIGITAL TERRORISM

Digital forensics is at times referred to as digital forensic science; this is because the subject is a branch in the field of forensic science. Digital forensics entails the investigation and recovery of digital evidence collected from computer crime. Initially, digital forensics was narrowed to computer data but with time it has evolved to encompass all forms of digital data storage devices. The evolution of digital forensics was uncontrolled between the 1970s and the late 1990s; however, national regulation and policies on the same were introduced in the beginning of the 21st century (Agarwal, Gupta, Saurabh & Chandra, 2011). Digital forensics can be used in various fields; the most common of these is to affirm or refute a certain hypothesis in civil and criminal investigations. Digital forensics may also be used in internal corporate audits or network intrusion investigations. Due to its reliability and effectiveness digital forensics is not been used to combat digital crime and digital terrorism.

Law enforcement officers today are aware that the sources of electronic data have increased exponentially especially with the popularity of activities such as social networking, text messaging, and email. This wide range of data is a key element of criminal investigations and an evidence source that is necessary in the prosecution of criminals. This significance of digital data stresses the need for not only its careful collection but also for having updated procedures for maintenance, archival, and handling of such data to ensure its suitability when presented before a court (Sammons, 2012).

The use of the internet has increased over the last decade. Statistics show that billions of people are online each day; this is part of the reason why the worldwide web is commonly referred to as the eighth continent due to the vast population found online. This population growth has not gone unnoticed; entrepreneurs, governments, various organizations and technology experts are tapping in to this growth to ensure positive development. However, it is not only people that intend good for the world that have noticed this growth. Criminals and terrorists are now using the internet and other forms of digital data in their unlawful activities. This calls for increased vigilance on the cyber world to protect innocent end-users from exploitation. Most cyber crimes are fraud related though there are several cases of murders, burglary and kidnappings of individuals after giving their personal information to unknown individuals on the worldwide web. Due to the rising number of fraudulent activities via digital networks, law enforcers are now shifting from a reactive position to a proactive one (Sammons, 2012). This entails the use of digital forensics to trace and detect digital crimes before they happen. This in turn helps promote cyber security and also privacy of digital information.

The processes involved in examining and filing legal suits for crimes committed online is not an easy one. The procedure involves an intricate network of tracking and collection of evidence, evaluating it, arranging it and then making a presentation before a court. One key limitation to the use of digital forensics is the application of encryption which disrupts investigators access to pertinent evidence that is locatable by the use of keywords. The

legal framework for compelling persons to disclose their encryption keys is still considerably new and hence not fully reliable.

When most people hear the word ‘ terrorism’ what comes into mind are bombings and mass murders. However, terrorism also entails the use of intimidation without violence to cause fear amongst the masses. Digital terrorism involves hacking various websites to deny the public various services or to access private information stored on computer networks that may be used to intimidate people into acting in a certain way. Digital terrorism also encompasses the advancement of racial and segregation views via digital networks. All these fall under the definition of terrorism since the people affected become afraid with the fear of how safe they are in their online activities, some of which are essential.

Many factors are put into thought when conducting a digital forensic investigation. There are five steps involved in such investigations: development of procedure and policy, assessment of evidence, acquisition of evidence, and examination, documenting and reporting of the evidence (Watters, Ventkatraman & Alazab, 2009). These steps are important as various studies show that several digital crimes cases have been ruled in favor of the defendants due to lack of credible digital evidence (Agarwal, Gupta, Saurabh & Chandra, 2011). Hence following the steps mentioned above helps ensure that the prosecution has a solid and provable case to present to the court. Lack of professional knowledge in digital forensics has also led to various prosecutions against criminals involved in digital terrorism ruled in favor of the defendants. However, various security organizations are

training their staff members on the use of digital forensics to help reduce this limitation.

The use of digital forensics is a growing trend in fighting digital crime and terrorism. Though the field faces various challenges, its reliability and future efficacy is irrefutable. The implementation of legal frameworks to support digital forensics and the training of law enforcers on its use will help reduce the limitations faced in digital forensic investigations.

Watters, P., Ventkatraman, S. & Alazab, M. (2009). Effective Digital Forensic Analysis of the NTFS Disk Image. UbiCC Journal 4(3), 551-558

Agarwal, A., Gupta, M., Saurabh, G. & Chandra, G. (2011). Systemic Digital Forensic

Investigation Model. International Journal of Computer Science and Security 5(1), 118-

131

Sammons, J. (2012). The Basics of Digital Forensics. New York: Syngress