Research paper on traditional forensics vs. live forensic acquisition

Law, Evidence

Introduction

Forensics refers to the use of scientific knowledge for the collection, analysis, and presentation of evidence to the courts (Guo, Jin & Hang, 2011). More specifically, forensic science refers to " the application of scientific techniques and principles to provide evidence to legal or related investigations and determinations" (Guo et al., 2011, p. 225).

Although forensic science has been employed in crime investigations since the early twentieth century (Palmer, 2002) through the use of traditional forensic techniques, the emergence of computers and other forms of technology has led to crimes that are being committed either in the cyber world or with the use of computers and other technologies. In response, a new field of forensic science has been developed, particularly live forensic acquisition, which is intended especially for the collection, analysis, and presentation of digital data as evidence. In this regard, this paper makes a comparison and contrast between traditional forensics and live forensic acquisition with regards to the methods they employ and the credibility that the courts accord them.

Comparison and Contrast

Methods

One of the differences between traditional forensics and live forensic acquisition is in the methods that they employ. In particular, some of the methods employed in traditional forensics include hair and fiber analysis, spectroscopy, chromatography, and serology (e. g. DNA examination) (Palmer, 2002). It also involves the examination of questionable documents, structural engineering, toxicology, odontology, anthropology, and pathology. As well, it involves tests such as psychological tests, polygraph tests, and behavioral tests. Traditional forensic methods are usually performed in-brick-and- mortar laboratories by experts such as trained practitioners and scientists. Traditional forensics also results in tangible evidence, such as blood type, fingerprints, and DNA analysis.

On the other hand, live forensic acquisition mainly makes use of computers and other technologies for the gathering and analysis of data. In particular, live forensics refers to “ a methodology that advocates extracting live, real time system data before shutting down the system to preserve memory, process, and network information that would otherwise be lost in a traditional forensic acquisition” (Grobler & Solms, 2009, pp. 2-3). It intends to minimize the impacts to the integrity of the system while in the process of gathering volatile forensic data. Moreover, it can refer to the acquisition of machines that are still running and from which both dynamic and static volatile data can be obtained. In general, live acquisition includes the transportation of data from the scene of the crime to a safe storage and location but does not include the interpretation of the gathered data (Lessing & Von Solms, 2008).

Live forensic acquisition is also related to cyber forensics, which US-CERT defines as “ the discipline that combines elements of law and computer science to collect and analyze

data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law” (as cited in Grobler & Von Solms, 2009, p. 2).

Unlike traditional forensic methods, live forensic acquisition techniques result in the generation of intangible evidence, such as application executables, server logs, audio and video files and recordings, graphical files, and application files (Craiger, Pollitt & Swauger, 2005) among others. These types of evidences are also subject to interpretation and to the complex process of transforming data into a form that can be analyzed. Live forensic acquisition analysis is also performed by computer experts, such as computer engineers and network specialists.

Whereas traditional forensic methods are used for investigating traditional crimes, such as murder, rape, or theft, live forensic acquisition methods are used for investigating virtual crimes or traditional crimes that involve the use of computers and other technologies. Examples include identity theft, child pornography, and computer hacking among others. These virtual crimes cannot be investigated using traditional forensic methods, which necessitated the development of live forensic acquisition techniques.

While the gathering of evidence using traditional forensic methods usually takes place after the crime has occurred, the gathering of evidence with the use of live forensic acquisition techniques can be conducted in near real-time and can have the capability of anticipating or predicting the next series of events (Palmer, 2002). However, it should be noted that while the law has concrete directives on how to deal with traditional forensic evidence, the law is not very clear when it comes to dealing with digital evidence.

Credibility

The evidence produced by traditional forensic methods is generally admissible in court proceedings. The results provided by traditional forensic methods are considered valid and credible for the most part because the methods employed for gathering such data have been the products of years of research in the various fields of science (Palmer, 2002). In particular, the advances that have been made in the fields of microscopy , chemistry, and medicine since the early twentieth century have paved the way for the adoption of scientific analysis in criminal investigations. This has introduced changes in the way that crimes were investigated, which used o be based on pure observation and intuition. With the implementation of scientific methods in forensic analysis, the perception with regards to evidence changed from one based on supposition to one based on reality. Moreover, since he development of scientific forensic methods started in universities, particularly with the assistance of well-known university professors, there was not much difficulty in the acceptance of these methods in court proceedings.

In contrast, the evidence that results from live forensic acquisition is not accorded with the same level of credibility and validity. For one, it is a fairly new field of forensics and as Palmer (2002) indicated, the scientific community did not take an active involvement in the development of the protocols, processes, and standards that are employed in the analysis of digital components. For another, not many in the judicial system understand this process. As such, when digital evidence is used in crime investigations or court proceedings, the court tends to rely on precedent rather than on repeatability and statistical significance when deciding on the admissibility of evidence that has been generated from digital sources.

Unlike the traditional forensic methods that are backed by a long history and that have been supported by universities and professional advocacy groups, live forensic acquisition has yet to establish its reliability, accuracy, and credibility. In particular, these techniques and the conclusions they imply have not yet been tested for reliability under experimental protocols or in controlled environments. At present, the only reason that most live forensic acquisition techniques are considered valid is because they have been previously used in courts to persuade the authorities; they have been used by practitioners or experts in the field; and because they are developed by well-known companies (Palmer, 2002).

However, as Palmer (2002) points out, even traditional forensic methods cannot be accorded with 100 percent accuracy and reliability. Although these methods have been the results of experimentations, these experiments also contained measures of error and other indices that explained the correctness and accuracy of the narrative and statistical results. As such, these small amounts of error, when taken collectively, can become significant. Moreover, human errors can also occur during the gathering of data, such as when collecting or handling DNA.

In this regard, whereas questions that can be raised about the validity of digital evidence can include questions on the reliability and credibility of the algorithms used, questions that can be raised about the validity of traditional forensic evidence can include questions such as whether bits of evidence were dropped on the floor or if any collection tools were missing.

Conclusion

This paper made a comparison and contrast between traditional forensics and live forensic acquisition, particularly with regards to the methods they employ and the degree of credibility and validity they hold in the courts. This paper discussed that traditional forensic methods are based on the sciences and are performed by trained practitioners such as scientists and doctors. These are the products of numerous experimentations and they produce tangible evidence. In contrast, live forensic acquisition is a new field that makes use of computers and other technologies for the collection, analysis, and presentation of data. It is not based on experimentations and has not undergone reliability tests. Techniques in this field of forensics are performed by computer experts and network specialists and the analysis of the gathered data results in intangible evidence.

Moreover, traditional forensics is used in the investigations of traditional crimes whereas live forensic acquisition techniques are used for the investigation of virtual crimes or traditional crimes that involved the use of technology. Whereas traditional forensic data is usually gathered after a crime, the gathering of data using live forensic acquisition techniques can be conducted in near real-time. However, while the law has clear directives on the admissibility of traditional forensic evidence, the law is unclear when it comes to the admissibility of digital evidence.

As such, traditional forensic evidence is perceived as more credible and valid by the courts whereas the treatment of digital evidence is based on precedent and the reputation of the companies that produce them. With the lack of reliability testing and experimentation, digital evidence is prone to being questioned. However, even the experimentations and reliability tests upon which traditional forensic methods are based are also prone to error as is the manual collection and the handling of physical evidence.

In conclusion, both fields of forensics have their pros and cons but for sure, they both aim for the same thing and that is the accurate investigations of crimes and the proper litigation of court cases.

References

Craiger, J. P., Pollitt, M. & Swauger, J. (2005). Law enforcement and digital evidence. In H.

Bidgoli (Ed.). Handbook of information security. New York: John Wiley & Sons.

Guo, H., Jin, B. & Huang, D. (2011). Research and review on computer forensics. In X. Lai et al.

Forensics in telecommunications, information and multimedia: Third International

ICST Conference, E-Forensics 2010, Shanghai, China, November 11-12, 2010, Revised

Selected Papers (pp. 224-233). New York: Springer.

Palmer, G. (2002). Forensic analysis in the digital world. International Journal of Digital

Evidence, 1(1). Retrieved from http://www2. tech. purdue. edu/cit/ Courses/cit556/readings/forensic_analysis. pdf.

Grobler, M. M. & Von Solms, B. (2009). A best practice approach to live forensic acquisition. In proceeding of: Information Security South Africa Conference 2009,

Africa, July 6-8, 2009. Proceedings ISSA2009. Retrieved from http://icsa. cs. up. ac. za/issa/2009/Proceedings/Full/1_Paper. pdf.

Lessing, M. & Von Solms, B. (2008). Live forensic acquisition as alternative to traditional

forensic processes. IT Incident Management & IT Forensics (IMF 2008), Mannheim,

Germany, 23 - 25 September, pp 1-9. Retrieved from

http://researchspace. csir. co.

za/dspace/bitstream/10204/3141/1/Lessing5_2008. pdf.