Review Article

Forensic odontology in the era of computer and technology

Patel J,[1] Singh HP,[2] Paresh M,[3] Verma C[4]

[1]***Dr Jaimin Patel***
MDS, Reader
Department of Oral Pathology
Institute of dental sciences
Bhubaneswar, Orissa, India

[2]***Dr Harkanwal Preet Singh***
MDS, Senior lecturer
[3]***Dr Mesurani Paresh***
MDS, Reader
[4]***Dr. Chanchal Verma***
Department of Oral Pathology
I.T.S Dental College, Ghaziabad,
Uttar Pardesh, India
[2,3]*Department of Oral Pathology*
Swami Devi Dyal Hospital and Dental College
Panchkula, Haryana, India

Received: 27-10-2012
Revised: 27-11-2012
Accepted: 28-12-2012

Correspondence to:
Dr. Harkanwal Preet Singh
hkps0320@gmail.com

ABSTRACT

We are living in the era of science and technology and it have infused with many aspects of our everyday life. With the advent of newer technologies the criminals have made full use of it which sometimes facade a challenging task to investigators such as forensic experts to catch the crime. This paper will discuss the need for computer forensics and application of technologies to be practiced in an effective and legal way, formalize basic technical issues, and point to references for further reading. It promotes the idea that the proficient practice of computer forensics and awareness of applicable laws is essential for today's networked organizations.

Key words: *Computer forensics, criminal, technology, odontology*

Introduction

Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the Federation Bureau Investigation (FBI) laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations. [1]

The use of computers in forensic dentistry has mirrored the use of computers in dentistry in general. There

has been a rapid acceptance and use of computers for management of all front-office and many clinical procedures. Their use has presented new tools for solving difficult forensic problems and has created new concerns regarding their application in general dentistry. [2]

Although there are myriad definitions of digital forensics, network forensics, software forensics, computer forensics, etc., each is a sub-discipline of forensics, that is, "The use of science and technology to investigate and establish facts in criminal or civil courts of law" (American Heritage Dictionary of the English Language, 2000). [3]

Definitions related to network forensics:

Computer forensics: It is the application of scientifically proven methods to gather, process, interpret, and to use digital evidence to provide a conclusive description of cyber crime activities. Cyber forensics also includes the act of making digital data suitable for inclusion into a criminal investigation. Today cyber forensics is a term used in conjunction with law enforcement, and is offered as courses at many colleges and universities worldwide." [4] Computer forensics is the process of conducting an examination into the contents of the data on a computer system using state of the art techniques to determine if evidence exists that can aid in internal or legal investigations. Forensic specialists use a wide array of methods to discover data and recover deleted, encrypted, and damaged files". [5]

Digital Evidence: Digital evidence is any information of probative value that is either stored or transmitted in a binary form (SWGDE 1998). This field includes not only computers in the traditional sense but also includes digital audio and video. It includes all facets of crime where evidence may be found in a digital form. [6]

Digital Forensics: Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis. [7]

Forensic Engineering: Forensic systems engineering is the discipline investigating the history of Information Technology failures. It therefore focuses on the post-mortem analysis and study of project disasters. The work involves a detailed investigation of the project, the environment, decisions taken, politics, human errors and the relationship between subsystems. The work draws upon a multidisciplinary body of knowledge and assesses the project from several directions and viewpoints. The concept of systems is a central tool for understanding the delicate relationships and their implications in the overall project environment. [8]

From the definitions acquired from the literature in the field of digital forensics, it would seem clear that each definition evolved from trying to solve a very specific problem. Most of these problems have

either related to issues of chain of custody and admissibility of digital evidence in criminal courts or to issues of intellectual property. Only the definition of Forensic Engineering addresses the use of forensic techniques to investigate technology failures.

The authors contend that it is time to begin defining an umbrella discipline, a branch of knowledge, incorporating the listed areas, and others, as sub-disciplines, while acknowledging the limitation of the scope to information technology connections. It is also time to begin formulating and standardizing definitions. While the authors believe that it is premature to impose such definitions or even the choice of terms, for the purposes of this discussion, the phrase "information systems etiology"

Basic components of Computer and network forensics methodologies:

Computer and network forensics methodologies consist of three basic components that Kruse and Heiser [7] refer to as the three A's of computer forensics investigations. These are:

- Acquiring the evidence while ensuring that the integrity is preserved.
- Authenticating the validity of the extracted data, which involves making sure that it is as valid as the original.
- Analyzing the data while keeping its integrity.

The field of digital forensics is undergoing a rapid metamorphosis: it is changing from skilled craftsmanship into a true forensic science. Part of this change is expressed by the interest in this field as an academic study. Ironically, the teaching portion of academe has led the way and research is trying to catch up. Research usually starts with a literature review. That is particularly difficult in this field for a number of reasons. Some of the work predates the Internet and therefore is only available in paper form, in largely obscure or unavailable documents. Much discussion and learning has not been published at all. And few are familiar with the work that has been published. [9]

The Forensic Process Model [10]

The U.S. Department of Justice published a process model in the Electronic Crime Scene Investigation: A guide to first responders that consists of four phases: -

- **Collection:** involves the evidence search, evidence recognition, evidence collection and documentation.
- **Examination:** designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation.
- **Analysis**: looks at the product of the examination for its significance and probative value to the case.
- **Reporting:** entails writing a report outlining the examination process and pertinent data recovered from

the overall investigation. Write the body of the paper here.

Application of software technology in Forensic odontology:

In past decade it had been observed that software technology has emerged as an indispensable part of forensic odontology. Several research studies with application of software technology to identify an individual has been proposed and found to give very reliable results.

Rugae pattern: Special software was designed called the Palatal Rugae Comparison Software (PR S Version 2.0) to match the clinical photographs taken using a SLR digital camera. The software recorded an accuracy of 99% in identification of individuals where as manual methods have shown high false positive and negative cases. [11]

Facial reconstruction: There are few studies which showed that with the application 3D-Computed tomography scan and computer software facial reconstruction can be done with low standard error of those measurements, from 0.85% to 3.09%. So, it can be used reliably in identification of individuals especially in mass disasters. [12]

Maxillary sinus in gender determination: Width, the length and the height of the maxillary sinuses were measured in Computerized Tomography scans with the application of software. Authors have concluded that Computerized Tomography measurements of maxillary sinuses may be useful to support gender determination in forensic medicine; however, with a relatively low-accuracy rate. [13]

Bite marks: Bite mark comparison protocols include measurement and analysis of the pattern, size, and shape of teeth against similar characteristics observed in an injury on skin or a mark on an object. Manual methods to trace the images in order to generate the dental cast to identify an individual are sometimes problematic. So, special softwares have been devised which have reduced this problem and have provided high accuracy. With application of software technology it is possible to artificially colour areas with equal intensity values and depict a 2-D image as a pseudo-3-D surface object. The use of image perception technology may allow visualization of a degree of detail unavailable with any other method. [14, 15]

Personal identification based on specific patterns of DMFS: Studies have been conducted to examine the overall utility of non-radiographic dental records for the establishment of individual identifications. It was found that even without radiographic lines of comparison, charts and notes that accurately detail a missing individual's antemortem dental condition can be essential for establishing an identification. Based on an analysis of two large datasets, individual dental patterns were determined using a special computer program (OdontoSearch) and were found to be generally unique, or at least very uncommon. Through this type of empirical comparison, it is possible to establish a

strong, quantifiable association with a missing individual. [16]

Conclusion

Law practitioners are in an uninterrupted battle with criminals in the application of digital/computer technologies, and require the development of a proper methodology to systematically search digital devices for significant evidence. So, we emphasize on the need for digital/computer forensics and application of technologies to be practiced in an effective and legal way and to formalize basic technical issues, and point to references for further reading.

References

1. Michael N, Mark MP, Lawrence P. Recovering and Examining Computer Forensic Evidence. Forensic Sci Comm 2000; 2(4):32-5.
2. Rawson RD. Computers in forensic dentistry. J Calif Dent Assoc 1996; 24(5):58-61.
3. American Heritage Dictionary of the English Language 2000. 4th ed. New York, NY: Houghton Mifflin.
4. ISP Webopedia 2005. Retrieved from http://isp.webopedia.com/TERM/C/cyber_ forensics.html
5. Digital Forensics of Texas, Inc. 2005. Available from http://home.swbell. net/txkidd/ forensics.html
6. National Center for Forensics Science 2005. Available from http://www.ncfs.org/home.html
7. Kruse W, Heiser J. Computer Forensics: Incident Response Essentials, Addison-Wesley 2002.
8. Dalcher, D. Forensics ECBS: The Way Forward, Proceedings of the Eighth Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems 2001.
9. Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic Digital Forensic Investigation Model. Int J Computer Sci Security 2011; 5(1):118-31.
10. National Institute of Justice. (July 2001) Electronic Crime Scene Investigation. A Guide for First Responders. Available from: http://www.ncjrs.org/pdffiles1/nij/187736 .pdf.
11. Hemanth M, Vidya M, Shetty N, Karkera BV. Identification of individuals using palatal rugae: Computerized method. J Forensic Dent Sci. 2010; 2(2): 86–90.
12. Sdos S, Ramos DL, Cavalcanti MG. Applicability of 3D-T facial reconstruction for forensic individual identification. Pesqui Odontol Bras 2003; 17(1):24-8.
13. Teke HY, Duran S, Canturk N, Canturk G. Surg Radiol Anat 2007; 29(1):9-13.

14. Van der Velden A, Spiessens M, Willems G. Bite mark analysis and comparison using image perception technology. J Forensic Odontostomatol 2006; 24:14-7.

15. Sweet D, Parhar M, Wood RE. Computer based production of bite mark comparison overlay. J Forensic Sci 1998; 43(5):1050-55.

16. Adams BJ. Establishing personal identification based on specific patterns of missing, filled, and unrestored teeth. J Forensic Sci 2003; 48(3):487-96.

Cite this article as: Patel J, Singh HP, Paresh M, Verma C. Forensic odontology in the era of computer and technology. Int J Med and Dent Sci 2013; 2(1):59-64.

Source of Support: Nil
Conflict of Interest: No