10.5005/jp-journals-10051-0127

REVIEW ARTICLE

Digital Forensics

[1]Vinod Sargaiyan, [2]Makrand Sapat, [3]Rajveer S Yadav, [4]Sateesh Bhatele, [5]Saurabh S Parihar, [6]Archana H Lanje

ABSTRACT

Digital forensics is the application of scientific principles to the process of discovering information from a digital device. A form of digital forensics has been around nearly as early as computers were invented, but forensic capabilities have witnessed many advances in the past years as digital forensic processes have matured and needs have become more prevalent. Digital forensics can involve nearly any digital device, not just computers, although technology often evolves faster than forensic capabilities do. Some of the common areas in which digital forensics are used include computers, printers, cell phones, mobile devices, global positioning systems, and storage media. Less common areas include automobile systems, appliances, office equipment, and other programmable devices.

Keywords: Crimes, Criminal, Digital, Forensic.

How to cite this article: Sargaiyan V, Sapat M, Yadav RS, Bhatele S, Parihar SS, Lanje AH. Digital Forensics. Int J Oral Care Res 2017;5(4):335-337.

Source of support: Nil

Conflict of interest: None

INTRODUCTION

With the proliferation of computers in our everyday lives, the need to include computer contents or traces as part of formal evidence has become inevitable. Computerized devices are part of our world in the form of laptops, desktop computers, servers, etc., but there are also many other storage devices that may contain forensic evidence. Devices, such as memory cards, personal digital assistants, and video gaming systems are among a myriad of devices that have the ability to accept input, provide output, and also store data. It is these data or the usage of these devices that is at the center of computer forensics.[1,2]

[1]Reader, [2-4]Senior Lecturer, [5]Postgraduate Student, [6]Professor and Head

[1,6]Department of Oral Pathology and Microbiology, Maharana Pratap College of Dentistry & Research Centre, Gwalior, Madhya Pradesh, India

[2]Department of Prosthodontics, Rungta College of Dental Sciences & Research, Bhilai, Chhattisgarh, India

[3,4]Department of Oral and Maxillofacial Surgery, Maharana Pratap College of Dentistry & Research Centre, Gwalior, Madhya Pradesh, India

[5]Department of Orthodontics, Maharana Pratap College of Dentistry & Research Centre, Gwalior, Madhya Pradesh, India

Corresponding Author: Vinod Sargaiyan, Reader, Department of Oral Pathology and Microbiology, Maharana Pratap College of Dentistry & Research Centre, Gwalior, Madhya Pradesh, India e-mail: dr.vinodsargaiyan@yahoo.co.in

DIGITAL FORENSICS ANALYSIS METHODOLOGY

The complete definition of digital forensics is as follows: The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal.[3,4]

The key elements of digital forensics are:

- The use of scientific methods
- Collection and preservation
- Validation
- Identification
- Analysis and interpretation
- Documentation and presentation

In general, the goal of digital forensic analysis is to identify digital evidence for an investigation. An investigation typically uses both physical and digital evidence with the scientific method to draw conclusions. Examples of investigations that use digital forensics include computer intrusion, unauthorized use of corporate computers, child pornography, and any physical crime whose suspect had a computer. At the most basic level, digital forensics has three major phases:

1. *Acquisition Phase*: It saves the state of a digital system so that it can be later analyzed. This is analogous to taking photographs, fingerprints, blood samples, or tire patterns from a crime scene. As in the physical world, it is unknown which data will be used as digital evidence so the goal of this phase is to save all digital values. At a minimum, the allocated and unallocated areas of a hard disk are copied, which is commonly called an image. Tools are used in the acquisition phase to copy data from the suspect storage device to a trusted device. These tools must modify the suspect device as little as possible and copy all data.[5,6]
2. *Analysis Phase*: It takes the acquired data and examines it to identify pieces of evidence. There are three major categories of evidence we are looking for:
   - Inculpatory evidence, which supports a given theory.

- Exculpatory evidence, which contradicts a given theory.
- Evidence of tampering, which cannot be related to any theory, but shows that the system was tampered with to avoid identification. This phase includes examining file and directory contents and recovering deleted content. The scientific method is used in this phase to draw conclusions based on the evidence that was found. Tools in this phase will analyze a file system to list directory contents and names of deleted files, perform deleted file recovery, and present data in a format that is most useful. This phase should use an exact copy of the original, which can be verified by calculating an MD5 checksum. It is important that these tools show all data that exist in an image. Regardless of the investigation setting (corporate, federal, or military), the steps performed in the acquisition and analysis phases are similar because they are dominated by technical issues, rather than legal.[7,8]

3. *Presentation Phase*: Although it is based entirely on policy and law, which are different for each setting, this phase presents the conclusions and corresponding evidence from the investigation. In a corporate investigation, the audience typically includes the general counsel, human resources, and executives. Privacy laws and corporate policies dictate what is presented. In a legal setting, the audience is typically a judge and jury, but lawyers must first evaluate the evidence before it is entered. In order to be admissible in a US legal proceeding, scientific evidence must pass the so-called Daubert test, which stems from the US Supreme Court's ruling in Daubert *vs* Merrell Dow Pharmaceuticals (1993).[9,10]

IMPLICATIONS OF DIGITAL FORENSICS

Digital forensics is commonly used in both criminal law and private investigation. Traditionally, it has been associated with criminal law, where the evidence is collected to support or oppose a hypothesis before the courts. As with other areas of forensics, this is often a part of a wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (e.g., to locate, identify, or halt other crimes). As a result, intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters, digital forensics forms part of the electronic discovery process. Forensic procedures are similar to those used in criminal investigations, often with different legal requirements and limitations. Outside of the courts, digital forensics can form a part of internal corporate investigations.[11,12]

A common example might be following unauthorized network intrusion. A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise both to establish the extent of any intrusion and in an attempt to identify the attacker. Such attacks were commonly conducted over phone lines during the 1980s, but in the modern era are usually propagated over the Internet.

The main focus of digital forensics investigations is to recover objective evidence of a criminal activity (termed *actus reus* in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.[13,14]

CONCLUSION

Digital forensics is a rapidly advancing field that has many challenges and crosswinds. The opportunities are endless, but they are not for the faint of heart. Frustration is a common partner, so the ability and mentality to press on through is a key characteristic an investigator should have. Someone who needs to be shown how to do everything may want to rethink their career options. A can-do attitude is essential, but the investigator does not need to do it alone. A variety of resources are available to assist, and most of the investigators who have worked through the learning curve to achieve competence are more than eager to help others do the same. Usually, they had others to lean on, so once you reach a level of expertise with the assistance of others, do not forget to return the favor.

REFERENCES

1. Reith M, Carr C, Gunsch G. An examination of digital forensic models. Int J Digital Evid 2002. Archived from the original on 2012 Oct 15. Retrieved 2010 Aug 2.
2. Kenneally EK. The Internet is the computer: the role of forensics in bridging the digital and physical divide. Digital Invest 2005;2(1):41-44.
3. Yang CH, Yen PH. Fast Deployment of Computer Forensics with USBs. 2010 International Conference on Broadband, Wireless Computing, Communication and Applications. Conference at Fukuoka, Japan.
4. Carnegie HH, Carnegie TV, Cranor L. Usability of forensics tools: user study. 2011 Sixth International Conference on IT Security Incident Management and IT Forensics, Carnegie Mellon University Pittsburgh, PA, USA.
5. Naqvi S, Dallons G, Christophe P. Applying Digital Forensics in the Future Internet Enterprise Systems—European SMEs' Perspective (CETIC). 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, Charleroi, Belgium.
6. Hildebrandt M, Kiltz S, Dittmann J. A Common Scheme for Evaluation of Forensic Software. 2011 Sixth International Conference on IT Security Incident Management and IT Forensics. Conference at Stuttgart, Germany.
7. Brinson A, Robinson A, Rogers M. A cyber forensics ontology: creating a new approach to studying cyber forensics. Digital Invest 2006;3S:S37-S43.

8. Law FY, Chow KP, Kwan MYK, Lai PKY. Consistency issue on live systems forensics. Future Generation Communication and Networking (FGCN) 2007. IEEE, Jeju, South Korea.
9. Shin YD. New digital forensics investigation procedure model. Fourth International Conference on Computing and Advanced Information Management. 2008. Conference at Gyeongju, South Korea.
10. Seokhee Lee, Hyunsang Kim, Sangjin Lee. "Digital evidence collection process in integrity and memory information gathering". 2005.Conference at Taipei, Taiwan
11. Manson D, Carlin A, Ramos S, Gyger A, Kaufman M, Treichelt J. Is the open way a better way? Digital Forensics using Open Source Tools. Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.
12. Rogers MK, Seigfried K. The future of computer forensics: a needs analysis survey. Computers Security 2004 Feb;23(1): 12-16.
13. Karyda M, Mitrou L. Internet forensics: legal and technical issues. Second International Workshop on Digital Forensics and Incident Analysis (WDFIA), 2007.
14. Garfinkel SL. Automating Disk Forensic Processing with SleuthKit, XML and Python, 2009. Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. Conference at Berkeley, California, USA.