Advances in Computer Forensics

Mohd Taufik Abdullah[1], Ramlan Mahmod[2] , Abdul Azim Ab. Ghani[3], Mohd Zain Abdullah[4], and Abu Bakar Md Sultan[5]

[1,2,3,5]Faculty of Computer Science and Information Technology
Putra University of Malaysia, 43400 UPM Serdang, Selangor, Malaysia
[4]Faculty of Technology and Information Science
National University of Malaysia, 43600 UKM Bangi,Selangor, Malaysia

Summary
Constant developments in information technology and communication have posed challenges for those policing cyber crimes. Due to the application of computer used to investigate computer-based crime has led to development of a new field called computer forensics. This paper discusses the research category in computer forensics and identifies key research issues of each of the category. Hopefully this paper would provide foundation and new ideas for the researcher to better understand the concepts of computer forensic. The outcome presents in this paper came from thoroughly review of recent computer forensic literatures.

Keywords:
Computer forensics, computer crime, ICT, forensic medicine, digital evidence

1. Introduction

The high-tech revolution in ICT such as the Internet and wireless networks, computers become more powerful with greater CPU speed and hard drive capacity has made new avenues of disseminating the information become available. The convergence of that technological advances and the pervasive used of computers worldwide has bring about many advantages to mankind, but as a result of this tremendous highly technical capacity made viable by computer, it provides avenues for misused and opportunities for committing crime. It also created new risks for the users of these computers and increased opportunities for social harm. The users, businesses and organizations worldwide have to live with a constant threat from hackers and hackers, who use a variety of techniques and tools to break into computer systems, steal information, change data and cause havoc.
The emergence of highly technical nature of computer crimes was created a new branch of forensic science known as computer forensics in which its root is derived from the practice of forensic medicine(Berghel, 2003; Gladyshev, 2004). Computer forensics is a concept and a new field(Garber, 2001; Fernandez *et al.*, 2005). According to, the widespread use of computer forensics is resulted from the act of two factors: the increasing dependence of law enforcement on computing and the ubiquity computers that followed from the microcomputer revolution.

This paper is organized as follows. Section 2 presents the definition of computer forensics. Section 3 briefly categorized the research issues in computer forensic according to recent review and we concluded in section 4.

2. Definition of Computer forensics

Computer forensics is a concept and a new field (Garber, 2001; Fernandez *et al.*, 2005). According to, the widespread use of computer forensics is resulted from the act of two factors: the increasing dependence of law enforcement on computing and the ubiquity computers that followed from the microcomputer revolution.

Computer forensics can be summarized as the process of identifying, collecting, preserving, analyzing and presenting the computer-related evidence in a manner that is legally acceptable by court (McKemmish, 1999; Noblett *et al.*, 2000; Robbins, 2000; Borck, 2001; Garber, 2001; Patzakis, 2003; Yasinsac, 2003; Slade, 2004; Bitpipe, 2005).

In Digital Forensics Research Workshop (DFRWS) held in 2001 has defined computer forensics as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital source for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (Palmer, 2001).

However, many experts feel that a precise definition is not yet possible because digital evidence is recovered from devices that are not traditionally considered to be computers (Hall and Davis, 2005). Some researchers prefer to expand the definition such as definition by Palmer (2001) to include the collection and examination

Manuscript received February 5, 2008
Manuscript revised February 20, 2008

of all forms of digital data, including that found in cell phones, PDAs, iPods, and other electronic devices.

3. Research category in computer forensics

Given the dynamics of form, size and content, predicting how the field of computer forensics will evolve is a difficult task as it is subject to a high degree of uncertainty. Based on various papers and Digital Forensics Research Workshop first technical report that we have reviewed, it seems that research in computer forensics can be categorized into five categories as shown in **Figure 1**.

3.1 Framework

Generally accepted computer forensics process framework is actively seeking by computer forensics researchers, practitioners, and customers. A framework will provide a common starting point from which established theory, for example, computer science and forensics science theory can be scientifically applied to the computer forensics science discipline. The framework will also enable the development of new theory and identifies the research and development requirements(Beebe and Clark, 2005).

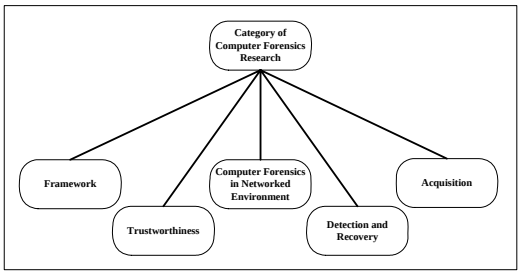

Figure 1: The five categories of computer forensics research

A number of models and methodologies have been developed in the computer forensics field such as by (McKemmish, 1999; Dittrich and Brezinski, 2000; Ashcroft, 2001; Palmer, 2001; Reith *et al.*, 2002; Kruse and Heiser, 2003; Mandia *et al.*, 2003; Carrier and Spafford, 2004b; Casey, 2004; Ciardhuáin, 2004; Nelson *et al.*, 2004; Beebe and Clark, 2005). Most of models reviewed have element identification, collection, preservation, analysis, and presentation. To make the step more clear and precise, some of them added addition detail steps into the element.

3.2 Trustworthiness

Transforming the nature of digital data that views as evidence is difficult in terms of integrity and fidelity. In addition, digital data is more easily to fabricate than physical data. Sommer (1997) has identified various stages of test to meet the conventional test of evidential reliability (authentication, accuracy, and completeness) of remote acquired computer files. Audit logs are important evidence source to support computer forensics and it needs to be secured and sufficiently tamper-resistant.

Most of existing tools and methods are allow anyone to alter any attribute associated with digital data. The form of digital data to be analyzed is usually transformed in some way and always processed before scrutiny (Palmer, 2001).

The high confidence and trust in the truthfulness of the evidence that allows decision-makers to act especially in courts of law is of great concern(Sommer, 1997; Hosmer, 2002). Truthfulness depends on fidelity and fidelity relies on integrity. A number of researches have been done to achieve guarantee integrity and fidelity of digital evidence.

Schneier and Kelsey (1999) have developed a general scheme that allows an audit logs and event logs keep on an insecure machine. Combination of physical tamper-resistant and periodic inspection of insecure machine could form the basis for highly trusted auditing capabilities.

In order to improve the integrity of digital evidence and provide higher assurance for digital chain of custody, secure and auditable time are introduced (Duren, 2002; Hosmer, 2002; Stone-Kaplan and Roter, 2003). A prototype programmable Hard Disk Interface has developed by Wick *et al.* (2004) to ensure the reliability of computer forensics tools consistently produce accurate and objective result in the evidence that they produce.

3.3 Computer Forensics in Networked Environments

Computer forensics in networked environments generally refers to the collection, combination and analysis of information on networks from various intrusion detection, auditing and monitoring (Palmer, 2001; Mohay *et al.*, 2003). It also known as network forensics (Palmer, 2001; Corey *et al.*, 2002; Mohay *et al.*, 2003). Mohay (2003) have outlined several problems in network forensic.

- The networks may span multiple time zones and multiple jurisdiction, necessitating the use of absolute trusted timestamps (to ensure the authentication and integrity of timestamps for each piece of network evidence) and ensuring that all jurisdictions collaborate.
- The network data will be available in both off-line and in real-time modes, the latter requiring the ability to capture and analyze data on the fly.
- The data could involve many different protocols and the amount of data could potentially be very large due to the increasing size of network bandwidth. A protocol

could also involve multiple layers of signal (e.g., Voice over IP (VoIP), HTTP tunnelling).
- The current set of computer forensics tools will not be able to handle the real-time and data size/volume.
- Techniques are required for rapidly tracing a computer criminal's network activities (e.g., IP addresses) and for mapping a network's topology. There needs to be a paradigm shift for network forensic techniques to analyze the rate and size of captured data.

A number of researchers have worked on this area such as collect information from computer networks to support forensics investigation.

3.4 Detection and recovery

Identify hiding methods and hiding places likely to be employed in digital realms. Detection and recovery is the heart of computer forensics. Data recovering is the result of applying extraordinary measures to extract information from locations in which it is known to reside. The goal of detection and recovery is to recognize the digital objects that may contain information about the incident and document them. The area of this research is including identifying the authorship, recovering digital evidence, classification, event reconstruction, analyzing, tracing and piecing.

The existing research on identifying the authorship have been done by (Sallis *et al.*, 1996; Vel, 2000; Corney *et al.*, 2002; Corney, 2003). There exist existing research on event reconstruction such as by (Stephenson, 2003; Carney and Rogers, 2004; Carrier and Spafford, 2004a; Gladyshev and Patel, 2004). The existing research on recovering hidden evidence is done by (Day and Ford, 1997; Casey, 2002; Wolfe, 2002)

3.5 Acquisition

The point of the acquisition is to copy and preserve the state of data that could be evidence. The forensic acquisition of media refers to the process of making a bit-for-bit copy, or image file, of a piece of media, which image files frequently used in civil or criminal court proceeding (Kornblum, 2004). Therefore, completeness and accuracy of acquisition process is required. In addition, the source of evidence must remains not altered by attackers or by normal processes innocently.

The increasing volume of potential data to search is creating a nationwide problem for law enforcement. Seizing all the computers at a search site, and examining them at the deepest levels are the most significant factors contributing to the examination backlog. In order to alleviate this problem, new data intake and data reduction strategies must be implemented. Data acquisition strategies must be adapted to the case-specific investigative goals, and these strategies must be pragmatic with regards to data volume and time constraints. Failure to recognize that yesterday's computer is not the equivalent of today's computer - and is not even remotely similar to tomorrow's computer - will inevitably result in lost investigative leads, and ineffective prosecutions.

A number of existing research have been done on acquisition such as by (Kornblum, 2002; Rose, 2003; Broucek and Turner, 2004; Mandelecha, 2004; Ring and Cole, 2004; Burdach, 2005).

4. Conclusion

In this paper, we have reviewed the literatures in computer forensics and identified five main categories of activity research in computer forensics. The five research categories are framework, trustworthiness, computer forensics in networked environments, detection and recovery and acquisition. The advances such as components, approaches, process of each category have been reviewed and discussed. Our future research will focus on event reconstruction. Event reconstruction will become important because digital crime investigators must be able to defend their hypotheses about why evidence exists. The event reconstruction gain major areas of interest topic discussed in DFRWS 2006.

References

[1] Ashcroft, J., 2001. Electronic Crime Scene Investigation Guide: A Guide for First Responders. National Institute of Justice.
[2] Beebe, N. L. and Clark, J. G. 2005. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2 (2). 147-167.
[3] Berghel, H. 2003. Digital village: The discipline of Internet forensics. Communications of the ACM, 46 (8). 15-20.
[4] Bitpipe 2005. Computer forensics. http://www.bitpipe.com/tlist/Computer-Forensics.html. Accessed on December 27, 2005.
[5] Borck, J. 2001. Leave the cybersleuthing to the experts. http://www.infoworld.com/articles/tc/xml/01/04/09/010409tccounter.html. Accessed on 22/12/2005.
[6] Broucek, V. and Turner, P. 2004. Intrusion Detection: Issues and Challenges in Evidence Acquisition. International Review of Law Computers & Technology, 18 (2). 149-164.
[7] Burdach, M. 2005. Digital forensics of the physical memory. http://forensic.seccure.net/pdf/mburdach_digital_forensics_of_physical_memory.pdf. Accessed on 21/6/2005.
[8] Carney, M. and Rogers, M. 2004. The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction. International Journal of Digital Evidence, 2 (4). 1-11.

[9] Carrier, B. and Spafford, E. H. 2004a. Defining Event Reconstruction of Digital Crime Scenes. Journal of Forensic Science, 49 (6). 1-8.
[10] Carrier, B. D. and Spafford, E. H. 2004b. A Digital Investigation Process Model. Available online at http://www.cerias.purdue.edu/news_and_events/events/symposium/2004/posters/pdfs/Digital%20Investigation%20Process%20Model.pdf.
[11] Casey, E. 2004. Digital Evidence and Computer Crime. Academic Press, San Diego, California, USA.
[12] Casey, E. 2002. Practical Approaches to Recovering Encrypted Digital Evidence. International Journal of Digital Evidence, 1 (3). 1-26.
[13] Ciardhuáin, S. Ó. 2004. An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3 (1). 1-22.
[14] Corey, V., Peterman, C., Shearin, S., Greenberg, M. S. and Bokkelen, J. V. 2002. Network forensics analysis. IEEE Internet Computing, 6 (6). 60 - 66.
[15] Corney, M., Vel, O. d., Anderson, A. and Mohay, G. 2002. Gender-Preferential Text Mining of E-mail Discourse for Computer Forensic. In Proceedings of the 18th Annual Computer Security Applications Conference 2002 (ACSAC 2002) (Las Vegas, NV, USA).
[16] Corney, M. W. 2003. Analysing E-mail Text Authorship for Forensic Purposes, Master of Information Technology, School of Software Engineering and Data Communication, Queensland University of Technology, Queensland, 181.
[17] Day, S. P. and Ford, S. 1997. Hard evidence from computers. In Proceedings of the European Conference on Security and Detection (ECOS 97) (Commonwealth Institute, London), IEEE, 19-20.
[18] Dittrich, D. and Brezinski, D. 2000. Intruder Discovery / Tracking and Compromise Analysis http://staff.washington.edu/dittrich/talks/blackhat/blackhat/index.html. Accessed on December 30, 2005.
[19] Duren, M. 2002. Can Digital Evidence Endure the Test of Time? In Proceedings of the 2nd Digital Forensics Research Workshop 2002, 1-7.
[20] Fernandez, J. D., Smith, S., Garcia, M. and Kar, D. 2005. Computer forensics: a critical need in computer science programs. Journal of Computing Sciences in Colleges, ACM, 20 (4). 315-322.
[21] Garber, L. 2001. Computer Forensics: High-Tech Law Enforcement. IEEE Computer Society's Computer Magazine, 34 (1). 22-27.
[22] Gladyshev, P. 2004. Formalising Event Reconstruction in Digital Investigation, Phd. Dissertation, Department of Computer Science, University College Dublin.
[23] Gladyshev, P. and Patel, A. 2004. Finite state machine approach to digital event reconstruction. Digital Investigation, 1 (2). 130-149.
[24] Hall, G. A. and Davis, W. P. 2005. Toward Defining the Intersection of Forensics and Information Technology. International Journal of Digital Evidence, 4 (1). 1-20.
[25] Hosmer, C. 2002. Proving the Integrity of Digital Evidence with Time. International Journal of Digital Evidence, 1 (1).
[26] Kornblum, J. 2002. Preservation of Fragile Digital Evidence by First Responders. In Proceedings of Digital Forensic Research WorkShop 2002 (Syracuse, NY), International Journal of Digital Evidence, 1-11.
[27] Kornblum, J. D. 2004. The Linux Kernel and the Forensic Acquisition of Hard Discs with an Odd Number of Sectors. International Journal of Digital Evidence, 3 (2).
[28] Kruse, W. G. and Heiser, J. G. 2003. Computer Forensics: Incident Response Essentials. Addison-Wesley, Boston, MA.
[29] Mandelecha, S. 2004. Forensics Repository, Master of Science, Computer Science, University of New Orleans, New Orleans, Louisiana. Available online at http://www.cs.uno.edu/~smandele/ThesisReport.doc.
[30] Mandia, K., Prosise, C. and Pepe, M. 2003. Incident Response & Computer Forensics. McGraw-Hill, USA.
[31] McKemmish, R. 1999. What is forensic computing? Trends and Issues in Crime and Criminal Justices (118). 1-6.
[32] Mohay, G., Anderson, A., Collie, B., Vel, O. d. and McKemmish, R. 2003. Computer and Intrusion Forensics. Artech House, Boston.
[33] Nelson, B., Phillips, A., Enfinger, F. and Steuart, C. 2004. Guide to computer forensics and investigations. ThomsonCourse Technology, Boston, Mass.
[34] Noblett, M. G., Pollitt, M. and Presley, L. A. 2000. Recovering and Examining Computer Forensic Evidence Forensic Science Communications. Available online at http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm.
[35] Palmer, G., 2001. A Road Map for Digital Forensic Research. The MITRE Corporation.
[36] Patzakis, J. 2003. Computer Forensics as an Integral Component of the Information Security Enterprise. http://www.computer-tutorials.org/ebooks/computerforensics.pdf.
[37] Reith, M., Carr, C. and Gunsch, G. 2002. An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1 (3). 1-12.
[38] Ring, S. and Cole, E. 2004. Taking a Lesson from Stealthy Rootkits. IEEE Security & Privacy, 2 (4). 38-45.
[39] Robbins, J. 2000. An Explanation of Computer Forensics. http://www.computerforensics.net/forensics.htm. Accessed on 13/6/2005.
[40] Rose, C. W. 2003. Windows Live Incident Response Volatile Data Collection: Non-Disruptive User & System Memory Forensic Acquisition. http://web.archive.org/web/20040218163741/http://www.sytexif.com/whitepaper.htm. Accessed on 12 March 2003.
[41] Sallis, P., Aakjaer, A. and MacDonell, S. 1996. Software forensics: old methods for a new science. In Proceedings of Software Engineering Education and Practice International Conference, IEEE, 81 - 485.
[42] Schneier, B. and Kelsey, J. 1999. Secure audit logs to support computer forensics. ACM Transactions on Information and System Security (TISSEC), 2 (2). 156-176.
[43] Slade, R. M. 2004. Software Forensics: Collecting Evidence from the Scene of a Digital Crime. McGraw Hill, New York.
[44] Sommer, P. 1997. Downloads, Logs and Captures: Evidence from Cyberspace. Journal of Financial Crime, 5JFC2. 138-152.
[45] Stephenson, P. 2003. Modeling of Post-Incident Root Cause Analysis. International Journal of Digital Evidence, 2 (2). 1-16.
[46] Stone-Kaplan, K. and Roter, M. 2003. Date, Time, and Time Zone Examination. http://www.computer-

tutorials.org/ebooks/Timezonewpv3.pdf. Accessed on 22/8/2005.
[47] Vel, O. d. 2000. Mining E-mail Authorship. In Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (Boston, MA, USA).
[48] Wick, C., Avramov-Zamurovic, S. and Lyle, J. 2004. Hard disk interface used in computer forensic science. In Instrumentation and Measurement Technology Conference (IMTC 04), IEEE, 1780 - 1783.
[49] Wolfe, H. B. 2002. Encountering Encrypted Evidence (potential). In Proceedings of Informing Science Conference, Inforing Science, 1601-1607.
[50] Yasinsac, A. E., R.F.; Marks, D.G.; Pollitt, M.M.; Sommer, P.M. 2003. Computer forensics education. Security & Privacy Magazine, 1 (4). 15 - 23.

Biography

Mohd Taufik Abdullah is a PhD student at the faculty of Computer Science and information Technology, Putra University of Malaysia. He holds a Master Degree in Software Engineering from UPM. His research interest includes computer forensics, and security computing.

Ramlan Mahmod holds a PhD from University of Bradford, United Kingdom. He is currently an Associate Professor at Faculty of Computer Science and Information Technology, Putra University of Malaysia, His research area is artificial intelligence and security computing.

Abdul Azim Ab. Ghani obtained his PhD from University of Strathclyde. Currently he is Associate Professor at the Department of Information System and dean of the Faculty of Computer Science and Information Technology, Putra University of Malaysia. His research interest is software engineering and software measurement.

Abdullah Mohd Zain holds a PhD from University. He is currently a Professor at the Department of Industrial Computing and deputy dean of the Faculty of Information Science and Technology, National University of Malaysia. His research interest is software engineering and software agents.

Abu Bakar Md Sultan holds a PhD from Putra University of Malaysia. He holds a Master Degree in Software Engineering from UPM. His research interest includes artificial intelligence, scheduling and software agents.