The future of digital forensics

Technology, Future

Abstract

Computer forensics as a field of study carefully collects and examines electronic evidence to assess the damage to computers caused by electronic attacks, recover the lost information and prosecute those responsible for such attacks. However, there are new developments in digital crimes that are posing challenges to computer forensics. This paper takes a look at such digital crimes and the different challengesthat they pose to computer forensics.

Introduction

As a relatively new and still growing field of study, computer forensics keeps facing new challenges that keep emerging with the advent of new technologies. Computer security is very important in the contemporary society where almost everything relies on computer from banking, marketing to making purchases online (Solomon et al , 2011, p54; Mohay, et al 2003, p99). This is the reason why computer security is very important as cybercrime poses a serious challenge to governments, business organisations and individuals. The new developments in digital crimes pose serious challenges to computer forensics thus calling for the need for the computer professionals to consistently look for new ways of mitigating the effects of such delirious acts so as to protect both organisations and individuals.

The new developments in digital crimes and the challenges to computer forensics

Vacca (2005, p66) says that computer forensics has quietly been able to resolve cases that would have otherwise not been possible to resolve in the last decade. Digital devices and computers have the ability of retaining data and as such are ubiquitous in the contemporary society. Criminals have taken advantage of this situation to pursue their own selfish interests. The contemporary criminals often use the same electronic devices used by everyone in the society like cellular camera phone, voice over internet protocol and text messaging in computer slang to protect their message from unauthorised audiences. Forensic examination often uncovers this trail and as such can reveal a lot of valuable information regarding such criminal activities although this trail often disappears when internet service providers overwrite logs thus making it very difficult to conduct any forensic audits (Shinder, 2002, p77). The same also happens when the data retention period expires thus creating a loophole for the criminals to cover up their trails.

The challenge of criminals covering up their trails is closely accompanied by the fact that the forensic officers often have to examine many different electronic devices containing large volumes of data (Kruse, &Heiser, 2003, p45 and Newman, 2007, p61. It is never easy for them to be effective given that they often work with limited resources thus making it very difficult for the officers to deliver exhaustive information in a timely manner. Additionally, the contemporary criminals are increasingly getting more skilled and as a consequence, are continuously able to conceal the devices and all related information that may provide useful leads to the forensic officers. For instance, a device like a microSD card is very small but has the capacity of holding information to the tune of two gigabytes. In essence, with

the advancement of newtechnology, the contemporary criminals are even getting more difficult to handle as they keep generating better efficient ways of concealing their messages and activities (Volonino, Anzaldua, & Godwin, 2007, p62).

There are softwares that are readily available in the stores with the ability of wiping hard drives to the specifications of the department of defence. These softwares are available for free download online or even at the local convenience store. This is making things very difficult for the forensic officers because anyone with an internet connection can freely get information and resources for countering forensic computing. These measures include things like steganography where all illicit files are hidden inside the ones that look innocuous (Phillips, &Enfinger, 2009, p76). The other ones are encryption and rigging computer cases.

Still on technology and innovation, Sheetz (2007, p13) claims thattechnology continues to emerge at a very fast rate whereasforensicsand other associated security technologies are still lagging behind. For instance, Sheetz (2007, p76) asserts that recent products like MSI Tegra and HP slate are two new technologies that the cyber criminals can take advantage of in pursuing their unlawful acts. Furthermore, the number of tested and standardised forensic tools for conducting forensic investigations on such new and other emerging gadgets are very limited hence making the work of forensic officers very difficult since they are not at par with the criminals who waste no time in embracing new technologies (Mohay et al, 2003, p34).

Maras (2012, p52) claims that the cyber criminals continuously create new methods of circumventing forensic and security techniques through different means like quickly embracing new technologies, targeting outdated or emerging technologies before their weaknesses are noticed and corrected. The contemporary cyber criminals have even gone further to devise anti forensic techniques that may at times require the forensic experts to carry out endless investigations into the attacks but still fail to generate enough information for generating meaningful inferences. These criminals have also noticed that the forensic officers often rely so much on windows operating system and have switched to using other operating systems like Mac OS and Linux to make it more difficult for the forensic officers to unearth their activities (Ec-Council2009, p98). The over reliance on Windows by the forensic officers is weakening the power of forensic officers in investigation other non-Windows systems and in the process giving the criminals an upper hand in continuing with their unlawful activities. This is the reason why computer forensics should embrace new better ways of investigation using all types of operating systems to ensure that the criminals are dealt with in the best way possible.

Conclusion

Computer forensics is a very important field as it plays a critical role in mitigating and investigating criminal activities. However, there are very many different challenges facing the forensic officers in the modern society as highlighted in the paper. This calls for quick adoption of new, better ways of dealing with the cyber criminals to regulate their activities in good time

before the whole situation spins out of hand. These new challenges can be addressed by pursuing an active approach to forensics and not allowing the cyber criminals to act first before moving in to generate solutions. The forensic officers should fully liaise with the manufactures of new devices and work together in tackling any use of such gadgets in unlawful activities. Computer forensics is an important field that should be enriched so as to not only mitigate the effects of cybercrime but also punish the criminals heavily to deter the criminals and other similar minded people from committing crimes.

Bibliography

Ec-Council (2009). Investigating Networking Intrusions and Cybercrime. Course Technology Ptr.

Kruse, W. G., &Heiser, J. G. (2003). Computer forensics: Incident response essentials. Boston, Mass.: Addison-Wesley.

Maras, M.-H. (2012). Computer forensics: Cybercriminals, laws, and evidence. Sudbury, Mass: Jones & Bartlett Learning.

Mohay, G. M., Anderson, A., Collie, B., Vel, O. ., &McKemmish, R. (2003). Computer and intrusion forensics. Boston, Mass: Artech House.

Newman, R. C. (2007). Computer forensics: Evidence collection and management. Boca Raton, FL: Auerbach Publications.

Phillips, N., &Enfinger, S. (2009). Guide to computer forensics and investigations. Clifton Park, N. Y: Delmar.

Sheetz, M. (2007). Computer forensics: An essential guide for accountants, lawyers, and managers. New Jersey: John Wiley & Sons.

Shinder, D. L. (2002). Scene of the cybercrime: Computer forensics handbook. Rockland: Syngress Media.

Solomon, M., Rudolph, K., In Tittel, ., Broom, N., & Barrett, D. (2011). Computer forensics jumpstart. Indianapolis, Indiana: Wiley Publishing, Inc.

Vacca, J. R. (2005). Computer forensics: Computer crime scene investigation. Hingham, Mass: Charles River Media.

Volonino, L., Anzaldua, R., & Godwin, J. (2007). Computer forensics: Principles and practices. Upper Saddle River, N. J: Pearson/Prentice Hall.