IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

Role of Digital Forensics in Combating Financial Crimes in the Computer Era

Ms. Juwariya Dalvi[1], Dr. Sachin Bhosale[2], Mrs. Pooja Devrukhkar[3]
Student, M.Sc.IT.[1]
Assistant Professor, Department of I.T[2,3]
I.C.S. College, Khed, Ratnagiri

Abstract: *Within the computer time, monetary violations have advanced in complexity and scope, requiring progressed techniques to examine and combat unlawful exercises. Computerized forensics plays a pivotal part in this scene by giving investigative techniques and devices to gather, analyze, and protect electronic prove related to budgetary violations. This paper investigates the multifaceted role of advanced forensics in tending to money related wrongdoings within the computer era.*

The integration of computerized innovations into budgetary frameworks has made unused openings for hoodlums, extending from advanced cyber-attacks to conventional extortion encouraged by advanced means. Digital forensics, as a teach, has developed as a crucial component within the battle against monetary violations. This paper analyzes the particular ways in which advanced forensics contributes to combating money related violations, including both proactive and responsive measures.

Proactively, computerized forensics includes the improvement of strong cybersecurity measures, chance evaluations, and proactive monitoring frameworks to identify and anticipate potential monetary violations. Reactively, it plays a urgent role within the consequence of an occurrence by conducting careful examinations, collecting electronic evidence, and supporting within the distinguishing proof and indictment of perpetrators.

The paper dives into the challenges confronted by computerized forensics experts within the energetic scene of monetary violations, counting issues related to security, encryption, and jurisdictional complexities. Besides, it investigates the advancing nature of budgetary violations, such as cryptocurrency-related offenses, and the adjustment of advanced forensics strategies to address these developing challenges.

Through case considers and real-world illustrations, this paper outlines the effectiveness of advanced forensics in revealing money related extortion, cash washing, and other illegal exercises. It highlights the intrigue nature of combating money related wrongdoings, emphasizing collaboration between law authorization, budgetary teach, and computerized forensics specialists.

Keywords: digital forensics, combating financial crimes, computer era.

REFERENCES

[1]. Anderson, R. C., Barton, R., Böhme, M. J., van Eeten, M., Levi, T. M. & Savage, S. (2013). Measuring the Cost of Cybercrime. In Böhme, R. (Ed.), The Economics of Information Security and Privacy. Springer.

[2]. Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013). Challenges to digital forensics: A survey of researchers and practitioners attitudes and opinions. 2013 Information Security for South

[3]. Africa - Proceedings of the ISSA 2013 Conference, pp. 1–8.

[4]. http://doi.org/10.1109/ISSA.2013.6641058

[5]. Adams, R. B. (2012). The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice. Journal of Digital Forensics, Security and Law, 8(4), pp. 25–48.

[6]. Adams, R. B. (2013). The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice. [Doctoral dissertation, Murdoch Unversity]. Retrieved from: http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf

ISSN 2581-9429 IJARSCT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

[7]. Casey, E. (2007) What Does "Forensically Sound" Really Mean? Digital Investigation, 4(2), pp. 49–50. doi: 10.1016/j.diin.2007.05.001.

[8]. Choo, K. R. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. Computers &Security 30(8), pp. 719-731.

[9]. Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security Privacy, 15(6), pp. 12–17. http://doi.org/10.1109/MSP.2017.4251117

[10]. Dorrell, D. D., & Gadawski, G. A. (2012). Financial forensics body of knowledge. John Wiley & Sons.

[11]. Du, X., Le-Khac, N., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. ArXiv, abs/1708.01730.

[12]. Eling, M. & Wirfs, J. H. (2016). Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class.I.VW HSG Schriftenreihe59(59), University of St.Gallen, Institute of Insurance Economics (I.VW-HSG).

[13]. European Central Bank. (2018, February 23). A Euro Cyber Resilience Board for pan-

[14]. European Financial Infrastructures. Retrieved from:

[15]. https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1.en.html

[16]. Homem, I. (2018). Advancing Automation in Digital Forensic Investigations [Doctoral Dissertation, Stockholm University, Department of Computer and Systems Sciences].

[17]. Hewling, M. (2010). Digital Forensics: The UK Legal Framework [Masters dissertation, University of Liverpool].

[18]. Harbawi, M., & Varol, A. (2016). The role of digital forensics in combating cybercrimes. 2016 4th International Symposium on Digital Forensic and Security (ISDFS), pp. 138-142.

[19]. Hassan, A., Lass, F., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the way out. ARPNJ Science and Technology 2(7), pp. 626-631.

[20]. United Nations. International Telecommunication Unit (ITU). (2017). Global Cybersecurity Index(GCI) 2017.

[21]. James, J., & Gladyshev, P. (2013). Challenges with Automation in Digital Forensic Investigations. ArXiv, abs/1303.4498.

[22]. Jaleshgari, R. (1999). Document Trading Online. Information Week755(136).

[23]. Kuchta K. J., (2000). Computer Forensics Today's Law, Investigations and Ethics Available from: http://www.liv.ac.uk/library/ohecampus/

[24]. Mugisha, D. (2019). Role and Impact of Digital Forensics in Cybercrime Investigations. International Journal of Cyber Criminology 47(3). Retrieved from:

[25]. https://www.researchgate.net/publication/331991596_role_and_impact_of_digital_forensics_ in_cyber_crime_investigations.

[26]. Mimoso, M. (2017). Maersk Shipping Reports $300M Loss Stemming from Not Petya Attack.

[27]. Threat Post - The Kaspersky Lab Security News Service.Retrieved from: https://threatpost.com/maersk-shipping-reports-300m-lossstemming-from-notpetyaattack/127477/

[28]. Macdermott, Á., Baker, T., & Shi, Q. (2018). IoT Forensics: Challenges For The IoT Era. In 9th IFIP International Conference on New Technologies Mobility and Security (NTMS) (pp. 1–5). Paris, France. http://doi.org/10.1109/NTMS.2018.8328748

[29]. McAfee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. Harvard Business Review 90(10), pp. 1-9.

[30]. McAfee & CSIS (2018). The Economic Impact of Cybercrime - No Slowing Down.

[31]. Mac Dermott, A. M., Baker, T., Buck, P., Iqbal, F., & Shi, Q. (2019). The Internet of Things: Challenges and Considerations For Cybercrime Investigations And Digital Forensics. International Journal of Digital Crime and Forensics(IJDCF) 12(1), pp. 1-13.

[32]. Mocas, S. (2004). Building Theoretical Underpinnings for Digital Forensics Research. Digital Investigation1(1), pp. 61–68. http://doi.org/10.1016/j.diin.2003.12.004

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

[33]. Okutan, A., & Cebi, Y. (2019). A framework for Cyber Crime Investigation. Procedia Computer Science 158, pp. 287–294.

[34]. Oruc, E., & Tatar, C. (2017). An investigation of factors that affect internet banking usage based on structural equation modelling. Computational Human Behavior 66, pp. 232–235.

[35]. Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence1(3), pp. 1–12.

[36]. Rogers, M. (2006). DCSA: A Practical Approach to Digital Crime Scene Analysis. In Tipton, H. F. & Krause , M. (Eds.), Information Security Management Handbook. Auerbach Publications.

[37]. Schatz, B. (2007). Bodysnatcher: Towards Reliable Volatile Memory Acquisition By Software. Digital Investigation4, pp. 126-134.

[38]. Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. Computer Law & Security Review26(3), pp. 304–308.

[39]. http://doi.org/10.1016/j.clsr.2010.03.002

[40]. Vrancianu, M., & Popa, L. A. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. The Amfiteatru Economic Journal, 1228: pp. 388403.

[41]. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.