References

[1] L. Caviglione, S. Wendzel and W. Mazurczyk, "The Future of Digital Forensics: Challenges and the Road Ahead," in IEEE Security & Privacy, vol. 15, no. 6, pp. 12-17, November/December 2017, doi: 10.1109/MSP.2017.4251117.

[2] P. Ambhore, A. Wankhade and B. Meshram, "Disk based Forensics Analysis", International Journal of Current Engineering and Technology, vol. 8, no. 2, pp. 389-392, 2018. Available: 10.14741/ijcet/v.8.2.33 [Accessed 18 November 2020].

[3] S.L. Garfinkel, "Digital Forensics Research: The Next 10 Years," Digital Investigation, vol. 7 supplement, 2010, pp. S64–S73.

[4] D. Klieiman, K. Timothy and M. Cross, "The Official CHFI Study Guide for Forensic Investigators," 2007.

[5] B. Carrier, "File System Forensic Analysis," Addison Wesley Professional, 2005.

[6] R. Chopade and V. Pachghare, "Ten years of critical review on database forensics research", Digital Investigation, vol. 29, pp. 180-197, 2019. Available: https://doi.org/10.1016/j.diin.2019.04.001 [Accessed 19 November 2020].

[7] "Database forensics", En.wikipedia.org, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Database_forensics [Accessed: 20- Nov- 2020].

[8] "What is Malware Forensics? – Hawk Eye Forensic", Hawkeyeforensic.com, 2020. [Online]. Available: https://hawkeyeforensic.com/2020/05/04/what-is-malware-forensics/. [Accessed: 20- Nov- 2020].

[9] Reddy N. (2019) Malware Forensics. In: Practical Cyber Forensics. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-4460-9_9

[10] "Types of Malware", usa.kaspersky.com, 2020. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/malware-classifications. [Accessed: 20- Nov- 2020].

[11] C. Malin, E. Casey and J. Aquilina, Malware forensics field guide for Windows systems. Waltham, MA: Syngress, 2012.

[12] "Malware", En.wikipedia.org, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Malware#Viruses. [Accessed: 20- Nov- 2020].

[13] "Ransomware", En.wikipedia.org, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Ransomware. [Accessed: 20- Nov- 2020].

[14] "Evasive malware goes mainstream - Help Net Security", Help Net Security, 2015. [Online]. Available: https://www.helpnetsecurity.com/2015/04/22/evasive-malware-goes-mainstream/. [Accessed: 20- Nov- 2020].

[15] Chhabra, Gurpal & Professor, Chhabra & Singh, Dilpreet & Professor, Bajwa. (2015). Review of E-mail System, Security Protocols and Email Forensics. International Journal of Computer Science & Communication Networks. 5. 201-211.

[16] A. Bhushan, K. Pogran, R. Tomlinson and J. White, "RFC 561 - Standardizing Network Mail Headers", Tools.ietf.org, 1973. [Online]. Available: https://tools.ietf.org/html/rfc561. [Accessed: 20- Nov- 2020].

[17] "Email Usage Statistics in 2019", Campaignmonitor.com, 2019. [Online]. Available: https://www.campaignmonitor.com/blog/email-marketing/2019/07/email-usage-statistics-in-2019/. [Accessed: 20- Nov- 2020].

[18] Enisa.europa.eu, 2020. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020. [Accessed: 20- Nov- 2020].

[19] Olalekan Adeyinka, "Internet Attack Methods and Internet Security Technology", Second Asia International Conference on Modeling & Simulation, May-2008.

[20] Kunal Pandove, Amandeep Jindal, Rajinder Kumar. "E-Mail Spoofing", International Journal of Computer Applications, Vol-5, No.-1, pp- 27-30, August 2010.

[21] P. Ramesh Babu, D. Lalitha Bhaskari, CH. Satyanarayana, "A Comprehensive Analysis of Spoofing", International Journal of Advanced Computer Science and Applications, Vol-1, No.-6, December 2010.

[22] Jitender Nath Srivastva, Maringati Hima Bindu, “EMail Spam Filtering using Adaptive Genetic Algorithm”, I. J Intelligent System and Applications, pp-54-60, January 2014.

[23] Kim-Kwang Raymond Choo, “The Cyber Threat Landscape: Challenges and future Directions”, Computer and Security, Science Direct, Elsevier, pp-719-731, 2011.

[24] Gori Mohamed .J, M. Mohammed Mohideen, Mrs.Shahira Banu. N, “E-Mail Phishing-An Open Threat to Everyone”, International Journal of Scientific and Research Publications, Vol-4, No.-2, Feb-2014.

[25] A. Case and G. G.Richard III, ”Memory forensics: The path forward”, Digital Investigation, vol. 20, pp. 23-33, 2017. Available: https://doi.org/10.1016/j.diin.2016.12.004 [Accessed 19 November 2020].

[26] N. Lord, ”What Are Memory Forensics? A Definition of Memory Forensics”, Digital Guardian, 2020. [Online]. Available: https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics. [Accessed: 20- Nov- 2020].

[27] N. Meghanathan, S. R. Allam and L. A. Moore, “Tools and Techniques for Network Forensics,” International Journal of Network Security & Its Applications, Vol. 1, No. 1, 2009, pp. 14-25.

[28] E. Casey, “Network Traffic as a Source of Evidence: Tool Strengths, Weaknesses, and Future Needs,” Journal of Digital Investigation, Vol. 1, No. 1, 2004, pp. 28-43. doi:10.1016/j.diin.2003.12.002

[29] B. Turnbull and J. Slay, ”Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics,” 2008 Third International Conference on Availability, Reliability and Security, Barcelona, 2008, pp. 1355-1360, doi: 10.1109/ARES.2008.135.