

Daftar Pustaka

- Albanna, F., & Riadi, I. (2017). Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security*, 15(1), 173–178. <https://doi.org/10.13140/RG.2.1.2967.0003>
- Babun, L., Sikder, A. K., Acar, A., & Uluagac, A. S. (2018). IoTDots: A Digital Forensics Framework for Smart Environments, (September). <https://doi.org/doi.org/1809.00745v1>
- Barua, A., Hoque, M., & Akter, R. (2014). Embedded Systems: Security Threats and Solutions. *Ajer.Org*, (12), 119–123. Retrieved from [http://www.ajer.org/papers/v3\(12\)/P031201190123.pdf](http://www.ajer.org/papers/v3(12)/P031201190123.pdf)
- Boztas, A., Riethoven, A. R. J., & Roeloffs, M. (2015). Smart TV forensics: Digital traces on televisions. *Digital Investigation*, 12(S1), S72–S80. <https://doi.org/10.1016/j.diin.2015.01.012>
- Davidoff, S., Ham, J., Davidof, S., & Ham, J. (2016). *Network Forensics Tracking Hackers through Cyberspace. Network Forensics Tracking Hackers through Cyberspace* (Vol. 28). <https://doi.org/10.1017/CBO9781107415324.004>
- Feynman, R. (2007). Programming Embedded Systems , Second Edition with C and GNU Development Tools.
- Jeong, D., Park, J., Lee, S., & Kang, C. (2015). Investigation methodology of a virtual desktop infrastructure for IoT. *Journal of Applied Mathematics*, 2015. <https://doi.org/10.1155/2015/689870>
- Kebande, V. R., & Ray, I. (2016). A generic digital forensic investigation framework for Internet of Things (IoT). *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 356–362. <https://doi.org/10.1109/FiCloud.2016.57>
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. <https://doi.org/10.6028/NIST.SP.800-86>
- Liu, J. (2015). IoT Forensics Issues strategies and challenges. *12 IDF Annual Conference*.
- Meffert, C. S., Clark, D. R., Baggili, I., Breitingner, F., Meffert, C., & Clark, D. (2017). Digital Commons @ New Haven Forensic State Acquisition from Internet of Things (FSAIoT): A General Framework and Practical Approach for IoT Forensics through IoT Device State Acquisition Forensic State Acquisition from Internet of Things

- (FSAIoT): A gener, 2017. Retrieved from <http://digitalcommons.newhaven.edu/%0Ahttps://doi.org/10.1145/3098954.3104053>
- Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, (December), 608–615. <https://doi.org/10.4108/icst.collaboratecom.2013.254159>
- Osman, Y., Osei, A., & Narendra, B. C. (2016). A Review of Prospects and Challenges of Internet of Things. *International Journal of Computer Applications*, 139(April), 33–39. <https://doi.org/10.5120/ijca2016909390>
- Ovidiu, V., & Friess, P. (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. *Scientific American* (Vol. 291). <https://doi.org/10.1038/scientificamerican1004-76>
- Palmer, G. (2001). A Road Map for Digital Forensic Research.
- Patel, K. K., & Patel, S. M. (2016). Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International Journal of Engineering Science and Computing*, 6(5), 6122–6131. <https://doi.org/10.4010/2016.1482>
- Perumal, S., Md Norwawi, N., & Raman, V. (2015). Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology. *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, 19–23. <https://doi.org/10.1109/ICDIPC.2015.7323000>
- Ramadhan, R. A., Prayudi, Y., & Sugiantoro, B. (2017). Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD). *Teknomatika*, 9(2), 1–13. Retrieved from <http://teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf>
- Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij), 3(May), 70–82. <https://doi.org/10.21831/elinvo.v3i1.19308>
- Rizal, R., Riadi, I., & Prayudi, Y. (2018). Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *Int. J. Cyber-Security Digit. Forensics*, 7(4).
- Tilva, M., & Rohokale, V. (2016). Network Forensics for detection of malicious packets in Internet of Things (IoT), (June).
- Watson, S., & Dehghantaha, A. (2016). Digital forensics: the missing piece of the Internet of Things promise. *Computer Fraud and Security*, 2016(6).

[https://doi.org/10.1016/S1361-3723\(15\)30045-2](https://doi.org/10.1016/S1361-3723(15)30045-2)

Yuwono, B., & Nugroho, S. P. (2015). Pengembangan Model Public Monitoring System, *12*(02).

Zawoad, S., & Hasan, R. (2015). FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 279–284. <https://doi.org/10.1109/SCC.2015.46>

