DAFTAR PUSTAKA

Abbas, T. M. J. (2015). Studying the Documentation Process in Digital Forensic Investigation *Framework*s/ Models. *Journal of Al-Nahrain University-Science*, *18*(4), 153–162. https://doi.org/10.22401/jnus.18.4.21

Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness *framework* for organizations. *Journal of Cloud Computing*, *8*(1). https://doi.org/10.1186/s13677-019-0133-z

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers and Security*, *105*.

Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, *28*, 126–138. https://doi.org/10.1016/j.diin.2019.02.001

Arshad, H., Jantan, A. Bin, & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, *14*(2), 346–376. https://doi.org/10.3745/JIPS.03.0095

Ashley DuVal. (2014). *History of Forensic Psychology*. Https://Forensicpsych.Umwblogs.Org. https://forensicpsych.umwblogs.org/research/criminal-justice/fingerprint-analysis/

Ayangbekun, O. J., Bankole, O. F., & Saka, B. A. (2014). Analysis of security mechanisms in Nigeria E-banking platform. *International Journal of Electrical and Computer Engineering*, *4*(6), 837–847. https://doi.org/10.11591/ijece.v4i6.6857

Badan Standarisasi Nasional. (2014). *SNI ISO-IEC 27037:2014* (pp. 1–44). Badan Standar Nasional.

Balogun, A. M., & Zuva, T. (2017). Open Ethical Issues in Digital Forensic Systems. *International Journal of EBusiness and EGoverment Studies*, *9*(1), 55–69.

Bang, J., Park, J., & Lee, S. (2022). Vision: An empirical *framework* for examiners to accessing password-protected resources for on-the-scene digital investigations. *Forensic Science International: Digital Investigation*, *40*,

301376. https://doi.org/10.1016/j.fsidi.2022.301376

Bani, I. A., & Al-Maliki, J. K. I. (2023). The Effects of Criminal Evidence Obtained Illegally. *Journal of Asian Multicultural Research for Social Sciences Study*, *4*(1), 63–74.

Bankole, F., Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation*, *40*.

Baror, S. O., Venter, H. S., & Adeyemi, R. (2020). A natural human language *framework* for digital forensic readiness in the public cloud. *Australian Journal of Forensic Sciences*, *00*(00), 1–26. https://doi.org/10.1080/00450618.2020.1789742

Bhardwaj, S., & Dave, M. (2023). Enhanced neural network-based attack investigation *framework* for network forensics: Identification, detection, and analysis of the attack. *Computers and Security*, *135*(April), 103521. https://doi.org/10.1016/j.cose.2023.103521

Buckles, D. J., & Chevalier, J. M. (2019). *Participatory Action Research: Theory and methods for engaged inquiry* (2nd ed.). Routledge.

Casey, E. (2011a). *Digital evidence and computer crime: forensic science, computers and the internet* (Third Edit). Academic Press.

Casey, E. (2011b). Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet. In *Elsevier*.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2010). A privacy threat analysis *framework*: Supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, *16*(1), 3–32. https://doi.org/10.1007/s00766-010-0115-7

Fahrezi Abdullah, R. A. (2023). Digital Forensic Urgence in Analyzing Electronic Evidence for Evidence of Criminal Actions in Information and Electronic Transactions. *Journal of Development Research*, *7*(2), Process. https://doi.org/10.28926/jdr.v7i2.238

Faizal, A., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A *Framework* for Digital Forensic Evidence Analysis. *Journal of Information Systems and Informatics*, *6*(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020a). PRECEPT: a *framework* for ethical digital forensics investigations. *Journal of Intellectual Capital*, *21*(2), 257–290. https://doi.org/10.1108/JIC-05-2019-0097

Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020b). PRECEPT: a *framework* for ethical digital forensics investigations. *Journal of Intellectual Capital*, *21*(2), 257–290. https://doi.org/10.1108/JIC-05-2019-0097

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*, 301169. https://doi.org/10.1016/j.fsidi.2021.301169

Goudbeek, A., Choo, K. K. R., & Le-Khac, N. A. (2018). A Forensic Investigation *Framework* for Smart Home Environment. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 1446–1451. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00201

Granja, F. T. M., & Rafael, G. D. R. (2017a). Model for digital evidence preservation in criminal research institutions-PREDECI. *International Journal of Electronic Security and Digital Forensics*, *9*(2), 150–166. https://doi.org/10.1504/IJESDF.2017.083989

Granja, F. T. M., & Rafael, G. D. R. (2017b). Model for digital evidence preservation in criminal research institutions-PREDECI. *International Journal of Electronic Security and Digital Forensics*, *9*(2), 150–166. https://doi.org/10.1504/IJESDF.2017.083989

Halboob, W., Mahmod, R., Udzir, N. I., & Abdullah, M. D. T. (2015). Privacy Levels for Computer Forensics: Toward a More Efficient Privacy-preserving Investigation. *Procedia Computer Science*, *56*(1), 370–375. https://doi.org/10.1016/J.PROCS.2015.07.222

Hasan, T., & Djaenudin, D. M. (2023). Pemetaan Bibliometrik Menggunakan VOSviewer Terhadap Perkembangan Hasil Penelitian Literasi Informasi Pada Jurnal Perpustakaan di Indonesia. *Jurnal Gema Pustakawan*, *11*(2), 110–124. https://jgp.ejournal.unri.ac.id

Henseler, H., & van Loenhout, S. (2016). Educating judges, prosecutors and

lawyers in the use of digital forensic experts. *DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe*, *24*, S76–S82. https://doi.org/10.1016/j.diin.2018.01.010

Horsman, G. (2018a). *Framework* for Reliable Experimental Design (FRED): A research *framework* to ensure the dependable interpretation of digital data for digital forensics. *Computers and Security*, *73*, 294–306. https://doi.org/10.1016/j.cose.2017.11.009

Horsman, G. (2018b). *Framework* for Reliable Experimental Design (FRED): A research *framework* to ensure the dependable interpretation of digital data for digital forensics. *Computers and Security*, *73*, 294–306. https://doi.org/10.1016/j.cose.2017.11.009

Horsman, G. (2022a). Conducting a 'manual examination' of a device as part of a digital investigation. *Forensic Science International: Digital Investigation*, *40*, 301331. https://doi.org/10.1016/j.fsidi.2021.301331

Horsman, G. (2022b). Defining principles for preserving privacy in digital forensic examinations. *Forensic Science International: Digital Investigation*, *40*, 301350. https://doi.org/10.1016/j.fsidi.2022.301350

Hughes, N., & Karabiyik, U. (2020). Towards reliable digital forensics investigations through measurement science. *WIREs Forensic Science*, *2*(4), 1–11. https://doi.org/10.1002/wfs2.1367

ISO/IEC 25010. (2011). ISO/IEC Systems and software engineering — Requirements and Evaluation. In *Ieee* (Vol. 2011, Issue IEEE).

Jain, N. (2015). Digital Forensic *Framework* using Feedback and Case History Keeper. *International Conference on Communication, Information & Computing Technology (ICCICT)*.

Jayaraman, I., & Stanislaus Panneerselvam, A. (2021). A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. *Journal of Ambient Intelligence and Humanized Computing*, *12*(5), 4911–4924. https://doi.org/10.1007/s12652-020-01931-1

Kember, D. (2000). Action Learning and Action Research: Improving the Quality of Teaching and Learning. In *Quality Assurance in Education* (Vol. 9, Issue 1). Kogan Page. https://doi.org/10.1108/qae.2001.9.1.54.3

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. The National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Krivchenkov, A., Misnevs, B., & Pavlyuk, D. (2019). Intelligent methods in digital forensics: State of the art. In *Lecture Notes in Networks and Systems* (Vol. 68). Springer International Publishing. https://doi.org/10.1007/978-3-030-12450-2_26

Kumar, K., Sofat, S., Aggarwal, N., & S.K.Jain, S. K. J. (2012). Identification of User Ownership in Digital Forensic using Data Mining Technique. *International Journal of Computer Applications*, *50*(4), 1–5. https://doi.org/10.5120/7756-0818

Losavio, M., Seigfried-Spellar, K. C., & Sloan, J. J. (2016). Why digital forensics is not a profession and how it can become one. *Criminal Justice Studies*, *29*(2), 143–162. https://doi.org/10.1080/1478601X.2016.1170281

Maratsi, M. I., Popov, O., Alexopoulos, C., & Charalabidis, Y. (2022). Ethical and Legal Aspects of Digital Forensics Algorithms: The Case of Digital Evidence Acquisition. *ACM International Conference Proceeding Series*, 32–40. https://doi.org/10.1145/3560107.3560114

Molina Granja, F., & Rodríguez Rafael, G. D. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 1. https://doi.org/10.1504/ijesdf.2017.10002624

Montasari, R., Peltola, P., & Evans, D. (2015). Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. *Communications in Computer and Information Science*, *534*, 83–95. https://doi.org/10.1007/978-3-319-23276-8_8

Moreb, M., Salah, S., & Amro, B. (2024). A Novel *Framework* for Mobile Forensics Investigation Process. *International Journal of Computing and Digital Systems*, *16*(1), 125–136. https://doi.org/10.12785/ijcds/160110

Neale, C., Kennedy, I., Price, B., Yu, Y., & Nuseibeh, B. (2022). The case for Zero Trust Digital Forensics. *Forensic Science International: Digital Investigation*, *40*, 301352. https://doi.org/10.1016/j.fsidi.2022.301352

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, *33*, 200908. https://doi.org/10.1016/j.fsidi.2020.200908

NIST. (2022). Zero Trust Architecture. *Controlling Privacy and the Use of Data Assets*, 127–134. https://doi.org/10.1201/9781003189664-11

Nortjé, J. G. J., & Myburgh, D. C. (2019). The search and seizure of digital evidence by forensic investigators in South Africa. *Potchefstroom Electronic Law Journal*, *22*(22), 1–42. https://doi.org/10.17159/1727-3781/2019/v22i0a4886

Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., Shin, H., Han, C., & Kim, J. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *Digital Investigation*, *24*.

Prayudi, Y., Ashari, A., & K Priyambodo, T. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Information Security*, *7*(11), 1–8. https://doi.org/10.5815/ijcnis.2015.11.01

Renaud, K., Bongiovanni, I., Wilford, S., & Irons, A. (2021). PRECEPT-4-Justice: A bias-neutralising *framework* for digital forensics investigations. *Science and Justice*, *61*(5), 477–492. https://doi.org/10.1016/j.scijus.2021.06.003

Saaty, L., T. (2008). Decision Making with the analytic hierarcy process. *International Journal Services Sciences*, *1*(1), 83–98. https://doi.org/10.1108/JMTM-03-2014-0020

Saleem, S., Popov, O., & Bagilli, I. (2014). Extended abstract digital forensics model with preservation and protection as umbrella principles. *Procedia Computer Science*, *35*, 812–821. https://doi.org/10.1016/j.procs.2014.08.246

Seigfried-Spellar, K. C., Rogers, M., & Crimmins, D. M. (2017). Development of A Professional Code of Ethics in Digital Forensics. *Annual ADFSL Conference on Digital Forensics, Security and Law*, *9*(c), 15. https://commons.erau.edu/adfsl/2017/papers/12

Simarmata, J., Manuhutu, M. A., & Yendrianof, D. (2021). *Dasar-dasar Teknologi Informasi* (R. Watrianthos (ed.)).

Sloan, J. (2015). There's no code of ethics to govern digital forensics – and we need

one. *Theconversation.Com*, *August*. https://theconversation.com/theres-no-code-of-ethics-to-govern-digital-forensics-and-we-need-one-45755

Soltani, S., & Seno, S. A. H. (2019). A formal model for event reconstruction in digital forensic investigation. *Digital Investigation*, *30*, 148–160. https://doi.org/10.1016/j.diin.2019.07.006

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Surveys and Tutorials*, *22*(2), 1191–1221. https://doi.org/10.1109/COMST.2019.2962586

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*, *40*, 301351. https://doi.org/10.1016/j.fsidi.2022.301351

Sudyana, D. (2019). Analysis and Evaluation Digital Forensic Investigation *Framework* Using Iso 27037:2012. *International Journal of Cyber-Security and Digital Forensics*, *8*(1), 1–14. https://doi.org/10.17781/p002464

Sutherland, I., Bovee, M., Xynos, K., & Read, H. O. L. (2023). Legal and ethical issues of pre-incident forensic analysis. *European Conference on Information Warfare and Security, ECCWS*, *22*(2023), 466–473. https://doi.org/10.34190/eccws.22.1.358

Tian, J., Wang, H., & Wang, M. (2021). Data integrity auditing for secure cloud storage using user behavior prediction. *Computers and Security*, *105*.

Tikhonov, A. (2019). Preservation of digital images: Question of fixity. *Heritage*, *2*(2), 1160–1165. https://doi.org/10.3390/heritage2020075

Xu, Y. Q., Jin, L. S., Chen, Z. S., Yager, R. R., Špirková, J., Kalina, M., & Borkotokey, S. (2022). Weight Vector Generation in Multi-Criteria Decision-Making with Basic Uncertain Information. *Mathematics*, *10*(4), 1–11. https://doi.org/10.3390/math10040572