Scopus

## Documents

Hakim, A.R.[a] , Ramli, K.[a] , Gunawan, T.S.[b c] , Windarta, S.[a]

**A Novel Digital Forensic Framework for Data Breach Investigation**
(2023) *IEEE Access*, 11, pp. 42644-42659.

**DOI:** 10.1109/ACCESS.2023.3270619

[a] Universitas Indonesia, Faculty of Engineering, Department of Electrical Engineering, Depok, 16424, Indonesia
[b] International Islamic University Malaysia, Kulliyyah of Engineering, Department of Electrical and Computer Engineering, Kuala Lumpur, 50728, Malaysia
[c] Telkom University, School of Electrical Engineering, Bandung, 40257, Indonesia

**Abstract**
Data breaches are becoming an increasingly prevalent and global concern due to their massive impact. One of the primary challenges in investigating data breach incidents is the unavailability of a specific framework that acknowledges the characteristics of a data breach incident and provides clear steps on how the investigative framework can comprehensively answer what, who, when, where, why, and how (5WH) questions. This paper aims to develop a novel digital forensic investigation framework that can overcome these data breach investigation challenges. The proposed framework utilizes the data breach breakdown phases to analyze data breach incidents according to their characteristics. The main contribution of our work is a novel digital forensic framework for data breach investigation that enhances the 5WH analysis depth by utilizing evidence classification and artifact visualization based on data breach breakdown phases. Furthermore, we design the framework components to provide comprehensive analysis results that make it easier for investigators to summarize the answers to the 5WH questions. To validate the framework, we apply it to a case study of enterprise-level data breach incidents. Based on the case study analysis, the proposed investigation framework successfully provides all the answers to the 5WH questions. This comprehensive answering ability is the study's fundamental strength compared to other digital forensic investigation frameworks. © 2013 IEEE.

**Author Keywords**
Data breach; digital forensics; framework; investigation

**Index Keywords**
Computer crime, Data visualization, Electronic crime countermeasures; Case study analysis, Case-studies, Comprehensive analysis, Data breach, Forensic investigation, Framework, Investigation; Digital forensics

**References**

- Widup, S., Pinto, A., Hylender, D., Bassett, G., Langlois, P.
*DBIR 2021 data breach investigation report*, p. 2021.
Verizon Bus., New York, NY, USA, Tech. Rep. 2021DBIR

- (2022) *The State of Data Breach Intelligence: 2022 Midyear Edition | Flashpoint*,
Online.

- *Elevating the Cybersecurity Discussion: Why CEOs Need to Get More Involved in Securing the Business*,
2022. Online.

- Schlackl, F., Link, N., Hoehle, H.
**Antecedents and consequences of data breaches: A systematic review**
*Inf. Manag.*, 59 (4).
Jun. 2022, Art.. Online.

- Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D.
**A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate**
(2018) *J. Cybersecurity*, 4 (1).
Jan. Art.

- Choong, P., Hutton, E., Richardson, P.S., Rinaldo, V.
  **Protecting a brand: Evaluating the cost of a security breach from a marketer's perspective**
  (2017) *Amer. J. Manag.*, 11 (1), pp. 59-67.

- Wang, P., D'Cruze, H., Wood, D.
  **Economic costs and impacts of business data breaches**
  (2019) *Issues Inf. Syst.*, 20, pp. 162-171.
  Apr

- Banker, R.D., Feng, C.
  **The impact of information security breach incidents on CIO turnover**
  (2019) *J. Inf. Syst.*, 33 (3), pp. 309-329.
  Sep. Online.

- Roumani, Y.
  **Detection time of data breaches**
  *Comput. Secur.*, 112 (2022).
  Jan. Art.

- Song, Z., Wang, G.A., Fan, W.
  **Firm actions toward data breach incidents and firm equity value: An empirical study**
  (2017) *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, pp. 4957-4966.
  Online.

- Kolevski, D., Michael, K., Abbas, R., Freeman, M.
  **Cloud data breach disclosures: The consumer and their personally identifiable information (PII)?**
  *Proc. IEEE Conf. Norbert Wiener 21st Century (CW)*, pp. 1-9.
  Wollongong, NSW, Australia: Institute of Electrical and Electronics Engineers, Jul. 2021,.
  Online.

- Meisner, M.
  **Financial consequences of cyber attacks leading to data breaches in healthcare sector**
  (2018) *Copernican J. Finance Accounting*, 6 (3), p. 63.
  Mar. Online.

- Malliouris, D.D., Simpson, A.
  **Underlying and consequential costs of cyber security breaches: Changes in systematic risk**
  *Proc. Workshop Econ. Inf. Secur.*, 2020, pp. 1-59.

- Muzatko, S., Bansal, G.
  **Consumer skepticism as it relates to E commerce data breaches and company efforts to enhance trust**
  *Proc. MWAIS*, 2020, pp. 1-5.

- Pool, J.K., Akhlaghpour, S., Fatehi, F., Burton-Jones, A.
  **Causes and impacts of personal health information (PHI) breaches: A scoping review and thematic analysis**
  (2019) *Proc. 23rd Pacific Asia Conf. Inf. Syst.*, pp. 71-85.
  D. Xu, J. Jiang, and H. W. Kim, Eds. Online.

- Aivazpour, Z., Valecha, R., Chakraborty, R.
  **The impact of data breach severity on post-breach online shopping intention**
  (2018) *Proc. 39th Int. Conf. Inf. Syst.*, pp. 481-489.
  Online.

- Martin, K.D., Borah, A., Palmatier, R.W.
  **Data privacy: Effects on customer and firm performance**

(2017) *J. Marketing*, 81 (1), pp. 36-58.
Online.

- Kashmiri, S., Nicol, C.D., Hsu, L.
**Birds of a feather: Intra-industry spillover of the target customer data breach and the shielding role of IT, marketing, and CSR**
(2017) *J. Acad. Marketing Sci.*, 45 (2), pp. 208-228.
Mar. Online.

- Durowoju, O., Chan, H.K., Wang, X.
**Investigation of the effect of e-platform information security breaches: A small and medium enterprise supply chain perspective**
*IEEE Trans. Eng. Manag.*, 69 (6), pp. 3694-3709.
Dec. 2022

- Haislip, J., Kolev, K., Pinsker, R., Steffen, T.
**The economic cost of cybersecurity breaches: A broad-based analysis**
(2019) *Proc. Workshop Econ. Inf. Secur. (WEIS)*, pp. 1-37.

- He, Z., HuangFu, J., Kohlbeck, M.J., Wang, L.
*The impact of customer's reported cybersecurity breaches on key supplier's relationship-specific investments and relationship duration*,
Feb. 2020. Online.

- Chua, H.N., Teh, J.S., Herbland, A.
**Identifying the effect of data breach publicity on information security awareness using hierarchical regression**
(2021) *IEEE Access*, 9, pp. 121759-121770.

- (2021) *Cost of a Data Breach Report 2021*,
Online.

- (2022) *IBM Security's Cost of a Data Breach Report 2022*,
IBM Corp., New York, NY, USA

- Morgan, S.
(2020) *Cybercrime to Cost the World $ 10.5 Trillion Annually by 2025*,
Online.

- Furnell, S., Heyburn, H., Whitehead, A., Shah, J.N.
**Understanding the full cost of cyber security breaches**
*Comput. Fraud Secur.*, 2020 (12), pp. 6-12.
2020

- Say, G., Vasudeva, G.
**Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches**
*Strategy Sci*, 5 (2), pp. 117-142.
Jun. 2020

- Khanafseh, M., Qatawneh, M., Almobaideen, W.
**A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics**
(2019) *Int. J. Adv. Comput. Sci. Appl.*, 10 (8), pp. 610-629.

- Ariffin, K.A.Z., Ahmad, F.H.
**Indicators for maturity and readiness for digital forensic investigation in era of industrial Revolution 4.0**
*Comput. Secur.*, 105 (2021).
Jun. Art.

- Overill, R.E., Collie, J.
**Quantitative evaluation of the results of digital forensic investigations: A review of progress**
(2021) *Forensic Sci. Res.*, 6 (1), pp. 13-18.
Jan

- Rogers, M., Goldman, J., Mislan, R., Wedge, T., Debrota, S.
**Computer forensics field triage process model**
(2006) *J. Digit. Forensics, Secur. Law*, 1 (2), pp. 1-21.
Online.

- Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C.
**Systematic digital forensic investigation model**
(2011) *Int. J. Comput. Sci. Secur. (IJCSS)*, 5 (1), pp. 118-131.
Online.

- Kohn, M.D., Eloff, M.M., Eloff, J.H.P.
**Integrated digital forensic process model**
(2013) *Comput. Secur.*, 38, pp. 103-115.
Oct

- Dimitriadis, A., Ivezic, N., Kulvatunyou, B., Mavridis, I.
**D4I—Digital forensics framework for reviewing and investigating cyber attacks**
*Array*, 5.
Mar. 2020, Art.

- Acar, K.V.
**Osint by crowdsourcing: A theoretical model for online child abuse investigations**
(2018) *Int. J. Cyber Criminology*, 12 (1), pp. 206-229.

- Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., Patsakis, C.
**SoK: Cross-border criminal investigations and digital evidence**
(2022) *J. Cybersecurity*, 8 (1), pp. 1-18.
Jan. Online.

- Zarpala, L., Casino, F.
**A blockchain-based forensic model for financial crime investigation: The embezzlement scenario**
*Digit. Finance*, 3 (3-4), pp. 301-332.
nos. Dec. 2021. Online.

- Kent, K., Chevalier, S., Grance, T., Dang, H.
**Guide to integrating forensic techniques into incident response**
(2006) *Nat. Inst. Standards Technol.*,
Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-86

- Fowler, K.
(2016) *Data Breach Preparation and Response: Breaches are Certain, Impact is Not*,
MA, USA: Elsevier

- Mir, S.S., Shoaib, U., Sarfraz, M.S.
**Analysis of digital forensic investigation models**
(2016) *Int. J. Comput. Sci. Inform. Secur.*, 14 (11), pp. 292-301.
Online.


**Correspondence Address**
Ramli K.; Universitas Indonesia, Indonesia; email: kalamullah.ramli@ui.ac.id

**Publisher:** Institute of Electrical and Electronics Engineers Inc.

**ISSN:** 21693536
**Language of Original Document:** English
**Abbreviated Source Title:** IEEE Access

2-s2.0-85159661346
**Document Type:** Article
**Publication Stage:** Final
**Source:** Scopus