VolWeb meets YARA for Socio-Technical Incident Response

Marco Ferrara[1], Davide Pio Posa[2], Gennaro Del Campo[2] and Andrea Garavaglia[3]

[1]*MNTCRL LABoratory*
[2]*SER&Practices, Spin-off of the University of Bari Aldo Moro*
[3]*Leonardo*

Abstract

The increasing convergence of technical and social layers within cyberspace calls for investigative tools that support both forensic depth and socio-technical intelligence. VolWeb is a digital forensic memory-analysis platform built on the Volatility 3 framework, designed to streamline evidence acquisition, automated artifact extraction, and collaborative incident response. By enabling centralized memory-image analysis, remote evidence upload, and integration with Cyber Threat Intelligence (CTI) platforms such as OpenCTI, VolWeb strengthens the analytical workflow of forensic and threat-intelligence teams.

Aligned with the principles of Cyber Social Security, VolWeb extends beyond technical investigation by correlating system-level artifacts with behavioral indicators, social-impact dynamics, and broader threat patterns. Furthermore, the platform incorporates centralized management of YARA rules, allowing analysts to upload, validate, and organise rules into logical rulesets that can be systematically applied during forensic investigations. This capability enhances pattern detection, improves interpretability for analysts, and contributes to a more holistic socio-technical understanding of cyber incidents.

Keywords

VolWeb, YARA, Threat Intelligence, Social Security, Cybersecurity

1. Introduction

The growing complexity of contemporary cyber threats increasingly blurs the boundary between purely technical incidents and broader socio-technical phenomena [1, 2]. Modern cyber operations are rarely confined to isolated system compromises; instead, they manifest as coordinated campaigns that intertwine malware activity, behavioral manipulation, strategic communication, and social impact [3]. In this context, traditional digital forensics tools—while technically robust—often fall short in supporting the analytical depth and contextual awareness required to understand cyber incidents as systemic events [4].

VolWeb[1] addresses this gap by positioning memory forensics as a foundational component of a broader socio-technical investigative framework. Built on top of the Volatility[2] 3 engine, the platform preserves the rigor and completeness of low-level memory analysis while extending its analytical scope toward Cyber Social Security principles [5]. This paradigm emphasizes the integration of technical evidence with behavioral indicators, threat intelligence, and operational context, enabling investigators to reason not only about how a system was compromised, but also why and with what broader implications [6].

The conceptual foundations of VolWeb are rooted in prior experiences with large-scale memory forensics platforms, most notably Orochi[3], a collaborative memory forensics platform developed by

1st Workshop on Symbiotic AI for Cyber Social Security: Human–AI Collaboration for Social Resilience and Trustworthy Digital Ecosystems (SAI4CCS 2026), co-located with the 2nd Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09–13, 2026, Cagliari, Italy

m.ferrara62@studenti.uniba.it (M. Ferrara); d.posa3@studenti.uniba.it (D. P. Posa); g.delcampo@serandp.com (G. D. Campo); andrea.garavaglia@leonardo.com (A. Garavaglia)
0009-0009-0257-3367 (D. P. Posa)

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

[1]https://github.com/k1nd0ne/VolWeb
https://github.com/imb0ru/VolWeb/tree/YARA-Integration
https://github.com/k1nd0ne/VolWeb/pull/42
[2]https://github.com/volatilityfoundation
[3]https://github.com/LDO-CERT/orochi

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-14

CEUR-WS.org/Vol-4329/paper13.pdf

Leonardo's Computer Emergency Response Team (LDO-CERT). Orochi demonstrated how Volatility-based forensics could be operationalized in complex organizational environments, enabling parallel analysis, centralized orchestration, and integration within structured incident response processes.

The development of VolWeb was directly inspired by both the technical architecture and the operational lessons learned from Orochi[4], as well as by insights gained during a preliminary technical meeting with the authorsThat exchange highlighted not only the strengths of Orochi in handling large forensic workloads but also the challenges related to analyst interaction, explainability, and the integration of forensic results into broader socio-technical decision-making processes.

A central design choice in VolWeb is the correlation of volatile-memory artifacts with higher-level threat intelligence constructs. Extracted indicators—such as malicious processes, injected code, persistence mechanisms, and anomalous execution patterns—are structured and normalized to facilitate cross-case comparison and enrichment . Through integration with Cyber Threat Intelligence (CTI) platforms such as OpenCTI[5], these artifacts can be contextualized within known adversary TTPs (Tactics, Techniques, and Procedures), campaigns, and threat actor profiles, supporting attribution hypotheses and strategic assessment. This capability is particularly relevant in scenarios such as large-scale cyber defense exercises or national-level incident response, where forensic findings must be rapidly translated into actionable intelligence [7].

In alignment with the operational requirements observed in high-intensity environments such as NATO CCDCOE Locked Shields[6], VolWeb further enhances collaborative and cognitive dimensions of DFIR (Digital Forensics and Incident Response). The platform supports centralized case management, shared analytical workspaces, and structured annotation of findings, enabling multidisciplinary teams—ranging from forensic analysts to cyber intelligence and legal experts—to operate on a common evidentiary base. This shared situational awareness is essential for maintaining coherence between technical analysis, legal evaluation, and strategic communication under time pressure.

A key enabler of this socio-technical integration is the centralized management of YARA rules[7] within VolWeb. Rather than treating YARA as an external or auxiliary capability, the platform incorporates rule creation, validation, organization, and execution as first-class forensic functions. Analysts can maintain curated rulesets aligned with specific threat models or investigative objectives and systematically apply them across multiple memory images [8]. This approach not only improves detection accuracy and scalability, but also enhances interpretability by making detection logic explicit, reproducible, and shareable across teams [9]. From a Cyber Social Security perspective, such transparency supports accountability, methodological rigor, and trust in forensic outcomes .

By combining low-level memory forensics with collaborative workflows, CTI integration, and explainable pattern-matching mechanisms, VolWeb exemplifies a shift from tool-centric analysis toward platform-based socio-technical intelligence. The result is an investigative environment capable of supporting both forensic depth and strategic reasoning, bridging the gap between technical evidence and its broader operational, organizational, and societal implications.

2. Related Work

The need to shift from reactive incident response toward proactive forensic readiness, integrating digital forensics into routine cybersecurity operations [10]. In this context, digital forensics enables the systematic analysis of cyber incidents, offering critical insights into their nature, origin, and impact [11, 12]. The value-based data protection has been proposed through structured data classification approaches that prioritize assets according to sensitivity and impact, enabling more effective allocation of security controls [13]. Complementary to this, randomized and unannounced cyberattack simulations have been suggested as a means to realistically assess incident response readiness, surpassing traditional

[4]https://github.com/LDO-CERT/orochi
[5]https://github.com/OpenCTI-Platform/opencti
[6]https://ccdcoe.org/locked-shields
[7]https://github.com/Yara-Rules

scheduled penetration testing [14]. The literature further underscores that forensic preparedness must be supported by comprehensive policies, continuous workforce training, inter-organizational collaboration, adherence to international standards (e.g., NIST, SANS), and advanced technical defenses, including honeypots and proactive monitoring mechanisms [15, 16].

Chen et al. [17] examine the need for new forensic processes, approaches, methods, and tools specifically designed for cloud and social network environments, which differ significantly from traditional digital forensics due to their distinct data storage and processing methods. Karabiyik et al. [18] provide a comprehensive survey of social network forensics, emphasizing the importance of analyzing data generated through online social networks for criminal and terrorist activity investigations, while also addressing defense methods for users against social attacks. Instead, Hijan [19] explores recent developments, including cloud forensics, social media forensics, and IoT forensics, identifying technical, operational, and personnel-related challenges while highlighting opportunities through artificial intelligence and intrusion detection. Sindhu & Meshram [20] propose combining digital forensic investigation with crime data mining to identify attack patterns, motives, and frequencies, enabling system administrators to minimize vulnerabilities.

Collectively, these contributions advocate for a holistic framework in which proactive digital forensics enhances organizational resilience against increasingly sophisticated cyber threats. So, this research paper introduces VolWeb, a platform that extends beyond traditional technical investigation by correlating system-level artefacts with behavioural indicators, social impact dynamics, and broader threat models. Furthermore, VolWeb integrates centralized YARA rule management, enabling analysts to upload, validate, and organize rules into logical sets that can be systematically applied throughout forensic investigations.

3. VolWeb meets YARA for Socio-Technical Incident Response

3.1. VolWeb: Architecture

VolWeb[8] is a web-based digital forensics platform designed to orchestrate and extend memory analysis workflows based on the Volatility 3 framework. Its primary goal is to reduce the operational complexity of memory forensics while preserving analytical depth, enabling investigators to perform scalable, repeatable, and collaborative analyses of volatile memory images. Unlike traditional command-line-driven approaches, VolWeb provides a centralized environment in which memory acquisition artifacts, analysis results, and investigative context are managed coherently at the case level.

It is designed around three closely interconnected objectives:

1. *Simplifying access to memory forensics.* VolWeb abstracts the complexity of Volatility through an intuitive interface without sacrificing analytical power, significantly reducing the time required to obtain actionable results and enabling effective investigations even by less experienced analysts.
2. *Standardizing investigative workflows.* It introduces a structured investigative framework that mitigates the inconsistencies and inefficiencies arising from the unstructured use of Volatility, ensuring completeness and reproducibility across teams with heterogeneous expertise.
3. *Fostering collaboration.* The platform supports collaborative investigations by providing a shared environment in which geographically and temporally distributed analysts can jointly work on cases, exchange observations, and develop a coherent understanding of security incidents.

At its core, VolWeb acts as an abstraction layer over Volatility 3, decoupling forensic execution from user interaction. Memory images can be remotely uploaded and associated with investigative cases, after which predefined or customized analysis pipelines are automatically executed. The results produced by Volatility plugins are normalized and stored in a structured format, allowing analysts to efficiently navigate artifacts such as running processes, loaded modules, network connections, injected

[8] https://github.com/k1nd0ne/VolWeb
https://github.com/imb0ru/VolWeb/tree/YARA-Integration
https://github.com/k1nd0ne/VolWeb/pull/42

code, and persistence mechanisms. This structured representation supports rapid triage, cross-analysis, and reproducibility—capabilities that are essential in time-constrained incident response scenarios.

The design philosophy of VolWeb draws inspiration from existing collaborative forensic platforms, particularly Orochi[9], developed by the Leonardo Computer Emergency Response Team (LDO-CERT). Orochi pioneered the concept of a web-based, multi-analyst environment for Volatility-driven memory analysis, demonstrating the viability and operational value of distributed forensic workflows. Insights gathered during preliminary meetings with Andrea Garavaglia, one of Orochi's core contributors, proved instrumental in shaping the architectural and functional directions pursued in VolWeb.

From a design perspective, VolWeb inherits several architectural principles originally explored in Orochi, particularly the separation between forensic execution and orchestration logic, as well as the emphasis on scalability and reproducibility of memory analysis. Early discussions with the Orochi development team highlighted the growing need for greater transparency, interpretability, and contextual enrichment of forensic results—requirements that guided the subsequent development of VolWeb. In response, VolWeb introduces a web-based investigative workspace with structured case management, extensible analysis pipelines explicitly supporting human-in-the-loop investigation, and native integration with Cyber Threat Intelligence frameworks and centralized YARA management. In this sense, VolWeb can be seen as a complementary evolution of Orochi's vision: retaining the rigor of automated memory forensics while embedding it within a platform designed to support collective sense-making and intelligence-driven incident response.

3.2. Architectural Design and Extension Model

VolWeb is designed around a modular and extensible architecture that explicitly supports future functional expansion (Figure 1). Rather than embedding all analysis logic within a monolithic workflow, the platform exposes well-defined extension points at both backend and frontend levels. These extension points enable the integration of new analytical capabilities without modifying the core system, ensuring maintainability and adaptability to evolving forensic requirements.

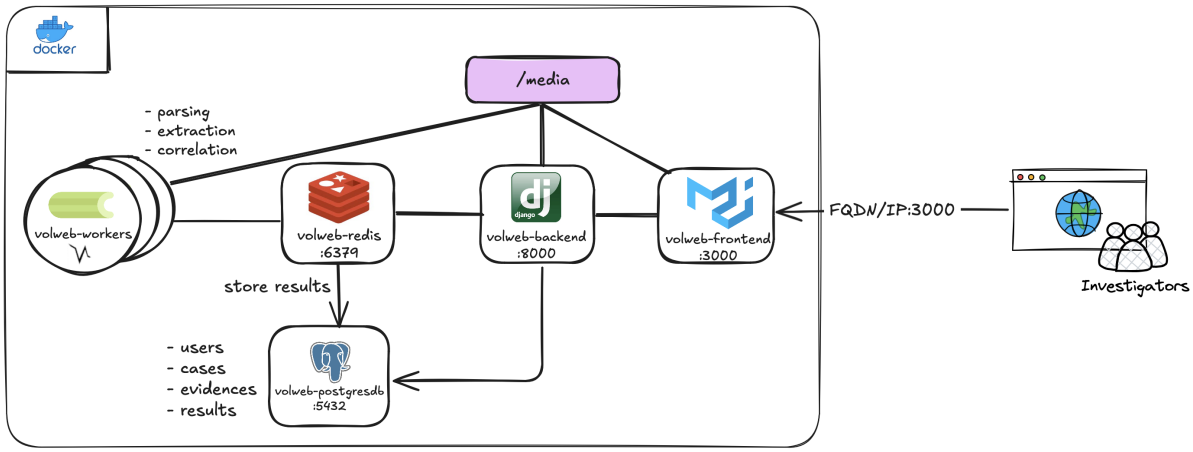


Figure 1: VolWeb Architecture

Key extension points include:

- *Analysis Pipeline Extensions*, allowing additional processing stages to be inserted before or after Volatility execution (e.g., pre-processing, triage, enrichment).
- *Artifact Processing Modules*, enabling the parsing, correlation, and enrichment of forensic outputs beyond default Volatility plugins.

[9]https://github.com/LDO-CERT/orochi

- *Visualization and Interpretation Layers*, supporting custom views and dashboards tailored to specific investigative objectives.
- *External Intelligence Integration Interfaces*, designed to correlate forensic findings with Cyber Threat Intelligence platforms.

This architectural approach transforms VolWeb from a visualization frontend into a platform capable of hosting advanced forensic and intelligence-driven capabilities.

3.3. Implemented Extensions: Centralized YARA Integration

Among the available extension points, the integration of YARA-based pattern matching represents the primary functional extension developed in this work. The choice of YARA is motivated by its widespread adoption as a standard for malware detection and classification, as well as by the operational requirements observed in high-intensity forensic scenarios.

The YARA[10] extension transforms VolWeb into a centralized rule-driven threat hunting environment. Instead of relying on ad hoc or external YARA executions, the platform introduces a native subsystem for YARA rule management, including rule upload, validation, organization, and logical grouping into reusable rulesets. These rulesets can be systematically applied during memory analysis, enabling consistent pattern matching across multiple memory images and investigative cases.

From an architectural perspective, the YARA subsystem operates as an independent backend module that interfaces with the VolWeb analysis pipeline. This design ensures isolation from core components while enabling tight integration with case management and result visualization. Scan results are stored alongside other forensic artifacts and presented in a structured and interpretable manner, facilitating analyst validation and knowledge sharing.

3.4. Impact on Forensic Workflow

The introduction of extensible analysis pipelines and centralized YARA management significantly enhances the operational capabilities of VolWeb. Analysts benefit from improved scalability, as pattern matching can be applied uniformly across large sets of memory images. Moreover, detection logic becomes explicit, auditable, and reusable, supporting methodological rigor and collaborative investigation.

By exposing and exploiting its extension points, VolWeb evolves from a tool for executing memory analysis into a flexible socio-technical forensic platform. The implemented extensions demonstrate how VolWeb can accommodate advanced detection mechanisms and lay the groundwork for future enhancements, including automated triage, behavioral correlation, and deeper integration with threat intelligence ecosystems.

4. Volweb in a Socio-Technical Incident Response: a Use Case

The implementation of VolWeb's extensions, while architecturally sound and functionally comprehensive, requires rigorous validation to demonstrate their effectiveness in real-world operational contexts [21]. This section presents the validation process conducted through the forensic analysis of a system compromised by WannaCry[11], the ransomware responsible for one of the most disruptive cyberattack campaigns in history. First observed in May 2017, WannaCry affected more than 230,000 computers across over 150 countries, causing estimated damages amounting to several billions of US dollars.

The selection of WannaCry as a case study is motivated by several converging factors that make it particularly suitable for a comprehensive evaluation. Its widespread notoriety and extensive documentation provide a well-established benchmark against which analytical results can be systematically compared. The availability of deactivated samples for research purposes, together with mature YARA

[10]https://yara.readthedocs.io
[11]https://www.europol.europa.eu/wannacry-ransomware

rules developed by the security community in the years following the outbreak, enables an objective assessment of detection capabilities. Moreover, the relative simplicity of WannaCry's propagation and encryption mechanisms, when compared to more recent ransomware families, allows the evaluation to focus on the validation of core forensic functionalities without being confounded by advanced evasion techniques. Finally, the historical impact of WannaCry makes it a relevant case study from both educational and operational perspectives, serving as a paradigmatic example of how memory forensics can contribute to the understanding and mitigation of large-scale cyber threats.

Specifically, the system identified a total of 851 matches (Figure 2). Among the rules that detected the ransomware were "TestWannaCry", multiple instances of "WannaCry_MemoryScan" and "FE_RANSOMWARE_WANNACRY". The "Component" column indicates which specific element of each rule generated the match - mainly strings named $a, $proc1, $proc2, $proc3 and $fileB4. The offsets show that the patterns were found in different areas of memory, confirming the distributed presence of the malware in the system.

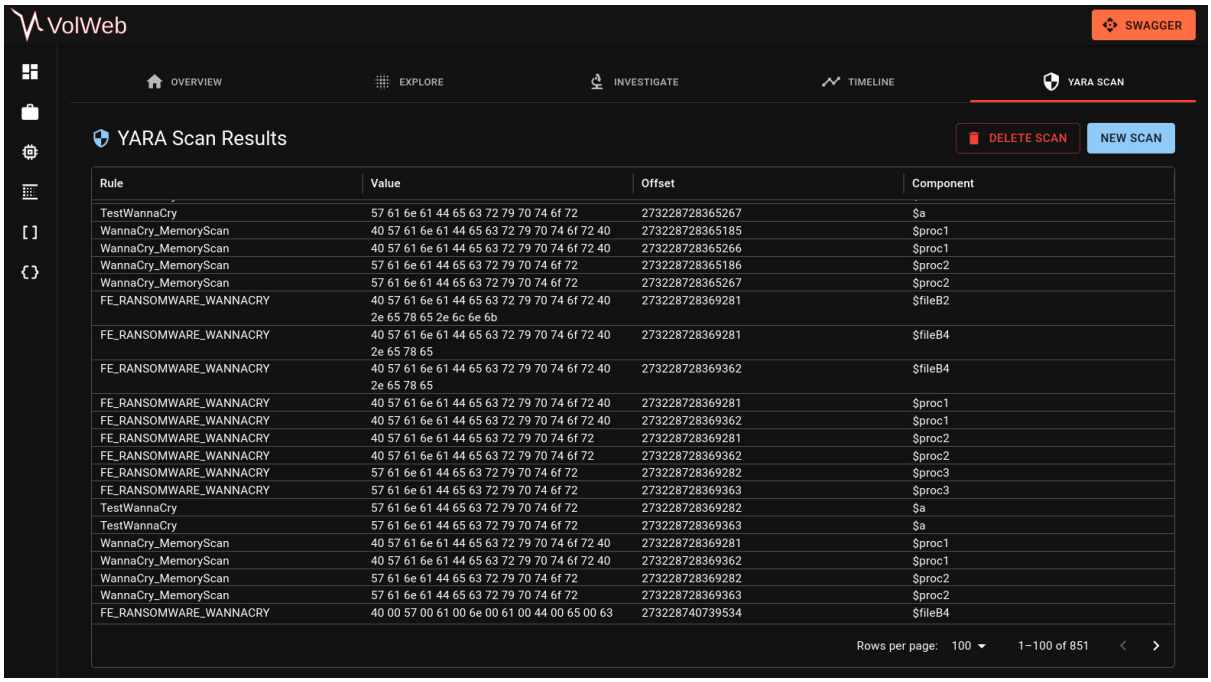


Figure 2: Scan results with the application of public rulesets

Instead, applying the custom rule "WannaCry_Custom" generated 5,442 matches (Figure 3). This is significantly higher than the public rulesets. This volume stems from the comprehensive nature of the rule, which identifies multiple indicators of ransomware: target file extensions ($ext1, $ext2, $ext3), malware-specific files ($file5), cache patterns ($cache), references to processes ($proc1), libraries ($dll3), characteristic paths ($path1, $path2) and suspicious VAD sizes ($vad_size).

The high number of matches, although indicative of redundancy, demonstrates that the YARA integration is working correctly and that VolWeb is able to handle and present large volumes of results while maintaining a responsive interface.

5. Conclusion

This paper presented VolWeb as a socio-technical memory forensics platform designed to address the evolving requirements of modern incident response. By integrating Volatility-based analysis, centralized YARA management, collaborative workflows, and threat intelligence correlation, VolWeb bridges the gap between low-level forensic evidence and strategic cyber situational awareness.

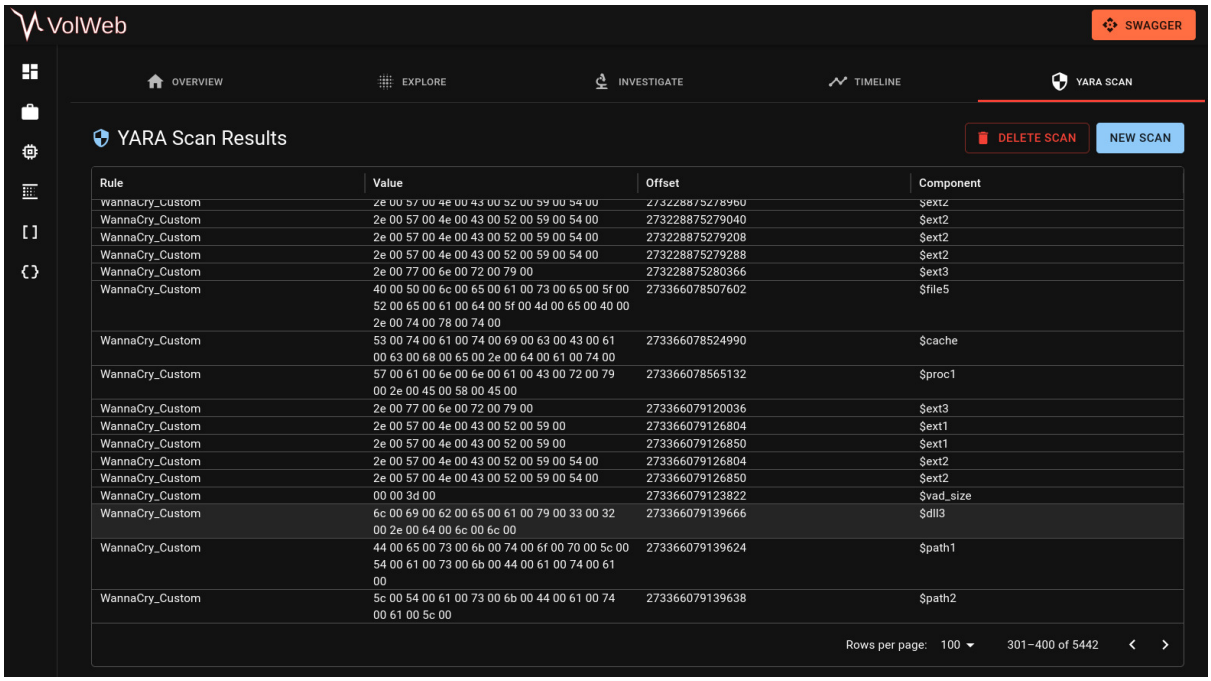


Figure 3: Scan results with the custom rule applied

The operational requirements derived from the need for scalable, explainable, and intelligence-driven DFIR tools. VolWeb demonstrates how these requirements can be addressed within a unified platform. Future work will focus on enhanced automation, advanced correlation mechanisms, and broader governance and compliance considerations.

Acknowledgments

This work was partially supported by the following projects: SERICS - “Security and Rights In the CyberSpace - SERICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU; Accordo Quadro CrASte - “Cyber Academy for Security and Intelligence”; SETH: Security Education and Training Hybrid-Wargame, Avviso “Reti - Sostegno alla ricerca collaborativa” - Codice progetto BM755Y1.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] V. S. Barletta, D. Caivano, C. Catalano, M. de Gemmis, D. Impedovo, Cyber social security education, in: L. T. De Paolis, P. Arpaia, M. Sacco (Eds.), Extended Reality, Springer Nature Switzerland, Cham, 2024, pp. 240–248.

[2] J. D. Patón-Romero, M. T. Baldassarre, M. Rodríguez, M. Piattini, Application of iso 14000 to information technology governance and management, Computer Standards and Interfaces 65 (2019) 180 – 202. doi:10.1016/j.csi.2019.03.007.

[3] J. S. Bardin, Cyber warfare, in: Computer and Information Security Handbook, Elsevier, 2025, pp. 1345–1380.

[4] M. Tretyak, L. Cherckesova, D. Korochentsev, E. Revyakina, A. Popov, Internet platform for analyzing computer memory of windows operating systems for conducting information security investigations, in: E3S Web of Conferences, volume 402, EDP Sciences, 2023, p. 03027.

[5] V. S. Barletta, M. Calvano, A. Sciacovelli, Cyber social security in multi-domain operations, in: 2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense), 2024, pp. 41–46. doi:10.1109/TechDefense63521.2024.10863352.

[6] M. T. Baldassarre, M. Piattini, F. J. Pino, G. Visaggio, Comparing iso/iec 12207 and cmmi-dev: Towards a mapping of iso/iec 15504-7, 2009, p. 59 – 64. doi:10.1109/WOSQ.2009.5071558.

[7] K. G. Boamah, A. Asante, A. Timean, K. F. Okai, Artificial intelligence integration in cyber incident response teams to enable faster containment, forensic accuracy, and resilient business continuity, International Journal of Science and Research Archive 17 (2025) 1263–1280.

[8] T. Baldassarre, N. Boffoli, D. Caivano, G. Visaggio, Managing software process improvement (spi) through statistical process control (spc), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 3009 (2004) 30 – 46. doi:10.1007/978-3-540-24659-6_3.

[9] M. Saltarella, G. Desolda, R. Lanzilotti, V. S. Barletta, Translating privacy design principles into human-centered software lifecycle: A literature review, International Journal of Human–Computer Interaction 40 (2024) 4465–4483. URL: https://doi.org/10.1080/10447318.2023.2219964. doi:10.1080/10447318.2023.2219964. arXiv:https://doi.org/10.1080/10447318.2023.2219964.

[10] B. K. Sharma, M. A. Joseph, B. Jacob, B. Miranda, Emerging trends in digital forensic and cyber security- an overview, in: 2019 Sixth HCT Information Technology Trends (ITT), 2019, pp. 309–313. doi:10.1109/ITT48889.2019.9075101.

[11] S. Banik, The role of digital forensics in cybersecurity investigations, International Journal of Advanced Engineering Technologies and Innovations 1 (2019) 294–302.

[12] V. S. Barletta, D. Caivano, C. Catalano, A. Gentile, D. P. Posa, A. Piccinno, Cyber digital twin to improve security education: the redteam knife approach, in: Proceedings of the 16th Biannual Conference of the Italian SIGCHI Chapter, CHItaly '25, Association for Computing Machinery, New York, NY, USA, 2025. doi:10.1145/3750069.3750102.

[13] K. Okereafor, R. Djehaiche, New approaches to the application of digital forensics in cybersecurity: a proposal, International Journal of Simulation: Systems, Scienece and Technology (IJSSST) 21 (2020) 36–1.

[14] R. Sabillon, J. Serra-Ruiz, V. Cavaller, J. J. Cano, Digital forensic analysis of cybercrimes: best practices and methodologies, International Journal of Information Security and Privacy (IJISP) 11 (2017) 25–37.

[15] M. Rawashdeh, Q. A. Al-Haija, Cybersecurity, forensic tools, and risk mitigation techniques, in: Cyber Security, Forensics and National Security, CRC Press, 2025, pp. 17–39.

[16] D. Paul Joseph, J. Norman, An analysis of digital forensics in cyber security, in: First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018, Springer, 2018, pp. 701–708.

[17] L. Chen, L. Xu, X. Yuan, N. Shashidhar, Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges, in: 2015 International Conference on Computing, Networking and Communications (ICNC), 2015, pp. 1132–1136. doi:10.1109/ICCNC.2015.7069509.

[18] U. Karabiyik, M. A. Canbaz, A. Aksoy, T. Tuna, E. Akbas, B. Gonen, R. S. Aygun, A survey of social network forensics, Journal of Digital Forensics, Security and Law 11 (2016) 8.

[19] A. I. Hijan, Digital forensic investigation tools for cases related to social media and cybersecurity, Ajrsp 5 (2023) 05–20.

[20] K. Sindhu, B. Meshram, Digital forensics and cyber crime datamining, Journal of Information Security 3 (2012) 196–201.

[21] M.-A. Storey, R. Hoda, A. Maciel Paz Milani, M. T. Baldassarre, Guiding principles for mixed methods research in software engineering, Empirical Software Engineering 30 (2025). doi:10.1007/s10664-025-10629-x.