INPLASY

INPLASY202370032

doi: 10.37766/inplasy2023.7.0032

Received: 09 July 2023

Published: 09 July 2023

Corresponding author:
Nuno Mourinho

19829@stu.ipbeja.pt

Author Affiliation:
Escola Superior de Tecnologia e Gestão de Beja, Beja, Portugal.

Protocol for a Systematic Review on the Impact of a Newly Developed Plugin in Autopsy Software for Virtualization and Control of Forensic Images on the Effectiveness and Efficiency of Cybercrime Investigations by Digital Forensic Investigators

Mourinho, N[1]; Candeias, M[2]; Bravo, R[3].

ADMINISTRATIVE INFORMATION

Support - The authors of this systematic review received no financial support or funding for this research from any public, private, or non-profit organization. All resources utilized for this study, including time and research tools, were provided by the authors themselves.

Review Stage at time of this submission - Data extraction.

Conflicts of interest - The authors declare that they have no conflicts of interest in relation to this research. There are no personal, professional, or financial relationships that could potentially influence or bias the authors' decisions, work, or manuscript. All authors confirm that they have no affiliations with or involvement in any organization or entity with a direct financial interest in the subject matter or materials discussed in this manuscript.

INPLASY registration number: INPLASY202370032

Amendments - This protocol was registered with the International Platform of Registered Systematic Review and Meta-Analysis Protocols (INPLASY) on 09 July 2023 and was last updated on 09 July 2023.

INTRODUCTION

Review question / Objective In digital forensic investigators examining cybercrime cases (P), does the use of a newly developed plugin that enables the virtualization and control of forensic images (I), compared to the current standard methods for investigating digital forensic images without the plugin (C), improve the ability to identify and analyze additional digital evidences, thereby enhancing the effectiveness and efficiency of investigations (O)?' This question will be investigated through a review and synthesis of existing experimental and observational studies that examine the use and efficacy of plugins for virtualizing and controlling forensic images (S).

Rationale The rationale for this systematic review emerges from the growing necessity for more efficient and effective digital forensic investigations, especially in the realm of cybercrime. As the digital world continues to evolve, so too does the sophistication of cybercrimes, thereby necessitating advanced tools and methods to effectively investigate and combat these crimes.

The proposed intervention, a newly developed plugin enabling the virtualization and control of forensic images, has the potential to significantly improve digital forensic investigations. However, its effectiveness compared to existing methodologies has yet to be comprehensively examined.

The plugin offers a promising advance in the field, with the potential to virtualize and control forensic

images more efficiently, thereby allowing investigators to identify and analyze additional pieces of digital evidence. If effective, this could significantly enhance the capabilities of digital forensic investigators in handling increasingly complex cybercrime cases.
Yet, despite the potential advantages, it is crucial to rigorously review the available evidence on this intervention before it is widely adopted in practice. This systematic review, framed using the PICOS model, seeks to answer whether this plugin can indeed improve the effectiveness and efficiency of digital forensic investigations compared to the current standard methods.
It will involve the synthesis of available experimental and observational studies examining the use and efficacy of this plugin, thereby providing a comprehensive evidence base to guide decision-making and practice in digital forensic investigations. This systematic review is, therefore, timely and relevant, given the pressing need for advanced tools and methods in digital forensic investigations.

Condition being studied The condition under study in this systematic review is not a traditional health condition or disease, but rather a circumstance within the field of digital forensics: the investigation of cybercrimes.
Cybercrime, a rapidly evolving and increasingly complex field, encompasses illegal activities that are conducted through digital means. It includes offenses such as hacking, identity theft, online fraud, cyberstalking, and cyberterrorism, among others. These criminal activities pose significant threats to individuals, businesses, and nations alike, leading to substantial economic losses and potential harm to national security.
Digital forensics is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices, often in relation to cybercrime. Digital forensic investigators analyze digital evidence to uncover what happened, how it happened, when it happened, and who was involved.
The specific aspect of this condition being examined in this review is the process of analyzing forensic images during cybercrime investigations. Forensic images are exact copies of digital data, and their analysis is crucial in understanding the nature and details of the cybercrime under investigation.
The intervention under review – a newly developed plugin that enables the virtualization and control of forensic images – has the potential to impact how these cybercrime investigations are conducted, potentially increasing their efficiency and effectiveness. Therefore, while this condition may not align with traditional conceptions of a health condition or disease, it nonetheless represents a significant area of interest with potentially far-reaching implications.

METHODS

Search strategy Our search strategy aims to be as comprehensive as possible to identify both published and unpublished studies. We will be conducting a systematic search using the following databases:
1. IEEE Xplore
2. ACM Digital Library
3. EBSCO
4. Web of Science
5. Scopus
6. Google Scholar (to identify any grey literature)

The search strategy will include terms related to each component of the PICOS framework. Here's an initial proposal for the search strategy, which should be adjusted according to each database's specifics:
• Population: ("Digital Forensics" OR "Cyber Forensics" OR "Cyber Investigators" OR "Cybercrime Investigators")
• Intervention: (("Plugin" AND “Autopsy Software”) OR "Software" OR "Digital Forensic Tools" OR "Forensic Imaging" OR "Virtualization")
• Comparison: ("Standard Method" OR "Conventional Tools" OR "Without Plugin")
• Outcomes: ("Efficiency" OR "Effectiveness" OR "Performance" OR "Detection Rate" OR "Additional Evidence")
• Study Design: ("Experimental Study")

The search will include both English and Portuguese-language articles to ensure a comprehensive and culturally diverse selection of relevant studies. All identified articles will undergo a title and abstract screening to assess eligibility based on pre-defined inclusion and exclusion criteria. Studies that appear to meet these criteria in either English or Portuguese will be retrieved for full-text review. This approach is designed to reduce language bias and provide a more global perspective on the impact and effectiveness of the digital forensics plugin under review.Additionally, the reference lists of all included studies will be manually searched to identify any other potentially relevant studies. The database search will be supplemented by a search of trial registers and relevant conference proceedings.
We will use a citation management software Zotero to de-duplicate the references and manage the screening and selection process. The search strategy may be revised in response to the findings, and any revisions will be documented in the final review.

Participant or population The participants in the studies to be addressed in this systematic review are digital forensic investigators involved in cybercrime investigations. These participants may encompass a variety of roles within the field of digital forensics, including but not limited to forensic analysts, forensic examiners, incident responders, and cybercrime investigators. They may work in a variety of settings such as law enforcement agencies, private corporations, cybersecurity firms, or government departments.The scope is not restricted to any particular geographic location or level of experience, as the intention is to capture a broad perspective on the impact of the newly developed plugin for the virtualization and control of forensic images. However, it is expected that all participants would have a basic competency in digital forensic investigation procedures and the handling of digital evidence.Importantly, the review will focus on studies involving actual use cases or simulation scenarios wherein these investigators utilize the plugin in the course of their digital forensic investigations, especially those relating to cybercrime. The emphasis is on practical application rather than theoretical analysis.

Intervention The intervention to be evaluated in this systematic review is a newly developed plugin that enables the virtualization and control of forensic images in digital forensic investigations. This tool represents a potential advancement in cybercrime investigation methodologies, offering the ability to virtualize and manipulate digital evidence more effectively.Specifically, the plugin is designed to assist digital forensic investigators by allowing for more efficient navigation through forensic images, potentially facilitating the discovery of additional digital evidence. This systematic review will assess studies examining the use of forensic images virtualization in real or simulated digital forensic investigations, with a focus on its potential to enhance the effectiveness and efficiency of cybercrime investigations.

Comparator The comparator for this systematic review will be the current standard methods used in digital forensic investigations for analyzing forensic images without the utilization of the newly developed plugin. These conventional methods may include a variety of software and manual procedures currently in widespread use among digital forensic investigators.These might encompass basic image viewing and analysis tools, proprietary forensic software suites, as well as manual inspection and analysis methods. The comparison aims to assess whether the introduction of the new plugin offers significant improvements in the effectiveness and efficiency of cybercrime investigations compared to these existing standard practices.

Study designs to be included The review will include a range of both experimental and observational study designs to provide a comprehensive overview of the available evidence.

Eligibility criteria In addition to the criteria specified in the PICOS sections, the following eligibility criteria will be used in this systematic review:Inclusion Criteria:1. Studies that are published or available in English or Portuguese.2. Studies that report on the practical application of the Autopsy plugin or other forensic image virtualization methods, rather than solely theoretical or conceptual aspects.3. Studies that provide sufficient information about the methods used and the outcomes measured to enable us to assess their quality and reliability.4. Studies where full text is available.Exclusion Criteria:1. Non-empirical studies such as opinion pieces, editorials, or letters to the editor, unless they contain original data.2. Studies with significant methodological flaws as determined during the quality assessment process.3. Pure medical studies where the “Autopsy” is not refered on the digital forensic context These criteria are designed to ensure that the review includes a comprehensive and reliable set of studies that are relevant to the review question and provide robust evidence about the effectiveness of the plugin in digital forensic investigations.

Information sources We will use a range of information sources to ensure a comprehensive and balanced coverage of relevant studies. These sources include:
1. Electronic Databases: The primary source of studies will be electronic databases including IEEE Xplore, ACM Digital Library, PubMed, Web of Science, Scopus, EBSCO, and Google Scholar.
2. Contact with Authors: Where necessary and possible, we will reach out to authors of studies for additional information, clarification, or to obtain full-text articles that are not otherwise accessible.
3. Trial Registers: We will also review relevant trial registers to identify any ongoing or unpublished studies that may be relevant to our review.
4. Grey Literature: In addition to peer-reviewed publications, we will also seek out grey literature, which includes technical reports, white papers, theses, dissertations, and conference proceedings. For this, we will use Google Scholar and specific databases for dissertations and theses.
5. Reference Lists: We will manually check the reference lists of included studies and relevant

reviews identified through the search to find additional studies that may not have been captured in the database search.
This multi-faceted approach will help ensure that our review is as comprehensive and inclusive as possible, capturing a wide range of studies that meet our eligibility criteria.We will use a range of information sources to ensure a comprehensive and balanced coverage of relevant studies. These sources include:
1. Electronic Databases: The primary source of studies will be electronic databases including IEEE Xplore, ACM Digital Library, PubMed, Web of Science, Scopus, EBSCO, and Google Scholar.
2. Contact with Authors: Where necessary and possible, we will reach out to authors of studies for additional information, clarification, or to obtain full-text articles that are not otherwise accessible.
3. Trial Registers: We will also review relevant trial registers to identify any ongoing or unpublished studies that may be relevant to our review.
4. Grey Literature: In addition to peer-reviewed publications, we will also seek out grey literature, which includes technical reports, white papers, theses, dissertations, and conference proceedings. For this, we will use Google Scholar and specific databases for dissertations and theses.
5. Reference Lists: We will manually check the reference lists of included studies and relevant reviews identified through the search to find additional studies that may not have been captured in the database search.
This multi-faceted approach will help ensure that our review is as comprehensive and inclusive as possible, capturing a wide range of studies that meet our eligibility criteria.

Main outcome(s) The main outcomes of this systematic review will focus on evaluating the effectiveness and efficiency of the newly developed plugin that enables virtualization and control of forensic images in digital forensic investigations.
1. Effectiveness: This will be measured by the number of additional pieces of digital evidence identified using the new plugin as compared to standard methods. Other indicators might include more comprehensive understanding of cybercrime scenarios or improved interpretation of digital evidence.
2. Efficiency: This will be evaluated in terms of time saved in the investigation process, measured from the point of employing the plugin to the point of evidence discovery.
Both of these outcomes will be measured across all stages of cybercrime investigations and at various points in time to understand the plugin's impact over different phases of an investigation. The effect measures will include the difference in means, and other relevant measures based on the data reported in the included studies. This will allow us to quantitatively assess the potential benefits of this plugin in digital forensic investigations.

Quality assessment / Risk of bias analysis For the management of records and data during this systematic review, we will employ a rigorous and organized approach:
1. References Management: We will use a reference management software Zotero to store, organize, and manage all references obtained from our search strategy. These tools will help in removing duplicates and facilitate the screening process.
2. Screening: Two independent reviewers will screen titles and abstracts, followed by a full-text review of selected studies. Disagreements will be resolved through discussion or consultation with a third reviewer.
3. Data Extraction: We will design a data extraction form to consistently capture all relevant information from each included study. The extracted information will include study characteristics, participant details, intervention and comparator details, and outcome data.
4. Data Storage: All extracted data will be stored in a secure, password-protected database to ensure data integrity and confidentiality.
5. Back-Up: Regular backups of the data will be made to prevent loss. The backup data will be stored in a separate secure location.
6. Data Analysis: We will use statistical software SPSS to conduct the quantitative data analysis. Any necessary coding for data analysis will be clearly documented and stored along with the data.

Strategy of data synthesis Data from included studies will be synthesized in a two-stage process.
Firstly, descriptive statistics will be used to summarize the characteristics of included studies, such as type of cybercrime cases examined, the detailed description of the intervention (i.e., the developed plugin), specifics about the comparison methods (i.e., standard investigative methods without the plugin), outcomes observed (i.e., quantity and quality of additional evidence identified), and the study design. This stage will also include a quality assessment of the studies using appropriate criteria.
Secondly, inferential statistics will be used to assess the overall effect of the intervention. Where possible, meta-analysis will be performed to statistically combine the results of the included studies, comparing the effectiveness of digital

forensic investigations using the new plugin against those using standard methods.
If quantitative synthesis is not appropriate due to the diverse nature of included studies, a narrative synthesis will be performed to discuss the findings qualitatively.
Subgroup analyses will be conducted based on different cybercrime types and characteristics of the digital forensic investigators (such as their level of expertise), if sufficient data is available.
Results will be presented with 95% confidence intervals and significance will be set at $p < 0.05$.
It is noteworthy that this strategy may be subject to modification, depending on the nature and quality of the studies retrieved.

Subgroup analysis Subgroup analyses will be considered to explore potential sources of heterogeneity and to better understand the impact of the developed plugin across different scenarios within the realm of digital forensic investigations.
1. Type of Cybercrime: The efficacy of the plugin may vary depending on the type of cybercrime under investigation, such as financial fraud, identity theft, hacking, cyberstalking, etc. Studies will be subgrouped based on the nature of the crime and analyzed separately.
2. Investigator Expertise: The effectiveness of the plugin could be influenced by the skill level and experience of the digital forensic investigators. Subgroup analysis will be performed comparing outcomes among novices, intermediate, and expert investigators.
3. Size of Forensic Images: The efficacy of the plugin might vary depending on the size of the forensic images being analyzed. Therefore, studies will be grouped based on the data size for subgroup analysis.
4. Type of Evidence Sought: The type of evidence investigators seek might influence the effectiveness of the plugin. Subgroups can be formed based on different categories of digital evidence, such as metadata, deleted files, network logs, etc.
5. Operating Systems: The effectiveness of the plugin may vary depending on the operating systems from which the forensic images are derived. Hence, subgroup analysis will be performed based on different operating systems like Windows, macOS, Linux, etc.
Please note that these subgroup analyses will be carried out if sufficient data is available from the included studies. These analyses are designed to help interpret the data more accurately and provide more nuanced insights into the effectiveness of the intervention across different contexts within the field of digital forensics.

Sensitivity analysis Given the nature of the study and the methodology being employed, no sensitivity analysis will be performed as part of this systematic review. The review will focus primarily on synthesizing evidence from the selected studies as per the defined PICOS criteria and conducting subgroup analyses as appropriate to better understand the differential impact of the intervention across various contexts. Robustness of the findings will be evaluated through comprehensive analysis of the data quality, thoroughness of the reported results, and consistency across the included studies. Any potential limitations inherent in this approach will be duly noted and discussed in the review.

Language restriction The search will be limited to studies published in English and Portuguese only.

Country(ies) involved All authors involved in this study are based in Portugal.

Keywords Digital Forensics; Cybercrime; Forensic Images; Plugin; Virtualization; Evidence Discovery; Investigation Efficiency; Cybersecurity; Forensic Tools; Intervention Efficacy.

Dissemination plans Our dissemination strategy is designed to ensure the broadest possible reach of our findings to relevant stakeholders including digital forensic investigators, cybersecurity professionals, and software developers.
1. Academic Publication: The primary output will be a paper detailing the review's findings, which will be submitted for publication in a peer-reviewed journal focused on digital forensics or cybersecurity.
2. Conference Presentations: Findings will be presented at relevant national and international conferences, providing an opportunity for direct engagement with the digital forensics community.
3. Research Network Sharing: The results will be disseminated through research networks and professional societies to reach investigators and practitioners in the field.
4. Workshops/Webinars: We plan to organize workshops or webinars to provide a deeper understanding of our findings and their practical application.
5. Online Dissemination: A summary of our findings will be made available on relevant websites and social media platforms to reach a broader audience.
6. Collaboration with Industry: We intend to share our findings with software development companies that might be interested in improving or developing new plugins for forensic images based on our study's results.

All these dissemination efforts will ensure our research is widely accessible, maximizing its potential to influence future developments in the field of digital forensics.

Contributions of each author

Author 1 - Nuno Mourinho - (Leading investigator): Will be responsible for the conception and design of the systematic review, carrying out the literature search, data extraction, data analysis, and drafting the initial manuscript.
Email: 19829@stu.ipbeja.pt
Author 2 - Mário Candeias - (Advisor/Peer Reviewer): Will provide strategic advice on the review design and methodology, assist in refining the literature search, and contribute to the interpretation of the findings. This author will also review and provide feedback on the drafts of the manuscript to ensure accuracy and completeness.
Author 3 - Rogério Bravo - (Advisor/Peer Reviewer): Will offer expertise in the field of digital forensics, help guide the interpretation of the results, and review the manuscript for technical accuracy. This author will also provide peer review of the study findings and manuscript drafts.