Risk-Based Digital Evidence Triage: A Framework for Artifact, Device, and Case Prioritization in Child Sexual Offense Investigations

Lukas Jaeckel[1,2(✉)] and Dirk Labudde[1,2]

[1] Technische Universität Bergakademie Freiberg, Akademiestraße 6, 09599 Freiberg, Germany
[2] University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Germany
{jaeckel1,labudde}@hs-mittweida.de

Abstract. Digital forensic investigators face increasingly large data volumes, resulting in significant delays in case processing. In the context of child sexual offense investigations, these delays are especially critical due to heightened social urgency and increased risks to victims. Although validated criminal psychological risk assessment instruments for sexual offenses are available, they are not yet integrated into digital evidence triage workflows. This paper introduces a conceptual framework for risk-based digital evidence triage in child sexual offense investigations. The framework systematically maps selected risk factors, such as indications of pedophilic interests and contact sexual offense history, to digital proxies derived from forensic artifacts and generates an explainable prioritization score. The framework enables both artifact- and device-level prioritization, allowing investigators to focus on the most relevant evidence first. Furthermore, the framework supports case-level prioritization by partially pre-filling instruments such as the Child Pornography Offender Risk Tool (CPORT). Finally, this paper discusses the strengths, limitations, and directions for future research of the presented approach.

Keywords: Digital Evidence Triage · Risk-Based Prioritization · Case Prioritization · Device Prioritization · Forensic Scoring Framework · Risk Assessment System · Explainable Digital Forensics

1 Introduction

Investigations of child sexual offenses are characterized by a high degree of urgency. On the one hand, investigators must check whether unknown victims need to be identified. On the other hand, experts must assess whether the accused

H. Neukirchen et al. (Eds.): ICDF2C 2026, LNICST 720, pp. 377–394, 2027.
https://doi.org/10.1007/978-3-032-37274-1_22

poses a high risk of committing further offenses. Many child sexual offense investigations concern not only the analogue world but also the digital space. In particular, child sexual abuse material (CSAM) is produced, acquired, possessed, and distributed [18]. In addition, initiating sexual contact with minors via the internet, known as cybergrooming, is an emerging problem [15]. The corresponding investigations involve a wide range of data storage devices, including computers, smartphones, cameras, and USB sticks, among others. As devices increase in number and capacity, investigators face large amounts of data that cannot be examined manually within reasonable time frames. This overload already causes significant case delays, highlighting the need for effective triage and prioritization in digital forensics [17]. Without systematic triage, critical evidence may be missed for extended periods, slowing victim identification and risk assessment. Efficient prioritization is necessary to allocate limited resources to the most relevant artifacts, devices, and cases. Current triage approaches in digital forensics primarily focus on search strategies, hash value comparisons, metadata-based filtering, or the use of artificial intelligence (AI) [17]. Furthermore, validated criminal psychological instruments can assess the risk of an offender committing further sexual offenses [13,14,22]. However, the instruments used in criminal psychology are disconnected from digital forensic workflows.

This work proposes a novel integration of criminal psychological risk assessment instruments and AI-assisted digital forensics triage. We introduce a conceptual framework for risk-based digital evidence triage tailored to child sexual offense investigations. The framework operationalizes selected criminal psychological risk factors as digital proxies and integrates them into a scoring engine that prioritizes individual artifacts. By aggregating these scores across seized devices, the framework enables device-level prioritization. It thus supports and relieves investigators in deciding which devices and artifacts should be analyzed first. In contrast to conventional triage, the proposed framework directly connects triage outputs to established risk assessment systems, facilitating partial pre-filling and case-level prioritization. The hybrid workflow combines automated proxy detection with expert validation. This approach aims to enhance investigative efficiency, sharpen focus on relevant evidence, and increase transparency.

Section 2 presents and discusses current digital forensic triage approaches and risk assessment instruments in criminal psychology. The research gap is identified and the need for a risk-based prioritization framework is highlighted. Section 3 introduces a conceptual framework for artifact and device prioritization. Risk factors from criminal psychology are mapped using digital proxies and integrated into a scoring engine. Section 4 shows how the framework could be implemented in practice and which existing methods could be used. Section 5 discusses the possibility of integrating the framework with risk assessment systems for prioritizing cases. Section 6 compares the strengths and weaknesses of the proposed system and includes legal and ethical considerations. Section 7 summarizes this work and provides an outlook for future work.

2 Related Work

Casey et al. [6] describe triage as the first level of a forensic examination. In this process, a targeted review is conducted to determine which sources of evidence are most useful and should be further processed. Casey et al. advocate moving away from the standard practice of examining everything, instead favoring a tiered, risk-based forensic strategy. This is the only known way for digital forensics laboratories to meet increasing demands without delaying investigations or compromising evidence.

Triage in digital forensics can pursue different objectives. Relevant devices can be detected from a large number of others [11,19]. In multimedia forensics, triage can accelerate the analysis of images and videos [12,21]. Furthermore, triage can detect the software that was executed on a compromised system [1,26]. This paper introduces a framework that uses a scoring system based on criminal psychological risk factors to identify the most relevant artifacts and devices for a given case. It also incorporates methods from multimedia forensics and AI.

Jusas et al. [17] critically reviewed a significant number of studies on digital triage and categorized the various approaches into two forms. The live digital triage is conducted on the live system, where the main goal is to obtain information rapidly. However, this form of triage carries the risk of system manipulation. In contrast, the postmortem triage is conducted on digital images in the laboratory. It focuses on ranking devices based on potentially relevant evidence. Both forms have similar relevance and employ a wide variety of methods, including keyword searches, hash value comparisons, and metadata filtering. Jusas et al. identify intelligent technologies as a research direction for the future. None of the presented studies pursues an interdisciplinary approach, such as combining digital triage with criminal psychological risk assessment approaches.

Horsman [16] created a risk-based hierarchy with 16 priority levels for prioritizing cases, using 'risk of harm' as a principal prioritization metric. Case backlogs can be addressed by managing time and resources more effectively through the hierarchy. The digital forensic laboratories are responsible for assigning cases to specific levels. However, the author does not provide a detailed description of how the assignment should be made for each individual case. Possible support through intelligent automation is not discussed.

Hanson and Thornton [14] developed Static-99 in the field of criminal psychology to assess the risks of further sexual offenses being committed. The instrument is intended exclusively for use with males aged 18 years or older who are known to have committed at least one sexual offense against a child or adult. The authors of Static-99 derived ten statistical risk factors from previous studies. The respective assessments of the risk factors result in a scale with four risk levels: low (0-1), medium-low (2-3), medium-high (4-5), and high (6+) [14]. Each factor was rated as 0 (not applicable) or 1 (applicable). Only the factor 'previous sexual offenses' was scored between 0 and 3, depending on the number of offenses. Due to statistical factors, the Static-99 is practical and easy to use, but it does not account for dynamic changes. Furthermore, the instrument does not include any specific evidence in the digital space. Consequently, a combination with triage

approaches would only be possible through extensive expansion by experts from both fields of research.

The Stable-2007 [13] was developed to assess the risk of recidivism in sexual offenses and takes stable-dynamic risk factors into account. The instrument is used for adult male offenders and was derived from a study involving 997 sex offenders from 16 regions. The authors of Stable-2007 describe 13 risk factors, which are rated 0 (no problem), 1 (minor problem), or 2 (definite problem). The determined total value is used to categorize the risks into three groups: low (0-3), medium (4-11), and high (12+) [13]. Trained experts are required, and digital evidence is explicitly not considered. For these reasons, linking Stable-2007 with triage methods from digital forensics appears unsuitable.

CPORT [24] is a risk assessment instrument for CSAM offenses to estimate the likelihood of future sexual crimes within the next five years. It is based on an initial study of 301 Canadian case files over a five-year observation period and focuses specifically on adult male sex offenders. The authors of CPORT described seven risk factors, whereby each applicable factor is rated 1:

1. Offender is aged 35 or younger.
2. Any prior criminal history.
3. Any prior or index failure on conditions.
4. Any prior or index contact sexual offense history.
5. Indications of pedophilic interests.
6. More boy than girl content ($\geq 51\%$) in CSAM.
7. More boy than girl content ($\geq 51\%$) in child nudity and other child content.

The sum of all factors results in a risk score that can be compared with CPORT scores from other cases [24]. Since determining the fifth factor is not trivial, the authors developed the Correlates of Admission of Sexual Interest in Children Scale (CASIC) [25]. CASIC contains six items, at least three of which must apply for the fifth risk factor of CPORT to be satisfied:

1. Never married.
2. Child pornography videos.
3. Child pornography stories.
4. Evidence interest in child pornography ($\geq$ two years).
5. Volunteering in a role with high access to children.
6. Engaging in online sexual communications with a minor.

In addition to CPORT, the Estimated Risk for Internet Sexual Offending (ERISCO) and the Kent Internet Risk Assessment Tool Version 2 (KIRAT-2) are also discussed in the literature on online CSAM offending [22]. However, Reichel et al. [22] note that ERISCO, which comprises almost 40 items, has not yet been empirically evaluated, while KIRAT-2, with 9 items, focuses almost exclusively on criminal history. Against this background, CPORT is currently the most suitable instrument for prioritizing artifacts, devices, and cases.

Despite a wide range of triage and risk assessment approaches, none of the existing methods integrates the two strategies. Triage is typically conducted as

the initial step in a forensic investigation, whereas risk assessment instruments are applied to estimate the recidivism risk of offenders after case processing. In contrast to other risk assessment tools, digital evidence could already be used to answer selected CPORT and CASIC items, while the remaining questionnaire items would continue to be completed manually by investigators or other experts. Accordingly, this work focuses on linking CPORT and CASIC with digital evidence triage to develop a risk-based prioritization framework for artifacts, devices, and cases. This approach is designed to help investigators prioritize cases of CSAM offenses and quickly identify relevant artifacts and devices. Since CPORT was originally developed for adult male offenders, the scope of this study is likewise limited to this offender group. To the best of our knowledge, no prior work has systematically combined digital evidence triage with established risk assessment instruments. Our study addresses this gap by proposing a conceptual framework that operationalizes selected CPORT and CASIC items through digital proxies.

3 Framework for Artifact and Device Prioritization

This section presents a conceptual framework for postmortem triage, which can be used to prioritize artifacts and devices. The prerequisite is that the defendant's devices have been seized. Section 2 showed that CPORT and CASIC are currently the most suitable risk assessment instruments in criminal psychology for transferring them to triage approaches in the digital space. Table 1 summarizes the possible proxy mapping of risk factors to digital artifacts.

Some of the corresponding risk factors relate to objective biographical data on the accused and information about his criminally relevant history. In the case of CPORT, such factors include the defendant's age, criminal history, and failure on conditions. The easiest way to make a corresponding assessment is through the investigator's knowledge. For this purpose, no analysis of the seized devices is required. Accordingly, these factors should not influence the prioritization of artifacts and devices. CPORT item 4, the contact sexual offense history, can also be answered by the investigators. However, the seized devices might also hold evidence of related contact sexual offenses that are not yet identified. CSAM could be found in the media files on the devices, created by the accused himself, and showing his own offense. The face, body, clothing, and voice can be analyzed in the CSAM files to identify the accused. Further indications about the accused may be provided by the background of the relevant media or the metadata from the used camera.

The indications of pedophilic interests can be determined by a forensic psychologist or by using CASIC. Two of the CASIC items do not require an analysis of the devices and should be irrelevant for artifact and device prioritization. Whether the accused was never married and whether he had volunteered in a role with high access to children can be answered by the knowledge of the investigators. The remaining four CASIC items can be analyzed using the data on the seized devices. The devices can be examined for the presence of CSAM

Table 1. Proxy mapping of criminal psychological risk factors to digital artifacts.

Risk Factors	Digital Artifacts
CPORT item 1	–
CPORT item 2	–
CPORT item 3	–
CPORT item 4	CSAM in media files depicting offenses committed by the accused
CPORT item 5	Three or more CASIC items are applicable
CPORT item 6	Most of CSAM in media files is of boys
CPORT item 7	Most of child nudity and other child content in media files is of boys
CASIC item 1	–
CASIC item 2	CSAM videos in media files
CASIC item 3	CSAM stories in text and document files
CASIC item 4	Metadata of CSAM and its thumbnails; timestamps in log files, caches and databases; browser and search history; networking in CSAM groups
CASIC item 5	–
CASIC item 6	Cybergrooming in social networks and instant messaging services

videos. Finding CSAM stories in the text and document files of the devices also increases the CASIC score. Various data sources on the devices are suitable for proving interest in CSAM over a period of more than two years. The browser and search history provide indications of such interest. For example, the defendant may have frequently searched for CSAM or related terms. He may also have regularly visited websites that enable the consumption and exchange of CSAM. In addition, metadata from CSAM files, directories, and thumbnails on the devices can provide information on when the defendant downloaded, created, or last viewed the files. Depending on the operating system, log files, caches, and databases may contain further timestamps relating to activities involving CSAM files. Networking in groups on internet forums, social networks, or instant messengers to exchange CSAM is also evidence of interest in CSAM. All of the described indicators can be placed in a time series to examine whether the accused has had an interest in CSAM for two or more years. To prove that the accused was engaging in online sexual communications with a minor, social network and instant messenger chats on the seized devices can be examined for cybergrooming.

CPORT item 6 is satisfied if more boy than girl content is depicted in CSAM. This risk factor can be investigated by analyzing the CSAM contained within the media files of seized devices. Similarly, child nudity and other child content in media files can also be checked concerning the boy-to-girl ratio. If at least 51% of the relevant files depict boys, CPORT item 7 was coded positively.

Applying criminal psychological risk assessment instruments, such as CPORT and CASIC, is traditionally a manual and time-consuming task, as experts must

first analyze seized devices before coding the respective items. Automation can accelerate this process by extracting and processing relevant information directly from digital artifacts. In particular, CPORT items 4, 5, 6, and 7, as well as CASIC items 2, 3, 4, and 6, can be partially pre-filled using digital proxies. This enables investigators to rely on prioritization from an early phase of case processing, rather than only after a full manual examination. The automated prioritization of artifacts and devices reduces backlog and directs attention to potentially high-risk material.

A scoring engine is required to automatically prioritize artifacts and devices based on the analyzed risk factors. To ensure a transparent and mathematically rigorous prioritization process, the scoring model distinguishes explicitly between proxies originating from CPORT and those derived from CASIC. In particular, CPORT proxies contribute directly to the device score. In contrast, CASIC proxies only increase the device score by 1 if at least three of them are satisfied, according to CPORT item 5. Let P_{CPORT} and P_{CASIC} denote the disjoint sets of CPORT- and CASIC-based proxies. The full proxy set P is then defined as:

$$P = P_{CPORT} \cup P_{CASIC}. \tag{1}$$

For each artifact a and each proxy $p \in P$, the relevance indicator $x_{a,p}$ is defined as:

$$x_{a,p} = \begin{cases} 1, \text{ if artifact } a \text{ satisfies proxy } p, \\ 0, \text{ otherwise.} \end{cases} \tag{2}$$

where applicable, proxies may also be assigned a confidence score $c_{a,p} \in [0, 1]$, that reflects the uncertainty inherent in machine-generated classifications (e.g., grooming detection, gender estimation). In this context, $c_{a,p} = 1$ represents the highest level of confidence. In addition, each proxy has an investigator-defined weight $w_p > 0$. This allows investigators' experience to be incorporated as domain-specific prior knowledge within a controlled parameterization of the scoring model. By default, $w_p = 1$. Weight assignments are transparently documented to ensure reproducibility and traceability. Through discussion within the investigative team and with recorded justification, w_p can be adjusted to reflect case-specific investigative priorities. This multidimensional scoring reflects not only relevance, but also urgency, complexity, and probative value. The artifact-level score $s(a)$ is then defined as:

$$s(a) = \sum_{p \in P} w_p \cdot x_{a,p} \cdot c_{a,p}. \tag{3}$$

The automated analysis of a device may return a prioritized list of artifacts with a score greater than 0. Investigators can review the list and the attached documentation to quickly examine and manually evaluate artifacts that are likely to be relevant. Device-level scoring is derived from the artifact-level proxies. For a device d, the CPORT and CASIC items are modeled as binary indicator variables:

$$\begin{aligned} X_{d,i}^{CPORT} &\in \{0, 1\}, \quad i \in \{4, 5, 6, 7\}, \\ X_{d,j}^{CASIC} &\in \{0, 1\}, \quad j \in \{2, 3, 4, 6\}. \end{aligned} \tag{4}$$

An indicator variable is set to 1 if the device's artifacts satisfy the proxy for the specific item. The device-level CPORT and CASIC scores are obtained by summing all corresponding indicator variables:

$$S_{CPORT}(d) = \sum_{i=4}^{7} X_{d,i}^{CPORT}, \quad S_{CASIC}(d) = \sum_{j \in \{2,3,4,6\}} X_{d,j}^{CASIC}. \tag{5}$$

The CPORT item 5 is satisfied if the CASIC score is at least 3. The described metric aligns with the conceptual logic of CPORT and CASIC, where risk is determined by the number of positively coded items. Based on Table 1, CPORT items 13 are excluded because they require background information unavailable through digital artifacts. The resulting device scores therefore range from 0 to 4, producing five distinct prioritization levels.

CPORT assumes the presence of CSAM on seized devices but does not integrate CSAM quantity into its scoring. As a result, devices that contain CSAM but do not fulfill any CPORT item may receive a risk score of 0. To prevent such cases from being deprioritized, we introduce the quantity of CSAM files $Q_{CSAM}(d)$ as a second, independent scoring dimension. The complete device-level risk score is thus expressed as a two-dimensional vector:

$$S_{risk}(d) = \big(S_{CPORT}(d), Q_{CSAM}(d)\big) \tag{6}$$

Devices with higher CPORT score $S_{CPORT}(d)$ take precedence. If two devices have the same CPORT score, the one with higher CSAM quantity $Q_{CSAM}(d)$ is prioritized. This extension preserves the primacy of validated psychological risk factors while ensuring that devices containing CSAM are not overlooked.

4 Proposed Workflow for Artifact and Device Prioritization

Building on the proxy mapping in Table 1 and scoring principles from the previous part, this section describes a structured forensic workflow that operationalizes artifact- and device-level prioritization (Fig. 1). The workflow is designed to process input from seized devices, extract relevant artifacts, map them to proxy definitions, and route the results through the scoring engine. The outputs are ranked artifact lists and aggregated device scores, accompanied by transparent documentation to support investigator validation. By distinguishing modular components, the workflow ensures flexibility and extensibility, for example, to support weighted or multidimensional scoring models.

Before the data from the seized devices can be analyzed, it must first be extracted and preprocessed. As this work focuses on scoring and prioritization, addressing acquisition challenges is beyond its scope. It is therefore assumed that relevant artifacts are already available in semi-structured formats, such as those produced by forensic tools (e.g., XML or JSON exports). Alternatively, the acquired data can be represented in an ontology, which enables artifacts to be

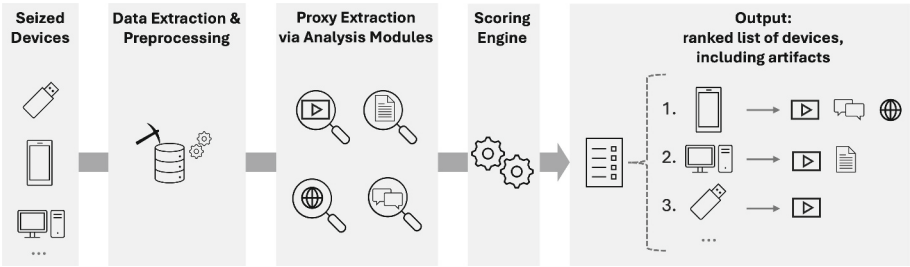

Fig. 1. Proposed workflow for prioritizing artifacts and devices, consisting of data extraction and preparation, proxy analysis modules, scoring engine, and output.

linked across sources and supports pattern recognition, reasoning, and visualization. A promising basis in this context is the Cyber-investigation Analysis Standard Expression (CASE) [5], an ontology-driven standard specifically developed to support cyber investigations.

Following data acquisition, each proxy from Table 1 is extracted by a dedicated analysis module. A module for the automatic detection of CSAM plays a central role in proxy extraction, since several criminal psychological items depend on its outcome. Specifically, CPORT items 4 and 6, as well as CASIC items 2, 3, and 4, require the detection of CSAM. Beyond coding these items, the quantity of CSAM files per device should also be incorporated into the scoring model, as discussed in Sect. 3. The module takes the media files of each device as input and outputs a list of files that are likely to constitute CSAM. Different approaches can be employed to implement this functionality. One established method is the comparison of hash values against known CSAM hash databases, with PhotoDNA being a particularly robust and widely used perceptual hashing technique [27]. Pereira et al. [20] proposed an alternative approach that leverages only file path information: rather than analyzing file content, they apply machine learning (ML) models to path strings and achieve promising results with character-based convolutional neural networks (CNNs). More advanced frameworks combine image and video content analysis with deep learning. For example, Gangwar et al. [10] developed a two-stage CNN architecture. In the first stage, images are classified as pornographic or non-pornographic. In the second stage, detected faces are analyzed to determine whether they belong to minors or adults. An image is classified as CSAM if it contains pornographic content and at least one minor is identified. While results are promising, such systems are vulnerable to errors in face detection. Beyond image and video files, textual artifacts also provide important evidence. Here, techniques from natural language processing (NLP) and ML can be employed to detect erotic or abusive content in documents and text files [3]. These methods can be complemented by keyword-based searches targeting CSAM-related terminology to identify CSAM stories. Suitable keywords (e.g., child, teen, preteen, or lolita) can be chosen by investigators or identified in studies, such as those by Westlake

et al. [29]. However, the reliability of such approaches depends strongly on context, vocabulary, and linguistic variation, and systematic evaluations in forensic settings are still lacking. In practice, the CSAM analysis module could integrate these approaches into a multi-stage pipeline. In the first step, files would be compared against hash databases of known CSAM and non-CSAM content. Consequently, known CSAM files are found quickly, and clearly irrelevant files can be excluded to reduce the amount of data. In a second step, suspicious file paths could be evaluated using ML models trained on path string features. Only files that remain unresolved after these steps would undergo content-based analysis with ML models and NLP methods. This cascading strategy ensures that computationally intensive image and text classification is applied only where necessary, thereby combining efficiency with high detection accuracy. As a result, the module forwards the artifacts identified as CSAM to the scoring engine.

CPORT item 4 can be addressed by a dedicated module that builds upon the outputs of the CSAM analysis module. While this module detects and classifies potential CSAM, the module for CPORT item 4 extends this functionality by assessing whether the accused is depicted in the detected material. This requires that reference images or videos of the accused be available for comparison. As a first step, metadata can be automatically examined to identify whether the recording device matches one of the seized devices. Additionally, CSAM can be subjected to person identification and face recognition methods to determine whether the accused is depicted. Amirgaliyev et al. [2] provide a comprehensive review of approaches in this field, demonstrating that CNNs currently achieve state-of-the-art performance, while classical computer vision methods, such as Support Vector Machines (SVMs) or Eigenfaces, remain viable options for resource-constrained settings. The module for CPORT item 4 can be extended beyond facial recognition to include additional modalities. One promising approach is speaker verification in videos, which requires reference voice recordings of the accused. Brydinskyi et al. [4] demonstrate that deep learning models achieve strong results in this domain, with embedding-based methods proving particularly robust for voice matching. Another complementary extension is place recognition, where images and videos are analyzed to determine whether they depict a known environment. If reference images of the accused's premises are available, CSAM can be examined for background similarities that may identify a premise as the crime scene. Schubert et al. [23] provide an overview of this emerging research field and outline potential techniques.

CPORT item 5 is coded as positive if at least three of the CASIC items 2, 3, 4, and 6 are satisfied for a device. CASIC item 2 can be evidenced if the CSAM module classifies videos from a seized device as relevant. Video detection can rely on filtering by file type or signature. The CASIC item 3 can be determined by filtering the text and document files from the CSAM module output.

For CASIC item 4, a dedicated module can analyze temporal aspects of relevant artifacts. First, metadata of files and directories identified by the CSAM module can be examined, with a focus on timestamps. The creation and modification dates, as well as the date of last access, are usually included and can be

associated with timeline events [7]. However, creation and modification dates are often unreliable, as they may be influenced by system processes. In contrast, the last access date can provide a stronger indication of user activity and may therefore be prioritized in an initial implementation. Second, browser and search histories can be screened for CSAM-related terms, provided such data are available on the seized devices. Suitable keyword lists can be derived from investigative practice or previous studies such as those by Westlake et al. [29]. As a result, the dates of relevant queries or page visits can be included in the time series. Third, the accused's participation in CSAM-related groups on social networks and instant messenger services can be considered. An initial approach could filter groups in which detected CSAM has been exchanged and record the timestamps of joining, first interaction, and last activity. As an extension, ML techniques could be explored to automatically identify CSAM-related groups from communication data. Together, these approaches would enable a time series that reflects the persistence of CSAM-related behavior and interest.

CASIC item 6 can be addressed by a module that analyzes communication data from seized devices. Its purpose is to identify grooming conversations in which the accused deliberately targets minors via social networks or instant messaging platforms. Felser et al. [9] noted that existing research has explored a variety of ML approaches, with SVM, Random Forest, and deep learning methods showing promising results. However, the authors emphasize that no single algorithm achieves the best results in all circumstances. Moreover, almost all studies are based on English-language datasets and largely neglect multimodal communication features, such as voice messages or shared media files. Since grooming detection is inherently complex and highly context-dependent, systematic evaluations are required to establish which methods are both reliable and efficient for integration into a triage framework, where rapid identification of suspect communications can directly influence investigative priorities.

A dedicated module for CPORT item 6 must first detect minors in the material and subsequently determine their gender. The relevant artifacts identified by the CSAM module serve as input for this process. In the first stage, similar to the CSAM pipeline, CNNs can be applied to recognize minors in images or videos. In the second stage, gender classification can be performed, for example, by extracting facial features with a deep CNN and processing them through a stacking classifier that combines multiple ML models [28]. For child-specific gender determination, separate datasets are available, including either real or synthetically generated facial images [8].

For CPORT item 7, the corresponding analysis module must determine whether boys or girls are more frequently depicted in non-CSAM images or videos that contain child-related content. The detection of minors and subsequent gender classification can be performed using approaches similar to those described for the CPORT item 6 module.

An overview of applicable candidate methods per analysis module is provided in Table 2. While the modules address specific criminal psychological proxies, their efficient integration into a prioritization system requires careful design and

implementation. Several strategies can be employed to achieve scalability. First, modules can be executed in parallel since they typically operate on distinct artifact types (e.g., images, text, communication logs). Second, a cascading strategy can be applied, in which general filters or the CSAM module provide preprocessed artifacts that are only forwarded to specialized modules if they are relevant. Third, shared preprocessing steps such as face detection should be centralized and their results distributed across modules to avoid redundant computation. Finally, prioritization can be made adaptive. Intermediate findings from one module may influence the execution order or weighting of others. Such design principles ensure that the system remains both efficient and flexible, which is critical in the triage context where rapid results are essential. However, the relative benefits and practical feasibility of these integration strategies in real-world forensic settings remain to be systematically evaluated.

Table 2. Practical implementation of the analysis modules. Each module addresses a specific criminal psychological risk factor proxy.

Analysis Module	Methods
CSAM module	Hash database comparison; suspicious file paths detection; combination of pornography & minor detection; detection of erotic texts with content involving minors
CPORT item 4 module	CSAM module results + recording device detection; person identification; face recognition; speaker verification; place recognition
CPORT item 5 module	Aggregation of the module results for CASIC 2, 3, 4, 6
CPORT item 6 module	CSAM module results + minor detection & gender determination
CPORT item 7 module	Minor detection & gender determination
CASIC item 2 module	CSAM module results + video filtering
CASIC item 3 module	CSAM module results + text & document filtering
CASIC item 4 module	Time series analysis using metadata analysis of CSAM module results; browser & search history analysis; CSAM group detection
CASIC item 6 module	Cybergrooming detection

For documentation, a JSON-based implementation could record for each device which artifacts are relevant, which items they satisfy, and the relevant content of complex artifacts. A higher-level file can record the satisfied items and the overall score, and reference the corresponding artifacts. Alternatively, in an ontology, scoring results and documentation could be linked directly to the artifacts themselves. Ultimately, a user interface would provide investigators with a prioritized list of devices, displaying each score together with the relevant

artifacts and documentation. This documented and transparent scoring ensures that prioritization results remain verifiable and actionable in forensic practice.

5 Integration with Risk Assessment Systems for Case Prioritization

This work follows a semi-automated approach to prioritize cases. On the one hand, information automatically extracted and processed during artifact- and device-level prioritization provides partial input to risk assessment instruments. On the other hand, investigators contribute their domain expertise to answer the remaining questions that cannot be resolved solely through digital evidence. Figure 2 illustrates the integrated system, where artifact and device prioritization inform the case-level risk assessment workflow. This approach aims to ensure that high-risk cases can be addressed more rapidly, while maintaining the transparency and expert oversight required in forensic practice.

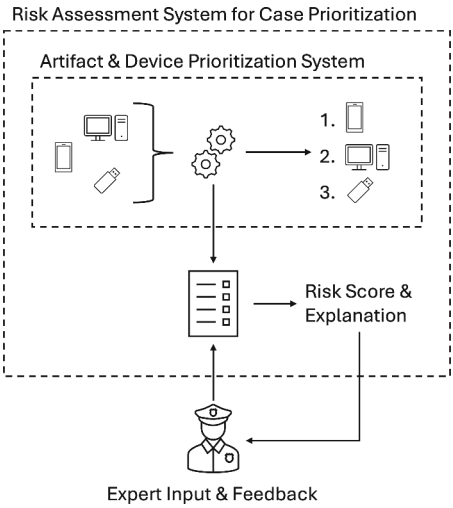

Fig. 2. Schematic design of a risk assessment system for case prioritization, including an integrated system for artifact and device prioritization.

We propose a risk assessment system in which investigators complete a digital questionnaire to provide case-specific information about the accused. This includes CPORT items 14 and CASIC items 1 and 5. Alternatively, such information could be represented in an ontology where relevant data are already stored. The remaining CPORT and CASIC items are automatically pre-filled by the prioritization system, using the ranked list of devices and associated documentation. If CPORT items 4 or 5, or CASIC items 2, 3, or 6 are met at the artifact- or device-level, they are considered satisfied for the entire case. For

CPORT items 6 and 7, statistics from all devices must be aggregated to calculate the global ratio across CSAM and other child-related content. To determine CASIC item 4 at the case-level, the duration of interest in CSAM across all devices is taken into account. These aggregations ensure that CPORT items 6 and 7, and CASIC item 4 are determined consistently at the case-level rather than per device. Finally, all satisfied CPORT items are aggregated into a score from 0 to 7, which represents the total number of CPORT items that can be positively coded for a given case.

To formalize case-level prioritization, let c denote a case consisting of a set of devices D_c. CPORT and CASIC items are derived from the investigator input and from the results of the proxies of each device. For case c, the CPORT and CASIC items are modeled as binary indicator variables:

$$\begin{aligned} X_{c,i}^{CPORT} &\in \{0,1\}, \quad i \in \{1,2,3,4,5,6,7\}, \\ X_{c,j}^{CASIC} &\in \{0,1\}, \quad j \in \{1,2,3,4,5,6\}. \end{aligned} \tag{7}$$

An indicator variable is set to 1 if the case's artifacts and devices satisfy the proxy for the specific item. The case-level CPORT and CASIC scores are obtained by summing all indicator variables:

$$S_{CPORT}(c) = \sum_{i=1}^{7} X_{c,i}^{CPORT}, \quad S_{CASIC}(c) = \sum_{j=1}^{6} X_{c,j}^{CASIC}. \tag{8}$$

The CASIC score must be at least 3 to fulfill CPORT item 5. As a second dimension for the case-level prioritization, the total CSAM volume across all devices is aggregated as:

$$Q_{CSAM}(c) = \sum_{d \in D_c} Q_{CSAM}(d). \tag{9}$$

The final case-level risk score is represented as a two-dimensional vector:

$$S_{risk}(c) = \big(S_{CPORT}(c), Q_{CSAM}(c)\big), \tag{10}$$

where cases are prioritized first by $S_{CPORT}(c)$, and in the event of a tie, by $Q_{CSAM}(c)$. This score provides investigators with a transparent and comparable measure to prioritize cases, supporting real-world decisions about which require immediate action. By focusing resources on cases with more risk factors, this system improves resource allocation and potentially enhances victim protection.

Since false positives are possible with the artifact- and device-level prioritization system, human verification remains essential. Investigators can view the ranked list of devices and their documentation at any time and are empowered to override system assessments. A user interface should present a prioritized list of devices, including scores, relevant artifacts, and associated CPORT or CASIC items. From this overview, investigators can drill down to artifact-level details, confirm or revoke relevance, adjust item weights, and add annotations. Transparency is supported by linking each score to the underlying artifacts and by displaying how investigator input affects prioritization results in real-time. Reports

are generated only after all artifacts have been manually reviewed, ensuring that the final output provides a complete audit trail with investigator-confirmed artifacts, calculated scores, generated explanations, and annotations. This design combines efficiency with forensic soundness, traceability, and legal admissibility.

6 Discussion

The proposed framework offers several notable strengths. It introduces a structured and explainable method for prioritizing artifacts, devices, and cases, which enables investigators to identify the most relevant evidence at an early stage. By mapping criminal psychological risk factors from validated instruments such as CPORT and CASIC to digital proxies, the system bases triage on established criminal psychological knowledge rather than on ad hoc heuristics. Structured documentation and investigator validation ensure transparency, making prioritization outcomes interpretable and auditable. The modular design enables the addition, adaptation, or replacement of analysis modules without requiring the restructuring of the entire system, thereby supporting adaptability to evolving forensic methods and investigative requirements. The semi-automated approach reduces investigator workload while maintaining expert oversight, achieving a balance between efficiency and forensic accuracy.

Several limitations of the framework should be recognized. The framework remains conceptual and has not yet been implemented or empirically evaluated in operational investigations. For triage purposes and the proxy analysis modules, the optimal balance between reliability, computational efficiency, and robustness against adversarial conditions remains an open research question. The accuracy of the system is contingent on the reliability of its component modules. For example, false positives or negatives in CSAM detection or cybergrooming classification can influence prioritization outcomes. While false positives can often be identified and corrected during investigator review, false negatives may leave relevant artifacts remaining undetected, thereby diminishing the completeness of the results. The framework also assumes that digital artifacts are available in semi-structured formats. In practice, data acquisition and preprocessing are complex and resource-intensive. Furthermore, the framework inherits the limitations of CPORT, which was developed for adult male offenders, restricting the system's applicability to this population and limiting its generalizability to broader investigative contexts.

The integration of automated prioritization with risk assessment tools also raises important legal and ethical considerations. Forensic outputs must remain auditable and subject to investigator correction to ensure their admissibility in court. It is essential to note that CPORT should only be used for risk assessment if no more than one CPORT item is missing [24]. Consequently, verification and supplementation by the investigators are indispensable. The framework should provide comprehensive traceability, including documentation of both automated results and subsequent investigator actions. Ethically, it is essential to prevent over-reliance on automated scores, as the system is designed to support, not

replace, professional judgment. The use of sensitive data, such as CSAM, necessitates strict adherence to legal safeguards and data protection requirements. As a result, any practical implementation of the framework must prioritize privacy, accountability, and proportionality.

7 Conclusion and Future Work

This paper introduced a conceptual framework for risk-based digital evidence triage in child sexual offense investigations. In view of the increasing amount of data, the presented framework is intended to support and relieve investigators. Selected items from validated risk assessment instruments, including CPORT and CASIC, are mapped to digital proxies derived from forensic artifacts. The framework enables multi-level prioritization at the artifact, device, and case levels. The proposed scoring engine, combined with structured documentation and investigator validation, provides a transparent and explainable basis for prioritization while maintaining forensic soundness. This approach addresses the gap between digital triage and criminal risk assessment and offers a novel decision-support tool for time-critical CSAM investigations.

Although the framework is promising, it remains conceptual and has yet to be implemented. Subsequent research will develop a prototype that integrates the analysis modules and scoring engine into existing forensic workflows. Planned evaluation will examine scalability, accuracy, and investigator usability in real case environments. Computational performance, including processing time and potential time savings relative to traditional methods, will also be evaluated. Obtaining real-world case data for evaluation remains a significant challenge. Collaboration with law enforcement agencies is therefore essential. Legal and ethical considerations, such as data protection, automation bias, and the admissibility of semi-automated assessments, require systematic review. Expanding the framework to include offender groups beyond the CPORT focus is also identified as a future research direction. The primary objective is to transition from a conceptual framework to an operational system that has been validated in practice. This progression will enable empirical evaluation of the effectiveness and efficiency of risk-based prioritization in investigations, thereby supporting forensic decision-making and facilitating adoption within law enforcement.

Acknowledgments. This work was made possible through funding from the ESF Plus program, which is co-financed by the European Union and the Free State of Saxony. The company FZ forensic.zone GmbH supported this work financially.

References

1. Al-Sharif, Z., Al-Saleh, M., Jararweh, Y., Alawneh, L., Shatnawi, A.: The effects of platforms and languages on the memory footprint of the executable program: a memory forensic approach. J. Univ. Comput. Sci. **25**, 1174–1198 (2019). https://doi.org/10.3217/jucs-025-09-1174

2. Amirgaliyev, B., Mussabek, M., Rakhimzhanova, T., Zhumadillayeva, A.: A review of machine learning and deep learning methods for person detection, tracking and identification, and face recognition with applications. Sensors **25**(5) (2025). https://doi.org/10.3390/s25051410
3. Barrientos, G.M., Alaiz-Rodríguez, R., González-Castro, V., Parnell, A.C.: Machine learning techniques for the detection of inappropriate erotic content in text. Int. J. Comput. Intell. Syst. **13**, 591–603 (2020). https://doi.org/10.2991/ijcis.d.200519.003
4. Brydinskyi, V., et al.: Comparison of modern deep learning models for speaker verification. Appl. Sci.**14**(4) (2024). https://doi.org/10.3390/app14041329
5. Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H., Nelson, A.: Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. Digit. Investig. **22**, 14–45 (2017). https://doi.org/10.1016/j.diin.2017.08.002
6. Casey, E., Ferraro, M., Nguyen, L.: Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence. J. Forensic Sci. **54**(6), 1353–1364 (2009). https://doi.org/10.1111/j.1556-4029.2009.01150.x
7. Du, X., Le, Q., Scanlon, M.: Automated artefact relevancy determination from artefact metadata and associated timeline events. In: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–8 (2020). https://doi.org/10.1109/CyberSecurity49315.2020.9138874
8. Farooq, M.A., Yao, W., Costache, G., Corcoran, P.: ChildGAN: large scale synthetic child facial data using domain adaptation in StyleGAN. IEEE Access **11**, 108775–108791 (2023). https://doi.org/10.1109/ACCESS.2023.3321149
9. Felser, J., Preuß, S., Labudde, D., Spranger, M.: Technical Perspectives of Sexual Online Grooming. In: Kuhle, L.F., Stelzmann, D. (eds.) Sexual Online Grooming of Children, Sexuality, Health and Society, vol. 2, chap. 4.4, pp. 263–296. Nomos, Baden-Baden, 1 edn. (2025)
10. Gangwar, A., González-Castro, V., Alegre, E., Fidalgo, E.: AttM-CNN: attention and metric learning based CNN for pornography, age and child sexual abuse (CSA) detection in images. Neurocomputing **445**, 81–104 (2021). https://doi.org/10.1016/j.neucom.2021.02.056
11. Gentry, E., McIntyre, R., Soltys, M., Lyu, F.: SEAKER: A Tool for Fast Digital Forensic Triage. In: Arai, K., Bhatia, R. (eds.) Advances in Information and Communication. 2019 Future of Information and Communication Conference (FICC), vol. 2, pp. 1227–1243. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-12385-7_87
12. Hales, G., Bayne, E.: Investigating Visualisation Techniques for Rapid Triage of Digital Forensic Evidence. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust, pp. 277–293. HCII 2019, Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-22351-9_19
13. Hanson, R.K., Harris, A.J.R., Scott, T.L., Helmus, L.: Assessing the risk of sexual offenders on community supervision: The dynamic supervision project. User Report 2007-05, Public Safety Canada, Ottawa, Ontario (2007)
14. Hanson, R.K., Thornton, D.: Static 99: Improving Actuarial Risk Assessments for Sex Offenders. Solicitor General of Canada, Ottawa (1999)
15. Hille, Z., Stelzmann, D., Kuhle, L.F.: Definition and Characteristics of the Phenomenon of Sexual Online Grooming. In: Kuhle, L.F., Stelzmann, D. (eds.) Sexual Online Grooming of Children, Sexuality, Health and Society, vol. 2, chap. 1.1, pp. 17–38. Nomos, Baden-Baden, 1 edn. (2025)

16. Horsman, G.: The hierarchy of case priority (HiCaP):- a proposed method for case prioritisation in digital forensic laboratories. Sci. Justice **62**(5), 594–601 (2022). https://doi.org/10.1016/j.scijus.2022.08.008
17. Jusas, V., Birvinskas, D., Gahramanov, E.: Methods and tools of digital triage in forensic context: survey and future directions. Symmetry **9**(4) (2017). https://doi.org/10.3390/sym9040049
18. Lee, H.E., Ermakova, T., Ververis, V., Fabian, B.: Detecting child sexual abuse material: a comprehensive survey. Forensic Sci. Int.: Digit. Investig.**34** (2020). https://doi.org/10.1016/j.fsidi.2020.301022
19. Lim, M., Jones, J.: A Digital Media Similarity Measure for Triage of Digital Forensic Evidence. In: Peterson, G., Shenoi, S. (eds.) Advances in Digital Forensics XVI. pp. 111–135. DigitalForensics 2020, Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-56223-6_7
20. Pereira, M., Dodhia, R., Anderson, H., Brown, R.: Metadata-based detection of child sexual abuse material. IEEE Trans. Dependable Secure Comput. **21**(4), 3153–3164 (2024). https://doi.org/10.1109/TDSC.2023.3324275
21. Quick, D., Choo, K.K.R.: Big forensic data management in heterogeneous distributed systems: quick analysis of multimedia forensic data. Softw.: Pract. Experience **47**(8), 1095–1109 (2017). https://doi.org/10.1002/spe.2429
22. Reichel, R., Daser, A., Gnielka, F., Schmidt, A., Blokland, A., Lehmann, R.: A review of risk factors for online and mixed child sexual abuse material offending: what is being researched?. J. Sex. Aggression, pp. 1–44 (2024). https://doi.org/10.1080/13552600.2024.2418100
23. Schubert, S., Neubert, P., Garg, S., Milford, M., Fischer, T.: Visual place recognition: a tutorial [tutorial]. IEEE Robot. Autom. Mag. **31**(3), 139–153 (2024). https://doi.org/10.1109/MRA.2023.3310859
24. Seto, M., Eke, A.: Predicting Recidivism Among Adult Male Child Pornography Offenders: Development of the Child Pornography Offender Risk Tool (CPORT). Law and human behavior **39** (2015). https://doi.org/10.1037/lhb0000128
25. Seto, M., Eke, A.: Correlates of Admitted Sexual Interest in Children Among Individuals Convicted of Child Pornography Offenses. Law Hum. Behav.**41** (2017). https://doi.org/10.1037/lhb0000240
26. Soltani, S., Hosseini Seno, S.A.: Detecting the software usage on a compromised system: a triage solution for digital forensics. Forensic Sci. Int.: Digit. Investig.**44** (2023). https://doi.org/10.1016/j.fsidi.2022.301484
27. Steinebach, M.: An analysis of PhotoDNA. In: Proceedings of the 18th International Conference on Availability, Reliability and Security, pp. 1–8. ARES '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3600160.3605048
28. waris, F., Da, F., Liu, S.: Stacked ensemble learning for facial gender classification using deep learning based features extraction. Cluster Comput. **27**, 11491–11513 (2024). https://doi.org/10.1007/s10586-024-04340-7
29. Westlake, B., Bouchard, M., Frank, R.: Comparing methods for detecting child exploitation content online. In: 2012 European Intelligence and Security Informatics Conference, pp. 156–163 (2012). https://doi.org/10.1109/EISIC.2012.25