Automation for Digital Forensics: Towards a definition for the community

Gaëtan Michelet, Frank Breitinger, Graeme Horsman

PII: S0379-0738(23)00219-0

DOI: https://doi.org/10.1016/j.forsciint.2023.111769

Reference: FSI111769

To appear in: *Forensic Science International*

Received date: 18 August 2022
Revised date: 23 December 2022
Accepted date: 21 June 2023

Forensic Science International, Volume 349, August 2023, Article Number 111769
DOI: 10.1016/j.forsciint.2023.111769

Automation for Digital Forensics: Towards a definition for the community

Gaëtan Michelet *a**, Frank Breitinger *a*, Graeme Horsman *b*

a School of Criminal Justice, University of Lausanne, 1015 Lausanne, Switzerland
b Cranfield University, College Rd, Cranfield, Wharley End, Bedford MK43 0AL, United Kingdom

Abstract

With the increasing amount of digital evidence per case, the automation of investigative tasks is of utmost importance to the digital forensics community. Consequently, tools are published, frameworks are released, and artificial intelligence is explored. However, as the foundation, i.e., a definition, classification, and common terminology, is missing, this resembles the wild west: some consider keyword searches or file carving as automation while others do not. We, therefore, reviewed automation literature (in the domain of digital forensics as well as other domains), performed three practitioner interviews, and discussed the topic with domain experts from academia. On this basis, we propose a definition and then showcase several considerations with respect to automation for digital forensics, e.g., what we classify as no/basic automation as well as full automation (autonomous). We conclude that it requires these foundational discussions to promote and progress the discipline through a common understanding.

Keywords: Automation, Definition, Practitioner interviews, Digital Forensic investigation, Investigative task

∗Corresponding author.
Email addresses: gaetan.michelet@unil.ch (Gaëtan Michelet),
frank.breitinger@unil.ch (Frank Breitinger),
Graeme.Horsman@cranfield.ac.uk (Graeme Horsman)
URL: https://www.FBreitinger.de (Frank Breitinger)

Automation for Digital Forensics: Towards a definition for the community

author name[a,b,c]

[a] *address1*
[b] *address2*
[c] *address3*

Abstract

With the increasing amount of digital evidence per case, the automation of investigative tasks is of utmost importance to the digital forensics community. Consequently, tools are published, frameworks are released, and artificial intelligence is explored. However, as the foundation, i.e., a definition, classification, and common terminology, is missing, this resembles the wild west: some consider keyword searches or file carving as automation while others do not. We, therefore, reviewed automation literature (in the domain of digital forensics as well as other domains), performed three practitioner interviews, and discussed the topic with domain experts from academia. On this basis, we propose a definition and then showcase several considerations with respect to automation for digital forensics, e.g., what we classify as no/basic automation as well as full automation (autonomous). We conclude that it requires these foundational discussions to promote and progress the discipline through a common understanding.

Keywords: Automation, Definition, Practitioner interviews, Digital Forensic investigation, Investigative task

1. Introduction

Automation for digital forensics[1] is not new and is almost as old as the discipline itself. Researchers and practitioners started developing tools that automatically parse file systems, recover deleted files, or search for keywords. There have also been discussions on what it requires to be acceptable in a court of law [1, 2]. The initial progress was slow, and researchers kept stressing the importance of automation as well as showcasing research gaps [3, 4, 5]. A survey among academics and practitioners by Al Fahdi et al. [6] showed that time and volume of data would be limitations. Most participants felt that automation is important as automating tasks can help to reduce the amount of manual workload. Over time researchers, practitioners, and software vendors focused on automation trying to find tasks, procedures, and processes that can be completed autonomously by software to accelerate the forensic investigative process, reduce the workload of practitioners, and potentially increase the quality of the investigation, i.e., possible reduction of human error. In more recent years, artificial intelligence (AI) and its value for automation have been explored [7, 8]. While software solutions enhanced the investigative process, the community also analyzed the challenges of designing and deploying automation. Casey and Friedberg [9] believe that automating an entire investigation is not feasible, as every investigation requires analytical skills and experience. However, automation can address subroutines such as the recovery of deleted files and folders, or the creation of a timeline from various artifacts. James and Gladyshev [10] point out that the “challenge comes when higher-level processes, such as analysis, are being automated, and also when the investigator begins to lose understanding of the underlying concepts of the investigation”. Today, automation is considered to be one of the most important research opportunities [11], and searching “automation digital forensics" reveals thousands of contributions attempting to advance the discipline.

Problem description. Despite this gain of research and tools in the domain, the meaning of automation for digital forensics has seen limited discussion. There is no definition nor a classification applicable to categorize automatic approaches. Terms used do not follow guidelines or provide a fully described set of criteria as part of any offered definition, e.g., what is the difference between digital forensics’ processes, procedures, tasks, and sub-routines? While, of course, there is a basic understanding of key concepts within the community, not having a definition leads to different judgments between individuals. Depending on their opinion, many, most, or few of the tasks that a practitioner carries out would be considered automation. In many cases, there are few purely manual tasks that a practitioner conducts (for example, a manual parse of unknown data using a hex editor, or a manual linking of the different artifacts found in a case). Even the fundamental act of parsing a file system before conducting an analysis cannot be considered a manual task as in most cases a specific tool is used (e.g., FTK Imager, Autopsy). Some consider such a task as automation whereas others may disagree.

[1] For the remainder of this article, we mostly write automation which refers to automation for digital forensics.

On the other hand, not all automation is the same: While some automated tasks are simplistic and well-established (used during most investigations), others are based on recent and complex technologies such as AI. Being aware of these differences is important and therefore it requires a way to classify or categorize approaches. For instance, two systems, A and B, recover deleted files. While A performs file carving based on header-footer-information, B utilizes other heuristics as well and can adjust its strategy (learn). From a practitioner's perspective, it is beneficial to know these differences in procedure without reading a comprehensive documentation or research article, e.g., as both have advantages and disadvantages: while A might recover fewer files, an investigator might not be able to explain (understand) how tool B is operating (missing transparency).

Contribution. Although this article cannot address all points raised, it provides an entry-level discussion of automation for digital forensics. We provide the following contributions:

- We present a definition of automation for digital forensics (Sec. 2).
- We discuss important aspects and considerations to achieve a common baseline (Sec. 3).
- We summarize three practitioner interviews and offer their view of automation (Sec. 4).
- We present four different concepts that are currently being explored to advance automation (Sec. 5).

We hope that this article stimulates the discussion within the community and helps create a unified understanding of what automation means in the context of a digital forensics investigation.

Impact. Definitions provide clarity, i.e., where do we want to go, which are potential risks, and what steps can we take to enhance the status quo? Without a global perspective, individuals and research groups will work in silos without seeing and understanding the big picture. As an example: more and more researchers utilize artificial intelligence to automate tasks. While AI works well for certain problems, it is important to understand the loss of transparency (an element of the definition). On the other hand, many individuals associate automation with 'being faster' while we argue that it is also worth automating processes to obtain more consistency even if they are less efficient. Consequently, our definition stresses important elements, not all of which are obvious.

Methodology. This work started with an unsuccessful search for definitions of 'automation for digital forensics', i.e., we have found that no one has defined automation in the context of digital forensics. As a result, it was considered necessary to expand our research to other disciplines to determine how automation is defined. In addition to discussions with academics (parts of this article have been previously presented[2] (orally), discussed, and feedback was incorporated), we interviewed three practitioners (a non-representative sample size but sufficient to obtain first insights) to not only reflect the academic per-spective. During the interviews, we confronted them with the first version of our definition. Obtained feedback was used to refine this article including the definition.

Outline. The next section introduces the terminology and the definition. The subsequent section, Considerations and deliberations, highlights various aspects of automation, such as differences in automation, its challenges, and drawbacks. The Automation from a practitioner's perspective section includes the results of three semi-structured interviews. In Enabling automation - current trends, we summarize some current trends and possibilities for automation before we present the Background and related work along with the Discussion and next steps. Finally, we summarize the important points of the paper in the Conclusion.

2. Towards a definition

Given the uniqueness of a digital forensics investigation, definitions from other works (outlined in Sec. 6) can only be used as guiding principles: they do not perfectly translate. Consequently, this section summarizes the used terminology and presents a definition for automation in the context of digital forensics.

2.1. Terminology

Other disciplines differentiate between assisted, automated, and autonomous. For instance, Gasser and Westhoff, Bundesanstalt für Straßenwesen [12, 13] summarize the differences in driving automation levels as follows:

Assisted describes a system that has supporting functionality (e.g., ESP). The driver has full responsibility and must monitor the correct functioning of the systems at all times.

Automated describes a system that takes over the driving for a short period where the driver can carry out another activity, e.g., write an Email. However, the system may notify the driver and the driver must react in a reasonable amount of time (i.e., one cannot rest in the back seat).

Autonomous means that the system has full responsibility. People on board are passengers and have no driving-related duties.

Digital forensics uses both terms (assisted and automated) as synonyms and thus we will not differentiate between them. Furthermore, autonomous, i.e., a system

[2] Intermediate results have been presented at **blinded for review**

completing the investigation, is often referenced as *full automation*.

In addition to these general descriptive terms, we have found several terms concerning automation such as process, subprocess, method, task, routine, subroutine, procedure, or technique. It will require a discussion of these terms and the development of a common glossary which is not the goal of this work but future work. For simplicity, this paper specifies the following:

1. Each investigation follows a method/process.
2. Each investigation consists of a series of n tasks (addressing the mandate) that need to be accomplished.
   - The order of completing tasks *may* be important, e.g., the acquisition must be completed before report writing.
   - Tasks are different in complexity and have different impacts on the investigation, e.g., file carving vs. report writing.
   - n is specific to each investigation because each investigation is different.
3. Tasks may be further divided into other tasks which are commonly called sub-tasks or steps.
   - While tasks may be similar among investiga-tions (higher granularity, e.g., analyze Email artifacts), sub-tasks/steps rely on the mandate (e.g., was the suspect at a certain location). Consequently, each investigation follows a different method/process.
4. A tool implements 1 to m tasks (or sub-tasks, steps) which we then qualify as automated (tasks can be completed manually, in that case, they are not qualified as automated). Note, $m = n$ denotes autonomous (full automation); normally $m \ll n$.
5. Ideally, tasks have a defined input and a defined output that can be validated which is important to ensure that automation works correctly. Tasks should also have appropriate error handling (this is difficult and discussed later).

Note, we keep it general and do not define where a task ends, and a sub-task/step starts; except that sub-tasks/steps are closer to the mandate.

Example. The *mandate* requires verifying if a phone was at a specific location at a certain time. Some *tasks* that need to be accomplished to address the mandate are (1) identifying, extracting, and analyzing relevant artifacts from the device, (2) identifying and contacting the telephone service provider (TSP), or (3) writing a report. Out of these tasks, some *sub-tasks/steps* can be derived such as (1.1) search for GPS coordinates in picture metadata (EXIF), (2.1) contact TSP and request cell tower location data for a given number/time, or (3.1) summarize the mandate and formulate a hypothesis. The extraction of data is completed automatically using appropriate software; to analyze the EXIF data, an examiner uses a tool parsing all available data and returns a visual representation (e.g., pins on a map). An investigator then manually combines the data obtained from the TSP and the EXIF data and writes the conclusion in a report.

2.2. Proposed definition

We came across several definitions that we deem suitable but not ideal, e.g., “a device or system that accomplices (partially or fully) a function that was previously carried out (partially or fully) by a human” [14, p13] or “any system that performs a process instead of a person to address forensic questions” [15].

To develop the definition, we discussed with peers (including interviewees), read product descriptions of software vendors (providing automation software), and researched articles to determine what is promoted and what are end-users looking for when investing in automation. For instance, Magnet Forensics [16] states that their tool Magnet-Automate improves both efficiency and continuity where the latter is improved by automating the workflow, streamlining the processes, and using available hardware in an optimal way. CCL Solutions Group [17] and MSAB [18], two other forensic software vendors, promote scalability and transparency, respectively. Non-forensic IT companies such as IBM [19] and VMware [20] express increased productivity, efficiency, consistency, and transparency that automation can bring. IBM Cloud Education [21] mentions better accuracy by using Robotic Process Automation (RPA, more details in Sec. 5). Techopedia [22], a general blog, specifies that automation can improve both efficiency and reliability. Identical terminology and goals are used in academic literature. Asquith and Horsman [23] discuss the potential of RPA for digital forensics and conclude that “productivity is potentially increased”. Franke and Srihari [24], who used the term computational forensics instead of automation, see its potential in increased efficiency but also point out the potential to “support standardized reporting on investigation results and deductions” (transparency, consistency). In summary, we see the following motivations of labs and organizations when they invest in automation:

- Productivity: replace repeatable processes to allow human resources to focus on unique (non-automated, more challenging) tasks. (efficiency)
- Continuity: eliminate manual transitions of digital evidence from one process to the next, allowing automation to perform such transitions and continue processing while examiners are not working (e.g., overnight, weekends, holidays). (efficiency)
- Scalability: distribute processing across available hardware to make the most use of existing resources

and handle growing data volumes more efficiently (reduce idle time). (efficiency)

- Consistency: reduce the risks of (different) examiners doing the same process in different ways, potentially having different results. (reliability)
- Accuracy: provide more accurate results due to better performance and absence of tiredness, especially for highly repetitive tasks. (reliability)
- Transparency: produce an audit trail of all tasks performed on digital evidence for quality assurance as well as court purposes[3].

Consequently, we present the following definition which is based on the three main categories listed in parentheses in the previous itemization:

> **Software or hardware that completes a task more efficiently, reliably, or transparently by reducing or removing the need for human engagement.**

The definition uses **or** indicating that automation may only fulfill one of these aspects. For instance, the automated task may be slower compared to a human completing the same task but if it is more reliable or transparent, it is still beneficial and aligns with the definition. Ideally, automation fulfills all aspects.

An aspect this definition does not mention is 'improved moral/working conditions' meaning that a motivator for automation can be the removal of disliked tasks from the investigators' duties. As disliked tasks are often repetitive tasks, one may argue that this element is covered by *productivity*.

3. Considerations and deliberations

A failure to define what automation is in the context of digital forensics makes it difficult to identify what concepts are considered automation and which are not. As a result, it is difficult to manage the risk that automation brings as it may not always be obvious that it is present. In the following, we highlight different perspectives that should be considered when working in the domain.

3.1. Ideal world of automation in DF vs. reality

The spectrum of automation reaches from *no/basic automation* to an *autonomous investigation* where we differentiate between the following three categories:

Autonomous investigation: In a fully automated environment, all n tasks comprising the investigation are automated including the transitioning between these tasks. An investigator provides all relevant data (in any form) to a system including the criminal charge. The system autonomously processes the data and returns a comprehensive report that can be handed to a prosecutor. The investigation is conducted *efficiently, reliably,* ***and*** *transparently* at all times and thus allows a thorough evaluation. From a digital forensics process model's perspective, each phase (collection(acquisition), examination, analysis, and reporting) is completely automated and connected; data between various phases and tasks is transferred automatically. This may be considered the hypothetical *fully automated approach*. However, achieving this is difficult (or maybe impossible), and at present, the field is arguably far from this position. On the other hand, it is questionable if practitioners and courts would accept these generated reports. Yet, for automation to be beneficial, it does not have to reach this level of deployment, where subsets of relevant automation can also be of value.

Automated task: A given task is completed automatically in an *effiient, reliable,* ***or*** *transparent* manner. As inputs and outputs are well defined, it is possible to assess the outcome (e.g., compare several tools). This has already been accomplished to a certain degree. For instance, let us assume the task known-file-filtering. All files are hashed using a reliable hash function, compared against a vetted database, and are either ignored (files are whitelisted) or considered relevant (files are blacklisted). The input could be a disk image and the output a list of files. For this task, all three properties of the definition are fulfilled.

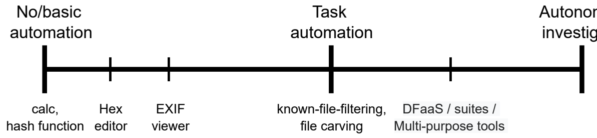
No/basic automation: This describes a scenario where no or only basic tools are available to the investigator to complete the task. We define a basic tool as a tool that has not been developed particularly for digital investigations, often comes with the operating system, and its impact on the investigation is small. Common examples are hash functions, hex editors, text processing software, or regex. With these tools, an examiner could theoretically still complete the task of known-file-filtering but would require more time. Tasks, that are currently not well-supported and are the responsibility of the investigator (manual tasks), are the decision-making process and the reporting.

The distinction between these categories is difficult. We, therefore, propose to see this as a spectrum allowing relative comparisons, as shown in Fig. 1, until a categorization scheme is developed. Table 1 offers additional automation considerations where a distinction is made between what the authors consider an 'Automated task' and an 'Autonomous investigation'. Here, some of the typical traits in regards to each type of automation are noted, rating from the type of data expected to be supplied to each of the types of the automation process, expectations of the

[3] Note, current trends go in the opposite direction and utilize blackboxes or unexplainable algorithms.

product of their use, and their role in the investigative process.

Figure 1: Automation spectrum with several examples: A calc or hash function is more basic than a Hex editor or an EXIF viewer; known-file-filtering or file carving are tasks that have been successfully automated; Digital Forensics as a Service (DFaaS), suites or multi-purpose tools complete various tasks but are still not autonomous.



Automated task[4]	Autonomous investigation
Known data inputted, known expected outcome (e.g., image file being parsed)	Unknown data (content on system), unknown output (do not know what the approach might say, or the decision being made)
Output expectation, e.g., set of files or GPS locations	No expectation
Detecting errors in the tool might be easier/more obvious	Error detection is more difficult as more complex
Preparatory in nature/support for examiner	Interpretive in nature
Task Processing	Investigative mindset
Operate under tighter conditions - rules for the tool to work are strict	As data may be unknown/unstructured - rules are less known
No/little decision support	Maximum decision support /decision is done

Table 1: Some differences between automated task and autonomous investigation (full automated).

3.2. Automation deadlock

Several elements explain the lack of automation for digital forensics:

Missing interfaces. The tools used by forensic laborato-ries are not created/suitable for automation. Most tools are designed to be user-friendly and only provide a GUI without supporting an alternative way of interacting with it such as a CLI or API, which limits the progress of automation. Although several tools allow expanding functionality using plugins, these plugins cannot be combined with other tools due to the different programming languages and interfaces.

Interoperability. While a data format can be considered a special type of interface, most tools utilize proprietary formats to store data as there is no accepted format to exchange case-related information. And even if there is such a format (CASE, as discussed in Sec. 5, is trying to fill this gap), it is questionable if software vendors would support it: proprietary formats force users to stick to one vendor allowing them to sell their products, and ensuring licenses are renewed.

Addressing these two challenges requires either retrofitting missing functionality (may be difficult), the development of a new generation of tools (expensive, etc.), or implementing tools that 'parse-and-translate' from one tool to another (expensive and difficult). However, we believe that interoperability and interfaces are essential to progress automation as there is yet no single tool that can cover all aspects of an investigation.

Practical realization. A third element is the knowledge, motivation, and resources of investigators: some may not have the skills to develop and propose a way to automate tasks. Others may have the skills but do not want to develop a new script/tool. Some might also have the needed skill and motivation, but lack resources, e.g., time or money, where in the latter case hiring external developers is also not possible. Another challenge is that each investigation is different and with it the underlying tasks. Building automation that is globally usable is difficult and may currently not even be possible without accepted interfaces and exchange formats.

3.3. Automation drawbacks

Relying on tools and automation too much may also have negative consequences. For instance, it may decrease the practitioner's investigative skills and the investigation quality (on the positive, it allows laymen to work on cases; [10]). Bugs are a second challenge leading to incorrect results [25] or biased algorithms due to poor training data [26]. Identifying these types of errors is often impossible due to a lack of transparency: the exact procedure of a tool is unknown (e.g., closed-source commercial tools), too complex (e.g., by applying artificial intelligence), or errors are not well communicated by the tool.

Discussions about some of the risks have already started. For instance, Ottmann et al. [2] are concerned about the usage of 'blackboxes' (e.g., mobile phone software suits from private companies) for forensic investigations; Deeks [27] stresses the importance of explainable AI. As we do not see this changing, we argue that validation and error handling are essential to progress:

Automation validation. If the technology itself cannot be validated as it is too complex or closed source, we see two other possibilities:

[4] While we list 'automated task', most differences also apply to 'no/basic automation'.

1. Input-output-validation: One may use datasets where the outcome is known (e.g., because the data was created for this purpose) and feed it to the tool. If the returned output matches the known output, the tool works correctly. Of course, the input data needs to be comprehensive to also cover special cases. An example is the computer forensics tool testing (CFFT) program by NIST [28].

2. Cross-comparison: The second possibility relies on having two or more tools addressing one task and (unknown) data. If all tools return identical results, it is likely that all tools work correctly. The more tools are compared, the higher the likelihood.

In both cases, standardized outputs are essential to allow an automatic comparison which is unfortunately not the case as mentioned in *interoperability* in Sec. 3.2. While a manual comparison is possible, this does not scale as ideally the validation should be done for every newly released version of a tool. Note, both validation concepts cannot assess the applied method, i.e., the tools may still follow completely different pathways to accomplish a goal.

Error-handling[5]. This is an area that is often neglected, and the question is: how should automation handle notifications and errors? Shall a user be notified instantly, shall there be a summary at the end, which errors shall (can) be ignored (may depend on an investigation), etc? Currently, developers treat errors/problems differently requiring result validation on the user side. This can be up to a point where it takes an examiner longer to assess the automated results than performing the task manually. Let us consider the following example: A tool automates the EXIF extraction from a set of pictures. Depending on the software, the tool could

- ignore pictures that do not contain EXIF information without notification
- list the pictures and say: no EXIF found
- be precisely stating that the EXIF data did not contain: GPS, resolution, camera model, etc. (which would result in a long list)
- provide an end-summary
- etc.

Now let us imagine the same application but running as a service in the cloud, i.e., pictures are sent and the service answers. To save resources (bandwidth), one may opt for a minimal solution and only return an answer if data is found. While this behavior seems logical, it will be difficult to make sure the service received all images and processed them; maybe there was a system error, data got lost, or the system quota was reached. Identifying and defining an appropriate default behavior for various use cases will be a challenge but essential so that people will trust automation.

3.4. Areas of application for automation

One requirement for the application of automation is the *consistency of the input*; it works well if the input has a defined structure. Consequently, it has proven itself particularly useful for tasks that require

Fixed translation/parsing: Converting data into a more human-readable representation. Examples include converting binary into hex or ASCII; interpreting EXIF information according to the specification; or displaying network communications (e.g., Wireshark).

Mathematical operations/statistics: Performing some sort of calculation on the input. Examples include creating the hash value of an input; Fast Fourier Transform for photography processing; or calculating the longest network connection.

Comparisons: Completing simple comparisons to find, highlight, filter, or sort. Examples include comparing hash values against a database; highlighting/filtering entries given a certain criterion; finding files larger than 1 GB; or finding all *.doc files.

Of course, automation is also applicable to a combination of these tasks such as keyword searches which require parsing input and performing comparisons. All these tasks have in common that there is no (complex) decision-making involved.

With the help of AI, this is slowly changing, and software is now able to make decisions based on previously encountered data (learning) which increases automation capabilities. For instance, machine learning has been utilized for classification and clustering to automatically prioritize data: da Cruz Nassif and Hruschka [29] tried various clustering algorithms along with different features such as the name of the document, frequency of words, etc., to organize documents. The idea was to cluster the relevant/related documents together. Du and Scanlon [30] proposed to prioritize files based on their metadata. First, files are hashed and compared against a 'known-to-be-of-interest' hash set. Matches are used as input to train classifiers (based on their metadata) which then is applied to the unknown files to determine if they are of interest or not.

3.5. What can be automated?

This section only considers software solutions and ignores approaches that require a combination of software and physical systems (e.g., a hardware write blocker).

[5] Defining 'error' and its implications on an investigation is beyond the scope of this article. For simplicity, we utilize the term error as any unexpected behavior such as bugs, relevant elements missing, wrong/incomplete results, etc.

We claim that *every task that can be formalized can be automated* whereas formalizing is the ability to state a problem (or describe a computing system) completely [31]. To describe a problem completely, it is divided into a se-ries of smaller (more trivial) problems that are easier to accomplish. This process is recursive, meaning that newly identified problems may be broken down further, and so on. Once a problem is 'simple enough', it can be auto-mated (i.e., implemented) and the process is completed. An important aspect of completely describing a problem is the consistency of inputs and outcomes which are often unknown/vague for forensic problems.

Simple enough. Determining if a problem is simple enough depends on the problem itself, the context, available technology, and advancements over time. For instance, while several months ago the problem of 'writing an essay on a given topic' would be difficult, it now can be considered 'simple enough' due to the release of Open-AI ChatGPT[6]. Generally, 'simple enough' means that the problem can be described with atomic steps such as hash-a-file, open-a-folder, or search-for-a-keyword.

Examples. Let us consider the problem of finding evidence that a device was at a certain location at a given period of time. Investigating this problem requires contacting the telephone service provider to request cell tower location data, analyze taken photos including metadata, or read text messages (undefined/variable input). All these inputs contain the information in different formats. To form a conclusion, findings need to be combined and the outcome is an indicator or likelihood which has been discussed by Casey et al. [32]. Other domains are often more straightforward, e.g., in the area of malware detection the input is a file (e.g., EXE on Windows) and the outcome is yes or no (a binary decision). Another example is incident response where software searches for indicators of compromise such as network traffic on unusual ports, spikes in the column of data, or connection to known-to-be malicious IPs. Of course, there are also forensic problems that can be completely described such as known-file-filtering where the input (disk image) and outcomes (set of files) are clear, and the simple enough problems are: parse and hash each file in a file system, compare the hash against a database, ignore known benign files (or list known malicious files).

We conclude that every problem is formalizable and automatable in theory, but not yet in practice as sometimes it is too complex to be implemented in a convenient manner. Autonomous investigations are unlikely.

3.6. What should be automated?

One answer (and following the definition) could be: everything that makes the investigation more efficient, more reliable, or more transparent should be automated. However, we believe that it also requires considering and balancing several other areas (no specific order; areas overlap):

Return on investment: From a business perspective, ROI is essential. Thus, if the task at hand frees up significant investigative capacities, helps reduce backlogs, or lowers costs, which outweighs the development cost, it should be automated. A task that occurs on rare occasions may yield no ROI. Making this decision requires defining the tasks and tracking how often a specific task is performed.

Feasibility: Given current technology, it may not be possible to automate a specific task. This can have different reasons such as the input format not being well defined, the complexity being too high, underlying technologies having high error rates, or requiring frequent human validation. On the other hand, some tasks cannot be completed by humans due to complexity (e.g., carving, blacklisting) and require automation.

Human satisfaction: Tasks that are disliked should be considered for automation to keep a good work ethic. We also argue that disliked tasks are more prone to human error.

An example is forensic report writing: This is done for every investigation, is time-consuming, and automating it would have a high ROI. According to our interviewees (see Sec. 4), this is also a less-liked activity. However, as evidence is not represented in a standardized format, mandates differ, and jurisdictions have different requirements, automated reporting seems unfeasible.

4. Automation from a practitioner's perspective

To include the practitioner's perspective, we conducted three semi-structured interviews with individuals from law enforcement. The objective was to learn what automation means to them, what repetitive tasks they face, and where automation is (not) used. While the sample size is not representative, we argue that first insights into the practitioner's perspective are sufficient for this article. In the future, more practitioners, as well as academics, shall be considered.

Context. Interviewees have 10+ years of experience in French law enforcement and/or the private sector. Candidates were selected as the authors have worked with them in the past, they had immediate availability as well as were available for follow-up questions, and they have some bearing on academia. Interviews were conducted by one or more authors and each lasted approximately one hour. The recordings of the interviews were manually transformed into a shortened transcript which served as the input for the upcoming paragraph. Note that a

[6] https://openai.com/blog/chatgpt/

preliminary version of this section was shared with interviewees as well as some follow-up questions were raised. Interview questions are listed in Appendix A.

Results summary. We started by asking what automation means to them, where one interviewee said to "complete repetitive tasks with a machine, without any human in the equation."[7] It was noticeable that all three interviewees agreed that automation means replacing repetitive tasks using computers to free up time but also to replace disliked tasks and tasks that cannot be manually completed by an investigator (e.g., manually performing known-file-filtering or keyword searches). Subsequently, we confronted them with *a preliminary definition*[8] that aligned with their conception. However, it was mentioned that 'reliable' may not always be the case and depends on the task. In particular, the example of image classification was given, and it was argued that humans still outperform algorithms. Interviewees agreed that at least one of the proposed characteristics (efficient, reliable, reduce human labor) should be met to qualify as automation.

When asked about repetitive tasks that they encounter in their daily work, one answered that "the most repetitive tasks are the administrative tasks: starting a case, collecting data, getting the items, ... up to the report delivery". These are often activities before the actual investigation starts like bag-and-tag devices, documenting them via pictures, traceability (i.e., access logs, hash sums), or performing a basic analysis of the devices (e.g., number of partitions, file system, existing user accounts, etc.). Interviewees described that by 'environment analysis' and 'case preprocessing'. We classify them as *secondary tasks* meaning that they only have a marginal contribution to the success (solving) of the case. Interestingly, the tasks mentioned were identical to tasks they dislike. There was a consent that all these repetitive tasks could at least partially be automated, but they are often not on the radar of vendors and software developers or only are automated for accounting purposes. At some point, all interviewees automated a repetitive task themselves where the driving factor was gaining time and eliminating a repetitive (boring) task. However, it required a careful assessment: is it worth automating this task, i.e., is there a time gain?

On the other hand, all agreed that it is difficult to impossible to automate tasks that relate to the expert's opinion such as connecting dots between various events, documenting them in an acceptable language, and providing explanations in court. The reason mentioned was that there is no standardized (formalized) procedure. However, assistance programs support efficiency, e.g., show all potential artifacts and the investigator makes the final decision. One expert believes that "the expert's work will always be needed, especially to explain elements to non-scientific people".

We then asked them if they can think of requirements a task must meet to be automatable. Surprisingly, the consent was it would require stable inputs (or changes in the input that can be foreseen). They also mentioned that it must be profitable; the practitioner must gain something out of it. Two important comments were: (1) experts still need to understand what is going on behind the scenes and be able to explain it in court if asked; (2) with recent developments in AI, exact repeatability may not be given, and a tool may return similar but not identical results for the same input especially if learning is involved.

Given a digital forensics process model, it seems that the automation focus has been 'early' phases: Acquisition receives significant automation support, analysis is balanced between the automation and the manual work, and the reporting phase is the least automated phase (this includes case management duties). Interviewees mentioned that rudimentary report automation exists. However, it is not sophisticated enough to answer the mandate's question(s). In contrast, providing automatically generated reports to judges could lead to misunderstandings and misinterpretations of the results. On the positive side, some parts of the reports can be automated with a template but the questions answering parts still need to be completed by a human.

A limitation/challenge mentioned was the fast evolution. For instance, an application may change its utilized data structures which can be as simple as 'switching two columns in an SQLite table' to relying on 'a novel proprietary format to store data'. The more is automated, the more likely is it that even minor changes may cause problems which conversely cause delays. Either permanent updates need to be ensured or focus on small tasks and modularization is needed to circumvent these problems.

Other interesting finding. Another challenge that came up when developing own tools or searching for existing tools (or generally gaining knowledge) is the aspect of sharing. On the positive side, interviewees reported that they aim to share their knowledge (no case details) and tools with immediate colleagues as well as on national and international platforms (usually not available to the public). However, the sheer number of channels and the commonly unstructured data (e.g., a forum entry, a message in a discord channel, or a mailing list) make it hard to keep track of and identify relevant information. Once an appropriate tool is identified, the question raises if the tool is reliable and accepted in court or if it may be better to do it yourself (reinvent the wheel).

[7] All citations in this section were freely translated and/or slightly reformulated for better readability.

[8] The definition presented to the interviewees was slightly different and read as follows: Software or hardware that reduces or removes the need for human engagement when completing a task to be more efficient, more reliable, or reduce human labor. The definition in Sec. 2 is the updated version incorporating the feedback.

5. Enabling automation - current trends

The following trends have been found aiming to improve the status quo of automation:

Digital Forensics as a Service. DFaaS summarizes the concept of a centralized service processing the data and allowing personnel to access case details. One existing implementation is Hansken which is based on XIRAF and was introduced by Baar et al., van Beek et al. [33, 34] and is maintained by the Netherlands Forensic Institute (NFI, [35]). Hansken is a central platform where forensic images are sent to and processed, i.e., a standard set of tools is run over the image such as file recovery, database extraction/parsing, email extraction, etc. This workflow comes with several advantages. For instance, storage and processing are done autonomously, separation by expertise (tech personnel develops new parsers, investigators focus on investigative work, and only little experienced individuals complete easier tasks such as feeding data to the system), or share information among a team. Hansken is an active project and is likely to improve over the years. A downside is that Hansken requires excessive processing power, and the setup is not as easy as installing a standalone application. Adjusting the interface and processes to personal needs may also be difficult.

Robotic Process Automation. According to IBM Cloud Education [21], RPA "uses automation technologies to mimic back-office tasks of human workers, such as extracting data, filling in forms, moving files, et cetera." It does this by emulating human behavior, e.g., clicking on a button, typing in text, or copying/pasting data. Thus, RPA is applicable to repetitive and standardized tasks that are unlikely to change. Conversely, a major problem with RPA is the lack of flexibility: a change of the procedure/task/GUI requires retraining, e.g., if a button is moved to a different position. The possibilities of RPA in a digital forensics' context have been discussed by Asquith and Horsman [23]. The authors presented two case studies and areas of applicability. The authors conclude that "RPA can carry out some of the basic pre-processing tasks undertaken in DF, however, their implementation requires specific planning within an organization to ensure that the digital environment is suitable for its use."

Workflow automation. Workflow automation uses rule-based logic to launch a series of tasks that run on their own without human intervention to optimize time and hardware usage. First, during the setup phase, one must decide which tasks can run in parallel and which are dependent on each other, e.g., the acquisition should be first, but then various parsers may run simultaneously. Once everything is in place, the idle time of hardware is reduced as machines can work during weekends or holidays. Existing solutions are either universal, i.e., can be used for various use cases such as Apache Airflow[9] or target digital forensics such as Cascade[10] or Magnet-Automate[11]. In addition to these partially commercial solutions, Wen et al. [36] propose a cloud-based framework that is divided into three modules: a data uploading module, an application store module (a place where all relevant tools and scripts are stored), and the queue-module which is managing the tasks and creating the queue based on the tasks that can be parallelized/serialized. Similarly, de Braekt et al. [37] proposed a "workflow management automation framework for handling common digital forensic tools". The authors also created a specific automated workflow for the acquisition phase and the cleanup/archiving process.

Cyber-investigation Analysis Standard Expression. CASE can be seen as a facilitator of automation by bringing a standardized representation of information. According to `caseontology.org`, CASE is a "specification for representing information commonly analyzed and exchanged by people and systems during investigations involving digital evidence. The power of CASE is that it provides a common language to support automated normalization, combination, and validation of varied information sources to facilitate analysis and exploration of investigative questions (who, when, how long, where)." Thus, it addresses one of the concerns raised in Sec. 3.2. CASE is an advancement of DFAX (Digital Forensic Analysis eXpression; Casey et al. [38]) and was proposed two years later by Casey et al., Casey et al. [39, 40]. CASE is a community-led project (under the Apache v2.0 License) allowing everyone to join and contribute. The project recently received a lot of attention from different institutions/organizations when it became part of the Linux Foundation [41].

6. Background and related work

Automation is relevant for many domains where it has been researched and defined, e.g., undersea teleoperators [42], air traffic control [14], or self-driving cars [12] which are summarized in Sec. 6.1. As these definitions do not transfer well to domains such as digital forensics, the subsequent section highlights work addressing automation for digital forensics. Note, this section uses peer-reviewed and non-peer-reviewed work like blog posts from companies ensuring a balance between academia and industry.

6.1. Automation in general

We searched for definitions for 'automation' from various domains to identify how automation is defined beyond the forensic domain. A key finding was that definitions

[9] `https://airflow.apache.org/`

[10] `https://www.cclsolutionsgroup.com/products/cascade`

[11] `https://www.magnetforensics.com/products/magnet-automate`

are influenced by domain specifics and the entity providing them. For instance, dictionaries like Cambridge Dictionary or knowledge databases like Wikipedia keep it general: "the use of machines and computers that can operate without needing human control" [43]. On the other hand, the International Society of Automation [44] defines it as "the creation and application of technology to monitor and control the production and delivery of products and services". Entities in the domain of 'business' reference this domain by business process automation (BPA) which according to Wikipedia is a form of digital transformation. We favored the proposed definitions by software companies such as VMware [20] "IT automation is the process of creating software and systems to replace repeatable processes and reduce manual intervention" or IBM [19] "automation is a term for technology applications where human input is minimized". IBM also divided automation into four types: basic automation, process automation, integration automation, and AI automation, which shows that levels of automation vary widely. While definitions differ, the listed benefits of automation mostly coincide among the different disciplines. Sources conclude that automation helps to free up human workers, to improve efficiency (accelerates), and enhance reliability (e.g., see Techopedia [22] or Servicenow [45]).

6.2. Automation for digital forensics

We also evaluated literature addressing automation for digital forensics and conclude: while the topic has been discussed by the community, a definition and common language for describing automation and its deployment in digital forensics is missing. Generally, we can say that most sources avoid 'defining' but instead point out the benefits of applying automation and other descriptive statements. For instance, the software vendor Magnet Forensics [46] describes the benefits for forensic labs of having automation as: it allows to streamline processes, "letting examiners off the hook for menial tasks like 'clicking next' time and again'; Deloitte [47] states that automation "saves significant time and expense, and allows investigators to focus more on where fraud might occur".

Similarly, the academic world discusses automation from various angles without defining it. For instance, Homem [48] addresses automation by the benefits it can bring: "efficiency, in the form of reducing the time and human labor effort expended, is sought after in digital investigations in highly networked environments through the automation of certain activities in the digital forensic process". James and Gladyshev [10] outline the challenges with automation, e.g., how automation ("push-button forensics") had a negative vibe back then but stress that forensics "would be impractical without some level of automation".

During our search, the closest three attempts to define automation were from: (1) Jarrett and Choo [49] who wrote "automation is the use of computer systems to automate the traditional process of information acquisition, processing, and interpretation"; (2) Borhaug [50] who stated that "automation refers to a system or process that can operate without human intervention. [... It] is the creation of technology and its application to control and monitor the production and delivery of various goods and services"; and (3) Bollé et al. [15] who said, "any system that performs a process instead of a person to address forensic questions".

6.3. Evolution of automation

At first, the development was focusing on simple tasks like parsing and data representation such as partition layouts and file systems (e.g., The Sleuth Kit [51]) or EXIF information [52]. Depending on who is asked, these tools may or may not be considered automation. With the increased usage of digital devices, the need for data recovery increased (e.g., file carving [53]) as well as the need for data prioritization and data reduction to find the needle in the haystack (e.g., known-file-filtering [54, 55]). This allowed investigators to focus on the investigative process instead of recovering/screening data. With a maturing domain, the community targeted more complex tasks requiring sev-eral individuals/teams to work on a given problem. One example is event reconstruction (timelining) which started with GUI-based tools allowing filtering/searching [56], towards complex super timelines [57] followed by data reduction as they became too massive, e.g., [58] automated the process of separating events into low and high-level events allowing a faster analysis. Today, many researchers focus on applying artificial intelligence to various digital forensic challenges. A major problem is that most data is unstructured and unlabeled, making the application of automation very difficult. In parallel, different ontologies such as CASE are developed (cf. Sec. 5) in order to pro-pose a standardized way to restructure/reorganize data. Having complete forensic cases in a structured format al-lows, for example, Case Based Reasoning (CBR) which is described by Mitchell [59] as utilizing a collection of previous cases and comparing the current cases based on a developed metric. Of course, AI is also applied to many other problems such as inconsistency checks on evidence [60] or separating relevant from irrelevant documents using clustering [29]. More complete overviews are provided by Du et al. [8], Iqbal and Alharbi [61], and Jarrett and Choo [49] who address and summarize the impact of artificial intelligence for automation in digital forensics. A challenge with AI is the missing transparency which started a discussion of explainable AI [62]. Addressing this last challenge is important because transparency and, more importantly, the chain of custody is critical to the acceptability of evidence in court.

7. Discussion and next steps

The goal of the presented definition is to establish a common understanding of automation for digital forensics. However, this topic requires more community feedback and further development.

One of the areas requiring more work is the underlying terminology. Currently, various terms are used as synonyms, e.g., method, process, task, sub-task, procedure, etc. Does the community want to differentiate between these terms (is there a need)? In this case, what do we automate, or can we automate on various levels, i.e., automating a task vs. automating a method? Is the outcome of automation always software? Eventually, this will lead to other points of interest like how automated approaches can be described allowing users to have a solid understanding without reading comprehensive documentation. For instance, does it require listing/providing error rates, the dataset it was tested on, or a short description of the underlying technology?

Furthermore, there should be a discussion on autonomous investigations (full automation), i.e., does the community agree on what has been proposed in Sec. 3.1? Is this even achievable or do we agree that we will never reach this point? Currently, most of the tools support the evidence preparation and transformation but the analysis (connecting the dots) is the examiner's responsibility and so is the report writing. If an autonomous investigation system will never be a reality, this means automation will always assist an examiner. In this case, is automation the best term or would 'computer-assisted forensics investigation' more appropriately describe it?

As the definition is kept broad, most if not all tools lay within this definition. For instance, an EXIF reader increases the efficiency of analyzing information by automatically parsing the hex data into a human-readable format; a tool conducting known-file-filtering removes the need for a human to parse files, compute their hashes, and compare them against a database (improved efficiency). If these tools are well tested, they complete the tasks more reliably (consistent; humans may make errors). As both approaches are different (one may argue that known-file-filtering is more complex than an EXIF parser), a definition alone is insufficient. This is especially true if we consider automated tasks that utilize machine learning. Hence, it requires a way to classify or categorize various approaches. This need to differentiate between rather simple and more complex forms of automation has also been raised by Al Fahdi et al. [63]. In their work, the authors define "the use of hashing to identify known and notable file" as rather simple and does not compare well with the proposed "Automated Forensic Examiner (AFE) that can utilize AI and criminal profiling to identify, extract and correlate suspect data."

A logical next step is the creation of a classification, categorization scheme, or matrix allowing for more granularity and a comparison of approaches. Other domains (including traditional forensic sciences) have introduced Levels of Automation (LoA). Some first thoughts on LoA are summarized in Appendix B. For instance, Swofford and Champod [64] presented a model for LoA in (traditional) forensic science to classify the level of "algorithm usage" in a decision-making process. The levels range from level 0 (no use of an algorithm) to level 5 (the algorithm is providing the decision). The most significant transition is from L2 to L3 where the decision-making transfers from the human to the algorithm. The model presented describes the use of an algorithm to make opinions/conclusions, which is a decision-centered model that does not transfer well for us. However, the switch between human vs. algorithm control is interesting.

From a practical perspective, more standardized interfaces are necessary to advance the domain. Having standardized interfaces allows developers to create modular approaches and should reduce the development of similar tools. The first step towards this idea is already accomplished with the CASE initiative which can be seen as a common data structure to represent forensic case data (input/output for tools). However, the question remains on how do we encourage (force) the utilization of these standards. Maybe this will require governments to intervene and regulate interfaces. This will help during the development of tools as we will have the possibility to focus on the automation of the task instead of worrying about the data type/structure management of the input and output.

An aspect that has been mostly ignored in this article which also requires discussion is the risk of automaton, e.g., due to missing transparency. Is it okay to utilize blackboxes/complex algorithms to make decisions on our behalf? Should we blindly trust vendors that their tools operate flawlessly? How can blackboxes be assessed and tested?

If practitioners cannot understand the tool's workflow, how will they justify findings in court? To avoid this discussion for now, we may focus on assisting investigators instead of making autonomous decisions that then cannot be explained. However, a discussion will be necessary especially once more AI is used to make decisions, e.g., if an AI is used to detect deepfakes (created by another AI).

8. Conclusion

Automation for digital forensics has become indispensable and the community has a vested interest in advancing this field. To establish a common understanding, this article proposed a definition that is based on the improvements labs and organizations like to see: productivity, continuity, scalability, consistency, accuracy, and transparency. Consequently, the article concludes with the following definition:

> **Software or hardware that completes a task more efficiently, reliably, or transparently by reducing or removing the need for human engagement.**

In addition, we conclude that advancing automation will be difficult if current deadlocks (missing interfaces, interoperability, and practical realization) as well as drawbacks of automation (automation validation or error-handling) are not addressed.

[1] Brian Carrier. Open source digital forensics tools: The legal argument, 2002. URL https://citeseerx.ist.psu.edu/doc_view/pid/29cd685bc0b461fb25f0c7d966fdfaad83d4fc94.

[2] Jenny Ottmann, Johannes Pollach, Nicole Scheler, Janine Schneider, Christian Rückert, and Felix Freiling. Zur blackboxproblematik im bereich mobilfunkforensik. *Datenschutz und Datensicherheit - DuD*, 45(8):546–552, 2021. doi: 10.1007/s11623-021-1487-1.

[3] III Richard and Vassil Roussev. Digital forensic tools: the next generation. In Nicholas Kolokotronis Panagiotis Kanellis, Eevangelos Kiountouzis and Drakoulis Martakos, editors, *Digital crime and forensic science in cyberspace*, pages 75–90. IGI Global, 2006. doi: 10.4018/978-1-59140-872-7.ch004.

[4] Nicole Beebe. Digital forensic research: The good, the bad and the unaddressed. In Gilbert Peterson and Sujeet Shenoi, editors, *Advances in Digital Forensics V*, pages 17–36, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. ISBN 978-3-642-04155-6. doi: 10.1007/978-3-642-04155-6_2.

[5] Simson L. Garfinkel. Digital forensics research: The next 10 years. *Digital Investigation*, 7:S64–S73, 2010. ISSN 1742-2876. doi: 10.1016/j.diin.2010.05.009. The Proceedings of the Tenth Annual DFRWS Conference.

[6] M. Al Fahdi, N.L. Clarke, and S.M. Furnell. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In *2013 Information Security for South Africa*, pages 1–8, 2013. doi: 10.1109/ISSA.2013.6641058.

[7] Alastair Irons and Harjinder Lallie. Digital forensics to intelligent forensics. *Future Internet*, 6(3):584–596, Sep 2014. ISSN 1999-5903. doi: 10.3390/fi6030584.

[8] Xiaoyu Du, Chris Hargreaves, John Sheppard, Felix Anda, Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. Sok: Exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450388337. doi: 10.1145/3407023.3407068.

[9] Eoghan Casey and Stroz Friedberg. Moving forward in a changing landscape. *Digital Investigation*, 3(1):1–2, 2006. ISSN 1742-2876. doi: 10.1016/j.diin.2006.01.007.

[10] Joshua James and Pavel Gladyshev. Challenges with automation in digital forensic investigations. *CoRR*, abs/1303.4498, 2013. doi: 10.48550/ARXIV.1303.4498.

[11] Laoise Luciano, Ibrahim Baggili, Mateusz Topor, Peter Casey, and Frank Breitinger. Digital forensics in the next five years. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450364485. doi: 10.1145/3230833.3232813.

[12] Tom M Gasser and Daniel Westhoff. Bast-study: Definitions of automation and legal issues in germany. In *Proceedings of the 2012 road vehicle automation workshop*, pages 1–20. Bergisch Gladbach: German Federal Highway Research Institute, 2012. URL https://onlinepubs.trb.org/onlinepubs/conferences/2012/Automation/presentations/Gasser.pdf.

[13] Bundesanstalt für Straßenwesen. Presse - selbstfahrende autos – assistiert, automatisiert oder autonom?, 03 2021. URL https://www.bast.de/DE/Presse/Mitteilungen/2021/06-2021.html. [accessed 2022-08-08].

[14] National Research Council. *The Future of Air Traffic Control: Human Operators and Automation*. Cambridge Cultural Social Studies. National Academies Press, 1998. ISBN 9780309064125. URL https://books.google.ch/books?id=FzI129gU5jAC.

[15] Timothy Bollé, Eoghan Casey, and Maëlig Jacquet. The role of evaluations in reaching decisions using automated systems supporting forensic analysis. *Forensic Science International: Digital Investigation*, 34:301016, 2020. ISSN 2666-2817. doi: 10.1016/j.fsidi.2020.301016.

[16] Magnet Forensics. Magnet AUTOMATE, n.d. URL https://www.magnetforensics.com/products/magnet-automate/. last accessed 2022-12-18.

[17] CCL Solutions Group. Cascade Forensic Automation, n.d. URL https://www.cclsolutionsgroup.com/forensic-products/cascade. last accessed 2022-12-18.

[18] MSAB. Mobile forensics solutions for Forensic Specialists, n.d. URL https://www.msab.com/roles/forensic-specialists/. last accessed 2022-12-18.

[19] IBM. What is automation?, n.d. URL https://www.ibm.com/topics/automation. last accessed 2022-12-12.

[20] VMware. What is IT automation?: VMware glossary, n.d. URL https://www.vmware.com/topics/glossary/content/it-automation.html. last accessed 2022-12-12.

[21] IBM Cloud Education. What is Robotic Process Automation (RPA)?, October 2020. URL https://www.ibm.com/cloud/learn/rpa. last accessed 2022-12-12.

[22] Techopedia. What is automation? - definition from Techopedia, June 2021. URL https://www.techopedia.com/definition/32099/automation. last accessed 2022-12-12.

[23] Alisha Asquith and Graeme Horsman. Let the robots do it! – Taking a look at Robotic Process Automation and its potential application in digital forensics. *Forensic Science International: Reports*, 1:100007, 2019. ISSN 2665-9107. doi: 10.1016/j.fsir.2019.100007.

[24] Katrin Franke and Sargur N Srihari. Computational forensics: An overview. In *International Workshop on Computational Forensics*, pages 1–10, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg. ISBN 978-3-540-85303-9. doi: 10.1007/978-3-540-85303-9_1.

[25] David Murray. Queensland authorities confirm ‘miscode’affects dna evidence in criminal cases, March 2015. URL http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b. [accessed 2022-08-08].

[26] Giulia Margagliotti and Timothy Bollé. Machine learning & forensic science. *Forensic science international*, 298:138–139, 2019. ISSN 0379-0738. doi: 10.1016/j.forsciint.2019.02.045.

[27] Ashley Deeks. The judicial demand for explainable artificial intelligence. *Columbia Law Review*, 119(7):1829–1850, 2019. URL https://www.jstor.org/stable/26810851.

[28] Barbara Guttman, James R Lyle, and Richard Ayers. Ten years of computer forensic tool testing. *Digital Evidence & Elec. Signature L. Rev.*, 8:139, 2011. URL https://heinonline.org/HOL/LandingPage?handle=hein.journals/digiteeslr8&div=15&id=&page=.

[29] Luís Filipe da Cruz Nassif and Eduardo Raul Hruschka. Document clustering for forensic analysis: An approach for improving computer inspection. *IEEE transactions on information forensics and security*, 8(1):46–54, 2012. doi: 10.1109/TIFS.2012.2223679.

[30] Xiaoyu Du and Mark Scanlon. Methodology for the automated metadata-based classification of incriminating digital forensic artefacts. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, ARES '19, pages 1–8, New York, NY, USA, 2019. Association for Computing Machinery. ISBN 9781450371643. doi: 10.1145/3339252.3340517.

[31] Dina Goldin and Peter Wegner. The interactive nature of computing: Refuting the strong church–turing thesis. *Minds and Machines*, 18(1):17–38, March 2008. doi: 10.1007/s11023-007-9083-1.

[32] Eoghan Casey, David-Olivier Jaquet-Chiffelle, Hannes Spichiger, Elénore Ryser, and Thomas Souvignet. Structuring the evaluation of location-related mobile device evidence. *Forensic Science International: Digital Investigation*, 32:300928, 2020. ISSN 2666-2817. doi: 10.1016/j.fsidi.2020.300928.

[33] R. B. van Baar, H. M. A. van Beek, and E. J. van Eijk. Digital Forensics as a Service: A game changer. *Digital Investigation*, 11:S54–S62, 2014. ISSN 1742-2876. doi: 10.1016/j.diin.2014.03.007.

[34] H.M.A. van Beek, E.J. van Eijk, R.B. van Baar, M. Ugen, J.N.C. Bodde, and A.J. Siemelink. Digital forensics as a service: Game on. *Digital Investigation*, 15:20–38, 2015. ISSN 1742-2876. doi: 10.1016/j.diin.2015.07.004. Special Issue: Big Data and Intelligent Data Analysis.

[35] H. M. A. van Beek, J. van den Bos, A. Boztas, E. J. van Eijk, R. Schramp, and M. Ugen. Digital forensics as a service: Stepping up the game. *Forensic Science International: Digital Investigation*, 35:301021, 2020. ISSN 2666-2817. doi: 10.1016/j.fsidi.2020.301021.

[36] Yuanfeng Wen, Xiaoxi Man, Khoa Le, and Weidong Shi. Forensics-as-a-Service (FaaS): Computer Forensic Workflow Management and Processing Using Cloud. In *The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization*, pages 208–214, 2013. URL http://personales.upv.es/thinkmind/dl/conferences/cloudcomputing/cloud_computing_2013/cloud_computing_2013_8_40_20185.pdf.

[37] Ronald In de Braekt, Nhien-An Le-Khac, Jason Farina, Mark Scanlon, and Tahar Kechadi. Increasing digital investigator availability through efficient workflow management and automation. In *2016 4th International Symposium on Digital Forensic and Security (ISDFS)*, pages 68–73. IEEE, 2016. doi: 10.1109/ISDFS.2016.7473520.

[38] Eoghan Casey, Greg Back, and Sean Barnum. Leveraging CybOX™ to standardize representation and exchange of digital forensic information. *Digital Investigation*, 12:S102–S110, 2015. ISSN 1742-2876. doi: 10.1016/j.diin.2015.01.014.

[39] Eoghan Casey, Sean Barnum, Ryan Griffith, Jonathan Snyder, Harm van Beek, and Alex Nelson. Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. *Digital Investigation*, 22:14–45, 2017. ISSN 1742-2876. doi: 10.1016/j.diin.2017.08.002.

[40] Eoghan Casey, Mariangela Biasiotti, and Fabrizio Turchi. Using standardization and ontology to enhance data protection and intelligent analysis of electronic evidence. In *Discovery of Electronically Stored Information Workshop*, 2017. URL https://serval.unil.ch/resource/serval:BIB_EFAFD05944CB.P001/REF.pdf.

[41] Linux Foundation. The cyber-investigation analysis standard expression transitions to Linux Foundation, December 2021. URL https://www.linuxfoundation.org/press/press-release/the-cyber-investigation-analysis-standard-expression-transitions-to-linux-foundation. last accessed 2022-12-12.

[42] Thomas B Sheridan and William L Verplank. Human and computer control of undersea teleoperators. Technical report, Massachusetts Inst of Tech Cambridge Man-Machine Systems Lab, 1978. URL https://apps.dtic.mil/sti/citations/ADA057655.

[43] Cambridge Dictionary. Automation from Cambridge Dictionary, n.d. URL https://dictionary.cambridge.org/dictionary/english/automation. last accessed 2022-12-12.

[44] International Society of Automation. What is automation? - ISA, n.d. URL https://www.isa.org/about-isa/what-is-automation. last accessed 2022-12-12.

[45] Servicenow. What is automation?, n.d. URL https://www.servicenow.com/now-platform/what-is-automation.html. last accessed 2022-12-12.

[46] Magnet Forensics. Why automation in digital forensics?, April 2020. URL https://www.magnetforensics.com/blog/why-automation-in-digital-forensics/. last accessed 2022-12-12.

[47] Deloitte. How can forensic investigators gain an edge using AI?, n.d. URL https://www2.deloitte.com/ch/en/pages/forensics/articles/forensic-investigators-gain-an-edge-with-ai.html. last accessed 2022-12-12.

[48] Irvin Homem. *Towards automation in digital investigations: Seeking efficiency in digital forensics in mobile and cloud environments*. PhD thesis, Department of Computer and Systems Sciences, Stockholm University, 2016. URL http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-130742.

[49] Aaron Jarrett and Kim-Kwang Raymond Choo. The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Science*, 3(6):e1418, 2021. doi: 10.1002/wfs2.1418.

[50] Tor Stian Borhaug. The paradox of automation in digital forensics. Master's thesis, NTNU, 2019. URL http://hdl.handle.net/11250/2617753.

[51] B. Carrier. *File System Forensic Analysis*. Pearson Education, 2005. ISBN 9780134439549. URL https://books.google.ch/books?id=Zpm9CgAAQBAJ.

[52] Paul Alvarez. Using extended file information (exif) file headers in digital evidence analysis. *International Journal of Digital Evidence*, 2(3):1–5, 2004. URL https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B1F944-FF4E-4788-E75541A7418DAE24.pdf.

[53] Anandabrata Pal and Nasir Memon. The evolution of file carving. *IEEE signal processing magazine*, 26(2):59–71, 2009. doi: 10.1109/MSP.2008.931081.

[54] Harald Baier. Towards automated preprocessing of bulk data in digital forensic investigations using hash functions. *it-Information Technology*, 57(6):347–356, 2015. doi: 10.1515/itit-2015-0023.

[55] Mark Scanlon. Battling the digital forensic backlog through data deduplication. In *2016 sixth international conference on innovative computing technology (INTECH)*, pages 10–14. IEEE, 2016. doi: 10.1109/INTECH.2016.7845139.

[56] Florian P Buchholz and Courtney Falk. Design and implementation of zeitline: a forensic timeline editor. In *DFRWS*, 2005. URL https://dfrws.org/sites/default/files/session-files/2005_USA_paper-design_and_implementation_of_zeitline_-_a_forensic_timeline_editor.pdf.

[57] Kristinn Guðjónsson. Mastering the super timeline with log2timeline. *SANS Institute*, 2010. URL https://www.sans.org/white-papers/33438/.

[58] Christopher Hargreaves and Jonathan Patterson. An automated timeline reconstruction approach for digital forensic investigations. *Digital Investigation*, 9:S69–S79, 2012. ISSN 1742-2876. doi: 10.1016/j.diin.2012.05.006.

[59] Faye Mitchell. The use of artificial intelligence in digital forensics: An introduction. *Digital Evidence & Elec. Signature L. Rev.*, 7:35, 2010. URL https://heinonline.org/HOL/LandingPage?handle=hein.journals/digiteeslr7&div=7&id=&page=.

[60] Pavel Gladyshev and Andreas Enbacka. Rigorous development of automated inconsistency checks for digital evidence using the b method. *International Journal of Digital Evidence*, 6(2):1–21, 2007. URL https://www.utica.edu/academic/institutes/ecii/publications/articles/1C35450B-E896-6876-9E80DA0F9FEEF98B.pdf.

[61] Salman Iqbal and Soltan Abed Alharbi. Advancing automation in digital forensic investigations using machine learning forensics. In B Suresh Kumar Shetty and Pavanchand Shetty H, editors, *Digital Forensic Science*, chapter 1. IntechOpen, Rijeka, 2020. doi: 10.5772/intechopen.90233.

[62] Louise Kelly, Swati Sachan, Lei Ni, Fatima Almaghrabi, Richard Allmendinger, and Yu-Wang Chen. Explainable artificial intelligence for digital forensics: opportunities, challenges and a drug testing case study. In B Suresh Kumar Shetty and

Pavanchand Shetty H, editors, *Digital Forensic Science*, chapter 9. IntechOpen, Rijeka, 2020. doi: 10.5772/intechopen.93310.

[63] M Al Fahdi, NL Clarke, and SM Furnell. Towards an automated forensic examiner (AFE) based upon criminal profiling & artificial intelligence. In *Proc. 11th Australian Digital Forensics Conference*. SRI Security Research Institute, Edith Cowan University, Perth, Western Australia, 2013. doi: 10.4225/75/57b3be61fb866.

[64] Henry Swofford and Christophe Champod. Implementation of algorithms in pattern & impression evidence: A responsible and practical roadmap. *Forensic Science International: Synergy*, 3:100142, 2021. ISSN 2589-871X. doi: 10.1016/j.fsisyn.2021.100142.

[65] Thomas B. Sheridan. *Telerobotics, Automation, and Human Supervisory Control*. MIT Press, 1992. ISBN 9780262193160. URL https://books.google.ch/books?id=eu41_M2Do9oC.

Appendix A. Practitioner interview question

The following questions served as input for our semi-structured interviews with the 3 practitioners:

- What does automation mean for you?
- What do you think of our working definition?
- Can you think of a procedure that qualifies as automated?
- Can you think of a repetitive task?
- Do you think it can be automated?
- Can you think of a process/procedure that cannot be automated?
- Did you have to automate a process? How did it go?
- Can you think of requirements that a process must fulfill in order to be automatable?
- If you could pick any process that would suddenly be automated (no limit), what would it be?
- Did you share the tool you created in order to automate a process?

Appendix B. Levels of Automation (LoA)

In non-forensic fields, those levels have already been introduced to better describe automation. A common model was proposed by Sheridan and Verplank [42] based on 10 LoA in man-computer decision-making. This work has frequently served as a baseline for other researchers who have adopted it to their needs. For instance, Sheridan [65] made minor modifications to the 10 levels resulting in a slightly more general description listed in Table B.2. Note that each new level carries with it additional capabilities and opportunities for machine error which is not discussed nor considered in these LoA. Each precludes human intervention to a greater extent [65, p357].

1	The computer offers no assistance, human must take all decisions and actio
2	The computer offers a complete set of decisions/action alternatives, or
3	narrows the selection down to a few, or
4	suggests one alternative, and
5	executes that suggestion if the human approves, or
6	allows the human a restricted veto time before automatic execution
7	executes automatically, then necessarily informs the human, and
8	informs the human only if asked, or
9	informs the human only if it, the computer, decides to.
10	The computer decides everything, acts autonomously, ignores the human

Table B.2: Levels of Automation from low (1) to high (10) proposed by [65, p.358]. Describes the distribution of tasks but does say nothing about the consequences.

Acknowledgments

We like to thank Felix Freiling and Eoghan Casey for their feedback and comments that greatly improved the manuscript. We would also like to thank the interviewees who made themselves available for the interview as well as for follow-up questions. Lastly, we thank the reviewers who provided excellent feedback and helped to improve this article.

Declaration of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Gaëtan Michelet: Conceptualization, Methodology, Investigation, Writing - Original Draft, Writing - Review & Editing, Visualization

Frank Breitinger: Conceptualization, Methodology, Investigation, Writing - Original Draft, Writing - Review & Editing, Supervision

Graeme Horseman: Conceptualization, Writing - Review & Editing

- Defining automation for digital forensic science
- Highlighting considerations to achieve a common understanding
- Presenting thoughts of automation from a practitioner's perspective (3 interviews)
- Summarizing existing concepts to enhance automation