Towards an Open-source Digital Investigation Platform

Simon Cardoso, Hugo Jean, Martin Cherrier, Adrien Dubettier, Tanguy Gernot, Emmanuel Giguet, Christophe Rosenberger

Towards an Open-source Digital Investigation Platform

Simon Cardoso, Hugo Jean, Martin Cherrier, Adrien Dubettier,
Tanguy Gernot, Emmanuel Giguet, Christophe Rosenberger
Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
firstname.surname@unicaen.fr

***Abstract*—Humans generate lots of data in the cyberworlds by their behaviors on social networks, interactions with computers or smartphones (writing documents, capturing images,...). Analyzing digital traces from Internet, hard drives or computers is an important issue considering the amount of data to process and the associated applications (criminal investigation, recruitment,...). In this paper, we propose an open-source software platform for such a task. It embeds many high-level evaluated tools. These tools rely on recent advances in artificial intelligence and deep learning. Our goal is to facilitate digital investigations conducted by criminal experts, researchers in digital archives, or IT engineers. This platform embeds many tools designed to process a document in order to extract some knowledge (as for example, determining if the filetype has been corrupted). We illustrate its benefit through the analysis of a real memory dump from a hard drive.**

***Index Terms*—Digital investigation, machine learning, software platform, benchmarking, artificial intelligence.**

I. Introduction

Digital forensics aims to support the finding of evidence from digital media like a computer, a mobile phone, a server or a network [13], [17], [19], [28]. Analyzing digital traces has many legal applications such as crime resolution or finding a missing person. It also finds applications in Art and Cultural Heritage where digital devices may contain material and traces related to the authors, their work, creation process, or correspondence. The discipline includes computer forensics, mobile device forensics, network forensics, forensic data analysis and database forensics. In this paper, we focus on computer forensics whose aim is to analyze material and traces in a computer to find digital evidence [16], [25].

Most digital investigations are conducted by experts appointed by the court or from police forces. Analyzing terabytes of data from a mass storage is not possible without any software in a short period of time: some digital investigations need to be achieved in less than 48 hours when the suspect was arrested and put in custody. To conduct examinations, a digital forensic expert has to choose software technologies from two distinct worlds [14], [20], [30]. Commercial off-the-shelf (COTS) softwares propose ready-to-use and well-integrated functionalities but are in general expensive since they include maintenance, support, and documentation. They may also lack of transparency, independence or impartiality in the evaluation of their tools. Because of their price, experts can only afford to buy a few of them. This is why rigorous independent evaluations of these commercial tools are necessary to assess their performance and make an informed choice [21], [24]. Free and Open-Source Software are also a possibility but are not always documented and the efficiency is often questionable [1], [2], [22]. Even if these tools are free, an informed choice must be made due to the limited time and resources of the investigation.

One of the objectives of Digital Forensic Science is to contribute to the professionalization of Digital Forensics by providing objective and independent evaluation protocols in order to lead to reproducible results. This aim leads to define evaluation protocols, with explicit guidelines, clear evaluation metrics, and dedicated datasets.

In this paper, we introduce a new open-source digital investigation platform. One key issue here is to benchmark all integrated tools through a rigorous protocol. Considering the legal consequences, we believe this is crucial to evaluate the performance of the tools, in terms of efficiency and computation time. A platform that implements a precise, similar, and quick evaluation process for different tools facilitates the evaluation work under controlled conditions and helps prioritize which tools to use. We also show that recent advances in deep learning [14], [27], [29] allow developing efficient tools for digital investigations. We intend to distribute freely the proposed platform under a partnership agreement. We believe it could be useful for many applications such as criminal investigation, research in privacy or culture heritage analysis.

The main contributions of this work are :

- a comparison of existing digital investigation platforms,
- the design of a software platform allowing using many tools under the same conditions. Note that all tools in the platform have been benchmarked rigorously,
- the presentation of a practical case with this platform using an experimental protocol and highlighting the need for an open, generic, efficient platform that can be used by all.

The paper is organized as follows. In section II, we present the main forensic toolkits and platforms in the literature. Section

III describes the proposed digital investigation platform. We detail its functionalities and its operational use. In section IV, we illustrate the benefit of the proposed platform for the operational investigation of a real hard drive. We conclude and give some perspectives in section V.

II. State-of-the-art

Computer forensics has for objective the analysis of digital traces among:

- Email correspondence;
- Deleted files and folders;
- Emails and messages;
- Social media communication;
- Software history;
- Internet activity and history;
- Analysis and reporting of documents.

A. Existing tools

Considering all these tasks, an expert has to use software to make an automatic analysis. According to [9], [23], we can mention the following forensic toolkits and platforms as the most popular ones, also resumed in Table I, sorted from oldest to newest:

- **X-Ways Forensics** [3] is a commercial disk analysis integrated environment with key features such as complete access to disks, file carving, image and email analysis, event list based on all kinds of timestamps. Concerning the fight against child pornography, it provides an interface to PhotoDNA which can recognize known pictures and it allows investigators to use a skin color detection module to sort the gallery view. This tool also allows analyzing RAM memory dump from windows. Figure 1 shows the graphical user interface of X-Ways Forensics.

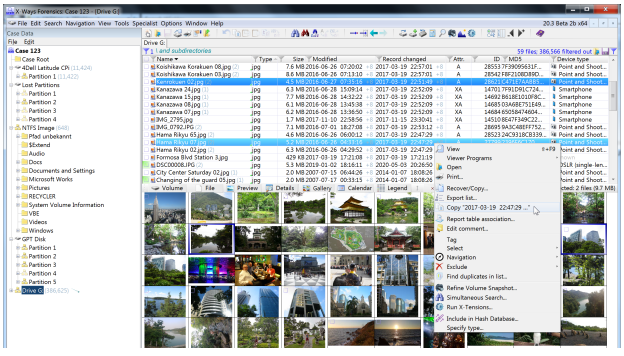

Fig. 1. X-Ways Forensics interface

- **ProDiscover Forensics** [4] is a commercial and comprehensive digital forensics software with different embedded tools (memory forensics, Preview and Image Disks,...). It allows full-text search with multilingual capabilities. Figure 2 shows the graphical user interface of ProDiscover.
- **SANS Investigative Forensic Toolkit (SIFT)** [5] is proposed as a Linux operating system and it includes most tools required for digital forensics analysis.

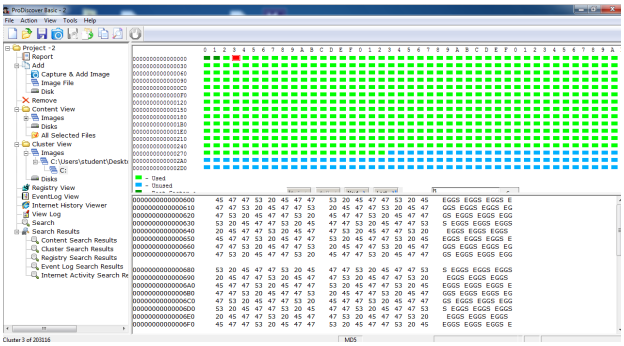

Fig. 2. ProDiscover Forensics interface

- **Forensic Toolkit (FTK)** [2] is a commercial disk analysis platform that creates full-disk forensic images and processes a wide range of data types from many sources, from hard drive data to mobile devices, network data and the Internet. It includes AI algorithms to automatically flag people, weapons, drugs, and to detect explicit content of CSAM (Child Sexual Abuse Material) in images and videos. It can aggregate the results of filters to display them as a timeline. Figure 3 shows the graphical user interface of Forensic Toolkit.

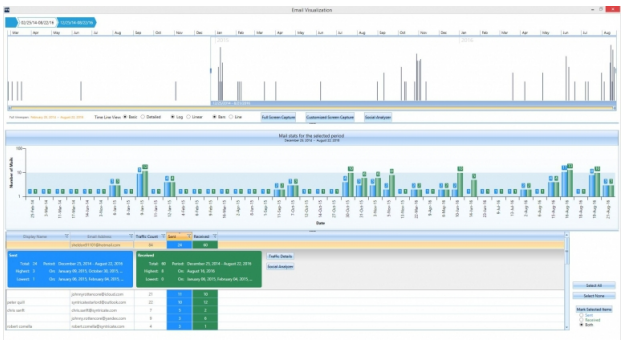

Fig. 3. Forensic Toolkit interface

- **Volatility Framework** [6] is open source memory forensics framework and written in Python and focus mainly on volatile memory forensics (i.e., RAM forensics). RAM analysis is important especially for qualifying malware or recovering passwords like those of open Truecrypt containers. Volatility only allows memory dump analysis: it is necessary to have another tool like *vmss2core* to perform the memory dump. This framework is used on the command line, and it is often necessary for the expert to create himself the memory profile corresponding to the dump and allowing its analysis. Thus, this tool is not easy to learn quickly.
- **Computer-Aided Investigative Environment (CAINE)** [7] is a Linux Live CD for forensic investigation based on Ubuntu. It is a Linux operating system like SIFT, but it is designed to be booted directly on the machine to be investigated. It offers a complete forensic environment

TABLE I
FUNCTIONALITIES OF THE MAIN FORENSIC TOOLS IN THE LITERATURE.

Software	Year	Functionnalities	Licence	Type
X-Ways Forensics [3]	2000	Disk cloning and imaging, access to logical memory of running processes, data interpreter.	commercial	platform
ProDiscover Forensics [4]	2001	Full Text Search with Multilingual, cloud forensics, social media artifacts, Web and Email Artifacts, Extensive Automation and Scripting, automatic report generation, integrated AI and ML tools for image and video analytics.	commercial	platform
SIFT [5]	2007	Forensic tools for file systems, memory and network investigations to perform in-depth forensic investigations.	open-source	OS
Forensic Toolkit (FTK) [2]	2007	Full-disk forensic images, process data types, decrypt files, crack passwords, reports generation.	commercial	platform
Volatility Framework [6]	2007	Volatile storage (RAM) analysis.	open-source	tool
CAINE [7]	2008	Interoperable environment that supports the digital investigator, a user friendly graphical interface, a semi-automated compilation of reports.	open-source	OS
Cellebrite Inspector [11]	2011	AI media categorization, Optical character Recognition, data searching, data filtering, encryption support, registry artifacts.	commercial	platform
Magnet Axiom [8]	2011	Memory and mobile dump analysis, multimedia analysis (nudity), Web and Email Artifacts, collaborative investigation, report generation.	commercial	platform
The Sleuth Kit (+Autopsy) [1]	2012	Timeline Analysis, viewing interface, Hash Filtering, Keyword Search, Web Artifacts, Data Carving, Multimedia, Indicators of Compromise.	open-source	tool
Oxygen Forensic Detective [12]	2013	Retrieve mail and web authentication tokens. Extract data from screen locked phones and mobile applications.	commercial	platform
OpenText EnCase [26]	2015	Extracts text evidence buried in PDFs, images and scanned documents, image identification of particular interest, filtetype identification.	commercial	platform

that is organized to integrate new software tools with a friendly graphical interface as shown in Figure 4.

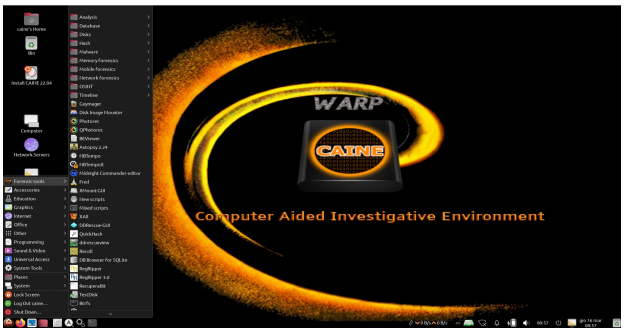

Fig. 4. CAINE interface

- **Cellebrite Inspector (ex blacklight)** [11] is a commercial software from Cellebrite, a huge Israeli digital intelligence company. The software can analyze large volumes of data by applying various filters. In particular, the expert can classify images and videos by AI, inspect the websites visited, and retrieve recent USB connections. Figure 5 represents Cellebrite Inspector's GUI.
- **Magnet Axiom** [8] is able to recover data from smartphones, computers, or stored in the cloud and provides the functionality to examine evidence across all these sources in a single case. In addition to traditional disk analysis functionalities, it includes content-based image retrieval (CBIR) to find similar images, such as pictures of the same room or pictures with similar scenery. Magnet AI provides explicit and CSAM content detection.

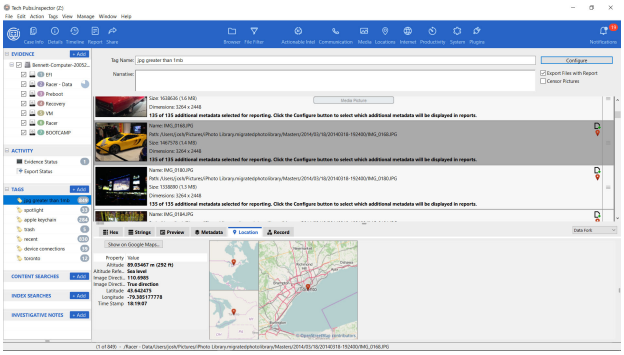

Fig. 5. Cellebrite Inspector interface

- **The Sleuth Kit (+Autopsy)** [1] is a set of command tools in order to check the disk image and recovering any lost files from them. The plug-in built in this framework makes it possible to incorporate new modules to build some automated scripts to get the result without any manual intervention. Autopsy allows using the Sleuth kit with a graphical interface shown in Figure 6.
- **Oxygen Forensic Detective** [12]: This platform is particularly well known for its ability to retrieve email and web authentication tokens. It also allows extracting data from screen locked phones but also from many mobile applications. Like many other tools, it allows the acquisition of data, then their filtering and aggregation in the form of a report. Figure 7 represents Oxygen Forensic

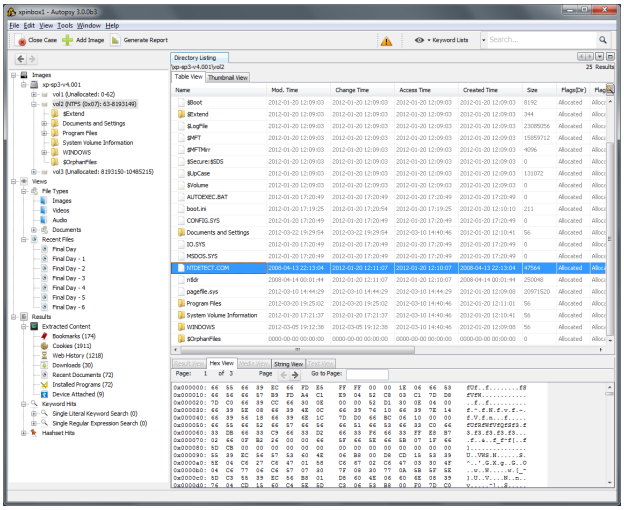

Fig. 6. Autopsy interface

Detective's GUI.

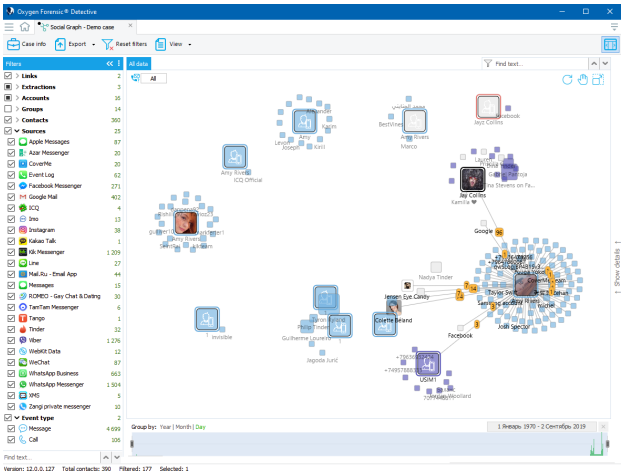

Fig. 7. Oxygen Forensic Detective interface

- **Opentext EnCase** [10]: it is a commercial software for digital forensics. It is complete and some tools can be customized. The company offers certifications for experts using this platform. The *.E01* file's extension, Encase Image File Format, is widely used as a disk image format and is supported in most forensic tools. Figure 8 represents EnCase's GUI.

B. Discussion

All these forensic tools are useful and many experts use them. For an expert, multiple criteria are important to make a choice between one or multiple tools. We list the five main expectations:

- Completeness: Even if existing tools could be complementary, it is better for an expert to use a single software for cost and training reasons. Thus, a tool must be efficient for different types of storage (persistent or not), for different operating systems (windows, Linux, Mac, android, iOS), with various technical constraints (formatting, visual access control, encryption, ...);
- Performance: It is difficult to estimate the performance of existing tools (computation time and efficiency). With experience, it is possible to have a judgment but forensics needs a scientific analysis to quantify objectively their relative performance. Thus, a scalable platform allowing the evaluation of many tools under similar conditions will allow such an evaluation;
- Usability: A forensic tool should be easy to use. For example, police officers are not necessarily trained to use command line tools. The tools must strike a balance between the advanced complexity of the proposed features and ease of use;
- Availability: An expert should be able to access to the tool. Of course, the cost of commercial solutions could be a barrier to use them. Moreover, the technical constraints of platform execution (RAM, graphics card, ...) must be accessible;
- Modularity: Once an expert has learned how to use a platform, they want to be able to stay on it when new innovative tools are released. Thus, the platform should be scalable and easily upgradeable by adding new external tools in the form of generic adaptive blocks.

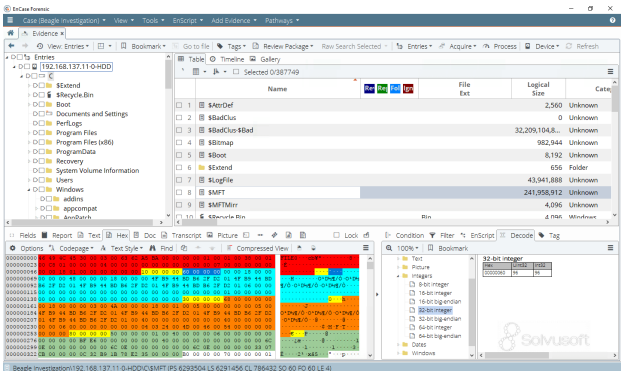

Fig. 8. EnCase interface

Table II presents our subjective evaluation of existing software. Commercial solutions offer a complete list of tools that a priori efficient (quantitative evaluation is not provided) but at quite a high cost (between 2K$ and 4K$) for an independent expert. However, these are all-in-one platforms that have made an effort to be accessible with a comfortable graphical interface. The proprietary code of these solutions is a barrier to their modularity. Open-source solutions offer specific tools or operating systems. Accessibility is less accomplished than commercial solutions, either because the use is made in the command line, or because it is necessary to use many specific graphic tools. As for example, the volatility framework is an open-source solution but dedicated for RAM analysis. SIFT, Autopsy and CAINE are composed of many free tools that are useful for a forensic expert. Nevertheless,

these tools are generally very modular and adaptable.

One of the main question remains, how efficient are these tools? We believe that it is necessary to benchmark forensic tools with a rigorous protocol by researchers. It would enhance at the same time the trust on forensic tools and their operational spread. With the quick evolution of artificial intelligence, many new tools can be defined and used for forensic applications. We can cite works on image geolocation based on its content [18], camera model identification [15]...We proposed in the next section our vision for an open-source forensic platform.

III. Proposed Methodology

We present in this section, the proposed methodology for digital forensics with the open-source platform we are developing. We intend to consider different types of digital traces among network packets, hard disks, Internet... In this paper, we focus particularly on hard drive analysis.

A. Disk image generation

Before analyzing the digital content of hard drives, we need to capture disk images. In our lab, we use a Forensic Recovery of Evidence Device (FRED) that allows us to securely image multiple drives simultaneously (with writing block). Figure 9 is an illustration of the device we use. We then use some scripts from the Sleuth Kit platform in order to generate two-disk images (files present in the hard drive and suppressed ones). At the moment, this part is not included in the proposed platform (we need to launch commands) but will be added very soon.

Fig. 9. Capture of memory dumps from hard drives.

We designed a software platform for digital investigation purposes (see Figure 10). This platform allows processing data from any sources (device, computer, hard drive, file directory ...). This platform has been developed in order to propose at the same time a public access (teaching, demonstrating tools,...) and a private one allowing a local analysis of operational data (criminal investigation, privacy analysis). Indeed, the main objectives of this platform are 1) to benchmark tools for digital investigation, 2) to provide a software tool for teaching digital investigation and 3) to propose an operational and open-source tool for investigators on real data.

A software core applies any tool/filter to all files present in the data source. The results are stored in a database that can be processed by the graphical user interface. Statistics about the dataset, represented by diagrams, and evaluation results can be visualized by the user.

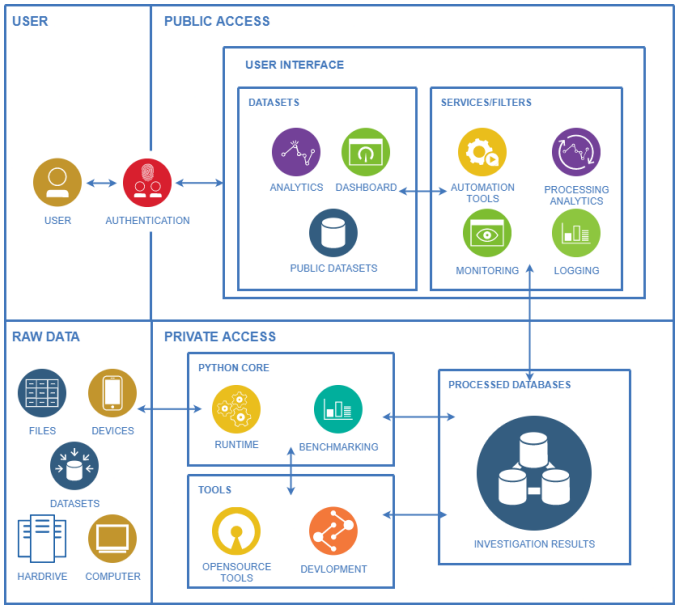

Fig. 10. Proposed digital investigation platform.

1) Benchmarking filters: Analyzing a hard drive consists in applying tools or filters to identify specific documents (like child pornography images). Figure 11 shows the different steps for benchmarking an investigation tool in our methodology. For this kind of activity, a reliable ground truth is necessary. A mapping function is necessary because the outputs of all tested tools are not necessarily the same. All benchmarking results are saved in the evaluation database. We applied this process all tested tools/filters by using a ground truth dataset and performance metrics. This allows us to embed only qualified tools in the software platform.

2) Implementation: The proposed architecture is based on the widespread concept of a front-end and back-end API system. The front-end handles all user interactions with the interface. It also serves all the analysis proposed by the application programming interface (API). The front-end is built around the Vue framework which enables a single page system when loading does not require page changes. The front-end communicates with the back-end API which acts as server-side logic and calculation. The back-end is implemented in Python with a RethinkDB database. Python allows us to serve seamlessly all the machine learning (ML) models as API

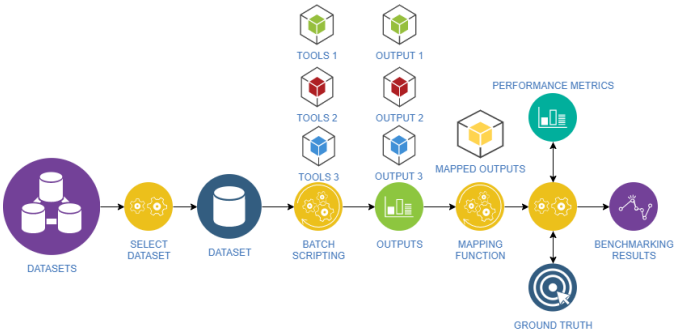

Fig. 11. Different processes for benchmarking investigation tools on datasets with ground truth.

endpoints, we also use Flask as server framework. Flask is also implemented in Python which allows easy manipulation of data without having to use bridges. The use of Python allows easy additions of features as a Python module increasing both the scalability and the genericity of the platform. RethinkDB is an open-source NoSQL JSON-document database, it allows schema-less storage. It is useful for our application where data is evolving as the user would not use the same filters all the time. The proposed software platform handles calculations as a set of tasks, our task scheduler Celery offers the ability to run tasks without having to wait for those. It uses Redis a key-value database for fast storage. The back-end (with the API) is containerized in a Docker, allowing fast deployment and easy network configuration within the container.

3) Graphical User Interface: The user interface allows two main usages. The first one consists in creating an investigation. This feature allows the user to choose a dataset (from a disk image) to analyze. The creation of a dataset gives the user a number of choices to suit the time required for processing. The interface permits the user to choose the folders and subfolders to be processed, as well as the filters to be applied (see Figure 14). The second mode is the file triage. The user can analyze a dataset that has already been processed (tools/filters have been applied to the dataset). It also has visualization features to highlight elements that might be important. Finally, it is possible to browse the dataset using the icon representing the file. Many graphical widgets allow a visual inspection of the disk content. As for example, it is possible, through the FileInfo tool, to see the proportion of each file category (images, text...) and to click on one category to filter the disk content (see Figure 13).

IV. Validation

We show in the next section some results when analyzing a real hard drive with the proposed platform.

A. Hard disk analysis

As an illustration, we analyzed the content of a hard disk that can be seen in Figure 9. Once the disk image has been created, we can use the proposed platform by selecting tools/filters to be applied on all files (see Figure 14). When the processing is done, the TethinkDB database is completed and the GUI allows the expert to analyze the content of the disk drive. We show in Figure 16 an illustration of tools/filters applications. Timelines provide information on the date of file creation. A cloud of words allows visualizing in a convenient way the content of text files in the selected sub-dataset (depending on the selection of files). We also can show the geolocation of images by taking into account metadata in images (EXIF) or by applying a deep learning model to estimate it from the image content such as [18]. Figure **??** presents as illustration some results when applying different filters (face detection, outdoor images, humans in images) in the selected hard drive.

B. Qualitative comparison with the literature

We made in this section a brief subjective evaluation of existing tools considering the criteria we listed in section II b). We believe the proposed platform is a very good contribution and we hope many researchers and engineers will participate to its development.

V. Conclusion and Perspectives

In this paper, we introduce an open digital investigation platform. Its objective is to propose efficient and qualified tools for experts in digital forensics (operational use, teaching,...). The proposed platform can be very easily deployed thanks to the use of Docker. We can add any high-level filters in a very convenient way. We are working as for example on video filters (explicit content and deep detection).

As perspectives of this work, we intend to add more tools and start to share it to the scientific community in 2024 with an agreement (to be sure it would be only used by experts). We also plan to build a serious game in digital forensics to disseminate the benefit of AI tools for digital forensics. We will be able to realize a demonstration at the conference.

References

[1] https://www.sleuthkit.org/.
[2] https://www.exterro.com/forensic-toolkit.
[3] https://www.x-ways.net/.
[4] https://www.prodiscover.com/prodiscover-forensics.php.
[5] https://www.sans.org/tools/sift-workstation/.
[6] https://www.volatilityfoundation.org/.
[7] https://www.caine-live.net/.
[8] https://www.magnetforensics.com/products/magnet-axiom/.
[9] https://www.educba.com/forensic-tools/.
[10] https://security.opentext.com/encase-forensic.
[11] Cellebrite inspector — analyze windows and mac computer data volumes.
[12] Oxygen forensic detective: an all-in-one digital forensic software.
[13] Mohammed I Alghamdi. Digital forensics in cyber security—recent trends, threats, and opportunities. *Cybersecurity Threats with New Perspectives*, 2021.
[14] Humaira Arshad, Aman Bin Jantan, and Oludare Isaac Abiodun. Digital forensics: review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, 14(2):346–376, 2018.
[15] Guru Swaroop Bennabhaktula, Enrique Alegre, Dimka Karastoyanova, and George Azzopardi. Camera model identification based on forensic traces extracted from homogeneous patches. *Expert Systems with Applications*, 206:117769, 2022.

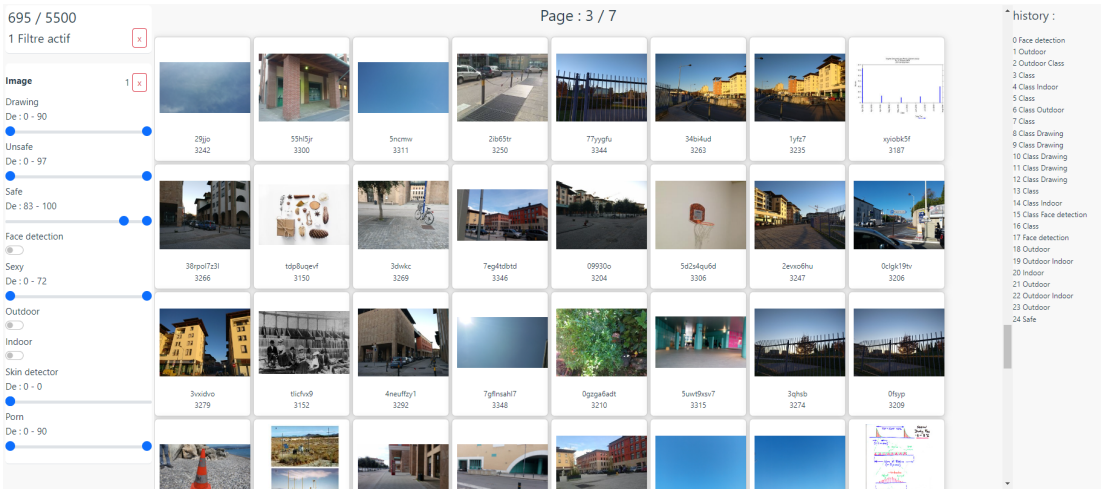

Fig. 12. Platform graphical user interface: (left side), active and available tools/filters, (center) file thumbnail, (right side) filters history.

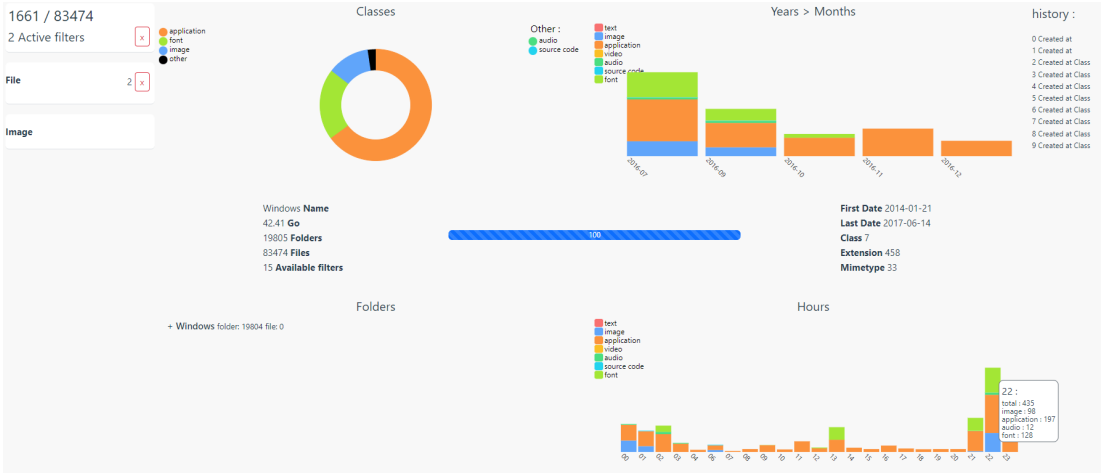

Fig. 13. Graphical visualization of an investigation.

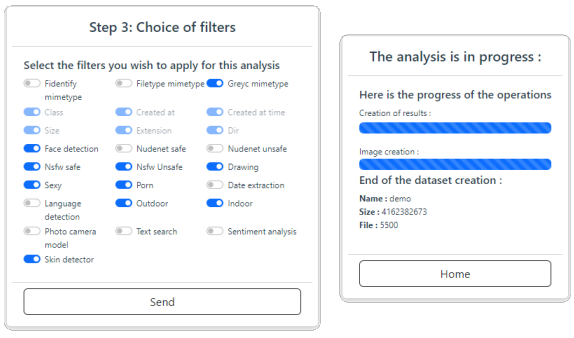

Fig. 14. Illustrations from the different steps for the analysis of a disk image.

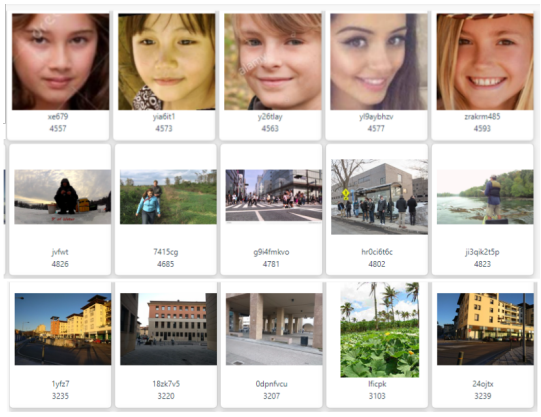

Fig. 15. Illustrations of filters results: (first row) face detection, (second row) outdoor images with humans, (last row) outdoor images.

[16] Shobha Bhatt, Geetanjali Garg, et al. Comparative analysis of acquisition methods in digital forensics. In *2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, pages 129–134. IEEE, 2021.

[17] Krupa Bhavsar, Ajay Patel, and Satyen Parikh. Approaches to digital forensics in the age of big data. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 449–453. IEEE, 2022.

[18] Patricia Callejo, Marco Gramaglia, Ruben Cuevas, and Angel Cuevas. A deep dive into the accuracy of ip geolocation databases and its impact

TABLE II
QUALITATIVE COMPARISON OF THE PROPOSED PLATFORM WITH EXISTING ONES.

Software	Completeness	Performance	Usability	Availability	Modularity
SIFT [5]	⋆⋆⋆	⋆⋆⋆	⋆⋆	⋆⋆⋆	⋆⋆⋆
ProDiscover Forensics [4]	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆	⋆
Volatility Framework [6]	⋆	⋆⋆⋆	⋆	⋆⋆⋆	⋆⋆⋆
X-Ways Forensics [3]	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆	⋆
Magnet Axiom [8]	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆	⋆
CAINE [7]	⋆⋆⋆	⋆⋆⋆	⋆⋆	⋆⋆⋆	⋆⋆⋆
Forensic Toolkit (FTK) [2]	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆	⋆
OpenText EnCase [26]	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆	⋆
The Sleuth Kit (+Autopsy) [1]	⋆⋆	⋆⋆⋆	⋆⋆	⋆⋆⋆	⋆⋆⋆
Contribution	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆

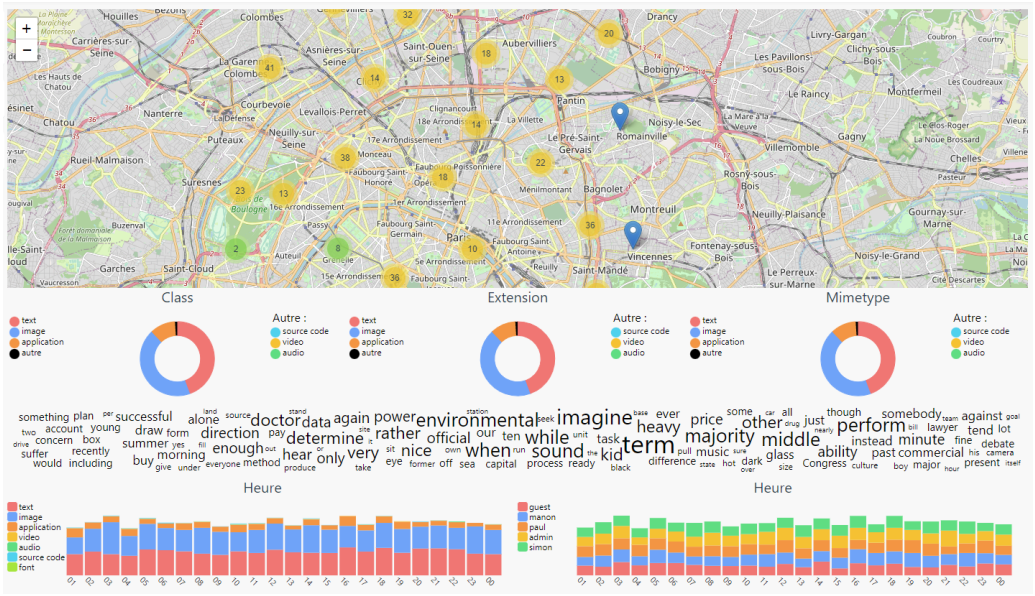

Fig. 16. Example of visualization tools during a digital investigation.

on online advertising. *IEEE Transactions on Mobile Computing*, 2022.

[19] Nitul Dutta, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, Emil Pricop, Nitul Dutta, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, and Emil Pricop. Introduction to digital forensics. *Cyber Security: Issues and Current Trends*, pages 71–100, 2022.

[20] Vihara Fernando. Cyber forensics tools: A review on mechanism and emerging challenges. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–7. IEEE, 2021.

[21] Alicia Francois and Alastair Nisbet. Forensic analysis and data recovery from water-submerged hard drives. *International Journal of Electronic Security and Digital Forensics*, 13(2):219–231, 2021.

[22] Christophe Grenier. Fidentify: Determine file type using photorec database, 2019.

[23] Abdul Rehman Javed, Waqas Ahmed, Mamoun Alazab, Zunera Jalil, Kashif Kifayat, and Thippa Reddy Gadekallu. A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, 10:11065–11089, 2022.

[24] Mayank Lovanshi and Pratosh Bansal. Comparative study of digital forensic tools. *Data, Engineering and Applications: Volume 2*, pages 195–204, 2019.

[25] Anita Patil, Soumi Banerjee, Dipti Jadhav, and Gautam Borkar. Roadmap of digital forensics investigation process with discovery of tools. *Cyber Security and Digital Forensics*, pages 241–269, 2022.

[26] Guidance Software Shawn H. McCreight, 1998.

[27] Ajay Shrestha and Ausif Mahmood. Review of deep learning algorithms and architectures. *IEEE access*, 7:53040–53065, 2019.

[28] Eric R Ramirez Thompson. Introduction to digital forensics. *Computers & Criminal Justice*, 2021.

[29] Athanasios Voulodimos, Nikolaos Doulamis, Anastasios Doulamis, and Eftychios Protopapadakis. Deep learning for computer vision: A brief review. *Computational intelligence and neuroscience*, 2018, 2018.

[30] Tina Wu, Frank Breitinger, and Stephen O'Shaughnessy. Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation*, 34:300999, 2020.