DigForASP: A European Cooperation Network for Logic-based AI in Digital Forensics

Stefania Costantini[1], Francesca A. Lisi[2], and Raffaele Olivieri[1]

[1] Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica
Università degli Studi dell'Aquila, Italy
Stefania.Costantini@univaq.it,Raffaele.Olivieri@gmail.com
[2] Dipartimento di Informatica &
Centro Interdipartimentale di Logica e Applicazioni (CILA)
Università degli Studi di Bari "Aldo Moro", Italy
FrancescaAlessandra.Lisi@uniba.it

Abstract. This short paper briefly describes DigForASP, a COST Action that aims to create a cooperation network for exploring the potential of the application of logic-based Artificial Intelligence in the Digital Forensics field, and to foster synergies between these fields. Specifically, the challenge is to address the Evidence Analysis phase, where evidence about possible crimes and crimes perpetrators collected from various electronic devices (by means of specialized software, and according to specific regulations) must be exploited so as to reconstruct possible events, event sequences and scenarios related to a crime. Evidence Analysis results are then made available to law enforcement, investigators, public prosecutors, lawyers and judges: it is therefore crucial that the adopted techniques guarantee reliability and verifiability, and that their result can be explained to the human actors.

Keywords: Computational Logic · Digital Forensics · Artificial Intelligence.

1 Introduction

An investigation consists, in general terms, in a series of actions and initiatives implemented by the investigators (law enforcement and judges) in order to ascertain the "*truth*" and acquire all possible information and data about a perpetrated crime and related facts with their logical implications. A large number of subjects are involved in this process, where they help to pursue a criminal activity, which could still be in progress. In an accurate vision, and according to the Italian Code of Criminal Procedure, investigations can be defined as "the set of activities carried out by the *officers* and *agents* of the *criminal police*". An investigation has, overall, the aim of establishing the existence of a crime and the consequences that it has determined (generic proof or "*de delicto*"), and identifying the criminals (specific proof or "*de reo*").

These activities start from the act of acquisition of the crime notice or from the analysis of a crime scene. Through a series of initiatives and actions, the investigation allows the collection of data and elements which, according to certain deductive logical reasoning, should lead to draw conclusions. Investigative cases are usually complex, and involve a number of factors that need to be taken into account. Most of the collected data are nowadays obtained through digital devices and platforms either seized from the suspects, or available on the Internet or shared by telecommunication companies.

Digital Forensics (DF) is a branch of criminalistics which in fact deals with the identification, acquisition, preservation, analysis and presentation of the information content of computer systems, or in general of digital devices. In particular, the phase of *Evidence Analysis* involves examining and aggregating evidence about possible crimes and crime perpetrators collected from various electronic devices (by means of specialized software, and according to specific regulations). This in order to reconstruct events, event sequences and scenarios related to a crime. Evidence Analysis results are made available to law enforcement, investigators, intelligence agencies, public prosecutors, lawyers and judges.

The COST Action DigForASP aims at creating a research infrastructure for the application of *Artificial Intelligence* (AI), together with other complementary areas, in the field of Digital Forensics. DigForASP constitutes a timely challenge for both areas: DF and AI. From the AI perspective, the proposed research infrastructure will foster the development of new theoretical results, methods and techniques that will contribute in the long term to the development of new software tools that will rely on a complex combination of concepts and results from different areas of *Knowledge Representation* (KR) and *Automated Reasoning* (AR) such as diagnosis, causal explanation, temporal reasoning about actions, epistemic reasoning, the treatment of incomplete knowledge, deontic and legal reasoning, inductive learning and formal concept analysis, which will be complemented by other ones needed for the purpose of the Action. At the same time, the application of (intelligent) automated tools to DF - capable of reliable and exhaustive exploration of evidence, and with a level of analysis that goes beyond the scope of human observation and in time - will constitute a breakthrough that will have a direct impact on the practical investigation of crime scenarios.

To meet the challenge, the Action has built a Network composed of researchers and engineers from the AI field together with DF experts belonging to Government Institutions and NGOs alongside scholars from the field of Information and Communication Technologies (ICT) and Law as well as social scientists, criminologists and philosophers (the latter for the ethical issues). The Network is carrying out a set of activities and building resources to promote interaction, exchange and cooperation between these different areas. It is enabling computer scientists to understand the main issues and open problems of Digital Forensics, especially Evidence Analysis, and it is helping to promote the exploitation of AI for addressing in an innovative, effective and adaptive way the key problems in this domain. Network partners is thus being able to identify KR&AR techniques which can be applied to Evidence Analysis, and to suggest guidelines for cre-

ating and developing suitable new techniques and methods aimed at advancing the state of the art in both DF and AI, strengthening European research and innovation capability in these areas. The long-term objective of the Network is to increase know-how and competences, so as to devise and to implement concrete projects and tools to be applied by Police Scientific Investigation Departments in solving real cases in COST Member Countries, COST Near Neighbour Countries (NNCs) and COST International Partner Countries (IPCs). This also by promoting coherent and effective cooperation with third countries.

The paper is organized as follows: In Section 2 we illustrate in some detail what is Digital Forensics, and which is the state of the art in the application of automated tools in this field. In Sections 3-4 we illustrate the progress that the DigForASP Action proposes over the state of the art, and the innovative aspects. In Section 5 we discuss the expected impact of the Action. In Section 6 we discuss the preliminary results achieved, and we conclude by discussing some future perspectives.

2 Digital Forensics: Overview and State of the art

Digital Forensics is a complex and rapidly evolving field, where methods for collecting evidence are varied, rapidly evolving and becoming increasingly sophisticated. In fact, such methods must continuously adapt to the evolution of technology. The aim is to identify digital sources of evidence, and to organize such evidence in order to make it robust in view of its discussion in court, either in civil or penal trials. DF is concerned with the analysis of possible sources of evidence after a crime has been committed.

Clearly, the development of DF is highly related to the development of ICTs in the last decades, and to the widespread diffusion of electronic devices and infrastructures. It involves various disciplines such as computer science, electronic engineering, various branches of law, investigation techniques and criminological sciences. Organizational aspects are also relevant and DF investigation involves, in general, several experts working with sophisticated instruments and software, with limited resources and tight timing. DF is divided into sub-fields according to the kind of data analyzed, including those extracted from the Internet.

The DF process involves the following *phases*:

1. Identification, i.e. retrieving, via suitable forms of investigation, devices that may possibly contain digital data useful to the identification of a potential crime perpetrator, or anyway useful to help the investigators in their activities.
2. Acquisition, i.e., retrieving evidence in the form of data collected either from storage devices or from network interception.
3. Preservation, where collected evidence is be stored and preserved (according to specific precise regulations) so as to guarantee integrity and authenticity.
4. Evidence Analysis, where the evidence collected is examined and aggregated to determine the existence of possible sources of proof that can be useful to law enforcement, investigators, public prosecutor, lawyers and judges in

various phases of trial. It involves examining fragmented, incomplete knowledge, and aggregating evidence items into complex scenarios possibly involving time, uncertainty, causality and alternative possibilities. Currently, no single established procedure exists for Evidence Analysis, which is usually performed by Scientific Investigation experts on the basis of their experience and intuition.
5. Presentation, where sources of evidence identified by means of Evidence Analysis are formalized in official documents.

Phases 1-3 are supported by a number of hardware and software tools, the latter being both proprietary and open source. These tools are continuously evolving to follow the evolution of the involved technologies and devices, and recently related procedures have been standardized in all communities. However, they do not require advanced reasoning capabilities. Phase 4, Evidence Analysis, is where the main thrust of the Action will lie. This phase requires advanced reasoning capabilities that are not currently supported by available devices and software. In fact, these are limited to data recovery (and data recognition) and to providing metadata (size, dates of creation/modification/elimination, etc.). Therefore, such retrieved data must be analysed by human experts, possibly with the support of available automated tools. However such tools, apart from text analysis, header files analysis and mining software packages, operate as a black box (i.e., they provide results without motivation or explanation), and for verification of the results one needs to perform a secondary analysis.

3 DigForASP: Progress beyond the State of the Art

Evidence Analysis involves examining fragmented incomplete knowledge, and aggregation of evidence items into complex scenarios possibly involving time, uncertainty, causality and alternative possibilities. Currently, no single established procedure exists for Evidence Analysis, which is usually performed by Scientific Investigation experts on the basis of their experience and intuition. The network is therefore focused on promoting formal and verifiable AI methods and techniques for Evidence Analysis that aim at the elicitation of sources of evidence. Relevant aspects to consider include:

- Timing of events and actions;
- Possible causal correlations;
- Contexts in which suspicious actions occurred;
- Skills of the involved suspects;
- Awareness of the involved suspects of committing a violation or a crime and of the degree of severity of the violation/crime.

Moreover, given available evidence, several possible underlying scenarios may exist that should be identified, examined and evaluated.The aim of the Action is that all the above should be performed via techniques that are verifiable with respect to the results they provide, how such results are generated, and

how the results can be explained. Therefore, such software tools can be reliable and provide a high level of assurance, in the sense of confidence in the systems correct behaviour. Otherwise there remains an undesirable uncertainty about the outcome of these stages, and different technicians analyzing the same case can reach different conclusions which may lead to different judgements in court.

In AI, several methods and techniques have been developed over the years for uncertain, causal and temporal reasoning, and for devising and examining alternative consistent scenarios that might be compatible with a set of known facts. To the best of our knowledge, these techniques have never been applied to Digital Forensics evidence analysis. Therefore, studying their applicability for development of suitable prototypes is per se a significant advance over the state of the art. Moreover, the application to such a challenging field will foster refinements and improvements of the known methods and techniques, and development of novel ones.

Unlike the phase of crime identification or detection, where the exploration of big data and the application of Machine Learning (ML) techniques can be useful, the phase of Evidence Analysis has particular requirements that make the proposal of DigForASP based upon KR and AR a much more promising approach, potentially becoming a breakthrough in the state-of-the-art. The final goal of Evidence Analysis is the formulation of verifiable evidence that can be rationally presented in a trial. Under this perspective, the results provided by ML classifiers or other types of black box recommender systems do not have more value than human witness suspicions and cannot be used as legal evidence. Logical methods provide a broad range of proof-based reasoning functionalities that can be implemented in a declarative framework where the problem specification and the computational program are closely aligned. This has the benefit that the correctness of such declarative systems based on Computational Logic can be formally verified. Moreover, recent research has led to new methods for visualising and explaining the results of computed answers (e.g., based on argumentation schemes). So one can not only represent and solve relevant problems, but also provide tools to explain the conclusions (and their proofs) in a transparent, comprehensible and justified way.

In summary, the rationale for the choice of Computational Logic relies on the fact that, by its very nature, it is based on precise formalizations, and thus allows for the affordable verification of desired properties of the systems that will be devised in the future as a follow-up of DigForASP. Verifiability, reliability and justifiability are keys features for software tools to be applied in a field such as Digital Forensics, where the evidence produced is aimed at the reconstruction of crimes and assist/facilitate the court in the decision process to establish if an accused is innocent or guilty.

4 DigForASP: Innovative Aspects

Although AI techniques have been applied to DF for different purposes, they have mainly been exploited for data retrieval and categorization. For instance, the

analysis of image and video multimedia files by pattern recognition algorithms or the detection of anomalies in large databases such as email exchanges, network transactions, etc. are examples of such applications. These tasks benefit from intelligent techniques and in particular from ML techniques. The Action takes a step beyond as it involves the main stakeholders in order to apply KR&AR methods to retrieved data in order to elicit evidence that can be used in a trial. For instance, from data items retrieved from different sources (like, e.g., mobile devices, social network activities, cloud computing tracks, etc.), we may obtain the set of all possible patterns of activity of a suspect during the execution of a crime. AR tools can constitute a crucial advantage since the amount of data to examine and interpret is large and keeps growing with the increasing adoption of digital devices in everyday life. Thus, the Action proposes innovations in the following two directions: 1) a substantial evolution of the current paradigm of evaluation and interpretation of data in DF analysis , which might be exportable, in the future, also to other Forensic Sciences; 2) a "breakthrough innovation" for the judicial system, based on the possibility of adopting intelligent, reliable and dependable decision-support systems for the reconstruction of facts, able to take into account the wide number of elements and variables involved in complex cases, so as to aid judges in their assessments and decisions.

5 Expected Impact of DigForASP

The innovative use of methods and techniques from a well-established research fiels (AI, in particular KR and AR) to a critical field (DF, in particular Evidence Analysis) where no significant previous efforts and results on computer-based intelligent decision support exist so far before, is already a potential breeding ground for new and significant scientific and technological results. In the long-term, a challenging interdisciplinary area such as Digital Forensics will, with the help of this Action, provide a strong impetus for new developments that may result in scientific breakthoughs, publications, software prototypes and tools. From the scientific perspective, Evidence Analysis constitutes an ideal application domain for logical reasoning in AI, as it combines different classical aspects of knowledge representation and reasoning. Even the underlying orientation and goal, the search for a proof , is aligned in both areas (a formal proof vs a valid argumentation in a trial). In the short term, DF can provide the AI community with non-trivial benchmarks of automated reasoning that constitute a breakthrough with respect to available synthetic or ad hoc examples used in the scientific literature. It will act as a proof of concept to check whether different available KR techniques and tools are directly applicable or, most probably, require adjustments to take into account the domain features.

From the socio-economical perspective, the use of AR tools will become, in the long-term, a positive benefit for all the involved stakeholders. Law enforcement, investigators, intelligence agencies, criminologists, public prosecutors, lawyers and judges will be provided with decision-support-systems that can effectively support them in their activities by providing motivated suggestions. In

the short-term, the most relevant impact will be a twofold improvement both on efficiency and quality. On the one hand, investigators will work more efficiently thanks to new tools that guide them, helping with hypotheses formulation, the exhaustive application of case-based reasoning on large collections of data, and the development of proofs that can be formally checked with correct logic-based inference systems: this will save enormous effort on tasks that are currently done by hand and in most cases require tedious repetitions to ensure that human errors will not spoil the validity of the final evidence. On the other hand, once the evidence is obtained, Computational Logic tools allow the formal proof obtained to be presented in a form that can be understood and followed step by step by non-expert humans so it can be transparently used as a trial evidence. In the long-term, such methods could yield an evidence certificate that will guarantee that an argument presented in a trial has been checked to be logically sound using a standardized formal verifier (in an analogous way to current applications of Formal Verification to Software Certifications) and according to tests performed on a relevant number of real cases. This kind of certificate could potentially allow ruling out cases of unintended (or intended) fallacies that are frequent in a purely rhetorical argumentation.

This long-term objective will be pursued and supported by the Action, where the inclusion of criminologists and criminal law experts in the network helps to ensure the uptake of the new technologies in the future. The new methods will also allow optimizing the use of available resources by relieving human experts from time-consuming and highly error-prone tasks that can instead be reliably performed by the future AI applications fostered by the Action results.

A potential risk concerning the proposed Action and its outcomes is that it may be difficult to convince the involved parties and the general public of the real applicability of such systems. While for some forensic techniques, such as DNA analysis, there is nowadays a high and widespread level of trust, an AI-based decision support system may initially appear unconvincing or even threatening. However, the general acceptance of DNA analysis paved the way for the introduction of other scientific methodologies. The non-technical Action partners will be helpful in identifying and enacting strategies for transforming scientific concept such as verifiability, completeness and correctness into humanistic and social concepts such as psychological reliability and trust, taking also into account specific cultural, legal and ethical aspects.

6 Preliminary results and future perspectives

Thanks to the experience gained over the years by investigators, via a study of many existing solved cases we have been able to claim with good reason that indeed a wide range of fragments of real cases can be mapped to computational problems, often to known ones. Modern investigative activities are composed of well-established practical steps, such as the crime scene reconstruction, alibi verification, as well as the analysis of huge amounts of data coming from data files, smart-phone and telephone logs. So, as a first step we have devised

a formulation of these sample problems [9, 5]. Such formulation exploits provably correct encodings of known mathematical problems to elicit scenarios from Digital Forensics data. In particular, we have chosen to represent (fragments of) cases in Answer Set Programming (ASP), which is a well-established paradigm for representing problems in $\mathbb{P}$ and $\mathbb{NP}$ or, with some extensions, even higher in the polynomial hierarchy (cf., among many, [15, 12, 13, 18, 11, 1, 10]). When applicable, the ASP formulations generate all possible scenarios compatible with the case's data and constraints. In the general case, this can be of great help as the human expert might sometimes overlook some of the possibilities: this has been verified by everyday practice, where different experts often generate different interpretations.

ASP has been selected for these first experiments because of its easy of use and readability, for the availability of efficient freely available inference engines ("ASP solvers") and for the possibility of performing proof of correctness of the software (the reader may refer to [16, 14, 17] for the definition of the underlying formal properties).

In a future perspective, we may notice that logical methods (like ASP) could provide a broad range of proof-based reasoning functionalities (including, e.g., time and time intervals logic, causality, forms of induction, etc.) that can be possibly integrated into a declarative framework for Evidence Analysis where the problem specification and the computational program are closely aligned. The encoding of cases via such tools would have the benefit that (at least in principle) correctness of such declarative systems based on computational logic can be formally verified. Moreover, recent research has led to new methods for visualizing and explaining the results of computed answers (e.g., based on argumentation schemes). So, one could not only represent and solve relevant problems, but might also employ suitable tools to explain the conclusions (and their proofs) in a transparent, comprehensible and justified way. The engine of such a future Decision Support System might be based, again remaining within a computational logic realm, on Multi-Context Systems (MCS) [2–4] and their agent-oriented extensions such as DACMACS (Data-Aware Commitment-based managed Multi-Agent-Context Systems, [7, 8]) and ACEs (Agent Computational Environments, [6]).

References

1. Baral, C.: Knowledge representation, reasoning and declarative problem solving. Cambridge University Press (2003)
2. Brewka, G., Eiter, T., Fink, M.: Nonmonotonic multi-context systems: A flexible approach for integrating heterogeneous knowledge sources. In: Logic Programming, Knowledge Representation, and Nonmonotonic Reasoning - Essays Dedicated to Michael Gelfond on the Occasion of His 65th Birthday. Lecture Notes in Computer Science, vol. 6565, Springer (2011)
3. Brewka, G., Eiter, T., Fink, M., Weinzierl, A.: Managed multi-context systems. In: IJCAI 2011, Proceedings of the 22nd Intl. Joint Conf. on Artificial Intelligence. IJCAI/AAAI (2011)

4. Brewka, G., Ellmauthaler, S., Pührer, J.: Multi-context systems for reactive reasoning in dynamic environments. In: ECAI 2014, 21st European Conf. on Artificial Intelligence, Proceedings. IJCAI/AAAI (2014)
5. Costantini, S. De Gasperis, G. and Olivieri, R.: Digital forensics and investigations meet artificial intelligence, Annals of Mathematics and Artificial Intelligence, in press (2019)
6. Costantini, S.: Ace: a flexible environment for complex event processing in logical agents. In: Engineering Multi-Agent Systems, Third International Workshop, EMAS 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9318. Springer (2015)
7. Costantini, S.: Knowledge acquisition via non-monotonic reasoning in distributed heterogeneous environments. In: 13th Int. Conf. on Logic Programming and Nonmonotonic Reasoning LPNMR 2013, Proceedings. Lecture Notes in Computer Science, vol. 9345. Springer (2015)
8. Costantini, S., De Gasperis, G.: Exchanging data and ontological definitions in multi-agent-contexts systems. In: Paschke, A., Fodor, P., Giurca, A., Kliegr, T. (eds.) RuleMLChallenge track, Proceedings. CEUR Workshop Proceedings, CEUR-WS.org (2015)
9. Costantini, S., Olivieri, R.: Digital forensics evidence analysis: An answer set programming approach for generating investigation hypotheses. In: 13th Int. Conf. on Logic Programming and Nonmonotonic Reasoning LPNMR 2015, Proceedings. Lecture Notes in Computer Science, vol. 9345, pp. 242–249. Springer (2015). Presented also at CILC 2015, 30th Italian Conference of Computational Logic, CEUR Workshop Proceedings 1459, CEUR-WS.org
10. Erdem, E., Gelfond, M., Leone, N.: Applications of answer set programming. AI Magazine **37**(3), 53–68 (2016), `http://www.aaai.org/ojs/index.php/aimagazine/article/view/2678`
11. Gelfond, M.: Answer sets. In: Handbook of Knowledge Representation. Chapter 7, pp. 285–316. Elsevier, Amsterdam, The Netherlands (2007)
12. Gelfond, M., Lifschitz, V.: Classical negation in logic programs and disjunctive databases. New Generation Computing **9** (1991)
13. Leone, N.: Logic programming and nonmonotonic reasoning: From theory to systems and applications. In: Logic Programming and Nonmonotonic Reasoning, 9th Intl. Conference, LPNMR 2007, Proceedings. Springer (2007)
14. Lifschitz, V., Pearce, D., Valverde, A.: Strongly equivalent logic programs. ACM Transactions on Computational Logic **2**, 526–541 (2001)
15. Lifschitz, V.: Twelve definitions of a stable model. In: Proceedings of the 24th Intl. Conference on Logic Programming. Lecture Notes in Computer Science, vol. 5366, Springer (2008)
16. Pearce, D.: A new logical characterization of stable models and answer sets. In: Non-Monotonic Extensions of Logic Programming, pp. 55–70. Lecture Notes in Artificial Intelligence, vol. 1216, Springer (1997)
17. Pearce, D., Valverde, A.: Synonymous theories in answer set programming and equilibrium logic. ECAI 2004, 16th European Conf. on Artificial Intelligence, Proceedings. IJCAI/AAAI (2004)
18. Truszczyński, M.: Logic programming for knowledge representation. In: Logic Programming, 23rd Intl. Conference ICLP 2007, Proceedings. Springer (2007)