Published in Proceedings of the International Workshop on Applications of AI to Forensics (AI2Forensics), online, 14 September 2020, which should be cited to refer to this work.

Digital Forensics & real cases: from Prosecutor's request to solution

Raffaele Olivieri[1] , **Stefania Costantini**[1] , **David Billard**[2] ,
[1]University of L'Aquila
[2]HESSO University of Applied Sciences in Geneva
raffaele.olivieri@gmail.com, stefania.costantini@univaq.it, David.Billard@hesge.ch

Abstract

The Digital Forensics (DF), as any other forensic discipline, is a science that follows rigorous methodologies and procedures could be generalized in steps.

During the activities related to a police investigation, particulary during the DF analysis or Digital Investigation (DI) activities, after the phases of data collection, further elaboration of the data is needed, by the investigators, for the contextualization of the objective elements in the real investigative case. The contextualization is required to search for facts, actions, events (and their sequences), as well as testing investigation hypothesis (verifiable) to be proposed as evidence in court during a trial. Very complex investigations, which often involve an enormous amount of heterogeneous data, represent a huge problem for the human mind when is needed to search the connection between events, facts or to demonstrate the existence of alternative scenario or solution. With considerable frequency, the investigative problem description may seems outline solutions which are non-linear, or seemingly even chaotic, but after a methodic analysis of the case, and its discompose in elementary components, many cases can be represented with a mathematical approach. The shape that the problems take on are typical of known optimization problems, belonging to various classes of complexity theory among which P, NP, or not far beyond, that can be thus expressed and often solvable with reasonable efficiency by using logic programming. Therefore, the aim of this demonstration is to present the formalization of some realistic investigative cases, via the reduction the case to the known optimization problem and find solution via simple logical programs using ASP (Answer Set Programming), and thus show how this approach leads to the formulation of concrete investigative hypotheses. In this way, the European Cost Action CA17124 called DigForASP (Digital forensics: evidence analysis via intelligent systems and practices), wants to delineate the future of the investigations, or simply the data contextualization, defining an implementation of a Decision Support System for investigators, by the integration of many techniques of Artificial Intelligence, Automated Reasoning and Computational Logic, the feasible implementation of intelligent agents as an aid for the human operator (specifically as a means to aid judges, lawyers, police, criminologists, etc.), supporting her/him in the checking of concrete investigative hypotheses.

During the demonstration, it will initially be illustrated how the requests of the judiciary evolved over the last twenty years and how they have become increasingly complex. The complexity arises from the need not only to search for existing data within a digital system, but today more and more frequently to correlate existing data with reasoning to carry out investigative evaluations.

Later it will be shown how an analysis of DF and DI is born and how today it is carried out by investigators with traditional methods.

Finally it will be illustrated some investigative cases approaching the use of logic programming with ASP (*Answer Set Programming*), led to formulation concrete investigative hypothesis.

Investigative cases are usually complicated, and involve a number of factors and several data to be taken into account. A formal explanation of such conclusions cannot in general be provided. After a deep analysis of a great number of DF real cases, as well as general investigations, we have reached the conclusione that many investigative problems can be reduce to computational problems, often to known ones. With this approach the reduction is clearly the analyst's responsibility and the solutions can however be found via the execution of algorithms, whose correctness can be proved.