C26 Non-Obvious Links in Online Frauds: Modeling and Comparison of Digital Traces, Context, and Actions

Timothy Bollé, School of Criminal Justice, University of Lausanne, Lausanne, Vaud 1015, SWITZERLAND; Eoghan Casey, PhD, University of Lausanne, Lausanne, Vaud, SWITZERLAND*

Learning Overview: After attending this presentation, attendees will better understand how to produce crime intelligence from real-world cases by combining techniques from forensic science and computer science and detecting non-obvious links and patterns. Attendees will also have a better understanding of the analysis of the detected links and patterns and of the resulting interpretation and decision-making processes.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by helping investigators and analysts to have a more complete vision of the available information, which will reduce the risk of missed opportunities caused by data silos and linkage blindness.

The goal of this research is to explore new and existing techniques and methods from forensic science, crime intelligence, and computer science to find non-exact or non-obvious similarities between online frauds. Perpetrators can easily switch to different online accounts or platforms, effectively changing their digital identity and the traces of their activities. As a result, exact comparison of digital traces is a limitation for link discovery in online fraud investigations. To overcome this limitation and to avoid linkage blindness, it is necessary to use near similarity comparison of distinctive characteristics of online frauds, including digital traces, context (spatio-temporal information), and actions taken by authors (*modus operandi*).

In order to correlate these distinctive characteristics, it is necessary to centralize the information and to structure it. This structure should allow the detection of links and patterns between entities. The main challenge here is the representation of actions and their context. The Cyber-investigation Analysis Standard Expression (CASE) will be tested to evaluate if it fits those objectives.[1]

In this work, a dataset of real-world online frauds will be used to test the validity of the proposed approach. After a general description of the dataset, algorithms to compute near similarity between digital traces are used to discover new links between cases. Furthermore, some of the cases will be studied more closely and represented using the CASE standard. The objective here is to model the actions taken by the authors, which allows their comparison, and then the detection and the analysis of patterns of actions.

An integral part of this work is to study the decision-making process of evaluating the links found using near similarity computations. An aspect of this evaluation could be to combine multiple information to look at the context of a given link and to compare the differences between nearly similar cases. It will help the investigator or the analyst to analyze the detected link and make suitable decisions.

Such crime intelligence approaches allow the centralization of information regarding multiple online fraud cases. It will help the investigators and the analysts to have a more complete vision of the available information, which will reduce the risk of missed opportunities caused by data silos and linkage blindness. Finding links and repetition between multiple cases is useful to have a better understanding of the various phenomenon in online frauds. This knowledge can be used in future investigations to obtain known useful traces and to apply efficient investigation methods and techniques. It can also be used to raise awareness about existing frauds. Linking cases committed by a potential same group of authors also allows them to be considered as one case, which increases the quantity of information about the group and is easier to handle for prosecutors.

Reference(s):

1. Casey, Eoghan, 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 (September 1, 2017): 14–45. https://doi.org/10.1016/j.diin.2017.08.002.

Forensic Intelligence, Near Similarity Computations, Online Frauds