Digital forensics tools improvement based on artificial intelligence

Floderus S., *Student*; Rosenholm L., *Student*
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
Blekinge Tekniska Högskola, Karlskrona, Sweden

The digital world is rapidly growing with new devices, smartphones and internet users. In addition, the Internet of Things is contributing to many more devices in circulation. This heavy number of devices also correlates with an increase in cybercrime. Current resources regarding law enforcement are very limited, while tools and techniques within digital forensic require human interaction and a great amount of time. With the use of artificial intelligence and machine learning, there are possibilities to improve current techniques and automate some parts of the process [1, 2].

There are four steps in a digital evidence process. The first step is to extract the data from a device such as a hard drive or USB (copy of the device by making a virtual hard drive). The second step is to make the data readable (e.g. decrypting data). The third step is to organize data. The last step is to analyze the data, find the evidence such as images, videos and timestamp, and so on [2]. There are current tools that aid investigators with these tasks such as FTK Imager for extracting data and Autopsy or Encase for organizing and analyzing data. Although these tools simplify the task, they do not rely on Artificial Intelligence [1].

A framework to collect and analyze relevant data that today is done manually could help save the time that directly affects the number of crimes that can be prosecuted. The current tools used for extracting data are efficient in recovering broken or deleted files and then categorizing or putting them into groups, but time-consuming and error-prone. There is a model proposed in [1] that still needs a real user to investigate but it will reduce the number of files that are relevant for the user to look through. This can be done in several steps, which are in this case smart acquisition, analysis, and presentation. They each have their own part to play to reduce the amount of data and information to work with.

1. P.H. Rughani, Artificial intelligence based digital forensics framework. *Int. Journal of Advanced Research in Computer Science*, **8(8)** (2017).
2. Z.J. Geradts, Forensic Challenges on Multimedia Analytics, Big Data and the Internet of Things. *ICETE* (2018).