AI FOR DIGITAL FORENSICS

HOW DOES AI CONTRIBUTE TO DIGITAL FORENSICS?

Rather too many people, faced with a difficult problem, opine that the solution either now or in the very imminent future lies in something called "artificial intelligence".

This has certainly been true of the difficulties of handling the vast quantities of digital evidence which can be located on computers of all sizes, smart phones and in the records generated by governments and other very large organisations.

Algorithms already play a significant role in helping digital forensics investigators analyze the vast amount of data that is created by mobile devices and stored on the cloud. Like many industries, demand outstrips supply when it comes to qualified, trained professionals who can sift through the backlog of digital forensics data relevant to modern criminal cases. Artificial Intelligence (AI) can help automate some processes and more quickly flag content or insights that would otherwise take investigators longer to uncover.

AI is another tool in the toolbox that is helping law enforcement agencies (and corporate in-house investigators) comb through the available data for insights—digital needles in the proverbial haystack.

AI functions can help with spotting and identifying elements in photos and videos, observing commonalities in communication, location, and times, and based on history, make educated guesses about where and when the next incident or crime might occur.

There is a trust factor to overcome with AI in digital evidence in criminal investigations. When evidence in a case is presented, the attorneys, judges, and jury members must grasp the broad concept of artificial intelligence in order to accept and feel comfortable with its growing role in digital forensics and in many modern criminal investigations.

All of that is to say that human beings will still have a role in criminal investigations. AI is a tool, but it's not an investigator. We're far away from that, if we ever get there at all. So while it's important to understand and harness this tool, it's equally not to conflate AI as analogous to an investigator.

1. **Digital investigators certainly use significant computer aids but very few of these can really be labelled "artificial intelligence". The analysis suites they use typically are able to: make a safe forensic copy of the contents of a computer or smartphone, extract obvious potential sources of evidence such as emails, text messages, social media postings, histories of Internet browsing, lists of file downloads and substantive files. Graphics, photo and video files can be viewed in a gallery. The entire contents can be indexed and not only the substantive files but associated time and date stamps and other meta data. Once indexed the investigator can then search for files by combinations of keywords and time and date.**
2. **Separate software can be used to scan an entire hard disk or storage medium for files which have previously been identified as "bad" child pornography, terrorist material, pirated intellectual property and so on. It does this by using file hashes, digital fingerprints – there are databases of file hashes and every time a file is encountered on a hard disk a file hash is created and compared against the database. The child sex database is called CAID – Child Abuse Image Database.**
3. **Increasingly too the software allows examinations to span several different digital devices so that an integrated view of the actions of a person of interest can be examined even if conversations took place using, for example, email, text messages and social media postings. Use is also made of data visualisation / link analysis techniques to demonstrate frequencies over time of contacts between phone numbers and between IP addresses, financial transactions and chronologies of events among others.**

AI IS IMPORATNT

1. **More advanced software allows the investigator to examine files at the bits and bytes level, to analyse hidden operating system features such as the Windows registry and also to interrogate a hard disk directly – these procedures may be necessary when some new product or service hits the IT market and becomes widely used. An important area is artefact research examining operating systems and application programs for features which might be put to forensic use.**
2. **The most advanced software even allows the well-trained investigator to create their own procedures in the form of scripts, for example to look for things which might be bank account details, credit card credentials, username and password combinations and so on.**
3. **But none of this involves artificial intelligence, although this phrase is rather vague and covers a number of different techniques. More**

properly we are talking about "machine learning". In machine learning a quantity of unsorted data files, statistics, graphics is offered to a program which is capable of deriving rules about that data. Once the rules have been discovered, a feat which may be beyond most humans, they can be applied to further similar unsorted data in order to make predictions or find conclusions. In the health field, given enough medical data, it may be possible to identify commonalities in diagnosis or treatment. In one form of predictive policing for example data can be collected about callouts for police vehicles to respond to incidents. A machine learning program can find rules which in turn can be used to point to situations where and when incidents are more likely to happen so that response teams can get to them more quickly.

4. **There are, however, weaknesses which should not be underestimated. The first of these is the quality and quantity of the training material offered to the learning program. If the training material is not representative of what you hope to predict results will be poorer. The larger the quantity of material the greater the chance that accurate rules will be derived. Secondly some material is more difficult to parse than others informal conversational language is a classic example. Third, anyone wishing to deploy machine learning has to look to the possibility of bad outcomes false and negative positives – where a prediction from machine learning gives a misleading result.**