**Introduction**

Forensic Investigation involves three major steps; Acquisition, Analysis, and Reporting. The investigator has to get them right, every time, so there’s not much room for errors when people’s lives are on the line. Digital Forensics is the branch of Forensic Science that deals with the same process of investigation but in the context of cyberspace. Since past few years, the world has seen a boom in rise of computation power, storage space and variety of electronic devices. The rise of storage and media formats further increases types and amount artefacts that one has to sift through to reconstruct the scenario and prepare a timeline for the chain of events. With the consumer grade products gaining storage capacity more than few terabytes and availability of applications for the ease of everyone for all day-to-day tasks the complexity, severity, and number of cyber crimes are increasing at an equal, if not at a faster rate. Almost every type of crime today has a digital touch to it, some related artefact residing in suspect or victim or any other person of interest’s computing device.

Digital Forensics has become an inevitable tool in the identification of cybercriminal activities due to its ability to extract valuable information and evidence from computing devices in a legally acceptable manner (Casey, 2010). However, over the course of past few years it has been facing a rise in challenges including but not limited to increased investigation time, explosion in data storage capacity leading to increased error rate and lack of automation. These are some of the limitations that can be overcome with the judicious use of Machine Learning & Artificial Intelligence algorithms by automating parts of digital forensic investigation that are otherwise performed manually. The idea is to pull together Acquisition, Analysis & Reporting phases and developing a solution that helps in setting a baseline for the investigators by automating time-consuming steps to speed up overall investigative process.

Some of the tasks can be automated by writing elegant algorithms that perform a series of pre-defined steps. Some, like image processing, can be achieved with the help of Machine Learning. The analysis phase is usually the most time-consuming one, it requires a lot of patience and searching to find evidence among artefacts. One of the tasks during this phase is suspect identification; while, for a human it is trivial when the number of images is few, but the difficulty of correct identification exponentially grows with the scale of case. This paper aims to solve above mentioned problems by providing an AI driven digital forensics framework to streamline the investigation process, by narrowing down the amount of evidence to be processed manually to an acceptable proportion.

The rest of the paper is structured with sections, “Related Work”, it presents existing use cases of automation in digital forensics and the ways its impacting data retrieval, analysis and data enrichment. “Execution Methodology”, the process and algorithm involved in developing this software. Section “Automated PoI Identifier” discusses a empirical method that applies deep learning and computer vision algorithms which are then evaluated in after mentioned test-cases. The next section follows an extensive “Discussion” before walking into “Conclusion” and “Future Work”.