18-2-22 Friday.

Digital Forensics.

Suhan. B. Revankar.
PES2UG19CS412

AI & ML has been around since a long time, but now we have enough computational power to develop strong 'Neural Network'. with help of strong hardware & software.

AI & ML has great advantages & used to craft. Cautomate, execute some serious crimes that can be deadly for people.
For instance, hackers can develop an ANN the scans new version of popular apps for unknown vulnerabilities. if its done manually it will take a long time.

ML & AI holds great forensic importance. Its a new field to dive in for forensic investigators & scope of research is really big.

Forensic Acquistion And Analysis

→ Challenges for DF

- Large Volume of data
- Complex Processing
- Legitimacy issue.
- Privacy Violation
- New "anti-forensic" trends.

The Below specific AI methods impact DF field.

① Knowledge Representation : computer programs requires so that it intelligently performs tasks

② Pattern Recognition : identify certain type of clusters of data in investigation can help to determine picture contents, Spams, e-mails & recognise folder in hard drives that contain questionable files.

Some AI techniques that help in DF.

① Live forensics : These identify, limit & eliminate threat on spot & enable one to plan on tackling the threat. While at this it important to look through criminal record to determine who might be responsible.

② Data Recovery : Restoration of data & using AI for scanning that was destroyed or deleted.

③ Password Recovery : This comes handy when investigators use AI, ML to bruteforce intelligently the passwords protected files & crack password to enable accus to files which can be evidence

④ known File Filtering : AI & ML can be employed for intelligently training the ANN models on malicious known snippets. Then getting the model on field to detect such snippets without executing the malicious code.

⑤ Timeline Analysis : This tells investigators the order of events that led to event under investigation. Using AI this proces can be more efficient than before & less time consuming.

Conclusion :

However, a lot of research work still needs to be done in this field. Proper & deeper analyse of volatile information would be beneficial as well as more in-depth analysis of Neural Networks might help us to get more familiar with machine learning programs in the scope of digital forensics.