ISSN No:-2456-2165

Digital Forensics and Artificial Intelligence A Study

[1]Mohammed Rahmat Ali
SADAF,9-8-256, Bada Bazar, Golconda Fort, Hyderabad-500008, Telangana State.

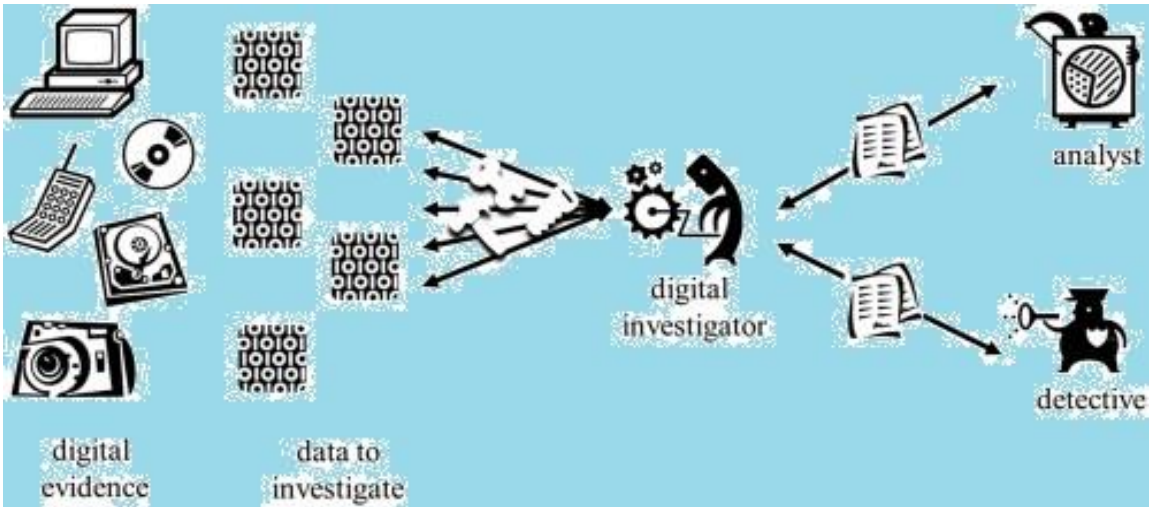
Abstract:- Digital Forensics is one of the fastest growing technology, which created a great impact on the techniques and tool used to analyse, monitor and visualize the crime scene and pull a proper method to handle the upcoming threats and attacks on the cyber or internet world. The modern use of Artificial Intelligence to reduce the human efforts and to attain maximum results with fewer amounts of faults has replaced the human in performing ability to machine oriented designed work which has the ability and capacity to minimize the fault and improve the quality. The use of Artificial Intelligence in the field of Digital Forensics, can impact the outcome and analyse the evidence in a better and efficient way to monitor the results.

Keywords:- *Digital Forensics, Artificial Intelligence.*

I. INTRODUCTION

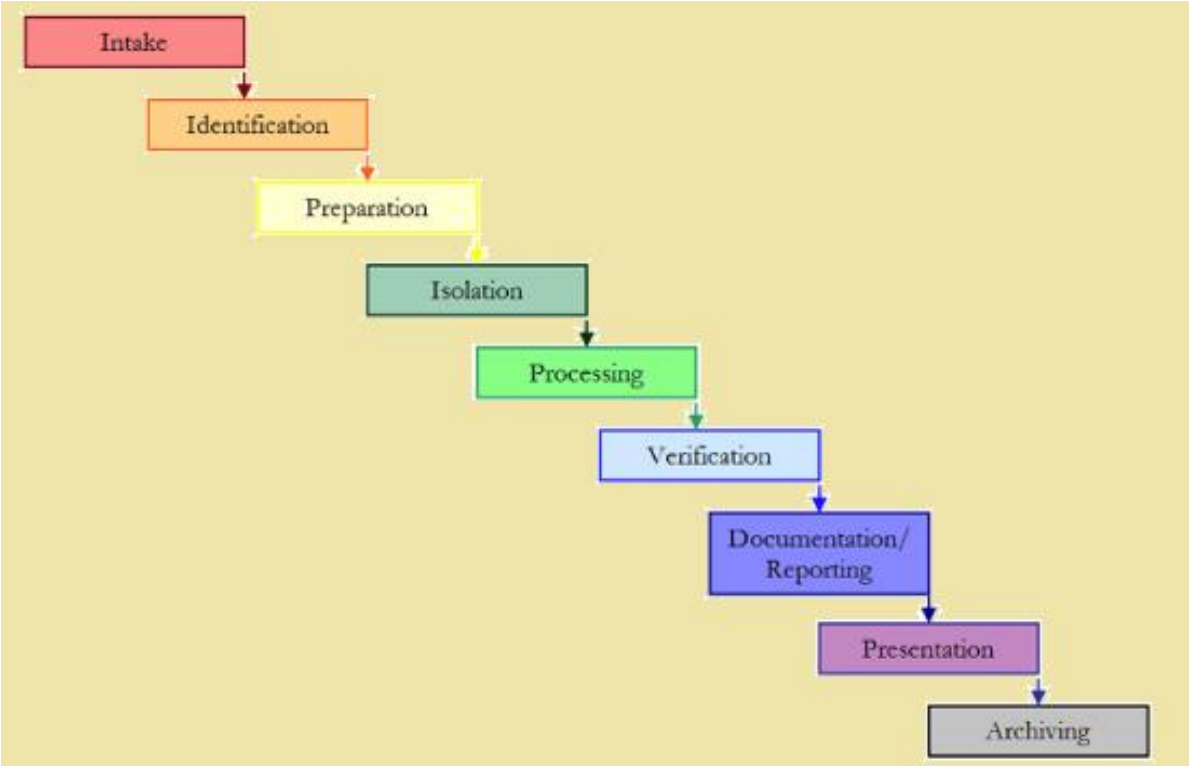
Digital forensic is a branch of science which deals with the protection of system and data associated towards its. Digital forensics also deals with occupying the evidence and analysing of the evidence to know the cause of the attack which part of the system was been attacked. Modern technology has advanced the future in a way that we can predict the future by the use of leading technology. Digital Forensics has a protection system that can determine the evidence and analyse those evidence for future. According to a recent industrial survey, ninety-four percent of the companies didn't respond against potential threat to company and bare a loss of worth $ 35 billion. Digital Forensics is a tool used to learning through which will increase the security and analysing ability of the system to monitor the risk of information and computer risks. Technological development, information creation and results can lead to new access for new security users and end-users, without knowing how to end users. When the middle or middle level is known, a safe and secure threat can be found on an incompatible but dangerous computer. It creates a crime and must be investigated and protected through trial proceedings.

The continued increase in digital media storage capabilities and the extensive presence of daily life coverage is increasing demand and verifying the full amount of data. By linking this problem, you analyse the appropriate size and analyse its performance and do not correct the current forensic devices. Thus, computer forensics specialists use more time. The problem with this test is to calculate the required account because most forensic devices do not distribute processing capabilities.



The difference in communication for forensic data, criminal investigators and prosecutors, the statistical evidence of the court's misinterpretation can easily led to Wrong decision and suspension of justice or wrong doing. Artificial Intelligence can provide new algorithms and best practices for development and supporting communication between stakeholders. Technology based on artificial intelligence, algorithms can communicate with statistical evidence and equality in construction of Artificial intelligence sample logic and structure illustration. Artificial Intelligence can also be given the model scenario to help making decisions and artificial intelligence enable different judges Test information for some ideas. Artificial Intelligence has developed tools and projects which are

practically analyzed through a realistic case study training meeting with the help of forensic law It is expected that this unit will have the final result Analytical tools to prevent legal errors and practical devices The model also allows for the support of legal practitioners Professional exchange between statistical and legal experiments professional.



II. DIGITAL FORENSICS AND CONVENTIONAL TOOLS

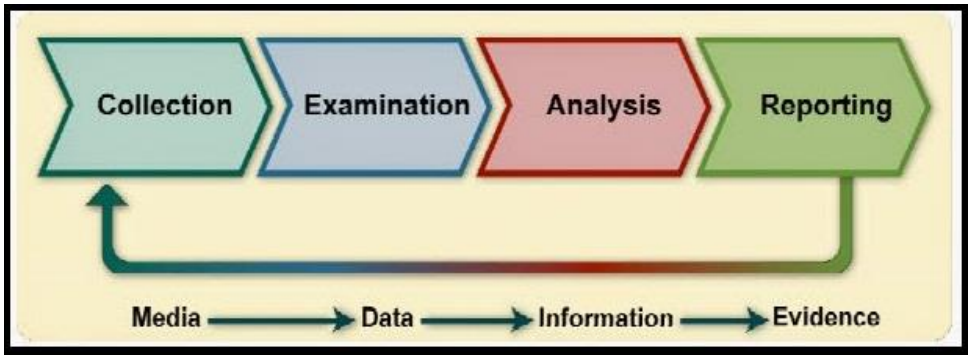
Digital forensics uses tools and methods to monitor and analyse the evidence and access the files been manipulated or been traced. The conventional methods collects all the possible evidence from different storage locations and present that data to monitor and analyse. The traditional process involves different types of acquiring the evidence from the following like backup files, logical acquension and physicalacquision.

➢ *Typical Forensics Analysis Step:*

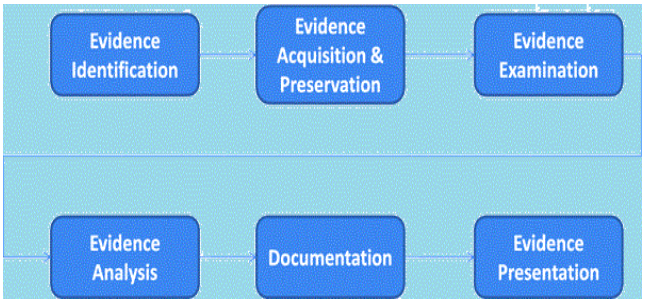
- Create timelines of events like the files system, last time file accessed, changed and created. Meta data from the file
- Mounting of disk image readonly.
- Generating list of all files allocated and deleted
- Analysing the key files
- Recover deleted files
- Files carving by handling the unallocated files.
- Search files inn Disk image.

➢ *Digital Forensics Investigation Process*

- Verification
- System description
- Evidence Acquisition
- Timeline analysis
- Media and artefacts analysis
- String or byte search
- Data recovery
- Reporting results.



➢ *The Forensics Investigation Process*
- Early task, will be there be an investigation
- Who will perform the investigation?
- Identification of item of internet
- Preservation of evidence
- Collection and taking control legally
- Examination a time consuming activity
- Analysis must be fully documented
- Presentation in the court of expert witness
- Decision as trail



➢ *Chain Of Custody Of Evidence*
- Who obtained the evidence
- Where and when it was obtained
- Who had the control or the position of evidence
- Secure storage in the mounted vault

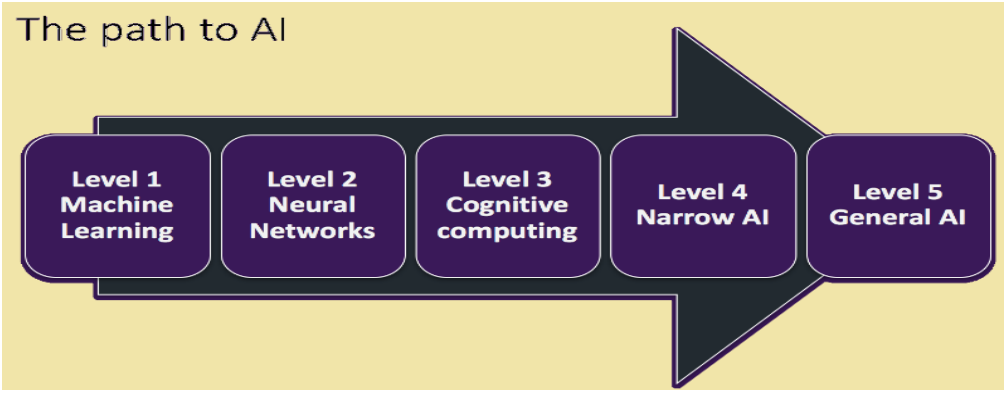
➢ *Digital Forensics Tools Classification*
- Disk and data captured tools
- Files viewer
- File analysis tool
- Registry analysis tool
- Internet analysis tool
- Email analysis tool mobile device analysis tool
- MAC OS analysis tool
- Network forensics tools
- Database forensics tools

III. ARTIFICIAL INTELLIGENCE IS ABOUT

Artificial intelligence is a study of intelligent devices and its procedure to pursue knowledge from the environment and from the previous results obtained. Artificial intelligence systems will generally show some of the following behaviours related to human intelligence: planning, learning, thinking, problem solving, representation of knowledge, perception, movement and manipulation, and to some knowledge of social intelligence and creativity. At very high levels, artificial intelligence can be categorised into two main types: narrow artificial intelligence and general artificial intelligence.

Narrow type of Artificial intelligence is what we see around us in today's computer. Intelligent systems that have been taught or learned to perform certain tasks without explicitly being programmed to do so. This type of intelligence in voice recognition and the language of Siri's default assistant on the Apple iPhone, in the vision recognition system of his self-driving car, is clearly in the proposed engine that suggests the products you love. In the past, unlike humans, this system can learn to perform certain tasks only, which is why it is called narrow artificial intelligence.

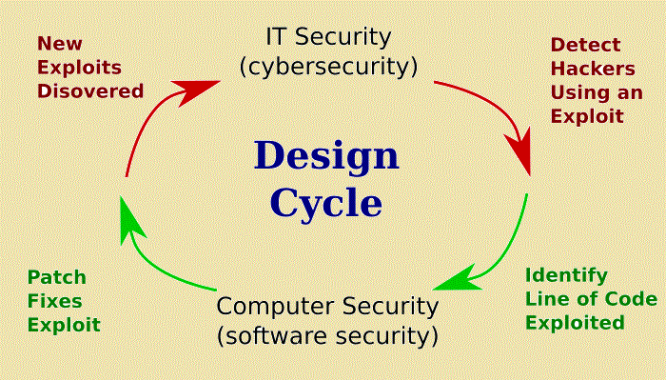
General Artificial intelligence is quite different as it is a kind of adaptive intelligence in humans that is flexible toward intelligence and that is capable of learning how to perform very different tasks, from cutting hair to scales, or thinking about different subjects based on accumulated experience.



IV. ARTIFICIAL INTELLIGENCE AND ITS IMPLEMENTATION IN DIGITAL FORENSICS

Artificial intelligence is used in the modern world to reduce the work loads of input to get maximum out comes and to manage the system by itself taking proper inputs from the previous results and by analysing the resultant values for the future course. Artificial Intelligence deals with the management of resources, analysing and complying resources and methods upon the use. Digital forensics has occupied almost every section of technology and every application. The use of artificial intelligence in field of security can help system analyse the pre deterministic approach to handle the errors and upcoming errors or security breaches and attacks. ArtificialIntelligence can also help us in predictingthepossible ways of analysing the problem and canbe resolved before the security is been compromised.

Artificial Intelligence can also help the field of digital forensics by implicating the methods and techniques used by the features of artificial Intelligence to provide maximum outcome of the evidence been analysed. The need of artificial intelligence in the field of digital forensics is to analyse the data and secondly to predict the possible ways a computer can be break through ij and the possible way to breach the computer.



Traditional forensics tools need external input from the users to work with the procedure of forensic process, but if we use artificial intelligence tools there is a provision that it may allocate the threat or breach for the computer to user in prior so that the security program can be executed and can handle the threat. Or in case the system is been breach, artificial intelligence can capture the evidence from the source and can maintain a record of the attacker.

Artificial intelligence can manage to get the sources of attack and attackers information so that it can be easy for the forensics experts to backtrack to the source to get the information and means by which the attack or breach occurred. The system can analyse the evidence and can separate the evidence from other documents. The analysis can also be quick and very reliable if the artificial intelligence or the machine analysis the machine. Or in other words if a machine communicates with the other machine the resultant value can vary to a human being. As human may occur errors the machine is capable of performing the task with less fault as per the algorithm is designed.

Artificial Intelligence can make the work easy and efficient and more reliable to as compared to humans, but may also lack is the supporting files and other evidences to the system, human intervention plays a prominent role but the use of artificial intelligence can make a major change. The detection and recovery method is based on the algorithm been designed by the system, The Program works according to the design of the system. The chance of predicting who the intruder is will ease for the forensics expert.

Artificial intelligence may apply any of the forensic tools designed so that the intruder cannot hide the evidence anywhere within the system which the traditional forensics tools fails to analyse. Whenthe intruder penetrates in to the system it leaves some of the evidences behind, and if the intruder knows which type of forensics tool will be used he will hide the information to those memory block where the forensic tool cannot find evidence. Resulting in no recoverable evidence. But if the forensic tool are been designed intelligently then the left over memory block may also be analysed and evidence can be analysed.

V. CONCLUSION

Digital forensics is the everlasting field of study which need continuous changes in functioning to maintain its efficiency. Proper changes should be made and at proper peak of technology. To improve the quality of the application it should be capable platform and independency and to be robust. The use of artificial intelligence in digital forensics can make very broad and recognisable changes in the field of security.

Artificial Intelligence will help the digital forensics tools to analyse the evidence and to make easier tasks for the forensics expert to analyse the data and to make proper conclusion to find the resultant of crime scene. It may also help the practice of pre-analysing the security threat with the past threats and also by storing threat records to update the system for the future use. By the use of forensics tool the system can be monitored and can be treated with the possible changes and solutions.

REFERENCES

[1]. https://www.researchgate.net/publication/220999758_Artificial_intelligence_applied_to_computer_forensics
[2]. https://accessdata.com/blog/the-coming-ai-revolution-in-digital-forensics
[3]. http://ijarcs.info/index.php/Ijarcs/article/viewFile/4571/4116
[4]. https://crimsonpublishers.com/fsar/pdf/FSAR.000554.pdf
[5]. http://sas-space.sas.ac.uk/5533/
[6]. https://pdfs.semanticscholar.org/5350/676fae09092b42731448acae3469cba8919c.pdf
[7]. https://www.deccanherald.com/content/636412/ai-deep-learning-revolution-digital.html
[8]. https://resources.infosecinstitute.com/category/computerforensics/introduction/#gref