INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CROSS-PLATFORM FORENSIC ANALYSIS: FROM AUTONOMOUS SYSTEMS TO PERSONAL DEVICES

AUTHOR – UPASANA GHOSH, ASSISTANT PROFESSOR, DEPARTMENT OF LEGAL SCIENCE, TECHNO INDIA UNIVERSITY.

BEST CITATION – UPASANA GHOSH**,** CROSS PLATFORM FORENSIC ANALYSIS: FROM AUTONOMOUS SYSTEMS TO PERSONAL DEVICES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (9) OF 2026, PG. 288-295, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

Artificial intelligence is rapidly becoming the most important applied science in all sectors of life. In the same way, the forensic department is also taking benefit from it in various ways. More individuals are realising the importance of AI in everyone's lives and working hard to comprehend it through digital science, which is now very convenient and available to anyone. Technology can make people's job easier, but it will never be able to replace humans. Forensic science is an area of forensic experts, and Artificial Intelligence will never be able to reach that level. It will only serve as a supplementary tool to human experts. It implements automation, which saves substantial time and money while allowing investigators to focus more on areas where fraud may occur. It assists forensics experts with detecting behaviour from massive volumes of unstructured data, such as videos, pictures, emails, and text files. It's a more dynamic method than rule-based testing, which can only assess fraud risk across a single data set. It eliminates information that might hamper an analytics-aided investigation. AI technology can assist in pattern recognition, such as identifying different components of a single image, detecting patterns in emails and messages, and matching new information with various forms of existing data in system databases. It can also assist detectives in connecting suspect information with existing criminal records and informing them of any past criminal conduct that the suspect in question may have been involved in. With the exponential rate of growth of storage capacity, such as USB, hard drives, optical media, and flash drives, it is getting more difficult for forensic science investigators to store and evaluate

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

all this data. AI has the potential to be a good tool to store, analyze and use this data for legal purposes.[316]

Keyword- cyber forensics, AI, electronic devices, netizens, law

INTRODUCTION

By using machine learning techniques, AI may quickly classify and rank data according to relevance which saves a lot of time and effort as compared to manual process of going through enormous datasets. This guarantees the foreign specialists to concentrate on the most relevant data. AI- driven log file analysis tools can interpret patterns found in these logs, allowing investigators to reconstruct events, spot anomalies. AI tools can also analyse behavioural patterns by identifying unusual or suspect behaviour and allows for pre-emptive action before a crime is to be attempted. AI systems have the capacity to identify complex patterns in large datasets which helps forensic investigators put disparate pieces of evidence together. AI's pattern recognition skills can be used to identify the tactics used in cybercrimes. AI- driven threat intelligence technologies are able to anticipate possible attacks through anomaly detection.[317]

AI algorithms, trained on extensive datasets of known malware samples, can detect and categorize unknown malwares. By machine learning techniques, these systems can analyse code and user behaviour to effectively pinpoint malicious software.[318]

Image and video analysis-

AI-driven tools with advanced algorithms for facial recognition and object detection can analyse images and videos from surveillance footage or analysing content from digital devices.[319]

Speech or voice recognition is a significant part of artificial intelligence applications. Through natural language processing, artificial intelligence can recognise and identify voice and meet the requirements of the users.

AI lie detector and heart rate monitor app can detect if a person is not telling the truth. In that app, a person can upload a video of the interview taken with the accused and the app will tell whether the person is telling a lie or the truth by detecting the heart rate and whether the accused person's speech is high, low or medium. This enables the cyber forensic experts to identify a cybercriminal.

FORENSIC ANALYSIS OF E-MAIL

Criminals use fake e-mails to numerous users so that the receiver finds it as a legitimate mail. This activity is also called phishing.[320] This is an attempt to induce netizens to reveal their personal information such as usernames, passwords and credit card details by impersonating as a trustworthy and legitimate individual or an organisation.[321] There are tools available that create fake mails. Forensic analysis of e-mails is an important element of cyber forensics as it helps establish the authenticity of an e-mail when suspected. An e-mail system is the hardware and software that controls the flow of e-mail. The two most important components of an e-mail system are the e-mail server and the e-mail gateway. E-mail servers are computers that forward, collect, store and deliver e-mail to their clients and e-mail gateways are the connections between e-mail servers. Mail server software is a network server software that controls the flow of e-mail, and the mail client software helps each user read, compose, send and delete messages. An e-mail

[316] Kamshad Mohsin, Artificial Intelligence in Forensic Science, SSRN Electronic Journal, http://dx.doi.org/10.2139/ssrn.3910244

[317] Monika Khindre, Deepti Monga, Role of Artificial Intelligence (AI) in Digital Forensic, International Journal of Law, Policy and Social Review, Volume 5, Issue 4, 2023, Page No. 121-123

[318] The Intersection Of Digital Forensics And Artificial Intelligence (AI) - Simplyforensic

[319] The Intersection Of Digital Forensics And Artificial Intelligence (AI) - Simplyforensic

[320] National-Cyber-Defence-Reference-Handbook-II.pdf

[321] CS.pdf

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

consists of two parts, header and the body.[322] Message headers are the important aspect of cyber forensics as it provides the entire path of e-mail's journey from its origin to its destination. The header includes the originating Internet Protocol (IP) address and other useful information. Headers of an e-mail can easily be spoofed by spammers and other irresponsible network users. The header contains several mandatory and optional fields, trace information and heading fields.[323] The body of an e-mail contains the actual message or data of an e-mail. The body of the e-mail may also contain attachments in the form of MIME or SMIME (secure or multipurpose Internet mail extensions). An extra degree of security known as S/MIME encrypts the communication using keys that are supplied by both the sender and the recipient. By limiting decryption to those who have the encryption keys, S/MIME offers even more anonymity.[324] It is a protocol that provides digital signatures and encryption of Internet MIME messages. SMTP or simple mail transfer protocol is a protocol for sending e-mail messages between servers. Gmail uses TLS (Transport Layer Security) by default to encrypt the connection when messages travel between email servers. TLS helps protect privacy by guarding against email manipulation and eavesdropping during transmission. TLS-encrypted e-mails are also referred to as normal encryption in Gmail.[325] In Gmail, emails that use TLS are also known as standard encryption. To identify an IP address of an e-mail the date and time must be found out. This may or may not be present in the header. Once the IP address is found, the Internet Service Provider details have to be found out. The Internet Service Provider plays an important role in e-mail forensics. The Internet Service Provider provides internet access to businesses, organizations, schools, colleges and individuals. Details available from the Internet Service Provider are name, address, and contact number of the subscriber of the Internet facility, type of IP address, any other relevant information regarding IP address at a particular given date and time, usage details, etc.[326]

To determine the source of e-mail, investigators must first examine the received section at the bottom of the header and work their way up in a bottom to top approach.

Fake e-mail creation tools are frequently used by cybercriminals. Therefore, it is possible that some e-mails have fake headers with fake 'from' e-mail addresses to fool investigators. Extreme caution and scrutiny should be practiced in investigating every part of the e-mail header. [327]

EmailOnDeck.com is a website where fake e-mail ids can be created temporarily and be deleted afterwards. [328]

FORENSIC ANALYSIS OF SMART PHONE

A smartphone has a contact address book, a planner, messenger, photos, and video camera, it has GPS navigation facility, it works as a Web Client to access Web-based applications and it is a platform for third- party applications. A smartphone has the basic information such as IMEI number, hardware and software version numbers with which the phone operates, and network information. The event log of smart phone includes records of events such as incoming and outgoing calls, missed calls, sent and received messages history, wi-fi sessions, etc. The SIM card of a smartphone contains the International Mobile Subscriber Identity, phone numbers and SMS messages. The contact address book contains names, nickname, prefix, suffix, joint name, photo and personal ringing tone, phone numbers, email address, company, job title, birthdays, last modification date and time. Speed dial information is also there in a smartphone. The messenger gives a lot of information to forensic analysts such as text messages, multi-media messages, email messages with attached files, files sent via Bluetooth. Some of the smartphone models

[322] National-Cyber-Defence-Reference-Handbook-II.pdf
[323] National-Cyber-Defence-Reference-Handbook-II.pdf
[324] National-Cyber-Defence-Reference-Handbook-II.pdf
[325] Learn about email encryption in Gmail - Gmail Help
[326] Nina Godbole, Sunit Belapure, Cyber Security, Wiley, 2011
[327] National-Cyber-Defence-Reference-Handbook-II.pdf
[328] Free Temporary Email - EmailOnDeck.com

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

contains GPS navigation feature too which helps the analysts to find out the movement of the criminal where he or she last used the smartphone. The Web Client of the smartphone holds useful information such as web cache files, bookmarks, pages view history, last opened URLs, search history and cookies. The IM client on the smartphone holds information such as IP, Login and password, contacts list, chat history and calls history. As smartphones are hand-held PCs, they also contain camera snapshots, video clips, voice records, sounds and Podcasts, Wi-Fi networks list, paired Bluetooth lists, activated SIM cars list. [329]Third-party applications installed in the smartphone are added information for forensics.[330] Through forensics of smart phone, retrieval of Text Messages (SMS), Photo, video, E-mail, Deleted messages, Web browsing history, Analysis of location history (via GPS, cell tower data or other means), Document or file, WhatsApp and other messaging/chat applications[331] message can be done.

FORENSIC ANALYSIS OF SIM CARD

In every mobile phone the SIM card plays a major role in communicating the information. In a crime if a mobile phone has been taken as the evidence, the first and the foremost thing is to investigate the SIM card.[332] The SIM card system consists of-

ICCID: ICCID is known as "Integrated circuit card identifier", which contains the 20-digits unique identification number. They are categorized into two types, Account Identification Number [AIN] and Issuer Identification Number (IIN).[333]

TMSI: It abbreviates as "Temporary Mobile Subscriber Identity", which is exchanged between the mobile phone and local network.[334]

ADN: It is abbreviated Dialing Number, in a simple word, the contacts number saved by subscriber.[335]

LND: It is abbreviated as Last Number Dialed, which records last phone number the user is been dialed.[336]

SMS: It is "Short Message Service", which allows the subscriber to communicate them with a short message. That sent and received through the mobile network. SMS is considered of the valuable assets for forensic investigation purpose.[337]

The forensic investigation of a SIM card is done by removing the SIM card from the cell phone and connecting it to SIM card reader. The hash value of the data in the SIM card is calculated to check the integrity of the data, that is, whether it has changed or not. The forensic tools which can extract data from the cell phone are-

- Encase Smartphone Examiner: This tool is specifically designed for gathering data from smartphones and tablets
- MOBILedit Forensic: This tool can analyze phones via Bluetooth, IrDA, or cable connection; it analyzes SIMs through SIM readers and can read deleted messages from the SIM card.
- pySIM: A SIM card management tool capable of creating, editing, deleting, and performing backup and restore operations on the SIM phonebook and SMS records.
- SIMpull: SIMpull is a powerful tool, a SIM card acquisition application that allows you to acquire

[329] [PDF] Advanced Techniques in Forensic Examination of Smartphones - Free Download PDF

[330] Nina Godbole, Sunit Belapure, Cyber Security, Wiley, 2011

[331] Recovering Digital Evidence with Mobile Device Forensics – Police and Security News

[332] C. Aanandha Subramanian, K. Suthendran, M. Satheesh Kumar, SIM Forensics: Extraction and Preparation of Digital Evidence using Sim Xtractor, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S2, December 2019

[333] C. Aanandha Subramanian, K. Suthendran, M. Satheesh Kumar, SIM Forensics: Extraction and Preparation of Digital Evidence using Sim Xtractor, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S2, December 2019

[334] C. Aanandha Subramanian, K. Suthendran, M. Satheesh Kumar, SIM Forensics: Extraction and Preparation of Digital Evidence using Sim Xtractor, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S2, December 2019

[335] C. Aanandha Subramanian, K. Suthendran, M. Satheesh Kumar, SIM Forensics: Extraction and Preparation of Digital Evidence using Sim Xtractor, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S2, December 2019

[336] C. Aanandha Subramanian, K. Suthendran, M. Satheesh Kumar, SIM Forensics: Extraction and Preparation of Digital Evidence using Sim Xtractor, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S2, December 2019

[337] C. Aanandha Subramanian, K. Suthendran, M. Satheesh Kumar, SIM Forensics: Extraction and Preparation of Digital Evidence using Sim Xtractor, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S2, December 2019

the entire contents of a SIM card. This capability includes the retrieval of deleted SMS messages, a feature not available on many other commercial SIM card acquisition programs.[338]

FORENSIC ANALYSIS OF DRONES

The use of drones has increased in recent years, and there has been an increase in drone accidents, causing the need for digital forensic investigations of drones. However, when using drone digital forensics, law enforcement and other investigative agencies must overcome a unique set of challenges. Additionally, there are additional ethical and legal considerations when using drones in criminal investigations. Digital forensic investigations of drone accidents are fraught with intricate challenges spanning technical, legal, and practical domains. The acquisition of crucial flight data stored on manufacturer servers is often hindered by legal restrictions and manufacturers' reluctance to share proprietary information. Ensuring the integrity of flight data proves difficult, with malicious alterations or deletions complicating the accurate reconstruction of accident sequences. Signal interference or communication loss during accidents further delay real-time data capture, creating challenges in reconstructing events. The absence of standardized tools and methodologies in drone forensics leaves investigators grappling with diverse systems and file formats. The complexity of drone software ecosystems, spanning flight control software, firmware, and third-party applications, demands deep expertise in various programming languages. Balancing the need for thorough investigations with privacy concerns becomes delicate, especially when accidents involve sensitive or private areas. [339]Drone technology is developing so fast that forensic experts need to adapt constantly. Additional layers of complexity are introduced by various factors like environmental factors, physical damage and the worldwide variety of regulatory frameworks. Finally, gathering evidence from remote accident is very challenging. A cooperative, interdisciplinary approach involving forensic specialists, attorneys, drone manufacturers and regulatory agencies is required to address these issues, with a focus on continuing forensics research and development to stay up to date with the technology.[340]

Drones are typically made of lightweight materials that can be easily damaged or destroyed during the investigation process.[341] Finding drones can be difficult because they are often small and can be easily destroyed or hidden by suspects. Environmental factors such as temperature, humidity, and dust may make it challenging for investigators to access actual evidence, such as parts of crashed drones or damage from an unusual flight occurrence. The recovery of evidence from drones can be made more difficult by the use of cloud-based storage systems because data may be kept in various locations. Privacy concerns, particularly when drones are used to collect data from individuals without their knowledge or consent or fly over restricted areas that may limit or restrict access to certain types of data or information during an investigation. In addition, drones can offer a more thorough view of a crime scene than conventional techniques, but they also pose special data security and privacy issues.[342] There are no laws or regulations governing the use of drones for this purpose in many countries, which can lead to potential legal issues if the drone is used improperly or without proper authorization.

With the rapid advancement of drone technology, Unmanned Aerial Systems (UAS)

[338] SIM — Card Forensics — Zentachain | by Zentachain | Medium
[339] Almusayli, A., Zia, T., & Qazi, E.-u.-H. (2024). Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology. Technologies, 12(1), 11. https://doi.org/10.3390/technologies12010011
[340] Almusayli, A., Zia, T., & Qazi, E.-u.-H. (2024). Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology. Technologies, 12(1), 11. https://doi.org/10.3390/technologies12010011
[341] Almusayli, A., Zia, T., & Qazi, E.-u.-H. (2024). Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology. Technologies, 12(1), 11. https://doi.org/10.3390/technologies12010011
[342] Almusayli, A., Zia, T., & Qazi, E.-u.-H. (2024). Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology. Technologies, 12(1), 11. https://doi.org/10.3390/technologies12010011

have become very useful in sectors like agriculture, industries, defence, filmmaking and surveillance. The need for forensics of drones arises when the drone is used for illegal purposes like smuggling, espionage, unauthorized surveillance, and even terrorism. The objectives of forensics of drone is to find out the operator of drone, the flight paths, date and time of flight paths, analyse the cameras, sensors, and navigators used in the drone, the videos and photos recorded in the drone, trace command and control links such as GPS, wi-fi. The tools used in forensics of drones are logic analyzers, chip readers, RF detectors, Cellebrite, Autopsy, FTK Imager, GPS Visualizer, Drone Decoder, Dat Con, Airdata UAV, BlackBox Extracto.[343] Drones, with their diverse functionalities and technological sophistication, create hurdles for forensic investigators in the collection, preservation, and analysis of digital evidence. The rapid advancements in drone capabilities, such as autonomous flight and encrypted communication, contribute to the intricacy of forensic examinations. Moreover, the specialized expertise required for effective drone forensics, including knowledge of aeronautics, electronics, and data science, poses a significant challenge for forensic professionals. Drones rely heavily on volatile memory, and the flight data stored therein will vanish if the battery drains out, which suggests that the battery life of a drone can impact the ability to retrieve flight data during a forensic investigation and that not all commercial drones have flight controllers that are equipped with data logging capabilities. Therefore, the ability to retrieve flight data may depend on the specific drone model and its features.

FORENSIC ANALYSIS OF AUTONOMOUS CARS

Autonomous Vehicles may contain ECUs (Electronic Controlling Units) for controlling various functions like braking, steering, infotainment, etc. ECUs often store diagnostic trouble codes (DTCs), event data, and sensor logs. These vehicles include cameras, radar, lidar, and ultrasonic sensors. May store footage, object detection data, and decision-making inputs. These cars have phone call logs, navigation history, voice commands, and app usage. It may sync with mobile devices, expanding the scope of evidence. They also have features like Global Navigation Satellite System (GNSS) / GPS to track the vehicle location, path history and geofencing violations. The forensics tools used in Avs are CANalyzer, Vehicle Spy, SavvyCAN, FTK Imager, Magnet AXIOM, EnCase, OpenCV, ROS (Robot Operating System), Matplotli, Tesla Explainer, Autel MaxiSys, Bosch Crash Data Retrieval System.[344]

FORENSICS OF ROBOTS

One such operating system called Robot Operating System (ROS) has been in use since 2007 and is one of the most popular Robot Operating Systems till date. It is mostly used for industrial and academic purposes. Robotic technology is using robot operating systems for the development of robotic ecosystems, and it is a meta operating system framework that connects robot-to-human and robot-to-robot interaction. It can be used as a middleware on Linux and Windows platforms. Being highly focused on mechanical robots, security has never been a focused area in the robot operating systems. In 2014, the ROS version was modified to ROS 2. The robot operating system has a peer-to-peer network connection, which consists of ROS master, nodes, topics, messages, and services. ROS has a publisher/subscriber model for transferring messages. This system has several independent nodes, which are interconnected with each other for communication.[345]

[343] ELHAAM DEBAS1,ABDULLAH ALBUALI, and M M HAFIZUR RAHMAN, Forensic Examination of Drones: A Comprehensive Study of Frameworks,Challenges, and Machine Learning Applications, IEEE Acsess, Digital Object Identifier 10.1109/ACCESS.2023.1120000

[344] Kim Strandberg , Member, IEEE, Nasser Nowdehi, and Tomas Olovsson , Member, IEEE, ASystematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection, IEEE TRANSACTIONS ONINTELLIGENTVEHICLES, VOL. 8, NO. 2, FEBRUARY2023

[345] Yash Patel, Parag H. Rughani, A SYSTEMATIC ANALYSIS OF ROBOTIC SECURITY AND INVESTIGATION, NFSU – Journal of Cyber Security and Digital Forensics Volume – 2, Issue – 2, December 2023 E – ISSN – 2583-7559

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 9 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- ROS Master - This node is the head communication hub of the robotic system. It has the responsibility of managing name services and providing connections between nodes. Whenever a new node is installed, it informs the master node about topics and publishing/subscribing. ROS master node will track the offered services and topics of the robot system, it maintains internal communication. If there will be no master node, then the nodes can not find each other for communication.[346]
- ROS Nodes - This node has a process to perform the computation of robotic systems. Each and every node has its own name, which is recorded in the ROS master. ROS nodes can receive information from other nodes, and send information to nodes. ROS nodes have to communicate with each other and report to ROS master nodes.[347]
- ROS Topic- a primary form of communication in robotic systems is Topic. Messages are communicated in the robotic system through the ROS topic. To identify the content of the messages ROS topic is used. ROS node will publish the message to the ROS topic. ROS topic will call back to the receiving node and transfer the information to another node. Topic names should be unique in the namespace, and content for ROS topics will state information, sensor data, motor commands, etc.[348]
- ROS Messages - Nodes are sending and receiving messages with each other. ROS Messages are information that a node will dispatch to other nodes. It is a data structure that can hold data in it. Messages will be in data type such as integer, floating-point, and boolean. The data type can be built-in or customized. [349]
- ROS Services - The node can advertise services in robotic systems. Services can be used to send a request and handle a reply. It represents an action that has defined the starting and ending. Services are in pairs; requesting form a node or responding to a node.[350]

FORENSIC ANALYSIS OF COMPUTERS

The system drive which contains the operating system for the forensic computer shall be restored from a system image. The system image contains backup of the system drive that contains a clean install of the operating system. It must be ensured that the forensic computer is functioning properly after system image restore. A target drive must be selected for the forensic examination. Target drive is a sterile piece of media used to store forensic image(s) and case related data. If necessary, the hard drive(s) from the computer and external media is to be removed. Label items of evidence for identification. For collection of evidence, the Control Media for the forensic computer is to be acquired. Control Media is a standard piece of media with a known hash value. The evidence must be acquired with an approved software or hardware tool using the proper acquisition procedure. Anti-virus programs may be run either on the original evidence using a write-blocker or on a forensic image mounted in forensic software unless the evidence drive is incompatible. Virus definitions for anti-virus software shall be checked for updates prior to running the program. Forensic image(s) must be added into approved forensic software tool(s) for evidence processing. Documentation provided by the submitting agency shall serve as the basis for processing and analysis of forensic image or images. Based on training and experience, the Forensic Scientist shall run the appropriate processing options for each tool utilized in the case, along with utilizing the appropriate file filter(s). Processing and analysis may include but

[346] Yash Patel, Parag H. Rughani, A SYSTEMATIC ANALYSIS OF ROBOTIC SECURITY AND INVESTIGATION, NFSU – Journal of Cyber Security and Digital Forensics Volume – 2, Issue – 2, December 2023 E – ISSN – 2583-7559

[347] Yash Patel, Parag H. Rughani, A SYSTEMATIC ANALYSIS OF ROBOTIC SECURITY AND INVESTIGATION, NFSU – Journal of Cyber Security and Digital Forensics Volume – 2, Issue – 2, December 2023 E – ISSN – 2583-7559

[348] Yash Patel, Parag H. Rughani, A SYSTEMATIC ANALYSIS OF ROBOTIC SECURITY AND INVESTIGATION, NFSU – Journal of Cyber Security and Digital Forensics Volume – 2, Issue – 2, December 2023 E – ISSN – 2583-7559

[349] Yash Patel, Parag H. Rughani, A SYSTEMATIC ANALYSIS OF ROBOTIC SECURITY AND INVESTIGATION, NFSU – Journal of Cyber Security and Digital Forensics Volume – 2, Issue – 2, December 2023 E – ISSN – 2583-7559

[350] Yash Patel, Parag H. Rughani, A SYSTEMATIC ANALYSIS OF ROBOTIC SECURITY AND INVESTIGATION, NFSU – Journal of Cyber Security and Digital Forensics Volume – 2, Issue – 2, December 2023 E – ISSN – 2583-7559

is not limited to the following-Deleted or hidden partitions, File Signature Analysis, Hash Analysis, Index Text, Expand Compound Files, Recover/bypass passwords, Internet History Analysis, Picture and Video Analysis, Email Analysis, Document Analysis, System Information, Deleted data, Data from unallocated space and file slack, Archives, Databases, Keyword and Pattern searches. [351]

CONCLUSION

The most challenging part of using artificial intelligence in digital forensics is the reliability and accuracy of AI tools. There is a risk of producing false results or there is a chance of overlooking crucial information. There is also a chance of hacking private and sensitive data by cyber attackers through phishing schemes which complicate the task of cyber forensic experts. AI tools created for cyber investigation can also be hacked by cyber criminals. Therefore, it is important for cyber forensic experts to ensure the correctness and authentication of the results produced by AI tools.

[351] Technical Procedure for Computer Forensic Examinations Digital Evidence Section Issued by Digital Forensic Scientist Manager, Version 2 Effective Date: 01/05/2018