Volume 8 | Issue 4 | November 2023 https://doi.org/10.46293/4n6 | ISSN : 2582-1172

DIGITAL FORENSICS(4N6)

INDIA'S 1st DIGITAL FORENSICS PUBLICATION

CyberPeace

Cyber Safeguard

Empowering

4N6 4N6 4N6 4N6

OUR SPONSORS & PARTNERS

DIGITAL FORENSICS(4N6)

INDIA'S 1st DIGITAL FORENSICS PUBLICATION

PARTNERS

CYBERFRAT
AN ERM COMMUNITY

NISC

NATIONAL CYBER DEFENCE RESEARCH CENTRE

Be The Change That You Wish To See In The Forensic Science
NYAYIK VIGYAN

StraightArc
Technologies Pvt. Ltd.

FORENSICS GURU .COM

CYSINFO

BRISK INFOSEC

Digital Investigators
DIA
Association

ninja
Information Security Seriously
ISO- 27001:2013 & 9001:2008 Certified

ARROW

TechLaw

INDIAN INFOSEC CONSORTIUM

CyberShrishti
For the Noobs by the Noobs

CYBER SECURE INDIA

CPC

ARNE
Advance Research Network

Cyber Katta

JEMISTRY
INFO SOLUTIONS

ARISTI NINJA

SAM
OFFENSIVE
TECHNOLOGIES

CyberHex

CopConnect
National Security Database

India Watch

DARK EYE
INTELLIGENCE

DIPLOMADS

SkillsDA®
Center for advance training

ISAC

CONFERENCE PARTNERS

ifip

2nd World Conference and Exhibition on
Forensic Science
June 11-12, 2018 Rome, Italy

DICE
DIGITAL INVESTIGATIONS
CONFERENCE & EXHIBITION

ASIA'S FOREMOST INFORMATION SECURITY CONFERENCE
GROUND ZERO
SUMMIT

HACKERS DAY

OUR TEAM

Our Founders

Lt. Col. (Dr.) Santosh Khadsare (Retd.)
Prince Boonlia

Our Mentors

Mr. Omveer Singh
Mr. Rakshit Tandon
Dr. Gaurav Gupta
Mr. Nilay Mistry

Technical Committee

Mr. Deepak Kumar (D3)
Mr. Tanmay Dikshit
Mr. Smith Gonsalves
Mr. Hriday Raval
Mr. Yugal Pathak
Mr. Ankit Bhisnoi
Mr. Deepanshu Sharma

Design and Development Committee

Mr. Aman Agarwal
Mr. Kritharth Jhala
Mr. Rishabh Sovani
Mr. Shubham Singh

Editor-In-Chief

Ms. Rakhi R Wadhwani
Mrs. Seema Khadsare
Major Vineet Kumar

Editorial Board

Mr. Deep Shankar Yadav
Ms. Evita K. Breukel
Ms. Sneha Joshi

Managing Editor

Ms. Jyoti Nene

Content Reader Committee

Mr. Rajesh Sharma
Ms. Sunita N
Ms. Anjali Chouhan
Ms. Vaishali Wahi

www.digital4n6journal.com

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

EDITORIAL NOTE

Dear Readers,

Hope you are all doing well. We are excited to share the latest Digital Forensics (4N6) issue, which is about Artificial Intelligence (AI). As we all know this is a hot topic today, and there are many visions of the future regarding this technology. The concept of AI has been prominently depicted in science fiction movies, but how does AI work in reality? Join and Explore with us as we investigate this fascinating topic in the latest issue of 4N6. Please read the Table of Contents to see what we have planned this time.
You can publish your own article, we would like to offer you the opportunity to write an article for our publication/blog to share your knowledge and experience with our readers. There are no additional charges.

We are grateful to all our authors, reviewers, designers, editors and proofreaders who contributed to our latest publication. Your insights and efforts have been invaluable.

We are excited to keep the collaboration going and invite others to join us in creating more exceptional content.

Let us work together to make a meaningful impact in our field.
Happy Reading!!!

Seema Khadsare
Editor-in-Chief

Rakhi R. Wadhwani

Rakhi R Wadhwani
Editor-in-Chief

Major Vineet Kumar
Editor-in-Chief

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

INDEX PAGE

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

ARTIFICIAL INTELLIGENCE APPLICATIONS IN CYBERSECURITY

Author/Writer: **Sejal Shibe**

Abstract:

Artificial Intelligence (AI) has emerged as a powerful tool in addressing the ever-evolving landscape of cybersecurity threats. This article explores the applications of AI in cybersecurity, highlighting its role in threat detection, prevention, and response. By analyzing various AI-driven techniques such as machine learning, deep learning, natural language processing, and anomaly detection, we demonstrate how AI enhances the ability to defend against cyberattacks. Additionally, this paper discusses the challenges and ethical considerations associated with AI in cybersecurity, providing insights into the future of this technology.

Keywords:

Introduction

The digital age has ushered in an era of unprecedented connectivity and convenience but has also exposed individuals, organizations, and nations to an array of cybersecurity threats. Cyberattacks continue to evolve in sophistication, making it increasingly challenging to protect against them using traditional security methods. Artificial Intelligence (AI) has emerged as a revolutionary technology capable of bolstering cybersecurity defenses by providing real-time threat detection, automated response mechanisms, and predictive analytics.

We will dive into the various applications of AI in cybersecurity, exploring the role of machine learning, deep learning, natural language processing, and anomaly detection in safeguarding digital assets in this article. We also discuss the ethical implications and challenges associated with AI in cybersecurity and conclude with a glimpse into the future of this technology.

AI in Threat Detection

Machine Learning in Threat Detection

Machine learning algorithms enable computers to learn from data and make predictions or decisions without being explicitly programmed. In cybersecurity, machine learning models are applied to identify patterns and anomalies in large datasets to detect threats. Some notable applications include:

1. **Malware Detection:** Machine learning algorithms can analyze file attributes and behavior to identify known and zero-day malware. Solutions like antivirus software often incorporate machine learning to enhance detection rates.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

2. **Intrusion Detection:** Anomaly detection algorithms use historical network data to identify deviations from normal behavior, signaling potential intrusions or suspicious activities in real time.

Deep Learning for Enhanced Detection

Deep learning, a subset of machine learning, focuses on neural networks with multiple layers. This approach has proven to be highly effective in cybersecurity, particularly in tasks such as:

1. **Threat Intelligence:** Threat intelligence uses deep learning models' incredible capacity to examine huge amounts of threat data, which includes things like malware signatures and network traffic patterns. In addition to exposing hidden hazards, this sophisticated research also makes it possible to predict upcoming assaults. Deep learning adds to the field of cybersecurity by revealing complex patterns and abnormalities within these datasets. By doing so, it offers proactive insights that allow enterprises to strengthen their defenses and stay one step ahead of cyber attackers in the never-ending cat-and-mouse game.

2. **Phishing Detection:** The combination of Natural Language Processing (NLP) with deep learning is very advantageous for phishing detection. To accurately identify phishing emails, this potent combination permits the careful evaluation of email content, sender behavior, and contextual cues. Deep learning evaluates sender behavior and contextual information, boosting the accuracy of identifying misleading and malicious emails, while natural language processing analyzes the text content for suspicious patterns. Together, they create a strong barrier against one of the pervasive and sneaky cyber dangers, enhancing email security with sophisticated, automated detection techniques.

AI in Threat Prevention

Automated Vulnerability Assessment

AI-driven vulnerability assessment tools can scan systems and applications to identify weaknesses that may be exploited by attackers. These tools leverage machine learning to prioritize vulnerabilities based on severity and potential impact, enabling organizations to proactively mitigate risks.

AI-Enhanced Authentication

AI plays a crucial role in enhancing user authentication mechanisms, offering multi-factor authentication (MFA) solutions that leverage behavioral biometrics, facial recognition, and voice recognition. This reduces the risk of unauthorized access, especially in critical systems.

AI in Threat Response

Automated Incident Response

AI-driven incident response systems can rapidly detect and respond to cyber threats, reducing the time between detection and mitigation. These systems can isolate compromised systems, halt malicious processes, and even suggest remediation strategies.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

- **Predictive Analytics for Threat Hunting**

Utilizing AI's capabilities, Predictive Analytics for Threat Hunting gives cybersecurity professionals the tools they need to actively look for prospective threats. AI improves the ability to foresee and neutralize impending assaults by digging into past data and extracting observable patterns and upcoming trends. Because it enables proactive rather than reactive security, this strategic approach is especially useful in addressing advanced persistent threats (APTs). Organizations can improve their security posture and proactively protect their digital assets against knowledgeable and persistent hackers by anticipating adversary actions through predictive analytics.

User Authentication

AI enhances authentication methods by incorporating factors like biometrics (fingerprint, facial recognition) and behavioral authentication. This makes it much harder for malicious actors to impersonate authorized users.

Challenges and Ethical Considerations

- **Data Privacy and Ethics**

The use of AI in cybersecurity raises concerns about data privacy and ethical considerations. Collecting and analyzing user data for threat detection must be conducted with transparency and adherence to privacy regulations to avoid potential misuse.

- **Adversarial Attacks**

Attackers are increasingly using AI to evade detection, leading to the development of adversarial attacks. This requires continuous improvements in AI models to defend against adversarial manipulation.

Future Scope

The future of AI in cybersecurity holds promise for even more sophisticated threat detection and response capabilities. Advancements in quantum computing and AI are likely to reshape the cybersecurity landscape, presenting both new challenges and opportunities.

Conclusion

Artificial Intelligence has become indispensable in cybersecurity, offering innovative solutions for threat detection, prevention, and response. As the cyber threat landscape continues to evolve, AI will remain a crucial tool in defending against malicious actors. However, it is essential to address ethical concerns and adapt to new challenges as AI technology advances.

References:

1. https://www.nist.gov/artificial-intelligence
2. https://www.techtarget.com/searchsecurity/definition/cybersecurity
3. https://www.researchgate.net/publication/320066760_A_survey_of_deep_learning-based_network_anomaly_detection
4. Goodfellow, I. J., et al. (2018). Deep Learning. MIT Press.
5. Deep learning in mobile and wireless networking: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2224-2287.

ABOUT THE AUTHOR:

Sejal Shibe

Sr. Manager- Cybersecurity Projects, CyberFrat

Expertise:
Sejal is a dynamic leader known for fostering team collaboration, driving innovation, and achieving exceptional results through effective communication and strategic decision-making. As the driving force behind CyberFrat's global community, Sejal adeptly manages a network of 25,000+ IT and cybersecurity experts, orchestrating cross-training initiatives and successful meet-ups online and offline across various cities in India. She also looks after organizing events, webinars, and meetups for knowledge sharing and professional growth for the CyberFrat community.

Additionally, takes charge of operations, sales, and marketing at CyberFrat, efficiently leading a dedicated team to drive business growth and foster community engagement. Also, she actively leads various cybersecurity academia projects, delivering impactful training and upskilling content to empower students in the field."

COIN SPECTOR

ILLUMINATE THE DARK CORNERS OF THE DIGITAL ECONOMY!

In today's fast-evolving financial landscape, cryptocurrency remains a domain where transparency is elusive. With the groundbreaking technology of Coinspector, the cloak of digital transactions is lifted.

WHY COINSPECTOR?

ON-PREMISE NODE INSTALLATION

Enhance your crypto investigations with on-premise node installation. Gain unparalleled data access and control, bolster security, and ensure real-time, accurate blockchain analysis.

IN-DEPTH ANALYSIS

Dive deep into concealed data, discern emerging trends, make decisions, and get a holistic grasp of intricate virtual assets.

RISK MANAGEMENT LIKE NEVER BEFORE

With the capability to identify and analyze looming threats, we empower organizations to strategize robustly, balancing both risk appetite and core objectives.

ABOUT US

With 30 years of expertise in Digital Forensics, we began by aiding law enforcement with top-tier software solutions. Recognizing the rise of digital currencies in illicit activities, we innovated with 'Coinspector' - our exclusive tool designed for precise Cryptocurrency Investigations. Trust in our legacy; ensure a secure digital future.

Lab Systems

+91 9324122665

sales@labsystems.co.in

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

ARTIFICIAL INTELLIGENCE APPLICATIONS IN CYBERSECURITY

Author/Writer: Dr. Bhagyashri R Hanji, Dept. of CSE, DSATM, Bengaluru.

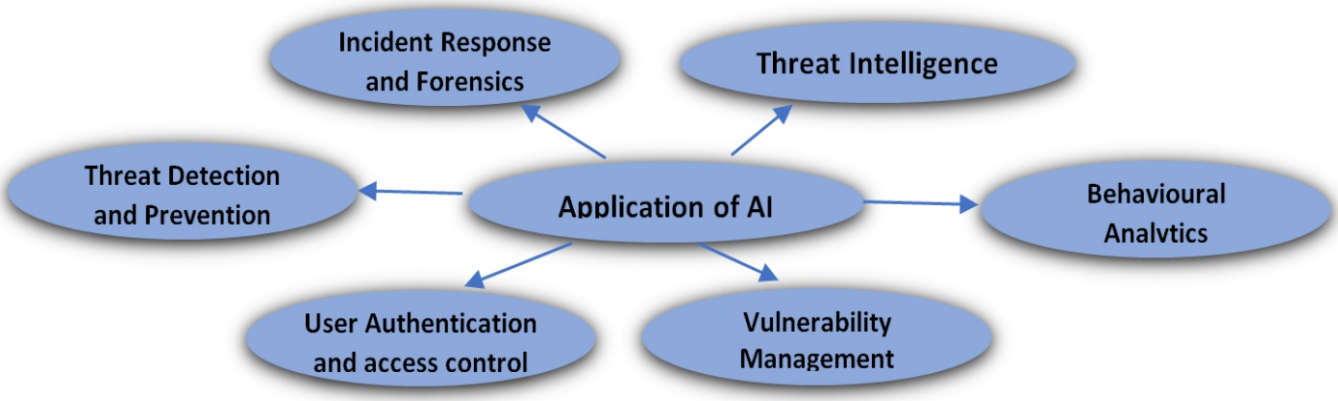
Email: bhagyashri-cse@dsatm.edu.in

Abstract

Technology Advancement has brought tremendous benefits, at the same time giving rise to new risks. Cybersecurity threats have become more sophisticated and predominant, posing important challenges to organizations and individuals. Artificial Intelligence has emerged as a powerful tool with its analysis and decision-making capacity, revolutionizing the field of cybersecurity. Artificial Intelligence in Cyber Security Market size was valued at USD 7.58 Billion in 2022 and is projected to reach USD 80.83 Billion by 2030, growing at a CAGR of 30.1% from 2023 to 2030. The market is expanding because of the rising trend of IoT adoption, the enormous increase in connected devices, and growing worries about the susceptibility of Wi-Fi networks to security threats. Integrating AI in cybersecurity systems poses a number of challenges such as Data manipulation, AI-powered cyber-attacks, Data unavailability, Privacy concerns and Attacks on the AI systems.

Importance of AI and AI Applications in Cybersecurity

AI systems can identify patterns and irregularities in data that may indicate possible threats. AI automates routine tasks, freeing up human analysts to focus on more complex issues. It adapts and learns from new threats, constantly improving its capabilities for safeguarding sensitive information.



AIML algorithms can analyse network traffic and identify suspicious activities, detect patterns and anomalies in large datasets, phishing emails, spam and malware. Continuous vulnerability assessment on networks and systems, automate the vulnerability management process and prioritize risk mitigation efforts. AI Techniques such as biometric authentication, facial recognition and voice recognition enhance security by replacing traditional methods. AI provides valuable perception to forensic analysts and assistance in incident response by automating the detection and containment of security incidents. AIML algorithms can monitor user behaviour and analyse user activities to create profiles and identify deviations from normal patterns. AI-powered systems can aggregate and analyse vast amounts of data from various sources, including social media, news articles, and security blogs. By correlating this information with real-time threat data, AI can provide valuable insights into emerging threats, enabling proactive defence measures. Cyber threats are becoming more numerous and sophisticated.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Modern security teams have a number of difficulties that make it difficult for them to protect data, control user access and swiftly identify and respond to threats. These difficulties include smart attackers, an expanding attack surface, a data explosion and an increasingly complicated infrastructure. Protecting data across hybrid environments, generating more accurate and prioritized threats and balancing user access needs and security are the important components to be analysed.

Hackers attempt to continually breach digital environments. Data and identity theft, phishing, and other cybercrimes are on the rise. Organizations hire qualified cybersecurity teams who persistently defend digital systems by utilizing emerging technologies, such as artificial intelligence, in order to prevent these attacks.

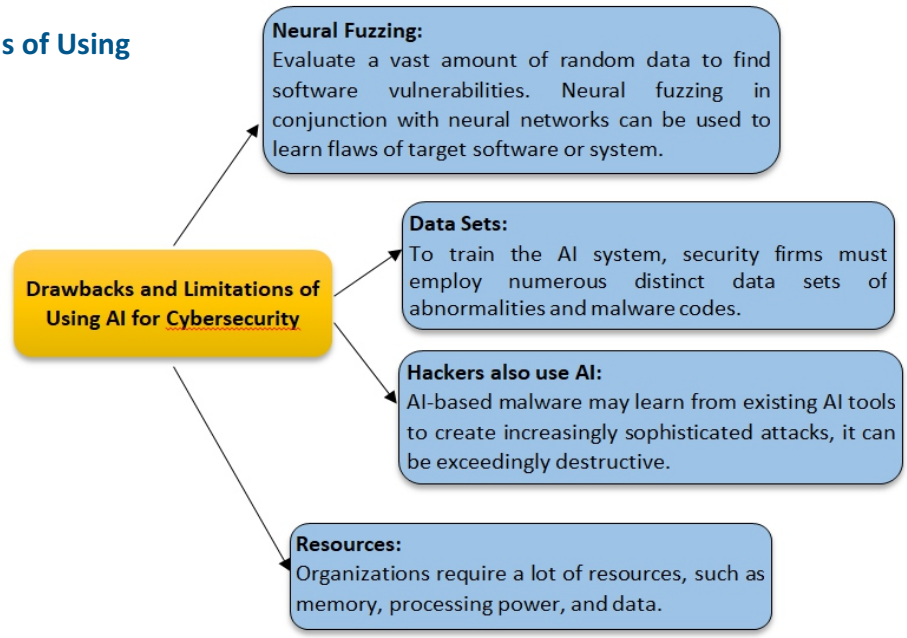
Artificial intelligence in cybersecurity examines system usage trends to spot possibly malicious behaviour or threat actors and foresee cyberattacks. Automated monitoring powered by AI safeguards systems round-the-clock and helps businesses take precautions before harm is done.

Malware and phishing detection, Knowledge consolidation, Detection and prioritizing of new threats, Breach risk prediction and Task automation are some important applications of AI in cybersecurity.
Malware is malicious software intended to do unlawful actions that are transferred to a user's computer. Typical malware actions include data removal, making unauthorized copies, Data protection, remotely accessing and managing a gadget, negative advertisement and Observing user behaviour. Any system that is online is susceptible to cybersecurity risks. Implementing and abiding by hundreds of security protocols and standards is necessary to prevent them. The millions of software flaws that are now in use make it impossible for cybersecurity experts to keep up, which is why manual threat detection always runs the danger of security leaks.

The IT asset inventory of large businesses is huge, and it can be difficult to assess each component for the risk of a security breach. AI algorithms can determine which parts are most vulnerable to a breach and even forecast the likely sorts of assaults.

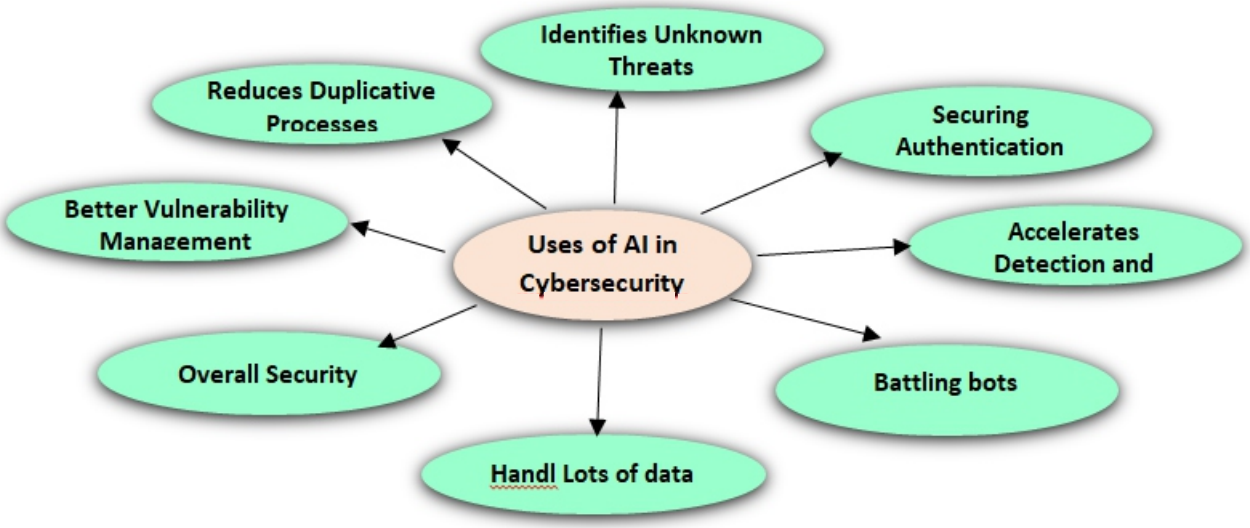
Every second matters while defending against online dangers. The more harm is done, the longer the countermeasures are in place. An attacker has plenty of time with a manual threat detection and mitigation method to steal or encrypt data, hide their traces, and leave backdoors in the system. Threat detection can be automated, and immediate action can be taken.

Drawbacks and Limitations of Using AI for Cybersecurity.



DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Uses of AI for cybersecurity



What is the future of AI for cybersecurity?

Both benefits and drawbacks of artificial intelligence exist in cyber security. On one hand, it strengthens cybercrime analysis, comprehension, and prevention, boosting the safety of businesses and customers. However, AI can be resource-intensive and not necessarily useful. Cybercriminals can also utilize it to enhance their attacks. VPNs are one sector that benefits from AI since machine learning enables them to defend users against online threats brought on by AI. One of the main benefits of AI technology is its speedy data analysis.

Need for AI in Cyber Security

Because hackers discover new ways to launch various types of assaults each year that have a specific goal, it is difficult for a normal human to recognize and stop all the threats faced by a corporation. If we fail to detect, identify, and prevent these new forms of unknown threats, the network could sustain significant harm, and they could have a significant impact on the company. There is considerable worry that cybercriminals would launch their own AI attacks. Additionally, hackers can trick systems that use learning.

How Is AI Trained for Cybersecurity?

When hackers try to access inside systems, they leave behind something called intrusion signatures. Large databases of digital footprints are compiled by security experts for future reference, to help identify weaknesses and unique patterns used by attackers. AI may be taught to detect intrusions as they happen with a sufficiently large database of intrusion signs and patterns.
As an illustration, one of the most effective attack strategies is breaking into embedded systems, such as video cameras, printers, and other kinds of network-connected devices. The default login information used by the hackers allows them access to these devices. These devices are breached by the hackers, giving them access to the rest of the network

Conclusion

Artificial intelligence has become an indispensable tool in the fight against cyber threats. With its ability to analyse massive amounts of data, detect anomalies, and adapt to new attacks, AI is transforming cybersecurity practices. Organizations that embrace AI in their cybersecurity strategies will benefit from improved threat detection, faster incident response, and enhanced protection against emerging threats. As the threat landscape continues to evolve, AI will undoubtedly play a vital role in safeguarding our digital world. To improve IT security performance at the enterprise level, using AI for cybersecurity is essential. To reduce breach risk, prioritize hazards, manage incident response, and detect malware attacks before they happen, security professionals can use the analysis and threat identification it offers. AI will advance cybersecurity and enhance enterprises' security posture despite any potential drawbacks.AI will advance cybersecurity and enhance enterprises' security posture despite any potential drawbacks.

References

1. https://www.ibm.com/security/artificial-intelligence?utm_content=SRCWW&p1=Search&p4=43700052660419533&p5=e&gclid=EAIaIQobChMIkqHU-N78gAMVgIFLBR3N-gTYEAAYASAAEgLIFfD_BwE&gclsrc=aw.ds

2. https://www.v7labs.com/blog/ai-in-cybersecurity

3. https://www.verifiedmarketresearch.com/product/artificial-intelligence-in-cyber-security-market/#:~:text=Artificial%20Intelligence%20In%20Cyber%20Security%20Market%20size%20was%20valued%20at,30.1%25%20from%202023%20to%202030.

4. https://www.altexsoft.com/blog/ai-cybersecurity/

5. https://www.engati.com/blog/ai-for-cybersecurity

6. https://www.knowledgehut.com/blog/security/ai-in-cyber-security#role-of-ai-in-cyber-security%C2%A0

7. https://aithority.com/guest-authors/ai-in-cybersecurity-applications-in-various-fields/

ABOUT THE AUTHOR:

Dr. Bhagyashri R Hanji

Professor, Computer Science and Engineering
Dayananda Sagar Academy of Technology and Management, Bengaluru

Expertise: Her areas of interest include Mobile Ad-hoc Networks, Wireless Networks, Information and Network Security.

Credentials: She currently works as a Professor in the Department of Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, India.

DRONA LABS By eSec Forte®

eSec Forte®

DRONA LABS

Drona Labs is a High-End Workbench-based labstation with ergonomic design and height adjustment for user-friendly adaptability.

The chassis is anti-static, non-skid and is painted with automotive paint.

Technical Specifications
Dual Intel Xeon Gold 6354, 18-core, 3.00GHz Base, 3.60 GHz Max Turbo, 39MB Cache
Intel C621A Chipset
1TB (16 x 64GB) DDR4 ECC RDIMM 2933 MHz
1TB SATA Internal Solid-State Drive for OS
1TB PCIe NVMe M.2 (2280) Internal Solid-State Drive Pro Series for Temp/Cache
2TB PCIe NVMe M.2 Internal Solid-State Drive Pro Series for Processing Data
40TB (4 x 10TB) Internal Hard Drive Enterprise SATA HDD 7200rpm for Data Storage
4 x 3.5" Read-Write 12Gbps Removable HDD SASIII/SATAIII Bays
4 x 3.5" Read Only 12Gbps Removable HDD SASIII/SATAIII Bays
4-port USB 3.1 Super Speed USB Bay
4-port USB-based Charging Bay
Tableau T356789iu Forensic Bridge with SAS/SATA/IDE/Firewire/USB/PCIe interfaces along with cables
Ventilation Tray with single cooling fan for holding suspect drive
Forensic Card Reader
4 x Power Sockets (each 220V, 6A)
BD-R / BDRE/ DVD-RW/CD-RW Blu-Ray Burner dual layer Combo Drive
Secure Fingerprint-based Power On and Windows Login
NVIDIA Quadro RTX A4000 16GB GDDR6 Graphics Card
2000-Watt 80 PLUS® PLATINUM Certified Fully Modular PSU
Dual 32" LED UHD 4K Curved Monitor mount with independent extendable arms on chassis
Full HD Webcam with Autofocus mounted on an extendable arm
8-port SATA/SAS RAID Controller with 1GB Cache
Intel X540 Chipset 10G (2 x RJ45 ports)
Embedded RFID Reader
Embedded LD Wireless Charging
Suitable MCB switch protected with an acrylic door on the rear chassis

- Lapboard with Wireless Keyboard and Mouse with Backlit and built-in Lithium-ion USB-based Rechargeable battery.
- Toughened Glass with placement markings of wireless charging, RFID reader, and LED Dimmer logo for better understanding.

DESIGNED AND MAKE IN INDIA

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

FORENSIC ATTRIBUTION OF CYBER INCIDENTS

Author/Writer: Yugal Pathak

Email: yugalpathak2012@gmail.com, cyberyuvi4u@gmail.com

Abstract

In this digital world as cyber incidents grow, digital forensics establishes its importance in hindering the growth of these cyber threats by successfully uncovering attack vectors and helping build resilient infrastructure. Forensic attribution involves tracing and identifying the perpetrators behind cyberattacks. This comprehensive analysis not only helps determine the motives and techniques used by threat actors but also aids in developing targeted countermeasures and strengthening cybersecurity defenses. The ability to accurately attribute cyber incidents empowers organizations and authorities to take appropriate legal actions and fosters international cooperation in addressing cyber threats. This article emphasizes the significance of forensic attribution in the modern cybersecurity landscape, emphasizing its potential to enhance incident response, deter future attacks, and safeguard digital ecosystems.

Introduction to Digital Forensics and Evidence

The discipline of digital forensics is continually developing day by day. It can be described as the process of analyzing digital evidence that has been obtained, processed, and stored in a legally binding way, by combining legal knowledge with computer and information systems (IS). The emphasis on legal acceptability is because digital forensics is frequently employed for investigations that are focused on legal or law enforcement matters that likely end up in court.

Digital investigations, such as employee monitoring, can be carried out independently by an organization. Although handling the evidence in a legally acceptable manner (chain of custody) may not be necessary in such a case, such investigations may nonetheless open a can of worms: It's possible to discover something that calls for legal action, such as sabotage or fraud. In such a scenario, for evidence to be admissible in court, it must be collected and documented in a legally acceptable manner. Additionally, digital forensics can be very helpful in fraud investigations and audit investigations.

Digital evidence is very brittle and is prone to loss or manipulation. Therefore, it is important to handle and maintain digital evidence in a way that prevents its distortion or destruction less likely.

Cyber Kill Chain

The Cyber Kill Chain serves as a systematic model in the realm of cybersecurity, breaking down the phases of a cyber-attack into distinct stages. This granular breakdown allows cybersecurity professionals to better comprehend, detect, and counteract potential threats at various points within the attack lifecycle.

The standard stages within the Cyber Kill Chain are as follows:

1. **Reconnaissance**: This phase marks the initiation of an attack. Cyber adversaries engage in extensive data gathering activities to profile their intended target comprehensively. This information includes details such as IP addresses, network topologies, system configurations, and potential entry points. By accumulating this intelligence, attackers identify vulnerabilities and weak points within the target's infrastructure.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

2. **Exploit Development**: With reconnaissance completed, attackers move on to developing malicious payloads or exploits. These payloads are meticulously crafted to take advantage of known vulnerabilities in the target's software, applications, or systems. Concurrently, attackers devise a delivery mechanism to facilitate the introduction of the payload into the target environment.

3. **Delivery**: This stage involves the actual transmission of the malicious payload to the target. Attackers utilize a variety of tactics, including but not limited to phishing emails, weaponized attachments, deceptive links, drive-by downloads, or compromising legitimate websites. The objective here is to trick or manipulate the target into inadvertently executing the malicious code.

4. **Exploitation**: Once the malicious payload infiltrates the target system and executes, the attackers leverage it to exploit the identified vulnerabilities. Successful exploitation grants unauthorized access to the compromised system or network, establishing a foothold for further malicious activities.

5. **Installation**: To ensure persistent control and access, attackers proceed to install additional tools, backdoors, or malware within the compromised system. These components are designed to maintain their presence even if the initial infection is discovered and removed.

6. **Command and Control (C2)**: In the final stage, attackers establish a covert command and control infrastructure. This infrastructure allows them to remotely manage the compromised system, execute commands, exfiltrate data, and potentially launch additional attacks. The C2 channel often operates discreetly to evade detection.

What is a Cyber Security Incident?

A cyber security incident refers to any unauthorized or malicious activity that compromises the confidentiality, integrity, or availability of computer systems, networks, or data. These incidents can include data breaches, malware infections, phishing attacks, ransomware, and more. Responding swiftly to incidents is crucial to prevent further damage, protect sensitive information, and restore normal operations.

Incident response teams investigate, mitigate, and recover from the incident while implementing measures to prevent future occurrences. The continuous evolution of cyber threats requires organizations to stay vigilant, maintain robust security measures, and educate users to minimize the impact of potential incidents.

Incident response Cycle

The incident response cycle is a structured approach used by organizations to detect, respond to, and recover from cybersecurity incidents. It involves several stages with a strong emphasis on forensics to understand the nature and scope of the incident fully.

1. **Preparation**: Proactively establish an incident response plan, assemble a dedicated team, and implement necessary tools and processes for efficient incident handling.

2. **Detection and Identification:** Continuously monitor systems for signs of anomalies and potential incidents. Quickly identify and verify security breaches or suspicious activities.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

3. **Eradication:** Remove the root cause of the incident and eliminate any malicious code or unauthorized access.

4. **Recovery:** Restore affected systems to their normal state and verify their integrity.

5. **Lessons Learned:** Analyze the incident to understand its cause, impact, and how it was handled. Identify areas for improvement and update incident response procedures accordingly.

Is forensic attribution necessary?

Forensics plays a crucial role throughout the incident response cycle. It involves collecting, preserving, analyzing, and interpreting digital evidence to determine the incident's who, what, when, where, and how. Forensics helps investigators reconstruct the attack timeline, identify attackers, and gather evidence for potential legal actions. By conducting thorough digital investigations, organizations can enhance their incident response capabilities and strengthen their defenses against future incidents.

Chain Of Custody

Chain of custody—also known as "continuity of evidence"—is required to guarantee that digital evidence has been gathered, processed, handled, and stored with due care so that it cannot be inferred that it has been altered or destroyed. Chain of custody is the process of documenting how digital evidence is obtained, processed, handled, stored, and protected, as well as who handled the evidence and why—from the time it is collected to the time it is presented as an exhibit (such as in a court or board hearing).

Forensic tools and methods can be used by auditors to check for compliance with organizational policies and regulatory requirements. Digital forensics, for instance, can assist in locating and tracing employees' unauthorized Internet access, network flaws and vulnerabilities, and malware incidents like intrusions and attacks that can be analyzed to ascertain how the breach occurred and prevent future attacks. In order to avoid losing a case, having a forensic readiness plan in place goes a long way toward ensuring that such investigations and any findings can be handled and presented.

What Is Forensic Readiness?

Digital Forensic readiness is defined as the capability of an organization to effectively collect, preserve, protect, and analyze digital evidence in a forensically sound manner for use in legal proceedings, employment tribunals, and other court matters.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Others define forensic readiness as an organization's capacity to utilize digital evidence to its fullest extent in case of legal investigations.

Planning for forensic readiness is a component of a good information risk management strategy. It is necessary to identify and evaluate risk areas, and steps must be taken to avoid and reduce the impact of these risks. A forensic readiness plan would be easier to implement for businesses that already have a solid information security framework and risk assessment. The objectives of a forensic readiness plan should be as follows:

- To collect legally admissible evidence without interfering with business processes.
- To collect evidence aimed at potential crimes and disputes that could harm an organization.
- To allow investigations to proceed at costs proportional to the incident.
- To minimize operations disruption caused by investigations.
- To guarantee that evidence has a positive impact on the outcome of any legal action.

Forensic Readiness Implementation

A forensic readiness plan is designed to prepare an organization for unforeseen incidents and data losses. An organization should review and evaluate security—technical controls, policies, procedures, and skill sets—as part of its preparation. This can be done by a competent forensic investigator, who will be able to suggest the right modifications and steps to take to enhance what is already in place and guarantee a good forensic readiness plan.

The organization's goals and risk tolerance must be determined, the security posture must be assessed, employees must be educated on the forensic readiness plan, and an action plan must be developed to address gaps in the status quo. It is easier to determine what risks are significant or relevant, what kinds of incidents are to be expected, and how to respond to them when goals, objectives, and risk appetite are known. Then, the level of security that is in place should be looked at to see if it is adequate and to find any potential flaws. To ensure compliance, employees must be informed and educated about the forensic readiness plan. Finally, appropriate measures are taken to close any gaps that have been discovered.

Forensic Readiness Checklist

A forensic readiness checklist for an organization should include (but not be limited to) the following pointers:

- Define the scenarios in the business that would necessitate digital evidence. This simplifies where and how evidence is collected and stored.
- Determine the kinds of evidence and the sources of potential evidence.
- Determine the requirements and capability for secure, forensically sound evidence.
- Make a plan for the right chain of custody and appoint a specific point of contact for the escalation mechanism.
- Make sure that SIEM/ SOC/ security teams focus on major incident detection and deterrence.
- Describe the circumstances under which a full-scale formal digital investigation should be carried out.
- Staff members should be trained in incident response procedures so that they know their role in digital evidence processing and how important and sensitive it is in the event of an incident.
- Describe the incident and its impact in digital evidence-based cases.
- Ensure legal review to make it easier to take the right steps after an incident.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

While many businesses are aware of the significance of disaster recovery and business continuity plans, they must also acknowledge the significance of planning for forensic readiness. The tendency is to react quickly, waiting for an incident to take place before attempting to handle it and conducting investigations—collecting evidence after the fact.

Standards involved in Digital Evidence Management

1. ISO/IEC 27037:2012: It provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition, and preservation of potential digital evidence that can be of evidential value. It guides individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.
   Devices such as digital storage media used in standard computers like hard drives, floppy disks, optical and magneto-optical disks, data devices with similar functions; mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards; mobile navigation systems; digital still and video cameras (including CCTV); standard computer with network connections; networks based on TCP/IP and other digital protocols; and devices with similar functions as above.

2. ISO/IEC 27041:2015:It guides assuring the suitability and adequacy of the forensic methods used to investigate digital evidence, describing methods through which all stages of the investigation process can be shown to be appropriate (proper and suitable in themselves, and correctly performed).

3. ISO/IEC 27042:2015:It guides the standard evidential controls (maintaining the chain of custody, scrupulous documentation etc.), the standard emphasizes the integrity of the analytical and interpretational processes such that different investigators working on the same digital evidence ought to come up with essentially the same results - or at least any differences should be traceable to choices they made along the way. Given the volume, variety, and complexity of digital evidence these days, that's quite a challenge, hence the drive for standardization, good practices, common terminology and sound, rational approaches.

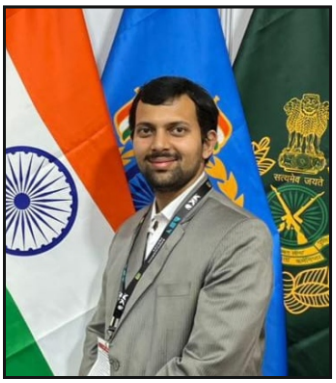
4. ISO/IEC 27043:2015: The fundamental purpose of the digital forensics standards ISO/IEC 27037, 27041, 27042 and 27043 is to promote good practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardization will (eventually) lead to the adoption of similar if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

Summary

Operations are disrupted as a result, some evidence may be altered or lost, and evidence may not be handled appropriately. These issues are greatly reduced by forensic readiness, especially since most of the necessary evidence is available before, during, and before the beginning of investigations. Due to constant monitoring and review, forensic readiness also helps ensure that employees comply with the organization's policies and regulatory requirements. Time and money are saved, potential incidents are reduced, business continuity and compliance are guaranteed, and operations are minimally disrupted.

References

1. https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness
2. https://www.sciencedirect.com/topics/computer-science/forensic-readiness
3. https://resources.infosecinstitute.com/topic/a-brief-introduction-to-forensic-readiness/
4. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf



ABOUT THE AUTHOR:

Mr. Yugal Pathak

Digital Forensic Researcher, SysTools Group
Email : yugalpathak2012@gmail.com,
cyberyuvi4u@gmail.com

Expertise:

Mr. Yugal Pathak is Cyber Security Researcher and he completed his Digital Forensic Internship at Cyber Forensics Lab, CERT-IN. He has experience of working with UP 100 Police, Developer for Creative Flakes Communications and other organizations and. He currently volunteers with many organizations including Kaspersky Cybermate, United Nation Peace Volunteer, Cyber Peace Foundation, eProtect Foundation, Udaan Foundation and local police.

eSec Forte®

DIGITAL FORENSICS

WE DO IT DIFFERENTLY

OUR CAPABILITIES

- FORENSIC LAB SETUP
- COMPUTER FORENSICS
- NETWORK FORENSICS
- MALWARE ANALYSIS
- MOBILE FORENSICS
- EMAIL FORENSIC SERVICES
- ADVANCED DIGITAL FORENSICS
- SOCIAL MEDIA MONITORING
- CDR & CELL SITE ANALYSIS
- DIGITAL FRAUD INVESTIGATION
- HARD DISK IMAGING SERVICES
- TAKEDOWN SERVICES
- THREAT INTELLIGENCE SERVICES
- INCIDENT & BREACH RESPONSE SERVICES

CAPACITY BUILDING

We impart training based on job profiles in addition to tool/technology based training.

First Responder	Lab Assistant	Lab Analyst / Examiner	Technical / Quality Manager	Expert Witness

FORENSIC CONSULTING

- Establishment/Upgradation of a Digital/Cyber Forensics Laboratory needs to be done with due thought process in adherence to global ISO/IEC standards and law of the land.
- In India IT Act under 79A mandates that government can notify labs as EEE (Examiner of Electronic Evidence) and Ministry of Information and Technology has a procedure which notifies government labs. **We at eSec Forte® Technologies will guide / consult / design lab provide services / provide products you need to meet the requirements so that your lab can be notified. We have all the experience and expertise to assist you.**

Lt Col (Dr.) Santosh Khadsare (Retd.)

VP-Digital Forensics and Incident Response (DFIR)

Drop a message at

forensics@esecforte.com

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

IMPORTANCE OF TRANSFER LEARNING IN DEEP LEARNING

Author/Writer: Nagaraj M. Lutimath

Email: nagarajlutimath@gmail.com

Article/Paper Highlights:

Transfer learning is a powerful technique used in Deep Learning. Deep learning is a subset of machine learning, which is essentially a neural network with three or more layers. These neural networks attempt to simulate the behaviour of the human brain. By harnessing the ability to reuse existing models and their knowledge of new problems, transfer learning has opened doors to training deep neural networks even with limited data. Transfer learning promotes Artificial Intelligence (AI) in less-developed application areas, as well as less technically developed geographical areas, even when not much-labelled data is available in such areas.

For example, suppose we wish to build a book recommendation system in a new online shopping application. Suppose that the book domain is so new that we do not have many transactions recorded in this domain. If we follow the supervised learning methodology in building a prediction model in which we use insufficient training data in the new domain, we cannot have a credible prediction model on users' next purchase. However, with transfer learning, one can look to a related, well-developed but different domain for help, such as an existing movie recommendation domain.

– Editorial Team, Digital Forensics (4N6)

Abstract

Exploiting transfer learning techniques, one can find the similarities and differences between the book and the movie domains. For example, some authors also turn their books into movies, and movies and books can attract similar user groups. Noticing these similarities can allow one to focus on adapting the new parts for the book recommendation task, which allows one to further exploit the underlying similarities between the data sets. Then, book domain classification and user preference learning models can be adapted from those of the movie domain.

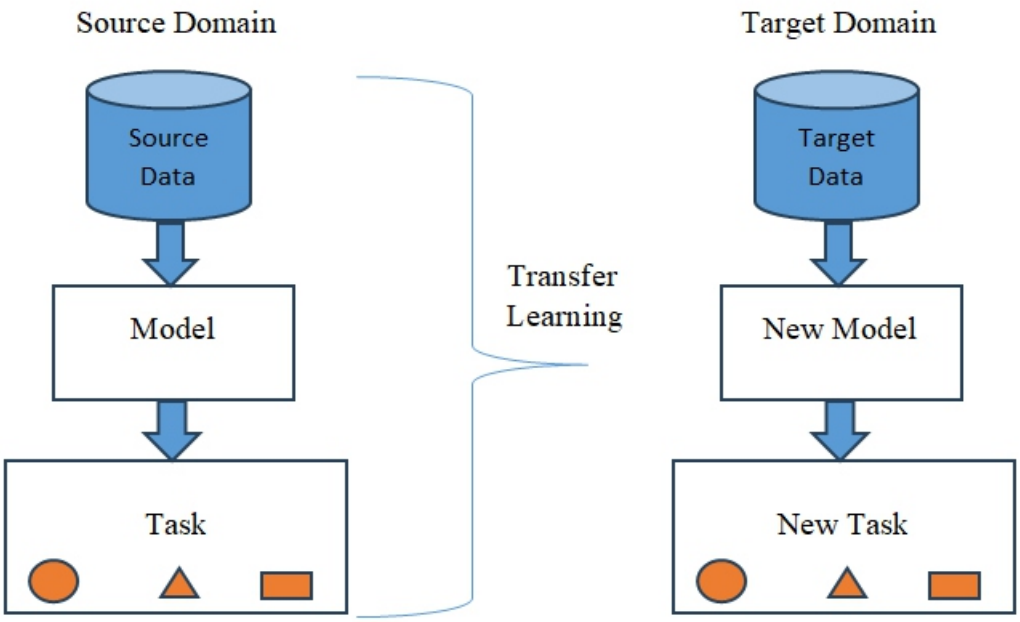
Based on the transfer learning methodologies, once we obtain a well-developed model in one domain, we can bring this model to benefit other similar domains. Hence, having an accurate "distance" measure between any task domains is necessary in developing a sound transfer learning methodology. If the distance between two domains is large, then we may not wish to apply transfer learning as the learning might turn out to produce a negative effect.

In machine learning, the distance between domains can often be measured in terms of the features that are used to describe the data. In image analysis, features can be pixels or patches in an image pattern, such as the colour or shape.

Introduction

In Natural Language Processing (NLP), features can be words or phrases. Once we know that two domains are close to each other, we can ensure that AI models can be propagated from the well-developed domains to less-developed domains, making the application of AI less data dependent. And this can be a good sign for successful transfer learning applications. Being able to transfer knowledge from one domain to another allows machine learning systems to extend their range of applicability beyond their original creation. This

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION



A transfer learning process is illustrated in Figure 1.1.

The process on the left corresponds to a traditional machine-learning process. The process on the right corresponds to a transfer learning process. As we can see, transfer learning makes use of not only the data in the target task domain as input to the learning algorithm but also any of the learning processes in the source domain, including the training data, models and task description. This figure shows a key concept of transfer learning: it counters the lack of training data problems in the target domain with more knowledge gained from the source domain.

When to transfer asks in which situations transferring skills should be done. Likewise, we are interested in knowing in which situations knowledge should not be transferred. In some situations, when the source domain and the target domain are not related to each other, brute-force transfer may be unsuccessful. In the worst case, it may even hurt the performance of learning in the target domain, a situation which is often referred to as negative transfer. Most current studies on transfer learning focus on "what to transfer" and "how to transfer," by implicitly assuming that the source domain and the target domain are related to each other. However, how to avoid negative transfer is an important open issue that is attracting more and more attention.

What to transfer determines which part of knowledge can be transferred across domains or tasks. Some knowledge is specific to individual domains or tasks, and some knowledge may be common between different domains such that they may help improve performance for the target domain or task.
Different answers to the question of "how to transfer" give a categorization for transfer learning algorithms as follows.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

1. In instance-based algorithms, the knowledge transferred corresponds to the weights attached to source instances;
2. In feature-based algorithms, the knowledge transferred corresponds to the subspace spanned by the features in the source and target domains;
3. In model-based algorithms, the knowledge to be transferred is embedded in part of the source domain models.
4. In relation-based algorithms, the knowledge to be transferred corresponds to rules specifying the relations between the entities in the source domain.

Transfer learning is typically employed in Computer Vision (CV) and Natural Language Processing (NLP) tasks. Both CV and NLP require large datasets and high computational power. Let's consider a CV task where you train a machine learning model to classify MRI images. You can retrain the same model to recognize images with other diseases, such as traumatic brain injuries or brain tumors. Thus, transfer learning helps achieve faster yet more accurate results.

1. **Natural language processing (NLP) -** Natural language processing refers to a system capable of comprehending and analyzing human language in audio or text files. The primary objective of NLP is to improve the quality of interaction between humans and machines. Day-to-day services such as voice assistants, speech recognition software, translations, and so on rely on NLP. Transfer learning strengthens ML models that handle NLP tasks. For example, transfer learning can be employed to train models simultaneously for detecting various language elements, specific dialects, phrases, or vocabularies. Moreover, transfer learning enables models to adapt to multiple languages. This implies that the models trained for the English language can be retrained and adapted to other similar languages or tasks. The knowledge of pre-trained models with the ability to recognize linguistic syntaxes can be transferred to other models that can predict the next word or phrase, considering the structure of previous sentences.
   For example, Google provides a 'Google Neural Translation Model (GNMT)' that is capable of cross-lingual translations. The model uses a pivot or common language between two discrete languages to accomplish the translation task. Let's say you intend to translate Russian to Korean. In this case, you must first transfer Russian to English and then English to Korean. At its core, the technique uses the data to learn the translation mechanism to better translate between a pair of languages.
2. **Computer vision (CV) -** Computer vision enables systems to derive meaning from visual data fed through images or videos. ML algorithms train on large datasets (images) and refine themselves to be able to recognize images or classify objects within the images. In such cases, transfer learning comes to the fore as it takes control of the reusable aspects of a CV algorithm and runs it on a newer model. Transfer learning can use models produced from large training datasets and apply them to smaller image sets. This can include determining the sharp edges of objects in the provided collection of images. Moreover, the layers that specifically identify edges in images can be determined and then trained based on the need.

3. **Neural networks (NN) -** Neural networks are key to deep learning as they are designed to simulate and replicate human brain functions. Training neural networks require a heavy load of resources due to the complexity of the models they tend to provide. Thus, transfer learning can be used here to reduce the resource demand and, at the same time, make the entire process more efficient. Several transferrable features are moved from one network to another to fine-tune the model development process. Knowledge application across tasks is of paramount importance in building neural nets.

References

[1] Qiang Yang, Hong Kong University of Science and Technology, Yu Zhang, Hong Kong University of Science and Technology, Wenyuan Dai, 4Paradigm Co., Ltd., Sinno Jialin Pan, Nanyang Technological University, Singapore, "Transfer Learning", Cambridge University Press, January 2020, Online ISBN:9781139061773.

[2] Paul Azunre, "Transfer Learning for Natural Language Processing", July 2021, ISBN 9781617297267.

[3[Zhi Yi, Yuyang Wang, "Transfer Learning on Interstitial Lung Disease Classification", proceeding in the 2021 International Conference on Signal Processing and Machine Learning (CONF-SPML), California, USA, 15th Feb 2021.

[4] Julius Godslove Femi; Ajit Kumar Nayak, "EQGTL: An Ensemble Model for Relevant Question Generation using Transfer Learning", in the proceedings of IEEE 2022 International Conference on Machine Learning, Computer Systems and Security (MLCSS), Bhubaneswar, India, 05th -06th Aug 2023.

[5] Shohei Chiba; Hisayuki Sasaoka, "Basic Study for Transfer Learning for Autonomous Driving in Car Race of Model Car ", in proceedings of IEEE 2021 6th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 20th-21st May 2021.

ABOUT THE AUTHOR:

Nagaraj M. Lutimath

Designation/Role: Associate Professor
College/Organization: Dayananda Sagar Academy of Technology and Management

Place: Bengaluru

Expertise: Artificial Intelligence, Machine Learning, Deep Learning, Image Processing, Transfer Learning

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Credentials:

Dr. Nagaraj M. Lutimath was born in Belagavi on 23rd July 1974.He completed BE in Computer Science and Engineering from Basaveshwar Engineering College Bagalkot in 1998 and MTech in Computer Science and Engineering from Basaveshwar Engineering College Bagalkot in 2007. He completed his PhD from VTU, Belagavi in July 2018. He is a guiding research scholar for PhD. He has worked in many reputed engineering colleges. Some of those colleges are Basaveshwar Engineering College, Bagalkot, Sambhram Institute of Technology, Bangalore and Rajiv Gandhi Institute of Technology, Bangalore.

He has published more than 40 research publications both in International Conferences and International Journals. He has conducted many workshops on R and data analytics and Network simulations. He worked as the session chair and reviewer of many international conferences and international journals. He is also a reviewer of International Journal of Engineering, Science and Technology, Elsevier Publisher. He has attended many seminars, workshops and conferences to enhance his knowledge.

He has received s Gurukul Academic Award for the “Best Research Paper'', at the International Award Conference on Multidisciplinary Research and Latest Innovation, 20th Nov 2022, Organized by J S University, Mainpuri, Shikohabad, Institute for Social Reforms and Higher Education Charitable Trust, Uttar Pradesh, India. Regd. NITI Aayog and Savitri Bai Phule Excellence Award for the “Savitri Bai Excellence Award-2022 for Best Researcher”, at the International Award Conference on Social Reforms and Higher Education, 17th Dec 2022, Organized by KJEI’s Trinity College of Engineering, Pune, India, Institute for Social Reforms and Higher Education Charitable Trust, Uttar Pradesh, India. Regd. NITI Aayog. He has worked as the Associate Professor in the department of Computer Science and Engineering, Sri Venkateshwara College of Engineering, Bangalore. Currently an Associate Professor in the department of Information Science and Engineering, East Point College of Engineering and Technology, Bengaluru. He is currently working as Associate Professor, Dayananda Academy of Technology in the department of Computer Science and Engineering.

SkillsDA®
Center for advance training

DIGITAL FORENSICS AND INCIDENT RESPONSE

COMPUTER FORENSICS

our Computer Forensics service provides expert analysis by utilizing advanced techniques in file system analysis, artifact recovery, and digital evidence preservation.

IMAGE & VIDEO FORENSICS

Image & Video enhancement, forgery detection, and metadata analysis, our Image & Video Forensics service authenticates and analyzes digital media, for legal and investigative needs.

MOBILE FORENSICS

Mobile Forensics service retrieves crucial information such as Deleted Data, SMS, call logs, and geolocation data, multimedia files offering insights.

DATA RETRIVAL

Our service salvages vital information from damaged or inaccessible storage media using specialized hardware and software techniques.

MEMORY FORENSICS

Through in-depth examination of volatile memory, our our service uncovers hidden digital evidence, revealing running processes and malware artifacts, essential for cybersecurity analysis and threat mitigation.

MALWARE FORENSICS

By dissecting malicious code, tracking origins, and employing reverse engineering, our Malware Forensics service fortifies systems against digital threats, safeguarding data and infrastructure.

NETWORK FORENSICS

Through meticulous examination,we enables organizations to capture, record, and analyze network traffic, uncovering patterns & anomalies that may indicate misconduct or unauthorized activity

INCIDENT RESPONSE

Offering a swift and coordinated approach to security breaches and cyber attacks, our Incident Response service neutralizes threats, minimizes damage, and restores systems efficiently, adhering to legal and regulatory compliance requirements.

Powered By:
INGU'S KNOWLEDGE ACADEMY PVT LTD
forensics@skillsda.com

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

LEVERAGING ARTIFICIAL INTELLIGENCE FOR ADVANCEMENTS IN DIGITAL FORENSICS

Author/Writer: **Ria Mahale**

Introduction

Digital forensics plays a crucial role in modern law enforcement, cybersecurity, and civil litigation, involving the preservation, analysis, and presentation of electronic evidence. Digital forensics is the process of collecting, analyzing, and preserving digital evidence in order to investigate and solve crimes. With the increasing amount of digital data being generated every day, digital forensics has become an essential part of modern law enforcement. However, the sheer volume of data can make it difficult for investigators to find relevant evidence and draw meaningful conclusions. This is where artificial intelligence (AI) comes in. AI can help automate and streamline the digital forensics process, making it faster and more efficient.

Problem Statement:

The digital forensics field faces several challenges, including the following:

- Traditional forensic methods are often inadequate to deal with modern digital devices and applications.
- The evolving threat landscape necessitates real-time detection and proactive measures.
- Ensuring the privacy and ethical handling of digital evidence is crucial.

Objectives:

The primary objectives include:

- Exploring AI-based digital forensic techniques and their applications.
- Investigating the benefits of AI in digital forensics, including improved efficiency and enhanced investigative capabilities.
- Discussing ethical and legal considerations associated with AI in digital forensics.
- Presenting case studies highlighting successful AI implementations.
- Identifying challenges and limitations of AI-powered digital forensics.
- Speculating on future directions and advancements in the field.

Literature Review:

Traditional Digital Forensics

Traditional digital forensics is an essential part of digital investigations, as it allows investigators to identify, preserve, and analyze evidence from digital devices and data. It typically relies on human expertise and established methodologies, such as using hash values to verify data integrity and signature-based detection to analyze malware. However, these techniques are limited in their ability to keep up with the rapid technological advances and increasing complexity of digital investigations. As a result, digital forensics is evolving to incorporate new technologies and techniques, such as machine learning and data analytics, to more efficiently and effectively identify potential evidence and assist in investigations.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Challenges in Traditional Forensics

Digital forensics, as a discipline, has been instrumental in investigating cybercrimes and securing digital evidence for legal proceedings. However, it faces several significant challenges in today's rapidly evolving digital landscape:

- **Data Volume and Complexity:** One of the foremost challenges is the sheer volume and complexity of digital data. With the exponential growth of digital devices and the internet, the amount of data generated daily is staggering. Digital forensics experts often deal with terabytes or even petabytes of data in a single case. This sheer volume makes it increasingly challenging to process, analyze, and store the data efficiently. Traditional forensics tools and methodologies struggle to keep up with this data deluge.

- **Evolving Threat Landscape:** Cybercriminals constantly adapt and develop new techniques to evade detection and forensic analysis. They employ sophisticated malware, encryption, and anonymization methods, making it harder for investigators to attribute attacks to specific individuals or groups. This cat-and-mouse game requires forensic experts to stay updated on the latest cyber threats and develop new investigative techniques.

- **Resource Intensity:** Traditional digital forensics is a resource-intensive process. It requires highly trained personnel with specialized skills and tools. Investigations often take a significant amount of time, leading to backlogs in cases. Law enforcement agencies and organizations need to allocate substantial human and financial resources to maintain effective digital forensics capabilities.

- **Data Encryption**: Encryption technologies have become widespread, enhancing data security but posing challenges for digital forensics. Encrypted data is inaccessible without the encryption keys, making it difficult to retrieve evidence from encrypted devices or communications. Investigative agencies must develop new methods for lawful access to encrypted data while respecting privacy rights.

- **Multimodal Data:** Digital forensics now involves analyzing diverse data types, including text, images, videos, audio recordings, and data from IoT devices. Each data type presents unique challenges and requires specialized tools and expertise. The integration of these data sources to reconstruct events or establish facts adds another layer of complexity to investigations.

AI in Digital Forensics:

Artificial intelligence (AI) has emerged as a promising solution to address the challenges of traditional digital forensics. AI encompasses machine learning, natural language processing (NLP), computer vision, and deep learning techniques that can analyze vast datasets, detect anomalies, and identify patterns not easily discernible by humans. AI-powered digital forensics leverages these capabilities to automate processes, expedite investigations, and enhance accuracy. Machine learning, for example, can automate the analysis of digital evidence and help investigators identify patterns and relationships. Data analytics can analyze large datasets to uncover insights and patterns that may be difficult for humans to detect. Signature-less detection algorithms can detect malware without relying on traditional signatures. Advanced decryption techniques are being developed to gain access to encrypted evidence. Finally, new methods are being developed to analyze data from IoT devices and other non-traditional sources.

AI Applications in Digital Forensics:

Artificial Intelligence (AI) has emerged as a powerful tool in the field of digital forensics, offering innovative solutions to address the challenges posed by the evolving digital landscape. Here, we provide a more detailed overview of AI's role in digital forensics:

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Automating Repetitive Tasks: AI, particularly machine learning techniques, is well-suited for automating repetitive and time-consuming tasks in digital forensics. For instance, AI algorithms can be trained to categorize and sort digital evidence, such as images, videos, or documents, based on predefined criteria. This automation significantly reduces the manual effort required for evidence organization and cataloging.

Pattern Recognition: AI excels at recognizing patterns within large datasets. In digital forensics, this capability is invaluable for identifying anomalies and suspicious activities. Machine learning models can be trained to recognize patterns associated with specific cyber threats or criminal behaviors. For example, AI can detect unusual network traffic patterns that might indicate a security breach or identify trends in financial transactions that suggest fraudulent activity.

Real-time Monitoring and Alerting: AI-driven systems can provide real-time monitoring of digital systems and networks. These systems continuously analyze data streams, looking for signs of unauthorized access, malware infections, or other security breaches. When suspicious activities are detected, AI can trigger alerts, enabling rapid response by cybersecurity teams or forensic experts. This real-time monitoring enhances the proactive defense against cyber threats.

Signature-Based Detection: Signature-based detection involves comparing the digital artifacts of files or code to known signatures of malicious software. Machine learning models can automate this process and identify variants of malware.

Data Extraction and Parsing: Natural Language Processing (NLP) and computer vision, subsets of AI, can be applied to extract and parse data from unstructured sources such as text documents, emails, or multimedia files. NLP techniques enable the automated extraction of text content, sentiment analysis, and authorship attribution, which can be crucial in email investigations and social media analysis. Computer vision is employed to analyze images and videos, identifying objects, faces, and relevant visual information.

Deep Learning for Complex Tasks: Deep learning, a subfield of AI, has demonstrated remarkable success in solving complex tasks in digital forensics. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), among others, can be applied to image and video analysis, text processing, and network traffic analysis. For example, CNNs can identify objects or faces in images, while RNNs can analyze sequences of network packets to detect intrusion attempts or malicious activities.

Natural Language Processing (NLP): NLP techniques are employed in digital forensics to analyze textual data from sources such as emails, chat logs, and social media. NLP can identify relevant keywords, sentiment analysis, and authorship attribution.

IoT Device Forensics: The Internet of Things (IoT) introduces new challenges in digital forensics due to the vast number of interconnected devices generating data. AI can be applied to analyze data from IoT devices, reconstruct events, and identify security breaches. Machine learning models can process sensor data from IoT devices to identify patterns indicative of unauthorized access or tampering.

Challenges and Limitations:

The integration of artificial intelligence (AI) in digital forensics brings significant benefits but also presents several challenges and limitations that need to be carefully considered:

Data Quality and Availability:
Challenge: AI models require high-quality data for training and analysis. Inaccurate, incomplete, or tampered data can lead to biased or unreliable results. Ensuring the integrity and authenticity of digital evidence is crucial.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Consideration: Organizations must invest in data quality assurance measures, including data validation, preservation of the chain of custody, and secure storage to maintain the integrity of digital evidence.

Resource Requirements:

Challenge: Implementing AI in digital forensics may demand substantial computational resources, including high-performance hardware and data storage. Smaller organizations with limited resources may face challenges in adopting AI.

Consideration: Resource allocation, including hardware and skilled personnel, must be carefully planned to ensure the effective deployment of AI tools in digital forensics.

Explainability and Interpretability:
Challenge: AI models, particularly deep learning models, can be highly complex and difficult to interpret. Understanding why a model makes a specific decision, especially in critical forensic scenarios, can be challenging.
Consideration: Efforts should be made to develop explainable AI techniques that provide insights into the model's decision-making process. Ensuring that forensic experts can understand and trust AI-generated results is essential.

Adaptation to Evolving Threats:
Challenge: Cyber threats are constantly evolving, with new malware variants, attack techniques, and evasion tactics emerging regularly. AI models need to adapt and evolve to effectively counter these threats.
Consideration: Continuous training and updating of AI models, along with staying informed about the latest cyber threats, are essential to maintaining the effectiveness of AI-driven forensic tools.

Human Expertise and Training:
Challenge: While AI can automate many tasks, human expertise remains irreplaceable in making critical decisions, interpreting results, and conducting in-depth forensic analysis.
Consideration: Forensic experts should receive training and education on AI technologies to effectively integrate AI into their workflows. Collaboration between AI experts and forensic professionals is essential to develop AI-driven tools that align with investigative needs.

Ethical Considerations:
Challenge: The use of AI in digital forensics raises ethical concerns related to privacy, bias, fairness, and transparency. Balancing the need for investigation with individual privacy rights is a fundamental challenge.
Consideration: Policymakers, legal experts, and forensic practitioners must work together to establish ethical guidelines and legal frameworks that address the responsible use of AI in digital forensics while respecting privacy and human rights.

Legal Considerations:
Challenge: The admissibility of AI-generated evidence in court proceedings may face legal challenges. Establishing the reliability and validity of AI-derived findings is essential for their acceptance in legal contexts.
Consideration: Legal frameworks may need to adapt to accommodate the use of AI-generated evidence, and guidelines for presenting AI-derived findings in court should be developed and adhered to.

Future Directions:

The field of digital forensics continues to evolve rapidly, driven by advancements in technology and the increasing complexity of cybercrimes. The integration of artificial intelligence (AI) in digital forensics holds great promise, and future directions in this domain are essential for staying ahead of cyber threats and enhancing investigative capabilities. Here are some key areas of focus for the future:

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

AI and Quantum Computing:
Advancements: Quantum computing is a rapidly developing field that has the potential to disrupt existing cryptographic methods and pose new challenges to digital forensics. On the other hand, quantum computing itself can be harnessed to accelerate certain AI algorithms, enabling faster data analysis and pattern recognition.
Implications: Future digital forensic experts and AI practitioners will need to stay informed about quantum computing developments and explore how to adapt AI techniques to secure digital evidence in a post-quantum world.

Federated Learning for Privacy-Preserving Forensics:
Advancements: Federated learning allows AI models to be trained on decentralized data sources without sharing sensitive information. This approach preserves privacy while enabling collaborative AI models for forensic analysis.
Implications: Federated learning can enhance privacy in digital forensics investigations, especially when dealing with sensitive personal or corporate data. Future directions involve the development of federated learning frameworks tailored to forensic applications.

AI-Driven Predictive Digital Forensics:
Advancements: Predictive analytics can be employed to anticipate cyber threats and vulnerabilities. AI models can continuously monitor digital systems and networks, identifying potential threats before they materialize.
Implications: Predictive digital forensics can enable proactive measures to prevent cyber incidents rather than reacting to them after the fact. This paradigm shift can significantly enhance cybersecurity strategies.

Advancements in Explainable AI:
Advancements: Addressing the challenge of AI model explainability is an ongoing area of research. Future advancements aim to make AI models more transparent and interpretable, ensuring that forensic experts can understand and trust AI-generated results.
Implications: Improved explainability in AI models will lead to better integration into forensic workflows, as experts can confidently use AI-generated insights in their investigations while maintaining a high level of transparency and accountability.

Conclusion:

Summary

The integration of artificial intelligence (AI) into digital forensics represents a pivotal development in the field, offering a range of benefits to enhance investigative capabilities and address the evolving challenges posed by cybercrimes. The key takeaways and implications of this research paper can be summarized as follows:

- AI technologies, including machine learning, deep learning, and natural language processing, offer significant promise in enhancing digital forensics.
- AI automation enhances efficiency by handling repetitive tasks, allowing human experts to focus on more complex aspects of investigations.
- AI-powered data analysis enables the identification of patterns and anomalies that may be challenging to detect manually.
- Real-time monitoring and detection capabilities empower organizations to respond rapidly to cyber incidents.
- AI solutions are scalable, making them adaptable to the dynamic nature of digital investigations.

Implications and Recommendations:

As AI continues to play an increasingly prominent role in digital forensics, several implications and recommendations arise:

- Organizations should prioritize ethical considerations, ensuring that AI-driven forensic processes respect individual privacy rights and are free from bias or discrimination.
- Collaboration between AI experts and forensic professionals should be fostered, encouraging interdisciplinary teams to develop AI tools tailored to forensic requirements.
- Training and education programs should be established to upskill forensic experts and AI practitioners, ensuring that they can effectively leverage AI technologies.
- Policymakers should work to adapt legal frameworks to accommodate the use of AI-derived evidence, ensuring that the reliability and validity of such evidence are established.

Final Thoughts:

The integration of artificial intelligence in digital forensics holds immense potential for combating cybercrimes, enhancing digital security, and safeguarding digital spaces. While challenges related to data quality, resource allocation, transparency, and legal considerations persist, the benefits are profound.

The future of digital forensics is closely intertwined with AI, and as AI technologies continue to evolve, so too will the capabilities of forensic experts. Through responsible and innovative use of AI, digital forensics will continue to evolve and adapt to the dynamic and evolving landscape of cyber threats.

In summary, AI in digital forensics is not just a technological advancement; it represents a transformative shift in how investigations are conducted and evidence is analyzed. With thoughtful consideration of ethical, legal, and practical aspects, AI can empower forensic experts to address the complex challenges of our digital age effectively.

References:

1. Casey, E. (2018). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
2. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7(1-2),
3. Nelson, B., & Phillips, A. (2009). Guide to computer forensics and investigations. Cengage Learning.
4. Abomhara, M., & Koien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders, and attacks. Journal of Cyber Security.
5. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137-144.
6. Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1). MIT press Cambridge.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

ABOUT THE AUTHOR:

Ria Mahale

Security Culture Strategist,

Culsight (An Initiative by CyberFrat)

Expertise:

Ria is a seasoned professional with a unique blend of technical expertise, strategic vision, and commitment to excellence, she is a driving force in the dynamic fields of Security Awareness Practice, Cyber Risk & Analytics. As the Security Culture Strategist at Culsight, she assists diverse organisations in comprehending the necessity of security awareness, fostering a robust security culture through tailored content, motion graphics, comic strips, posters, and gamification.

Ria is at the forefront of Culsight mission to fortify organizations to build a security culture and also address the aftermath of human firewall failures and design tabletop exercises for senior management. She leads efforts to guide and empower individuals and organizations, fostering a cybersecure culture that's resilient in the face of ever-evolving digital challenges bolstering organizational resilience.

DRONA SERIES By eSec Forte

eSec Forte®

FORENSIC WORKSTATION SERIES

Developed to handle complex digital forensics processing and analysis and designed to ensure ease in operability.

PRODUCT DATASHEET

- **Biometric Access**
- **Persistent Memory**
- **Intel Dual Xeon Motherboard / AMD Dual EPYC compatible chipset**
- **1080p FHD Webcam with Autofocus**
- **27" LED FHD with Built-in Speakers mounted on Chassis**
- **20-Bay Proprietary Extended Frontal Cabinet with F-Mount**

Product Origin India

Technical Specifications

Model	EF-BEWS (BASIC)	EF-MEWS (MEDIUM)	EF-HEWS (HIGH END)
Series	Drona Series - I	Drona Series - P	Drona - X
Power Supply	Upto 1000W Modular	Upto 1600 Watts Fully Modular PSU	Upto 2200 Watts RPS
Cabinet	12-Bay Proprietary Cabinet	16-Bay Proprietary Extended Frontal Cabinet with F-Mount	20-Bay Proprietary Extended Frontal Cabinet with F-Mount
Chipset	Intel Z690 / AMD TRX40	Intel Xeon W or Dual Scalable Silver Series / AMD WRX80	Intel Dual Xeon Motherboard / AMD Dual EPYC compatible chipset
Processor	Intel Core i9 series / AMD Thread Ripper 3970 series	Intel Xeon W-3300 / AMD Thread Ripper 3990 series	Intel Xeon Scalable Gold or Platinum Series / AMD EPYC 7003 Series
No. of cores	Upto 16cores / Upto 32 cores	Upto 38 cores / Upto 64 cores	Upto 40cores / Upto 64 cores
RAM	Upto 256GB Non-ECC RAM	Upto 512 GB ECC RAM	Upto 4TB ECC RAM
OS Drive	500GB SATA SSD	1TB SATA SSD Plus / Pro Series	960GB Enterprise SATA SSD
Cache Drive	500GB NVMe M.2 SSD	1TB NVMe M.2 SSD Plus / Pro Series	960GB Enterprise NVMe M.2 SSD
Processing Drive	---	2TB NVMe NVMe M.2 SSD Plus / Pro Series	2 x 1.92TB Enterprise M.2 / U.2 SSD in RAID 0
Data Drive	4TB SATA HDD	12TB SATA Enterprise HDD in RAID 5 (4 x 4TB)	24TB SASIII/SATAIII Enterprise HDD in RAID 5 (4 x 8 TB)
Graphics Memory	6GB GDDR6	8GB GDDR6	14GB GDDR6
Standard HDD Bays	4 x 3.5" Removable 6Gbps HDD Hot-Swap Bays (compatible for SAS and SATA drives)		
	1 x 3.5" Removable IDE HDD Bay (optional)		
	1 x 3.5" Removable 68-pin SCSI HDD Bay (optional)		

Technical Specification

Model	EF-BEWS (BASIC)	EF-MEWS (MEDIUM)	EF-HEWS (HIGH END)
Series	**Drona Series - I**	**Drona Series - P**	**Drona - X**
Enterprise 12Gbps HD Mini-SAS Bays (Forensic)	---	4 x 3.5" Removable 12Gbps HD Mini-SAS HDD Hot-Swap Bays (Write Protected)	
	---	4 x 3.5" Removable 12Gbps HD Mini-SAS HDD Hot-Swap Bays (Read / Write)	
Forensic Card Reader	Supports read-only access to CF/UDMA, SDHC / SDXC, MicroSD, MS / DUO		
Forensic Bridge	5.25" Integrated Forensic Bridge with SAS/SATA/Firewire/USB/PCIe interfaces		
Ventilation Tray	Integrated Retractable Ventilation Tray with non-skid surface with dual performance fans along with auto on/off feature		
RAID Controller	---	8-port RAID Controller with 1GB Cache	8-port RAID Controller with 2GB Cache compatible with CacheVault supporting super capacitors
DVD Writer	Standard DVD Writer	Blue-Ray DVD Writer	Blue-Ray DVD Writer
Integrated System Security	---	Biometric System Power On	Biometric System Power On
Chassis KeyLock	Yes	Yes	Yes
Integrated System Performance Monitor	---	3.5" LCD For Performance Monitoring, System Info & Admin Control	3.5" LCD For Performance Monitoring, System Info & Admin Control
Integrated Biometric OS Login	---	---	Yes
Ports			
BackPanel USB (Rear)	4 x USB 3.2 Gen 1, 1 x USB 3.2 Gen (2 x2) / 3 x USB 3.2 Gen 2 / 4 x USB 3.2 Gen 2 & 6 x USB 3.2 Gen 1	6 x USB 3.2 Gen 2, 1 x 3.2 Gen 2 (2x2), 2 x 3.2 Gen 2, 4 x USB 2.0 / 6 x USB 3.2 Gen 1	6 x USB 3.2 Gen 1, 2 x USB 3.2 Gen 2 / 2 x USB 2.0, 4 x USB 3.0
Standard USB Bay (Lower Side Panel)	---	4-port USB 3.1 Gen 1 bay for charging phones	8-port USB 3.1 Gen 1 bay for charging phones
Rapid USB Bay (Lower Side Panel)	---	2-port USB 3.2 Gen 2 bay for rapid data transfer and charging (1 x Type A, 1 x Type C)	4-port USB 3.2 Gen 2 bay for rapid data transfer and charging (1 x Type A, 1 x Type C)
Bluetooth & Wifi	Dual- Band Wifi & Bluetooth 5.0		
Ethernet			
Gigabit NIC	Yes	Yes	---
10Gbps NIC	---	Yes	Yes
Fibre Channel NIC	---	---	Yes
Integrated Wireless Charging for mobile	---	Yes	Yes
System Integrated Webcam	---	720p HD Webcam	1080p FHD Webcam with Autofocus
System Cooling			
Air Cooling/Liquid Cooling	Compatible	Compatible	Compatible
Performance Cooling compatible	---	Compatible	
Standard System Peripherals	Membrane Keyboard & Mouse with backlit		Membrane Keyboard & Mouse with backlit embedded in Lapboard
Advanced System Peripherals	---	---	15-point Jog Shuttler embedded in lapboard (optional)
Audio	8-channel		
Remote Management	---	IPMI 2.0	
Adapter kits	PCIe Card SSD Adapter, PCIe M.2 SSD Adapter, PCIe Adapter for Apple SSD, PCIe U.2 SSD Adapter, Apple 2016+ PCIe SSD Adapter, 4" PCIe cable and Drive Adapter Kit		
Dimensions (W x H x D) in inches	30" x 28" x 12"	30" x 28" x 12"	30" x 28" x 12"

New Delhi
A-2/10, A-2 Block, Rohini Sector- 5, New Delhi – 110085

Gurugram
Plot No. 285, 2nd & 3rd Floor, Udyog Vihar, Phase- IV, Gurugram, 122015

Mumbai
Plot C-59, Bandra Kurla Complex, Bandra East, Mumbai – 400051

Bangalore
143, 3rd Floor, 10 th Cross, Indiranagar 1 st stage, Bangalore – 560038

Singapore
1 North Bridge Road, # 11-10, High Street Centre, Singapore - 179094

Sri Lanka
Level 26 & 34, East Tower, World Trade Center, Echelon Square, Colombo, 00100, Sri Lanka

Tel: +91 124 4264666 **Mail:** contact@esecforte.com **Web:** www.esecforte.com

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

USING ARTIFICIAL INTELLIGENCE TO IMPROVE DIGITAL FORENSICS

Author/Writer: Akash Mishra

Email: akash_mishra@mallareddyuniversity.ac.in, aaksmishra@gmail.com

Abstract

The integration of Artificial Intelligence (AI) and Machine Learning (ML) in digital forensics has revolutionized investigative processes, offering significant efficiency gains. This abstract explores the multifaceted impact of AI on digital forensics, where it automates tasks like data analysis, evidence prioritization, and anomaly detection, resulting in substantial time and resource savings. Despite its advantages in addressing challenges related to data volume, encryption barriers, and evolving technology, AI introduces limitations such as the lack of human intuition, algorithmic biases, ethical concerns, high implementation costs, and uncertainties in legal admissibility. A collaborative approach, combining AI with human expertise, is crucial for responsible implementation. Transparency, adherence to ethical standards, and ongoing collaboration between digital forensic specialists and legal professionals are vital components in navigating these challenges and ensuring the ethical use of AI in digital forensics.

Keywords – Artificial Intelligence (AI), Digital Forensic, Investigation, Machine Learning (ML), Digital Evidence, Pattern Recognition, Link Analysis, Data Privacy, Legal Considerations, Natural Language Processing (NLP)

Introduction: Artificial Intelligence (AI) is a field that aims to create machines that can mimic human intelligence. This involves developing computer systems and algorithms that can think, learn, and behave like humans. One subset of AI is Machine Learning (ML), which allows computer systems to learn from experience without being explicitly programmed.

AI and ML play a crucial role in digital forensics, which involves analysing digital devices and materials to gather evidence related to criminal activities. These technologies offer significant benefits to investigators, as they can automate various processes, flag relevant content, and predict potential threats.
With the help of AI and ML algorithms, investigators can quickly sift through large volumes of data, identify patterns, and categorize and prioritize data, saving time and effort. ML algorithms can analyse historical data, identify patterns associated with malicious activities, and generate predictive models to anticipate future threats, allowing investigators to take preventive measures.

AI and ML can also assist in anomaly detection by learning the normal behaviour of a system or network and identifying deviations from that behaviour. By automatically flagging anomalies, investigators can focus their attention on potentially suspicious activities and respond swiftly and effectively to security incidents.
Overall, AI and ML technologies enhance the efficiency and effectiveness of investigations, allowing investigators to uncover evidence quickly and proactively identify security risks. This empowers digital forensics investigators to protect digital systems, mitigate risks, and ensure a safer digital environment.

Digital Forensics and associated Challenges

Digital forensics is a branch of science that focuses on protecting computer systems and the data associated with them. It involves collecting and analysing evidence to determine the cause of an attack and identify the specific part of the system that was targeted. Technology has advanced to the point that we can now use leading technology to predict future threats and enhance our security measures. The main purpose of digital forensics is to protect systems by gathering evidence and analysing it for future reference

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Digital forensics faces several challenges that can complicate the investigation and analysis of digital evidence. Here are some of the key challenges in digital forensics:

Volume and Complexity of Data: The increasing volume and complexity of digital data pose a significant challenge for investigators. With the proliferation of digital devices and storage media, such as computers, smartphones, cloud services, and IoT devices, the amount of data that needs to be processed and analysed is immense. Dealing with large datasets and various data formats can overwhelm investigators and lead to delays in the investigation process.

Data Heterogeneity: Digital evidence comes in various formats, including documents, emails, images, videos, social media posts, and network traffic. Each format requires specific tools and techniques for analysis, and interoperability issues between different software and hardware platforms can hinder data extraction and interpretation.

Encryption and Security Measures: Encryption and security measures employed by individuals and organizations can make it difficult for investigators to access and decrypt digital evidence. Encrypted data and password-protected devices may require sophisticated techniques or cooperation from involved parties to overcome these barriers.

Anti-Forensic Techniques: Perpetrators may employ anti-forensic techniques to hide or destroy digital evidence. These techniques include data wiping, file fragmentation, steganography (hiding data within other files), encryption, and the use of anonymization tools or services. Detecting and recovering evidence that has been deliberately obfuscated or manipulated requires advanced forensic skills and specialized tools.

Rapidly Evolving Technology: Technology is continually evolving, introducing new devices, software, communication protocols, and storage methods. Staying up to date with the latest technological advancements and understanding their forensic implications is a constant challenge for digital forensic investigators. They need to adapt their skills, techniques, and tools to effectively investigate evidence from emerging technologies.

Data Privacy and Legal Considerations: Digital forensics investigations often involve sensitive personal information and require adherence to strict legal and ethical guidelines. Investigators must navigate complex privacy laws, data protection regulations, and jurisdictional issues to ensure the admissibility and integrity of digital evidence. Balancing the need for investigation with respect for privacy rights can be challenging.

Timeliness: In some cases, digital forensic investigations need to be conducted quickly to prevent the loss or destruction of evidence. This is particularly relevant in incidents involving cybercrime, where evidence can be transient and easily altered. Investigators need to work efficiently to collect, preserve, and analyse digital evidence promptly.

Applications of AI in Digital Forensics

AI can assist digital forensic specialists in several key ways, including automating data analysis, prioritizing evidence, analysing textual and visual data, detecting patterns and relationships, identifying anomalies, generating predictive models, and automating repetitive tasks.

Automated Data Analysis: AI enables automated data analysis, allowing for the rapid and efficient analysis of large volumes of digital data. By automating this process, AI algorithms can sift through various types of structured and unstructured data, including emails, documents, chat logs, and social media posts. Through this analysis, AI can identify patterns, correlations, and anomalies in the data. This capability helps forensic specialists by allowing them to focus their efforts on relevant and potentially incriminating evidence, ultimately saving valuable time and resources.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Digital Evidence Triage: AI-powered tools in digital forensics can perform initial triage on digital evidence, prioritizing and categorizing data based on its relevance and potential significance to an investigation. Using AI algorithms, these tools can flag suspicious files, images, or communication patterns, enabling investigators to prioritize their examination and focus on the most critical pieces of evidence first. This automated triage process saves time and helps investigators efficiently allocate their resources to areas of highest importance, enhancing the overall effectiveness of the investigation.

Language and Image Processing: AI techniques, including natural language processing (NLP) and computer vision, play a crucial role in analysing textual and visual evidence in digital forensics. NLP enables the analysis of text-based communications, such as emails or chat conversations, by extracting relevant information, detecting sentiment, and identifying keywords associated with criminal activities. This helps investigators uncover hidden insights and understand the context of the communication. On the other hand, computer vision algorithms can analyse images or videos to identify objects, faces, or scenes that are relevant to an investigation, providing valuable visual evidence. By leveraging these AI techniques, forensic specialists can extract meaningful information from textual and visual data, assisting them in building a comprehensive understanding of the case.

Pattern Recognition and Link Analysis - AI algorithms are capable of analysing vast amounts of digital evidence and identifying patterns and relationships that may not be immediately apparent to human investigators. By processing data from multiple sources, AI can connect seemingly unrelated pieces of information, helping to establish links between individuals, entities, or events. This ability to uncover hidden connections can be instrumental in identifying networks of criminals, understanding their methods of operation, and gaining insights into the broader context of criminal activity. AI's capacity to analyse data from various angles and make connections that humans might overlook significantly enhances the investigative process in digital forensics.

Anomaly Detection: AI can be instrumental in detecting anomalies in digital data, which can serve as indicators of unauthorized access, malicious activities, or data tampering. By leveraging machine learning algorithms, AI systems can learn and establish patterns of normal behaviour within a system or network. When there is a deviation from these established patterns, AI algorithms can raise alerts and flag potential security breaches or insider threats. Anomaly detection techniques employed by AI can analyse various data sources, including network logs, user behaviour, system configurations, and file access patterns. By continuously monitoring and comparing current data with historical data, AI algorithms can identify abnormal activities or behaviours that may signify a security incident.

The ability of AI to automatically detect anomalies reduces the reliance on manual monitoring and enables investigators to focus their attention on areas that require further investigation. By quickly identifying potential security breaches, AI empowers forensic specialists to respond promptly, mitigate risks, and prevent further damage. AI can adapt and improve its anomaly detection capabilities over time by learning from new data and incorporating evolving threat intelligence. This ensures that AI systems remain up-to-date and effective in identifying emerging patterns of suspicious activities.

Predictive Analysis: AI techniques, such as machine learning are highly valuable in digital forensics for predictive analysis. By analysing historical data and identifying patterns associated with malicious activities, AI can generate predictive models to anticipate future threats and incidents. This proactive approach allows forensic specialists to stay ahead of cybercriminals and take preventive measures to protect digital systems and data.

Machine learning algorithms can identify evolving cybercrime techniques, recognize indicators of compromise, and predict potential security breaches. This enables investigators to implement proactive security measures, such as system upgrades, patching vulnerabilities, or strengthening network defences, to mitigate risks before they materialize.

By leveraging AI-powered predictive models, digital forensic specialists can allocate their resources effectively, prioritize potential threats, and focus their investigations on high-risk areas. This not only enhances the security posture of organizations but also helps in the early detection and prevention of cyber-attacks, minimizing potential damage and loss.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Automation and Efficiency: AI can significantly improve the efficiency of digital forensic investigations by automating repetitive and time-consuming tasks. AI-powered tools can handle various aspects of the investigation process, allowing forensic specialists to focus their time and expertise on more complex analysis and decision-making.

One area where AI excels is data extraction. AI algorithms can automatically extract relevant information from large volumes of digital data, such as documents, emails, or databases. This automation saves investigators from manually sifting through massive amounts of information, enabling them to quickly identify and collect pertinent evidence. AI can assist in evidence preservation by automatically identifying and tagging digital evidence, ensuring its integrity and maintaining a proper chain of custody. This reduces the risk of human error and strengthens the admissibility of the evidence in legal proceedings.

AI-powered tools can also streamline the process of report generation. By analysing the collected data and generating comprehensive reports, AI algorithms can save time and effort for investigators, who would otherwise need to compile the information manually. This not only speeds up the investigation process but also enhances the accuracy and consistency of the generated reports.

By automating repetitive tasks, AI enables digital forensic specialists to focus on critical analysis, interpretation, and decision-making, which are essential for uncovering the truth and presenting compelling evidence in criminal investigations.

Challenges in Using AI over Human Expertise

While AI offers significant benefits to digital forensic specialists, it is important to note that human expertise and judgment are still crucial in interpreting results, validating findings, and ensuring the ethical and legal use of AI technologies. AI should be viewed as a supportive tool that complements and enhances the skills of forensic specialists, rather than replacing their expertise.

AI in digital forensics has numerous benefits, but it also has limitations that need to be considered. These include the lack of human intuition, potential biases and errors in algorithms, ethical concerns, high implementation costs, and uncertainties surrounding the legal admissibility of AI-generated evidence.

Lack of human intuition: In the field of digital forensics, one of the limitations of AI is the lack of human intuition. Although AI systems are highly proficient in analysing data and identifying patterns, they may overlook significant contextual cues that human investigators would typically recognize. Human intuition and experience play a vital role in making informed decisions and drawing accurate conclusions during a digital forensic investigation.

Human investigators possess a deep understanding of the complexities and nuances involved in criminal activities, which allows them to interpret evidence in a broader context. They can leverage their intuition to identify subtle connections, assess the credibility of information, and make critical judgments that AI systems may struggle with. Furthermore, human investigators can adapt their investigative approach based on the unique circumstances of each case. They can employ creative thinking, leverage their knowledge of legal and investigative procedures, and consider external factors that may influence the evidence. These aspects of human intuition and experience are not easily replicated by AI systems.

While AI can significantly enhance the efficiency and effectiveness of digital forensic investigations by automating tasks and analysing large volumes of data, it is essential to recognize the value of human intuition in the decision-making process. Collaborating the strengths of AI technology with the expertise of human investigators can lead to more comprehensive and accurate results in digital forensic investigations.

Bias and errors: One limitation of AI in digital forensics is the potential for bias and errors in AI algorithms. AI algorithms rely on the data they are trained on, and if this data is biased or contains errors, it can lead to biased or erroneous results. This can be particularly problematic if the training data is not representative of the diverse range of scenarios and contexts encountered in digital forensic investigations.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Bias in AI can arise from various sources, such as biased data collection methods, biased labelling of training data, or biased algorithm design. If the AI system is trained on data that disproportionately represents certain demographics or types of crimes, it may produce biased results that can potentially lead to incorrect conclusions or unjust outcomes. Errors in AI can occur due to various factors, including inaccuracies in the training data, limitations of the algorithms used, or unexpected edge cases that the AI system has not been trained to handle. These errors can result in false positives or false negatives, where relevant evidence is missed or irrelevant information is flagged.

To mitigate these limitations, it is crucial for digital forensic specialists to validate and verify the results of AI analysis manually. They should critically assess the outputs of AI algorithms, cross-reference the findings with other sources of information, and exercise their professional judgment to ensure the accuracy and reliability of the results. Human expertise and oversight are essential for identifying and addressing any biases or errors that may arise from the AI system.

By being aware of the potential for bias and errors in AI algorithms and taking steps to validate and verify the results, digital forensic specialists can mitigate these limitations and ensure that the use of AI in their investigations is reliable and unbiased.

Ethical concerns: The use of AI in digital forensics presents ethical concerns that revolve around privacy, data protection, and transparency. As AI systems handle large amounts of digital data, it is crucial to ensure that individuals' privacy rights are respected throughout the investigative process.

One ethical concern is the potential for unauthorized access to personal or sensitive information during data collection and analysis. It is important to implement strict protocols and safeguards to protect the privacy of individuals involved in investigations. This includes obtaining necessary permissions, anonymizing data when possible, and ensuring secure storage and transmission of information.

Data protection: Data protection is another ethical consideration. AI algorithms rely on extensive data sets for training and analysis, and it is essential to adhere to relevant data protection regulations and guidelines. This includes obtaining informed consent for data usage, implementing appropriate security measures to prevent data breaches, and securely disposing of data once it is no longer needed.

Transparency is a crucial ethical principle in the use of AI. It is important to be transparent about the use of AI algorithms, their capabilities and their limitations. Investigators should provide clear explanations of how AI is used in the forensic process and communicate the potential impact on individuals' rights and freedoms. Transparent practices help build trust and enable individuals to understand the implications of AI technology in their digital forensic investigations.

Adhering to legal and ethical standards is paramount in the use of AI in digital forensics. Organizations and forensic specialists should stay informed about relevant laws and regulations governing data protection, privacy, and transparency. They should also adopt ethical frameworks and guidelines specific to the use of AI in their practice.

By addressing these ethical concerns, digital forensic specialists can ensure that the use of AI is conducted in a responsible and ethical manner, respecting individuals' rights, protecting their data, and promoting transparency throughout the investigative process.

High Implementation Costs: Implementing AI technology in digital forensics can indeed be associated with high costs. The adoption of AI requires investment in various areas, including infrastructure, software, and personnel training, which can pose financial challenges for organizations. Infrastructure costs involve acquiring and maintaining the necessary hardware and computing resources to support AI algorithms. AI systems often require powerful processors, high-capacity storage, and specialized hardware accelerators to handle the computational demands of data analysis. Setting up and maintaining such infrastructure can be expensive.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Software costs encompass the acquisition or development of AI algorithms and related software tools. Depending on the specific requirements and capabilities needed for digital forensic investigations, organizations may need to invest in commercially available AI software solutions or develop their own custom algorithms. Licensing fees, software updates, and ongoing maintenance can contribute to the overall cost.

Personnel training is another aspect that adds to the cost. AI technologies require skilled professionals who have expertise in machine learning, data analysis, and AI implementation. Training existing staff or hiring specialized personnel with AI knowledge can involve significant expenses, including recruitment costs, salaries, and continuous professional development to stay updated with evolving AI techniques. Furthermore, organizations may need to invest in continuous research and development to keep up with advancements in AI technologies. This involves staying informed about the latest developments, attending conferences, and collaborating with experts in the field. Such activities can require additional financial resources. Despite the high costs, organizations should consider the potential long-term benefits that AI can bring to digital forensics, such as increased efficiency, improved accuracy, and enhanced investigative capabilities. It is essential to conduct a cost-benefit analysis to evaluate the return on investment and assess the potential impact on operational effectiveness and investigation outcomes.

To mitigate the financial burden, organizations can explore partnerships, collaborations, or shared resources with other institutions or agencies. Additionally, as AI technology continues to advance, there is a possibility of cost reduction and increased availability of more affordable AI solutions in the future. The high cost of implementing AI in digital forensics is a valid consideration, organizations should carefully assess the potential benefits and explore strategies to manage and optimize costs while maximizing the value derived from AI technologies in their investigative processes.

Legal admissibility: The legal admissibility of AI-generated evidence is indeed a significant concern in the field of digital forensics. While AI technologies can assist in analysing and processing digital evidence, their acceptance in legal proceedings is subject to certain requirements and challenges.

Courts typically require evidence to be reliable, relevant, and authenticated to ensure its admissibility. When it comes to AI-generated evidence, the challenge lies in establishing the reliability and trustworthiness of the algorithms and processes used to generate the evidence. One key consideration is the transparency and explainability of AI algorithms. Courts may require clear documentation and explanations of how the AI system functions, how the evidence was generated, and the underlying principles and methodologies involved. Lack of transparency and the "black box" nature of certain AI algorithms can raise doubts about the integrity and validity of the evidence.

Another crucial aspect is the authentication and validation of AI-generated evidence. Courts may require evidence to be properly authenticated, ensuring that it has not been tampered with or manipulated. This can be more complex with AI-generated evidence, as the algorithms and processes involved may be difficult to authenticate without expert testimony or supporting documentation. Additionally, there may be concerns regarding biases or errors in AI algorithms, which could affect the accuracy and reliability of the evidence. Courts may require evidence to be free from biases and errors and may scrutinize the training data and methodologies used in AI systems.

To address these concerns, it is important for digital forensic specialists and legal professionals to work together to establish standards and guidelines for the admissibility of AI-generated evidence. This may involve developing industry best practices, conducting research, and engaging in discussions with legal experts and policymakers. Furthermore, organizations utilizing AI in digital forensics should maintain comprehensive documentation and records of the AI processes, including the training data, algorithms used, and validation procedures. This documentation can help establish the reliability and credibility of the evidence in court.

It is worth noting that the admissibility of AI-generated evidence may vary across jurisdictions, as legal systems and standards differ. Therefore, it is crucial to consult with legal experts and stay updated on the evolving legal landscape regarding the acceptance of AI-generated evidence

The legal admissibility of AI-generated evidence remains uncertain, and it is essential for digital forensic specialists and legal professionals to address the challenges related to transparency, authentication, and validation to enhance the chances of acceptance in legal proceedings.

Conclusion - The incorporation of AI and ML into digital forensics significantly improves investigative efficiency by automating data analysis, evidence prioritization, and anomaly detection, resulting in substantial time and resource savings. While AI effectively tackles challenges like data volume, encryption barriers, and evolving technology, it comes with drawbacks such as the absence of human intuition, algorithmic biases, ethical concerns, high implementation costs, and uncertainties regarding legal admissibility. A collaborative approach, synergizing AI capabilities with human expertise, is imperative. Transparent documentation, adherence to ethical standards, and sustained cooperation between digital forensic specialists and legal professionals are vital to navigating these challenges responsibly and ensuring the ethical use of AI in digital forensics.

References:

01. Casey, E., 2011. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. (3rd ed.). Academic Press. https://dl.acm.org/doi/book/10.5555/2021194
02. Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac,N.-A. and Scanlon, M. (2020) SoK: exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. Proceedings of the 15th International Conference on Availability, Reliability and Security. http://dx.doi.org/10.1145/3407023.3407068
03. Qadir, S., Noor, B., 2021. Applications of Machine Learning in Digital Forensics. 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2). https://doi.org/10.1109/icodt252288.2021.9441543
04. Stoney, D.A., Stoney, P.L., 2015. Critical review of forensic trace evidence analysis and the need for a new approach. Forensic Science International 251, 159–170. https://doi.org/10.1016/j.forsciint.2015.03.022
05. Elgohary, H.M., Darwish, S.M., Elkaffas, S.M., 2022. Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. IEEE Access 10, 14669–14679. https://doi.org/10.1109/access.2022.3147809
06. Mosli, R., Li, R., Yuan, B. and Pan, Y., 2016, May. Automated malware detection using artifacts in forensic memory images. In 2016 IEEE Symposium on Technologies for Homeland Security (HST) (pp. 1-6). IEEE. https://doi.org/10.1109/ths.2016.7568881

ABOUT THE AUTHOR:

Akash Mishra

Assistant Professor

Department of Digital Forensic School of Science

Malla Reddy University, Hyderabad

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Expertise -

Mr. Akash Mishra stands out as an exceptional figure and researcher in the realm of Digital Forensics and Cybersecurity. His extensive background and expertise in these domains have played a pivotal role in advancing investigative practices and law enforcement operations. He holds a Master's degree in Digital Forensic & Information Security from the National Forensic Science University and a degree in Electronics & Communication Engineering from Biju Patnaik University of Technology, Odisha. Notably, his specialization in Drone Forensics, Mobile Forensics, Social Network Analysis and Cloud Forensics underscores his commitment to staying abreast of technological advancements and their impact on digital investigations. His collaborations with state police organizations reflect his practical engagement and the acknowledgment of his valuable insights by law enforcement professionals.

Serving as an Assistant Professor at the Department of Digital Forensics at Malla Reddy University, Hyderabad, Mr. Akash Mishra is dedicated to nurturing the next generation of digital forensics experts. His influence extends beyond academia, as he also serves as a Cyber Security Evangelist, sharing his knowledge and expertise through his role as a Resource Person for Digital Forensic & Cyber Crime Investigations at various State Police, Universities, and Social organizations. His participation as a keynote speaker and panelist in news debates and conferences further solidifies his influential presence and the respect he commands in the field. He has written numerous articles in Regional Daily regarding Digital Forensics & Cyber security Awareness. Undoubtedly, Mr. Akash Mishra's contributions have left a lasting impact on the domains of digital forensics and cybersecurity.

eSec Forte®

Capacity Building In

Digital Forensics

First Responder (Onsite/CFL) – 05 Days

- Cardinal Rules of Digital Forensics
- Process, Tools & Techniques
- Volatile Memory Forensics
- Network Traffic Analysis
- Imaging Live Systems
- Documentation Preparation / Validation
- Seizure Procedure
- Packing and Transportation
- Preservation of Digital Assets

DF Examiner / Analyst – 10 Days

- Understanding Hard Disks and File Systems
- File Systems Analysis using FTK imager and open-source tools
- Volatile Memory Forensics
- OS Forensics
- Mobile Forensics
- Email Forensics
- Social Media Forensics
- Anti-forensics

DF Assistant (CFL) - 05 Days

- Imaging of Digital Assets
- Cloning of Digital Assets
- Hash Verification
- Preservation of Digital Assets
- Maintenance of CFL
- Record Keeping

Technical / Quality Manager – 03 days

- Report Writing
- IT Act
- CFTT (NIST)
- ISO/IEC 27037
- ISO/IEC 27041
- ISO/IEC 27042
- ISO/IEC 27043

Expert Witness – 02 Days

- IT Act
- IEA (Relevant part)
- Moot Court
- 79A (Examiner of Electronic Evidence)

GURUGRAM | DELHI | MUMBAI | BANGALORE | SINGAPORE | SRI LANKA | DUBAI

Tel: +91 124 4264666 **Mail:** contact@esecforte.com **Web:** www.esecforte.com

Research Report on

Phishing campaign, imitates KYC App by State Bank Of India

Disclaimer

This report is purely based on technical findings made by the research team during an investigation. It does not intend to malign or in any way target any country, actor or person. All the information provided in this report has been extracted during the investigation and information might be changed after generating the reports.

Research Report on Phishing Campaign, imitates SBI-KYC App by State Bank of India

The Research Wing of CyberPeace Foundation has received a text message containing a link asking users to complete KYC for their respective State Bank of India account.

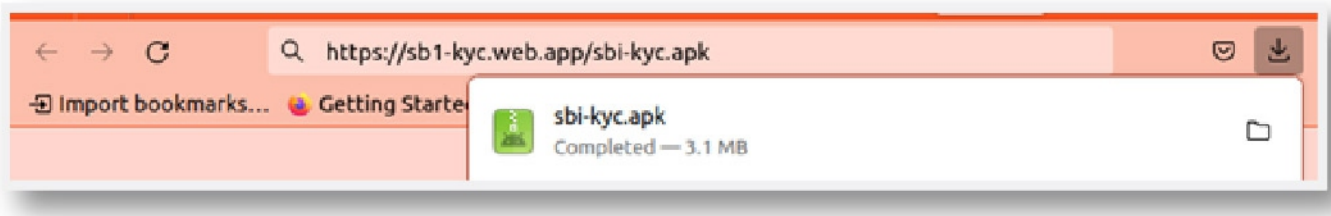
Case Study

The Research Wing of CyberPeace Foundation and Autobot Infosec Private Limited have looked into it to come to a conclusion that the campaign is either legitimate or online fraud.

Link

https://sb1-kyc.web[.]app/sbi-kyc.apk

When an individual visits the link **"https://sb1-kyc.web[.]app/sbi-kyc.apk"** it starts downloading the application **sbi-kyc.apk**



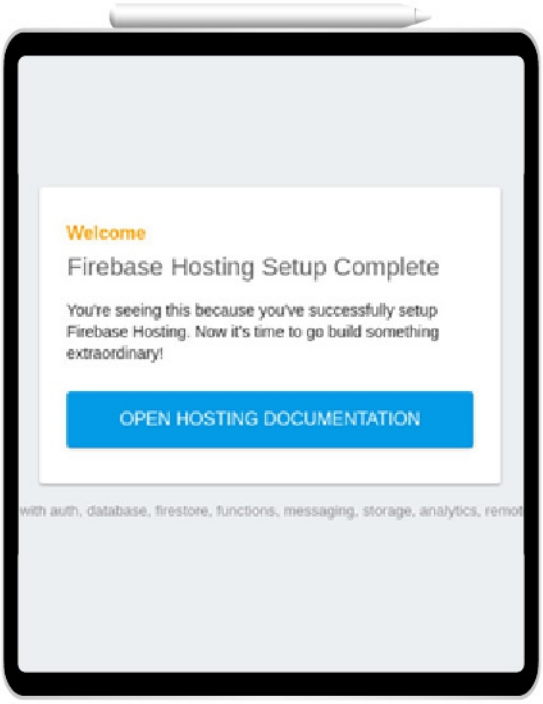
In-Depth Analysis

Domain Name	sb1-kyc.web[.]app
IP Address	199.36.158.100
HTTP Source code	200 [Active]
ISP	Google LLC
ASN	54113
Country	United States
State/Region	California

Domain Name: web.app
Registry Domain ID: 300A2C851-APP
Registrar WHOIS Server: whois.nic.google
Registrar URL: http://www.markmonitor.com
Registrar: MarkMonitor Inc.
Sponsoring Registrar IANA ID: 292

Updated Date: 2022-12-12T09:28:46+00:00
Creation Date: 2019-01-08T22:05:04+00:00
Registrar Registration Expiration Date: 2024-01-08T22:05:04+00:00

Registrant Organization: Charleston Road Registry, Inc.
Registrant Country: US



Nameservers: ns1.googledomains.com
ns2.googledomains.com
ns3.googledomains.com
ns4.googledomains.com

By visiting the url **https://sb1-kyc.web[.]app** we came to know the site is hosted using Firebase technology.

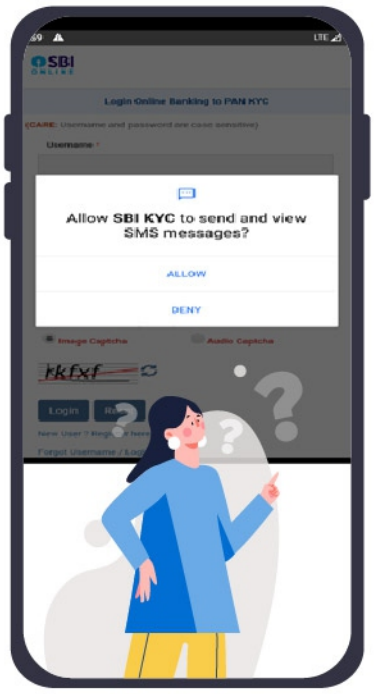
Note: Firebase is a Google-owned platform that provides developers with a set of tools and services to build, develop, and grow their applications. Firebase provides developers with a wide range of features such as real-time database, authentication, hosting, cloud functions, storage, and more. It also provides an API to interact with these services, making it easy for developers to add these features to their applications without having to manage the underlying infrastructure. The platform is designed to help developers build better applications faster and with less effort, and it is commonly used for building mobile and web applications.

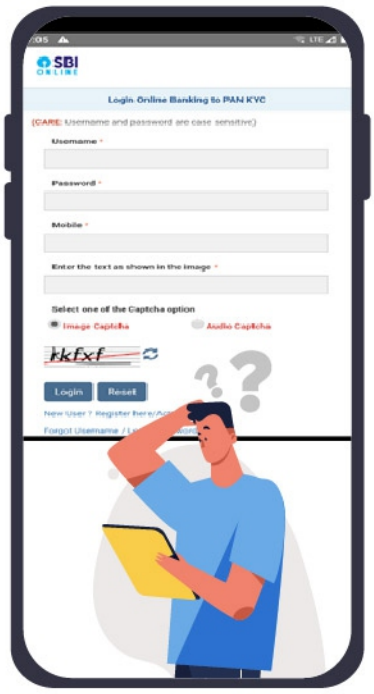
HTTP Header Response

HTTP/1.1 200 OK	
Connection:	close
Content-Length:	3259052
Cache-Control:	max-age=3600
Content-Type:	application/vnd.android.package-archive
Etag:	"17db3cf1de32f77518507ae48ae78de7816ef3ecb4da2ef6d479008b7db2e942"
Last-Modified:	Fri, 27 Jan 2023 11:00:43 GMT
Strict-Transport-Security:	max-age=31556926; includeSubDomains; preload
Accept-Ranges:	bytes
Date:	Wed, 08 Feb 2023 04:36:59 GMT
X-Served-By:	cache-iad-kjyo7100068-IAD
X-Cache:	MISS
X-Cache-Hits:	0
X-Timer:	S1675831019.895643,VS0,VE470
Vary:	x-fh-requested-host, accept-encoding
alt-svc:	h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400

Application Analysis

Once the user installs the sbi-kyc.apk application on an android device, like any other android application, the app asks the user to give the following permissions as shown here:





The application pretends itself to be appearing from the State Bank of India. It gives users a message “Login Online Banking to PAN KYC”. It asks users to enter **Username, Password, Mobile number** belonging to their SBI online Banking account.

We noticed the Captcha appearing in the login section is static which remains the same, every time users relaunch the application.

Application Details

App name	SBI KYC
Package name	com.mykycandroid.vxy1
App Security Score	**52/100**
Main Activity	com.example.android.MainActivity
Target SDK	32

Application Icon

Hash Details

MD5	02fef8c41ddcac396eec86219c8b553f
SHA1	8564c39126506e27fa84ba452e8f4b79bff5d0ee
SHA256	5c9fb34f1f12a8fe9adf1a41bde6ce35eb379a9621f35d84c41d589e78f338ee

Application Certificate Details

Issuer	C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Valid From	2008-04-15 22:40:50+00:00
Valid To	2035-09-01 22:40:50+00:00
Serial Number	0xb3998086d056cffa
Hash Algorithm	md5
PublicKey Algorithm	RSA

Application Permission Details

```
<manifest android:versionCode="1" android:versionName="1.0" android:compil
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="22" android:targetSdkVersion="32" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
```

Application Permissions

Permissions	Status	INFO	Description
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows an application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows an application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.

Code Analysis

SI No	ISSUE	SEVERITY	STANDARDS
1	App can read/write to External Storage. Any App can read data written to External Storage.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2
2	The App logs information. Sensitive information should never be logged.	Info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	**CWE:** CWE-312: Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2

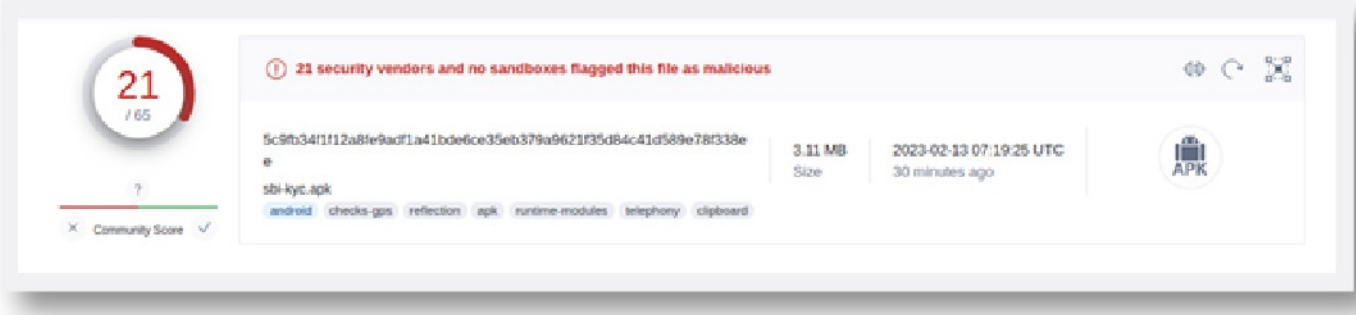
Domain Connected

DOMAIN	GEOLOCATION
ns2.9appsdownload.org	**IP:** 172.67.143.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203
connectivitycheck.gstatic.com	**IP:** 142.250.67.163 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514
www.google.com	**IP:** 142.251.42.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514

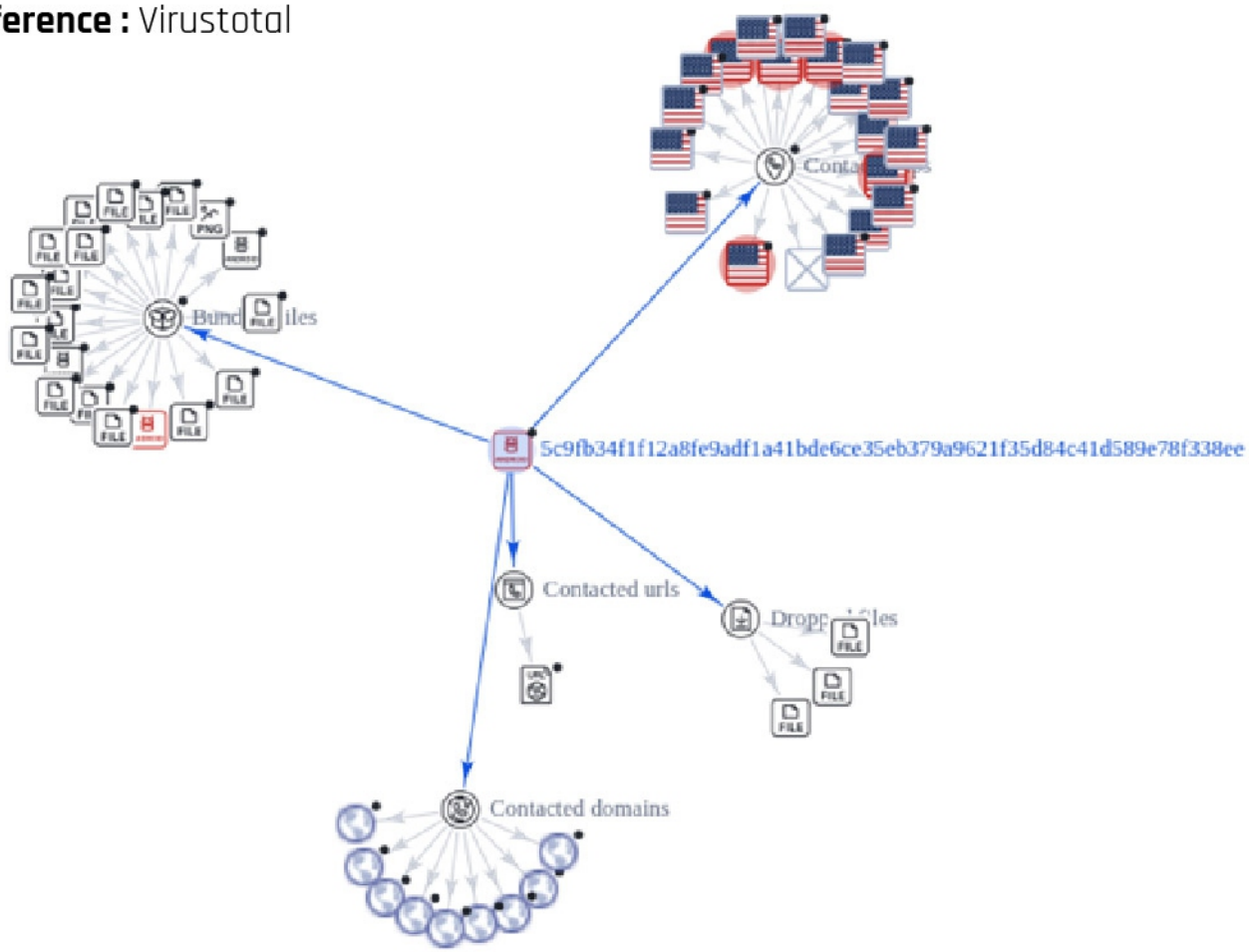
Interesting Strings

- http://*/*
- http://schemas.android.com/apk/res/android
- https://*/*
- https://ssl.gstatic.com/accessibility/javascript/android/

The application is flagged as malicious by 21 Security Vendors on Virustotal.



Reference : Virustotal



Conclusive Summary

- The campaign appears to be an offer from the State Bank of India, but it is hosted on a third-party domain instead of the official State Bank of India website, raising suspicion.
- Cybercriminals utilised Google's Firebase technology to disseminate the Malicious application on Cyberspace.
- The application asks several access permissions of the device such as read and write to sms, internet.
- Cybercriminals used the icon of Yono application which is the official banking app of SBI, while creating the malicious application in order to lure the users.
- The application asks for several financial details from the user.
- The application is flagged as malicious by several Security Vendors.
- Customers who desire to perform KYC for availing more benefits, download relevant apps, believing that the chosen app will assist them. However, they are not always aware that the app may be fraudulent.

CyberPeace Advisory

- CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms. One must always think before clicking on such links, or downloading any attachments from unauthorised sources.
- Downloading any application from any third party sources instead of the official app store should be avoided. This will greatly reduce the risk of downloading a malicious app, as official app stores have strict guidelines for app developers and review each app before it gets published on the store.
- Check the app's permissions before you install it. Some malicious apps may request access to sensitive information or resources on your device. If an app is asking for too many permissions, it's best to avoid it.
- Keep your device and the app-store app up to date. This will ensure that you have the latest security updates and bug fixes.
- Falling into such a trap could result in a complete compromise of the system, including access to sensitive information such as microphone recordings, camera footage, text messages, contacts, pictures, videos, and even banking applications and could lead users to financial loss.
- Do not share confidential details like credentials, banking information with such types of Phishing scams.
- Never share or forward fake messages containing links on any social platform without proper verification.

Issued by

Research Wing, CyberPeace Foundation.
Research Wing, Autobot Infosec Private Ltd.

"INFUSING CYBERPEACE IN CYBERSPACE"

www.cyberpeace.org | secretariat@cyberpeace.net

Secretariat : B-55, Harmu Housing Colony, Birsa Munda Rajpath,
Ranchi, Jharkhand, 834002

/cyberpeacefoundation /cyberpeacengo /cyberpeacefoundation

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

DRONE FLIGHT DATA PROCESSING AND INVESTIGATING THE ARTIFACTS IN DRONE

Author/Writer: **Ankit Bishnoi**

Article -

This section will look at Drone Flight Data Processing and investigating the artifacts in Drone. Drone forensics is essential in addressing the growing concerns related to the misuse of drones. This paper emphasizes the significance of drone flight data processing in forensic investigations. The extraction and analysis of flight data, including flight logs, GPS coordinates, and sensor information, are vital for reconstructing flight paths, identifying operators, and gathering evidence. The paper highlights the crucial role of accurate and timely data processing in supporting law enforcement, privacy protection, and national security. It also calls for ongoing research to keep pace with evolving drone technologies, ensuring a safer and responsible use of drones in our interconnected world.

What information can be extracted from drones?

As previously mentioned, drones, much like computers and smart devices, store a substantial amount of data that can be retrieved by a certified digital forensics expert. This data can be obtained from the drone itself and the servers it interacted with during its operational use.

This data includes:

1. Information about the drone's operator, Drone's serial number and internal component details (MAC address, IMEI, IMSI).
2. Captured photos, Recorded video footage, Dates, and timestamps, about geographic locations, photos, and videos with EXIF metadata
3. Details regarding take-off, landing, return, and home locations, encompassing both frequently used and preferred flying areas.
4. Comprehensive flight history, including specific locations and flight paths, Flight plans and intended purposes.
5. Altitude measurements at various points during the flight, Payload weights.
6. Activity logs for restricted zones, GPS status during flight.
7. Paired devices, SSID (Service Set Identifier), Wi-Fi data, IP (Internet Protocol) information, Bluetooth data, Status of 3G and 4G connectivity, Firmware version, Pilot control input, Pilot-configured settings, Data related to the file system
8. Records of atmospheric conditions at each stage of the flight.

An adept forensic data analyst can also recover deleted records and investigate the interactions between the drone and the server with which it exchanged data.

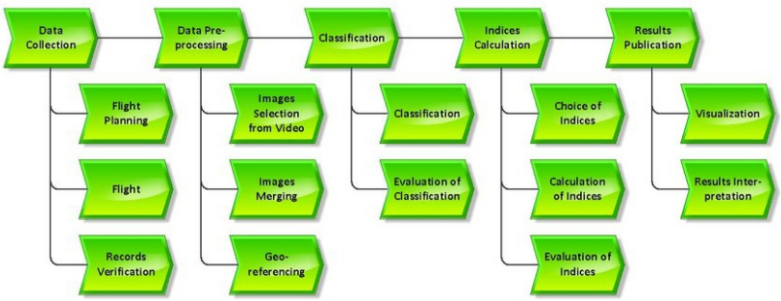


Fig. 1 – Processing of data from Drone

Retrieval of log file

1. Retrieve data from the drone.
2. Power on the remote control and iPad.
3. Activate the drone.
4. In the DJI GO app, access the settings menu on the right. Tap the drone icon at the top, scroll to the bottom, and select "Enter Flight Data mode."
5. Connect the drone to your computer using a microUSB cable. The drone should be recognized as a USB storage device.
6. Copy the latest set of DAT files. It's common for a single drone flight to generate multiple DAT files.
7. Convert the DAT files to CSV format. To do this, you will require DatCon, which can be obtained from https://datfile.net/DatCon/downloads.html.
8. Run DatCon in your preferred manner for executing jar files (e.g., using "java -jar <filename>" on Linux).
9. In the top menu, go to "Categories" and ensure both "Basic" and "Experimental" options are selected. In the top menu, access "Parsing Options" and confirm that it's set to "Engineered Only." Also, check the boxes for "Allow Invalid DatHeader" and "Allow Excessive Errors."
10. In DatCon's main interface, set the Sample Rate to 100Hz.
11. Click on the area that says, "Click here to specify .DAT file" and pick one of the files downloaded from the drone. Ensure that the .CSV radio button is chosen. You might also want to select the radio button in the KML section for Ground Track if you intend to create a file compatible with Google Earth, using the onboard GPS, rather than the RTK.
12. Finally, press the prominent "GO!" button at the bottom. A CSV file will be generated in the same directory as your DAT files. Repeat this process for each of your DAT files.

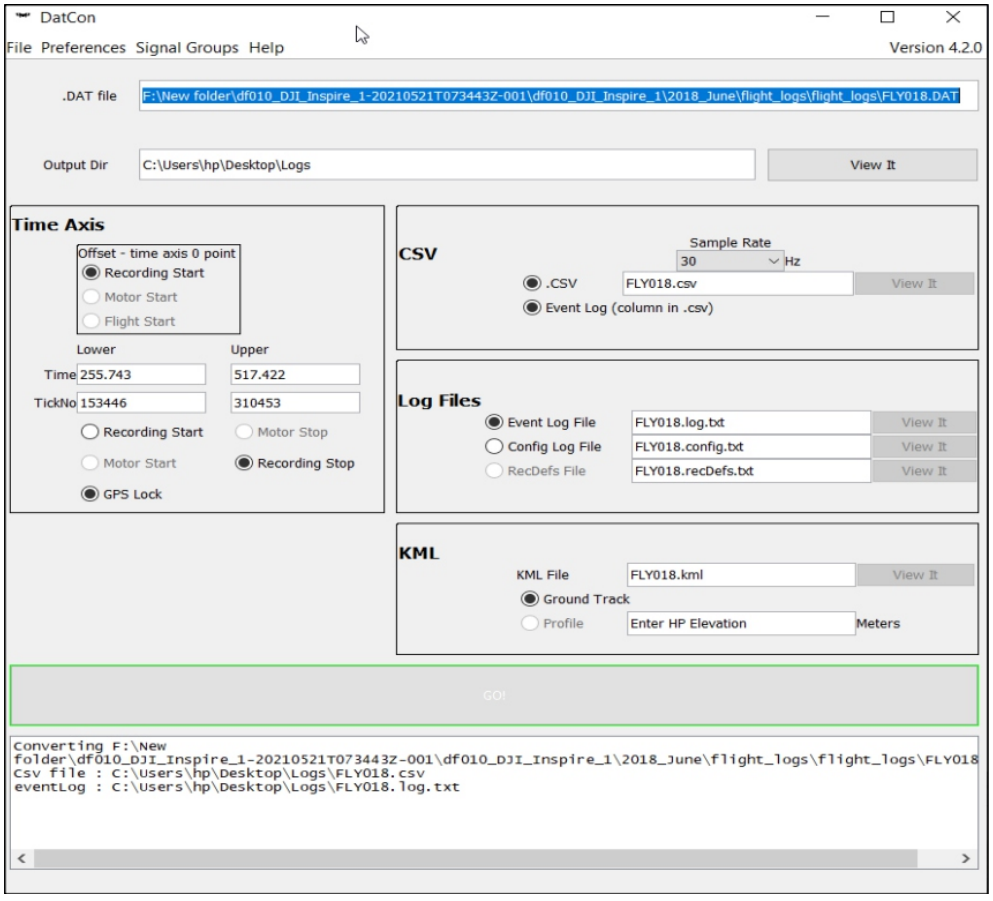


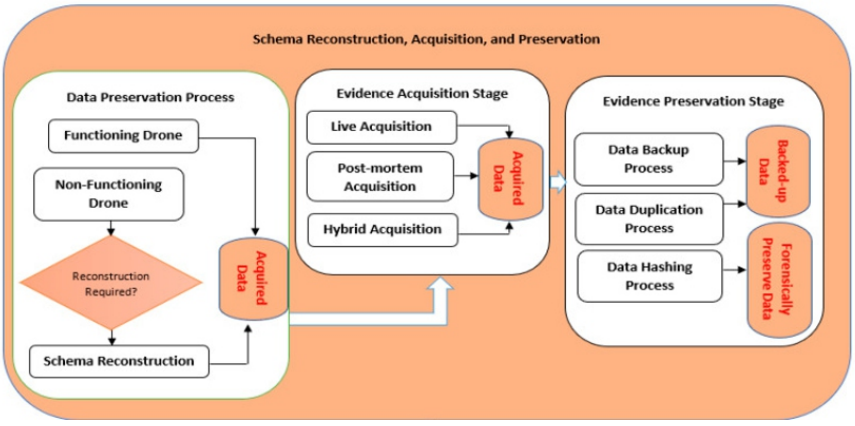
Fig. 2 DatCon software

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Forensic Procedure –

Extracting data from a drone for investigation involves several steps. Here's a general process for extracting data from a drone:

1. Secure the Drone: First, secure the drone as evidence. If the drone is operational, it's essential to safely power it down to prevent remote control by the operator or the loss of data.
2. Isolate Power: Disconnect or remove the drone's power source to prevent data from being overwritten or modified.
3. Chain of Custody: Maintain a chain of custody to document the handling of the drone from the moment it is collected. This ensures the integrity of the evidence.
4. Physical Examination: Inspect the drone for any physical damage, modifications, or signs of tampering. Document the drone's make and model and any visible serial numbers.
5. Data Storage Media: Identify and locate the data storage media on the drone, such as internal memory, SD cards, or other storage devices. In some cases, drones may have multiple storage locations.
6. Data Extraction: Use specialized tools and equipment to extract data from the storage media. This may involve removing the storage media and connecting it to a forensic workstation or using specialized software to access the data remotely.
7. Forensic Imaging: Create a forensic image of the storage media. A forensic image is a bit-for-bit copy of the original data, ensuring its integrity. This image will be used for analysis while preserving the original evidence.
8. Data Analysis: Examine the extracted data for evidence of interest. This can include flight logs, images, videos, telemetry data, and configuration settings. Analyze the data to reconstruct flight paths and understand the drone's activities.
9. Metadata Analysis: Analyze metadata associated with the data, such as timestamps, geospatial information, and any other relevant details that can provide context to the investigation.
10. Communication Analysis: If applicable, investigate communication data between the drone and its remote controller, ground stations, or other devices. This can provide insights into command and control activities.
11. Hashing and Verification: Verify the integrity of the extracted data by comparing cryptographic hash values of the original data and the forensic image. Any discrepancies could indicate tampering.
12. Documentation: Maintain detailed records of all actions taken during the data extraction process, including the tools, software, and hardware used.
13. Reporting: Prepare a comprehensive forensic report that outlines the findings, methodology, and any potential evidence discovered during the investigation. This report should be suitable for presentation in a legal context if necessary.
14. Expert Testimony: If the case goes to court, a forensic expert may be called upon to provide testimony regarding the findings and the extraction process.



DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

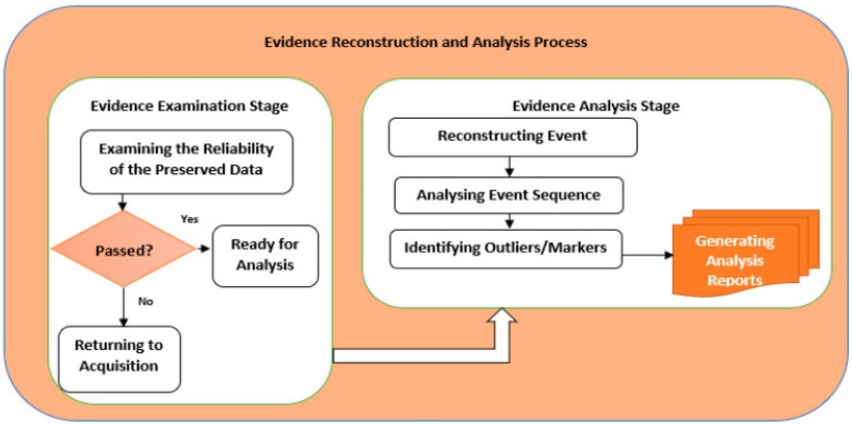


Fig. 3 Forensic approach in drone cases

Different Artifacts extracted from a Drone

```
Converting F:\New folder\df010_DJI_Inspire_1-20210521T073443Z-001\df010_DJI_Inspire_1\2018_June\flight_logs\flight_logs\FLY005.DAT
Csv file : C:\Users\hp\Desktop\Logs\FLY005.csv
eventLog : C:\Users\hp\Desktop\Logs\FLY005.log.txt
configLog : C:\Users\hp\Desktop\Logs\FLY005.config.txt
kml File : C:\Users\hp\Desktop\Logs\FLY005.kml
```

Fig. 4 Different file types found in a Drone.

	A	B	C	D	E	F	G	H
1	Clock:Tick#	Clock:offsetTime	IMU_ATTI(0):press:D	IMU_ATTI(0):alti:D	IMU_ATTI(0):roll:C	IMU_ATTI(0):pitch:C	IMU_ATTI(0):yaw:C	IMU_ATTI(0):accelX
2	22455	0	1747.4263	1748.3524	2.664284113	44.51774466	-26.08077128	0.7375344
3	22476	0.035	1748.6841	1748.3501	2.812338975	44.45077361	-26.11341744	0.70884216
4	22497	0.07	1748.3972	1748.3518	2.960140431	44.43437396	-26.18507502	0.6982451
5	22518	0.105	1747.1036	1748.3542	3.03868438	44.48331451	-26.29600783	0.6995395
6	22539	0.14	1747.5216	1748.3522	3.013114298	44.56071172	-26.46443521	0.7243127
7	22560	0.175	1747.2229	1748.3501	2.97079538	44.67011994	-26.67427471	0.7412535
8	22581	0.21	1747.9122	1748.3546	2.967402855	44.84577104	-26.87526819	0.74999946
9	22602	0.245	1747.6007	1748.35	2.963202007	45.05614615	-27.02772227	0.75348854
10	22623	0.28	1748.4398	1748.356	2.95064622	45.24586478	-27.14264609	0.7504761
11	22644	0.315	1748.1334	1748.3568	2.961020562	45.38219484	-27.20236232	0.72883755
12	22665	0.35	1748.1233	1748.3597	2.951334214	45.47749512	-27.2191618	0.7263432
13	22686	0.385	1747.4067	1748.358	2.890097779	45.50714266	-27.23508899	0.73025906
14	22707	0.42	1748.6738	1748.3618	2.803881452	45.47188652	-27.26810398	0.7407246
15	22728	0.455	1748.0875	1748.3583	2.721385991	45.40162827	-27.33104158	0.7644143
16	22749	0.49	1747.6526	1748.3557	2.705625543	45.2950241	-27.42222888	0.7608285
17	22770	0.525	1748.3411	1748.3514	2.734798426	45.17835673	-27.51981367	0.72048527
18	22791	0.56	1747.6237	1748.3479	2.767241301	45.09310092	-27.57959999	0.7117192
19	22812	0.595	1748.4628	1748.3453	2.768004728	45.05633187	-27.59005395	0.7020954
20	22833	0.63	1747.1812	1748.3434	2.706125181	45.05372498	-27.56482753	0.74202466
21	22854	0.665	1748.3037	1748.346	2.567153199	45.05085391	-27.49379502	0.7216615
22	22875	0.7	1747.5803	1748.3411	2.375876952	45.05297731	-27.34906958	0.72586685
23	22896	0.735	1746.9888	1748.3383	2.159324146	45.07266348	-27.11437197	0.7456247
24	22917	0.77	1748.1088	1748.3381	1.933109936	45.06704696	-26.7782997	0.7477653
25	22938	0.805	1747.2433	1748.3406	1.731492368	45.04238695	-26.32484281	0.75742

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

	A	B	C	D	E	F	G
1		fsk_rssi	voltage	current	altitude	latitude	longitude
2	20170803 13:51:06:950	-30	15.6	0	-0.15	39.957764	-106.207146
3	20170803 13:51:07:101	-28	15.6	0	-0.15	39.957764	-106.207146
4	20170803 13:51:07:113	-28	15.6	0	-0.14	39.957764	-106.207146
5	20170803 13:51:07:117	-28	15.6	0	-0.13	39.957764	-106.207146
6	20170803 13:51:07:121	-29	15.6	0	-0.13	39.957764	-106.207146
7	20170803 13:51:07:123	-28	15.6	0	-0.13	39.957764	-106.207146
8	20170803 13:51:07:170	-28	15.6	0	-0.13	39.957764	-106.207146
9	20170803 13:51:07:187	-28	15.6	0	-0.12	39.957764	-106.207146
10	20170803 13:51:07:211	-29	15.6	0	-0.12	39.957764	-106.207146

Fig. 5 Artefacts from a Drone in .dat file

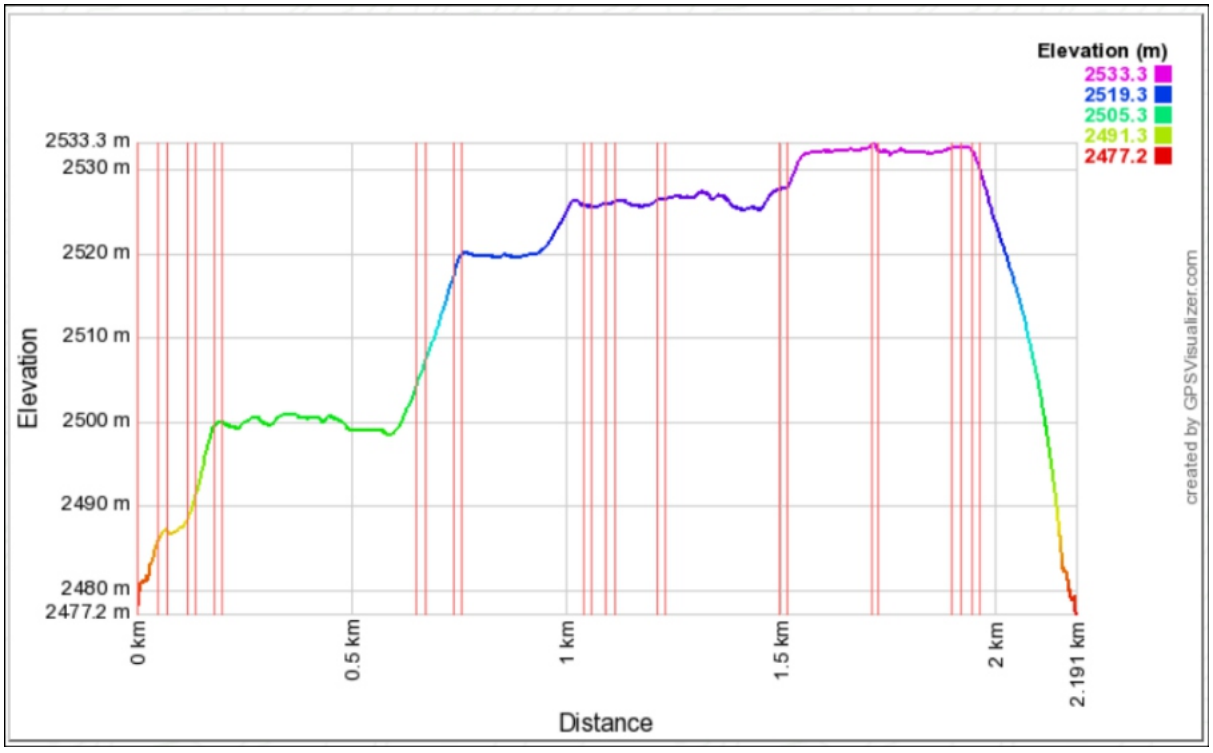


Fig. 6 Drone elevation and distance plotting from data in dat file

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Fig. 7 Plotting KML file on google earth to trace the route.

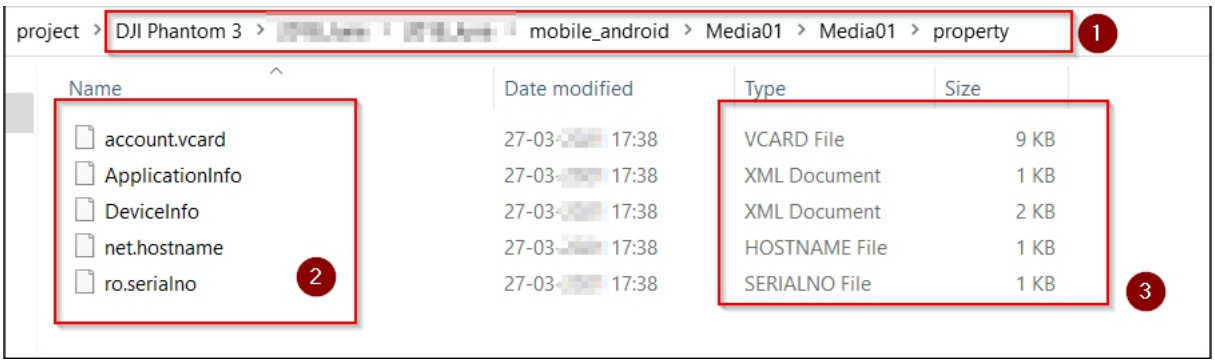


Fig. 8 Different evidence files extracted from a Drone.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Time	Flight Mode	GPS	Altitude	Speed	Home Distance	Battery	Battery Voltage	Cell 1	Cell 2	Cell 3	Cell 4	Cell Deviation	Message
1m 10.4s	P-GPS	18 satellites	70.9 ft	37.8 mph	1,583.5 ft	90%	15.558 V	3.876 V	3.892 V	3.891 V	3.899 V	0.023 V	
1m 10.6s	P-GPS	18 satellites	70.9 ft	37.4 mph	1,592.4 ft	90%	15.558 V	3.876 V	3.892 V	3.891 V	3.899 V	0.023 V	
1m 10.7s	P-GPS	18 satellites	70.9 ft	37.5 mph	1,597.0 ft	90%	15.558 V	3.876 V	3.892 V	3.891 V	3.899 V	0.023 V	
1m 10.8s	P-GPS	18 satellites	70.9 ft	37.2 mph	1,601.0 ft	90%	15.558 V	3.876 V	3.892 V	3.891 V	3.899 V	0.023 V	
1m 10.9s	P-GPS	18 satellites	70.9 ft	37.4 mph	1,605.5 ft	90%	15.558 V	3.876 V	3.892 V	3.891 V	3.899 V	0.023 V	
1m 11s	P-GPS	18 satellites	70.9 ft	37.0 mph	1,609.6 ft	90%	15.558 V	3.876 V	3.892 V	3.891 V	3.899 V	0.023 V	

Fig. 9 Drone statics at different timestamp

File Name	File Size (Bytes)	MD5 Hash Value
FLY017.DAT	205,496,320	42FDBE67089FDE01B5F1C4F27AF97F44
FLY017.CSV	35,070,466	44196203416EB2E0F0A71D6AD3AFF436
FLY017.DAT	205,496,320	42FDBE67089FDE01B5F1C4F27AF97F44
FLY017.CSV	35,070,451	4A088109155A13796DD5456C5E7BB890

Fig. 10 Taking Hash dump of flight data

```
ï»¿Atom ftyp @ 0 of size: 24, ends @ 24
Atom mdat @ 24 of size: 1481988989, ends @ 1481989013
Atom moov @ 1481989013 of size: 204052, ends @ 1482193065
    Atom mvhd @ 1481989021 of size: 108, ends @ 1481989129
    Atom udta @ 1481989129 of size: 128, ends @ 1481989257
        Atom FIRM @ 1481989137 of size: 40, ends @ 1481989177
        Atom CAME @ 1481989177 of size: 40, ends @ 1481989217
        Atom SETT @ 1481989217 of size: 40, ends @ 1481989257
    Atom trak @ 1481989257 of size: 114791, ends @ 1482104048
        Atom tkhd @ 1481989265 of size: 92, ends @ 1481989357
        Atom mdia @ 1481989357 of size: 114691, ends @ 1482104048
```

Fig. 11 Atom value analysis

These atoms are important for the verification of the camera model, firmware version, and serial number, which aids in identifying the use of any customized device attached to the drone. This draws the importance of examining media files forensically to discover anti-forensic techniques that could be used.

Future concerns related to Drone Forensics

- Data access: Extracting encrypted drone data.
- Data integrity: Ensuring data remains unaltered.
- Drone ID: Identifying drone make and model, many use home-made drones.
- Anonymity: Identifying anonymous operators.
- Expertise: Multidisciplinary knowledge needed.
- Legal hurdles: Navigating regulations.
- Tech changes: Adapting to evolving drone tech.
- Remote collection: Retrieving data from remote areas.
- Data interpretation: Expert analysis of collected data.

ABOUT THE AUTHOR:

Ankit Bishnoi

DFIR Analyst – eSec Forte Technologies

Email Address: alstonbishnoi29@gmail.com

LinkedIn: https://www.linkedin.com/in/ankit-bishnoi-0819

Expertise:

Ankit is enthusiast in the field of Incident Response & DFIR Specialist, and Infosec Trainer. He is well experienced in managing projects from the blue team to the purple team.

Credentials:

Ankit is currently working as a DFIR Specialist. Also, he holds many certifications like CHFI, CEH, CCIO, Paloalto, LogRhytm, Eset Certified, etc. He is targeting several assignments in Threat Analysis, Cyber Security, Incident Response, and Digital Forensics.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

SOLID STATE DEVICES (SSD) FORENSICS

Maintaining integrity of SSDs due to garbage collection, secure delete, wear leveling and data remapping is an issue and makes it difficult for the forensic investigator to make the digital evidence tenable in the court of law as the hash value of the evidence changes with time. Firstly, it is recommended that along with the hash of the digital evidence individual file hashes be taken and secondly after due permission from the court the SSD controller chip be disassociated with the memory storage to prevent the TRIM command from execution. The changes to be endorsed in the 'Chain of Custody' form.

-Lt. Col. (Dr.) Santosh Khadsare (Retd.)

Introduction

"If there is anyone has challenged the Locard's principle of exchange from digital forensics point of view, it is the Solid State Devices (SSDs)"

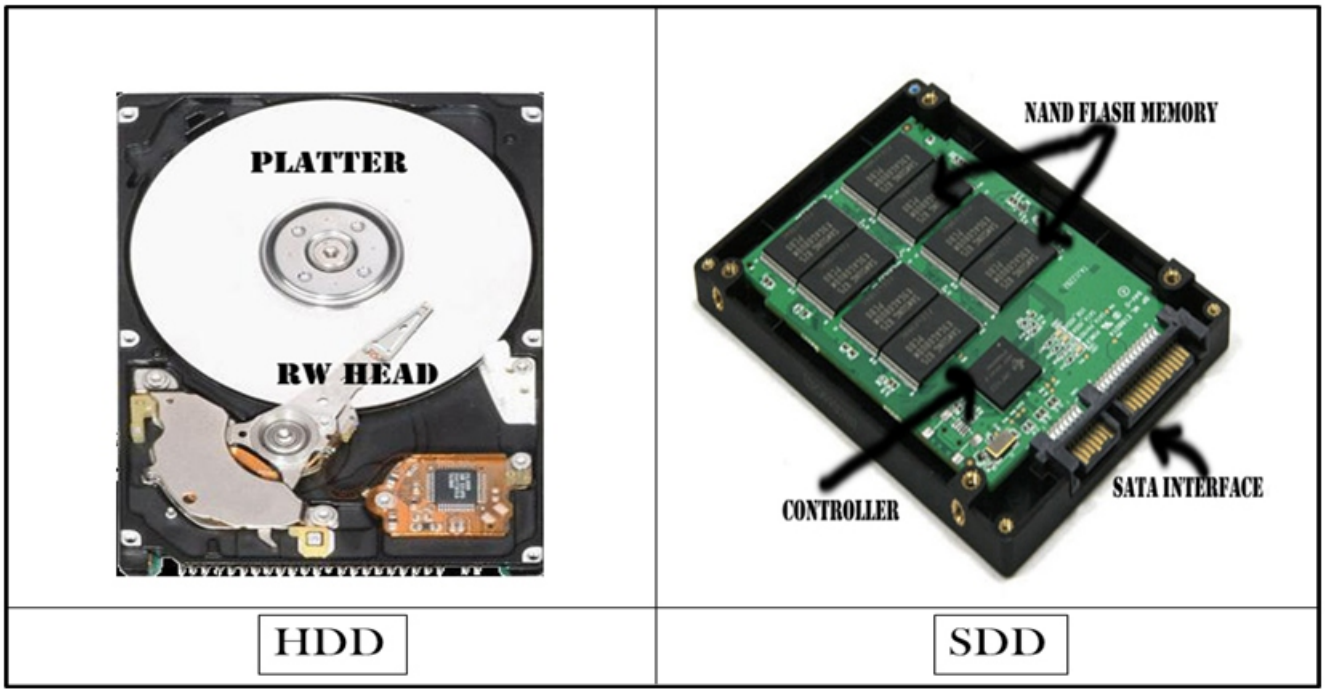
Gone are the days when a cyber forensic investigator could claim that if something was ever present in the digital evidence he will reproduce it. Erasing of one's tracks in, the digital world has become much easier as the perpetrator needs no technical acumen but just some common sense to replace the existing storage media of this weapon (laptop/mobile phone /computing device) with SSDs. When the D-day arrives the perpetrator has to press the trigger of this weapon by issuing 'delete' command. That's all.

One of the best definition of digital forensics was given at Digital Forensics research Conference (DFRWS) in 2001.It stated **"Digital Forensics is use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".**

Solid State Devices

To begin with solid-state refers to electronic components, devices, and systems based on the semiconductor in which the electrons or other carriers of charge are confined entirely within the solid material. In a solid-state component, the current is confined to solid elements and compounds meant specifically to switch and amplify it. Shifting the focus to the storage drives in the various state of art gadgets in which the SSDs are gaining foothold at a very fast pace. The Hard Disk Drives (HDD) are being replaced by the new entrant in all the computing devices to mention a few are laptops, desktops, mobile phones, etc. The other storage medium such as flash drives and secondary storage media have also shifted to this new technology. Some advantages of having a SSD in place of a HDD is no moving parts, less access time, reliability and energy savings

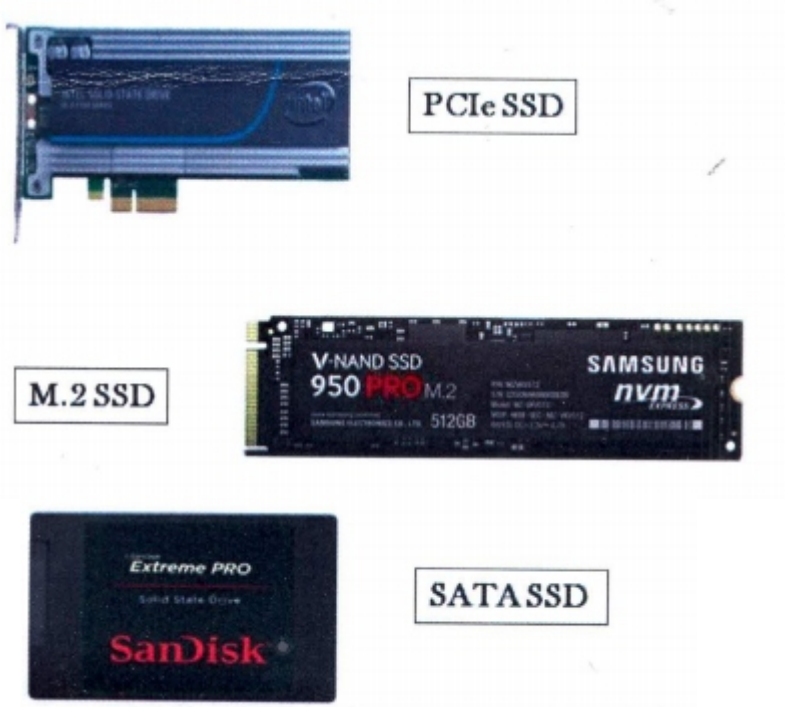
DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION



SSDs have introduced dramatic changes to the principles of digital forensics. Identification of SSD as digital evidence is also turning out to be a challenge to begin with. You find SSDs being used everywhere be it mobile phone, digital cameras, laptop /desktop storage media, USB drives, etc. Once digital evidence comes for cyber forensic investigation, the investigator should be able to identify the same or he may lose out on the integrity part as due to various technical issues the hash value of the evidence changes. The court of law has to be explained various technical hurdles faced during SSD forensics and the reasons of change in hash values.

M.2 Evolution of Sleek and Lighter SATA SSDs.

First Generation SSD drives were available as 2.5" disks which was a limitation when making ultra-portable devices. The solution to this problem was M.2 form factor. Devices conforming to the M.2 form factor can use Serial Advanced Technology Attachment (SATA), Peripheral Component Interconnect - Express (PCI-E) or USB3.0 connectivity. M.2 devices require a standard PCI-E connector. While most M.2 SSD drives conform to the AHCI specification, supporting all the features of their full-size counterparts and being recognized by the OS as a standard SATA SSD, some models conform to the newer Non Volatile Memory Express (NVMe) specification that requires a different driver stack.M.2 SSD drive can be Legacy SATA, PCI-E using Advance Host Controller Interface (AHCI) or PCI-E using NVMe



PCI Express (PCI-E) SSDs. PCI-E, or PCI Express, is a physical connectivity standard. PCI-E SSD drives are available in a wide range of form factors including full-size desktop expansion boards, M.2, proprietary and soldered portable storage solutions. PCI-E SSDs can use AHCI or NVMe for interfacing.

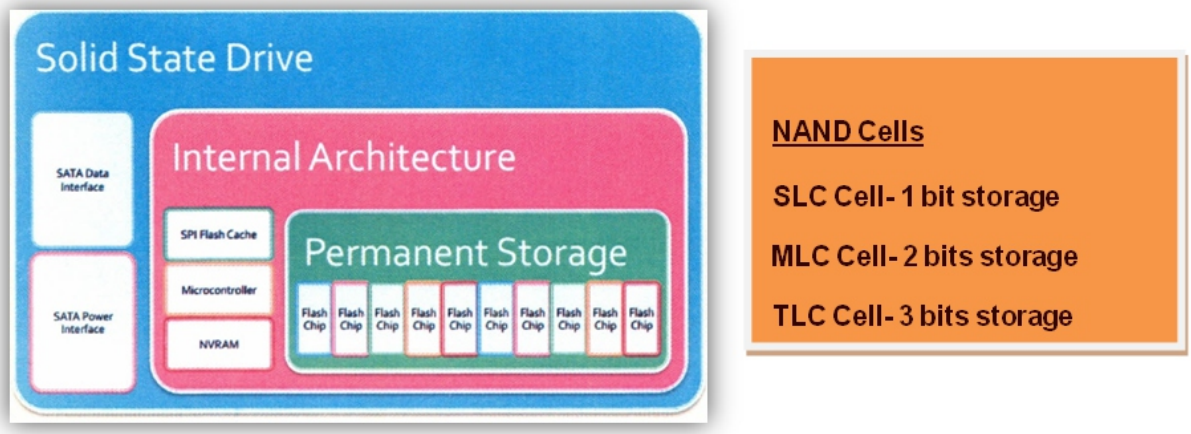
On a logical level, PCI-E SSD drives can work via the AHCI or NVMe interface. In general, the following compatibility matrix applies to PCI-E:

- **Mac OS X**: Trim command 'is supported on all Apple devices with factory installed PCI-E SSD drives.
- **Mac book with Windows**: Proprietary PCI-E SSD drives are used Apple Mac books. Windows is installed as double-boot or independent Operating System. In these configurations, trim pass-through is supported where applicable.
- **Windows**: Trim support for PCI-E drives depends on Windows version and the presence of the correct driver. In Win 7 trim not supported on PCI-E drives regardless of the drivers, even if the PCI-E SSD would accept the command. **Win 8, 8.1 and Win 10**: trim is supported with native Microsoft drivers. Trimming in NVMe-based PCI-E SSDs is also supported

NVM Express (NVMe) SSDs. NVMe is a modern logical interface specification that replaces the old AHCI. NVMe is employed in certain high-end PCI-E SSD models in various form factors. Apple Mac Book 2015 uses NVMe interface on a proprietary SSD drive soldered to the motherboard. NVMe is still fairly new, with some motherboards failing to recognize NVMe storage as bootable devices. Similar to SATA SSD drives that exist as 2.5" drives and as slim M.2 boards, NVM Express devices are also available as full-size PCI Express expansion cards, laptop-size boards and 2.5" drives that look similar to SATA SSD drives, only utilizing a PCI Express interface through the U.2 connector instead of a SATA port.

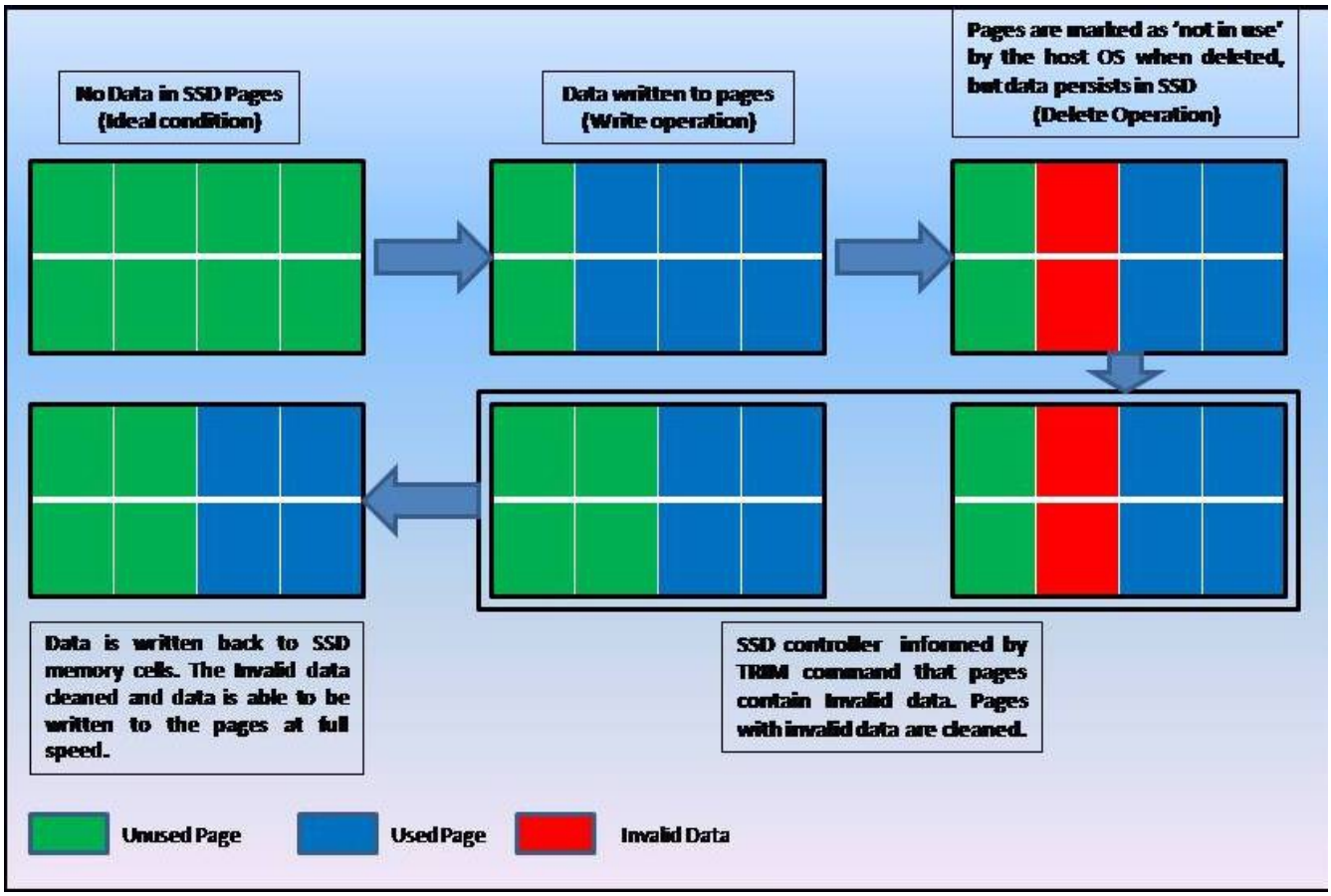
Exploring SSDs Picture speaks better than words. NOR flash and NAND flash are the components of SSD. SSDs have limited erase-write cycles and the read accuracy decreases after a certain number of reads.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION



SSD Architecture

'TRIM 'Scare. There is a lot of talk that deleted artifacts cannot be reconstructed from TRIM-enabled SSD drives, due to garbage collection (GC) operation in the background even after the device is switched off. Exceptions are always there. TRIM does not affect most environments in RAID configuration, NAS configuration, older Windows (also does not work on file systems other than NTFS) or on external SSD drives attached as a USB enclosure or connected via a FireWire port.



DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Self Corrosion. Even switching off the affected device immediately after TRIM has been issued, does not stop the destruction. Once the power is back, wiping will continue, even if installed into a write-blocking imaging device. If a self-destruction process has already started, there is no practical way of stopping it. The TRIM command is issued to the SSD controller by the operating system as the user deletes a file or goes for formatting the storage medium. This background garbage collection procedure occurs at the hardware level within the SSD itself and is called as "Self Corrosion."

Over Provisioning. Allocating a specific, permanent amount of free space on an SSD, is a widely- used method for improving both SSD Performance and Endurance and is termed as Over-Provisioning (OP). Providing free space to accomplish the NAND management tasks such as Garbage Collection, Wear-Leveling, Bad Block Management means the SSD does not have to waste time preparing space on demand, a process that requires more time as data is copied, erased, and recopied. NAND flash memory's fundamental unit of is of 4 kilobyte (4KB) page, and there are 128 pages in a block. Write operation can happen one blank (or erased) page at a time. Pages have to be first erased and then written. Erasing take place block wise i.e entire blocks of pages must be erased at one time. The SSD actually writes to a different, blank page and then updates the logical block address (LBA) table (much like the MFT of an HDD).

Solid State Devices have of space for extra write operations, as well as for the controller firmware, failed block replacements, and other unique features that vary by SSD controller manufacturer. The minimum reserve is simply the difference between binary and decimal naming conventions. Performance of the SSD begins to decline after it reaches about 50% of its capacity. 28 GB space out of 128GB resulting configuration as a 100GB SSD with 28% over-provisioning.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Wear leveling. To extend the life of SSDs a process termed as Wear Leveling is used. Data is stored in blocks in SSDs and each block can tolerate a limited number of erase cycles before becoming unreliable. For example, SLC NAND flash is typically rated at about 100,000 program/erase cycles. In Wear leveling data is arranged so that the write/erase cycles are evenly distributed among all the blocks in the storage device. Wear leveling is controlled by the flash controller on the device, and uses a wear leveling algorithm to determine which physical block to use each time data is programmed.

Dynamic wear leveling and Static wear leveling are the two types of solid-state drive (SSD) wear leveling. Dynamic wear leveling pools erased blocks and selects the block with the lowest erase count for the next write. Static wear leveling, on the other hand, selects the target block with the lowest overall erase count, erases the block if necessary, writes new data to the block, and ensures that blocks of static data are moved when their block erase count is below a certain threshold. Static wear leveling is a robust method with most efficient use of memory array maximizes device life but requires high power consumption and can slow write operations. While Dynamic wear leveling is easier to implement and does not have impact on the device performance.

SSD Forensic Challenges

TRIM Impact on Forensics. Theses commands are executed by the microcontroller, once triggered cannot be stopped. TRIM commands will finish even if the SSD is powered cycled. A cyber investigator will not be able to read deleted data from a TRIM-enabled SSD, and users can effectively erase whole partitions just seconds before acquisition.

Wear Leveling Impact on Forensics. It concern forensic examiners for two more reasons. First examiners may get a different hash value each time they image solid state drive. Hash values are a mathematical algorithm represented. By a string of numbers and letters that are unique to a set of data, much like a digital fingerprint. Forensic examiners use hash values to verify they have an exact, bit for bit, copy of the original data prior to analysis. The original hash value of the data, and the copy, should be the same. Secondly, an examiner will find it difficult to forensically recover data such as deleted files. The valuable data can appear at any location in the memory array instead of where it should be due to wear leveling and over.

Compressing Controller Effect on Forensics. Compression algorithms are proprietary to the chipset manufacturer hence there is no way to decompress data through off-chip analysis. These SSDs have to be sent back to the manufacturer which is an expensive and time-consuming process and is subscribed to only in most critical investigations.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Other Challenges. Many other issues playa spoilsport during forensic investigation of SSDs.

- IDE interface allows logical data reads, but hides the internal data structures.
- Internals of SSDs are not well understood. There may be many places where forensic value data may be hidden.
- Since there are no accepted standards, every manufacturer does as per his will. They also protect their implementation details from being read.
- Due to NAND flash technology the same techniques which are used on HDD cannot be used.
- Carving and free space analysis if possible is a formidable task.

SSD Forensics

Hardware. SSD drive are either attached directly to the computer's SATA interface or connected via a write blocking device of the same type that is also used to investigate magnetic hard drive. Write blockers prevent user-induced modification to the data stored on the SSD drive, not that of the TRIM command and the disk's internal garbage collector. It is essential to realize that an SSD drive connected via a write blocking device will continue performing background garbage collection, possibly destroying the last remnants of deleted information from the disk. Preventing the operation of the internal garbage collection is only possible by physical disconnecting the build-in controller from actual flash chips, and accessing information stored in the chips directly. This method is not popular as it requires special skills and custom hardware.

PC-3000 Flash SSD Edition. Professional hardware-software solution for recovering data from all types of Flash memory based storage devices (USB Flash, SD, MS, XD, MMC, CF, Voice Recorder, iPhone, and SSD when standard interface of such drives can't access data.

SSD Adaptors. Adapters are used to image SSQ's SATA forensic bridges or duplicators.

Imaging M.2 and PCI-E SSDs. Imaging and M.2 or PCI-E SSD drive requires the use of a dedicated adapter. Considering that are at least three different types of M.2 SSDs (here we will not talk about the differences between B-Key and M-key connectors), you are looking for a solution to support M.2 SATA (AHCIL M.2 PCI-E (AHCI) and M.2 PCI-E (NVMe) devices. Atola Disk Sense is one of the hardware imaging device that creates forensically sound disk images that can be analyzed with software forensic tools.

Software. Software analysis tools can take over once an image of the SSD is created. Tools such as Nuix, Encase, FTK, Cyber Check and Belk soft Evidence Center can be used for analysis. Belk soft Evidence Center is an integrated solution for forensic analysis of computer and mobile devices with support for 700 types of digital evidence: pictures and videos, documents, mobile apps, encrypted files and volumes, data from browsers, instant messengers, clouds and social media, system files, registries, SQLite databases, and more.

Future of SSD Forensics. By physically detaching the controller and using custom hardware toread information directly from the flash ships, investigators could extract traces of destroyed information that could be stored in various areas of the flash chips.

A group of scientists from University of California designed an FPGA-based device providing direct access to flash chips of the SSD drive while bypassing the controller. The researchers estimated the cost of their prototype as $1000, while their estimate for building production units using microcontrollers instead of FPGA's was as little as $200.

Conclusion

Technology is evolving at a rapid pace around the globe and the Solid State Devices (SSDs) have spearheading the storage wars in the digital world. Faster speed, low power consumptions and absence of moving parts are the need of the hour and the SSDs have placed all these on the table for you. But are giving sleepless nights to the forensic investigators who are running against time when the SSDs arrive for cyber forensic investigation. Maintaining integrity because of garbage collection, recovery of deleted data due to secure delete, smart carving, data remapping, free space analysis, hardware and software for analysis tools and many other questions are left for the forensic investigator to answer. How will these questions be answered only time will tell.

References

1. What Has Changed in 2016 in the Way SSD Drives Self-Destruct Evidence. Demystifying eMMC, M.2, NVMe, and PCI-E. by Yuri Gubanov, Oleg Afonin (Belk soft Research)
2. Recovering Evidence from SSD Drives: Understanding TRIM, Garbage Collection and Exclusions Yuri Gubanov, Oleg Afonin (Belk soft Research)
3. http://chang-gu.blogspot.in/2015/06unique-challenges-in-ssd-forensic.html
4. http://www.seagate.com/in/en/tech-insights/ssd-over-provisioning-benefits-master-ti/
5. http://www.samsung.com/global/business/semiconductor/minisite/SSD/global/html/whitepaper"/whitepaper05.html
6. http://searchsolidstatestorage.techtarget.com/definition/wear-leveling
7. http://www.iacpcybercenter.org/solid-state-drives-ssd-issues-and-challenges/
8. http://www.slideshare.net/digitalassembly/challenges-of-ssd-forensic-analysis

About the Author

Santosh Khadsare is an Information Security professional who specializes in Digital Forensics. He is a B.E (Electronics and Telecommunications) and possesses additional qualifications such as CHFI, CEH, RHCSA, Advance Cyber Forensic Course (CDAC), Cyber Crime Investigator, Access Data Certified Professional. He has 17 years plus of rich experience in field of Information Security, Digital Forensics, Cyber Audit, Cyber Laws and Incident Response, He has been a speaker in various international conferences such as **C0C0N 2016, HAKON 2016, National Cyber Defense Summit 2016** and **GovInfoSec Summit Asia 2016**.He has also authored various articles on information security and Digital forensics in national and international publications. He also won the COMMUNITY STAR award at NULLCON International Cyber Security Conference 2017.

Lt. Col. (Dr.) Santosh Khadsare (Retd.)

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Interview Questionnaire - Ms. Rakhi R Wadhwani

1. As a seasoned expert in cyber security, could you provide a brief overview of your career journey, highlighting key milestones and pivotal moments that have shaped your expertise in this field?

My journey in the infosec space has been very enriching, exciting and full of challenges. The learnings and discussions you have on a day-today basis working with colleagues and customers always encourage me to take another step further.

I found the Information Security to be fascinating and decided to pursue this as the application of the skill is endless. Now it has been more than 23+ years since I started looking at getting work in this domain and the excitement keeps me going.

My journey into the cyber security domain was not by my choice. Even in the school days, there were no specific choices for this domain. However, I always wanted to be in the technology domain. As it happened, my first job was in Information Technology; this is when I realized my passion for cyber security which I then took up seriously to build my professional career.

2. Cyber security is a rapidly evolving domain. How do you recommend aspiring cyber security professionals stay current with industry trends and advancements, and what resources or strategies have been particularly valuable in your own professional development?

The world of security is dynamic and ever-changing, necessitating ongoing learning and adaptation. Whether you work in security, own a business, or are just curious, you should keep up with the latest security trends and best practices to protect your information and assets from physical attacks, cyberattacks, and other dangers.

- Following security news publications that cover breaking news, emerging threats, industry changes, and perspectives from experts.
- Reading security blogs that provide in-depth analysis, insights, tips, and guidance from security professionals, practitioners, researchers, and enthusiasts.
- Security podcasts are an excellent way to keep up with the most recent security trends and best practices if you prefer to listen to reading.
- Attending security webinars that include live or recorded presentations, demonstrations, discussions, and Q&A sessions on various security themes, concerns, and solutions.
- Enrol in security courses that offer structured and complete learning paths, modules, tests, and certifications if you want to go deeper and obtain additional skills and knowledge on certain security domains, subjects, or technologies.
- Finally, joining security communities that provide platforms, forums, networks, and events for security professionals, enthusiasts, and learners to interact, collaborate, share, and learn from one another.

3. In your extensive experience, what do you believe are the most critical skills and qualities that aspiring cyber security professionals should cultivate to excel in the field?

India is one of the most targeted nations in the world, and in recent years, server access assaults, ransomware attacks, and data thefts have attacked our businesses in particular. Finding the security experts to take on these positions is crucial, but given how ransomware has taken off, it's obvious that these needs should be given more of a priority. There are a select few most sought-after skills for ambitious professionals who are eager to pursue a career in cybersecurity.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

- Understanding of Malware: It's highly valued to be able to employ modern threat prevention tools that are made to find, recognize, and block advanced persistent threats. There are modern systems that successfully identify malware by utilizing AI/ML technologies.
- Familiarity with these tools is essential:
    - Programming and coding expertise is required for the majority of technology-related employment.
    - Understanding of Network: Security breaches frequently target network vulnerabilities. Cybersecurity specialists need to be aware of how the network used by their company operates.
    - Knowledge of Encryption: Cybersecurity experts should have a solid understanding of data encryption techniques that can safeguard data and prevent illegal access.
    - Threat Modelling: A crucial skill since it serves as the foundation for identifying security requirements and creating security policies.
    - Risk Assessment: It can be useful to be responsible and skilled at seeing potential hazards and evaluating their seriousness and potential impact.
    - Collaboration: Collaboration is key to exploiting weaknesses and spotting threats. When it comes to handling breaches and incident response, the position also calls for collaboration with other corporate units.
    - Threat Knowledge: It's critical to stay informed on the threat environment and various attack vectors.
    - Controls and Frameworks: An organization's data and business activities can be secured with the aid of a cybersecurity framework, which offers a set of best practices, rules, tools, and security protocols.
    - Cloud Security: As more and more companies transition to cloud environments, having knowledge of cloud security is essential.
    - The development of cyber resilience requires the use of cyber literacy, which also presents an opportunity for increased interaction and collaboration between the public and commercial sectors.

4. Cyber security leaders often face the challenge of balancing robust security measures with business operational requirements. Can you share your perspective on achieving this balance effectively, and how you've managed it in your career?

Organizations constantly struggle to strike the right balance between business needs and security in today's fast-paced, interconnected environment. Strong security measures are necessary to safeguard sensitive data and defend against online threats. Businesses must, however, continue to be flexible, aggressive, and receptive to shifting consumer needs. In order to guarantee long-term success and sustainability, it is crucial to strike the proper balance between these two crucial factors.

I firmly believed that security should always come before commercial needs when I first started my career in security. Conflicts with the business teams did, however, occasionally arise when we unintentionally constituted a bottleneck for their requirements. I improved my knowledge of many business fields as I advanced in my profession and was exposed to the business side of operations, and I also grew more adaptive and agile.

I now have a better understanding of the missions and objectives of organizations, and I also see how crucial it is to strike a balance between commercial needs and security requirements. It was vital to interact with the business side, understand their needs, and deliver targeted security suggestions and implementations rather than pushing solutions out of context.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Security personnel can benefit the firm by adopting a more business-focused mentality. Making better decisions when deploying security measures is made possible by understanding the complexities of the business. Security experts can learn about the goals, difficulties, and priorities of business teams by actively engaging with them. Security experts can recommend and put into place security measures that are in line with the particular requirements and risk tolerance of the firm thanks to this collaboration.

Together, security and business teams may create cutting-edge solutions that safeguard vital assets while easing the accomplishment of corporate objectives. It is crucial to recognize that security is a tool to support the broader goals of the company and not a goal in and of itself. With this strategy, security is maintained as a facilitator rather than a barrier. Here are some tactics for striking a balance between business needs and security requirements: Security By Design, Risk Assessment and Prioritization, Collaboration and Communication, Continuous Monitoring and Adaptation, Employee Education and Awareness

5. Many organizations today face a shortage of cybersecurity talent. What advice do you have for CISOs and leaders on attracting and retaining top cyber security talent in their teams?

Attracting and retaining top cybersecurity talent is a critical challenge for many organizations today, given the increasing importance of cybersecurity in the digital age. Here is some advice for Chief Information Security Officers (CISOs) and leaders on how to address this talent shortage effectively:

- **Competitive Compensation:** Offer competitive salaries and benefits.
- **Professional Development:** Invest in professional development opportunities.
- **Career Advancement Paths:** Provide clear career advancement paths within the organization.
- **Challenging Projects:** Assign challenging and meaningful projects to cybersecurity team.
- **Flexible Work Arrangements**: Consider offering flexible work arrangements which helps attract talent from diverse locations and accommodate work-life balance.
- **Supportive Work Environment:** Foster a supportive and inclusive work environment.
- **Recognition and Rewards:** Recognize and reward outstanding performance.
- **Collaboration and Learning:** Encourage collaboration and knowledge sharing among team members.
- **Cybersecurity Culture:** Promote a cybersecurity culture throughout the organization.
- **Recruitment and Networking:** Build a strong recruitment and networking strategy.
- **Employee Feedback:** Regularly seek feedback from the cybersecurity team.
- **Cybersecurity Tools and Resources:** Provide your team with the best tools and resources to do their jobs effectively.
- **Mentorship and Leadership Development:** Implement mentorship programs and leadership development initiatives.
- **Incentives for Staying Current:** Offer incentives for staying current with the rapidly evolving cybersecurity landscape.
- **Cybersecurity Awareness and Training for All Employees:** Promote cybersecurity awareness and training not just for the cybersecurity team but for all employees.
- **Diversity and Inclusion Initiatives:** Embrace diversity and inclusion initiatives.

Remember that retaining cybersecurity talent is an ongoing process. Continuously assess your strategies and adapt them to the evolving needs and expectations of your team members. By prioritizing the well-being and professional growth of your cybersecurity professionals, you can build a strong and resilient cybersecurity team.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

6. You've specialized in areas like Digital Forensics, Ethical Hacking, and Information Security and Privacy. How have these specializations allowed you to contribute significantly to enhancing cyber security within organizations?

It is difficult to think of one 'major contribution' so I shall let that pass because every assignment has brought about a sense of accomplishment learning and joy. So, every assignment is a major contribution to my own growth and to the growth and well-being of the organization for which it was done.

7. For cyber security students aiming to specialize in areas like Information Risk Management or Regulatory Compliance, what guidance or career pathways would you suggest to help them achieve their goals?

Specializing in areas like Information Risk Management or Regulatory Compliance within the field of cybersecurity can be a rewarding career choice, as organizations increasingly recognize the importance of managing risks and complying with data protection regulations. Here are some guidance and career pathways to help students achieve their goals in these specialized areas:

- **Foundation in Cybersecurity**: Start by building a solid foundation in cybersecurity.
- **Cybersecurity Education**: Pursue formal education in cybersecurity.
- **Certifications**: Obtain relevant certifications: Consider certifications such as: Certified Information Systems Security Professional, Certified Information Security Manager, Certified in Risk and Information Systems Control, Certified Information Systems Auditor, Certified Risk Manager, Certified Regulatory Compliance Manager, etc.
- **Gain Practical Experience**: Gain hands-on experience through internships, entry-level positions, or cybersecurity-related projects.
- **Specialized Training**: Seek specialized training in risk management and compliance.
- **Legal and Regulatory Knowledge**: Develop a deep understanding of relevant laws and regulations.
- **Soft Skills**: Develop strong communication, problem-solving, and analytical skills.
- **Networking**: Join professional organizations and attend industry conferences.
- **Specialization in Risk Management**: If you're interested in information risk management, consider specializing further in areas such as enterprise risk management, cybersecurity risk assessment, or business continuity planning.
- **Specialization in Regulatory Compliance**: For regulatory compliance, focus on specific industries like healthcare (HIPAA), finance (PCI DSS), or international data protection regulations (GDPR). Gain expertise in the relevant compliance frameworks.
- **Consulting or In-House Roles**: Decide whether you want to work in a consulting capacity, helping multiple clients with compliance and risk management, or if you prefer an in-house role within an organization. Both offer unique career paths.
- **Continual Learning**: Cybersecurity is an ever-evolving field. Stay committed to continuous learning and professional development to remain current with emerging threats, technologies, and best practices.
- **Build a Portfolio**: Document your projects, achievements, and contributions in risk management or compliance. Having a portfolio of your work can be valuable when applying for jobs or promotions.

Remember that career paths in cybersecurity can vary, and it's essential to align your education and experiences with your specific interests and career goals. Networking with professionals already established in the field can provide valuable insights and guidance for your journey.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

8. In your role as a trainer in cyber security, what key principles or best practices do you emphasize to help students bridge the gap between theoretical knowledge and practical skills in the field?

Bridging the gap between theoretical knowledge and practical skills in cybersecurity is essential for students to become effective professionals in the field. As a cybersecurity trainer, I would emphasize several key principles and best practices to help students develop this critical bridge:

- **Hands-On Labs and Projects**: Encourage students to participate in hands-on labs, capture-the-flag (CTF) challenges, and real-world projects. These activities help students apply theoretical concepts to practical scenarios.
- **Simulations and Cyber Ranges**: Cyber Security Simulations, Virtual Environments and Cyber ranges provide a safe space for students to practice defending against and mitigating cyberattacks and these exercises mimic real-world scenarios and enhance practical skills.
- **Problem-Solving Skills**: Cybersecurity often involves complex and rapidly evolving threats. Teach students how to analyze problems, research solutions, and adapt to new challenges.
- **Tool Proficiency**: Familiarize students with essential cybersecurity tools and technologies. Ensure they understand how to use firewalls, intrusion detection systems, vulnerability scanners, and other security software effectively.
- **Critical Thinking and Decision-Making**: Train students to think critically and make informed decisions under pressure as quick and effective decision-making can be crucial to mitigating threats.
- **Risk Assessment and Management**: Teach students how to conduct risk assessments and prioritize security measures based on the level of risk. This includes identifying vulnerabilities, assessing their potential impact, and developing mitigation strategies.
- **Ethical Hacking and Penetration Testing**: Encourage students to explore ethical hacking and penetration testing. These activities involve actively trying to identify vulnerabilities in systems, applications, or networks, providing practical experience in assessing security.
- **Incident Response Training**: Help students understand the incident response process. Simulate security incidents and guide them through the steps of detection, analysis, containment, eradication, and recovery.
- **Secure Coding Practices**: If applicable, emphasize secure coding practices. Developers with cybersecurity knowledge can write more secure code, reducing vulnerabilities in software applications.
- **Continuous Learning**: Instil a culture of continuous learning in students. The cybersecurity landscape evolves rapidly, so staying up-to-date with the latest threats, technologies, and best practices is essential.
- **Soft Skills**: Highlight the importance of soft skills, such as communication, teamwork, and presentation skills. Effective communication is vital when explaining complex security issues to non-technical stakeholders.
- **Certifications and Industry Standards**: Encourage students to pursue relevant certifications like CompTIA Security+, Certified Information Systems Security Professional, Certified Ethical Hacker, etc.
- **Real-World Scenarios**: Use real-world examples and case studies to illustrate the practical application of cybersecurity principles. Share stories of cybersecurity incidents and how they were mitigated.
- **Collaborative Learning**: Foster a collaborative learning environment where students can share their experiences and learn from each other. Group projects and discussions can enhance practical understanding.
- **Mentorship and Internships**: Encourage students to seek mentorship opportunities and internships in the cybersecurity field. Learning from experienced professionals can provide valuable practical insights.

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

By focusing on these principles and best practices, cybersecurity trainers can help students develop the skills and mindset needed to bridge the gap between theory and practice effectively in this ever-evolving field.

9. Building relationships and collaboration are crucial in cyber security. What strategies have you employed to effectively communicate security priorities and cultivate a culture of security awareness within organizations?

Employees' understanding of and attitude toward securing the data and computer systems of their company is known as security awareness. It is crucial for stopping cyberattacks, data breaches, and compliance infractions that could damage the company's reputation and performance. But many businesses find it difficult to instil a culture of security awareness among their employees, particularly when those employees work remotely or with personal devices.

- Evaluate your present level of awareness: The first step in raising security awareness is to assess the gaps and hazards that need to be closed in your current situation.
- The second stage in raising security awareness is to give your employees frequent training and instruction that is tailored to their individual positions and responsibilities.
- Reward good behaviour and constructive criticism: The third stage in raising security awareness is to reward good behaviour and constructive criticism among your employees.
- Including leadership and organization stakeholders and making them role models and champions of security culture is the fourth stage in raising security awareness.
- Implementing and enforcing rules and controls that outline and govern the security standards and expectations inside your business is the fifth step in raising security awareness.
- Measuring the performance of your awareness program and its effects on your company is the sixth step in raising security awareness.

10. As a respected author in the field, what inspired you to share your knowledge and insights through your publications, and how do you believe these resources benefit both students and industry professionals?

Authors in various fields are often motivated by a combination of factors when sharing their knowledge and insights through publications:

- Passion for the Subject
- Desire for Impact
- Academic and Professional Recognition
- Educational Purposes
- Industry Advancement
- Personal Fulfilment

The benefits of these publications are significant for both students and industry professionals such as but not limited to: Knowledge Transfer, Skill Development, Problem Solving, Networking and Collaboration, Career Advancement, Innovation and Progress.

11. Can you highlight emerging cyber security trends or challenges that CISOs and leaders should be prepared to address in the coming years, and how they can navigate these evolving landscapes?

Due to the widespread use of computerized systems in industry, organizations, and even governments due to the Digital Revolution, cybersecurity has become a top priority to protect data from various online assaults or any unwanted access.

- **Growing Trend in Automotive Hacking:** The usage of Bluetooth and Wi-Fi by current automobiles for communication exposes them to a number of security flaws and hacker risks.
- **AI's potential:** Building automated security systems, natural language processing, facial detection, and automatic threat detection all rely heavily on AI. Threat detection systems with AI capabilities can anticipate new assaults and immediately alert administrators to any data breach.
- **Mobile is the New Target:** All of our personal information, including our emails, texts, financial transactions, and images, poses a greater risk to us as people.
- **Cloud is also potentially vulnerable**: Although cloud applications still have strong security measures in place, user mistake, malicious software, and phishing attempts often originate at the user end.
- **Data Breach:** Data is the new OIL. Any minuscule glitch or error in the system creates a potential opening for hackers to access user data.
- **IoT with 5G network**: The connectivity between numerous devices creates openings for outside interference, assaults, or an unidentified software issue.
- **Automation and Integration:** With today's frantic work demands, experts and engineers are under more pressure than ever to provide rapid and effective solutions.
- **Targeted ransomware:** Industries in industrialized countries rely substantially on particular software to carry out their regular operations.
- **State-Sponsored Cyber Warfare:** Even if there have been few attacks, the friction between the western and eastern worlds frequently makes international headlines and has a big impact on events like elections.
- **Insider Threats:** Human error continues to be one of the main causes of data breaches. Millions of stolen data can bring down a whole corporation on any bad day or purposeful loophole.
- **Cybersecurity for Remote employees:** Because they frequently use less secure networks and devices, remote employees may be more susceptible to cyberattacks.
- **Social engineering attacks**: Businesses need to make sure that their employees are taught to spot unusual conduct and report it, as well as that there are safeguards in place to guard against these kinds of attacks.

12. Lastly, what motivates and sustains your passion for cyber security and compliance work, and what words of encouragement or inspiration would you offer to those pursuing a career in this ever-evolving and critical field?

At one stage, the pursuit of material wealth was definitely a big motivation factor. So, what really motivates me is the challenge of solving technical and people problems, and learning constantly.
I would suggest, to get involved in the security community. This is a good way to network with other professionals, a great way to learn and a good way to help others. Joining local security community has opened up so many opportunities as well as opportunities to give back to the community.

Ms. Rakhi R Wadhwani

Volume 8 | Issue 4 | November 2023 | INR 500

www.digital4n6journal.com

EDITORS :

Ms. Seema Khadsare

Ms. Rakhi R. Wadhwani

Jyoti Nene

Evita K Breukel

Deep Shankar Yadav

DIGITAL FORENSICS (4N6)

INDIA'S 1st DIGITAL FORENSICS PUBLICATION