TITLE: Digital Forensic

Theme I- Role of Digital Evidence

Sub Theme: The Evolving Role of Digital Evidence in Modern Economy

Team Code: TC 232

Author: Vaishnavi C

2nd Year BBA LLB student at School of Law, Dayananda Sagar University,

Innovation Campus, Kudlu Gate, Hosur Road, Bangalore – 560 114,

INDIA

Email: Mahvaibind@gmail.com

Phone no: +91 7406653051

Co-Author: Chaitanya G,

2nd Year BA LLB student at School of Law, Dayananda Sagar University,

Innovation Campus, Kudlu Gate, Hosur Road, Bangalore – 560 114,

INDIA

Email: kchaithanya918@gmail.com

Phone no: +91 7204874204

Introduction:

The digital economy has emerged as an innovative economy that utilizes digital technologies and electronic communication to conduct economic and business activities across a wide range of sectors, including e-commerce, digital marketing, digital financial services, software development, computer games, and cloud services. The use of digital technologies and electronic communication has resulted in a significant shift towards online business interactions, leading to improved user experiences, faster processing, and easier access to services and products. The digital economy has significant impacts on various economic, social, and cultural fields, including changes in the way people work and interact with each other, promoting more flexible and remote work arrangements, and increasing global connectivity. Additionally, the digital economy has impacted education, healthcare, entertainment, and other sectors. Advances in technology and electronic communication have driven the global economy towards digitization, and the role of the digital economy in advancing global digitalization is critical. Its impact is expected to continue to increase in the coming years.

How Digital Evidence has been Evolved in Forensic Science:

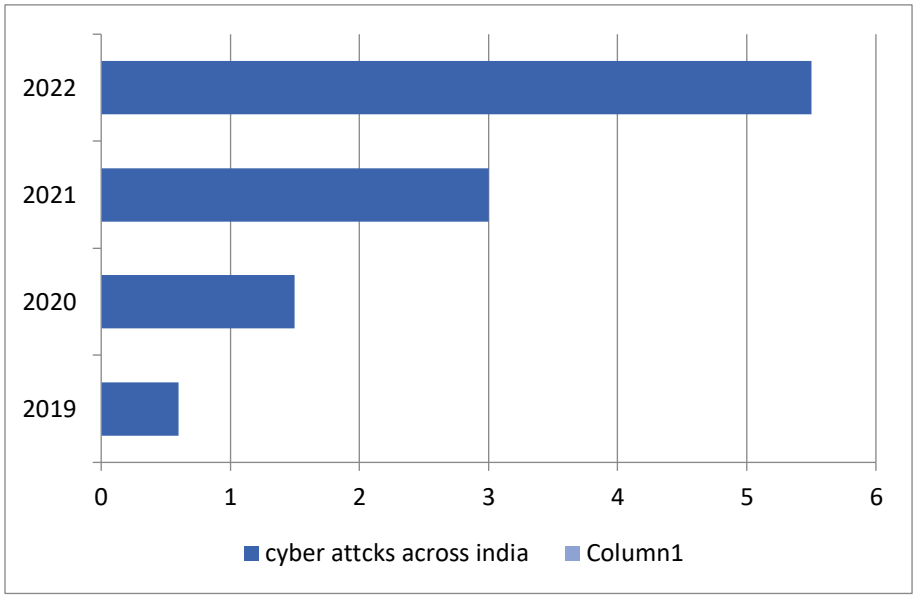
The Information Technology (IT) Act, 2000, which established the legal recognition of digital evidence and laid the groundwork for forensic investigations, gave rise to digital forensics in India. An urgent need for forensic competence resulted from the quick rise in cybercrime, which includes hacking, data breaches, and online fraud, as well as growing reliance on digital devices. Progress was slowed by early obstacles like a shortage of skilled personnel, poor infrastructure, and low awareness, **but notable events like the 2008 Mumbai terror attacks and well-known cases like the Sunanda Pushkar death case highlighted the significance of digital intelligence collection.** Forensic capabilities have expanded in both the public and commercial sectors as a result of government initiatives and training programs that helped close the skill gap. It is always changing in tandem with technological breakthroughs, regulatory frameworks, and cybersecurity measures to effectively counteract digital threats.[1]

Cyber Security and Digital Evidence: Protecting and proving in Digital World:

[1]International Journal of Digital Evidence Spring 2002 Volume 1, Issue 1
https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

Digital evidence collection is crucial in cybersecurity, it serves as the backbone for investigating cybercrimes and breaches. **This process involves the accurate gathering, preservation, and analysis of data from various digital sources, including computers, networks, and mobile devices.** Effective evidence collection requires conformance to legal and procedural standards to ensure that the evidence remains intact and admissible in court. Advanced tools and techniques, such as forensic imaging and live memory analysis, are employed to capture volatile data and trace cyber threats accurately. Ultimately, the ability to collect and analyse digital evidence not only aids in solving crimes but also strengthens overall cybersecurity defences by identifying vulnerabilities and preventing future incidents. [2]

The Cost of Cyber Attacks: India's Digital Crime Report:



More than 1.3 million Cyber Attacks were reported across India in 2022. This was a significant increase compared to 2019. India saw a significant jump in Cyber Crimes reported in 2022 from the previous year. That year, over 65 thousand Cyber Crime incidents were registered.

[2] https://www.geeksforgeeks.org/

Karnataka and Telangana accounted for the highest share during the measured time period. furthermore, **India's ranked third in terms of internet user numbers**.[3]

The year 2024 has marked a new high in Cyber Crimes in India. As per data, the number of **average complaints has increased to 7000 per day**. In just the first 4 months, around **7,40,000 cases** were registered on the Cyber Crime portal, and this number surged to **12lakh** by September 2024. beyond the shocking case numbers, there are huge losses of capital too. Victims have collectively loss over **₹120 crores** to cyber frauds in the first nine months of 2024 alone. This depicts that **cybercrime in India** is **increasing significantly, demanding immediate attention and action.**

From Screens to Cells: "How Digital Evidence Leads to Modern Arrests"

The rise of technology has transformed the criminal justice system, with digital evidence playing a critical role in solving modern crimes. From **incriminating WhatsApp messages to GPS data pinpointing a suspect's location,** the digital footprint often provides crucial leads in criminal trials. In India, the legal framework governing digital evidence has evolved, but challenges such as admissibility, jurisdiction, and privacy concerns remain significant hurdles. India has taken significant steps to incorporate digital evidence into its judicial system. Several laws and amendments govern the collection, preservation, and admissibility of digital evidence.

Key Legislations

Indian Evidence Act, 1872: Sections 65A talks about Secondary evidence may be given of the existence, condition, or contents of a document in the following cases which cannot conveniently be examined in Court and the fact to be proved is the general result of the whole collection and Section 65B specifically addresses the admissibility of electronic evidence, and also digital records must be certified to be admissible in court.

Information Technology (IT) Act, 2000: Recognizes electronic records and digital signatures as valid evidence. Provides safeguards against cybercrimes, such as hacking and identity theft.

Bharatiya Nyaya Suraksha Sanhitha (BNSS) 2023: Governs the procedures for the collection, seizure, and examination of digital evidence.

[3] Published by Tanushree basuroy ~Dec 6th, 2023 https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/#statisticContainer

Bharatiya Nyaya Sanhitha (BNS) 2023: Penalizes cybercrimes and provides guidelines for prosecuting offenders. These laws create a robust foundation, but practical challenges often arise due to gaps in implementation and technical understanding.[4]

"The critical role of Digital Evidence in Modern Law Enforcement"

Dark Web forensics involves the identification, collection, preservation, extraction, and investigation of digital evidence from the Dark Web, with the aim of presenting it in a legally acceptable format. It's crucial that this evidence is admissible in court. To investigate cybercrimes facilitated through the Tor browser (which is often the gateway to the dark web), forensic experts must obtain RAM dumps from the suspect's device and analyze them to uncover any malicious activities conducted through the Tor browser. This may include tracing visited websites, accessed emails, and downloaded programs. Maintaining a robust chain of custody is crucial in digital forensics to track the handling of evidence from collection to presentation in court. This involves documenting each individual who accessed the evidence, the actions taken, and ensuring the evidence remains unaltered. Emerging technologies, such as blockchain, are being explored to enhance the traceability and integrity of digital evidence chains. Statistics reveal fascinating insights about its use, such as the amount of illegal content, cybercrime trends, and even marketplaces for stolen data. However, not everything on the dark web is unlawful. [5] "**At least 20 per cent of cybercrimes in India involve the usage of the dark web by online attackers,**" this is the study conducted by Lisianthus Tech.

"**The cases related to Dark Web and How it made them compensate for it"**

Peter Scully case

This is one of the most horrifying stories on this list. Peter Scully, an Australian citizen, is serving a life sentence in the Philippines after being convicted of raping minors and human trafficking. **He is also on trial for torture, murder, and spreading child pornography**. He did all these horrifying acts, recorded and uploaded them on the dark web.

The Silk Road

This infamous marketplace on the **dark web operated between 2011 and 2013 with a total sale revenue of 9.5 million bitcoins**. The creator, Ross Ulbricht (Dread Pirate Roberts), is

[4] Published by Sneha Mahawar ~April 3rd, 2022 https://blog.ipleaders.in/all-you-need-to-know-about-section-65-of-the-indian-evidence-act-1872/#Section_65A_of_Indian_Evidence_Act_1872
[5] Published by Juhan H ~ feb 26th, 2025 https://preyproject.com/blog/dark-web-statistics-trends

estimated to have **grossed over 13 million in the site's two years of operation**. The platform was a real dark market where merchants sold their products as they would on Amazon or eBay. Drugs, guns, or other illegal products and content were just a few clicks and Bitcoins away. You could buy anything you want. Ross was eventually apprehended in 2013 through investigative techniques and operational security mistakes on his part. **He was sentenced to life imprisonment for creating and operating the platform**. However, similar platforms like Deep Bay, Sheep Marketplace, RAMP, and Black Market Reloaded are still operational on the dark web.

Conclusion

Digital evidence has become a cornerstone of modern forensic investigations, shaping law enforcement, cybersecurity, and legal proceedings. The rise of cybercrimes, fueled by the expanding digital economy, necessitates robust forensic capabilities and legal frameworks like the IT Act, 2000, and Bharatiya Sakshya Adhiniyam, 2023. Challenges such as jurisdictional issues, privacy concerns, and dark web activities demand continuous advancements in forensic tools and investigative techniques. Strengthening digital evidence collection, preservation, and admissibility is crucial for combating cyber threats. By enhancing cybersecurity measures, global cooperation, and forensic expertise, digital evidence will remain a powerful tool in ensuring justice in the digital era.