National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

INDIAN DIGITAL FORENSIC MARKET REPORT (2025)

Knowledge Partner

Deloitte.

Table of contents

Foreword

While digitisation has contributed to the country's progress, it has also created a larger playground for cybercriminals. Cybersecurity threats have increased in number and complexity. This intricacy and surge in online criminal activities have made it essential to implement advanced data security measures and deploy effective digital forensics tools and technologies to combat and prevent these threats.

Digital forensics has become a crucial element in investigations related to cybercrimes, as well as other criminal and civil cases. It provides valuable information to investigators who are tracing an illegal activity while preserving the evidence. It is essential for eliminating cyber threats and is a key part of incident response. The ever-changing nature of cyberattacks, evolving user practices and the complexities associated with rapid technological advancements amplify the demand for digital forensic expertise.

As the scope and demand for digital forensics expand, ranging from criminal and civil investigations to internal corporate inquiries and compliance requirements, the demand for digital forensic tools, services and skilled professionals has surged. This growing demand leads to a paradigm shift in India's digital forensics market, resulting in its ongoing expansion.

This report delves into the dynamics of the digital forensic market, examining key players, emerging technologies and evolving methodologies that drive innovation within the sector. The findings are based on extensive research and insights from global industry, domestic key market players and eminent forensic stakeholders. The diverse perspectives will help readers grasp the complexities of the digital forensics ecosystem and provide the knowledge needed to understand the current market and future trends.

Vinayak Godse
Chief Executive Officer
Data Security Council of India (DSCI)

Foreword

In an era of unprecedented digital expansion, the role of digital forensics has never been more critical. As organisations, governments and individuals embrace digital transformation, the vast proliferation of data has created immense opportunities and significant risks. Cyber threats, data breaches, ransomware attacks, financial frauds, etc., have escalated to an alarming scale, impacting every sector across the globe. Securing digital ecosystems, ensuring data integrity and investigating cyber incidents are no longer optional but imperative.

Today's challenges are more complex than ever and require innovative solutions, adaptability and strong collaborations. Cybercriminals use AI, encrypted communication and emerging technologies to evade detection, making forensic investigations increasingly difficult. Deepfake technology, digital evidence tampering, jurisdictional complexities and cross-border cybercrimes further complicate the landscape.

Digital forensics has emerged as a critical security, compliance and governance pillar. From financial institutions securing transactions and multinational corporations safeguarding Intellectual Property (IP) to law enforcement agencies tracking cyber criminals, its role is indispensable in today's digital landscape. As one of the fastest-growing digital economies, India is at the forefront of digital transformation. With over a billion digital users, an expanding fintech ecosystem and an evolving regulatory landscape, the need for advanced digital forensics capabilities has never been greater. From law enforcement agencies investigating cybercrimes to enterprises securing critical infrastructure, India presents an immense growth opportunity for forensic solutions, skill development and innovation. The nation's ability to build forensic resilience, invest in cutting-edge technology and develop a skilled workforce will determine how it can safeguard its digital future.

As a global leader in consulting, Deloitte has worked alongside governments, Fortune 500 companies and law enforcement agencies to help them navigate this evolving landscape. Our experience has reinforced the fundamental truth that digital forensics is no longer about responding to cyber incidents but building resilience, mitigating risks and maintaining trust in the digital world.

This report offers deep insights, strategic evaluations and a forward-looking perspective on the digital forensics market. It serves as a call to action for businesses, governments and industry leaders to embrace forensic innovation, strengthen global collaboration and shape the future of digital security. Though the challenges ahead are significant, the opportunities to redefine digital forensics globally have never been greater.

Nikhil Bedi
Partner and Leader -
Risk, Regulatory & Forensic
Deloitte India

Executive summary

The Indian digital forensics market has experienced steady growth in recent years and is valued at approximately INR1,603 crore (US$0.19 billion) for FY2023–24. The market is poised for rapid expansion and is estimated to reach INR11,829 crore (US$1.39 billion) by FY 2029–30, reflecting a CAGR of nearly 40 percent during this period. The global digital forensics market, valued at INR53,950 crore (US$6.5 billion), is projected to grow at a CAGR of 11 percent and reach approximately INR1,20,350 crore (US$14.5 billion) by 2030.

The Indian digital forensics market is anticipated to expand its share of the global market from the current 3 percent to 10 percent by 2030. This rapid growth can be attributed to India's evolving digital forensic sector, which is developing faster than the more mature global market.

Market segmentation by component reveals that software has the biggest market share (54 percent), followed by services. However, there is an increasing need for services in the government and private sectors, which is projected to play an important role in the future.

Market segmentation by end-user reveals that government is the largest user, with 81 percent market share in the digital forensics market. Law enforcement agencies make the highest contribution in this segment, with cybercrime investigations accounting for the largest share, followed by cybersecurity incident response. The government is primarily focused on procuring forensic products and tools, while services lead the private sector. Growth is expected to increase across these sectors in the coming years.

Market segmentation by type reveals that mobile forensics occupies 55 percent of the segment and is expected to grow significantly because of its broad and varied use. The market size of the "Others" segment, which includes cloud forensics, IoT forensics and other transformative and emerging technologies, is currently at 13 percent. Due to the rapid advancement of technology and its application across industries, this segment is also anticipated to grow rapidly and take on new dimensions.

Market segmentation in India by region reveals that the Western region leads the market by 32 percent, followed by the Southern region at 30 percent. The Northern region has a steady market of 28 percent, driven mainly by government agencies, followed by the Eastern region. The market is influenced by the government's efforts and each region's unique industrial landscape. Growth is anticipated in all regions of the country, propelled by the public and private sectors.

The digital forensics market in India is anticipated to grow significantly due to the rapid adoption of digital forensics by the government and the public sector and the frequency and complexity of cybercrimes. Other contributing factors include the proliferation of handheld devices, the emergence of transformational technologies, growing awareness of digital security, regulatory and statutory compliances and data privacy requirements.

The government's efforts to establish a developed digital forensic ecosystem, as well as its propensity to produce domestic goods by creating a level playing field for regional firms, is expected to strengthen the growth momentum.

Shortage of trained professionals, high costs associated with adopting digital forensics solutions, increasing complexities and encryption methods, underdeveloped academic and research ecosystems, lack of understanding, inadequate infrastructure and administrative and financial constraints are major restraints that hamper the market growth.

Other possible elements that, if supported, could further advance the digital forensic ecosystem include public-private cooperation, industry-academia collaboration, emphasis on research and development and ongoing innovation, fostering the start-up ecosystem, developing domestic standards, international collaborations, raising awareness and progressive capacity-building initiatives.

Chapter 1

Introduction

Rapid technological breakthroughs and rising digital device usage have led to the proliferation of cybercrimes, which pose serious risks to people, businesses and countries. Cybercrime differs from typical crimes as it is more complicated, borderless and can take many forms. Gaining awareness of its changing transnational features and intricacies is necessary, and everyone involved must coordinate and collaborate for better resolutions. Cybercrimes have wide-ranging effects, including monetary loss, interruptions to business operations and harm to one's reputation.

Numerous cyberattacks are occurring across the country, and it is anticipated that these attacks will rise globally as well. Digital investigators and prosecutors need to understand how cybercriminals operate, assess their methods and plan proactive and reactive measures. Cyber vandals have exploited the interconnected digital world, while forensic techniques have struggled to keep up, raising significant concerns.

This study explores the dynamics, key drivers and industry characteristics of the Indian digital forensics market. It also thoroughly examines and reports on the challenges and opportunities faced by all stakeholders—government organisations, start-ups, resellers, Original Equipment Manufacturers (OEMs) and corporations—to help strengthen the country’s digital forensic ecosystem.

Scope of the study

The report provides an overview of the Indian digital forensics market, covering its current size, segmentation and growth potential. It also includes an analysis of past growth patterns, a projection of future growth and the anticipated CAGR. The market's dynamics are also examined by considering various parameters, including growth drivers, possible disruption risks, and other outside variables that affect the market. Sector-specific insights, including the growth opportunities, challenges and market strategies, have also been analysed. Relative development trajectories, growth trends in the percentage share of the Indian market, and comparative analysis in relation to the global market are also included.

Assumptions and hypotheses

- The period considered for this study is from 2019 to 2023, and the forecast period for calculation is from 2025 to 2030, with 2024 as the base year.
- INR is the base currency. US$ is used for comparison purposes.
- The base year's exchange rate conversion is also considered for the forecast period.
- The sample population for the survey was identified based on primary and secondary research conducted at the beginning of this study.
- Key players for the primary interviews were identified based on their market share and their influence on the digital forensic domain.
- The weighted average was adopted for segmentation analysis, authenticity and closer estimates.
- The bottom-up approach assesses market numbers by aggregating data from individual components, sectors, or companies to estimate the overall market size.
- A top-down approach validated the estimated numbers by starting with the overall market size or trends and breaking them into smaller segments or components.

Market definitions

The digital forensics market refers to the industry operating in areas of products and services related to digital forensics, covering the areas of disk forensics, mobile forensics, memory forensics, drone forensics, e-discovery, etc.

By region

This includes regional segmentation of the digital forensic market based on selling digital forensic software and hardware tools and professional services, including investigations, incident response, consulting, capacity building and support. Sub-groups include region-wise analysis viz., the North, South, East and West regions of the country.

By components

This includes segmentation by digital forensic hardware and software tools and platforms used for performing digital forensic investigations, including data acquisition, processing, analysis, recovery and review. Physical devices include duplicators, write blockers and forensic workstations. Services offered by digital forensic professionals and support provided by OEMs and resellers are also included while segmenting the market under this category.

By types

This includes segmentation analysis by computer forensics, mobile forensics and other digital forensics categories, such as Network forensics, e-mail forensics, cloud forensics, social media forensics, IoT forensics, disk forensics and database forensics.

By end-user

This includes shares occupied by the government and private sector in the end-usage of products or services related to the digital forensics market. Priorities and requirements in these segments, including procurement of goods and services, are studied and reported.

Limitations

- Changes in the inflation rates have not been accounted for while forecasting the market numbers.
- Companies for which financials are not available are also considered on a best-effort basis.
- Unreported developments of companies that have not been officially announced in the public domain are not considered.
- The growth forecast is also based on interviews with key leaders, who may have an optimistic outlook.
- Market segmentation data is derived from inputs provided by key industry players and is considered to be accurate.

Chapter 2

Research methodology

The findings in this report are based on primary and secondary research, along with survey responses from a representative sample of the population. Activities performed in bringing out this report include identification of the major players in the Indian digital forensics market, data collection through surveys and interviews, validation through publicly available information, triangulation (a process of cross-checking data by comparing multiple independent sources), fusion (combining different datasets and insights to create a coherent analysis), analysis, estimation and forecasts using internal models, report preparation and quality check by Deloitte and DSCI between August 2023 and December 2024. Below are the stages of study that were completed before the report was finalised.

Stakeholder identification and preparatory work

- Key players were identified through an extensive study that included discussions with industry executives, interviews and insights from major players, examination of yearly financial reports and analysis of market data.
- The study also included the identification of "new entrant" start-ups and their potential effect on the digital forensic market.
- The identified stakeholders were inclusive, diverse and representatives of government organisations, OEMs, resellers, service providers, corporations, SMEs and academic institutions.
- Mapping of the stakeholders with their corresponding activities, associated products and/or services and end-users was performed.
- The type and nature of information that is available to the respective stakeholders and the mechanisms for obtaining it were determined.

Primary research

- An online digital forensic market survey was rolled out to the representative digital forensic professionals, including government officials, industry leaders, academicians and researchers involved in leadership or management functions to obtain market data, insights and opinions.
- Insights from industry experts across the value chain were gathered through extensive face-to-face or telephonic interviews to obtain quantitative and qualitative inputs.
- Consultations with the stakeholder groups were also conducted to understand the market dynamics.
- The financial statements of the identified stakeholders were collated and analysed from the MCA Portal.
- Critical qualitative and quantitative insights were derived from the data collated during the primary research.
- Validation of data obtained through diverse sources was also performed.

Secondary research

- Meaningful insights on the prevailing market, innovations, advancements in technology and other related information were gathered through secondary sources, including:

Government reports, white papers and press releases

Industry reports, magazines, technical brochures, product specifications blogs and company websites

Research papers, journals and articles, conference proceedings and other publications.

- Information was also gathered through conferences, meetings and brainstorming sessions involving key stakeholders.
- Other publicly available information and proprietary data repositories were also used.

Data triangulation and analysis

- Endogenous and exogenous data collected during the study stages were verified and converted for quantitative and qualitative insights. Preliminary analysis focused on defining the Indian digital forensics market and major players and identifying authentic and key data points to estimate the market size.
- Literature review, analysis and comparison of data from secondary sources were undertaken to gain further understanding of the digital forensic landscape.
- Bottom-up and Top-down approaches were employed, and in-house market estimation and forecasting models were used to estimate market size and growth rates.
- Data triangulation using multiple methods and data sources was undertaken to analyse the data and to arrive at closer to accurate estimates.
- Market segmentation was based on primary interviews with industry experts and other corresponding inputs from secondary sources.
- The weighted average was considered to obtain the market segmentation and ensure accuracy.
- Historical growth data was analysed and trends were identified to develop the estimates.
- Impact analysis was performed to identify major factors, including the drivers and restraints, that would influence the market.
- Variables that could potentially influence the forecast were identified and factored.
- A comparative analysis of the global and Indian digital markets was conducted to determine the percentage and relative growths of the Indian market in the global arena, both now and in the future.

Quality assurance and report creation

- Reviews were undertaken by Deloitte India and DSCI teams for quality checks and validation at various levels.
- Sanity checks by Industry leaders, experts and professionals were also performed.
- A holistic research methodology was adopted to estimate and forecast quality output.
- The report's contents were thoroughly scrutinised and questioned for accuracy and reliability.
- The parameters that could affect the market were accounted for to the maximum extent after thorough analysis, validation and verification before arriving at the final quantitative and qualitative data.
- After the data was curated, the report was prepared and underwent multiple reviews.
- The report provides detailed insights into the digital forensic ecosystem in India, from size to forecasts and market influencers.

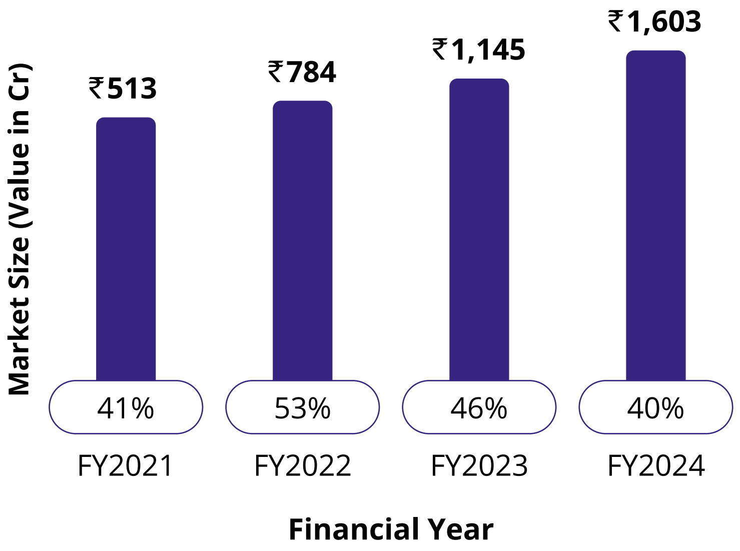
Chapter 3

Market insights

Market overview

Digital forensic industry analysis

The digital forensics market in India is following an upward trajectory, and the market posted a ~47 percent CAGR between FY2019–20 and FY2022–23 and is at INR1,603 crore in FY2023–24. The industry has grown significantly due to government policies that ensure adequate funding to improve the digital forensic ecosystem. The market is estimated to reach INR11,829 crore by 2030, with a CAGR of about 40 percent. This growth is driven by the increasing need for the digitisation of businesses, rising cybercrime, regulatory needs and more robust data security. The government and private sectors' emphasis on digital forensics, raising demand for specialised tools and services across industries such as law enforcement, cybersecurity and enterprise IT, is also driving the market. While the government is the major consumer of digital forensic products, the corporate sector remains the primary consumer of digital forensic services.



Market presence among players

Domestic companies are increasingly gaining market share in digital forensics. Indian companies focus on fulfilling the needs of the government and private sectors, with the largest share going to the government sector. These players have harvested the increasing need for digital forensics in law enforcement, corporate investigations and regulatory compliance. While global OEMs maintain a strong market presence, particularly with a higher focus on digital forensic tools and more emphasis on mobile forensics, Indian players are gaining an edge by focusing on tailoring solutions more suitable for government organisations.

Geographical distribution of market demand

The demand for digital forensics services and solutions is not evenly distributed in India. There is a concentration in the Western and Southern regions, while the Northern region also contributes to this to a certain extent. The eastern region holds slightly less of the market share, and receivers of service are regional law enforcement agencies. However, market dynamics suggest that the growth in demand for digital forensics is spreading across different regions, driven by government and corporate firms.

Impact of technological trends on market growth

Technological advancements are the primary force driving the growth of the digital forensics market in India. Due to the high importance given to mobile data recovery and investigation, mobile forensics is becoming a major focus area. As the number of mobile devices and the volume of mobile data continue to rise, digital forensics providers in India are increasingly investing in mobile and cloud forensics tools to fulfil this growing demand. Furthermore, the use of AI and machine learning in forensic tools is helping to automate data processing and increase the speed and accuracy of forensic investigations. These technologies allow digital forensics companies to quickly explore massive datasets, which is critical in situations of cybercrime, corporate espionage and IP theft. Companies integrating AI/ML capabilities with conventional methodologies will gain a competitive advantage.

Key observations

The digital forensics market is witnessing robust growth, driven by increased cybersecurity incidents, stricter regulatory requirements and rapid digital adoption across industries. IT modernisation and remote/hybrid working have fuelled spending on public cloud services, witnessing double-digit growth since 2019. According to the study, the digital forensic market posted a CAGR of 47 percent from 2020 to 2023, with projections indicating a growth rate of 40 percent from 2024 to 2030. The role of the private sector in the digital forensic industry is expanding rapidly, with organisations across various industries increasingly adopting digital forensics to address security challenges, regulatory requirements and risk management needs. This trend is fuelled by increased cybercrime, mainly via mobile handsets. Emerging technologies such as AI, cloud computing and blockchain will transform forensic procedures, while regulatory frameworks will drive demand across industries. As cyber threats advance, digital forensics will play a critical role in cybersecurity and legal compliance, cementing its importance across industries.

Analysis of market forces

The market for digital forensics is experiencing unparalleled growth, driven by several key factors reshaping the landscape. Below are the primary forces driving this expansion:

Increase in cybercrimes

With the rapid advancement of technology, cybercrimes such as online fraud, data breaches and cyberattacks have become significant concerns. Recent findings have revealed that the rate of cybercrime in India has surpassed 129 incidents per lakh population,1 highlighting the urgent need for effective digital forensic capabilities to investigate and mitigate these threats. As cybercriminals become more adept, the demand for advanced forensic tools and expertise continues to rise.

Rising number of digital users

India is home to one of the largest digital user bases in the world. The growing digital footprint significantly amplifies the volume and diversity of data that must be analysed and safeguarded. The rapid proliferation of smartphones, tablets and IoT devices highlights the need for specialised mobile forensic solutions to address the evolving technological landscape. As digital activity expands, the demand for advanced forensic solutions to manage this vast data intensifies.

Government Initiatives and Infrastructure Development

Recognising the critical role of digital forensics in combating cybercrime, the Indian government is taking proactive steps to strengthen its forensic capabilities. These initiatives aim to bolster forensic infrastructure across the country, with a strong focus on digital forensics, ensuring that law enforcement agencies and forensic labs are equipped to address the challenges posed by modern cybercrimes.

Increase in Awareness and Demand for Skilled Professionals

As cybersecurity threats continue to escalate, there is a growing awareness among organisations, government agencies and the general public regarding the importance of digital forensics in protecting digital assets and data integrity. This awareness drives public and private sector investments in improving forensic capabilities. A survey revealed that India will require 90,000 forensic scientists over the next nine years to meet the growing demand for skilled professionals.2 This demand underscores the need for training and educational initiatives to equip a new generation of forensic experts and develop specialised courses and certifications to fill this skills gap.

Analysis of market entry potential

The barriers to entry in the digital forensics market are considered moderate, largely due to the need for significant investment in specialised technology, tools and expertise. However, the growing demand for digital forensics services presents opportunities for new players to enter the market. New entrants can lower their entry costs by using cloud-based solutions and open-source tools, which could intensify competition among established and emerging players.

India's rapidly expanding digital landscape further contributes to the demand for robust digital forensics solutions. As more individuals and organisations adopt digital technologies, the volume of data requiring analysis in forensic investigations shall grow exponentially. This surge in data, coupled with the evolving cyber threat landscape, creates significant opportunities for businesses that can provide specialised digital forensics services to address these challenges.

The market for digital forensics in India has seen impressive growth, increasing from INR1,145 crore in 2023 to INR1,603 crore in 2024. Projections indicate that by 2030, the market will reach INR11,829 crore, reflecting an accelerating demand for digital forensic tools and services. This growth is driven not only by the increasing volume and complexity of digital evidence but also by the expanding threat of cybercrime, further underscoring the importance of advanced forensic capabilities.

Key factors influencing market entry potential

Growing Digital Ecosystem: India's digital ecosystem is expanding rapidly, with wide adoption of technologies such as mobile devices, cloud computing, IoT (Internet of Things) and cryptocurrency. These technologies present unique challenges for digital forensics professionals, as they generate vast amounts of data that must be captured, analysed and preserved in a forensically sound manner.

Evolving cybercrime landscape: The rapid rise in cybercrime, including high-profile incidents of ransomware attacks, data breaches and financial fraud, is increasing the demand for advanced digital forensics solutions. In India, cybercrime has evolved from isolated incidents to widespread attacks that affect public sector institutions, private enterprises and individuals. These growing cyber threats require sophisticated forensics tools to uncover critical evidence and support legal investigations. Given the complexities of modern cybercrime, digital forensics professionals are encouraged to adopt cutting-edge tools and methodologies that can handle emerging threats. There is also a growing need for professionals who can analyse a combination of traditional data and non-traditional data sources.

Government initiatives: The Indian government is heavily investing in enhancing its digital forensics infrastructure, recognising the importance of cybercrime investigations in a rapidly digitising society. Programmes such as the National Forensic Infrastructure Enhancement Scheme aim to bolster the capacity of forensic labs and law enforcement agencies (LEAs) to investigate digital crimes more effectively. Such initiatives improve investigative capabilities and open new opportunities for businesses that provide digital forensics tools and training to support government efforts.

Regulatory and legal requirements: Moreover, the increasing implementation of cybersecurity regulations and the Digital Personal Data Protection Act (DPDPA), 2023 will further drive the need for digital forensics solutions that comply with legal frameworks for data privacy, evidence handling and cybercrime investigations. As the regulatory landscape evolves, businesses must adapt their products to stay compliant and meet growing demand.

Evaluation of buyer bargaining power

The bargaining power of buyers plays a crucial role in shaping the digital forensics market in India. This power is largely driven by key stakeholders such as LEAs, other government entities and large enterprises, with the Indian government being the dominant consumer. These buyers are increasingly demanding cost-effective, customisable and comprehensive solutions that can address the growing range of digital threats. Consequently, vendors, such as OEMs, resellers and service providers, are pressured to differentiate themselves through competitive pricing, advanced features and exceptional customer service.

Key factors influencing buyer bargaining power

Government as the largest consumer: The Indian government dominates the digital forensics market, representing approximately 80 percent of the consumer share. This includes government entities such as LEAs, Forensic Science Laboratories (FSLs), training institutes and regulatory bodies.

Purchasing power: With such a significant market share, the government enjoys substantial purchasing power. Government agencies often have large budgets allocated to areas such as cybersecurity and digital forensics, which enables them to negotiate better pricing, terms and service contracts with vendors. This puts pressure on vendors to offer competitive pricing and ensure high-quality solutions to meet the stringent requirements of these agencies.

Tender-based procurement: Government procurement of digital forensics tools and services is typically tender-based, where vendors must meet specific technical performance, compliance and pricing criteria. The tender process allows the government to select the best offering from multiple bidders, often forcing vendors to lower prices or offer additional services to win the contract.

Big Four consulting firms: The Big Four (Deloitte, PwC, EY and KPMG) are another significant group of buyers with high bargaining power in the digital forensics market. These firms are major players in the private sector, providing digital forensics services to businesses dealing with cybercrime, fraud, data breaches and regulatory compliance.

Customised solutions for large enterprises: Large enterprises often require high-end, customised digital forensics solutions to address specific challenges, such as fraud detection, cybercrime investigations or compliance with evolving data privacy laws. This demand for tailored solutions provides them with substantial bargaining power, allowing them not only to negotiate better terms but also to demand highly specialised and premium features from vendors.

Appraisal of supplier bargaining power

The bargaining power of suppliers in the digital forensics market in India is generally moderate, with a few factors that either enhance or limit their influence. While the availability of open-source tools and the increasing adoption of cloud infrastructure has reduced reliance on specific vendors, suppliers offering highly specialised forensic solutions, such as OpenText, Magnet Forensics International Inc., MSAB Inc., Exterro Group LLC, Cellebrite DI Ltd. and Oxygen Forensics Inc., retain significant bargaining power, especially when it comes to cutting-edge technology and compliance with legal standards.

Key factors influencing supplier bargaining power

Niche market and limited competition: Digital forensics is a highly specialised field that requires advanced technical knowledge, tools and expertise. Unlike other broader IT sectors, the number of suppliers who can offer digital forensics solutions that meet the necessary standards is limited. Key players such as Guidance Software Inc., Magnet Forensics International Inc., MSAB Inc., Exterro Group LLC, Cellebrite DI Ltd., Oxygen Forensics Inc., etc., dominate the market, alongside a few Indian resellers and service providers. This limited supply of high-quality and specialised solutions creates a situation where suppliers hold significant bargaining power. These products are often critical for law enforcement agencies, government bodies and private enterprises dealing with cybercrime investigations. As a result, the suppliers of these tools can dictate terms more effectively, especially when the products are essential for sensitive operations.

Continuous innovation and R&D: The digital forensics industry is heavily technology-driven and research-oriented. Forensic tools must also adapt as cyber threats evolve to keep pace with new challenges, including advances in IoT, cloud computing and cryptocurrency. OEMs that invest heavily in R&D to improve or introduce cutting-edge technologies, such as AI-powered forensic tools, cloud-based solutions or advanced mobile forensics, command a higher price point and greater use over customers. Innovation in this sector is critical for maintaining a competitive edge, and suppliers who can stay ahead of technological trends are in a strong position to influence the market, thus increasing their bargaining power.

Patented technologies and exclusivity: Many leading digital forensics tools are based on proprietary algorithms or patented technologies. Suppliers that control these proprietary solutions hold an exclusive position in the market, preventing competitors from offering identical or equivalent products. This exclusivity enables suppliers to set higher prices, as they provide unique features or functionalities that other vendors cannot easily replicate. As a result, these suppliers can dictate pricing, terms of service and support contracts, making them dominant players in the digital forensics market. This exclusivity strengthens their bargaining power by limiting the options available to potential buyers.

Complex regulatory environment: The digital forensics sector is highly regulated, especially in law enforcement and government investigations. Forensic tools must adhere to strict standards regarding evidence handling, data integrity and admissibility in court. The regulatory hurdles create high barriers to entry as evidence processed and investigated in a government-notified lab is only admissible in a court of law. New entrants face significant challenges in obtaining the necessary approvals, thereby reducing their competitive advantage and strengthening the influence of incumbent players.

Specialised skills and training support: Digital forensics tools are complex and require specialised skills to operate effectively. Consequently, vendors often provide training and certification programmes to ensure users can fully use their tools. Suppliers who offer comprehensive training and certification services build strong, long-term relationships with their customers, making it more difficult for buyers to switch to alternative vendors. The ability to provide ongoing technical support, training programmes and certifications not only enhances the value proposition of the tools but also cements the supplier's position as a trusted collaborator. This increases their bargaining power, as customers depend on their expertise and support for effective tool implementation.

Examination of substitute threats

The emergence of products or services that can replace or significantly reduce the need for existing solutions presents a significant challenge to any market. The digital forensics market is no exception, as it faces increasing threats from substitute products and services. These substitutes, including new technologies, alternative investigative methods and evolving regulatory frameworks, can potentially disrupt the demand for traditional digital forensics tools and services. As cybercrime and digital threats proliferate in India, digital forensics remains critical for investigative agencies, businesses and law enforcement. However, the growing availability of substitute solutions poses a need to reassess the role of traditional forensics and understand the shifting market dynamics.

Key substitute threats in the digital forensics market in India

Automated cybersecurity solutions and AI-driven threat detection

- The increasing popularity of AI-based cybersecurity platforms, such as Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) and Security Orchestration, Automation and Response (XSOAR), presents a major threat to traditional digital forensics solutions in India. These platforms use ML and AI to detect, mitigate and prevent cyber threats in real time. Their proactive approach to cybersecurity reduces the need for manual intervention, and by identifying threats such as ransomware, malware, and phishing, organisations can address potential breaches before they escalate.
- While AI-driven cybersecurity platforms are not yet direct substitutes for digital forensics in terms of evidence collection or post-incident investigations, they serve as effective preventive measures. By detecting and neutralising cyber threats early, these platforms can reduce the volume of incidents that require in-depth forensic investigations. This shift towards real-time, predictive threat detection, combined with the growing capabilities of ML, is pushing businesses and government agencies to rely increasingly on automated systems to mitigate risks before they necessitate forensic intervention.
- In the long run, as AI and ML algorithms continue to improve, the number of incidents that require traditional digital forensics procedures could significantly reduce, potentially diminishing the demand for human-driven investigations in some cases.

Cloud-based forensics solutions

- The rapid adoption of cloud computing and cloud storage has fundamentally altered the landscape of digital forensics. Cloud-based forensics tools now enable investigators to collect, analyse and preserve digital evidence that resides across multiple cloud environments without relying on traditional on-premises solutions.
- Cloud-based solutions offer significant advantages, including scalability, flexibility and cost efficiency, compared with traditional forensics tools, which often require substantial investments in hardware, local storage and physical infrastructure. These platforms also allow for remote collection and analysis of data, enabling digital forensic professionals to access data across various cloud services (e.g., AWS, Azure, Google Cloud) and mobile apps with ease.
- With the growing volume of data generated by devices such as smartphones, IoT devices and web applications, cloud-based forensics presents a strong alternative to traditional, on-site forensic investigations. Forensic experts no longer need to visit physical locations or rely on on-premises systems to gather evidence. Instead, cloud-based tools can access data remotely and perform the necessary analysis from anywhere, making them more efficient and cost-effective.
- As businesses and government agencies continue to embrace cloud-based infrastructure for storing and processing large volumes of data, cloud forensics is increasingly seen as a viable substitute for traditional forensic methods. The shift to cloud-based forensics could reduce the need for traditional, localised investigations, particularly when dealing with large-scale data from complex, distributed environments.

Analysis of competitive rivalry intensity

The digital forensics market in India is witnessing increased competition as global technology giants and local service providers enter the space. This player influx shapes the market dynamics and intensifies competition across various sectors.

Entry of global and local players

- The market is being shaped by the simultaneous entry of global forensics firms alongside Indian resellers and service providers. The international companies bring well-established products and services, offering various forensic tools for data recovery, cybercrime investigation and digital evidence analysis. At the same time, local players aim to capture a significant portion of the market by providing region-specific services, catering to the unique needs of Indian customers.
- While international players benefit from their established global reputation, Indian players have the advantage of local knowledge and personalised services. However, this dual presence creates an intense competition environment, as both types of players seek to gain market share.

Fragmented market landscape

- Despite the presence of large global players, the digital forensics market in India remains highly fragmented, with numerous regional service providers and resellers targeting specific segments. This fragmentation fuels intense competition as smaller players strive to establish their niches in this rapidly growing sector.
- As the market matures, this fragmentation is likely to reduce over time through consolidation, but in the current phase, it fuels competitive rivalry. Each global or local player is striving to capture as much market share as possible. For businesses in the digital forensics space, staying ahead in terms of technological innovation, pricing and service offerings is crucial to navigating this fragmented landscape.

Limited scope for service providers

- For other resellers and service providers, the market is more challenging. With only a small share of the market available to them and given the high cost of digital forensic tools and services, these smaller players face limited opportunities to scale. The expensive nature of digital forensics tools and the high level of expertise required to deliver these services also make it difficult for these organisations to operate profitably.
- This leaves little room for smaller enterprises to act as independent consumers of digital forensics tools, further consolidating power in the hands of a few major players—primarily government agencies and large firms.

Technology overview

Future trends

Cloud forensics

With the rapid expansion of cloud computing in India, cloud forensics has emerged as a critical component of digital investigations. Businesses, organisations, government agencies and individuals increasingly rely on cloud-based services, necessitating robust forensic methodologies to analyse, preserve and investigate digital evidence in cloud environments. Forensic analysts face new challenges in gathering and analysing data stored in cloud environments. Investigating data stored in the cloud requires specialised tools and techniques to extract evidence from remote servers while keeping the data integral. Key challenges are data volatility, legal compliance across multiple jurisdictions and the complexities of multi-tenant architectures. Moving forward, cloud forensics will depend on the development of more advanced tools to address these challenges and enable investigators to effectively collect and analyse evidence from evolving cloud platforms. The increasing sophistication of cloud systems will drive the need for digital forensics to adapt continuously, ensuring that it remains capable of addressing the unique demands of cloud-based investigations.

Mobile forensics

The fast adoption rate of smartphones and handheld devices makes mobile forensics an important area for LEAs and businesses investigating cybercrimes. Modern smartphones pose significant challenges because of advanced encryption and security features, which make extraction and analysis challenging. Future advancements in mobile forensics depend on addressing a variety of complexities, including cross-platform compatibility and advanced decryption techniques.

IoT forensics

The proliferation of IoT devices, ranging from smart home systems to wearable devices and interconnected industrial machines, has opened new dimensions to digital forensic investigations. The rapid growth of IoT and human interface devices and their adoption in sectors such as healthcare, manufacturing and urban infrastructure makes IoT forensics a crucial area of focus. Investigators need specialised tools and techniques as these devices contain voluminous and diverse data, necessitating specialised methods.

Electronic discovery (e-discovery)

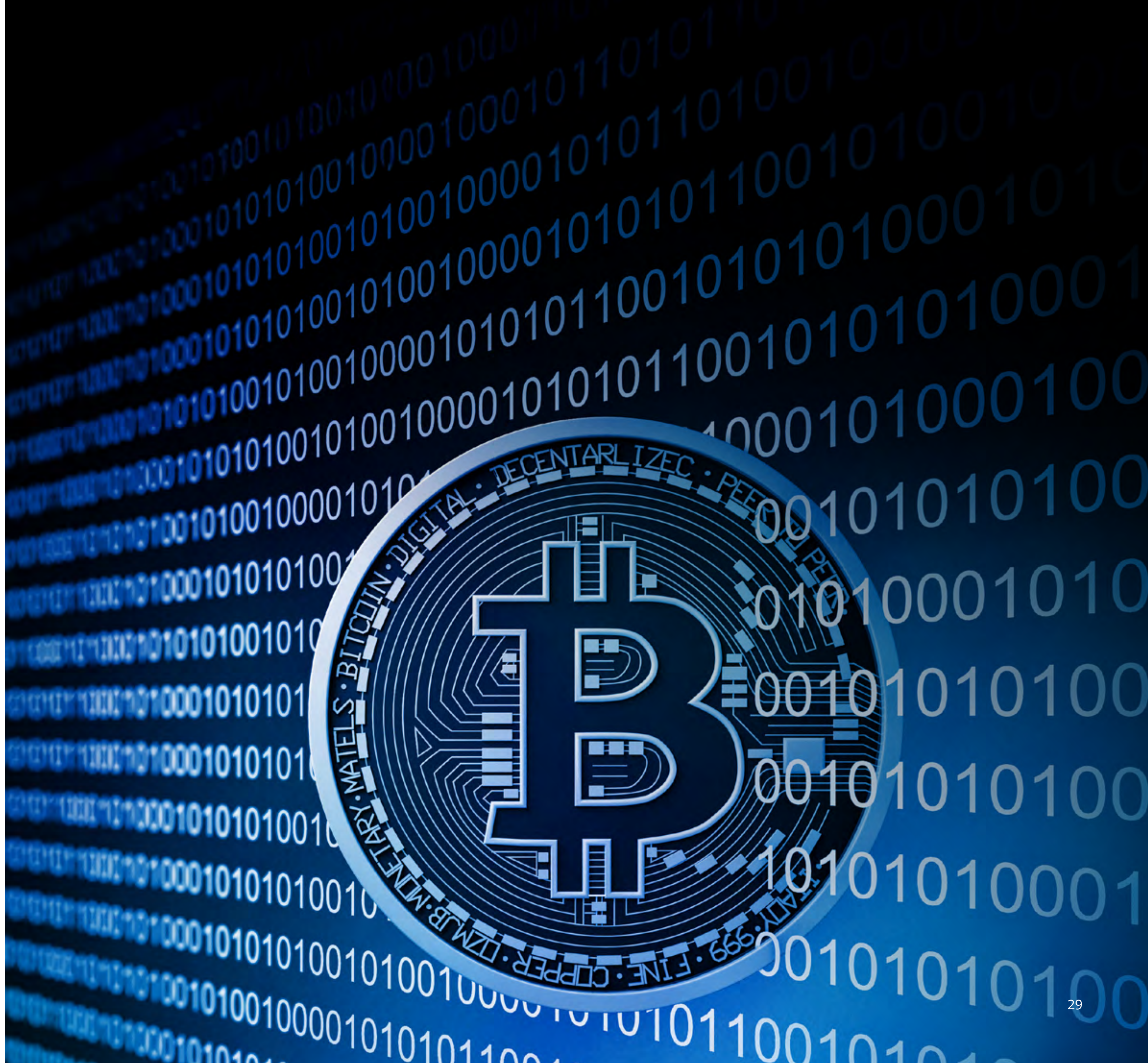
The increasing digitisation in official procedures has elevated the role of e-discovery in digital forensics. With the growth in storage capacities of devices and prioritisation towards cloud technology, the amount of data getting stored digitally has increased significantly. The need to investigate and/or review such huge amounts of data has uplifted the role of e-discovery. These data discovery tools aid in the identification, preservation and analysis/review of Electronically Stored Information (ESI) crucial for investigations, compliance and litigation purposes. The digital forensics market in India is increasingly shifting towards e-discovery platforms due to their unmatched utility.

Blockchain forensics

The recent proliferation of cyberattacks with cryptocurrency, such as ransom, has necessitated the adoption of cutting-edge skills, capabilities and tools to investigate such offences. Blockchain forensics can aid in investigating the flow of cryptocurrencies, eventually leading to the perpetrator. The field is evolving and focuses on tracing transactions and identifying digital assets on blockchain networks. As the use of cryptocurrencies grows, forensic tools are also evolving to trace digital assets across exchanges and wallets, even in decentralised systems. In India, this specialisation is gaining attention as the government seeks to regulate cryptocurrency transactions, prompting law enforcement to integrate blockchain analysis tools into cybercrime investigations.

Digital currency

Besides cryptocurrencies, many countries, including India, are actively exploring digital currency due to its numerous advantages, such as enhanced financial inclusion, reduced transaction costs and improved payment efficiency. The Reserve Bank of India (RBI) launched a pilot project for the blockchain-based digital currencies, E-Rupee-Wholesale (e₹-W), on 1 November 2022 and E-Rupee-Retail (e₹-R) on 1 December 2022. The project is in its nascent stage and evolving before becoming part of everyday financial transactions. With the advent of digital currencies and other digital assets, new challenges in tracking, analysing and securing financial transactions will emerge, requiring specialised forensic methodologies.



Technology advancements and innovations

AI and ML

AI and ML are transformational technologies that facilitate real-time investigations. Network traffic analysis, threat detection and identification of patterns synonymous with malicious activity are some areas where the technology is gaining prominence. The technology is also used in analysing diverse file formats, including videos and images, to deduce inputs that otherwise would have been impossible to perceive. This transformational technology is continuously used in digital forensics to automate investigations and improve efficiency and speed. Deep learning also enables the profiling of criminals and the prediction of patterns.

Big data analytics

Big data analytics in digital forensics is a relatively new and rapidly evolving concept as it enables forensic investigators to process and analyse voluminous data quickly. This advanced technology will facilitate the analysis of diverse and complex datasets to identify hidden relationships and patterns and detect correlations. This technology is indispensable for investigations of greater size and scale.

Augmented and Virtual Reality

Augmented Reality (AR) and Virtual Reality (VR) are expected to revolutionise digital forensics. Potential application areas include advanced visualisation and simulated crime scene training environments for forensic analysts to enhance their skills. The technology enhances real-world interactions by overlaying digital data and reconstructing the crime scene to augment the evidence collection and analysis process.

Quantum computing

Quantum computing is another evolving technology with potential applications in cybersecurity and digital forensics. By outpacing traditional computers in specific calculations, the field provides new dimensions in solving complex cryptographic problems and accelerating data analysis. Although in a nascent stage, other probable uses include encryption breaching, forensic tool innovations and the creation of advanced simulations to better understand cyber incidents and facilitate efficient investigations.

Cyber security and digital forensics

Combining cyber threat intelligence and digital forensics is a fast-emerging hybrid model intended for countering cyber threats effectively. Cyber deception technologies such as honeypots and decoy systems are integrated with digital forensics workflow to gather information to understand the Tactics, Techniques and Procedures (TTPs). The details would enable the investigators to anticipate and respond to the threats effectively. This real-time incident response activity will efficiently counter a cyber menace and play a significant role in next-generation cyber defence.

Impact of COVID-19 on the industry

- During the COVID-19 pandemic, markets and industries were suddenly disrupted, leading to widespread lockdowns. This abrupt shift resulted in massive job losses, affecting countless individuals. As many searched for ways to make a living, some became desperate and turned to fraudulent activities, contributing to a significant rise in cybercrimes.
- Cybercrime knows no borders, and the surge in malicious online activities quickly became a global concern that demanded immediate attention. The need for digital forensic services and tools became apparent to combat this increase in cybercrime.
- The demand for digital forensics was particularly felt by government agencies and industries such as Banking, Financial Services and Insurance (BFSI), telecommunications and IT. As cyber threats grew, so did the need for advanced forensic tools and skilled cybersecurity professionals. This created a domino effect, driving growth in the digital forensics market in revenue and services.
- The pandemic raised awareness about digital forensics and highlighted the importance of protecting consumer data. As a result, the market has continued to grow in the post-pandemic era. Factors such as the ever-evolving technological landscape, new security practices such as Bring Your Own Device (BYOD) policies, and the continued focus on cybersecurity have all contributed to the market's ongoing expansion.

Chapter 4

Market dynamics

Market drivers

Digital Public Infrastructure

The proliferation in digital payment transactions, from INR2,071 crore in FY2017–18 to INR18,592 crore in FY2023–24 at a CAGR of 44 percent [3], facilitated by over 138 crore biometric IDs with 1 crore daily e-KYC transactions granted over 50 crore bank accounts[4] ; the upward growth trajectory of the e-commerce industry, achieving a Gross Merchandise Value (GMV) of over INR 5 lakh crore in the fiscal year 2023, marking a 22 percent increase from the previous year and with an expected CAGR of 27 percent[5] few statistics provide insights into the rapidly expanding Digital Public Infrastructure in India. The pace of digital transformation and its application in various sectors will create a demand for new digital forensic solutions and services, driving the digital forensic market.

Consumer explosion

The rapid growth of digital consumers in India is evident, with 97.1 crore registered internet users, 115 crore wireless subscribers[6] and over 46.2 crore social media users—all showing an upward trend. With 5G subscriptions projected to exceed 270 million by the end of 2024 (accounting for 23 percent of total mobile subscriptions) and expected to reach 970 million by 2030 (representing 74 percent of mobile subscriptions)[7], this growth signals a fast-evolving digital ecosystem. This presents substantial opportunities for businesses and service providers to engage with a vast, increasingly connected consumer base. The increasing development in the use of digital devices and the adoption of newer technology will greatly propel digital footprints, driving the growth of the digital forensics industry in India.

Cybercrime surge

The number of reported cybercrime complaints has increased exponentially, from 26,049 in 2019 to 15,56,218 in 2023, with 740,957 complaints reported in just the first four months of 2024. This represents an alarming growth of 113.7 percent in 2022 and 60.9 percent in 2023, to an average of over 7,000 complaints daily.[8] The surge in cybercrime, coupled with the increasing complexity, diversity and scope of attacks across various sectors, presents new challenges necessitating robust digital forensics investigation techniques involving advanced solutions and expertise, thereby driving the market.

Statutory and regulatory requirements

Introduction of new provisions in the legislation to adapt to technological advancements and to combat crimes; redefining the evidentiary nature and admissibility of electronic evidence, classifying cybercrime as an organised crime; widening the scope of cybercrime to include crimes committed electronically and intangible thefts; addition of a new section to address terrorism originating from digital space, usage of audio-video and electronic communications in the new criminal laws are critical drivers. Digital evidence now plays a vital role in the majority of criminal cases—estimated at over 90 percent.[9] Compliance with directives, regulations and guidelines issued by nodal agencies and regulators such as CERT-IN, RBI and SEBI further fuels the need for digital forensic expertise. As regulatory requirements surrounding data privacy intensify globally, with stringent provisions outlined in data protection laws such as the DPDP Act 2023 and GDPR, organisations must rely on digital forensic solutions to ensure compliance with data breach, security and integrity standards. These factors collectively contribute to the accelerating demand for digital forensics in a rapidly evolving legal and technological landscape.

Enterprise Digital Forensics and Incident Response (DFIR)

The ongoing digital transformation and the shift of business entities from traditional practices to digital platforms and technologies are significantly boosting the digital forensics market. Corporate digital forensics investigators play a pivotal role within organisations, supporting diverse functions such as internal investigations, risk mitigation, litigation support and corporate security. The rapid expansion of the service segment, particularly in areas such as incident response, capacity building, readiness assessments and forensic consulting, are key contributors to this growth. Further, the rapid rise of Global Capability Centres (GCCs), especially in India, which accounted for about 1,580 out of 2,740 GCCs globally in FY2023,[10] posting a CAGR of 5.9 percent is creating significant opportunities for digital forensics services. The increasing specialisation of digital forensics within the GCC sector further amplifies its demand, emerging as a critical driver in the market's growth.

Translational developments

Ongoing advancements in technologies such as AI, IoT, cloud computing, blockchain and cybersecurity protocols, along with the rapid expansion of global communication networks and devices, are introducing new challenges that drive the need for innovative tools and expert services in digital forensics. The emergence of transformative technologies such as quantum computing, virtual and AR and automated forensic tools further complicate the landscape, necessitating more sophisticated approaches to digital investigations.

The rise of trends such as Bring Your Own Device (BYOD) policies and hybrid work environments adds another layer of complexity, creating new vulnerabilities and data security concerns. Data analytics for identifying patterns and anomalies, predictive and proactive analysis for threat detection, behaviour profiling algorithms, etc., are potential drivers towards new avenues. These developments collectively contribute to the growing demand for advanced digital forensic solutions and expertise.

Government initiatives

The launch of the National Forensic Infrastructure Enhancement Scheme (NFIES), with an outlay of INR2,254[11] crore for the period from 2024–25 to 2028–29 is a significant driver for the growth of the digital forensics market. Other government initiatives, including the Cyber Commandos programme, Cyber Fraud Mitigation Centres (CFMC) and the Samanvay platform (a Joint Cybercrime Investigation Facility System), are set to enhance the country's cybersecurity and forensic capabilities. Further, setting up additional off-campuses of the National Forensic Sciences University (NFSU), augmenting and modernising Central Forensic Science Laboratories (CFSLs) and capacity building initiatives for Law Enforcement Officers are key market drivers.[12] Initiatives by the Ministry of Electronics and Information Technology (MeitY), such as sponsored projects to foster technological independence and the development of an indigenous R&D ecosystem, are expected to significantly boost digital forensics. These projects focus on creating homegrown technology, products and solutions, particularly in areas such as Digital Forensics. Moreover, the formulation of the Cyber Forensic Roadmap for India by C-DAC, MeitY, is poised to accelerate the country's digital forensics market.[13] The Directorate of Forensic Science Services (DFSS) also plays a pivotal role in advancing the field by supporting extramural research and development through competitive funding. These interdisciplinary research and innovation initiatives are expected to further transform the forensic science landscape in India and drive growth in the industry.

Market restraints

Resource inadequacy

A major challenge restraining the growth of the digital forensics market in India is the shortage of skilled professionals. Survey responses from over 70 percent of the sample population identified the lack of qualified professionals as one of the industry's most significant obstacles. Several factors, including the rapidly evolving threat landscape, technological advancements, the increasing complexity of investigations, resource constraints and the insufficient availability of educational and training programmes, further substantiate this issue. Digital forensics is an ever-evolving field with abundant opportunities and requires highly specialised expertise. As demand continues to outpace supply, a talent gap is emerging, threatening to impact investigations' speed and effectiveness. This shortage of skilled professionals can hinder the growth of the digital forensics market, making it a critical challenge that needs to be addressed to ensure the sector's continued advancement.

Financial constraints

The high cost of digital forensic tools and services presents another significant constraint on the growth of the digital forensics market. The substantial investment required for procuring these tools can create financial barriers for many organisations. The rapid pace of technological advancements further complicates this issue, as solutions need constant updates and capacity-building exercises, which can place considerable financial strain on organisations. The lack of indigenous digital forensic tools forces many organisations to rely on expensive foreign solutions, making it an unviable option for them as they struggle to justify the high costs. Additionally, with a limited number of players in the market, end-users are left with fewer choices and face higher prices for available solutions. These factors collectively create significant obstacles to widespread adoption and growth in the market.

Administrative challenges

Underutilisation of budget, administrative delays and high vacancies, especially in government organisations, are major factors that negatively impact the digital forensics market. The cumbersome administrative and financial controls and delays in getting funds, notably at the state level, hinder the growth. Financial, staffing and infrastructural constraints in government laboratories further weaken the market. Given that the government is the predominant end-user of digital forensics services, these challenges profoundly impact the market. However, with the introduction of various recent government initiatives aimed at modernising infrastructure, improving funding mechanisms and addressing staffing gaps, these issues are expected to be mitigated in the near future, paving the way for a more robust and dynamic digital forensics market.

Lack of forensic awareness

The majority of law enforcement officers lack the specialised qualifications required to effectively investigate cybercrimes or handle cases involving computer technology and electronic evidence. Investigating cybercrimes demands a unique skill set that combines technical, investigative and legal knowledge, which many officers are not equipped with. Moreover, while forensic procedures are intended to be repeatable and consistent, discrepancies often arise due to inadequate training, inconsistent adherence to established protocols and a lack of standardisation across agencies. Different LEAs may implement variations of recognised procedures or develop their own operational guidelines, leading to inconsistencies in the handling of digital evidence. This lack of uniformity further compounds the challenges in digital forensics investigations. Additionally, private digital forensic experts often lack awareness of evidentiary rules, which can affect the admissibility of electronic evidence in court. The recognition of digital evidence in judicial proceedings faces numerous hurdles due to the growing complexity of the technology and a general lack of understanding within the legal system. The regulatory ecosystem governing digital forensics in India is fragmented and yet to mature and involves multiple laws, regulations and standards applicable across different sectors. This lack of a cohesive framework can delay legal and judicial proceedings, ultimately affecting the efficiency and success of investigations and legal processes, thereby dampening the market.

Academic and research challenges

The educational ecosystem for digital forensics in India is still in its early stages and has yet to mature. Shortage of specialised faculty, infrastructure and laboratories hampers the development of expertise, and it becomes challenging to cultivate a skilled workforce capable of meeting the increasing demands of the industry. Also, the absence of a standardised framework outlining the essential qualifications and training required to become a digital forensic expert has resulted in a gap in the competency levels of professionals entering the field. The limited focus on research and development, coupled with insufficient funding, further restricts the growth opportunities in the field. To foster the growth of the digital forensics market, it is critical to establish clear educational standards, invest in research and development and build the necessary infrastructure.

Complexity

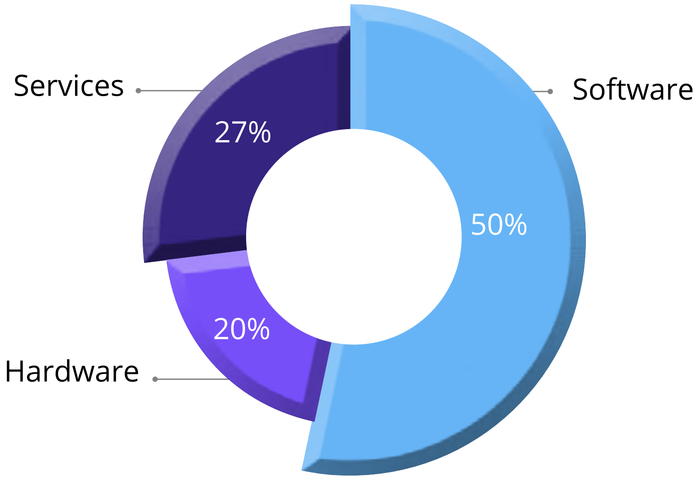
The growing complexity of digital investigations has become a significant challenge due to several factors, including the diversity of digital devices and software platforms, the proliferation of emerging digital services and the vast array of physical and virtual storage locations. Additionally, anti-forensics techniques have further complicated the recovery and analysis of digital evidence. Investigators are now required to navigate various data formats and types, each demanding specialised tools and techniques for effective analysis. The increasing volume of data, advancements in encryption technologies and the evolving sophistication of cyber criminals add additional layers of difficulty to investigations. Moreover, the emergence of stricter privacy regulations further complicates the process by placing additional legal and compliance constraints. These factors collectively create significant challenges for investigators, potentially slowing down the process of digital forensic investigations and influencing the overall effectiveness of cybercrime response efforts.

Chapter 5

Market size and segmentation

The Indian digital forensics market is valued at INR1,603 crore (US$0.19 billion) for FY2023–24, reflecting an impressive CAGR of approximately 40 percent from FY2022–23. This represents about 3 percent of the global digital forensics market, which is valued at approximately US$6.5 billion. Driven by a strong growth trajectory and increasing industry momentum, the Indian digital forensics market is expected to maintain a robust CAGR of approximately 40 percent. Projections indicate that the market will reach INR11,829 crore (US$1.39 billion) by FY2029–30. To gain a comprehensive understanding of the growth drivers and opportunities within the Indian market, a segmentation analysis was conducted, focusing on key factors such as forensic domains, technological components, end-use industries and geographical regions. This detailed analysis offers deeper insights into the specific elements propelling market growth and identifies high-potential areas for expansion within India's evolving digital forensics landscape.

Market segmentation by components



Hardware

- Hardware, including specialised devices such as forensic servers/workstations, write blockers, disk duplicators and mobile device analysis kits, holds a significant share of approximately **20 percent** of the Indian digital forensics market.
- Growth in this segment is largely driven by government initiatives focused on modernising and augmenting digital forensic capabilities across India. These efforts are aimed at enhancing the country's ability to handle complex digital investigations.
- The rapid advancement and innovation in computing hardware are driving this segment forward. Enhanced processing power, coupled with declining costs and the widespread availability of storage through larger device capacities and cloud-based solutions, has transformed the data landscape. Advancements in network connectivity have introduced new challenges, requiring ongoing updates to digital forensic technologies to keep up with these changes.
- However, India faces a challenge with a limited number of local manufacturers specialising in digital forensic hardware, which results in a dependency on imported equipment. This reliance raises costs and causes delays and complications with servicing and maintenance, affecting overall operational efficiency. The digital forensics hardware market in India stands to benefit significantly from policy measures such as tax reductions, incentives for local manufacturing and increased investment in forensic research and training programmes. These actions could help stimulate domestic production, reduce reliance on imports and drive further growth in the sector.

Software

- Software solutions account for **54 percent** of the Indian digital forensics market, with tools dedicated to the forensic acquisition, analysis and decryption of data from various devices. Leading global providers in this space include Cellebrite, OpenText, Magnet Forensics and Exterro.
- Domestic players are focusing on localising software solutions and offering cost-effective alternatives while addressing the unique challenges in India. They are collaborating with government organisations to enhance the country's cyber forensic capabilities and better meet the specific needs of Indian law enforcement and agencies.
- Forensic tools are evolving to incorporate advanced capabilities, particularly by integrating AI and ML. New features such as natural language query support, automated data correlation and speech-to-text capabilities for voice notes enable predictive analysis and streamline the forensic analysis process, enhancing the overall efficiency of investigations.
- The scalability of cloud-based forensic solutions is another key factor driving market growth, particularly in supporting organisations that adopt remote or hybrid work models. Cloud solutions enable remote data acquisition and real-time analysis, using tools such as F-Response and EnCase and using EDR (Endpoint Detection and Response) or XDR (Extended Detection and Response) capabilities to enhance security and efficiency.
- The increasing rate of digitisation is amplifying the demand for data recovery and e-discovery solutions, further propelling the software segment. The growing frequency of data loss incidents and the need for efficient restoration of lost or corrupted data are driving the growth of the data recovery segment. Similarly, the rising need to investigate and review vast, diverse datasets is fuelling the e-discovery segment, as organisations require more advanced tools for handling large volumes of information.
- Rapid advancements in technology, driven by the need for faster processing times and improved resource usage, are set to accelerate the development of more adaptable and efficient digital forensic software. As these tools continue to evolve, they will become increasingly essential for organisations to stay ahead in the face of growing cybersecurity threats and complex digital investigations.

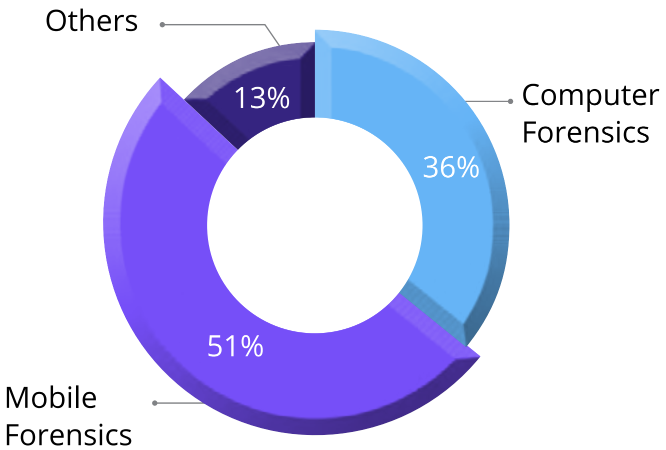
Services

- Managed Forensic Services (MFS) is increasingly gaining traction and currently accounts for **27 percent** of the market share within this segment. These services include outsourced offerings such as incident response, forensic consulting, litigation support and forensic audits.
- Due to the high costs associated with building in-house forensic capabilities, many organisations opt to rely on third-party forensic services. This segment is dominated by global leaders such as the Big Four consulting firms, as well as other major players who provide comprehensive solutions tailored to organisational needs.
- Domestic service providers and Small And Medium-Sized Enterprises (SMEs) now offer cost-effective investigation and incident response services. The scope of these services has expanded beyond post-incident investigations to include proactive support and preparedness measures, reflecting the evolving landscape.
- Training and consulting services are becoming increasingly critical to address the skills gap in the Indian market. With initiatives from academic institutions such as the National Forensic Sciences University (NFSU) and collaboration with corporate and domestic players, this area is gaining significant momentum, helping to build a robust talent pool for the future.
- Discovery and data management services, predominantly provided by the Big Four consulting firms, are emerging as a key area within the digital forensics landscape. These services focus on identifying, preserving and analysing Electronically Stored Information (ESI), which is critical for investigations, compliance and litigation. Given the rapid digital transformation across industries, this domain is expected to experience significant growth.
- Digital forensic businesses also provide data recovery services, which assist organisations in recovering lost data due to hardware failures, human errors, or cyberattacks. This addresses a growing need as data integrity becomes more vulnerable.
- The Indian digital forensic services market is poised for significant expansion due to the rise in cybersecurity threats and incidents, increasing regulatory and compliance requirements and a growing demand for outsourced MFS.
- Strategic investments in advanced technologies, regulatory compliance solutions and workforce development will be essential to meet the market's increasing demands. This dynamic environment creates a promising future for digital forensic service providers in India as they adapt to new threats and technological advancements.
- The services segment is expected to hold a significant market share, as digital forensic services complement digital forensic hardware and software to streamline identifying and examining critical data. A major portion of the costs involved in providing such services is attributed to skilled employees, licensing fees and ongoing training.
- Government organisations, especially law enforcement agencies, along with corporate entities, increasingly rely on digital forensic professionals to investigate a wide range of digital offences, including computer-related crimes, data breaches and IP theft. Domestic players, alongside global corporations such as the Big Four, cater to these needs by offering affordable, specialised solutions and providing technical support tailored to the Indian context.

Market segmentation by type

Computer forensics

- Computer forensics remains the centre of focus, with a **36 percent** market share, and has gained significance in recent years due to the growing occurrences of cybercrimes and the need for digital evidence in legal proceedings.
- This segment delves into investigating a range of financial frauds, data breaches, insider threats, intellectual property theft and other issues.
- Requirements for analysing and recovering data from computers, laptops and storage devices in digital forensic investigations drive the computer forensics segment.



- Furthermore, advancements in malware detection and analysis and broad coverage for various operating systems and devices, among other key essentials, promote the significance of this area of forensics.

Mobile forensics

The mobile forensics segment is the fastest-growing segment, driven by the increased usage of smartphones and handheld devices.

- In India, mobile forensics holds about **51 percent** market share, the largest in forensics.
- Growth is further fuelled by the increasing adoption of mobile payment systems and social media platforms, which are frequent targets of cybercrimes.
- Other typical cases that drive this segment involve SMS fraud, mobile malware, data theft, etc.
- Law enforcement agencies, government organisations, corporations, private investigators and individuals are increasingly availing the services of mobile forensics professionals to investigate various digital offences involving mobile phones.

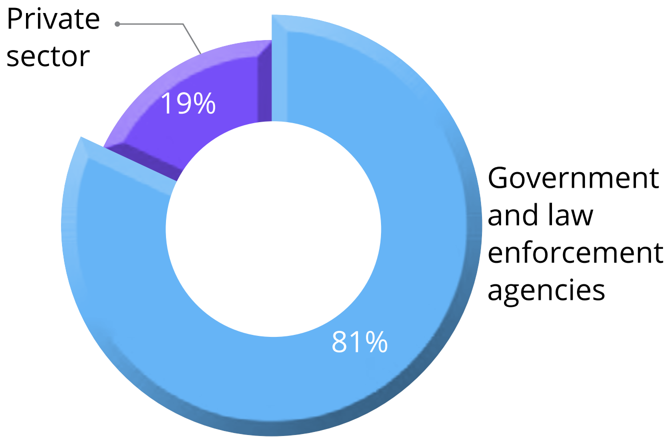
Other types of forensics

- Other emerging fields, such as cloud forensics, IoT forensics, network forensics and cryptocurrency forensics, are steadily gaining focus and constitute **13 percent** of the market share.
- These specialised areas address the unique challenges of decentralised systems and encrypted digital assets that hold the IT industry's future.
- Network forensics is vital for identifying and mitigating ransomware and other attacks propagating through network resources. The segment's growth in India is driven by rising cybersecurity awareness among IT and telecom firms, which account for a significant portion of cyber incidents.
- Network forensics is expected to have a significant market share in the future, as wireless communication devices are vulnerable to data theft, and network forensics helps identify the source of security breaches. The growing insecurities among methods such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are making the domain of network forensics indispensable in various industries.
- As cloud adoption grows, cloud forensics is becoming increasingly relevant for investigating cyber incidents in remote working models and cloud-based environments. As business entities move towards cloud-based solutions, this segment is expected to witness explosive growth.
- Moreover, digital forensic solution providers are moving towards cloud-based solutions, which provide various advantages, including scalability, flexibility and cost-effectiveness. The move is further accelerated due to the growing volume, diversified distribution of digital data and the requirement for remote access and cooperation.
- IoT forensics is another emerging field propelled by the increasing use of IoT devices in sectors such as smart manufacturing, healthcare and logistics. This growing segment addresses the unique forensic needs of interconnected devices and sensors.

Market segmentation by industry

Government and law enforcement agencies

- Government organisations are the largest consumer of hardware and software forensic tools, accounting for approximately **81 percent** of the Indian market.
- This remarkable growth in the digital forensics market could be attributed to the exponential increase in cybercrimes and other criminal activities involving computer systems. Law enforcement agencies rely increasingly on digital forensics to investigate and prosecute cybercriminals.
- The benefits of digital forensics, including its efficiency in evidence collection, suspect identification and event reconstruction backed by regulatory requirements, drive the demand for digital forensics in law enforcement.
- Technological advancements, including cloud computing and the Internet of Things, throw new challenges, rendering digital forensics solutions indispensable for effectively investigating cybercrimes.
- India's defence and national security agencies use digital forensics to address cybersecurity threats, prevent espionage and protect national infrastructure.
- Regulatory authorities, such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI), require digital forensics to ensure compliance in regulated industries such as banking and finance. These agencies perform forensic audits and investigations to detect financial fraud and maintain data integrity.



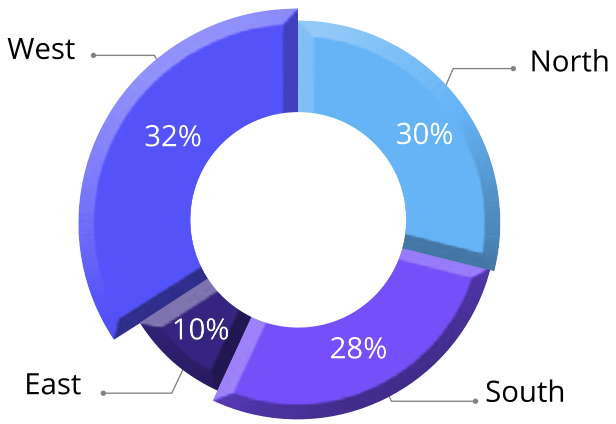
- Judiciary relies upon digital forensics to examine evidence in digital evidence cases. Various activities are undertaken to ensure the admissibility of digital evidence in legal proceedings, supporting various civil, criminal and corporate litigation.
- Digital forensics also plays a significant role in counter-terrorism. Government agencies use computer forensics to investigate cybercrime cases and extract hidden and deleted evidence artefacts, thus revealing hidden secrets from the evidence being examined and strengthening the position and credibility of digital forensics.
- Investments in regional forensic labs and partnerships with global vendors are also expected to drive the digital forensics market and strengthen law enforcement capabilities.
- These forces and work areas make the government sector a major consumer in the digital forensics market.

Private sector

- The private sector's role in the digital forensic industry is expanding rapidly, with organisations increasingly adopting digital forensics to address security challenges, regulatory requirements and risk management needs. A rise in cyber threats drives this trend, as do stringent data protection laws and an increasing reliance on digital platforms for core business functions. Currently, the private sector holds a **19 percent** share as an end-user in the digital forensic industry.
- The primary reason the private sector holds a **19 percent** share is that many private companies, particularly SMEs, prefer outsourced digital forensic services due to cost-effectiveness.
- Managed forensic services providers offer on-demand investigation and incident response, allowing companies to access specialised expertise without significant upfront investment. This model is gaining traction as more businesses prioritise cybersecurity and compliance due to cost-effectiveness.
- Enterprise is another emerging digital forensics market client segment that includes banking, healthcare and technology. Enterprises use digital forensics to protect sensitive data, investigate internal security incidents and maintain regulatory compliance.
- The private sector in India's digital forensic industry is poised for substantial growth, driven by regulatory needs, the increasing sophistication of cyber-attacks and the widespread adoption of digital systems. However, realising this growth will require overcoming challenges such as cost barriers, skills shortages and evolving compliance requirements.
- With strategic investment in advanced technologies and skills development, the private sector can enhance its digital forensic capabilities and build a more secure digital ecosystem.

Market segmentation by geography

The digital forensics market in India can be segmented geographically based on major regions, reflecting differences in demand, industry maturity, regulatory enforcement and key industries across these regions. Here is an overview of how the market is distributed geographically:



Western India

- Western India has a significant market share of **32 percent**, driven by financial hubs such as Mumbai and Pune.
- High concentration of financial services, including banks, insurance companies and stock exchanges, are critical users of digital forensic services.
- Western India has a strong demand for forensic services focused on financial crimes, insider threats and compliance audits.
- Numerous financial institutions and a growing number of cybersecurity firms and forensic specialists in Mumbai and Pune further strengthen the region's capabilities and market maturity.
- Initiatives of the central and state government authorities are also driving the market.
- Presence of NFSU and its efforts in developing a digital forensic ecosystem across the country is another significant factor propelling the market in the region.
- Due to its advanced technical infrastructure and high cyber threats, the Western region will continue to drive the digital forensic market.

Southern India

- Southern India has a market share of **30 percent**, driven by tech cities such as Bengaluru, Hyderabad and Chennai due to the IT sector's demand.
- Large IT and technology firms, including major software companies, cloud service providers and telecom companies, constitute the consumer base in this region.
- These industries are at high risk for cyber threats and require robust digital forensic capabilities to investigate security incidents and maintain data integrity.
- The market is driven by a skilled workforce and specialised forensic labs catering to the requirements.
- Bengaluru, often called India's tech hub, sees demand from tech giants and start-ups, contributing significantly to the region's market share.
- The emerging interests of state government authorities in developing and modernising digital forensic facilities are also driving the market.
- Southern region is expected to grow fastest, with significant technological businesses and government agencies working to strengthen cybersecurity and digital forensics ecosystems.

Northern India

- Northern India occupies **28 percent** of the market share, primarily driven by government and law enforcement agencies.
- Corporate entities in Delhi and NCR region, including Noida and Gurugram, are other major users of digital forensics.
- Demand for digital forensic services is due to industry-specific regulatory and statutory compliances, cybersecurity needs and investigations.
- The digital forensic market in North India is growing steadily, focusing on enterprise and government-led investigations.
- The presence of cybersecurity companies, forensic training institutes and regulatory bodies also strengthens the market in the region.
- The growing number of digital forensic service providers and a strong emphasis on law enforcement and corporate cybersecurity, this segment is expected to develop further.
- Digital evidence recovery and e-discovery services are in increasing demand due to rigorous data protection and privacy requirements.

Eastern India

- Eastern India is a growing market with a **10 percent** market share, and incoming infrastructure and border security investments drive growth.
- There is growing demand for digital forensics in manufacturing and critical infrastructure sectors, especially energy and utilities.
- This region also serves as a gateway to neighbouring countries, leading to an increased focus on border and cross-border digital forensic needs.
- The digital forensic market is still emerging, and compared with other parts of India, there is limited specialised forensic infrastructure.
- However, government initiatives to improve cybersecurity in the region have led to increased demand for forensic services.

Chapter 6

Sector-specific insights

Government sector

Current scenario

The Ministry of Home Affairs (MHA), Government of India, plays a predominant role in the digital forensic domain in the government sector. The Directorate of Forensic Science Services (DFSS) under the MHA governs the Central Forensic Science Laboratories (CFSL). CFSLs, state forensic science laboratories and specialised cybercrime labs play a significant role in investigating crimes involving digital forensics. Central and state governments are reengineering existing forensic science laboratories or establishing new labs by adopting new tools and techniques for efficient investigations.

The Indian Cybercrime Coordination Centre (I4C), MHA, enhances the coordinated response of Law Enforcement Agencies (LEAs) to cybercrimes. The National Cyber Forensic Laboratory (NCFL) at Delhi and Hyderabad investigates important digital fraud/cyber forensics cases. Indian Computer Emergency Response Team (CERT-In) plays a significant role in safeguarding India's cyber landscape. The National Forensic Sciences University (NFSU), set up under the Act of Parliament in 2020, provides a quality and trained forensic workforce nationwide. To make our country self-reliant in computer forensics, MeitY and other government funding organisations are also involved in fostering, encouraging and promoting R&D in this domain, which is expected to transform the country's overall forensic science and innovation landscape.

Challenges

The government sector faces several challenges in digital forensics related to workforce, budget, tools and technology. A shortage of qualified experts in the field makes building and maintaining strong forensic teams challenging.

Government agencies often face budgetary constraints that can limit investments in digital forensic capabilities. Adequate funding is essential to acquire state-of-the-art tools and technologies, establish forensic laboratories and provide continuous training to personnel. Government agencies must keep pace with these advancements to effectively investigate and analyse digital evidence. However, outdated technologies and tools can hinder investigations and limit the capacity to handle complex cases.

Regular technology assessments and strategic investments in modern tools and equipment are essential. Regular evaluation of digital forensic processes and procedures is necessary to identify gaps, inefficiencies and areas for improvement. Conducting post-incident reviews, analysing performance metrics and incorporating stakeholder feedback can drive continuous process enhancement and ensure the effectiveness of digital forensic capabilities. Key challenges are highlighted below:

- **Workforce shortage:** One of the major challenges the government sector faces is a shortage of skilled digital forensic professionals. Digital forensics requires specialised knowledge and expertise; finding qualified personnel can be difficult.
- **Budget constraints:** Adequate funding is essential to build and maintain robust digital forensic capabilities within the government sector. However, budget constraints can limit the investment in acquiring cutting-edge tools and technologies, providing training to personnel and establishing infrastructure for digital forensic laboratories.
- **Rapidly evolving technology:** The government sector faces the challenge of keeping up with rapidly evolving technologies. Digital forensics requires staying abreast of the latest hardware, software and digital devices that may be encountered during investigations.

- **Complex digital ecosystem:** The increasing complexity of the digital ecosystem poses challenges for the government sector in digital forensics. Investigations may involve various devices, operating systems, networks and applications.
- **Encryption and privacy concerns:** Encryption technologies challenge government agencies to access and decrypt digital evidence. Strong encryption methods can make retrieving relevant data from seized devices or intercepted communications difficult.
- **International jurisdiction and cooperation:** Digital forensics often involves cross-border investigations, presenting jurisdictional challenges for government agencies.
- **Lack of standardisation:** The lack of standardised methodologies, tools and procedures across government agencies can pose challenges in digital forensics. Inconsistent practices and procedures may impact the reliability and admissibility of digital evidence in court.

Focus areas

To enhance capacity in digital forensics within the government sector, here are some potential opportunities:

- **Investing in human resource development:** Allocate resources to recruit, train and retain skilled digital forensic professionals. Provide comprehensive training programmes covering technical skills and legal knowledge relevant to digital investigations. Foster a continuous learning and professional development culture to keep the workforce updated with the latest forensic techniques and technologies.
- **Strengthen collaboration and partnerships:** Foster collaboration among government agencies, law enforcement and the private sector to use expertise and resources. Establish partnerships with academic institutions, research organisations and industry experts to share knowledge, conduct joint research projects and develop innovative solutions. Collaborations can enhance the government's digital forensic capabilities and help address emerging challenges.
- **Increase budgetary allocation:** Ensure sufficient budget allocation for digital forensic capabilities, including investments in state-of-the-art tools, equipment, software licenses and infrastructure. Adequate funding will enable the government sector to acquire advanced forensic technologies, update existing resources and maintain robust digital forensic laboratories.
- **Foster R&D:** Encourage and support research and development initiatives in digital forensics within government agencies. Promote the development of new methodologies, tools and technologies that can enhance investigative capabilities. Establish funding mechanisms and grants to incentivise research in digital forensics and encourage collaboration between researchers and practitioners.
- **Develop Standard Operating Procedures (SOPs):** Establish standardised operating procedures and guidelines for digital forensic investigations. SOPs ensure consistency and reliability in forensic practices, evidence collection, preservation and analysis. Regularly review and update these procedures to align with evolving technologies and legal requirements.
- **Enhance international cooperation:** Strengthen collaboration with international counterparts and establish frameworks for information sharing and joint investigations. Develop partnerships to exchange best practices, share intelligence and improve cross-border cooperation in combating cybercrime. International cooperation is crucial in addressing global cyber threats and transnational digital investigations.
- **Establish digital forensic training institutes:** Develop specialised training institutes or centres of excellence in digital forensics. These institutes can provide comprehensive training programmes for government personnel, law enforcement officers and other stakeholders. Offer certification programmes and professional development courses to build a skilled and certified workforce in digital forensics.
- **Implement quality assurance measures:** Establish quality assurance mechanisms to ensure the accuracy, reliability and integrity of digital forensic processes and outcomes. Regular audits, proficiency testing, adherence to international standards and best practices can enhance digital forensic investigations' credibility and evidence's admissibility in legal proceedings.
- **Stay updated with technological advancements:** Continuously monitor and adapt to emerging technologies and trends in digital forensics. Stay informed about new devices, software, encryption and data storage techniques. Regularly evaluate and acquire cutting-edge tools and technologies to enhance investigative capabilities and handle complex digital evidence.
- **Strengthen legislative support:** Advocate for legislation and policies that support digital forensics and address emerging challenges. Collaborate with legal experts and policymakers to ensure that laws and regulations keep pace with technological advancements. Foster a legal framework that facilitates digital investigations while protecting privacy rights and upholding the principles of due process.
- **Dedicated cadre:** Establishing a dedicated cadre for cyber security and digital forensics officers is crucial to building a robust protective and digital investigative framework in India. A separate cadre with continuous skill development, hands-on training in advanced forensic tools and exposure to emerging technologies will ensure domain expertise, operational continuity and the development of a highly skilled workforce capable of addressing the rapidly evolving challenges in cybercrime and digital investigations.

Private sector

Current scenario

In India's private sector, digital forensics is increasingly vital for businesses to combat rising cyber threats, especially as digital transformation accelerates. Companies in finance, healthcare, telecom and IT recognise the importance of digital forensics in investigating data breaches, intellectual property theft and insider threats. With incidents of cyberattacks on the rise, businesses are proactively investing in digital forensics to secure sensitive information and comply with regulations such as the Information Technology Act and the new Digital Personal Data Protection (DPDP) Act of 2023. This regulation mandates stricter data protection measures, creating a demand for advanced forensic capabilities to meet compliance requirements and prevent penalties.

Leading players, including private forensic service providers and security consultancies, are expanding to meet the demand. The government's support for innovation and infrastructure, such as mobile and cloud forensics tools, also bolsters digital forensic capabilities. Specialised start-ups are also emerging, providing cost-effective and regionally focused solutions tailored to meet the needs of the Indian markets.

Challenges

The private sector in India faces several challenges in implementing effective digital forensics capabilities:

- **Skilled resource constraints:** Digital forensics requires specialised tools and skilled personnel, which are costly. Many private organisations, particularly small and midsized enterprises, may lack the budget to invest in advanced forensic tools or to employ dedicated digital forensics experts.
- **Acute talent shortage:** India has a limited pool of trained digital forensic professionals, making hiring qualified personnel difficult. This talent gap leads to delays in investigations and a heavy reliance on third-party vendors for forensic services, which can be costly and potentially compromise data privacy.
- **Compliance with data privacy and regulations:** Compliance with data protection laws, including the Digital Personal Data Protection (DPDP) Act, 2023 and other regulatory requirements, requires organisations to implement rigorous data handling and investigative processes. Failure to adhere can result in penalties. Private companies often struggle to balance forensic needs with privacy requirements, especially when dealing with cross-border data transfers or multiple jurisdictions.
- **Rapidly evolving cyber threats:** Cyberattacks are becoming more sophisticated, with attackers employing new techniques to evade detection. This makes it challenging for private companies to maintain up-to-date forensic capabilities to respond effectively. Continuous training and technology upgrades are needed to address these evolving threats, adding to operational costs.
- **Legal and procedural barriers:** Digital forensic evidence must meet legal standards to be admissible in court, which requires strict protocol adherence.
- **Dependence on external vendors:** Given the high costs and expertise required, many private sector entities outsource digital forensic tasks. While this approach allows organisations to access expert services and advanced tools, they must conduct due diligence when selecting third-party partners. With the right selection, third-party vendors can effectively support the private sector's digital forensic needs while maintaining data confidentiality and integrity. To further strengthen this process, ongoing investment, training and clear regulatory frameworks will be crucial to ensure the effective management of digital forensics in India.

Opportunities for growth

The private sector in India has multiple growth opportunities in digital forensics, driven by increased cyber risks, regulatory needs and technological advancements. Here are some key growth avenues:

- **Increasing demand for digital forensics and incident response services:** with growing numbers and increasing complexity of cyberattacks, businesses in finance, healthcare and e-commerce require bespoke digital forensic services as part of their cybersecurity plans. This demand for specialised forensic services presents growth opportunities for private firms focused on preventing data breaches and cybercrime.
- **Expansion of cloud and mobile forensics:** The rapid adoption of cloud computing and mobile devices has brought new data acquisition and analysis challenges. As organisations adopt these technologies, there is increasing demand for specialised forensic services for cloud and mobile environments. Private companies can expand their service offerings in these emerging areas.
- **Regulatory compliance and data privacy needs:** New regulations, such as the DPDP Act, have increased the need for businesses to comply with new data protection standards. This creates an opportunity for private digital forensic companies to offer compliance services such as IT audits, incident response and digital forensics to help businesses meet regulatory requirements.
- **Innovation in forensic tools development:** There is a growing demand for specialised forensic tools tailored to address the unique challenges of the Indian market, including local languages, regional data formats and specific privacy standards. Start-ups and established companies can innovate and develop affordable, tailored solutions for the diverse needs of various industries.
- **Training and certification programmes:** As the digital forensics talent pool in India is still developing, private sector firms can create training and certification programmes. This helps address the skills gap and provides new revenue streams for companies offering cybersecurity and digital forensics expertise.

Academic sector

Current scenario

The academic sector of digital forensics provides learners and researchers with essential expert technical knowledge, competence and digital forensic research skills in cybercrime investigation and its application in emerging areas such as IoT and drone forensics.

In India, academia plays a crucial role in advancing the field of digital forensics through research, specialised programmes and collaboration with law enforcement and the private sector. Universities and institutions across India offer specialised courses, diplomas and certifications in digital forensics and cybersecurity. Notable institutions apart from the National Forensic Science University, such as the Indian Institute of Technology (IIT) and the National Institute of Technology (NIT), have introduced digital forensic courses as part of computer science and cyber law curriculums. Programmes focus on teaching students the fundamentals of forensic analysis, malware detection, network forensics and cybercrime investigation.

Academic programmes are addressing the significant skills gap in digital forensics. By equipping students with technical skills in data recovery, encryption analysis and evidence handling, academic institutions are preparing a workforce capable of meeting the growing demand for cyber forensic experts in both public and private sectors.

Challenges

The academia sector in India faces several challenges in implementing effective digital forensics capabilities:

- **Inadequate digital forensic lab infrastructure:** Digital forensics requires specialised tools for data recovery, encryption analysis and malware detection, which are often expensive and not readily available in academic settings. Many universities and institutions lack state-of-the-art forensic labs with the latest software and hardware necessary for digital forensic analysis.
- **Shortage of human resources**: There is an acute shortage of qualified digital forensics professionals in India due to the lack of specialised academic programmes, training centres and research opportunities. The absence of well-defined curriculums and tailored educational pathways for digital forensics contributes to a skills gap, leaving industries struggling to fill positions. Academia must expand and modernise educational offerings, provide hands-on training and align more closely with industry requirements.
- **Limited academia-industry partnerships:** Collaboration between academia and the digital forensic industry is relatively limited in India. Industry partnerships can provide students with hands-on training, internships and exposure to real-world forensic challenges, but such opportunities remain scarce. Students and researchers lack practical insights into the industry's demands and challenges without these collaborations.
- **Restricted access to case studies:** Digital forensics often involves working on sensitive cases with confidentiality requirements. Academic institutions may have limited access to case studies or real-life data, which restricts the hands-on experience students need to fully understand forensic processes and investigative methods.
- **Limited awareness among students:** Digital forensics is still a developing field in India and many students are unaware of it as a career path. Compared to software engineering or data science, digital forensics may appear niche and less lucrative, resulting in lower enrolment in available courses.
- **Lack of exposure:** While awareness of cybercrimes is adequately made available to the masses, digital forensics is a specialised field, often introduced only at the postgraduate level or as part of advanced computer science courses. Thus, there is limited exposure to forensic topics at the undergraduate level, which narrows the pipeline of students interested in pursuing careers in this area.
- **Limited publishing and research funding:** Conducting and publishing high-quality research requires significant time and resources. Indian academic institutions may struggle to publish internationally recognised research papers in digital forensics due to a lack of funding or skilled researchers.

Opportunities for growth

The academic sector in India has multiple growth opportunities in digital forensics. Recent government initiatives to establish educational institutes with digital forensics as a major focus, partnerships with industry and government forensic labs, and a curriculum focused on emerging technologies will be key to bridging the skill gap, advancing research and building a robust digital forensic ecosystem in India. By seizing the following opportunities, academia can play a transformative role in India's digital forensic sector.

- **Deployment of emerging technologies:** Developing curricula that cover blockchain forensics, cloud forensics and IoT security would address current gaps in staying updated on emerging technologies. Academic programmes can prepare students for evolving challenges by including them in coursework.
- **Collaboration with private and public sectors:** Partnering with cybersecurity firms, consulting firms, government agencies and law enforcement can help academia access resources, tools and real-world case data, enhancing the practical experience for students and researchers. Joint research projects could focus on developing indigenous forensic tools and methodologies.
- **R&D in digital forensics:** Academia has an opportunity to lead the creation of indigenous digital forensic tools, reducing dependency on costly foreign technologies. With India's large mobile user base and unique digital landscape, local tools such as mobile and social media forensics can be designed specifically for regional needs.
- **Student-driven research projects:** Encouraging students to participate in digital forensic research projects can promote innovation and engagement in developing in-house digital forensic hardware and software. Competitions, hackathons, seminars and research symposiums in digital forensics provide hands-on learning experiences, inspiring students to explore careers in the field.
- **Awareness through workshops and seminars:** Offering specialised workshops, certification programmes and short-term training for law enforcement and the judiciary can strengthen academia's role in forensic education. These programmes would equip professionals with forensic skills, bridging knowledge gaps and enhancing the effectiveness of digital crime investigations.

Chapter 7

Global and Indian digital forensics markets

The digital forensics market in India shares many similarities with the global market but has distinct differences due to regional factors, regulatory frameworks, technological adoption and industry focus. Here is a comparison of both:

Market size and growth rate

Global market: Per the secondary research, the value of the global digital forensics market stands at ~US$6.5 billion and is expected to post a CAGR of 11 percent from 2024 to 2030, reaching an estimated market size of US$14.5 billion by the end of the decade. Major growth drivers include increasing cybercrime, AI and machine learning advancements, regulatory compliance needs and rapid digital transformation across BFSI, healthcare and government sectors.

Indian market: While smaller in absolute terms, at US$0.19 billion, India's digital forensics market is growing rapidly, with a projected CAGR of ~40 percent over the same period. The demand is primarily driven by rapid digital adoption in private and government sectors, increased cyber-attacks and regulatory developments.

FY2024	FY2025	FY2026	FY2027
$187.2M	$265.9M	$380M	$540.1M

FY2028	FY2029	FY2030
$750M	$1,010M	$1,350M

Indian digital forensic market size

The value of the Indian digital forensic market is forecast at US$1.39 billion compared with the estimated global value of US$14.5 billion. India holds 3 percent of the digital forensic market share, but by 2030, India will have 10 percent of the global digital forensic market. This will be because the Indian market is experiencing high growth, especially in regulated industries, and is catching up in technology integration, which is driven by rising cybersecurity concerns and regulatory reforms. While both markets face similar challenges, such as skills shortages and cost constraints, India’s unique regulatory landscape and rapid digital adoption are likely to continue fuelling its digital forensics growth at an accelerated rate.

Key drivers

Global market: Cyber threats such as ransomware, insider threats and phishing scams are primary drivers of digital forensics globally. The rising adoption of cloud computing and IoT devices worldwide also creates additional demand for forensic services to secure these new environments. Regulatory compliance, especially with frameworks such as GDPR and HIPAA in Europe and the US, mandates incident investigation and data protection, further fuelling demand.

Indian market: India's market is heavily influenced by recent regulatory requirements provided by RBI, SEBI and CERT-In, including the DPDP Act, which enforces stringent data protection and breach notification standards. The financial services, telecom and government sectors lead in forensic adoption, driven by high exposure to cyber risks and strict compliance mandates from bodies such as the RBI and SEBI. Additionally, India's rapid transition to digital payments and remote work has created significant demand for digital forensics to address related security risks.

Sector-wise demand

Global market: Globally, the BFSI and government sectors are the most significant users of digital forensics, followed by healthcare, telecom and critical infrastructure. The increased use of electronic health records in healthcare and the digitisation of public administration have driven strong growth in these sectors. Cloud and IoT forensic capabilities are also in significant demand across industries.

Indian market: The government sector is dominant in India primarily because it handles high volumes of sensitive data. The country's government sector also invests significantly in digital forensics for national security and cyber defence. Healthcare and manufacturing are emerging sectors for digital forensics as they embrace digital transformation and IoT.

Challenges

Global market: The global market faces challenges such as a shortage of skilled forensic professionals, the complexity of managing cross-border data regulations and high costs associated with cutting-edge forensic technologies. These challenges impact the ability of smaller companies to adopt advanced forensic solutions and necessitate reliance on managed forensic services.

Indian market: In India, the challenges are compounded by a pronounced shortage of skilled digital forensics professionals, limited awareness of digital forensics among Small and Medium Enterprises (SMEs) and high costs that deter SMEs from adopting in-house forensic solutions. Additionally, India's legal and regulatory landscape regarding cyber and data protection is still developing, which adds complexity for companies aiming to comply with evolving standards.

Future trends and opportunities

Global market: Globally, the digital forensics market is rapidly integrating advanced technologies such as AI and machine learning, cloud forensics, blockchain and big data analytics. AI is increasingly used for faster and more accurate analysis, while blockchain is explored for secure data handling and evidence integrity. The global digital forensics market is expected to keep expanding as cyber threats evolve and technologies such as AI, IoT and blockchain continue to develop. As regulations become stricter worldwide, companies across regions must invest in digital forensics to ensure compliance, investigate breaches and secure digital assets.

Indian market: While India is adopting AI and cloud-based forensics, the market is in an earlier phase of technological integration compared with North America and Europe. However, as the country's tech sector matures and demand increases, the adoption of AI, ML and blockchain in forensic investigations is expected to grow. Cloud forensics is particularly gaining traction as organisations move their operations online. The market is expected to grow significantly in India, driven by digital transformation initiatives, increased cybercrime and regulatory requirements. Government initiatives, such as establishing cyber forensic labs and developing cybersecurity infrastructure, will play a critical role in market growth. The private sector, especially SMEs, is anticipated to increasingly rely on managed forensic services due to cost and expertise limitations.

Chapter 8

Future of digital forensics market in India

The digital forensics market in India is experiencing rapid growth, fuelled by the country's accelerating shift towards digitisation. As digital technologies advance, so do the complexities of cyber threats. This growth in digital adoption has created a pressing need for specialised tools and expertise in digital forensics. With its vast population and rapidly expanding digital user base, India presents a dynamic landscape for the evolution of this market.

The following trends and factors are expected to shape the future of India's digital forensics industry:

Rise in cyberattacks

As India becomes increasingly dependent on digital platforms for business, government and personal activities, cyberattacks are expected to rise significantly. Cybercrimes such as data breaches, ransomware, fraud and intellectual property theft are becoming more sophisticated and widespread.

This surge in cyber threats drives the demand for advanced digital forensics solutions, which will be essential for investigating and mitigating the damage caused by such incidents. In the future, digital forensics will become a key component of cybersecurity strategies, helping organisations and authorities respond more effectively to cyberattacks.

Demand for advanced forensic solutions

As cyberattacks evolve in sophistication, there will be an increased demand for cutting-edge forensic solutions. Traditional forensic tools are often inadequate to handle the new challenges that emerging threats pose. To stay ahead of the curve, India will see a growing need for technologies such as:

AI and ML integration: AI and ML are set to revolutionise digital forensics by enabling more efficient analysis of digital evidence. These technologies can automate tasks such as data categorisation, anomaly detection and evidence sorting, drastically reducing the time and resources needed for investigations. The integration of predictive analytics will also improve the ability to anticipate cyber threats and mitigate risks before they materialise, further driving the need for AI-driven forensics tools.

Growth of blockchain forensics: With the rise of cryptocurrencies and decentralised finance, the need for blockchain forensics is becoming more prominent. It is essential for tracking cryptocurrency transactions, ensuring transparency and identifying illicit activities such as money laundering. Tools capable of investigating blockchain transactions and providing insights into cryptocurrency flows will play a crucial role in criminal investigations and regulatory enforcement, particularly in the financial sector. As India's digital financial ecosystem grows, so will the demand for blockchain forensics expertise.

Government initiatives

The Indian government is taking steps to bolster the country's cybersecurity framework, which will significantly impact the growth of the digital forensics market. Several initiatives are in place to improve digital security and forensic capabilities:

National cybersecurity strategy: The Indian government's increasing focus on cybersecurity, highlighted by the National Cyber Security Policy 2020, underscores the importance of digital forensics in safeguarding the country's digital infrastructure. The policy aims to enhance national cyber defence, creating a demand for more sophisticated forensic tools and expertise.

National forensic infrastructure enhancement scheme: In 2024, the government introduced a major initiative to enhance forensic capabilities. The scheme provides a financial outlay of INR2,254 crore from 2024 to 2029, aiming to modernise forensic laboratories, improve training programmes and integrate digital forensics into law enforcement practices.

Stricter regulations and compliance standards

With the rise in digital data breaches and privacy concerns, new laws and regulations are being implemented to ensure better data protection. The DPDP Act, 2023 and other legislations will create a need for robust digital forensics solutions to ensure compliance and investigate data breaches.

Regulatory compliance

As data privacy laws become stricter, organisations will require digital forensics tools to verify compliance, conduct audits and investigate potential violations. The role of digital forensics in enforcing these regulations will become increasingly important in sectors such as finance, healthcare and e-commerce.

Chapter 9

Strategic insights and growth roadmap

Increasing cybersecurity threats

Cyber threats continuously grow in numbers and sophistication, escalating demand for digital forensics solutions. The rise of cybercrimes such as data breaches, ransomware and financial fraud in major and industry-driving sectors such as BFSI, healthcare and government makes digital forensics an imperative need. This creates direct pressure on organisations to invest in digital forensic and cyber security solutions to ensure faster and more accurate threat detection, investigation and response.

Regulatory pressures and compliance

India is making big waves to strengthen its data protection and cybersecurity laws, and businesses are expected to adhere to these new compliance requirements. Companies are investing in digital forensics solutions to ensure that they can investigate and mitigate any data breaches or cyberattacks, avoid fines and penalties and maintain consumer trust.

Technological advancements in digital forensics

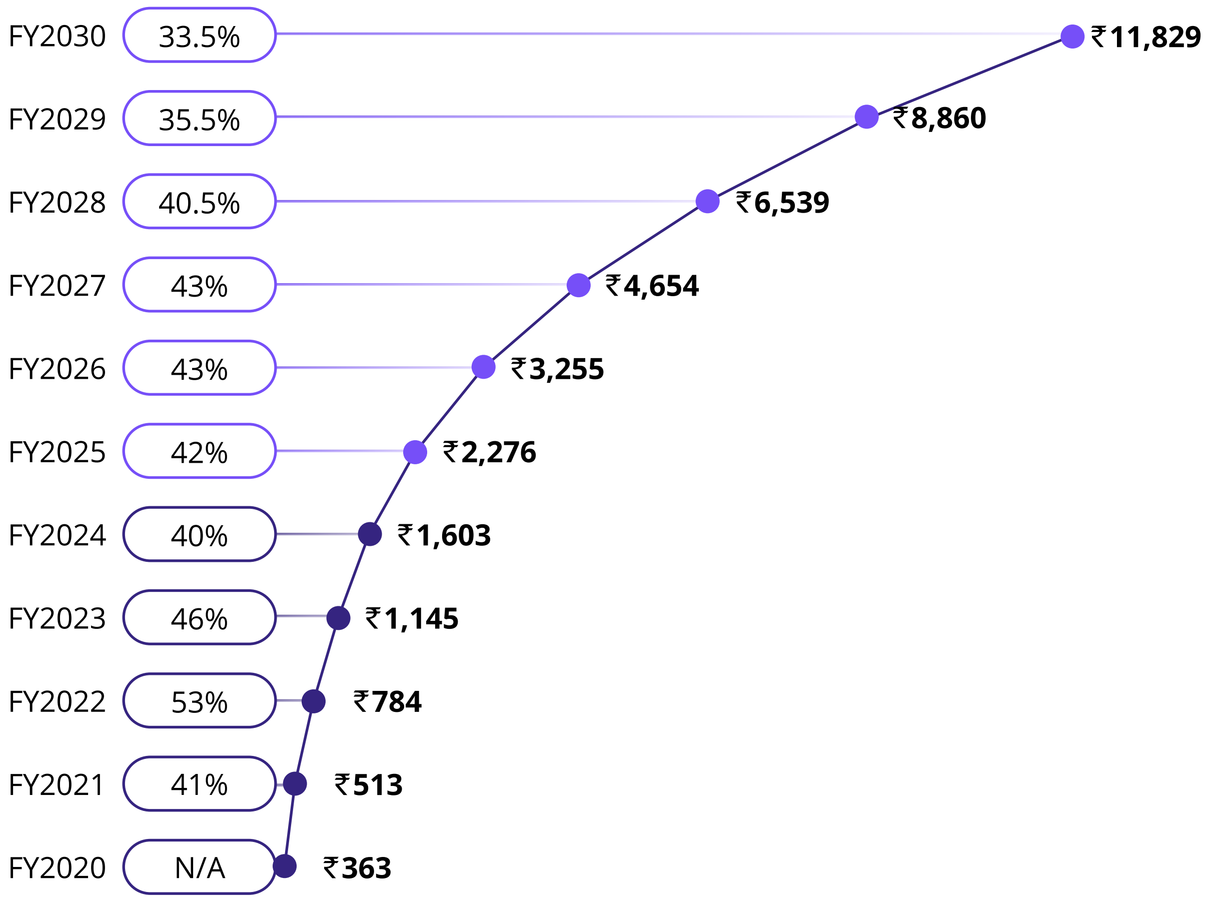
Integrating AI and ML technologies has significantly improved digital forensics. AI and ML are reducing the turnaround time needed for investigations while increasing the accuracy of digital investigations.

Shift towards Managed Service Providers (MSP)

Partnering with MSPs has proven to be a cheap and efficient strategy. Therefore, many SMEs are turning to MSPs for their digital forensics needs. The growing adoption of MSPs creates significant business entry opportunities for digital forensics companies to expand their market presence by offering end-to-end cybersecurity and digital forensics services.

Growth trajectory for the digital forensics market in India (2020-2030)

Partnering with MSPs has proven to be a cheap and efficient strategy. Therefore, many SMEs are turning to MSPs for their digital forensics needs. The growing adoption of MSPs creates significant business entry opportunities for digital forensics companies to expand their market presence by offering end-to-end cybersecurity and digital forensics services.



Projected Growth

The Indian digital forensics market is expected to reach INR11,829 crore by FY2030 while maintaining strong yearly growth over the next several years. The market will likely maintain a CAGR of 42 percent during FY2024–FY2025, driven by increasing awareness, expanding digital infrastructure and the urgent need for cybersecurity solutions across sectors.

Chapter 10

Key recommendations

The acute shortage of trained digital forensic professionals in India makes hiring qualified personnel difficult, leading to investigation delays. Public-private collaboration to use expertise and resources would ensure optimum usage and address the talent gap.

Fostering industry-academia partnerships would enhance knowledge sharing and facilitate students with hands-on training, internships and exposure to real-world forensic demands and challenges. Such collaborations would drive innovative tools and solutions to elevate the digital forensic ecosystem.

Continuous innovation is an integral aspect of ensuring novel solutions. Encouraging R&D initiatives would promote the development of new methodologies, c that can enhance investigative capabilities. Establishing funding mechanisms and grants to incentivise research in digital forensics and encouraging collaboration between researchers and practitioners through initiatives such as Hackathons and All India Forensic Science Conferences held annually are the proper steps towards this direction. Similarly, a conference dedicated to digital forensics can be held annually where CFSLs, SFSLs and other LEA-specific agencies can present research papers and discuss upcoming challenges. This will ensure a continual growth path that will pave the way for enriching the digital forensics market.

Promoting start-ups with proper resources and opportunities would boost innovation levels, leading to digital forensic solutions that would cater to the Indian market and fulfil requirements at the global level. Standardising the operating procedures and developing guidelines for digital forensic investigations would ensure consistency and reliability in forensic practices. Government agencies’ lack of standardised methodologies, tools and procedures poses severe challenges. Inconsistent practices and procedures impact the reliability and admissibility of digital evidence in court. Establishing domestic standards customised to local requirements can open up new dimensions and elevate Indian presence on the global spectrum. Periodic review and updates in alignment with the evolving technologies and legal requirements would enhance the credibility of digital forensic investigations and the admissibility of evidence in legal proceedings.

Strengthening collaboration with private and international counterparts and establishing frameworks for information sharing and joint investigations is crucial for addressing global cyber threats and transnational digital investigations. Such cooperation will also develop partnerships to exchange best practices, share intelligence and improve cross-border cooperation in combating cybercrime.

Establishing specialised digital forensic training institutes or centres of excellence in digital forensics can provide comprehensive training programmes for government personnel, law enforcement officers and other stakeholders. Customised certification programmes and professional development courses would yield a skilled and certified workforce.

Investing in human resource development is a significant factor that could catapult the Indian market to the global level. Considering the ever-changing dynamics of the digital forensic ecosystem and the unique skill set that is required, it is essential to allocate resources to recruit, train and retain skilled digital forensic professionals. Providing comprehensive training programmes that cover technical skills and legal knowledge and fostering a culture of continuous learning and professional development to keep the workforce updated with the latest forensic techniques and technologies are crucial. Hackathons and the All-India Forensic Science Conference held annually are the proper steps towards this direction. Annual conferences dedicated to digital forensic professionals, both domestic and international, would be another step forward. A comprehensive capacity development programme to build and retain a skilled pool of digital forensic professionals will ensure a robust framework and empower the country in the digital forensic arena.

A push for digital forensics at the grassroots level would make the country a strong force in the domain market. Challenges include inadequate digital forensic lab infrastructure in academic settings, restricted access to case studies, creating awareness among students, creating more exposure at the undergraduate level, supporting student-driven research projects, awareness through workshops and seminars, target course offerings, domestic training and certification programmes, etc., are some of the measures that could be undertaking for making India a global force.

Investing in updated forensic tools tailored to handle emerging technologies, such as cloud and mobile forensics, is crucial. This includes leveraging AI and ML to streamline data analysis, automate processes and improve the accuracy and speed of forensic investigations.

Private companies should integrate data protection measures within their forensic processes to align with regulatory frameworks such as the DPDP Act. This involves regular compliance audits, data privacy assessments and the implementation of best practices for data handling to avoid potential legal and financial liabilities.

Partnering with specialised digital forensic service providers can be cost-effective for companies lacking the resources for full in-house forensic teams. These partnerships can offer expertise and state-of-the-art forensic solutions without the need for significant internal investments.

The outcome of this initiative would have long-term and far-reaching impacts and elevate the country to the next level in the global scenario.

References

1. India saw 129 cybercrimes per lakh population in 2023 | India News - The Times of India (https://timesofindia.indiatimes.com/india/india-saw-129-cybercrimes-per-lakh-population-in-2023/articleshow/106524847.cms)
2. India will need 90,000 forensic scientists in 9 years: Amit Shah | Mysuru News - Times of India (https://timesofindia.indiatimes.com/city/mysuru/india-will-need-90000-forensic-scientists-in-9-years-amit-shah/articleshow/97408206.cms)
3. Digital Payments | Department of Financial Services | Ministry of Finance | Government of India (https://financialservices.gov.in/beta/en/page/digital-payments)
4. 4. Report of Indias G20 Task Force On Digital Public Infrastructure.pdf (https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf)
5. India's E-commerce Boom: Growth, Trends & Future Prospects | IBEF (https://www.ibef.org/industry/ecommerce)
6. The Indian Telecom Services Performance Indicators July–September, 2024 (https://www.trai.gov.in/sites/default/files/2025-01/QPIR_01012025_0.pdf)
7. TELECOM REGULATORY AUTHORITY OF INDIA New Delhi, 22"4 January, 2025 (https://trai.gov.in/sites/default/files/2025-01/PR_No.06of2025_0.pdf)
8. Cybercrime surge in India: Over 7,000 daily complaints in 2024, key locations identified in Southeast Asia (https://ddnews.gov.in/en/cybercrime-surge-in-india-over-7000-daily-complaints-in-2024-key-locations-identified-in-southeast-asia/)
9. A survey of prosecutors and investigators using digital evidence: A starting point - PMC (https://pmc.ncbi.nlm.nih.gov/articles/PMC10311201/#bib1)
10. India GCC Landscape Report – The 5 Year Journey | nasscom (https://nasscom.in/knowledge-center/publications/india-gcc-landscape-report-5-year-journey)
11. Press Release:Press Information Bureau (https://pib.gov.in/PressReleasePage.aspx?PRID=2039649)
12. https://pib.gov.in/PressReleasePage.aspx?PRID=2039061 (https://pib.gov.in/PressReleasePage.aspx?PRID=2039061)
13. Unveiling Cyber Forensics R&D Roadmap of India by MeitY (https://www.cdac.in/index.aspx?id=cs_cf_CFS_StratagemNew)
14. Digital 2024: India — DataReportal – Global Digital Insights (https://datareportal.com/reports/digital-2024-india)
15. Explore the Ericsson Mobility Report November 2024 (https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2024)

Glossary

AI	Artificial Intelligence
ANSR	Association of National Service Providers
AWS	Amazon Web Services, A cloud computing platform offering a wide range of services for computing, storage and data management.
BFSI	Banking, financial services, Insurance
Big4	Top four consultancy firms: Deloitte, KPMG, PWC and E&Y
Blockchain	A decentralised digital ledger
BNS	Bharatiya Nyaya Sanhita
BNSS	Bharatiya Nagarik Suraksha Sanhita
BSA	Bharatiya Sakshya Adhiniyam
BYOD	Bring Your Own Device, A policy allowing employees to use their personal devices for work purposes.
CAGR	Compound annual growth rate
CBI	Central Bureau of Investigation
CEO	Chief Executive Officer
CERT-IN	Computer Emergency Response Team – India
CFMC	Cyber Fraud Mitigation Centres
CFSLs	Central Forensic Science Laboratories
CIO	Chief Information Officer
CISO	Chief Information Security Officer
cryptocurrency	A digital currency designed to work through a computer network
DFS	Directorate of Forensic Science
DPDP Act 2023	Digital Personal Data Protection Act, 2023
ED	Enforcement Directorate
EDR	Endpoint Detection and Response, A security solution for real-time monitoring and response to threats on endpoints like computers and mobile devices.
e-KYC	electronic Know Your Customer
FIPS	Federal Information Processing Standard
FMCG	Fast-Moving Consumer Goods
FSLs	Forensic Science Laboratories are laboratories that analyse evidence, including digital evidence, in criminal investigations.
FY	Financial Year
GCC	Global Capability Centres
GDPR	General Data Protection Regulation
GMV	Gross Merchandise Value
HIPPA	Health Insurance Portability and Accountability Act
I4C	Indian Cybercrime Coordination Centre
IBEF	India Brand Equity Foundation
IoT	Internet of Things, A network of connected devices that collect and exchange data over the internet
ISO	International standard-setting NGO
IT	Information Technology
LEAs	Law Enforcement Agencies, Agencies responsible for enforcing laws and investigating crimes, including cybercrimes.
MCA	Ministry of Corporate Affairs
MeitY	Ministry of Electronics and Information Technology
MHA	Ministry of Home Affairs
ML	Machine Learning
MSS	Managed Security Services
MSSP	Managed Security Services Provider
NASSCOM	National Association of Software and Service Companies
NFIES	National Forensic Infrastructure Enhancement Scheme
NFSU	National Forensic Sciences University
NIA	National Investigation Agency
OEM	Original Equipment Manufacturer
open-source Tool	Software having source code freely available on the internet
PDPB	Personal Data Protection Bill
PIB	Press Information Bureau
R&D	Research and Development
RBI	Reserve Bank of India
Resellers	Third-party sellers of forensic tools and services
Samanvay platform	Joint Cyber Crime Investigation Facility System
SEBI	Securities and Exchange Board of India
SMEs	Subject Matter Experts
Threat detection	Identifying and analysing malicious activity that could compromise security
TRAI	Telecom Regulatory Authority of India
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
XDR	Extended Detection and Response, A unified security platform that enhances threat detection and response across multiple layers of an organisation's IT infrastructure.
XSOAR	Security Orchestration, Automation and Response, A set of tools and processes that help automate security operations, integrate security systems and streamline incident response.

Acknowledgements

We extend our heartfelt gratitude to the esteemed members of the digital forensic industry, including distinguished government officers, industry leaders, forensic experts, dedicated professionals in the corporate sector, academicians, students, etc., who actively participated in our study and generously shared their invaluable insights.

Our sincere appreciation goes out to all for their significant contribution and unwavering support. We recognise their pivotal role with great acknowledgement, as without their involvement, this report would not have come to fruition. On behalf of DSCI and Deloitte India, we express our sincere thanks for their indispensable collaboration.

The report aims to immensely benefit all concerned stakeholders in the digital forensic domain who are integral to the adoption and dissemination of the technology, product and support. It is intended to act as a ready reckoner for everyone who needs to start, look up and engage with other important stakeholders while dealing with digital forensics.

About DSCI and Deloitte

About DSCI

The Data Security Council of India (DSCI) is a premier industry body on data protection in India, set up by NASSCOM, committed to making cyberspace safe, secure, and trusted through best practices, standards, and initiatives in cybersecurity and privacy. Bringing together governments, industry sectors such as IT-BPM, BFSI, and telecom, as well as data protection authorities, think tanks, and industry associations, DSCI drives policy advocacy, thought leadership, capacity building, and outreach initiatives.

As part of its commitment to strengthening India’s cybersecurity ecosystem, DSCI, in collaboration with the Ministry of Electronics & Information Technology (MeitY), Government of India, established the National Centre of Excellence (NCoE) for Cybersecurity Technology Development. NCoE is dedicated to catalyzing cybersecurity technology development and entrepreneurship, fostering innovation across critical and emerging security domains. With state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE enables research, technology development, and solution validation for adoption across government and industry. By translating innovation and research into market-ready solutions, NCoE is driving the creation of an integrated technology stack, featuring cutting-edge, homegrown security products and solutions.

About Deloitte

Deloitte is one of the world’s largest and most diversified professional services organisations, providing assurance, tax, strategy, risk & transactions, and technology & transformations services through more than 460,300 professionals in more than 150+ countries. Our organisation includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touche Tohmatsu India LLP (DTTI LLP) is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate.

In India, Deloitte is recognised as one of the country’s top professional services firms, spread across 14 cities namely – Ahmedabad, Bengaluru, Bhubaneswar, Chennai, Coimbatore, Goa, New Delhi, Hyderabad, Jamshedpur, Kochi, Kolkata, Mumbai, Noida, and Pune. With over 36000 professional staff, our professionals are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments.

Connect with us

Deloitte India

K.V. Karthik
Partner and Leader -
Forensic & Financial
Crime
kvkarthik@deloitte.com

Sachin Yadav
Partner -
Forensic & Financial
Crime
sachyadav@deloitte.com

Jayant Saran
Partner -
Forensic & Financial
Crime
jsaran@deloitte.com

DSCI

Teja Chintalapati
Principal Manager -
Cyber Innovation
teja.chintalapati@dsci.in

Contributors

Deloitte India

Sachin Yadav

K V Baskar

Mohammad Azam Nizami

Nachiketa Sharma

Rishi Dhamija

Shailesh Kand

DSCI

Dr N Sarat Chandra Babu

Niharika Singh

Teja Chintalapati

DSCI

PROMOTING DATA PROTECTION

The information contained in this report has been obtained or derived from sources believed by DSCI to be reliable. However, DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information. We shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. The material in this publication is copyrighted. You may not distribute, modify, transmit, reuse or use the contents of the report for public or commercial purposes, including the text, images, presentations, etc. without prior consent from DSCI.

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This document contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this document, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this document, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this document.

The content of this document is based on information available at the time of writing and is subject to change. We do not undertake any obligation to update or revise the content based on new information or developments. The M&A outlook discussed in this document is subject to market risks, including but not limited to economic fluctuations, geopolitical events, and regulatory changes. These factors can significantly impact the accuracy of the predictions made herein. Any mention of specific companies, deals, or industries is not an endorsement or recommendation.