Quality Mantra Aug, 2025

A Newsletter of International Certification Services

Special Issue On

From Jugaad to Justice: Resourceful Forensic Solutions in Real Cases

Quality Mantra Aug, 2025
A Newsletter of International Certification Services

Cybersecurity regulations : India

CMD

Dr. Sundar Kataria

It is a global village with shrieking world boundaries & advantages information Technology has brought transformation of online digital Operation enhancing efficience & effectives of the origination operation.

As the world grapples with rampant cyberattacks, policymakers in the region have toughened their data security measures and business compliance is crucial

AI can help to shren with Indian buiesness facing cyber attack it so to global average of it is important to it so to global average of it is imp to strength security of information data.

The Information Technology (IT) Act, 2000, is the primary legislation dealing with cybersecurity, data protection and cybercrime. that covers many front activity & its key features are

- Granting statutory recognition and protection to electronic transactions and communications;
- Aiming to safeguard electronic data, information and records; Aiming to prevent unauthorised or unlawful use of computer systems; and
- Identifying activities such as hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft as punishable offences.

Rules and regulations framed under the IT Act regulate different aspects of cybersecurity as follows:

Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (2013 rules), established the Computer Emergency Response Team (CERT-In) as the administrative agency responsible for collecting, analysing and disseminating information on cybersecurity incidents, and taking emergency response measures. These rules also put in place obligations on intermediaries and service providers to report cybersecurity incidents to the CERT-In.

Directions on information security practices, procedure, prevention, response and reporting of cyber incidents for a safe and trusted internet, issued in 2022 by the CERT-In, add to and modify existing cybersecurity incident reporting obligations under the 2013 rules.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI rules) require companies that process, collect, store or transfer sensitive personal data or information to implement reasonable security practices and procedures.

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021) require intermediaries to implement reasonable security practices and procedures to secure their computer resources and information, maintaining safe harbour protections. Intermediaries are also mandated to report cybersecurity incidents to the CERT-In.

Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, oblige companies that have protected systems – as defined under the IT Act – to put in place specific information security measures.

Cybersecurity of critical information infrastructure (CII) – defined as any computer resource that can have a debilitating impact on national security, the economy, public health or safety if incapacitated or destroyed – is regulated by guidelines issued by the National Critical Information Infrastructure Protection Centre (NCIIPC)

Since cybersecurity is a cross-cutting issue, India has a complex inter-ministerial and inter-departmental institutional framework for cybersecurity, with several ministries, departments and agencies performing key functions. For instance, the Ministry for Electronics and Information Technology (MeitY) deals with policy relating to IT, electronics and the internet, including cyber laws. It set up the CERT-In as a nodal agency for co-ordination and handling of cyber incident response activities.

The Ministry of Home Affairs looks at internal security, including cybersecurity. For this purpose, it has set up the cyber and information security division, comprising a cybercrime wing, cybersecurity wing and monitoring unit. To combat cybercrime, it also established the Indian Cyber Crime Co-ordination Centre in 2018. The NCIIPC, the nodal agency for CII, is set up under the National Security Adviser.

Information Security Measures

At the federal level, the IT Act places security obligations on organisations handling sensitive personal data. These are laid out in SPDI rules requiring companies to institute managerial, technical, operational and physical security control measures. The rules are also subject to ISO/IEC 27001 international standards on information security management

Sectoral regulators and nodal agencies also prescribe security measures. The Reserve Bank of India prescribes standards for banks, including setting a mechanism for dealing with and reporting incidents, cyber crisis management, and arrangements for continuous surveillance of systems and the protection of customer information. It also mandates banks to follow the ISO/IEC 27001 and ISO/IEC 27002 standards.

A similar framework is applicable to non-banking finance companies. The Securities Exchange Board of India requires stock exchanges, depositories and clearing corporations to follow standards such as ISO/IEC 27001, ISO/IEC 27002 and COBIT 5.

Cyber Incident Reporting

The 2013 rules require organisations to report incidents to the CERT-In within a reasonable time. Incidents include denial of service attacks, phishing and ransomware incidents, website defacements, and targeted scanning of networks or websites.

In April 2022, the CERT-In issued a new directive modifying obligations under the 2013 rules, including requirements to report cybersecurity incidents within six hours, syncing system clocks to the time provided by government servers, maintaining security logs in India, and storing additional customer information. The IT Rules 2021 also require intermediaries to notify the CERT-In of security breaches as part of their due diligence obligations

Cybercrimes

Traditional criminal actions such as theft, fraud, forgery, defamation and mischief – all of which are covered under the Indian Penal Code, 1860 – might be included in cybercrimes. The IT Act addresses modern offences such as tampering, hacking, publishing obscene information, unauthorised access to protected systems, breach of confidentiality and privacy, and publishing false digital signature certificates. Sending threatening messages by email, defamatory messages by email, forgery of electronic records, cyber fraud, email spoofing, web-jacking and email abuse are also punishable offences.

Future Path

The federal government, through the National Cyber Security Co-ordinator, is formulating a new national cybersecurity strategy. This aims to address certain gaps in India's cybersecurity framework and enhance the country's overall cybersecurity posture.

The government is also considering revamping the IT Act to align with advances in the global and domestic digital and technology environment. This may change the existing cybercrime, incident reporting, and security measures and standards framework.

India has been continues making importance of cyber security along with global cyber security practises, poles, guiding & Regulations to protect information & data covering international standard practice, Rules & Regulation

Quality Mantra Aug, 2025
A Newsletter of International Certification Services

Mr. Nivrtee Magar

Securing Digital Footprint_Cyber Forensics

Vice President Forensic

Introduction

In today's hyper-connected world, each of us generates vast amounts of data across multiple platforms—from emails, cloud storage, and social media to IoT devices and mobile apps. This accumulated information forms our digital footprint, a virtual identity that can be as revealing—and vulnerable—as our physical one. The digital footprint includes everything from browsing history and geolocation data to metadata embedded in images and documents. With this exponential increase in digital interactions, our personal and organizational data becomes an attractive target for cyber criminals.

As cyber threats multiply in frequency and complexity, cyber forensics emerges as a crucial discipline. It enables professionals to trace digital attacks, preserve electronic evidence, and support investigations in both corporate and criminal scenarios. Understanding how to secure digital footprints is now essential for everyone, from individuals to large enterprises.

Understanding the Digital Footprint

A digital footprint refers to the data trail users leave behind when they interact with digital services. It is generally categorized into two types:

- Active Digital Footprint: This consists of the data users intentionally share online, such as social media posts, emails, blogs, and uploaded files. It includes every action that is knowingly performed over the internet.
- Passive Digital Footprint: This comprises the data that is collected without the user's direct input or consent. Examples include IP addresses, browser type, cookies, and device metadata. Websites and apps often collect this information silently for analytics and advertising purposes.
-

While active footprints are usually visible and somewhat controllable, passive footprints often go unnoticed. Both types, however, are crucial for forensic investigations as they can provide evidence of a user's intent, behavior, and digital presence over time.

The role specificity of EnMS well integrates with complementary standards of ISO namely 14001 (Environmental Management), ISO 26000 (Social Responsibility), ISO 37001 (Anti-Bribery), ISO 45001 (Occupational Health), and ISO 27001 (Information Security). The integration of ESG with EnMS transforms businesses into internationally recognized, climate resilient and socially responsible, through the alignment of their operational excellence. Cumulatively resulting in cost reduction, efficient energy use, improved ESG ratings, and risk mitigation. Benefiting the Policymakers to achieve standardized energy data access, alignment with climate targets, and harmonized ESG reporting across industries.

The Expanding Cyber Threat Landscape

Digital footprints have become a goldmine for malicious actors. Here are some of the key threats that exploit this data:

- Credential Stuffing: This technique involves using previously stolen username-password combinations to gain unauthorized access to other services.
- Phishing & Social Engineering: By analyzing personal data available online, attackers craft convincing fake messages or profiles to trick victims into revealing sensitive information
- Digital Impersonation: Fraudsters can use photos, names, and public data to create fake identities that can be used for scams, misinformation, or defamation.
- Behavioral Tracking: Companies and hackers alike can track user behavior for profiling, which can be used for both targeted marketing and cyber attacks.

With the increasing integration of IoT and mobile devices in everyday life, the volume and granularity of digital footprints have grown significantly, heightening security and privacy concerns.

Securing the Digital Footprint Proactively

While cyber forensics plays a crucial role in post-incident investigation, it can also be applied proactively to secure digital assets and prevent breaches. The following technologies and strategies are central to this approach:

- Endpoint Detection and Response (EDR): These solutions continuously monitor and respond to threats on end-user devices. They help detect abnormal behaviors such as unauthorized data transfers or malicious application execution.
- Security Information and Event Management (SIEM): SIEM platforms aggregate logs from multiple systems to detect and respond to threats in real time. They are crucial for maintaining forensic readiness
- Multi-Factor Authentication (MFA): Adding an extra layer of identity verification greatly reduces the chances of unauthorized access, even if credentials are compromised.
- Data Loss Prevention (DLP): These tools monitor data transfers and prevent sensitive information from being sent outside an organization's network
- User Behavior Analytics (UBA): UBA tools use machine learning to identify deviations from normal user behavior, signaling potential insider threats or account compromise.

Implementing these tools and policies ensures that digital evidence is readily available in case of a breach and that the attack surface is minimized.

Cyber Forensics in Action: Technical Scenarios

Cyber forensic tools and techniques come into play in various real-world situations. Below are two common technical scenarios that showcase the role of digital forensics:

Scenario 1: Ransomware Attack Investigation

Trigger: A user opens a malicious email attachment that encrypts files across the network.

Response: Forensic experts use tools like FTK (Forensic Toolkit) to image affected disks and analyze metadata. Memory dumps are examined using Volatility to identify malware behavior and persistence mechanisms.

Outcome: The root cause is identified, and compromised systems are isolated and remediated
Scenario 2: Insider Data Theft
Trigger: An employee is suspected of copying sensitive data to a USB drive.
Response: Tools such as USB Devies and Windows Audit Pol are used to extract USB device history and analyze file access logs.
Outcome: Investigators confirm unauthorized file transfers and take disciplinary or legal action.

Legal and Ethical Considerations

The collection and analysis of digital evidence must adhere to stringent legal and ethical standards:

- Chain of Custody: All evidence must be documented from collection to court presentation to ensure its integrity.
- Data Privacy Laws: Compliance with regulations such as GDPR (Europe), CCPA (California), and India's IT Act is critical.
- Jurisdictional Issues: Cross-border data flow can complicate forensic investigations due to conflicting legal requirements.
- Consent and Warrants: Especially in corporate environments, investigators must be careful to operate within the boundaries of consent and authorization.

Failure to adhere to these principles can result in inadmissible evidence, legal liability, or reputational damage.

AI and the Future of Cyber Forensics

Artificial Intelligence is poised to revolutionize cyber forensics in the following ways:

- **Predictive Forensics:** AI algorithms trained on historical data can predict potential threats, allowing pre-emptive action.
- **Automated Triage:** Machine learning can quickly sift through large volumes of logs and files to identify the most relevant evidence.
- **Deepfake Detection:** AI tools are being developed to identify synthetic media, which is increasingly used for disinformation and blackmail.

These advancements are making forensic investigations faster, more accurate, and increasingly scalable.
these advancements are making forensic investigations faster, more accurate, and increasingly scalable.

Challenges Ahead

Despite technological progress, digital forensics faces numerous challenges:

- Encryption: While essential for privacy, encryption also makes evidence recovery difficult.
- Anti-Forensics Techniques: Criminals use tools to wipe data, alter metadata, or mislead investigators.
- Cloud and IoT Complexity: Data is often distributed across multiple servers and devices, making acquisition and preservation complex.
- Tool Reliability and Validation: Forensic tools must be tested for accuracy and consistency to be accepted in court
- Tackling these challenges requires continued investment in research, training, and international collaboration.

Conclusion

As we navigate the digital age, securing our digital footprint is no longer optional. Cyber forensics provides a structured, scientific approach to uncovering and preventing cybercrimes. By incorporating forensic readiness into security strategies, organizations can not only respond to incidents more effectively but also deter them. The future demands a deeper synergy between cybersecurity, digital privacy, legal frameworks, and emerging technologies. It is only through this integrated effort that we can build a resilient digital society.

Ms. Riddhi Ghosalkar

Legal Admissibility of Forensic Evidence in Insurance Litigation

Dy. Manager - Forensic (North Branch)

Forensic evidence has become a cornerstone of contemporary justice systems, providing objective, science-backed insights that assist in uncovering the truth. It has transformed traditional methods of investigation by reducing dependence on eyewitnesses and introducing more reliable, evidence-based tools that can both establish guilt and support claims of innocence.

The formal recognition of forensic testimony in India began with the Indian Evidence Act of 1872, which laid the initial legal foundation for admitting expert opinions in court. Over the years, this framework has undergone considerable refinement through legislative changes and judicial interpretation.

The enactment of three new criminal laws in 2023 i.e. the Bharatiya Sakshya Adhiniyam (BSA), Bharatiya Nyaya Sanhita (BNS), and Bharatiya Nagarik Suraksha Sanhita (BNSS), marks a transformative shift in India's legal landscape. These laws aim to bring greater clarity, structure, and technological alignment to the justice system.

One of their significant outcomes is the formal reinforcement of the role of forensic evidence, which now holds increased relevance not just in criminal trials but also in insurance litigation. In claims involving fire, theft, arson, manipulated accidents, and suspected fraud, forensic findings play a decisive role in claim validation and dispute resolution.

Relevance of Forensic Evidence in Insurance Litigation

In insurance claims, forensic evidence plays a critical role in:

i. Determining the cause of loss (e.g., short-circuit, mechanical failure, deliberate sabotage)
ii. Verifying or contesting the validity of claims
iii. Identifying potential policy violations or fraud
iv. Supporting subrogation or third-party liability claims

Fire origin and cause reports, CCTV footage, damage pattern analysis, mechanical/electrical forensic assessments, and expert opinions are frequently relied upon in such matters.

1) Legal Admissibility Under Bharatiya Sakshya Adhiniyam (BSA), 2023

The Bharatiya Sakshya Adhiniyam replaces the Indian Evidence Act, 1872. It formalizes the evidentiary value of expert opinion, digital evidence, and electronic records, which are all integral to modern forensic investigation.
Key Provisions Relevant to Forensic Evidence:

I. Section 22: Forensic opinions are admissible if they relate to facts in issue or relevant facts.
ii. Section 39: Recognizes expert opinion on matters requiring special knowledge, including fire cause analysis, technical examination of vehicles, electrical short circuits, etc.
iii. Section 61-63: Clearly defines and allows the admissibility of electronic and digital records as evidence, provided they meet conditions of integrity and authenticity.
iv. Section 65: Admits secondary digital evidence (e.g., CCTV clips, drone surveillance, device logs) if produced in accordance with prescribed digital formats and certifications.

In insurance litigation, expert reports, if backed by credentials and scientific methodology, now have a clearer legal footing. Courts are more inclined to treat these reports as primary evidence, rather than merely corroborative or advisory.

2) Procedural Provisions under BNSS, 2023

The Bharatiya Nagarik Suraksha Sanhita, which substitutes the Criminal Procedure Code, 1973, introduces specific mechanisms to strengthen the forensic process:
i. Section 106: Mandates scientific investigation in suitable cases, enabling police to refer matters to forensic experts early in the case.
ii. Section 110: Allows forensic experts to record evidence via electronic means, facilitating remote testimony in insurance litigation.
iii. Section 336: Recognizes the admissibility of electronically stored information, provided it is not tampered and is produced through a verifiable chain of custody.

These provisions ensure that forensic evidence collected in cases of suspicious fire, arson, etc, can be procedurally preserved and used in civil or insurance-related trials.

3) Offenses Under Bharatiya Nyaya Sanhita (BNS), 2023, and Their Forensic Linkages

While BNS is largely a replacement of the Indian Penal Code (IPC), it introduces changes in terminology and structure, which impact forensic applications in criminally investigated insurance cases.

I. Section 316: Mischief by fire or explosive to property, applicable in arson-related insurance claims.

ii. Section 324: Cheating and fraud, central to staged accidents or manipulated claims.
iii. Section 69(4): Destruction or alteration of electronic records, relevant where claimants tamper with logs, footage, or telematics data. Forensic methods such as residue analysis, burn pattern studies, circuit board examination, and digital data recovery are vital in proving or disproving these offenses.

Judicial Precedents and Trends

Several cases have recognized the validity of forensic reports in deciding insurance disputes:

i). Courts have upheld claim denials based on forensic findings in several cases showing deliberate tampering or staged incidents.
ii). In fire insurance disputes, burn pattern analysis and circuit examination is treated as conclusive when corroborated with photographic evidence and timelines.
iii). Expert cross-examination has been allowed even in claims, reinforcing the need for structured, defensible forensic reports.

The overhaul of India's criminal and evidentiary laws in 2023 marks a progressive step toward embracing scientific justice. Forensic evidence is now not just an investigative tool but a legally empowered instrument of truth in insurance-related litigation.

With the Bharatiya Sakshya Adhiniyam recognizing expert testimony and digital records, and the BNSS ensuring procedural rigor in evidence handling, forensic evidence, when properly collected and presented, carries significant weight in Indian Justice System.


Mr. Suraj Matondkar

Case Report: TP Reconstruction

General Manager- Reconstruction

Title

Accident Reconstruction Analysis of Head-On Collision between Maruti Suzuki Ciaz (KA03NB2646) and Tata Tiago (KA64M2627)

- Insured Vehicle - Maruti Suzuki Ciaz (KA03NB2646)
- Third Party vehicle- Tata Tiago (KA64M2627)

Case Description

On 08th September 2024, around 18:30 hrs, a fatal road traffic accident occurred on the Koratagere–Madhugiri road in Tumakuru district, Karnataka. The accident involved a Maruti Suzuki Ciaz (KA03NB2646) traveling from Madhugiri to Koratagere and a Tata Tiago (KA64M2627) traveling in the opposite direction. The Ciaz, while attempting to overtake a truck, collided head-on with the oncoming Tiago.

Multiple occupants from both vehicles sustained fatal injuries, including children. Injuries involved head trauma, fractures, and internal bleeding. The driver of the Ciaz and several passengers died on the spot, while others succumbed later in hospital. The Tiago occupants also suffered fatalities.

ICS Assure Services Pvt. Ltd. was appointed to conduct a scientific analysis of the scene, involved vehicles, and surrounding circumstances to determine contributing factors and to establish the root cause, assess the liability, and provide expert opinion for TP insurance claim assessment.

Methodology / Forensic Approach

1. Evidence Collection & Scenario Review:
   - Review of case details, vehicle numbers, sequence of events, and statements.
2. Spot and Roadway Analysis:
   - Analysis of road elevation, visibility, and signage.
   - Analysis of gradient.
3. Vehicle Damage Inspection:
   - Inspection of damages to both vehicles.
   - Analysis of crush zones, windshield damage, roof dents, dashboard collapse.
4. Driver Behavior and Licensing:
   - Verification of Tiago driver lacked a valid license.
   - Assessment about compliance with Rules of the Road, 1989.
5. Reconstruction Simulation:
   - Mapping of vehicle paths and probable collision sequence.
   - Evaluation of line of sight obstruction due to elevation and ahead truck.

Findings / Observations

a) Vehicle Damage:

I. Maruti Ciaz:

- Severe damage to front bumper, hood, windshield.
- Left rear dent and roof damage up to B-pillar.
- Interior dashboard heavily deformed.

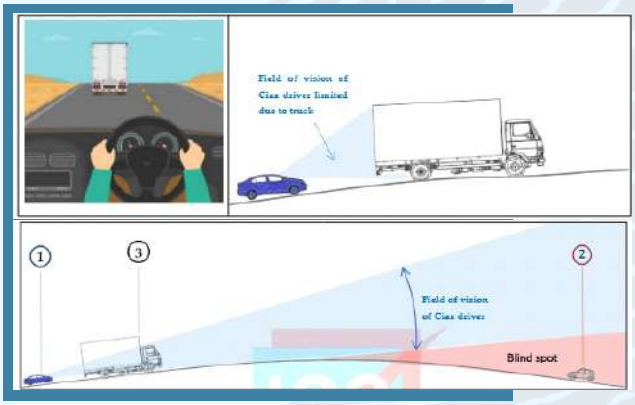
ii. Tata Tiago:

- Frontal damage matching Ciaz's pattern.
- Windshield and mirror destruction.
- Dashboard impact consistent with deceleration trauma.

b) Scene Analysis:

- Single-lane road with an 80 km/h speed limit.
- Road had a crest/elevation at the collision site.
- Ciaz attempted overtaking on uphill slope behind a truck.
- Tiago was traveling down the slope in the middle of the road.

Interpretation & Analysis



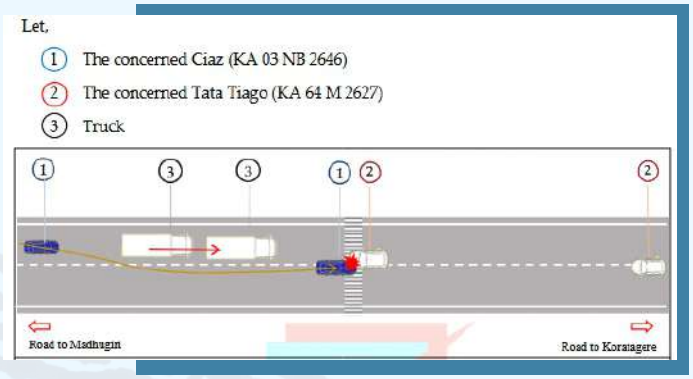
1. Role of Road Elevation&Environmental Factors:

a) Road elevation created a blind crest for Ciaz driver.
b) Obstruction by truck ahead further reduced visibility.
c) Elevated road created blind spots that severely impaired the Maruti Ciaz driver's ability to detect oncoming vehicles.

2.Limited Reaction Time:

a)Tiago emerged into view too late for evasive action.
b)Standard human reaction time (1.5 seconds) was insufficient due to blind spot.

3.Violation of Lane Discipline by Tiago:



a) Tiago was travelling centrally instead of on the left edge.

b) As per Rules of the Road, 1989, driver must stay on left.

c)This deviation reduced clearance for overtaking.

4.Driver Licensing:

a) No license found for Tiago driver.
b) Classified as unskilled driver — increasing liability.

5.Vehicle Alignment and Impact Zone:

a) Graphical correlation confirmed frontal offset head-on impact.
b) Both vehicles suffered matching crush patterns.
c) Final positions supported witness claims and trajectory mapping.

6.Negligence by Tata Tiago Driver:

a) Unlicensed driving indicates lack of formal training.
b) Driving centrally instead of on the left violates traffic norms.
c) Reduced lateral clearance and sudden appearance contributed directly to collision.
d) While the Ciaz attempted to overtake, the field-of-view was obstructed due to the elevated road and truck ahead. The Tiago driver's incorrect positioning and unlicensed status are dominant causative factors.

Opinion:

- The accident was primarily caused due to the Tiago's incorrect road positioning and lack of valid driving credentials.
- Secondary contributory factors include road elevation-induced blind spots and field-of-view restrictions.
- From a TP claim liability standpoint, greater negligence rests with the Tiago driver (TP).

Quality Mantra Aug, 2025
A Newsletter of International Certification Services

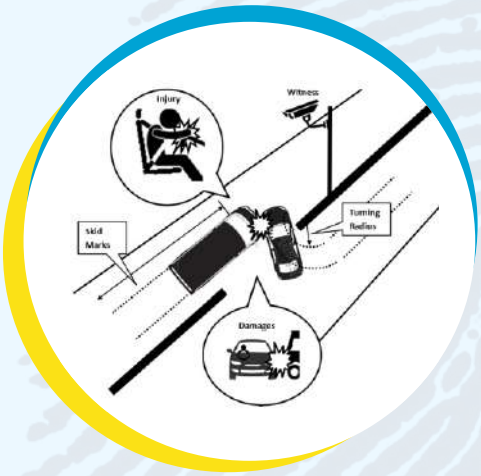
Case Report_ OD Reconstruction

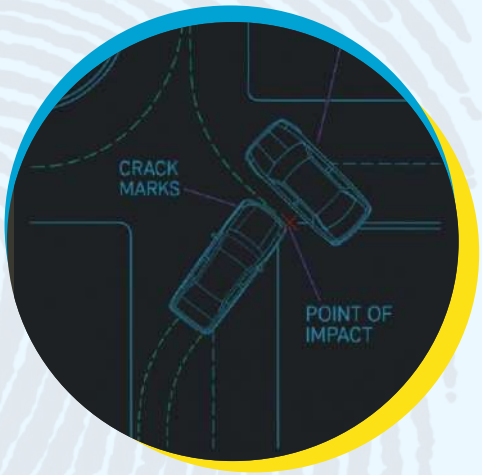
Sr. Engineer Motor Claims

Mr. Dinesh Chavan

Introduction: The Forensic Lens on Accident Reconstruction: Accident reconstruction, a specialized discipline within forensic science, involves the scientific analysis of vehicular collisions to determine how and why an incident occurred. Leveraging principles of physics, engineering, biomechanics, and digital modeling, reconstruction experts assess impact angles, speed calculations, structural deformations, and environmental evidence to uncover the truth behind reported events.

In the context of insurance claims particularly Own Damage (OD) cases this forensic approach is instrumental in verifying the legitimacy of the incident narrative, detecting inconsistencies, and preventing fraudulent claims. By meticulously interpreting damage patterns and scene dynamics, forensic analysts contribute objective, evidence-based insights that support accurate claim adjudication and legal defensibility.



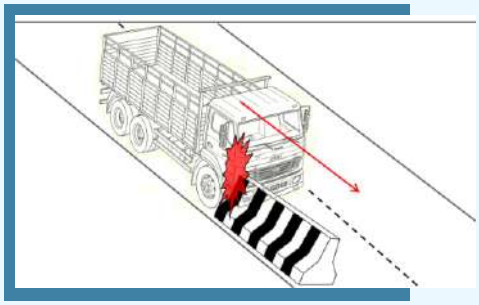


Case Title:

Scientific Reconstruction of a Complex OD Claim Involving Multi-Angle Impact Dynamics

Case Description:

This report focuses on an Own Damage claim involving a mid-sized commercial vehicle allegedly impacted by a roadside milestone. Upon initial inspection, the observed damages lacked coherence with the insured's version of events. The challenge was to validate the reported scenario through a structured forensic investigation and uncover any potential misrepresentation.

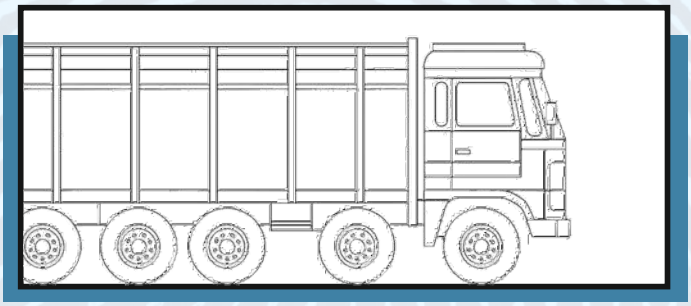


Methodology / Forensic Approach:

1. Spot Technical Assessment: close examination of the accident scene, impact zone, and damage profile.

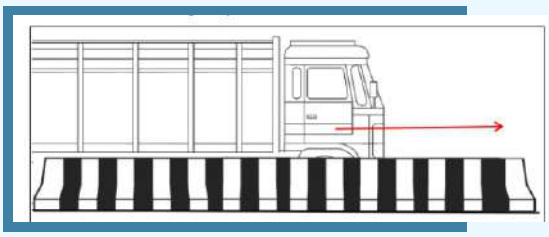
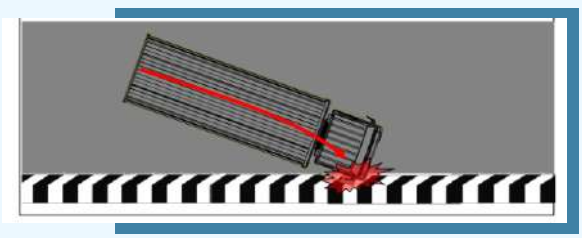


2.Damage Profiling & Correlation: Evaluated consistency between vehicle deformation and object geometry:



4.Vehicle Inspection: Assessed structural members, cabin, headlights, and other components for force distribution:

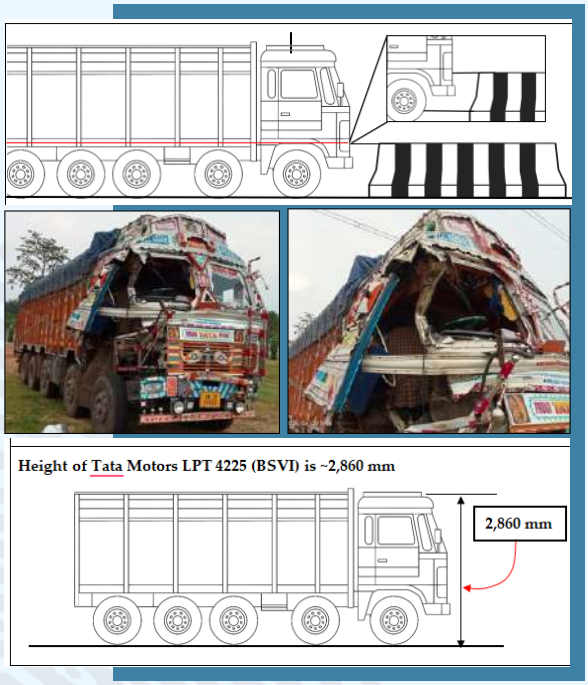

1. Scenario Representation: Simulation to test multiple angles and speeds of collision with the alleged object.

Findings / Observations:

The alleged point of impact (milestone ~100 cm height) did not align with the deformation height on the vehicle body.

Thus the Guard wall is approximately 1000 mm tall, while the overall height of the truck is around 2860 mm. If the truck had collided with the Guard wall , the damage would be expected to be confined to the lower frontal portion of the truck—specifically the front bumper, front Tyres, and headlamp area.



Interpretation & Analysis:

The collective evidence suggested a non-dynamic impact scenario. The damage did not exhibit the typical crumple zones or deformation patterns expected from a frontal impact with a rigid object. The forensic model exposed discrepancies in vehicle trajectory, force application, and claimed narrative raising critical red flags.

Conclusion:

This OD reconstruction case reflects the value of methodical, science-backed forensic investigation in insurance claims. It highlighted the divergence between the claimed incident and actual physical evidence, emphasizing the necessity of multi-layered validation. The ICS Assure forensic team, through a structured OD reconstruction framework, successfully identified inconsistencies and safeguarded against a potentially fraudulent payout.

Up Coming Training Calendar- September - 2025

Training Name	Date	Time	Fees	Mode
LEAD AUDITOR TRAINING ISO 14001:2015	14th to 18th Oct 2025	10.00 am to 5.00pm	20000 + 18% GST	Online
INTERNAL AUDITOR ISO 9001:2015	10th & 11th Oct 2025	10.00 am to 5.00pm	7000 + 18% GST	Online
LEAD AUDITOR TRAINING ISO 9001:2015	27th to 31st Oct 2025	10.00 am to 5.00pm	18000 + 18% GST	Online

Forensic Idioms Quiz

Q1. If an employee is "caught red-handed" in the office, what does it mean?
A) They were using a red pen
B) They were caught doing something wrong at the very moment
C) They were working overtime
D) They were handling confidential files

Q2. In a corporate investigation, "the smoking gun" refers to:
A) A coffee machine in the pantry
B) The strongest and undeniable proof
C) A fake clue planted by someone
D) A weapon kept in the office

Q3. When HR says "it's an open-and-shut case", they mean:
A) The office door was left open
B) The case is complicated and unsolved
C) The situation is simple and clear with an obvious outcome
D) The case will remain a secret

Q4. A "cold case" in workplace terms means:
A) A project kept in the freezer
B) An old issue with no progress or leads
C) A complaint solved instantly
D) A problem with IT systems

Q5. To "crack the case" in corporate life means:
A) To damage company records
B) To solve a challenging problem successfully
C) To accuse someone unfairly
D) To close an unresolved file

Answer:
1.B) They were caught doing something wrong at the very moment, 2.B) The strongest and undeniable proof, 3.C) The situation is simple and clear with an obvious outcome, 4.B) An old issue with no progress or leads, 5.B) To solve a challenging problem successfully

September Month Birthday's- 2025

Sr. No.	Emp. Name	Emp. Code	Station	Emp. Dob
01	Vaibhav Satnambhai Shrivastav	ICS/1032	Surat	02-Sep
02	Mayuresh - Gaikwad	ICSA/6560	ICS-Assure - Reconstruction	04-Sep
03	Girish Parmar	ICS/6498	ICS-GGL-ZONE-2	05-Sep
04	Hirenkumar Chauhan	ICS/6419	ICS-GGL-ZONE-1	05-Sep
05	Ranu Yadav	ICST/2904	ICS-Technology	06-Sep
06	Mahipal Singh	ICS/1182	Jaipur	06-Sep
07	Mayurkumar Gamit	ICS/6499	ICS-GGL-ZONE-2	06-Sep
08	Upendra Chaudhari	ICS/6568	ICS-IGL New Delhi	07-Sep
09	Mohammad Rehan Fazal	ICS/5502	ICS-ONGC-Ankleshwar	07-Sep
10	Vaibhav Tomar	ICS/6687	ICS-IGL New Delhi	08-Sep
11	Vikram Singh	ICS/6639	ICS-IGL New Delhi	08-Sep
12	Ravi Chauhan	ICS/6588	ICS-IGL New Delhi	08-Sep
13	Ritesh Singh	ICS/6360	ICS-ONGC-Mehsana	08-Sep
14	Chandan Kumar	ICS/6001	ICS-ONGC Tripura	09-Sep
15	Ashish singh Panwar	ICS/6653	ICS-IGL New Delhi	09-Sep
16	Ajit Kumar Yadav	ICS/6542	ICS-IGL New Delhi	09-Sep
17	Manish Patel	ICS/4956	ICS-Reliance Ro Project	09-Sep
18	Mubarak Sandole	AAA/4475	Ausadha	09-Sep
19	Parth Mashru	ICS/5683	ICS-ONGC-Mehsana	09-Sep
20	Eknath Bhanage	ICS/5899	ICS-MNGL-Pune	10-Sep
21	Lokesh Bundel	ICS/6647	ICS-IGL Rajasthan	10-Sep
22	VinodKumar Yadav	ICST/5648	ICS-Technology	10-Sep
23	Swaroop Devassy	ICS/5585	ICS-ONGC-Offshore	10-Sep
24	Pranesh Pandurang Rewale	ICS/1382	Mumbai-TPA	10-Sep
25	Miralkumar Patel	ICS/6475	ICS-GGL-ZONE-2	11-Sep
26	Rohit Dhamankar	ICS/6450	ICS-MGL Steel	12-Sep
27	Amit Kumar	ECD/5886	ECD-GAIL-HVJ-SURVEY PART B	12-Sep
28	Jitendra Kumar Patel	ICS/3788	ICS-ONGC-Mehsana	13-Sep
29	Nikhilkumar Vasava	ICS/5544	ICS-ONGC-Ankleshwar	14-Sep
30	MD ENAYATULLAH .	ICS/6363	ICS-ONGC-WADU	14-Sep
31	Pushpendra Kumar	ICS/6439	New Delhi	15-Sep

September Month Birthday's- 2025

Sr. No.	Emp. Name	Emp. Code	Station	Emp.
32	Abhilash .	ECD/6536	ECD-GAIL-HVJ-SURVEY	15-Sep
33	Atharwa Gotad	ICS/6698	Mumbai-Admin	16-Sep
34	Arfat Pathan	SUR/5777	Training centre	17-Sep
35	Abhishek Kumar	ICS/6537	ICS-IGL New Delhi	17-Sep
36	Sandeep - Pandey	ICS/5362	ICS-ONGC-WADU	19-Sep
37	Yashkumar Prajapati	ICS/5931	ICS-ONGC-Mehsana	19-Sep
38	Kameshwar Singh	ICS/2282	Udaipur	19-Sep
39	Jayesh Kumar Prajapati	ICS/4092	ICS-ONGC-Mehsana	19-Sep
40	Bhupendra kumar Kantilal Panchal	ICS/833	Ahmedabad	19-Sep
41	Akash Patel	ICS/6491	ICS-GGL-ZONE-2	20-Sep
42	Chiragkumar Patel	ICS/6425	ICS-GGL-ZONE-1	20-Sep
43	Sunil	ICS/4935	New Delhi	20-Sep
44	ShaniKumar Patel	ICS/5666	ICS-ONGC-WADU	21-Sep
45	Sandesh Mahadik	ICS/6381	Mumbai-TenderCell	22-Sep
46	Naushad Ansari	ICS/5344	ICS-VENDOR	21-Sep
47	Nitin Kumar	ECD/4717	ECD-IOCL	21-Sep
48	Kashish Gupta	ICS/6526	Mumbai-IT	22-Sep
49	Maharshi Barot	ICS/6361	ICS-ONGC-WADU	22-Sep
50	Mohammed Azhar Shah	ICST/1702	Mumbai-ECD	25-Sep
51	Rambhan Vishwakarama	ICS/6382	ICS-Lakshya Powertech	25-Sep
52	Poornima Upadhyay	ICSA/6365	ICS-Assure-Delhi	25-Sep
53	Pradeep Pandurang Palkar	ICS/140	Mumbai-Finance	27-Sep
54	Kandarpkumar Patel	ICS/5818	ICS-ONGC-WADU	27-Sep
55	MD Tanweer Alam .	ICS/6344	ICS-MGL Steel	27-Sep
56	Sachin Patkar	ICS/5192	ICS-ONGC-Offshore	27-Sep
57	Sandeep More	ICS/1374	Indore	27-Sep
58	Sivakumar T	ICS/6276	ICS-ONGC-Cauvery Asset	28-Sep
59	Roshankumar Patel	ICS/5737	ICS-ONGC-Ankleshwar	29-Sep
60	Abhijit Mahak Singh	ICS/2111	Navi Mumbai	30-Sep
61	Md Afjal Ansari .	ICS/6404	ICS-VENDOR	30-Sep
62	Sohel Ansari	ICSA/6388	ICS-Assure - Reconstruction	30-Sep
63	Nitin Kumar .	ICS/6461	ICS-ONGC-Bokaro	30-Sep

Horoscope Month of September - 2025

Aries

This month is about harnessing the power of collaboration and using your social connections to achieve your goals. Don't shy away from expressing your bold ideas, but be flexible and adaptable to integrate other's contributions. Opportunities for joint ventures, investments, or even lucrative freelance work can arise through unexpected connections. Focus on quality time with your loved ones, plan exciting outings, and engage in activities that strengthen your bond.

Taurus

This is a potent month to set ambitious goals, take the initiative, and showcase your talents. Expect recognition and potential leadership opportunities. Money matters might feel like a roller coaster. Unexpected expenses could crop up but don't fret. Family ties strengthen as you prioritise quality time. Support loved ones, but don't neglect your own needs. While your overall health appears fine, fatigue and stress might creep in. Prioritise sleep and healthy eating.

Gemini

It's a month for introspection, reevaluation, and potentially shedding old skin to emerge stronger. You might uncover hidden talents or be drawn to challenging, high-stakes projects. Don't shy away from delving into the complex or pursuing unconventional paths. Financial matters might require scrutiny and wise investments. Be cautious of risky ventures and sudden spending urges. This is also an excellent time to explore alternative healing modalities or address lingering emotional issues.

Cancer

It's a month for introspection, reevaluation, and potentially shedding old skin to emerge stronger. You might uncover hidden talents or be drawn to challenging, high-stakes projects. Don't shy away from delving into the complex or pursuing unconventional paths. Financial matters might require scrutiny and wise investments. Be cautious of risky ventures and sudden spending urges. This is also an excellent time to explore alternative healing modalities or address lingering emotional issues.

Leo

Buckle up for a dynamic month filled with collaboration, opportunities, and personal growth. Polish your social skills and leverage your connections. Be open to unexpected opportunities that could lead to financial gains. Remember, teamwork makes the dream work. Don't be afraid to express your affections boldly. Family ties strengthen as you prioritise quality time. But be mindful of potential power struggles within the family dynamics, and approach situations sympathetically..

Virgo

This month encourages you to be diligent and meticulous. You'll shine in roles demanding precision and organisation. Take initiative, offer solutions, and showcase your expertise. Negotiate raises confidently, explore freelance options, or invest in skill development. Romance might take a backseat to shared responsibilities or acts of kindness. However, don't neglect affection – a thoughtful gesture or a helping hand can speak volumes. Consider preventative health measures like checkups.

Horoscope Month of September - 2025

Libra

Family ties deepen this month. Expect heart-warming gatherings and meaningful conversations. Offer support to loved ones in need, and don't shy away from expressing your emotions. At work, your communication skills will be razor-sharp, making presentations and negotiations flow effortlessly. Financial gains are possible, but be mindful of overindulging in your newfound pleasure-seeking tendencies. Attend social gatherings and indulge in flirtatious banter, but don't confuse fleeting flings with genuine connections.

Scorpio

While career pursuits may take a backseat this month, focusing on your inner world can profoundly impact your overall well-being and future direction. At work, maintain professionalism and focus on completing ongoing tasks diligently. Relationships with parents, siblings, or housemates could require your attention. If single, you might encounter someone special through family gatherings or social events within your close circle. Prioritise saving and creating a secure financial foundation.

Sagittarius

Your mind will buzz with ideas this month, and you'll have a strong urge to express yourself and connect with others. This is a great time to learn new skills and embark on new projects. This is an excellent time to market yourself or your business, as your communication skills are sharp. However, be mindful of not over promising or appearing scattered. However, with so much mental energy, finding healthy outlets and avoiding burnout is important. Singles might find romance through online connections..

Capricorn

This is an auspicious month for career growth. A promotion, raise, or recognition for your hard work could be on the horizon. Don't shy away from expressing your ideas and taking initiative. Network strategically, and be bold in pursuing your goals. Singles, your focus might be on building your career and finances first, leaving romance on the back burner. Those committed should express appreciation to their partner and spend quality time together.

Aquarius

The planets are aligning for professional growth this month. You'll exude confidence and decisiveness, attracting recognition and opportunities. You might receive unexpected gains or secure lucrative deals. However, avoid impulsive spending and prioritise long-term investments over fleeting luxuries. Be open to unexpected connections, but don't rush into anything serious. Offer support, be present for your loved ones, and respect their individuality.

Pisces

This is a month for emotional healing and strengthening family bonds. Forgive past hurts and nurture your loved ones with compassion and understanding. Singles might encounter someone special through spiritual connections. You might succeed in research, writing, or any field requiring solitude and focus. Trust your intuition when making career decisions; don't be afraid to explore unconventional paths.

ICS Festival Greetings

SURYAANSH

Training & Convention Center (Residential), Palghar, Maharashtra.

About Us

Nestled near Mumbai, in the serene surroundings of Palghar, Suryaansh Training & Convention Center stands as an epitome of luxury and tranquility, offering an unparalleled experience that caters to your every need, whether you're seeking a serene getaway or planning a grand event.

At Suryaansh, we believe that every journey deserves a touch of luxury, every stay should be unforgettable, and every traveller deserves seamless experiences. We are your premier destination for hotel bookings, committed to transforming your travel dreams into reality. Established with a passion for hospitality and a commitment to excellence, Suryaansh is a leading name in the travel industry, with a team of dedicated professionals deeply passionate about curating exceptional travel experiences.







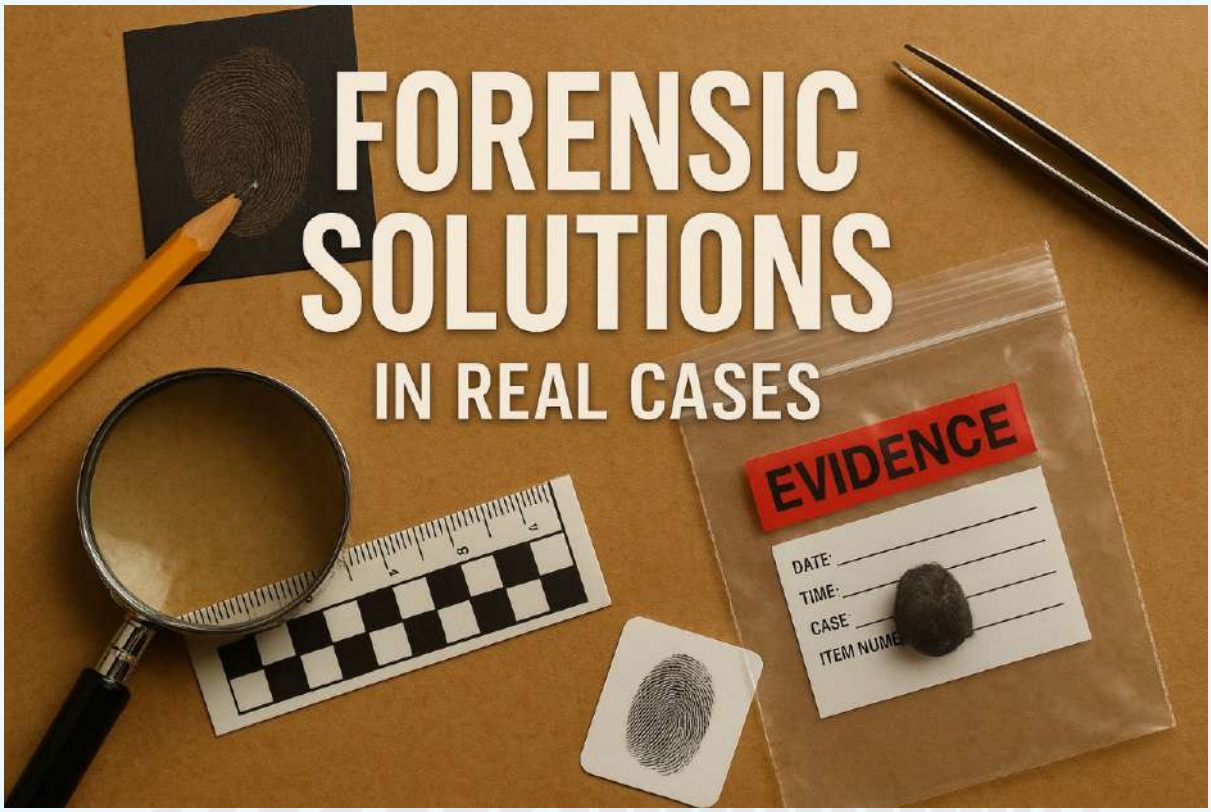

Vision:

"Our vision at Suryaansh is to be Your Gateway to Memorable Stays", where every journey is imbued with luxury, every stay is etched into memory, and every traveller experience seamless excellence. As your premier destination for hotel bookings, we are committed to transforming your travel dreams into reality. At Suryaansh Training & Convention Centre, we extend this vision to become the ultimate destination for events, training programs, and leisure getaways, setting new standards of excellence in hospitality and service."

Mission:

"Our mission at Suryaansh is simple yet ambitious: to redefine the way people travel by providing unforgettable experiences through world-class facilities, impeccable service, and a commitment to excellence in everything we do. We are dedicated to leveraging cutting-edge technology and innovative solutions to streamline the booking process, enhance convenience, and elevate the overall travel experience for our guests. With a relentless focus on customer satisfaction and continuous improvement, we strive to set new standards of excellence in the travel industry."

www.suryaansh.org



Please send us your valuable comments & suggestions on suggestions@icsasian.com. To subscrite for a free Subscription send us a mail with subject “Subscribe for QUALITYMANTRA"at suggestions@icsasian.com

Be a part of the Publication, Share your Ideas, thoughts, Vision and Knowledge, Join us in our mission of a Quality World. Please send your article in 300-500 words with your name and photograph to quality.mantra@icsasian.com.

This Edition Compiled and Presented by ICS Corporate Office Team

International Certification Services Pvt. Ltd.
Corporate Office

22/23 Goodwill Premises, Swastik Estate, 178 CST Road, Kalina, Santacruz (E),
Mumbai- 400 098. Maharashtra, INDIA.
Tel: 022-42200900, **Email:** info@icspl.org / **Web:** www.icspl.org

BRANCH OFFICE
*Ahmedabad*Bangalore *Belgaum*Chennai *Gandhidham *Hyderabad *Indore *Jaipur
*Ludhiana *Mumbai *Nasik *New Delhi *Pune *Udaipur *Vadodara *Vapi

OVERSEAS OFFICE
*Dubai(UAE) *Nepal* Oman* Qatar* SriLanka* Uganda* USA*

Web : www.icsasian.com / www.icspl.org

ICS Group Companies

ECD Think Corrosion, Think ECD · AUSADHA · ICS ASSURE · ICS TECHNOLOGIES Enriching People, Enriching Technology · Saanidhaanam ....DIScoverABILITY A Reason To Live · intech Information Technology Simplified · SURYA ISH · Ausadh Pharma Pvt. Ltd.