India's 1st Digital Forensics Journal

# DIGITAL 4n6 JOURNAL

Digital 4n6 Journal

Issue 01 | Aug 2016

LAUNCH ISSUE

Follow us: @D4N6J www.digital4n6journal.com ₹ 250

## FOREWORD

It gives me immense pleasure to be part of India's first Digital Forensics Journal. Computer Forensics is vital to investigation of cyber incident to establish the modus-operandi, origin, motive and identity of perpetrator. Cyber Forensic investigation is the key to unfold the mysteries of cyber crime, cyber attacks, cyber terrorism, cyber espionage, financial frauds, drug trafficking and many more Brute realities of Cyber World, which is detrimental to stablity, economy, Intellectual property and secrets of any Nation State.

Digital Forensics has become a integral part of any legal process. A valuable data that has been lost or deleted by offender can be retrieved, preserved and produced as electronic evidence admissible in court of law.

I congratulate team of Digital 4n6 Journal for their relentless dedicated work to open new vistas for cyber security professionals, law enforcement agencies, defence forces and all those who are fighting the invisible offenders of Cyber Space.

Arun Sahni

**Lt Gen Arun Sahni, PVSM, UYSM, SM &VSM**
**(Former GOC in C, Indian Army)**

**Strategic Analyst & Sr Advisor**

# MESSAGE

Welcome to the Digital 4n6 Journal!
It is a privilege and an honor to be a part of this journal which will act as a medium for exchange of concepts and opinions related to the field of Digital Forensic Investigation. This journal covers topics ranging from the digital forensics, research activities, events undergone, future prospects and opportunities available to explore in this field.

Digital 4n6 Journal is a congregation of experts and enthusiasts who have come together to live a dream and contribute towards Digital India initiative by enhancement of awareness and skills in this niche field. Through this journal the knowledge will be shared between the law enforcement agencies, Govt. establishments,industry,students, academia and experts This journal will also provide a platform for addressing challenges faced by the investigators during in digital forensic investigation.

Your contribution here reflects your genuine interest and commitment to enhancing our newly launched journal. By construing to leading experts in this field, you will be equipped with knowledge that I hope it will be a key aspect for capability building at your end.

On behalf of the team, I thank you for your participation in this journal and wish you a never ending learned journey!

Regards,

Mr. R V Suthar

Patron

# INDEX

1. USN JOURNAL: Everything About This Forensic Artifact. . . . . . . . . . . .7
*By Prince Boonlia*

2. Automating Linux Malware Analysis Using Limon Sandbox . . . . . . . . . . 15
*By Monnappa K A*

3. The Capability and Capacity Conundrum in the National Cyber Security Universe. . . . . . . . . . . . . . . . . . . . . . . . . . . .24
*By Dinesh Bareja*

4. Digital Forensics: From The Forensic Lab To The Crime Scene. . . . . . 29
*By Binoj Koshy, Nilay Mistry and Khyati Jain*

5. Honeypot Aided Cyber Crime and Network Forensics Investigation. .34
*By Deep Shankar Yadav*

6. SSD and e-MMC Forensics. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 40
*By Yuri Gubanov, and Oleg Afonin*

7. 21st Century Cyber Forensics. . . . . . . . . . . . . . . .. . . . . . . . . . . . . . . . . . .46
*By Deepak Kumar*

8. Hike Messenger: Make It More Secure. . . . . . . . . . . . . . . . .. . . . . . . . . . .49
*By Harshal Patel*

9. Admissibility Of Electronic Evidence In India. . . . . . . . . . . . . . . . . . . . . . .52
*By Yogesh Pandit*

10.Young Start-up in India : An Interview. . . . . . . . . . . . . . . . . . .. . . . . . . . . .59
*( Mr Rutvij Vora, CTIO, Career Khojj )*

11.Here's Why You Should Never Sell Your *Used* Pen Drive. . . . . . . . . . . . .
*By Ashutosh Barot, Aishvarya Dave and Karan Maniar*

# 21st CENTURY CYBER FORENSICS

*Deepak Kumar*
*Deepakniit14@gmail.com*

## Introduction

The past sixty years have witnessed the most rapid transformation of human activity in history, with digital electronic technology as the driving force. Nothing has been left untouched. The way people communicate, live, work, travel, and consume products and services have all changed forever. The digital revolution has spurred the rapid expansion of economic activity across the face of the planet.

**Digital Forensics** aka digital forensic science, cyber forensic, computer forensic;  is the youngest branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. It's an art or science where procedures focus on **IPAD** (*Identification, Preservation, Analysis, and Documentation*) in such a manner that is legally acceptable by court of law and judiciary.

From conventional crimes to Cyber-Crime, computer digital evidence plays indispensable role in nefarious activities either as a target, medium or containing evidence and thus, requiring specialist to gather evidence. It's like an old saying quote ***"Once the documents have been posted online (intentionally or accidently), The genie is out of the bottle"***. And then the real proceeding initiates whether on who is going to deal with the case. Most of the people have misconception about digital forensics, they think it's all about data recovery and actually that is just a single part of it. Digital forensics deals with many emerging treats such as Scarewares, Ransomwares , Digital Divorces, Internet of Things (IoT) Devices, Digital crypto currency, Deep Web ToR, Intellectual Property Theft and many more.

## Some Cases

Cybercrime has caught the eye of the world due to a glut of high-profile, well-publicized cases of compromised computer systems at organizations like Sony, Target, Home Depot, J.P. Morgan Chase, Bangladesh Cyber Heist, Twitter, LinkedIn case. Some Bollywood and Political cases like Vyapam scam, Aarushi Talwar's murder, Sunanda Pushkar Tharoor, Jiah khan, IPL Match Fixing case, etc.

## LECHNO (Legal + Techno) Dimension

Growing volumes of digital storage and the changes in technologies are making the traditional methods for examining electronic evidence unsustainable. In recent years, we have seen law enforcement and corporate investigators taking a different approach, which achieves the same or better results as traditional methods, but much faster. Even the individual must be aware about various computer forensic and Incident Response Procedures guidelines i.e. International Organization of Computer Evidence (IOCE), Scientific Working Group on Digital Evidence (SWGDE), Association Chief Police Officer (ACPO). When handling electronic evidence, most investigators apply a traditional methodology. For each device, a forensic technician would typically:

- *Plug the device into a write blocker*
- *Acquire a forensic image of the entire device*
- *Make a copy of the forensic evidence image*
- *Analyze the data stored on the forensic image copy*
- *Write a report on the results of this analysis.*

The technician would then repeat this process for each device related to this case. Having completed this process for all devices, investigators would then use his knowledge to correlate between the artifacts. And most important thing about integrity; the hash value plays a significant role in establishing the authenticity and integrity of data/evidence in the digital world particularly in Cryptography, Data Analyses and Forensic Imaging etc. Hash Value popularly known as

Fingerprint of data or called Digital Fingerprint and is a one way function

**Forensic Challenges**

The digital forensic investigators are more concerned about cloud forensics and encryption. The other challenges are legal, device proliferation, cross-border cooperation, lack of training and intelligence, new application artifacts, Tor Proxy. One of the major challenges for the Government of India in fighting cyber-crime is the lack of analytical and technical training for the law enforcement agencies. India, however, still faces daunting challenges with cyber-crimes as law enforcement agencies that are not well-equipped. There is lack of policies at the national level as regards to the training of the state police, judges and lawyers on ICT related laws and procedures and essential ways of tackling cyber-crime activities.

The main challenge is the lack of awareness when it comes to reporting cyber-crimes in India. This is partly due to lack of policies on staff rotation within certain law enforcement agencies. There is urgent need for capacity building in the field of cyber forensics as well as cyber security and the government need to put in place proper forensic investigatory infrastructure with legal frameworks and jurisdictions to tackle cyber--crimes.

**Skills for Forensicators**

The competitive corporate market has to secure their IT assets from sabotage, inherent systems vulnerabilities and prevent intruders from gaining unauthorized access to their business critical data. Organizations need services of computer forensics professionals who can analyze their computer and network systems in case of any break-in to determine how the attacker gained access. This gradual increase in cyber-crime has led to a massive surge in the demand. The main skills every Cyber-Forensic Professionals must possess are:

- Knowledge of Computer Networking Concepts
- Working knowledge of Web Servers, Application and Hacking Technologies
- Sound knowledge of the relevant law, Compliance and Standards
- Well versed with investigating Deep web, Bitcoin and other crypto-currencies
- Strong understanding of incident prevention and incident response
- Thorough understanding of Browser and Social Media Forensics
- Cloud Computing, File System and its architecture
- Smartphone and Anti-Forensic tools concepts
- Reverse Engineering and Malware Analysis
- Working knowledge Cryptography and Steganography
- Cyber Intelligence and Analysis
- Updated knowledge of the latest IT Security and Forensic technologies

**Conclusion**

Digital Forensics is majorly focused on standards and tools with Proper Chain of Custody. It’s not at all like what you see on "CSI: Crime Scene Investigation or CID". Computer forensics can be tiresome, dreary, boring, and downright drudgery. One way of creating awareness on digital forensics is by utilizing popular mediums such as social networking sites. In present scenario, the criminals are becoming tech savy while committing crimes. Therefore, forensics needs such a crime analysis technique to catch criminals and to remain ahead in the eternal race between the criminals and the law enforcement. The agencies should use the latest state of art technologies to give themselves the much-needed edge. Availability of relevant and timely information is of utmost necessity in conducting of daily business and activities particularly in crime investigation and detection.