



# **DIGITAL FORENSICS**

**&**

# **LEGAL FRAMEWORK**

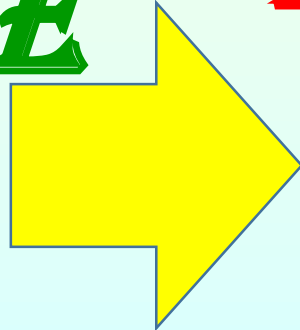
**ARVIND KUMAR CHAURASIA**  
**JOINT COMMISSIONER, I.R.S.**  
**DEPUTY DIRECTOR, WCCB, HQ.**  
**REGIONAL DEPUTY**  
**DIRECTOR/ASSISTANT MANAGEMENT**  
**AUTHORITY (CITES), WCCB**  
**(NORTHERN REGION),**  
**NEW DELHI**







**WILDLIFE  
CRIME**



**DIGITAL FORENSICS**

**&**

**LEGAL FRAMEWORK**



**ARVIND KUMAR CHAURASIA  
JOINT COMMISSIONER, I.R.S.  
DEPUTY DIRECTOR, WCCB, HQ. &  
REGIONAL DEPUTY DIRECTOR, WCCB  
(NORTHERN REGION), NEW DELHI**





# Have People Lost Faith in Wildlife Law Enforcement?

PANGOLIN FESTIVAL

## Villagers deify pangolin to protect the animal

In a region where hunting and poaching of pangolins are rampant, villagers pledge to protect them by giving equal reverence to the animal as their village deity

Varsha Torgalkar • Mar 01, 2021 • Ratnagiri, Maharashtra



Residents of Dugave village worship a replica of the pangolin, along with village deity Goddess Waghjai, as a way of pledging their protection (Photo by Bhau Katdare)

# OUTLINE OF PRESENTATION

- **Let's Discuss a Hypothetical Transnational Wildlife Trafficking Scenario**
- **Why digital forensics?**
- **What is digital forensics?**
- **Schematic presentation of various steps of digital forensics**
- **Investigative process for digital forensics**
- **Various methods of data extraction**
- **Data integrity**
- **Various types of Forms**
- **Forensic hardware & software**
- **Archival of digital evidence**
- **Legal provisions under various Acts**
- **Case Laws**



# Let's Discuss a Hypothetical Transnational Wildlife Trafficking Scenario





# WHY DIGITAL FORENSICS?

## Malawi Achieves 91 Percent Conviction of Wildlife Crimes - Beefs Up 'Docrated' Fight Against Vice



Pixabay

16 APRIL 2021

**Nyasa Times**  
Malawi breaking online news source

By Wanangwa Mtawali

Malawi achieved 91% conviction rate of 251 wildlife crime cases, says an overview of wildlife prosecutions prepared by the Department of National Parks and Wildlife (DNPW).

24-06-2021

**Vs.**

THE HINDU

MENU  
HOME NEWS OPINION BUSINESS SPORT ENTERTAINMENT **Free Games** CROSSWORD+ SCIENCE

CITIES ▾ BENGALURU CHENNAI **COIMBATORE** DELHI HYDERABAD KOCHI KOLKATA MUMBAI KOZHIKODE MADURAI

NEWS > CITIES > COIMBATORE

COIMBATORE

### 'Rate of conviction in wildlife crimes is 2%'

STAFF REPORTER

SALEM, OCTOBER 03, 2019 23:16 IST  
UPDATED: OCTOBER 03, 2019 23:16 IST

SHARE ARTICLE | | A | A | A

**Coordination between public and dept. must: Wildlife Inspector**

The rate of conviction in wildlife crimes is as low as 2%, A.Madhivannan, Wildlife Inspector, Wildlife Crime Control Bureau (WCCB), said here on Thursday.

An awareness session on wildlife crimes as part of World Wildlife Week was held on Thursday and 100 participants including school, college students, Forest Guards and other Forest Department officials took part.

Mr. Madhivannan said, "though there are stringent laws against wildlife crimes, the rate of conviction is between 2% and 3%. Many are not aware about such laws. This affects our conservation efforts. There needs to be coordination between the public and the Forest Department to improve the conviction rate and reduce wildlife crimes."

He added that the WCCB was formed following jurisdictional issues in investigating such crimes.



# WHY DIGITAL FORENSICS?

Member secretary of Assam State Legal Service Authority (ASLSA), Nayan Shankar Barua coordinated the interactive session..... He pointed out that ignorance on the law in vogue and negligence in handling wildlife crime cases were mostly responsible for wildlife crime cases lost in the legal battle, the statement said.

## Assam: Concern over low conviction rate in wildlife crime cases at interactive session in Manas National Park

 by NE NOW NEWS GUWAHATI , February 21, 2021 9:07 pm



Dr. Bibhab K Talukdar interacting with the participants.

 Share on Facebook

 Share on Twitter



Low conviction rate in respect of wildlife crime cases has remained a cause for concern as it was reflected during an interactive session on wildlife issues in [Manas National Park](#).

# WHY DIGITAL FORENSICS?

## THE ECONOMIC TIMES | News

English Edition ▼ | 29 January, 2021, 10:49 PM IST | E-Paper

### Damaged mobile phone helped NIA nail JeM conspiracy behind the 2019 Pulwama attack

#### Synopsis

The mobile phone belonged to a Pakistani militant, Mohammed Umar Farooq (24), killed a month after the attack, according to the NIA. On Tuesday, the agency filed a 13,800-page charge-sheet against 19 accused persons including JeM chief Maulana Masood Azhar, his brother Rouf Asgar and cousin Ammar Alvi, all Pakistani nationals.



NEW DELHI: Video clips, WhatsApp chats and photographs retrieved from a damaged mobile phone helped the National Investigation Agency (NIA) nail the conspiracy behind the 2019 Pulwama suicide attack. The mobile phone belonged to a Pakistani militant, Mohammed Umar Farooq (24), killed a month after the attack, according to the NIA.

On Tuesday, the agency filed a 13,800-page charge-sheet against 19 accused persons including Jaish-e-Mohammad (JeM) chief **Maulana Masood Azhar**, his



# WHY DIGITAL FORENSICS?

## Drug dealer jailed after sharing a photo of cheese that included his fingerprints

By Rob Picheta, CNN

Updated 1310 GMT (2110 HKT) May 25, 2021



The block of mature blue cheese that proved Carl Stewart's undoing.

**(CNN)** — A drug dealer whose fingerprints were analyzed by police when he shared a photo of his hand holding a block of cheese has been sentenced to 13 years and six months in prison.

Carl Stewart, 39, from Liverpool, northwestern England, sent a picture on an encrypted device of a block of Stilton he had found in upmarket British grocery store Marks & Spencer, Merseyside Police said in a press release.

But the photograph was discovered by police, who used it to analyze his fingerprints and identify Stewart.

# WHY DIGITAL FORENSICS?

Printed from

**THE TIMES OF INDIA**

## Tuticorin police seize four tusks, arrest two

Nov 3, 2020, 09.00 PM IST



TUTICORIN: A special team of the Tuticorin police involved in a hunt for ganja peddlers seized four tusks from a duo on Tuesday.

The accused have been identified as G Rajavel, 33, of George Road and M Muniyasami, 43, of Ganesan Colony, Tuticorin.

Superintendent of police S Jayakumar said a special team on the lookout for ganja peddlers stumbled upon the duo. “While going through the WhatsApp chats of one of them, the team saw the pictures of tusks. On further probe, we identified the sellers. Later, we caught the duo, posing as prospective buyers,” the SP said, adding that the accused tried to flee when they realised that it was a trap.

However, they were held by a team from Tuticorin south police station comprising sub-inspector Shankar, head constable Saravana Ramesh and constable Pradeep.

The police seized four tusks measuring, 25cm, 26 cm, 31cm and 34cm-in length. Their two motorcycles were also seized. The accused and the seizure items were handed over to the forest department.

A case was registered against the duo under sections the Wildlife Protection Act, 1972.



# WHY DIGITAL FORENSICS?

Stop the Illegal Wildlife Trade

## Stop the Illegal Wildlife Trade: How smugglers are being caught by their own mobile phone data

Technology that can find links in complex criminal webs has become the latest tool in the fight against poachers, writes **Namita Singh**



Wednesday 10 February 2021 11:56 | 2 comments



Customs officials display elephant tusks seized in Thailand (Getty)

# WHY DIGITAL FORENSICS?

## Using digital forensics to Apprehend wildlife criminals

24 August 2020 12:02 am 0 - 987

Google Bookmark

Facebook

+ More

A A A





# WHY DIGITAL FORENSICS?

## **Kerala forest department moots high-end cyber forensic lab to combat wildlife crimes**

*Though there is a rise in wildlife crimes cases nationally, there is no major increase in wildlife crimes in Kerala.*



Published: 24th February 2020 02:37 AM | Last Updated: 24th February 2020 02:37 AM

🔒 | A+ A A-



Image used for representational purpose only.

# Data Never Sleeps

**2020** This Is What Happens In An Internet Minute



Created By:  
@LoriLewis  
@OfficiallyChadd



# What is Digital Forensics?





Digital forensics is a branch of forensic science that includes the identification, recovery, investigation, validation, and presentation of facts regarding digital evidence found on computers or similar digital storage media devices.



# Digital Forensics



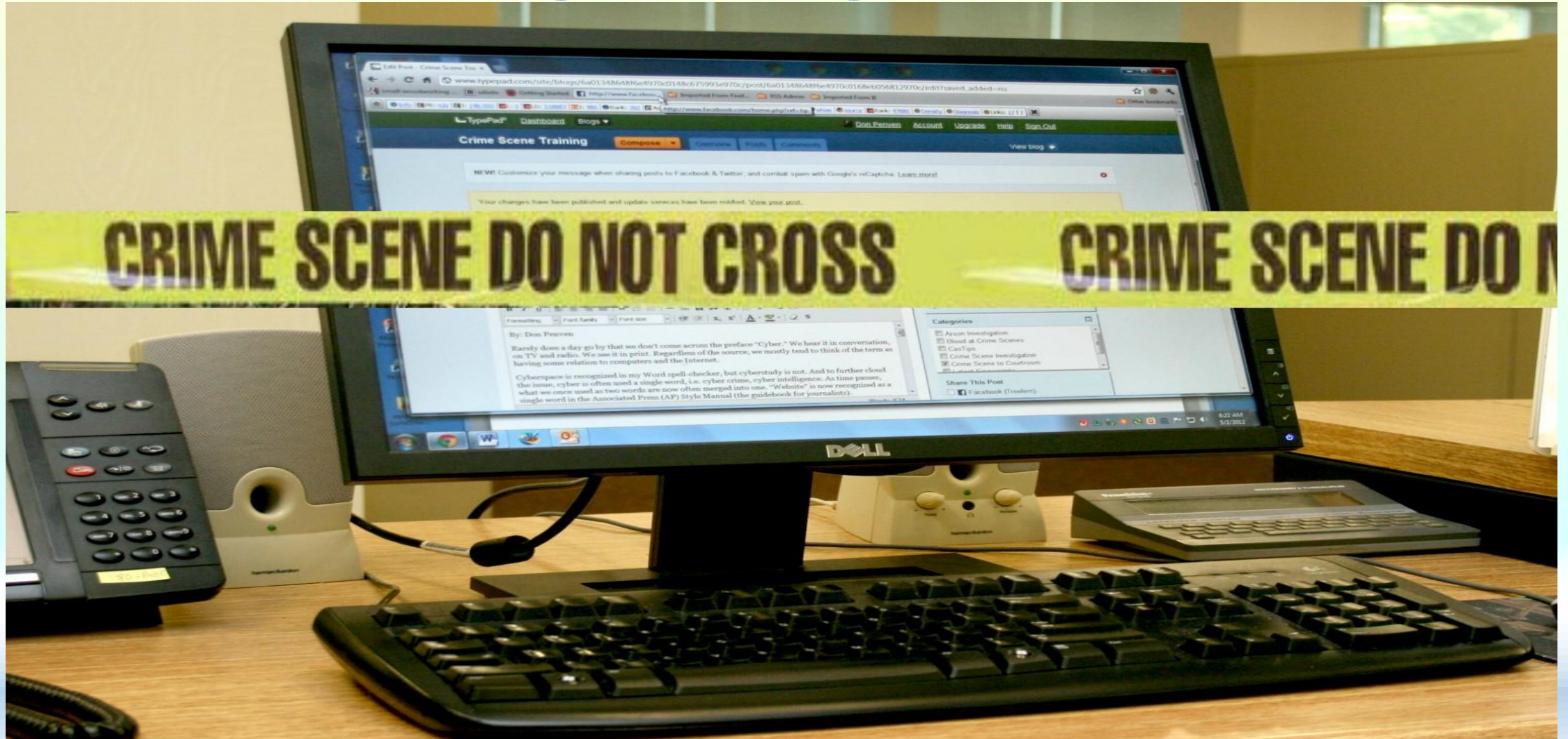
# Investigative Process For Digital Forensics Science

## DIGITAL FORENSIC PROCESS





# Securing the Digital Devices



# Faraday Bag



Faraday bags are a type of Faraday cage made of flexible metallic fabric. They are typically used to block remote wiping or alteration of wireless devices recovered in criminal investigations by blocking electromagnetic fields.



# Air Bubble Bags

Protect seized data storage devices/mobiles from physical damage



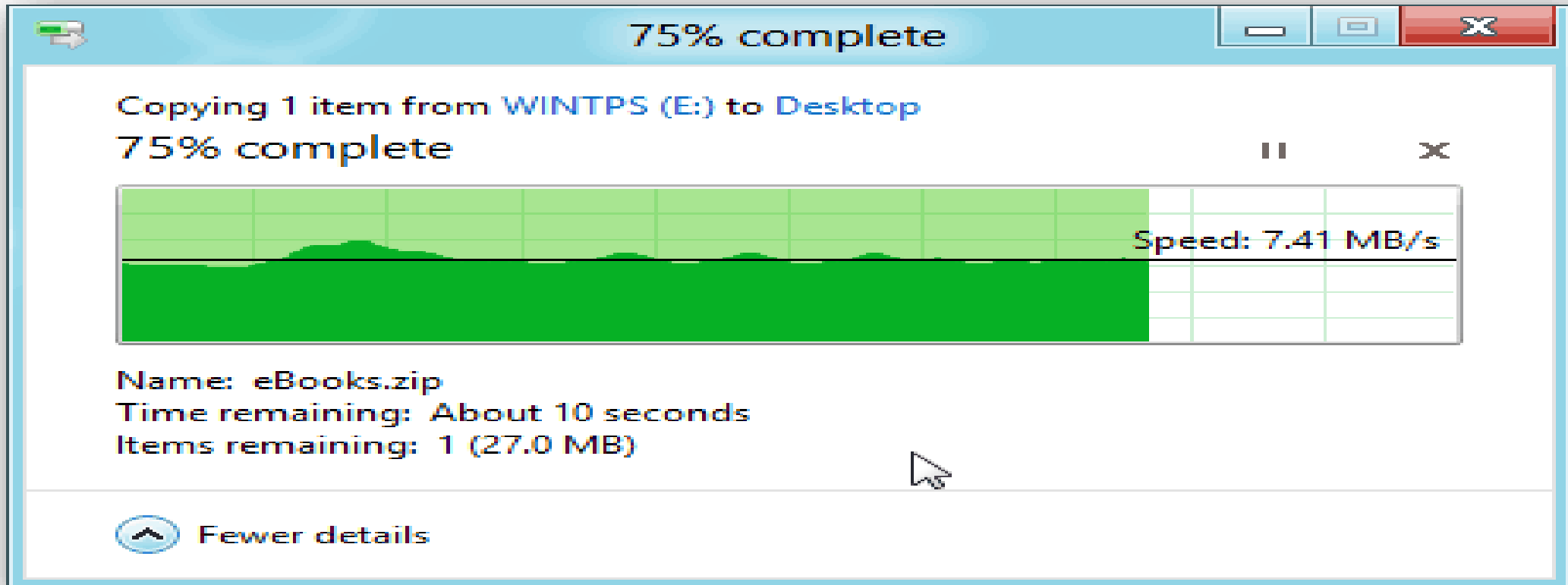
# Extraction of Data

## Copying Data/Disk Imaging (Mirroring)/Disk Cloning





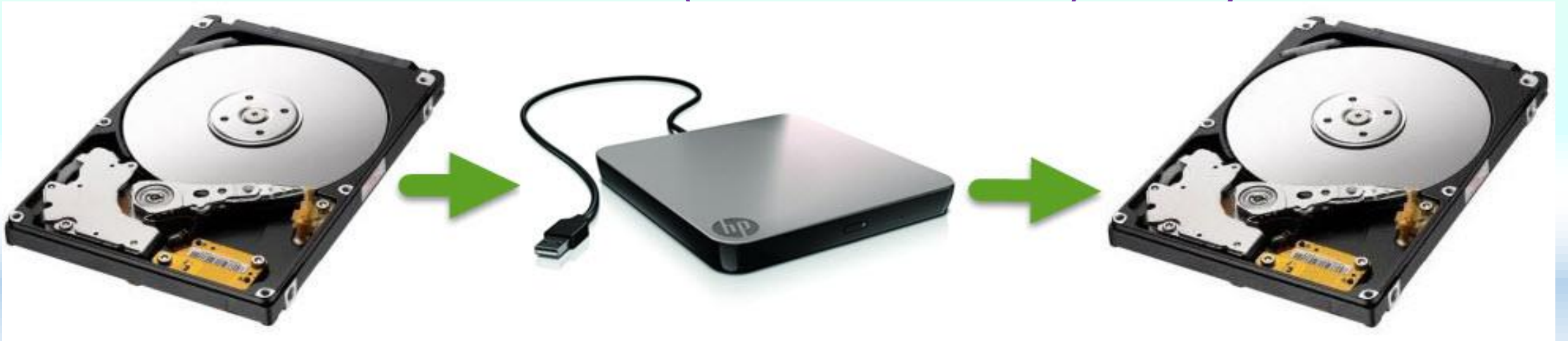
# Copying Data



**We can not get deleted data from a data storage device by this method.**

# Disk Imaging

- A disk image, in computing, is a computer file containing the contents and structure of a disk volume or of an entire data storage device, such as a hard disk drive, tape drive, floppy disk, optical disc, or USB flash drive.
- It completely captures all files/data sector by sector on system and replicates all data.
- We can retrieve deleted data (if not overwritten) also by this method.





# Disk Cloning

- Disk cloning is the process of creating a 1-to-1 copy of a hard disk drive (HDD) or solid state drive (SSD), not just its files.
- It creates exact replica of hard disk drive (HDD) or solid state drive (SSD) being cloned.
- We can retrieve deleted data (if not overwritten) also by this method.



## Disk Cloning



*VS*

## Disk Imaging



**Disk Imaging:** Imaging creates a large compressed file of your drive. Because the image file itself is large, they are often saved to external drives or the cloud.

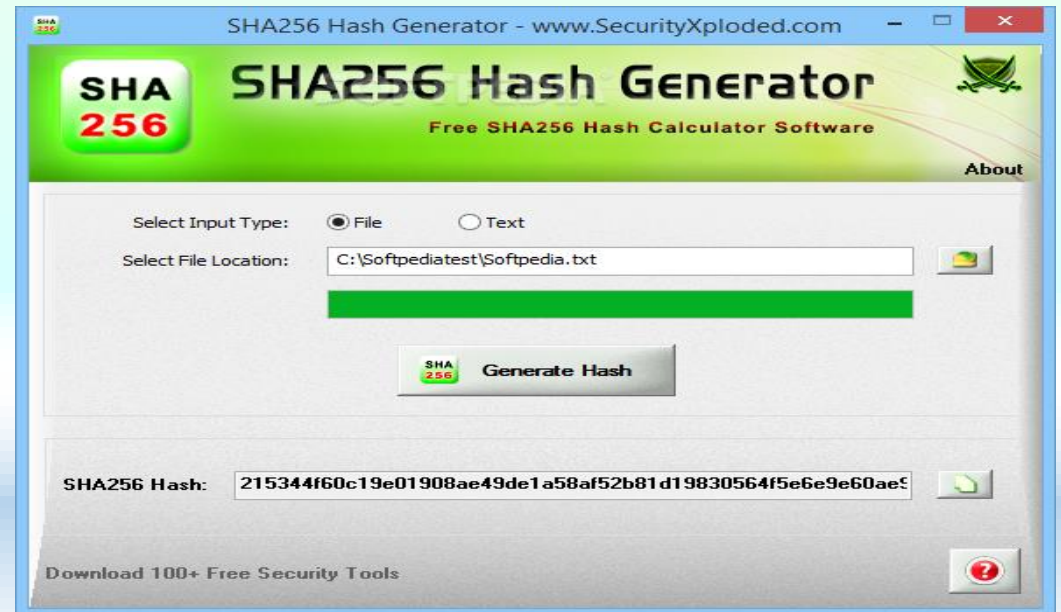
**Disk Cloning:** Cloning creates an exact, uncompressed replica of your drive. If a hard drive fails, you can remove it and replace it with the cloned drive.



# Data Integrity

- Write-Protect Device/Write Blocker
- Hash Value

Not maintaining integrity of seized data in the process of custody of digital device and/or absence of appropriate documentation in this regards, will not only hamper the investigation, but it may also expose the investigating officers to criminal liability under section 72 of ITAA 2008, for breach of confidentiality and privacy.



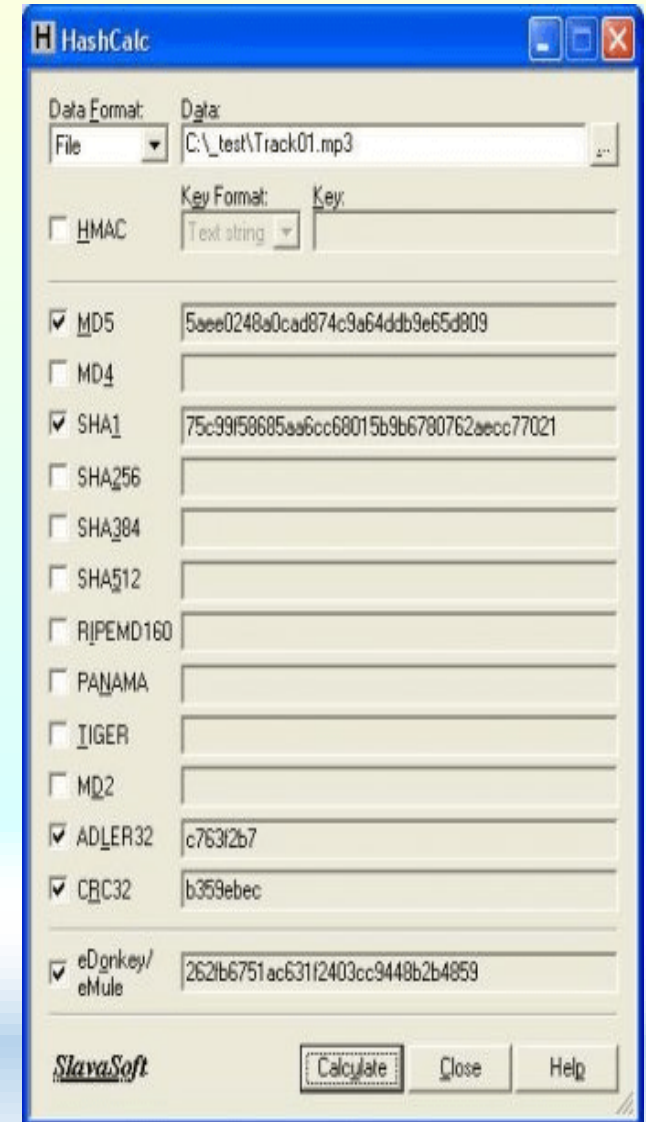
# Write Blocker

- Write Blocker is a tool designed to prevent any write access to the hard disk, thus permitting read-only access to the data storage devices without compromising the integrity of the data.
- When a system, seized on a particular date, is switched on at a later date to view its content, the date and time of opening these files automatically gets modified, rendering the evidence on such disks inadmissible in a court proceeding. Similarly, accessing a system or hard disk in any way, without the use of “write-protect” devices, causes change in the hash value or digital fingerprint of the disk. This again would render the evidence on such disks inadmissible.
- Write Blockers are basically of 2 types:
  1. **Hardware Write Blocker**
  2. **Software Write Blocker**

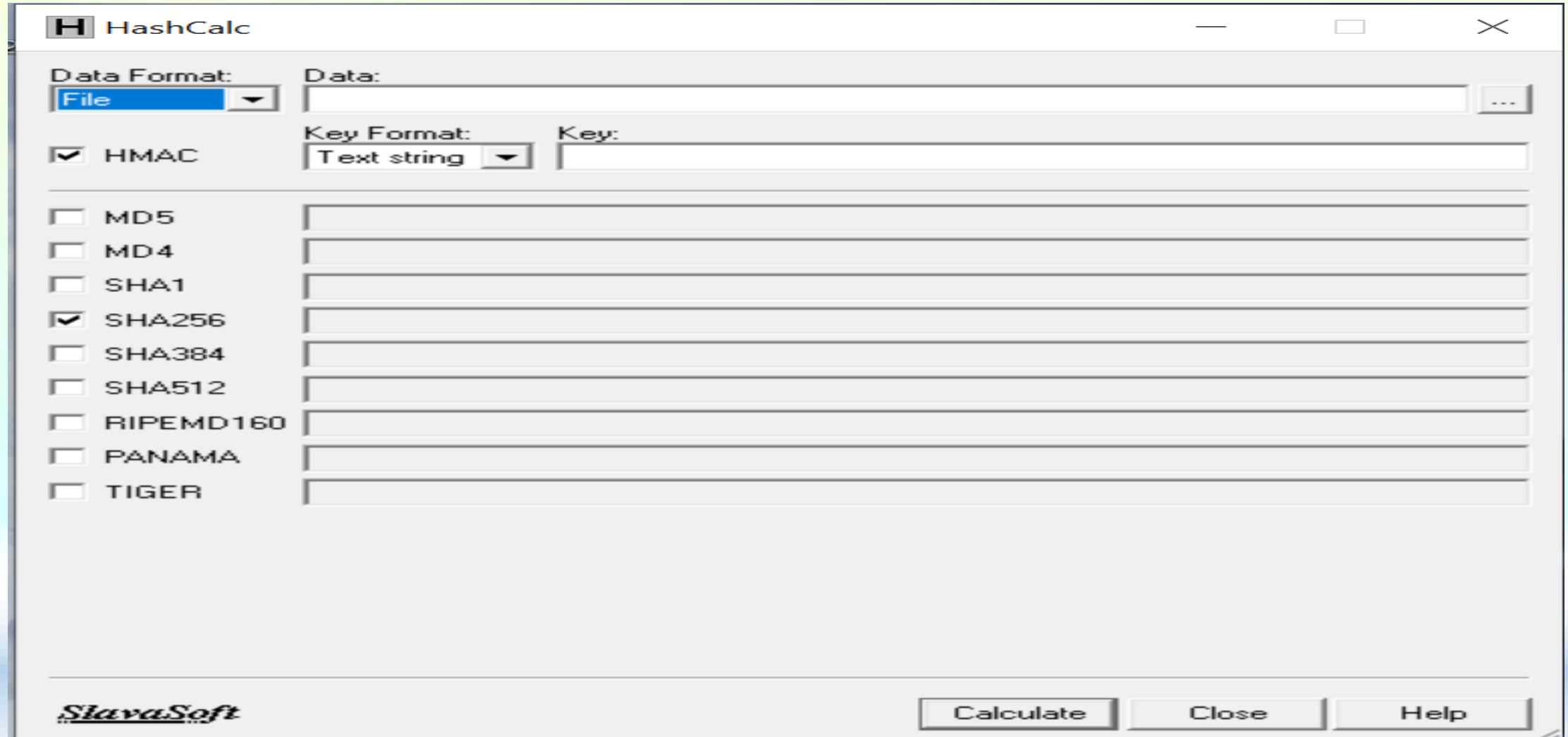


# Hash Value

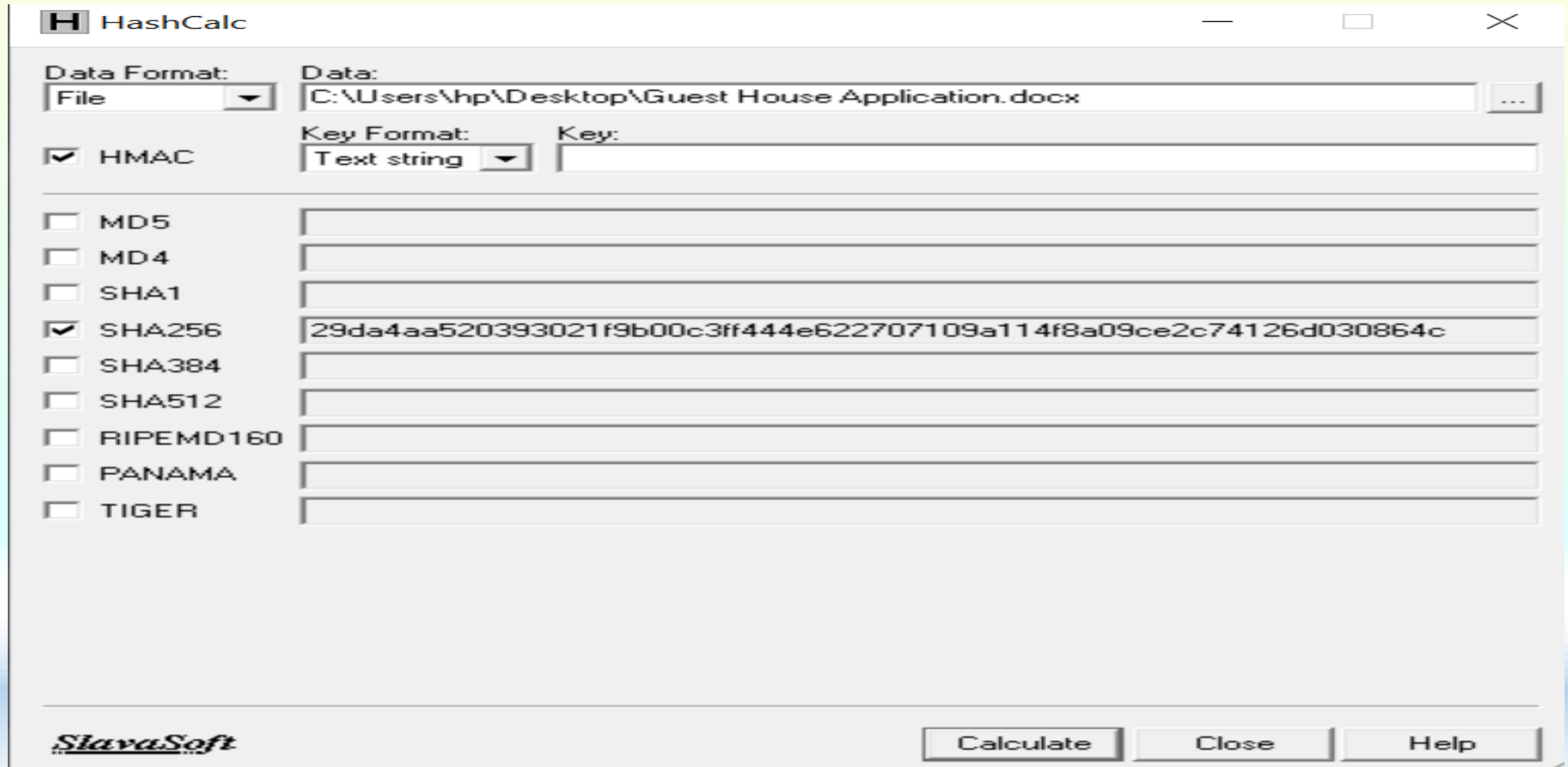
- Hash value is an important aid in establishing the chain of custody of seized digital device. It is indispensable for the field level officers to understand how hash value can be generated and altered. Hash value of every seized digital device, being a critical detail, has to be necessarily entered in the Panchnama drawn during the search operations.
- **Hash values** can be thought of as fingerprints for files. The contents of a file are processed through a cryptographic algorithm, and a unique numerical **value** – the **hash value** - is produced that identifies the contents of the file.



# Hash Calculators

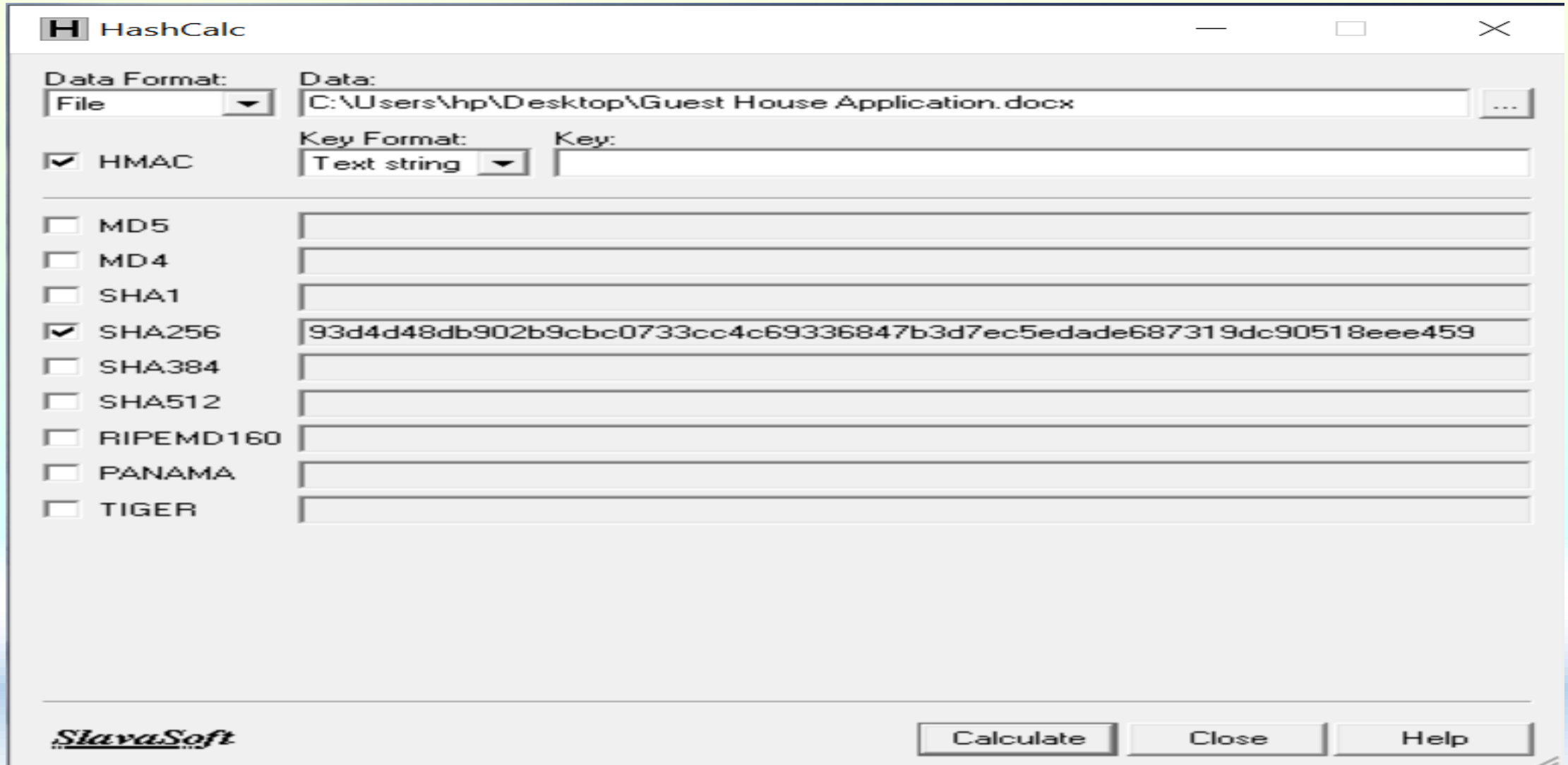


# Hash Calculators





# Hash Calculators



# Digital Evidence Collection Form

<b>Digital Evidence Collection Form</b>			
Name of Officer :			
File No. & Name of Person :			
Date:	Time:	Premise Address :	
Examiner's Name & Details -			
Forensic Software used:			
Version:			
<b>Computer Information</b>			
<input type="checkbox"/> Laptop	<input type="checkbox"/> Desktop	<input type="checkbox"/> Server	<input type="checkbox"/> File/Folder
<input type="checkbox"/> Others	If Others, specify		
<b>System State</b> - On / Off / Hibernation / Sleep			
If Switched On, what is visible on Screen -			
<b>System Information</b>	Make:	Model:	
	Serial No:	Size:	
<b>Shutdown Type</b> - Normal / Power Plug Pulled / Battery Removed			
Is media encrypted? Yes / No      Type of Encryption -			
Storage Copy Details		Working Copy Details	
Make:	Model:	Make:	Model:
Serial No:		Serial No:	
Is the Hard Disk replaced back?		Date:	Time:
Has the Signature of the witnesses been taken?      Yes / No			
Note by the Investigating Officer regarding potential evidences in the digital device(s):			

# Mobile Device Collection Form

<b>Mobile Device Collection Form</b>			
Name of Officer :			
File No. & Name of Person :			
Date:	Time:	Premise Address :	
Examiner's Name & Details -			
Forensic Software used:			
Version:			
<b>Mobile Information</b>			
<input type="checkbox"/> Basic Phone	<input type="checkbox"/> iOS	<input type="checkbox"/> Android	<input type="checkbox"/> Blackberry
<input type="checkbox"/> Windows	If Others, specify		
<b>Mobile State</b> - On / Off / Hibernation / Sleep			
If Switched On, what is visible on Screen -			
<b>Mobile Information</b>	Make:	Model:	
	Serial No:	Size:	
<b>Shutdown Type</b>	Normal / Battery Removed		
Is media encrypted? Yes / No      Type of Encryption -			
<b>Storage Copy Details</b>		<b>Working Copy Details</b>	
Make:	Model:	Make:	Model:
Serial No:		Serial No:	
Is the SD Card replaced back?		Date:	Time:
Has the Signature of the witnesses been taken?      Yes / No			
Note by the Investigating Officer regarding potential evidences in the digital device(s):			



# Chain of Custody Form

<u>Chain of Custody Form</u>					
Name of The Person					
Date	Time	Premises Address			
Description					
Reason/Action	Received From	Received by	Data	Time	Signature of person from whom received

# Digital Evidence Matrix

S No.	Name of Device	Device Type	Name of Party	Relationship with Main Accused	Whether any Incriminating Evidence found in Device?	Nature of Evidence found in Device	Whether Party was confronted with the Evidence?	Response of the Party at being confronted with Evidence

# Certificate

## [Under Section 65B(4)(C) of the Indian Evidence Act, 1872]

### **CERTIFICATE**

**(Under Section 65B(4)(C) of the Indian Evidence Act, 1872**

Certified that the proceedings, pertaining to F.No. \_\_\_\_\_ dated \_\_\_\_ under Section \_\_\_\_ of the \_\_\_\_\_

Our Case Number: \_\_\_\_\_ related to data retrieval from the \_\_\_\_\_ were carried out by the undersigned using authorized forensic software and hardware, and retrieved data were given in hard copy/printouts as \_\_\_\_\_ and/or soft copy as \_\_\_\_\_. The contents of the hard copy/printouts and/or soft copy are true reproduction of the retrieved data.

It is also certified that at the time of data retrieval, the computer system was under my control and was working properly during the process, and there is no distortion in accuracy of the data.

It is further certified that the conditions, as laid down in Section 65B(2)(a) to 65B(2)(d) of the Indian Evidence Act, 1872 regarding admissibility of the aforesaid contents of hard copy/printouts and/or soft copy in respect of the retrieved data are fully satisfied. The details, as stated above, are true to the best of my knowledge and belief.

(Signature)

(Name in Bold Letters)

(Designation)

(Organization)



# Disk Imaging Tools

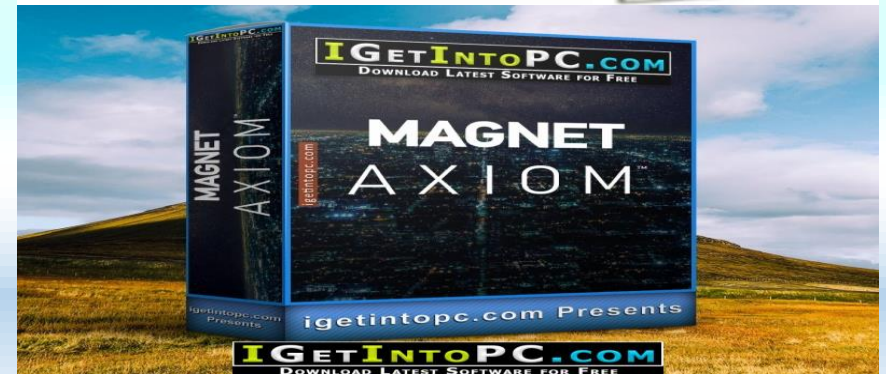


**Disk Image Viewer**

# Forensic Hardware & Software

## Disk Imaging Tools

<u>Sr. No.</u>	<u>Name</u>	<u>Description</u>
1	Access Data Forensic Toolkit (FTK)	<ol style="list-style-type: none"><li>1. Developed by Access Data.</li><li>2. Multi-purpose tool commonly used to index acquired media.</li><li>3. The licensed version of FTK Imager can handle deleted files also, which is not possible in free version.</li></ol>
2	EnCase Forensic	EnCase contains tools for operations such as acquisition, analysis and reporting.
3	Magnet Axiom	Enables recovery of digital evidence from most sources including smartphones, cloud, computers, IoT devices and third-party images.



# Forensic Hardware & Software

## Memory Forensic Tools

Sr. No.	Name	Description
1.	CaptureGUARD Physical Memory Acquisition Hardware ExpressCard	Capable of imaging the physical memory of the computer connected.





# Mobile Forensic Tools



# Forensic Hardware & Software

## Mobile Forensic Tools

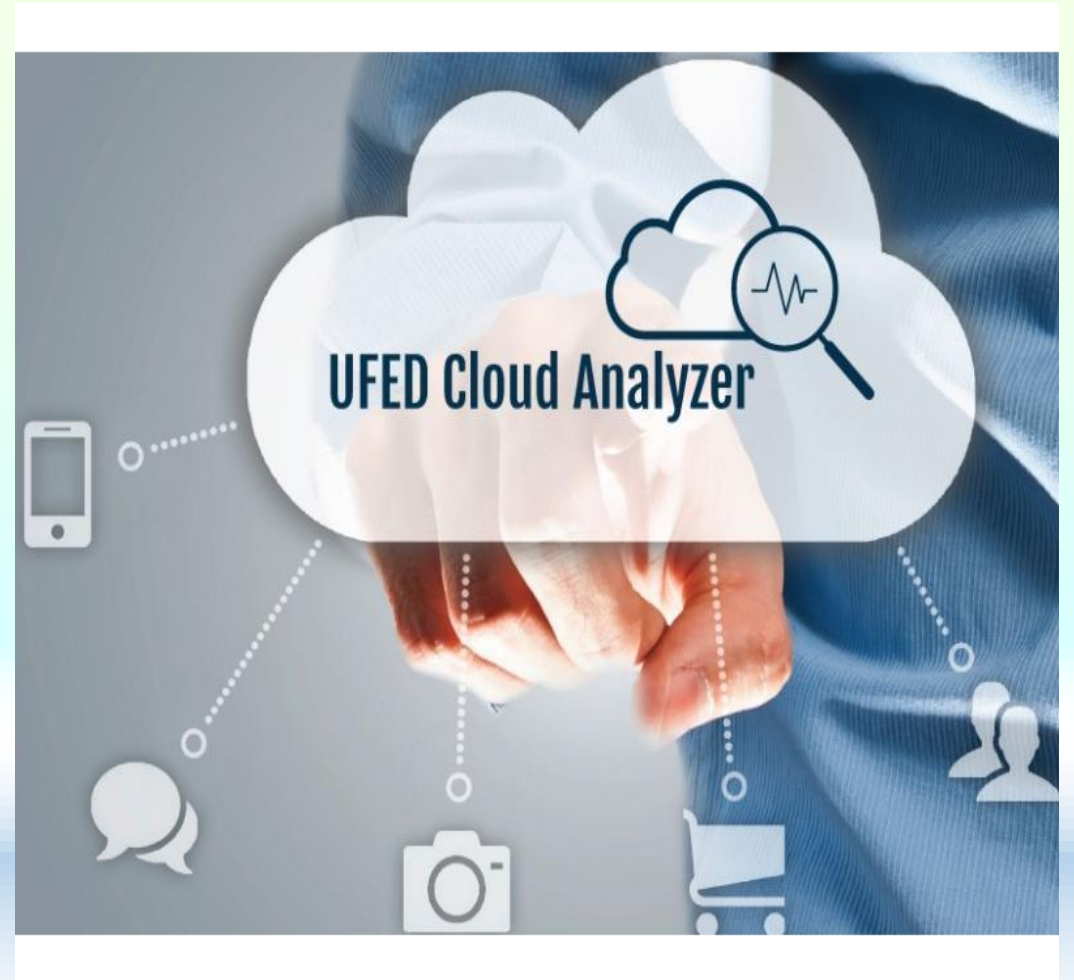
<u>Sr. No.</u>	<u>Name</u>	<u>Description</u>
1	<b>UFED Touch Ultimate</b>	Capable of Extracting all data (even if deleted) from the widest range of devices including legacy and feature phones, smartphones, portable GPS devices, tablets and phones manufactured with Chinese chipsets.
2	<b>Oxygen Forensic Suite</b>	<ol style="list-style-type: none"> <li>1. Extract data from passcode-locked iOS devices.</li> <li>2. Android analysis: physical dump, backup or OxyAgent utility approach.</li> <li>3. Extract geo-data from Fitness apps.</li> <li>4. Ability to view device usage activity and find the most active day.</li> </ol>
3	<b>Elcomsoft IOS Forensic Toolkit</b>	Perform physical/logical acquisition of Apple devices. Image device file system, extract device secrets and decrypt the file system image.
4	<b>Paraben's Device</b>	Enables the investigator to perform logical and physical data acquisitions, deleted data recovery, and full data dumps, on approximately 2400 models of cell phones, PDAs/smartphones, and portable GPS units.



# Forensic Hardware & Software

## Tool for Social Media

<u>Name</u>	<u>Platform</u>	<u>Description</u>
Cellebrite UFED Cloud Analyzer	Social media accounts - Facebook, Twitter, Instagram, etc.	UFED Cloud Analyzer provides forensic practitioners with instant extraction, preservation and analysis of private social media accounts.

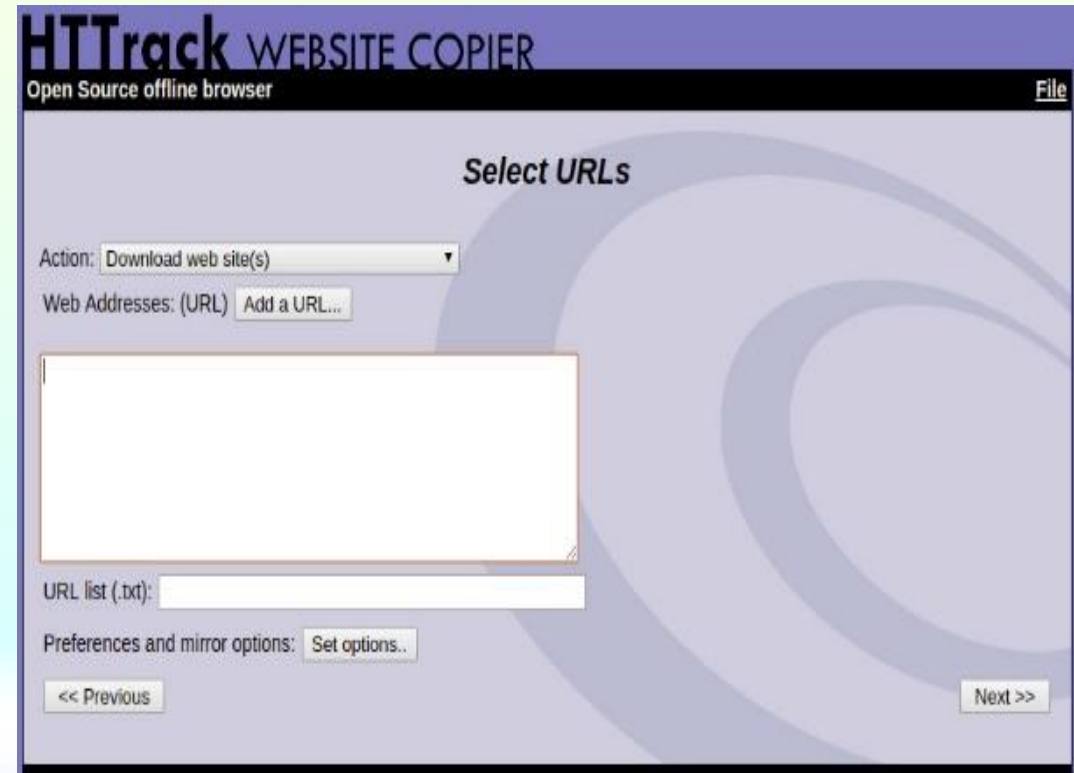




# Forensic Hardware & Software

## HTTrack Website Copier

HTTrack is a free software and easy-to-use offline browser utility which allows one to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.



# Forensic Hardware & Software

## True Traveller (Developed by C-DAC)

True Traveller is a complete solution for performing digital forensics seizure, acquisition and analysis. This product includes a laptop with software tools installed and an integrated disk imaging hardware solution. The kit can be easily carried to scene of crime and can carry out on-site forensic data acquisition. The kit is capable of acquiring Mobile phone data and SIM card data using Software installed on the laptop. The Imaging hardware tool performs hashing using MD5, SHA1 and SHA2 hashing algorithms. The unit also supports wiping of destination disk for sterilizing the media.



# Archival of Digital Evidence

- Archival of Digital evidence is an important aspect to ensure authenticity, traceability, and auditing of the digital evidence.
- Directions must be issued to the authorized custodians to preserve all the electronic and hard copy documents related to the case.
- All the digital devices must be stored in a place which is completely secure, fire-proof, water-proof and free from electromagnetic interference which may corrupt the digital evidences.
- All the digital devices must be stored in an access-controlled location preferably under CCTV and a register maintaining records of every person entering or exiting the facility.



# Relevant Provisions of Various Acts

- **Information Technology Act, 2000 [as amended by the Information Technology (Amendment) Act, 2008]**
- **The Indian Telegraph Act, 1885**
- **Indian Penal Code, 1861**
- **Criminal Procedure Code, 1973**
- **Indian Evidence Act, 1872**
- **The Wildlife (Protection) Act, 1972**
- **The Bankers' Books Evidence Act, 1891**

# Information Technology Act, 2000 [as amended by the Information Technology (Amendment) Act, 2008]

- **Section 2(1)(i): "computer"** means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.
- **Section 2(1)(k): "computer resource"** means computer, computer system, computer network, data, computer data base or software.
- **Section 2(1)(o): "data"** means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

**Section 2(1)(r):** "electronic form" with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

**Section 2(1)(t):** "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro fiche.

**Section 79A** of the IT Act, as amended, explains "electronic form evidence" as any information of probative value that is either stored, or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines.

*The other most crucial question in cybercrime investigation regarding the reliability of digital evidence has also been clarified by Section 79A of the IT Act, 2000, as amended, which empowers the Central government to appoint any department or agency of Central or State government as **Examiner of Electronic Evidence**. This agency will play a crucial role in providing expert opinion on electronic form of evidence.*



# Notification of Forensic labs as 'Examiner of Electronic Evidence' under Section 79A of the Information Technology Act, 2000

- In 2017, the Ministry of Electronics and Information Technology (MeitY) came up with a scheme for identification and selection of Examiner of Electronic Evidence, in terms of Section 79A of the IT Act 2000.
- The objective of the notified scheme, as detailed in the 'Scheme for Notifying Examiner of Electronic Evidence', is to ascertain the competence of all desiring Central Government or a State Government agencies and to qualify them to act as Examiner of Electronic evidence as per their scope of approval through a formal accreditation process. Once notified, such Central, State Government agencies can act as the "Examiner of Electronic Evidences", and provide an expert opinion of digital evidences before any court.

**As of June 2020, the following labs have been notified as “Examiner of Electronic Evidence” under Section 79A of the IT Act, 2000:**

1. Forensic Science Laboratory - Government of National Capital Territory, New Delhi;
2. Computer Forensic and Data Mining Laboratory (CFDML) - Serious Fraud Investigation Office (SFIO), Ministry of Corporate Affairs, New Delhi;
3. Directorate of Forensic Science - Government of Gujarat, Gandhi Nagar, Gujarat;
4. Central Forensic Science Laboratory (CFSL) - Ministry of Home Affairs, Hyderabad, Telangana;
5. State Forensic Science Laboratory, Karnataka, Police Department, Bengaluru;
6. Cyber Forensic Laboratory, Army Cyber Group, Directorate General of Military Operations, Signals Enclave, New Delhi; and
7. Regional Forensic Science Laboratory, Northern Range, Dharamshala, Himanchal Pradesh

# Section 69 of the Information Technology Act, 2000 as amended in 2008

## **Section 69 (1) Power to issue directions for interception or monitoring or decryption of any information through any computer resource. –**

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do **in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence**, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

# Section 69 of the Information Technology Act, 2000 as amended in 2008

**Section 69 (2)** The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

**Section 69 (3)** The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-**(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or**

- **(b) intercept, monitor, or decrypt the information, as the case may be; or**
- **(c) provide information stored in computer resource.**



# Section 69A(1) in The Information Technology Act, 2000

Where the Central Government or any of its officer specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, *in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above*, it may subject to the provisions of sub-section (2) for reasons to be recorded in writing, by order, *direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.*

# **Section 69A(2) in The Information Technology Act, 2000**

The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

# Section 69 of the Information Technology Act, 2000 as amended in 2008

**Section 69 (4)** The subscriber or intermediary or any person who fails to assist the agency referred to in subsection (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

# Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

2

THE GAZETTE OF INDIA : EXTRAORDINARY

[PART II—SEC. 3(ii)]

**MINISTRY OF HOME AFFAIRS**  
(CYBER AND INFORMATION SECURITY DIVISION)

**ORDER**

New Delhi, the 20th December, 2018

**S.O. 6227(E).**—In exercise of the powers conferred by sub-section (1) of section 69 of the Information Technology Act, 2000 (21 of 2000) read with rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, the Competent Authority hereby authorises the following Security and Intelligence Agencies for the purposes of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource under the said Act, namely:—

- (i) Intelligence Bureau;
- (ii) Narcotics Control Bureau;
- (iii) Enforcement Directorate;
- (iv) Central Board of Direct Taxes;
- (v) Directorate of Revenue Intelligence;
- (vi) Central Bureau of Investigation;
- (vii) National Investigation Agency;
- (viii) Cabinet Secretariat (RAW);
- (ix) Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only);
- (x) Commissioner of Police, Delhi.

[No.14/07/2011-T]

RAJIV GAUBA, Union Home Secy.



# Legal Recognition Of Electronic Records

- Section 4 of Information Technology Act, 2000: Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-
  - a. rendered or made available in an electronic form; and
  - b. accessible so as to be usable for a subsequent reference.

# The Indian Telegraph Act, 1885

## Lawful Interception of Communication

### Section 5(2) in The Indian Telegraph Act, 1885

On the occurrence of any public emergency, or in the interest of the public safety, *the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may*, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, *shall not be transmitted*, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order.

# Rule 419A of the Indian Telegraph Rules, 1951

- Directions for interception of any message or class of messages under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said (Act)) shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government. *In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be.*

# Rule 419A of the Indian Telegraph Rules, 1951

## Provided that in emergent cases—

- (i) in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or
- (ii) for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible;

the required interception of any message or class of messages shall be carried out with the prior approval of the Head or the second senior most officer of the authorized security *i.e.* Law Enforcement Agency at the Central Level and the officers authorised in this behalf, not below the rank of Inspector General of Police at the state level *but the concerned competent authority shall be informed of such interceptions by the approving authority within three working days and that such interceptions shall be got confirmed by the concerned competent authority within a period of seven working days. If the confirmation from the competent authority is not received within the stipulated seven days, such interception shall cease and the same message or class of messages shall not be intercepted thereafter without the prior approval of the Union Home Secretary or the State Home Secretary, as the case may be.*



# Rule 419A of the Indian Telegraph Rules, 1951

## Review Committee:

- The Central Government and the State Government, as the case may be, shall constitute a Review Committee. The Review Committee to be constituted by the Central Government shall consist of the following, namely:
  - (a) Cabinet Secretary — Chairman
  - (b) Secretary to the Government of India Incharge, Legal Affairs — Member
  - (c) Secretary to the Government of India, Department of Telecommunications — Member
- The Review Committee to be constituted by a State Government shall consist of the following, namely:
  - (a) Chief Secretary — Chairman
  - (b) Secretary Law/Legal Remembrancer Incharge, Legal Affairs — Member
  - (c) Secretary to the State Government (other than the Home Secretary) — Member

# Rule 419A of the Indian Telegraph Rules, 1951

- The Review Committee shall meet *at least once in two months* and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-section (2) of Section 5 of the said Act. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above it may set aside the directions and orders for destruction of the copies of the intercepted message or class of messages.
- *Records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorized security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements.*

# Agencies Empowered for Lawful Interception

The competent authority in the central government has authorised 10 agencies for this purpose - Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Central Bureau of Investigation, National Investigation Agency, Cabinet Secretariat (RAW), Directorate of Signal Intelligence (for service areas of Jammu and Kashmir, North East and Assam only) and Commissioner of Police, Delhi.

# Indian Penal Code, 1861

- **Section 29A. “Electronic record”** –The words "electronic record" shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000.
- **Section 175. Omission to produce document or electronic record to public servant by person, legally bound to produce it** – Whoever, being legally bound to produce or deliver up any [document or electronic record] to any public servant, as such, intentionally omits so to produce or deliver up the same, shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five hundred rupees, or with both;  
or, if the [document or electronic record] is to be produced or delivered up to a Court of Justice, with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees or with both.



- **Section 201. Causing disappearance of evidence of offence, or giving false information to screen offender** – Whoever, knowing or having reason to believe that an offence has been committed, causes any evidence of the commission of that offence to disappear, with the intention of screening the offender from legal punishment, or with that intention gives any information respecting the offence which he knows or believes to be false,
  - *If a capital offence* - shall, if the offence which he knows or believes to have been committed is punishable with death, be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine;
  - *If punishable with imprisonment for life* – and if the offence is punishable with imprisonment for life, or with imprisonment which may extend to ten years, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine;
  - *If punishable with less than ten years' imprisonment* – and if the offence is punishable with imprisonment for any term not extending to ten years, shall be punished with imprisonment of the description provided for the offence, for a term which may extend to one-fourth part of the longest term of the imprisonment provided for the offence, or with fine, or with both.

# Code of Criminal Procedure, 1973

- **Section 91 – Summons to produce document or other thing:**

Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.

- **Section 161 – Examination of witnesses by police:**

(1) Any police officer making an investigation under this Chapter, or any police officer not below such rank as the State Government may, by general or special order, prescribe in this behalf, acting on the requisition of such officer, may examine orally any person supposed to be acquainted with the facts and circumstances of the case.

(2) Such person shall be bound to answer truly all questions relating to such case put to him by such officer, other than questions the answers to which would have a tendency to expose him to a criminal charge or to a penalty or forfeiture.

(3) The police officer may reduce into writing any statement made to him in the course of an examination under this section; and if he does so, he shall make a separate and true record of the statement of each such person whose statement he records.

## Section 164 – Recording of confessions and statements before a Magistrate

- Any Metropolitan Magistrate or Judicial Magistrate may, whether or not he has jurisdiction in the case, record any confession or statement made to him in the course of an investigation under this Chapter or under any other law for the time being in force, or at any time afterwards before the commencement of the inquiry or trial: Provided that no confession shall be recorded by a police officer on whom any power of a Magistrate has been conferred under any law for the time being in force.
- The Magistrate recording a confession or statement under this section shall forward it to the Magistrate by whom the case is to be inquired into or tried.

## **Section 166A in The Code Of Criminal Procedure, 1973: *Letter of request to competent authority for investigation in a country or place outside India***

**(1) Notwithstanding anything contained in this Code, if, in the course of an investigation into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India, any Criminal Court may issue a letter of request to a Court or an authority in that country or place competent to deal with such request to examine orally any person supposed to be acquainted with the facts and circumstances of the case and to record his statement made in the course of such examination and also to require such person or any other person to produce any document or thing which may be in his possession pertaining to the case and to forward all the evidence so taken or collected or the authenticated copies thereof or the thing so collected to the Court issuing such letter.**

**(2) The letter of request shall be transmitted in such manner as the Central Government may specify in this behalf.**

**(3) Every statement recorded or document or thing received under sub- section (1) shall be deemed to be the evidence collected during the course of investigation under this Chapter.**



# Indian Evidence Act, 1872

*By way of the second schedule to the IT Act, Amendments to the Indian Evidence Act, 1872 have been brought, so as to, give electronic records, a legal recognition as evidence. The relevant amendments are as under:*

- **In Section 3 –**

- in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;
- The amended definition of “evidence” in section 3 is reproduced for proper understanding of the term.
- “Evidence” –“Evidence” means and includes-
- (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called **oral evidence**;
- (2) all documents including electronic records produced for the inspection of the Court;
- such documents are called **documentary evidence**.

- **In Section 17**, for the words "oral or documentary," the words "**oral or documentary or contained in electronic form**" shall be substituted.
- **After Section 22**, the following section shall be inserted, namely: -  
When oral admission as to contents of electronic records are relevant.  
**Sec.22A.** Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.“
- **In Section 34**, for the words "Entries in the books of account", the words "**Entries in the books of account, including those maintained in an electronic form**" shall be substituted.

# Admissibility Of Electronic Records

*Special provisions as to evidence relating to electronic record have been inserted in the form of section 65A & 65B, after section 65 of the Indian Evidence Act 1872. These provisions are very important and they govern the integrity of the electronic record as evidence, as well as, the process for creating electronic record.*

**(1) Section 65A:** The contents of electronic records may be proved in accordance with the provisions of section 65B.

**(2) Section 65B:**

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:

- a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
- b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
- c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
- d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities



(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether-

a. by a combination of computers operating over that period; or

b. by different computers operating in succession over that period; or

c. by different combinations of computers operating in succession over that period; or

d. in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

- (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-
- a. identifying the electronic record containing the statement and describing the manner in which it was produced;
  - b. giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
  - c. dealing with any of the matters to which the conditions mentioned in subsection(2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, -

- a. information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
- b. whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
- c. a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

*Explanation.* - For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.

# Section 45 in The Indian Evidence Act, 1872

**Opinions of Experts**—When the Court has to form an opinion upon a point of foreign law or of science or art, or as to identity of handwriting [or finger impressions], the opinions upon that point of persons specially skilled in such foreign law, science or art, [or in questions as to identity of handwriting] [or finger impressions] are relevant facts.



# Section 45A in The Indian Evidence Act, 1872

**Opinion of Examiner of Electronic Evidence** —When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 is a relevant fact.

# Wildlife Protection Act, 1972

**Section 50(5):** Any person who, without reasonable cause, fails to produce anything, which he is required to produce under this section, shall be guilty of an offence against this Act.

**Section 50(8):** *Notwithstanding anything contained in any other law for the time being in force*, any officer not below the rank of an Assistant Director of Wild Life Preservation or [an officer not below the rank of Assistant Conservator of Forests authorised by the State Government in this behalf] shall have the powers, for purposes of making investigation into any offence against any provision of this Act,—

(a) to issue a search warrant;

(b) to enforce the attendance of witnesses;

(c) *to compel the discovery and production of documents and material objects; and*

(d) to receive and record evidence.]

# What CBIC, Ministry of Finance, Gol, Has Done

**Instruction No. 03/2018 – Customs**

F.No. 394/21/2018-Cus (AS)  
Government of India  
Ministry of Finance  
Department of Revenue  
Central Board of Excise & Customs  
(Anti-Smuggling Unit)  
\*\*\*

New Delhi, dated 16<sup>th</sup> February 2018

To  
All Principal Chief Commissioners/Chief Commissioners of Customs / Customs (Preventive),  
All Principal Chief Commissioners/Chief Commissioners of Customs & CGST,  
All Principal Commissioners/Commissioners of Customs / Customs (Preventive),  
All Principal Commissioners/Commissioners of Customs & CGST,  
The Director General, Directorate General of Revenue Intelligence

Madam / Sir,

**Subject: Providing the CDR & customer Details - regarding**

It has been brought to the notice of the Board that field formations are approaching DRI for seeking CDRs and Customer details of phone numbers from telecom service providers.

2. This is reportedly being done as telecom service providers are not providing these details to the field formations since they are not a designated 'Law Enforcement Agency' like DRI under the provisions of Section 5(2) of Indian Telegraph Act, 1885.

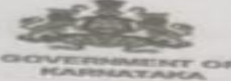
3. In view of the above, it is clarified that field formations can obtain the SDR/CDR details directly from telecom service providers under the provisions of Section 108 of the Customs Act, 1962 which empowers any Gazetted Officer of Customs to summon any person to give evidence or to produce documents. For investigation purposes, DRI also obtains SDR/CDR details from telecom service providers under the provisions of Section 108 of the Customs Act, 1962. Hence, field formations may not refer such matters to DRI and seek the required details directly from the telecom service providers under the provisions stated above.

Yours faithfully,

  
(Rohit Anand)

Under Secretary to the Government of India

# What Karnataka Govt. Has Done

  
 GOVERNMENT OF KARNATAKA

No. ACS/Home/16/CDR/2014

Karnataka Government Secretariat  
Vidhana Soudha  
Bangalore, dated:20/07/2020.

**NOTIFICATION**

In exercise of the powers vested under Rule 2(d) and 4 of The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rule 2009, the Government of Karnataka, in its notification dated 09/07/2019 had authorised the following officers of the Karnataka Forest Department to receive Call Detail Records (CDR), Subscriber Detail Record(SDR) Dumps, Tower Locations and Tower Dumps on monthly basis from the Telecom Service Providers while discharging their duties under The Karnataka Forest Act 1963 and Wildlife Protection Act 1972 for a period upto 30/06/2020.

Sl. No.	Designation of the Officer	NIC Mail ID
01	Additional Principal Chief Conservator of Forest (Wildlife)	apccfwl@aranya.gov.in
02	Additional Principal Chief Conservator of Forest (Vigilance)	apccfvig@aranya.gov.in
03	Conservator of Forests & Director, BRT, TR	dcfwlchm@aranya.gov.in
04	Conservator of Forests & Director, RGNP, Hunsur	dcfhnswl@aranya.gov.in

The said authorization is further extended only to the following officers from 20/07/2020 to 31/03/2021.

Sl. No.	Designation of the Officer	NIC Mail ID
01	Additional Principal Chief Conservator of Forest (Wildlife)	apccfwl@aranya.gov.in
02	Additional Principal Chief Conservator of Forest (Vigilance)	apccfvig@aranya.gov.in

And, further the Additional Principal Chief Conservator of Forest (Wildlife), Mobile Number- +91 9480128128 is authorized to obtain SMS based Location Service from 20/07/2020 to 31/03/2021.

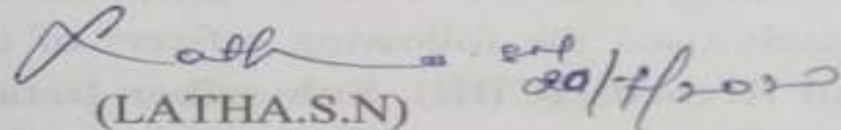


# What Karnataka Govt. Has Done

-2-

The Officers, so authorized shall comply with all the direction laid down under The Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rule 2009 and in accordance with the direction given by the Supreme Court in it's judgment dated:18.12.1996 in Writ Petition (C) No. 256/1991 (People's Union Civil Liberties PUCL V/s Union of India and Another) reported in A.I.R.1997S.C.568, and the copies of the intercepted messages shall be destroyed when no longer required.

BY ORDER AND IN THE NAME OF  
GOVERNOR OF KARNATAKA

 20/7/2020  
(LATHA.S.N)

UNDER SECRETARY TO GOVERNMENT,  
HOME DEPARTMENT (CRIMES)

# The Bankers' Books Evidence Act, 1891


**Section 4: Mode of proof of entries in bankers' books:** Subject to the provisions of this Act, a certified copy of any entry in a banker's books shall in all legal proceedings be received as prima facie evidence of the existence of such entry, and shall be admitted as evidence of the matters, transactions and accounts therein recorded in every case where, and to the same extent as, the original entry itself is now by law admissible, but not further or otherwise.

# The Covid-19 has shifted everything online — including wildlife trafficking

While reports show at least a 50 per cent decline in illegal wildlife trade activities in Southeast Asia in 2020, experts say traders have shifted from face-to-face interactions and increased their presence on online platforms.







**Village Hunter**  
233,162 subscribers

[SUBSCRIBE](#)

youtube.com/watch?v=6QK0t8kBYSQ

Search

[SIGN IN](#)

Up next AUTOPLAY

- Primitive Technology: Egg And Quail Birds Hunting With in...  
Village Hunter  
1.8M views  
24:30
- Primitive Technology: Revenge Hunting And Cooking Monitor...  
Village Hunter  
1.3M views  
22:50
- Primitive Technology : Biggest Fish Hunting and cooking ...  
Village Hunter  
1.79K views  
20:19
- primitive technology: Cow'S Leg Theft Hunter | Large Size Grille...  
Village Hunter  
2.2M views  
26:13
- Primitive Technology: Find Bees By Fire Smoke Naturally ...  
Primitive Kid Tool  
2.6M views  
10:24
- Primitive technology :Lucky Hunter Trapped and 4 Rabbit...  
Village Hunter  
961K views  
New  
22:57
- Yummy cooking BBQ goat grilled recipe - Cooking skill

Primitive Technology: Monitor Lizard In The Deep WholeCatch by Hand | Natural Hunt in Village Hunter  
421,115 views  
2.7K likes 835 comments  
[SHARE](#) [SAVE](#)

[Village Hunter](#)  
Published on Aug 29, 2019  
[SUBSCRIBE 233K](#)







Secure | [https://www.amazon.in/Real-Genuine-Cobra-Snake-Buckle/dp/B074PX3J6H/ref=pd\\_rhf\\_ee\\_p\\_img\\_1?\\_encoding=UTF8&psc=1&refRID=56K626JSHOW5GNXRWKSQ](https://www.amazon.in/Real-Genuine-Cobra-Snake-Buckle/dp/B074PX3J6H/ref=pd_rhf_ee_p_img_1?_encoding=UTF8&psc=1&refRID=56K626JSHOW5GNXRWKSQ)

amazon.in  
Clothing & Accessories

Deliver to Vishal SOUTH WES... 110066 Shop by Category Vishal's Amazon.in Today's Deals Amazon Pay Sell Customer Service

AMAZON APP WINS

Hello, Vishal Your Orders Try Prime Your Lists Cart

Amazon Fashion WOMEN MEN KIDS BAGS & LUGGAGE SPORTSWEAR BRANDS SALES & DEALS 30 DAY RETURNS Restrictions Apply

Clothing & Accessories > Men > Accessories > Belts & Suspenders > Real Genuine Cobra Snake Head Hook and Loop Men Belt Buckle

Treasure Gurus

### Real Genuine Cobra Snake Head Hook and Loop Men Belt Buckle

Be the first to review this item

Available from these sellers.

- Genuine Authentic Cobra Head Hook and Loop Mens Belt Buckle, Sure to make a statement wherever you wear it
- 100% Real taxidermy Cobra head snake buckle has amazing detailing, from its beady eyes to the multicolored scales
- Hood of the Cobra is stretched to feature a hook and loop style closure on the back of the buckle, ideal for everyday use

Report incorrect product information.

Amazon Business

Need a GST Invoice on this product? [Sign in from/create business account](#)

**The maximum order quantity for this product is limited to 5 units per customer**

Please note that orders which exceed the quantity limit will be auto-canceled. This is applicable across sellers.

1 offer from ₹ 7,099.00

Deliver to Vishal - South West ... 110066

See All Buying Options

Add to Wish List

Have one to sell? Sell on Amazon

Roll over image to zoom in

# Nodal e-mail IDs of Various Agencies

<u>S.No</u>	<u>Service Provider</u>	<u>Contact Details</u>
1		<a href="mailto:gitanjali@google.com">gitanjali@google.com</a> <a href="mailto:lis-global@google.com">lis-global@google.com</a> <a href="mailto:lis-apac@google.com">lis-apac@google.com</a>
2		<a href="mailto:in-legalpoc@yahoo-inc.com">in-legalpoc@yahoo-inc.com</a>
3		<a href="mailto:legal@rediff.co.in">legal@rediff.co.in</a>
4		<a href="mailto:indiacc@microsoft.com">indiacc@microsoft.com</a> <a href="mailto:msnwwcc@microsoft.com">msnwwcc@microsoft.com</a>
5		<a href="mailto:records@fb.com">records@fb.com</a> <a href="mailto:facebook_grievance_officer_fb@support.facebook.com">facebook_grievance_officer_fb@support.facebook.com</a>
6		<a href="mailto:support@whatsapp.com">support@whatsapp.com</a>
7.		<a href="mailto:grievance-officer-in @ twitter.com">grievance-officer-in @ twitter.com</a>

# Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

## NOTIFICATION

New Delhi, the 27<sup>th</sup> October, 2009

**G.S.R. 781 (E).**— In exercise of the powers conferred by clause (z) of sub-section (2) of section 87, read with sub-section (2) of section 69A of the Information Technology Act 2000, (21 of 2000), the Central Government hereby makes the following rules, namely:

1. **Short title and commencement.**— (1) These rules may be called the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.  
(2) They shall come into force on the date of their publication in the Official Gazette.
2. **Definitions.**— In these rules, unless the context otherwise requires,—
  - (a) "Act" means the Information Technology Act, 2000 (21 of 2000);



# Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

**3. Designated Officer.**— The Central Government shall designate by notification in Official Gazette, an officer of the Central Government not below the rank of a Joint Secretary, as the "Designated Officer", for the purpose of issuing direction for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource under sub-section (2) of section 69A of the Act.

**4. Nodal officer of organisation.**— Every organisation for the purpose of these rules, shall designate one of its officer as the Nodal Officer and shall intimate the same to the Central Government in the Department of Information Technology under the Ministry of Communications and Information Technology, Government of India and also publish the name of the said Nodal Officer on their website.

**5. Direction by Designated Officer.**— The Designated Officer may, on receipt of any request from the Nodal Officer of an organisation or a competent court, by order direct any Agency of the Government or intermediary to block for access by the public any information or part thereof generated, transmitted, received, stored or hosted in any computer resource for any of the reasons specified in sub-section (1) of section 69A of the Act.



# Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

**6. Forwarding of request by organisation.—** (1) Any person may send their complaint to the Nodal Officer of the concerned organisation for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource:

Provided that any request, other than the one from the Nodal Officer of the organisation, shall be sent with the approval of the Chief Secretary of the concerned State or Union territory to the Designated Officer.

THE GAZETTE OF INDIA : EXTRAORDINARY

[PART II SEC. 3(i)]

Provided further that in case a Union territory has no Chief Secretary, then, such request may be approved by the Adviser to the Administrator of that Union territory.

(2) The organisation shall examine the complaint received under sub-rule (1) to satisfy themselves about the need for taking of action in relation to the reasons enumerated in sub-section (1) of section 69A of the Act and after being satisfied, it shall send the request through its Nodal Officer to the Designated Officer in the format specified in the Form appended to these rules.

(3) The Designated Officer shall not entertain any complaint or request for blocking of information directly from any person.

(4) The request shall be in writing on the letter head of the respective organisation, complete in all respects and may be sent either by mail or by fax or by e-mail signed with electronic signature of the Nodal Officer.

Provided that in case the request is sent by fax or by e-mail which is not signed with electronic signature, the Nodal Officer shall provide a signed copy of the request so as to reach the Designated Officer within a period of three days of receipt of the request by such fax or e-mail.

(5) On receipt, each request shall be assigned a number alongwith the date and time of its receipt by the Designated Officer and he shall acknowledge the receipt thereof to the Nodal Officer within a period of twenty four hours of its receipt.



# Form U/R 6(2) of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

**FORM**  
[See rule 6(2)]

**A. Complaint**

1. Name of the complainant : \_\_\_\_\_  
(Person who has sent the complaint to the Ministry/Department/State Govt./Nodal Officer)

2. Address : \_\_\_\_\_  
City : \_\_\_\_\_ Pin Code: \_\_\_\_\_

3. Telephone : \_\_\_\_\_ (prefix STD code)      4. Fax (if any) : \_\_\_\_\_

5. Mobile (if any): \_\_\_\_\_

6. Email (if any): \_\_\_\_\_

**B : Details of website/ computer resource/intermediary/ offending information hosted on the website**  
(Please give details wherever known)

7. URL / web address : \_\_\_\_\_

8. IP Address : \_\_\_\_\_

9. Hyperlink : \_\_\_\_\_

10. Server/Proxy Server address : \_\_\_\_\_

11. Name of the Intermediary : \_\_\_\_\_

12. URL of the Intermediary : \_\_\_\_\_

(Please attach screenshot/printout of the offending information)

13. Address or location of intermediary in case the intermediary is telecom service provider, network service provider, internet service provider, web-hosting service provider and cyber café or other form of intermediary for which information under points (7), (8), (9), (10), (11) and (12) are not available.

# Form U/R 6(2) of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

## C. Details of Request for blocking

14. Recommendation/Comments of the Ministry/State Govt : \_\_\_\_\_  
\_\_\_\_\_

15. The level at which the comments/ recommendation have been approved  
(Please specify designation) : \_\_\_\_\_

16. Have the complaint been examined in Ministry/State Government : Y/N

17. If yes, under which of the following reasons it falls (please tick):

- (i) Interest of sovereignty or integrity of India
- (ii) Defence of India
- (iii) Security of the State
- (iv) Friendly relations with foreign States
- (v) Public order
- (vi) For preventing incitement to the commission of any cognisable offence relating to above

## D. Details of the Nodal Officer forwarding the complaint alongwith recommendation of the Ministry/State Govt. and related enclosures

18. Name of the Nodal Officer: \_\_\_\_\_

19. Designation : \_\_\_\_\_

20. organisation : \_\_\_\_\_

21. Address : \_\_\_\_\_  
\_\_\_\_\_

City : \_\_\_\_\_ Pin Code: \_\_\_\_\_

22. Telephone: \_\_\_\_\_ (prefix STD code) 23. Fax (if any): \_\_\_\_\_

24. Mobile (if any): \_\_\_\_\_

25. Email (if any): \_\_\_\_\_

## E. Any other information :

F. Enclosures :  
1.  
2.  
3.

Date :

Place:

Signature

[No. 9(16)/2004-EC]  
N. RAVI SHANKER, Jt. Secy.



# Designated Officer U/R 3 of Form U/R 6(2) of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

2

THE GAZETTE OF INDIA : EXTRAORDINARY

[PART II—SEC. 3(ii)]

## MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

(Personnel-I Section)

### NOTIFICATION

New Delhi, the 29th October, 2020

**S.O. 4042(E).**—In supersession of this Ministry's Notification No. 1(5)/2009-CLF&E dated 20th January 2010 published in the Gazette of India *vide* S.O. 117(E) dated 20th January 2010 and in exercise of the powers conferred by sub-section (1) of Section 69A of the Information Technology Act, 2000 (21 of 2000) read with rule 3 of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, the Central Government hereby authorises and designates the Director (National Cyber Coordination Centre) (being an officer of the Central Government not below the rank of Joint Secretary), in the Ministry of Electronics and Information Technology, Government of India, Electronics Niketan, 6 Central Government Offices Complex, New Delhi - 110003, as the Designated Officer for the purpose of the said rules.

[F. No. 2(1)/2017-Pers.I]

RAJIV KUMAR, Jt. Secy.

## List of Nodal Officers from Ministries / Departments of Central Governments under the provisions of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

S.No	Ministry/Deptt.	Name	Nodal Officer	Address	Contact Details	Fax	email
1	Council of Scientific & Industrial Research	Sh. A Wahid	Scientist Gr. IV(6)	Anusandhan Bhavan, 2 Rafi Marg, New Delhi-110 001	23320880	-	awahid@cdsir.res.in
2	Defence Dept. of Ex-servicemen Welfare	Sh. M.M. Singh	Deputy Secretary (res - I)	Room No. 237, B-Wing, Sena Bhawan, New Delhi-11	23015772	-	-
3	Defence Research & Development	Dr. A.L. Moorthy	Director DESIDOC	405, Crescent Apartment, Pocket 2, Sector 18A, Dwarka, New Delhi - 110075	23812252, 23802404,	23813465	director@desidoc.drdo.in
4	Delhi Police	-	DCP	Economic Offences Wing, Crime Branch, Delhi Police	011-23364421	-	-
5	Ministry of Law & Justice, Department of Legal Affairs	Sh. C.O. Rajan	Deputy Secretary	Room No. 433A, A-Wing, Shashtri Bhawan, New Delhi-11001	23388763, 23388004	-	-
6	Department of Telecom	Sh. R.S. Rana	Asstt. Director (PG-I)	Sanchar Bhawan, 20 Ashoka Road, New Delhi-1	23036222	23752224	-
7	Department of Agriculture	Ms. Dimple Verma	Director	Room No.284-A, Krishi Bhawan, New Delhi	23386053	-	d.verma@nic.in
8	Department of Biotechnology	Sh. T. Madan	Adviser	Room - 707, Block-2, CGO Complex, New Delhi- 110003	24361813	24362884	-
9	Department of Chemicals & Petrochemicals	Shri Lalsanglur	Economic Adviser	-	23381395	-	lal.sanglur@nic.in
10	Department of Defence Production	Sh. Hazari Lal	Director (B&C)	Room No. 146, B-Wing, Sena Bhawan, New Delhi	23792069	-	-
11	Department of Economic Affairs	Sh. V.K. Sharma	Dy. Secy (Budget Monitoring)	Room No. 238-B, North Block, New Delhi-110001	23095069,	23092883	sharma.vijayk@nic.in
12	Department of Financial Services, Ministry of Finance	Dr. Tarseem Chand	Deputy Secretary	3rd Floor, Jeevandeep, Parliament Street, New Delhi-1	23340673	23742207, 23747019,	-
13	Department of Health & Family Welfare	Sh. Pravin Srivastav	DDG (Stats)	Room No.518-A, Nirman Bhawan, New Delhi	23061238	-	ddg-stats-mohfw@nic.in
14	Department of Posts	Shri K.K.Sharma	General Manager	Centre for Excellence in Postal Technology, Mysuru 570010	-	-	gmcept@indiapost.gov.in
15	Department of Public Enterprises	Sh. G.S. Basran	Dy. Secretary	Room No. 410, Block-14, Public Enterprises Bhavan, CGO Complex, New Delhi-110003	24360736,	-	dsadm-dpe@nic.in



## List of Nodal Officers from Ministries / Departments of Central Governments under the provisions of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

S.No	Ministry/Deptt.	Name	Nodal Officer	Address	Contact Details	Fax	email
16	Department of Revenue, Min. of Finance	Sh. P.V. Subba Rao	Director (Narcotics Control)	Room No 48-A, North Block, New Delhi	23092688	-	pv.subbarao@nic.in
17	DSIR Technology+B7	Sh. Vimal Kumar Varun	Scientist E	Room No. 3, Administrative Block, DSIR, Technology Bhavan, New Mehrauli Road,	26516078	-	vkv@nic.in
18	Indian Space Research Organisation, Dept.of space	Sh. Rajiv Ratan Chetwani	Director, DSIM	Antariksh Bhavan, New BEL Road, Bangalore-560231	080-23415415	080-22172155	rajiv@isro.gov.in
19	International Boundary Directorate (SGO), Survey of India		Director	L-II Block, Brassey Avenue, Church Road, New Delhi	-	-	-
20	Legislative Department, Ministry of Law & Justice	Sh. S.R. Dhaleta	JS & Legislative Counsel	Room No. 430A, A-Wing, Shastri Bhawan, N Delhi-11001	23384832, 26189124	23384832	-
21	Ministry of Food Processing Industry	-	Shri S K Nanda, Under Secretary	Panchsheel Bhawan, Room No 117, August Kranti Marg, New Delhi - 49	-	-	-
22	Ministry of Mines	Sh. V.K. Thakral	Joint Secretary	Shastri Bhawan, New Delhi	23384741	23387937	vkthakral.dom@sb.nic.in
23	Ministry of Petroleum & Natural Gas	Sh. Dependra Pathak	Director (R&A)	Room No. 203, B-Wing, Shastri Bhawan, New Delhi-110 001	23386526,	23074409	dependra.pathak@nic.in
24	Ministry of Power	Sh. M. Ravi Kanth	Joint Secretary	Room No. 202, Shram Shakti Bhawan, Rafi Marg, New Delhi-110001	237148842	23714842, 23717519	-
25	Ministry of Road Transport & Highways	Sh. S.K. Dash	Jt. Secy (T&A)	Transport Bhawan, 1 Parliament Street, New Delhi	-	-	-
26	Ministry of Urban Development	Sh. Vijay Kumar Sharma	Director (Admn)	Room No. 235, "C" Wing, Nirman Bhawan, New Delhi	23061979,	23061379	dir-adm-mud@nic.in
27	Ministry OF COAL	Shri Rajesh Kumar Sinha	Jt. Secretary	Room No. 321-A, Shastri Bhawan, New Delhi-110001	23384887		jsla.moc@nic.in
28	Ministry of Earth Sciences	-	Director	Block-12, CGO Complex, New Delhi - 110003	-	-	-
29	Ministry of Enviroment & Forest	Sh. Alok Agarwal	Deputy. Secretary	Room 122, Paryavaran Bhawan, CGO Complex, Lodi Road, New Delhi-3	-	-	-
30	Ministry of External Affairs	Ms Garima Paul	Under Secretary	Room No. 141, A-Wing, Shastri Bhawan, New Delhi	23387524	-	dsdd@mea.gov.in

## List of Nodal Officers from Ministries / Departments of Central Governments under the provisions of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

S.No	Ministry/Deptt.	Name	Nodal Officer	Address	Contact Details	Fax	email
31	Ministry of Home Affairs (I4C)	Shri Himanshu Pande	DGM	North Block, New Delhi	23093697	-	-
32	Ministry of Information and Boradcasting	Sh. Amit Katoch	Director(BC)	Room No. 761, A-Wing, 7th Floor, Shashtri Bhawan, New Delhi-1	23386394	-	amit.katoch@nic.in
33	Ministry of Shipping	Sh. Ashwani Kumar	Deputy Secretary	Room 428, Transport Bhavan, Sansad Marg, N Delhi-110001	23710220,	23356713	ashwani.hub@nic.in
34	Ministry of Steel	Sh. Sunil Prakash	Dy. Secy	Udyog Bhavan, New Delhi	23063854	23063236	-
35	Ministry of Textile	Sh. Inderjit Singh	Director	Room No. 231, 2nd Floor, Udyog Bhawan, New Delhi	-	-	-
36	Ministry of Water resources	Sh. Srikanta Panda	Director (IT)	627, Shram Shakti Bhawan, Rafi Marg, New Delhi-110001	23714374,	-	dirit-mowr@nic.in
37	Railway Board, Ministry of Railways	Sh. R. B. Das	Executive Director (C&IS)	Rail Bhavan, Raisina Road, New Delhi - 110 001	23384751,	-	edcis@rb.railnet.gov.in
38	Ministry of Tribal Affairs	Dr. Naval Jit Kapoor	Joint Secretary	-	23073489	-	kapoor.naval@gov.in
39	Ministry of Coporate Affairs	Shri Sanjay Jain	Director	-	-	-	-
40	Department of Drinking Water & Sanitation	Shri Rajeev Jauhari	Deputy Secretary	-	24361062	-	rajeev.j@nic.in
41	Department of Higher Education	Shri Syed Ekram Rizwi	Director	Room No.419, C-Wing, Shashtri Bhawan, New Delhi	23383872	-	syed.rizwi@gov.in
42	Ministry Of Defence	Lieutenant Colonel Amit Dhingra	Lieutenant Colonel	Room No.922, Integrated HQ of Ministry of Defence, DHQ PO, New Delhi-110011		-	amit.digra.392n@gov.in
43	Ministry of Toursim	Shri Pankaj Kumar Devrani	Under Secretary	IT Division , Transport Bhawan,1 Parliament Street, New Delhi	23311237	-	pankaj.devrani@gov.in
44	Ministry of Women and Child Development	Shri. S.Sasikumar	Joint Director	Room No. 434, A-Wing, Shastri Bhawan, New Delhi-110001	011-23385691	-	sasikumar.s@gov.in

## List of State Nodal Officers under the provisions of Section 69A Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

S.No	State/UT	Name	Nodal Officer	Address	Contact No.	Fax (if any)	e-mail address
1	A & N Islands	Sh. A. James	OSD(IT)-2	IT Section, A&N Admin., Govt. Polytechnic Campus, Junglighat (P.O.), Pahargaon, Port Blair-744 103	03192-232820	03192-250587	james@and.nic.in
2	Andhra Pradesh	Smt. M Sailaja	Special Officer	Room No. 208, A-Block, IT&C Department, A.P. Secretariat, Hyderabad-500022	040-23456408	040-23451092	so_portal_itc@ap.gov.in
3	Arunachal Pradesh	Dr. Navdeep Singh Brar, IPS	Superintendent of Police	Police Headquarters, Itanagar	0360-2291363	-	spsit@arunpol.nic.in
4	Bihar	Sh. Rahul Singh	Secretary	Department of Information Technology, 2nd Floor, Technology Bhawan, Bailey Road, Patna - 800015	0612-2545315	0612-2545316	prsec_it@bihar.gov.in
5	Chandigarh	Sh. Arjun Sharma, IAS	Director Information technology,	Department of Information Technology, 5th Floor, Addl. Delux Building, Sector 9, Chandigarh - 160009	0172-2740641	0172-2740005	dit-chdut@nic.in
6	Chhattisgarh	Sh. Vinod Kumar Gupta	Chief Executive Officer	CHIPS office, IT & BioTech Department, Mantralaya, D.K.S. Bhawan, Raipur-492001	0771-4066205	0771-4066205	ceochips@nic.in
7	D&N Haveli	Sh. B.S. Jaglan	Director (IT)	Room No. 207-208, Secretariat, Amli, Silvassa-396 230	0260-2640351	0260-2640351	-
8	Delhi NCT	Dr. Vasanthkumar	Secretary, IT	Department of IT, GNCTD, 9th Floor, Delhi Secretariat, IP Estate, New Delhi-110002	011-23392061	-	-
9	Goa	-	The Director	Dept. of IT, 'IT Hub', 2nd floor, Altinho, Panaji, Goa - 403001	0832-2221505 / 2221509	0832-2221490	dir-dit.goa@nic.in
10	Gujarat	Sh. Dhananjay Dwivedi, IAS	Secretary	Science & Tech. Dept.. Block - 7, 5th Floor, New Sachivalaya, Gandhinagar- 382 010	079-23259999	079-23250325	secdst@gujarat.gov.in

## List of State Nodal Officers under the provisions of Section 69A Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009


11	Haryana	Sh Vijayendra kumar,	Secretary to Govt. of Haryana, Electronics & Information	SCO 109-110, 2nd Floor, Sector 17B, Chandigarh	0172-2704922	0172-2705529	madhartron-hry@gov.in, ssit@hry.nic.in
12	Himachal Pradesh	Sh. Rajeev Sharma	Joint Director (IT)	-	0177-2628914	-	rajeev.sharma@hp.gov.in
13	Jammu & Kashmir	-	Inspector General of Police, CID, J&K	Govt of J&K, Information Technology Department, Civil Secretariat, Jammu/Srinagar	-	-	dspsmi.cid@jkpolice.gov.in
14	Jharkhand	Sh. Amitabh Kumar	Regional Dy. Director	Revenue & Land Reforms Department, Project Bhawan, Dhurva, Ranchi-834002	0651-2400930	0651-2401083	-
15	Karnataka	Sh. H.S. Shankar	Project Officer	HRMS Project, Room No. 145-A, M.S. Building, Gate No. 2, Dr. B R Ambedkar Veedhi, Bangalore 560001	080-22372410, 22032547	080-22259109	srprog3-egov-dpar@karnataqka.gov.in
16	Kerala	-	Principal Secretary	Information Technology Department, Central Secretariat, Trivandrum - 695 001	0471-2327438	0471-2314284	secy@it.kerala.gov.in
17	Lakshadweep	Sh. Puneet Kumar Patel, DANICS	Director (Information Technology)	Department of Information Technology, Administration of the UT of Lakshadweep, Kavaratti - 682 555	04896-263168	-	lak-dit@nic.in
18	Madhya Pradesh	Shri Pramod Agrawal	Principal Secretary	Department of Science & Technology, Govt. Of Madhya Pradesh	0755-2441025	-	psit@mp.gov.in
19	Maharashtra	Sh. Sanjay Barve	Commissioner State Intelligence Deptt. Mumbai	Old council road, 2nd floor, Shahid Bhagatsingh Marg, Colaba, Mumbai-400001	022-22024161	-	-
	Maharashtra	Sh. Sanjay Saxena	Jt. Commissioner of Police	Annex-II bldg, 1st floor, Crawford market, D.N.Road, Mumbai- 400001	022-22620406	-	cp.mumbai.jtcp.crime@mahapolice.gov.in
	Maharashtra	-	Special IG Police (West), CID, Pune, Maharashtra	Criminal Investigation Department, Maharashtra State, Near Modern Law College, Pune University Chowk, Chavannagar,	020-25638441	-	-

## List of State Nodal Officers under the provisions of Section 69A Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

S.No	State/UT	Name	Nodal Officer	Address	Contact No.	Fax (if any)	e-mail address
20	Manipur	N. Deben	Additional Director(IT), Government of Manipur	Department of Information Technology, 4th Floor, Western Block, New Secretariat, Imphal-795001		-	n.deben@nic.in
21	Meghalaya	Sh. B. Tiwari	Special Officer	Information Technology & Communication Department, Government of Meghalaya, NIC Building, Ground Floor,	-	-	-
22	Mizoram	Dr. Lalthlamuana	Chief Informatics Officer & JS, Department of ICT, Govt. Of	Mizoram Secretariat Annexe - I, Third floor, Treasury Square,Aizawl - 796001, Mizoram	0389- 2319637	0389-2319632	muana.mizo@gmail.com
23	Nagaland	Sh. K.T. Sukhalu	Secretary IT&C	Nagaland Civil Secrétariat, Kohima - 797004	0370-2270253	0370-2270430	-
24	Odisha	Sh. Saroj Kumar Tripathy	DGM	Orissa Computer Application Centre, OCAC Building, Plot N/1-7D, Acharya Nagar, PO-RRL. Bhubaneswar-751013	0674-2588295, 2588083, 2588280	0872-2582842	saroj.tripathy@ocac.in
25	Puducherry	Sh. A.S. Sivakumar	Director (IT)	Directorate of IT, No. 505 Kamraj Salai, PRD Complex, Saram, Puducherry - 605 013	0413-2246090	0413-2246090	dir.pon@nic.in
26	Punjab	-	Director	Department of Governance Reforms, D-241, Near Quark city, Industrial Area Phase-8B, Mohali.	0172-2970868	-	dgr@punjab.gov.in
27	Rajasthan	Sh. A.M. Deshpande	Technical Director & Jt. Secretary	IT Building, Yojana Bhawan, Tilak Marg, Jaipur, Rajasthan	0141-2228544	-	amdeshpande@rajasthan.gov.in
28	Tamil Nadu	The Superintendent of Police	Crime Branch - Criminal Investigation Department	No. 220, Pantheon Road, Egmore, Chennai - 600 008.	044-28511600	044-28512510	cbcyber@nic.in
29	Telangana	Sh. Rajiv Trivedi, IPS	Principal Secretary to Govt, Home Department	Secretariat, Government of Telengana, Hyderabad	040-23452143	-	prlsecy_home@telengana.gov.in
30	Tripura	Apurba Roy	Director (IT)	Directorate of Information Technology, Govt. of Tripura, ITI Road, Indranagar, Agartal, Tripura(W), PIN-799006	0381-235-5751	0381-235-5751	itdept-tr@gov.in
31	Uttar Pradesh	-	Special Secretary	IT & Electronics Dept., Babu Bhawan, II Floor, No. 209, U.P. Admn. Lucknow	-	-	-
32	Uttarakhand	-	Uttra Portal Subject Specialist	ITDA, 93, Phase-II, Vasant Vihar, Dehradun	-	-	-
33	West Bengal	Shri Surajit Kumar Dey	Special Superintendent of Police	Crime Investigation Department, Bhabani Bhaban, 31 Belvedere Road, Alipore, Kolkata - 700027	33-24490254	-	nodal1cyber@cidwestbengal.gov.in



# Digital Platforms Are Also Responding to Direct Requests Made By Enforcement Officials

 Gmail Kirupa Sankar <kirupasha@gmail.com>

---

**(no subject)**  
2 messages

**YouTube Legal Support Team** <legal+1cqzfiijd2e530j@support.youtube.com> Fri, May 7, 2021 at 7:22 AM  
Reply-To: YouTube Legal Support Team <legal+1cqzfiijd2e530j@support.youtube.com>  
To: kirupasha@gmail.com

Hello,

We received your YouTube complaint and sent it for review. We will get back to you as soon as possible.

Regards,

The YouTube Legal Support Team

On May 6, 2021 Contact Us Form wrote:

```
Country: IN
Fulllegalname: Kirupasankar M Regional Deputy Director Wildlife Crime
Control Bureau SR Chennai Govt of India
behalf: self
email_prefill: kirupasha@gmail.com
cite_law: Wildlife Protection Act, 1972
hyperlink: https://legislative.gov.in/sites/default/files/A1972-53_0.pdf
content_issue: other
other_url: https://youtu.be/hw9961QaXXY
content: Youtube video (https://youtu.be/hw9961QaXXY) shows hunting of
monitor lizard in forest area allegedly in the state Tamil Nadu, India.
These activities are illegal with respect to Wildlife Protection Act, 1972
of the Government of India. Persons shown and associated with this video
have committed offences under section 2, 9, 39,44,49B of the Act and are
liable to be punished under Section 51 of the act.
```

Therefore, it is requested to provide the details of the persons uploaded/ in the video, so that legal proceedings against them can be initiated. Further, it is pertinent to mention here that the Publication of this video promotes the commission of such offenses against the Wildlife by innocent viewers and may also induce criminality among the community through Youtube. Therefore, it is requested to immediately stop the publication of this video on Youtube and render support for the prosecution of the offenders involved in the commission.

affirmation\_one: I declare that the information in this notice is true and complete.

Signature: Kirupasankar M



# Digital Platforms Are Also Responding to Direct Requests Made By Enforcement Officials



Kirupa Sankar <kirupasha@gmail.com>

(no subject)

1 message

YouTube Legal Support Team <legal+0ecvm1an27nc40j@support.youtube.com>  
Reply-To: YouTube Legal Support Team <legal+0ecvm1an27nc40j@support.youtube.com>  
To: kirupasha@gmail.com

Fri, May 7, 2021 at 12:40 PM

Hello,

After review of your legal complaint, the content in question has been blocked from view on the country domain.

Regards,

The YouTube Legal Support Team

On May 6, 2021 Contact Us Form wrote:

Country: IN  
Fulllegalname: Kirupasankar M Regional Deputy Director Wildlife Crime Control Bureau SR Chennai Govt of India  
behalf: self  
email\_prefill: kirupasha@gmail.com  
cite\_law: Wildlife Protection Act, 1972  
hyperlink: [https://legislative.gov.in/sites/default/files/A1972-53\\_0.pdf](https://legislative.gov.in/sites/default/files/A1972-53_0.pdf)  
content\_issue: other  
other\_url: <https://youtu.be/dtkuggwWAHw>  
content: Youtube video (<https://www.youtube.com/watch?v=dtkuggwWAHw&amp;t=273s>) shows hunting of Monitor Lizard in forest area in the state Tamil Nadu, India. These activities are illegal with respect to Wildlife Protection Act, 1972 of Government of India. Persons showed/ associated in this video are liable to be punished under sections 2, 9, 39, 44, 49B and 51 of the Act for 3-7 of imprisonment.

Further, it is pertinent to mention here that the video has been uploaded on 04/11/2020 and 262,186 times viewed by public. Publication of this video promotes the commission of such offences against the Wildlife by innocent viewers and may also induce criminality among the community through Youtube. Therefore, it is requested to immediately stop publication of this video on Youtube.

Dr. Kirupasankar M, IFS  
Regional Deputy Director cum  
Assistant Management Authority of CITES,  
Government of India.  
C2A, Rajaji Bhavan, Besant Nagar,  
Chennai- 600 090, Tamil Nadu, India.  
E-mail: [rddsr@wccb.gov](mailto:rddsr@wccb.gov)

affirmation\_one: I declare that the information in this notice is true and complete.  
Signature: Kirupasankar M

https://www.youtube.com/watch?v=dtkuggwWAHw

YouTube

Search

Video unavailable  
This content is not available on this country domain due to a legal complaint from the government.

#Villagevettaikaran  
உடும்பு வேட்டை | உடம்பு பிடித்து சமையல் | உடும்பு கறி | village vettaikaran

966,796 views • Nov 4, 2020

LIKE DISLIKE SAVE ...



# DARKNET & CRYPTOCURRENCY: A Challenge For Digital Forensics



## Cryptocurrency

*A type of digital money with an encryption that makes it secure. Users of the currency remain anonymous.*





### Ivory Rhino Horn

Price: \$ 250000 / 23.251613 BTC

[send message](#) [view profile](#)

**Ivory Rhino Horn**

Price: \$ 250000

Vendor: [\[View Listings\]](#) peterclark +10, 0, 100% New Vendor PGP Verified

Payment method: **Escrow**

Ships From: sweden

Category: Others

Stock Remaining: 87568

**Ivory Rhino Horn**

Ivory Rhino Horn

weight: 2.550kg  
length: 64cm

\$250000 (two hundred fifty thousand us dollars)

more info: [elfenben@protonmail.com](mailto:elfenben@protonmail.com)

Place Order





Silk Road 3.1  
the darknet's most resilient marketplace

[home](#) [messages](#) [notifications](#) [profile](#) [orders](#) [support](#) [wallet](#) [settings](#) [uchat](#) [faq](#) [forums](#) [logout](#)

[TBP](#) [TBS](#) [TBD](#) [last unread comment](#) [last unread pm](#) [tickets summary](#)

Welcome back comrades

You may now place your orders and pay for the order as instructed.  
(We are aware that there was a issue with wallets not being credited, if you sent BTC to your wallet and never was credited, please open a support ticket and we will resolve this for you.)



### 2gr Good Quality Cocaine 70%75%

Price: \$ 92 / 0.007019 BTC

Highly Sold

[send message](#) [view profile](#)

2gr Good Quality Cocaine 70%75%

Price: \$ 92

Vendor: [\[View Listings\]](#) Amsterdam2015 +18271, 620, 97% Level 5 ★★★★★ PGP Verified

Payment method: Finalize Early (FE)

Ships From: Netherlands

Category: Cocaine

Stock Remaining: 87567

**2gr Good Quality Cocaine 70%75%****Price: \$ 92**Vendor: [View Listings] Amsterdam2015 **+18271, 620, 97%** **Level 5 ★★★★★** **PGP Verified**Payment method: **Finalize Early (FE)**

Ships From: Netherlands

Category: Cocaine

Stock Remaining: 87567

**2gr Good Quality Cocaine 70%75%**

Good Quality Cocaine

We strive to offer the best service possible and will send your packages fast and with stealth

Here for the long term. We offer quality products at a fair price.

Arrives in stealth, by express post. Please encrypt your address and write it exactly as you need it on the envelope.  
Please send any sensitive information using the PGP key  
Feel free to contact us if you have any questions

-When ordering, please send me your adress info.  
like shown below . (All information will be deleted after shipment. )

name:  
address:  
city and postal code/zip:  
country:

## Place Order

Standard quantity is 1. More than 1 will multiply the listing price.

Quantity

Shipping Address  
Addresses are encrypted by Silk Road automatically with vendor's PGP.  
Please use this format for the shipping address:  
  
Natalia Evan  
40 Main Street  
Long Island, New York  
50492  
United States

Shipping Address

Additional Info

Shipping Option

If the vendor has given a discount code use it here.

Discount Code (Optional)

This will be a FE order.

Place Order

## Your order with Amsterdam2015

*Open a support ticket for this order*

# WAITING FOR BUYER TO PAY

Buyer please send exactly **0.007059 BTC** to 3CcpCbqsSomKGUr2mNd39AeViHPYqgAvAS

**BUYER MAKE SURE TO PAY THE BITCOIN NETWORK MINING FEE!**

Cancel This Order

Check For Payment

~~~~~PAYMENT STATUS~~~~~

Pay address: 3CcpCbqsSomKGUr2mNd39AeViHPYqgAvAS

Amount to send: 0.007059 BTC

Amount received (unconfirmed): BTC

Amount received (confirmed): BTC

**Remaining amount to pay: 0.00705900 BTC**

Buyer: **1234567890qaz**

Vendor: **Amsterdam2015**

Order: (1x) **2gr Good Quality Cocaine 70%75%**

Shipping method: World Wide

Add-Ons:





Silk Road 3.1  
the darknet's most resilient marketplace

[home](#) [messages](#) [notifications](#) [profile](#) [orders](#) [support](#) [wallet](#) [settings](#) [uchat](#) [faq](#) [forums](#) [logout](#)

[TBP](#) [TBS](#) [TBD](#) [last unread comment](#) [last unread pm](#) [tickets summary](#)

[Welcome back comrades](#)

You may now place your orders and pay for the order as instructed.  
(We are aware that there was a issue with wallets not being credited, if you sent BTC to your wallet and never was credited, please open a support ticket and we will resolve this for you.)

24 HOUR DEPOSIT PROMO!

All deposits of 0.03 BTC or higher will be doubled!

The bonus amount can only be used towards a order and can't be withdrawn.

The max that can be deposited and doubled is 0.1 BTC and it can only be done once

35xmYkSztc4HVb38ShBLHXaa5QasnDrdgF

The above address is your BTC market wallet deposit address.

### Transactions

IDBTC Address Amount Received Date Requested Status

No records found.

### Withdraw Funds

Your exact balance: 0.00000000 BTC (USD 0.00)

## CASE STUDY 1 - INDIA

### Wildlife trade on the Darknet

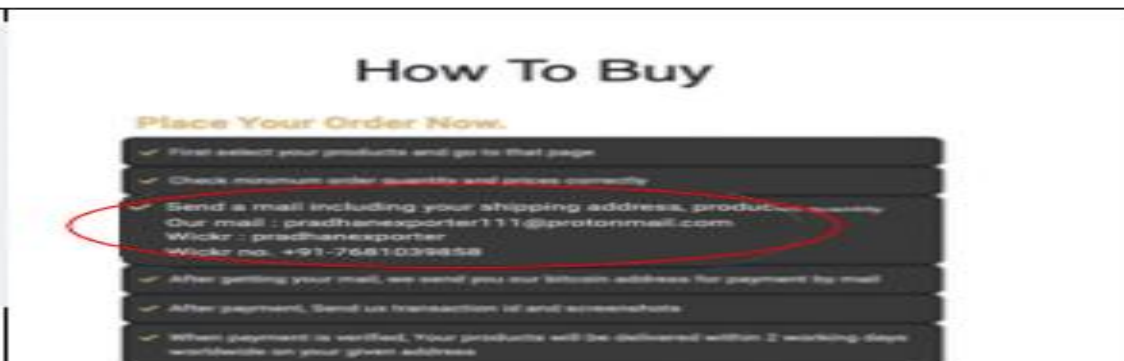
In 2020, with the support of the INTERPOL Cybercrime Directorate and the Innovation Centre, searches were conducted on the Darknet.<sup>16</sup> The purpose of this research was part of a request to INTERPOL from its National Central Bureau (NCB) in Delhi, in order to share information about the online sale of a number of wildlife iconic species. By linking Darknet and Clear web user' accounts it is possible for law enforcement authorities, to conduct a more complete investigation, and identify other criminal activities undertaken by wildlife traffickers. This full picture helps member countries to identify online wildlife traffickers for enforcement actions.

#### Tor Onion page

The below information was accessible on tor Hidden Service: <http://p3nwp6tkzd47gsq.onion> and is offline since 29 December 2019.



**Figure 2:** Screenshot of the onion hidden service home page Pradhan Exporter



**Figure 3:** Screenshot of the page displaying the instructions

From this data, we can extract information and companies that can be subpoenaed:

Proton Mail provider -> Switzerland  
Telephone number cc +91 -> India  
Wickr – Instant Messaging -> USA

<sup>16</sup> The content is stored in order to be further searched and retrieved. However, dynamic web content, some databases, and blocked or private sites that require specific authorization all represent a sector that cannot be indexed. This is called the Deep Web. Within the Deep Web, there is the Darkweb (a collection of websites) that runs on overlay networks, which are defined as the Darknet. The most notable example of these overlay networks is Tor (The Onion router). A specific piece of software, the Tor Browser, is required to access hidden services and browse anonymously using the Tor network. (INTERPOL – Illegal Wildlife Trade in the Darknet, 2017)

The Pradhan Exporter hidden service advertises the sale of counterfeit bills, rice puller coin, animals and fake documents. The animals' category included: Royal Bengal Baby tiger, Double headed snake, Pangolin, Elephant Ivory and Stag Beetle.

Additional analysis of the *Onion Service frequently asked questions "FAQ page"*, revealed that payments could be made in Bitcoins, Ethereum, Bitcoin Cash or from a skrill wallet<sup>17</sup>.

The *FAQ page* also makes reference to **Cash Gold**.<sup>18</sup>

*Transcript:*

Question: "are you legit"

Answer: "If by "legitimate ", you mean "a real company", then yes. Cash God is a real cash selling company. We have successfully met more than 5.000 orders since early 2019".

It is noticeably unusual to find a reference to another illegal service and actor inside the *FAQ page*.

In November 28, 2019, another Hidden Service available at: "<http://p3nwk2avgctcfw4dl.onion>"<sup>19</sup> was advertising similar products with the exact same *FAQ page* but with different contact details: [p3nwpc6tkzd47gsq@email4tor.com](mailto:p3nwpc6tkzd47gsq@email4tor.com) and Wickr pro: [p3nwpc6tkzd47gsq@email4tor.com](https://www.wickr.com/pro/p3nwpc6tkzd47gsq@email4tor.com). It is noticed how the email moniker is a reference to the other Onion URL.

### Real world or Clearnet links

Additional OSINT searches revealed the below Instagram account under "Pradhanexporter".



Figure 4: Screenshot of Instagram account "Pradhanexporter"

<sup>17</sup> It is PaySafe Payment Solutions provider operating under the Central Bank of Ireland, [www.skrill.com](http://www.skrill.com), last accessed on 20 April 2021.

<sup>18</sup> O Cash Gold is a criminal group claiming to be based in the United States and selling real USD banknotes deemed unfit (quote: "100% real USD Currency stolen from the FED before it could be shredded"). One such god cash onion was hosted at <http://cashilnjsubk5go.onion/faq.html>, last accessed on 20 April 2021.

<sup>19</sup> <https://onionlandsearchengine.com/v?q=access+hilton+hotel+certificate+documents&l=http%253A%252F%252Fp3nwk2avgctcfw4dl.onion&p=62&u=294004736&strip=0&vwsr=0>, last accessed on 20 April 2021.





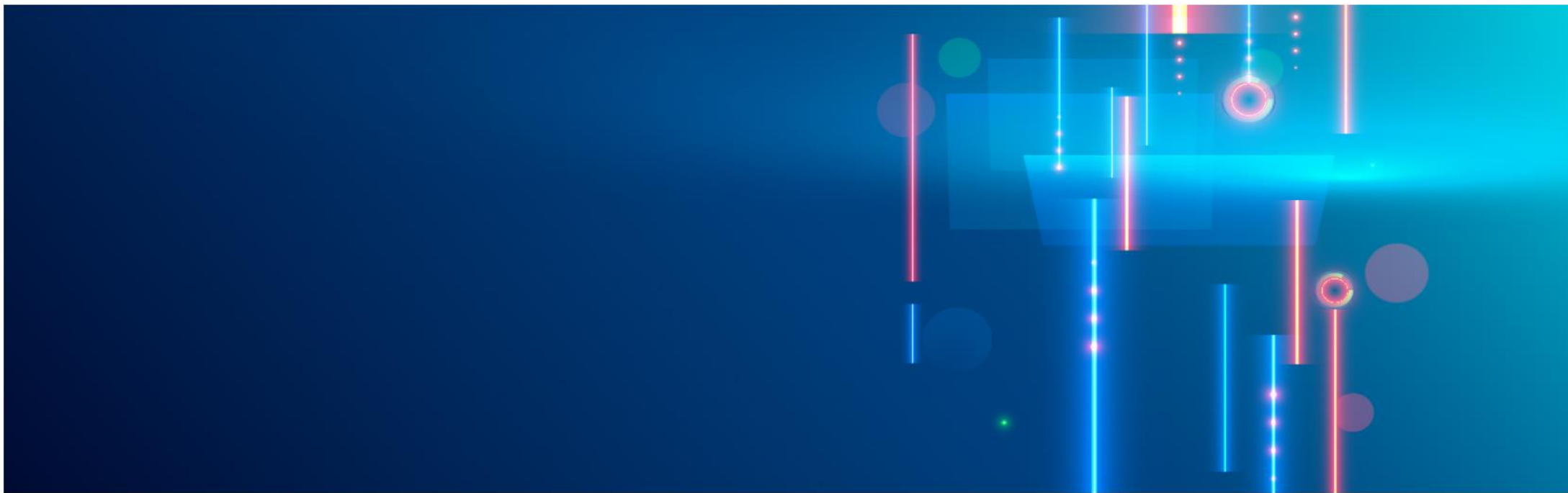
**Figure 5:** Screenshot of an Instagram post by “deepweb127”, displaying a comment by user “pradhnexporter” with the same Indian phone number as the one used on the onion hidden service

The searches were made on marketplaces and websites on anonymous networks, as well as on Clearnet platforms. The collected information detected several illegal activities, such as counterfeit money, illicit wildlife trade and forged documentation. INTERPOL submits this type of alerts via its NCBs who coordinate with National Cybercrime Labs and other cyber specialized units to follow up and take any operational actions they deem necessary.

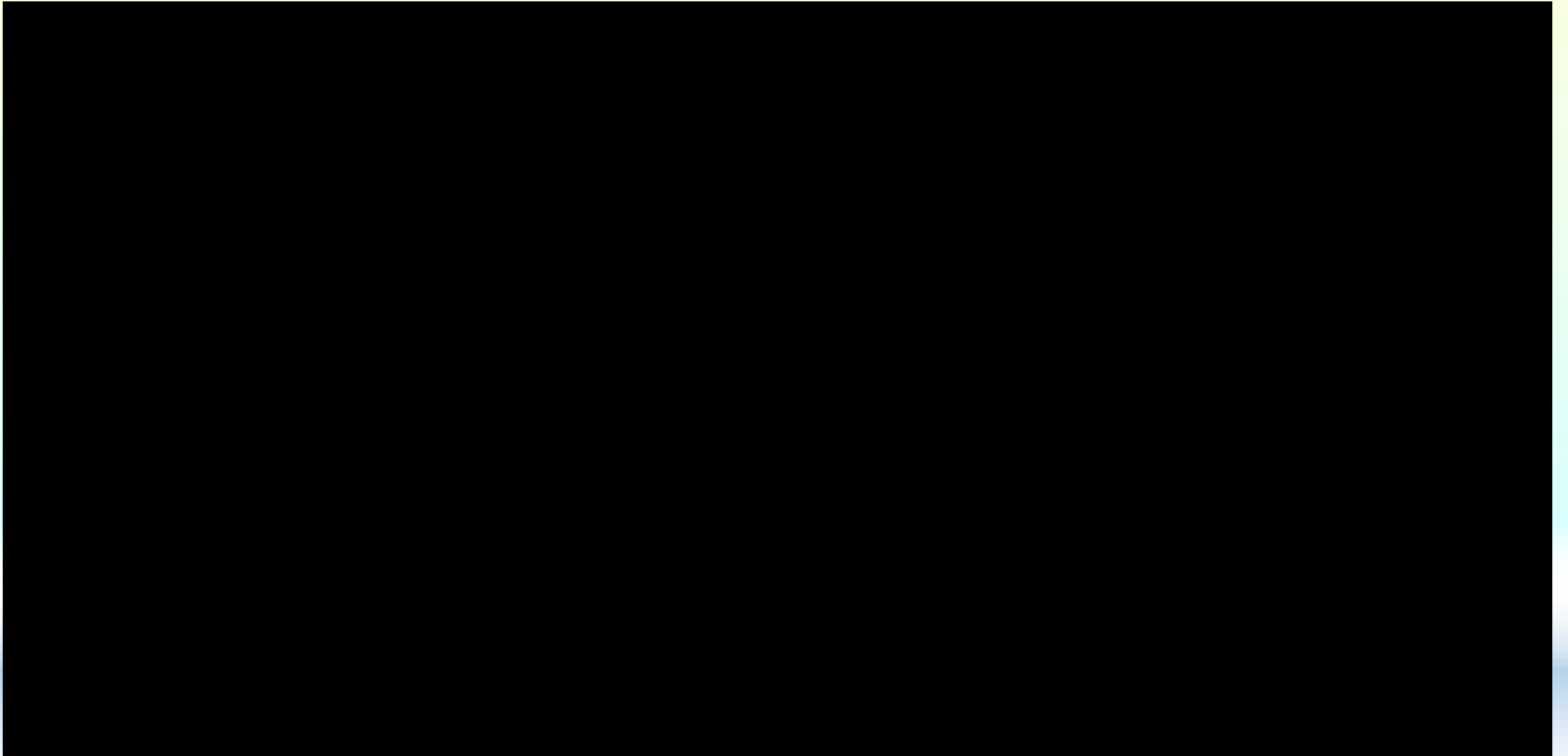




About us ▾ Tools & Resources ▾ Contribute ▾ Contact us ▾



# UNODC EXECUTIVE DIRECTOR MESSAGE





## The Practical Guide for Requesting Electronic Evidence across Borders

The *Practical Guide for Requesting Electronic Evidence Across Borders* provides practitioners with best practice from experts in the field, legal procedures from States, and contact points to assist practitioners on how to request and produce the electronic evidence needed for trial. Both, the 2018 and 2021 editions of the Practical Guide can be accessed by registered users of the CNA Directory. Access to the CNA Directory is reserved to central and competent national authorities and Permanent Missions to the United Nations.



As a result of the success and increased interest in the 2018 edition of the Practical Guide, UNODC will launch in 2021 an updated version which encompasses the latest development in this fast-evolving area of expertise.

### REQUEST AN ACCOUNT

Request an account

### DOWNLOAD THE PRACTICAL GUIDE (COMING SOON)

English

### SERVICE PROVIDERS MAPPING

Download

### 1ST EDITION OF THE PRACTICAL GUIDE (2018)



The first edition of the Practical Guide was developed by UNODC in 2018 and is currently still accessible to registered users.

English French Russian Spanish Portuguese



## Model Forms on Preservation and Disclosure of Electronic Data

A set of three stand-alone model forms on preservation of electronic data, voluntary disclosure, and emergency disclosure. These model forms are conceived as a tool for ready use by national authorities seeking to send data request to service providers.

Emergency Disclosure Request

Request for the preservation of electronic data

Voluntary Disclosure Request





## Model Mutual Legal Assistance Resources

This section includes standardized templates, checklists and model provisions on mutual legal assistance involving electronic evidence.

These model resources have been developed considering good practices and the need to foster harmonized mutual legal assistance practices. It is also the place where to find updates on the ongoing process of updating the [UNODC Model Law on Mutual Legal Assistance in Criminal Matters](#).

### MODEL MLAR FOR STORED ELECTRONIC EVIDENCE

---

[Model\\_MLAR\\_for\\_stored\\_electronic\\_evidence.pdf](#)

### MODEL MLAR FOR REAL-TIME COLLECTION OF TRAFFIC DATA OR CONTENT DATA

---

[Model\\_MLA\\_request\\_for\\_real-time\\_collection\\_of\\_traffic\\_data\\_or\\_content\\_data.pdf](#)

### MLA REQUEST CHECKLIST

---

[MLA\\_Request\\_Checklist.pdf](#)

 **Case Law Database** ▼



- ▼ **Country** 1
  - India 5
- ▼ **Crime Type** 1
  - Crimes that affect the environment 5
- ▼ **Date of Offending** 2
  - 1996 1
  - 2003 1
- ▶ **Decision/Verdict Date** 6
- ▼ **Sentenced Date** 5
  - 1997 1
  - 2003 3
  - 2007 1
  - 2011 1
  - 2014 1
- ▼ **Defendant's Gender** 1
  - Male 1
- ▼ **Verdict** 1
  - Guilty 1
- ▼ **Court** 3
  - Delhi High Court 3
  - Madhya Pradesh High Court 1
  - Supreme Court of India 3
- ▼ **Legal System** 1
  - Common Law 5
- ▼ **Latest Court Ruling** 2
  - High Court 4
  - Supreme Court 4
- ▼ **Type of Court/Tribunal** 2
  - Administrative 2
  - Civil 5


Search Cases 🔍

Additional criteria:

**Crime Type: Crimes that affect the environment** × **Country: India** ×


Found 8 cases [Clear all search criteria](#)

- INDx007**     **Hasan Khan v State of Madhya Pradesh**

 India Verdict Date: 2014-04-15  
Sentence Date: 2014-04-15


A charge sheet dated 28-12-2014 was issued to the appellant. Certain charges were leveled against the appellant pertaining to his conduct. It is said that while performing duties in the control room on 17-01-2014, in an illegal manner, the appellant went from his duty place and was involved in illegal hunting of forest animal in violation to the M.P. Police Regulation. Similar allegations are made with regard to unauthorized absence from duty. Inter alia contending that the allegations did not constitute misconduct

[Show more ...](#)
- INDx005**     **Princl. Conservator of Forests v J.K. Johnson & Ors.**

 India Verdict Date: 2011-10-17  
Sentence Date: 2011-10-17

The question raised in this appeal is: whether a specified officer empowered under Section 54(1) of the Wild Life (Protection) Act, 1972 as amended by the Wild Life (Protection) Amendment Act, 2002 (Act 16 of 2003) to compound offences has power, competence and authority, on payment of a sum of money by way of composition of the offence by a person who is suspected to have committed offence against the Act, to order forfeiture of the seized items.

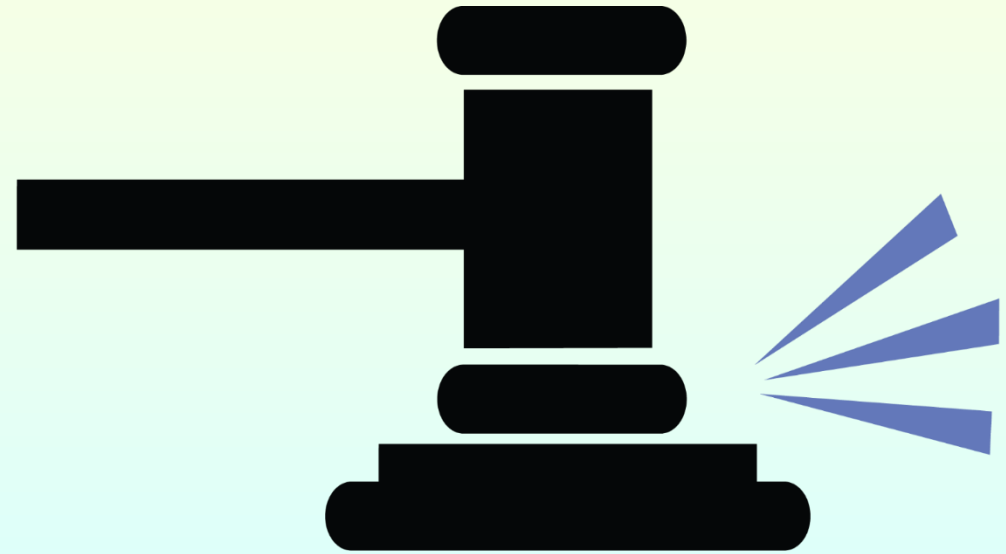
[Show more ...](#)
- INDx001**     **Sansar Chand v Rajasthan**

 India Verdict Date: 2010-10-20

No text
- INDx002**     **Cottage Industries Exposition v Union Of India And Ors.**

 India Verdict Date: 2007-09-03  
Sentence Date: 2007-09-03

On 6th April 1996, 16th April 1996 and 12th May 1996, M/s Istihaq & Co. supplied various types of shawls to the petitioner company. The supplies included shawls which have been seized by the respondent. On 7th November, 1996, the petitioner No. 2 made arrangement for the export of the



# CASE LAW

# Case Law1:Anvar P.V vs. P.K Basheer , *2014(10) SCC 473*

The Supreme Court observed that electronic evidence by way of primary evidence was covered by Section 62 of the Indian Evidence Act to which procedure of Section 65B of the Act was not admissible. However, for the secondary evidence, procedure of Section 65B of the Act was required to be followed.



## Case Law 2: Shradha Shipping Co. v. Adhithri Trading Co, 2014 SSC OnLine Bom 2273

Certificate under section 65B of the Evidence Act must be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) so that the electronic record produced can be taken as admissible evidence. Hence, **private consultant with no responsible official position and no free access to computer cannot issue a 65B certificate.**

# Case Law 3: Shafi Mohammad vs. State of Himachal Pradesh, Special Leave Petition (Crl.) No. 2302 Of 2017

**The Supreme Court observed –**

- The applicability of the procedural requirement under Section 65B(4) of the Act of furnishing a certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such a certificate being in control of the said device and not of the opposite party.
- A person who is in possession of authentic evidence but on account of manner of proving, such document is kept out of consideration by the court in absence of certificate under Section 65B(4) of the Evidence Act, which party producing cannot possibly secure, will lead to denial of justice.
- *A party who is not in possession of a device from which the document is produced cannot be required to produce a certificate under Section 65B (4) of the Act. Thus, the requirement of certificate under Section 65B is not always mandatory.*

# Case Law4: Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal, CA nos. 20825-20826 of 2017

- Is Requirement of Certificate U/s 65-B(4) of the Indian Evidence Act Mandatory for Production of Electronic Evidence?
- In this Order of Apex Court of 2019, Shafi judgment of Apex Court(Sr No.06 ) was cited and the matter was referred to Larger Bench for reconsideration, in view of conflicting precedent in Anvar P V case (Sr. No. 01)

# Case Law5:Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020 SCC OnLine SC 571 , decided on 14.07.2020

- **Supreme Court** in a reference dealing with the interpretation of Section 65B of the Evidence Act, 1872 that deals with admissibility of electronic records, the 3-judge bench of RF Nariman, S. Ravindra Bhat and V. Ramasubramanian, JJ has held that the certificate required under Section 65B(4) is a condition precedent to the admissibility of evidence by way of electronic record, as correctly held in by the 3-judge bench in Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, and incorrectly “clarified” by a division bench in Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
- The Court further clarified that the required certificate under Section 65B(4) is unnecessary if the original document itself is produced.



The 3-judge bench in the present case, holding the [Shafhi Mohammad judgment](#) to be incorrect said,

“the major premise of [Shafhi Mohammad \(supra\)](#) that such certificate cannot be secured by persons who are not in possession of an electronic device is wholly incorrect. *An application can always be made to a Judge for production of such a certificate from the requisite person under Section 65B(4) in cases in which such person refuses to give it.*”

Clarification on [Anvar P.V. case](#):

*“the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him.* In cases where the “computer” happens to be a part of a “computer system” or “computer network” and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4).”

# Stage Of Furnishing The Certificate To The Court

*The Court also took note of the fact that Section 65B does not speak of the stage at which such certificate must be furnished to the Court, and said that in cases where such certificate could be procured by the person seeking to rely upon an electronic record, such certificate must accompany the electronic record when the same is produced in evidence. However, in cases where either a defective certificate is given, or in cases where such certificate has been demanded and is not given by the concerned person, the Judge conducting the trial must summon the person/persons referred to in Section 65B(4) of the Evidence Act, and require that such certificate be given by such person/persons. This, the trial Judge ought to do when the electronic record is produced in evidence before him without the requisite certificate in the circumstances aforementioned.*

# NEVER DO THIS AS IT FACILITATES WILDLIFE POACHING





**OVERDOSE IS  
INJURIOUS TO  
HEALTH**

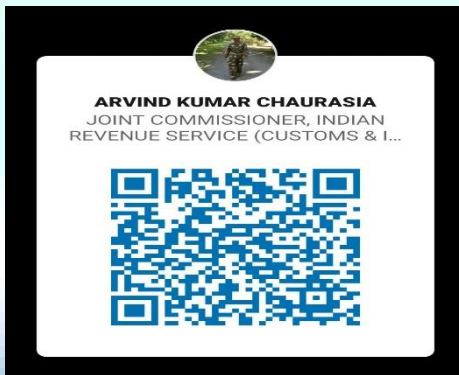






# FOLLOW ME

<https://www.linkedin.com/in/arvind-kumar-chaurasia-1b2b791b9/>



<https://twitter.com/ArvindK43241589>

# Contact Me



[+918141130511](tel:+918141130511)

[ARVIND.IRS@GOV.IN](mailto:ARVIND.IRS@GOV.IN)