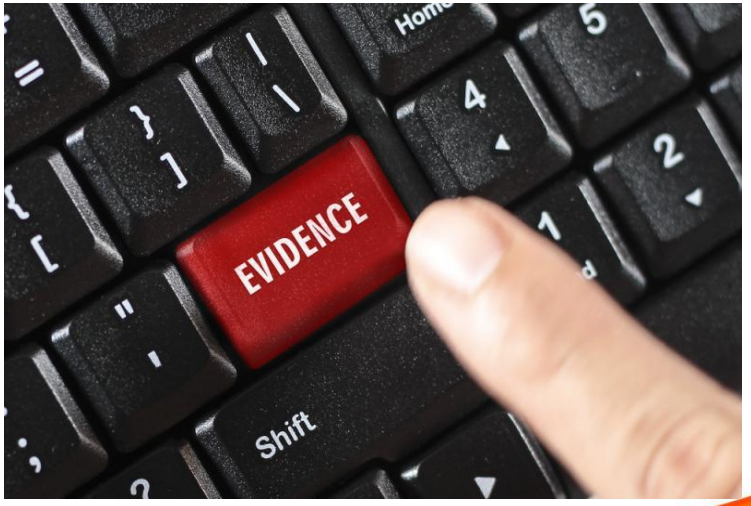
CYBER CRIMES, SECURITY AND FORENSICS



M. KRISHNA

M.Sc, M.Tech(IT),GCIH(SANS), CPE, CHFI, PGDCL

Asstt Director and HoD,

DIGITAL FORENSIC DIVISION,CFSL, HYDERABAD.

DIRECTORATE OF FORENSIC SCIENCE, (MHA)

OVERVIEW

- *Background*
- *Cyber crimes*
- *Cyber Security*
- *Cyber forensics*
- *Conclusions*

INFORMATION REVOLUTION

Computer (computation) + Communication (Transfer) → Network

is

INFORMATION TECHNOLOGY

Basis of

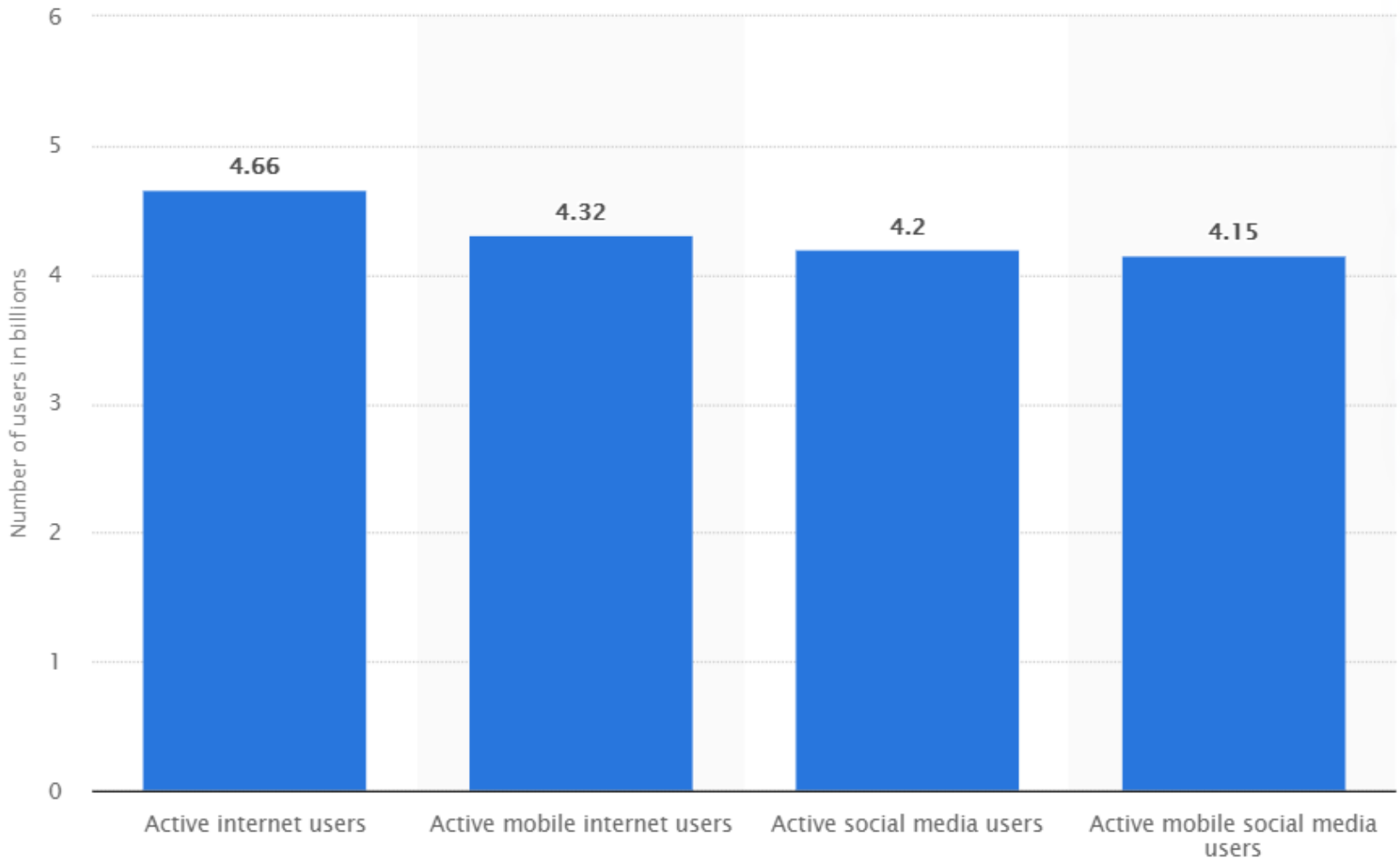
DIGITAL CONVERGENCE

STATS ON ELECTRONICALLY STORED INFORMATION (ESI)

- *95% of all information is generated in digital form.*
- *Most electronic documents are never created as hard copy*
- *Information can be compressed*
- *Information is readily and frequently replicated.*

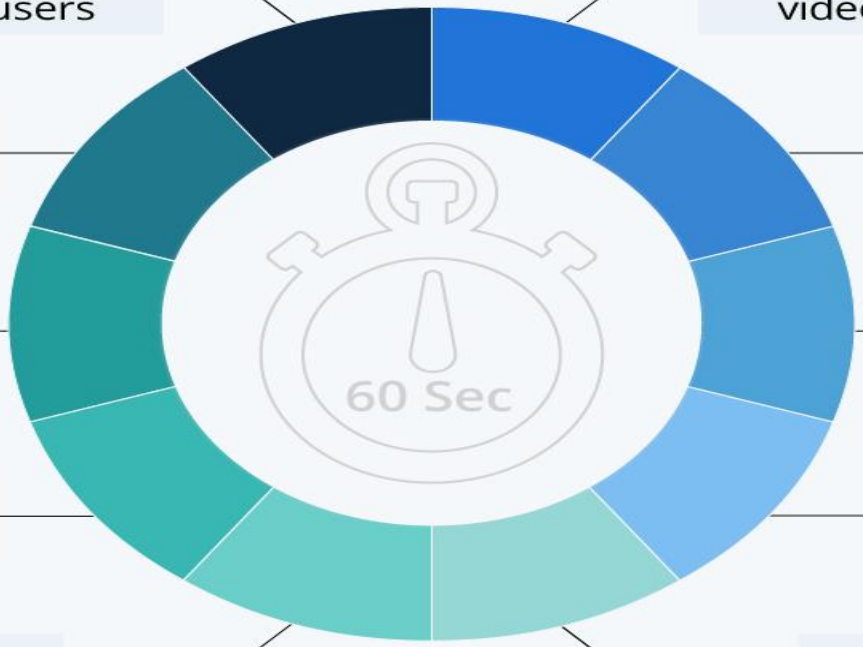
Global digital population as of January 2021

(in billions)



A Minute on the Internet in 2020

Estimated amount of data created on the internet in one minute



NETFLIX
404,444 hours of video streamed by users

500 hours of video uploaded by users

TikTok
2,704 app installations

347,222 stories

amazon
6,659 packages shipped

52,083 users connected

zoom
208,333 participants in meetings

41.7m messages shared

319 new users gained

28 new tracks added to library

Source: Visual Capitalist

statista

Life e-Fixed

- **e-REVOLUTION**

e- BUSINESS

e- COMMERCE

e- GOVERNANCE

e- SECURITY

e- THIEVES

FUTURE MAY BE M-THIEVES

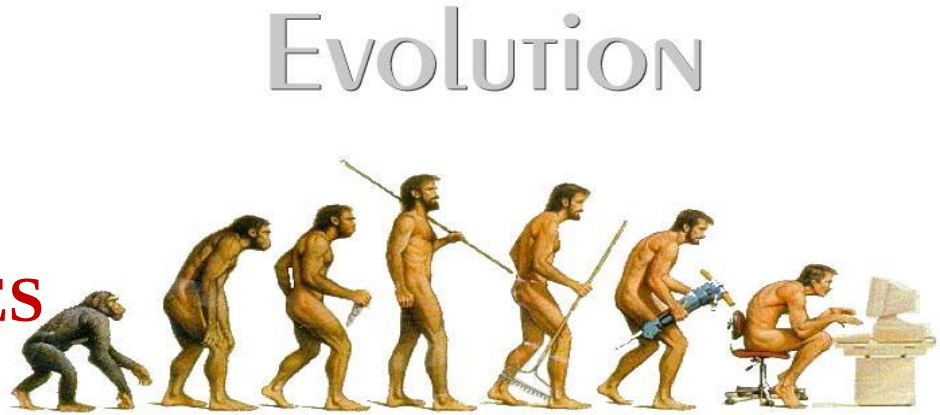
e-INVESTIGATOR

e-CREATE

e-COLLATE

e-COLLABORATE

e-INVESTIGATE



Although India's growing digital infrastructure is an economic booster, it could also play into the hands of cyber crooks, including thrill-seekers, vandals, thieves or even state-sponsored conmen

With **32 crore** internet users last year, India is the fastest growing internet market in the world

PERILS OF PROGRESS

India is the **5th** most vulnerable country for cyberattacks, says SophosLabs, a global leader in network security

India needs at least **5 lakh** more personnel to protect its cyber space

A DOUBLE-EDGED SWORD

Internet of Things
Programming of devices to function without human intervention. High-speed trains and automated aeroplanes could be vulnerable to hacking

Surveillance drones
Drones connected to a server could be hacked into and used for aerial attacks

Bitcoins
Digital, decentralised currency that is circulated on the internet to avail goods and services. In the absence of a regulatory body for such digital transactions, it can be used to carry out illegal activities

Dark web
It uses a software called Tor for anonymous communication. "Dark web"—the underworld of the cyber space—may abet child pornography, prostitution, illegal trade and terrorism

3D printing
Process of making three-dimensional objects from digital files. A 3D printer, when connected to a server, can be hacked and used to design weapons.

Cody Wilson from Texas created the first fully 3D-printed gun last year. He uploaded the file online, and **1,00,000** people downloaded them. The state department then erased the file.

SECURING CYBERSPACE

CERT-IN
Computer Emergency Response Team-India
National agency for non-critical sectors such as banking and telecom
Established in 2004
Employs 75 experts

NCIIPC
National Critical Information Infrastructure Protection Centre
Protects critical infrastructure such as atomic energy units, power plants and defence
Set up in 2014

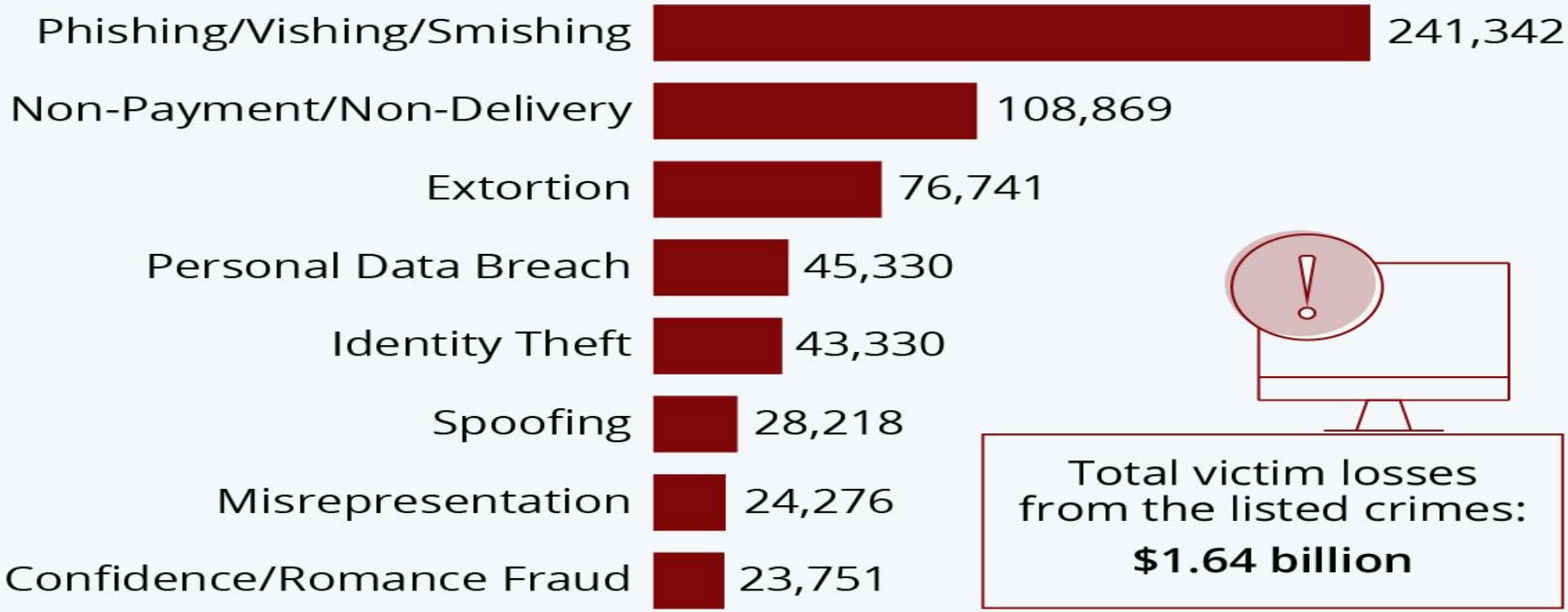
- The National Cyber Coordination Centre is being set up to improve coordination among all cybersecurity agencies
- Cyber Swachchta Kendra, under the IT ministry, acts as a botnet-cleaning and malware analysis centre
- RBI is setting up a new cybersecurity cell to monitor cyber threats in the banking and economic sector

OTHER INSTITUTIONS
- National Crisis Management Centre
- National Informatics Centre
- CBI
- National Investigation Agency

25% of the attacks target the ministry of defence

The Most Common Types of Cyber Crime

Number of Americans who fell victim to the following types of internet crime in 2020



Total victim losses from the listed crimes:
$1.64 billion

Source: The FBI's Internet Crime Complaint Center

VICTIM ORGANISATIONS

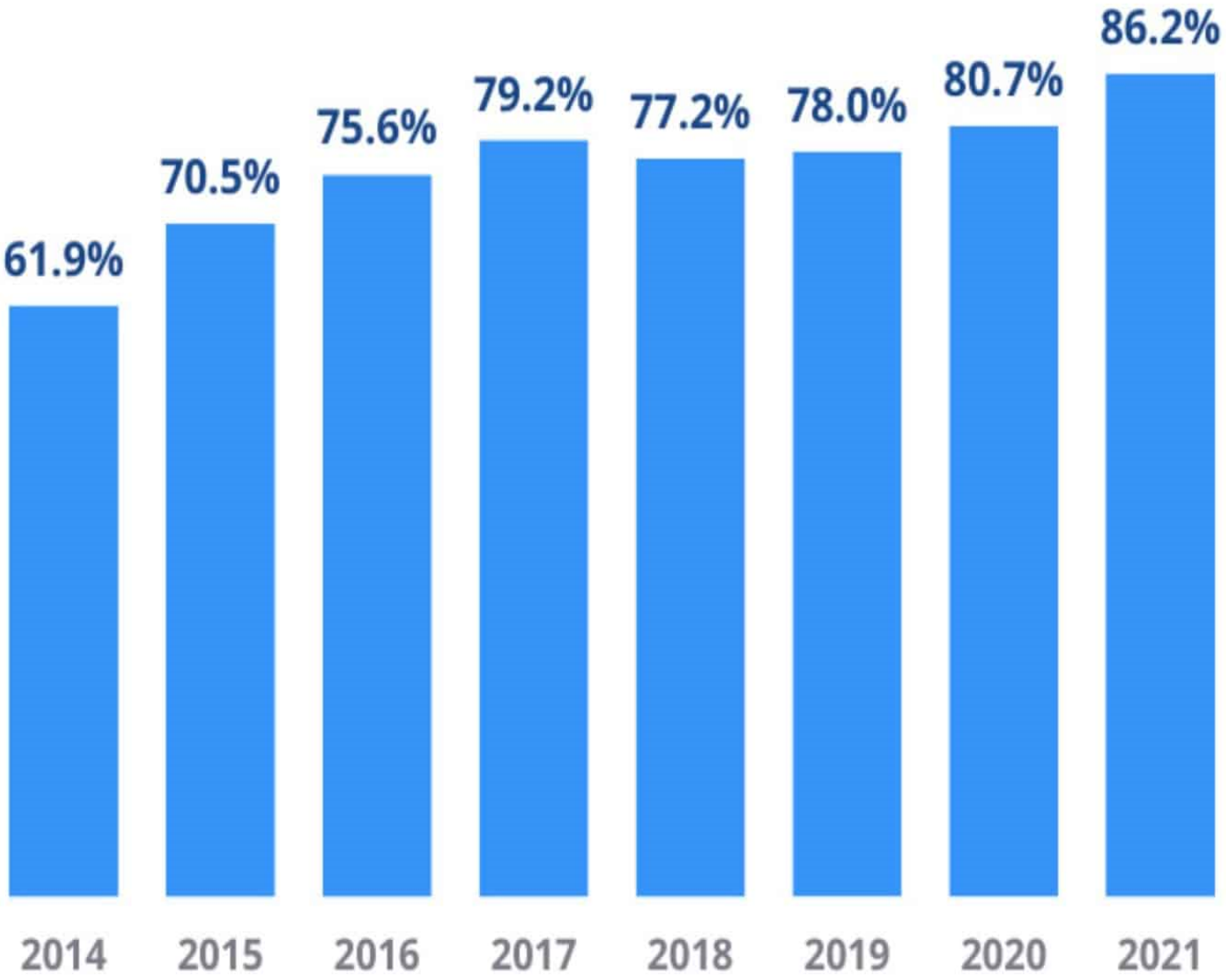


Figure 2: Percentage of organizations compromised by at least one successful attack.

Cyber Crimes-India (NCRB STAT)

TABLE 9A.1

Cyber Crimes (State/UT-wise) - 2018-2020

SL	State/UT	2018	2019	2020	Mid-Year Projected Population (in Lakhs)	Rate of Total Cyber Crimes (2020)	Chargesheeting Rate (2020)
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
STATES:							
1	Andhra Pradesh	1207	1886	1899	526.0	3.6	40.1
2	Arunachal Pradesh	7	8	30	15.2	2.0	33.3
3	Assam	2022	2231	3530	347.9	10.1	19.4
4	Bihar	374	1050	1512	1219.0	1.2	65.0
5	Chhattisgarh	139	175	297	292.4	1.0	87.4
6	Goa	29	15	40	15.5	2.6	50.0
7	Gujarat	702	784	1283	691.7	1.9	47.1
8	Haryana	418	564	656	292.1	2.2	49.6
9	Himachal Pradesh	69	76	98	73.6	1.3	41.9
10	Jharkhand	930	1095	1204	381.2	3.2	53.0
11	Karnataka	5839	12020	10741	665.0	16.2	72.9
12	Kerala	340	307	426	353.7	1.2	70.6
13	Madhya Pradesh	740	602	699	837.6	0.8	85.6
14	Maharashtra	3511	4967	5496	1236.8	4.4	27.1
15	Manipur	29	4	79	31.4	2.5	0.0
16	Meghalaya	74	89	142	32.6	4.4	1.4
17	Mizoram	6	8	13	12.1	1.1	57.1
18	Nagaland	2	2	8	21.8	0.4	-
19	Odisha	843	1485	1931	454.7	4.2	33.5
20	Punjab	239	243	378	301.8	1.3	62.4
21	Rajasthan	1104	1762	1354	786.1	1.7	26.8
22	Sikkim	1	2	0	6.7	0.0	-
23	Tamil Nadu	295	385	782	761.7	1.0	53.1
24	Telangana	1205	2691	5024	375.4	13.4	42.5
25	Tripura	20	20	34	40.4	0.8	26.3
26	Uttar Pradesh	6280	11416	11097	2289.3	4.8	49.9
27	Uttarakhand	171	100	243	113.1	2.1	63.0
28	West Bengal	335	524	712	977.2	0.7	45.9
	TOTAL STATE(S)	**26931**	**44511**	**49708**	**13151.8**	**3.8**	**47.5**
UNION TERRITORIES :							
29	A&N Islands	7	2	5	4.0	1.3	62.5
30	Chandigarh	30	23	17	12.0	1.4	30.0
31	D&N Haveli and Daman & Diu@	0+	3+	3	10.4	0.3	100.0
32	Delhi	189	115	168	203.2	0.8	66.3
33	Jammu & Kashmir@	73*	73*	120	133.4	0.9	42.4
34	Ladakh @	-	-	1	3.0	0.3	-
35	Lakshadweep	4	4	3	0.7	4.4	-
36	Puducherry	14	4	10	15.5	0.6	100.0
	TOTAL UT(S)	**317**	**224**	**327**	**382.1**	**0.9**	**59.7**
	TOTAL ALL INDIA	**27248**	**44735**	**50035**	**13533.9**	**3.7**	**47.5**

- Crime Rate is calculated as Crime Incidence per one lakh of population

TABLE 9A.1 Page 1 of 1

- Population Source: Report of Technical group on Population Projections(July, 2020) National Commission on Population, MoHFW
- As per data provided by States/UTs
- States/UTs may not be compared purely on the basis of crime figures

'+' Combined data of erstwhile D&N Haveli UT and Daman & Diu UT

'*' Data of erstwhile Jammu & Kashmir State including Ladakh

'@' Data of newly created Union Territory

Global Cybercrime Damage Costs:

- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

ALL FIGURES ARE PREDICTED BY 2021

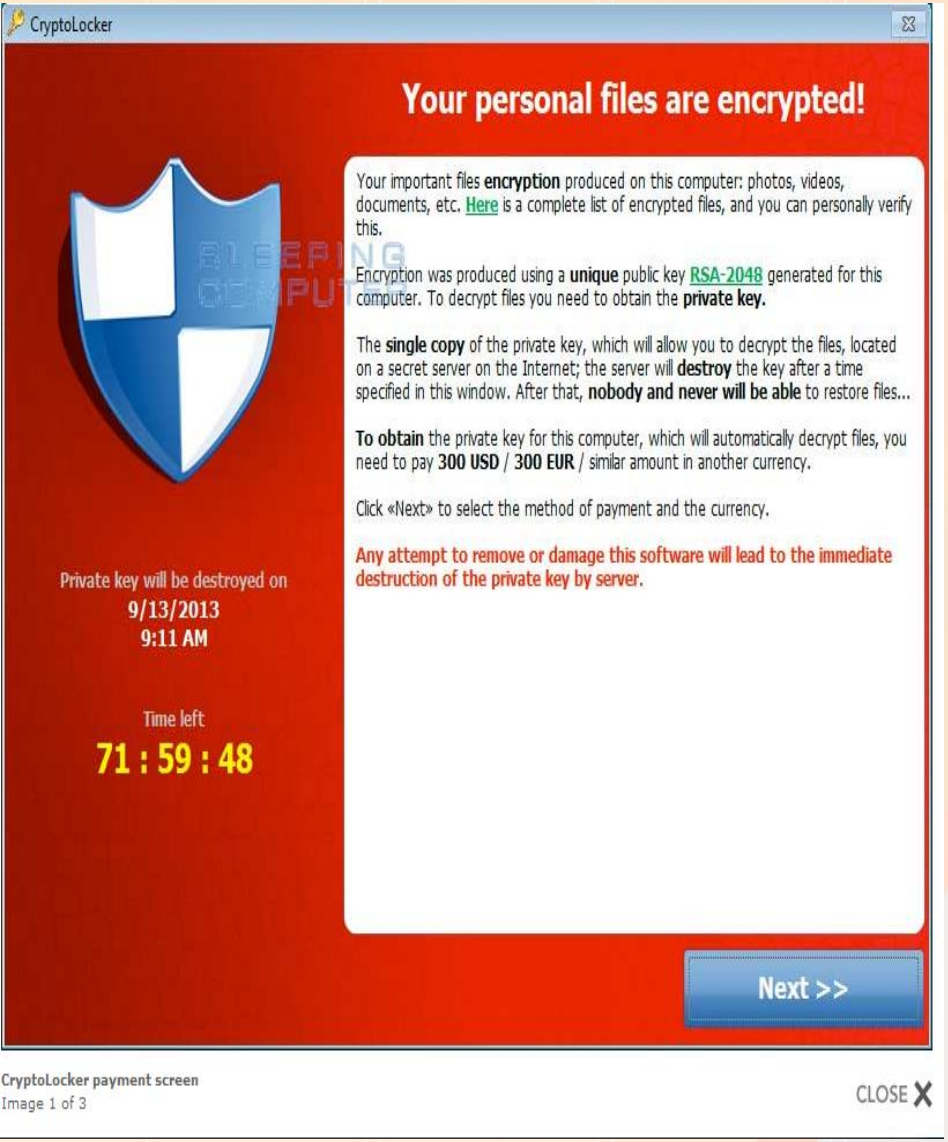
* SOURCE: CYBERSECURITY VENTURES

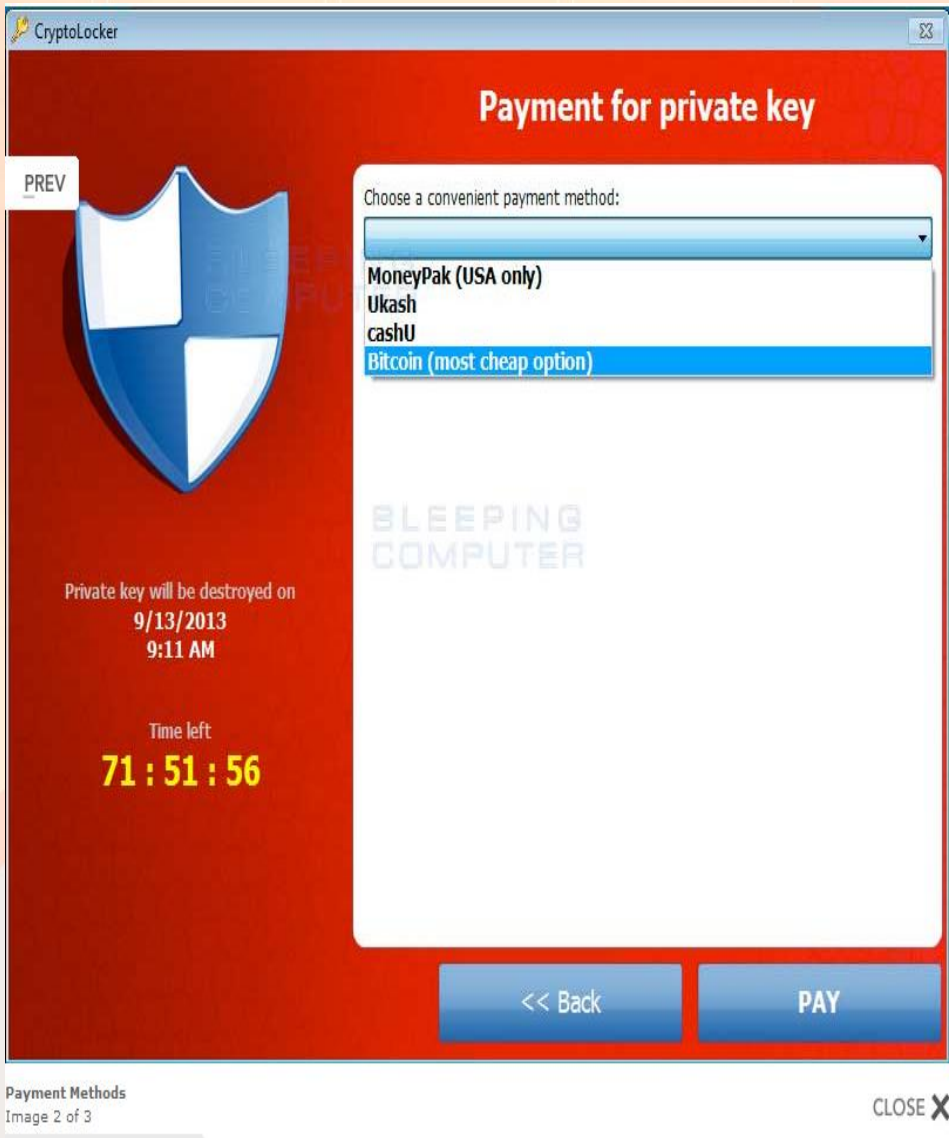
CYBERSECURITY VENTURES

MALWARE INFECTION TRENDS

- *STUXNET*
  - *DISCOVERED IN MID JUNE 2010 BY A SECURITY COMPANY VIRUS BLOKADA.*
  - *IT TARGETS SIEMENS INDUSTRIAL SYSTEMS AND EQUIPMENTS RUNNING MICROSOFT WINDOWS LIKE SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION)SYSTEMS.*
  - *FIRST TO TAKE THE PAY LOAD TO INFECT THE INDUSTRIAL CONTROL SYSTEMS (ICS), PLC'S(PROGRAMMABLE LOGIC CONTROLS).*
  - *SPREAD THRU REMOVABLE DRIVES LIKE USB FLASH DRIVES*
  - *IRAN IS THE WORST AFFECTED COUNRY.*
  - *DEMO OF INFECTION.*

RANSOMWARE ATTACK





Growth in ransomware damage and costs worldwide

US$325 MILLION — 2015

US$5 BILLION — 2017

US$11.5 BILLION — 2019

US$20 BILLION — 2021

Source: Cybersecurity Ventures

FinancesOnline
REVIEWS FOR BUSINESS

Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data? (n=1,182)

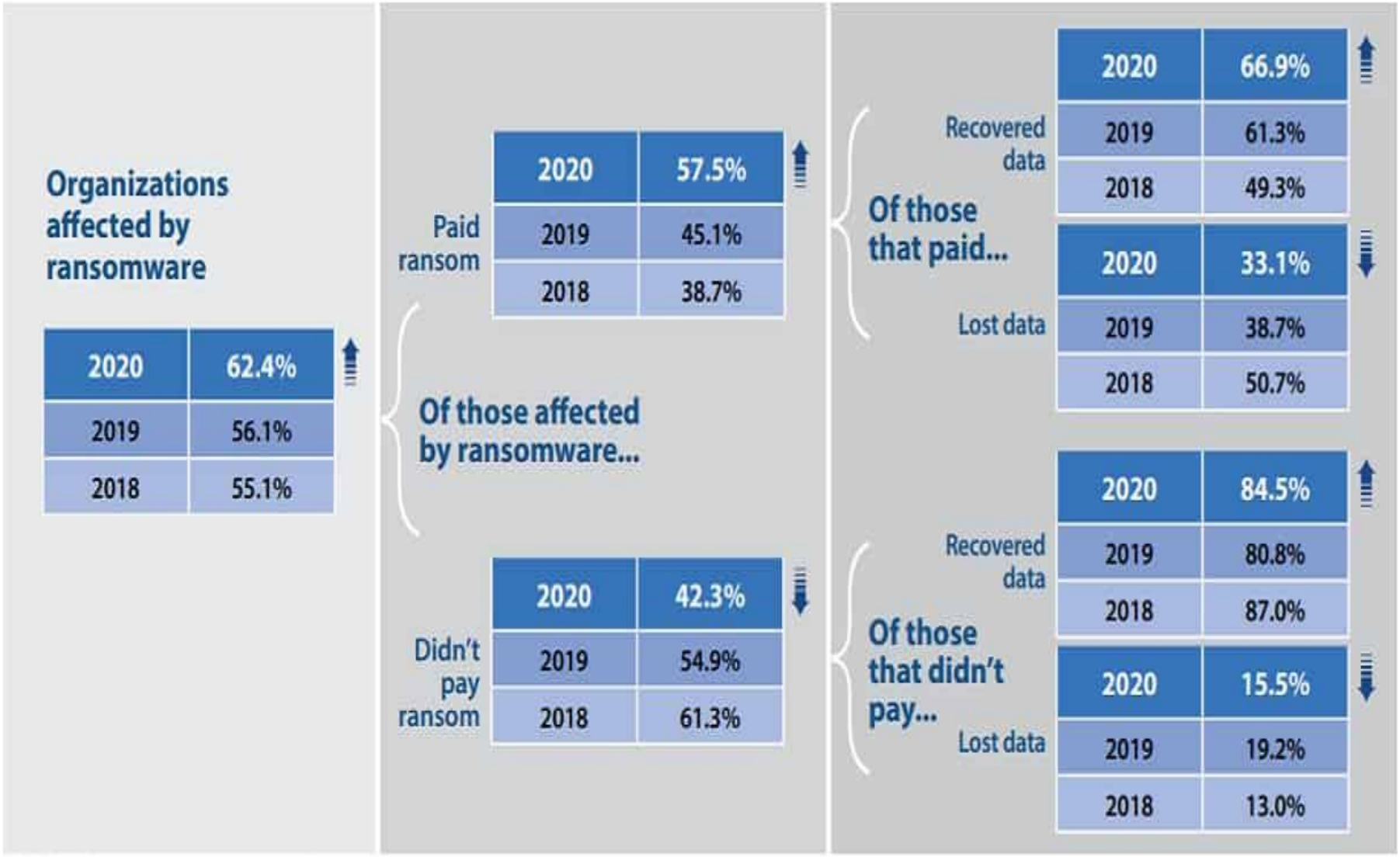


Table 1: Key ransomware statistics.

Phishing – The Identity Theft

- ***The process of tricking or socially engineering organizations customers into imparting their confidential/personal information for nefarious use.***

- ***"In the last year, phishing attacks targeted 57 million Internet users.On average, three to five percent of all individuals who received a phishing e-mail fell victim to the fraud." (Source: Verisign, June 28, 2004)***

Phishing attacks

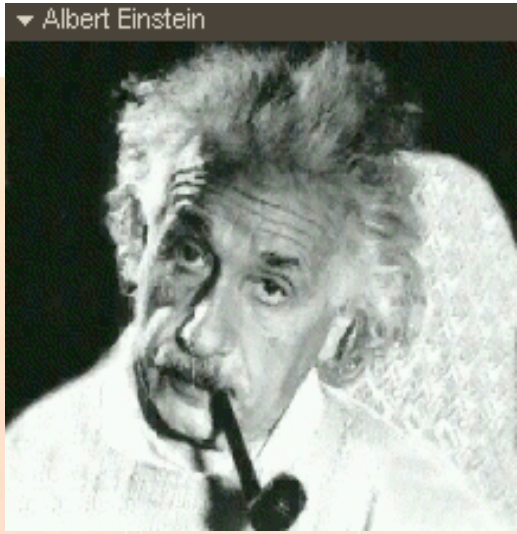
- *Fake e-mails*
- *Key loggers*
- *Screen grabbing softwares*
- *Fake websites*
- *Job offer sites*
- *Man in the middle attack etc,.*

INFORMATION SECURITY

- *TO BUILD A COMPLETE SECURE SYSTEM - A MYTH*
- *INFORMATION SECURITY - PROACTIVE Vs REACTIVE*
  - *OS are hardened, FIREWALLS, IDS/IPS's, HONEYPOTS,, Security polices & procedures (compliance)*
  - *Detection process should be more mature than defence mechanisms where securing 100% is impossible. The fear of detection is more deterrent than the challenge of prevention.*
  - *As the technology continues to change, organizations must take steps to understand the related risks that will evolve with technology.*

Risk accepted by one, imposed on all

Technological Progress

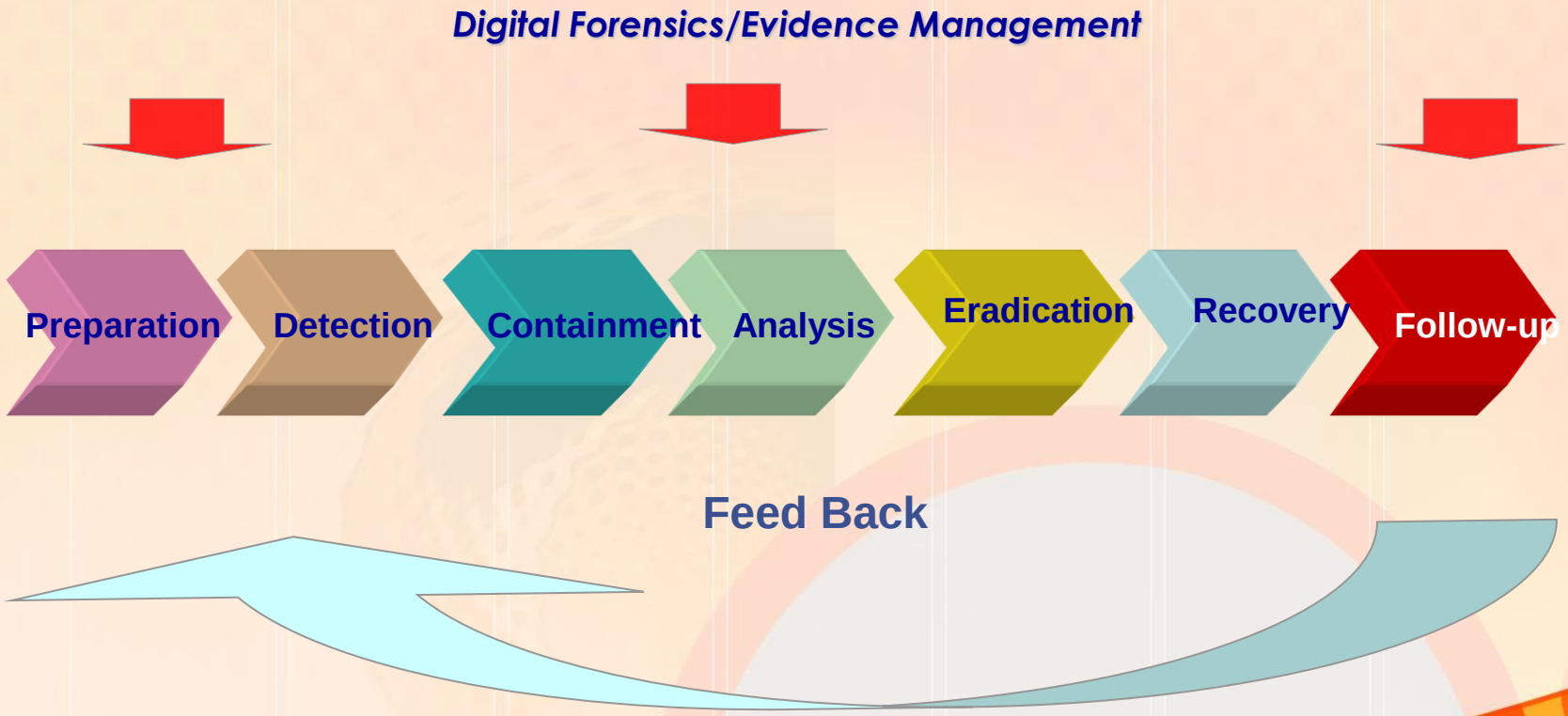


Albert Einstein said "Technological progress is like an axe in the hands of a pathological criminal."

"Security is not a one-time activity but rather a continuous, risk managed process,"

- *ISAlliance Executive Director Dave McCurdy*.

Incident Response Methodology (PDCAERF)



MAJOR PROBLEM ?

LINKING THE CRIME TO THE CRIMINAL

PHYSICAL WORLD

VIRTUAL WORLD

THE SOLUTION

DIGITAL FORENSICS

Findings the needle in the haystack, locate and recover digitally based evidence

Definition of Forensics Science

- Forensic science is "the *Application of physical sciences to law in the search for truth in civil, criminal and social behavioral matters to the end that injustice shall not be done to any member of society*" (Source: Handbook of Forensic Pathology College of American Pathologists 1990).

- Forensic science is "*the application of scientific techniques and principles to provide evidence to legal or related investigations and determinations*" (Forensic science : an encyclopedia of history, methods, and techniques, 2006)
- *Aim*:
  - determining the evidential value of crime scene and related evidence

WHAT IS DIGITAL EVIDENCE?

- ***DIGITAL EVIDENCE IS ANY INFORMATION OF PROBATIVE VALUE THAT IS EITHER STORED OR TRANSMITTED IN A BINARY FORM" (SWG)***

- ***DIGITAL EVIDENCE INCLUDES COMPUTER EVIDENCE, DIGITAL AUDIO, DIGITAL VIDEO, CELL PHONES, USBs, MSDs, DVDs, CDs ETC……..ALL DIGITAL, BUT WITH DIFFERENT OUTPUTS.***

Computer Forensics

"A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format."

- Dr. H.B. Wolfe

1

"The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing of expert opinion in a court of law or other legal and/or administrative proceeding as to what was found."

- CSI

2

Forensics Computing is the science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law.

3

Notification As per IT Act (Amendment) 2008

CHAPTER XIIA

EXAMINER OF ELECTRONIC EVIDENCE

Central Government to notify Examiner of Electronic Evidence.

79A. The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation.—For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.'.

Insertion of new section 45A.

(*b*) after section 45, the following section shall be inserted, namely:—

Opinion of Examiner of Electronic Evidence.

"45A. 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. 21 of 2000.

Explanation.—For the purposes of this section, an Examiner of Electronic Evidence shall be an expert.";

CFSL, HYDERABAD NOTIFIED AS EXAMINER OF ELECTRONIC EVIDENCE ON 28TH MARCH 2018.

भारत का राजपत्र
The Gazette of India

असाधारण
EXTRAORDINARY
भाग II—खण्ड 3—उप-खण्ड (ii)
PART II—Section 3—Sub-section (ii)
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 1275] नई दिल्ली, बुधवार, मार्च 28, 2018/चैत्र 7, 1940
No. 1275] NEW DELHI, WEDNESDAY, MARCH 28, 2018/CHAITRA 7, 1940

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

अधिसूचना

नई दिल्ली, 26 मार्च, 2018

का.आ. 1411 (अ).— सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21वां) की धारा 79क द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, केन्द्र सरकार एतद्वारा गृह मंत्रालय, न्यायविज्ञान सेवा निदेशालय के अधीन केन्द्रीय न्यायविज्ञान प्रयोगशाला, हैदराबाद को भारत में निम्नलिखित कार्यक्षेत्र के साथ इलेक्ट्रॉनिक साक्ष्य के परीक्षक के तौर पर अधिसूचित करती है, अर्थात :

कार्यक्षेत्र : (क) कम्प्यूटर (मीडिया) न्यायविज्ञान-फ्लॉपी डिस्क ड्राइव को छोड़कर;

(ख) मोबाइल उपकरण न्यायविज्ञान

[सं. 1(13)/2015-सीएलएफई]

एस. गोपालकृष्णन, संयुक्त सचिव

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

NOTIFICATION

New Delhi, the 26th March, 2018

S.O. 1411(E).— In exercise of the powers conferred by section 79A of the Information Technology Act 2000 (21 of 2000), the Central Government hereby notifies Central Forensic Science Laboratory, Hyderabad under Directorate of Forensic Science Services, Ministry of Home Affairs as Examiner of Electronic Evidence within India with the following scope, namely:-

(a) Computer (Media) Forensics excluding Floppy Disk Drive;

(b) Mobile Devices Forensics.

[No. 1(13)/2015-CLFE]

S. GOPALAKRISHNAN, Jt. Secy.

1890 GI/2018

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064 and Published by the Controller of Publications, Delhi-110054.

Cyber Forensic Principles

Data Integrity

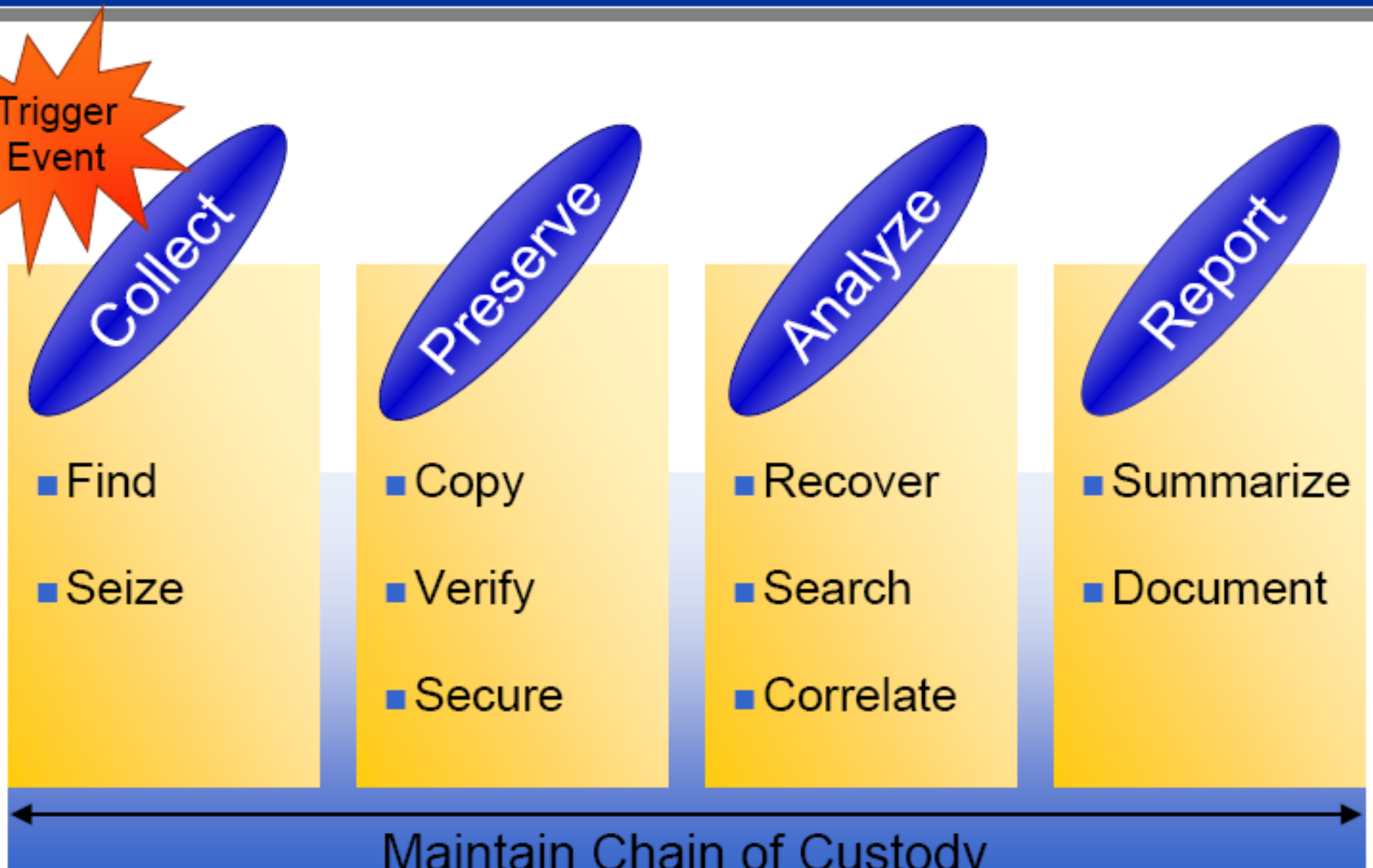
Free from Contamination

Full Documentation

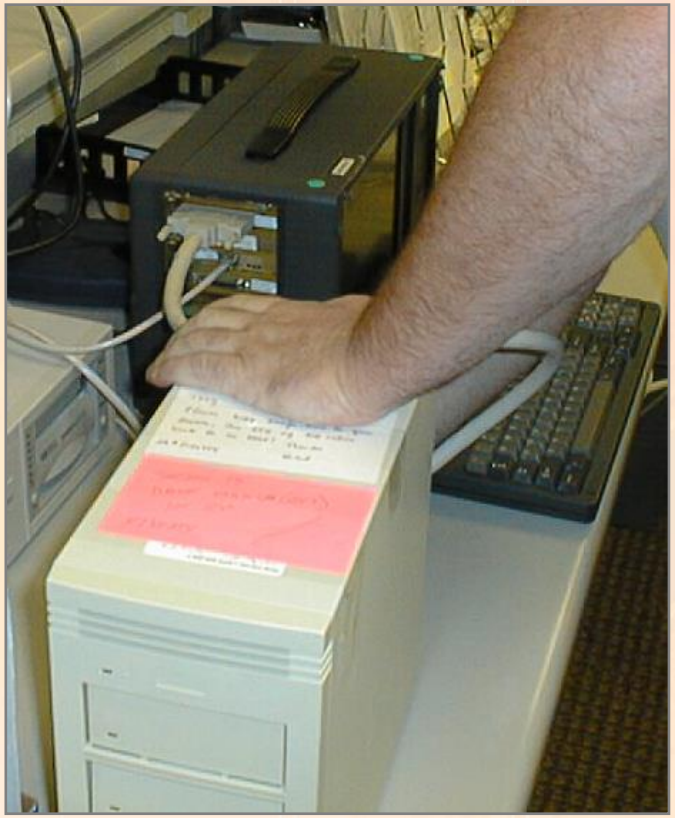
Scientific Methodology

Cyber Forensics Examination

Acquire, Authenticate, Analyze: Forensic Investigative Process

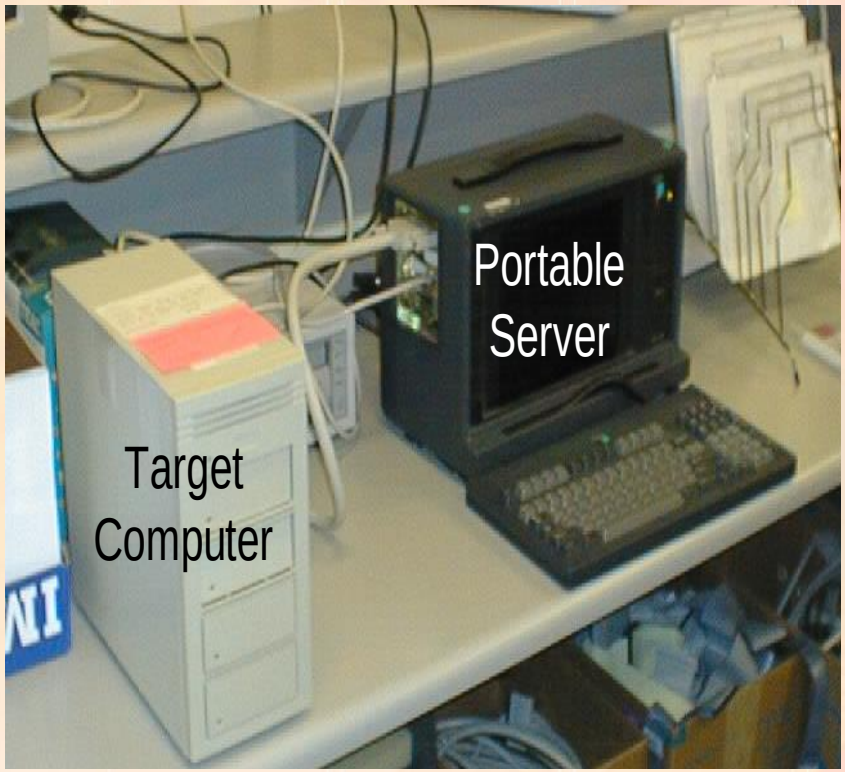


THE CYBER FORENSIC PROCESS



- *FOUR STAGES*
  - *ACQUIRE*
  - *AUTHENTICATE*
  - *ANALYZE*
  - *DOCUMENT*
  - *PRESENTATION*

ACQUIRE (1st Stage)



- A TRUE MIRROR IMAGE IS A SECTOR BY SECTOR COPY OF EVERY SECTOR OF THE ORIGINAL MEDIA
- FORENSICALLY SOUND MEANS EVERY BIT OR BYTE NOT JUST MOST OF THE BITS AND BYTES.

Collect Volatile Evidence

"Volatile evidence" is evidence that will disappear soon, such as information about active network connections, or the current contents of volatile memory.

Volatile System Information

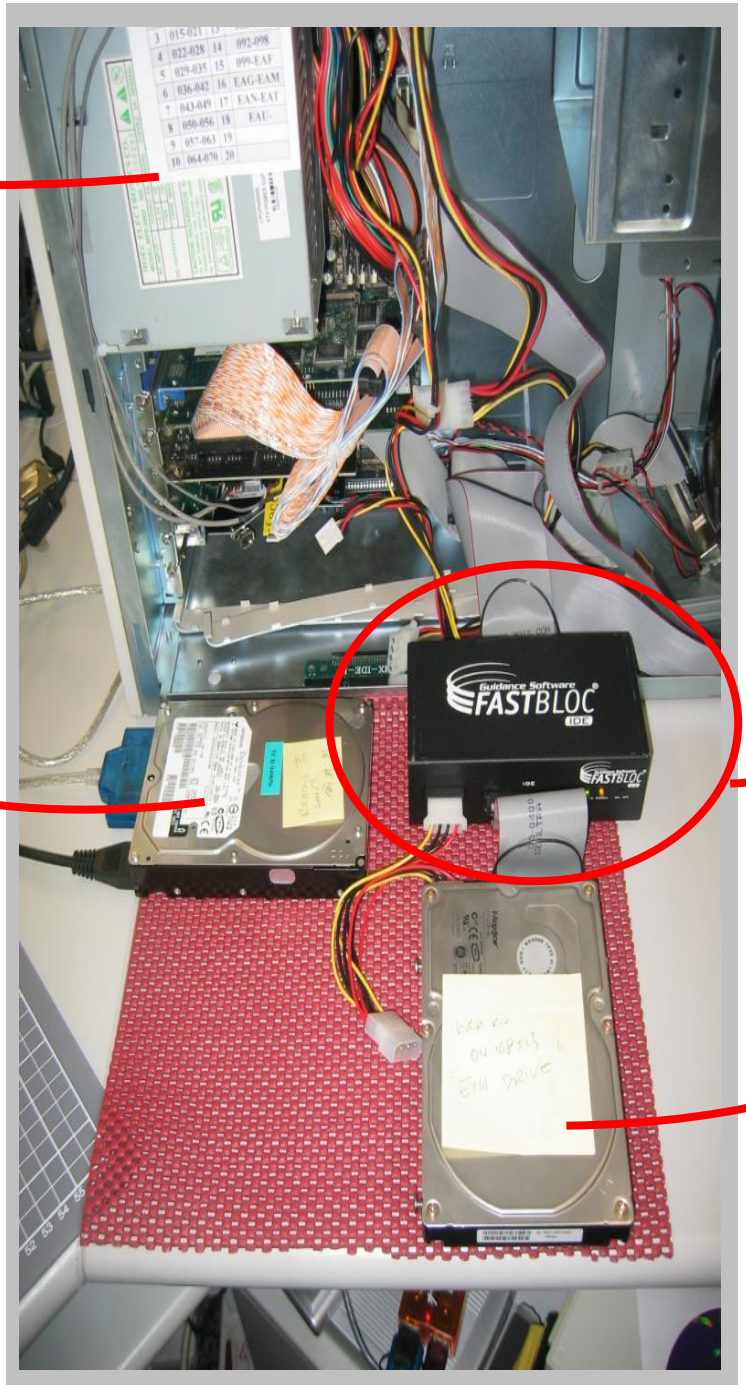
- System profile
- Current system date and time
- Command history
- Current system uptime
- Running processes
- Open files, start up files, clipboard data
- Logged on users
- DLLs or shared libraries

MAKE SUSPECT DRIVE READ ONLY

- PREVENT ACCIDENTAL WRITES TO THE SUSPECT HARD DRIVE USING A WRITE BLOCKER

Exhibit Computer

The Government hard disk is used to store the Image of the exhibit HDD



By using Write Protection device (EnCase FASTBLOC in this example, the original hard disk can be free from contamination

The original exhibit

FORENSIC FALCON AND SOLO 4

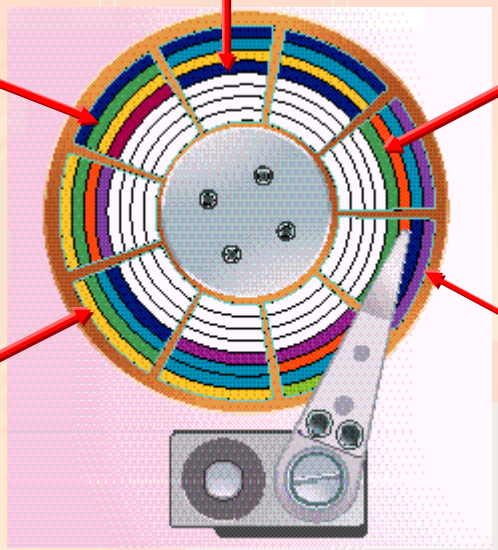
Why use Forensic Tools?

Your data "iceberg"

The data found by common tools

The additional data found by FORENSIC SOFTWARE TOOLS (Deleted, renamed, hidden, difficult to locate.)

WHY TO IMAGE



Unallocated space

File slack

Hidden files

Temporary files

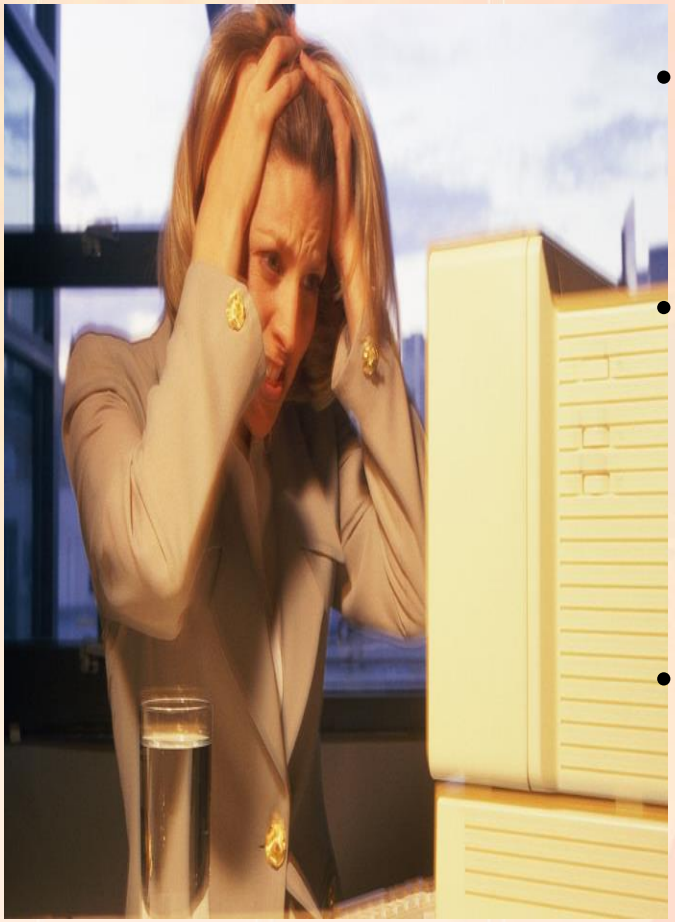
History files

Formatted disks

AUTHENTICATION (2nd Stage)

- *ONCE IMAGING (DUPLICATION OF SUSPECT HARD DISK) IS COMPLETED, IT HAS TO BE AUTHENTICATED TO VERIFY THAT ALL THE INFORMATION AVAILABLE ON THE SUSPECT DISK HAS BEEN COPIED OR NOT. HOW IT IS DONE*

AUTHENTICATE



- *IS THE DUPLICATE AUTHENTIC ?*
- *JUSTIFIED WITH HASH VALUE*
  - *ACQUISITION HASH VALUE = VERIFICATION HASH*
- *MD5 HASH VALUE*

ALL THIS FOR WHAT ?

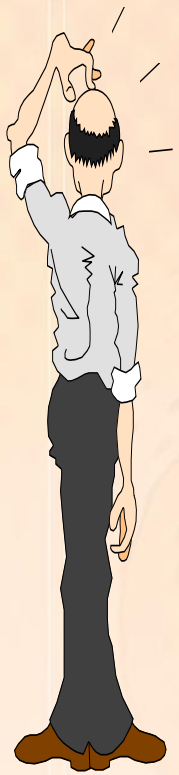
- HASH ensures integrity of the IMAGE

1234 5678 9879
5689 7850 6985
8965 2345 9865
4598 3265 4587
9875 6423 5147
3265 8975 6542
3265 5689 6325
8975 3215 6521

Message Digest 1
(Acquisition Hash)

Message Digest 2
(verification hash)

ANALYSIS



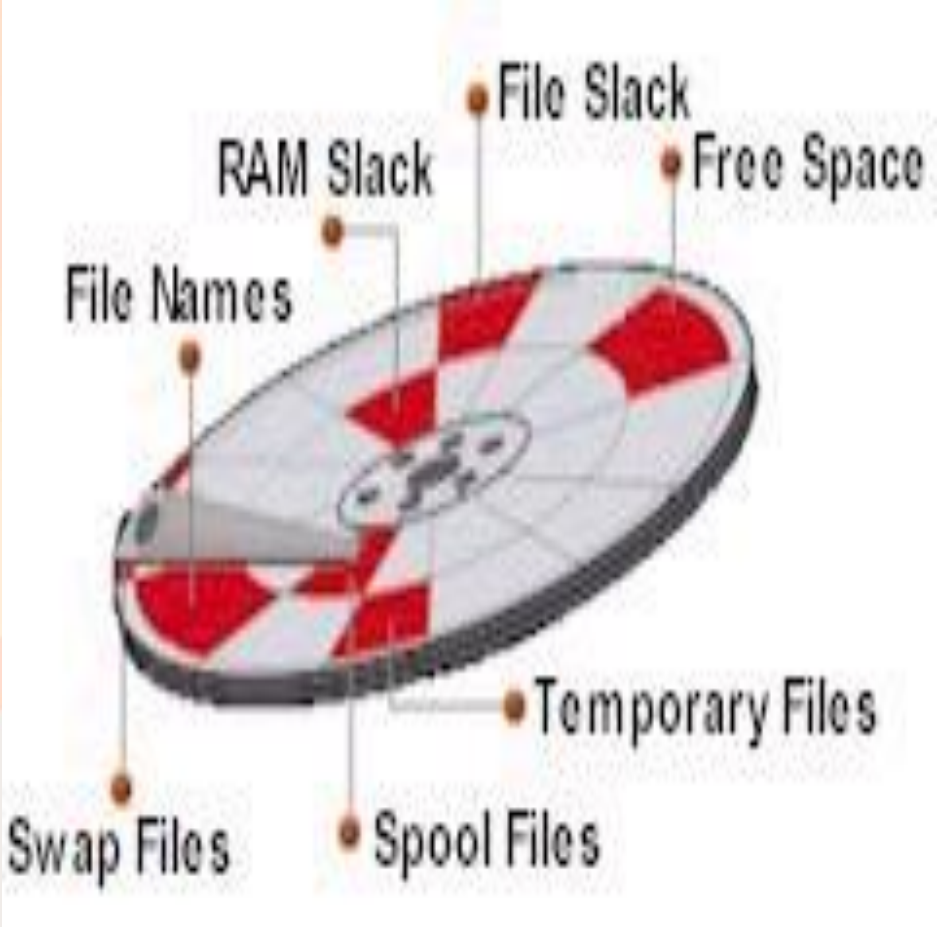
- *EXTRACT, PROCESS, INTERPRET*
  - *EXTRACT - MAY PRODUCE BINARY 'GUNK' THAT ISN'T HUMAN READABLE*
  - *PROCESS - MAKE IT HUMANLY READABLE*
  - *INTERPRET - REQUIRES A DEEPER UNDERSTANDING OF HOW THINGS FIT TOGETHER*

EVIDENCE SEARCH – A FEW

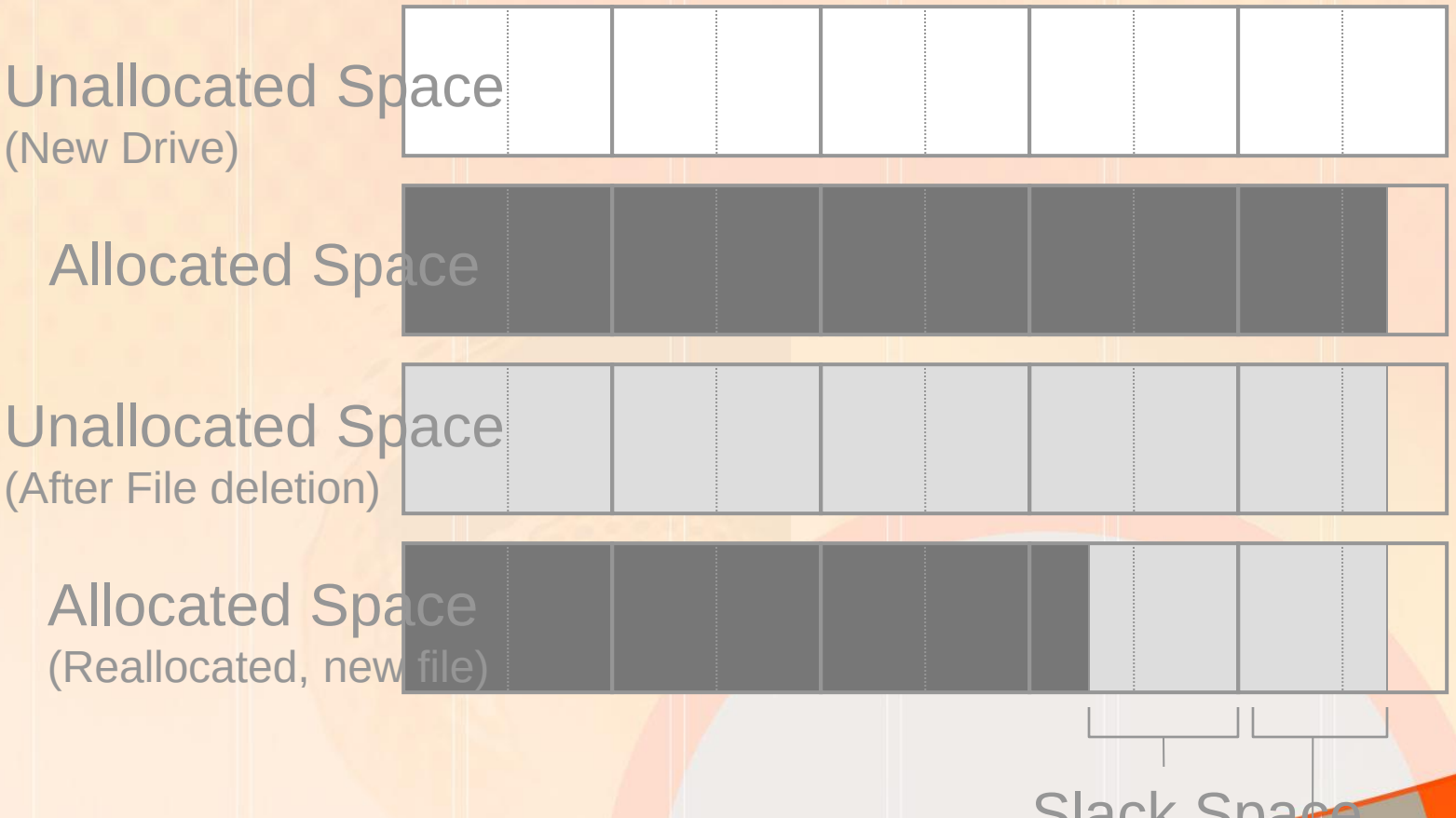
- *ACTIVE FILES*
- *DELETED FILES*
- *SOFTWARE APPLICATIONS*
- *HIDDEN PARTITIONS, FILES*
- *ENCRYPTED FILES*
- *PASSWORD PROTECTED*
- *STEGANO FILES*
- *LOG FILES*

UNALLOCATED SPACE

- SPOOL FILES
- TEMPORARY FILES
- E-MAIL FILES
- TEMPORARY INTERNET FILES
- INSTALLATION FILES



Why is Slack Space Important?



DELETED DOESN'T MEAN GONE - RECOVERY OF DELETED DATA

- DELETE SIMPLY MAKES SPACE AVAILABLE AGAIN

- LIBRARY CARD CATALOG ANALOGY

Benefits of Forensics Readiness

1. Evidence can be gathered to act in the company's defense if subject to a lawsuit
2. In the event of a major incident, a fast and efficient investigation can be conducted and corresponding actions can be followed with minimal disruption to the business
3. Forensic readiness can extend the target of information security to the wider threat from cybercrime, such as intellectual property protection, fraud, or extortion
4. Fixed and structured approach for storage of evidence can considerably reduce the expense and time of an internal investigation
5. It can improve and simplify law enforcement interface
6. In case of a major incident, proper and in-depth investigation can be conducted

CHALLENGES

- *INCRESE IN ANTI-FORENSIC TRENDS*
  - *Defilers toolkit*
  - *Evidence eliminator*
  - *Shredding*
  - *Encryption*
  - *Passwords*
  - *Steganography*
- *ANALYSIS OF TERABYTES OF DATA*
  - *Data mining & dataware housing*
  - *Need intelligent systems to classify data*
- *MAINFRAME DIGITAL FORENSICS*
  - *Current tools and methodologies mainly provide for Windows, Unix/ Linux and Mac.*

“For secure computing environment and adequate trust & confidence in electronic transactions ”

“THINK SECURITY”

QUESTIONS

THANK YOU,

FOR PARTICIPATION AND PATIENCE.

M. KRISHNA

M.Sc, M.Tech(IT),GCIH(SANS), CPE, CHFI, PGDCL

Asstt Director and HoD,

DIGITAL FORENSIC DIVISION,CFSL, HYDERABAD.

Mail: krishforensics@gmail.com

098494 72339 (M)