Unit 3: Cyber Forensics Labs and Challenges before Law Enforcement Agencies

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The requirement for cyber forensics lab and how to build it.
- The details of examiner of electronic evidence by government of India.
- Computer Emergency Response Team India.
- Challenges before law enforcement agencies in India while investigation.
- Dark web and how Law enforcement deals with it.

1.2 INTRODUCTION TO CYBER FORENSIC LABS

Cyber Forensic lab is a facility where digital evidences are examined, analysed and the forensic report is been produced. There is a specific way to establish a cyber-forensic facility. Let's discuss certain points which are taken into consideration for setting up a cyber-forensic lab.

1.3 CYBER FORENSIC LAB STRUCTURE

- **LAB SPACE**

  The cyber forensic facility should be located at secured premises. The facility should not be congested and should have enough working space. There should be adequate and uninterrupted electricity. The forensic lab should have an effective cooling system without any humidity present inside the lab. There should be good internet connectivity at high speed. There should be enough desk and benches with the antistatic floor. There should be a lock for every room with an access control mechanism to prevent unauthorised access.[134]

- **REQUIRED EQUIPMENTS**

  There should be multiple hardware write blockers which supports all types of connectivity. E.g. SATA, Firewire, USB etc. There should be a high configuration computer system with the fastest speed of processing. There should be multiple good monitor. The forensic lab should have hardware filled kit. There should be enough blank hard disk and storage container which is called as evidence vault. There should be all sort of data and power cables with static bags. There should be enough supplies of packaging and labelling material. For network connectivity, there should be enough networking devices.

- **APPROPRIATE SOFTWARE**

  Forensic lab requires different types of software for different analysis purpose. There are a few examples like Encase, Accessdata FTK, Net force suit, Oxygen mobile forensic, Passware password recovery, Helix live CD etc.

[134] meity.gov.in. <https://meity.gov.in/writereaddata/files/annexure-i-pilot-scheme-for-notifying-examiner-of-electronic-evidence-under-section-79a-of-the-information-technology-act-2000.docx>

- **CYBER FORENSIC EXPERT**

  The cyber lab requires a team of cyber forensic expert with detailed knowledge of computing technology. These experts should be certified for the software and hardware installed in a forensic lab. These experts should have experience of expert witness testimony at court trials.

- **SOP(STANDARD OPERATING PROCEDURE)**

  There should be an established set of policies and procedures to be followed in a forensic lab for different purposes. E.g. wearing gloves before handling any evidence etc.

  There should be standard and approved format to prepare a chain of custody form. Examination notes, observation, finding and reports etc.

- **TRAINING AND UPGRADATION**

  To cop up with changing technology, the experts working with the forensic lab should undergo training every six months. The hardware and software used for the forensic examination should be upgraded as per requirement.

  The cyber forensic lab is a dedicated facility to carry out a forensic examination of digital evidence. These labs are mainly set up by government centrally and state wise.

1.4 EXAMINER OF ELECTRONIC EVIDENCE

The Information Technology Act, 2000 empowers the Central Government under section 79A to notify any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence for the purposes of providing expert opinion on electronic form evidence before any court or other authority specified by notification in the Official Gazette. The Explanation clause of section 79A further articulates that the “Electronic Form Evidence” means

any information of probative value that is either stored or transmitted in electronic form and includes evidence, digital data, digital video, cell phones, digital fax machine etc.[135]

a) In line with the above requirement, MeitY has formulated a scheme for notifying the Examiner of Electronic Evidence. The objective of the scheme is to ascertain the competence of all the 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 evidence before any court.
The scheme is based on international standards like ISO/IEC 17025 (A Standard on General requirements for the competence of testing and calibration laboratories) and ISO/IEC 27037 (A Standard on Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence). The evaluation process includes an examination of the technical, skilled professional manpower in digital forensics, licensed tools and equipment, availability of suitable environment to carry out such evaluation as also the availability of a proper quality management system and reasonable experience to demonstrate their overall competency in this area.

Following is the listed lab of government as Examiner of Electronic Evidence

1. Cyber Forensic Laboratory, Army Cyber Group, DGMO, Signals Enclave, New Delhi
2. State Forensic Science Laboratory, Madiwala, Bangalore
3. Central Forensic Science Laboratory(CFSL), Hyderabad
4. Directorate of Forensic Science, Gandhi Nagar Gujarat
5. Computer Forensic and Data Mining Laboratory (CFDML), Serious Fraud Investigation Office (SFIO),
6. Notification of Forensic Science Laboratory Govt of NCT, Rohini New Delhi

1.5 INTRODUCTION TO COMPUTER EMERGENCY RESPONSE TEAM INDIA (CERT-In)

[135] The Impact of Technology on Organized Crime <https://www.sydneycriminallawyers.com.au/blog/the-impact-of-technology-on-organised-crime/>

CERT-In is a government body working under the ministry of electronics and information technology. It is operational since 2004. CERT-In is a national nodal industry responding to the computer security incident as and when they occur. As per the amendment in IT Act, CERTIN has been designated to serve the following functions in the area of cybersecurity as a national agency.[136]

- Collection analysis and examination of cyber incident.
- Forecast and alert cybersecurity incident.
- Co-ordination of cybersecurity responsibilities.
- Emergency measures for handling cybersecurity incidents.
- Issue guideline advisory, notes, whitepapers related to information security practices, procedures, preventions, response and reporting of cyber incidents.

CERTIN not only provides incident response services but also security quality management services. CERTs vision is to proactively contribute to securing cyberspace for India. CERTs mission to enhance the security of India's technology infrastructure through pro-active actions and effective collaborations. CERTIN has signed a memorandum of understanding with 7 countries of Shanghai Co-operation Organisation. With this MOU, participating countries can exchange technical information on cyber-attacks, incident response and solution to counter global cyber-attacks.

1.6 OBJECTIVES OF CERT-In

- Preventing cyber-attacks against the country's cyberspace.
- Enhancing security awareness among common citizen.
- Responding to cyber-attacks and minimizing the damage as well as recovery time.

CERTIN function on 24 hours basis on all days of the year including government and other holidays. The contact details of CERTIN are published on website www.cert-in.org.in

[136] Nouh, Mariam & Nurse, Jason & Webb, Helena & Goldsmith, Michael (2019) Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement

Following are the types of cybersecurity incident need to be reported to CERTIN

- Targeted scanning of critical network systems.
- Compromise of critical system information.
- Unauthorized access to IT systems.
- Defacement of website or intrusion of the website.
- Malicious code attacks such as spreading virus, worm, Trojan, botnet, spyware etc.
- Attacks on the server such as database, mail and DNS.
- Identity theft, spoofing phishing attacks.
- Denial of service and distributed denial of service attacks.
- Attack on critical infrastructure, SCADA systems and wireless networks.
- Attacks on applications such as e-commerce and e-governance.

1.7 CHALLENGES BEFORE LAW ENFORCEMENT AGENCIES

As technology has brought lots of many changes into every organization, Law enforcement agencies (LEA) are not the exception for it.[137] Many LEAs are going under transformation and still in the adoption phase for this technological advancements. Make in India and Digital India is the current era for our country. But we are still in the process of replacing traditional ways while these positive changes around us. This has created a crucial challenge in the field of investigations as well. Let's understand the real situation and challenges faced by LEA in this digital era.

1.8 CHALLENGES WHILE INVESTIGATION

Due to the use of technology by criminals in their act the speed of execution of any crime has increased a lot.[138] LEA has to compete with the speed of the fraudster. Criminals are real users of advanced technology and find out many new technological ways to commit crimes. LEA's challenges start from understanding the use of technology by criminals in the given scenario.

[137] S W Brenner Cybercrime: Criminal Threats from Cyberspace, 2nd Edition. Praeger Security International. ABC-CLIO, LLC, 2018

[138] Hunton, Paul Managing the technical resource capability of cybercrime investigation. A UK law enforcement perspective. Public Money & Management, 32(3):225–232, 2012

Let’s divide the changes faced by LEA into 3 categories:-

1) ***Pre Investigation***

a) Not clear Understanding of the Jurisdictions:-

Due to jurisdictional issues of the cyberspace, many Investigation officers are not clear about who should investigate the scenario which involves different geographically distant location. For example, Person who is living in Bangalore who is over business trip in Pune receives the SMS which says his debit card is used in Delhi and his bank belongs to Chennai. Such a Situation confuse the Investigation officer that which state investigation agency is the right authority to investigate the given situation.

b) Lack of technological background

Nowadays, Criminals are using technology not only in cybercrimes but also in traditional crimes. IO are mainly Police Inspectors which may not be from a technical background. It becomes very difficult for them to understand the overall situation and that’s why it affects the speed of execution

2) ***During Investigation***

A. Lack of technological expertise
B. Availability of the required equipment’s
C. Absence of standard operating procedures for investigation
D. In Adequate expert witness

3) ***During Court trials***

- Cross border investigation
- Admissibility of electronic evidence
- Hash Value calculation

One challenge computer investigators face is that while computer crimes know no borders, laws do. What's illegal in one country may not be in another. Moreover, there are no standardized

nternational rules regarding the collection of computer evidence. Some countries are trying to change that. [139]

1.9 DARK WEB (DARKNET)

The dark web, which is also called a darknet, is an encrypted portion of the internet which cannot be indexed by search engines. It is purposefully created portion of the internet which is not for public view. In order to access the dark web, the special anonymous browser is used. Websites on the dark web have an unconventional naming structure. Hence, anyone who wants to access such websites needs to know them in advance.

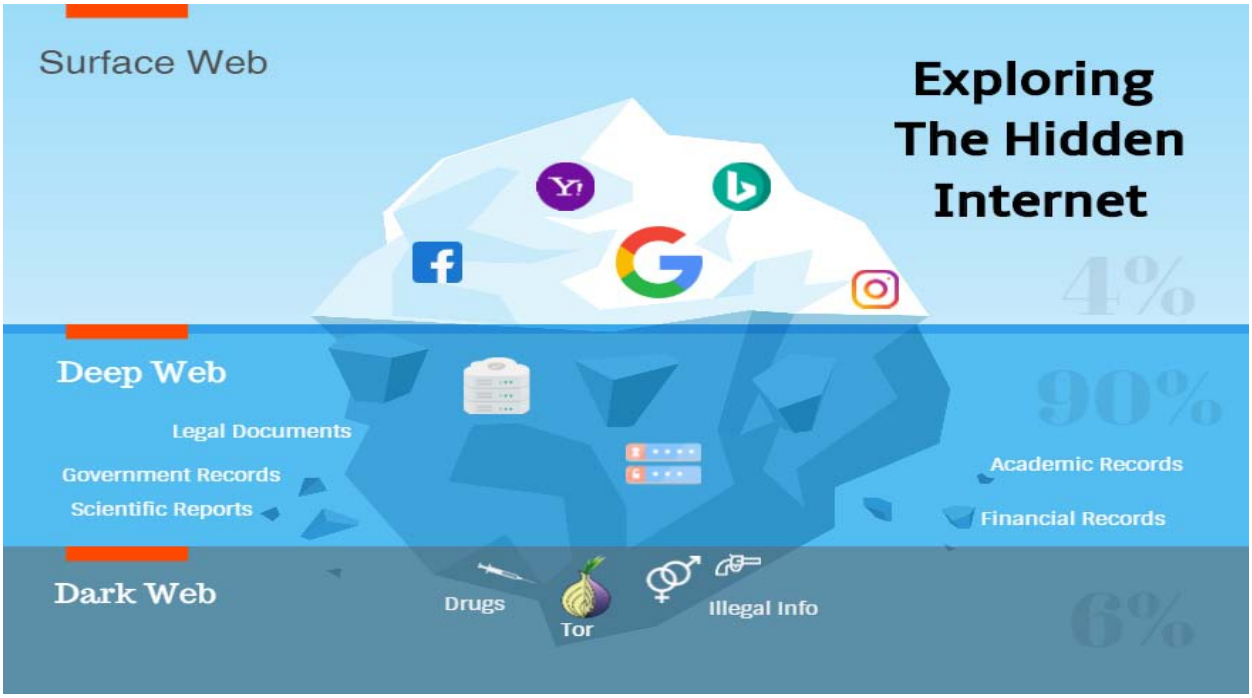


Figure 4.1:- The Internet is like an iceberg where most of the people can see only the surface and majority of the portion stays hidden.

The World Wide Web is considered as an iceberg, in which the regular sites that common people visit is the top layer of the iceberg. This includes common sites such as Wikipedia, Google and

[139] Scott R Senjo An analysis of computer-related crime: Comparing police officer perceptions with empirical data. Security Journal, 17(2):55–71, 2004

even the millions of blogs that come and go daily. This portion is just 4% of the overall internet is known as surface web.[140]

Then it comes the portion of the deep web in which personal records, government documents and confidential information which are not meant for public view and are understandably kept safe. This information forms an ecosystem for many surface web applications. Hence, they are many times directly connected to the surface web. In order to dive into the Deep web pages one has to know that URL beforehand.[141]

The dark web is the underworld of the internet. It is the subsection of the deep web. But if anyone who is seeking access to Dark web pages, requires special software with the correct decryption key, as well as access rights and knowledge of where to find the content. The Dark Web is slightly more complicated because most of the times it runs on networks of the private servers, allowing communication only via specific means. This enables a high degree of anonymity and makes it difficult for authorities to shut down or monitor it.

If a cyber-attacker hacks into your organization and exfiltrates valuable business information such as customer records, or a disgruntled insider decides to try and sell some stolen intellectual property, they will simply prefer the dark web.

Unfortunately, the highest amount of anonymity and privacy has led to Dark Web to become a place where many illegal activities take place.[142]

DARK WEB BROWSER

Accessing the dark web requires the use of an anonymizing browser which is called Tor. It is free software that users download from the Internet to anonymously access the dark web.

Thousands of volunteers around the globe host and operate series of proxy servers through which tor browser routes the webpage request, rendering the real IP address unidentifiable and untraceable.

[140] Michael Chertoff and Toby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, Paper Series: No 6, February 2015, p 1

[141] Verisign, The Domain Name Industry in Brief, Volume 13, Issue 3, September 2016. A top-level domain is one at the top of the Internet's domain name system (DNS) hierarchy. For instance, the top-level domain is .com

[142] Stephanie Pappas, "How Big Is the Internet, Really?," Live Science, February 18, 2016

This process works well for the anonymity and privacy of the user, the Tor browser experience is typically unreliable and slow. One does not have direct control over his surfing because it is routed through different server hence use of credential seems to be unreliable via such service.

DARK WEB WEBSITES

The websites which are hosted over the surface web have ended in .com or other common suffixes, but the dark web URLs typically end in .onion which is a special-use domain suffix. Dark web sites are not easy to remember as well because of its URLs are a mix of letters and numbers. For example, one of the most infamous dark web marketplaces was the Silk Road, best known for selling illegal drugs that was eventually busted by the FBI which went by the URLs silkroad6ownowfk.onion and silkroad7rn2puhj.onion.

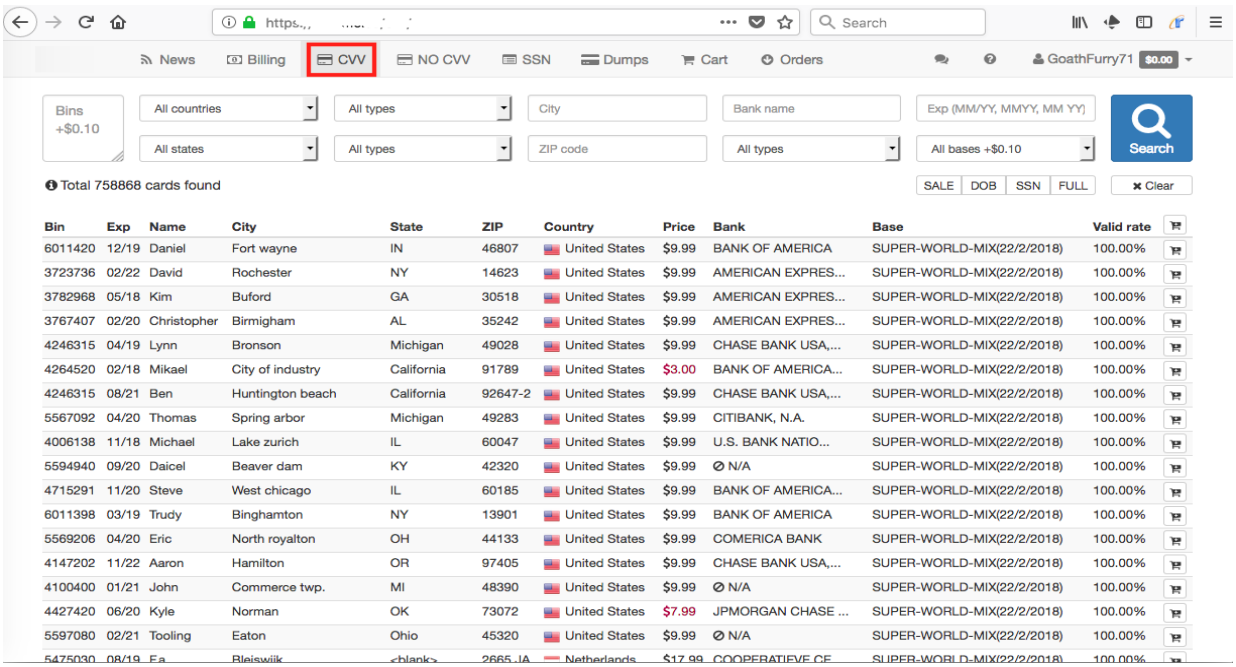
WHAT YOU CAN DO AT DARKNET?

As darknet is famous for anonymous surfing one can buy credit card numbers, all types of drugs, guns, counterfeit money, stolen subscription credentials, hacked subscription like Netflix accounts and software that is created and used by criminals to break into someone's computer. One can buy login credentials to a $50,000 Bank of America account for $500 or get $3,000 in counterfeit $20 bills for $600. One can buy illegal drugs with express shipping included in it. One can hire a hacker to attack computers for you. One can buy a lifetime subscription for Netflix account or pornographic websites just for 6$. One can buy usernames and passwords of business rivals.[143]

Hence, more legitimate companies are beginning to have a presence on the dark web. The cryptocurrency is very much useful for the users who can purchase anything on the dark web without revealing their identity.

Darknet acts as freedom which is given at large to do whatever you want without being identified. This thing provokes the criminal intentions of the person to strongly come out and to be followed by one.

[143] Andy Greenberg, "An Interview with Darkside, Russia's Favorite Dark Web Drug Lord," Wired.com, December 4, 2014



Bin	Exp	Name	City	State	ZIP	Country	Price	Bank	Base	Valid rate
6011420	12/19	Daniel	Fort wayne	IN	46807	United States	$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
3723736	02/22	David	Rochester	NY	14623	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3782968	05/18	Kim	Buford	GA	30518	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3767407	02/20	Christopher	Birmigham	AL	35242	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	04/19	Lynn	Bronson	Michigan	49028	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4264520	02/18	Mikael	City of industry	California	91789	United States	$3.00	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	08/21	Ben	Huntington beach	California	92647-2	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5567092	04/20	Thomas	Spring arbor	Michigan	49283	United States	$9.99	CITIBANK, N.A.	SUPER-WORLD-MIX(22/2/2018)	100.00%
4006138	11/18	Michael	Lake zurich	IL	60047	United States	$9.99	U.S. BANK NATIO...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5594940	09/20	Daicel	Beaver dam	KY	42320	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4715291	11/20	Steve	West chicago	IL	60185	United States	$9.99	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
6011398	03/19	Trudy	Binghamton	NY	13901	United States	$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
5569206	04/20	Eric	North royalton	OH	44133	United States	$9.99	COMERICA BANK	SUPER-WORLD-MIX(22/2/2018)	100.00%
4147202	11/22	Aaron	Hamilton	OR	97405	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4100400	01/21	John	Commerce twp.	MI	48390	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4427420	06/20	Kyle	Norman	OK	73072	United States	$7.99	JPMORGAN CHASE ...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5597080	02/21	Tooling	Eaton	Ohio	45320	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
5475030	08/19	Ea	Bleiswijk	<blank>	2665 JA	Netherlands	$17.99	COOPERATIEVE CE	SUPER-WORLD-MIX(22/2/2018)	100.00%

Figure 4.2:- stolen card details are sold in the underground market on the Internet.

DARKNET USERS

Out of the billions of internet users accessing the internet on an everyday basis, Dark Web use remains around 3 per cent. Because of the nature of stuff over the dark web, one can easily understand that the dark web is mainly used by criminals, terrorist and activist but that is not the only case.[144]

The ethical use of the dark web is done by law enforcement or threat intelligence agencies. Security professionals may search through the dark web for signs of security or data breaches, evidence of illegal activity or newly emerging cyber threats. The dark web also hosts a large amount of educational information that cannot be found elsewhere, such as banned books, collections of news articles and discussion forums.

DANGERS OF THE DARK WEB

[144] Beshiri, Arbër & Susuri, Arsim (2019) Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications.

Accessing the dark web and using the tools or services found there, can be associated with high risks for an individual user or an enterprise. A few dangers that users should be aware of before browsing the dark web includes:

- Unknown Infection of viruses or malware especially ransomware,
- Installation of spyware such as key loggers.
- Infection of the system with Remote access tools (RAT) with new signatures.
- Distributed denial of service (DDoS) attacks.
- Identity theft, credential theft or phishing.
- Compromise of personal, customer, financial or operational data.
- Leaks of your own intellectual property or trade secrets.
- Spying, webcam hijacking or cyberespionage.

DARK WEB FROM LAW ENFORCEMENT VIEW POINT

Use of the dark web brings in unique challenges for law enforcement agencies in India. The law enforcement officer feels that if there were some police presence on the dark web, they will be in a better position to deal with the possible attack. Cyber experts say that some officers go undercover on the dark web to keep track of illegal activities going on there. That monitoring the dark web can help to boost cybersecurity, identify breaches and vulnerabilities. An officer said that prior to the Cosmos Bank fraud in Pune in which Rs 94 crore was fraudulently transferred from the bank, there was chatter on the dark web about people looking for details on Indian banks. This shows the Indian LEA officers mainly believes gathering evidence on the dark web activity is comparatively difficult but not impossible.[145]

In order to combat with such highly technical types of criminal activities, there is a need for police officers to be trained in changing cyber trends who are dedicated only to cyber-crime and not transferred to other police units. Hence, this leaves us with the hope that the expert criminals

[145] Dilipraj, E (2014) Terror in the Deep and Dark Web. 9. 121-140

cannot permanently hide in places like darknet and they are under radar even they stay in this underworld of the internet.

1.10 LET'S SUM UP

In this chapter, we have studied about the cyber forensic labs and the structure of it. We also studied about Computer emergency response team India and its objectives. Finally, we ended the discussion with the Dark web and challenges while investigation.

1.11 FURTHER READING

- Saran, Vaibhav & A.K.GUPTA,. (2014). Cyber Crime & Their Forensic Investigation.
- Yeboah-Boateng, Ezer & Akwa-Bonsu, Elvis. (2016). Digital Forensic Investigations: Issues of Intangibility, Complications and Inconsistencies in Cyber-crimes. Journal of Cyber Security and Mobility. 4. 87-104. 10.13052/jcsm2245-1439.425.
- Ficci.in (2019), http://ficci.in/spdocument/22982/FICCI%20-%20EY%20Report%20-%20Confronting%20the%20New%20Age%20Cyber%20Criminal.pdf (last visited Nov 27, 2019).
- Digitalcommons.law.scu.edu (2019), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1219&context=scujil (last visited Nov 27, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Summarize about cyber forensic lab structure?**

- Lab Space
- Required Equipments
- Appropriate Software
- Cyber Forensic Expert

- SOP(Standard Operating Procedure)
- Training and upgradation

2. What is CERT-In?

CERT-In is a government body working under the ministry of electronics and information technology. It is operational since 2004. CERT-In is a national nodal industry responding to the computer security incident as and when they occur.

3. What are the objectives of CERT-In?

- Preventing cyber-attacks against the country's cyberspace.
- Enhancing security awareness among common citizen.
- Responding to cyber-attacks and minimizing the damage as well as recovery time.

4. What is the Dark Web?

The dark web, which is also called a darknet, is an encrypted portion of the internet which cannot be indexed by search engines. It is purposefully created portion of the internet which is not for public view. In order to access the dark web, the special anonymous browser is used. Websites on the dark web have an unconventional naming structure. Hence, anyone who wants to access such websites needs to know them in advance.

1.13 ACTIVITY

Briefly explain what is dark web, how it is being used and the dangers pertaining to it? Elucidate the illicit activities that has been taking place via the dark web with a case study? (1000 words)