LAW INSIDER

DIGITAL EVIDENCE AND DIGITAL FORENSICS

FINAL SESSION

LI

Investigation

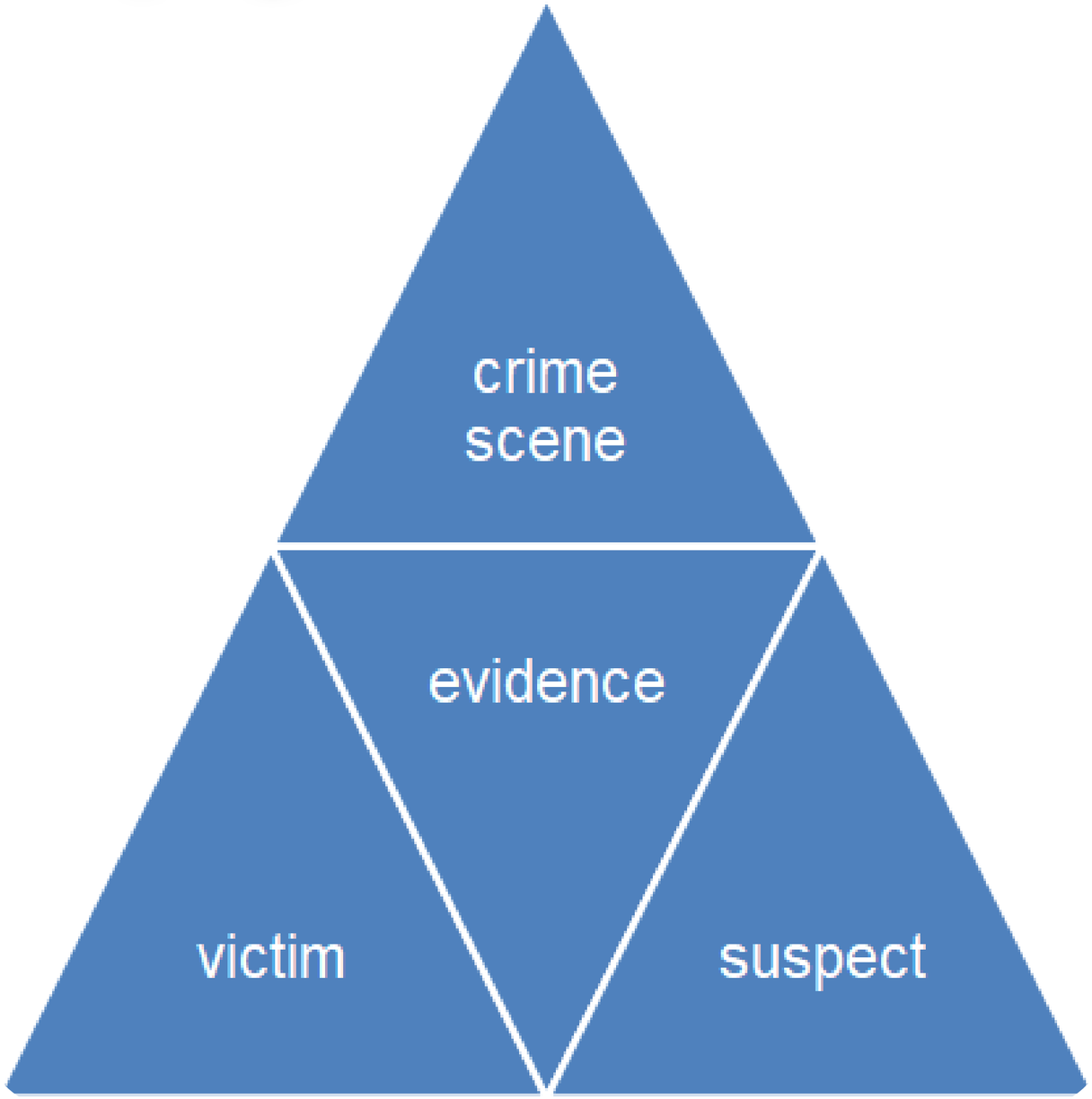
- Collect evidence
- Arrive at key issues to be investigated
- Complete the investigative findings

Judicial Process

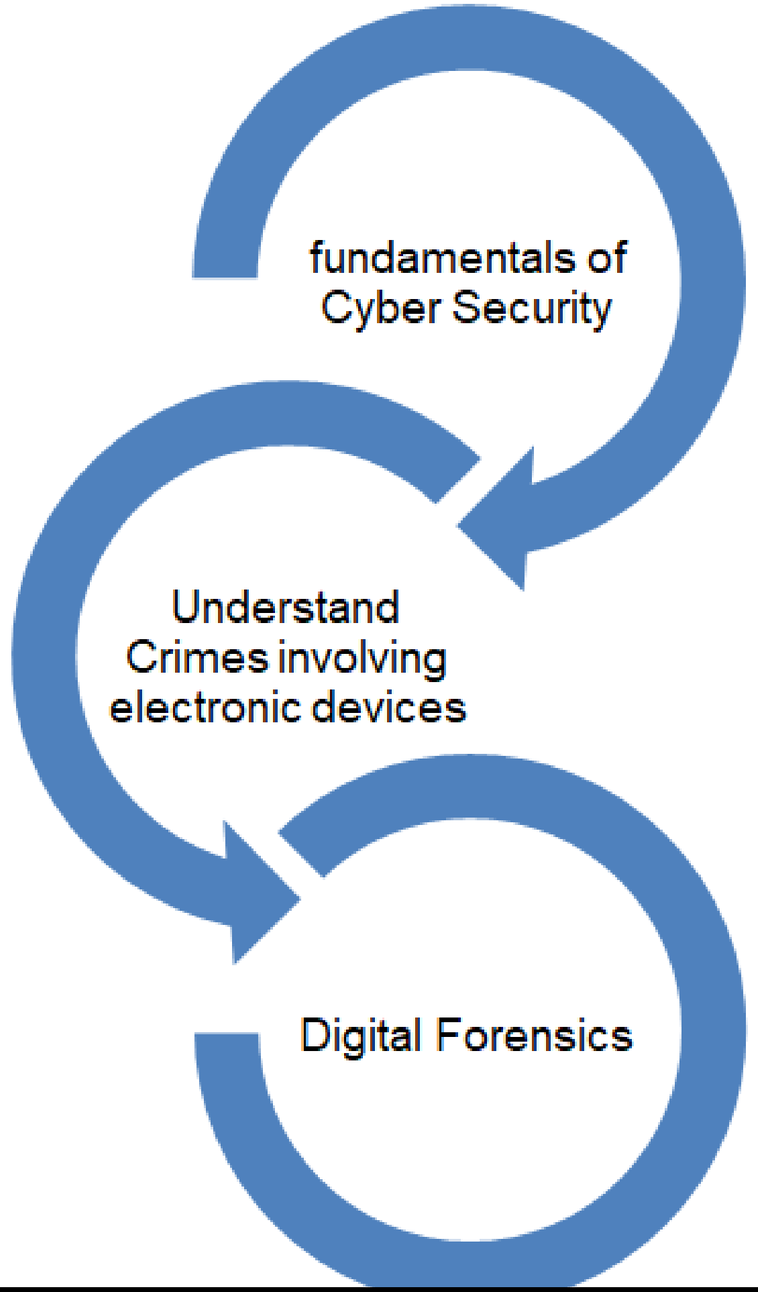
- Used to prove or disprove facts
- Foundation of litigation process like arguments
- Verdict is always based on Evidence
- Best and unimpecheable

WWW.LAWINSIDER.IN

Interplay of elements of Crime



WWW.LAWINSIDER.IN



LI
WWW.LAWINSIDER.IN

Cyber security and Cyber Crime

Cyber Security- Attempts to protect Computing Devices, Network, Computer Programs, Data therein from unauthorized access, attack, damage or modification.

SECURITY is inversely proportional to AVAILABILITY

The Confidentiality–Integrity–Availability triad

Protection from

- unauthorised access
- unauthorised use
- disclosure

Ensures:

- Authorised access
- Redundancy
- Prevention of data loss

Alteration of information

- In storage
- In transit
- In process

LI

CYBER CRIME ATTACKS EACH OF THE PILLARS OF CIA TRIADE

Confidentiality-

Stealing of your information like bank details, your mobile OTP

or your personal pictures

Integrity-

Changing the contents of the information stored therein

Availability-

Making your device inaccessible-Ransomeware, DDOS attacks

Cyber security focusses on protection of each of these areas:-

Confidentiality
identification of an object of person
user-id & passwords
biometrics
access cards

Integrity
change detections
checksum
backups
at rest and in transit

Availabilty
ensuring access to information even if compromised
hardware redundancies
software updates
backup and recovery

LI

Section 43A in The Information Technology Act, 2000

Compensation for failure to protect data. –Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

LI

LI

Explanation. –For the purposes of this section,–

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

WWW.LAWINSIDER.IN

LI

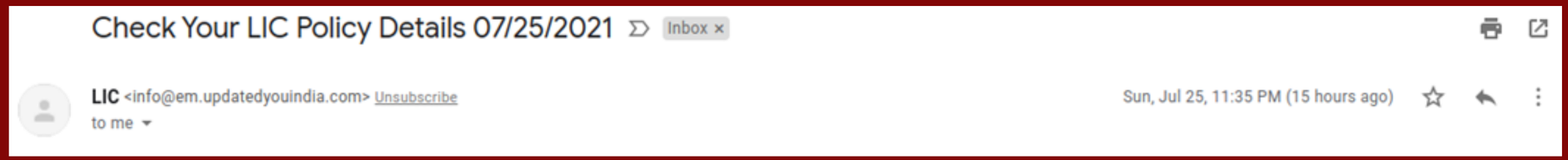
Aims of Cyber Security

Take reasonable precautions to make the task of attacker as difficult as possible because there is nothing called 100% security.

Basic levels of Security Controls

- Use Anti-Virus(updated)
- Update all your software like windows/android/iOS/Adobe.....
- Use two factor authentication where ever possible(OTP)
- Always use mix or pattern and passwords(mobile devices)
- Block all unsolicited calls/messages
- Always access only https://....sites
- Whenever accesing any bank/credit card site look for Norton SECURED powered by Symantec or similar

Whenever replying or acting any email, do read the email id you are replying to-



- Always use updated browser e.g Microsoft Edge and not Internet Explorer

HACKING IS FUN ! .....NOT REALLY, IT's A SERIOUS BUSINESS

Disclaimer: Every content shown, communicated or demonstrated is for education and training purpose only and only for the targetted audience. Any misuse or absue of any or all of this content can cause serious harm to the user or on whom it is used. Such actions are against the law and can lead to serious consequences including criminal prosecution and claims for damages.

PLEASE DO NOT TRY ANY OF THIS UNLESS YOU ARE SURE YOU CAN AFFORD TO BE CALLED AS CRIMINAL OR ARE WILLING TO PAY DAMAGES.

LI

Ethical or UnEthical–Steps followed

Information Gathering/Reconnaisance/Footprinting

Passive–OSINT, Publically Available Information

Active–Social Engineering, Dumpster Diving

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

LI

Anonymity

CONVENIENCE DISCLAIMER

least private and secure
most convenient

casual surfing
shopping
social media

Most private and secure
least convenient

discrete
shopping/social media
against the law
dark web
stalking/investigations

LI

Level1- Basic security posture required when ever you use your device password protection/biometrics

Level 2 – Hiding your identity multiple identities/alter egos

Level 3 – Hiding your Digital Footprint (anonymity on Web)

Level 3 – Hiding your Digital Footprint (anonymity on Web)

LI

InCognito Mode
VPN
TOR(The Onion Router)
ProxyChains
OS on Disk

Investigations

VPN–Virtual Private Network(Access the unaccessible)

IPv4 Address	**193.32.85.33** **Hide my IP with VPN**
IPv6 Address	**Not detected**
IP Location	Moscow, Moskva (RU) [Details]
Proxy	No proxy present
Device Type	Linux
OS	Linux
Browser	Chrome
User Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Screen Size	1600px X 900px
Cookie	Enabled
Javascript	Enabled

99% Anonymity with TOR Browser

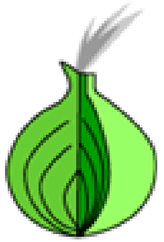
https://www.torproject.org/download/

WWW.LAWINSIDER.IN

Congratulations. This bro

https://check.torproject.org

This page is also available in the following languages: English Go



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **89.144.12.17**

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Relay Search.

Donate to Support Tor

Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous

LI

WWW.LAWINSIDER.IN

https://whatismyipaddress.com

WhatIs MyIPAddress .com

Enter Keywords or IP Address...

Search

ABOUT PRESS BLOG CONTACT

MY IP | IP LOOKUP | HIDE MY IP | VPNS ▾ | TOOLS ▾ | LEARN ▾

My IP Address is:

IPv6: ? 2a0b:f4c0:16c:1::1

IPv4: ? 185.220.100.255

My IP Information:

ISP: F3 Netze e.V.
Services: Network Sharing Device
City: Firuzabad
Region: Fars Province
Country: Iran

Your private information is exposed!

HIDE MY IP ADDRESS NOW

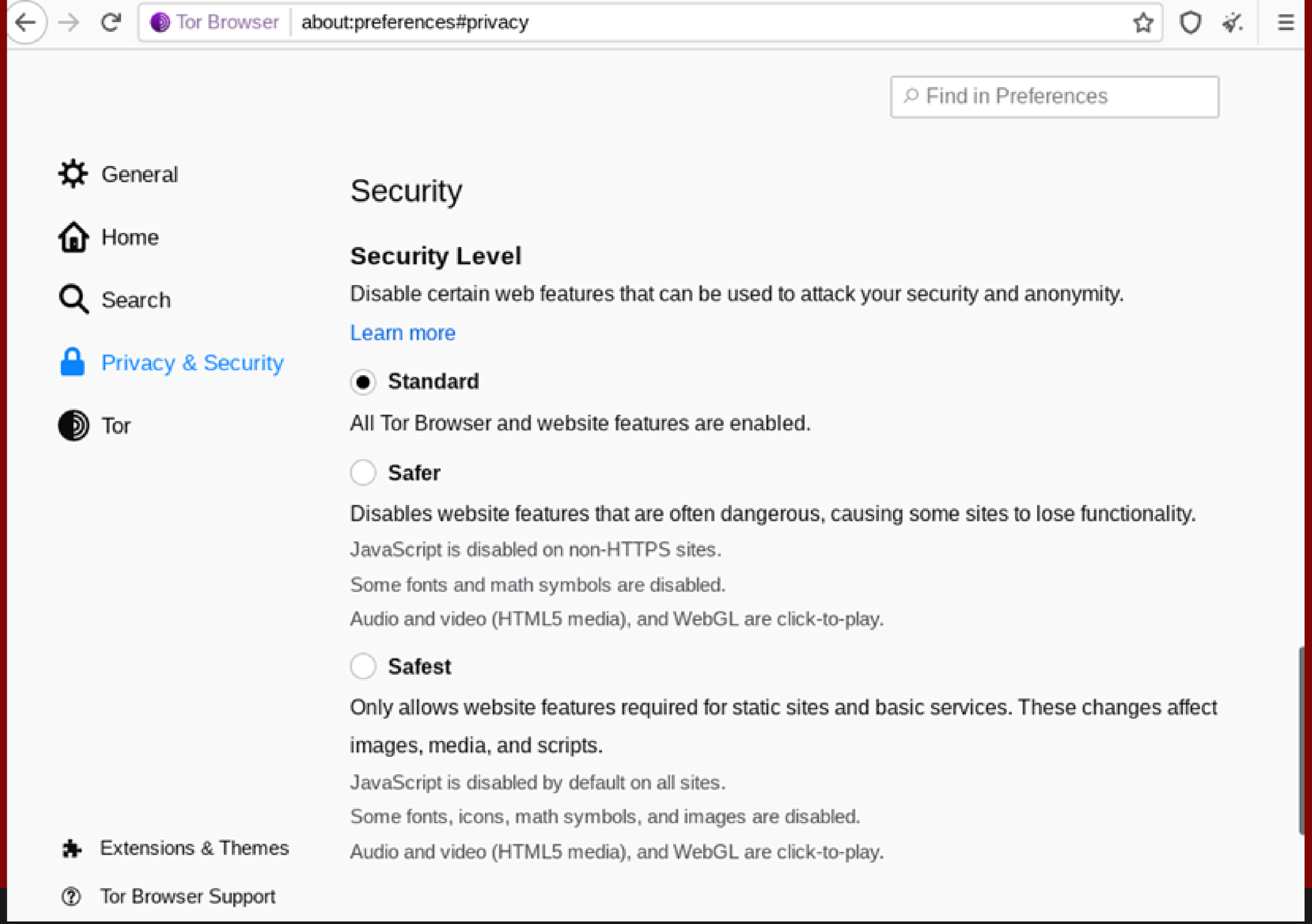
Show Complete IP Details

Location not accurate?

Update My IP Location

LI

WWW.LAWINSIDER.IN



LI
WWW.LAWINSIDER.IN

Complete Anonymity

WWW.LAWINSIDER.IN

Google Fu

Information Gathering–Passive

Investigation with image reverse search

Metadata in images case study   Metadat viewer

Location identification from photo or video

Advanced Search operators

Estimating time using shadow in a photo

When and where image was taken

Information Gathering–Passive

Recovering Deleted data with Photorec

OSINT domain lookup

Mr E

Information Gathering–Active

Burner mobile numbers

Disposable Email Id

LI

WWW.LAWINSIDER.IN

Learning Objectives

Develop the mindset of a computer forensics examiner

Understanding various methoidologies

Understand abd develop skills used by examiners

Exposire to few examining tools

Forensics Case studies

John F Kennedy Assasination

Mysterious death of Napolean

Who, What, When, Where, How, Why?

How is Computer Forensics different

- Cause and Effect across multiple continents.
- Technology evolving on daily basis.
- Offenders may be far more educated and skilled than investigators.
- Volumes of Data involved.
- Technical Incompetence of investigators, prosecutors, defense and even judges. .
- Data/Information has to be always read within context

How is Computer Forensics different?

- Cause and Effect across multiple continents
- Technology evolving on daily basis
- Offenders may be far more educated and skilled than investigators
- Volumes of Data involved
- Technical Incompetence of investigators, prosecutors, defense and even judges
- Data/Information has to be always read within context

LI

Why We Need Computer Forensics?

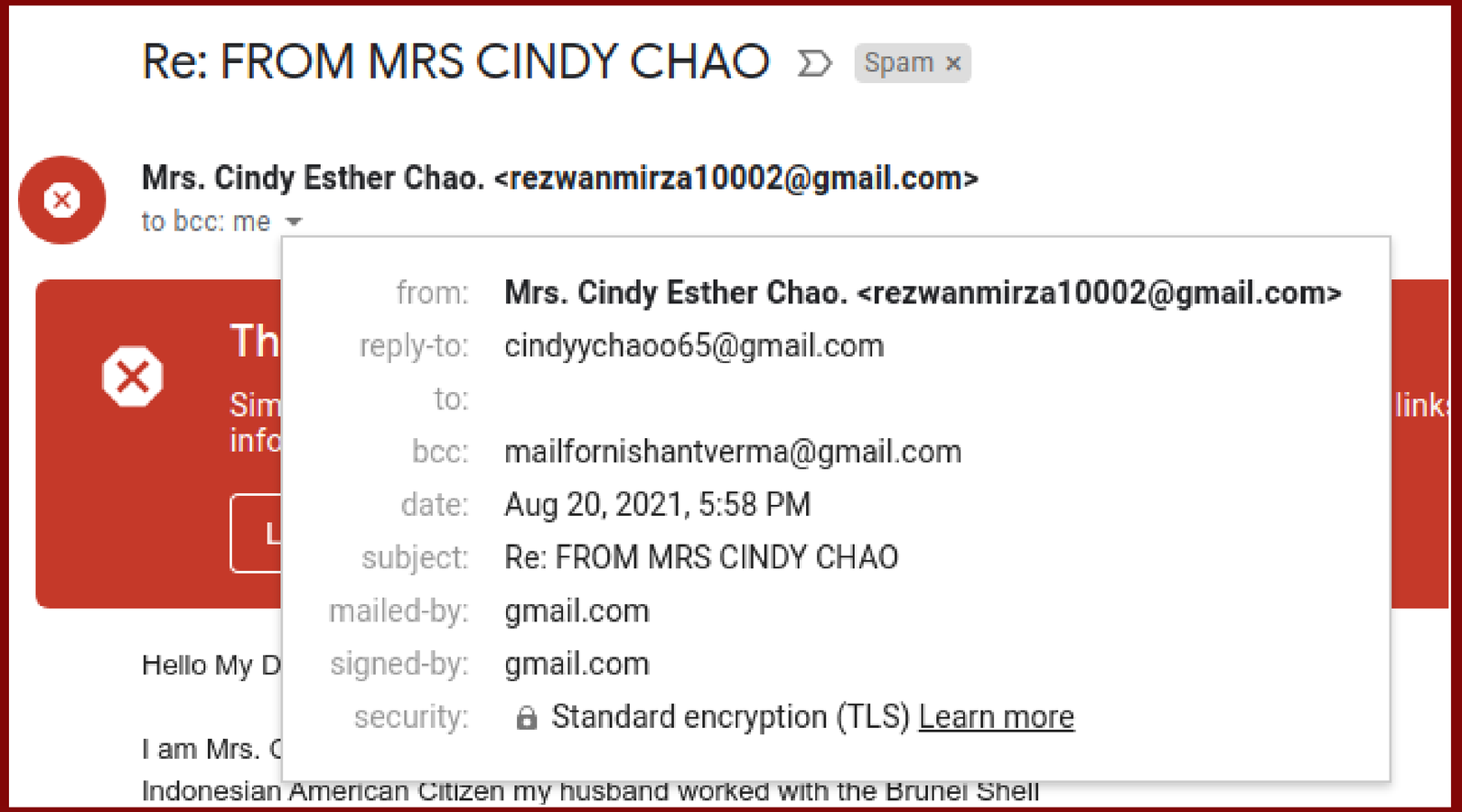
- Inappropriate Use of Computer Systems
- Determining a Security Breach
- Detection of Disloyal Employees
- Evidence for Disputed Dismissals
- Malicious File Identification
- Theft of Information Assets
- Forgeries of Documents

LI

Computer Forensics in Action

- Email Forensics/Investigation
- Comupter Data Investigation(Autopsy)
- Mobile Device Investigation

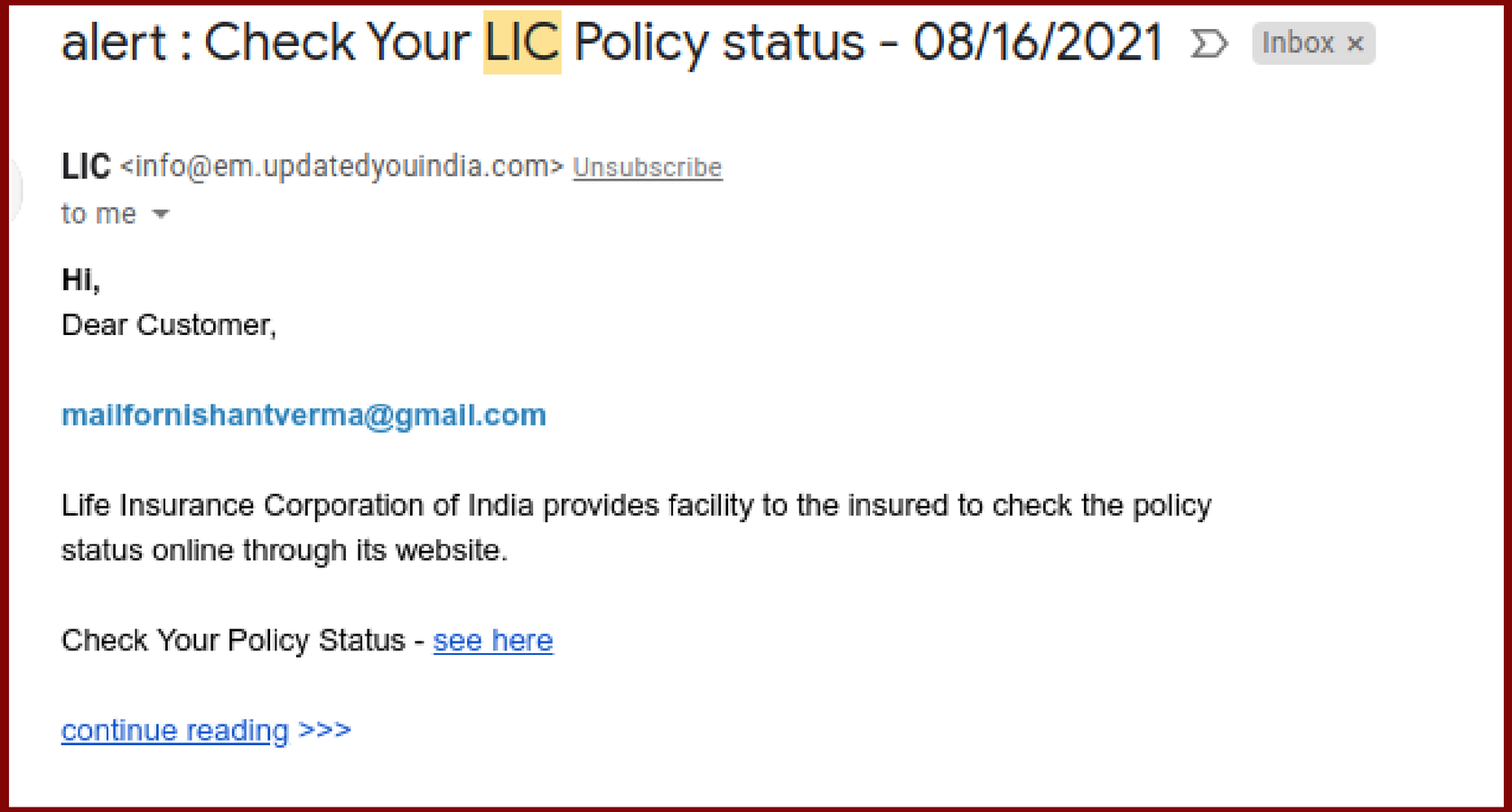
EmailForensics in Action



- microsoft.com
- rnicrosoft.com

- hdfcbank.com
- hdfc-bank.com

EmailForensics in Action


alert : Check Your LIC Policy status - 08/16/2021 Inbox ×

LIC <info@em.updatedyouindia.com> Unsubscribe
to me

Hi,
Dear Customer,

mailfornishantverma@gmail.com

Life Insurance Corporation of India provides facility to the insured to check the policy status online through its website.

Check Your Policy Status - see here

continue reading >>>

- microsoft.com
- rnicrosoft.com

- hdfcbank.com
- hdfc-bank.com

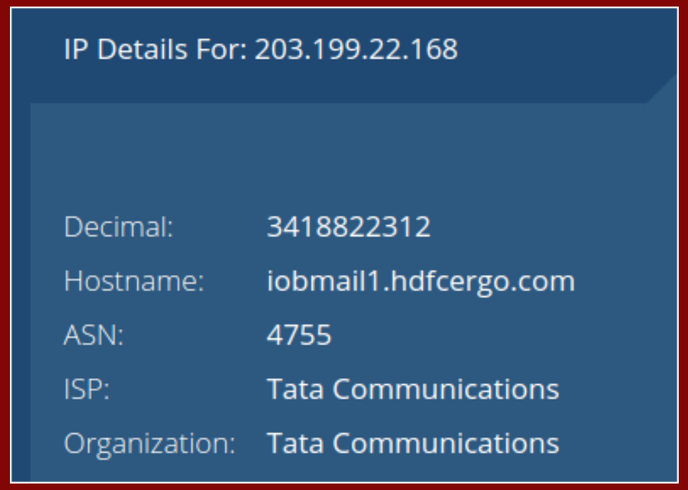
EmailForensics in Action

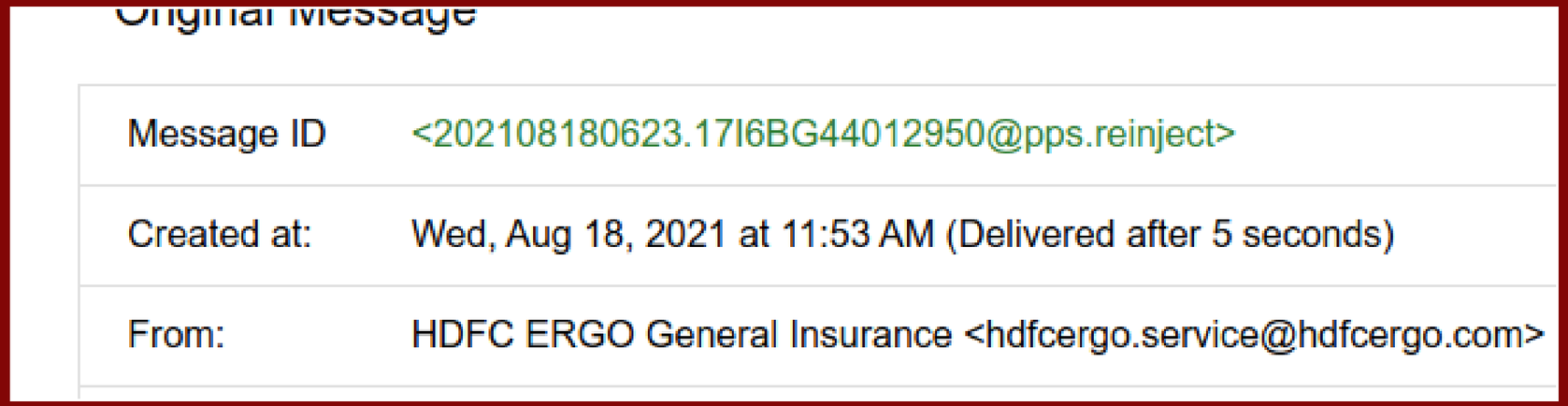
Original Message

Message ID	<CANgfO9dUuO5y6=wWEd+a6mPWG9qW5LPzZBr8yu3jPSOYqozgXg@mail.gmail.co
Created at:	Fri, Aug 20, 2021 at 6:01 PM (Delivered after 1 second)
From:	"Mrs. Cindy Esther Chao." [illegible]

```
X-Gm-Message-State: AOAM533JZDxePGF9PUfgYAMfg/aZxL0ZrpTyJibRLw6plpGMmGcuyR71 4CymcZ+Rzm4+fMWAlVlTQAXsZdiBwJ3hJ15BU5w=
X-Google-Smtp-Source: ABdhPJzHKLA2pm8PNqOBpwRG6ft2upjhP7mzS3ldVzwH5sfTzSaXVmgUSGdImd62glZZTYpGNm5qzdMrC5idmzg+fPg=
X-Received: by 2002:a05:6902:4ca:: with SMTP id v10mr25822689ybs.149.1629462712145; Fri, 20 Aug 2021 05:31:52 -0700 (PDT)
MIME-Version: 1.0
Received: by 2002:a25:b221:0:0:0:0:0 with HTTP; Fri, 20 Aug 2021 05:31:51 -0700 (PDT)
Reply-To: cindyychaoo65@gmail.com
From: "Mrs. Cindy Esther Chao." <rezwanmirza10002@gmail.com>
Date: Fri, 20 Aug 2021 20:31:51 +0800
Message-ID: <CANgfO9dUuO5y6=wWEd+a6mPWG9qW5LPzZBr8yu3jPSOYqozgXg@mail.gmail.com>
Subject: Re: FROM MRS CINDY CHAO
To: undisclosed-recipients:;
Content-Type: text/plain; charset="UTF-8"
Bcc: mailfornishantverma@gmail.com
```

EmailForensics in Action






```
Return-Path: <hdfcergo.service@hdfcergo.com>
Received: from antispam10.hdfcergo.com (iobmail1.hdfcergo.com. [203.199.22.168])
        by mx.google.com with ESMTPS id o12si4886482pfu.229.2021.08.17.23.23.26
        for <MAILFORNISHANTVERMA@gmail.com>
```

Future of Computer related offences

- Crimes involving Robots(TERMINATOR)
- Artificial Intelligence
- Machine Learning

Question of law vs. Question of fact

Computer Forensics-Conclusion

- Much beyond the definition of Cyber Crime
- Required in both Civil and Criminal cases
- Expect Investigation to be faulty and questionable
- Involve external Cyber Forensic expert at the earliest
- READ-STUDY-UPGADE
- Can help establish yourself agianst the so called multi generation law families and senior advocates who know tricks that will soon be obsolete.

LI

We Appreciate your Time

Thank You!

WWW.LAWINSIDER.IN