SNS COLLEGE OF ENGINEERING

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

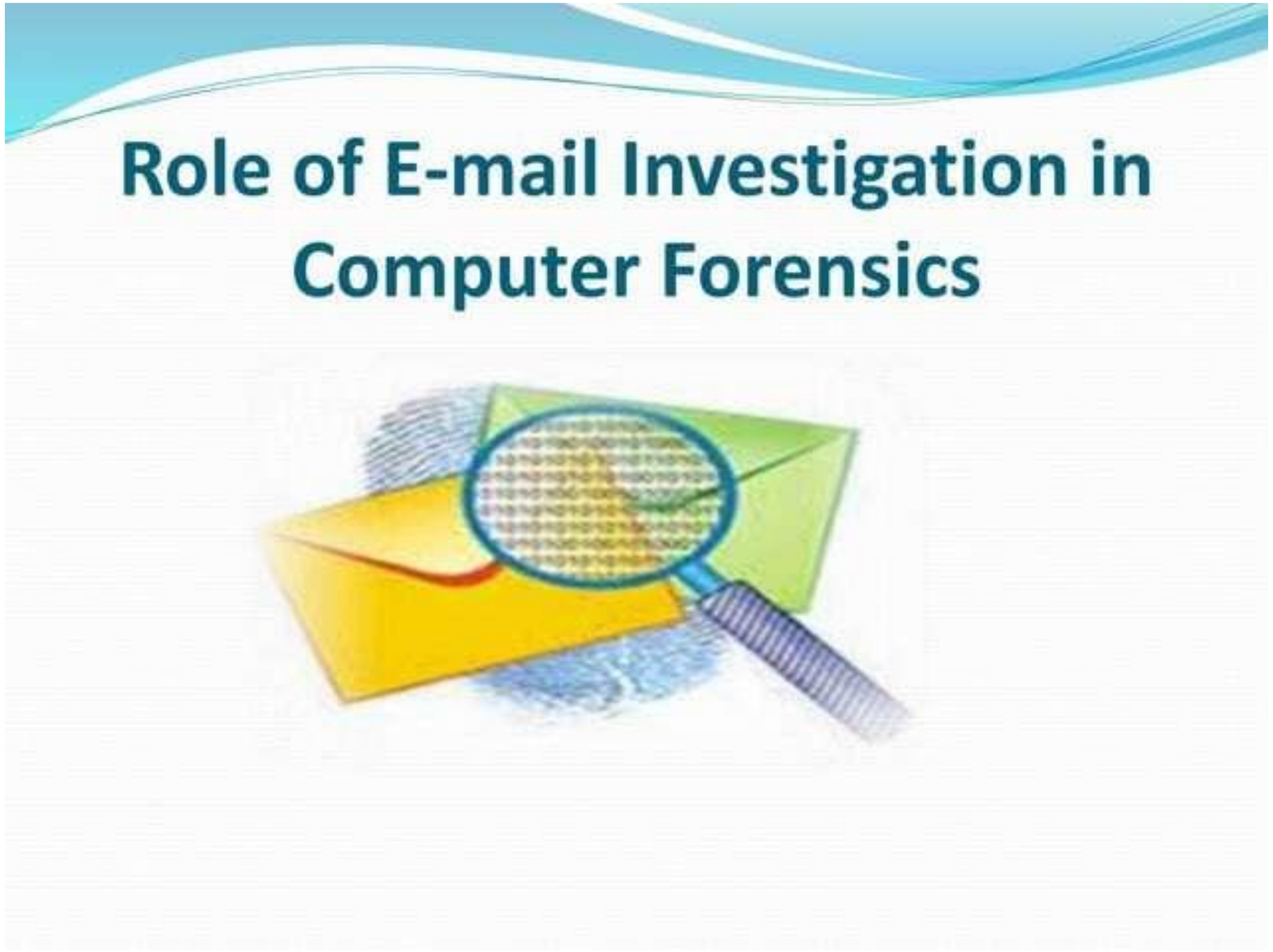
DEPARTMENT OF CSE (IoT, Cyber Security including Blockchain Technology)

19SB502 – CYBER FORENSIC AND INVESTIGATIONS

III YEAR/ V SEMESTER

UNIT 3 – ANALYSIS AND VALIDATION

TOPIC 3 – Email investigations

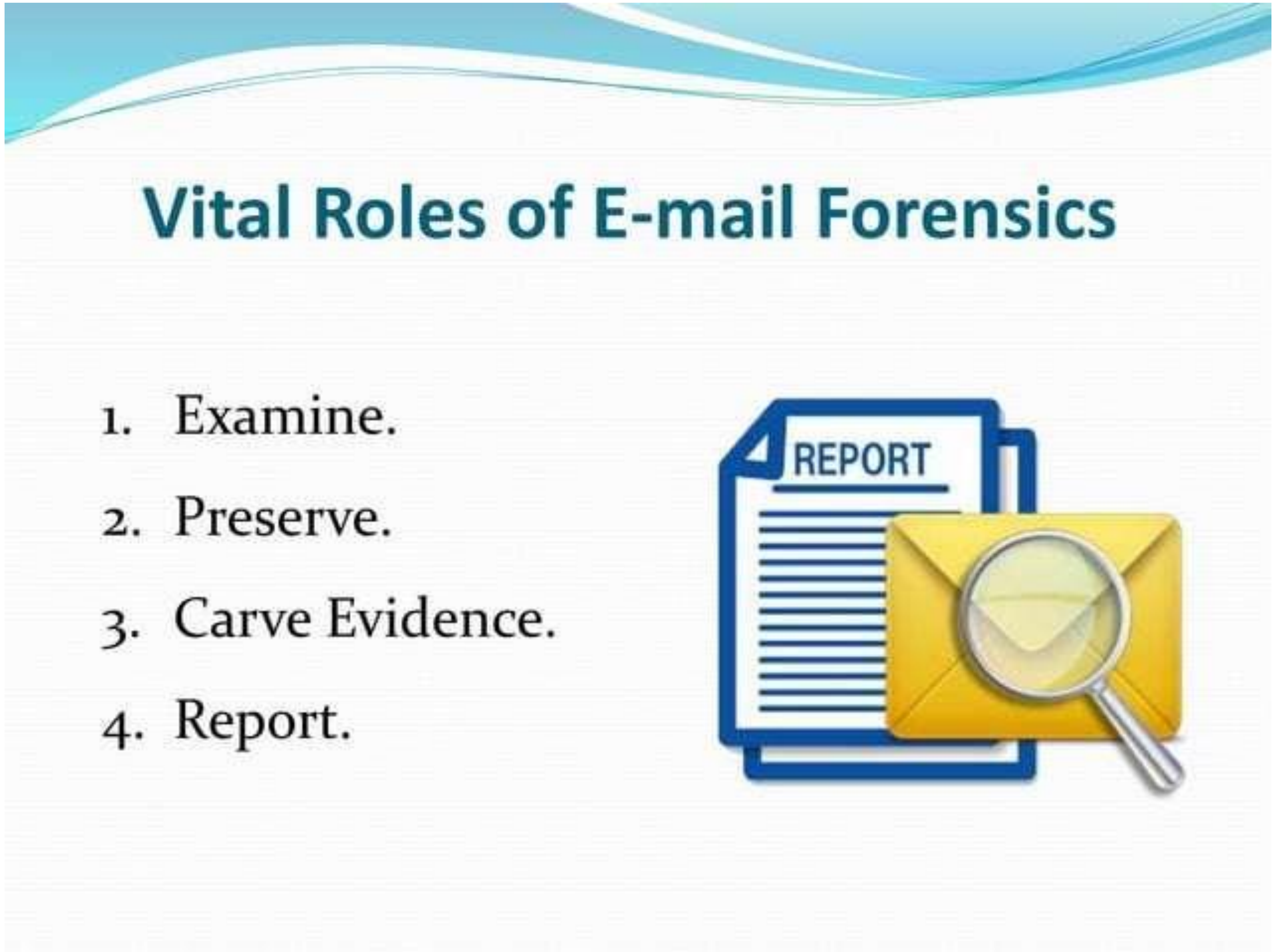


Role of E-mail Investigation in Computer Forensics

❖ Introduction

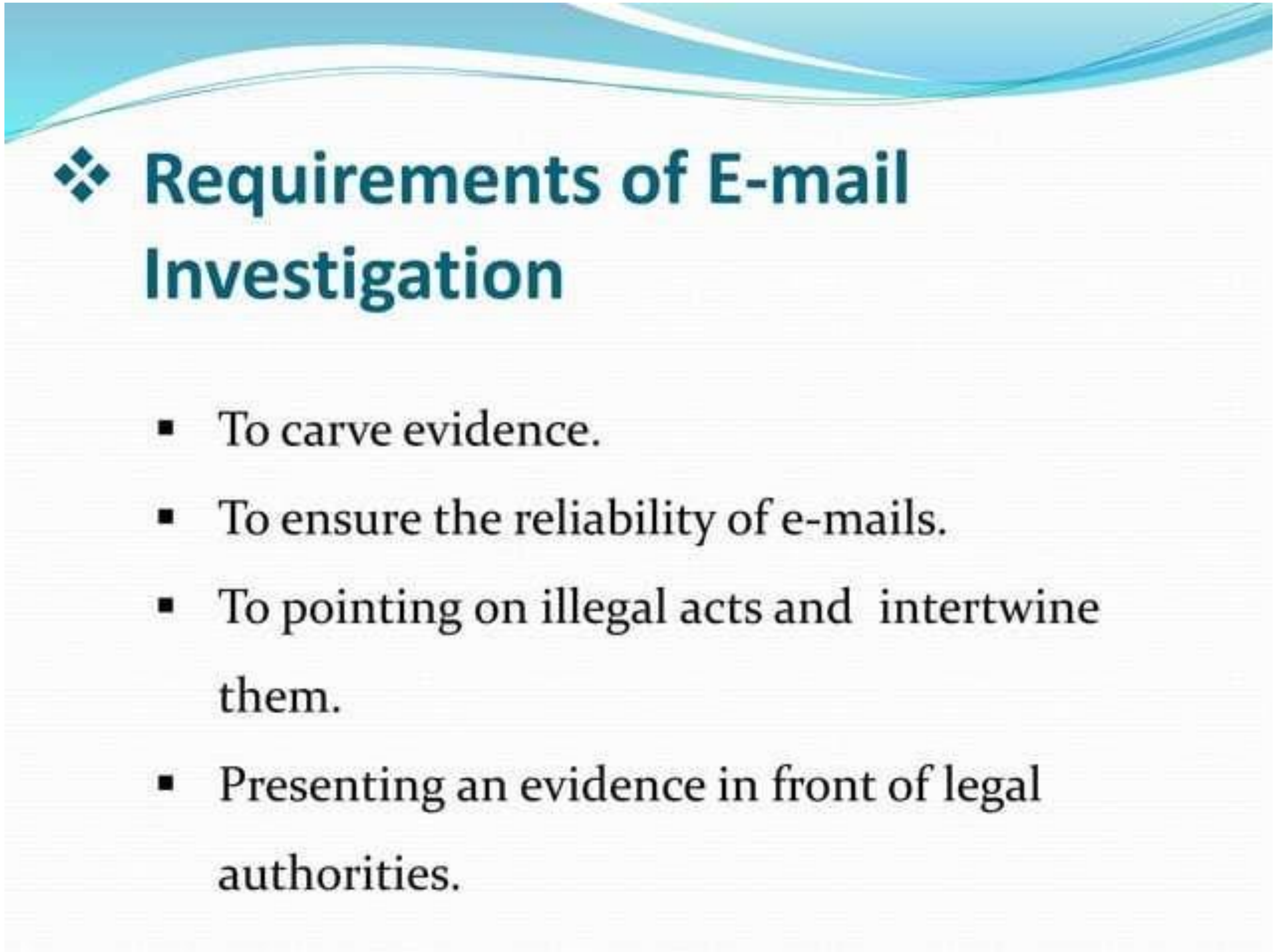
What is E-mail investigation?

"E-mail investigation is a digital forensics process of finding out evidences from suspect emails that allows investigator to examine, preserve, and reveal digital evidence"(branch of forensics science).



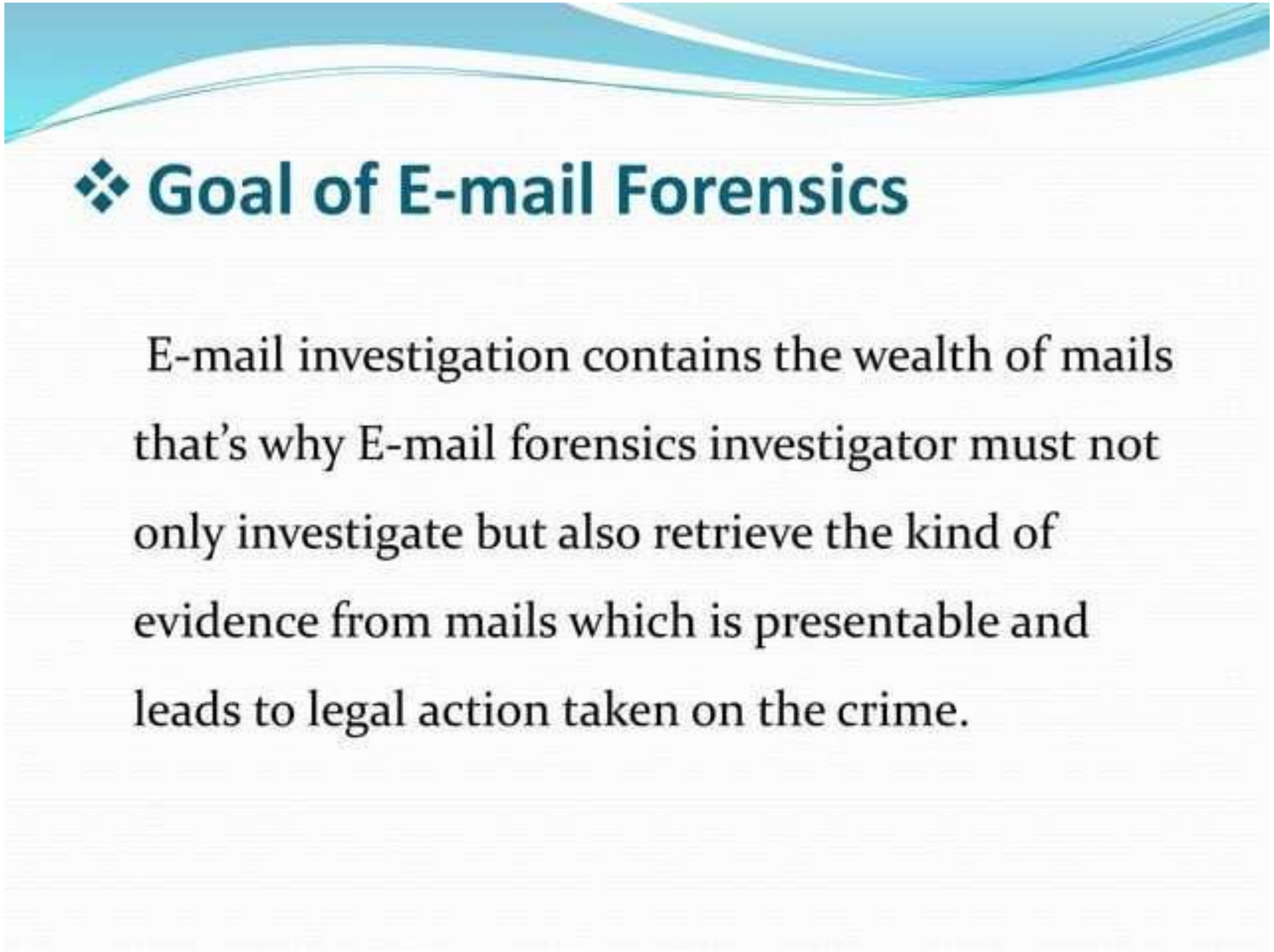
Vital Roles of E-mail Forensics

1. Examine.
2. Preserve.
3. Carve Evidence.
4. Report.



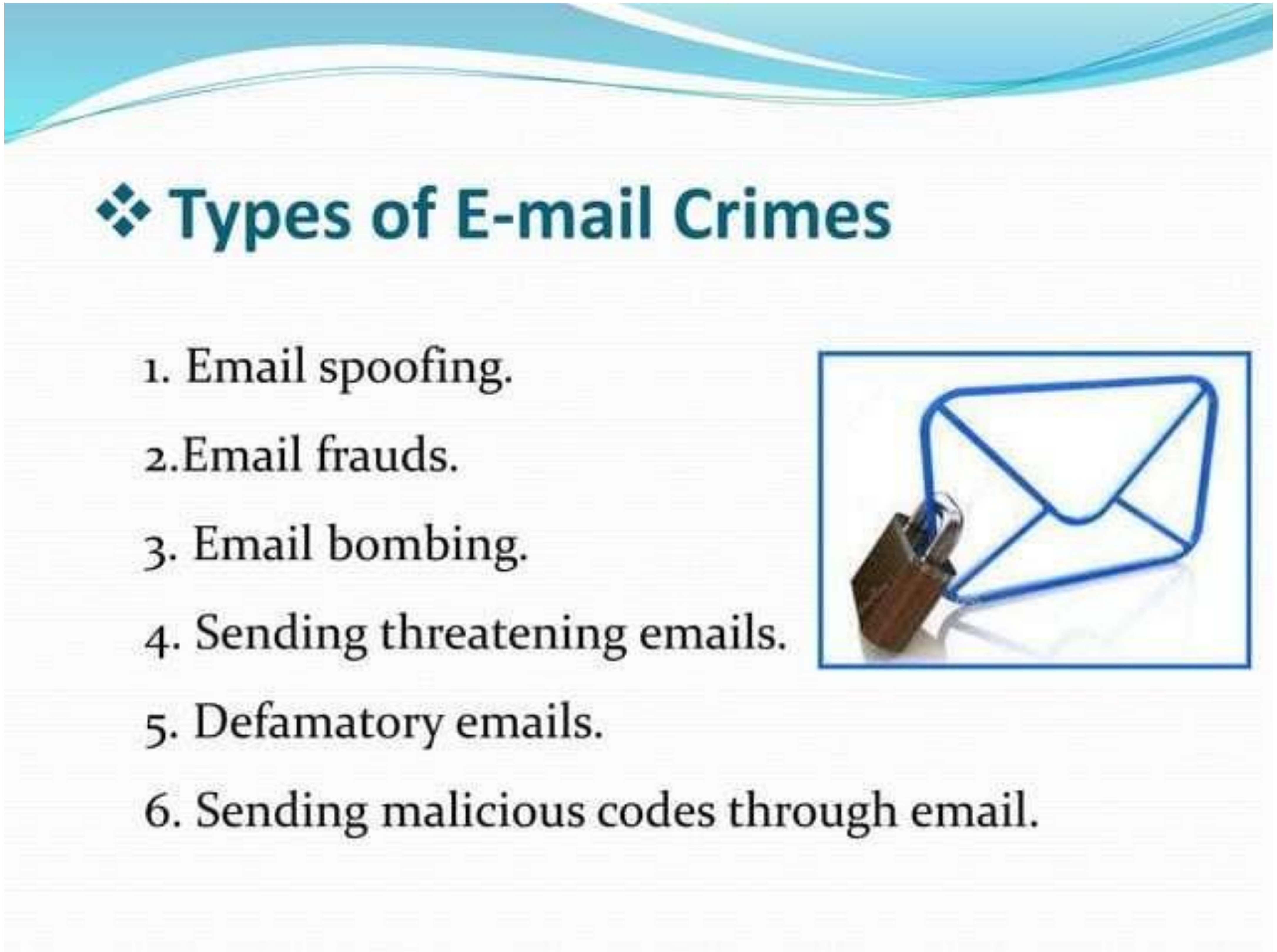
Requirements of E-mail Investigation

- To carve evidence.
- To ensure the reliability of e-mails.
- To pointing on illegal acts and intertwine them.
- Presenting an evidence in front of legal authorities.



❖ Goal of E-mail Forensics

E-mail investigation contains the wealth of mails that's why E-mail forensics investigator must not only investigate but also retrieve the kind of evidence from mails which is presentable and leads to legal action taken on the crime.



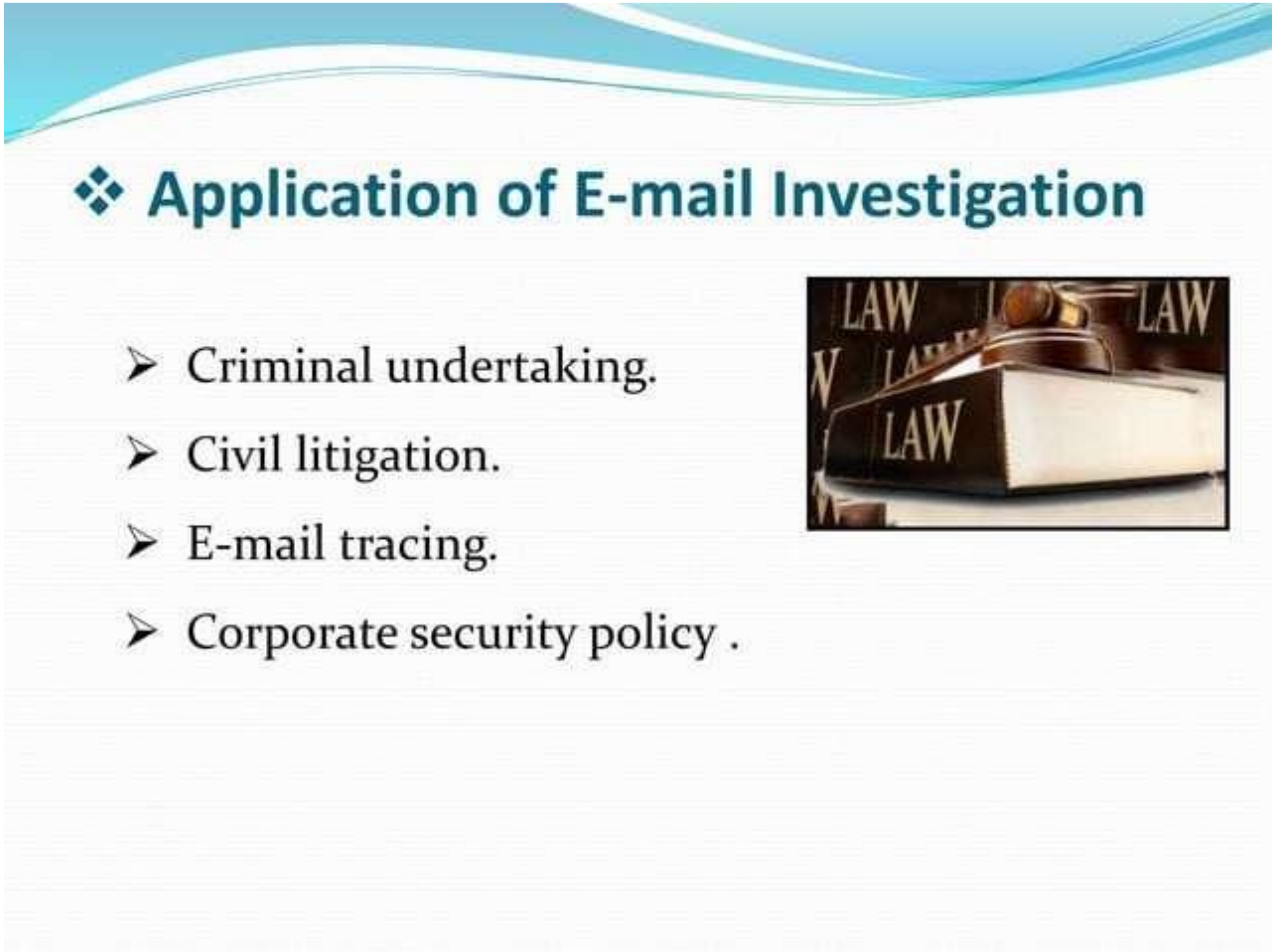
❖ Types of E-mail Crimes

1. Email spoofing.
2. Email frauds.
3. Email bombing.
4. Sending threatening emails.
5. Defamatory emails.
6. Sending malicious codes through email.

Investigating E-mails from Public Servers

Try to ignore the use of your own email-id while investigating .Use public severs like yahoo, Hotmail..,etc.

- Public: Whatever@hotmail.com

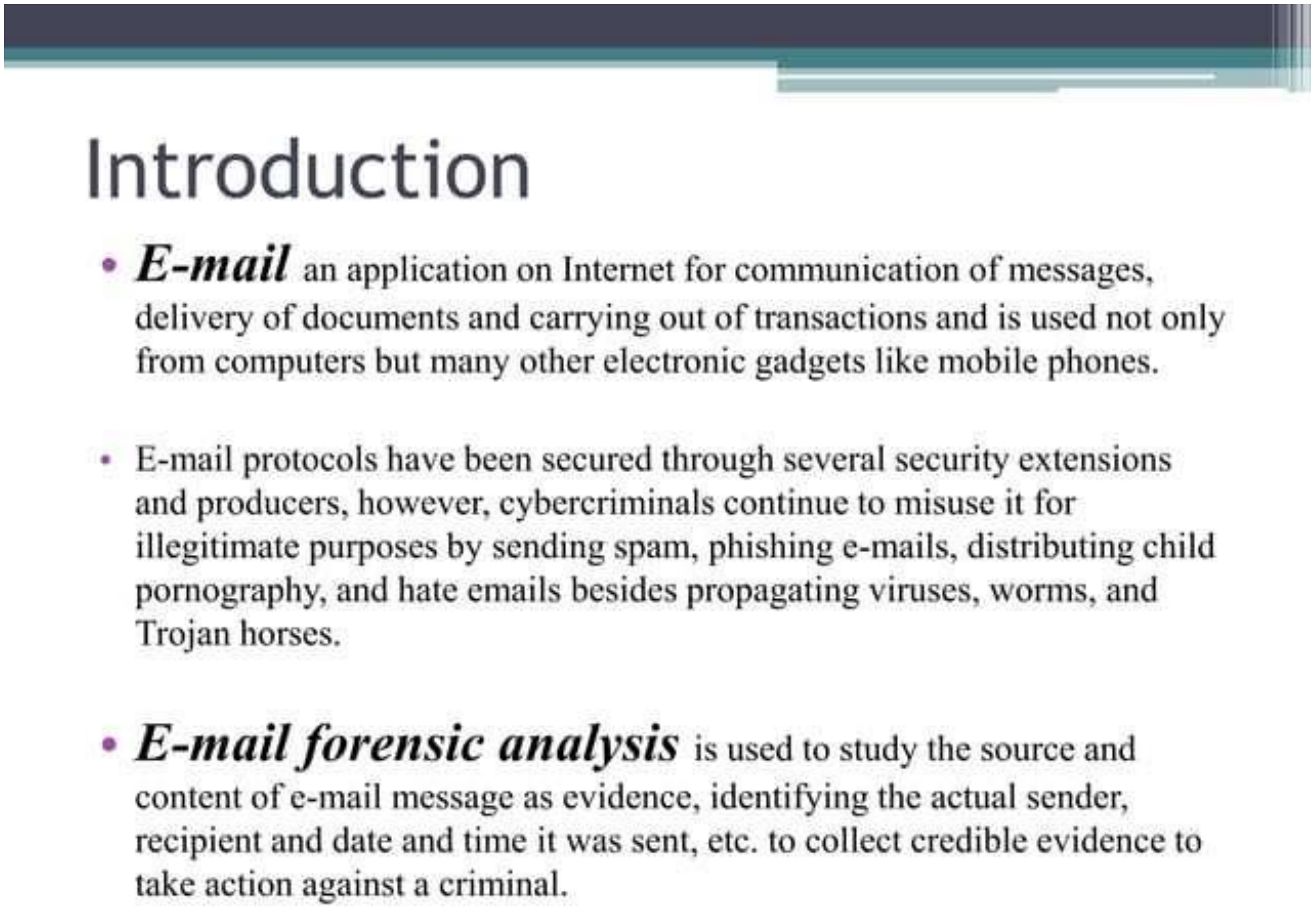


❖ Application of E-mail Investigation

- ➢ Criminal undertaking.
- ➢ Civil litigation.
- ➢ E-mail tracing.
- ➢ Corporate security policy .

Use specified E-mail Investigating tool

- AccessData’s FTK Imager.
- MailXaminer.
- Encase.
- DBXtract.
- Paraben, etc.



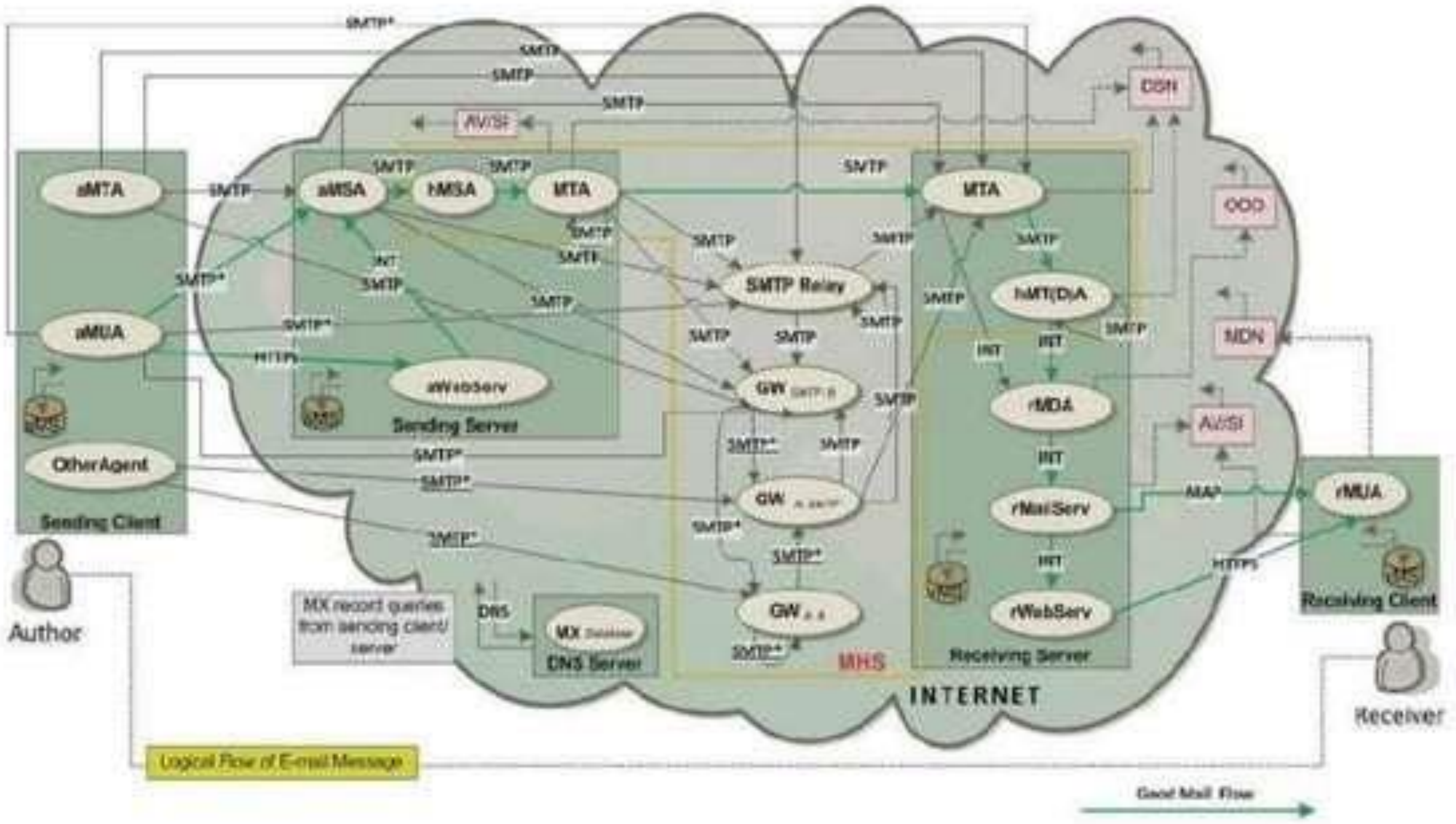
Introduction

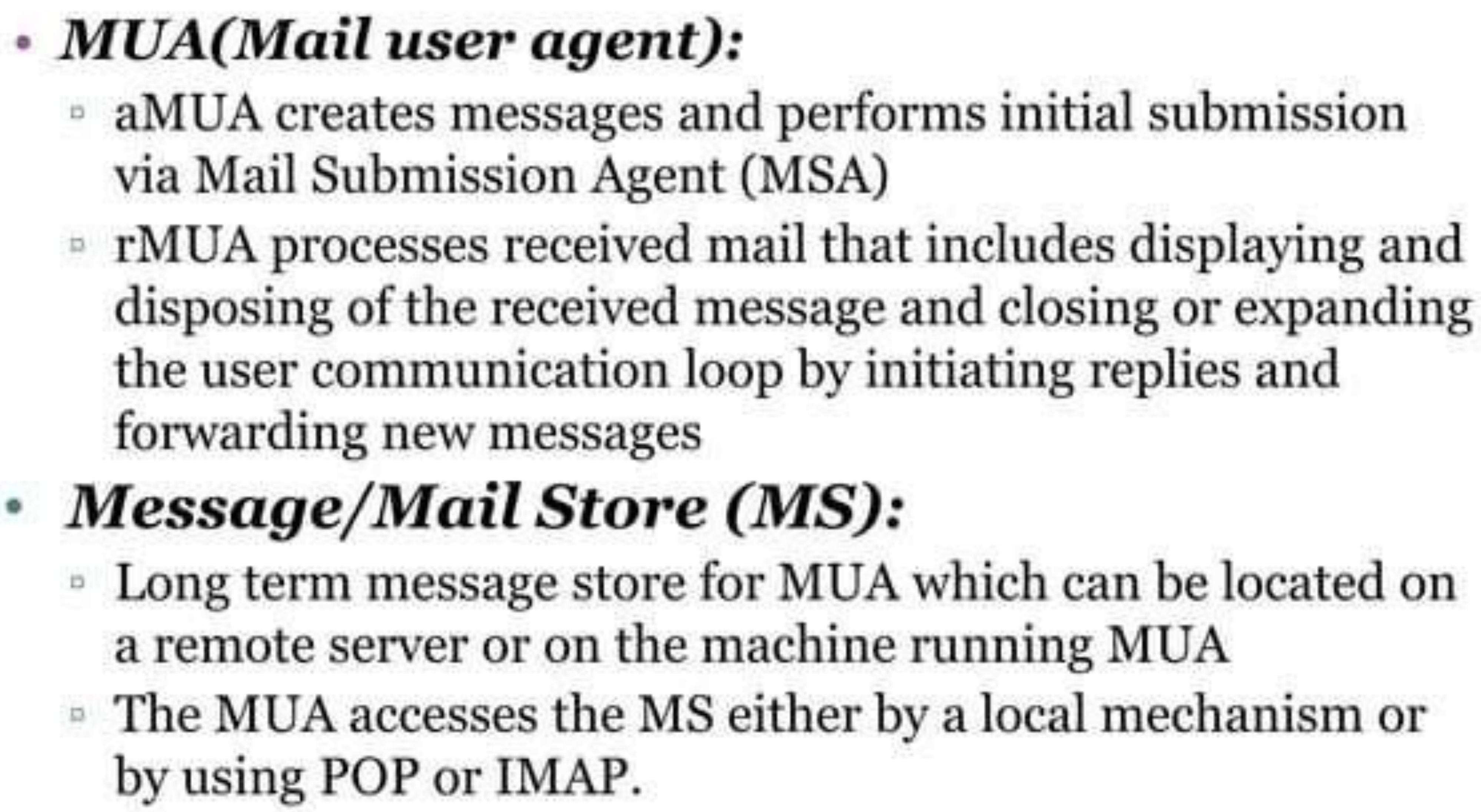
- ***E-mail*** an application on Internet for communication of messages, delivery of documents and carrying out of transactions and is used not only from computers but many other electronic gadgets like mobile phones.

- E-mail protocols have been secured through several security extensions and producers, however, cybercriminals continue to misuse it for illegitimate purposes by sending spam, phishing e-mails, distributing child pornography, and hate emails besides propagating viruses, worms, and Trojan horses.

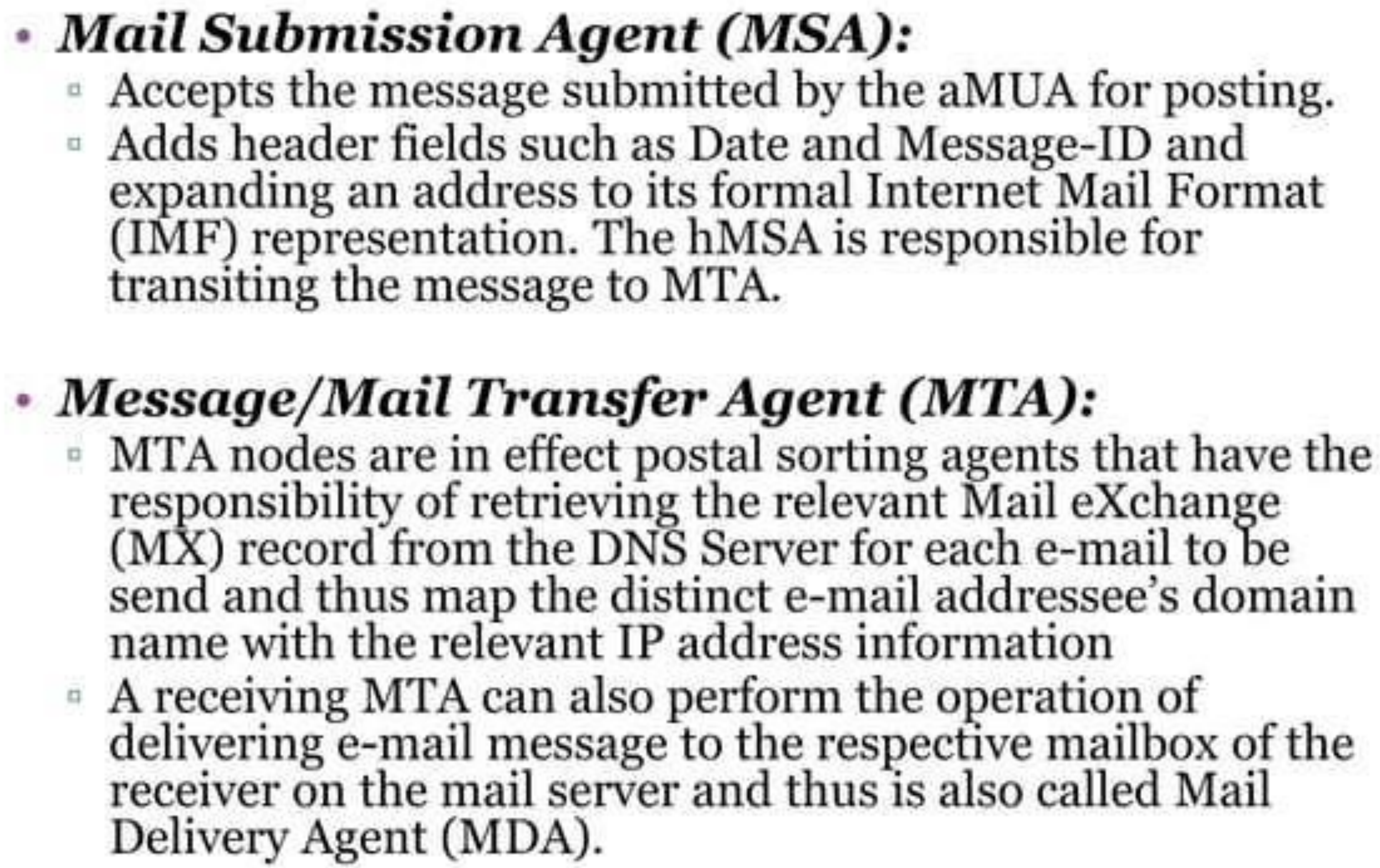
- ***E-mail forensic analysis*** is used to study the source and content of e-mail message as evidence, identifying the actual sender, recipient and date and time it was sent, etc. to collect credible evidence to take action against a criminal.

E-mail Architecture

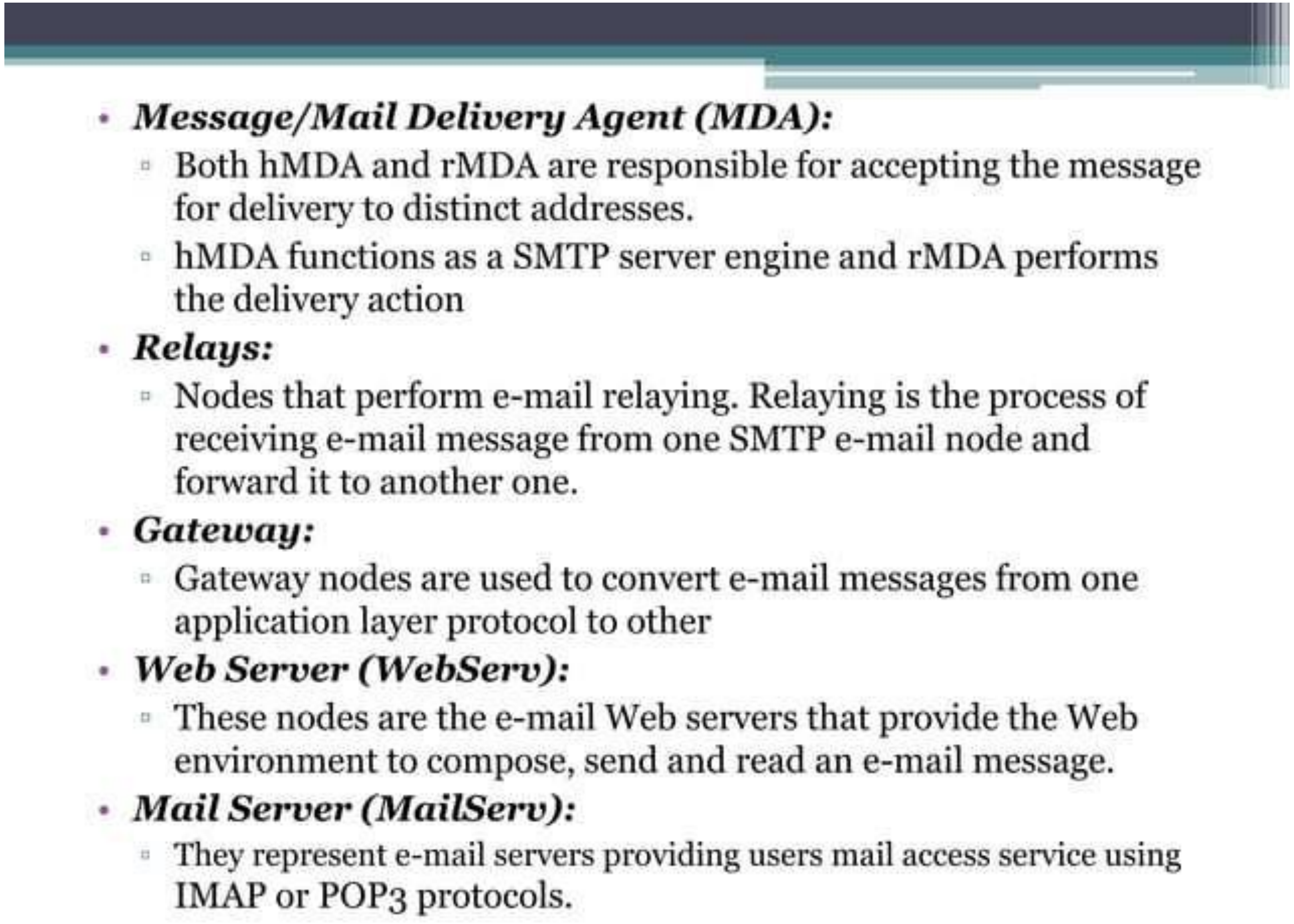




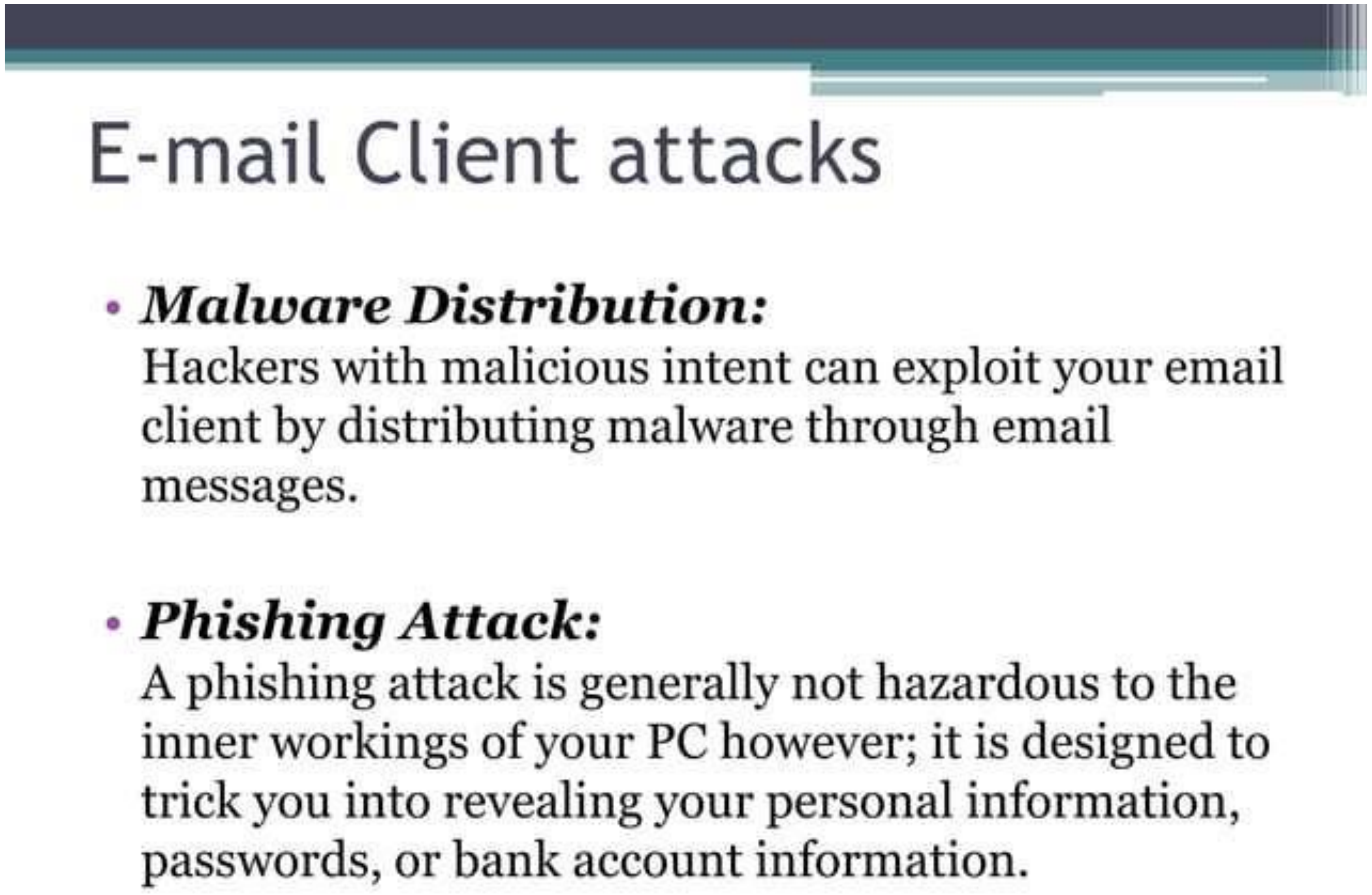
- ***MUA(Mail user agent):***
  - aMUA creates messages and performs initial submission via Mail Submission Agent (MSA)
  - rMUA processes received mail that includes displaying and disposing of the received message and closing or expanding the user communication loop by initiating replies and forwarding new messages
- ***Message/Mail Store (MS):***
  - Long term message store for MUA which can be located on a remote server or on the machine running MUA
  - The MUA accesses the MS either by a local mechanism or by using POP or IMAP.



- ***Mail Submission Agent (MSA):***
  - Accepts the message submitted by the aMUA for posting.
  - Adds header fields such as Date and Message-ID and expanding an address to its formal Internet Mail Format (IMF) representation. The hMSA is responsible for transiting the message to MTA.
- ***Message/Mail Transfer Agent (MTA):***
  - MTA nodes are in effect postal sorting agents that have the responsibility of retrieving the relevant Mail eXchange (MX) record from the DNS Server for each e-mail to be send and thus map the distinct e-mail addressee's domain name with the relevant IP address information
  - A receiving MTA can also perform the operation of delivering e-mail message to the respective mailbox of the receiver on the mail server and thus is also called Mail Delivery Agent (MDA).



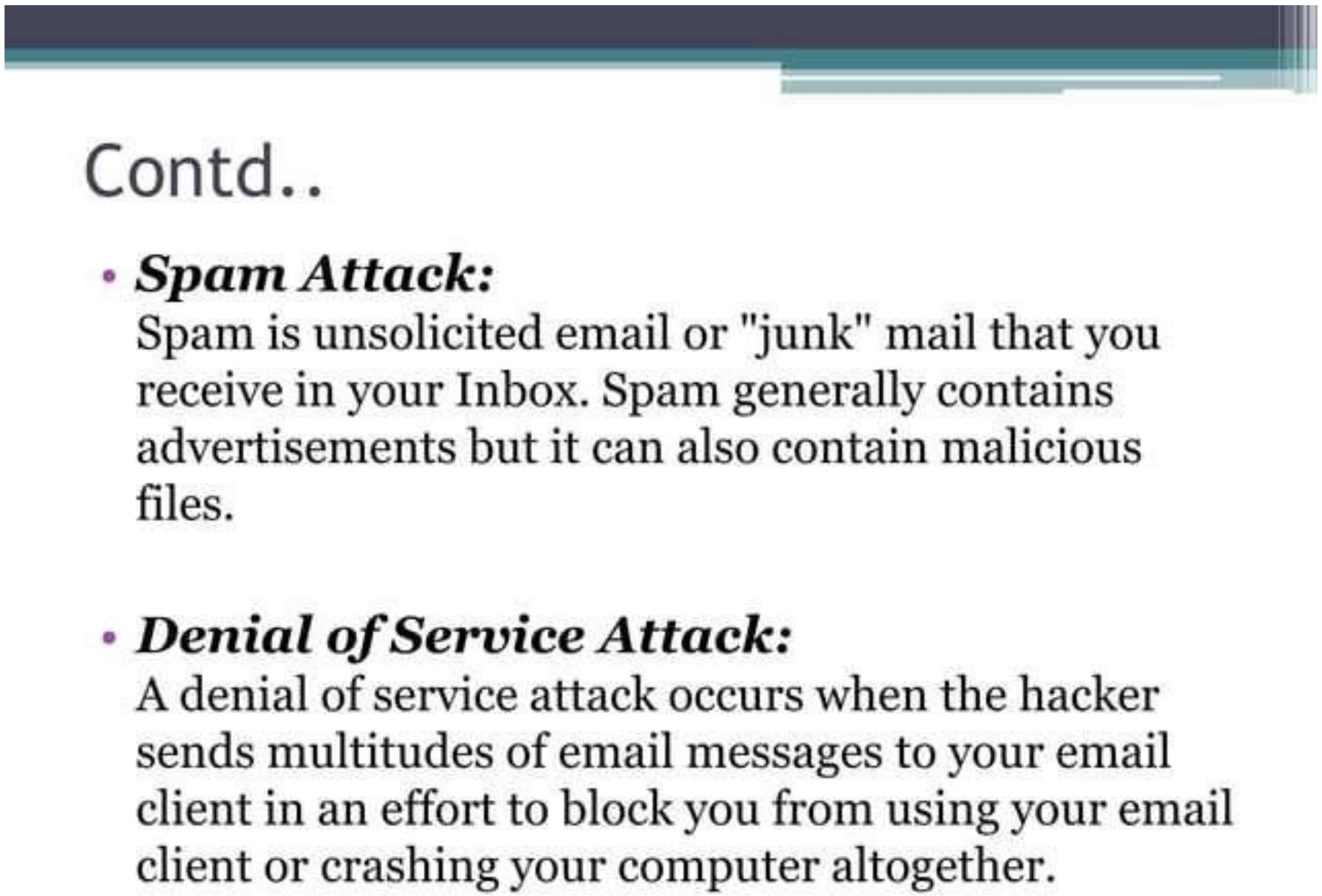
- ***Message/Mail Delivery Agent (MDA):***
  - Both hMDA and rMDA are responsible for accepting the message for delivery to distinct addresses.
  - hMDA functions as a SMTP server engine and rMDA performs the delivery action
- ***Relays:***
  - Nodes that perform e-mail relaying. Relaying is the process of receiving e-mail message from one SMTP e-mail node and forward it to another one.
- ***Gateway:***
  - Gateway nodes are used to convert e-mail messages from one application layer protocol to other
- ***Web Server (WebServ):***
  - These nodes are the e-mail Web servers that provide the Web environment to compose, send and read an e-mail message.
- ***Mail Server (MailServ):***
  - They represent e-mail servers providing users mail access service using IMAP or POP3 protocols.



E-mail Client attacks

- ***Malware Distribution:***
  Hackers with malicious intent can exploit your email client by distributing malware through email messages.

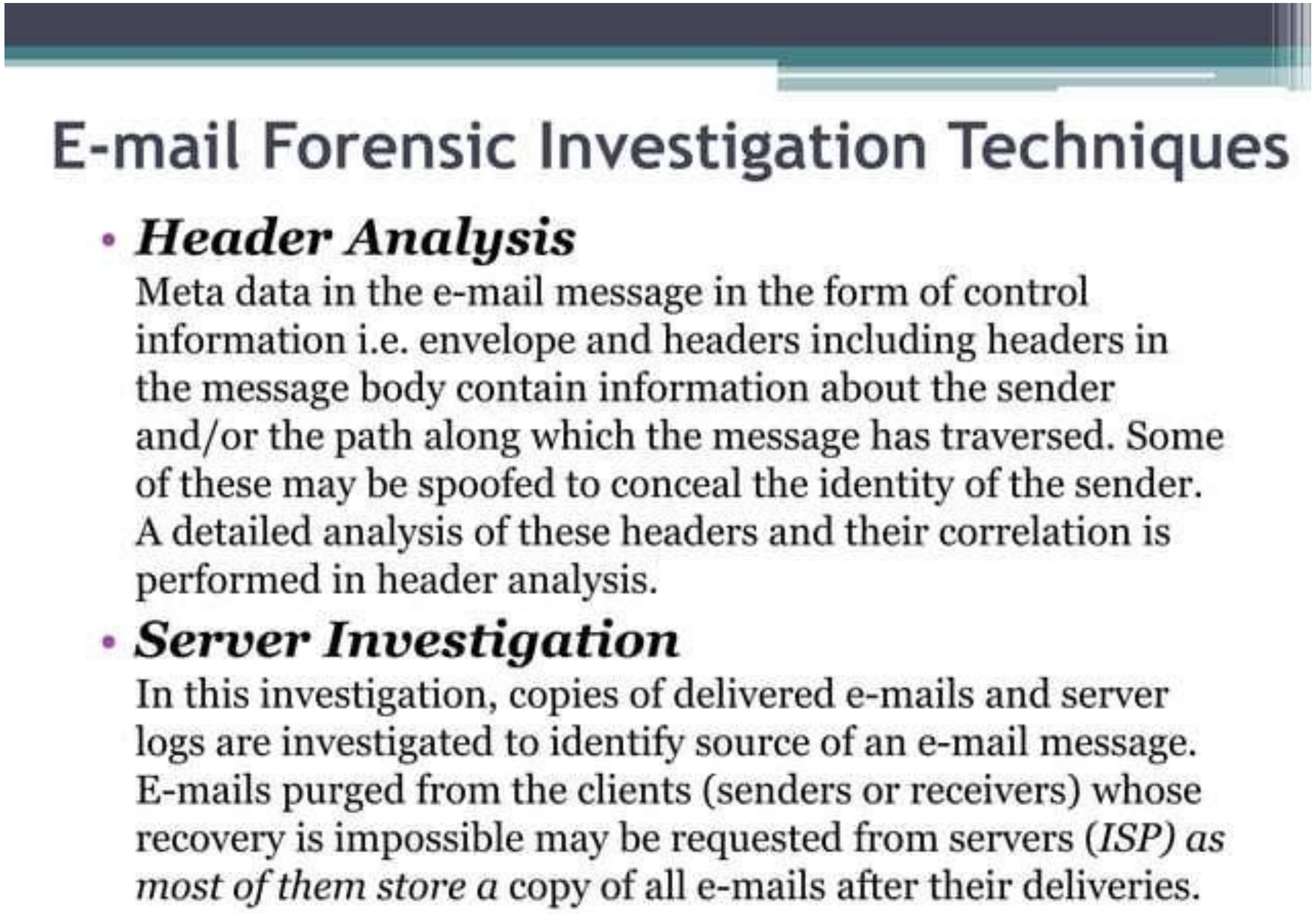
- ***Phishing Attack:***
  A phishing attack is generally not hazardous to the inner workings of your PC however; it is designed to trick you into revealing your personal information, passwords, or bank account information.



Contd..

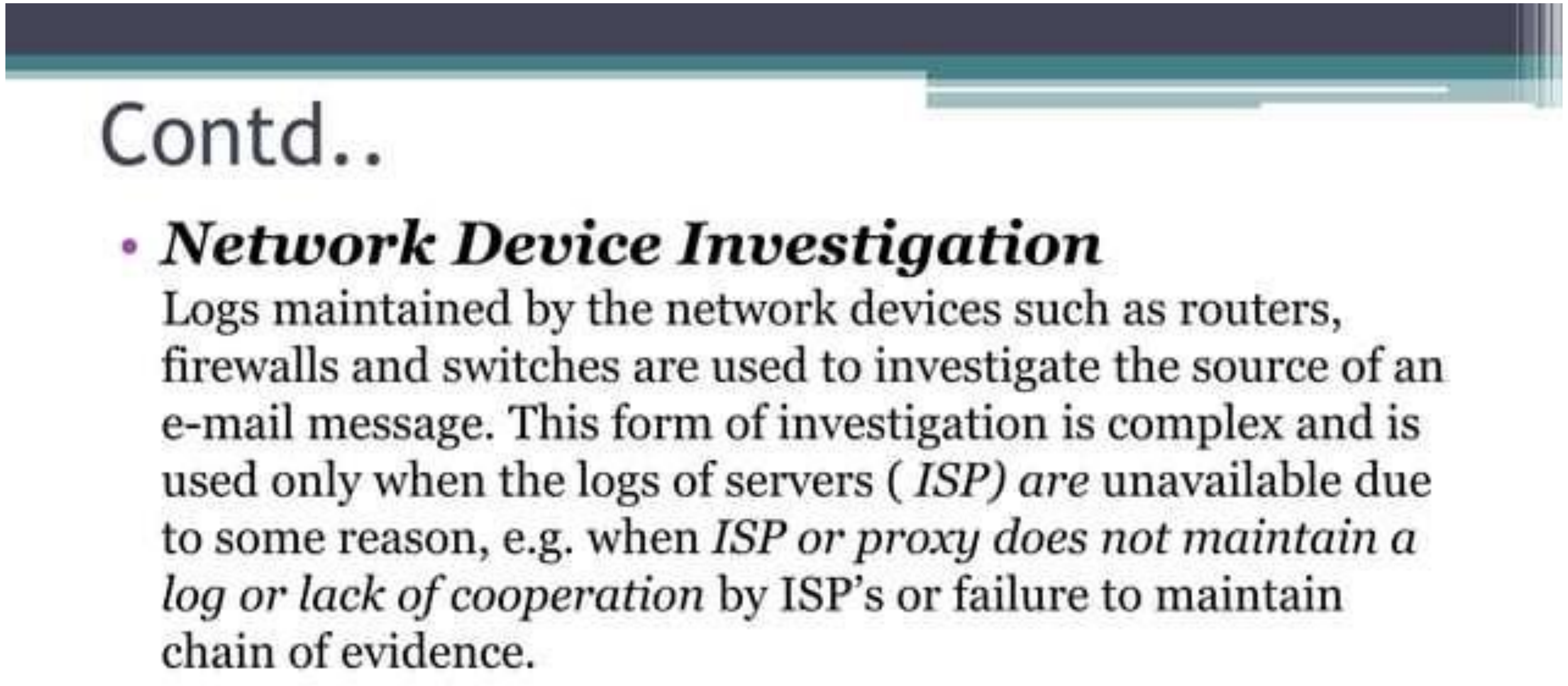
- ***Spam Attack:***
  Spam is unsolicited email or "junk" mail that you receive in your Inbox. Spam generally contains advertisements but it can also contain malicious files.

- ***Denial of Service Attack:***
  A denial of service attack occurs when the hacker sends multitudes of email messages to your email client in an effort to block you from using your email client or crashing your computer altogether.



E-mail Forensic Investigation Techniques

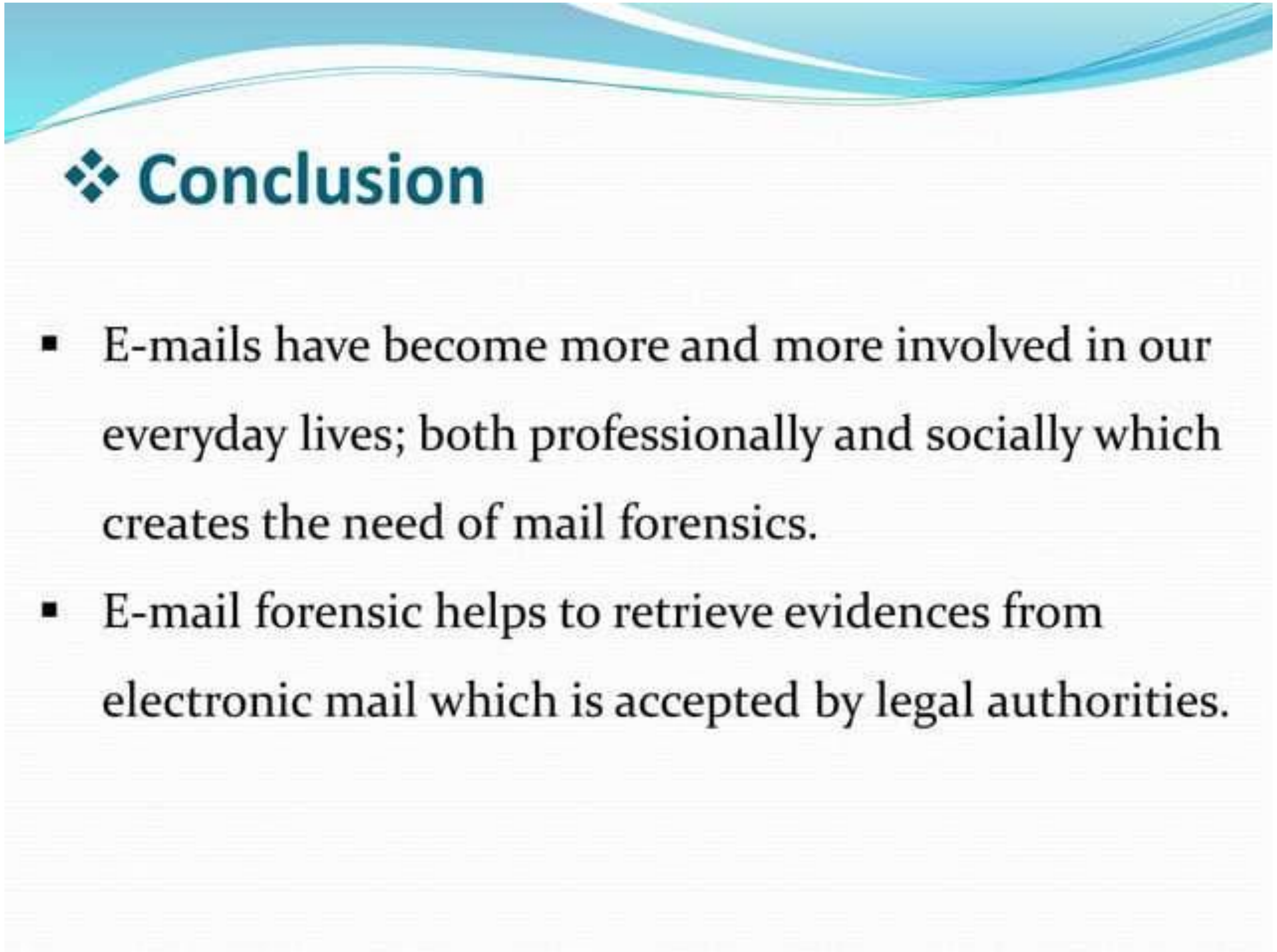
- ***Header Analysis***
  Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis.
- ***Server Investigation***
  In this investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers *(ISP) as most of them store a* copy of all e-mails after their deliveries.



Contd..

- ***Network Device Investigation***

  Logs maintained by the network devices such as routers, firewalls and switches are used to investigate the source of an e-mail message. This form of investigation is complex and is used only when the logs of servers (*ISP) are* unavailable due to some reason, e.g. when *ISP or proxy does not maintain a log or lack of cooperation* by ISP's or failure to maintain chain of evidence.



❖ Conclusion

- E-mails have become more and more involved in our everyday lives; both professionally and socially which creates the need of mail forensics.
- E-mail forensic helps to retrieve evidences from electronic mail which is accepted by legal authorities.

THANK YOU