Introduction to Email Forensics

Email Forensics হলো ডিজিটাল ফরেনসিকসের একটি শাখা, যেখানে ইমেইলের মাধ্যমে সংঘটিত অপরাধ যেমন: স্প্যাম, স্পুফিং, ফিশিং, ম্যালওয়্যার অ্যাটাচমেন্ট, ইত্যাদি বিশ্লেষণ ও তদন্ত করা হয়। এটি ব্যবহার করে তদন্তকারীরা ইমেইলের উৎস, সময়, প্রেরক, কনটেন্ট, সংযুক্তি, ও সার্ভারের মাধ্যমে ট্রেস করে অপরাধীকে চিহ্নিত করে।

---

১. Email Protocol Basics (ইমেইল প্রোটোকলের মৌলিক ধারণা)

ইমেইল প্রোটোকল বলতে বুঝায় সেই প্রযুক্তিগত নিয়মাবলী যেগুলোর মাধ্যমে ইমেইল পাঠানো, গ্রহণ করা এবং সংরক্ষণ করা হয়।

✓ SMTP (Simple Mail Transfer Protocol)

- **ব্যবহার হয়:** ইমেইল পাঠাতে (Send)
- **পোর্ট:** 25 (অথবা 587/465 with encryption)
- **কাজের ধরন:**
  প্রেরকের ইমেইল সার্ভার থেকে প্রাপকের মেইল সার্ভারে মেইল পৌঁছে দেয়।

🔍 উদাহরণ:
আপনি `user@aibl.com` থেকে `recipient@gmail.com`-এ মেইল পাঠালেন। SMTP ব্যবহৃত হয় এই মেইলটি গুগলের মেইল সার্ভারে পৌঁছানোর জন্য।

✓ POP3 (Post Office Protocol v3)

- **ব্যবহার হয়:** ইমেইল রিসিভ (Receive) করার জন্য
- **পোর্ট:** 110 (SSL হলে 995)
- **কাজের ধরন:**
  মেইল সার্ভার থেকে ইমেইল *ডাউনলোড করে লোকাল মেশিনে* সংরক্ষণ করে।
  একবার ডাউনলোড হয়ে গেলে সাধারণত সার্ভার থেকে মুছে ফেলে।

🔍 সমস্যা: আপনি যদি একাধিক ডিভাইসে ইমেইল দেখতে চান, POP3 উপযুক্ত নয়।

✅ IMAP (Internet Message Access Protocol)

- **ব্যবহার হয়:** ইমেইল রিসিভ ও ম্যানেজ করার জন্য
- **পোর্ট:** 143 (SSL হলে 993)
- **কাজের ধরন:**
  সার্ভারে ইমেইল রেখে বিভিন্ন ডিভাইসে *সিঙ্ক করে অ্যাক্সেস* করতে দেয়।
  POP3-এর তুলনায় বেশি ফিচারড ও স্মার্ট।

🔍 সুবিধা: মোবাইল, ল্যাপটপ, ডেস্কটপে একই ইমেইল দেখা যায়, কারণ এটি সার্ভার বেইসড।

Email Threats (ইমেইল সংক্রান্ত হুমকি)

Email হলো সবচেয়ে প্রচলিত সাইবার অ্যাটাক চ্যানেল। নিচে কিছু সাধারণ ইমেইল থ্রেট ব্যাখ্যা করা হলো:

⚠️ Phishing (ফিশিং)

Phishing হলো এমন একটি সামাজিক প্রকৌশল (social engineering) কৌশল, যেখানে ভুয়া ইমেইলের মাধ্যমে ব্যবহারকারীর কাছ থেকে ব্যক্তিগত তথ্য (যেমন: পাসওয়ার্ড, ব্যাংক ডিটেইলস) বের করে নেওয়া হয়।

🔍 ফরেনসিক বিশ্লেষণে কী খোঁজা হয়:

- ভুয়া URL
- misleading domain (e.g., `apple-secure-login.com`)
- Suspicious attachments (PDF, Word, EXE)
- Header থেকে প্রকৃত প্রেরক শনাক্ত

⚠️ Spoofing (স্পুফিং)

Spoofing মানে ইমেইলের প্রেরক আইডি বা হেডার জাল করে কাউকে বিভ্রান্ত করা।

📌 উদাহরণ: আপনি দেখছেন ইমেইল এসেছে `ceo@yourbank.com` থেকে, কিন্তু বাস্তবে তা এসেছে অন্য কোথাও থেকে।

🔍 ফরেনসিক টুল দিয়ে:

- SPF, DKIM, DMARC যাচাই
- IP address ও mail path ট্রেস
- Mail header field mismatch চিহ্নিত

⚠ Spamming (স্প্যামিং)

Spamming মানে অবাঞ্ছিত প্রচুর ইমেইল পাঠানো – যা সাধারণত মার্কেটিং বা ম্যালওয়্যার ছড়ানোর জন্য করা হয়।

 ফরেনসিক বিশ্লেষণে:

- একাধিক প্রেরকের IP address blacklist চেক
- Mail server logs থেকে frequency বিশ্লেষণ
- Similar content pattern খুঁজে বের করা

🔍 ফরেনসিক ইনভেস্টিগেশনে কী দেখা হয়?

এলিমেন্ট	বিশ্লেষণ
Email Header	IP, Server path, authentication flags
Attachments	Virus, macro, or malware presence
URL in email	Phishing link বা redirect খোঁজা
Sender details	Fake domain, spoofed identity
Timestamps	বিভিন্ন server timestamp এর অমিল

---

2. 🛍 Understanding Email Headers (ইমেইল হেডার বিশ্লেষণ)

ইমেইল হেডার হলো ইমেইলের *"metadata"* বা ব্যাকগ্রাউন্ড তথ্য, যা জানায় ইমেইলটি **কখন, কোথা থেকে, কীভাবে ও কার মাধ্যমে পাঠানো হয়েছে**।

হেডার বিশ্লেষণের মাধ্যমে আপনি বের করতে পারেন:

- ইমেইলের উৎস IP
- ইমেইল স্পুফিং হয়েছে কি না
- প্রকৃত প্রেরক কে
- ইমেইলটি কোন কোন সার্ভার ঘুরে এসেছে

📄 Email Header Structure (হেডারের গঠন)

একটি পূর্ণ ইমেইল হেডারে সাধারণত নিচের উপাদানগুলো থাকে:

উপাদান	বর্ণনা
`Return-Path:`	Bounce-back এর ঠিকানা বা প্রকৃত প্রেরক
`Received:`	কোন কোন সার্ভার ঘুরে এসেছে – একাধিকবার থাকে
`From:`	প্রেরকের নাম ও ইমেইল
`To:`	প্রাপক
`Subject:`	ইমেইলের বিষয়
`Date:`	কখন পাঠানো হয়েছে
`Message-ID:`	ইউনিক মেইল আইডি
`DKIM-Signature:`	DomainKey সাইনেচার (স্পুফিং শনাক্তে সহায়ক)
`SPF:`	Sender Policy Framework ফলাফল
`MIME-Version:`	ইমেইলের ফরম্যাট
`User-Agent:`	কোন অ্যাপ্লিকেশন থেকে পাঠানো হয়েছে

🔎 Key Header Fields বিশ্লেষণ

✅ 1. `Received:` Field

এই ফিল্ডটি সবচেয়ে গুরুত্বপূর্ণ। এটা জানায় ইমেইলটি কোন কোন সার্ভার পেরিয়ে এসেছে। প্রতিবার যেই সার্ভার মেইল ফরোয়ার্ড করে, একটি `Received:` লাইন যুক্ত হয়।

📌 মূল বিষয়:

- নিচ থেকে উপরের দিকে পড়তে হয় (Top one is the latest)
- প্রতিটি `Received:` লাইন দেখায়:
  - From: কোথা থেকে এসেছে
  - By: কোন সার্ভার নিয়েছে
  - With: কোন প্রোটোকল ব্যবহার হয়েছে (SMTP)
  - Timestamp: কখন পাঠানো হয়েছে

🔍 ব্যবহার:

যদি প্রথম `Received:` IP ঠিকানা সন্দেহজনক হয় বা spoof করা হয়, তাহলে সেটি ধরে তদন্ত শুরু হয়।

✅ 2. `Return-Path:` Field

এটি ইমেইল ডেলিভারিতে কোনো সমস্যা হলে (বাউন্স ব্যাক) যে ঠিকানায় ফিরে যাবে।

📌 যদি `From:` এবং `Return-Path:` আলাদা হয়, তাহলে spoofing হওয়ার সম্ভাবনা বেশি।

🔍 উদাহরণ:

```
plaintext
From: ceo@yourbank.com
Return-Path: attacker@evil.com
```

এখানে স্পষ্ট স্পুফিং ঘটেছে।

✅ 3. `Message-ID:` Field

- এটি একটি ইউনিক আইডি যা ইমেইল পাঠানোর সময় জেনারেট হয়
- ফরম্যাট: `<random_string@domain.com>`
- একে ট্র্যাক করে বোঝা যায়, ইমেইল কোথা থেকে উৎপন্ন হয়েছে

🔍 স্পুফিং/ফিশিং মেইলে এই ফিল্ডটি অনেক সময় অনুপস্থিত বা অস্বাভাবিক থাকে

🕒 Time-Zone Mismatches (সময় অঞ্চলের গরমিল)

যদি হেডারের টাইমস্ট্যাম্পগুলো বিভিন্ন টাইমজোনে হয়, তাহলে সেটা **স্পুফিং বা ফরজ হেডার** ইঙ্গিত দিতে পারে।

🔍 উদাহরণ:

```
Received: from mail.fake.com (IP...) by mail.google.com with ESMTPS id...
  Mon, 27 May 2025 10:12:34 -0500 (CDT)

Received: from desktop (unknown IP) by mail.fake.com
  Mon, 27 May 2025 21:00:34 +0900 (JST)
```

👉 এখানে দেখা যাচ্ছে যে ইমেইলটি **জাপান সময় অনুযায়ী পরে পাঠানো হলেও আগে সার্ভারে পৌঁছেছে** – যা বাস্তবে সম্ভব নয়, তাই এটি ফরজড।

🕵️‍♂️ Forged Header Detection (জাল হেডার চিহ্নিতকরণ)

কিছু সাধারণ ট্রিক:

বিশ্লেষণ	সমস্যা
IP mismatch	Header-এ থাকা IP Whois বা blacklist এ চেক করুন
Received field inconsistent	সময় গরমিল, নাম/আইপি অস্বাভাবিক
SPF/DKIM ফলাফল fail	প্রকৃত সার্ভার নয়, স্পুফিং সম্ভাবনা

Return-path আলাদা	প্রেরক অন্য কেউ
Message-ID ভুয়া ডোমেইন	ইমেইল সার্ভারের অংশ না

Free Tools for Email Header Analysis

টুল	কাজ
MxToolbox Header Analyzer	হেডার পেস্ট করলে IP, SPF, DKIM, Routing বিশ্লেষণ
Google Admin Toolbox	ইমেইল ট্রেস ও latency বিশ্লেষণ
Mailheader.org	Received chain বিশ্লেষণ ও IP জিওলোকেশন
IPVoid/DomainTools	IP Blacklist বা Geo Info চেক

🔎 ৩. ইমেইলের উৎস শনাক্তকরণ (Tracking the Source of an Email)

ইমেইল ফরেনসিকে সবচেয়ে গুরুত্বপূর্ণ ও কার্যকর অংশ হলো — **ইমেইলটি কে পাঠিয়েছে, কোথা থেকে পাঠিয়েছে, এবং আইপি ঠিকানার ভিত্তিতে অবস্থান শনাক্ত করা।** এজন্য নিচের স্টেপগুলো অনুসরণ করতে হয়:

🔎 IP Address Extraction (আইপি ঠিকানা বের করা)

প্রথমে আমাদের জানতে হবে প্রেরকের IP Address কোথায় পাওয়া যাবে।

📨 ইমেইল হেডার বিশ্লেষণ (Header Analysis):

ইমেইল হেডারে থাকে একাধিক `Received:` লাইন।
সাধারণত নিচের দিকে থাকা **প্রথম `Received:` হেডারটি** মূল প্রেরকের সার্ভারের তথ্য বহন করে।

✅ উদাহরণ:

```
plaintext
CopyEdit
Received: from [192.168.0.100] (unknown [203.112.45.72])
by mail.example.com (Postfix) with ESMTP;
Wed, 28 May 2025 12:00:00 +0600
```

➡ এখানে IP = **203.112.45.72** → এটি হচ্ছে প্রেরকের Public IP (যদি স্পুফ না করা হয়)।

📌 কিছু ক্ষেত্রে IP গুলো **private IP range** (যেমন: 192.168.x.x, 10.x.x.x) হতে পারে, যেগুলো ইনটারনাল নেটওয়ার্কের IP – তাই তখন real IP পেতে SMTP log বা Webmail log দরকার হতে পারে।

🌐 WHOIS ও IP Geolocation Tools ব্যবহারের মাধ্যমে উৎসের অবস্থান চিহ্নিতকরণ

একবার IP পাওয়ার পর, এখন সেটিকে বিশ্লেষণ করতে হয়:

✅ (ক) WHOIS বিশ্লেষণ (Who Owns the IP?)

WHOIS টুলস:

- 🔗 https://whois.domaintools.com
- 🔗 https://ipinfo.io
- 🔗 https://whois.arin.net

বুঝে নিতে পারবেন:

- IP কোন ISP বা সংস্থা ব্যবহার করছে
- Abuse Contact Email (ISP-এর কাছে রিপোর্ট পাঠানো যায়)
- Registration Region

📌 উদাহরণ WHOIS output:

```
NetName: BANGLALION-WIMAX
Country: BD
OrgName: Banglalion Communications Ltd.
Abuse Email: abuse@banglalion.com.bd
```

✅ (খ) IP Geolocation (IP এর ভূ-অবস্থান নির্ধারণ)

Free Tools:

- 🔗 https://www.iplocation.net
- 🔗 https://tools.keycdn.com/geo
- 🔗 https://db-ip.com

এতে আপনি জানতে পারবেন:

- দেশ (Country)
- শহর বা অঞ্চল (City, Region)
- টাইমজোন
- Approximated Coordinates (Latitude, Longitude)

📌 উদাহরণ:

IP	Location
203.112.45.72	Dhaka, Bangladesh
45.67.89.120	Frankfurt, Germany

⊘ ⚠□ স্পুফিং ও ফেইক IP এর বিপদ

অনেক সময় হ্যাকাররা:

- VPN / Proxy / TOR ব্যবহার করে ইমেইল পাঠায়
- তখন WHOIS/Geo Info ভুল বা বিভ্রান্তিকর হয়
- তাই একাধিক হেডার এবং লগ বিশ্লেষণ গুরুত্বপূর্ণ

□ টুলস সমন্বিত তালিকা:

কাজ	ফ্রি টুলস	উদ্দেশ্য
IP বের করা	Gmail "Show Original" / Header Viewer	হেডার বিশ্লেষণ
WHOIS চেক	ipinfo.io, arin.net	আইপি মালিকানা নির্ধারণ
GeoLocation	iplocation.net, db-ip.com	অবস্থান নির্ধারণ
Header Analyzer	MXToolbox Email Header Analyzer	IP ও delay বিশ্লেষণ

🔎 ৪. ইমেইল ক্লায়েন্ট বিশ্লেষণ (Analyzing Email Clients)

ইমেইল ফরেনসিকে বিভিন্ন ইমেইল ক্লায়েন্ট যেমন Microsoft Outlook, Mozilla Thunderbird, Apple Mail ইত্যাদির লোকাল ডেটা ফাইল বিশ্লেষণ করা হয়। এগুলোর ভিতর সংরক্ষিত থাকে ইমেইল বার্তা, সংযুক্তি (attachments), মেটাডেটা এবং আরও অনেক কিছু, যা তদন্তে গুরুত্বপূর্ণ ভূমিকা রাখে।

📧 Microsoft Outlook – PST ও OST ফাইল বিশ্লেষণ

✓ ফাইল টাইপ:

টাইপ	ব্যাখ্যা
`.PST`	Personal Storage Table (POP3/Archive Data)
`.OST`	Offline Storage Table (Exchange/IMAP Cached Data)

✅ PST/OST থেকে কী তথ্য পাওয়া যায়:

- Inbox, Sent, Draft ইমেইল কপি
- সংযুক্তি (Attachments)
- Headers, Message-ID, IP info
- Deleted ইমেইল (Recoverable)
- Calendar, Contacts, Tasks

✅ বিশ্লেষণের জন্য ফ্রি টুলস:

টুল	কাজ
MFCTest (Microsoft Tool)	OST/PST read and test
Kernel PST Viewer (Free)	PST ফাইল ব্রাউজ
PstViewer Pro (Trial)	PST/OST Preview + Export
FTK Imager	PST Mount এবং Export
Emailchemy (Partial free)	PST to EML conversion

✅ ফরেনসিক নোট:

- Outlook-এর OST ফাইল এনক্রিপ্টেড হলে Exchange Profile দরকার।
- Deleted items → Recoverable Items folder থেকেও উদ্ধার সম্ভব (in PST/OST structure)।

📨 Mozilla Thunderbird – MBOX বিশ্লেষণ

✅ ফাইল টাইপ:

Thunderbird MBOX ফরম্যাট ব্যবহার করে। এটি একটি টেক্সট বেসড ফাইল, যেখানে সব ইমেইল ধারাবাহিকভাবে সংরক্ষিত থাকে।

✅ বিশ্লেষণযোগ্য তথ্য:

- ইমেইল Body ও Headers
- Attachments (embedded or external)
- Spam/Junk folder review
- Drafts এবং Sent items

✅ ফ্রি টুলস:

টুল	কাজ
MBox Viewer **(Free)**	MBOX ফাইল পড়া
Aid4Mail MBOX Analyzer (Trial)	Search & export MBOX
Thunderbird Profile Viewer	লোকাল profile data এক্সট্রাক্ট
Autopsy (with Email Parser plugin)	MBOX থেকে structured view তৈরি

📌 **নোট:** Thunderbird profile path:
`C:\Users\<Username>\AppData\Roaming\Thunderbird\Profiles\`

🍎 Apple Mail (macOS Mail)

✅ ডেটা স্টোরেজ:

Apple Mail সাধারণত MBOX structure-এ ডেটা সংরক্ষণ করে:

```
javascript
CopyEdit
~/Library/Mail/V9/
```

✅ বিশ্লেষণযোগ্য বিষয়:

- MBOX ফাইল (Per Folder)
- Attachments
- Plist config files (for account info)
- Timestamps, message flags
- Deleted/Flagged messages

🎤 Webmail Forensics

(Gmail, Yahoo, Outlook.com ও Cache-Based Evidence বিশ্লেষণ)

Webmail ফরেনসিক হল ব্রাউজার-ভিত্তিক ইমেইল সার্ভিস যেমন Gmail, Yahoo Mail, Outlook.com ইত্যাদির ব্যবহৃত ইতিহাস, ক্যাশ, লগইন ট্রেইল, এবং ব্রাউজার-সংরক্ষিত ডেটা বিশ্লেষণ করা।

✅ Gmail Forensics

📌 Evidence Sources:

- Gmail login/logout history (Google Account Activity)
- Security Alert Emails (suspicious login, 2FA bypass)
- Gmail headers (for IP, Message-ID)
- Google Takeout (for full mailbox archive)

📌 Tools:

- **Google Takeout**: সম্পূর্ণ Gmail archive (MBOX ফরম্যাটে)
- **Mbox Viewer**: Gmail MBOX analysis
- **Gmail Header Analyzer** (by Google or MXToolbox)

📌 Headers থেকে তথ্য:

- X-Originating-IP
- Message-ID
- SPF/DKIM/DMARC Status

✅ Yahoo & Outlook.com Forensics

📌 Yahoo/Outlook থেকে প্রাপ্ত তথ্য:

- Login history (via Account Settings → Recent Activity)
- Mailbox export (Outlook Import, EML conversion)
- Suspicious login alert messages
- Email headers

📌 Headers থেকে কী পাবেন:

- Return-Path
- Received chain
- Authentication-Results (SPF, DKIM)

📌 Tools:

- **WebMail Extractor Tools**
- **Email Header Analyzer** (https://mxtoolbox.com/EmailHeaders.aspx)
- **Browser Cache Viewer (NirSoft)**

✅ Cache & Browser-Based Evidence

📌 Browser Cache/Artifacts:

- Webmail Login credentials (saved password vaults)
- Email previews/screenshots (cached HTML content)
- Webmail session tokens
- Browser autofill data
- Cookies for webmail sessions

📌 **Forensic Tools:**

টুল	উদ্দেশ্য
NirSoft Web Browser PassView	Saved passwords দেখতে
ChromeCacheView / MozillaCacheView	ব্রাউজার cache দেখতে
Belkasoft Evidence Center	Complete webmail session extraction
Web Historian (Magnet Forensics)	Browsing history timeline তৈরি

🔎 ৬. Investigating Email Logs

Mail Server Logs (Postfix, Sendmail, Exchange)

ইমেইল ফরেনসিকে Mail Server log বিশ্লেষণ গুরুত্বপূর্ণ, কারণ এখান থেকে জানা যায় কে কাকে কখন ইমেইল পাঠিয়েছে, কোন আইপি থেকে পাঠানো হয়েছে, authentication পাস হয়েছে কিনা ইত্যাদি।

✅ Postfix Logs

📌 লগ ফাইল:

`/var/log/maillog` বা `/var/log/mail.log`

📌 দেখার কমান্ড:

```
bash
CopyEdit
grep 'from=' /var/log/mail.log
```

📌 দেখতে পাবেন:

- Sender, Recipient
- Queue ID
- Status (sent, deferred, bounced)

📌 উদাহরণ:

```
sql
CopyEdit
Jan 25 10:12:01 mail postfix/smtpd[1234]: 1234ABCD:
from=<attacker@example.com>, to=<victim@example.net>
```

✅ Sendmail Logs

📌 লগ ফাইল:
`/var/log/maillog`

📌 কী তথ্য পাওয়া যায়:

- Relay chain
- Authentication result
- Message-ID
- Delivery status

📌 কমান্ড:

```
bash
CopyEdit
grep 'sendmail' /var/log/maillog
```

✅ Microsoft Exchange Logs

📌 লগ টাইপ:

- **Message Tracking Logs**
- **SMTP Receive Logs**
- **Audit Logs (O365)**

📌 লগ লোকেশন (on-prem):
`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking`

📌 PowerShell কমান্ড:

```
powershell
CopyEdit
Get-MessageTrackingLog -Sender "attacker@domain.com"
```

📌 Audit logs ব্যবহার করে জানানো যায়:

- Mail Read/Send সময়
- Login IP
- Delegate Access used or not

✅ Email Gateway Forensic Traces

📌 Email Gateway/Filter (Mimecast, Cisco ESA, Barracuda, Proofpoint ইত্যাদি) লগে থাকে:

- Threat detection logs
- Attachment scanning logs
- URL rewriting
- Quarantine history

📌 তথ্য:

- Blocked/Allowed email
- Virus/Malware attached
- SPF/DKIM Failed
- Policy-violated content

📌 Gateway forensic tools:

- SIEM Integration (LogRhythm, Splunk)
- Gateway Web Dashboards
- Email Logs Export (CSV)

🔑 ৭. Email Recovery Techniques (ইমেইল পুনরুদ্ধার কৌশল)

Email Forensics-এ একটি গুরুত্বপূর্ণ কাজ হলো **মুছে ফেলা (deleted)** বা **চিহ্ন না থাকা ইমেইল** পুনরুদ্ধার করা। এটি সম্ভব হয় বিভিন্ন ফরম্যাটের মেইলবক্স (PST, OST, MBOX) থেকে এবং ফরেনসিক ইমেজ বা ফাইল কার্ভিং টুলের মাধ্যমে।

✅ Deleted Email Recovery from PST/OST (Outlook)

📌 **PST (Personal Storage Table)** এবং **OST (Offline Storage Table)** ফাইল Microsoft Outlook দ্বারা ব্যবহৃত হয়।

🔍 পুনরুদ্ধার প্রক্রিয়া:

1. **ScanPST.exe** (Microsoft Inbox Repair Tool):
    - Outlook PST ফাইল স্ক্যান করে corrupted/hidden ইমেইল খুঁজে বের করে।
    - লোকেশন:

```
java
CopyEdit
C:\Program Files (x86)\Microsoft Office\root\OfficeXX\SCANPST.EXE
```

2. **Recovery Software ব্যবহার করে**:
   - **Free Tools:**
     - **PST Walker**
     - **Kernel PST Viewer** (read-only)
   - **Paid Tools (trial version):**
     - Stellar Phoenix PST Recovery
     - SysTools Outlook Recovery
3. **Forensic Software দিয়ে Analysis**:
   - **Autopsy + PST Plugin** ব্যবহার করলে Deleted PST ইমেইল দেখা যায়।
   - **Belkasoft Evidence Center** – outlook artifact scan করে।

✅ Deleted Email Recovery from MBOX (Thunderbird, Apple Mail)

📌 MBOX ফরম্যাট সাধারণত Mozilla Thunderbird, Apple Mail ব্যবহার করে।

🔍 *পুনরুদ্ধার পদ্ধতি:*

1. **MBOX Manual Inspection**:
   - MBOX ফাইল খুলে নোটপ্যাড বা MBOX Viewer দিয়ে পড়া যায়।
   - Deleted ইমেইল অনেক সময় "marked as deleted" হয় কিন্তু সত্যিকার অর্থে মুছে ফেলা হয় না।
2. **Tools for Recovery**:
   - **Free Tools:**
     - **Mozilla Thunderbird + ImportExportTools NG Add-on** (backup/restore)
     - **Aid4Mail MBOX Viewer**
   - **Advanced Forensics Tools**:
     - Autopsy with MBOX plugin
     - FTK Imager (for carving deleted MBOX from disk)

✅ Use of Forensic Image & Carving Tools

Deleted ইমেইল সরাসরি পাওয়া না গেলে, তখন **Disk Image** নিয়ে file carving করে মেইল ফাইল রিকভার করা হয়।

🎁 *File Types to Look For:*

- `.pst`, `.ost`, `.mbox`, `.eml`, `.dbx`, `.idx`

Tools:

টুল	উদ্দেশ্য
FTK Imager	Disk/partition image capture এবং logical file extraction
Autopsy	Deleted email carving + MBOX, PST plugin
Photorec	Raw file carving (PST, MBOX, EML)
Bulk Extractor	Email address extraction, file carving
X-Ways Forensics	PST carving এবং deleted content recovery
Magnet AXIOM (paid)	Email + Artifact timeline analysis

FTK Imager দিয়ে Deleted PST Carving:

1. Evidence drive image তৈরি করুন
2. File System > Email ফোল্ডার স্ক্যান করুন
3. `.pst` ফাইল carve করুন
4. Outlook অথবা PST Viewer দিয়ে analyze করুন

🛠 Email Forensics Tools (Free + Paid)

Tool Name	Description	Free/Paid	OS
FTK Imager	Image creation & email extraction	✓ Free	Windows
Autopsy	GUI-based forensic tool with email plugins	✓ Free	Windows/Linux
MailXaminer	Deep email analysis with PST, OST, MBOX support	✗ Paid	Windows
Forensic Email Collector (FEC)	Collects emails directly from IMAP/Webmail	✗ Paid	Windows
EmailTracer (Online)	IP ও email trace করার টুল	✓ Free	Web-based
Header Analyzer (MxToolbox)	ইমেইল হেডার বিশ্লেষণ	✓ Free	Web-based
P2 Commander (Paraben)	Outlook forensic analysis	✗ Paid	Windows
Mbox Viewer	MBOX ফাইল ভিউ ও এনালাইসিস	✓ Free	Windows
PST Viewer (Kernel, NirSoft)	PST/OST ফাইল দেখার জন্য	✓ Free (basic)	Windows