Email Forensics: Full Analysis and Investigation Workflow

This presentation covers email forensics, a vital branch of digital forensics. We will explore its objectives, common attack types, and the detailed workflow for analyzing suspicious emails. Learn about essential tools and prevention strategies.

Introduction to Email Forensics

Digital Forensics Branch

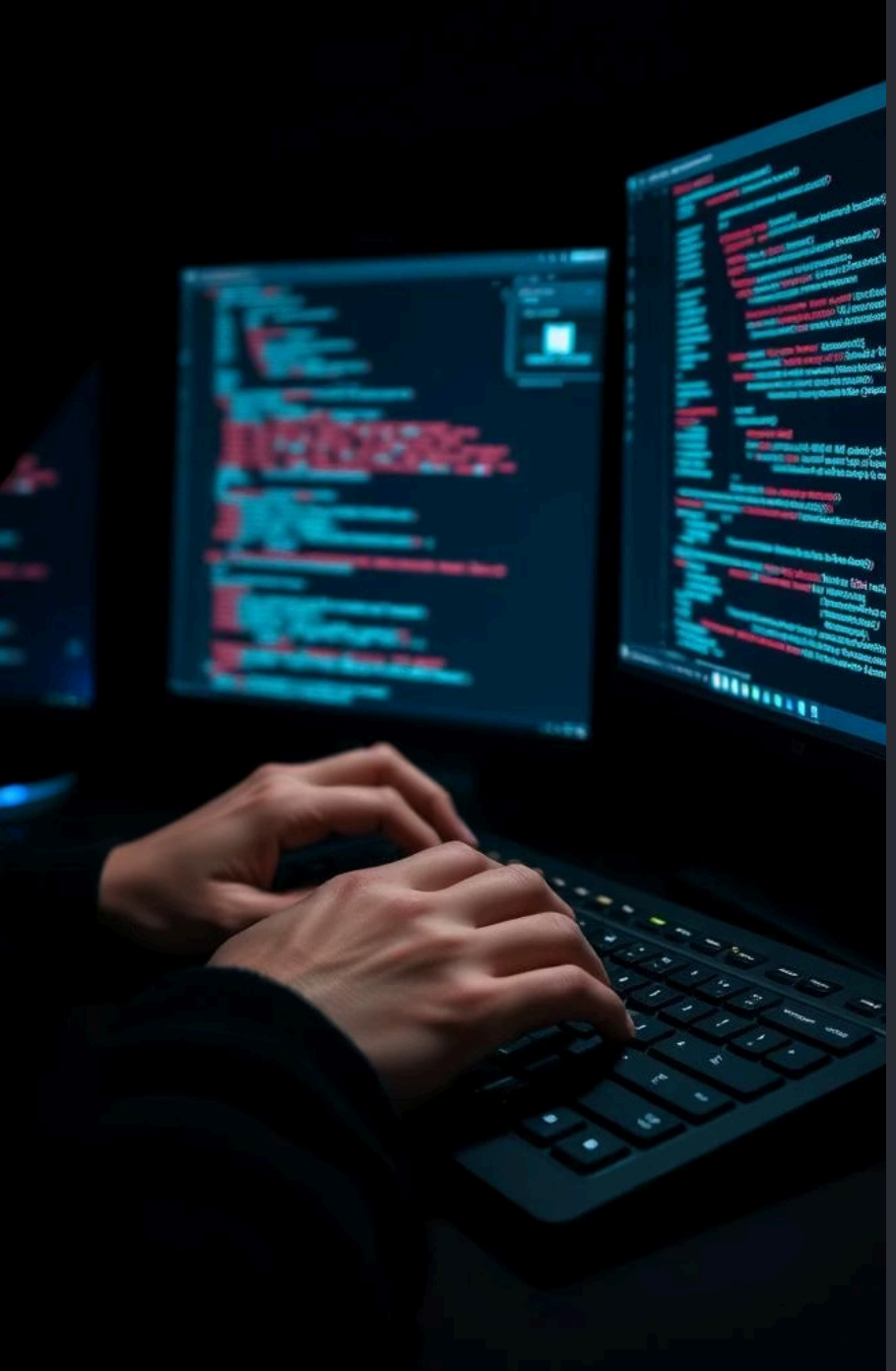
Focuses on recovering and analyzing email messages.

Combat Cybercrime

Detects and prevents phishing, fraud, malware, and impersonation.

Key Objectives

Trace origins, identify malicious content, gather evidence, understand attacker behavior.



Common Email Attack Types

Attack Type	Description
Phishing	Fake emails trick users into revealing credentials or clicking malicious links.
Spear Phishing	Targeted phishing, often impersonating internal staff or executives.
Business Email Compromise (BEC)	Attacker impersonates high-ranking person to request fund transfers.
Malware/Ransomware	Attachments or links install harmful software.
Spoofing	Fake email addresses used to appear legitimate.

Cyber Attacks via Email

Attack Vectors

- Malicious attachments (Word, Excel, EXE, ZIP)
- Links to phishing websites
- Remote Access Trojans (RATs) in scripts
- Credential harvesting via fake login pages

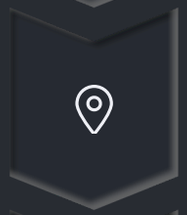
Real-World Scenario

1. Phishing email sent to employee.
2. Employee opens attachment or clicks link.
3. Malware installs, creates backdoor.
4. Threat actor gains remote access.
5. Data exfiltration or ransom demands follow.

How Email Is Analyzed (Workflow)

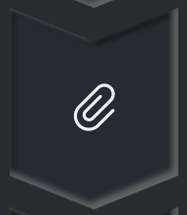
Email Header Analysis

Check paths, SPF, DKIM, DMARC, and source IP.



IP Location & Reputation

Geolocate IP, check for suspicious or blacklisted IPs.

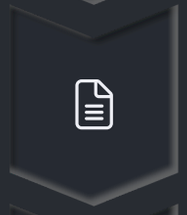


Attachment Analysis

Submit to sandboxes for malware behavior.

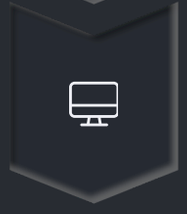
Link Analysis

Scan URLs for malicious content.



Content Analysis

Look for unusual language, impersonation, grammar errors.



Email Client Metadata

Check sending platform from email source.

Tools for Email Forensic Analysis

MXToolbox

Analyze headers, SPF, DKIM, DNS records.

VirusTotal

Scan links, attachments, IPs.

ANY.RUN

Interactive malware analysis for attachments.

IPlocation.net

Geolocate IP addresses.

Digital Forensic Investigation Process

Incident Detection

Employee reports or security tools flag suspicious email.

Preservation of Evidence

Export email, secure log files and artifacts.

Examination

Analyze header, body, links, attachments; use sandboxes.

Analysis

Correlate data with threat intelligence; map behavior to MITRE ATT&CK.

Reporting

Document IOCs; recommend actions (block IP, user awareness).

Prevention & Mitigation Tips

Employee Training

Educate on phishing awareness.

Email Authentication

Use SPF, DKIM, DMARC.

Filtering & Antivirus

Deploy email filtering and antivirus tools.

Endpoint Protection

Enable EDR for comprehensive security.