Computer Forensics

Week 10: E-MAIL AND SOCIAL MEDIA INVESTIGATIONS

Lecturer: Lemi Agrey Oliver

codingissweet@gmail.com

KUMI UNIVERSITY

Content

- Exploring the Role of E-mail in Investigations
- Exploring the Roles of the Client and Server in E-mail
- Investigating E-mail Crimes and Violations
- Understanding E-mail Servers
- Using Specialized E-mail Forensics Tools
- Applying Digital Forensics Methods to Social Media Communications

Exploring the Role of E-mail in Investigations

- Email evidence is crucial in computing investigations.
- Digital forensics investigators must understand email processing to gather essential evidence.
- With the rise of email scams, such as phishing and spoofing, investigators need skills to examine and interpret unique email content.
- Investigators may need to determine the authenticity of phishing emails.
- "Tracing an E-mail Message" teaches how to verify email and web addresses to check for spoofing.
- Phishing emails often use legitimate-looking links to deceive recipients and collect personal information.
- Pharming involves DNS poisoning to redirect users to fake websites, despite correct web addresses.

Exploring the Role of E-mail in Investigations+

- Investigators can check for redirection by viewing the email's HTML source code.
- The Nigerian Scam (419 scam) began in the 1970s and 1980s, transitioning from letters to fax and email, using typical patterns like asking for bank account access or promising rewards.
- Scams often feature uppercase text and poor grammar, with common themes like fake sweepstakes winnings.
- A landmark spoofing email lawsuit occurred in February 2001: Suni Munshani v. Signal Lake Venture Fund.
- Munshani claimed to receive an email instructing him to purchase $25 million in options.

Exploring the Role of E-mail in Investigations++

- Signal Lake found no record of the email on its servers.
- An impartial discovery firm found Munshani altered an email using a text editor.
- The ESMTP number in the email's header, unique to each message, exposed the fraud.
- More details on the case can be found at http://signallake.com/email_forensics_library/SMunshaniVsSL.pdf.

Exploring the Roles of the Client and Server in E-mail

- Email can be accessed via the Internet or an intranet (internal network).
- Both environments use a client/server architecture with a central email server and connected client computers.
- The server runs an email server program (e.g., Microsoft Exchange Server), while client computers use email programs (e.g., Microsoft Outlook) to interact with the server.
- Users' email access is controlled by permissions set by the email server administrator to ensure privacy.
- Users authenticate themselves to retrieve messages from the server.
- Intranet email systems are private, managed internally, and follow strict business practices and security policies.

Exploring the Roles of the Client and Server in E-mail+

- Intranet email addresses usually follow a company-determined naming convention (e.g., jsmith@somecompany.com).
- Internet email services (e.g., Gmail, Yahoo) are public, allowing users to create accounts with chosen usernames.
- Public email addresses do not follow a standardized naming convention, making tracking more challenging for investigators.(e.g codingissweet@gmail.com)
- Cloud-based email services are becoming common, offering global access but adding complexity for digital investigations depending on the service level agreement.

Investigating E-mail Crimes and Violations

➢ Objective of Email Investigations

- Identify the perpetrator of the crime or policy violation.
- Gather evidence.
- Present findings for reprimands, prosecution, or arbitration.

➢ Legal Considerations

- Be aware of privacy laws relevant to your jurisdiction (e.g., Electronic Communications Privacy Act and Stored Communications Act in the U.S.).

➢ Jurisdictional Differences

- Email crimes and violations vary by location.

Investigating E-mail Crimes and Violations+

- Example, Sending unsolicited emails is illegal in Washington State but may not be elsewhere.
- Consult with an organization's attorney to understand local email crime definitions.

➢ Common Email Crimes

- Email is frequently used in crimes such as narcotics trafficking, extortion, sexual harassment, stalking, fraud, child abductions, terrorism, and child pornography.
- Investigators often find emails linking suspects to crimes or policy violations.

➢ Scope of Communication Mediums

- Crimes or policy violations can involve emails, text messages, and social media communications.

Understanding Forensic Linguistics

- **Forensic linguistics** is a field at the intersection of language and law.
- The **International Association of Forensic Linguists** categorizes it into:
  - Language and law
  - Language in the legal process
  - Language as evidence
  - Research and teaching
- Language as evidence is crucial for this book's focus.
- Recognizing familiar writing styles can help identify authorship of emails.

Understanding Forensic Linguistics+

- Forensic linguistics involves:
- Analyzing voice recordings to identify speakers
- Comparing emails and writings to verify authorship
- Assessing chats, voicemails, and text messages
- Forensic linguists help determine authorship based on tone and style, as depicted in crime dramas.
- **Liz Martinez's article** discusses the capabilities and limitations of forensic linguistics.
  - Accepted in many courts globally as a valid science
  - Helps identify speaker's dialect and origin
  - Useful in verifying authenticity of suicide notes, text messages, and social media posts
  - Cannot determine an author’s truthfulness or gender

Understanding Forensic Linguistics++

- Forensic linguistics applies to civil, criminal, and cyberterrorism cases.
- The **median income** for a forensic linguist is around $65,000 per year.
- **Educational opportunities** include bachelor's and master's degrees in forensic linguistics.

Examining E-mail Messages

- **Initial Steps**
  - Access the victim's computer or mobile device to retrieve email evidence.
  - Use the victim’s email client to locate and copy potential evidence.
  - Log in to the email service to access protected or encrypted files if needed.
- **Corporate and Criminal Investigations**, Ensure policies are in place for corporate investigations.
- Obtain warrants to access or copy files on a server for criminal investigations.
- **Handling Stalking Cases**, If direct access to the victim’s computer is not possible, guide the victim over the phone to open and print a copy of the offending email, including the header.

Examining E-mail Messages+

- **Importance of Email Headers**, Email headers contain unique identifying numbers like IP addresses
- Headers help trace the email to the suspect.
- **Case Study - Munshani Case**
  - An email header revealed the suspect email was fake due to identical ESMTP IDs with another email.
  - Unique ESMTP IDs are assigned by UNIX servers based on the precise date and time.
  - No record of the suspect email was found on the company's email server.
- **Tracing Emails**
  - Investigators use headers and encoding to trace the route of emails through servers.
  - This information helps determine the sender's location or identity.

Examining E-mail Messages++

- **Further Reading**, For detailed examination of email headers, refer to "The E-mail Forensics GuideBook" (www.freeviewer.org/email-forensics/).
- **Recovering Deleted Emails**, Sometimes it’s necessary to recover deleted emails.
- Instructions for recovering emails are provided in “Using Magnet AXIOM to Recover E-mail”.

Copying an E-mail Message

- Copy and print the email involved in the crime or policy violation,
- Forward the email as an attachment to another address if required by your organization’s guidelines.
- In the following slides, we shall discuss, the guidelines for handling emails in various email programs.
- Even if you don't have access to all programs, these guidelines can help in similar scenarios.
- **Example Using Outlook,** Instructions are given for copying an email message to a USB drive using Outlook.
- Steps may vary slightly depending on the Outlook version.
- Similar procedures apply for other email programs.

General Steps for Copying Emails[1]

- **The following are the steps for** copying emails to a USB drive in case of Outlook or Outlook Express.
- 1. Insert a USB drive into a USB port.
- 2. Open File Explorer, navigate to the USB drive, and leave this window open.
- 3. Start Outlook by going to the Start screen, typing Outlook, and pressing Enter.
- 4. In the Mail Folders pane, click the folder containing the message you want to copy. For example, click the Inbox folder. A list of messages in that folder is displayed in the pane in the middle. Click the message you want to copy.

General Steps for Copying Emails[1]

- 5. Resize the Outlook window so that you can see the message you want to copy and the USB drive icon in File Explorer.
- 6. Drag the message from the Outlook window to the USB drive icon in File Explorer.
- 7. Click the File tab, and then click Print to open the Print pane. After printing the e-mail so that you have a copy to include in your final report, exit Outlook.

Copying an E-mail Message+

➢ Copying Emails Using GUI Programs

- Drag and drop the email to a storage medium (e.g., folder, drive).
- Save the email in a different location through the program's save option.

➢ Copying Emails Using Command-Line Programs

- Open the email message.
- Use the copy option, typically found at the bottom of the screen.

➢ Working with Email Copies

- Always work with the copied email, not the original.
- This prevents accidental alterations to the original evidence.

Viewing E-mail Headers

- To view email headers, use the email client that created the message.
- Instructions are provided for accessing email headers in various email programs, including, Windows GUI clients and Common web-based email providers
- After accessing the headers, copy and paste them into a text document.
- Recommended text editors, includes, Windows Notepad+, Linux vim, Nano (UNIX), macOS TextEdit
- The next section explains how to examine email headers.

Viewing E-mail Headers

- In a forensics lab or elsewhere, familiarity with multiple email programs is beneficial.
- Suspects may use different email programs, so it's important to identify which one they use.
- Many people have web-based email accounts (e.g., Gmail, Yahoo!), so look for evidence of these accounts.

Steps for retrieving email outlook header[1]

- Start Outlook, and then select the message you copied in the previous section.

Steps for retrieving email outlook header[1]

- Double-click the message, and then click File, Properties. The “Internet headers” text box at the bottom contains the message header.
- Select the message header text, and then press Ctrl+C to copy it to the Clipboard.
- Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.
- Save the document as Outlook header.txt in your work folder. Then close the document and exit Outlook.

Viewing Gmail Web e-mail[1]

- Start your Web browser, and log on to Gmail.
- Open an e-mail, click the down arrow next to the Reply circular arrow, and click Show original.
- A new tab opens in your browser that shows basic information at the top, such as the message ID, from, to, and subject line. As you scroll down, you can see the header details along with the original message and encoding. Click the Download Original link to open the “Opening original_msg.txt” dialog box. Click Open with Notepad (default) and click Okay. Save the file in your work folder with the default name.

Examining E-mail Headers

- Examine the saved email header to gather information about the email and trace the suspect's location.
- Key information to find
  - Originating email’s domain address or IP address
  - Date and time the email was sent
  - Filenames of any attachments
  - Unique message number, if available
- To open and examine an e-mail header, follow these steps:
- Open File Explorer and navigate to your work folder.
- Double-click a .txt file containing message header text, such as Outlook header.txt. The message header opens in Notepad.

Examining Additional E-mail Files

- Email programs save messages on the client computer or leave them on the server, depending on client and server settings.
- Emails can be saved in separate folders for record-keeping.
  - In Outlook, emails can be saved in .pst files (for sent, draft, deleted, and received emails) or .ost files (offline files).
  - .pst files allow offline access to emails.
  - With cloud-hosted Exchange servers, .ost files may be stored on the device, while .pst files remain on the server, requiring network administrator access to retrieve them.

Examining Additional E-mail Files+

- Email programs often include additional features like address books, calendars, task lists, and memos, which can provide valuable investigative information.
- Web-based emails are saved as web pages in browser cache folders.
  - Web-based email providers often offer IM services (e.g., Yahoo! Messenger, Google Talk, Facebook Messenger), saving messages in various file formats.
  - IM files are usually stored in specific folders (e.g., Users\username\AppData or Program Files in Windows 8.1).
- Special tools may be needed to read proprietary IM file formats.

Examining Additional E-mail Files++

- Some IM programs do not save chat content by default; users must change settings to enable saving.
  - Message fragments might be found in the suspect's Pagefile.sys file.
  - Windows Messenger stored messages in RTF format readable by most word processors.
  - Despite Microsoft no longer supporting Windows Messenger, it may still be encountered in investigations.
- Investigating these files on a victim's computer can help document corroborating evidence.

Tracing an E-mail Message

- Determine an email's origin by examining the header using free Internet tools.
- This process is called "tracing."
- Internet lookup tools can help trace the email's origin.
- If an email address includes a company name, visit the company's website to find the domain administrator.
- If the contact isn't listed or the domain lacks a website, use registry sites to find the contact:
  - www.arin.net: American Registry for Internet Numbers (ARIN) to map IP addresses to domain names and find the domain's contact.

Tracing an E-mail Message+

- www.internic.com: Similar to ARIN, used for finding domain IP addresses and contacts.
- www.google.com: Search engine for additional information and postings on discussion boards.

➢ Use these websites to find the suspect's full email address and contact information.

➢ Verify findings by checking network email logs against the email addresses, as suspects might provide false information.

Using Network E-mail Logs

- Network administrators keep logs of inbound and outbound traffic handled by routers.
- Routers use rules to allow or deny traffic based on IP addresses.
- Routers typically track all traffic flowing through their ports.
- These logs can help trace the path of a transmitted email.
- Network administrators can provide the necessary log files.
- Review router logs to find the victim's (recipient’s) email and its unique ID number.
- Network administrators also maintain firewall logs that filter Internet traffic.

Using Network E-mail Logs+

- Firewall logs can verify if an email message passed through the firewall.
- Firewalls track Internet traffic to and from protected networks.
- Firewall log files can be opened with text editors like Notepad (Windows) or vim (Linux).
- Some firewalls require special programs to read their log files.

Understanding E-mail Servers

- A mail server (sometimes called an email server) is a software program that sends and receives email. Often, it is used as a blanket term for both mail transfer agents (MTA) and mail delivery agents (MDA), each of which perform a slightly different function.[2]
- Email servers use protocols and maintain logs for their services.
- As an investigator, your focus is on retrieving email information, not understanding the server's inner workings.
- Collaborate with network or email administrators to find needed data or files.
- If administrators are unavailable, research online or use forensics tools to investigate.
- Email servers handle and record emails differently:
  - Some use databases, others use flat file systems.
  - Logs can record email transactions by default or need configuration.

Understanding E-mail Servers+

- Email administrators log operations and traffic for:
  - Disaster recovery.
  - Ensuring firewall and email filters function correctly.
  - Enforcing company policies.
- Logging can be disabled or set to circular logging, which overwrites logs after a set size or time.
  - Example: Monday's log (Mon.log) is overwritten the next Monday.
  - Backups are needed to access overwritten logs.
- Email logs typically include, Received email messages, IP addresses, dates and times, client access times, contents, system-specific info.
- Logs are usually in plain text, readable by text editors like Notepad or vim.

Understanding E-mail Servers++

- Administrators often set servers to continuous logging mode.
  - Logs can be combined or separated (e.g., date/time, size, IP address).
- Separate logs help filter or sort data using headers with timestamps and IP addresses.
- Contact the suspect's network/email administrator promptly as logs may only be kept for 30 days or less.
- Email servers may retain copies of emails, even if deleted by users.
  - Deleted emails are not fully removed until the system is backed up.
  - Administrators might recover deleted emails without full server restoration.
  - Similar to file deletion on hard drives, emails marked for deletion can be recovered until overwritten.
  - Administrators can recover emails from backups if provided with date and time stamps

Examining UNIX E-mail Server Logs

- UNIX systems offer many email server programs, with Postfix and Sendmail being common examples.
- Sendmail is often the default for FreeBSD systems like CentOS.
- Configuration files, like /etc/mail/sendmail.cf for Sendmail, determine logging and handling of emails.
- /etc/syslog.conf includes email logging instructions for Sendmail, specifying how events are logged.
- Postfix, another common UNIX email server, uses /etc/postfix/master.cf and /etc/postfix/main.cf for configurations.
- Email files are typically stored in /var/mail for Sendmail and /var/spool/postfix for Postfix.

Examining UNIX E-mail Server Logs++

- The syslog.conf file in UNIX systems specifies where to save different email log files, like /var/log/maillog for SMTP communication records.
- The maillog file contains important information for investigations, including IP addresses and timestamps.
- UNIX systems usually store log files in /var/log, but administrators can change this location.
- The find or locate command can be used to find email logs if they're not in the expected location.
- The UNIX man pages provide assistance for finding default file locations.
- Client computers create a /home/username/mail directory for email storage.

Examining UNIX E-mail Server Logs++

- If the UNIX email server stores messages on the server, access can be requested through the UNIX administrator.
- UNIX email servers typically don’t use groups to prevent unauthorized access to emails, but groups can be set up for investigative purposes with appropriate authorization.

Examining Microsoft E-mail Server Logs

- Exchange Server is Microsoft's email server software, using an Exchange database based on the Microsoft Extensible Storage Engine (ESE).
- Important files for investigations include .edb database files, checkpoint files, and temporary files.
- .edb files store messages formatted with Messaging Application Programming Interface (MAPI).
- Exchange logs data changes (transactions) in transaction logs, with a checkpoint file marking the last write point to prevent data loss.
- .tmp files are created during busy periods to prevent data loss when converting binary data.
- Exchange maintains logs for tracking emails, retrievable using Windows PowerShell cmdlet.

Examining Microsoft E-mail Server Logs+

- Tracking.log records messages if the Message Tracking feature is enabled, providing timestamps, sending computer's IP address, and email contents with verbose logging.
- The troubleshooting log, viewable in Windows Event Viewer, helps troubleshoot and investigate Exchange environments, showing events with ID numbers and severity levels.
- The Event Properties dialog box in Event Viewer provides detailed information about email events, useful for investigating suspected tampering with email servers.

Using Specialized E-mail Forensics Tools

- In cases where email administrators are unavailable or the email environment is highly customized, data recovery and forensics tools can be used to recover email files.
- Tools like Magnet AXIOM, Autopsy, and OSForensics, as well as others specifically designed for email recovery, can be utilized.
- These tools can recover deleted attachments, analyze email logs, and decode email headers.
- Searching for .db files or using .log as search criteria can locate email database files and log files.
- Forensics tools enable the retrieval of email database files, personal email files, offline storage files, and log files.

Using Specialized E-mail Forensics Tools+

- Data recovery tools simplify the extraction of data from email servers and clients without requiring in-depth knowledge of their operation.
- When serving as an expert witness, understanding email system functions is necessary for explaining findings to non-technical individuals.
- After comparing email logs with messages, verification of email account details, message IDs, IP addresses, and timestamps is essential for warrant consideration.
- Follow evidence-handling rules and control measures during evidence collection.
- Document procedures and tools used during evidence collection, whether creating an image or copying specific folders.

Using Specialized E-mail Forensics Tools++

- Some tools can scan email database files on suspect computers to recover deleted emails and associated attachments.
- Documenting the restoration of deleted emails and viewing associated files ensures proper documentation of the examination process.

Using a Hex Editor to Carve E-mail Messages

- Few vendors offer products for analyzing email in systems other than Microsoft, such as macOS Mail or Evolution.
- A method is described for acquiring Evolution email directories and extracting messages using Hex Workshop, applicable to email systems storing messages in flat plaintext files (mbox format).
- Vendor-specific email file systems like Microsoft .pst or .ost use MIME formatting, making them challenging to read with standard editors.
- To carve emails from Evolution, the .evolution directory and its subdirectories need to be copied to another storage medium for analysis.

Using a Hex Editor to Carve E-mail Messages+

- Exporting this directory from an image file to a target drive path or using the Linux tar command is an easy way to extract email data for forensic analysis.
- Acquiring the .evolution directory from a Linux computer allows for comparison of email messages with other email formats, like .pst files, to detect differences and uncover additional email addresses.

Recovering Outlook Files

- Forensics examiners often need to reconstruct .pst files and email messages.
- Advanced tools like Magnet AXIOM, OSForensics, X-Ways Forensics, AccessData FTK, and Guidance Software EnCase can partially or fully recover deleted .pst files.
- Reconstructing these files usually requires additional effort to extract their contents.
- The scanpst.exe tool, included with Microsoft Office, can repair both .ost and .pst files.
- It can be run from File Explorer or a command prompt to process and rebuild data into a .pst file accessible by Outlook or other tools.

Recovering Outlook Files+

- Guidance Software uses the SysTools plug-in for extracting .pst files from EnCase Forensic.
- This plug-in supports Outlook versions up to 2013 and doesn't require Outlook installation to examine emails.
- DataNumen Outlook Repair is a highly regarded tool for recovering email data from Outlook and other formats.
- It can recover files from VMware, Virtual PC, ISO images, and other backup types.
- This tool is utilized in various hands-on projects for email data recovery.

Applying Digital Forensics Methods to Social Media Communications

- Social media sites like Twitter, Facebook, LinkedIn, and YouTube are used for communication, business, fundraising, and more. These online social networks (OSNs) contain valuable information for investigations, including
  - Evidence of cyberbullying and witness tampering
  - Company positions on issues
  - Intellectual property rights violations
  - Details of who posted information and when

Applying Digital Forensics Methods to Social Media Communications+

- The use of social media in legal cases is increasing. For example, evidence from LinkedIn can show intellectual property theft, as seen in a case where an employee copied company records before leaving for a competitor.
- Law enforcement frequently uses social media for background checks, corroborating data, verifying alibis, and identifying suspects and witnesses.
- A significant challenge is authenticating the author and information in social media posts. For instance, in the case U.S. v. Brown, the court accepted Facebook chats as evidence after Facebook authenticated the chats and other witnesses corroborated the content.

Applying Digital Forensics Methods to Social Media Communications+

- Digital investigators use techniques like big data analytics to sift through the vast amount of data on social media. This data includes videos, pictures, GPS locations, text messages, emails, tweets, and posts.
- Investigations often involve multiple jurisdictions and require warrants or subpoenas to access information from social media servers.
- Facebook provides two types of profiles, basic subscriber info (e.g., last login, email, phone number) and Neoprint (e.g., friends, groups, videos, undeleted photos), which typically require a warrant to access.
- Cases can range from companies selling illegal merchandise to verifying alibis through posts. Investigators need a comprehensive approach to determine relevant evidence, which now includes examining social media and cloud data in addition to physical devices like cell phones and laptops.

Social Media Forensics on Mobile Devices

- In mid-2017, Facebook had 2 billion users globally, with 1.74 billion (87%) being mobile users.
- Twitter had 328 million monthly users, with 80% accessing via mobile devices.
- A 2012 study analyzed Facebook, Twitter, and MySpace usage on BlackBerries, iPhones, and Android devices, discovering that iPhone physical acquisitions required "jailbreaking" to gain root access and bypass provider restrictions.
- Evidence artifacts varied by social media platform and device type.
- On iPhones, a SQLite database for Facebook was found, containing friend lists, IDs, phone numbers, and upload tracking files. Similar databases were found on Twitter.

Social Media Forensics on Mobile Devices+

- On Android devices, Facebook friends appeared in the contacts list due to synchronization.
- iPhones and Android devices provided the most information, often stored in SQLite databases.
- Following standard forensic procedures—starting with a logical acquisition followed by a physical acquisition—can yield substantial evidence, especially on unlocked devices.

Forensics Tools for Social Media Investigations

- Few tools are available for social media forensics, and many have shifted from free or low-cost to being part of forensics suites like FTK Social Analyzer, or offer limited trial periods.
- Legal challenges arise concerning the admissibility of evidence gathered by these tools in court or arbitration, and investigators may need additional warrants or subpoenas if unrelated evidence is found during an investigation.
- Permission from the individuals whose information is being examined may be necessary when using social media forensics software.
- Many tools use customized web crawlers to gather data, but they often take too long to be efficient.

Forensics Tools for Social Media Investigations+

- Some effective software packages are available, such as X1 Social Discovery, which can operate in two Facebook modes: using a credentialed user account (requiring the person's username and password) and a public account (for examining publicly accessible posts). X1 also supports Twitter and YouTube investigations.
- Researchers have also developed an open-source tool for targeting Facebook accounts.
- A warrant or subpoena is generally required to obtain records from online social networks (OSNs), but cooperative individuals might provide their usernames and passwords voluntarily.
- If cooperation isn't possible, investigators can access only public profiles or become friends with someone connected to the target to gain limited information.
- When conducting such investigations, start with a workstation free of personal information or use a virtual machine with a bridged network to ensure a different IP address from the host computer.

Reference

1. Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning.
2. (N.d.). Retrieved from https://www.cloudflare.com/learning/email-security/what-is-a-mail-server/
3. Sun, J. R., Shih, M. L., & Hwang, M. S. (2015). A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure. *Int. J. Netw. Secur.*, *17*
4. Oettinger, W. (2020). *Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing Ltd.