EMAIL Forensics:

Questions to ask for.

1. **Who sent the email?**
2. **When was it sent?**
3. **Where was it sent from?**
4. **Is there relevant content?**

EMAIL Structures

Email Structure:

- Header: Metadata Like Sender, recipient, timestamp, and routing information.
- Body: Content of the email, which include text, images, multimedia
- Attachments: Often carrying critical information.

Email Body Analysis:

- Manual Review: Using forensic tool or manually read each message.
- Keyword Searching: Filter emails based on specific keywords or phrases.
- Data reduction: Remove duplicate emails.

Email Attachments:

- Formats:
- Identifications: Matching attachments with corresponding emails.
- Security Risks: Virus scanning of attachments.

Email Headers

Email Transmission Path:

- Mail Client: Email Originate from email client, Application like Outlook, web based.
- Mail Transfer Agent (MTA): Client communicates with MTA, Server running the SMTP and responsible for transmission.
- Route: MTA Identifies recipient's server and forwards emails. Emails may transverse multiple MTAs.

Key Metadata in Email header:

- Message-ID: Unique tracking number for the email.
- Received: Email's path with server IP address, timestamps, and time zones. Validate authenticity. *(Always analyze from Bottom to Up)*
- X-Originating-IP: Reveal the sender's IP address, (removed from Gmail and outlook)
- X-Mailer: Email client used, (Field is now missing Gmail and Outlook)

- X-Forwarded-For: Email was forwarded from another source, Possibly Load-balancing, or proxy servers.
- X-BarracudaApparent-Source-IP: Unique to barracuda devices, Optional provides the apparent source IP address.

Headers: https://www.iana.org/assignments/message-headers/message-headers.xhtml

X-headers: - X-Headers are experimental or extensions to normal RFC headers. Mail providers can create X-Headers for internal tracking or administrative purposes.

Key Elements to Analyse

1. **Received Headers**: Start from the bottom and work your way up. These headers detail the servers the email passed through.
2. **SPF Records**: Check for valid SPF records. Apple, for example, publishes SPF records.
3. **DKIM**: Look for DKIM signatures to verify message integrity.
4. **Return Path**: Verify that the return path is from a legitimate source, not a suspicious domain.
5. **Message ID**: Compare with known legitimate messages to check for consistency.

Construction of Message ID: Typically combines the current date/time with unique system identifiers like a process ID or domain name.

Detection: Checking the message ID format can help detect forged emails.

SPF, DKIM, DMARC

SPF (Sender Policy Framework)

- **Authentication**: SPF serves as a validation mechanism, allowing organizations to specify which mail servers are authorized to send emails on behalf of their domain.
- **Received-SPF**: This header field indicates the outcome of SPF validation. A "pass" typically signifies a legitimate email, while a "fail" might indicate a potentially suspicious email.

DKIM (DomainKeys Identified Mail)

- **Authentication**: DKIM adds a digital signature to emails, validating both the source and content of the email.
- **DKIM-Signature**: This header field contains the DKIM signature and associated information. A successful DKIM validation usually results in a "pass" status.

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

- **Authentication**: By aligning the "header from" address with SPF and DKIM information, DMARC provides an additional layer of email authentication.

- **dmarc**: This header field displays the DMARC policy status, which can be "pass," "fail," "none," or other designated states. It also indicates policy actions like "p=REJECT" or "p=NONE."

Host-Based Email

Host-based email stores are local email archives stored on a computer, distinct from server-based email archives.

Host-Based Email Archives:

1. Index File and Message Store

- **Index File:** Store metadata about the emails like read status, flags, and reply or forward information.
- **Message Store:** This is where the actual email messages, attachments, contacts, and calendar items are stored.

2. Associated Email Clients

This association provides investigators with clues about where to find these archives by reviewing installed applications or searching for specific file extensions.

Role of Outlook .PST (Personal storage table) Files:

Most common host-based email archives.

- PST files serve as a single repository for emails, folders, attachments, contacts, and calendar items.
- Newer versions of .PST files can store up to 50 GB of data.
- .PST files offer encryption options ranging from "No encryption" to "High encryption,"
- Deleted messages may still be present in .PST files, but specialized tools are required to recover this data.

.OST (Offline Storage Table) Files:

Especially with features like "Cached Exchange Mode.

- .OST files allow users to access their emails even when offline,
- .OST files from Outlook 2013 contain a cached version of the last 12 months of user Exchange data and can be up to 50 GB in size.
- Conversion to .PST format using third-party tools is often required for easier access and analysis.

.PST File Locations:

1. **Outlook 2019, Outlook 2016, Outlook 2013, Outlook 2010:** C:\Users\[username]\Documents\Outlook Files
2. **Outlook 2007, Outlook 2003 and earlier:**

C:\Users\[username]\AppData\Local\Microsoft\Outlook

.OST File Locations:

1. **Outlook 2019, Outlook 2016, Outlook 2013. Outlook 2010, Outlook 2007:** C:\Users\[username]\AppData\Local\Microsoft\Outlook
2. **Outlook 2003:** C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\Outlook

Notes:

- The AppData and Local Settings folders are hidden by default.
- The locations mentioned above are default paths, but users can change the location of .PST and .OST files, so it's always a good practice to check the actual locations in Outlook settings or through the registry.

.PST Location Registry Key:

- HKEY_CURRENT_USER\Software\Microsoft\Office\xx.0\Outlook
- (Replace xx.0 with the version of Outlook you are using, e.g., 16.0 for Outlook 2016/2019 and 15.0 for Outlook 2013.)

.OST Location Registry Key:

- HKEY_CURRENT_USER\Software\Microsoft\Office\xx.0\Outlook
- (Again, replace xx.0 with your Outlook version.)

Tip: Forensic tools like FTK, EnCase, and specialized utilities like scanost.exe and pffexport can assist investigators in analysing these archives or kernel OST/PST Viewer.

Outlook Attachments recovery

1. When attachments are reviewed or opened in outlook they are save in content.outlook folder on local drive
2. Starting from outlook 2007, attachments in this folder are deleted when outlook is close, but there are exceptions like outlook crashes or open files.

Location:

Default location:
C:\Users\<Username>\AppData\Local\Microsoft\Windows\INetCache\Content.outlook\

Registry key folder location:

HKCU\Software\Microsoft\Office\<Version>\Outlook\Security\OutlookSecureTempFolder\

Forensic techniques:

$MFT (to determine exact time of attachment opened)

$Logfile, $USNJournal, and Copies of $MFT in VSS for traces of attachments, even outlook removed them.

Email Client:

Email Program, Email software that enables users to send, manage email messages.

Exported Email files: Thunderbird's .EML Files, which might contain crucial information.

Identifying Email client: Review installed program, Internet search.

Calendar Entires: .ICS files commonly used for calendar data.

Address books: .WAB, .PAB, .VCF, .MAB, NNT common.

Task Lists: Task lists reside with calendar files in SQLite Format with .SDB extension.

Corrupted Email Archives: Tool like scanpst.exe can repair corruption.

Email Encryption:

Individual message encryption:

- **Public-Key protocols:** (S/MIME) and (PGP/MIME)
- **File extensions:** Look out of PGP or P7M (S/MIME) Extensions as indicator of encryption.

Client-Side encryption:

- Outlook and Lotus Notes support encryption for locally stored archives.

Network-Based Mail encryption:

- TLS/SSL

Common Traits of Email clients and Investigation considerations:

1. File Structure:
   - Copy all mail directories during export for data recovery.
2. Message storage:
   - Message stored in Text form, use of search tool to locate and review using text editors.
3. Access control:
   - Tools Like Mail Pass View in recovering passwords for email client.
4. Data recovery:
   - Email archives are often hidden, requiring alternate for review.

Outlook Specifics:

- File Format: stored in .pst file.

- Default encryption options for added security.
- Accessible until compaction or cleanup.

Email Storage: Server vs Workstation.

Locations:

1. Server-Based: Hosts most recent email traffic.
2. Workstation-Based storage: Hold offline or archived email data.

Recommended tools for analysis:

1. Forensic suites: X-ways, Encase, FTK
2. Dedicated email tools: Systools Mail examiner, Aid4Mail, Emailchemy, Logikcull

Microsoft Exchange: (Market Leader)

1. Exchange 2007: .EDB database files, located C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group\Mailbox Database.edb
2. Prior to Exchange 2007: .EDB and .STM Files
3. .log files: data recovery, capturing before committing to .EDB
4. Eseutil tool: data import into .EDB files for recovery and analysis.

Recoverable Items (Folder) In Microsoft exchange:

Hidden folder within the user's Mailbox in Microsoft exchange.

1. Not directly accessible via outlook or webapp
2. Moves with mailbox across databases.
3. Deleted mailbox: 30 days, soft deletes: 14 days.
4. Mailbox auditing off by default

Tool for accessing and analysing "Recoverable Item"

1. Exchange admin centre (EAC)
2. Forensic suites: Encase, X-ways, FTK
3. PowerShell commands: Exchange management shell.

https://learn.microsoft.com/en-us/powershell/module/exchange/?view=exchange-ps#mailboxes

Below are some commonly used PowerShell commands to work with the "Recoverable Items" folder:

1. **Get-MailboxFolderStatistics**

```
Get-MailboxFolderStatistics -Identity <MailboxIdentity> | Where-Object {$_.FolderPath -like '*Recoverable Items*'}
```

2. Search-Mailbox

```
Search-Mailbox -Identity <MailboxIdentity> -SearchQuery 'folderpath:"Recoverable Items"'
```

3. New-MailboxSearch

```
New-MailboxSearch -Name "RecoverableItemsSearch" -SourceMailboxes <MailboxIdentity> -SearchQuery 'folderpath:"Recoverable Items"'
```

4. Get-RecoverableItems

```
Get-RecoverableItems -Identity <MailboxIdentity>
```

5. Restore-RecoverableItems

```
Restore-RecoverableItems -Identity <MailboxIdentity> -FilterItemType IPM.Note
```

Notes:

- Replace **<MailboxIdentity>** with the actual mailbox identity or email address.
- Ensure you have the necessary permissions to execute these cmdlets, typically requiring Exchange Admin or Compliance Management roles.

Email Evidence from Network-Based servers:

1. Live imaging is often the viable option.
2. Export each mailbox or a PST file, Tool: - Exchange management shell.
3. Leveraging Server backups like WSB (windows server backup can provide reliable and efficient way to capture exchange data).

Email data extraction from exchange server:

- **New-MailboxImportRequest**: Used to import mailbox data.
- **New-MailboxExportRequest**: Used to export mailbox data.

Commands for exchange 2010 SP1 and above:
Example Syntax:

```
New-MailboxExportRequest -Mailbox akash_patel -FilePath \\Server\Folder\akash_patel.pst
```

Export with Date Range and Advanced Filtering:

```
New-MailboxExportRequest -Mailbox akash_patel -ContentFilter {(body -like "*Welcome*") -and (Received -gt "01/01/2024" -and Received -lt "03/01/2024")} -FilePath \\Server\Folder\akash_AdvancedFiltered.pst
```

Export Multiple Mailboxes:

```
Get-Mailbox -ResultSize Unlimited | Where-Object {$_.RecipientTypeDetails -eq "UserMailbox"}
| New-MailboxExportRequest -FilePath \\Server\Folder\AllMailboxes.pst
```

Incremental Export:

```
New-MailboxExportRequest -Mailbox rob_lee -IncludeFolders "#Inbox#" -FilePath
\\Server\Folder\Akash_Incremental.pst -IsArchive
```

Commands for Exchange Server 2007:

Example Commands:

```
Export-Mailbox -Identity akash@gmail.com -PSTFolderPath C:\akash.pst Get-Mailbox -
Database 'Corporate' | Export-Mailbox -PSTFolderPath C:\PST
```

Export with Date Range:

```
Export-Mailbox -Identity akash@gmail.com -StartDate "01/01/2022" -EndDate "03/01/2022" -
PSTFolderPath C:\akash_DateFiltered.pst
```

Export to Network Location:

```
Get-Mailbox -Database 'Corporate' | Export-Mailbox -PSTFolderPath
\\Network\Share\Corporate.pst
```

Export Specific Folder:

```
Export-Mailbox -Identity akash@gmail.com -IncludeFolders "\Sent Items" -PSTFolderPath
C:\akash_SentItems.pst
```

For Exchange Server 2003, 2000, and 5.5:

For older versions of Exchange, the primary tool for exporting mailbox data is ExMerge.

Example command:

```
ExMerge -B -F C:\userlist.txt -D C:\PST\ -S ExchangeServerName
```

Refernces:

[1] New-MailboxExportRequest:
https://learn.microsoft.com/en-us/powershell/module/exchange/new-mailboxexportrequest?view=exchange-ps&redirectedfrom=MSDN
[2] -ContentFilter Parameter:
https://learn.microsoft.com/en-us/exchange/filterable-properties-for-the-contentfilter-parameter?redirectedfrom=MSDN
[3] Using the Exchange Management Shell:

https://learn.microsoft.com/en-us/previous-versions/tn-archive/cc505910(v=technet.10)?redirectedfrom=MSDN

Compliance Search in Microsoft exchange:

Compliance Search: tool for email investigations, internal audits, and incident response enable administrators and investigators to search across multiple mailboxes in exchange.

- Export search result to .PST files on identified object.
- Single search is capped at 500 mailboxes and 50 GB data.

In Action:

New-ComplianceSearch -name "Legal Case 280" -ExchangeLocation "Operations" -ContentMatchQuery "'Query' AND 'Akash'"

Exchange 2010:

Exchange 2010 relied on "Multi-Mailbox Search." While less refined than Compliance Search, it offered advanced searching capabilities within a designated Discovery Management user group.

Why Compliance Search Matters

Compliance Search is a must-have for modern email management and forensic investigations. When leveraging Compliance Search, always ensure you are adhering to forensic best practices.

References

[1] Use Compliance Search to Search All Mailboxes in Exchange 2016: https://learn.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/compliance-search?view=exchserver-2019&redirectedfrom=MSDN
[2] New-ComplianceSearch: https://learn.microsoft.com/en-us/powershell/module/exchange/new-compliancesearch?view=exchange-ps&redirectedfrom=MSDN
[3] Exchange 2010 £-Discovery Multi-Mailbox Search: https://www.exchangeinbox.com/article.aspx?i=148

Content Search in Office 365

Search tool within the Office 365 Security & Compliance Center that allows administrators and investigators to search across all mailboxes within an organization.

Example of initiating a Content Search via PowerShell:
New-ComplianceSearch -name "Legal Case 80" -ExchangeLocation "Operations" -ContentMatchQuery "'Widget' AND 'Akash'"

Auditing and Logging:
Office 365 offers built-in auditing is not enabled by default.

Enable auditing for a user via PowerShell:

```
Set-Mailbox -Identity "Akash Patel" -AuditEnabled $true
```

Set all available logging options for mailbox owner accounts:

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -AuditEnabled $true -AuditOwner "Create,HardDelete,MailboxLogin,Move,MoveToDeleteditems,SoftDelete,Update"
```