Exchange Forensic

Compliance Features in Exchange 2010/2013/2016

Jona, 8. September 2016

damian.pfammatter@compass-security.com

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@compass-security.com
www.compass-security.com

Scope

What this Talk is about…

- Explore basic **Exchange Features** to gather and analyze Data in E-Mail Investigations
- Preserve and analyze Data from live running Servers

This is where most E-Mail Forensic Investigation should **start** (Exchange Server Level)…

…do deeper Analysis (E-Mail Clients), if required information could not be found.

…and what not?

- Marketing expensive 3rd-Party Tools to copy and analyze Exchange Data
- Obtaining Backup Copies of entire Exchange Server Databases

Agenda

Focus on Exchange 2010/2013/2016 **On-Premises**, similar Features available in Exchange Online

- Importance of E-Mail Forensics
- Exchange 2016 Architecture
- Exchange Compliance Features
  - Message Tracking
  - Single Item Recovery
  - In-Place / Litigation Hold
  - Mailbox Auditing
  - Administrator Auditing
  - Others (Transport Rules, Journaling, Archiving, Full Backups)
- Take Home Message

Including some Examples of how to behave malicious…

… and how to get caught!

Importance of E-Mail Forensics

- Most utilized Form of Communication for Businesses and Individuals
- **Critical System** for any Organization
- Powerful Messaging Systems
  - Full-Blown Databases
  - Document Repositories
  - Contact / Calendar Managers

Expected Total Number of worldwide **E-Mail Accounts** by the End of 2016...
… over **4.3 Billion**

[Radicati Group]

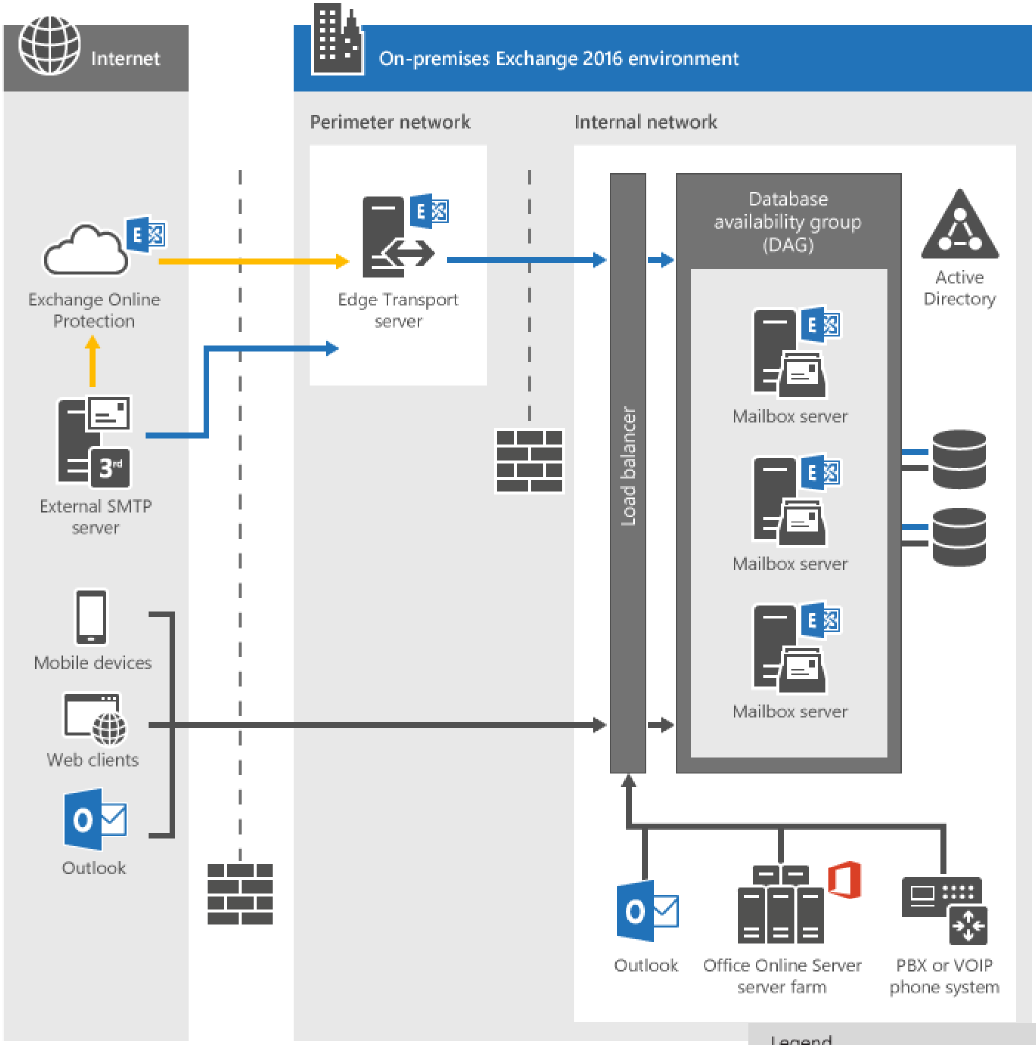
Employees on average spend **13 Hours** per week in their E-Mail Inbox

[McKinsey & Company]

Threats

- Information Stealing / Leakage
- Impersonation / Identity Theft
- Anonymity
- …

Exchange 2016 Architecture



- Edge Transport Servers
  - Handle external Mail Flow
  - Perimeter Network
  - Antispam and Mail Flow Rules
- Mailbox Servers
  - Transport Service
    - Route Mails
  - Client Access Service
    - Accept Client Connections
  - Unified Messaging Service
    - Voice Mail / Telephony
  - Mailbox Databases
    - Process / Render
    - Store

Source: https://technet.microsoft.com/de-ch/library/jj150491(v=exchg.160).aspx

Exchange Compliance Features

Message Tracking

Microsoft Exchange provides a Number of Messaging Policy and Compliances Features to retain Messages for:

- Litigations and Investigations
- Legal and Regulatory Requirements
- Business

Mailbox Auditing

Administrator Auditing

In-Place / Litigation Hold

Single Item Recovery

Transport Rules
Journaling / Archiving
Full Backup

Exchange Compliance Features

Message Tracking

- Record **E-Mail Traffic** within an Organization
- Learn about **Message Flow**
  - Sender
  - Recipient
  - Message Subject
  - Date / Time
- Feature of the **Transport Service**
  - Records even Message travelling on the same Mailbox Server

- Can also be used to
  - Troubleshoot Mail Flow
  - Analyze E-Mail Traffic Patterns

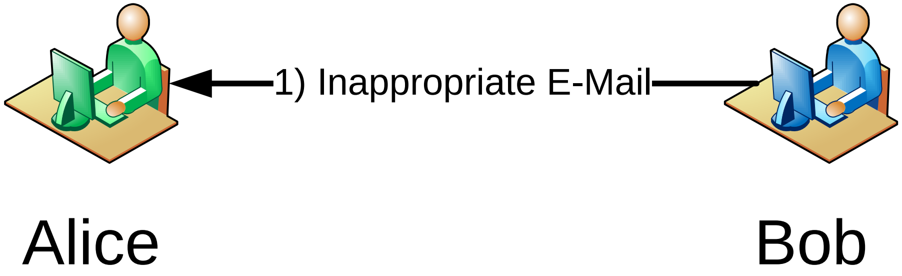
Enabled by default for 30 Days (all Mailboxes)

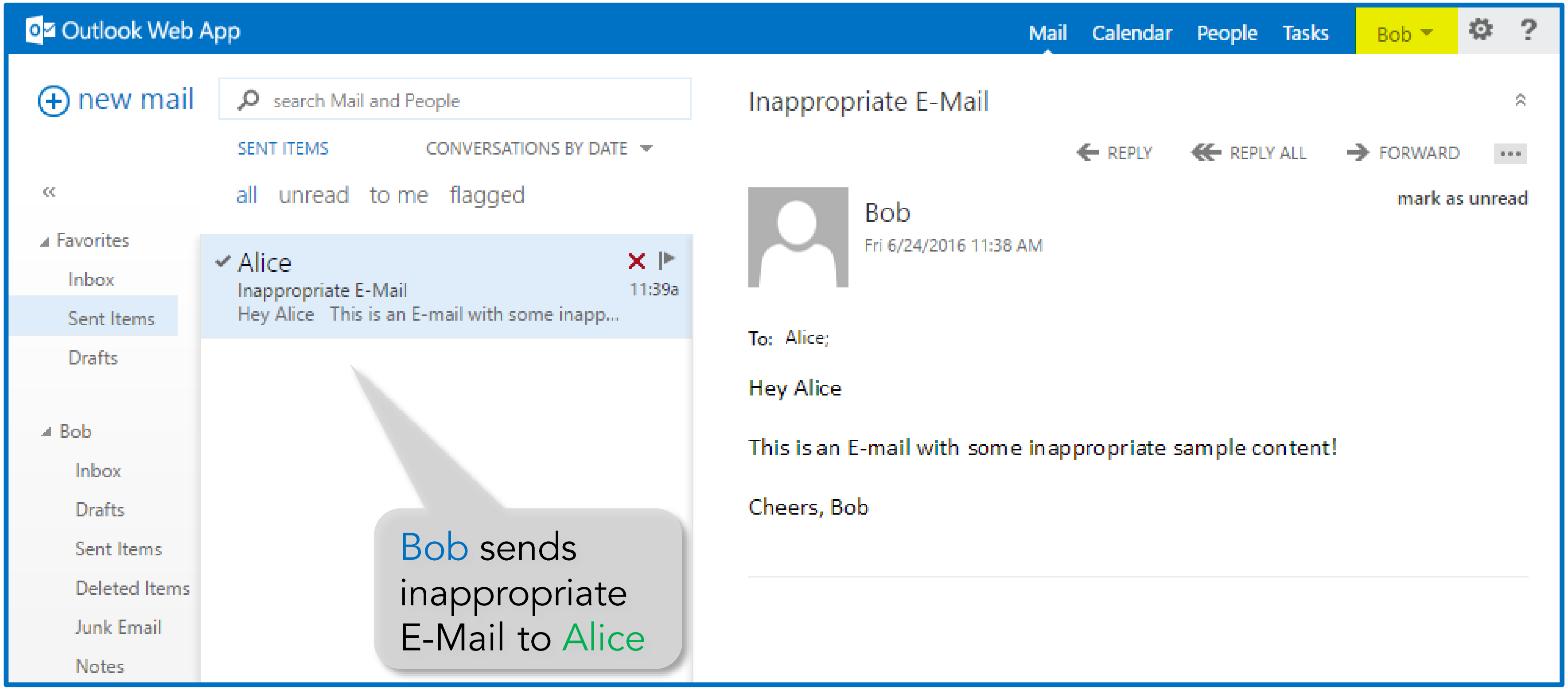
Exchange deletes older Logs to keep the specified Folder Maximum
→ Might keep less than 30 Days

```
[PS]> Get-TransportServer | FL *Tracking*

MessageTrackingLogEnabled                  : True
MessageTrackingLogMaxAge                   : 30.00:00:00
MessageTrackingLogMaxDirectorySize         : 1000 MB (1,048,576,000 bytes)
MessageTrackingLogMaxFileSize              : 10 MB (10,485,760 bytes)
MessageTrackingLogPath                     : C:\[…]\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled    : True
```

Scenario A – Tracking Message Flows

Malicious Activity





Alice
Inappropriate E-Mail 11:39a
Hey Alice This is an E-mail with some inapp...

Inappropriate E-Mail

Bob
Fri 6/24/2016 11:38 AM

To: Alice;

Hey Alice

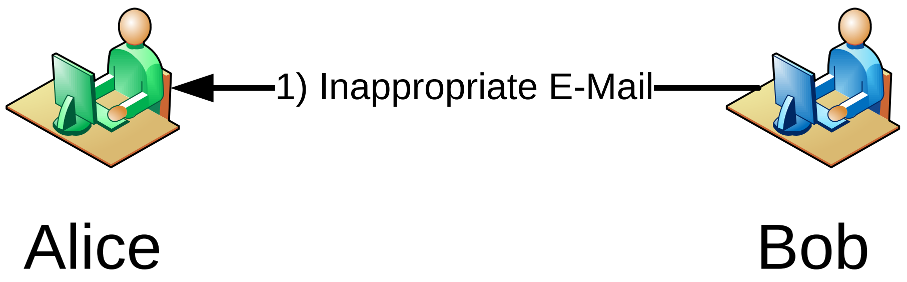
This is an E-mail with some inappropriate sample content!

Cheers, Bob

Bob sends inappropriate E-Mail to Alice

Scenario A – Tracking Message Flows

Detection – Message Tracking

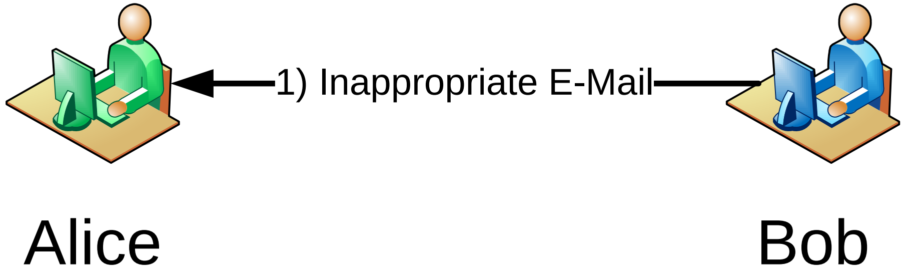


```
[PS]> Get-TransportServer
          | Get-MessageTrackingLog
          –Sender “bob@compass-security.com” –Recipients “alice@compass-security.com”
          | Select TimeStamp,EventId,Sender,Recipients,MessageSubject
          | Sort TimeStamp

Timestamp          : 24.06.2016 11:38:44
EventId            : RECEIVE
Sender             : bob@compass-security.com
Recipients         : {alice@compass-security.com}
MessageSubject     : Inappropriate E-Mail

[CUT BY COMPASS]
```

Exchange received E-Mail from Bob

Scenario A – Tracking Message Flows

Detection – Message Tracking



```
[PS]> Get-TransportServer
        | Get-MessageTrackingLog
        –Sender “bob@compass-security.com” –Recipients “alice@compass-security.com”
        | Select TimeStamp,EventId,Sender,Recipients,MessageSubject
        | Sort TimeStamp

[CUT BY COMPASS]

Timestamp          : 24.06.2016 11:39:10
EventId            : DELIVER
Sender             : bob@compass-security.com
Recipients         : {alice@compass-security.com}
MessageSubject     : Inappropriate E-Mail
```

Proof:

- E-Mail sent / received by Bob / Alice

Problem:

- Log does not contain E-Mail Body

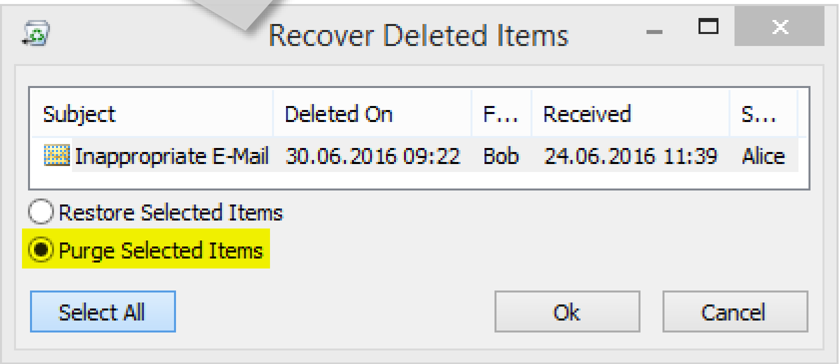
Exchange delivered E-Mail to Alice

Exchange Compliance Features

Single Item Recovery

- **Preserve** Mailbox Items
  - Preserve Items that Users purged
  - Administrator can still recover such purged Items
- *Recoverable Items / Purges*

Purge Items in Outlook/OWA using the *Recover Deleted Items* Feature



Recover Deleted Items

Subject	Deleted On	F...	Received	S...
Inappropriate E-Mail	30.06.2016 09:22	Bob	24.06.2016 11:39	Alice

○ Restore Selected Items

● Purge Selected Items

```
[PS]> Get-Mailbox Bob | FL SingleItemRecoveryEnabled, RetainDeletedItemsFor,
          RecoverableItemsQuota, RecoverableItemsWarningQuota

SingleItemRecoveryEnabled          : False
RetainDeletedItemsFor              : 14.00:00:00
RecoverableItemsQuota              : 30 GB (32,212,254,720 bytes)
RecoverableItemsWarningQuota       : 20 GB (21,474,836,480 bytes)
```

Disabled by default

Exchange Compliance Features

Litigation / In-Place Hold

- **Preserve** Mailbox Items
  - Deleted Items are not purged
  - Prevent automated Deletion (by Retention Policies)
  - Copy of original Item retained when modified
- Typically used during **Investigation**
  - Users do not notice they are on Hold
- Litigation Hold
  - Preserve all Items until Hold is removed
  - *Recoverable Items / Purges*
- In-Place Hold
  - Preserve Items based on Query Parameters and Hold Period
  - *Recoverable Items / DiscoveryHold*

In case neither of

- SingleItemRecovery
- Litigation Hold
- In-Place Hold

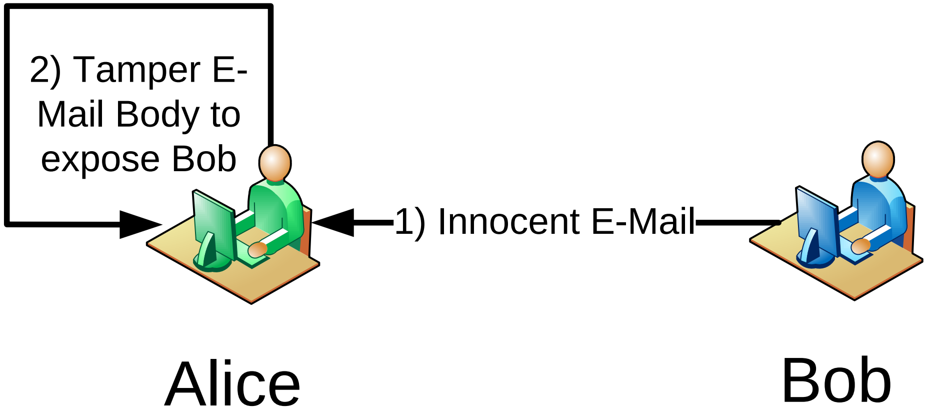
are enabled (all disabled by default), Users can permanently delete Items from their Mailbox.

Litigation / In-Place Hold are disabled by default

```
[PS]> Get-Mailbox Bob | FL *Hold*

LitigationHoldEnabled        : False
[CUT BY COMPASS]
LitigationHoldDate           :
LitigationHoldOwner          :
LitigationHoldDuration       : Unlimited
[CUT BY COMPASS]
InPlaceHolds                 : {}
```

Scenario B – Investigating Modifications

Malicious Activity



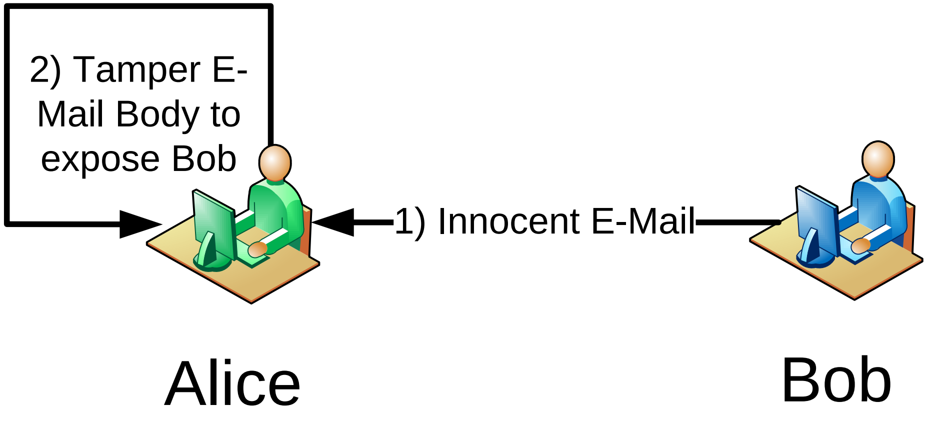
Assumption:

- Litigation Hold or
- In-Place Hold (with appropriate Parameters)

was enabled on Alice's Mailbox before E-Mail was received.

Scenario B – Investigating Modifications

Detection – In-Place / Litigation Hold

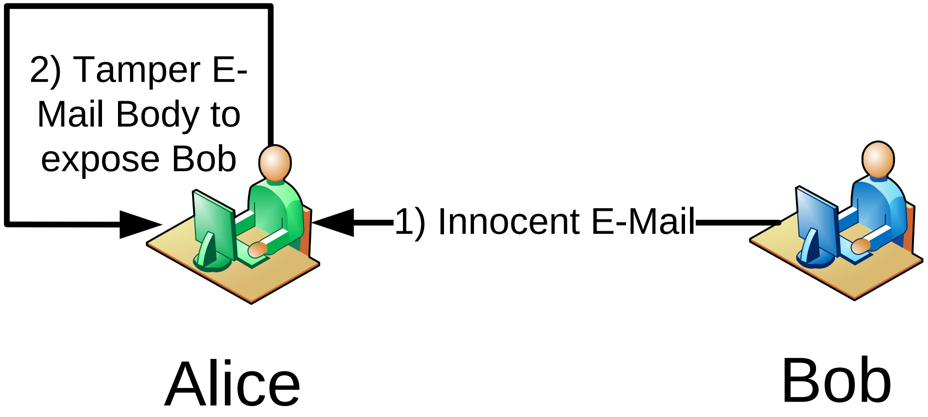


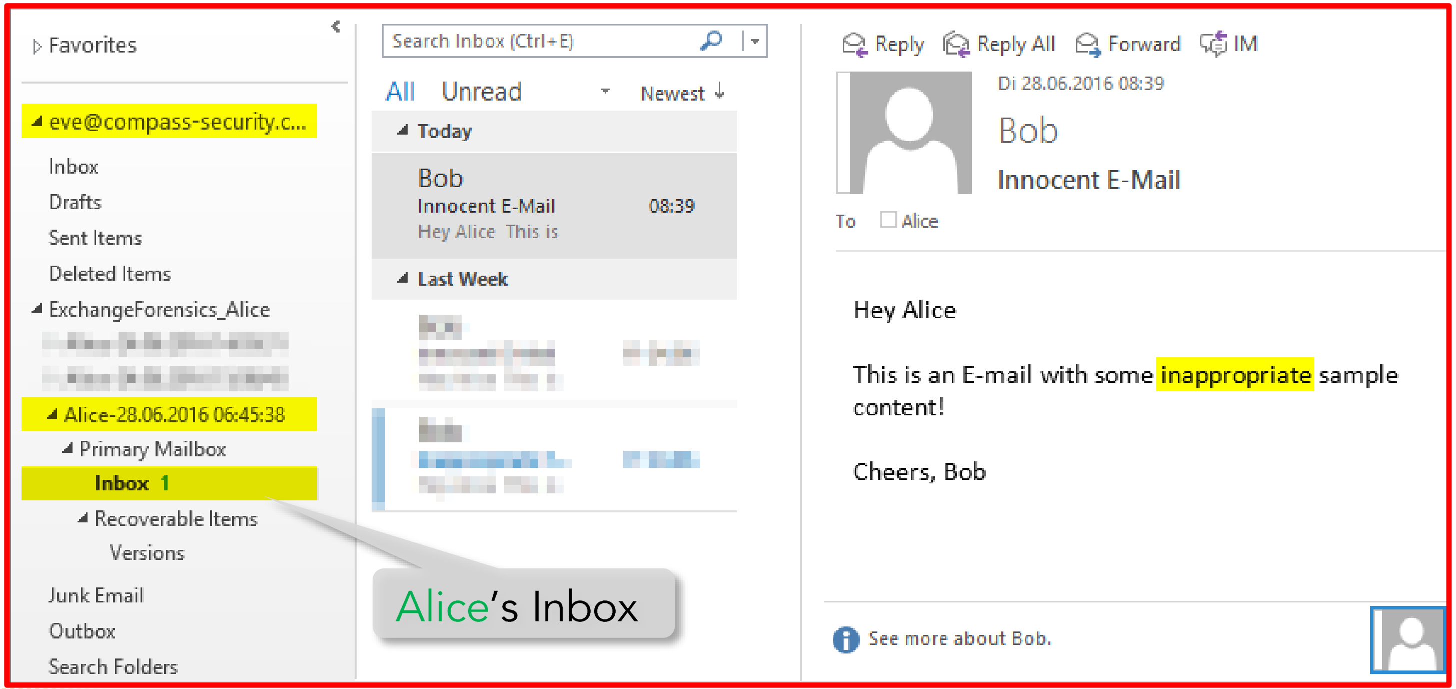
```
[PS]> Search-Mailbox Alice –TargetMailbox Eve
            –TargetFolder "ExchangeForensics_Alice" –LogLevel Full

[CUT BY COMPASS]

Identity          : compass-security.com/Users/Alice
TargetMailbox     : compass-security.com/Users/Eve
Success           : True
TargetFolder      : \ExchangeForensics_Alice\Alice-28.06.2016 06:45:38
ResultItemsCount  : 4
ResultItemsSize   : 120.6 KB (123,475 bytes)
```

Search Alice's Mailbox and make Results available to Eve

Scenario B – Investigating Modifications

Detection – In-Place / Litigation Hold





Bob
Innocent E-Mail 08:39
Hey Alice This is

Di 28.06.2016 08:39
Bob
Innocent E-Mail
To □ Alice

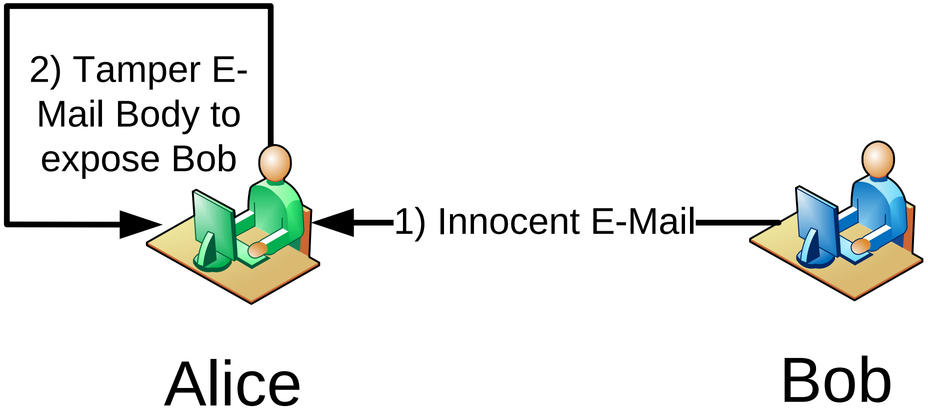
Hey Alice

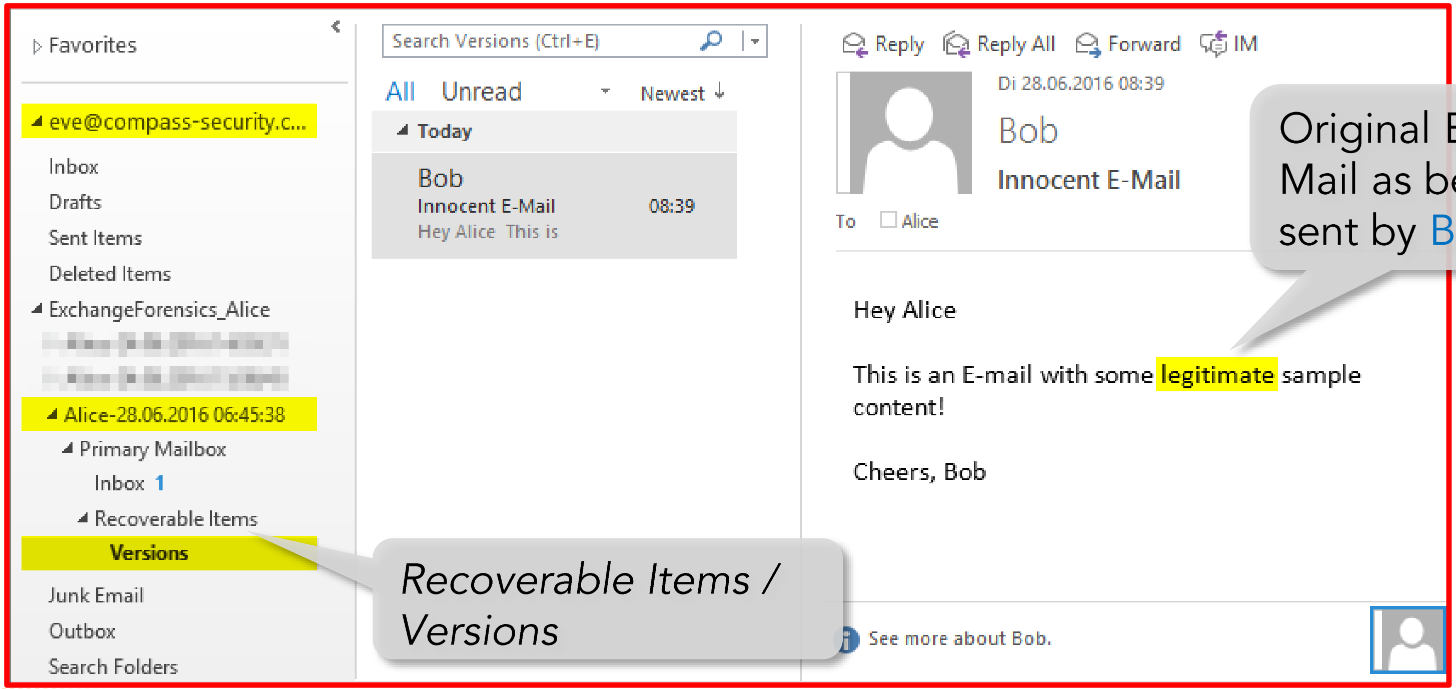
This is an E-mail with some inappropriate sample content!

Cheers, Bob

Scenario B – Investigating Modifications

Detection – In-Place / Litigation Hold





eve@compass-security.c...
Inbox
Drafts
Sent Items
Deleted Items
ExchangeForensics_Alice
[redacted]
Alice-28.06.2016 06:45:38
Primary Mailbox
Inbox 1
Recoverable Items
Versions
Junk Email
Outbox
Search Folders

Today
Bob
Innocent E-Mail 08:39
Hey Alice This is

Di 28.06.2016 08:39
Bob
Innocent E-Mail
To □ Alice

Hey Alice

This is an E-mail with some legitimate sample content!

Cheers, Bob

See more about Bob.

Original E-Mail as being sent by Bob

Recoverable Items / Versions

Exchange Compliance Features

Mailbox Auditing

- Track **who** accesses a Mailbox
  - Admin
  - Delegate
  - Owner
- Track **what** Actions are taken
  - Create
  - Copy
  - Send
  - Delete
  - Etc.
- *Recoverable Items / Audits*

```
[PS]> Get-Mailbox Alice | FL *Audit*

AuditEnabled       : False
AuditLogAgeLimit   : 90.00:00:00
AuditAdmin         : {Update, Move, SendAs, […]}
AuditDelegate      : {Update, SendAs, […]}
AuditOwner         : {}
```

Disabled by default

Exchange Compliance Features

Mailbox Auditing

- Track **who** accesses a Mailbox
  - Admin
  - Delegate
  - Owner
- Track **what** Actions are taken
  - Create
  - Copy
  - Send
  - Delete
  - Etc.
- *Recoverable Items / Audits*

Problem:

- When enabled, requires more Space on the corresponding Mailbox (similar for other Compliance Features)

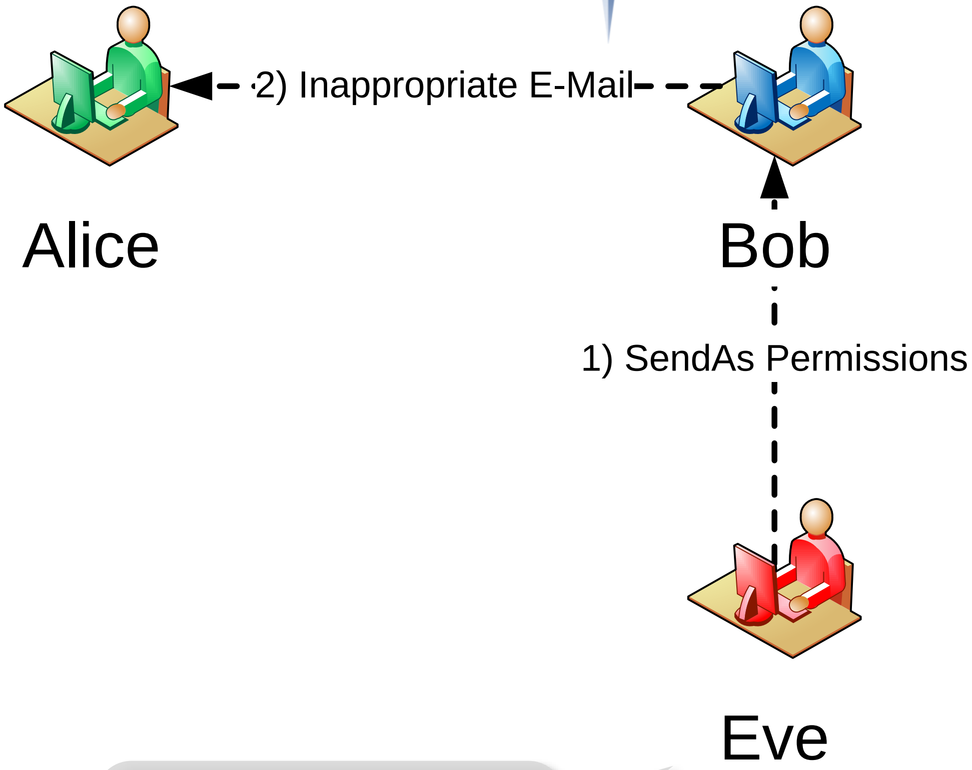
Solution – Auditing Policy:

- Record Key Actions only (Send, Delete, …)
- No noticeable Impact in Terms of Storage and Performance

→ Resolves many Investigations

Scenario C – Investigating SendAs

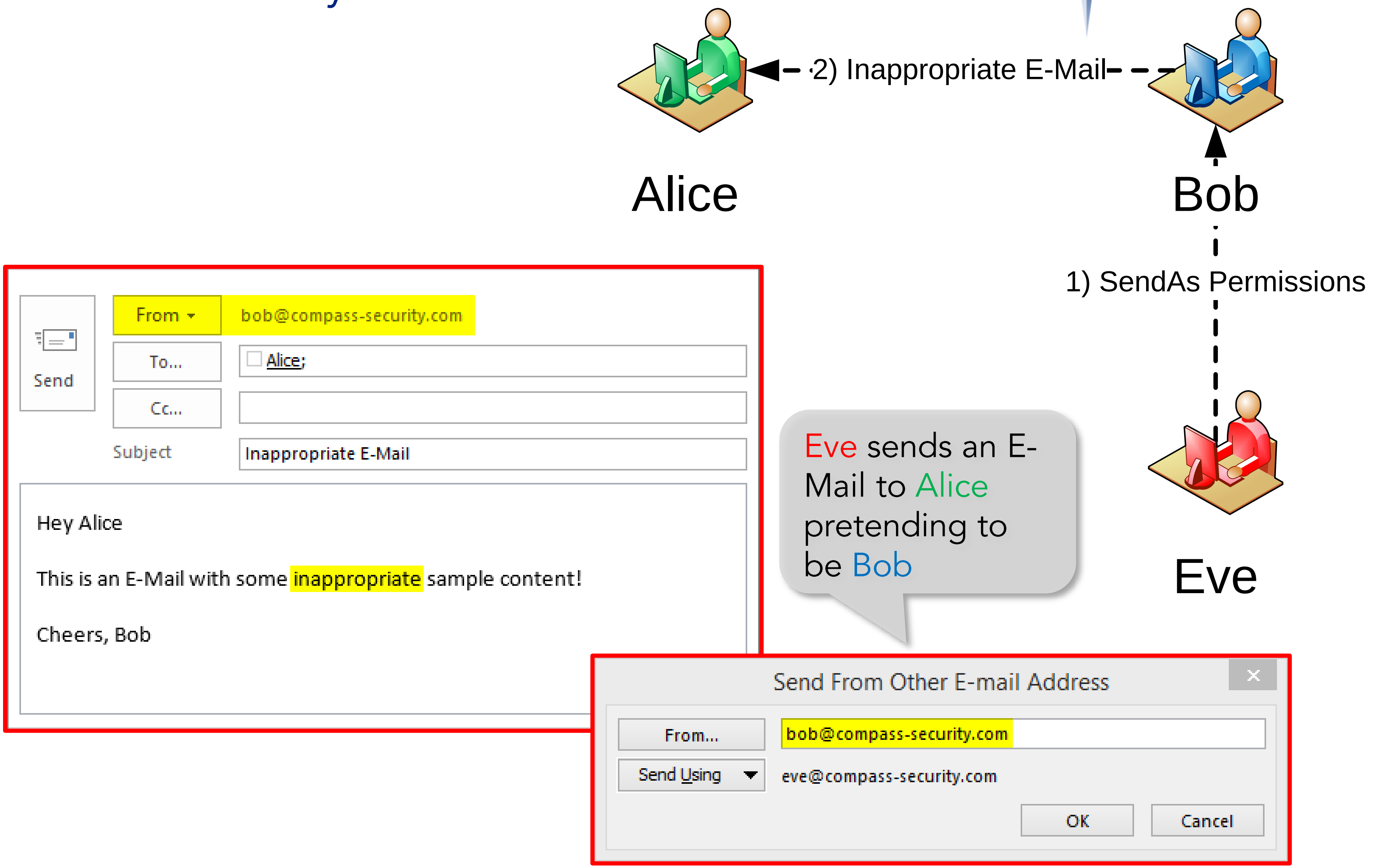
Malicious Activity



Eve managed to gain *SendAs* Permission on Bob's Mailbox

Scenario C – Investigating SendAs

Malicious Activity



Eve sends an E-Mail to Alice pretending to be Bob

From: bob@compass-security.com

To: Alice;

Subject: Inappropriate E-Mail

Hey Alice

This is an E-Mail with some inappropriate sample content!

Cheers, Bob

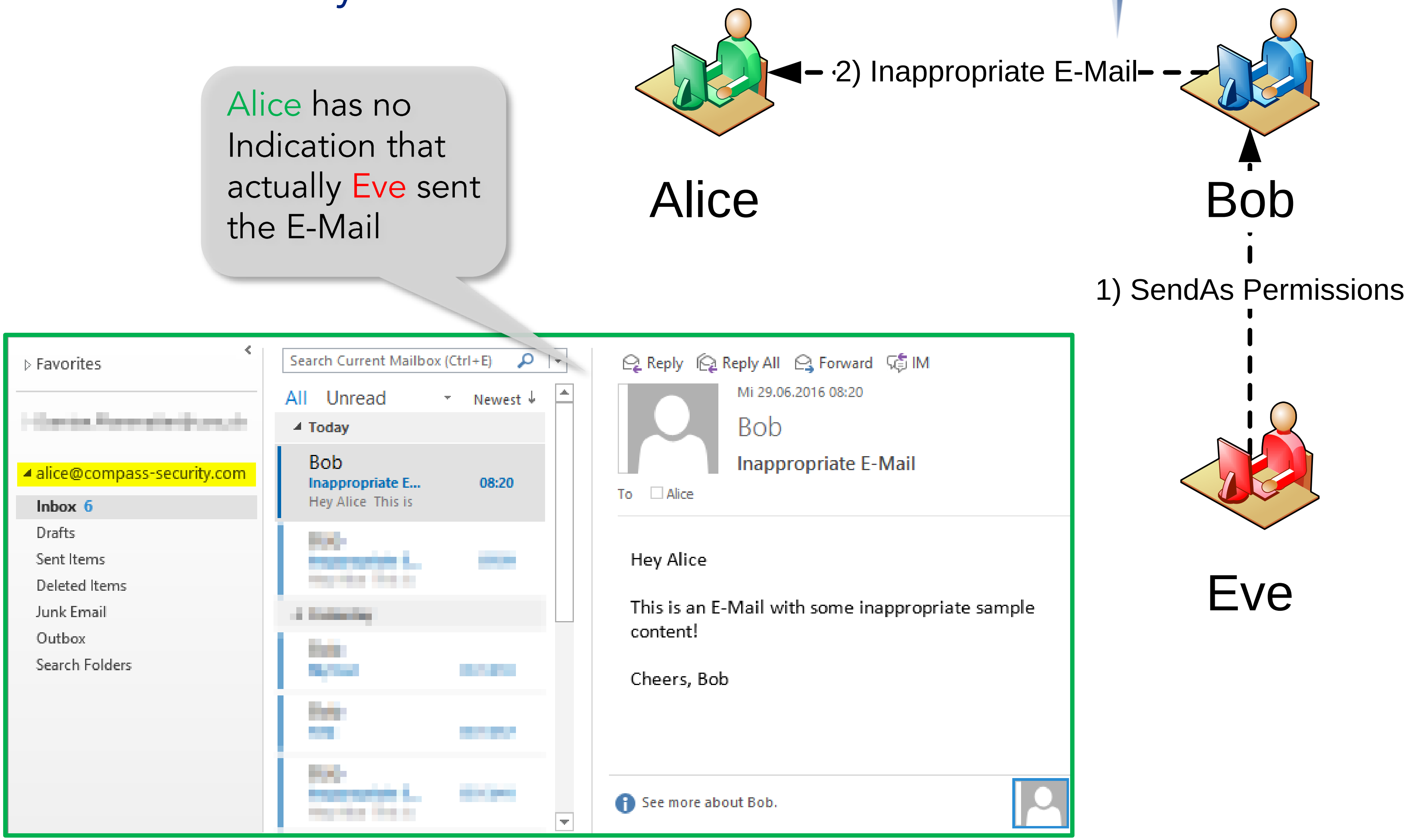
Send From Other E-mail Address

From... bob@compass-security.com

Send Using: eve@compass-security.com

Scenario C – Investigating SendAs

Malicious Activity



Alice has no Indication that actually Eve sent the E-Mail

Bob
Inappropriate E... 08:20
Hey Alice This is

Mi 29.06.2016 08:20

Bob

Inappropriate E-Mail

To □ Alice

Hey Alice

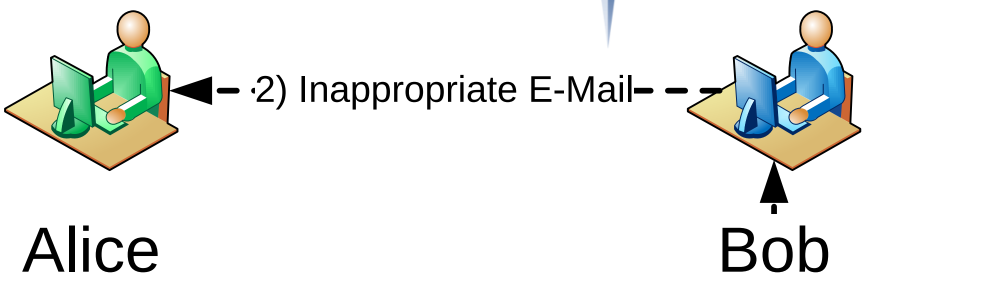
This is an E-Mail with some inappropriate sample content!

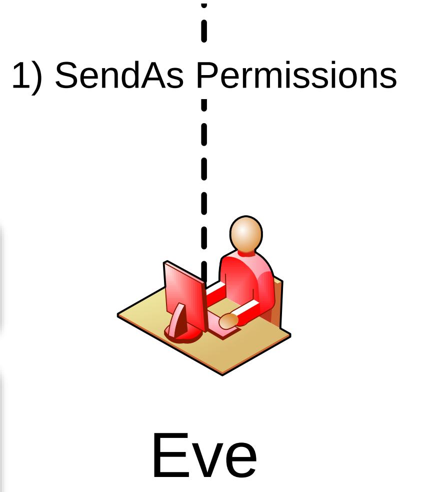
Cheers, Bob

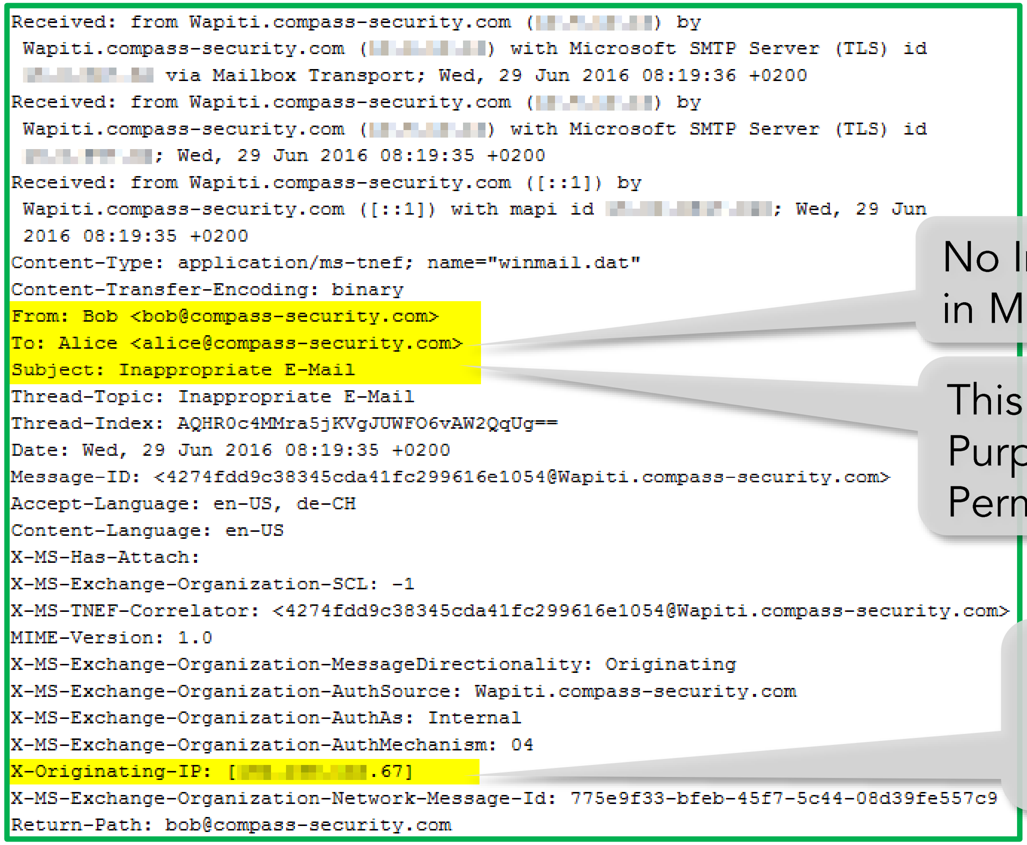
See more about Bob.

Scenario C – Investigating SendAs

Malicious Activity







```
Received: from Wapiti.compass-security.com ([redacted]) by
 Wapiti.compass-security.com ([redacted]) with Microsoft SMTP Server (TLS) id
 [redacted] via Mailbox Transport; Wed, 29 Jun 2016 08:19:36 +0200
Received: from Wapiti.compass-security.com ([redacted]) by
 Wapiti.compass-security.com ([redacted]) with Microsoft SMTP Server (TLS) id
 [redacted]; Wed, 29 Jun 2016 08:19:35 +0200
Received: from Wapiti.compass-security.com ([::1]) by
 Wapiti.compass-security.com ([::1]) with mapi id [redacted]; Wed, 29 Jun
 2016 08:19:35 +0200
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Bob <bob@compass-security.com>
To: Alice <alice@compass-security.com>
Subject: Inappropriate E-Mail
Thread-Topic: Inappropriate E-Mail
Thread-Index: AQHR0c4MMra5jKVgJUWFO6vAW2QqUg==
Date: Wed, 29 Jun 2016 08:19:35 +0200
Message-ID: <4274fdd9c38345cda41fc299616e1054@Wapiti.compass-security.com>
Accept-Language: en-US, de-CH
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <4274fdd9c38345cda41fc299616e1054@Wapiti.compass-security.com>
MIME-Version: 1.0
X-MS-Exchange-Organization-MessageDirectionality: Originating
X-MS-Exchange-Organization-AuthSource: Wapiti.compass-security.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [[redacted].67]
X-MS-Exchange-Organization-Network-Message-Id: 775e9f33-bfeb-45f7-5c44-08d39fe557c9
Return-Path: bob@compass-security.com
```

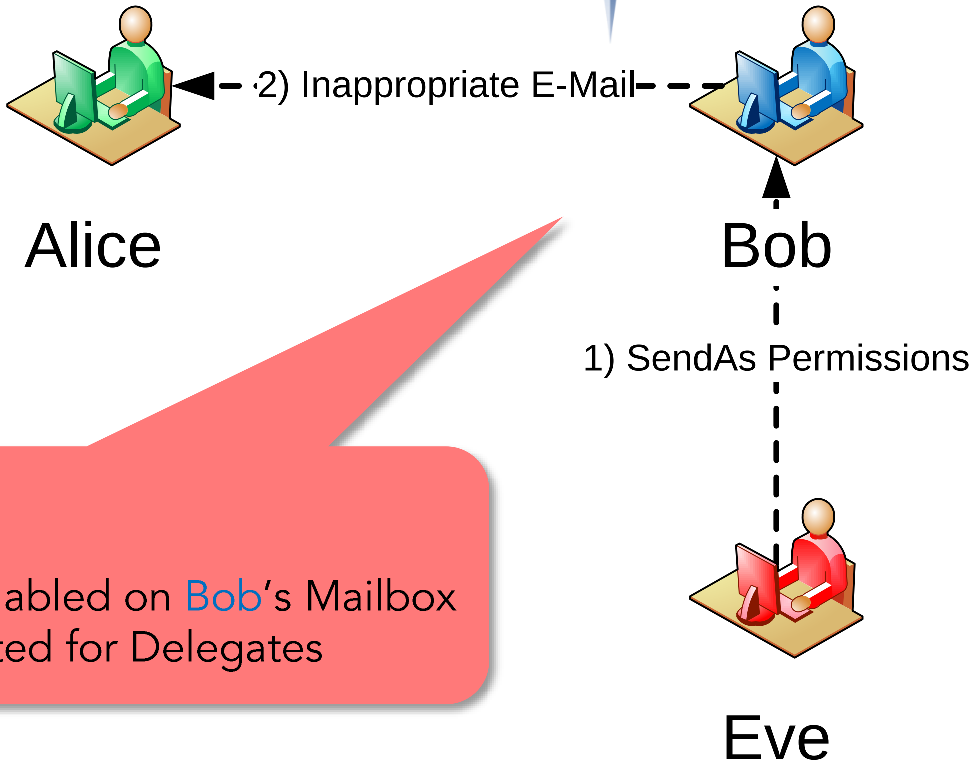
No Indication even in Message Headers

This is the whole Purpose of *SendAs* Permissions

IP Reference could potentially be used to show that the E-Mail was sent from Eve's Machine

Scenario C – Investigating SendAs

Detection – Mailbox Auditing



Assumption:

- Mailbox Auditing enabled on Bob's Mailbox
- *SendAs* Action audited for Delegates

Scenario C – Investigating SendAs

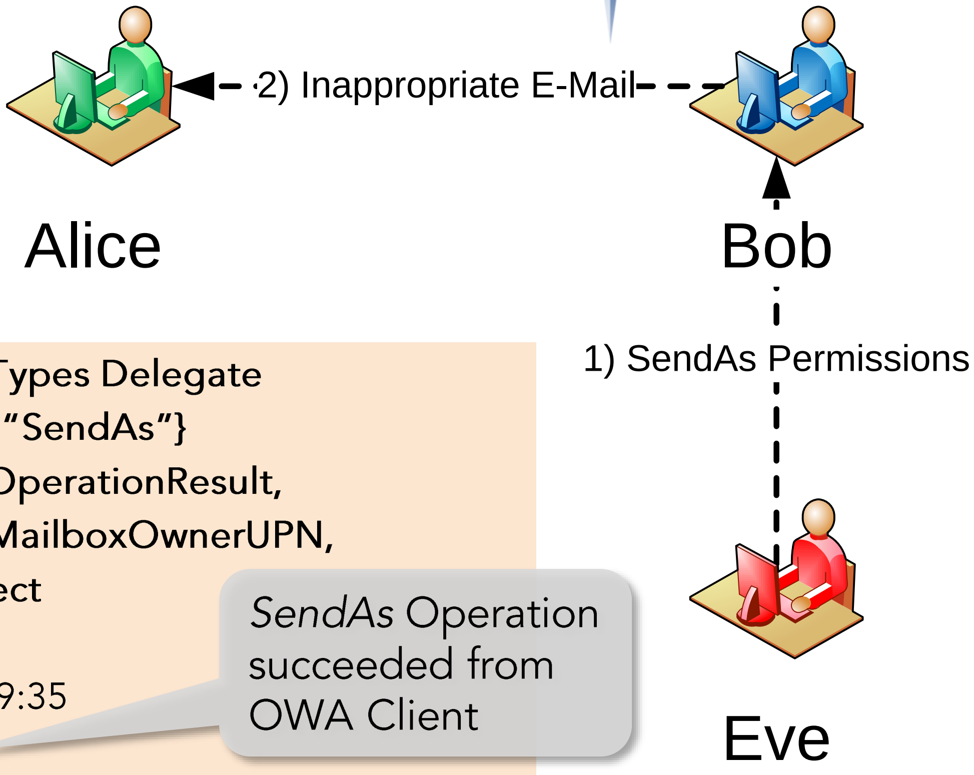
Detection – Mailbox Auditing

Return Mailbox Accesses by Users other than the Owner (*Delegates*)

```
[PS]> Search-MailboxAuditLog Bob –LogonTypes Delegate
          –ShowDetails | ?{$_.Operation –eq “SendAs”}
          | Select LastAccessed, Operation, OperationResult,
          ClientInfoString, ClientIPAddress, MailboxOwnerUPN,
          LogonUserDisplayName, ItemSubject

LastAccessed              : 29.06.2016 08:19:35
Operation                 : SendAs
OperationResult           : Succeeded
ClientInfoString          : Client=OWA; Mozilla/[CUT BY COMPASS]
ClientIPAddress           : [CUT BY COMPASS].67
MailboxOwnerUPN           : bob@compass-security.com
LogonUserDisplayName      : Eve
ItemSubject               : Inappropriate E-Mail
```

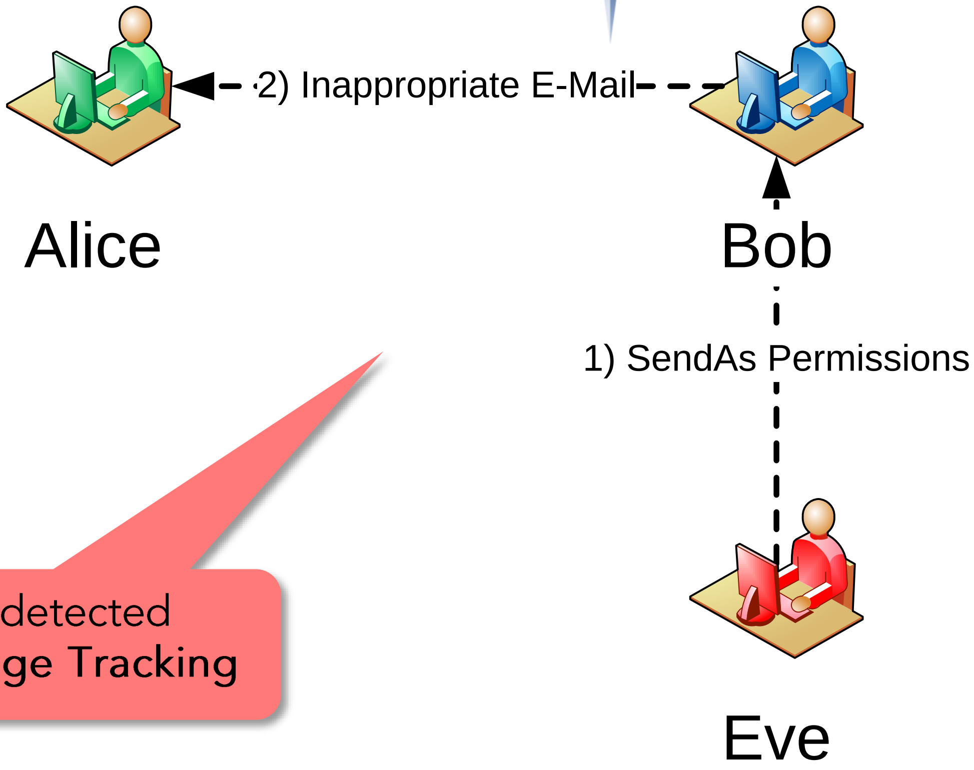
SendAs Operation succeeded from OWA Client

Eve sent an E-Mail with Subject “Inappropriate E-Mail” from Bob’s Mailbox



Scenario C – Investigating SendAs

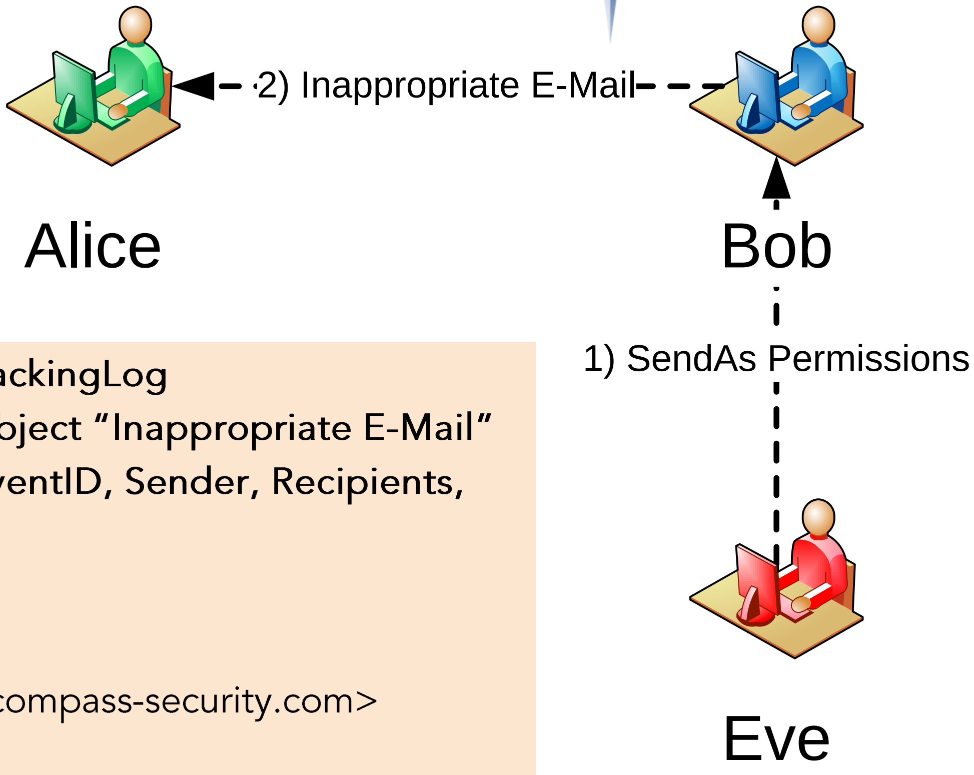
Detection – Message Tracking



Can also be detected using **Message Tracking**

Scenario C – Investigating SendAs

Detection – Message Tracking

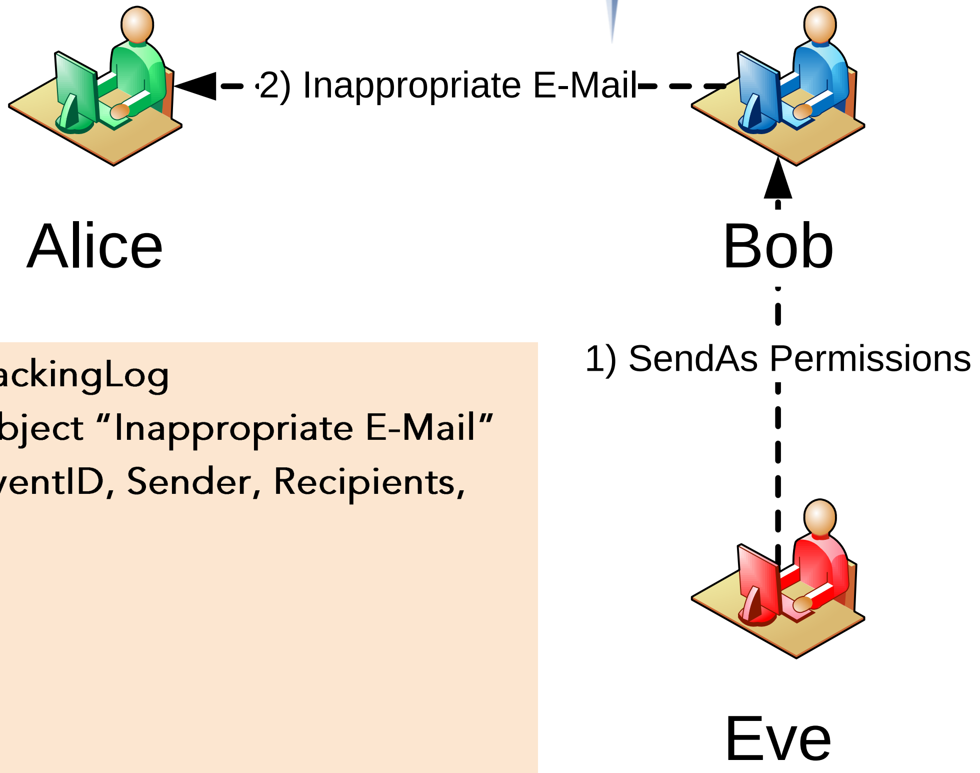


```
[PS]> Get-TransportServer | Get-MessageTrackingLog
        –ResultSize Unlimited –MessageSubject “Inappropriate E-Mail”
        | Select TimeStamp, MessageID, EventID, Sender, Recipients,
        MessageSubject | Sort TimeStamp

Timestamp        : 29.06.2016 08:19:35
MessageId        : <424274fdd […]@Wapiti.compass-security.com>
EventId          : RECEIVE
Sender           : eve@compass-security.com
Recipients       : {alice@compass-security.com}
MessageSubject   : Inappropriate E-Mail

[CUT BY COMPASS]
```

Exchange received the E-Mail from Eve’s Mailbox

Scenario C – Investigating SendAs

Detection – Message Tracking

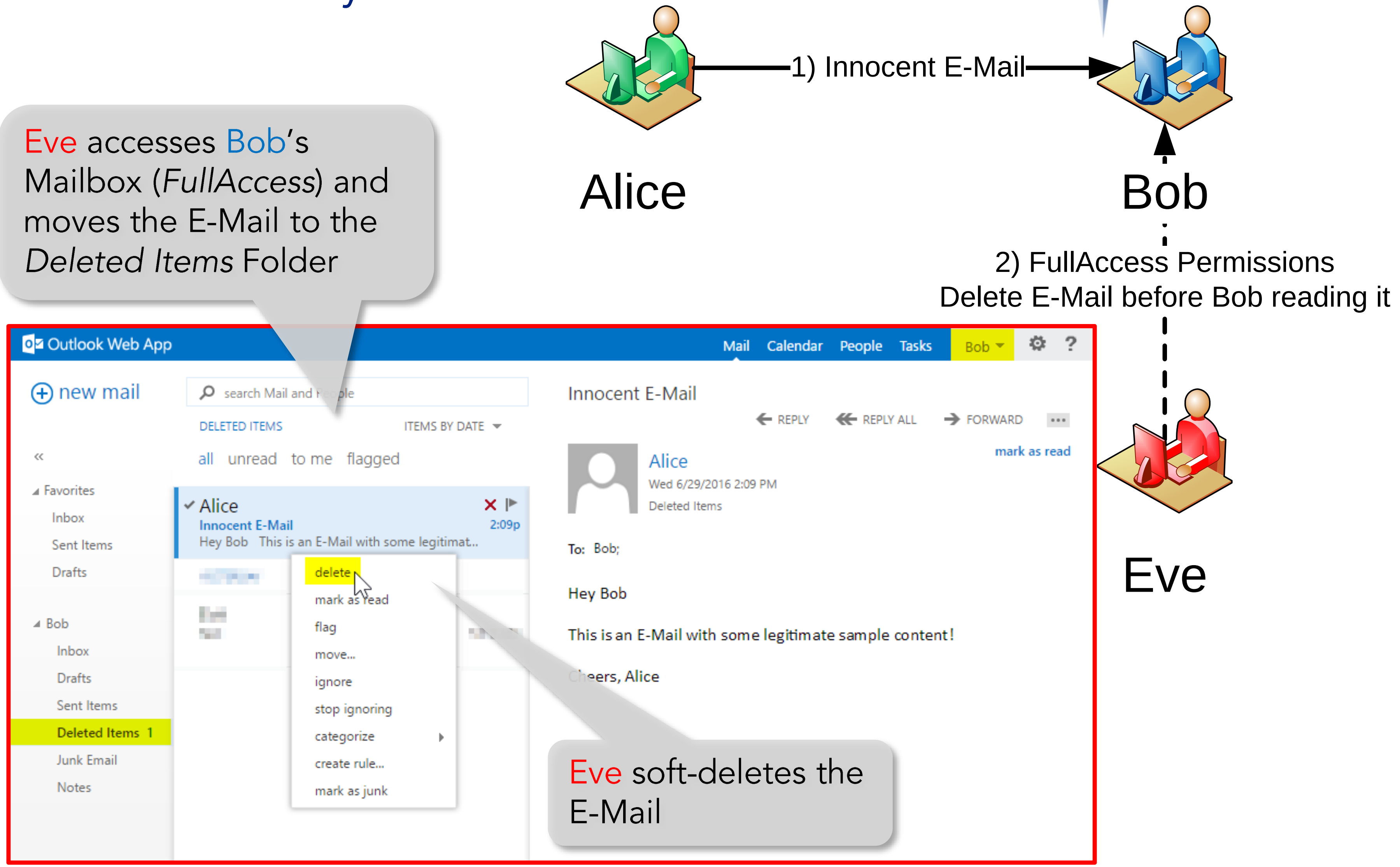


```
[PS]> Get-TransportServer | Get-MessageTrackingLog
        –ResultSize Unlimited –MessageSubject “Inappropriate E-Mail”
        | Select TimeStamp, MessageID, EventID, Sender, Recipients,
        MessageSubject | Sort TimeStamp

[CUT BY COMPASS]

Timestamp       : 29.06.2016 08:19:36
MessageId       : <424274fdd […]@Wapiti.compass-security.com>
EventId         : DELIVER
Sender          : bob@compass-security.com
Recipients      : {alice@compass-security.com}
MessageSubject  : Inappropriate E-Mail
```

Exchange modified Sender to Bob (*SendAs*) and delivered E-Mail to Alice

Scenario D – Investigating Deletes

Malicious Activity



Eve accesses Bob’s Mailbox (*FullAccess*) and moves the E-Mail to the *Deleted Items* Folder

Innocent E-Mail

Alice
Wed 6/29/2016 2:09 PM
Deleted Items

To: Bob;

Hey Bob

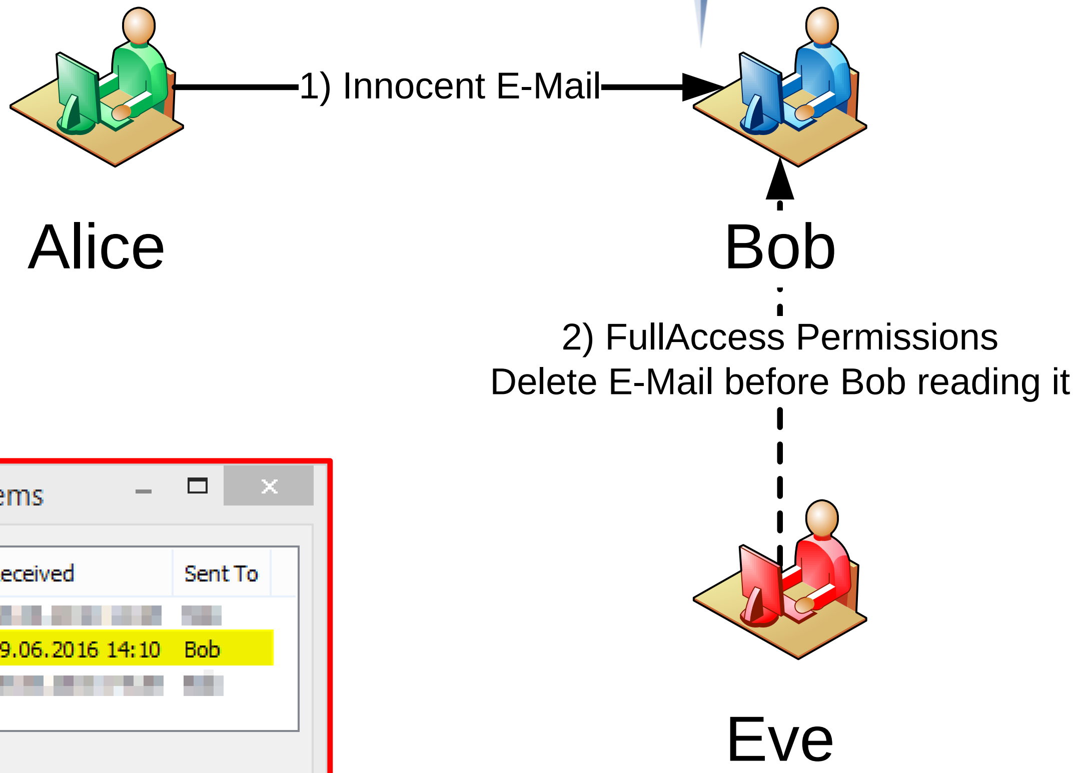
This is an E-Mail with some legitimate sample content!

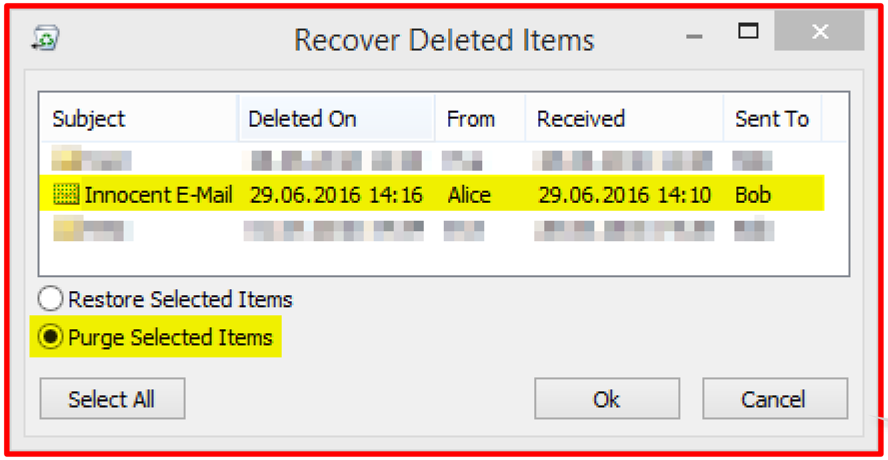
Cheers, Alice

Eve soft-deletes the E-Mail

Scenario D – Investigating Deletes

Malicious Activity


1) Innocent E-Mail
Alice
Bob
2) FullAccess Permissions
Delete E-Mail before Bob reading it
Eve



Subject	Deleted On	From	Received	Sent To
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Innocent E-Mail	29.06.2016 14:16	Alice	29.06.2016 14:10	Bob
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

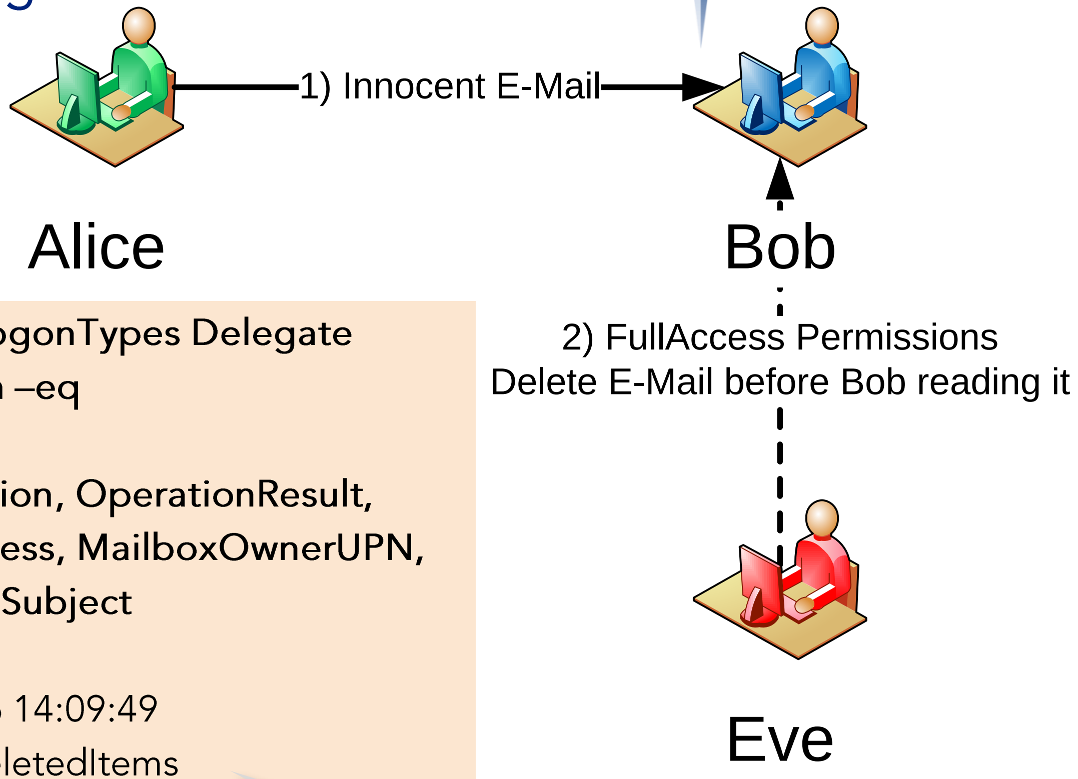
○ Restore Selected Items
● Purge Selected Items

Eve hard-deletes the E-Mail using the *Recover Deleted Items* Feature

Scenario D – Investigating Deletes

Detection – Mailbox Auditing

Search Accesses to Bob's Mailbox by other Users (*Delegates*)



1) Innocent E-Mail

Alice

Bob

2) FullAccess Permissions
Delete E-Mail before Bob reading it

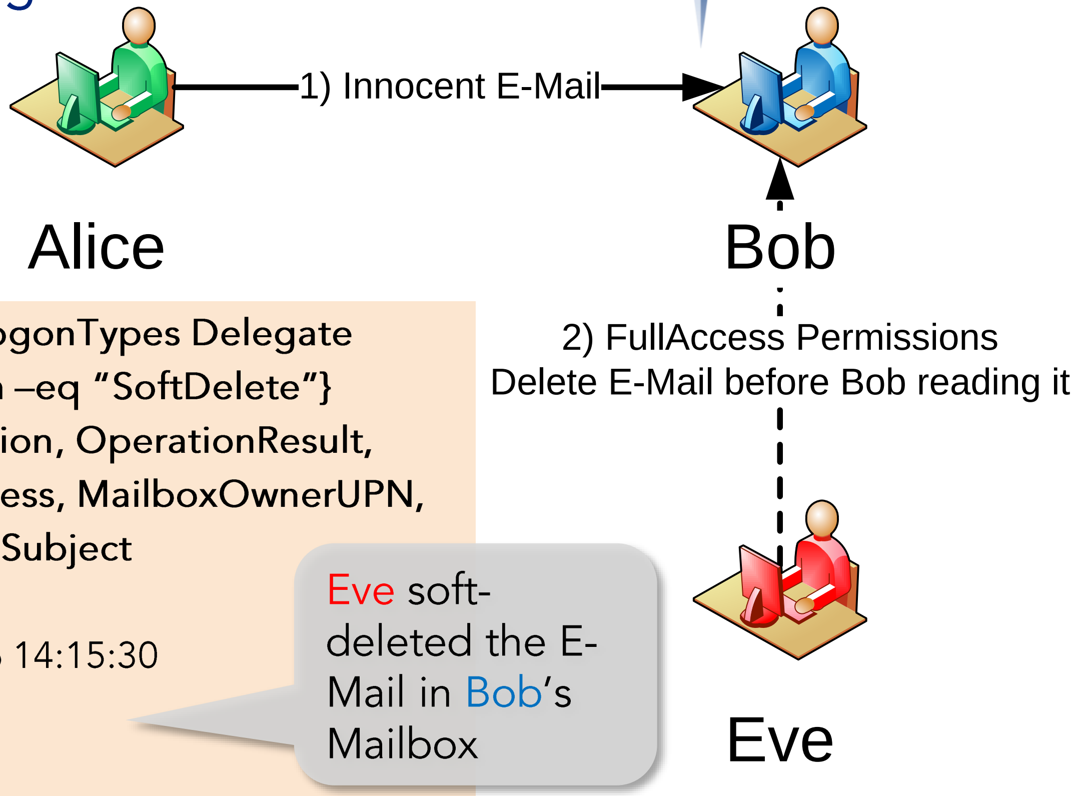
Eve

```
[PS]> Search-MailboxAuditLog Bob –LogonTypes Delegate
            –ShowDetails | ?{$_.Operation –eq
            "MoveToDeletedItems"}
            | Select LastAccessed, Operation, OperationResult,
            ClientInfoString, ClientIPAddress, MailboxOwnerUPN,
            LogonUserDisplayName, ItemSubject

LastAccessed                  : 29.06.2016 14:09:49
Operation                     : MoveToDeletedItems
OperationResult               : Succeeded
ClientInfoString              : Client=OWA;[CUT BY COMPASS]
ClientIPAddress               : [CUT BY COMPASS].67
MailboxOwnerUPN               : bob@compass-security.com
LogonUserDisplayName          : Eve
ItemSubject                   : Innocent E-Mail
```

Eve moved the E-Mail in Bob's Mailbox to the *Deleted Items* Folder

Scenario D – Investigating Deletes

Detection – Mailbox Auditing

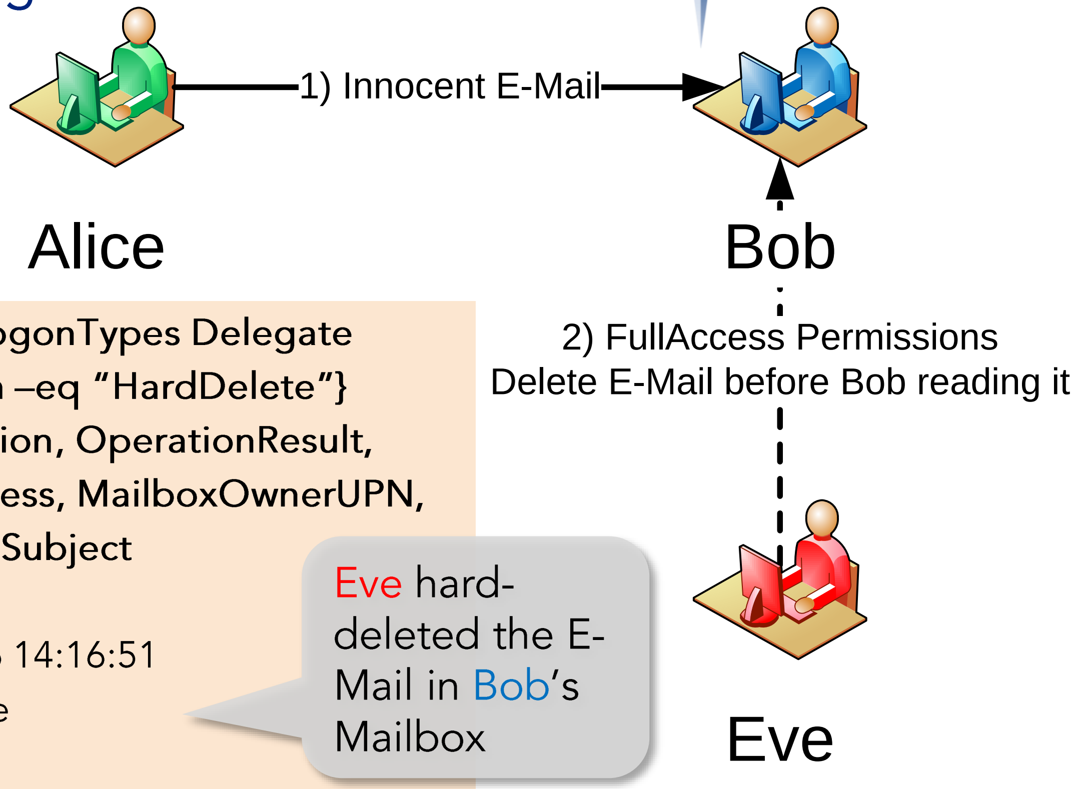

1) Innocent E-Mail
Alice
Bob
2) FullAccess Permissions
Delete E-Mail before Bob reading it
Eve

```
[PS]> Search-MailboxAuditLog Bob –LogonTypes Delegate
            –ShowDetails | ?{$_.Operation –eq “SoftDelete”}
            | Select LastAccessed, Operation, OperationResult,
            ClientInfoString, ClientIPAddress, MailboxOwnerUPN,
            LogonUserDisplayName, ItemSubject

LastAccessed             : 29.06.2016 14:15:30
Operation                : SoftDelete
OperationResult          : Succeeded
ClientInfoString         : Client=OWA;[CUT BY COMPASS]
ClientIPAddress          : [CUT BY COMPASS].67
MailboxOwnerUPN          : bob@compass-security.com
LogonUserDisplayName     : Eve
ItemSubject              : Innocent E-Mail
```

Eve soft-deleted the E-Mail in Bob’s Mailbox

Scenario D – Investigating Deletes

Detection – Mailbox Auditing


1) Innocent E-Mail
Alice
Bob
2) FullAccess Permissions
Delete E-Mail before Bob reading it
Eve

```
[PS]> Search-MailboxAuditLog Bob –LogonTypes Delegate
            –ShowDetails | ?{$_.Operation –eq “HardDelete”}
            | Select LastAccessed, Operation, OperationResult,
            ClientInfoString, ClientIPAddress, MailboxOwnerUPN,
            LogonUserDisplayName, ItemSubject

LastAccessed            : 29.06.2016 14:16:51
Operation               : HardDelete
OperationResult         : Succeeded
ClientInfoString        : Client=OWA;[CUT BY COMPASS]
ClientIPAddress         : [CUT BY COMPASS].67
MailboxOwnerUPN         : bob@compass-security.com
LogonUserDisplayName    : Eve
ItemSubject             : Innocent E-Mail
```

Eve hard-deleted the E-Mail in Bob’s Mailbox

Exchange Compliance Features

Administrator Auditing

- Log Changes made by **Administrators** to Exchange
  - Trace **who** changed **what** and **when**
  - Enabled by default (90 days)
- Changes to Administrator Auditing **Configuration** are always logged
  - Even when Administrator Auditing is disabled
- Stored in a hidden dedicated **Arbitration Mailbox**
  - Cannot be opened in Outlook or OWA

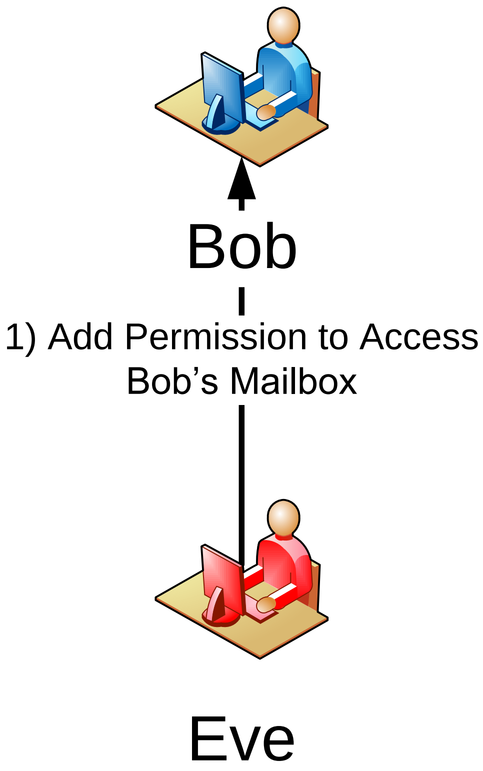
```
[PS]> Get-AdminAuditLogConfig | FL *Audit*

AdminAuditLogEnabled        : True
AdminAuditLogCmdlets        : {*}
AdminAuditLogParameters     : {*}
AdminAuditLogExcludeCmdlets: {}
AdminAuditLogAgeLimit       : 90.00:00:00
```

Default Settings

Scenario E – Step 1

Tracking Mailbox Permission Assignments

Malicious Activity



Detection – Administrator Auditing

```
[PS]> Search-AdminAuditLog
          –Cmdlets Add-MailboxPermission

[CUT BY COMPASS]

ObjectModified          : ... Bob ...
CmdletName              : Add-MailboxPermission
CmdletParameters        : {Identity, User, AccessRights}
ModifiedProperties      : {}
Caller                  : ... Eve ...
Succeeded               : True
Error                   : None
RunDate                 : 17/06/2016 10:00:00

[CUT BY COMPASS]
```

Identity of Mailbox getting Permissions added (Bob)

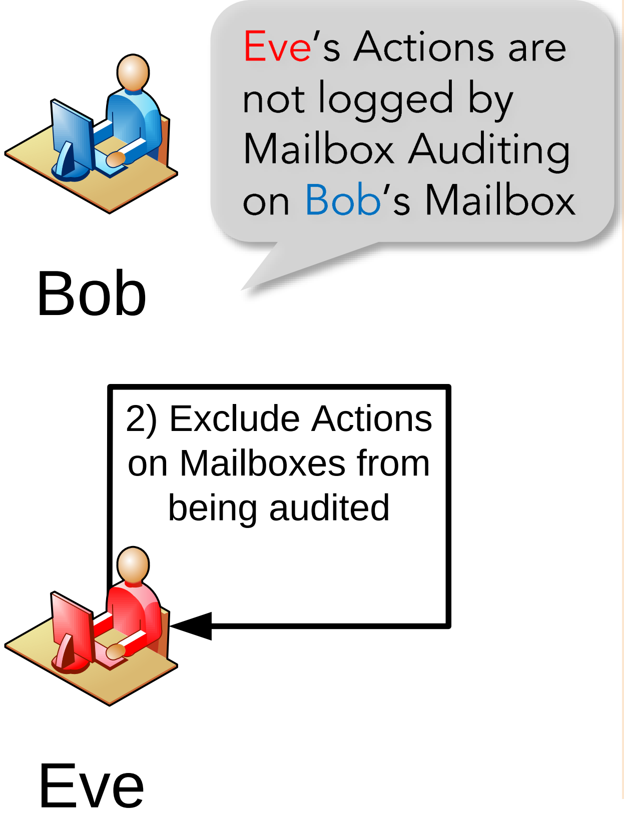
User that the Permissions are granted to (Eve)

Granted Permissions (e.g. FullAccess)

Scenario E – Step 2

Tracking Audit Bypass Changes

Malicious Activity



Eve's Actions are not logged by Mailbox Auditing on Bob's Mailbox

Bob

2) Exclude Actions on Mailboxes from being audited

Eve

Detection – Administrator Auditing

```
[PS]> Search-AdminAuditLog
            –Cmdlets Set-MailboxAuditBypassAssociation

[CUT BY COMPASS]

ObjectModified                : ... Eve ...
CmdletName                    : Set-MailboxAuditBypassAssociation
CmdletParameters              : {AuditBypassEnabled, Identity}
ModifiedProperties            : {AuditBypassEnabled}
Caller                        : ... Eve ...
Succeeded                     : True
Error                         : None
RunDate                       : 17/06/2016 10:10:00

[CUT BY COMPASS]
```

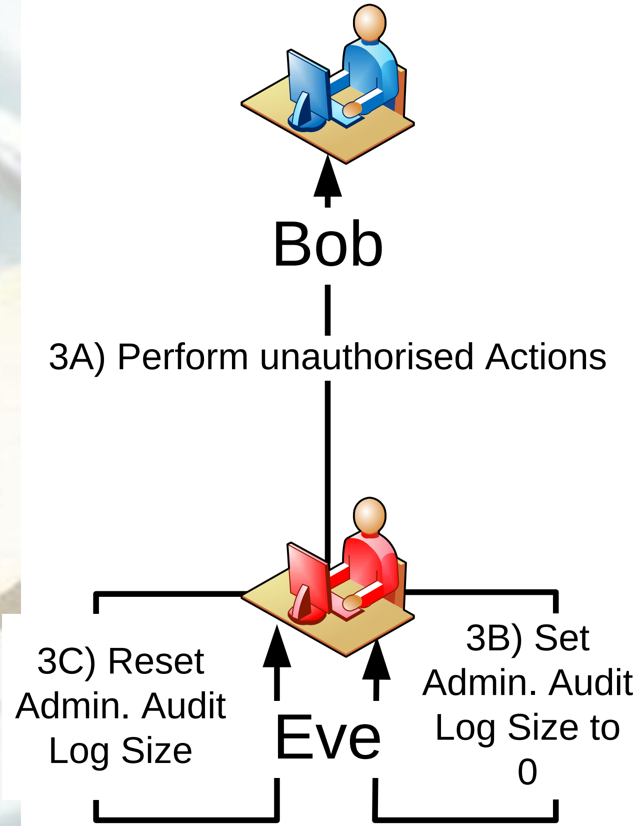
Enable / Disable Audit Bypass

User Account to be bypassed from Mailbox Audit Logging (Eve)

Scenario E – Step 3

Tracking Administrator Audit Log Clearance

Malicious Activity


Bob
3A) Perform unauthorised Actions
3C) Reset Admin. Audit Log Size
Eve
3B) Set Admin. Audit Log Size to 0

Mailbox Auditing on Bob’s Mailbox do not log Eve’s Actions

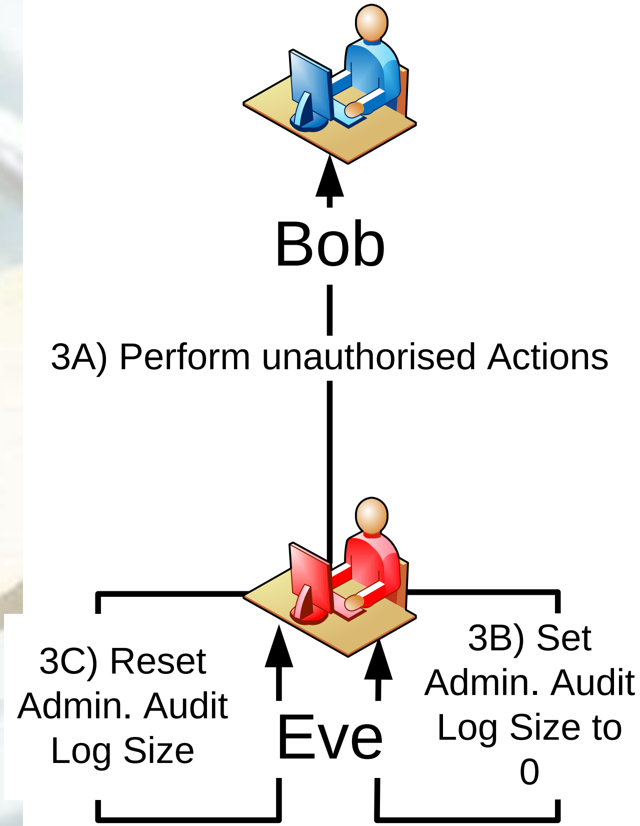
Admin. Audit Log records Audit Bypass Change

Deletes all **previous** entries of the Admin. Audit Log

Scenario E – Step 3

Tracking Administrator Audit Log Clearance

Malicious Activity


Bob
3A) Perform unauthorised Actions
Eve
3C) Reset Admin. Audit Log Size
3B) Set Admin. Audit Log Size to 0

Detection – Administrator Auditing

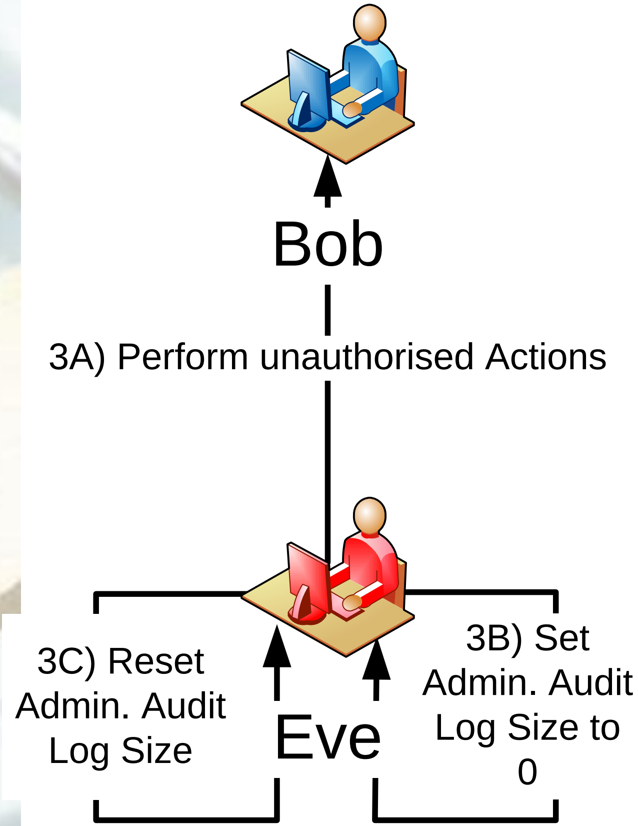
```
[PS]> Search-AdminAuditLog
           –Cmdlets Set-AdminAuditLogConfig

[CUT BY COMPASS]

ObjectModified              : Admin Audit Log Settings
CmdletName                  : Set-AdminAuditLogConfig
CmdletParameters            : {AdminAuditLogAgeLimit}
ModifiedProperties          : {AdminAuditLogAgeLimit}
Caller                      : ... Eve ...
Succeeded                   : True
Error                       : None
RunDate                     : 17/06/2016 10:20:00

[CUT BY COMPASS]
```

Specifies how long Log Entries are kept

Scenario E – Step 3

Tracking Administrator Audit Log Clearance

Malicious Activity


Bob
3A) Perform unauthorised Actions
3C) Reset Admin. Audit Log Size
Eve
3B) Set Admin. Audit Log Size to 0

Potential Remediation:

- Regular Backups or Log Forwards, e.g. to Splunk
- Ideally, trigger Backup before AdminAuditLogConfig Cmdlet is run

→ Log unauthorized Admininstrator Actions

Exchange Compliance Features

Transport Rules

- Look for specific Conditions in Messages
- Take certain Actions on them

Journaling

- Place Copy of Target E-Mails into a designated Mailbox
- Usually remaining on Mailbox Server

Archiving

- Backing up Data
- Store Copies to separate Environment
- Regulatory Compliance, Retention, Server Maintenance

Full Backup

- Backup Copies of entire Exchange Database(s)

Take Home Message

Compliances Features in Exchange

Message Tracking

- Track Message Flow
- Enabled by default

Mailbox Auditing

- Track Mailbox Accesses
- Disabled by default

→ Recording Key Actions may resolve many Investigation with limited Impact

In-Place / Litigation Hold

- Preserve Mailbox Items
- Disabled by default

→ Use when expecting Litigation

Administrator Auditing

- Tracks Configuration Changes
- Enabled by default

Single Item Recovery

- Recover deleted Items
- Disabled by default

Transport Rules

Journaling / Archiving

Full Backup

Questions

Thank You for the Attention!

→ Now let's enjoy some Beers…

References

- E-Mail Forensics in a Corporate Exchange Environment
  Nuno Mota, Senior Microsoft Messaging Consultant, UK IT Services Provider
  http://www.msexchange.org/articles-tutorials/exchange-server-2013/compliance-policies-archiving/e-mail-forensics-corporate-exchange-environment-part1.html
- Litigation Hold vs. Single Item Recovery vs. Retention Hold
  Nuno Mota, Senior Microsoft Messaging Consultant, UK IT Services Provider
  http://www.msexchange.org/kbase/ExchangeServerTips/ExchangeServer2010/ManagementAdministration/LitigationHoldvs.SingleItemRecoveryvs.RetentionHold.html
- Microsoft TechNet
  https://technet.microsoft.com

Appendix A

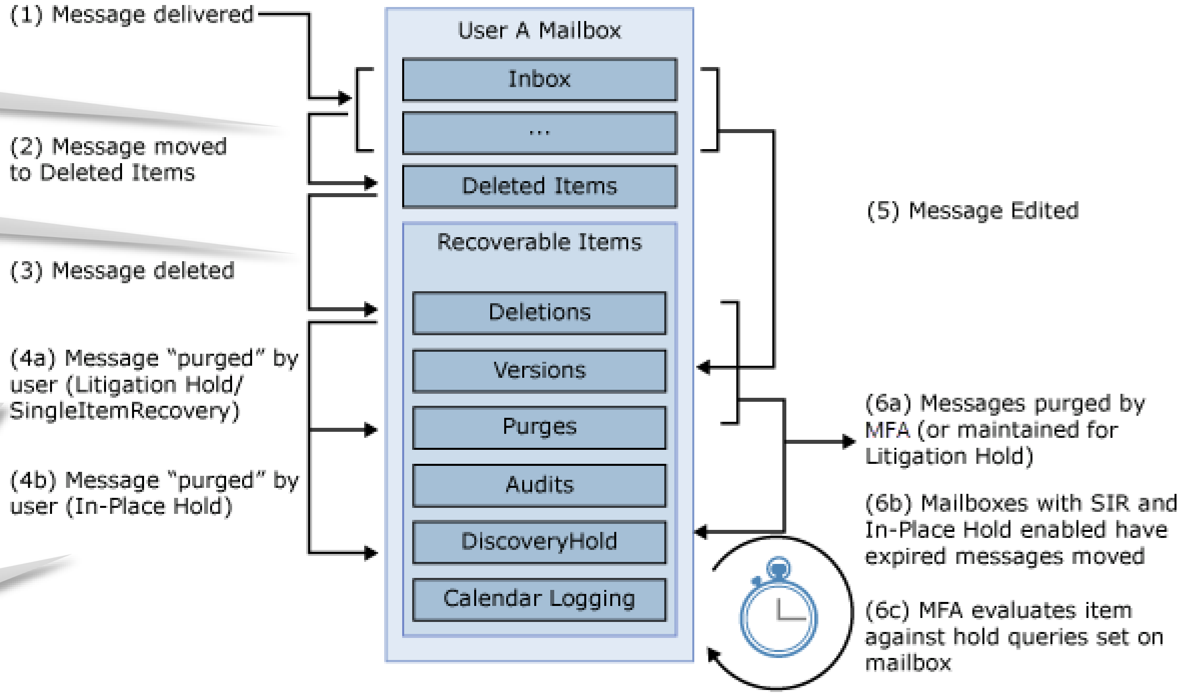
Recoverable Items Folder

(2) MoveToDeletedItems

(3) SoftDelete

Recover Deleted Items Feature in Outlook or OWA

(4) HardDelete


(1) Message delivered
(2) Message moved to Deleted Items
(3) Message deleted
(4a) Message "purged" by user (Litigation Hold/ SingleItemRecovery)
(4b) Message "purged" by user (In-Place Hold)
User A Mailbox
Inbox
...
Deleted Items
Recoverable Items
Deletions
Versions
Purges
Audits
DiscoveryHold
Calendar Logging
(5) Message Edited
(6a) Messages purged by MFA (or maintained for Litigation Hold)
(6b) Mailboxes with SIR and In-Place Hold enabled have expired messages moved
(6c) MFA evaluates item against hold queries set on mailbox

Source: https://technet.microsoft.com/en-us/library/ee364755(v=exchg.150).aspx