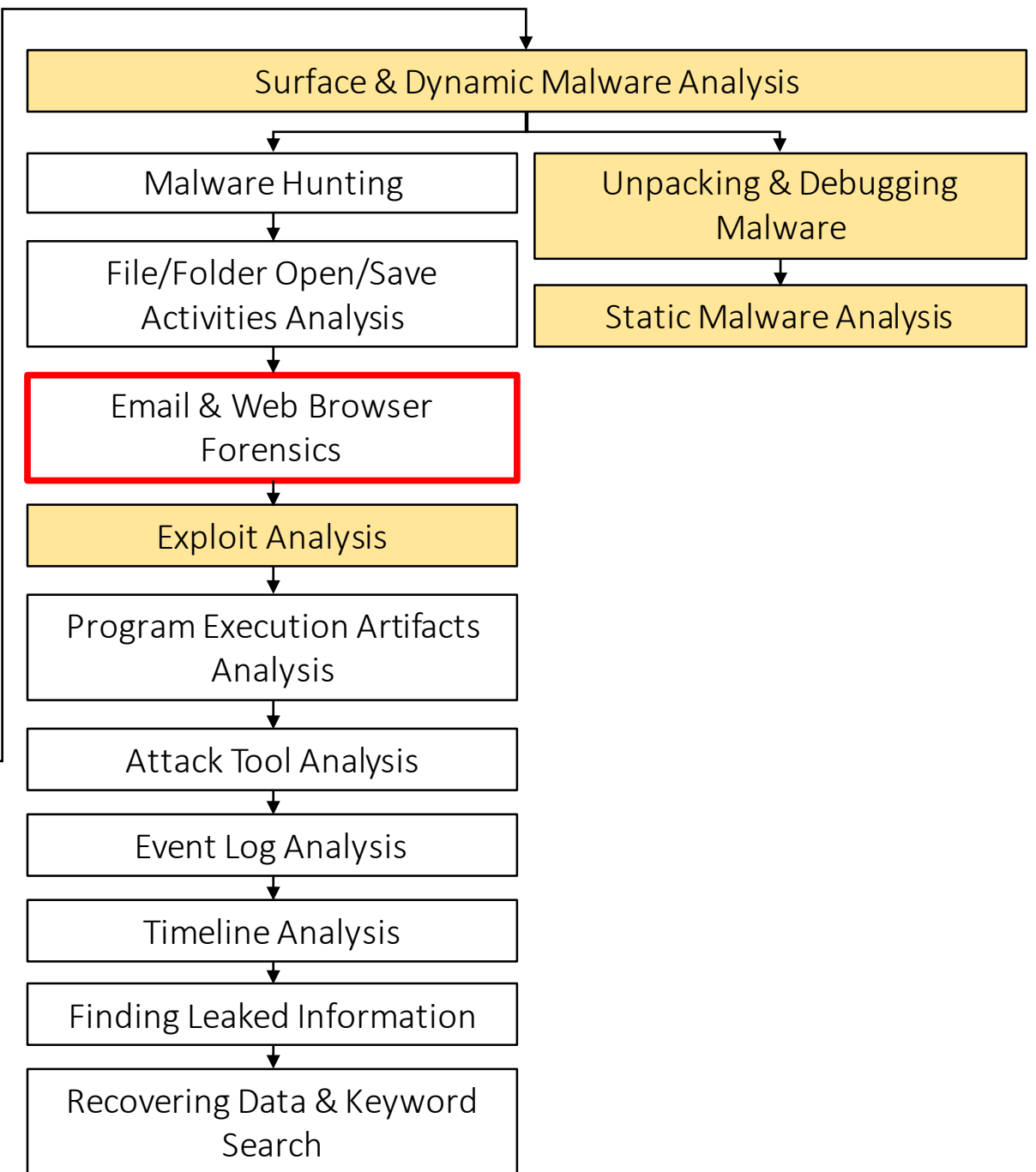
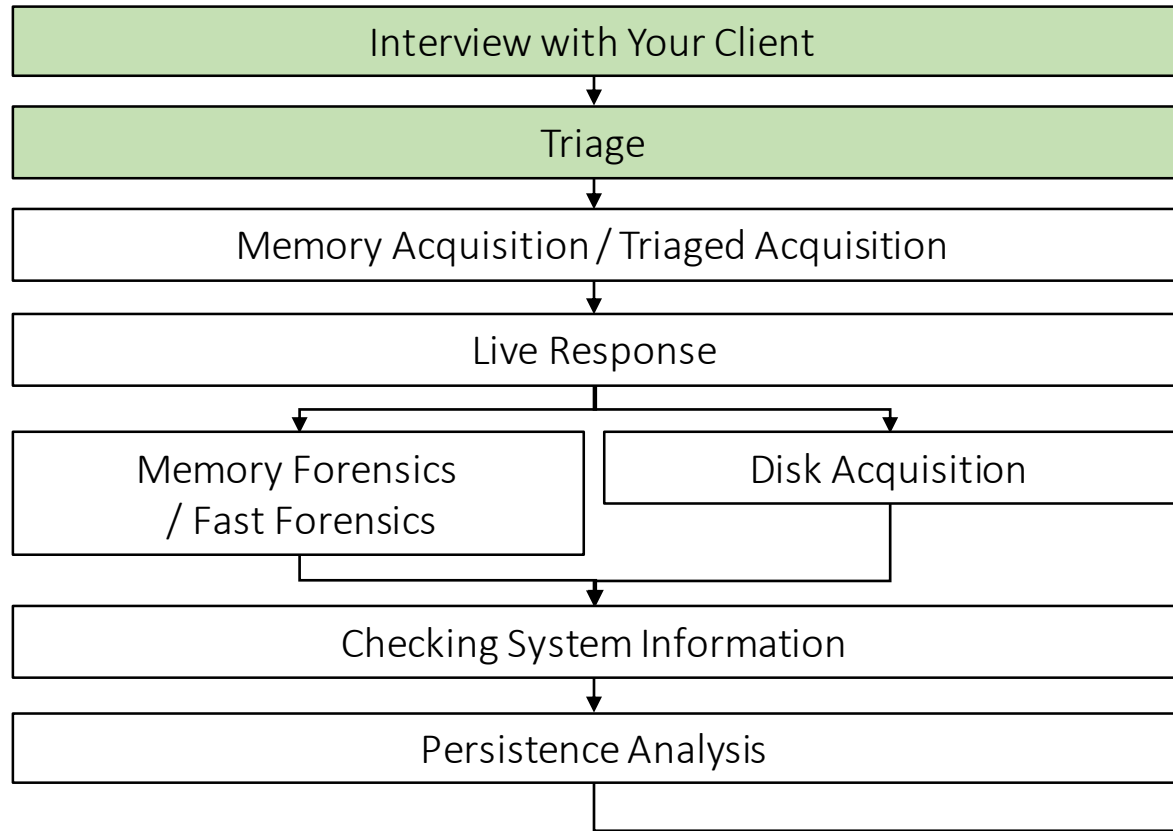


E-mail Forensics



The Major Root Causes

- In order to discover the root cause of the infection, we need to check several sources.
 - E-mails
 - Web (social engineering and drive by download, including watering hole attack)
 - Messengers (Skype, WhatsApp) and SNS Apps (Twitter, Facebook, ...)
 - Removable disks including USB thumb drive
- It is because, the root cause of many targeted attacks are in the paths. Especially, e-mails and web browser artifacts are the two major causes of attacks.

E-mail Forensics 101

E-mail Forensics 101

- What is E-mail Forensics?
 - It is a technique to investigate e-mails.
- Why E-mail Forensics?
 - We use this technique to find evidences of insider incidents in common (in eDiscovery).
 - Here, this is an incident involving malware. We investigate e-mails to specify when and how the user was infected with the malware.
 - Identifying infection routes is important for preventing recurrence.
 - However, we should try not to read the contents of e-mails as much as possible from the privacy point of view, unlike eDiscovery. Try to get just attachment files and links.

E-mail Forensics 101

- We will need to perform analysis on either client side or server side.
- On typical Windows enterprise environments, Exchange Server, Exchange Online or Office 365 are used as mail servers, and Outlook is used as a client software.

MUA Forensics

MUA Forensics

- Outlook
 - The mailbox for each user is stored as one of these formats.
 - PST
 - OST
 - NST
 - In common, in case of combining with Exchange / Office 365 and Outlook, the mailbox format on the client will be OST format (Exchange) or NST format (Office 365). If you export it from an Exchange server, the format will be PST.
- Thunderbird
 - Modified mboxrd format + SQLite
 - Since a mailbox of Thunderbird is portable, we can refer to the existing mails by acquiring all the contents under the path below and deploying them on an analysis PC where Thunderbird is installed.
 - %AppData%\Thunderbird
 - %LocalAppData%\Thunderbird

MUA Forensics

- Viewer/Parser
 - There are many commercial tools, but there are only a few free tools.
- PST
 - libpff
 - SysTools PST to MBOX Converter (Demo version)
 - Kernel Outlook PST Viewer (Demo version)
- OST
 - libpff
 - SysTools OST Viewer (Demo version)
 - Kernel OST Viewer (Demo version)
- NST
 - Kernel NST Viewer (Demo version)

MUA Forensics

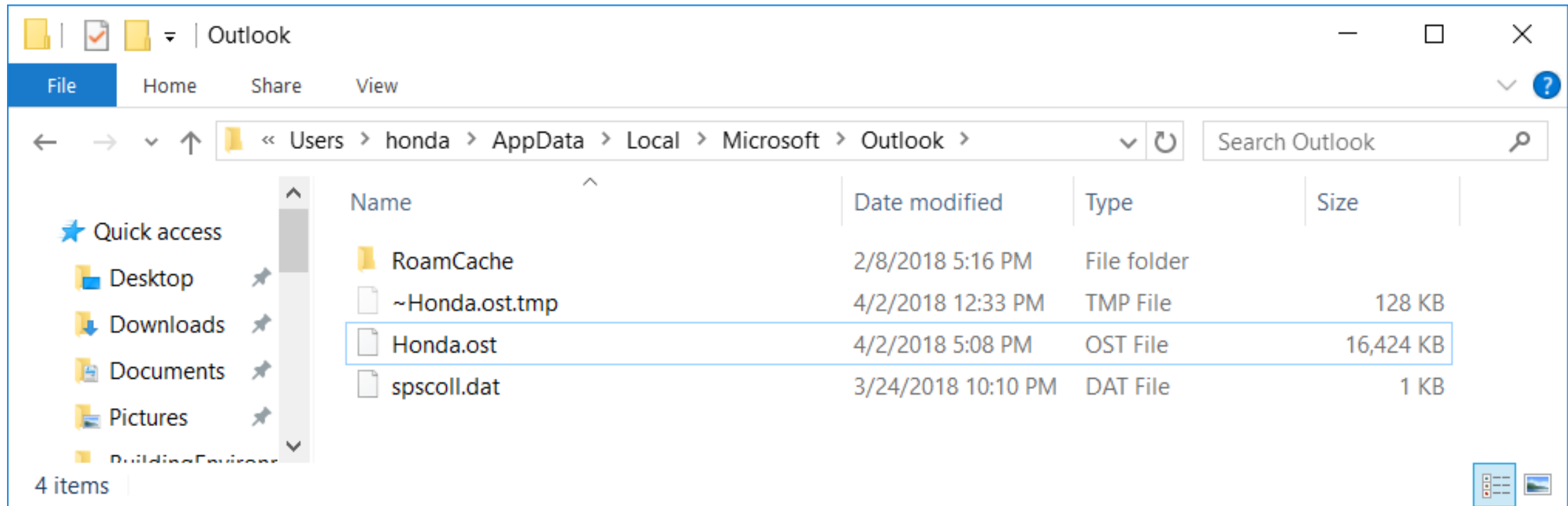
- libpff
 - Open Source Software.
 - We can extract email information including message header, message body and attachment files with pffexport command from PST and OST format by parsing them.
 - They are libraries and commands with command line interface.

MUA Forensics

- SYSTools OST Viewer
 - The demo version of this software is just a viewer for the OST format, and it does not have export feature of emails and attachments.
 - However, if you view an email with this software, the mail will be extracted and placed in the path below as “.eml” format.
 - %AppData%\CDTPL
 - Typical location of %AppData% is “C:\Users\<USERNAME>\AppData\Roaming”.
 - You can acquire the mail header, body and attachment files if you copy the mail.

MUA Forensics

- %LocalAppData%\Microsoft\Outlook



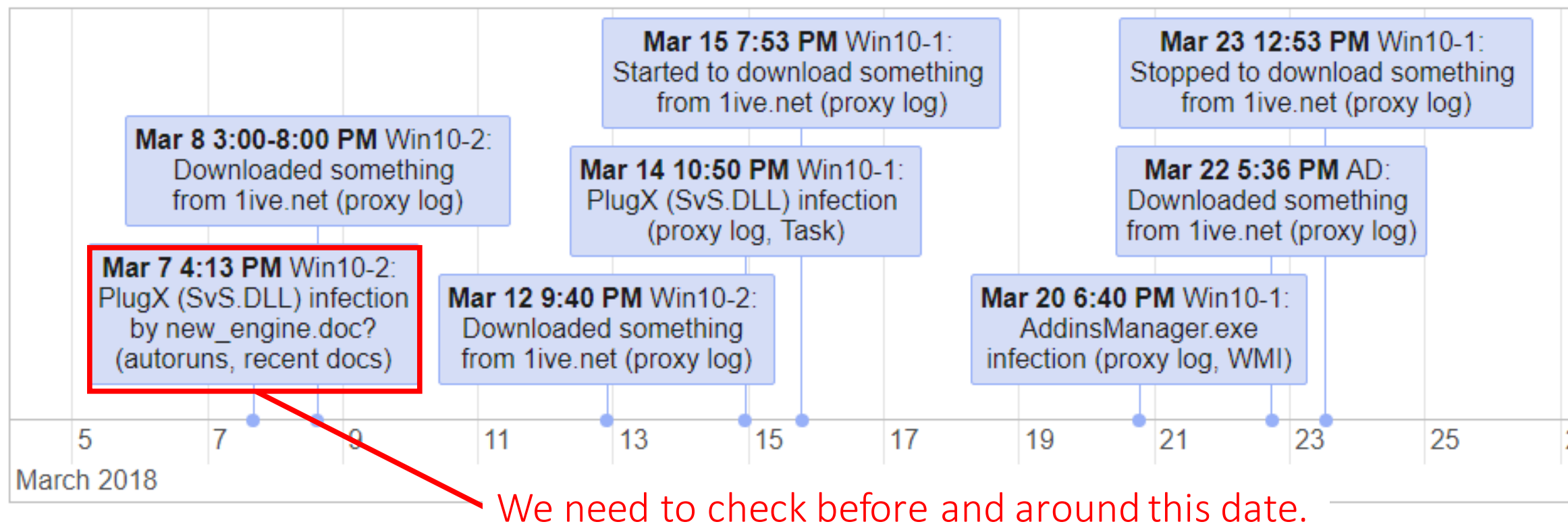
<https://support.office.com/en-us/article/find-and-transfer-outlook-data-files-from-one-computer-to-another-0996ece3-57c6-49bc-977b-0d1892e2aacc?ui=en-US&rs=en-US&ad=US>

Lab 1

Outlook Forensics with libpff

Outlook Forensics with libpff (1)

- This is the analysis results so far. We found the infection date (on March 7 at 4:13 PM) on Client-Win10-2.



Outlook Forensics with libpff (2)

- Mount this image with Arsenal Image Mounter with “Write temporary” option.
 - E:\Artifacts\scenario1_E01\Client-Win10-2_honda.E01

Outlook Forensics with libpff (3)

- libpff (pffexport)
 - Run “cmd_admin.exe” on the shortcut folder and execute this command.

```
pffexport -m all -t C:\Users\taro\Desktop\Honda.ost -c windows-932  
g:\Users\honda\AppData\Local\Microsoft\Outlook\Honda.ost
```

Note that you will need to change the drive letters corresponding to your environment. Enter this in a single line.

- -m : It specifies export mode. “all” could recover deleted data.
- -t : It is for specifying an export folder.
- -c : It is to specify a code page.
 - This OST file came from a Japanese environment, which uses a code page “CP932”.
 - See the URL below to find code pages.

[https://msdn.microsoft.com/en-us/library/windows/desktop/dd317756\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/dd317756(v=vs.85).aspx)

Outlook Forensics with libpff (4)

- libpff (pffexport)
 - Open PowerShell, and find message numbers on March 7, 2018 with this command.

```
chcp 932 ; Select-String "^Date: .* 7 Mar 2018" ( Get-ChildItem  
C:\Users\taro\Desktop\Honda.ost.export -Recurse | Where-Object { $_.Name -match  
"InternetHeaders.txt" } | Select-Object -ExpandProperty FullName ) | % {$_ .ToString() }
```

Enter this in a single line.

```
Desktop\Honda.ost.export\ルート - メールボックス\IPM_SUBTREE\受信トレイ\Message00131\InternetHeaders.txt:19:Date:  
Wed, 7 Mar 2018 14:36:24 +0900  
Desktop\Honda.ost.export\ルート - メールボックス\IPM_SUBTREE\受信トレイ\Message00132\InternetHeaders.txt:20:Date:  
Wed, 7 Mar 2018 14:41:29 +0900  
(snip)  
Desktop\Honda.ost.export\ルート - メールボックス\IPM_SUBTREE\受信トレイ\Message00144\InternetHeaders.txt:9:Date:  
Wed, 7 Mar 2018 16:17:41 +0900
```

Outlook Forensics with libpff (5)

- libpff (pffexport)
 - Next, find the attachment file names with this command.

```
Get-ChildItem C:\Users\taro\Desktop\Honda.ost.export -Recurse | Select -ExpandProperty  
FullName | Select-String "\\Message001[34]" | Select-String "\\Attachments\\" | %  
{$_.ToString()}
```

Enter this in a single line.

```
C:\Users\taro\Desktop\Honda.ost.export\ルート -  
メールボックス\IPM_SUBTREE\受信トレイ\Message00137\Attachments\1_invoice-KT20180307.xlsx  
C:\Users\taro\Desktop\Honda.ost.export\ルート -  
メールボックス\IPM_SUBTREE\受信トレイ\Message00139\Attachments\1_18-02-22-(tsaito).xls  
C:\Users\taro\Desktop\Honda.ost.export\ルート -  
メールボックス\IPM_SUBTREE\受信トレイ\Message00140\Attachments\1_new_engine.doc  
C:\Users\taro\Desktop\Honda.ost.export\ルート -  
メールボックス\IPM_SUBTREE\受信トレイ\Message00141\Attachments\1_invoice-KT20180307-2.xlsx  
(snip)
```

Several attachment files were found.

Outlook Forensics with libpff (5)

- libpff (pffexport)
 - Save the file we are looking for to Desktop on your VM. We will use this later in “Exploit Analysis” section.

```
copy "C:\Users\taro\Desktop\Honda.ost.export\ルート - メールボックス\IPM_SUBTREE\受信トレイ\Message00140\Attachments\1_new_engine.doc" $env:USERPROFILE\Desktop\new_engine.doc
```

Enter this in a single line

Outlook Forensics with libpff (6)

- libpff (pffexport)
 - You can see headers if you see "InternetHeaders.txt".

```
notepad "C:\Users\taro\Desktop\Honda.ost.export\ルート - メールボックス\IPM_SUBTREE\受信トレイ\Message00140\InternetHeaders.txt"
```

Enter this in a single line.

(snip)

To: <honda@ninja-motors.net>

From: Meguro <neguro@yapoo.co.jp>

This domain name isn't yahoo. The third character isn't "h", but "p".

Subject: =?UTF-8?B?5paw5Z6L44Ko440z44K4440z44Gu6K mz5aCx?=

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="-----E4130898EA5DCBBDD32F0276"

Content-Language: en-US

Message-ID: <20180307070742.872EFC1B46@mail.ninja-motors.net>

Date: Wed, 7 Mar 2018 16:07:42 +0900

The attacker sent this mail at this date.

(snip)

Outlook Forensics with libpff (7)

- libpff (pffexport)
 - You can get the URLs in the mails by executing the following command if needed.

```
Select-String "http?s://\" (Get-ChildItem C:\Users\taro\Desktop\Honda.ost.export -Recurse |  
Select-Object -ExpandProperty FullName | Select-String "\\Message001[34][0-9]\\Message\" ) | %  
{$_}.ToString() }
```

Enter this in a single line.

```
Desktop\Honda.ost.export\ルート - メールボックス\TPM_SUBTREE\受信トレイ  
\Message00138\Message.html:572: <a href="http://www.twitter.com/" target="_blank"></a>  
Desktop\Honda.ost.export\ルート - メールボックス\TPM_SUBTREE\受信トレイ  
\Message00138\Message.html:604: <a href="http://www.facebook.com" target="_blank"></a>  
(snip)
```

Outlook Forensics with libpff - Summary

- We got a suspicious mail.
 - The mail was sent at **March 7, 2018 at 4:07 PM (JST)** .
 - The attachment file name is “new_engine.doc”.
- We found that the attachment file was opened, from the investigation we have done on “Open/Save documents” artifacts.

Exchange Server Forensics

Exchange Server Forensics

- Exchange EDB
 - The mailbox database is saved as the EDB format (Extensible Storage Engine (ESE) Database (EDB) File format), which is also used in the Active Directory database (NTDS.DIT) and web access history of IE/Edge.
 - Unfortunately, many EDB viewers cannot read EDB from Exchange.
 - Nirsoft ESEDB Viewer
 - Most of the columns are empty.
 - Libesedb
 - Unknown ID (type 12) cause parse error.

Exchange Server Forensics

- Exchange EDB Parser/Viewer
 - SYSTools Exchange Recovery (Commercial / Free Demo)
 - Kernel Exchange EDB Viewer (Commercial / Free Demo)
 - Stellar Exchange EDB PST Converter (Commercial / Free Demo)
 - CodeTwo Backup For Exchange (Commercial)
 - Veeam Microsoft Exchange Recovery (Commercial)

Exchange Server Forensics

“%SystemDrive%” is typically “C:”.

- Common Exchange EDB file paths
 - 2010
 - %SystemDrive%\Program Files\Microsoft\Exchange Server\V14\Mailbox\Mailbox Database <<random number>>\mailbox database <<random number>>.edb
 - %SystemDrive%\Program Files\Microsoft\Exchange Server\V14\Mailbox\ Public Folder Database\Public Folder Database.edb
 - <https://technet.microsoft.com/en-us/library/hh441717.aspx>
 - https://social.technet.microsoft.com/Forums/de-DE/b38ce59d-07eb-4ded-a2c5-328e2894393e/exchange-2010-log-dateien-versehentlich-gelscht?forum=exchange_serverde
 - 2013/2016
 - %SystemDrive%\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database <<random number>>\mailbox database <<random number>>.edb
 - <https://social.technet.microsoft.com/Forums/ie/en-US/ae7839bd-e67e-494d-8fab-b0f2d45fed63/file-on-mailbox-database?forum=exchangesvradmin>

Exchange Server Forensics

- Finding the EDB file
 - You can use the command below to get the EDB file path in recent OS and Exchange versions.

```
Get-MailboxDatabase -Status | Select-Object edbfilepath
```

- <https://blogs.technet.microsoft.com/heyscriptingguy/2012/12/10/powertip-find-the-path-to-exchange-mailbox-database/>

Exchange Server Forensics

- SYSTools Exchange Recovery
 - You can filter with a period of dates for exporting e-mails.
 - Demo version of this software is for free. We can export up to 25 items per mail folder.
 - You can also get previewed mails under the directory below.
 - C:\Users\taro\AppData\Roaming\CDTPL\SysTools Exchange Recovery

Lab 2

Exchange Server Forensics with SYSTools Exchange Recovery

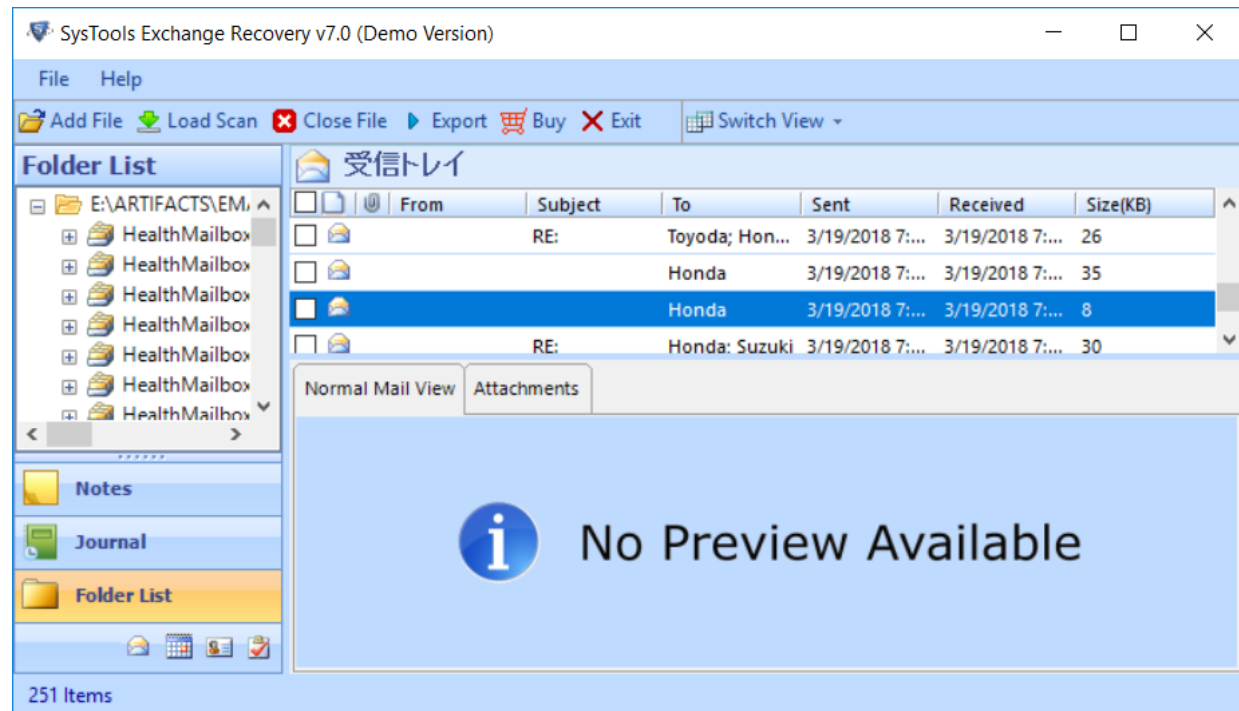
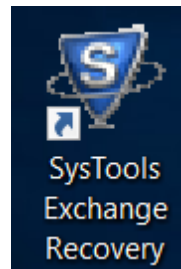
Exchange Server Forensics with SYSTools Exchange Recovery

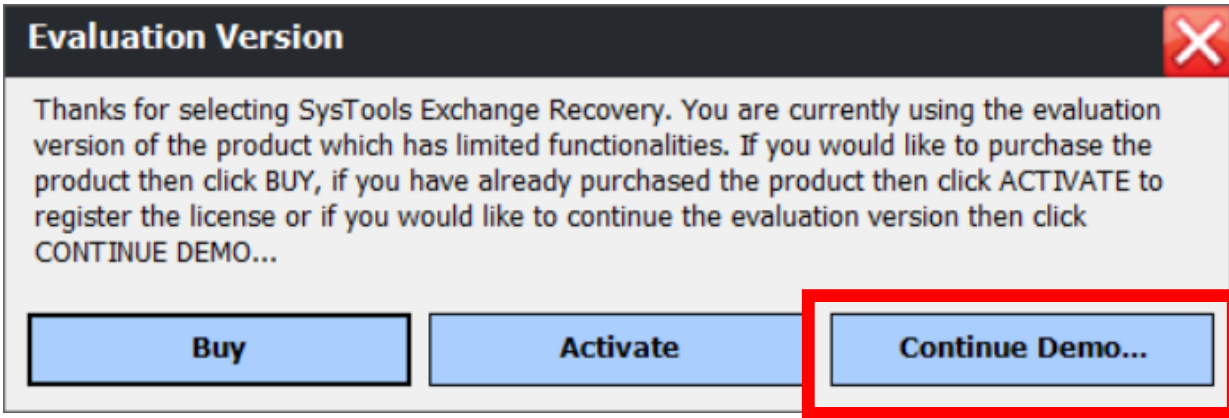
- Mount the Exchange Server's disk Image below with Arsenal Image Mounter with "Write temporary" option.

- E:\Artifacts\scenario1_E01\Exchng-Win2016-disk1.E01

From now on, we assume this image is mounted with the drive letter "I".

- Open SYSTools Exchange Recovery on the shortcuts folder.

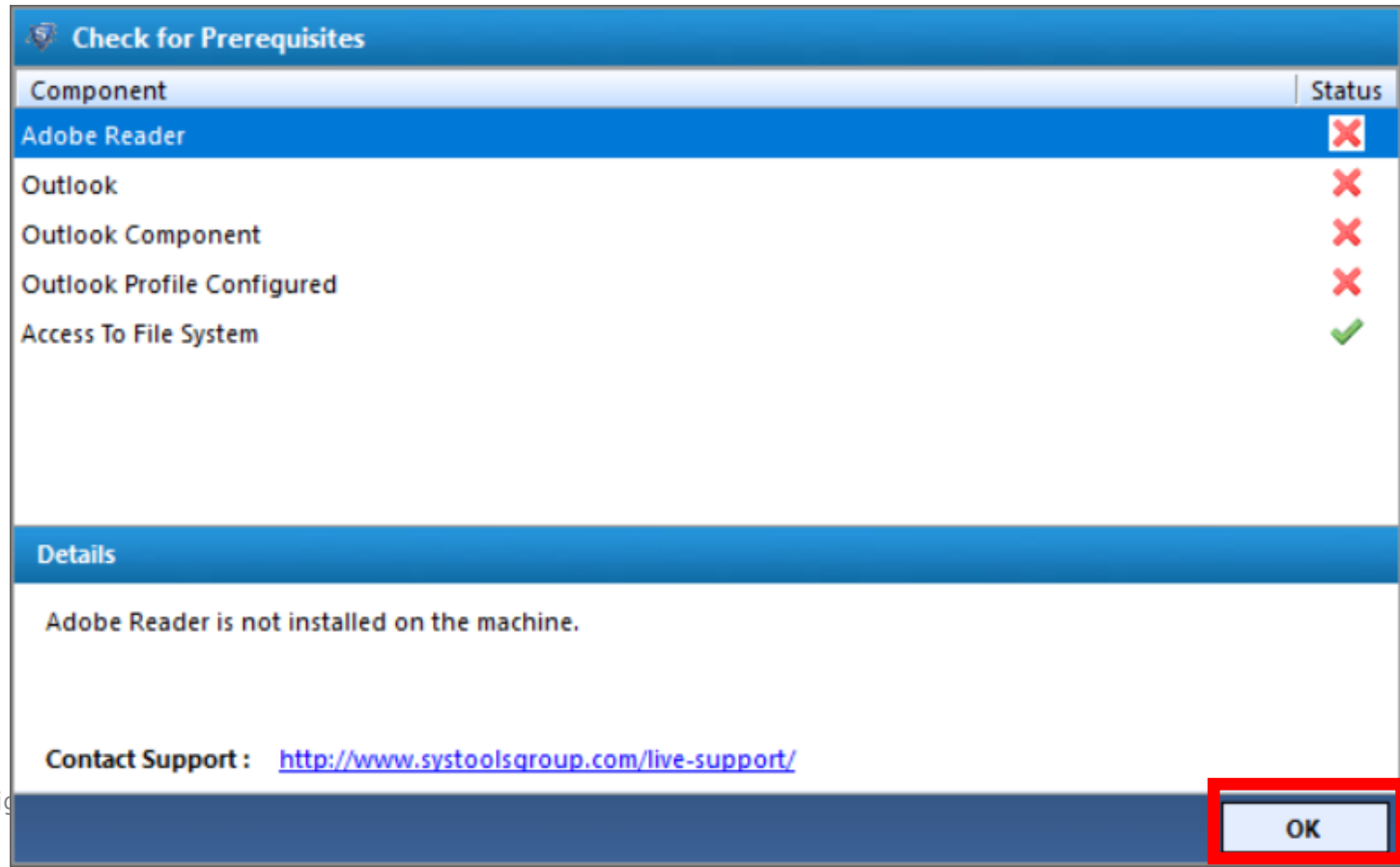




Press “Continue Demo...” when you get this message.

asics with SYSTools

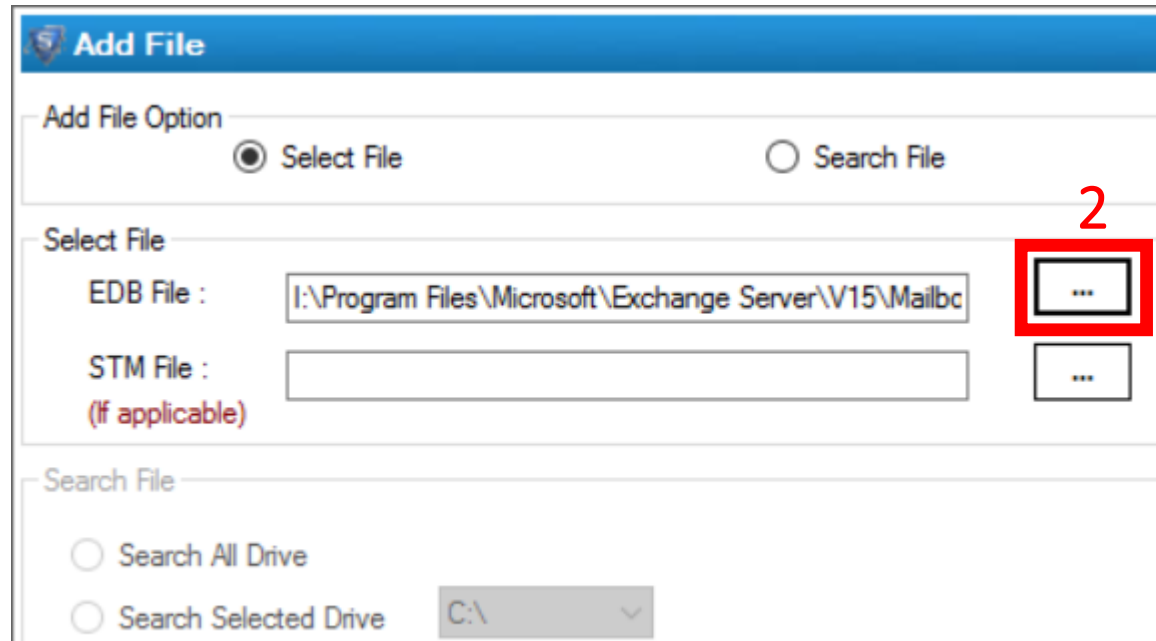
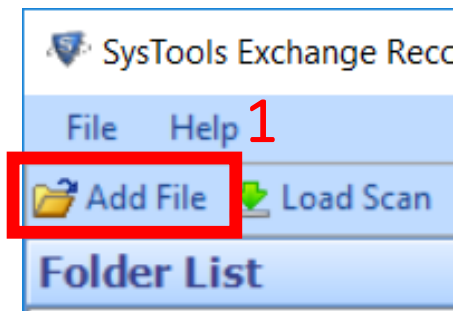
Click “OK” when you get this message.



Exchange Server Forensics with SYSTools

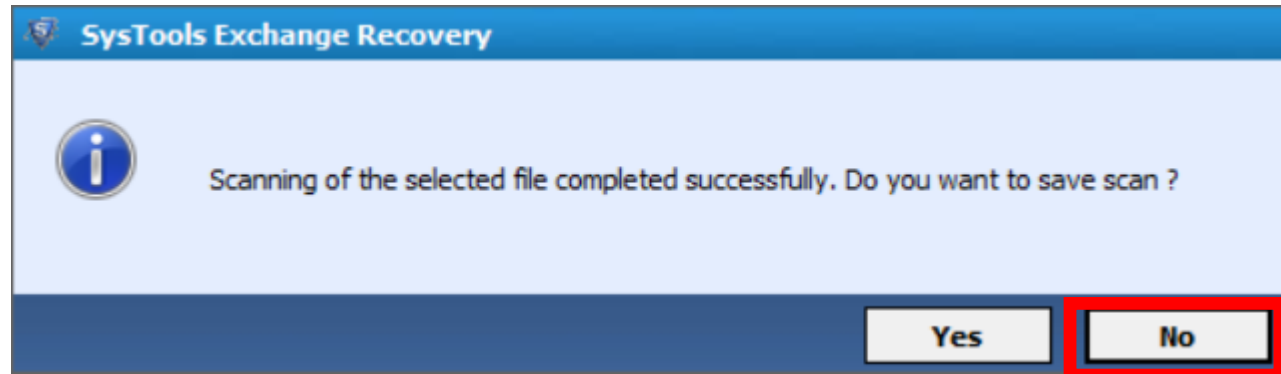
Exchange Recovery

- Click “Add File” on the toolbar.
 - Choose the EDB file below and press “Add” in “Add File” dialog.
 - I:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1886701956\Mailbox Database 1886701956.edb
- Note that you may need to change the drive letters corresponding to your environment.

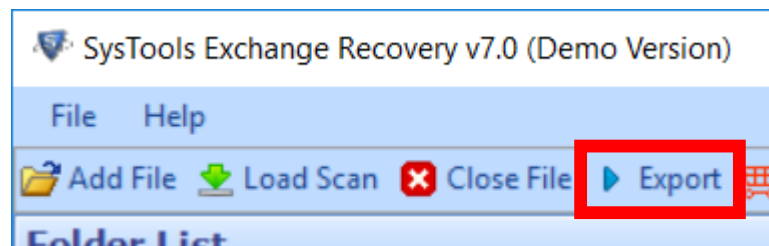


Exchange Server Forensics with SYSTools Exchange Recovery

- Press “No” when the dialog below is shown.



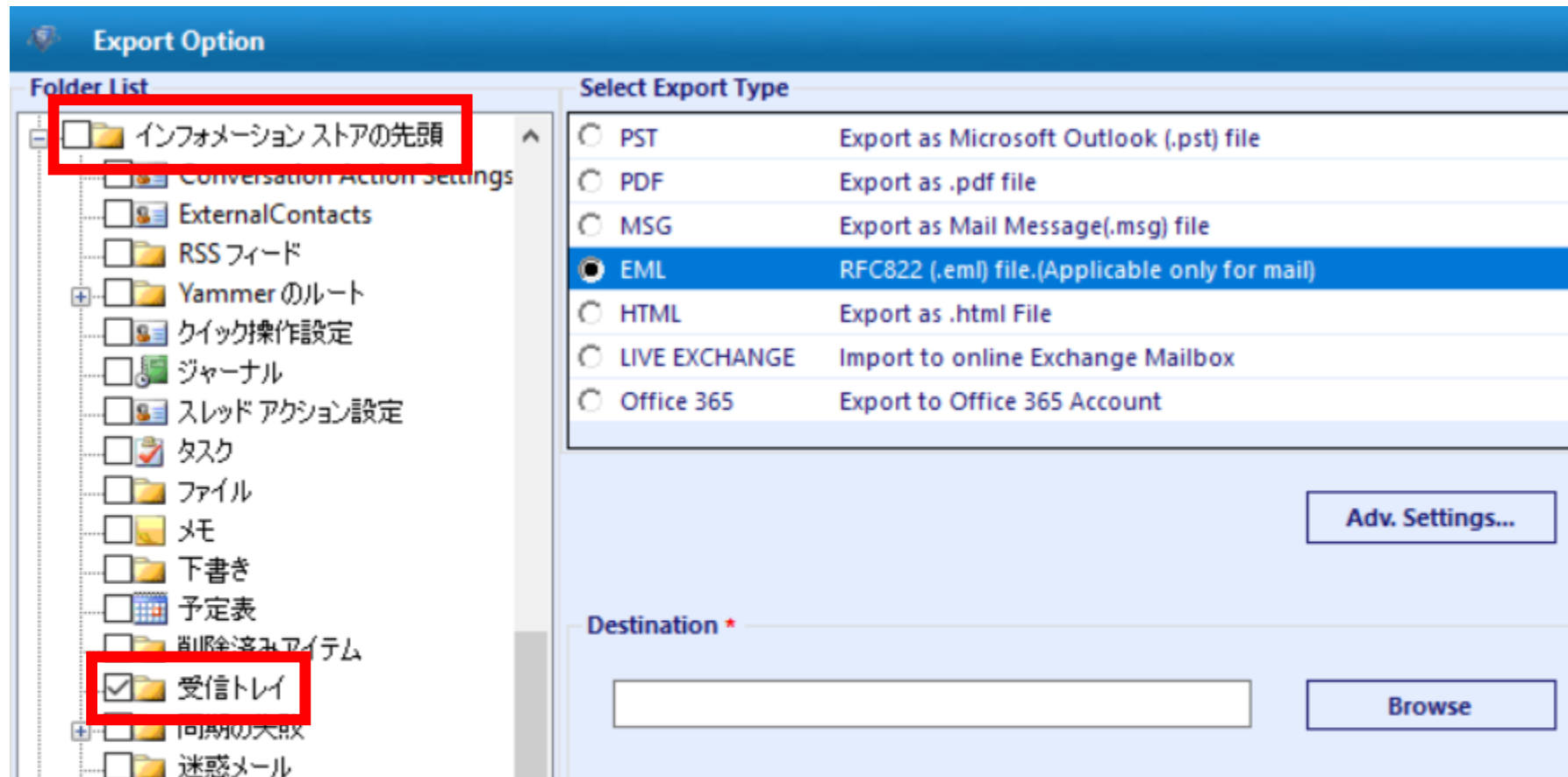
- Click “Export”.



Exchange Server Forensics with SYSTools

Exchange Recovery

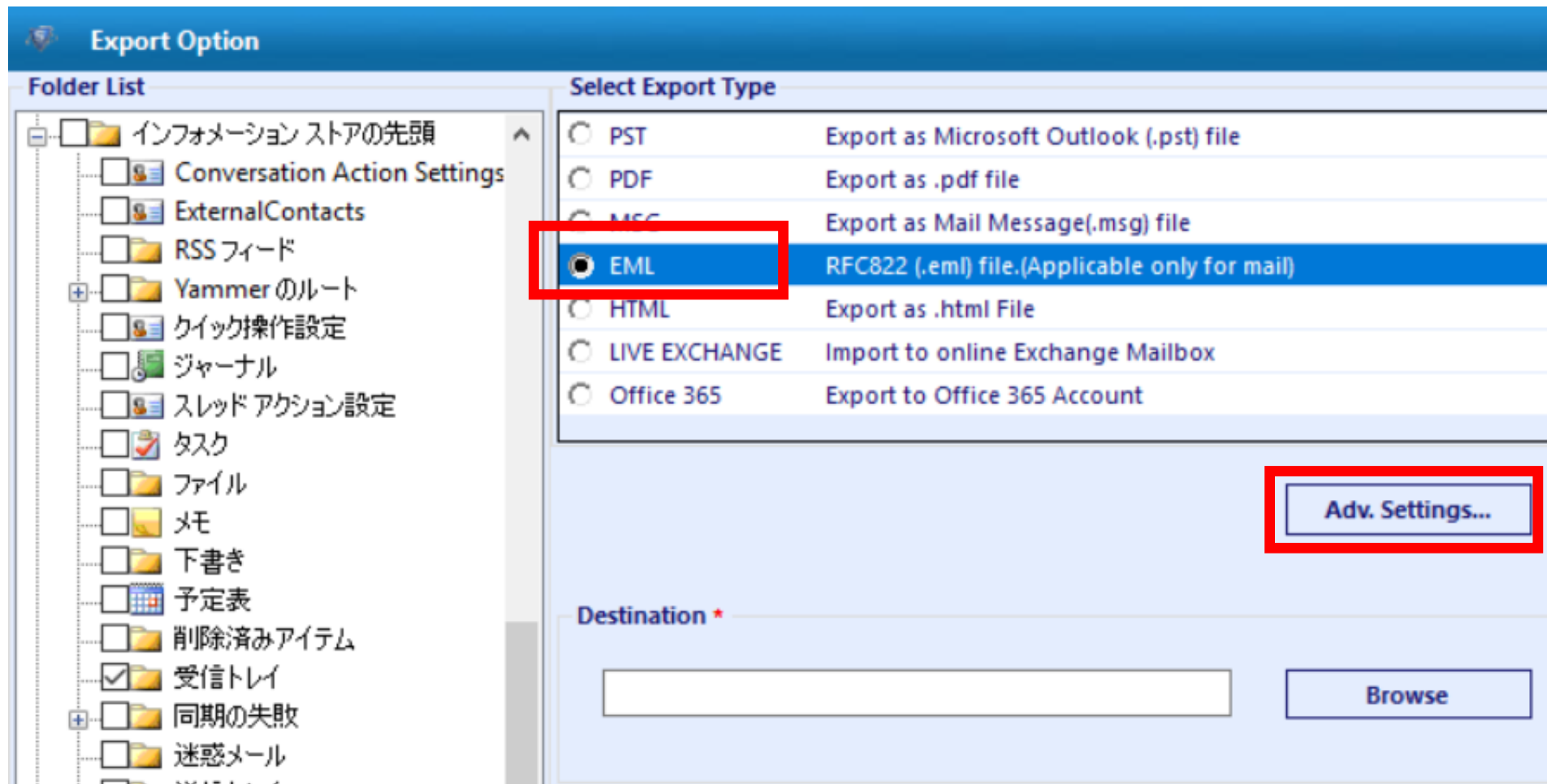
- Honda -> Orphan -> インフォメーションストアの先頭 (Top of Information Store) -> 受信トレイ (inbox)



Exchange Server Forensics with SYSTools

Exchange Recovery

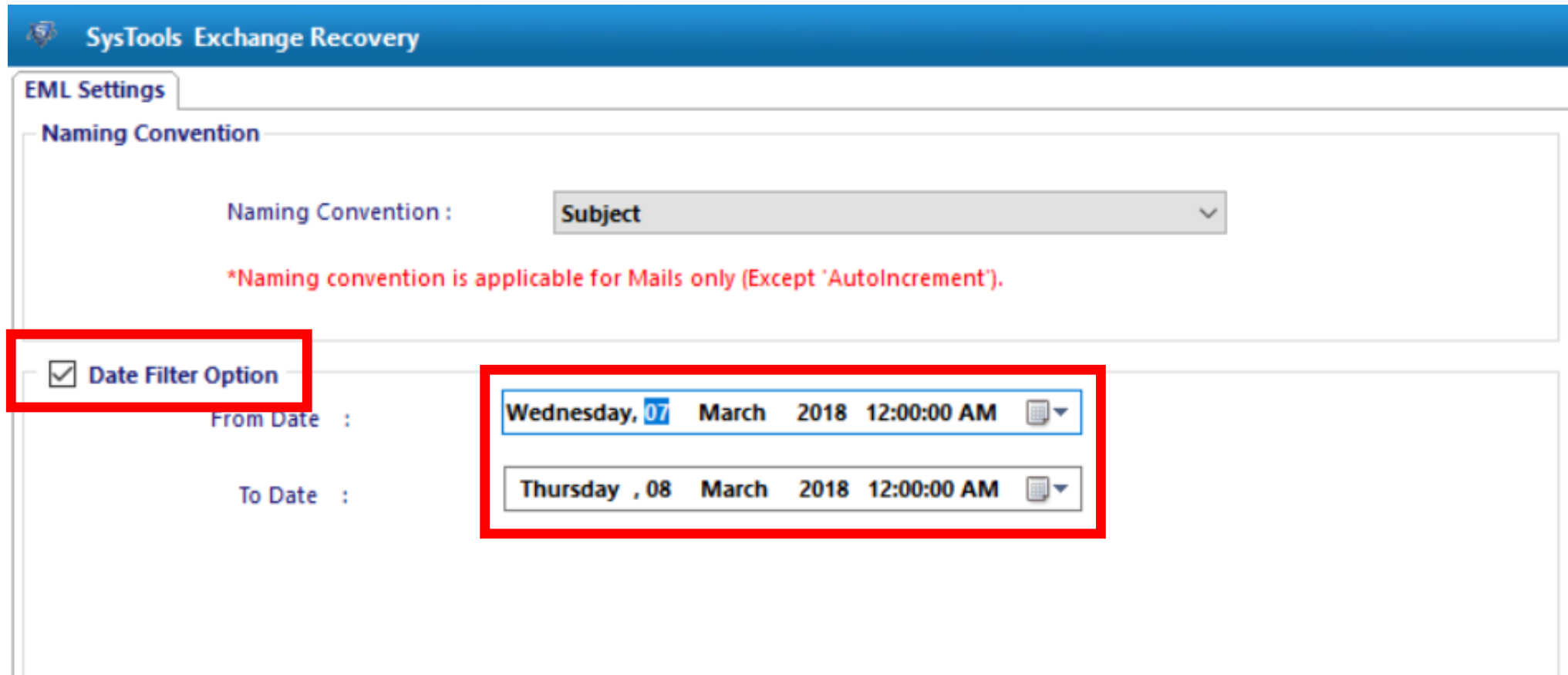
- Select “EML” and press “Adv. Settings...”.



Exchange Server Forensics with SYSTools

Exchange Recovery

- Set from March 07, 2018 at 12:00 AM to March 08, 2018 at 12:00 AM as date filter, and press “Save”.



The screenshot shows the 'SysTools Exchange Recovery' application window. The 'EML Settings' tab is active. Under the 'Naming Convention' section, a dropdown menu is set to 'Subject'. A red note states: '*Naming convention is applicable for Mails only (Except 'AutoIncrement')'. Below this, the 'Date Filter Option' checkbox is checked and highlighted with a red box. The 'From Date' field is set to 'Wednesday, 07 March 2018 12:00:00 AM' and the 'To Date' field is set to 'Thursday, 08 March 2018 12:00:00 AM', both of which are also highlighted with a red box.

SysTools Exchange Recovery

EML Settings

Naming Convention

Naming Convention : Subject

*Naming convention is applicable for Mails only (Except 'AutoIncrement').

☒ **Date Filter Option**

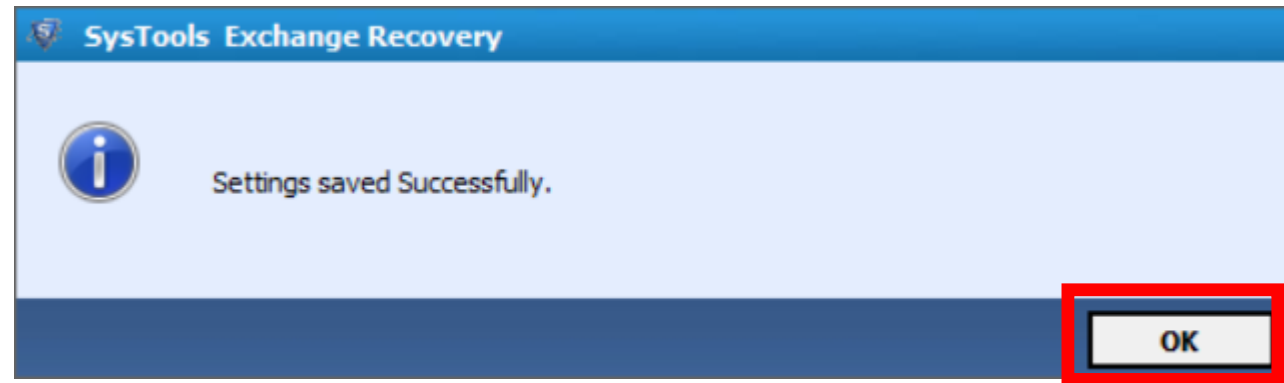
From Date : Wednesday, 07 March 2018 12:00:00 AM

To Date : Thursday, 08 March 2018 12:00:00 AM

Exchange Server Forensics with SYSTools

Exchange Recovery

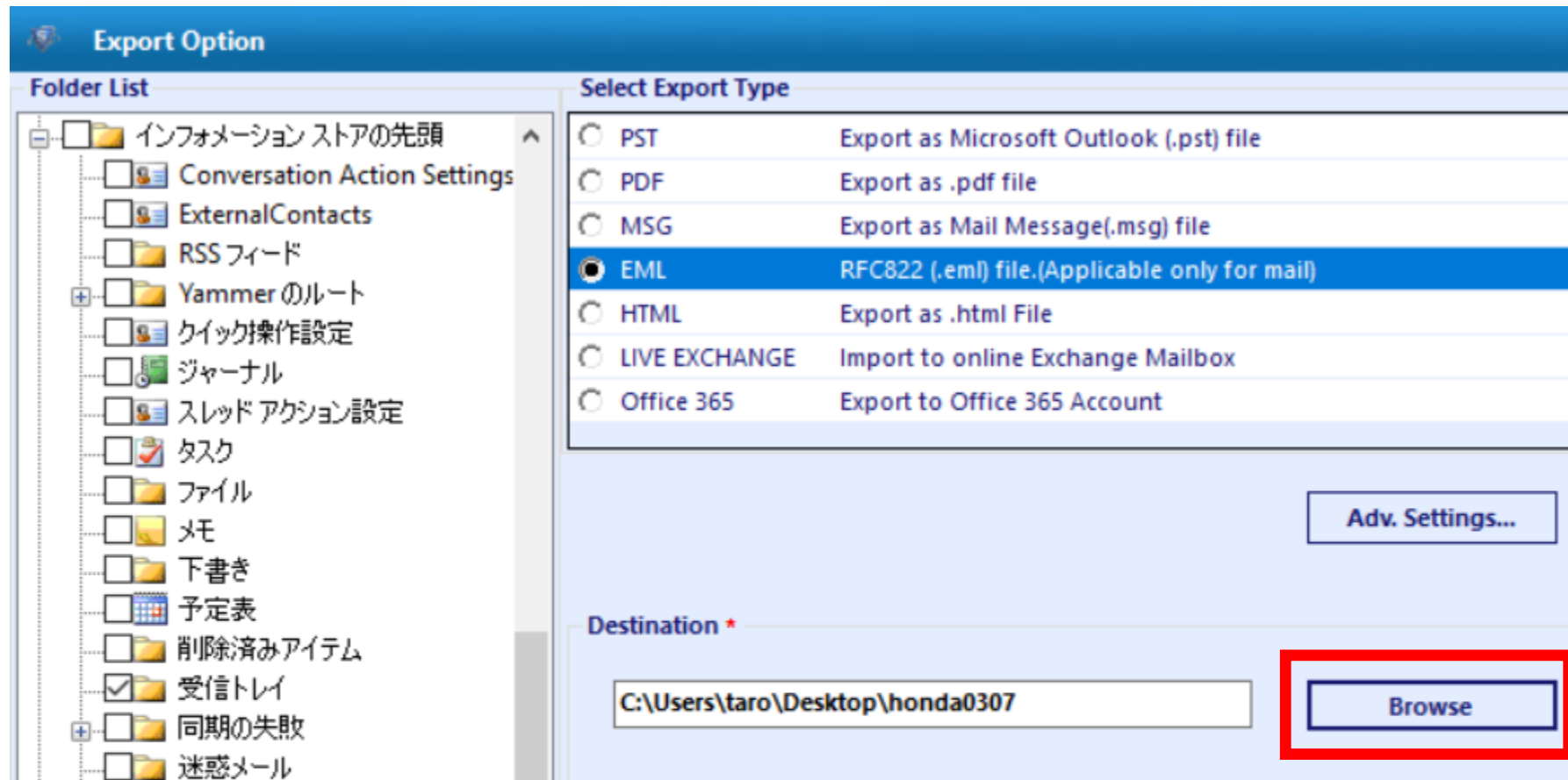
- SYSTools Exchange Recovery
 - Press “OK” when you see the message.



Exchange Server Forensics with SYSTools

Exchange Recovery

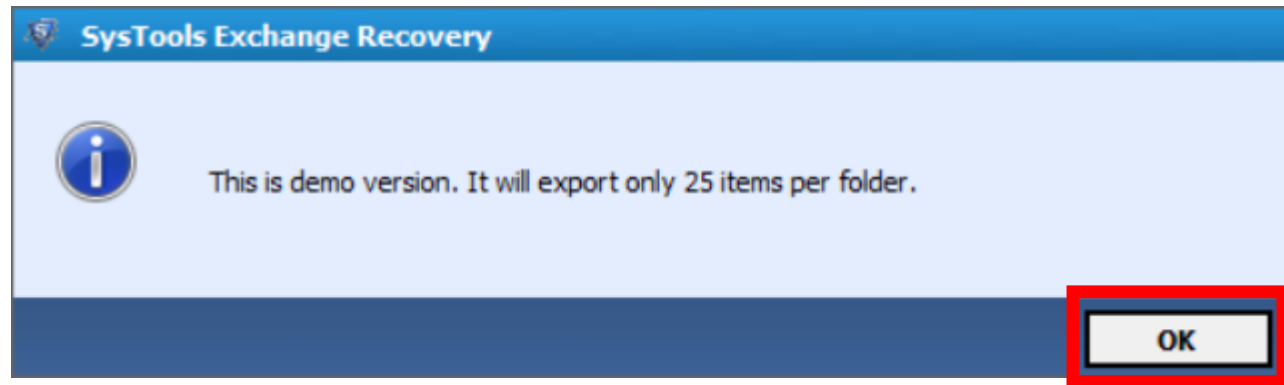
- SYSTools Exchange Recovery
 - Press “Browse” and choose a destination folder, then press “Export”.



Exchange Server Forensics with SYSTools

Exchange Recovery

- SYSTools Exchange Recovery
 - Press “OK” when you find the message.



Exchange Server Forensics with SYSTools Exchange Recovery

- SYSTools Exchange Recovery
 - You can get the exported emails.

The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Desktop > honda0307 > Honda'. The left sidebar shows 'Quick access' with 'Desktop' selected. The main pane displays a list of files with columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
SysTools_no subject(1).eml	5/4/2018 10:51 PM	Thunderbir...	402 KB
SysTools_no subject(2).eml	5/4/2018 10:51 PM	Thunderbir...	12 KB
SysTools_no subject.eml	5/4/2018 10:51 PM	Thunderbir...	32 KB
SysTools_RE_ (1).eml	5/4/2018 10:51 PM	Thunderbir...	12 KB
SysTools_RE_ (2).eml	5/4/2018 10:51 PM	Thunderbir...	14 KB
SysTools_RE_ (3).eml	5/4/2018 10:51 PM	Thunderbir...	8 KB
SysTools_RE_ (4).eml	5/4/2018 10:51 PM	Thunderbir...	15 KB
SysTools_RE_ (5).eml	5/4/2018 10:51 PM	Thunderbir...	30 KB
SysTools_Re_ (6).eml	5/4/2018 10:51 PM	Thunderbir...	44 KB
SysTools_Re_ (7).eml	5/4/2018 10:51 PM	Thunderbir...	102 KB
SysTools_Re_ (8).eml	5/4/2018 10:51 PM	Thunderbir...	46 KB
SysTools_RE_ .eml	5/4/2018 10:51 PM	Thunderbir...	10 KB
SysTools_配信不能_ (1).eml	5/4/2018 10:51 PM	Thunderbir...	9 KB
SysTools_配信不能 .eml	5/4/2018 10:51 PM	Thunderbir...	9 KB

Overlaid on the bottom right is a Mozilla Thunderbird window showing an email message. The 'Subject' field is empty, and the 'To' field is 'Honda <>☆'. The message body contains Japanese text and a list of instructions.

Subject

To Honda <>☆

新しい規格で製造された新型エンジンの詳細を入手しました。
画像とあわせて添付ファイルにまとめてありますので、ご確認ください。

以下の手順でファイルを開き、中の画像を閲覧できます。

1. 添付ファイルを保存する。
2. 添付ファイルをダブルクリックして開く(MS WORDで開く)。
3. 画面上方メッセージバーの[編集を有効にする]をクリックする。
4. 同じくメッセージバーの[コンテンツの有効化]をクリックする。

*画像が大きいのので復号の処理が必要です。

目黒

> 1 attachment: new_engine.doc 291 KB

E-mail Forensics – Tips

Exchange Server Forensics with Another Method

- You can acquire PST files from EDB on running Exchange Servers.
 - Exchange Management Shell (Exchange PowerShell) (+ ESEUtil).
 - New-MailboxExportRequest cmdlet
 - <https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/New-MailboxExportRequest?view=exchange-ps>
 - [https://technet.microsoft.com/en-us/library/mt784720\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/mt784720(v=exchg.160).aspx)
 - <https://social.technet.microsoft.com/wiki/contents/articles/29986.exchange-troubleshooting-recover-mailbox-from-edb-file-with-free-built-in-tools.aspx>
 - <https://www.codetwo.com/admins-blog/exchange-mailbox-backup-pst-pros-cons/>
 - Tips for using New-MailboxExportRequest cmdlet
 - <https://docs.microsoft.com/en-us/powershell/exchange/?view=exchange-ps>
 - <https://deangrant.wordpress.com/2013/10/04/the-term-new-mailboxexportrequest-is-not-recognized/>
 - <https://anandthearchitect.com/2012/10/16/exchange-2010-new-mailboxexportrequestaccess-to-the-path-is-denied/>
 - EAC (Exchange Admin Center)
 - [https://technet.microsoft.com/en-us/library/mt784720\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/mt784720(v=exchg.160).aspx)

Office 365 / Exchange Online Forensics

- To export Office 365 mailboxes to your local PC, see the URLs below.
 - Office 365 Admin Center + eDiscovery Export tool
 - <https://www.codetwo.com/admins-blog/how-to-export-office-365-mailboxes-to-pst-using-ediscovery/>
 - [https://technet.microsoft.com/en-us/library/dn440164\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dn440164(v=exchg.160).aspx)
 - Outlook
 - <https://support.office.com/en-us/article/export-or-backup-email-contacts-and-calendar-to-an-outlook-pst-file-14252b52-3075-4e9b-be4e-ff9ef1068f91>
 - Third Party Tools
 - SysTools Office 365 Backup & Restore Software (Commercial)
 - <https://www.systoolsgroup.com/office365-backup/>
 - bitrecover EML Converter Wizard (Commercial)
 - <https://www.bitrecover.com/eml-converter/>

E-mail Forensics – Wrap up

What We Learned in This Chapter

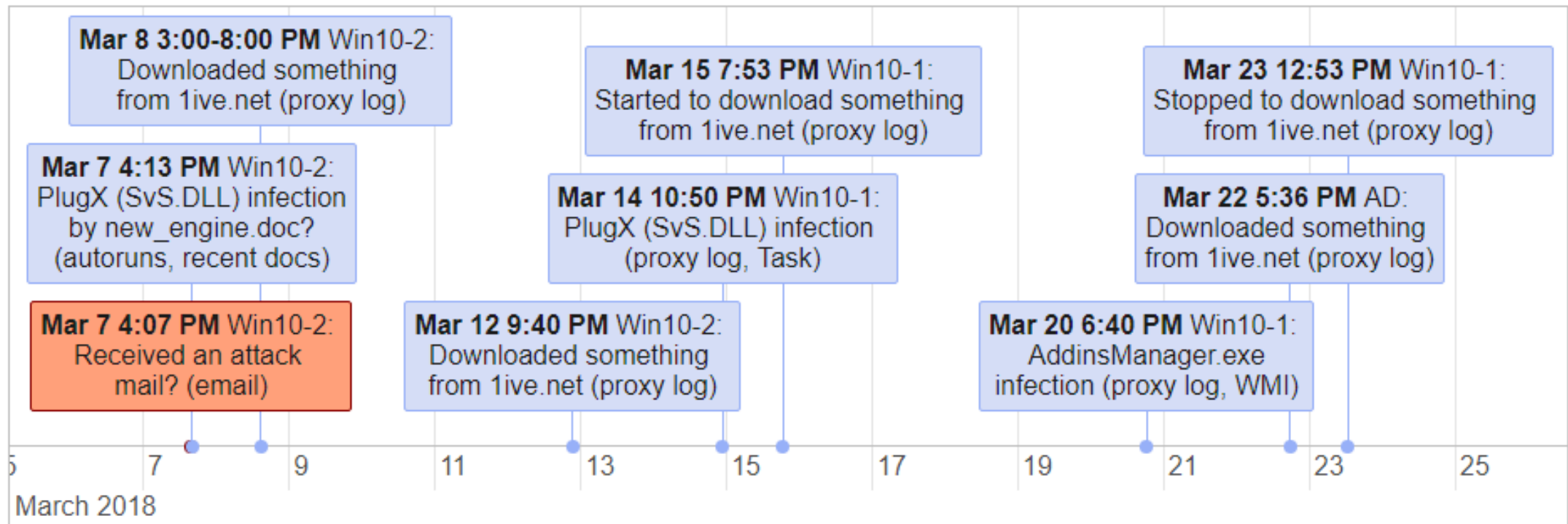
- Several tools can parse OST and PST files that are found on clients with Outlook.
- Exchange servers have mailboxes as an EDB file.
 - We can parse it in several ways.

Considerations on E-mail Forensics

- You should just extract attachment files and URLs around the infection dates.
- Do not read contents of mails from the privacy point of view.

What We Learned in This Chapter – Scenario 1

- We got several suspicious e-mails and we have an evidence that the user seems to have opened them. We will need to analyze the file named “new_engine.doc” in detail, in the exploit analysis section.



Tools

- PST
 - libpff
 - <https://github.com/libyal/libpff>
 - SysTools PST to MBOX Converter (Demo version)
 - <https://www.systoolsgroup.com/outlook-to-mbox.html>
 - Kernel Outlook PST Viewer (Demo version)
 - <https://www.kerneldatarecovery.com/pst-viewer.html>
- OST
 - libpff
 - <https://github.com/libyal/libpff>
 - SysTools OST Viewer (Demo version)
 - <https://www.systoolsgroup.com/ost-viewer.html>
 - Kernel OST Viewer (Demo version)
 - <https://www.kerneldatarecovery.com/ost-viewer.html>

Tools

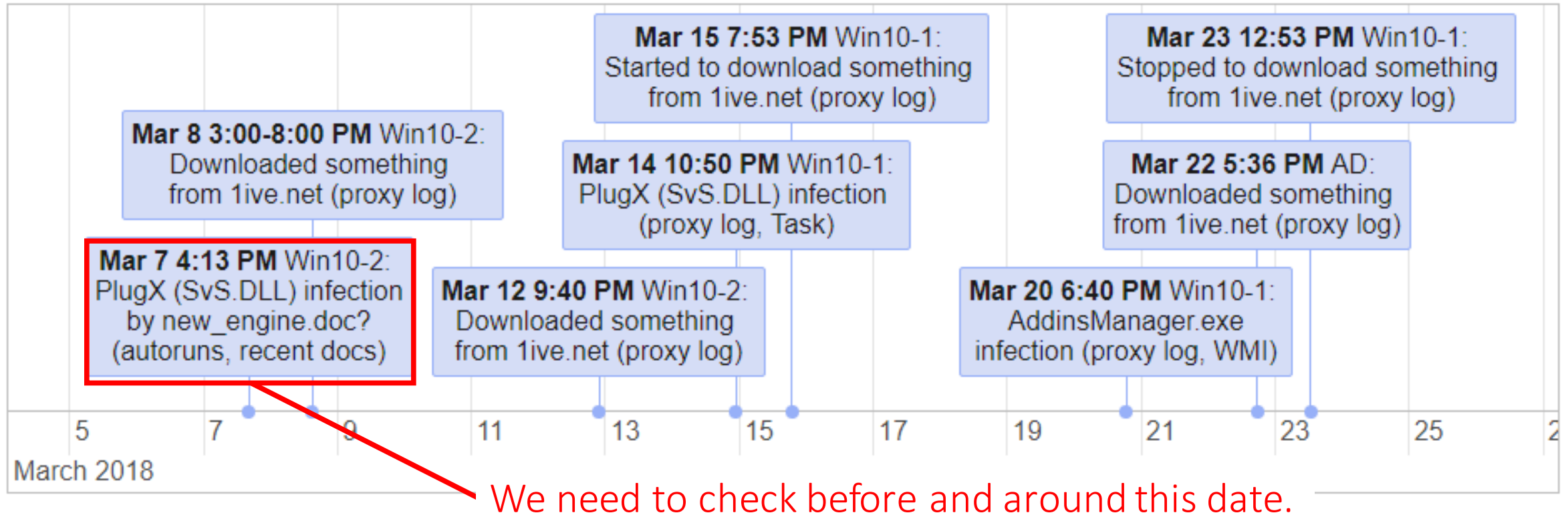
- Exchange EDB
 - SYSTools Exchange Recovery
 - <https://www.systoolsgroup.com/exchange-recovery.html>
 - Kernel EDB Viewer
 - <https://www.kerneldatarecovery.com/edb-viewer.html>
 - Veeam Microsoft Exchange Recovery
 - <https://www.veeam.com/microsoft-exchange-recovery.html>
 - Stellar Exchange EDB PST Converter
 - <http://www.stellarservertools.com/exchange-edb-pst-converter.php>
 - CodeTwo Backup For Exchange
 - <http://www.codetwo.com/backup-for-exchange/>

Appendix 1: Extra Exercise 1

Outlook Forensics with SYSTools OST Viewer

Outlook Forensics with SYSTools OST Viewer (1)

- This is the analysis results so far. We found the infection date (on March 7 at 4:13 PM) on Client-Win10-2.



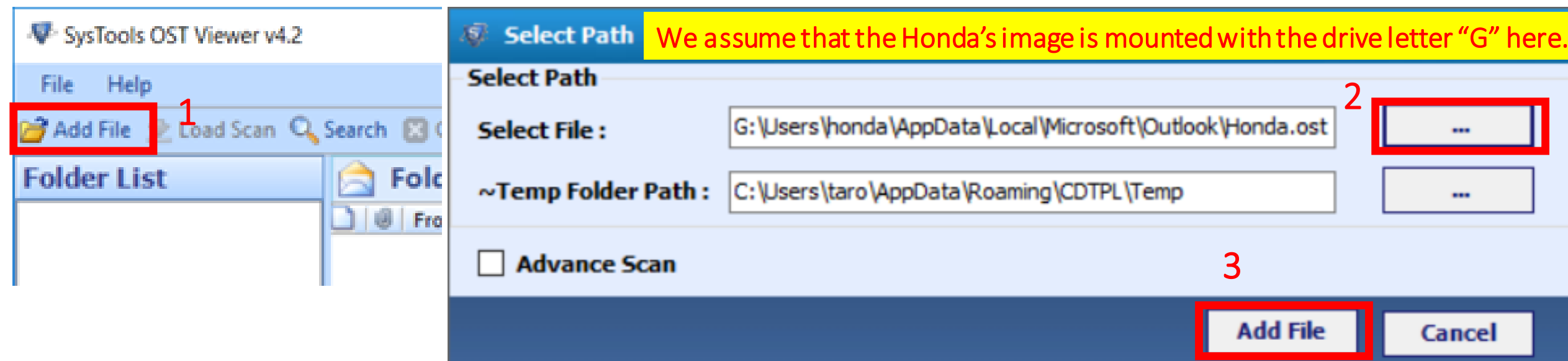
Outlook Forensics with SYSTools OST Viewer (2)

- Mount this image with Arsenal Image Mounter with “Write temporary” option.
 - E:\Artifacts\scenario1_E01\Client-Win10-2_honda.E01
- Open “SysTools OST Viewer” on the shortcut folder.
- By the way, you can skip this exercise if you do not like GUI based investigation. We will perform the same exercise with a CUI based application.

Outlook Forensics with SYSTools OST Viewer (3)

- Click “Add File” on the toolbar
- Choose the OST file below and press “Add File” in “Select Path” dialog.
 - G:\Users\honda\AppData\Local\Microsoft\Outlook\Honda.ost

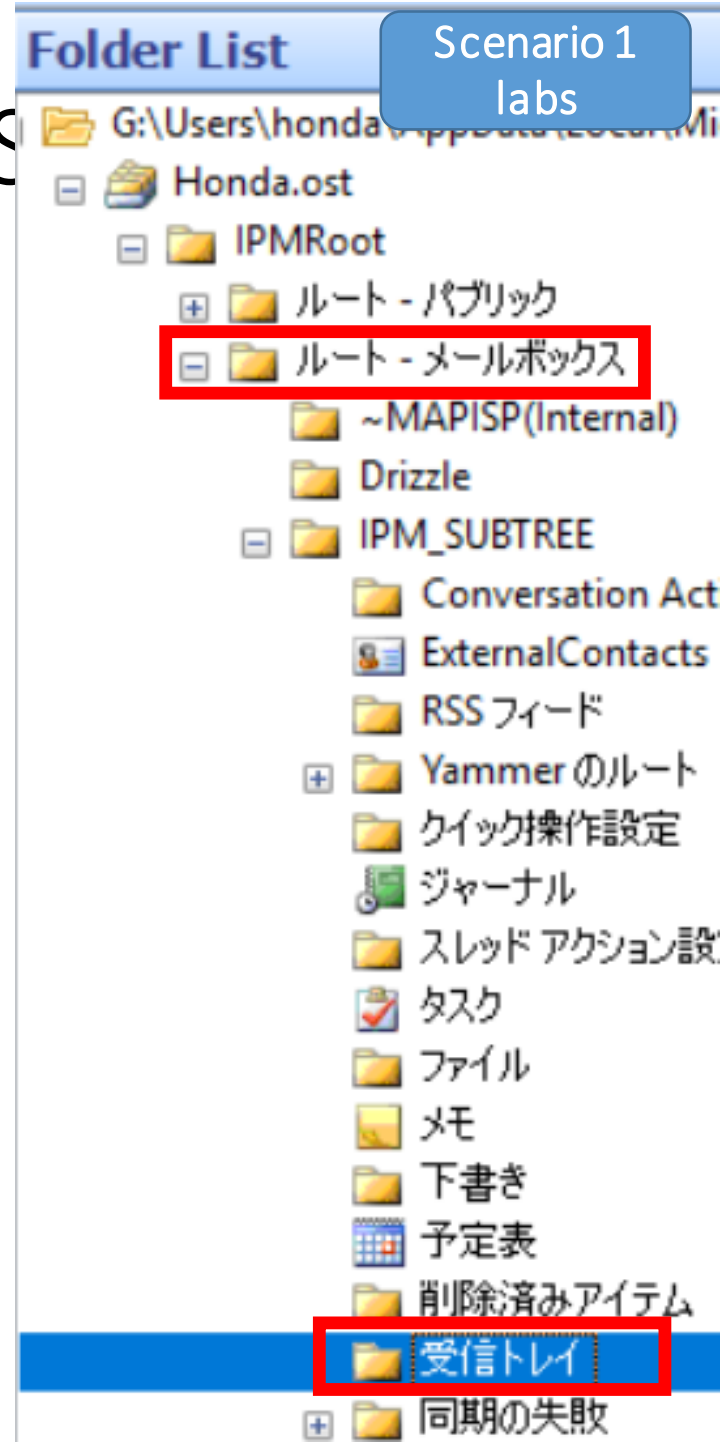
Note that you may need to change the drive letter corresponding to your environment.



Outlook Forensics with SYSTools OS

(4)

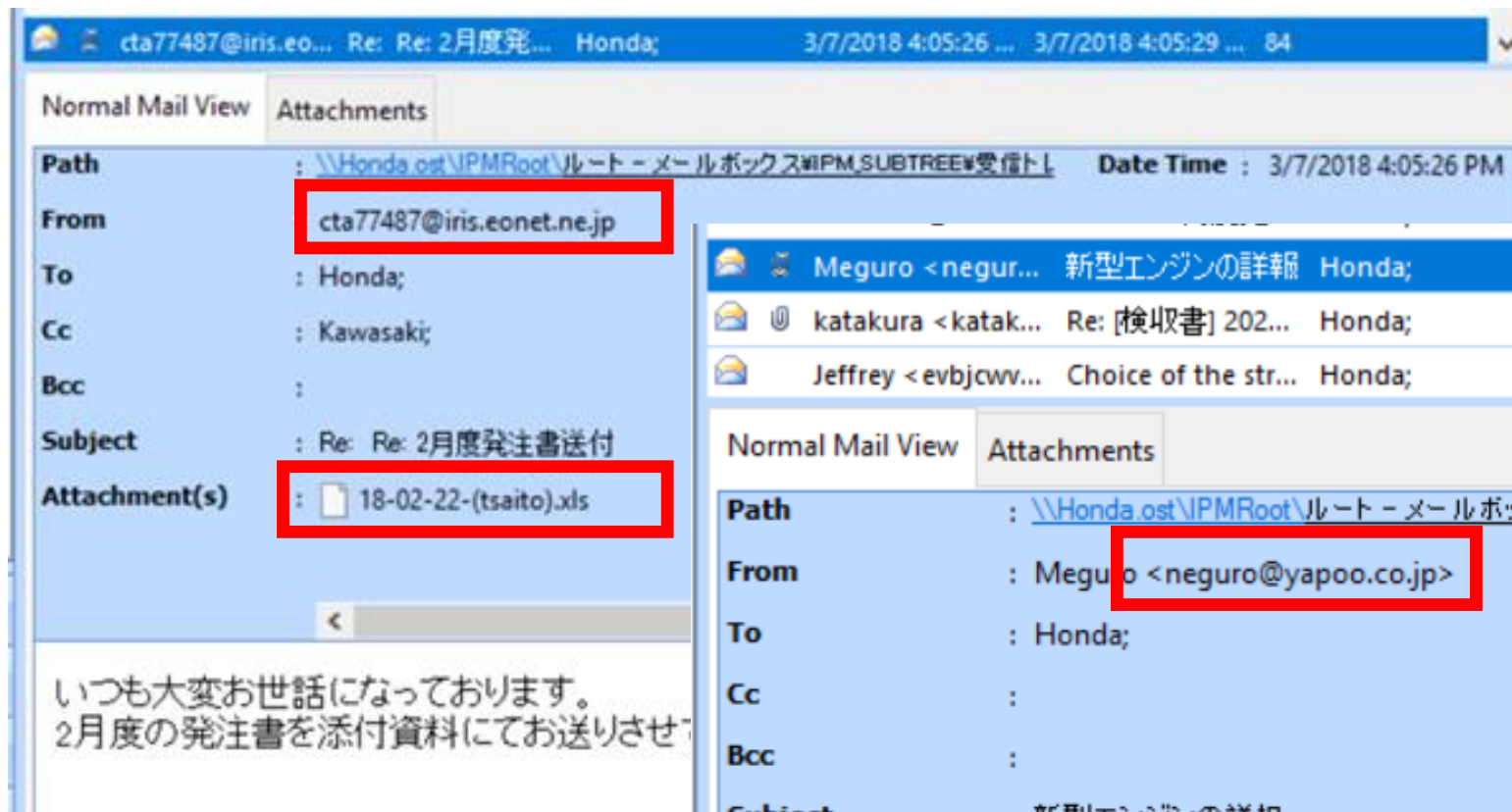
- Follow the direction below to open inbox.
 - IPMRoot -> ルート - メールボックス -> IPM_SUBTREE -> 受信トレイ
 - ルート - メールボックス : root mail box
 - 受信トレイ : Inbox
 - Sorry in Japanese...



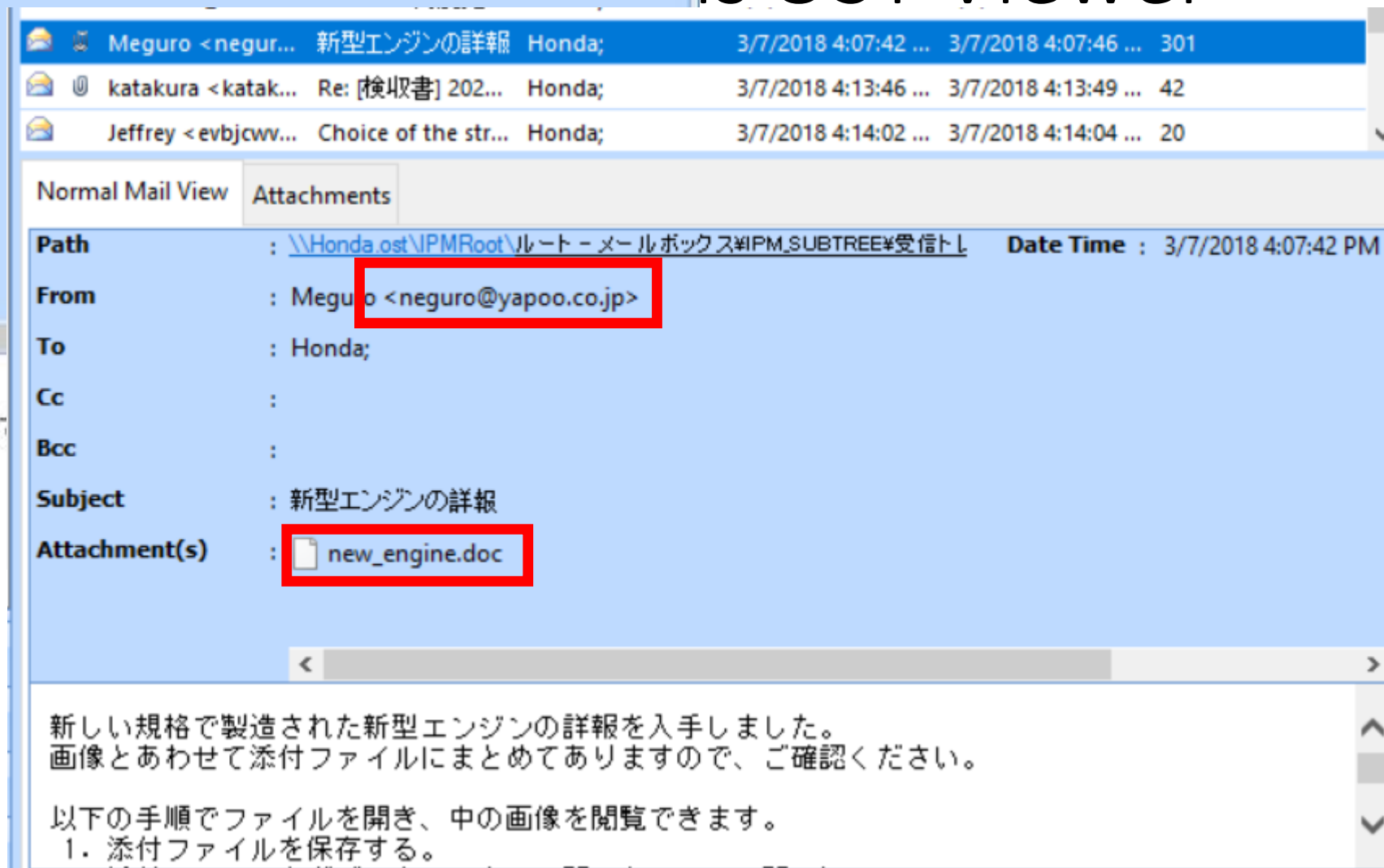
Outlook Forensics with SYSTools OST Viewer (5)

- Let's Investigate E-mails around March 7, 2018 at 4:13 PM because we already know the infection date. We have also found a suspicious filename, which the user opened, named "new_engine.doc".
 - Look for emails with attachments.
 - Or URLs within emails.
- Caution:
 - In the mailbox we are seeing from now on, there are many SPAM mails and sexual topics included in them. Do not look at the mail texts.
 - As a general theory, you should try **not to see the texts** while performing incident response from the privacy point of view.

Is OST Viewer



You can find several suspicious mails in inbox around March 7. But the most suspicious one is the mail on the right figure. You can tell it from the attachment filename.



Outlook Forensics with SYSTools OST Viewer (7)

- If you want to get this mail data, go to the folder below. You can get the mail you are seeing in eml format.
 - %AppData%\CDTPL
 - C:\Users\taro\AppData\Roaming\CDTPL
- Double-click the file, then you can see the message and get the attachment file with Thunderbird like the next page.
 - If you have multiple eml files, open all of them!

Ol

• Sy

File Home Share View

← → ↕ ↗ This PC > Local Disk (C:) > Users > taro > AppData > Roaming > CDTPL

Name	Date modified	Type	Size
SysTools Exchange Recovery	4/30/2018 4:45 PM	File folder	
Temp	5/2/2018 5:33 PM	File folder	
1b5942e9-810c-4cea-9ad4-95e01fe3153...	5/2/2018 5:33 PM	Thunderbird Docu...	402 KB

Mailbox Databa: OneDrive This PC Desktop Documents Downloads Music Pictures Videos Local Disk (C:) usbdisk (E:) システムで予約済み Local Disk (G:) usbdisk (E:) Artifacts BuildingEnvironr old System Volume I tmp Win10x64en

3 items 1 item selected 401 KB

新型エンジンの詳細 - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From Meguro <neguro@yapoo.co.jp> ☆

Subject 新型エンジンの詳細 3/7/2018 4:07 PM

To Honda <> ☆

新しい規格で製造された新型エンジンの詳細を入手しました。
画像とあわせて添付ファイルにまとめてありますので、ご確認ください。

以下の手順でファイルを開き、中の画像を閲覧できます。

1. 添付ファイルを保存する。
2. 添付ファイルをダブルクリックして開く (MS WORDで開く)。
3. 画面上方メッセージバーの[編集を有効にする]をクリックする。
4. 同じくメッセージバーの[コンテンツの有効化]をクリックする。

*画像が大きいのので復号の処理が必要です。

目黒

1 attachment: new_engine.doc 291 KB Save

The result of the RecentDocs

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc

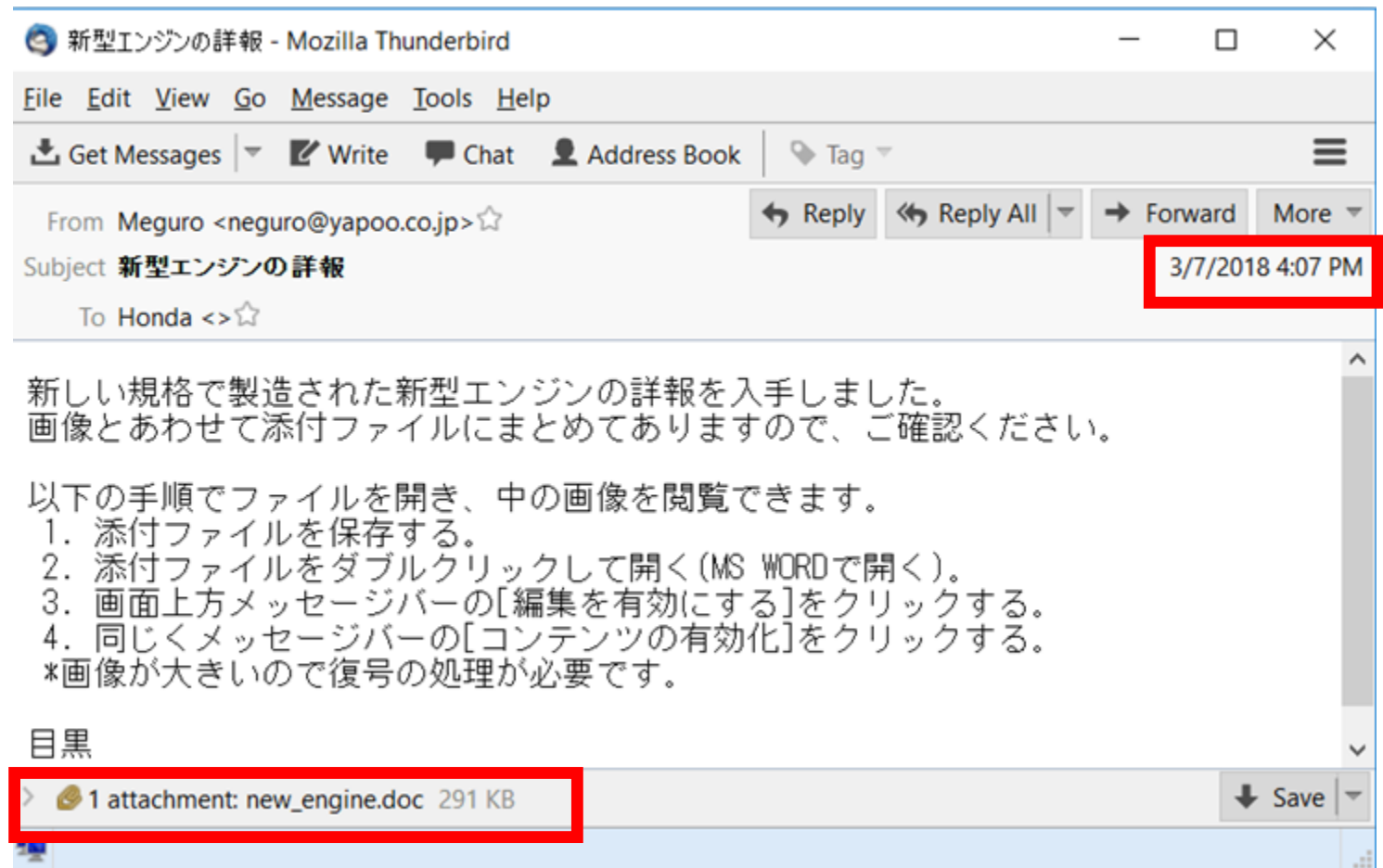
LastWriteTime Wed Mar 7 07:12:38 2018 (UTC)

MRUListEx = 0

0 = new_engine.doc

March 7, 16:12 2018 (JST)

As you saw in the previous chapter, this user opened a document with the same name, and the dates are very close!



Outlook Forensics with SYSTools OST Viewer - Summary

- We got a suspicious mail.
 - The mail was sent at **March 7, 2018 at 4:07 PM (JST)** .
 - The attachment file name is “new_engine.doc”.
- We found that the attachment file was opened, from the investigation we have done on “Open/Save documents” artifacts.
- Save it to Desktop of your VM.
 - We will need to check if the document is really malicious or not.
 - We will check this in the “Exploit analysis” section.