Daniella Boulos, Julianna Russo, Tyler Kaminer
Nov 14, 2024
NIST Case: Email Investigation
Computer Forensics

Use regripper to determine when mozilla thunderbird could have been installed

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r SOFTWARE -p uninstall
Launching uninstall v.20200525
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2021-03-21 20:11:33Z
  Microsoft Update Health Tools v.2.75.0.0

2021-03-10 00:40:27Z
  Microsoft Edge

2021-03-10 00:33:57Z
  Mozilla Maintenance Service v.78.8.1

2021-03-10 00:33:54Z
  Mozilla Thunderbird 78.8.1 (x64 en-US) v.78.8.1
```

Search file directory csv file for thunderbird link files

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ cat file_directory_original.csv | grep -F 'lnk' | grep -i 'thunderbird' | cut -f 1,2

r/r 93410-128-4:        ProgramData/Microsoft/Windows/Start Menu/Programs/Mozilla Thunde
rbird.lnk
r/r 93411-128-4:        Users/Public/Desktop/Mozilla Thunderbird.lnk
```

Use icat to extract thunderbird's link files

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 93410-128-4 >> ../Export
s/Email/'Mozilla Thunderbird (1).lnk'

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 93411-128-4 >> ../Export
s/Email/'Mozilla THunderbird (2).lnk'
```

Use lnkinfo to analyze link files

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Email]
└─$ lnkinfo Mozilla\ Thunderbird\ \(1\).lnk
lnkinfo 20181227

Windows Shortcut information:
        Contains a link target identifier
        Contains a relative path string
        Contains a working directory string

Link information:
        Creation time                   : Mar 10, 2021 00:33:47.666736900 UTC
        Modification time               : Mar 05, 2021 00:44:09.000000000 UTC
        Access time                     : Mar 10, 2021 00:33:52.431631700 UTC
        File size                       : 437744 bytes
        Icon index                      : 0
        Show Window value               : 0x0006adf0
        Hot Key value                   : 44528
        File attribute flags            : 0x00000020
                Should be archived (FILE_ATTRIBUTE_ARCHIVE)
        Drive type                      : Fixed (3)
        Drive serial number             : 0xde4315ea
        Volume label                    :
        Local path                      : C:\Program Files\Mozilla Thunderbird\thunderbi
rd.exe
        Relative path                   : ..\..\..\..\Program Files\Mozilla Thunderbi
rd\thunderbird.exe
        Working directory               : C:\Program Files\Mozilla Thunderbird
```

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Email]
└─$ lnkinfo Mozilla\ THunderbird\ \(2\).lnk
lnkinfo 20181227

Windows Shortcut information:
        Contains a link target identifier
        Contains a relative path string
        Contains a working directory string

Link information:
        Creation time                   : Mar 10, 2021 00:33:47.666736900 UTC
        Modification time               : Mar 05, 2021 00:44:09.000000000 UTC
        Access time                     : Mar 10, 2021 00:33:57.387435500 UTC
        File size                       : 437744 bytes
        Icon index                      : 0
        Show Window value               : 0x0006adf0
        Hot Key value                   : 44528
        File attribute flags            : 0x00000020
                Should be archived (FILE_ATTRIBUTE_ARCHIVE)
        Drive type                      : Fixed (3)
        Drive serial number             : 0xde4315ea
        Volume label                    :
        Local path                      : C:\Program Files\Mozilla Thunderbird\thunderbi
rd.exe
        Relative path                   : ..\..\..\Program Files\Mozilla Thunderbird\thu
nderbird.exe
        Working directory               : C:\Program Files\Mozilla Thunderbird
```

Reference the file directory csv file to find emails

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ cat file_directory_original.csv | grep -i 'outlook' | grep -iE 'inbox|sent|draft' |
cut -f 1,2
r/r 85034-128-3:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/Drafts-1
r/r 93671-128-4:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/Drafts-1.msf
r/r 93647-128-4:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/Drafts.msf
r/r 93677-128-3:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/INBOX
r/r 93634-128-4:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/INBOX.msf
r/r 93847-128-3:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/Sent-1
r/r 93676-128-4:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/Sent-1.msf
r/r 93649-128-4:        Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.defau
lt-release/ImapMail/outlook.office365.com/Sent.msf
```

Use icat to extract emails

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 93677-128-3 >> ../Export
s/Email/INBOX

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 93847-128-3 >> ../Export
s/Email/Sent-1

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 85034-128-3 >> ../Export
s/Email/Drafts-1
```

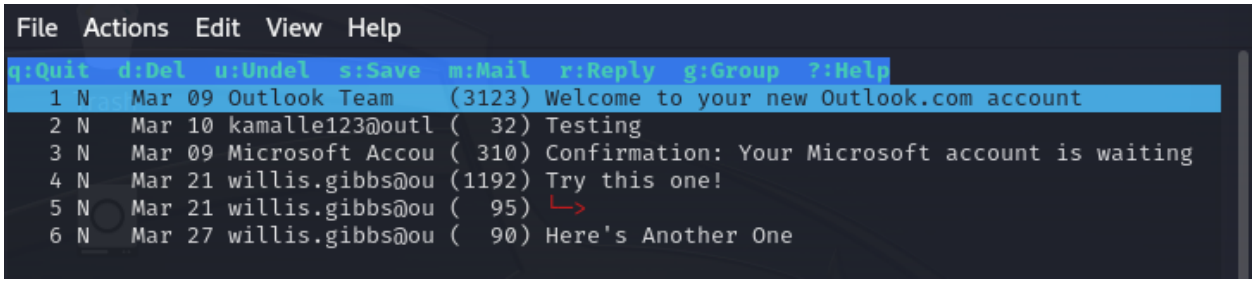
Verify you have the email files

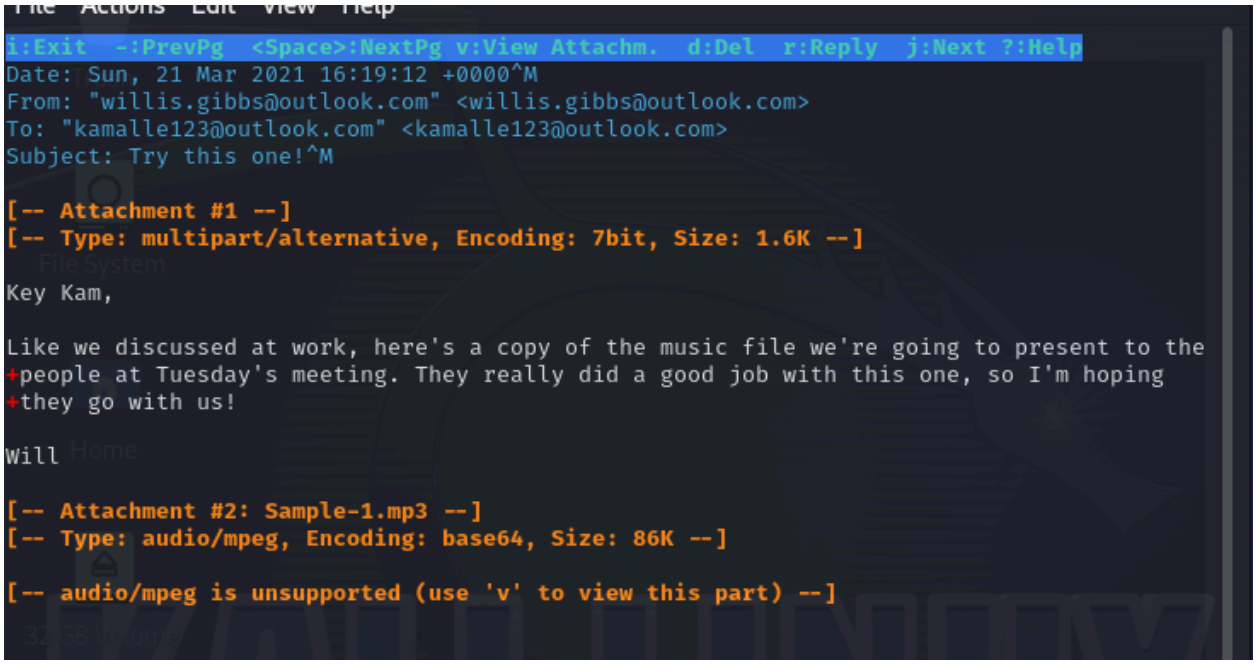
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Email]
└─$ sudo ls
 Drafts-1  'Mozilla Thunderbird (1).lnk'   Sent-1
 INBOX     'Mozilla THunderbird (2).lnk'
```

Use mutt to view Kamryn's emails

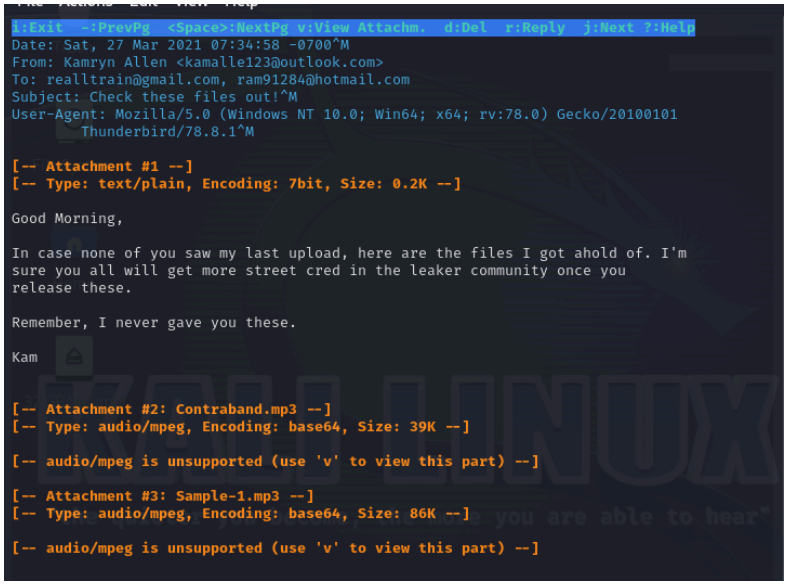
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Email]
└─$ mutt -f INBOX -R

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Email]
└─$ mutt -f Sent-1 -R

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Email]
└─$ mutt -f Drafts-1 -R

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Email]
└─$
```

Use mutt to view Kamryn's inbox





Use mutt to view Kamryn's sent



Use mutt to view Kamryn's draft