

### 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
  Home
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 >> ../Exports/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 >> ../Exports/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.default-release/ImapMail/outlook.office365.com/Drafts-1
r/r 93671-128-4:      Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.default-release/ImapMail/outlook.office365.com/Drafts-1.msf
r/r 93647-128-4:      Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.default-release/ImapMail/outlook.office365.com/Drafts.msf
r/r 93677-128-3:      Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.default-release/ImapMail/outlook.office365.com/INBOX
r/r 93634-128-4:      Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.default-release/ImapMail/outlook.office365.com/INBOX.msf
r/r 93847-128-3:      Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.default-release/ImapMail/outlook.office365.com/Sent-1
r/r 93676-128-4:      Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.default-release/ImapMail/outlook.office365.com/Sent-1.msf
r/r 93649-128-4:      Users/Kamryn/AppData/Roaming/Thunderbird/Profiles/cslktqas.default-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 >> ../Exports/Email/INBOX

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

(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
$ icat -o 104448 ../Case_Materials/Disk_Image_ID-20210327.001 85034-128-3 >> ../Exports/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

```
File Actions Edit View Help
q:Quit d:Del u:Undel s:Save m:Mail r:Reply g:Group ?:Help
1 N Mar 09 Outlook Team (3123) Welcome to your new Outlook.com account
2 N Mar 10 kamalle123@outl ( 32) Testing
3 N Mar 09 Microsoft Accou ( 310) Confirmation: Your Microsoft account is waiting
4 N Mar 21 willis.gibbs@ou (1192) Try this one!
5 N Mar 21 willis.gibbs@ou ( 95)
6 N Mar 27 willis.gibbs@ou ( 90) Here's Another One

File Actions Edit View Help
!:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help
Date: Sun, 21 Mar 2021 16:19:12 +0000^M
From: "willis.gibbs@outlook.com" <willis.gibbs@outlook.com>
To: "kamalle123@outlook.com" <kamalle123@outlook.com>
Subject: Try this one!^M

[-- Attachment #1 --]
[-- Type: multipart/alternative, Encoding: 7bit, Size: 1.6K --]
File System
Key Kam,

Like we discussed at work, here's a copy of the music file we're going to present to the
+people at Tuesday's meeting. They really did a good job with this one, so I'm hoping
+they go with us!

Will Home

[-- Attachment #2: Sample-1.mp3 --]
[-- Type: audio/mpeg, Encoding: base64, Size: 86K --]

[-- audio/mpeg is unsupported (use 'v' to view this part) --]
```

## Use mutt to view Kamryn's sent

```
File Actions Edit View Help
!:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help
Date: Sat, 27 Mar 2021 07:34:58 -0700^M
From: Kamryn Allen <kamalle123@outlook.com>
To: realltrain@gmail.com, ram91284@hotmail.com
Subject: Check these files out!^M
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Thunderbird/78.8.1^M

[-- Attachment #1 --]
[-- Type: text/plain, Encoding: 7bit, Size: 0.2K --]

Good Morning,

In case none of you saw my last upload, here are the files I got ahold of. I'm
sure you all will get more street cred in the leaker community once you
release these.

Remember, I never gave you these.

Kam

[-- Attachment #2: Contraband.mp3 --]
[-- Type: audio/mpeg, Encoding: base64, Size: 39K --]

[-- audio/mpeg is unsupported (use 'v' to view this part) --]

[-- Attachment #3: Sample-1.mp3 --]
[-- Type: audio/mpeg, Encoding: base64, Size: 86K --] you are able to hear"

[-- audio/mpeg is unsupported (use 'v' to view this part) --]
```

Use mutt to view Kamryn's draft

