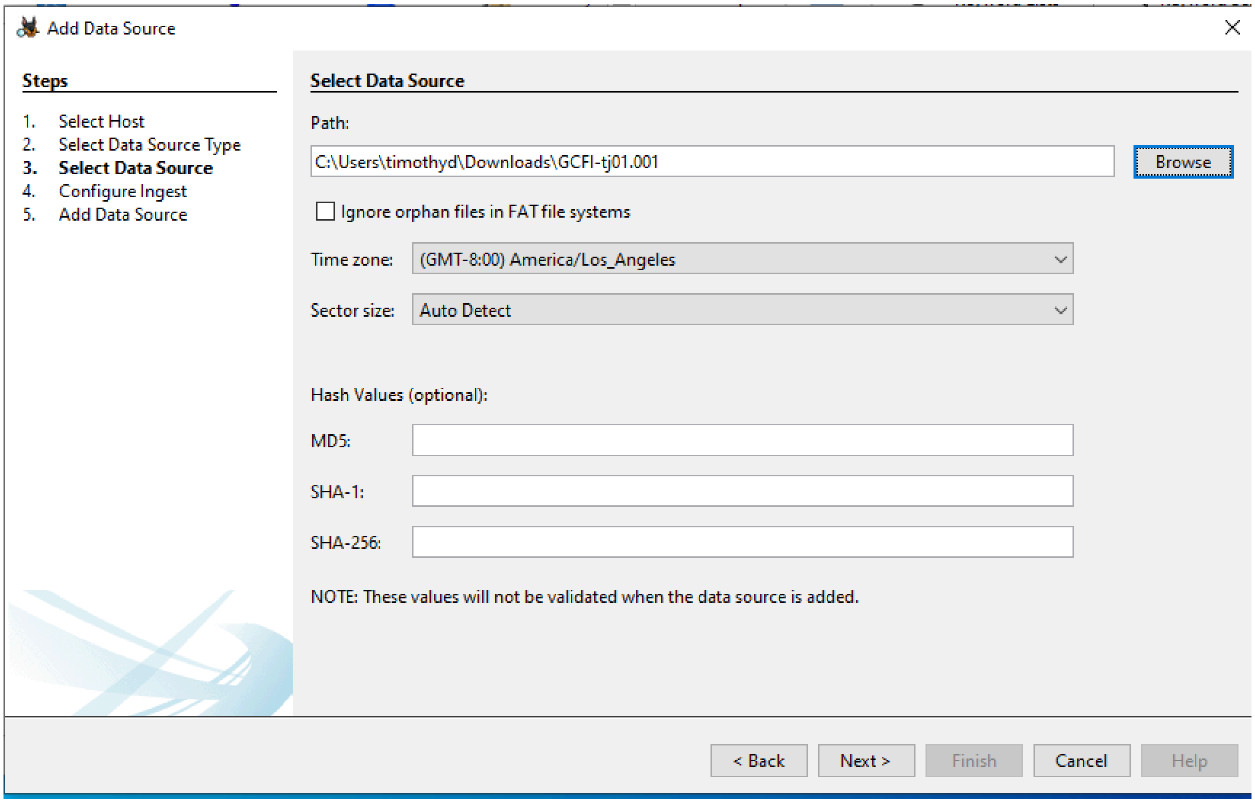
Task 1:



Add Data Source

**Steps**

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

**Select Data Source**

Path: C:\Users\timothyd\Downloads\GCFI-tj01.001

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

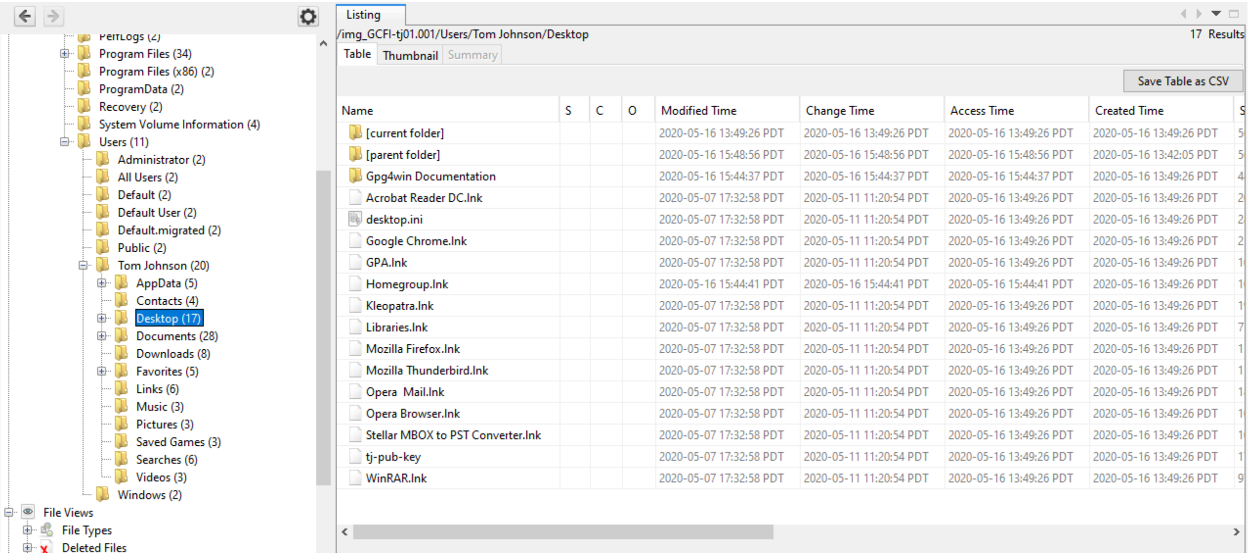
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

In this step, I have created a new case in Autopsy and imported “GCFI-tj01.001" Disk Image.



PerfLogs (2)
Program Files (34)
Program Files (x86) (2)
ProgramData (2)
Recovery (2)
System Volume Information (4)
Users (11)
Administrator (2)
All Users (2)
Default (2)
Default User (2)
Default.migrated (2)
Public (2)
Tom Johnson (20)
AppData (5)
Contacts (4)
Desktop (17)
Documents (28)
Downloads (8)
Favorites (5)
Links (6)
Music (3)
Pictures (3)
Saved Games (3)
Searches (6)
Videos (3)
Windows (2)
File Views
File Types
Deleted Files

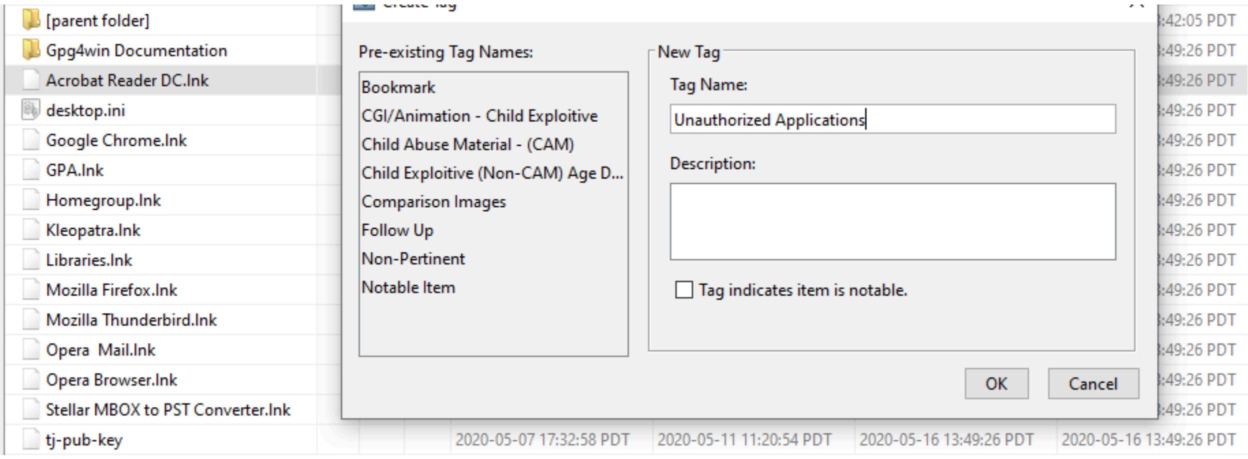
Listing

/img_GCFI-tj01.001/Users/Tom Johnson/Desktop

17 Results

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | S |
|---|---|---|---|---|---|---|---|---|
| [current folder] | | | | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 5 |
| [parent folder] | | | | 2020-05-16 15:48:56 PDT | 2020-05-16 15:48:56 PDT | 2020-05-16 15:48:56 PDT | 2020-05-16 13:42:05 PDT | 5 |
| Gpg4win Documentation | | | | 2020-05-16 15:44:37 PDT | 2020-05-16 15:44:37 PDT | 2020-05-16 15:44:37 PDT | 2020-05-16 13:49:26 PDT | 4 |
| Acrobat Reader DC.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 2 |
| desktop.ini | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 2 |
| Google Chrome.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 2 |
| GPA.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| Homegroup.lnk | | | | 2020-05-16 15:44:41 PDT | 2020-05-16 15:44:41 PDT | 2020-05-16 15:44:41 PDT | 2020-05-16 13:49:26 PDT | 1 |
| Kleopatra.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| Libraries.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 7 |
| Mozilla Firefox.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| Mozilla Thunderbird.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| Opera  Mail.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| Opera Browser.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| Stellar MBOX to PST Converter.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| tj-pub-key | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 1 |
| WinRAR.lnk | | | | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT | 9 |

In this step, I have created the case and expanded the file directory to be in Tom Johnson’s Desktop folder.



| | | | | |
|---|---|---|---|---|
| [parent folder] | | | | :42:05 PDT |
| Gpg4win Documentation | | | | :49:26 PDT |
| Acrobat Reader DC.lnk | | | | :49:26 PDT |
| desktop.ini | | | | :49:26 PDT |
| Google Chrome.lnk | | | | :49:26 PDT |
| GPA.lnk | | | | :49:26 PDT |
| Homegroup.lnk | | | | :49:26 PDT |
| Kleopatra.lnk | | | | :49:26 PDT |
| Libraries.lnk | | | | :49:26 PDT |
| Mozilla Firefox.lnk | | | | :49:26 PDT |
| Mozilla Thunderbird.lnk | | | | :49:26 PDT |
| Opera Mail.lnk | | | | :49:26 PDT |
| Opera Browser.lnk | | | | :49:26 PDT |
| Stellar MBOX to PST Converter.lnk | | | | :49:26 PDT |
| tj-pub-key | 2020-05-07 17:32:58 PDT | 2020-05-11 11:20:54 PDT | 2020-05-16 13:49:26 PDT | 2020-05-16 13:49:26 PDT |

Pre-existing Tag Names:

- Bookmark
- CGI/Animation - Child Exploitive
- Child Abuse Material - (CAM)
- Child Exploitive (Non-CAM) Age D...
- Comparison Images
- Follow Up
- Non-Pertinent
- Notable Item

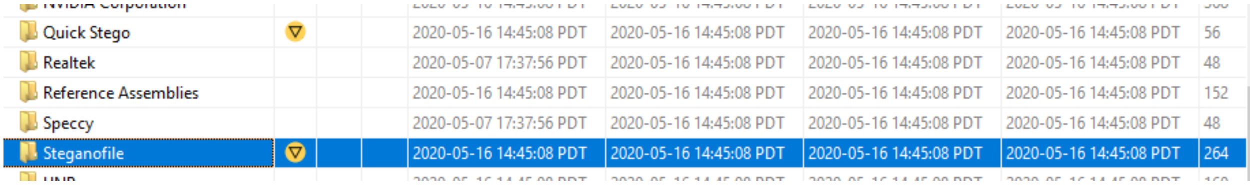
New Tag

Tag Name: Unauthorized Applications

Description:

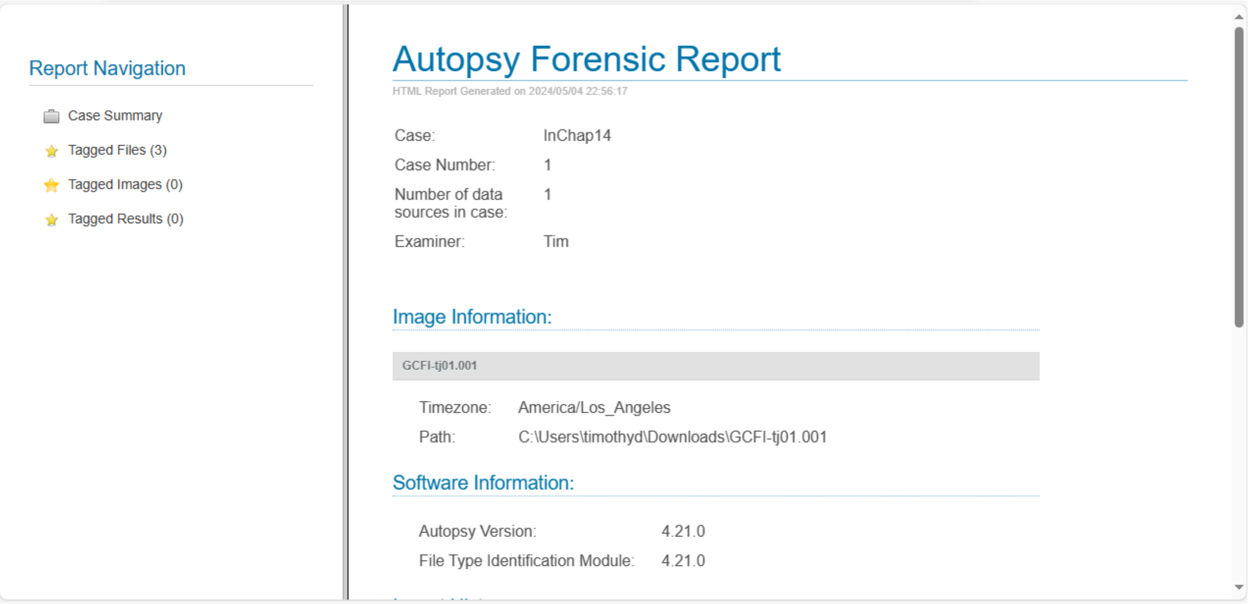
□ Tag indicates item is notable.

Here I am creating a new tag for the “Acrobat Reader DC.lnk” file.



| | | | | | |
|---|---|---|---|---|---|
| Quick Stego | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 56 |
| Realtek | 2020-05-07 17:37:56 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 48 |
| Reference Assemblies | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 152 |
| Speccy | 2020-05-07 17:37:56 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 48 |
| Steganofile | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 2020-05-16 14:45:08 PDT | 264 |

Here I am adding the steganography folders to the tag we just created.



Report Navigation

- Case Summary
- Tagged Files (3)
- Tagged Images (0)
- Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2024/05/04 22:56:17

| | |
|---|---|
| Case: | InChap14 |
| Case Number: | 1 |
| Number of data sources in case: | 1 |
| Examiner: | Tim |

Image Information:

GCFI-tj01.001

| | |
|---|---|
| Timezone: | America/Los_Angeles |
| Path: | C:\Users\timothyd\Downloads\GCFI-tj01.001 |

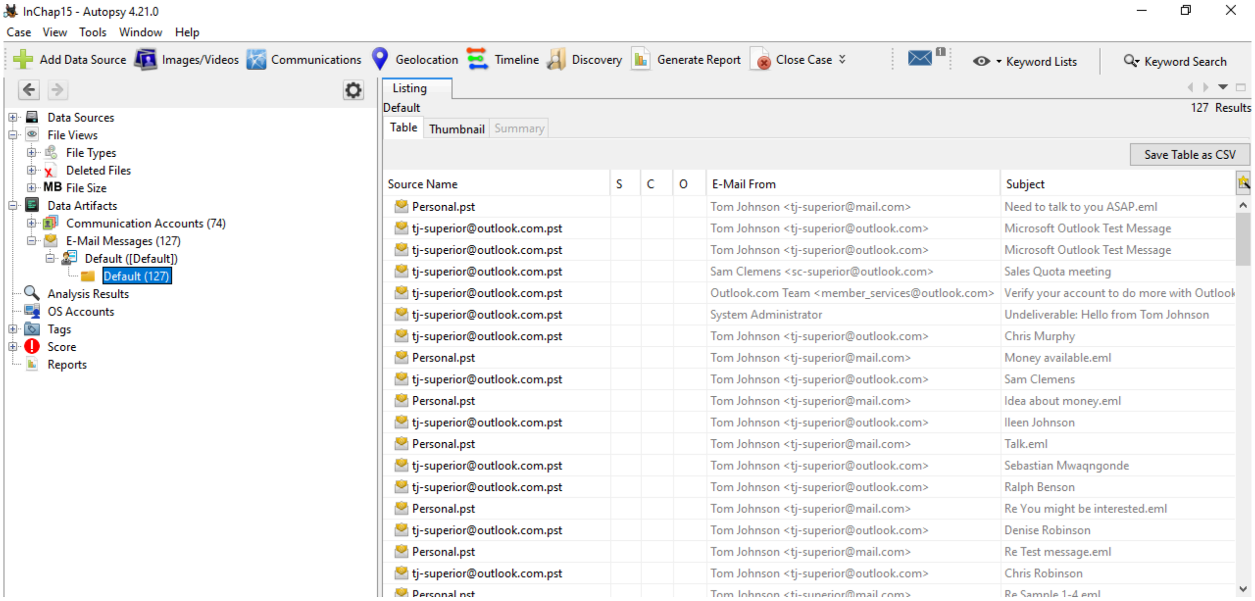
Software Information:

| | |
|---|---|
| Autopsy Version: | 4.21.0 |
| File Type Identification Module: | 4.21.0 |

Here I have created the report.

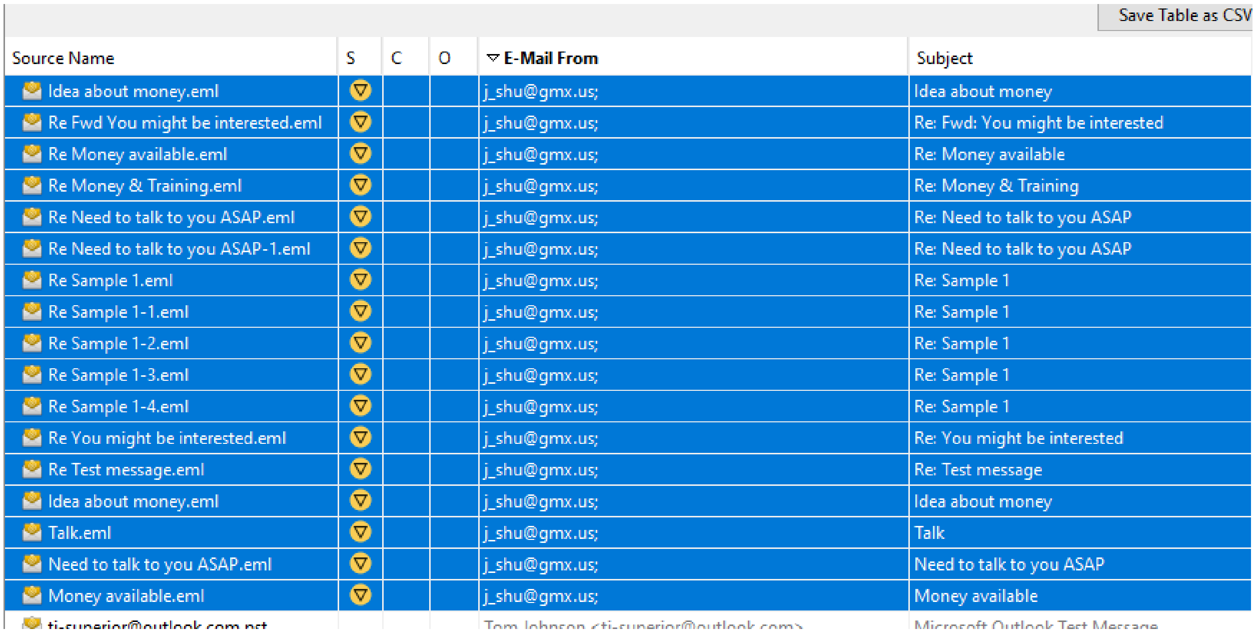
Upon creating a case and adding the “GCFI-tj01.001" image to it, we were able to see all the program files, documents, emails and images that were downloaded onto this computer. This is important to the case because it allows the investigators to understand what activities were conducted on the computer. Being able to analyze these things lets the investigators understand the user's intentions and motives. It also allows for reconstructing the timeline of events that happened on the computer as well.

## Task 2:



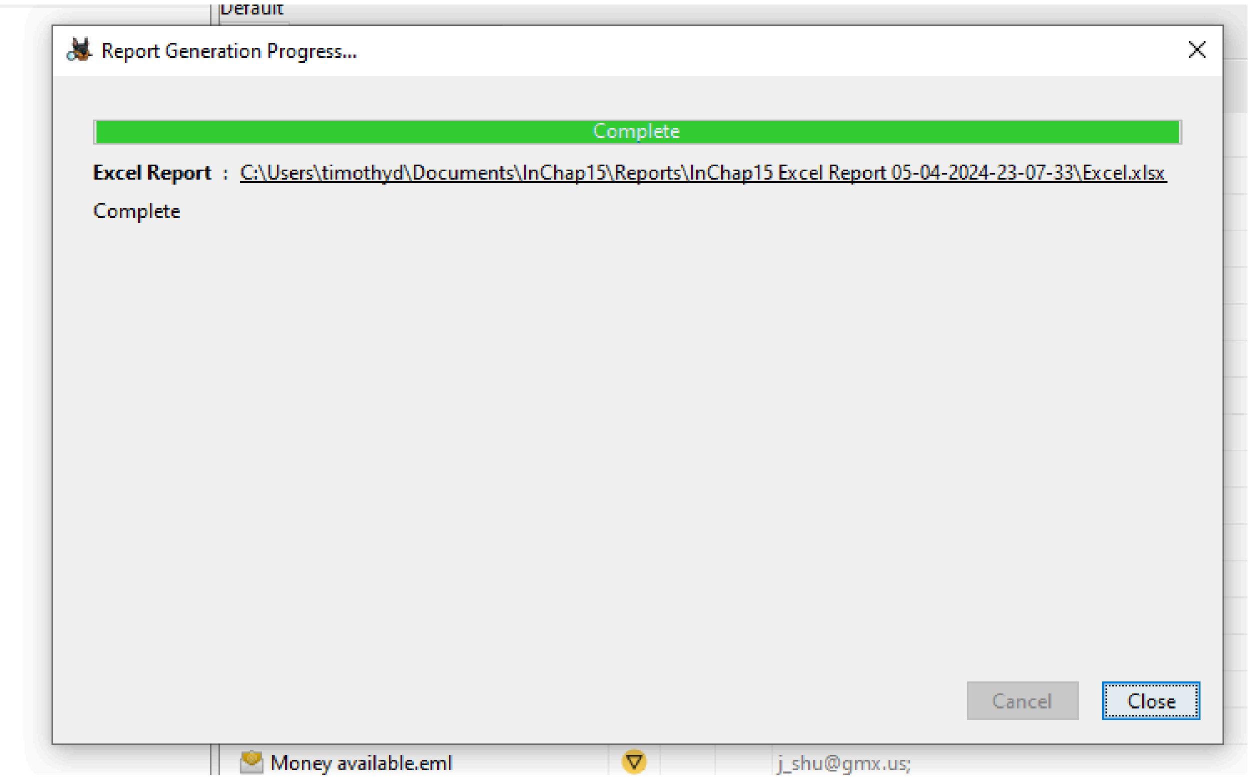
| Source Name | S | C | O | E-Mail From | Subject |
|---|---|---|---|---|---|
| Personal.pst | | | | Tom Johnson <tj-superior@mail.com> | Need to talk to you ASAP.eml |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Microsoft Outlook Test Message |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Microsoft Outlook Test Message |
| tj-superior@outlook.com.pst | | | | Sam Clemens <sc-superior@outlook.com> | Sales Quota meeting |
| tj-superior@outlook.com.pst | | | | Outlook.com Team <member_services@outlook.com> | Verify your account to do more with Outlook |
| tj-superior@outlook.com.pst | | | | System Administrator | Undeliverable: Hello from Tom Johnson |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Chris Murphy |
| Personal.pst | | | | Tom Johnson <tj-superior@mail.com> | Money available.eml |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Sam Clemens |
| Personal.pst | | | | Tom Johnson <tj-superior@mail.com> | Idea about money.eml |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Ileen Johnson |
| Personal.pst | | | | Tom Johnson <tj-superior@mail.com> | Talk.eml |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Sebastian Mwaqngonde |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Ralph Benson |
| Personal.pst | | | | Tom Johnson <tj-superior@mail.com> | Re You might be interested.eml |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Denise Robinson |
| Personal.pst | | | | Tom Johnson <tj-superior@mail.com> | Re Test message.eml |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Chris Robinson |
| Personal.pst | | | | Tom Johnson <tj-superior@mail.com> | Re Sample 1-4.eml |

In this step, I have created a new case and imported “GCFI-tj01.001" Disk Image. I then added “98C3CC2242C784CD544A2908E57D5019” as the md5 hash.



| Source Name | S | C | O | E-Mail From | Subject |
|---|---|---|---|---|---|
| Idea about money.eml | ▽ | | | j_shu@gmx.us; | Idea about money |
| Re Fwd You might be interested.eml | ▽ | | | j_shu@gmx.us; | Re: Fwd: You might be interested |
| Re Money available.eml | ▽ | | | j_shu@gmx.us; | Re: Money available |
| Re Money & Training.eml | ▽ | | | j_shu@gmx.us; | Re: Money & Training |
| Re Need to talk to you ASAP.eml | ▽ | | | j_shu@gmx.us; | Re: Need to talk to you ASAP |
| Re Need to talk to you ASAP-1.eml | ▽ | | | j_shu@gmx.us; | Re: Need to talk to you ASAP |
| Re Sample 1.eml | ▽ | | | j_shu@gmx.us; | Re: Sample 1 |
| Re Sample 1-1.eml | ▽ | | | j_shu@gmx.us; | Re: Sample 1 |
| Re Sample 1-2.eml | ▽ | | | j_shu@gmx.us; | Re: Sample 1 |
| Re Sample 1-3.eml | ▽ | | | j_shu@gmx.us; | Re: Sample 1 |
| Re Sample 1-4.eml | ▽ | | | j_shu@gmx.us; | Re: Sample 1 |
| Re You might be interested.eml | ▽ | | | j_shu@gmx.us; | Re: You might be interested |
| Re Test message.eml | ▽ | | | j_shu@gmx.us; | Re: Test message |
| Idea about money.eml | ▽ | | | j_shu@gmx.us; | Idea about money |
| Talk.eml | ▽ | | | j_shu@gmx.us; | Talk |
| Need to talk to you ASAP.eml | ▽ | | | j_shu@gmx.us; | Need to talk to you ASAP |
| Money available.eml | ▽ | | | j_shu@gmx.us; | Money available |
| tj-superior@outlook.com.pst | | | | Tom Johnson <tj-superior@outlook.com> | Microsoft Outlook Test Message |

Here, I have selected all the emails that include “GMX” in the sender. Then I have added the “GMX Email” tag to them.



Complete

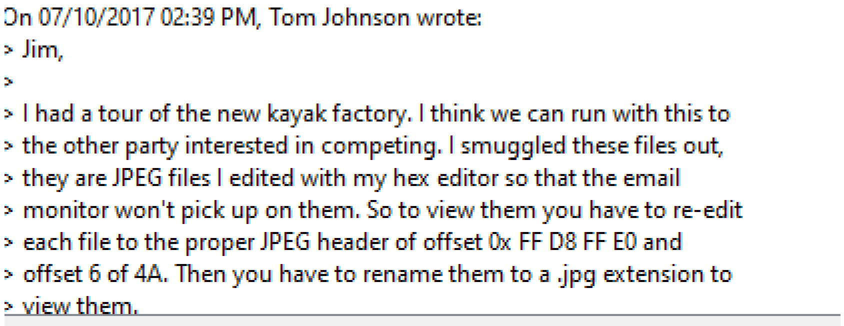
**Excel Report** : C:\Users\timothyd\Documents\InChap15\Reports\InChap15 Excel Report 05-04-2024-23-07-33\Excel.xlsx

Complete

In this step, I have created an excel report configuring all tags.

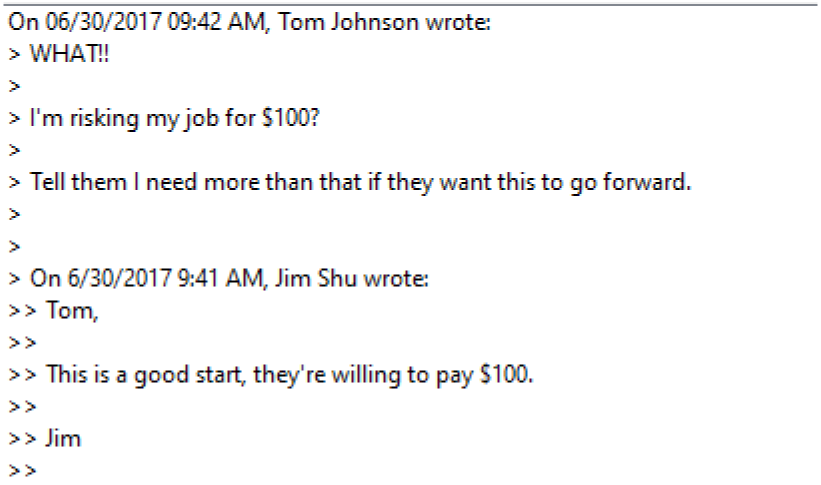
The methods that we used to obtain the emails was using Autopsy to create a case and add the “GCFI-tj1.001" image as a data source. Then we added “98C3CC2242C784CD544A2908E57D5019” as the hash for validation and chain of custody proof. When creating the case, we deselected all the ingest modules besides “Email Parser”. From here, we were able to access all the emails that were on Mr.Shu’s computer. We specifically looked for emails that contained “GMX” in them by sorting the emails and then putting tabs on any of them that included “GMX” in the email address.

We were able to search through all of Mr.Shu’s emails that contained “GMX” in the email address. In an email from Tom Johnson to Mr.Shu, Mr.Johnson is explaining to Mr.Shu how he has toured the new kayak factory and took a couple of pictures. He is planning to sneak some pictures out and send them to the other parties competing.



```
On 07/10/2017 02:39 PM, Tom Johnson wrote:
> Jim,
>
> I had a tour of the new kayak factory. I think we can run with this to
> the other party interested in competing. I smuggled these files out,
> they are JPEG files I edited with my hex editor so that the email
> monitor won't pick up on them. So to view them you have to re-edit
> each file to the proper JPEG header of offset 0x FF D8 FF E0 and
> offset 6 of 4A. Then you have to rename them to a .jpg extension to
> view them.
```

They then seem to have some further talks about investments. Mr.Shu is trying to get the investors to put down more money and is constantly communicating this to Mr.Johnson. Mr.Johnson knows what he is doing may cost him his job but he is still willing to go forward with it if it allows him to receive more money. Mr.Shu is eventually able to get the investors to go up to $500.



```
On 06/30/2017 09:42 AM, Tom Johnson wrote:
> WHAT!!
>
> I'm risking my job for $100?
>
> Tell them I need more than that if they want this to go forward.
>
>
> On 6/30/2017 9:41 AM, Jim Shu wrote:
>> Tom,
>>
>> This is a good start, they're willing to pay $100.
>>
>> Jim
>>
```

The chain of custody was maintained because when creating the case, we added “98C3CC2242C784CD544A2908E57D5019” as the hash for the image. This was for chain of custody proof because it gives this image and unique ID. After completing my investigation, I closed Autopsy ensured my computer was locked. This makes sure that the case and the image of Mr.Shu’s computer will not be tampered with.