Maria Valencia

CSC 153

Lab 14 & 15

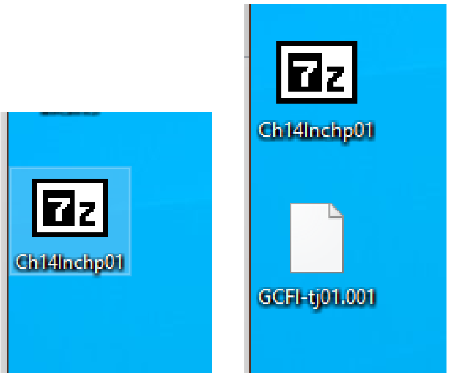
Report Writing and Testimony

Task 1 – Generate Report Findings

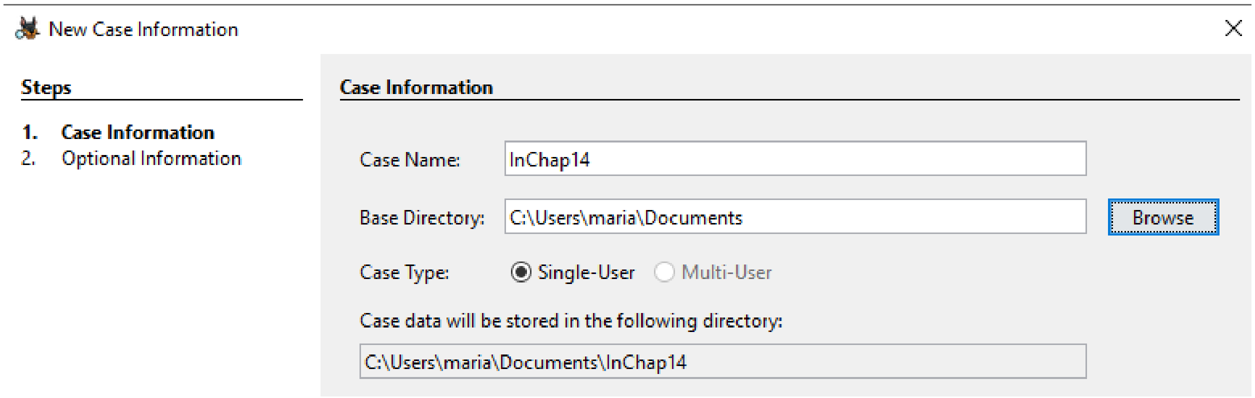
In this task, I will analyze a subject image and collect findings using autopsy. The findings will then be exported as a report that can be included within testimony.

Step 1: Collect Image and Create Case

I downloaded the "Ch14Inchp01.exe" to my windows VM and extracted the GCFI-tj01.001 image by double clicking the executable.



I started Autopsy and created a new case named "InChap14" with my name as the investigator.


New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

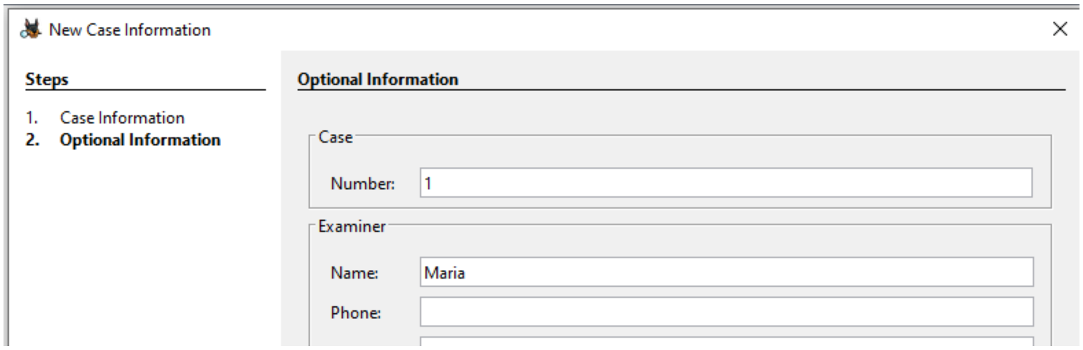
Case Name: InChap14

Base Directory: C:\Users\maria\Documents

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\maria\Documents\InChap14



Case

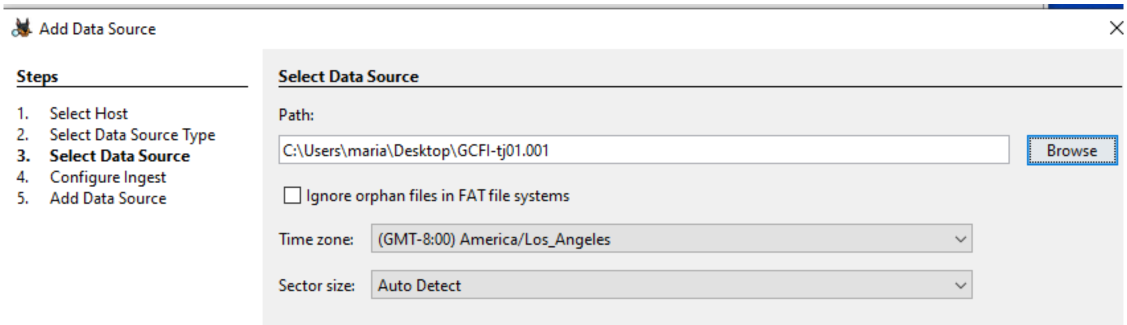
Number: 1

Examiner

Name: Maria

Phone:

Next, I imported the GCFI-tj01.001 Disk Image to the case data sources. I deselected all ingest modules and selected “File Type Identification” module.

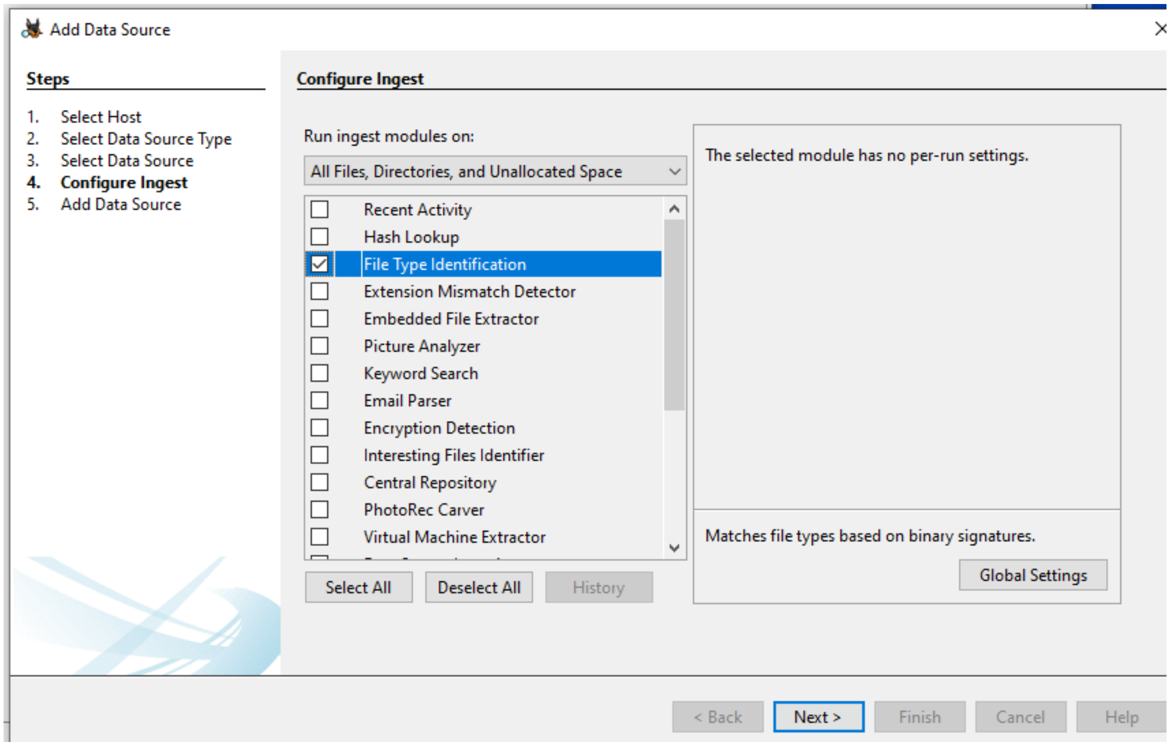


Path: C:\Users\maria\Desktop\GCFI-tj01.001

□ Ignore orphan files in FAT file systems

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

Sector size: Auto Detect



Run ingest modules on: All Files, Directories, and Unallocated Space

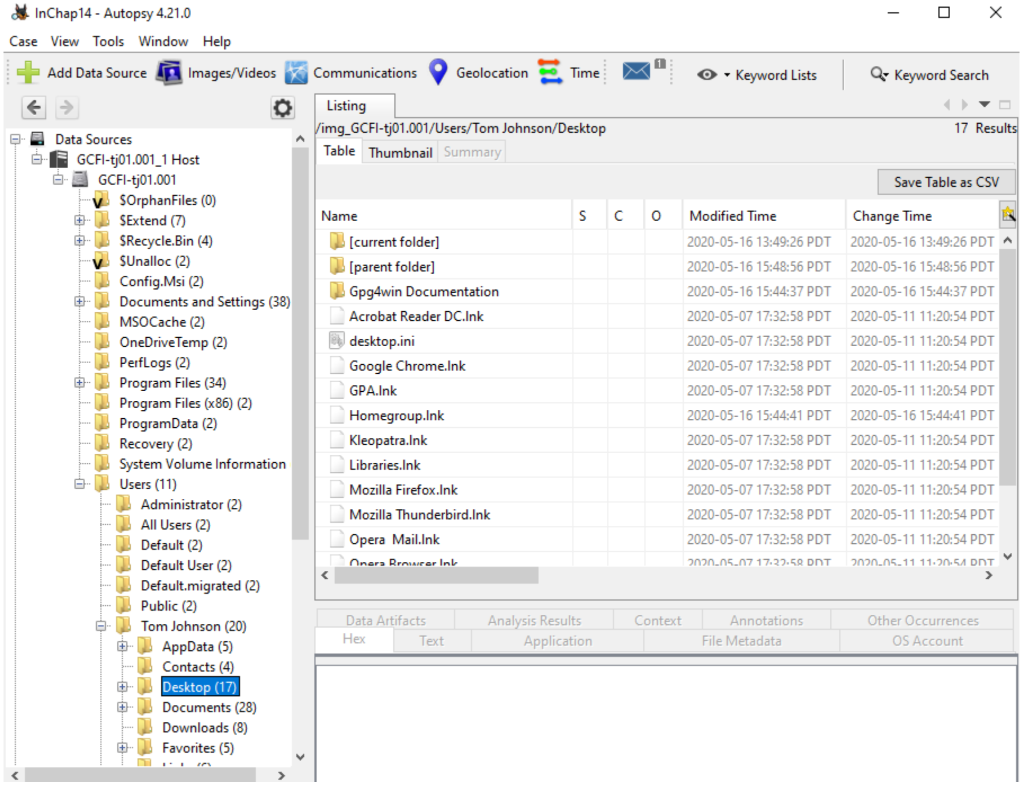
- □ Recent Activity
- □ Hash Lookup
- ☑ File Type Identification
- □ Extension Mismatch Detector
- □ Embedded File Extractor
- □ Picture Analyzer
- □ Keyword Search
- □ Email Parser
- □ Encryption Detection
- □ Interesting Files Identifier
- □ Central Repository
- □ PhotoRec Carver
- □ Virtual Machine Extractor

The selected module has no per-run settings.

Matches file types based on binary signatures.

Step 2: Identify and Tag Evidence

With the case created, image sourced and analyzed, I expanded the Data Sources menu in the left pane file tree. Then, i expanded the GCFFI-tj01.001, Users, and Tom Johnson folders then clicked on Desktop to display its contents.

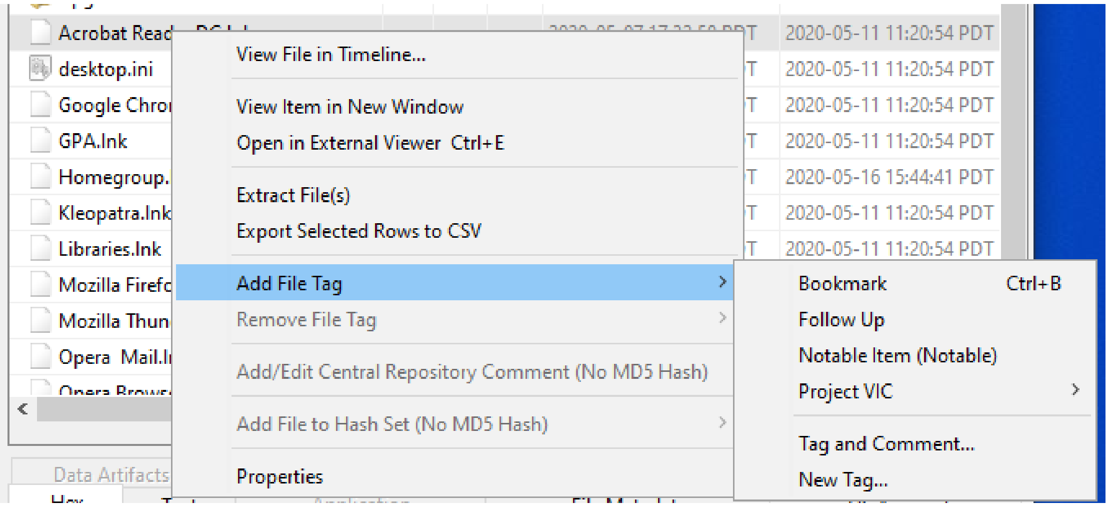


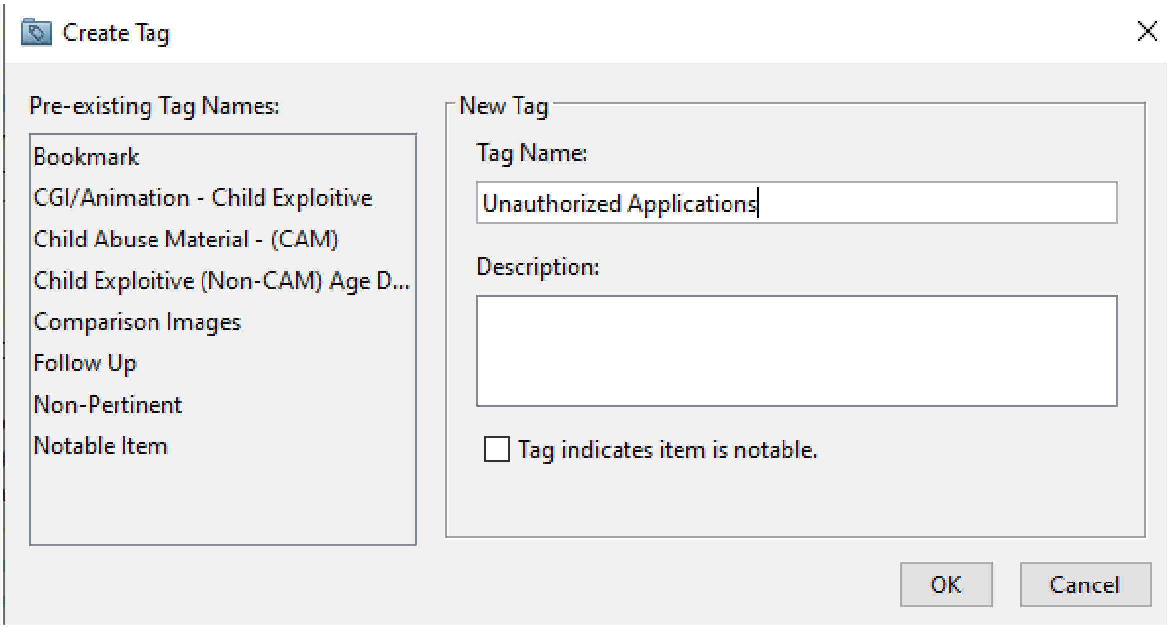
/img_GCFI-tj01.001/Users/Tom Johnson/Desktop

17 Results

Name	S	C	O	Modified Time	Change Time
[current folder]				2020-05-16 13:49:26 PDT	2020-05-16 13:49:26 PDT
[parent folder]				2020-05-16 15:48:56 PDT	2020-05-16 15:48:56 PDT
Gpg4win Documentation				2020-05-16 15:44:37 PDT	2020-05-16 15:44:37 PDT
Acrobat Reader DC.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
desktop.ini				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
Google Chrome.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
GPA.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
Homegroup.lnk				2020-05-16 15:44:41 PDT	2020-05-16 15:44:41 PDT
Kleopatra.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
Libraries.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
Mozilla Firefox.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
Mozilla Thunderbird.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
Opera Mail.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT
Opera Browser.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT

From within the Result Viewer pane, I tag the “Acrobat Reader DC.lnk” file and created a new tag name “Unauthorized Applications” and tagged the file.





Create Tag

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

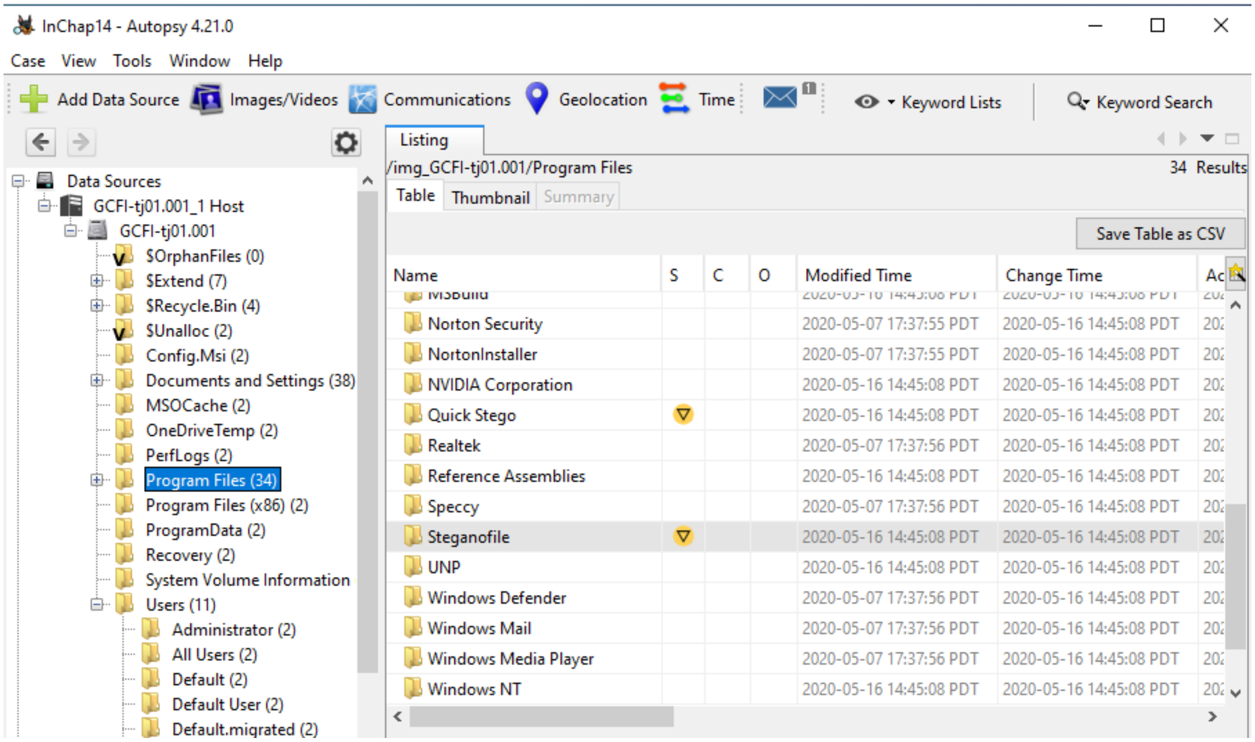
New Tag

Tag Name: Unauthorized Applications

Description:

☐ Tag indicates item is notable.

Using the Tree Viewer pane, I navigated to “Program Files” and added any steganography application folders to the Unauthorized Applications tag.



InChap14 - Autopsy 4.21.0

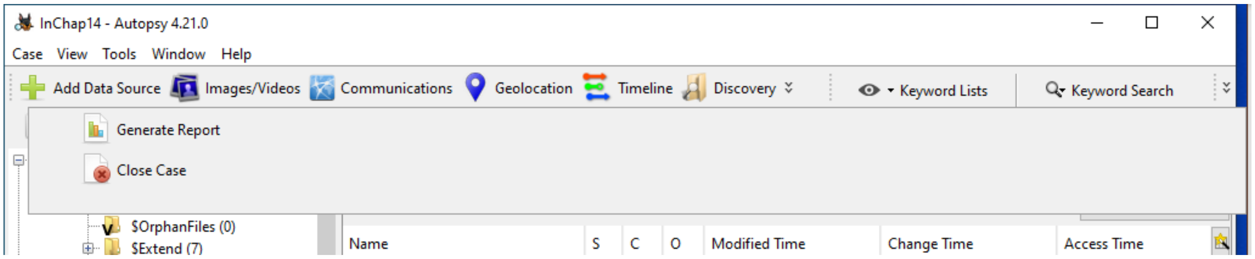
- Data Sources
  - GCFI-tj01.001_1 Host
    - GCFI-tj01.001
      - $OrphanFiles (0)
      - $Extend (7)
      - $Recycle.Bin (4)
      - $Unalloc (2)
      - Config.Msi (2)
      - Documents and Settings (38)
      - MSOCache (2)
      - OneDriveTemp (2)
      - PerfLogs (2)
      - Program Files (34)
      - Program Files (x86) (2)
      - ProgramData (2)
      - Recovery (2)
      - System Volume Information
      - Users (11)
        - Administrator (2)
        - All Users (2)
        - Default (2)
        - Default User (2)
        - Default.migrated (2)

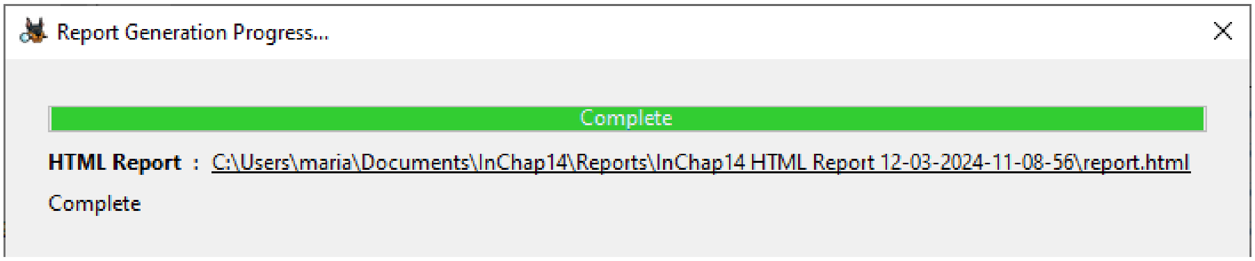
/img_GCFI-tj01.001/Program Files 34 Results

Name	S	C	O	Modified Time	Change Time	Ac
MSBuild				2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	202
Norton Security				2020-05-07 17:37:55 PDT	2020-05-16 14:45:08 PDT	202
NortonInstaller				2020-05-07 17:37:55 PDT	2020-05-16 14:45:08 PDT	202
NVIDIA Corporation				2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	202
Quick Stego	▽			2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	202
Realtek				2020-05-07 17:37:56 PDT	2020-05-16 14:45:08 PDT	202
Reference Assemblies				2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	202
Speccy				2020-05-07 17:37:56 PDT	2020-05-16 14:45:08 PDT	202
Steganofile	▽			2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	202
UNP				2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	202
Windows Defender				2020-05-07 17:37:56 PDT	2020-05-16 14:45:08 PDT	202
Windows Mail				2020-05-07 17:37:56 PDT	2020-05-16 14:45:08 PDT	202
Windows Media Player				2020-05-07 17:37:56 PDT	2020-05-16 14:45:08 PDT	202
Windows NT				2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	202

Step 3: Generate Report

With the unauthorized applications tagged, I pressed the “Generate Report” in the top tool bar.

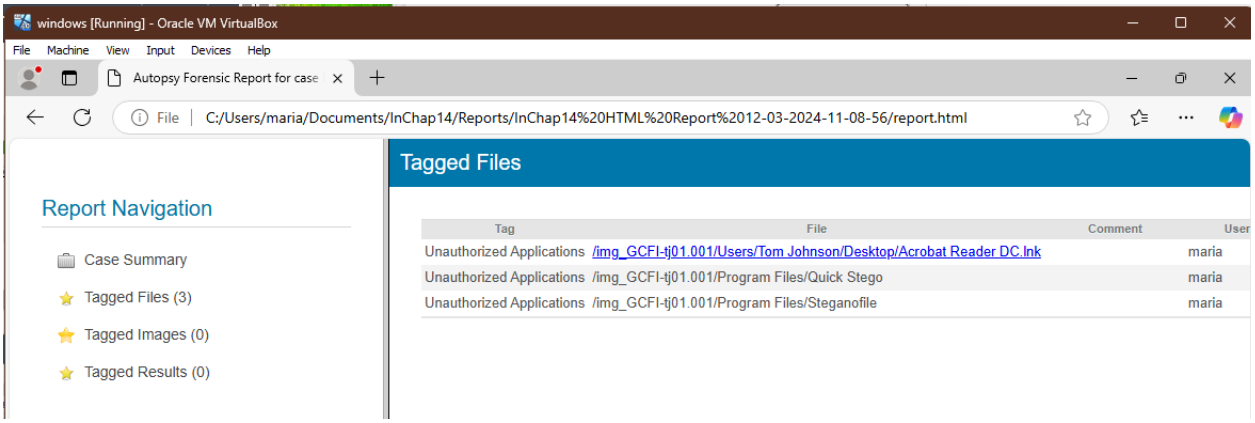




HTML Report : C:\Users\maria\Documents\InChap14\Reports\InChap14 HTML Report 12-03-2024-11-08-56\report.html

Complete

After, I navigated to the report and reviewed its contents.


windows [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Autopsy Forensic Report for case
File
C:/Users/maria/Documents/InChap14/Reports/InChap14%20HTML%20Report%2012-03-2024-11-08-56/report.html
Report Navigation
Case Summary
Tagged Files (3)
Tagged Images (0)
Tagged Results (0)

Tagged Files

Tag	File	Comment	User
Unauthorized Applications	/img_GCFI-tj01.001/Users/Tom Johnson/Desktop/Acrobat Reader DC.lnk		maria
Unauthorized Applications	/img_GCFI-tj01.001/Program Files/Quick Stego		maria
Unauthorized Applications	/img_GCFI-tj01.001/Program Files/Steganofile		maria

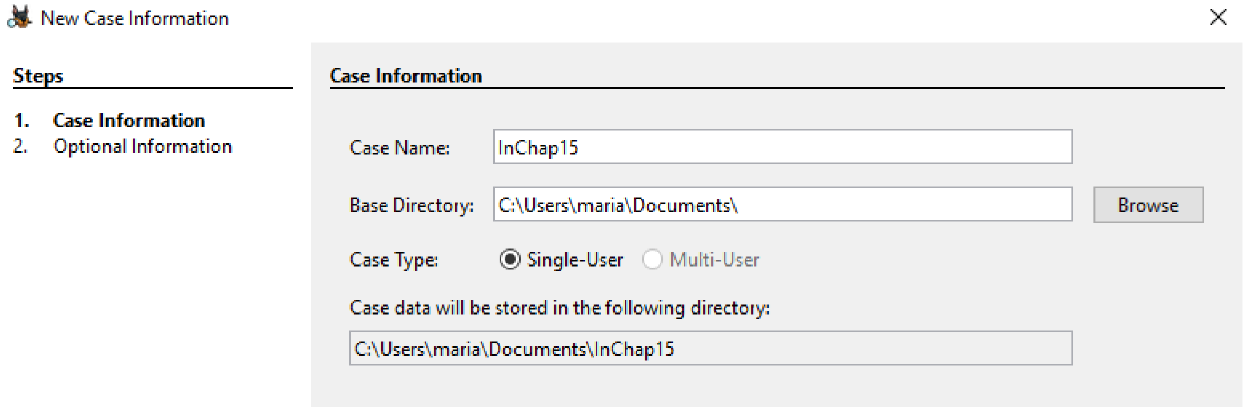
In this task, I conducted a forensic examination of unauthorized file types and prepared a report. I used autopsy to tag certain files and used the generate report feature to generate a report of the tagged “unauthorized applications”. Then, an HTML report was generated, in it were three tagged files. Although we cannot see anything besides the files, seeing the files itself is important. They are important because they will make extracting data easier as we know where to look now.

Task 2 – Preparing Evidence for Testimony

In this task, I will gather emails from a forensic image and prepare testimony describing how I extracted emails, their contents, and how chain of custody was maintained.

Step 1: Obtain Image and Create Case

I used the same file from step 1 of task 1 in this step. The only difference is that I created a new case in Autopsy called “inChap15”, with my name still being in the investigator field.



New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

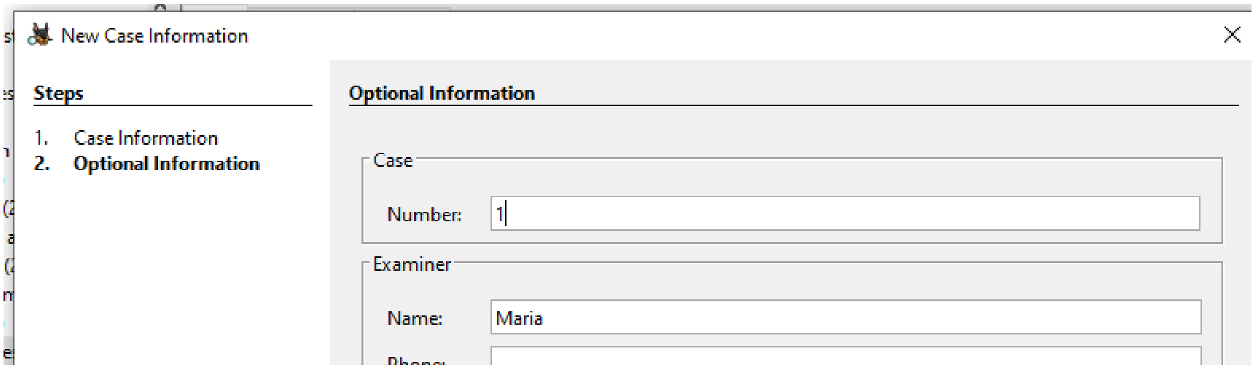
Case Name: InChap15

Base Directory: C:\Users\maria\Documents\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\maria\Documents\InChap15



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

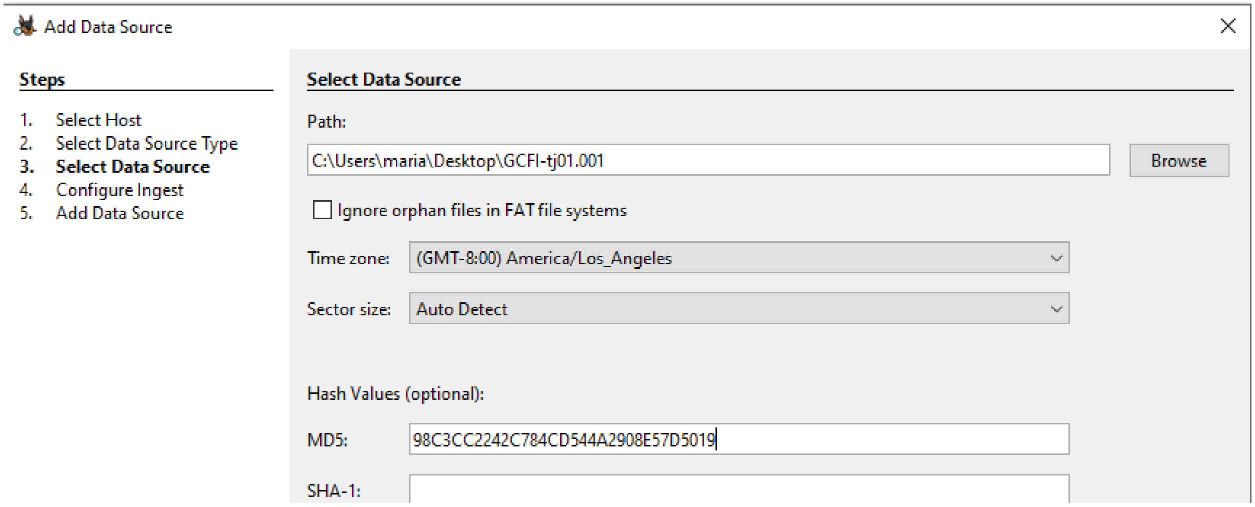
Number: 1

Examiner

Name: Maria

Phone:

Once the case was created, I added the “GCFI-tj01.001” image as the data source with the hash "98C3CC2242C784CD544A2908E57D5019” for validation and chain of custody proof. Then, i only ingested the “Email Parser”.



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\maria\Desktop\GCFI-tj01.001

□ Ignore orphan files in FAT file systems

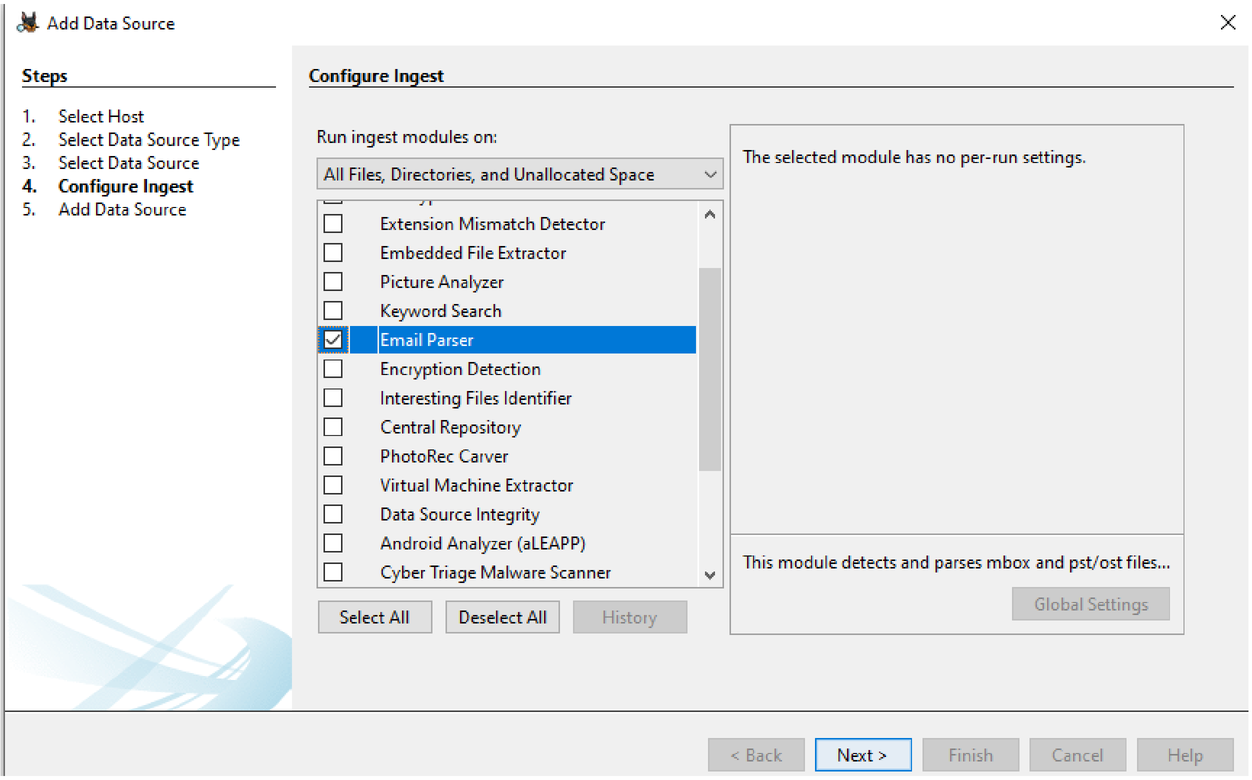
Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

MD5: 98C3CC2242C784CD544A2908E57D5019

SHA-1:



Add Data Source

Steps

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

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

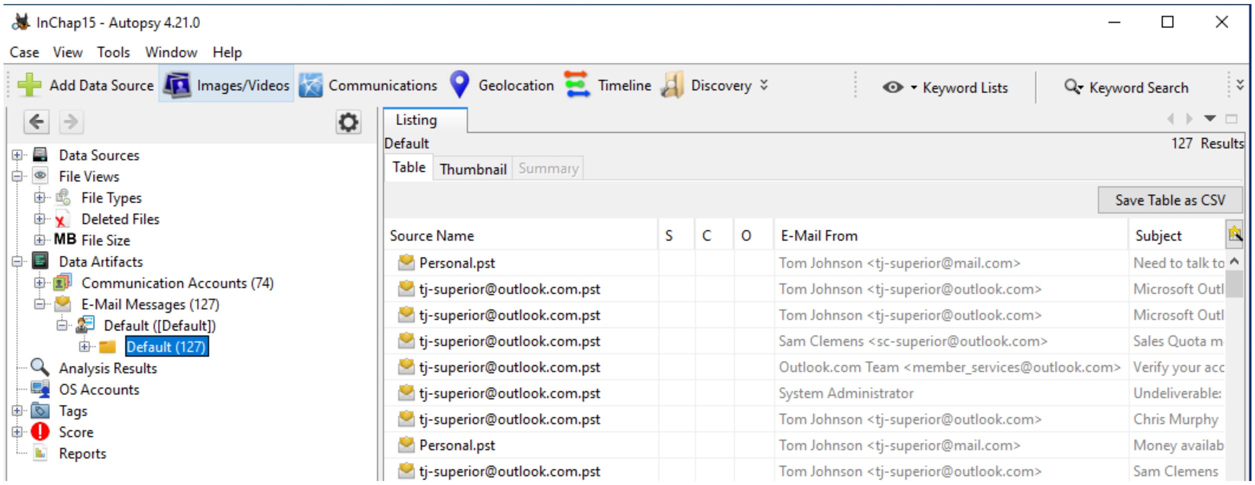
□ Extension Mismatch Detector
□ Embedded File Extractor
□ Picture Analyzer
□ Keyword Search
☑ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Central Repository
□ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity
□ Android Analyzer (aLEAPP)
□ Cyber Triage Malware Scanner

The selected module has no per-run settings.

This module detects and parses mbox and pst/ost files...

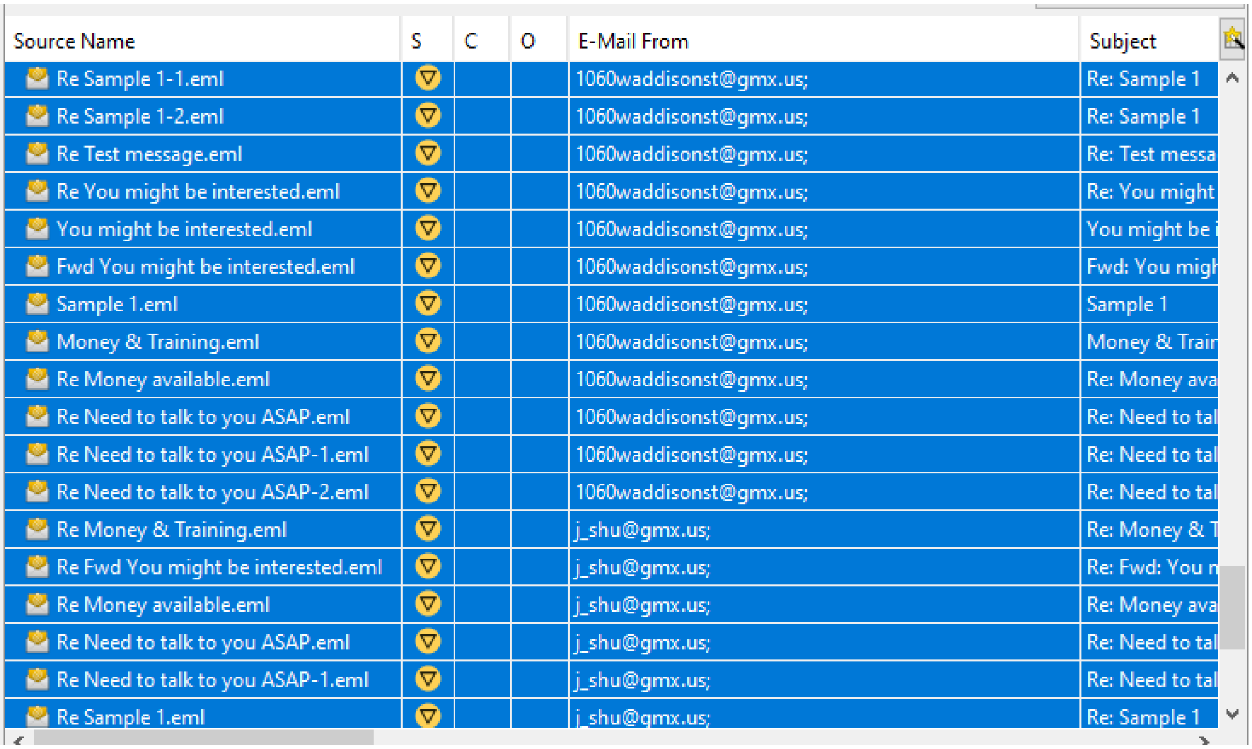
Step 2: Analyze Emails

Once the case was created and the email parser analyzes emails. I navigated to “Data Artifacts”, “E-Mail Messages”, and “Default” folders to identify all emails found in the image.



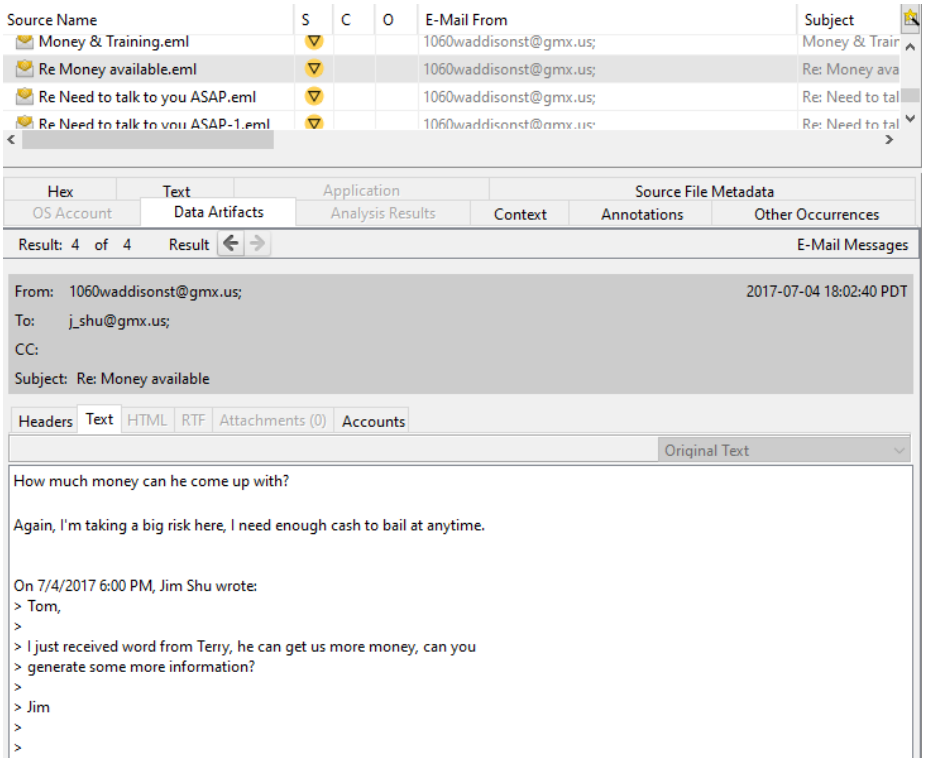
Source Name	S	C	O	E-Mail From	Subject
Personal.pst				Tom Johnson <tj-superior@mail.com>	Need to talk to
tj-superior@outlook.com.pst				Tom Johnson <tj-superior@outlook.com>	Microsoft Outl
tj-superior@outlook.com.pst				Tom Johnson <tj-superior@outlook.com>	Microsoft Outl
tj-superior@outlook.com.pst				Sam Clemens <sc-superior@outlook.com>	Sales Quota m
tj-superior@outlook.com.pst				Outlook.com Team <member_services@outlook.com>	Verify your acc
tj-superior@outlook.com.pst				System Administrator	Undeliverable:
tj-superior@outlook.com.pst				Tom Johnson <tj-superior@outlook.com>	Chris Murphy
Personal.pst				Tom Johnson <tj-superior@mail.com>	Money availab
tj-superior@outlook.com.pst				Tom Johnson <tj-superior@outlook.com>	Sam Clemens

Next, I selected all emails with anyone at the gmx.us email address and tagged with the label “GMX Email”.



Source Name	S	C	O	E-Mail From	Subject
Re Sample 1-1.eml	▽			1060waddisonst@gmx.us;	Re: Sample 1
Re Sample 1-2.eml	▽			1060waddisonst@gmx.us;	Re: Sample 1
Re Test message.eml	▽			1060waddisonst@gmx.us;	Re: Test messa
Re You might be interested.eml	▽			1060waddisonst@gmx.us;	Re: You might
You might be interested.eml	▽			1060waddisonst@gmx.us;	You might be i
Fwd You might be interested.eml	▽			1060waddisonst@gmx.us;	Fwd: You migh
Sample 1.eml	▽			1060waddisonst@gmx.us;	Sample 1
Money & Training.eml	▽			1060waddisonst@gmx.us;	Money & Trair
Re Money available.eml	▽			1060waddisonst@gmx.us;	Re: Money ava
Re Need to talk to you ASAP.eml	▽			1060waddisonst@gmx.us;	Re: Need to tal
Re Need to talk to you ASAP-1.eml	▽			1060waddisonst@gmx.us;	Re: Need to tal
Re Need to talk to you ASAP-2.eml	▽			1060waddisonst@gmx.us;	Re: Need to tal
Re Money & Training.eml	▽			j_shu@gmx.us;	Re: Money & T
Re Fwd You might be interested.eml	▽			j_shu@gmx.us;	Re: Fwd: You n
Re Money available.eml	▽			j_shu@gmx.us;	Re: Money ava
Re Need to talk to you ASAP.eml	▽			j_shu@gmx.us;	Re: Need to tal
Re Need to talk to you ASAP-1.eml	▽			j_shu@gmx.us;	Re: Need to tal
Re Sample 1.eml	▽			j_shu@gmx.us;	Re: Sample 1

I selected two emails and reviewed the contents for use in my written testimony.



Source Name	S	C	O	E-Mail From	Subject
Money & Training.eml	▽			1060waddisonst@gmx.us;	Money & Trair
Re Money available.eml	▽			1060waddisonst@gmx.us;	Re: Money ava
Re Need to talk to you ASAP.eml	▽			1060waddisonst@gmx.us;	Re: Need to tal
Re Need to talk to you ASAP-1.eml	▽			1060waddisonst@gmx.us;	Re: Need to tal

Result: 4 of 4 Result

E-Mail Messages

From: 1060waddisonst@gmx.us; 2017-07-04 18:02:40 PDT

To: j_shu@gmx.us;

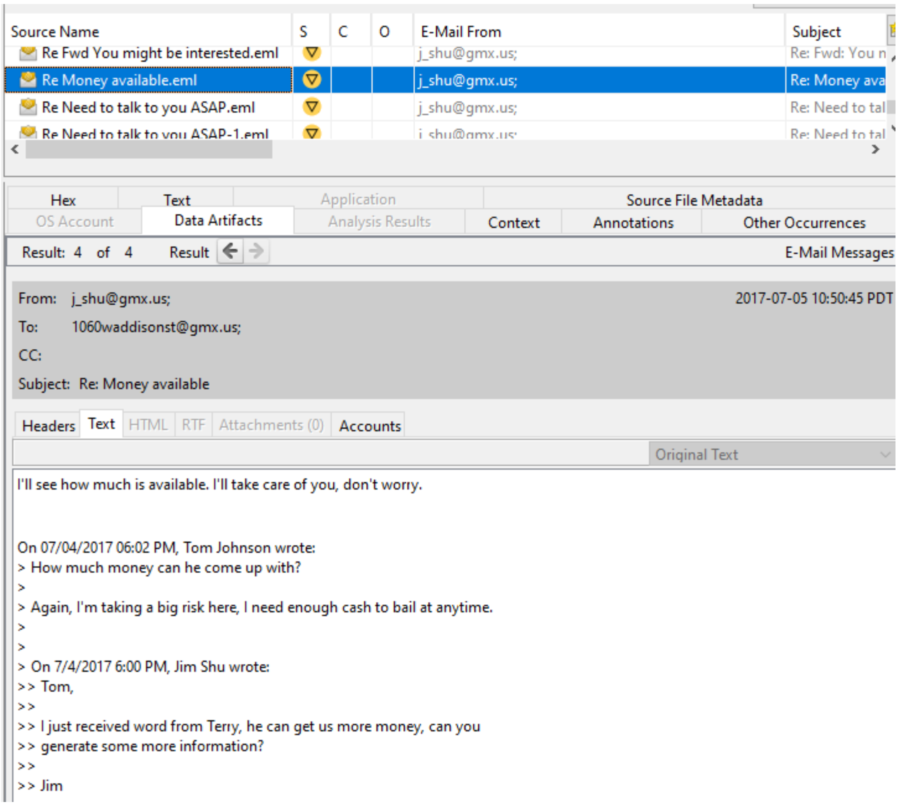
CC:

Subject: Re: Money available

How much money can he come up with?

Again, I'm taking a big risk here, I need enough cash to bail at anytime.

On 7/4/2017 6:00 PM, Jim Shu wrote:
> Tom,
>
> I just received word from Terry, he can get us more money, can you
> generate some more information?
>
> Jim
>
>



Source Name	S	C	O	E-Mail From	Subject
Re Fwd You might be interested.eml	▽			j_shu@gmx.us;	Re: Fwd: You n
Re Money available.eml	▽			j_shu@gmx.us;	Re: Money ava
Re Need to talk to you ASAP.eml	▽			j_shu@gmx.us;	Re: Need to tal
Re Need to talk to you ASAP-1.eml	▽			j_shu@gmx.us;	Re: Need to tal

Result: 4 of 4 Result

E-Mail Messages

From: j_shu@gmx.us; 2017-07-05 10:50:45 PDT

To: 1060waddisonst@gmx.us;

CC:

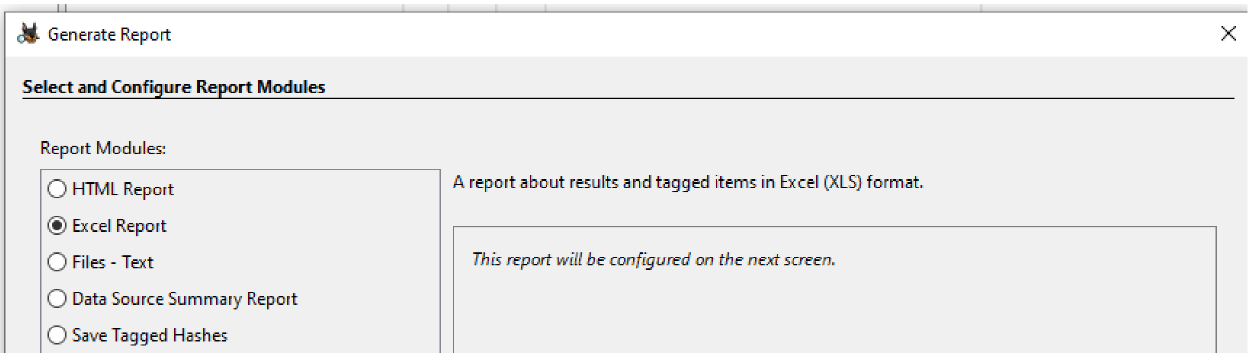
Subject: Re: Money available

I'll see how much is available. I'll take care of you, don't worry.

On 07/04/2017 06:02 PM, Tom Johnson wrote:
> How much money can he come up with?
>
> Again, I'm taking a big risk here, I need enough cash to bail at anytime.
>
>
> On 7/4/2017 6:00 PM, Jim Shu wrote:
>> Tom,
>>
>> I just received word from Terry, he can get us more money, can you
>> generate some more information?
>>
>> Jim

Step 3: Prepare Report

I pressed the Generate Report button and created an Excel Report configuring all tags.


Generate Report

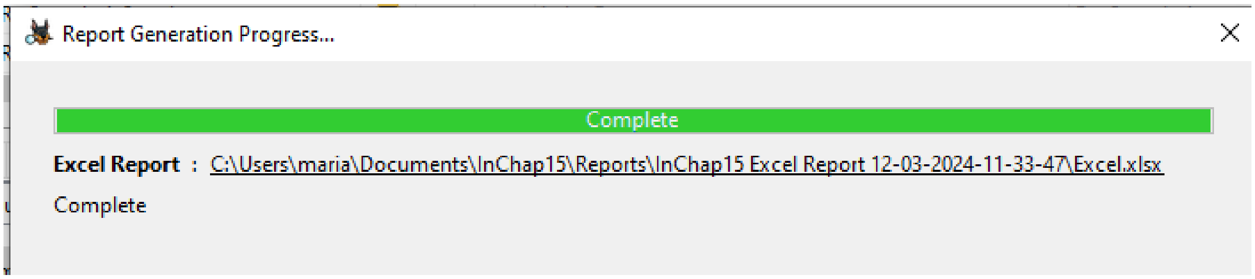
Select and Configure Report Modules

Report Modules:

○ HTML Report
● Excel Report
○ Files - Text
○ Data Source Summary Report
○ Save Tagged Hashes

A report about results and tagged items in Excel (XLS) format.

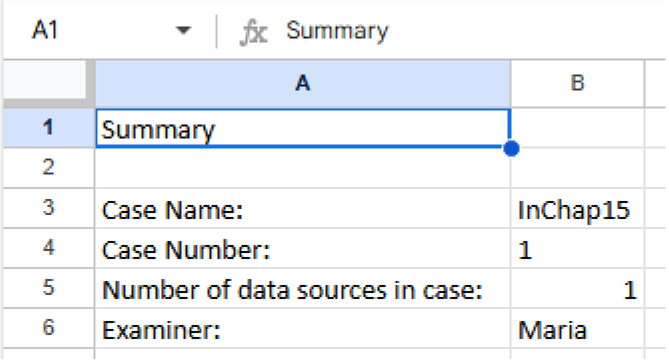
This report will be configured on the next screen.


Report Generation Progress...

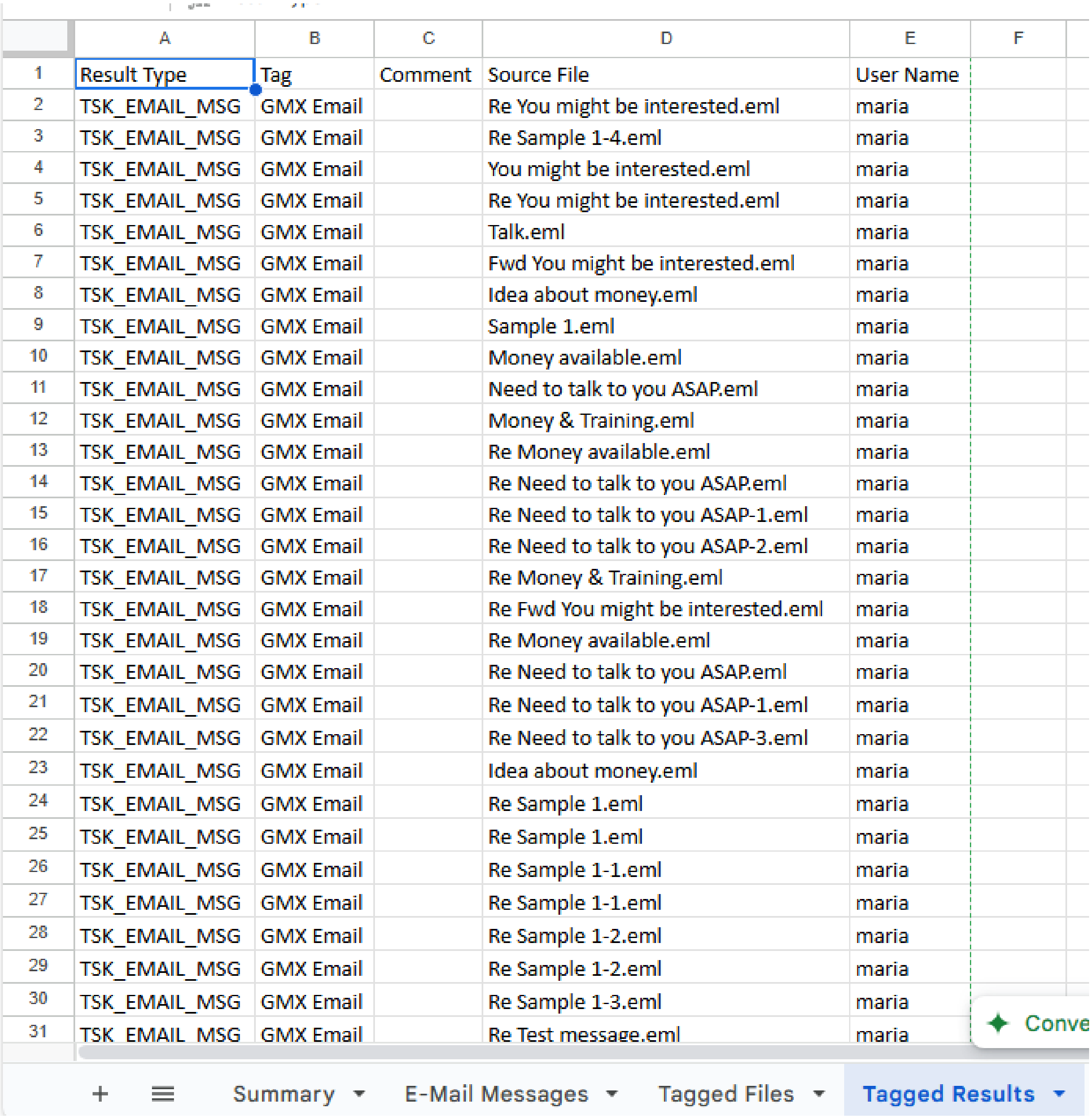
Complete

Excel Report : C:\Users\maria\Documents\InChap15\Reports\InChap15 Excel Report 12-03-2024-11-33-47\Excel.xlsx

Complete


A1 fx Summary

	A	B
1	Summary	
2		
3	Case Name:	InChap15
4	Case Number:	1
5	Number of data sources in case:	1
6	Examiner:	Maria



	A	B	C	D	E	F
1	Result Type	Tag	Comment	Source File	User Name	
2	TSK_EMAIL_MSG	GMX Email		Re You might be interested.eml	maria	
3	TSK_EMAIL_MSG	GMX Email		Re Sample 1-4.eml	maria	
4	TSK_EMAIL_MSG	GMX Email		You might be interested.eml	maria	
5	TSK_EMAIL_MSG	GMX Email		Re You might be interested.eml	maria	
6	TSK_EMAIL_MSG	GMX Email		Talk.eml	maria	
7	TSK_EMAIL_MSG	GMX Email		Fwd You might be interested.eml	maria	
8	TSK_EMAIL_MSG	GMX Email		Idea about money.eml	maria	
9	TSK_EMAIL_MSG	GMX Email		Sample 1.eml	maria	
10	TSK_EMAIL_MSG	GMX Email		Money available.eml	maria	
11	TSK_EMAIL_MSG	GMX Email		Need to talk to you ASAP.eml	maria	
12	TSK_EMAIL_MSG	GMX Email		Money & Training.eml	maria	
13	TSK_EMAIL_MSG	GMX Email		Re Money available.eml	maria	
14	TSK_EMAIL_MSG	GMX Email		Re Need to talk to you ASAP.eml	maria	
15	TSK_EMAIL_MSG	GMX Email		Re Need to talk to you ASAP-1.eml	maria	
16	TSK_EMAIL_MSG	GMX Email		Re Need to talk to you ASAP-2.eml	maria	
17	TSK_EMAIL_MSG	GMX Email		Re Money & Training.eml	maria	
18	TSK_EMAIL_MSG	GMX Email		Re Fwd You might be interested.eml	maria	
19	TSK_EMAIL_MSG	GMX Email		Re Money available.eml	maria	
20	TSK_EMAIL_MSG	GMX Email		Re Need to talk to you ASAP.eml	maria	
21	TSK_EMAIL_MSG	GMX Email		Re Need to talk to you ASAP-1.eml	maria	
22	TSK_EMAIL_MSG	GMX Email		Re Need to talk to you ASAP-3.eml	maria	
23	TSK_EMAIL_MSG	GMX Email		Idea about money.eml	maria	
24	TSK_EMAIL_MSG	GMX Email		Re Sample 1.eml	maria	
25	TSK_EMAIL_MSG	GMX Email		Re Sample 1.eml	maria	
26	TSK_EMAIL_MSG	GMX Email		Re Sample 1-1.eml	maria	
27	TSK_EMAIL_MSG	GMX Email		Re Sample 1-1.eml	maria	
28	TSK_EMAIL_MSG	GMX Email		Re Sample 1-2.eml	maria	
29	TSK_EMAIL_MSG	GMX Email		Re Sample 1-2.eml	maria	
30	TSK_EMAIL_MSG	GMX Email		Re Sample 1-3.eml	maria	
31	TSK_EMAIL_MSG	GMX Email		Re Test message.eml	maria	

Report

Summary:

- In this report, I gathered emails from a forensic image and prepared testimony describing how I extracted emails, their contents, and how chain of custody was maintained.

Forensic Methods Used to Obtain the Emails:

- The forensic methods I used to obtain the emails was through the use of Autopsy and its tools. Specifically, when creating this case, I chose to only ingest the Email Parser. By doing this, the case automatically analyzes all of the emails, making it simpler to search for specific emails.
- After, I analyzed the email messages and selected only emails with the "gmx.us" email address. I tagged the emails with the "gmx.us" email with "GMX email". After tagging all the gmx emails, I selected two emails to review its contents. Finally, I generated a report through excel using the autopsy tool "Generate Report".

Facts Derived from the Emails and Content:

- The two emails that caught my attention were from Tom Johnson and Jim Shu which had the subject: "Money Available".
- Tom Johnson's email is 1060waddisonst@gmx.us
- Jim Shu's email is j_shu@gms.us
- When I clicked on the first email, It was from Tom Johnson to Jim Shu. Tom wrote "How much money can he come up with? Again, I'm taking a bog risk here, I need enough cash to bail at any time". This email was sent to Jim Shu at 6:02pm on 07/04/2017.
- The second email I analyzed was a response from Jim Shu to Tom Johnson. The reply was sent at 10:50pm on 07/05/2017. The email said "I'll see how much is available. I'll take care of you, don't worry. "

Maintenance of Chain of Custody:

- The chain of custody was strictly maintained by documenting each step of the evidence handling process. The evidence was collected using forensic tools with screenshots of every step. Access to this evidence was limited to only myself during the investigation and will be handed over to my professor. These measures ensured the integrity of the evidence throughout the investigation.

Date and Time of Analysis:

- 12/03/2024 at 11:00am