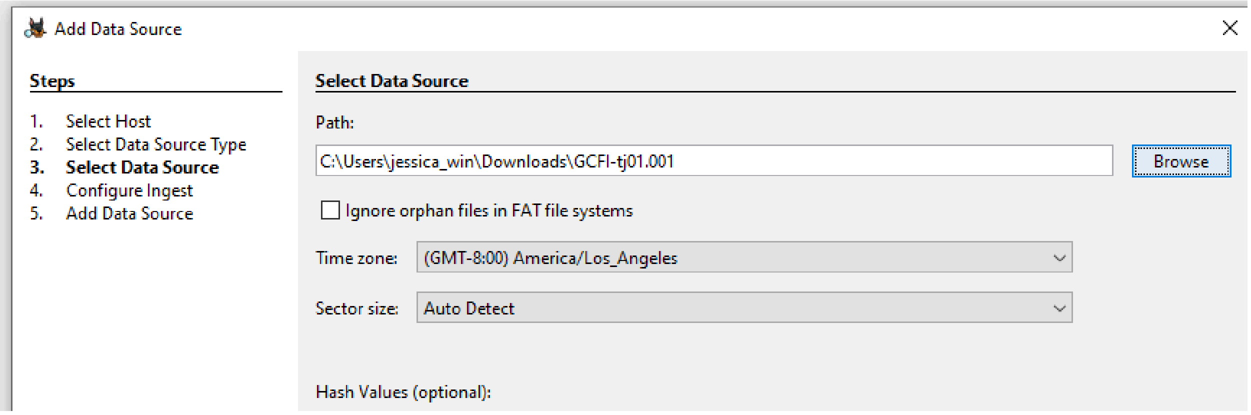
Task 1: Generate Report Findings

Step 1: Collect Image and Create Case



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

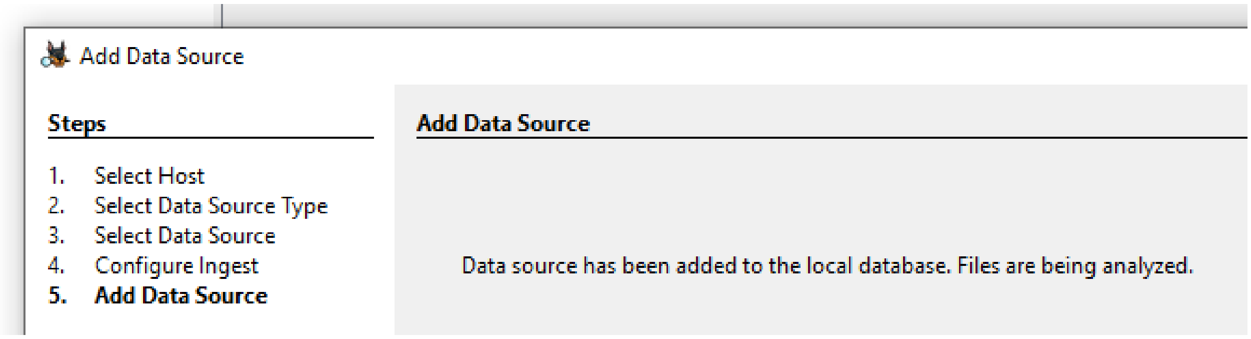
Path: C:\Users\jessica_win\Downloads\GCFI-tj01.001

□ Ignore orphan files in FAT file systems

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

Sector size: Auto Detect

Hash Values (optional):



Add Data Source

Steps

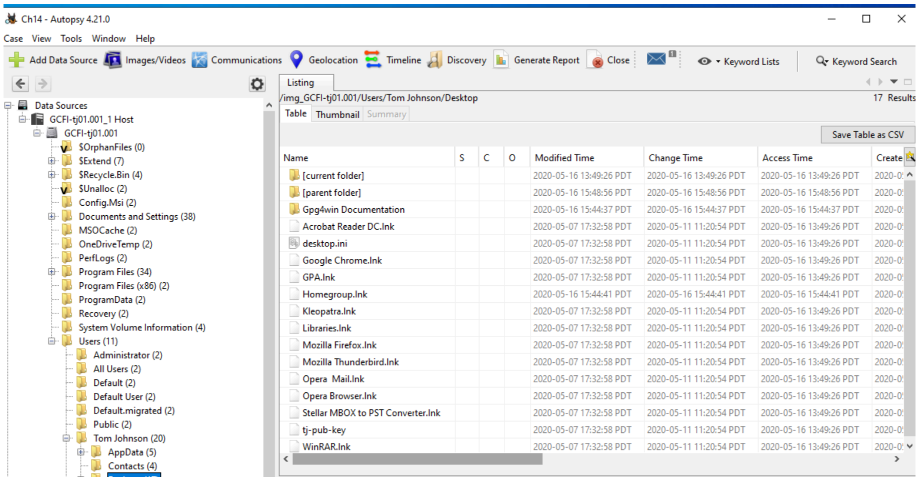
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

Successfully added disk image onto a new case in Autopsy.

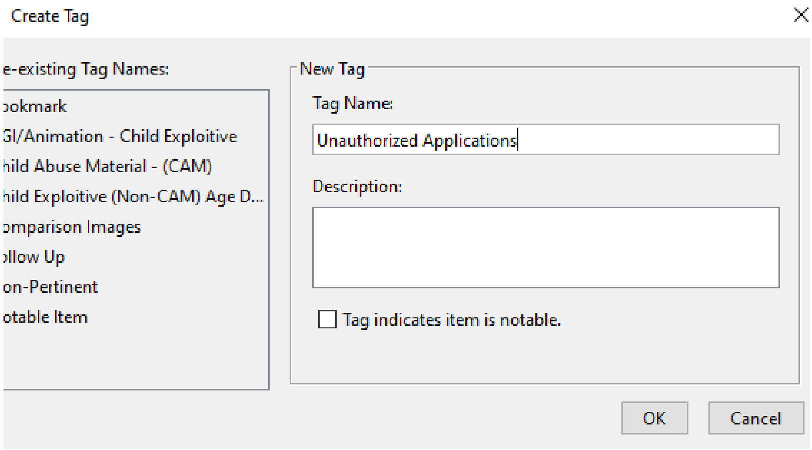
Step 2: Identify and Tag Evidence



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 (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)

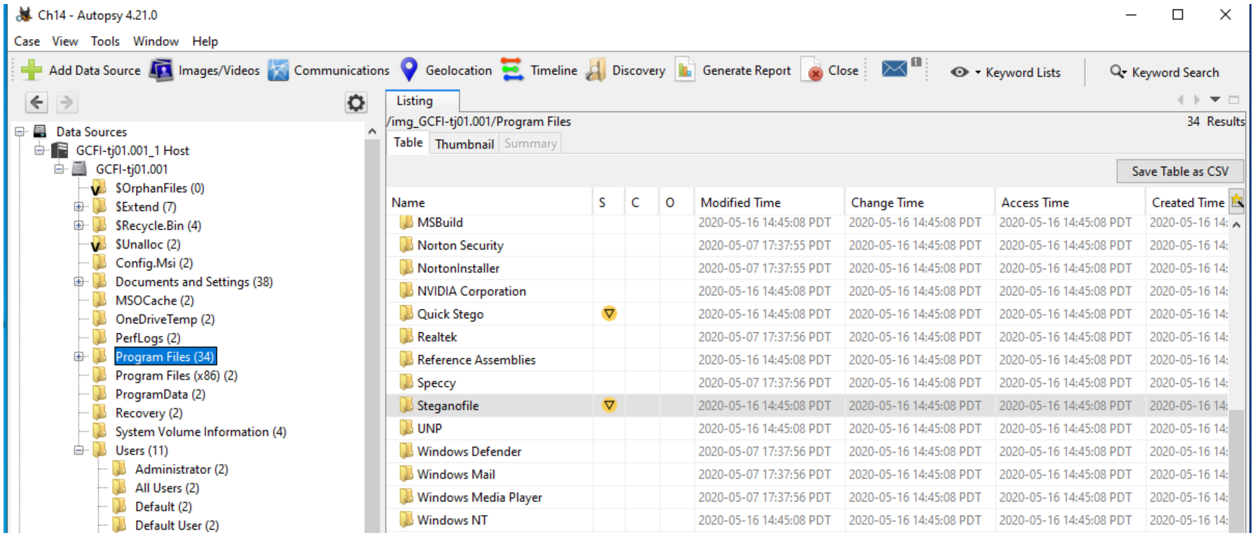
/img_GCFI-tj01.001/Users/Tom Johnson/Desktop 17 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Create
[current folder]				2020-05-16 13:49:26 PDT	2020-05-16 13:49:26 PDT	2020-05-16 13:49:26 PDT	2020-0:
[parent folder]				2020-05-16 15:48:56 PDT	2020-05-16 15:48:56 PDT	2020-05-16 15:48:56 PDT	2020-0:
Gpg4win Documentation				2020-05-16 15:44:37 PDT	2020-05-16 15:44:37 PDT	2020-05-16 15:44:37 PDT	2020-0:
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	2020-0:
desktop.ini				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
Google Chrome.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
GPA.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
Homegroup.lnk				2020-05-16 15:44:41 PDT	2020-05-16 15:44:41 PDT	2020-05-16 15:44:41 PDT	2020-0:
Kleopatra.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
Libraries.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
Mozilla Firefox.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
Mozilla Thunderbird.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
Opera Mail.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
Opera Browser.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
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	2020-0:
tj-pub-key				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:
WinRAR.lnk				2020-05-07 17:32:58 PDT	2020-05-11 11:20:54 PDT	2020-05-16 13:49:26 PDT	2020-0:



e-existing Tag Names:
ookmark
GI/Animation - Child Exploitive
hild Abuse Material - (CAM)
hild Exploitive (Non-CAM) Age D...
omparison Images
ollow Up
on-Pertinent
otable Item

New Tag
Tag Name: Unauthorized Applications
Description:
☐ Tag indicates item is notable.



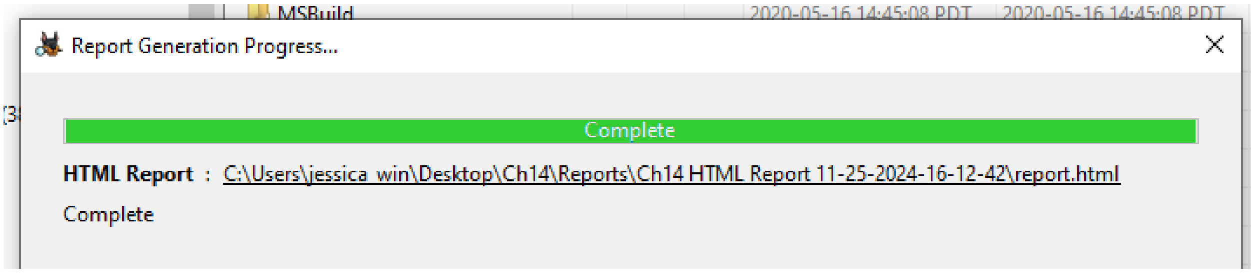
Data Sources
GCFI-tj01.001_1 Host
GCFI-tj01.001
$OrphanFiles (0)
$Extend (7)
$Recycle.Bin (4)
$Unalloc (2)
Config.Msi (2)
Documents and Settings (38)
MSOCache (2)
OneDriveTemp (2)
PerfLogs (2)
Program Files (34)
Program Files (x86) (2)
ProgramData (2)
Recovery (2)
System Volume Information (4)
Users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

/img_GCFI-tj01.001/Program Files 34 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
MSBuild				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:
Norton Security				2020-05-07 17:37:55 PDT	2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	2020-05-16 14:
NortonInstaller				2020-05-07 17:37:55 PDT	2020-05-16 14:45:08 PDT	2020-05-16 14:45:08 PDT	2020-05-16 14:
NVIDIA Corporation				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:
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:
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:
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:
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:
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:
UNP				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:
Windows Defender				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:
Windows Mail				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:
Windows Media Player				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:
Windows NT				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:

Successfully tagged unauthorized content on the disk image.

Step 3: Generate Report

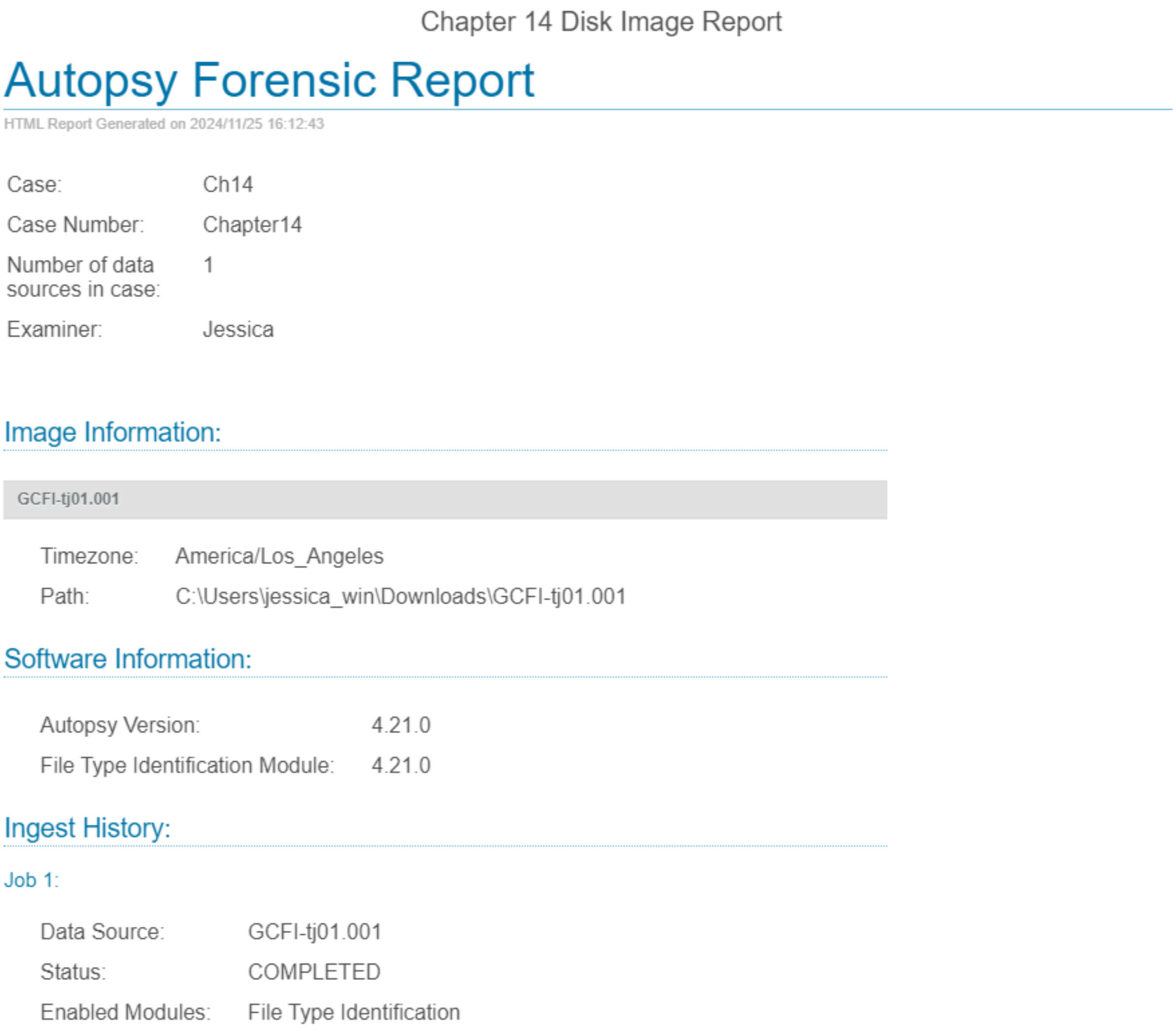


MSBuild 2020-05-16 14:45:08 PDT 2020-05-16 14:45:08 PDT

Report Generation Progress...

HTML Report : C:\Users\jessica_win\Desktop\Ch14\Reports\Ch14 HTML Report 11-25-2024-16-12-42\report.html

Complete



Chapter 14 Disk Image Report

Autopsy Forensic Report

HTML Report Generated on 2024/11/25 16:12:43

Case:	Ch14
Case Number:	Chapter14
Number of data sources in case:	1
Examiner:	Jessica

Image Information:

GCFI-tj01.001

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

Software Information:

Autopsy Version:	4.21.0
File Type Identification Module:	4.21.0

Ingest History:

Job 1:

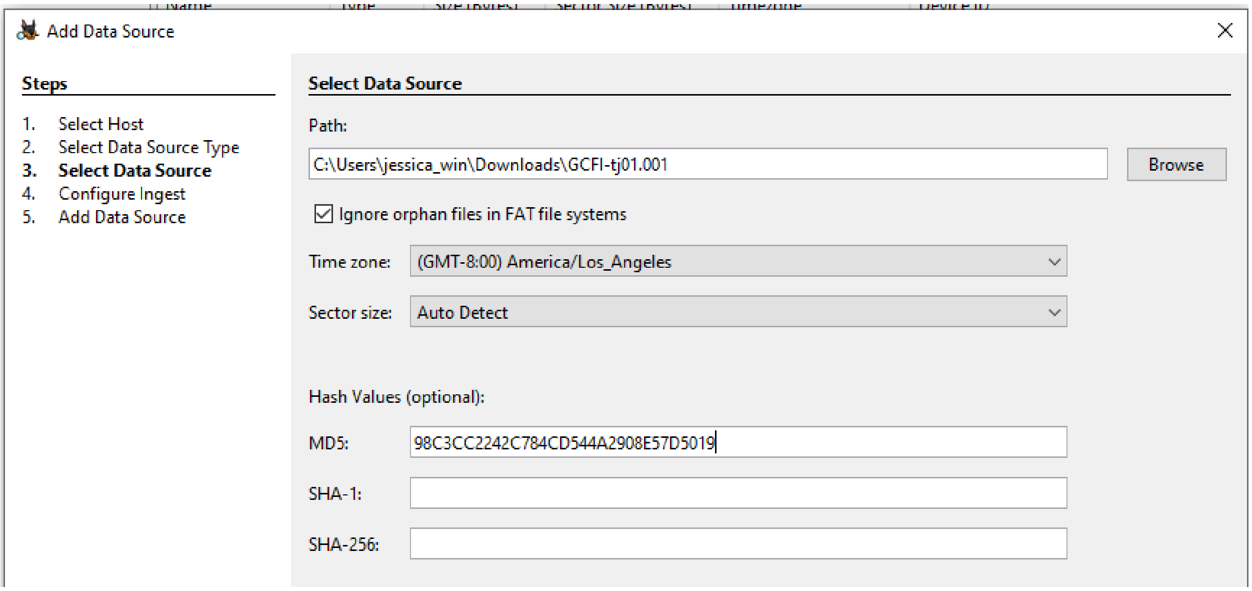
Data Source:	GCFI-tj01.001
Status:	COMPLETED
Enabled Modules:	File Type Identification

Successfully generated a report that holds information meaningful to the case at hand.

Three suspected files were found on the suspect's computer, all of which related to Stegonography and the editing of files. This could possibly suggest that the suspect hid data in certain files, or had data that they wanted to hide. I suggest other files should be analyzed for potential hidden messages or information.

Task 2: Preparing Evidence for Testimony

Step 1: Obtain Image and Create Case



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\jessica_win\Downloads\GCFI-tj01.001

☑ Ignore orphan files in FAT file systems

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

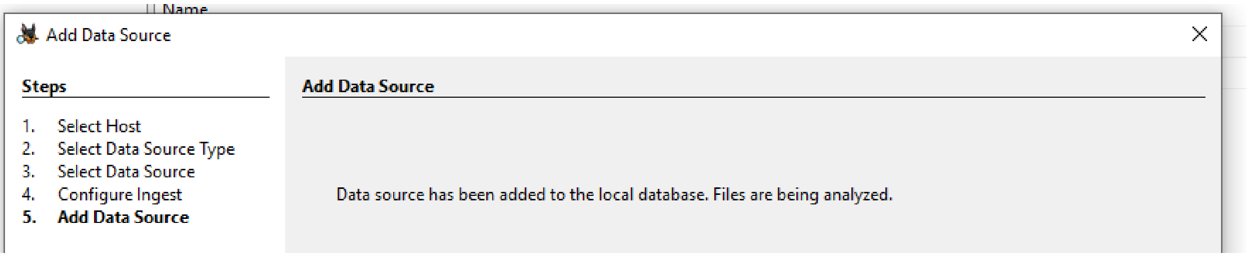
Sector size: Auto Detect

Hash Values (optional):

MD5: 98C3CC2242C784CD544A2908E57D5019

SHA-1:

SHA-256:



Add Data Source

Steps

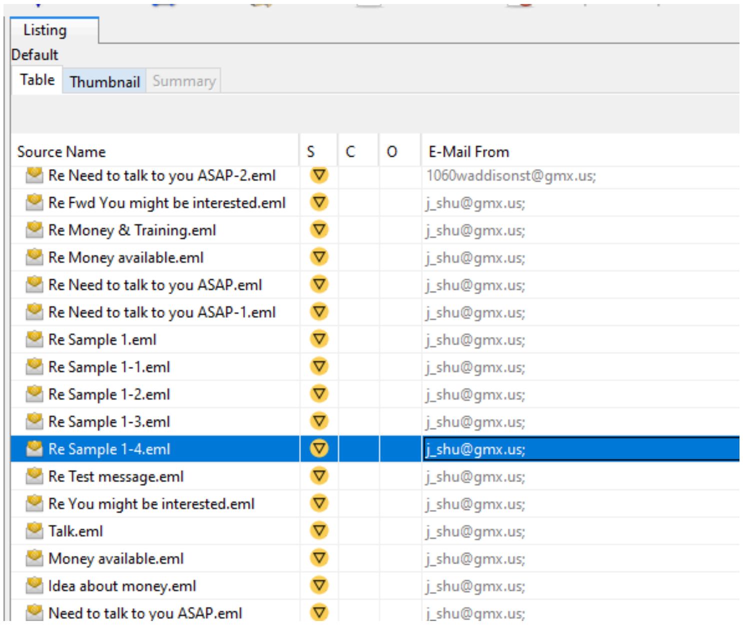
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

Successfully added case with hash and Email Parser ingested.

Step 2: Analyze Emails

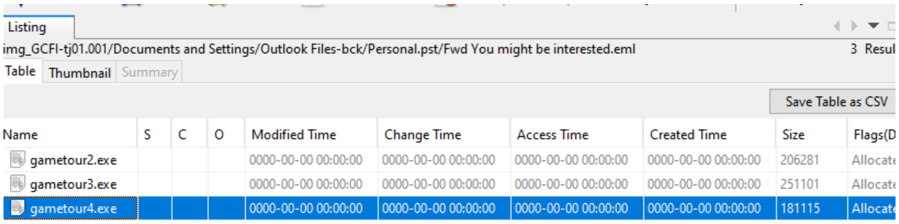


Listing

Default

Table | Thumbnail | Summary

Source Name	S	C	O	E-Mail From
Re Need to talk to you ASAP-2.eml	▽			1060waddisonst@gmx.us;
Re Fwd You might be interested.eml	▽			j_shu@gmx.us;
Re Money & Training.eml	▽			j_shu@gmx.us;
Re Money available.eml	▽			j_shu@gmx.us;
Re Need to talk to you ASAP.eml	▽			j_shu@gmx.us;
Re Need to talk to you ASAP-1.eml	▽			j_shu@gmx.us;
Re Sample 1.eml	▽			j_shu@gmx.us;
Re Sample 1-1.eml	▽			j_shu@gmx.us;
Re Sample 1-2.eml	▽			j_shu@gmx.us;
Re Sample 1-3.eml	▽			j_shu@gmx.us;
Re Sample 1-4.eml	▽			j_shu@gmx.us;
Re Test message.eml	▽			j_shu@gmx.us;
Re You might be interested.eml	▽			j_shu@gmx.us;
Talk.eml	▽			j_shu@gmx.us;
Money available.eml	▽			j_shu@gmx.us;
Idea about money.eml	▽			j_shu@gmx.us;
Need to talk to you ASAP.eml	▽			j_shu@gmx.us;



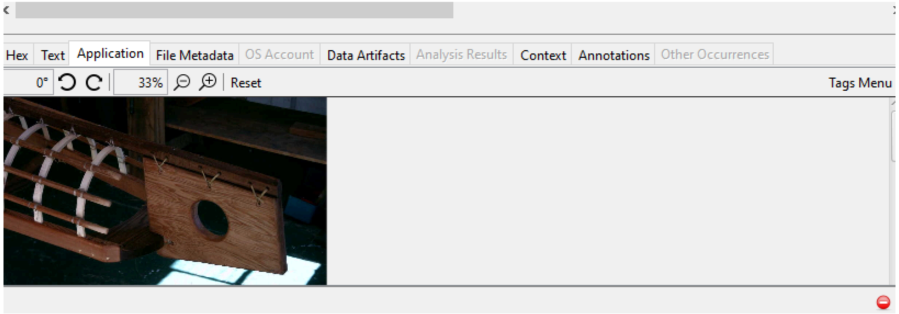
Listing

img_GCFI-tj01.001/Documents and Settings/Outlook Files-bck/Personal.pst/Fwd You might be interested.eml 3 Resul

Table | Thumbnail | Summary

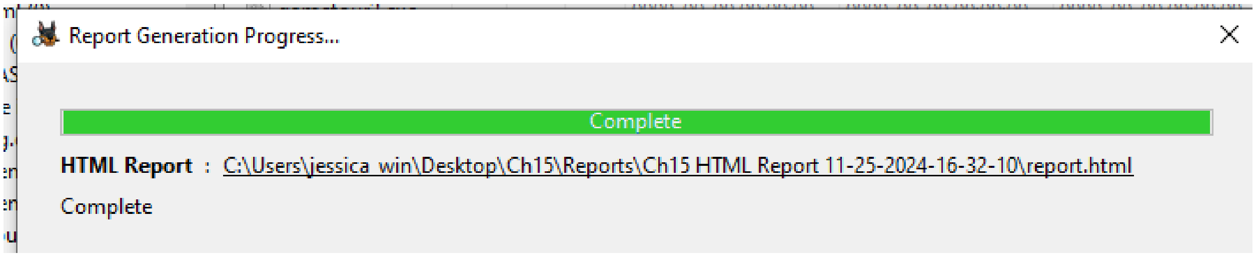
Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D
gametour2.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	206281	Allocate
gametour3.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	251101	Allocate
gametour4.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	181115	Allocate



Successfully tagged all @gmx emails and analyzed the contents of a few of them.

Step 3: Generate Report

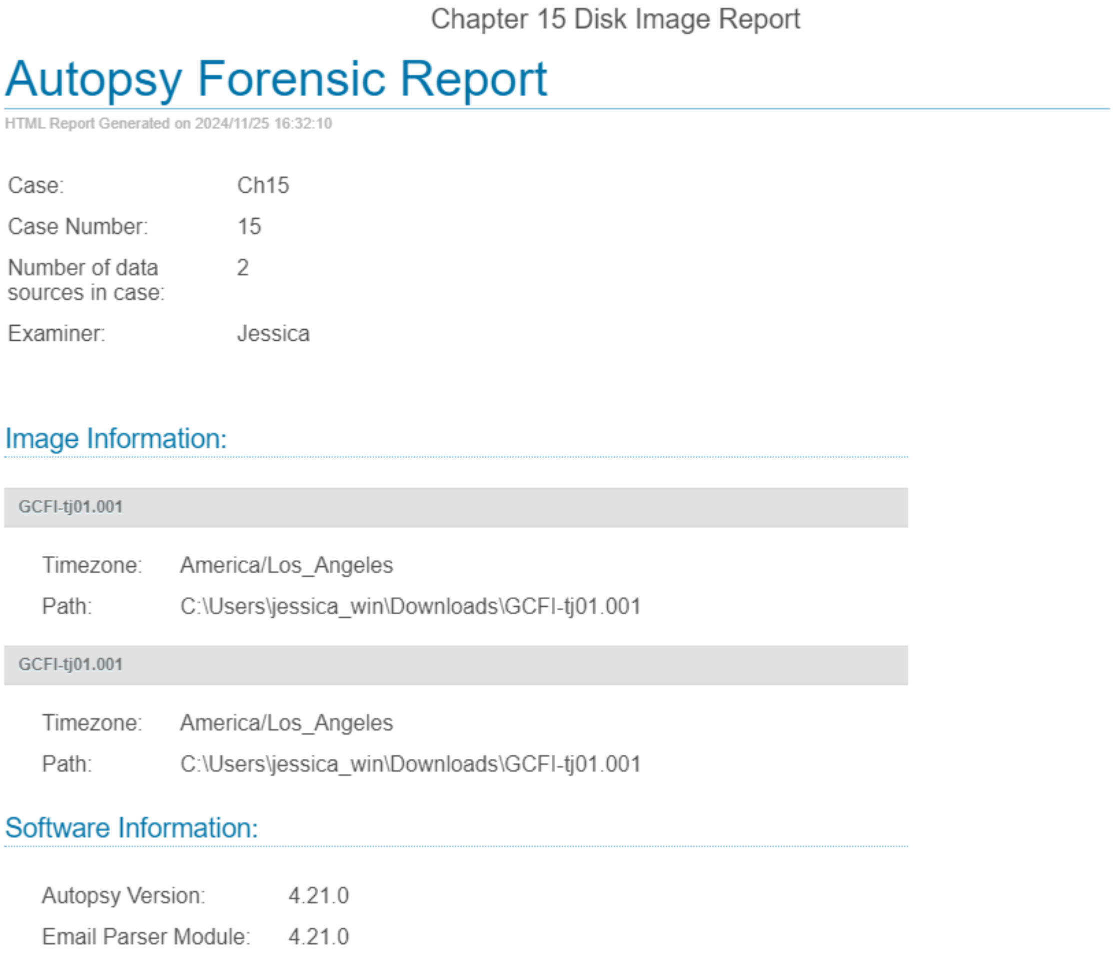


Report Generation Progress...

Complete

HTML Report : C:\Users\jessica_win\Desktop\Ch15\Reports\Ch15 HTML Report 11-25-2024-16-32-10\report.html

Complete



Chapter 15 Disk Image Report

Autopsy Forensic Report

HTML Report Generated on 2024/11/25 16:32:10

Case:	Ch15
Case Number:	15
Number of data sources in case:	2
Examiner:	Jessica

Image Information:

GCFI-tj01.001

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

GCFI-tj01.001

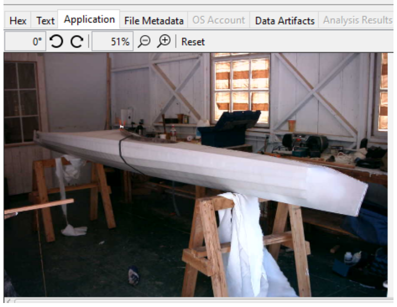
Timezone:	America/Los_Angeles
Path:	C:\Users\jessica_win\Downloads\GCFI-tj01.001

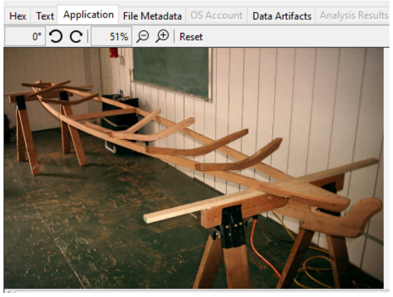
Software Information:

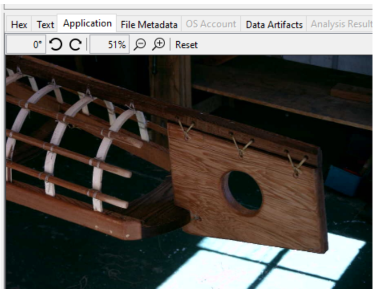
Autopsy Version:	4.21.0
Email Parser Module:	4.21.0

For this case, Autopsy (a digital forensics tool) was used to acquire a copy of the disk image of the suspect and was further analyzed. The case was created with a hash once the data source was added. Once it was loaded, the email parser revealed the information the suspect had in their incoming and outgoing email correspondence.

There were a few personal email from @gmx.us email accounts with subject lines regarding things the suspect would be interested in (with pictures), money, training, and urgent response from the sender. Most of the emails don't have physical content that Autopsy could detect but it did find a few pictures as shown:







In terms of the chain of custody of the evidence, the evidence was copied straight from the suspect disk as an identicial image. It was then given to a single digital investigator to analyze and parse through. That investigate then submitted the evidence to court immediately after finding relevant facts and information to present.