

Task 1

Autopsy 4.20.0

CaseViewToolsWindowHelp

Add Data Source

Images/Videos

Communications

Geolocation

Timeline

Discovery

Generate Report

Close Case

New Case Information

Steps

1. Case Information

2. Optional Information

Case Information

Case Name:

InChap01

Base Directory:

C:\Users\micha\OneDrive\Desktop\Spring and Summer 2023

Browse

Case Type:

Single-User

Multi-User

Case data will be stored in the following directory:

C:\Users\micha\OneDrive\Desktop\Spring and Summer 2023\InChap01

< Back

Next >

Finish

Cancel

Help

New Case Information



Steps

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

Optional Information

Case

Number: InChap01

Examiner

Name: John Gavigan

Phone:

Email:

Notes:

Organization

Organization analysis is being done for:

Not Specified

Manage Organizations

< Back

Next >

Finish

Cancel

Help

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\micha\OneDrive\Desktop\Spring and Summer 2023\IST 454\Ch01InChap01-1.dd

Browse

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/Indianapolis

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.










< Back

Next >

Finish

Cancel

Help

Listing Office							
Table Thumbnail Summary							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
 Billing Letter.doc				2005-12-09 06:50:28 EST	0000-00-00 00:00:00	2005-12-09 00:00:00 EST	2005-12-09 06:59:05 EST
 Regrets.doc				2005-12-09 06:50:52 EST	0000-00-00 00:00:00	2005-12-09 00:00:00 EST	2005-12-09 06:59:09 EST
 f0000000_13_October_2003.doc			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
 f0000049_02_November_2003.doc			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
 Income.xls			0	2005-12-09 06:52:18 EST	0000-00-00 00:00:00	2005-12-09 00:00:00 EST	2005-12-09 06:59:07 EST

Create Tag

Pre-existing Tag Names:

Bookmark

CGI/Animation - Child Exploitive

Child Abuse Material - (CAM)

Child Exploitive (Non-CAM) Age Difficult

Comparison Images

Follow Up

Non-Pertinent

Notable Item

New Tag

Tag Name:

Recovered Office Documents





Description:










Letter to Laura Roper from George Montgomery, regarding ownership of a domain name

☐ Tag indicates item is notable.

OK

Cancel

Listing Plain Text						
Table Thumbnail Summary						
Name	S	C	O	Modified Time	Change Time	Access Time
 confirmation.txt				2005-12-09 06:52:58 EST	0000-00-00 00:00:00	2005-12-09 00:00:00 EST
 letter 1.txt				2005-12-09 06:51:50 EST	0000-00-00 00:00:00	2005-12-09 00:00:00 EST

Listing	Keyword search 1 - George	×
Keyword search		
Table	Thumbnail	Summary
Name	Keyword Preview	Location
 Unalloc_4_121344_1474560	address listed below.«George» Montgomery3467 Main Street	/img_Ch01InChap01-1.dd/\$Unalloc/Unalloc_4_121344_147...
 Client Info.mdb	Ballard WA 98107 5 Thomas «George»	/img_Ch01InChap01-1.dd/Client Info.mdb
 Billing Letter.doc	address listed below.«George» Montgomery3467 Main	/img_Ch01InChap01-1.dd/Billing Letter.doc
 confirmation.txt	you for your business«George»-----	/img_Ch01InChap01-1.dd/confirmation.txt
 f0000000_13_October_2003.doc	address listed below.«George» Montgomery3467 Main	/img_Ch01InChap01-1.dd/\$CarvedFiles/1/f0000000_13_O...
 Income.xls	00 \$ 800.00 Thomas «George» \$ 450.00 ...	/img_Ch01InChap01-1.dd/Income.xls
 f0000049_02_November_2003.doc	nowhere.comRegards,«George» Montgomery-----	/img_Ch01InChap01-1.dd/\$CarvedFiles/1/f0000049_02_N...
 letter1.txt	Please contact me ASAP.«George»-----	/img_Ch01InChap01-1.dd/letter1.txt
 Regrets.doc	nowhere.comRegards,«George» Montgomery-----	/img_Ch01InChap01-1.dd/Regrets.doc

Listing

Keyword search 1 - George






Keyword search 2 - (\{?\}[a-zA-Z0-...

Keyword search

Table

Thumbnail

Summary

Name	Keyword Preview	Location
 Unalloc_4_121344_1474560	hyperlink mailto:«george.montgomery@nowhere.com» geo...	/img_Ch01InChap01-1.dd/\$Unalloc/Unalloc_4_121344_147...
 Billing Letter.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01-1.dd/Billing Letter.doc
 f0000000_13_October_2003.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01-1.dd/\$CarvedFiles/1/f0000000_13_O...
 f0000049_02_November_2003.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01-1.dd/\$CarvedFiles/1/f0000049_02_N...
 Regrets.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01-1.dd/Regrets.doc

Discovery Generate Report 16 Keyword Lists Keyword Search

Listing Keyword search 1 - George x Keyword search 2 - (\{?\}[a-zA-Z0-... x 5 Results

Office

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time
Billing Letter.doc	▼	📄		2005-12-09 06:50:28 EST	0000-00-00 00:00:00
Regrets.doc	▼			2005-12-09 06:50:52 EST	0000-00-00 00:00:00
f0000000_13_October_2003.doc	▼		0	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000049_02_November_2003.doc	▼		0	0000-00-00 00:00:00	0000-00-00 00:00:00
Income.xls	▼		0	2005-12-09 06:52:18 EST	0000-00-00 00:00:00

< >

Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Hex	Text	Application	File Metadata	OS Account
Page: 1 of 1	Page < >	Go to Page: 1	Jump to Offset	
0x00000000: D0 CF 11 E0 A1 B1 1A E1	00 00 00 00	00 00 00 00	00 00 00 00^
0x00000010: 00 00 00 00	00 00 00 00	3E 00 03 00	FE FF 09 00>
0x00000020: 06 00 00 00	00 00 00 00	00 00 00 00	01 00 00 00
0x00000030: 19 00 00 00	00 00 00 00	00 10 00 00	FE FF FF FF
0x00000040: 00 00 00 00	FE FF FF FF	00 00 00 00	18 00 00 00

Task 2

For this investigation, I used Autopsy to review the deleted contents on George’s USB drive. The USB drive contained several objects, including: a MS Excel file, a MS Access file, four MS Word files, and two plain text files. The Excel spreadsheet, titled “Income,” showed several transactions with customers in the month of January, and indicated that George made \$3,945.00 that month. There was also a record of customers in a MS Access file called “Client Info”. This file had six customers listed with their personal information, and it also had the domain names that went with each client. The word files show correspondence from George to his clients, Laura and Randall, who were looking to get domains from him. There were also communications with someone named Earl, but the nature of the work mentioned in the communications is unknown. Below are screenshots of the previously mentioned items.

|13 October 2005

Laura Roper
48 Mockingbird Lane
Seattle, WA 98119

Dear Laura,
Per our conversation, you want to register a domain with the name of www.lauras_stuff.com.
You have already chosen IT Connection Servers to host your website.

I have been in contact with them to get the necessary information. My fee for the registration process is \$500. Please send a check or money order to the address listed below.

George Montgomery
3467 Main Street
Bellevue, WA 98980

If you fail to do so within 30 days of receipt of this letter, the domain ownership will revert to [me](#) and I will sell it to the highest bidder.

Please call me at (206) 555-1212 or email me at george.montgomery@nowhere.com.

Regards,

George Montgomery

|02 November 2005

Randall Watson
89 Darnell Street
Des Moines, WA 98000

Dear Mr. Watson,
I regret to inform you that all five versions of the domain name that you chose have already been purchased. If you have other variations, please let me know by calling me at (206) 555-1212 or email me at george.montgomery@nowhere.com

Regards,

George Montgomery











D6					150
	A	B	C	D	E
1	January Cash Flow				
2					
3	Income	Setup	Contact	Confirmation	Total
4	Laura Roper	\$ 450.00	\$ 75.00	\$ 150.00	\$ 675.00
5	Earnest Bell	\$ 450.00	\$ 250.00	\$ 150.00	\$ 850.00
6	Frank Haron	\$ 575.00	\$ 75.00	\$ 150.00	\$ 800.00
7	Thomas George	\$ 450.00	\$ 120.00	\$ 150.00	\$ 720.00
8	Randall Watson	\$ 575.00	\$ 175.00	\$ 150.00	\$ 900.00
9					
10				Grand Total	\$ 3,945.00

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
Client Info.mdb	✓		0	2005-12-09 06:53:58 EST	0000-00-00 00:00:00	2005-12-09 00:00:00 EST	2005-12-09 06:59:01 EST	104448	Allocated








Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings Indexed Text Translation									
Page: 1 of 1 Page Matches on page: - of - Match 100% Reset									
Client Id	First Name	Last Name	Street Address	City	State	Zip			
1	Randall	Watson	89 Darnell Street	Des Moines	WA	98000			
2	Laura	Roper	48 Mockingbird Lane	Seattle	WA	98119			
3	Earnest	Bell	12891 Dexter Ave	Bellevue	WA	98769			
4	Frank	Haron	5679 Washington Streetq	Ballard	WA	98107			
5	Thomas	George	567 Port Ave	Seattle	WA	98118			
6	Claude	Finsk	1789 Through Drive	Seattle	WA	98791			
Client ID	Domain Name	ISP or NSP	IP Address	Registered Through	Date Registered	Next Renewal			
1	www.lauras_stuff.com	Groups.com	123.13.78.231	InterNIC	9/13/03	9/13/05			
2	www.nature.com	others.com	89.34.98.123	InterNIC	10/2/03	10/2/05			

I reviewed the text, hex, and metadata for each object on the USB drive, and I also performed searches for email addresses and for any mention of “George.” The results of the investigation indicate that George had a business where he would register domain names that other people wanted, and then he would charge them for the domain. This is supported by the list of customers, financial information, and the communications that were found on the drive. By referencing the metadata for each of the files, we can see that George was interacting with them between 6:50:00 and 6:59:09 EST. However, it is unknown what device George used for his work.

Sources

Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time
 Unalloc_4_121344_1474560				address listed below.«George» Montgomery3467 Main Street	George	0000-00-00 00:00:00	0000-00-00 00:00:00
 Client Info.mdb			0	Ballard WA 98107 5 Thomas «George»	George	2005-12-09 06:53:58 EST	2005-12-09 00:00:00 EST
 Billing Letter.doc				address listed below.«George» Montgomery3467 Main	George	2005-12-09 06:50:28 EST	2005-12-09 00:00:00 EST
 confirmation.txt				you for your business«George»-----	George	2005-12-09 06:52:58 EST	2005-12-09 00:00:00 EST
 f0000000_13_October_2003.doc			0	address listed below.«George» Montgomery3467 Main	George	0000-00-00 00:00:00	0000-00-00 00:00:00
 Income.xls			0	00 \$ 800.00 Thomas «George» \$ 450.00 ...	George	2005-12-09 06:52:18 EST	2005-12-09 00:00:00 EST
 f0000049_02_November_2003.doc			0	nowhere.comRegards,«George» Montgomery-----	George	0000-00-00 00:00:00	0000-00-00 00:00:00
 letter1.txt				Please contact me ASAP.«George»-----	George	2005-12-09 06:51:50 EST	2005-12-09 00:00:00 EST
 Regrets.doc				nowhere.comRegards,«George» Montgomery-----	George	2005-12-09 06:50:52 EST	2005-12-09 00:00:00 EST

Data Artifacts - Metadata

Source Name	S	C	O	Organization	Date Modified	Program Name	Date Created
 Billing Letter.doc				Starships CMS	2005-12-09 14:50:00 EST	Microsoft Word 9.0	2002-11-23 03:06:00 EST
 Client Info.mdb							
 Regrets.doc				Starships CMS	2005-12-09 14:50:00 EST	Microsoft Word 9.0	2002-11-23 03:12:00 EST
 Income.xls				Starships CMS	2005-12-09 14:52:18 EST	Microsoft Excel	2002-11-23 03:17:08 EST
 f0000000_13_October_2003.doc				Starships CMS	2005-12-09 14:50:00 EST	Microsoft Word 9.0	2002-11-23 03:06:00 EST
 f0000049_02_November_2003.doc				Starships CMS	2005-12-09 14:50:00 EST	Microsoft Word 9.0	2002-11-23 03:12:00 EST