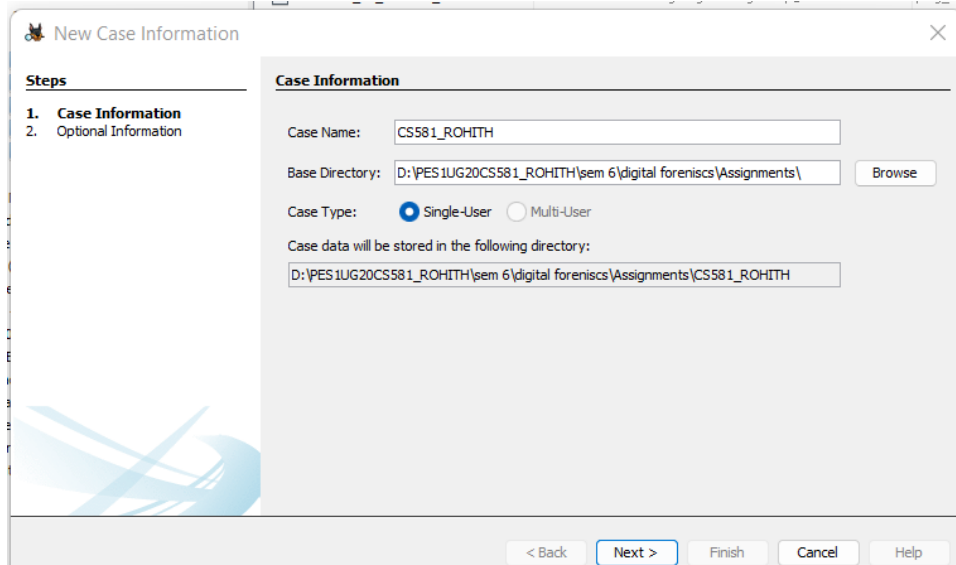


PES1UG20CS581
ROHITH H
J SEC

DIGITAL FORENSICS ASSIGNMENT -05

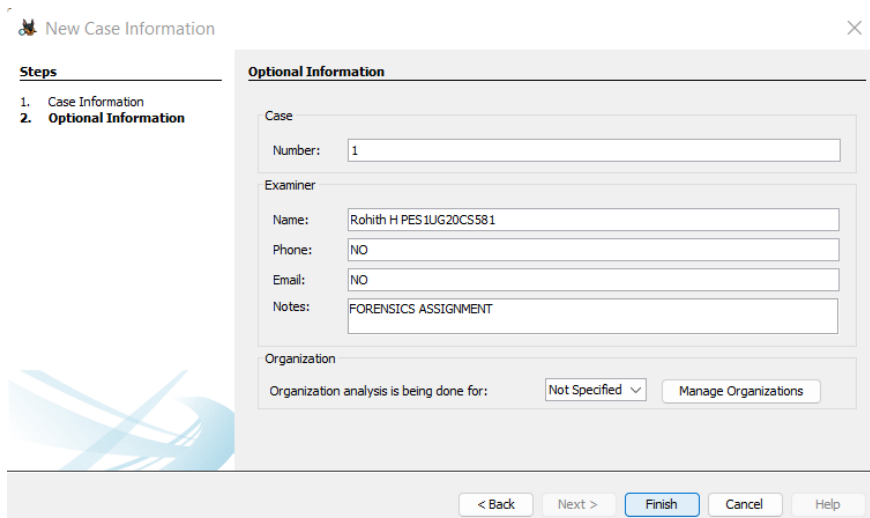
Forensics Autopsy screenshot



The screenshot shows the 'New Case Information' dialog box in the Autopsy application. The 'Steps' panel on the left indicates that the current step is '1. Case Information'. The 'Case Information' section contains the following fields:

- Case Name:** CS581_ROHITH
- Base Directory:** D:\PES1UG20CS581_ROHITH\sem 6\digital forensics\Assignments\ (with a 'Browse' button)
- Case Type:** Single-User (selected with a radio button, Multi-User is unselected)
- Case data will be stored in the following directory:** D:\PES1UG20CS581_ROHITH\sem 6\digital forensics\Assignments\CS581_ROHITH

At the bottom of the dialog, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted.



The screenshot shows the 'New Case Information' dialog box in the Autopsy application, specifically the 'Optional Information' step. The 'Steps' panel on the left indicates that the current step is '2. Optional Information'. The 'Optional Information' section contains the following fields:

- Case Number:** 1
- Examiner:**
 - Name:** Rohith H PES1UG20CS581
 - Phone:** NO
 - Email:** NO
 - Notes:** FORENSICS ASSIGNMENT
- Organization:**
 - Organization analysis is being done for:** Not Specified (with a dropdown arrow and a 'Manage Organizations' button)

At the bottom of the dialog, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Finish' button is highlighted.

The Screenshot Shows all the Files which contains the Keyword that is George

PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -05

InChap01 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Keyword Lists Keyword Search

Listing Keyword search 1 - George Keyword search 2 - ([?][a-zA-Z0-9...]

Keyword search 9 Results

Name	Keyword Preview	Location
Unalloc_4_121344_1474560	address listed below.«George» Montgomery3467 Main Street	/img_Ch01InChap01.dd/\$
Client Info.mdb	Ballard WA 98107 5 Thomas «George»	/img_Ch01InChap01.dd/C
Billing Letter.doc	address listed below.«George» Montgomery3467 Main	/img_Ch01InChap01.dd/B
confirmation.txt	you for your business«George»-----	/img_Ch01InChap01.dd/o
f0000000_13_October_2003.doc	address listed below.«George» Montgomery3467 Main	/img_Ch01InChap01.dd/\$
Income.xls	00 \$ 800.00 Thomas «George» \$ 450.00 ...	/img_Ch01InChap01.dd/I
f0000049_02_November_2003.doc	nowhere.comRegards,«George» Montgomery-----	/img_Ch01InChap01.dd/\$
letter1.txt	Please contact me ASAP.«George»-----	/img_Ch01InChap01.dd/I
Regrets.doc	nowhere.comRegards,«George» Montgomery-----	/img_Ch01InChap01.dd/R

Save Table as CSV

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: 1 of 1 Match 100% Reset

Text Source: Search Results

George Montgomery

-----METADATA-----

Application-Name: Microsoft Word 9.0
Author: Amelia Phillips
Character Count: 336
Company: Starships CMS
Content-Type: application/msword
Creation-Date: 2002-11-23T03:12:00Z
Edit-Time: 1200000000
Keywords:
Last-Author: Amelia Phillips
Last-Modified: 2005-12-09T14:50:00Z
Last-Save-Date: 2005-12-09T14:50:00Z
Page-Count: 1
Revision-Number: 2
Template: Normal.dot
Word-Count: 58
X-Parsed-By: org.apache.tika.parser.DefaultParser
X-TikaOrigResourceName: E:\Course Technology\Computer Forensics\Chapter 2 files\Chapter 2 AU2\case files\In chapter\Regret
s.doc
cp:revision: 2
cp:subject:

This Screenshot shows all the Files that contains the email with the keyword Gerge

PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -05

InChap01 - Autopsy 4.20.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Keyword Lists Keyword Search

Data Sources

- File Views
- File Types
 - By Extension
 - Images (0)
 - Videos (0)
 - Audio (0)
 - Archives (0)
 - Databases (0)
 - Documents
 - HTML (0)
 - Office (5)
 - PDF (0)
 - Plain Text (2)
 - Rich Text (0)
 - By MIME Type
- Deleted Files
 - File System (4)
 - All (6)
- MB File Size
 - MB 50 - 200MB (0)
 - MB 200MB - 1GB (0)
 - MB 1GB+ (0)
- Data Artifacts
 - Metadata (6)
- Analysis Results
- Keyword Hits (19)
- OS Accounts
- Tags
- Reports

Listing Keyword search 1 - George Keyword search 2 - ([a-zA-Z0-9...]

Keyword search 5 Results

Name	Keyword Preview	Location
Unaloc_4_121344_1474560	hyperlink mailto:george.montgomery@nowhere.com<geo...	/img_Ch01InChap01.dd/\$Ur
Billing Letter.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/\$Bilr
f000000_13_October_2003.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/\$Ce
f0000049_02_November_2003.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/\$Ce
Regrets.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/Reg

Save Table as CSV

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: 1 of 10 Match 100% Reset

Text Source: Search Results

HYPERLINK mailto:george.montgomery@nowhere.com
george.montgomery@nowhere.com
Regards,
George Montgomery
www.laures_stuff.com
http://www.laures_stuff.com/
george.montgomery@nowhere.com
mailto:george.montgomery@nowhere.com
Normal

Heading 1

Default Paragraph Font

Hyperlink

Amela PhillipsE:\Course Technology\Computer Forensics\Chapter 2 files\Chapter 2 AU2\case files\in chapter\Billing Letter.doc
Amela Phillips2C:\Chap02\case files\in chapter\Billing Letter.doc
Unknown
Times New Roman
Symbol
Arial
13 October 2003
Amela Phillips
Amela Phillips
13 October 2003
Amela Phillips
Normal.dotl
Amela Phillips
Microsoft Word 9.0

PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -05

This Screenshot shows the Hexadecimal Values of the Files which contains the keyword Geoge

The screenshot displays the Autopsy 4.20.0 interface. The left sidebar shows the file system tree with categories like Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts, Metadata, Analysis Results, Keyword Hits, OS Accounts, Tags, and Reports. The main window is titled 'Keyword search 1 - George' and shows 5 results. The results table lists files and their locations, with a 'Keyword Preview' column showing the search results. Below the table, the 'Hex' tab is selected, displaying a hex dump of the file data. The hex dump shows the keyword 'George' in multiple locations, with the corresponding ASCII values 'G', 'e', 'o', 'r', 'g', 'e' visible in the right column.

Name	Keyword Preview	Location
Unalloc_4_121344_1474560	hyperlink.mailto:george.montgomery@nowhere.com<geo...	/img_Ch01InChap01.dd/\$Ur
Billing Letter.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/Billr
f0000000_13_October_2003.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/\$Ce
f0000049_02_November_2003.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/\$Ce
Regrets.doc	1212 or email me at <george.montgomery@nowhere.com>...	/img_Ch01InChap01.dd/Reg

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Page: 1 of 82 Go to Page: 1 Jump to Offset Launch in HxD

0x00000000: D0 CF 11 E0 A1 B1 1A E1 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: 2A 00 00 00 00 00 00 00 00 10 00 00 2C 00 00 00>.....
0x00000040: 01 00 00 00 FE FF FF FF 00 00 00 00 29 00 00 00>.....
0x00000050: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000060: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000070: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000080: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000090: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000000a0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000000b0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000000c0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000000d0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000000e0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000000f0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000130: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000140: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000150: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000160: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000170: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000180: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x00000190: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000001a0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000001b0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000001c0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....
0x000001d0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF>.....