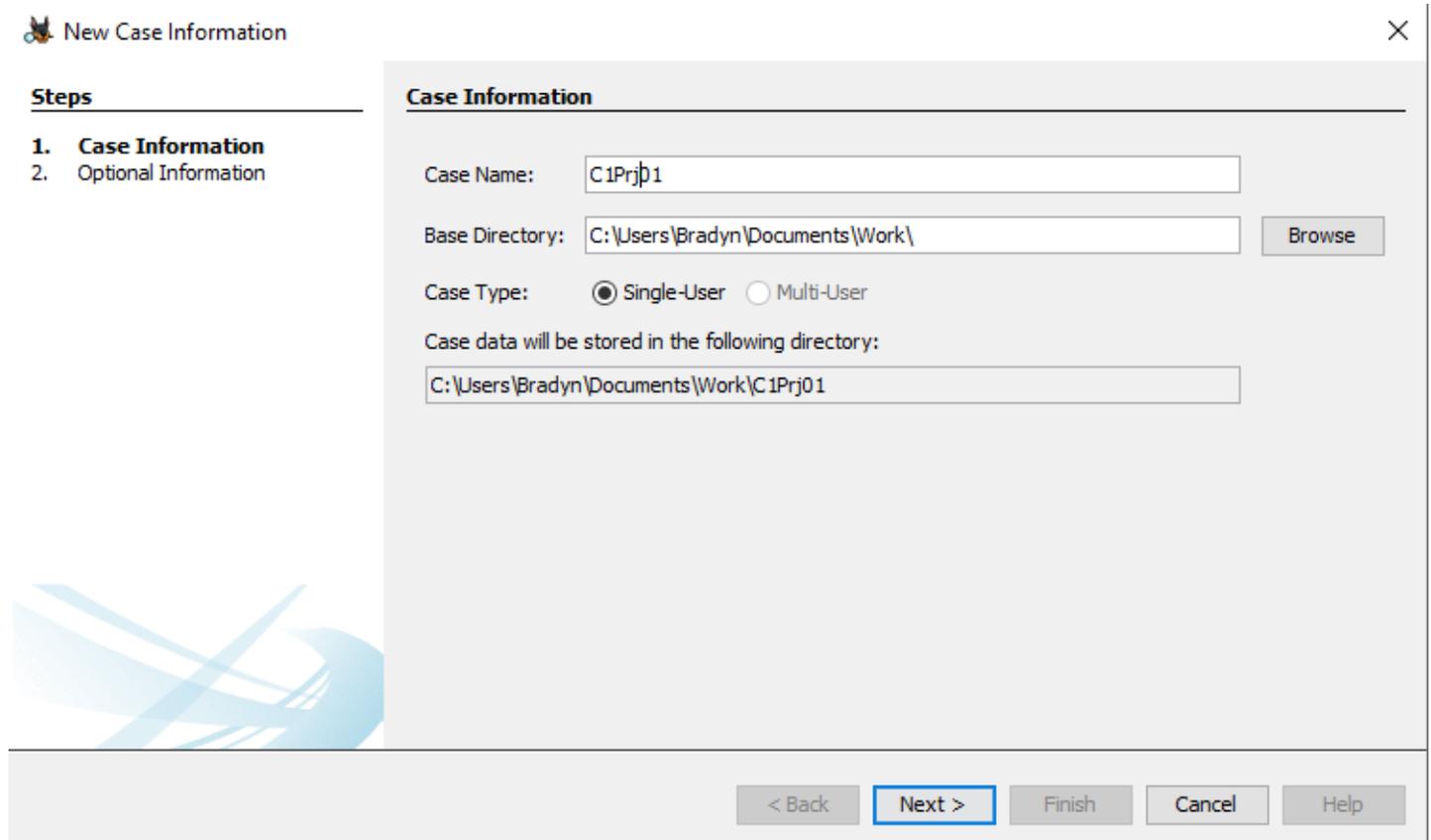


Step 1: Start Autopsy for Windows, and click the Create New Case icon. In the New Case Information Window, enter C1Prj01 in the Case Name text box, and click browse next to the Base Directory text box. Navigate to and click your work folder, and then click next.



Bradyn Ritchie

ITN 276

Chapter 1: Hands On Project 1-1

Step 2: In the additional information window, type C1Prj01 in the Case Number text box and your name in the examiner text box, and then click finish.

New Case Information

Steps

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

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for:

< Back Next > **Finish** Cancel Help

Bradyn Ritchie

ITN 276

Chapter 1: Hands On Project 1-1

Step 3: In the select data source window, click the select data source type list arrow, and click disk image or VM file. Click the browse button next to the browse for an image file text box, navigate to and click your work folder and the C1Prj01.E01 file, and then click open. Click next.

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:

Ignore orphan files in FAT file systems

Time zone:

Sector size:

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

Step 4: In the configure ingest modules window, click select all. Click next and then finish.

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

- 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
- Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Global Settings

Select All Deselect All History

< Back Next > Finish Cancel Help

Bradyn Ritchie

ITN 276

Chapter 1: Hands On Project 1-1

Step 5: In the tree viewer pane, expand views, file types, by extension, and documents.

The screenshot shows the Autopsy 4.19.3 interface. The left pane displays a tree view with 'Documents' expanded under 'File Types'. The right pane shows a table of document results.

File Type	File Extensions
HTML (0)	.htm, .html
Office (1)	.doc, .docx, .odt, .xls, .xlsx, .ppt, .pptx
PDF (0)	.pdf
Plain Text (1)	.txt
Rich Text (0)	.rtf

At the bottom of the interface, a status bar indicates 'Analyzing files from C1Prj01.E01' at 90% completion, with a '(1 more...)' button and a page number '2'.

Bradyn Ritchie

ITN 276

Chapter 1: Hands On Project 1-1

Step 6: Examine each subfolder under documents. Determine which folder might contain files of interest to this case.

The screenshot shows the Autopsy 4.19.3 interface. The left sidebar displays a tree view of file types, with 'Plain Text (1)' selected under the 'Documents' folder. The main pane shows a table listing the file 'suicide1.txt'.

Name	S	C	O	Modified Time	Change Time	Access Time
suicide1.txt				2002-11-22 20:29:46 EST	0000-00-00 00:00:00	2005-12-09 00:00:00 EST

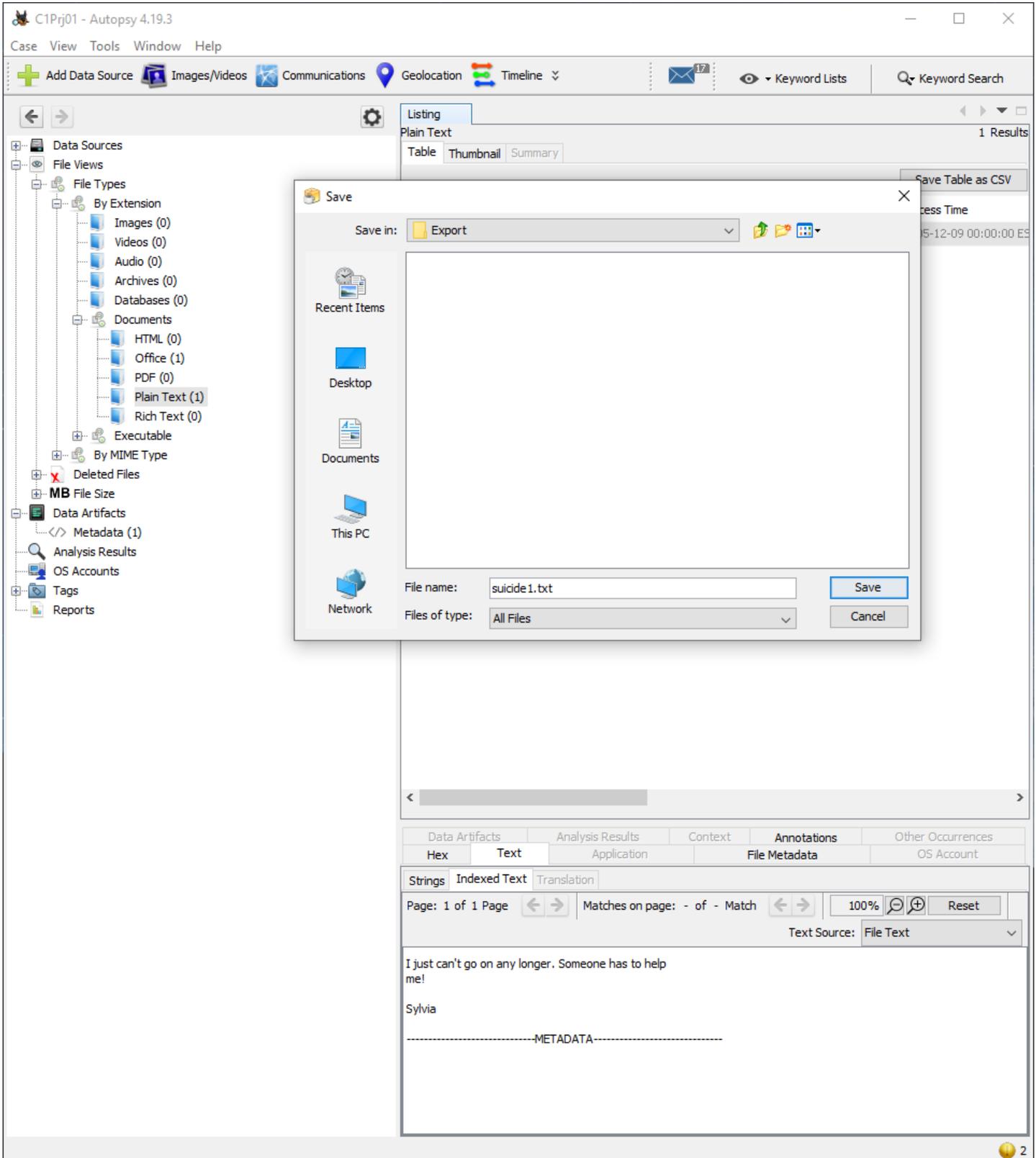
Below the table, there are tabs for 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The 'Text' tab is active, showing 'Page: 1 of' and 'Script: Latin - Basic'. A scroll bar is visible at the bottom of the main pane.

Bradyn Ritchie

ITN 276

Chapter 1: Hands On Project 1-1

Step 7: If you found any files related to the case, select the files as a group, right-click the selection, and click extract file(s). In the save dialog box, click save to save the files automatically in Autopsy's case subfolder: Work\Chap01\Projects\C1Prj01\Export.



Bradyn Ritchie

ITN 276

Chapter 1: Hands On Project 1-1

Step 8: Write a short report of no more than two paragraphs, including facts from any contents you found.

By using autopsy, I was able to find some interesting files, such as a file named "suicide1.txt" and "SylviasAssets.xls" that contain important information to the case. The "suicide" file contained a hidden cry for help from Sylvia saying that she "couldn't go any longer". The assets file contained financial information about Sylvia's stocks, life insurance, savings accounts, annuities, bonds, and real estate. These were the only two files located inside the C1Prj01.E01 file. Based on this evidence, I think it is safe to assume that there was no foul play involved in Sylvia's death. Therefore, it should be ruled as a suicide.