

Assignment 3.1: Examine the Evidence Using Autopsy

Joshua A. Wortz

University of San Diego

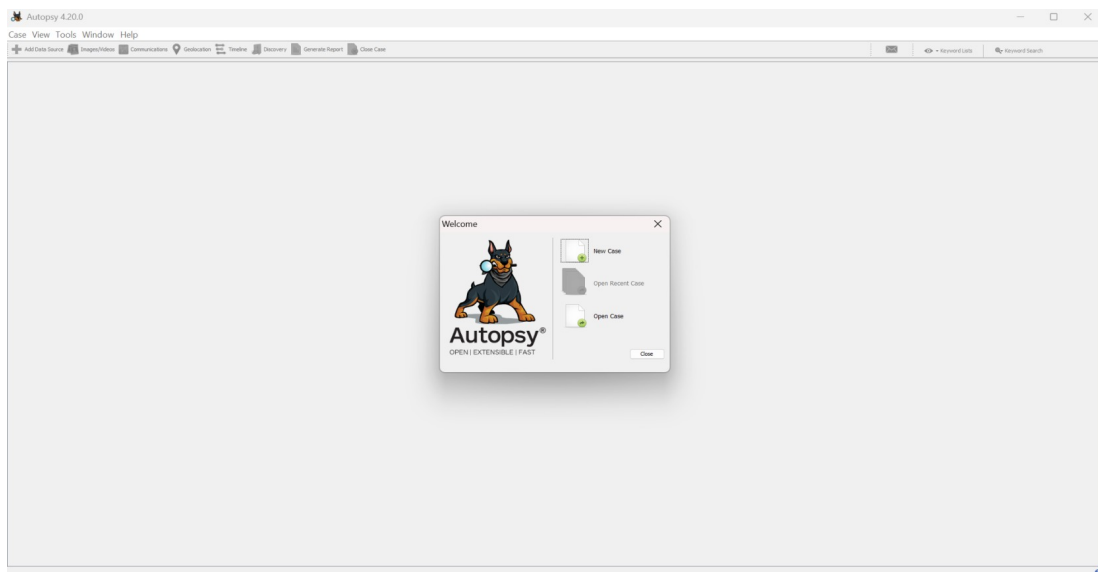
CSOL-590

Prof. Fulton

01/26/2026

1. Open Autopsy

Figure 1



Autopsy has opened.

2. Create new case

Figure 2

The screenshot shows the 'New Case Information' dialog box. It has a title bar with the Autopsy logo and a close button. On the left, there is a 'Steps' section with two items: '1. Case Information' (selected) and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields and controls: 'Case Name' with the text 'CSOL590M3'; 'Base Directory' with the text 'C:\Users\joshu\Assignment 3.1\' and a 'Browse' button; 'Case Type' with two radio buttons, 'Single-User' (selected) and 'Multi-User'; and a text box for 'Case data will be stored in the following directory:' containing 'C:\Users\joshu\Assignment 3.1\CSOL590M3'. At the bottom, there are five buttons: '< Back', 'Next >' (highlighted), 'Finish', 'Cancel', and 'Help'.

A new case was created.

3. Add evidence

Figure 3

The screenshot shows the 'Add Data Source' dialog box with the 'Select Data Source' step selected. The 'Steps' list on the left includes: 1. Select Host, 2. Select Data Source Type, 3. **Select Data Source**, 4. Configure Ingest, and 5. Add Data Source. The 'Path' field contains 'C:\Users\joshu\Assignment 2.1\CSOL590\CSOL590-02\Mod2_Joshua\Wortz-02.E01' with a 'Browse' button. There is an unchecked checkbox for 'Ignore orphan files in FAT file systems'. The 'Time zone' is set to '(GMT-8:00) America/Los_Angeles' and 'Sector size' is 'Auto Detect'. Below these are optional hash value fields for MD5, SHA-1, and SHA-256. A note states: 'NOTE: These values will not be validated when the data source is added.' At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Evidence was added through the USB drive image from last assignment.

4. Select Ingest Options

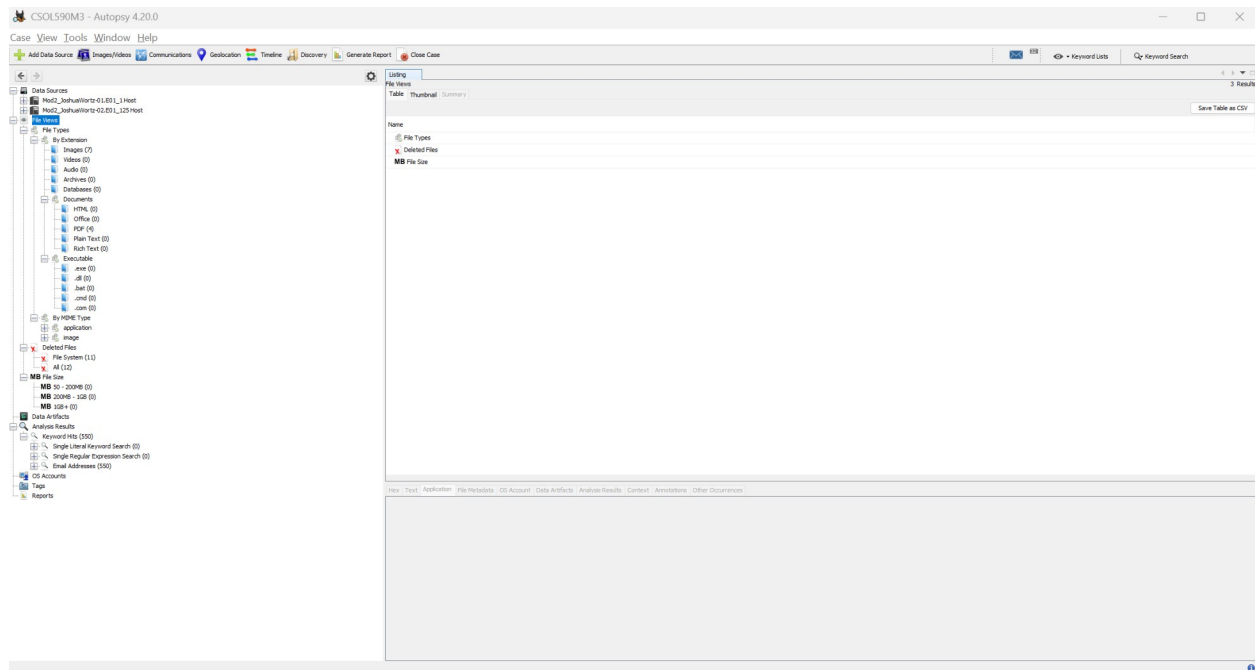
Figure 4

The screenshot shows the 'Add Data Source' dialog box with the 'Configure Ingest' step selected. The 'Steps' list on the left includes: 1. Select Host, 2. Select Data Source Type, 3. Select Data Source, 4. **Configure Ingest**, and 5. Add Data Source. The 'Run ingest modules on:' dropdown is set to 'All Files, Directories, and Unallocated Space'. A list of modules is shown with checkboxes: 'Recent Activity' (checked), 'Hash Lookup' (checked), 'File Type Identification' (checked), 'Extension Mismatch Detector' (checked), 'Embedded File Extractor' (checked), 'Picture Analyzer' (checked), 'Keyword Search' (checked), 'Email Parser' (checked), 'Encryption Detection' (checked), 'Interesting Files Identifier' (checked), 'Central Repository' (checked), 'PhotoRec Carver' (checked), and 'Virtual Machine Extractor' (checked). Below the list are buttons for 'Select All', 'Deselect All', and 'History'. On the right, a text box states 'The selected module has no per-run settings.' and a description at the bottom says 'Extracts recent user activity, such as Web browsing, recently us...' with a 'Global Settings' button. At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Options were selected.

5. Review results

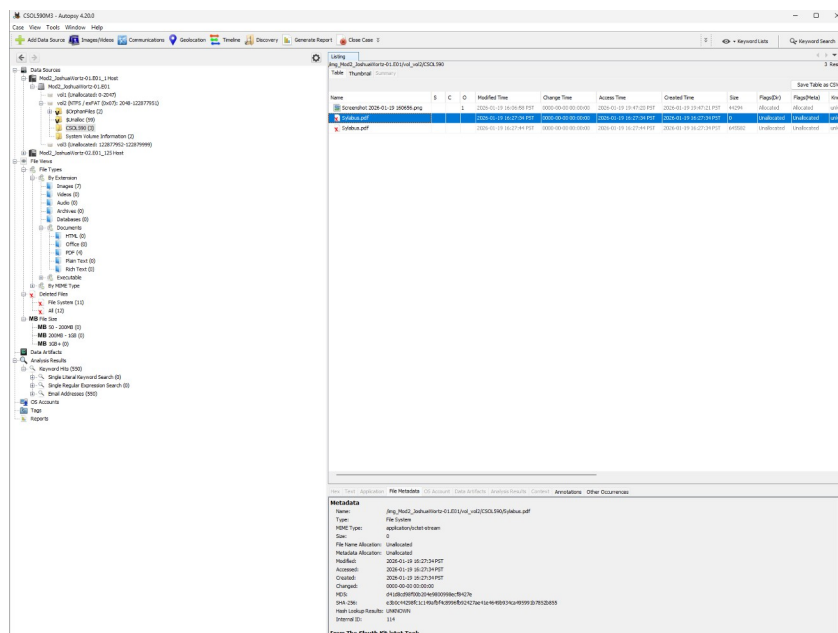
Figure 5



Home Screen View.

6. Find the deleted file

Figure 6



The deleted syllabus file was located.

7. Note dates and hash value

Figure 7

Metadata	
Name:	/img_Mod2_JoshuaWortz-01.E01/vol_vol2/CSOL590/Sylabus.pdf
Type:	File System
MIME Type:	application/octet-stream
Size:	0
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2026-01-19 16:27:34 PST
Accessed:	2026-01-19 16:27:34 PST
Created:	2026-01-19 16:27:34 PST
Changed:	0000-00-00 00:00:00
MD5:	d41d8cd98f00b204e9800998ecf8427e
SHA-256:	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
Hash Lookup Results:	UNKNOWN
Internal ID:	114

Dates and hash from the deleted file.

8. Add in original image

Figure 8

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

Added Original Image

9. Find the original file

Figure 9

The screenshot shows the Autopsy 4.20.0 interface. On the left, the 'Data Sources' pane shows a tree structure with 'Mod2_JoshuaWirtz-01.E01_1.img' selected. The 'File Views' pane shows a list of file types, including 'File System (11)', 'Deleted Files (1)', and 'All (12)'. The 'File System (11)' view is expanded, showing a list of files. The 'File System (11)' view is expanded, showing a list of files. The 'File System (11)' view is expanded, showing a list of files.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location	Save Ta	MD5 Hash
DiskManagement.log				2026-01-19 16:07:13 PST	0000-00-00 00:00:00	2026-01-19 16:07:12 PST	2026-01-19 16:07:13 PST	0	Unallocated	Unallocated	unknown	[img_Mod2_JoshuaWirtz-01.E01]vol_02(DiskManagemen...		0110c0590c
DiskManagement.log				2026-01-19 16:07:13 PST	0000-00-00 00:00:00	2026-01-19 16:07:12 PST	2026-01-19 16:07:13 PST	0	Unallocated	Unallocated	unknown	[img_Mod2_JoshuaWirtz-02.E01]vol_02(DiskManagemen...		
DiskManagement.log				2026-01-19 16:07:16 PST	0000-00-00 00:00:00	2026-01-19 16:07:16 PST	2026-01-19 16:07:13 PST	44294	Allocated	Allocated	unknown	[img_Mod2_JoshuaWirtz-01.E01]vol_02(DiskManagemen...		76e9f1936d
ScreenShot 2026-01-19 16:06:59.png				2026-01-19 16:06:59 PST	0000-00-00 00:00:00	2026-01-19 16:07:20 PST	2026-01-19 16:07:21 PST	44294	Allocated	Allocated	unknown	[img_Mod2_JoshuaWirtz-01.E01]vol_02(COL590M3)Scre...		76e9f1936d
DiskManagement.log				2026-01-19 16:07:16 PST	0000-00-00 00:00:00	2026-01-19 16:07:16 PST	2026-01-19 16:07:13 PST	44294	Allocated	Allocated	unknown	[img_Mod2_JoshuaWirtz-02.E01]vol_02(DiskManagemen...		
ScreenShot 2026-01-19 16:06:59.png				2026-01-19 16:06:59 PST	0000-00-00 00:00:00	2026-01-19 16:07:20 PST	2026-01-19 16:07:21 PST	44294	Unallocated	Unallocated	unknown	[img_Mod2_JoshuaWirtz-02.E01]vol_02(COL590M3)Scre...		
ROX00000.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	44294	Unallocated	Unallocated	unknown	[img_Mod2_JoshuaWirtz-02.E01]vol_02(Carved)Reed1...		

The 'Metadata' pane shows the following information for the selected file:

- Name: [img_Mod2_JoshuaWirtz-01.E01]vol_02(DiskManagement.log)
- Type: File System
- HTIME Type: mmap.log
- Size: 44294
- File Name Allocation: Allocated
- Metadata Allocation: Allocated
- Modified: 2026-01-19 16:07:16 PST
- Accessed: 2026-01-19 16:07:20 PST
- Created: 2026-01-19 16:07:13 PST
- Changed: 0000-00-00 00:00:00
- MD5: 76e9f1936d5f6e374326999999999999
- SHA-256: 3d492d67381c4b4b1c3f9b4e4c7c32c5e5a0f9e4031245089de980791ca01
- Hash Lookup Results: UNKNOWN
- Internal ID: 0

Original File location

10. Are the dates the same?

Yes, the dates are the same.

11. Are the hash values the same?

No, the hashes are different

12. Can you tell when the file was deleted?

The file was deleted at 16:27 {ST

References

Wortz, J. (2026). Various Images [Digital]. Personal PC, Oceanside, CA.