

## Lab Report

Name: Inor Wang

Title: Volume Shadow Copy Analysis

Case: 25-T104

Date: 10/02/2025

## *Table of Contents*

<b>Document Revision History .....</b>	<b>3</b>
<b>Executive Summary .....</b>	<b>4</b>
<b>Synopsis .....</b>	<b>6</b>
<b>Evidence Analyzed .....</b>	<b>7</b>
<b>Tools Used .....</b>	<b>8</b>
Workstation .....	8
Software.....	8
<b>Analysis Findings.....</b>	<b>9</b>
Overview of Examination Procedures .....	9
Evidence Reviewed .....	9
Key Findings .....	10
<b>Conclusion.....</b>	<b>28</b>
<b>References .....</b>	<b>29</b>

Document Revision History

Name	Revision Date	Version	Description
Inor Wang	10/01/2025	0.1	Draft
Inor Wang	10/02/2025	0.2	Draft

## Executive Summary

On October 1, 2025, Inor Wang submitted a forensic report to Professor Jacob D. Stauffer documenting an examination of Windows Volume Shadow Copies (VSCs) captured in shadow-copy-capture.vmdk.zip. The objective was to determine whether specific files changed across snapshots, identify co-occurring file modifications, and validate findings at the NTFS/MFT level. The evidence set was verified with MD5, SHA-1, and SHA-256 hashes to preserve integrity and support a defensible chain of custody. The workflow was step-by-step and reproducible, with exact offsets, commands, and screenshots.

Key findings from the examination are as follows:

- **Snapshot Baseline:** The oldest VSC used for comparison was ShadowCopy 7 (2019-01-17 22:15:28, system filestamp). Subsequent analyses references v7-v10.
- **\\Docs\\text2.txt:** No content change across v7–v10. Timestamps remained constant (Modified 2019-01-17 13:54:31 UTC; Created 13:49:48 UTC; Entry Modified 13:56:44 UTC). Hex analysis of the MFT confirmed a resident \$DATA (0x80) stream with Value Length = 0x1C (28 bytes) at offset 0x00D8B154, matching the visible string “Normal Activity in text2.txt.” Extra bytes seen in hex were resident-attribute slack/unused space, not logical file content.
- **\\Docs\\doc3.doc:** Content changed once between v7 and v8.
  - v7 content: “Incriminating Evidence in doc3.doc”.
  - v8-v10 content: “Change made to doc3.doc”.
  - Correlated timestamp shift: Modified/Entry Modified = 2019-01-17 14:17:31 UTC (v8).
- **\\Pictures\\drone.jpg:** Content changed twice at v9 and v10, text overlay on image.
  - v7-v8: drone image (no text overlay).
  - v9: same image with text overlay of “Incriminating Evidence in drone.jpg” (Modified/Entry Modified 14:21:53 UTC).
  - v10: same image with text overlay of “Normal Activity in drone.jpg” (Modified/Entry Modified 14:21:53 UTC).

- **Co-occurring file changes in \Docs within ~5 minutes of doc3.doc:** Multiple files were altered in close temporal proximity to the doc3.doc edit (14:17:31 UTC).
  - text4.txt: 14:16:31 UTC (content changed to “Change made to text4.txt”).
  - doc2.doc: 14:19:20 UTC (content changed to “Change made to doc2.doc”).
  - text5.txt: 14:20:15 UTC (content changed to “Change made to text5.txt”).
- **Tool Comparison:**
  - ShadowExplorer: GUI browsing and file export from VSCs; no VSC metadata view.
  - VSSadmin: Metadata-only; no file browsing/export capabilities
  - ShadowCopyView: Combines both, filesystem browsing + export and VSC metadata. This lab was conducted mostly using ShadowCopyView.

The evidence demonstrates that text2.txt remained unchanged across all snapshots, while doc3.doc and drone.jpg exhibited discrete, timestamped content modifications, and text4.txt, doc2.doc, and text5.txt changed within minutes of the doc3.doc edit, consistent with intentional, coordinated activity. Hex-level NTFS review (MFT, \$DATA) substantiated logical content lengths and explained residual bytes as attribute slack. As a best practice, examining multiple tools (ShadowExplorer, ShadowCopyView, VSSadmin, WinHex) was essential to reconcile data and metadata views, reduce the risk of tool-specific blind spots, and produce accurate, defensible findings.

The methods and results of this investigation should be considered in the context of learning how to navigate the volume shadow copies to find actionable insights for digital forensics investigations.

## Synopsis

A set of Volume Shadow Copies (VSCs) from a Windows 7 system, packaged as shadow-copy-capture.vmdk.zip, was provided for offline analysis. The examiner conducted a forensic review to identify content and metadata changes across four shadow copies, focusing on \Docs\text2.txt, \Docs\doc3.doc, and \Pictures\drone.jpg, and to determine any additional files in \Docs modified within five minutes of doc3.doc. The examiner also located the MFT entry for \Docs\text2.txt in the oldest VSC difference file using a hex editor and explained the findings in the context of NTFS structures. The workflow is step-by-step and reproducible, with explicit tool usage (WinHex/X-Ways, ShadowExplorer, ShadowCopyView/NirSoft, and vssadmin) and annotated screenshots embedded inline.

### Client Questions:

1. Determine if the content of the \Docs\text2.txt file changed over the course of the four volume shadow copies in the image. If it did not change, explain how you know this. If it did change, explain how and when the content changed. (By 'explain how,' I mean provide screen print snippets and/or visually describe the change. By 'when,' I mean provide the exact modification date/time stamp when the change took place.)
2. Do the same for \Docs\doc3.doc
3. Do the same for \Pictures\drone.jpg
4. What other file(s) in the Docs folder changed within five minutes of doc3.doc? How and when was it changed?
5. Using a hex editor, find the MFT entry for \Docs\text2.txt in the oldest VSC difference file. Provide a screen print of the sector containing the file content. Describe and explain what you see, relative to the NTFS file system.
6. Compare (what's similar?) and contrast (what's different) with regard to the data and metadata parsed by ShadowExplorer ([shadowexplorer.com](http://shadowexplorer.com)), ShadowCopyView ([NirSoft.net](http://NirSoft.net)), and VSSadmin (native, built-in Windows command line utility).

### Scope of Work:

- Acquisition of the evidence file from Professor Stauffer in the UTSA Canvas website.
- Analysis of shadow copy directory capture using WinHex, ShadowExplorer, ShadowCopyView, and VSSadmin.
- Verification of evidentiary integrity using MD5, SHA1, and SHA256 cryptographic hashes.

## Evidence Analyzed

This section provides details of the digital evidence collected

<b>Evidence ID</b>	<b>E001</b>
<b>Name</b>	shadow-copy-capture.vmdk.zip
<b>Type</b>	Zip archive data, at least v2.0 to extract, compression method=deflate
<b>Size</b>	5.78 MB
<b>MD5</b>	1FC73360C4B3933ED966B7EFB51EE69A
<b>SHA1</b>	FFCABE3438B90DC3B88EFD2D5DBDDFA32C445062
<b>SHA256</b>	43A0F545832909256EB901FAFD5EB273842528E4B7583198CDC57134E35434F7

## Tools Used

### Workstation

Hostname	Operating System	Build	Physical / Virtual	Built
IS-4523-001-WINDOWS	Windows 11	2021	Virtual	09/06/2025

### Software

Name	Version	Release	Purpose
WinHex (X-Ways)	21.0	Jun 2025	Hex/disk/RAM editor; examine and carve artifacts (incl. Registry hives) and image media
Shadow Explorer	0.9.462	Sep 2016	Enumerate Shadow Copies and export earlier versions of files/folders
ShadowCopyView (NirSoft)	1.16	Dec 2023	View shadow snapshots; copy out previous file versions for analysis
VSSadmin (Microsoft)	N/A	Sep 2025	List/manage shadow copies & storage
FTK Imager (AccessData)	4.5.0.3	Sep 2020	Mounts the .VMDK file, enabling analysis of volume shadow copies
LibreOffice Writer (The Document Foundation)	25.8.1.1	Aug 2025	Word processing; used to read contents of .doc files
Notepad (Microsoft)	11.2507.26.0	Sep 2025	Plain text editing; used to read contents of .txt files
Photos (Microsoft)	2025.11080.28001.0	Sep 2025	Image viewing and basic editing; used to view contents of .jpg files



## Analysis Findings

### Overview of Examination Procedures

The forensic analysis of the provided **Volume Shadow Copies (VSCs)**, captured in shadow-copy-capture.vmdk.zip and supplied by Professor Stauffer, was conducted by the **examiner** on a mounted Windows 7 volume. The evidence set was verified via **MD5, SHA-1, and SHA-256** to ensure integrity and a defensible chain of custody. The examiner performed a step-by-step, reproducible workflow with **inline screenshots** and exact commands/paths, in accordance with the assignment rubric and required template.

Additional targeted analysis was performed using:

- **WinHex (X-Ways)** → to examine NTFS structures, locate the \Docs\text2.txt MFT record in the oldest VSC difference file, and capture hex-level screenshots tied to sector/offset references.
- **ShadowExplorer** → to enumerate shadow copies, browse prior file versions (e.g., \Docs\text2.txt, \Docs\doc3.doc, \Pictures\drone.jpg), and export items for comparison across the four VSCs.
- **ShadowCopyView (NirSoft)** → to list and inspect VSC snapshots, correlate snapshot creation times with file modification events, and extract prior versions for side-by-side content/metadata comparison.
- **VSSadmin (Microsoft)** → to validate shadow storage and snapshot inventory (vssadmin list shadows, vssadmin list shadowstorage) and to timestamp snapshots for “when” analyses.
- **FTK Imager (AccessData)** → mounted the .vmdk file, allowing the examiner to analyze of the volume shadow copies using external tools listed previously.

Throughout the process, all findings were documented, and cryptographic hash values were maintained for validation.

### Evidence Reviewed

1. **shadow-copy-capture.vmdk.zip (E001):** Shadow copy directory capture

## Key Findings

1. Determine if the content of the \Docs\text2.txt file changed over the course of the four volume shadow copies in the image. If it did not change, explain how you know this. If it did change, explain how and when the content changed. (By 'explain how,' I mean provide screen print snippets and/or visually describe the change. By 'when,' I mean provide the exact modification date/time stamp when the change took place.)

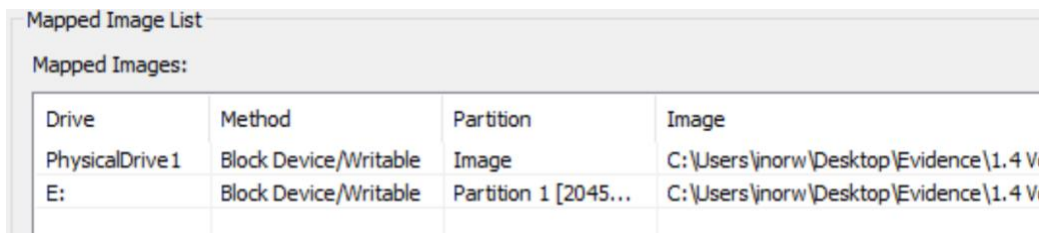
- **Analysis Performed:**

- The volume shadow copies of “Windows 7 Shadow 20190117.vmdk” was analyzed through NirSoft’s ShadowCopyView application.
- The “Windows 7 Shadow 20190117.vmdk” image file was mounted to the filesystem with write permissions through AccessData’s FTK Imager application as shown in Figure 1.
- The examiner analyzed the Modified Time, Created Time, and Entry Modified Time of text2.txt throughout all volume shadow copies as shown in Figures 2-5.
  - The modified time (01/17/2019 1:54:31 PM UTC), created time (01/17/2019 1:49:48 PM UTC), and entry modified time (01/17/2019 1:56:44 PM UTC) are all the same amongst all volume shadow copies.
- The examiner copied text2.txt file from all volume shadow copies to the filesystem as shown in Figure 6.
- The examiner accessed text2.txt file from all volume shadow copies, as shown in Figure 7, to examine the contents to determine if the file’s contents have been changed.
  - The content of the .txt file stay the same amongst all volume shadow copies. The content is: “Normal Activity in text2.txt”

- **Answer:**

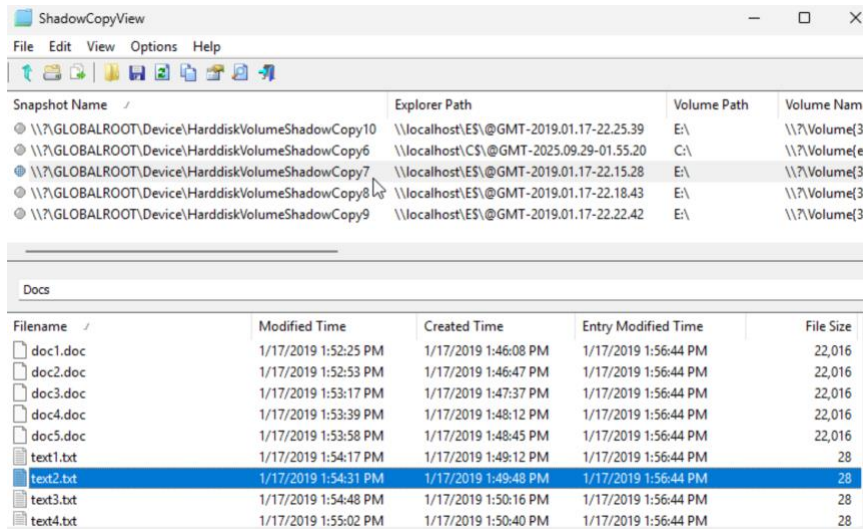
The content of \Docs\text2.txt file has NOT changed over the course of the four volume shadow copies in the image. As shown in Figures 2-5, the Modified Time, Created Time, and Entry Modified Time of text2.txt has stayed consistent amongst all volume shadow copies. Additionally, the examiner copied text2.txt file onto his filesystem and the examiner accessed each .txt file to view the contents as shown in Figure 6 and 7. The contents stayed consistent amongst all volume shadow copies. **Therefore again, the content of \Docs\text2.txt has NOT changed over the course of the four volume shadow copies as shown in Figures 2-7.**

- **Supporting Evidence:**



Drive	Method	Partition	Image
PhysicalDrive1	Block Device/Writable	Image	C:\Users\jnorw\Desktop\Evidence\1.4 Vc
E:	Block Device/Writable	Partition 1 [2045...	C:\Users\jnorw\Desktop\Evidence\1.4 Vc

Figure 1. The “Windows 7 Shadow 20190117.vmdk” image file mounted as E: with writable settings on

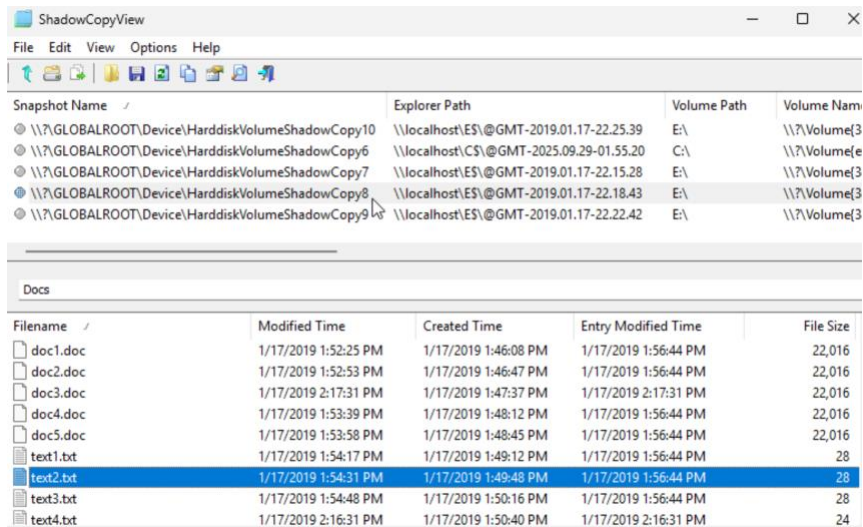


Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 1:52:53 PM	1/17/2019 1:46:47 PM	1/17/2019 1:56:44 PM	22,016
doc3.doc	1/17/2019 1:53:17 PM	1/17/2019 1:47:37 PM	1/17/2019 1:56:44 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016
text1.txt	1/17/2019 1:54:17 PM	1/17/2019 1:49:12 PM	1/17/2019 1:56:44 PM	28
text2.txt	1/17/2019 1:54:31 PM	1/17/2019 1:49:48 PM	1/17/2019 1:56:44 PM	28
text3.txt	1/17/2019 1:54:48 PM	1/17/2019 1:50:16 PM	1/17/2019 1:56:44 PM	28
text4.txt	1/17/2019 1:55:02 PM	1/17/2019 1:50:40 PM	1/17/2019 1:56:44 PM	28

Figure 2. Metadata of text2.txt in volume shadow copy v7 within ShadowCopyView

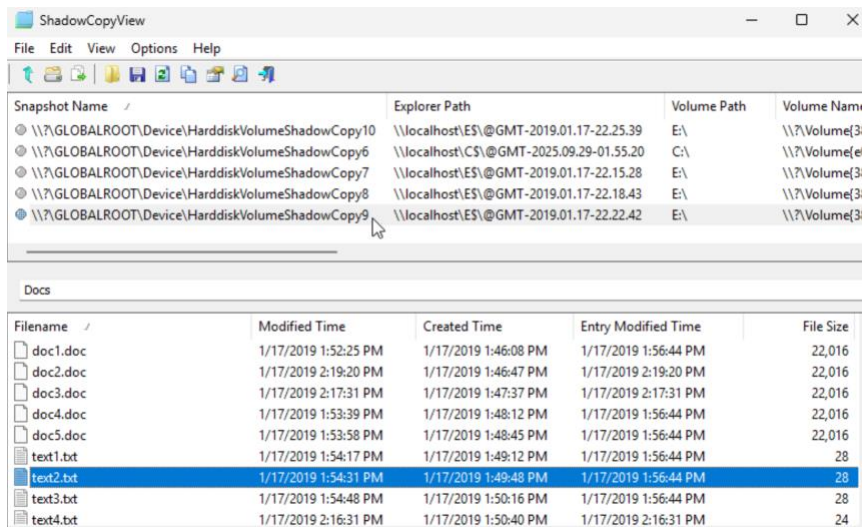


Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 1:52:53 PM	1/17/2019 1:46:47 PM	1/17/2019 1:56:44 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016
text1.txt	1/17/2019 1:54:17 PM	1/17/2019 1:49:12 PM	1/17/2019 1:56:44 PM	28
text2.txt	1/17/2019 1:54:31 PM	1/17/2019 1:49:48 PM	1/17/2019 1:56:44 PM	28
text3.txt	1/17/2019 1:54:48 PM	1/17/2019 1:50:16 PM	1/17/2019 1:56:44 PM	28
text4.txt	1/17/2019 2:16:31 PM	1/17/2019 1:50:40 PM	1/17/2019 2:16:31 PM	24

Figure 3. Metadata of text2.txt in volume shadow copy v8 within ShadowCopyView



Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 2:19:20 PM	1/17/2019 1:46:47 PM	1/17/2019 2:19:20 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016
text1.txt	1/17/2019 1:54:17 PM	1/17/2019 1:49:12 PM	1/17/2019 1:56:44 PM	28
text2.txt	1/17/2019 1:54:31 PM	1/17/2019 1:49:48 PM	1/17/2019 1:56:44 PM	28
text3.txt	1/17/2019 1:54:48 PM	1/17/2019 1:50:16 PM	1/17/2019 1:56:44 PM	28
text4.txt	1/17/2019 2:16:31 PM	1/17/2019 1:50:40 PM	1/17/2019 2:16:31 PM	24

Figure 4. Metadata of text2.txt in volume shadow copy v9 within ShadowCopyView

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 2:19:20 PM	1/17/2019 1:46:47 PM	1/17/2019 2:19:20 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016
text1.txt	1/17/2019 1:54:17 PM	1/17/2019 1:49:12 PM	1/17/2019 1:56:44 PM	28
text2.txt	1/17/2019 1:54:31 PM	1/17/2019 1:49:48 PM	1/17/2019 1:56:44 PM	28
text3.txt	1/17/2019 1:54:48 PM	1/17/2019 1:50:16 PM	1/17/2019 1:56:44 PM	28
text4.txt	1/17/2019 2:16:31 PM	1/17/2019 1:50:40 PM	1/17/2019 2:16:31 PM	24

Figure 5. Metadata of text2.txt in volume shadow copy v10 within ShadowCopyView

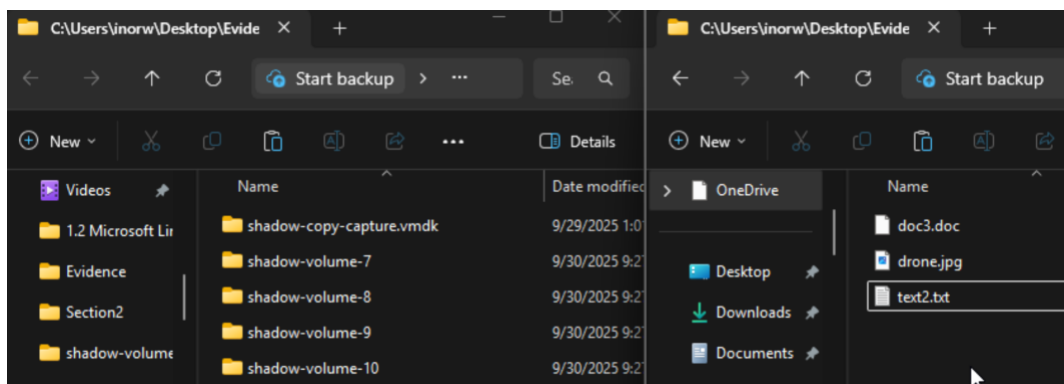


Figure 6. Showing filesystem containing four directories named, "shadow-volume-\*" (7-10), containing: doc3.doc, drone.jpg, and text2.txt. These files were copied from their corresponding volume shadow copy within ShadowCopyView

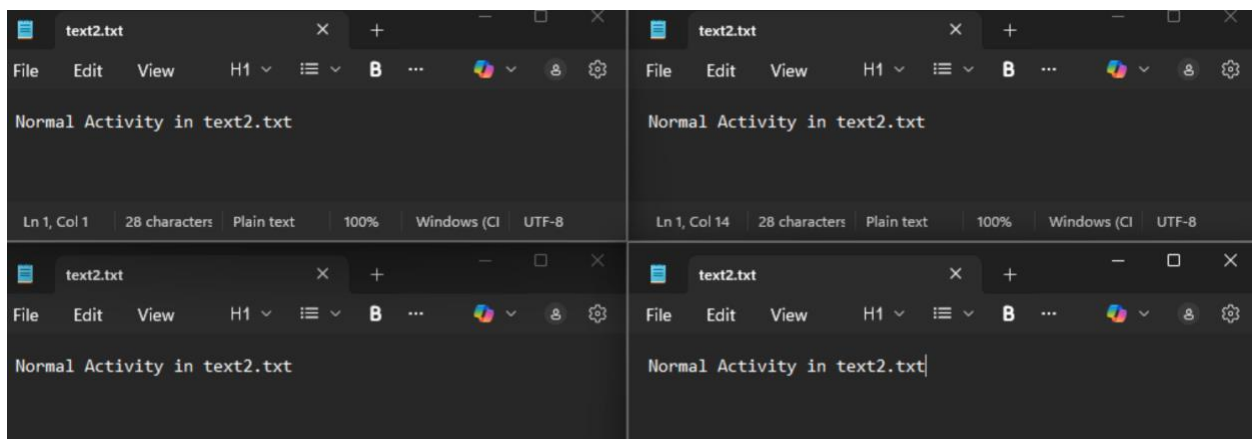


Figure 7. All four text2.txt from volume shadow copy v7-10 accessed via Windows 11 Notepad (showing no content change)

## 2. Do the same for \Docs\doc3.doc

- **Analysis Performed:**

- The volume shadow copies of “Windows 7 Shadow 20190117.vmdk” was analyzed through NirSoft’s ShadowCopyView application.
- The examiner analyzed the Modified Time, Created Time, and Entry Modified Time of doc3.doc throughout all volume shadow copies as shown in Figures 8-11.
  - doc3.doc within volume shadow copy v7:
    - Modified time is *01/17/2019 1:53:17 PM UTC*
    - Created time is *01/17/2019 1:47:37 PM UTC*
    - Entry modified time is *01/17/2019 1:56:44 PM UTC*
  - doc3.doc within volume shadow copy v8:
    - Modified time is *01/17/2019 2:17:31 PM UTC*
    - Created time is *01/17/2019 1:47:37 PM UTC*
    - Entry modified time is *01/17/2019 2:17:31 PM UTC*
  - doc3.doc within volume shadow copy v9:
    - Modified time is *01/17/2019 2:17:31 PM UTC*
    - Created time is *01/17/2019 1:47:37 PM UTC*
    - Entry modified time is *01/17/2019 2:17:31 PM UTC*
  - doc3.doc within volume shadow copy v10:
    - Modified time is *01/17/2019 2:17:31 PM UTC*
    - Created time is *01/17/2019 1:47:37 PM UTC*
    - Entry modified time is *01/17/2019 2:17:31 PM UTC*
- The examiner accessed doc3.doc file from all volume shadow copies, as shown in Figure 12, to examine the contents to determine if the file’s contents have been changed.
  - The content of the .doc file has **not stayed the same** amongst all volume shadow copies.
  - The content of doc3.doc within the volume shadow copy v7 is: “Incriminating Evidence in doc3.doc”
  - The content of doc3.doc within the volume shadow copy v8-10 is: “Change made to doc3.doc”

- **Answer:**

The content of \Docs\doc3.doc file has changed over the course of the four volume shadow copies in the image. As shown in Figure 12, the content of doc3.doc within the volume shadow copy v7 was “Incriminating Evidence in doc3.doc” and then was changed to “Change made to doc3.doc” within the volume shadow copy v8 and stayed the same all in volume shadow copy v9-10. Additionally, the modified and entry modified time changed from 01/17/2019 1:53:17 PM UTC (doc3.doc within volume shadow copy v7) to 01/17/2019 2:17:31 PM UTC (doc3.doc within volume shadow copy v8) as shown in Figures 8 and 9. **Therefore in conclusion, the content of \Docs\doc3.doc was changed from “Incriminating Evidence in doc3.doc” to “Change made to doc3.doc” at 01/17/2019 2:17:31 PM UTC from volume shadow copy v7 to v8, as shown in Figures 8-12.**



- **Supporting Evidence:**

ShadowCopyView

File Edit View Options Help

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3...}

Docs

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 1:52:53 PM	1/17/2019 1:46:47 PM	1/17/2019 1:56:44 PM	22,016
doc3.doc	1/17/2019 1:53:17 PM	1/17/2019 1:47:37 PM	1/17/2019 1:56:44 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016

Figure 8. Metadata of doc3.doc in volume shadow copy v7 within ShadowCopyView

ShadowCopyView

File Edit View Options Help

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3...}

Docs

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 1:52:53 PM	1/17/2019 1:46:47 PM	1/17/2019 1:56:44 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016

Figure 9. Metadata of doc3.doc in volume shadow copy v8 within ShadowCopyView

ShadowCopyView

File Edit View Options Help

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3...}

Docs

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 2:19:20 PM	1/17/2019 1:46:47 PM	1/17/2019 2:19:20 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016

Figure 10. Metadata of doc3.doc in volume shadow copy v9 within ShadowCopyView

The screenshot shows the ShadowCopyView application. The top pane lists several volume shadow copies. The bottom pane shows the contents of 'doc3.doc' from volume shadow copy v10, with a table of metadata.

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 2:19:20 PM	1/17/2019 1:46:47 PM	1/17/2019 2:19:20 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016

Figure 11. Metadata of doc3.doc in volume shadow copy v10 within ShadowCopyView

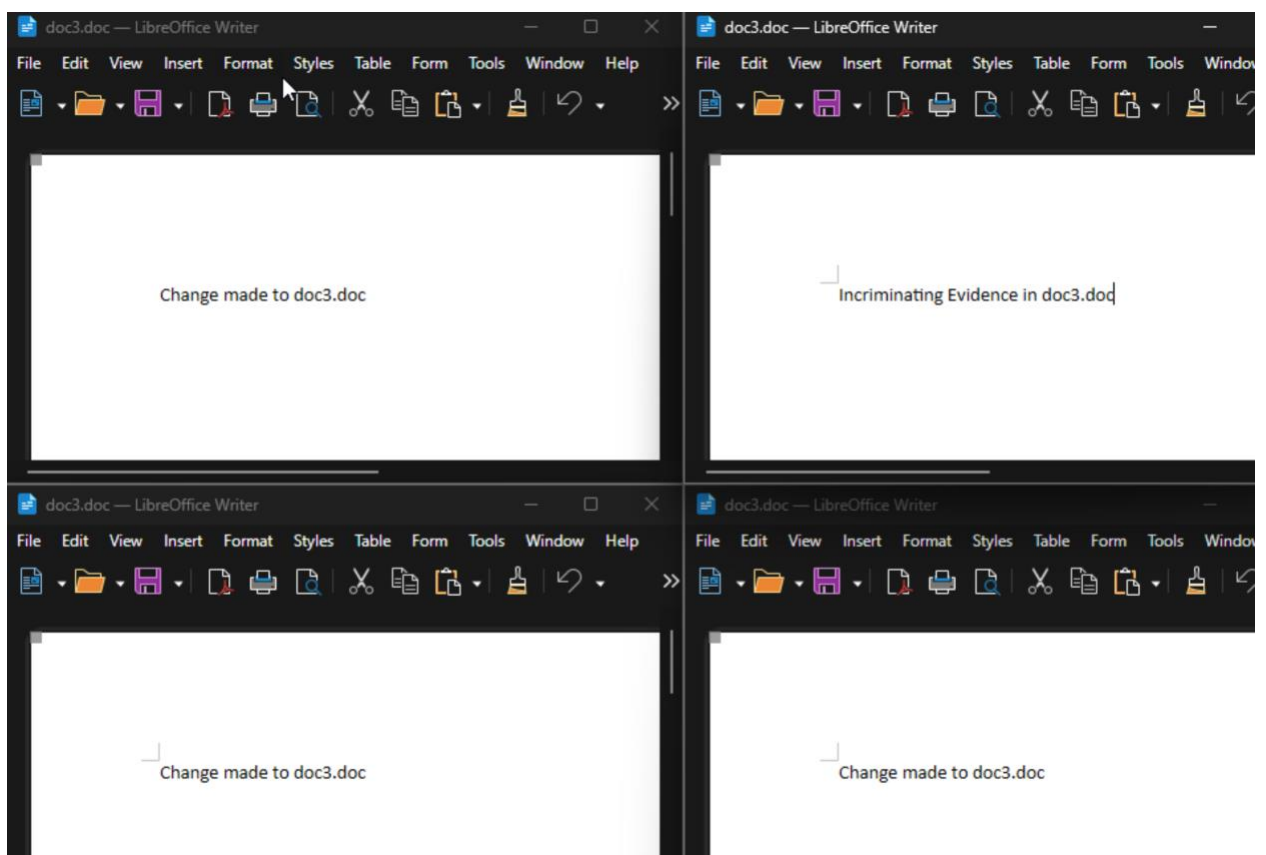


Figure 12. All four doc3.doc from volume shadow copy v7-10 accessed via LibreOffice Writer (showing content change)

### 3. Do the same for \Pictures\drone.jpg

- **Analysis Performed:**

- The volume shadow copies of “Windows 7 Shadow 20190117.vmdk” was analyzed through NirSoft’s ShadowCopyView application.
- The examiner analyzed the Modified Time, Created Time, and Entry Modified Time of drone.jpg throughout all volume shadow copies as shown in Figures 13-16.
  - drone.jpg within volume shadow copy v7:
    - Modified time is *01/17/2019 2:04:45 PM UTC*
    - Created time is *01/17/2019 2:04:45 PM UTC*
    - Entry modified time is *01/17/2019 2:04:45 PM UTC*
  - drone.jpg within volume shadow copy v8:
    - Modified time is *01/17/2019 2:04:45 PM UTC*
    - Created time is *01/17/2019 2:04:45 PM UTC*
    - Entry modified time is *01/17/2019 2:04:45 PM UTC*
  - drone.jpg within volume shadow copy v9:
    - Modified time is *01/17/2019 2:21:53 PM UTC*
    - Created time is *01/17/2019 2:04:45 PM UTC*
    - Entry modified time is *01/17/2019 2:21:53 PM UTC*
  - drone.jpg within volume shadow copy v10:
    - Modified time is *01/17/2019 2:24:12 PM UTC*
    - Created time is *01/17/2019 2:04:45 PM UTC*
    - Entry modified time is *01/17/2019 2:24:12 PM UTC*
- The examiner accessed drone.jpg file from all volume shadow copies, as shown in Figure 17-18, to examine the contents to determine if the file’s contents have been changed.
  - The content of the .jpg file has **not stayed the same** amongst all volume shadow copies.
  - The content of drone.jpg within the volume shadow copy v7-8 contains an image of a drone.
  - The content of drone.jpg within the volume shadow copy v9 contains an image of a drone and a text overlay stating: “Incriminating Evidence in drone.jpg”.
  - The content of drone.jpg within the volume shadow copy v10 contains an image of a drone and a text overlay stating: “Normal activity in drone.jpg”.

- **Answer:**

The content of \Pictures\drone.jpg file has changed over the course of the four volume shadow copies in the image. As shown in Figure 17, the content of drone.jpg within volume shadow copy v7-8 contained a picture of a drone, then was changed to the same picture of a drone but with text overlay stating “Incriminating Evidence in drone.jpg” within drone.jpg in volume shadow copy v9, and then lastly was changed to the same picture of a drone but with text overlay stating “Normal Activity in drone.jpg”. Additionally, the modified and entry modified time changed from 01/17/2019 2:04:45 PM UTC (drone.jpg in volume shadow copy v7-8) to 01/17/2019 2:21:53 PM UTC



(drone.jpg in volume shadow copy v9) and then to 01/17/2019 2:24:12 PM UTC (drone.jpg in volume shadow copy v10) as shown in Figures 17 and 18. **Therefore in conclusion, the content of \Pictures\drone.jpg was changed. The content started out as an image of a drone (volume shadow copy v7-8), then to the same image with text overlay stating “Incriminating Evidence in drone.jpg” (volume shadow copy v9), and then to the same image with text overlay stating “Normal Activity in drone.jpg” (volume shadow copy v10). The content was modified at 01/17/2019 2:21:53 PM UTC and 01/17/2019 2:24:12 PM UTC.**

- **Supporting Evidence:**

The screenshot shows the ShadowCopyView application window. The top table lists snapshots, with 'ShadowCopy7' selected. Below, the 'Pictures' folder is expanded, showing a list of files. 'drone.jpg' is highlighted in blue.

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3...}

Filename	Modified Time	Created Time	Entry Modified Time	File Size
bear.jpg	1/17/2019 2:01:07 PM	1/17/2019 2:01:07 PM	1/17/2019 2:14:16 PM	35,660
bokeh.jpg	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	22,296
car.jpg	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	44,122
coast.jpg	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	58,546
dark sky.jpg	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	75,371
drone.jpg	1/17/2019 2:04:45 PM	1/17/2019 2:04:45 PM	1/17/2019 2:04:45 PM	29,921
ferris wheel.jpg	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	90,216

Figure 13. Metadata of drone.jpg in volume shadow copy v7 within ShadowCopyView

The screenshot shows the ShadowCopyView application window. The top table lists snapshots, with 'ShadowCopy8' selected. Below, the 'Pictures' folder is expanded, showing a list of files. 'drone.jpg' is highlighted in blue.

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3...}

Filename	Modified Time	Created Time	Entry Modified Time	File Size
bear.jpg	1/17/2019 2:01:07 PM	1/17/2019 2:01:07 PM	1/17/2019 2:14:16 PM	35,660
bokeh.jpg	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	22,296
car.jpg	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	44,122
coast.jpg	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	58,546
dark sky.jpg	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	75,371
drone.jpg	1/17/2019 2:04:45 PM	1/17/2019 2:04:45 PM	1/17/2019 2:04:45 PM	29,921
ferris wheel.jpg	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	90,216

Figure 14. Metadata of drone.jpg in volume shadow copy v8 within ShadowCopyView

ShadowCopyView

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\.\Volume{3}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\.\Volume{e}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\.\Volume{3}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\.\Volume{3}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\.\Volume{3}

Filename	Modified Time	Created Time	Entry Modified Time	File Size
bear.jpg	1/17/2019 2:01:07 PM	1/17/2019 2:01:07 PM	1/17/2019 2:14:16 PM	35,660
bokeh.jpg	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	22,296
car.jpg	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	44,122
coast.jpg	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	58,546
dark sky.jpg	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	75,371
drone.jpg	1/17/2019 2:21:53 PM	1/17/2019 2:04:45 PM	1/17/2019 2:21:53 PM	55,810
ferris wheel.jpg	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	90,216

Figure 15. Metadata of drone.jpg in volume shadow copy v9 within ShadowCopyView

ShadowCopyView

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\.\Volume{3}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\.\Volume{e}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\.\Volume{3}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\.\Volume{3}
\\.\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\.\Volume{3}

Filename	Modified Time	Created Time	Entry Modified Time	File Size
bear.jpg	1/17/2019 2:01:07 PM	1/17/2019 2:01:07 PM	1/17/2019 2:14:16 PM	35,660
bokeh.jpg	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	1/17/2019 2:02:02 PM	22,296
car.jpg	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	1/17/2019 2:02:56 PM	44,122
coast.jpg	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	1/17/2019 2:03:50 PM	58,546
dark sky.jpg	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	1/17/2019 2:04:18 PM	75,371
drone.jpg	1/17/2019 2:24:12 PM	1/17/2019 2:04:45 PM	1/17/2019 2:24:12 PM	54,420
ferris wheel.jpg	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	1/17/2019 2:05:19 PM	90,216

Figure 16. Metadata of drone.jpg in volume shadow copy v10 within ShadowCopyView

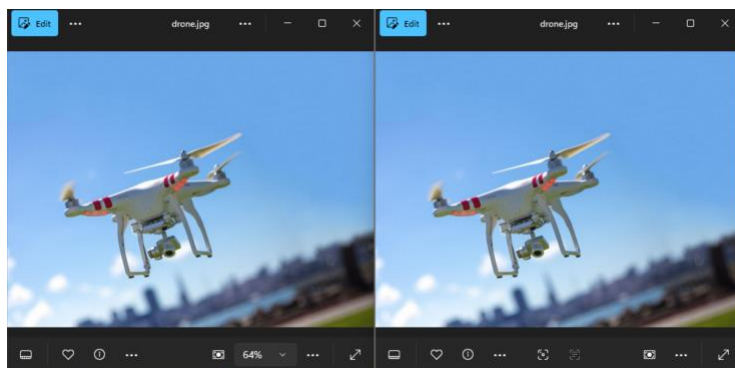


Figure 17. drone.jpg from volume shadow copy v7-8 accessed (showing no content change)

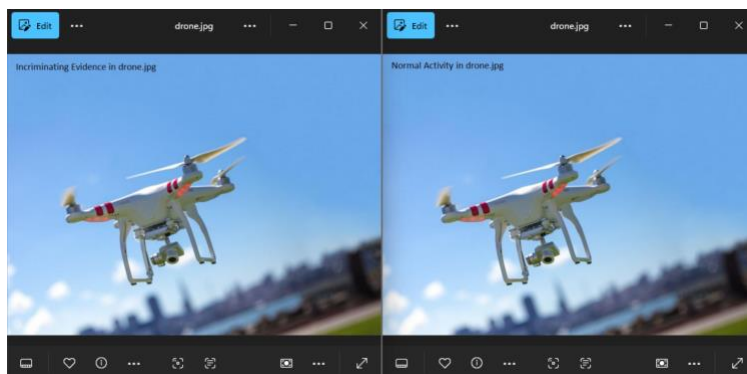


Figure 18. drone.jpg from volume shadow copy v9-10 accessed (showing content change)

*4. What other file(s) in the Docs folder changed within five minutes of doc3.doc? How and when was it changed?*

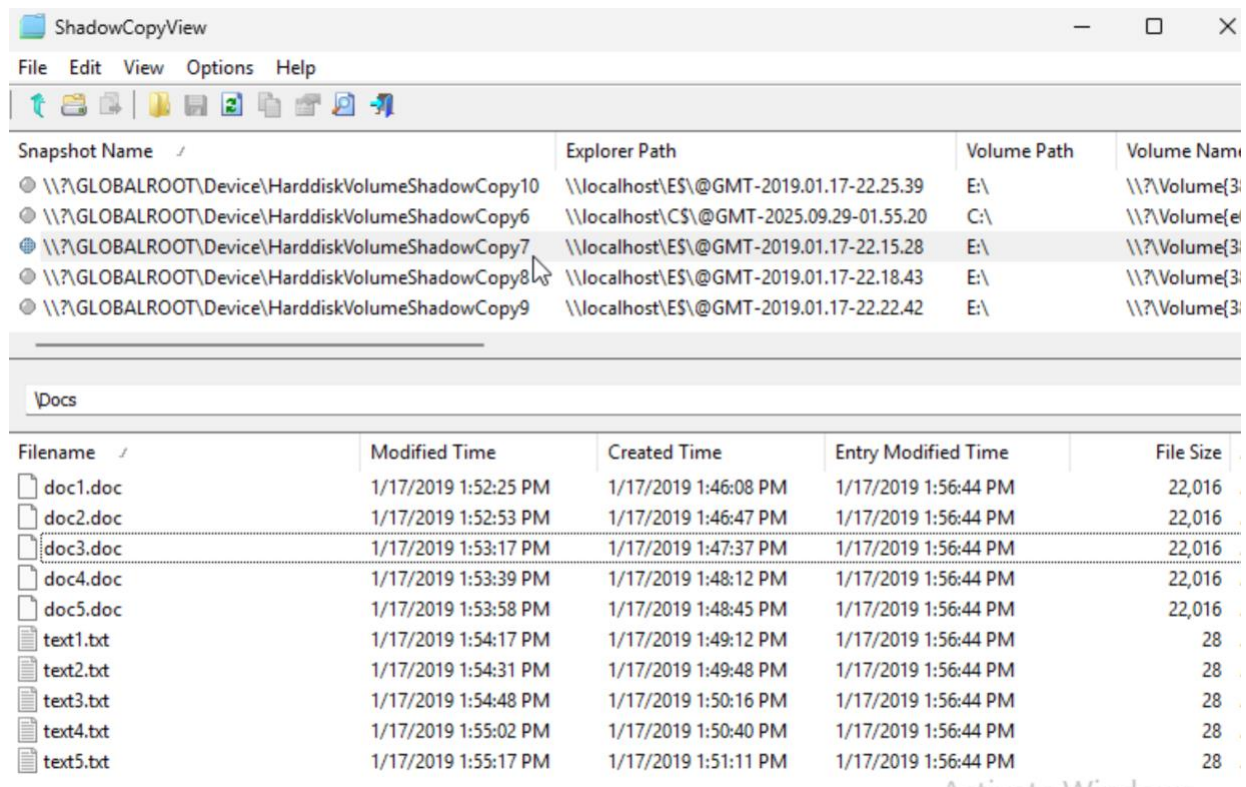
- **Analysis Performed:**

- The volume shadow copies of “Windows 7 Shadow 20190117.vmdk” was analyzed through NirSoft’s ShadowCopyView application.
- The examiner analyzed the Modified Time, Created Time, and Entry Modified Time of all files. The original state of all files is shown in Figure 19. The modification of text4.txt is shown in Figure 20, and modification of text5.txt and doc2.doc is shown in Figure 21.
  - Original state
    - text4.txt within volume shadow copy v7:
      - Modified time is *01/17/2019 01:55:02 PM UTC*
      - Entry modified time is *01/17/2019 01:56:44 PM UTC*
    - text5.txt within volume shadow copy v7:
      - Modified time is *01/17/2019 01:55:17 PM UTC*
      - Entry modified time is *01/17/2019 01:56:44 PM UTC*
    - doc2.doc within volume shadow copy v7:
      - Modified time is *01/17/2019 01:52:53 PM UTC*
      - Entry modified time is *01/17/2019 01:56:44 PM UTC*
  - Changed state
    - text4.txt within volume shadow copy v8:
      - Modified time is *01/17/2019 02:16:31 PM UTC*
      - Entry modified time is *01/17/2019 02:16:31PM UTC*
    - text5.txt within volume shadow copy v9:
      - Modified time is *01/17/2019 02:20:15 PM UTC*
      - Entry modified time is *01/17/2019 02:20:15PM UTC*
    - doc2.doc within volume shadow copy v9:
      - Modified time is *01/17/2019 02:19:20 PM UTC*
      - Entry modified time is *01/17/2019 02:19:20PM UTC*
- The examiner accessed text4.txt, text5.txt, and doc2.doc as shown in Figures 22-24.
  - The examiner accessed text4.txt file from volume shadow copy v7 and v8.
    - The content of text4.txt within volume shadow copy v7 is: “Normal Activity in text4.txt”.
    - The content of text4.txt within volume shadow copy v8 is: “Change made to text4.txt”.
  - The examiner accessed text5.txt file from volume shadow copy v7 and v9.
    - The content of text5.txt within volume shadow copy v7 is: “Normal Activity in text5.txt”.
    - The content of text5.txt within volume shadow copy v9 is: “Change made to text5.txt”.
  - The examiner accessed doc2.doc file in volume shadow copy v7 and v9.
    - The content of doc2.doc within volume shadow copy v7 is: “Normal Activity in doc2.doc”.
    - The content of doc2.doc within volume shadow copy v9 is: “Change made to doc2.doc”.

- **Answer:**

Within five minutes of the modification of doc3.doc, three other files in the Docs folder, text4.txt, text5.txt, and doc2.doc, were also changed. Specifically, *text4.txt* was modified on January 17, 2019, at 02:16:31 PM UTC, with its content altered from “Normal Activity in text4.txt” to “Change made to text4.txt” as shown in Figures 19, 20, and 22. Shortly afterward, *doc2.doc* was modified on January 17, 2019, at 02:19:20 PM UTC, changing from “Normal Activity in doc2.doc” to “Change made to doc2.doc” as shown in Figures 19, 21, and 24. Finally, *text5.txt* was modified on January 17, 2019, at 02:20:15 PM UTC, with its content updated from “Normal Activity in text5.txt” to “Change made to text5.txt” as shown in Figures 19, 21, and 23. These coordinated modifications, occurring within minutes of each other, indicate deliberate changes across multiple files in the Docs folder. **In conclusion, the evidence shows that text4.txt, text5.txt, and doc2.doc were intentionally altered in close proximity to the modification of doc3.doc.**

- **Supporting Evidence:**



The screenshot shows the ShadowCopyView application window. The top pane displays a list of Volume Shadow Copies. The bottom pane shows the contents of the 'Docs' folder within the selected shadow copy (v7).

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{e...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{3...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{3...}

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 1:52:53 PM	1/17/2019 1:46:47 PM	1/17/2019 1:56:44 PM	22,016
doc3.doc	1/17/2019 1:53:17 PM	1/17/2019 1:47:37 PM	1/17/2019 1:56:44 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016
text1.txt	1/17/2019 1:54:17 PM	1/17/2019 1:49:12 PM	1/17/2019 1:56:44 PM	28
text2.txt	1/17/2019 1:54:31 PM	1/17/2019 1:49:48 PM	1/17/2019 1:56:44 PM	28
text3.txt	1/17/2019 1:54:48 PM	1/17/2019 1:50:16 PM	1/17/2019 1:56:44 PM	28
text4.txt	1/17/2019 1:55:02 PM	1/17/2019 1:50:40 PM	1/17/2019 1:56:44 PM	28
text5.txt	1/17/2019 1:55:17 PM	1/17/2019 1:51:11 PM	1/17/2019 1:56:44 PM	28

Figure 19. Showing all the contents of the Docs folder within Volume Shadow Copy v7 (Original state of all files)



Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{...}

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 1:52:53 PM	1/17/2019 1:46:47 PM	1/17/2019 1:56:44 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016
text1.txt	1/17/2019 1:54:17 PM	1/17/2019 1:49:12 PM	1/17/2019 1:56:44 PM	28
text2.txt	1/17/2019 1:54:31 PM	1/17/2019 1:49:48 PM	1/17/2019 1:56:44 PM	28
text3.txt	1/17/2019 1:54:48 PM	1/17/2019 1:50:16 PM	1/17/2019 1:56:44 PM	28
text4.txt	1/17/2019 2:16:31 PM	1/17/2019 1:50:40 PM	1/17/2019 2:16:31 PM	24
text5.txt	1/17/2019 1:55:17 PM	1/17/2019 1:51:11 PM	1/17/2019 1:56:44 PM	28

Figure 20. Showing all the contents of the Docs folder within Volume Shadow Copy v8 (Text4.txt was modified)

Snapshot Name	Explorer Path	Volume Path	Volume Name
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10	\\localhost\ES\@GMT-2019.01.17-22.25.39	E:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6	\\localhost\CS\@GMT-2025.09.29-01.55.20	C:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7	\\localhost\ES\@GMT-2019.01.17-22.15.28	E:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8	\\localhost\ES\@GMT-2019.01.17-22.18.43	E:\	\\?\Volume{...}
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9	\\localhost\ES\@GMT-2019.01.17-22.22.42	E:\	\\?\Volume{...}

Filename	Modified Time	Created Time	Entry Modified Time	File Size
doc1.doc	1/17/2019 1:52:25 PM	1/17/2019 1:46:08 PM	1/17/2019 1:56:44 PM	22,016
doc2.doc	1/17/2019 2:19:20 PM	1/17/2019 1:46:47 PM	1/17/2019 2:19:20 PM	22,016
doc3.doc	1/17/2019 2:17:31 PM	1/17/2019 1:47:37 PM	1/17/2019 2:17:31 PM	22,016
doc4.doc	1/17/2019 1:53:39 PM	1/17/2019 1:48:12 PM	1/17/2019 1:56:44 PM	22,016
doc5.doc	1/17/2019 1:53:58 PM	1/17/2019 1:48:45 PM	1/17/2019 1:56:44 PM	22,016
text1.txt	1/17/2019 1:54:17 PM	1/17/2019 1:49:12 PM	1/17/2019 1:56:44 PM	28
text2.txt	1/17/2019 1:54:31 PM	1/17/2019 1:49:48 PM	1/17/2019 1:56:44 PM	28
text3.txt	1/17/2019 1:54:48 PM	1/17/2019 1:50:16 PM	1/17/2019 1:56:44 PM	28
text4.txt	1/17/2019 2:16:31 PM	1/17/2019 1:50:40 PM	1/17/2019 2:16:31 PM	24
text5.txt	1/17/2019 2:20:15 PM	1/17/2019 1:51:11 PM	1/17/2019 2:20:15 PM	24

Figure 21. Showing all the contents of the Docs folder within Volume Shadow Copy v8 (Text5.txt and doc2.doc was modified)

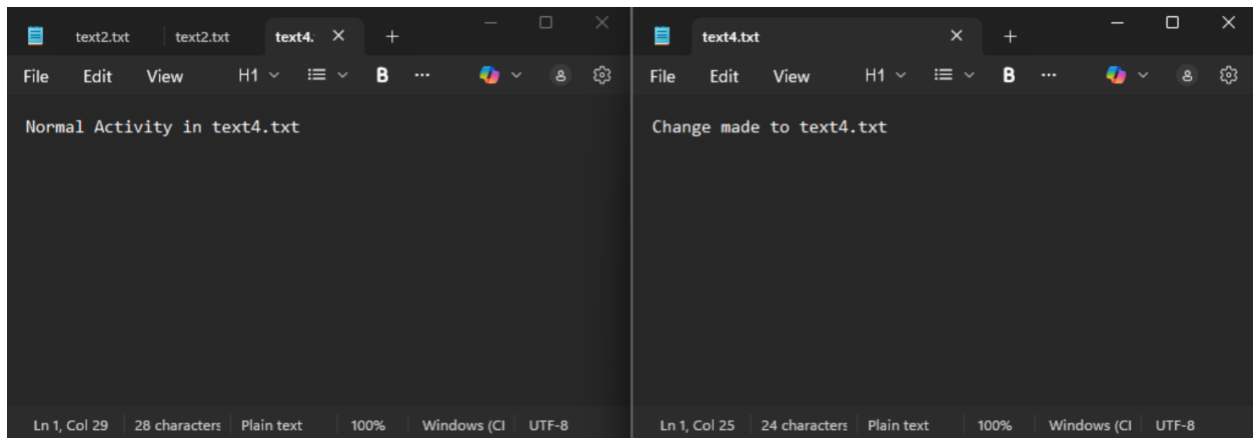


Figure 22. Showing the contents of text4.txt in volume shadow copy v7 and v8 (content was changed)

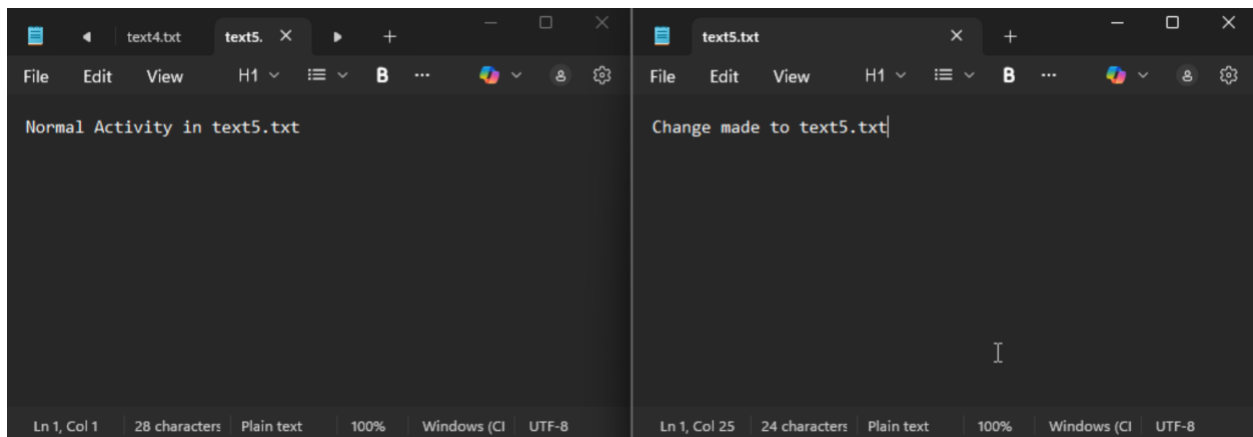


Figure 23. Showing the contents of text5.txt in volume shadow copy v7 and v9 (content was changed)

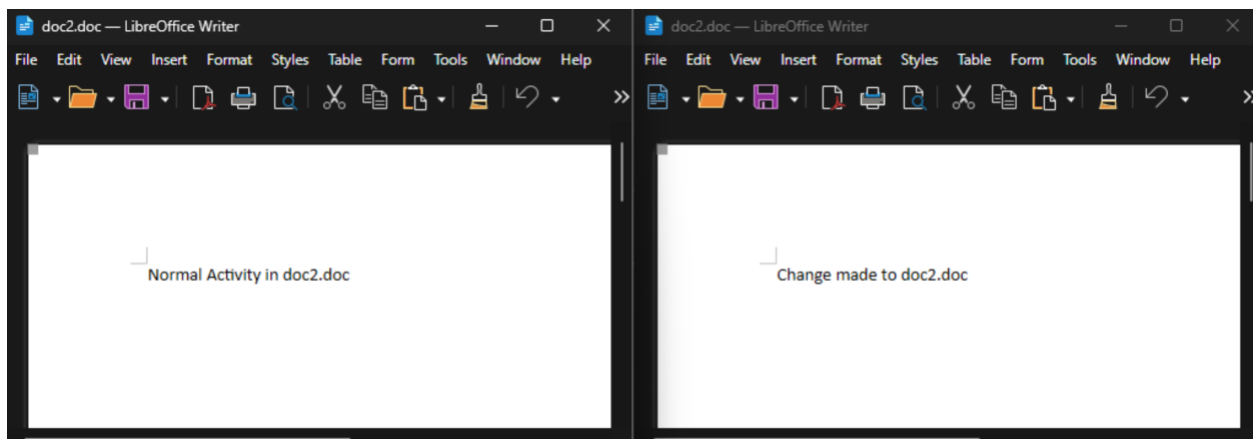


Figure 24. Showing the contents of doc2.doc in volume shadow copy v7 and v9 (content was changed)

5. Using a hex editor, find the MFT entry for \Docs\text2.txt in the oldest VSC difference file. Provide a screen print of the sector containing the file content. Describe and explain what you see, relative to the NTFS file system.

- **Analysis Performed:**

- The examiner mounted “Windows 7 Shadow 20190117.vmdk” in FTK Imager and then opened the E: drive (mounted drive) in WinHex, as shown in Figure 25.
- The examiner then found the oldest volume shadow copy difference file, as shown highlighted in Figure 26, and opened it within WinHex for further analysis.
- The examiner then located the MFT entry of text2.txt, spanning offsets 0x00D8B000 to 0x00D8B3F0, as shown in Figure 27.
  - The \$DATA attribute, beginning at offset 0x00D8B148, spans 700-bytes, ending at 0x00D8B3F0
    - This is because \$DATA is usually 700 bytes and starting from offset 0x00D8B148, with a 700-byte length, the ending offset is 0x00D8B3F0
  - The file content is: “Normal Activity in text2.txt”.
- Within the \$DATA attribute header, at offset 0x00D8B154, a 4-byte little-endian value (1C 00 00 00) indicates that the file content length is 28 bytes.
- As shown in Figure 28, when accessed via the NTFS file system in Windows 11 Notepad, the file content of text2.txt is: “Normal Activity in text2.txt”.

- **Answer:**

The file content of text2.txt within the oldest volume shadow copy difference file is consistent across both the hex editor (MFT entry) and the NTFS file system. The content is: “Normal Activity in text2.txt.” As shown in Figure 27, additional strings appear in the MFT entry that are not visible when the file is opened in the NTFS file system. These extra bytes are likely leftover slack space or metadata stored in the unused portion of the MFT record. The NTFS file system uses the Value Length field (at offset 0x00D8B154, showing “1C 00 00 00” = 28 in little-endian) to determine that the file has exactly 28 bytes of valid content. Therefore, only the string “Normal Activity in text2.txt” is displayed. **In conclusion, the hex editor view may reveal slack space or metadata beyond the logical content, but the NTFS file system correctly limits the file to its declared 28-byte length.**

- **Supporting Evidence:**

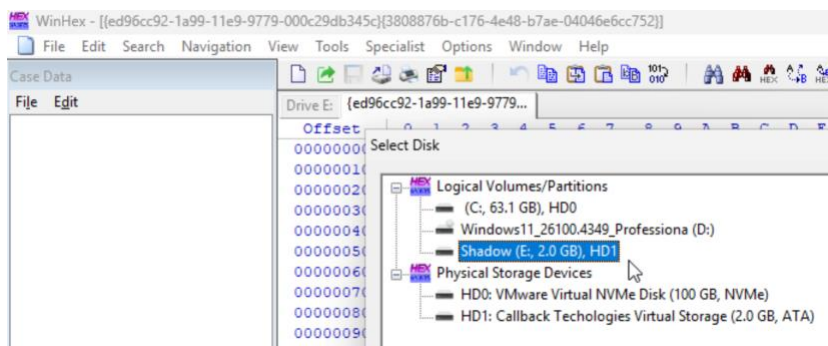


Figure 25. Opening the E: drive disk (“Windows 7 Shadow 20190117.vmdk”) in WinHex

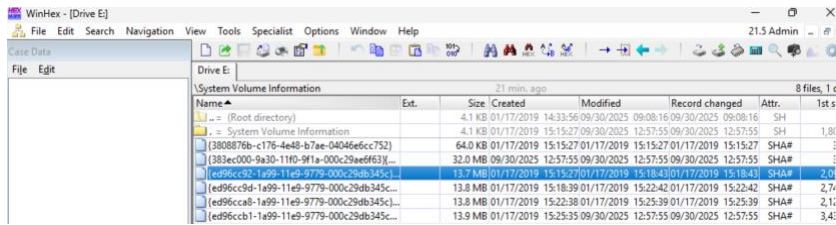


Figure 26. Finding the oldest volume shadow copy difference file within the mounted E: drive ("Windows 7 Shadow 20190117.vmdk") and opening it

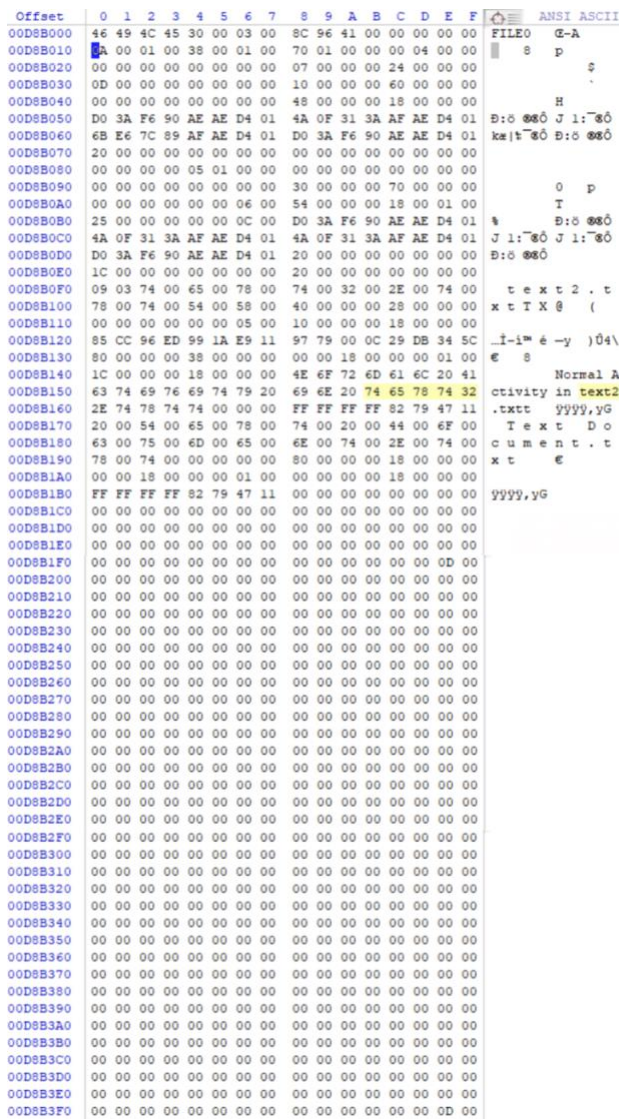


Figure 27. Full MFT entry of text2.txt within the oldest volume shadow copy difference file (1024 bytes in length, from offset 00D8B000 to 00D8B3F0)

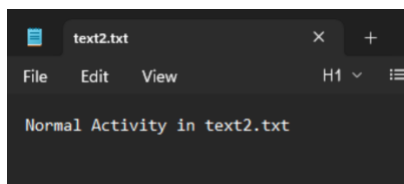


Figure 28. Accessed contents of text2.txt in NTFS filesystem via Windows 11 Notepad



6. Compare (what's similar?) and contrast (what's different) with regard to the data and metadata parsed by ShadowExplorer ([shadowexplorer.com](http://shadowexplorer.com)), ShadowCopyView ([NirSoft.net](http://NirSoft.net)), and VSSadmin (native, built-in Windows command line utility).

- **Analysis Performed:**

- It is important for cybersecurity professionals to cross-reference findings with multiple tools, as each may present limitations or omit certain details.
- The examiner analyzed the data and metadata of the oldest volume shadow copy difference file parsed by ShadowExplorer, VSSadmin, and ShadowCopyView, as shown in Figures 29-31.
  - ShadowExplorer
    - Provides a graphical interface to browse the NTFS file system within a shadow copy. It allows file access and export but does not display shadow copy metadata.
  - VSSadmin
    - A native Windows command-line utility that lists shadow copies and their metadata (creation times, volume associations, storage usage). It does not display the NTFS file system or allow file export.
  - ShadowCopyView
    - Offers both NTFS file system browsing and shadow copy metadata. Like ShadowExplorer, it supports file access/export, but it also includes metadata details similar to VSSadmin.

- **Answer:**

ShadowExplorer, VSSadmin, and ShadowCopyView each provide different perspectives on volume shadow copies, and understanding their strengths and limitations is critical in forensic work. ShadowExplorer offers a graphical interface that allows users to browse the NTFS file system and export files from a shadow copy. However, it does not display metadata, which limits its usefulness for timeline and context analysis. VSSadmin, by contrast, is a command-line utility that provides metadata such as creation times, volume associations, and storage usage, but it does not allow file system browsing or file export. ShadowCopyView combines both functions, enabling browsing and exporting of files from the NTFS file system while also presenting metadata similar to VSSadmin. It is important for cybersecurity professionals to examine each tool available to them to determine which tools are most effective for the specific task at hand. Some investigations may require metadata-focused analysis, where VSSadmin provides quick and reliable results, while others may demand file-level access for recovery, where ShadowExplorer or ShadowCopyView would be more suitable. ShadowCopyView is the most comprehensive of the three, offering both metadata and file content access, but corroborating findings with multiple tools ensures accuracy and completeness. **In conclusion, ShadowExplorer and ShadowCopyView are similar in enabling file recovery, but only ShadowCopyView provides metadata visibility, whereas VSSadmin remains limited to metadata reporting.** From a forensic perspective, cross-tool validation is essential, as using multiple utilities reduces the risk of overlooking critical evidence and strengthens the reliability of investigative findings.

- **Supporting Evidence:**

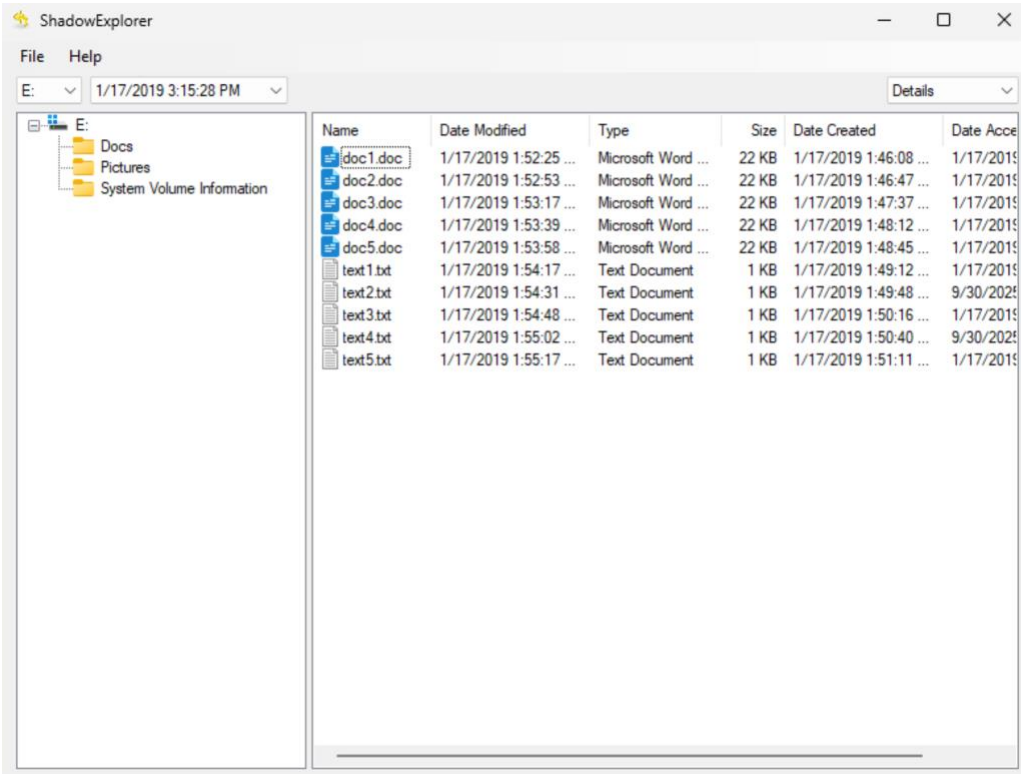


Figure 29. ShadowExplorer parsing data from volume shadow copy

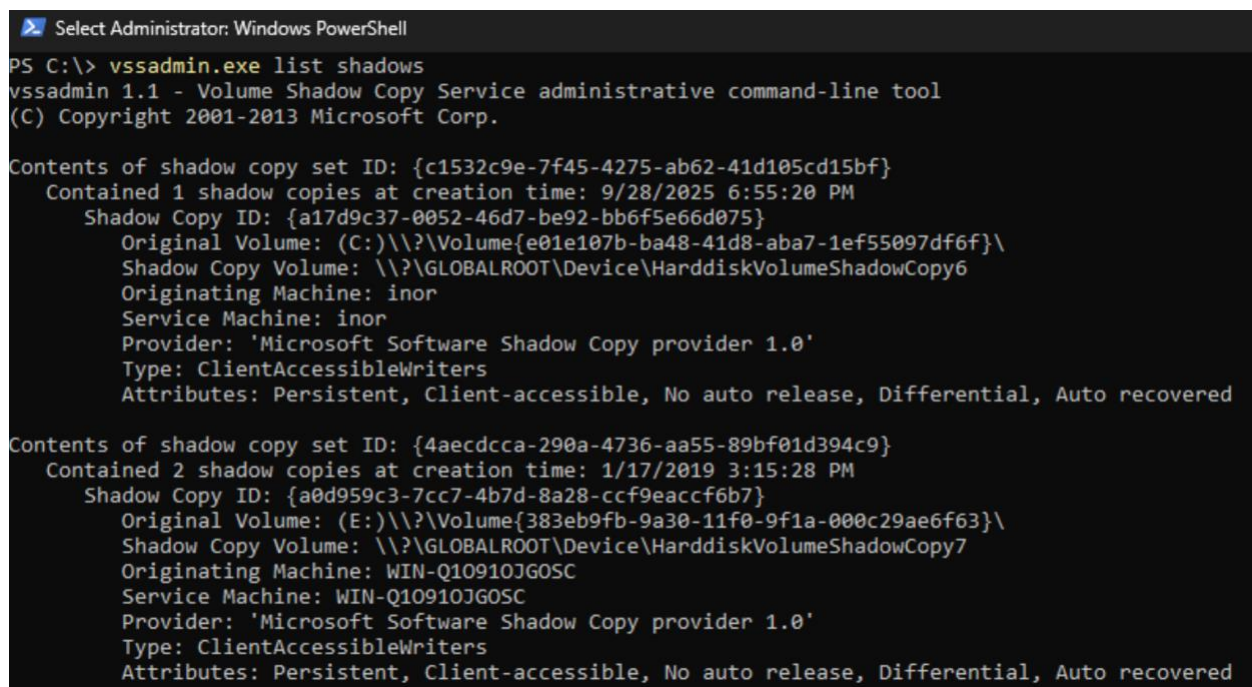


Figure 30. VSSadmin parsing metadata from volume shadow copy

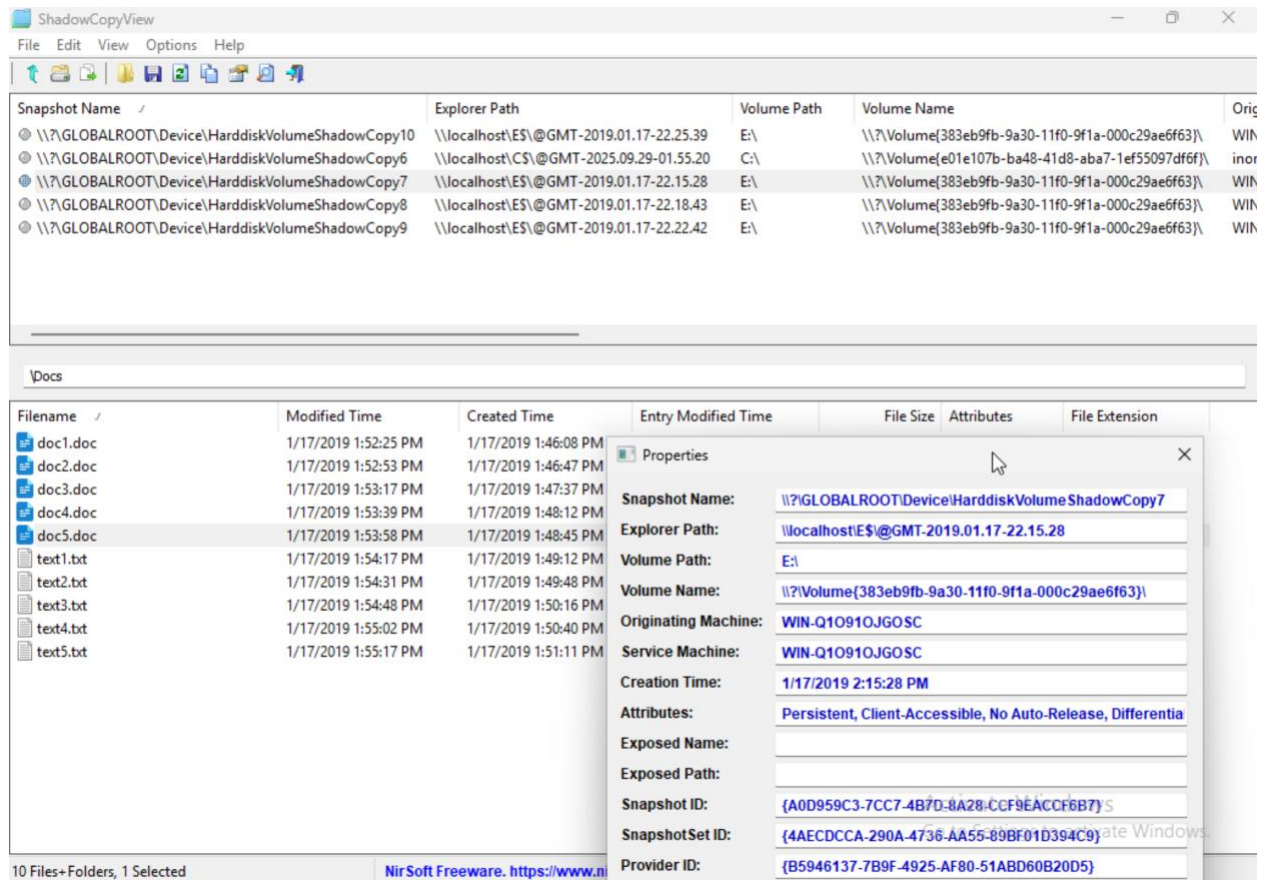


Figure 31. ShadowCopyView parsing metadata and data from volume shadow copy

## Conclusion

The examiner, Inor Wang, enjoyed this lab! There is no critique from me. Thank you.

## References

- Carvey, H. A. (2014). Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8 (Fourth edition). Syngress.
- Johansen, G., & Safari, an O. M. C. (2020). Digital Forensics and Incident Response—Second Edition.
- Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory. Wiley.
- Malware forensics field guide for Windows systems digital forensics field guides. (2012). Syngress.
- Oettinger, W., & Safari, an O. M. C. (2020). Learn Computer Forensics.