

[Lab report](#): 11/30/2023 02:42 PM UTC

Computer Forensics

Chapter 5 - Working with Windows and CLI Systems

Start:

11/30/2023 02:42 PM UTC

Finish:

11/30/2023 03:50 PM UTC

Elapsed (min):

68.0

Status:

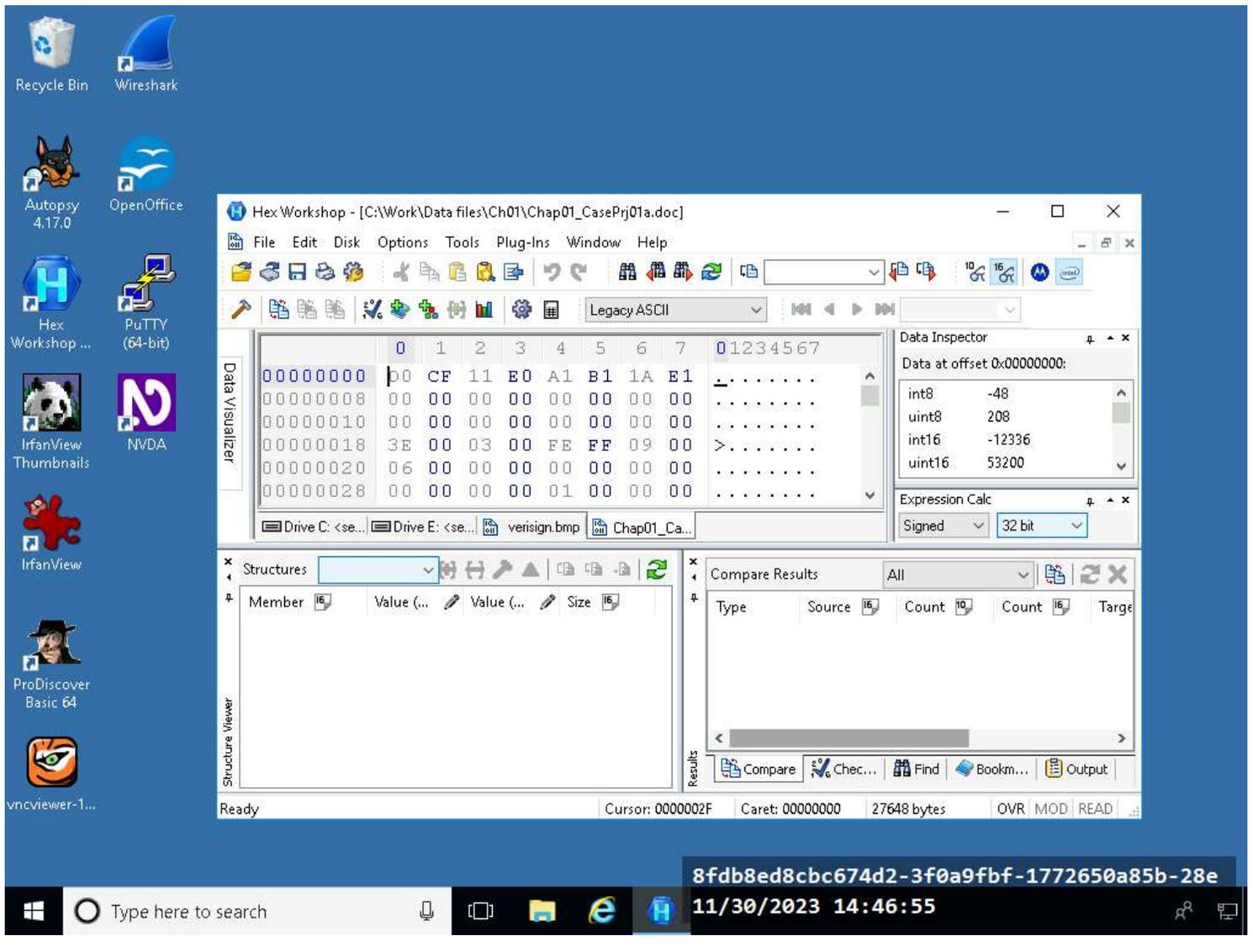
Submitted

1. Screenshot

Actioned

Item completed: 11/30/2023 02:46 AM

Value: 0



2. Screenshot

Actioned

Item completed: 11/30/2023 02:58 AM

Value: 0

OSForensics - Deleted Files

Workflow

- Start
- Triage Wizard
- Manage Case
- File Name Search
- Create Index
- Search Index
- Recent Activity
- Deleted Files Search
- Mismatch File Search
- Memory Viewer
- Prefetch Viewer
- Raw Disk Viewer**
- Registry Viewer
- File System Browser
- SQLite DB Browser
- Web Browser
- Passwords
- System Information
- Verify / Create Hash

Raw Disk Viewer

Disk: Drive-C: [Logical Drive (Forensics Mode)]

Jump to ... Search ... Bookmarks ... Decode ... Right-click in the disk viewer for additional options

Hex	00	08	0123456789ABCDEF
0x000000000000C047000	DOCF11E0A1B11AE1	0000000000000000	
0x000000000000C047010	0000000000000000	3E000300EFFF0900	>
0x000000000000C047020	0600000000000000	0000000010000000	
0x000000000000C047030	2F00000000000000	0010000031000000	1
0x000000000000C047040	01000000FFFFFFF	000000002E000000	
0x000000000000C047050	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047060	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047070	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047080	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047090	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0470A0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0470B0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0470C0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0470D0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0470E0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0470F0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047100	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047110	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047120	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047130	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047140	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047150	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047160	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047170	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047180	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047190	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0471A0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0471B0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0471C0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0471D0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0471E0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C0471F0	FFFFFFFFFFFFFFF	FFFFFFFFFFFFFFF	
0x000000000000C047200	ECA5C1007F800904	0000F012BF000000	
0x000000000000C047210	0000001000000000	00080000F30A0000	
0x000000000000C047220	0E00626A626AE6E6	E6E6000000000000	bjbj
0x000000000000C047230	0000000000000000	0000000009041600	
0x000000000000C047240	34100000848C0100	848C0100F3020000	4
0x000000000000C047250	0000000000000000	0000000000000000	
0x000000000000C047260	0000000000000000	00000000FFFFFF00	
0x000000000000C047270	0000000000000000	FFFFFFFF00000000	

8fdb8ed8cbc674d2-3f0a9fbf-1772650a85b-28e

11/30/2023 14:58:02

3. Screenshot

Actioned

Item completed: 11/30/2023 03:40 AM

Value: 0

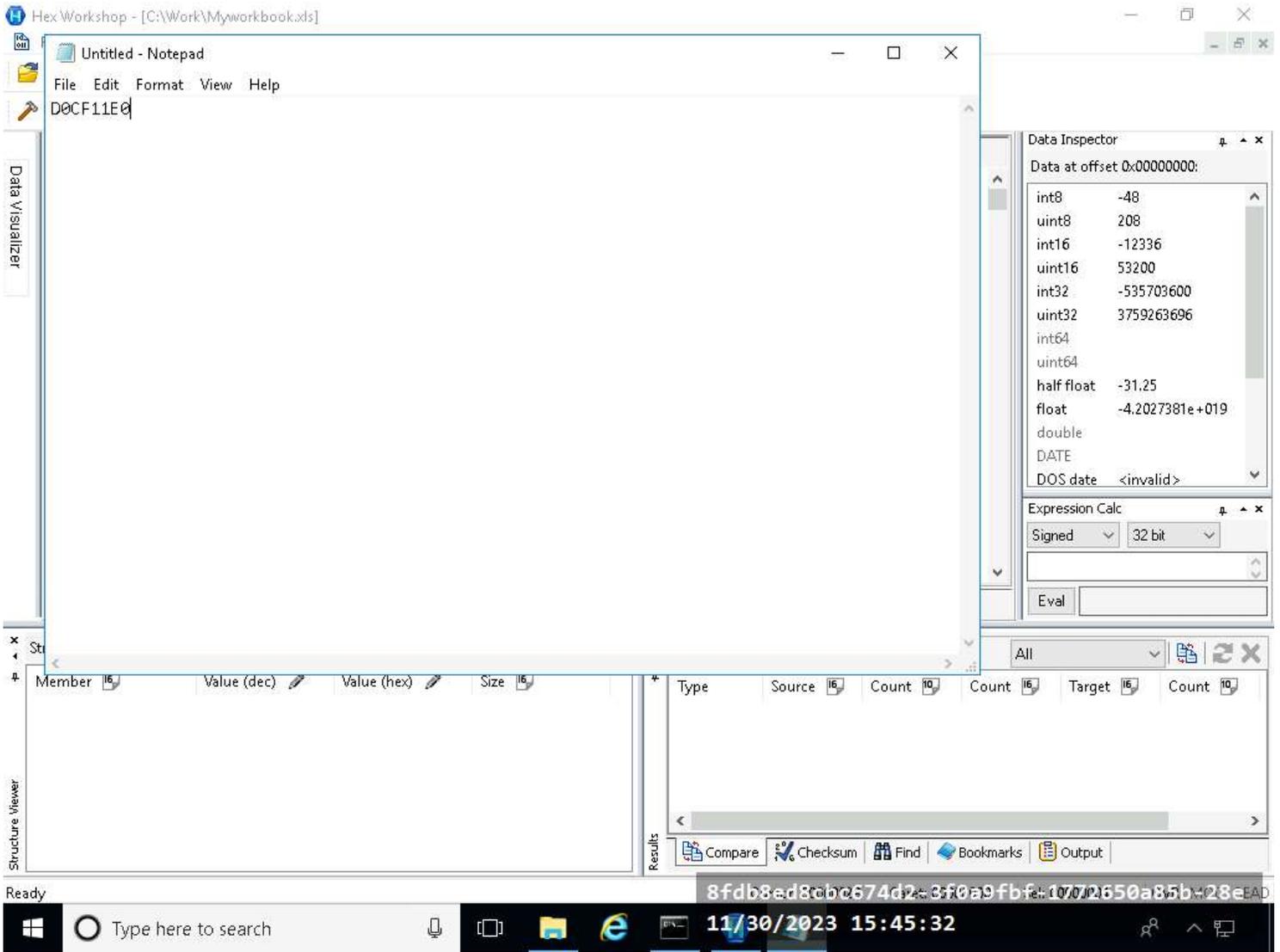
The screenshot displays the OSForensics - InChap05 application window. The main pane is titled 'Raw Disk Viewer' and shows a hex dump of a disk sector. The hex dump is organized into three columns: 00, 08, and 0123456789ABCDEF. The data in the 00 column is a series of 0x0000000000000000 values. The 08 column contains hex values, and the 0123456789ABCDEF column contains ASCII text fragments. Visible text includes '.R.NTFS', 'sk read error', 'B.O.O.T.M.G.R.', and 'Sector 1'. The interface includes a sidebar with various tools like 'Start', 'Triage Wizard', 'File System Browser', and 'Registry Viewer'. The taskbar at the bottom shows the date and time as 11/30/2023 15:40:59.

4. Screenshot

Actioned

Item completed: 11/30/2023 03:45 AM

Value: 0



5. Question

Actioned

Item completed: **11/30/2023 03:49 AM**

Value: **1**

Answer: **MBR**

PASS

6. Question

Actioned

Item completed: **11/30/2023 03:49 AM**

Value: **1**

Answer: **ADS**

PASS

7. Question

Actioned

Item completed: **11/30/2023 03:49 AM**

Value: **1**

Answer: **EFS**

PASS

8. Question

Actioned

Item completed: **11/30/2023 03:50 AM**

Value: **1**

Answer: **Registry**

PASS

9. Question

Actioned

Item completed: **11/30/2023 03:50 AM**

Value: **1**

Answer: **FAT28**

PASS

Score : 5 out of 5 (100%)