

1. Screenshot

Actioned

Item completed: 12/01/2023 09:04 AM

Value: 0

The screenshot shows the OSForensics - VM Forensics application window. The interface includes a left sidebar with a 'Workflow' section containing various tools like 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, Hash Sets, Create Signature, Compare Signature, Drive Preparation, Forensic Imaging, Mount Drive Image, and Install to USB. The main area is titled 'Manage Case' and contains a 'Select Case' section with buttons for New Case..., Import Case..., Load Case, and Delete Case. Below this is a table with columns for Title, Create Date, and Location. The table shows an entry for 'VM Forensics' with a green checkmark, a title of 'Error: Could not load case details', a create date of '01 December 2023, 21:00:13', and a location of 'C:\Users\Admin\Documents\PassMark\OSForensics\Cases\VM Forensics'. Below the table is a 'Manage Current Case' section with buttons for Edit Case Details..., Generate Report..., View Log..., Add External Report..., Add Device..., Add Attachment..., Add Note..., and Add Evidence Photo... The bottom section is titled 'Case Items' and contains a table with columns for Title, Module, Case Item, Category, and Date Added. The table shows an entry for 'Drive-C' with a title of 'Devices', a module of 'Case Manager', a case item of 'C:', and a date added of '01 Dec'. The Windows taskbar at the bottom shows the search bar, task view button, and several open applications. The system tray displays the date and time as '12/01/2023 21:04:24' and a security notification for '8fdb8ed8cbc674d2-3f0a9fbf-1772650a85b-28e'.

OSForensics - VM Forensics

Workflow

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

Hash Sets

Create Signature

Compare Signature

Drive Preparation

Forensic Imaging

Mount Drive Image

Install to USB

Manage Case

Select Case

New Case...

Import Case...

Load Case

Delete Case

Title	Create Date	Location
Error: Could not load case details	N/A	C:\Users\Admin\Documents\PassMark\OSForensics\Cases\
✓ VM Forensics	01 December 2023, 21:00:13	C:\Users\Admin\Documents\PassMark\OSForensics\Cases\VM Forensics

Manage Current Case

Edit Case Details...

Generate Report...

View Log...

Add External Report...

Add Device...

Add Attachment...

Add Note...

Add Evidence Photo...

Case Items

Title	Module	Case Item	Category	Date Added
Devices				
Drive-C	Case Manager	C:		01 Dec

Open

Delete

Properties

Verify

8fdb8ed8cbc674d2-3f0a9fbf-1772650a85b-28e

12/01/2023 21:04:24

2. Screenshot

Actioned

Item completed: 12/01/2023 09:06 AM

Value: 0

The screenshot displays the OSForensics - VM Forensics application window. The left sidebar contains a 'Workflow' menu with various tools like Deleted Files Search, Mismatch File Search, Memory Viewer (selected), Prefetch Viewer, Raw Disk Viewer, Registry Viewer, File System Browser, SQLite DB Browser, Web Browser, Passwords, System Information, Verify / Create Hash, Hash Sets, Create Signature, Compare Signature, Drive Preparation, Forensic Imaging, Mount Drive Image, and Install to USB. The main area is titled 'Memory Viewer' and has tabs for 'Live Analysis' and 'Static Analysis'. Below these are buttons for 'Refresh', 'Select Window', and 'Dump Physical Memory'. A table lists running processes with columns for Process, PID, CPU %, Total CPU Time, User Time, Kernel Time, and Process Create Time. The 'Process Info' tab is active, showing details like Image Path, Product, Description, Version, User Name, Integrity Level, Digitally Signed, and Digital Signer. A filter bar at the bottom right shows 'Filter by: None' and a hash '8fdb8ed8cbc674d2-3f0a9fbf-1772650a85b-28e'. The taskbar at the bottom shows the Windows logo, a search bar, and the date/time '12/01/2023 21:06:20'.

Process	PID	CPU %	Total CPU Time	User Time	Kernel Time	Process Create Time
Idle	0	67.19%	00:14:26.359	00:00:00.000	00:14:26.359	01/12/2023, 20:55:32
System	4		00:00:24.265	00:00:00.000	00:00:24.265	01/12/2023, 20:55:32
Secure System	48		00:00:00.000	00:00:00.000	00:00:00.000	01/12/2023, 20:55:30
LogonUI.exe	272		00:00:00.375	00:00:00.156	00:00:00.218	01/12/2023, 20:55:42
smss.exe	348		00:00:00.265	00:00:00.000	00:00:00.265	01/12/2023, 20:55:32
dwm.exe	424		00:00:00.218	00:00:00.015	00:00:00.203	01/12/2023, 20:55:42
csrss.exe	472		00:00:00.359	00:00:00.031	00:00:00.328	01/12/2023, 20:55:41
wininit.exe	544		00:00:00.156	00:00:00.000	00:00:00.156	01/12/2023, 20:55:41
csrss.exe	560		00:00:00.203	00:00:00.078	00:00:00.125	01/12/2023, 20:55:42
winlogon.exe	636		00:00:00.125	00:00:00.046	00:00:00.078	01/12/2023, 20:55:42
osf64.exe	648	2.34%	00:00:09.921	00:00:04.656	00:00:05.265	01/12/2023, 20:57:38
services.exe	676		00:00:02.687	00:00:00.781	00:00:01.906	01/12/2023, 20:55:42
lsass.exe	684		00:00:01.484	00:00:00.953	00:00:00.531	01/12/2023, 20:55:42
svchost.exe	780		00:00:00.031	00:00:00.000	00:00:00.031	01/12/2023, 20:55:42

3. Screenshot

Actioned

Item completed: 12/01/2023 09:15 AM

Value: 0

WinHex - [testdump.mem]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

testdump.mem

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000177410	20	25	67	20	69	6E	20	61	20	6E	6F	6E	2D	46	46	53	%g in a non-FFS
000177420	33	20	66	6F	72	6D	61	74	74	65	64	20	46	56	2E	0A	3 formatted FV.
000177430	00	00	00	00	54	52	55	45	00	00	00	00	46	41	4C	53	TRUE FALS
000177440	45	00	00	00	11	12	13	14	15	16	17	18	00	04	07	09	E
000177450	0A	0C	0F	10	7F	FF	04	00	25	00	73	00	00	00	00	00	y % s
000177460	00	00	00	00	25	00	2E	00	2A	00	61	00	2E	00	65	00	% . * a . e
000177470	66	00	69	00	00	00	00	00	00	00	00	00	49	6E	69	74	f i Init
000177480	69	61	6C	69	7A	65	44	65	62	75	67	41	67	65	6E	74	ializeDebugAgent
000177490	00	00	00	00	3E	3E	3E	20	25	61	20	28	25	6C	78	2C	>>> %a (%lx,
0001774A0	20	25	70	2C	20	25	70	29	0A	00	00	00	2D	2D	2D	20	%p, %p) ---
0001774B0	25	61	3A	20	44	65	62	75	67	67	65	72	45	6E	61	62	%a: DebuggerEnab
0001774C0	6C	65	64	20	25	61	0A	00	00	00	00	00	4D	69	63	72	led %a Micr
0001774D0	6F	73	6F	66	74	20	55	45	46	49	20	42	6F	6F	74	20	osoft UEFI Boot
0001774E0	44	65	62	75	67	67	65	72	20	49	6E	69	74	69	61	6C	Debugger Initial
0001774F0	69	7A	65	64	0A	00	00	00	00	00	00	00	0A	42	75	67	ized Bug
000177500	63	68	65	63	6B	0A	00	00	00	00	00	00	20	20	20	20	check
000177510	42	75	67	63	68	65	63	6B	20	43	6F	64	65	3A	20	30	Bugcheck Code: 0
000177520	78	25	78	2C	20	25	70	2C	20	25	70	2C	20	25	70	2C	x%x, %p, %p, %p,
000177530	20	25	70	0A	00	00	00	00	00	00	00	00	20	20	20	20	%p
000177540	43	6F	6E	74	65	78	74	3A	20	25	70	2C	20	45	78	63	Context: %p, Exc
000177550	65	70	74	69	6F	6E	20	52	65	63	6F	72	64	20	25	70	eption Record %p
000177560	0A	00	00	00	55	6E	75	73	65	64	00	00	53	74	61	74	Unused Stat
000177570	65	43	68	61	6E	67	65	33	32	00	00	00	53	74	61	74	eChange32 Stat
000177580	65	4D	61	6E	69	70	75	6C	61	74	65	00	44	65	62	75	eManipulate Debu
000177590	67	49	6F	00	41	63	6B	00	52	65	73	65	6E	64	00	00	gIo Ack Resend
0001775A0	00	00	00	00	53	74	61	74	65	43	68	61	6E	67	65	36	StateChange6
0001775B0	34	00	00	00	42	72	65	61	6B	69	6E	00	54	72	61	63	4 Breakin Trac
0001775C0	65	49	6F	00	43	6F	6E	74	72	6F	6C	52	65	71	75	65	eIo ControlReque
0001775D0	73	74	00	00	46	69	6C	65	49	6F	00	00	3C	69	6E	76	st FileIo <inv
0001775E0	61	6C	69	64	3E	00	00	00	00	00	00	00	52	65	63	65	alid> Rece
0001775F0	69	76	65	64	00	00	00	00	00	00	00	00	54	69	6D	65	ived Time
000177600	6F	75	74	00	3E	3E	3E	20	42	64	43	6F	6D	52	65	63	out >>> BdComRec
000177610	65	69	76	65	50	61	63	6B	65	74	3A	20	6C	6F	6F	6B	eivePacket: look
000177620	69	6E	67	20	66	6F	72	20	54	79	70	65	3A	20	25	61	ing for Type: %a

Page 2,746 of 7,909,259 Offset: 1774CC 8fdb8ed8cb674d2-3f0a9fbf-1772650a85b-28e...

12/01/2023 21:15:32

testdump.mem [unregistered]
C:\Work\Data files\Ch10\Projects
File size: 4.1 GB
4,429,185,024 bytes
Default Edit Mode: original
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 01/12/2023 21:08:46
Last write time: 01/12/2023 21:09:31
Attributes: A
Icons: 0
Mode: Text
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 35x16=560
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 20.8 GB free
Jsers\Admin\AppData\Local\Temp
Data Interpreter
8 Bit (±): 77
16 Bit (±): 26,957
32 Bit (±): 1,919,117,6...

4. Question

Actioned

Item completed: **12/01/2023 09:16 AM**Value: **1**Answer: **Type 1****PASS**

5. Question

Actioned

Item completed: **12/01/2023 09:16 AM**Value: **1**Answer: **SIFT Workstation****PASS**

6. Question

Actioned

Item completed: **12/01/2023 09:17 AM**Value: **1**Answer: **Wireshark****PASS**

7. Question

Actioned

Item completed: **12/01/2023 09:17 AM**Value: **1**Answer: **WinHex****PASS**

8. Question

Actioned

Item completed: **12/01/2023 09:18 AM**Value: **1**Answer: **order of volatility (OOV)**

PASS

Score : 5 out of 5 (100%)