# **Research Question:**

How do the differences in digital artifacts between Windows 10 and Windows 11 affect the methodologies and effectiveness of forensic analysis?

Author: Rithik Oza Date of Submission: December 3, 2024

# Abstract:

The transition from Windows 10 to Windows 11 brings significant changes to system architecture, artifact handling, and security features, with far-reaching implications for digital forensic investigations. This study explores the effects of these changes on the discovery, extraction, and analysis of digital evidence. Using a controlled environment with identical datasets on both operating systems, the research focuses on five key artifact categories: registry entries, event logs, prefetch files, thumbnail caches, and file metadata.

Windows 11 introduces notable improvements, including more detailed metadata, advanced logging capabilities, and enhanced caching systems, enabling more robust artifact tracking. Security upgrades, such as the implementation of TPM 2.0 and mandatory UEFI boot, bolster system integrity but also pose challenges to traditional forensic techniques. Additionally, the operating system's focus on user-centric functionality adds complexity, presenting both opportunities and challenges for investigators.

This research emphasizes the importance of adapting forensic methodologies to Windows 11's modernized ecosystem. Updates to forensic tools, targeted training, and collaboration with software developers are essential to address the challenges posed by these advancements. By offering a detailed comparison of the two systems, this study provides forensic professionals with practical insights and strategies to navigate the complexities of Windows 11 and ensure effective digital investigations in an ever-evolving technological landscape.

Research Question:	
Abstract:	2
Forensics Acquisition and Exam Preparation:	
Experiment Setup:	
Methodology	
Artifact Identification and Collection	
1. Event Logs	7
2. Registry Entries	7
3. File Metadata	
4. Prefetch Files	
5. Thumbnail Cache	
Findings and Forensics Analysis:	
Event Logs	
System Log Analysis:	
System Configuration:	
Virtualization Platforms:	
Activity Focus:	
Security and Boot:	
Security Log Analysis:	
VBoxHardening:	
Observations	
win11 sandbox logs:	
Observations	
Registry Entries:	
Anaysis:	
Active Setup	
App Paths	
AppInit DLLs	
Authentication (LogonUI)	
File Associations	
Security and Certificates	
Audio Devices	
Persistence and Security Configurations	
System Upgrade and Compatibility	
Persistence Mechanisms	
Registry and Backup Settings	
Security and Logging	
Application Compatibility	
Device Management	
Crash and Diagnostic Settings	

Performance and Code Pages	
File Metadata	20
Analysis:	
Chromium Extensions	20
Chromium Profiles	20
Data Source Usage	
Encryption	
Extension Mismatch	21
Favicons	21
Installed Programs	21
Metadata	21
Operating System	21
Recent Documents	21
Shell Bags	21
Case Summary	21
USB Devices	21
Web Accounts	
Web Bookmarks	
Web Cache	
Web History	
Prefetch Files	23
Analysis	24
File Metadata (SourceFilename, Created, Modified, Accessed)	24
Executable Names and Run Details	24
Hash and Size	24
Volume Information	
Directories and Loaded Files	25
Parsing Errors	25
Observations	
Thumbnail Cache	
Analysis of Thumbnail Cache CSV Logs	27
1. Structure of the Logs	27
MetaData	27
2. Key Comparisons	
Filename and Hash	
Offsets and Sizes	
Checksums	
Location	
Overall Observations	
ision	

# **Forensics Acquisition and Exam Preparation:**

- Downloaded and added the Windows 10 and 11 image files from the official Microsoft website to the Windows 11 Documents section.
  - The workstation's specifications are as follows:
    - Laptop: Dell Precision 5550
    - Operating System: Windows 11 Pro 23H2
    - o Processor: Intel(R) Core(TM) i7-10850H CPU @ 2.70GHz 2.71 GHz
    - Installed RAM: 16.0 GB (15.7 GB usable)
    - System Type: 64-bit operating system, x64-based processor
- The tools used for this analysis are:

•

- o Dell Precision 5550 laptop
- Autopsy 4.21.0: To extract and analyze artifacts.
- o AccessData FTK Imager 4.7.1.2
- Virtual Box Mangager 7.1.4
- VMware Workstation Pro 17.0 : To simulate Windows 10 and Windows 11 environments.
- RegRipper 4.0: To parse and extract relevant registry keys efficiently.
- PECmd 1.0 (original tool): To analyze Prefetch files.
- Thumbcache\_viewer\_64: To analyse Cache files.
- The verified hash value of Windows 10 and 11. To create fairness after the iso files had been added (windows 10 iso is added in VirtualBox, and windows 11 iso has been added to VMware), the vmdk version of those have been hashed.

	Drive/Image Verify Results	Name	Size Type	Date Modified	
	Drive/Image Verify Results				
	in a mage tany tasang	- 🗆 X	Drive/Image Verify Results	- 0 X	
			Ξ		
	Name	Windows 11 x64.vmdk	Name	win10_copy.vmdk	
	Sector count	167772160	Sector count	104857600	
B	MD5 Hash		MD5 Hash		
	Computed hash	9e52ec6f158ef62abfcb468510b1bc8b	Computed hash	a443ab25194415da4785e95041d0690c	
8	SHA1 Hash		SHA1 Hash		
	Computed hash	60e700d173445a2494bf618bddbd7bc86adfe	Computed hash	a6d0e0e76db2d88be548fe68aa6708b9d8327	1
8	Bad Blocks List		Bad Blocks List		
	Bad block(s) in image	No bad blocks found in image	Bad block(s) in image	No bad blocks found in image	
		Close		Close	
		000000000010 43 50 41 75 32 81 F9 02- 000000100 00 66 68 00 02 00 00 66- 000000110 53 65 55 66 00 00 00- 000000120 61 68 00 00 07 CD 1A 5A- 000000118 18 0B 70 77 EB 08 AD 86- 000000116 01 50 D7 8B F0 AC 3C 00- 0000001516 10 EB F2 F4 EB FD BC 3- 0000001516 10 EB F2 F4 EB FD BC 3- 0000001516 10 EB F2 F4 EB F0 BC 3- 00000001516 10 EB F2 F4 F50	38         08         00         00         00         66         53         66         -fh           10         66         68         00         7C         00         00         66         SfUf           12         F6         EA         00         7C         00         00         CD         ah           17         EB         03         A0         B5         07         32         E4	fsf thfsf ff. f22∂€f. €- ¶.e. µ.2a .6a <tf. ēş¥fādē ¢.às</tf. 	

Hash verifcation of Windows 10 and 11 (note there is no reverification as there would be changes to system).

# **Experiment Setup:**

To simulate a typical user environment and observe artifact generation, a zip folder named 'test' was created and moved into both Windows 10 and Windows 11 systems. This folder contained:

Basic installers and software commonly used, which are as follows:

- spacedesk\_driver\_Win\_10\_64\_v2128
- Remote Mouse
- AlternativeA2dpSetup-1.5.0.1
- BtTweakerSetup-1.4.8.1
- NZXT-CAM-Setup
- AccessData\_FTK\_Imager\_4.7.1
- LockDownBrowser-2-1-2-09-536515735
- Latest-ADB-Installer
- Attack\_SharkX3Mouse
- DroidCam.Setup.6.5.2
- Firefox Installer

Random photos donwloaded form web representing standard user-generated content are, as follows:

- ♦ w1
- ♦ w2
- ♦ w3
- w4
- image-16d18f05-d55a-4fae-bea9-c081b43a2ff0.png

The software contained in the folder "test", have all been installed on both the systems, and the same images have been deleted to simulate a perfect environment where all the user data is the same; however, the operating system has changed.

# Methodology

## **Artifact Identification and Collection**

To comprehensively analyze and catalog the differences in digital artifacts, the research focuses on five critical artifacts:

## 1. Event Logs

Description: Event Viewer logs provide a record of system and user activities, including file interactions.

Method of Collection:

Due to the use of VMs, the event logs can be directly taken from the VM's directory file. There are two types of log files; the first one correlates to the changes made in the system and the other one correlates to security changes due to the system changes.

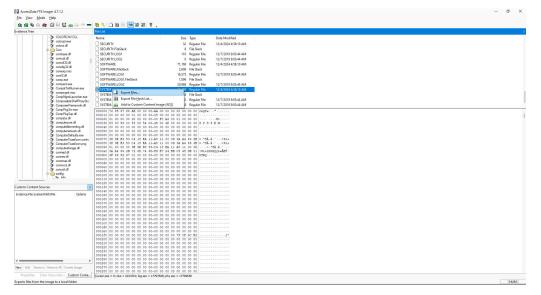
Both types of log files will be examined and compared to the same type of log file of the other operating system. The files are stored in "win10/Event logs" and "win11/Event logs" for windows 10 and 11 respectively.

## 2. Registry Entries

Description: Registry entries record software installations and file interactions.

Method of Collection:

Used Autopsy to extract files "win10/Registry files; win11/Registry files" and Regripper to analyze relevant registry hives, specifically SYSTEM, SOFTWARE which focuses on entries related to the test folder's contents. The exported files are stored in "win10/Registry files; win11/Registry files" for windows 10 and 11 respectively.



Exporting SYSTEM registry file from autopsy(same for SOFTWARE)

e Help			File Help		
Hive File:	D:\all\reghive\SYSTEM_win10	Browse	Hive File:	D:\all\reghive\SYSTEM_win11	Browse
Report File:	D:\all\reghive\win10systemreg.txt	Browse	Report File:	D:\all\reghive\win11systemreg.txt	Browse
usbdevicesf usbstor2Dor usbstor2Done. utilitiesDone. volsnapDon wssDone. wdfilterDone. wpdbusenum wpdbusenum tgDone. zerologonDo	e. Done.	1	usbdevices. usbstorDone. usbitorsDone. usbitiesDone. volanapDor vsDone. wdfiterDone. wpbtDone. zerologonD 0 plugins con	ie, e, ne, e, Done,	Ľ

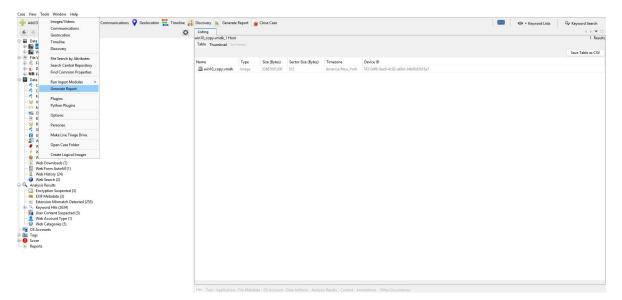
Regripper parsing all the registry files

## 3. File Metadata

Description: Metadata includes timestamps for file creation, modification, and access.

Method of Collection:

The results of the complete Autopsy ingest for both of the operating system will then be exported in HTML format (most informative report generated by Autopsy), and the similarites and differences observed. The generated report for windows 10 and 11 is in location "win10/reports; win11/reports" respectively.



Selecting the data source for generating report after the Autopsy ingest has finished(same for Windows 11).

ise View Tools Window Help		
	🕽 Geolocation 🗮 Timeline 🚚 Discovery 🔝 Generate Report 🍙 Close Case	🔤 🐵 • Keyword Lists 🔍 Keyword Search
← →	O Listing	() ¥ 0
Data Sources	win10_copy.vmdk_1 Host	1 Resul
win10_copy.vmdk_1 Host	Table Thumbnail Summary	
Ele Vindows 11 x64.vmdk_425427 Host     Ele Views		Save Table as CSV
He Vews     File Types	Name Type Size (Bytes) Sector Size (Bytes) Timezone Device ID	
Y Deleted Files	win10_copy.vmdk Image 53687091200 512 America/New_York 743134f6-9ee9-4c52-s68d-34b80d5616a7	
MB File Size		
Data Artifacts     Chromium Extensions (28)	Generate Report X	
Chromium Extensions (28)     Chromium Profiles (1)	Construction response of the second s	
- K Favicon (39)	Configure Report	
M Installed Programs (42)		
- O Metadata (79)	Select which data to report on:	
Operating System Information (1)     Recent Documents (16)	<ul> <li>All Results</li> </ul>	
- 3 Run Programs (417)	All Tagged Results	
- 🐔 Shell Bags (5)	Specific Tanged Results	
USB Device Attached (2)	C second region region	
Web Accounts (1)     Web Bookmarks (5)	Select All	
- Web Cache (1023)		
- 🌚 Web Cookies (125)	Deselect All	
Web Downloads (7)		
Web Form Autohill (1)		
Web Search (2)		
C Analysis Results		
- Difference Encryption Suspected (3)		
- EUF Metadata (3) Extension Mismatch Detected (253)		
⊕ S Keyword Hits (2634)	Choose Result Types	
- We User Content Suspected (3)	Croose to any types	
- 2 Web Account Type (1)		
G Accounts		
Tags		
Score	<back net=""> Finish Cancel Help</back>	
Reports		
	Hex Test Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences	
	Lee Abbroard Lacaresean Analysis and Astronomy Course Analysis of the Articles	

Exporting all the results of Autopsy ingest into an HTML report(same for Windows 11).

### 4. Prefetch Files

Description: Prefetch files reveal program execution history, including interactions with the test folder's installers.

Method of Collection:

Collect prefetch files, the location in my case is :

win10\_copy.vmdk/Partition 1 [51198MB]/NONAME [NTFS]/[root]/Windows/Prefetch

After all the prefetch files have been exported to destination folder using PECmd(win10/Prefetchpecmd; win11/Prefetchpecmd), compare both the csv files.

Data FTK Imager 4.7.1.2					-	
v <u>M</u> ode <u>H</u> elp						
1 4 🕿 🛛 🖓 🖓 🗛 🔿 🖷	• 🖪 🥄 🗋 🖹 🗎 🐱 😹 🕷 🦧 🚬					
20	File List					
🕮 🛅 DiagTrack	Name	Size	Type	Date Modified		
🗄 🚞 DigitalLocker	SVCHOST.EXE-DD94A43F.pf.FileSlack	3	File Slack			
Downloaded Program Files ht DtcInstall.log	VSSVC.EXE-04D079CC.pf.FileSlack		File Slack			
ELAMBKUP	SVCHOST.EXE-8FD92526.pf.FileSlack		File Slack			
B-C en-GB	SPPEXTCOMOBJ.EXE-58C1C601.pf.FileSla		File Slack			
en-US	SI30			12/4/2024 2:23:13 AM		
explorer.exe			NTFS Index All			
E Conts	MICROSOFTEDGE_X64_131.0.2903CDF5		Regular File	12/4/2024 2:07:08 AM		
GameBarPresenceWriter	SETUP.EXE-D1DBE09B.pf		Regular File	12/4/2024 2:07:00 AM		
Globalization	DENTITY_HELPER.EXE-81C5A103.pf		Regular File	12/4/2024 2:10:15 AM		
🕀 🧰 Help	SLUI.EXE-A65918C4.pf		Regular File	12/4/2024 2:10:08 AM		
HelpPane.exe	MSEDGE.EXE-BA103771.pf	42	Regular File	12/4/2024 2:09:57 AM		
ildentityCRL	MSEDGE.EXE-BA103778.pf	21	Regular File	12/4/2024 2:20:15 AM		
	MSEDGE.EXE-BA103772.pf	23	Regular File	12/4/2024 2:10:11 AM		
ImmersiveControlPanel	MSEDGE.EXE-BA103773.pf	20	Regular File	12/4/2024 2:10:11 AM		
inboxApps	MSEDGE.EXE-BA103774.pf	5	Regular File	12/4/2024 2:10:10 AM		
🔅 🇀 INF	BACKGROUNDTASKHOST.EXE-3E9BC537.pf	13	Regular File	12/4/2024 2:10:05 AM		
Input Method	ELEVATION_SERVICE.EXE-FDD452DA.pf	5	Regular File	12/4/2024 2:10:05 AM		
installer	SVCHOST.EXE-00BB3EFB.pf		Regular File	12/4/2024 2:22:59 AM		
L2Schemas     LanguageOverlayCache	WUAUCLT.EXE-830BCC14.pf		Regular File	12/4/2024 1:59:50 AM		
LiveKemelReports	THORIUM.EXE-66FB8EDE.pf		Regular File	12/4/2024 2:23:51 AM		
E Cas	THORIUM.EXE-66FB8EDF.pf		Regular File	12/4/2024 2:23:51 AM		
🗄 🧰 Media	THORIUM.EXE-66FB8EE0.pf		Regular File	12/4/2024 2:23:50 AM		
p mib.bin	THORIUM.EXE-66FB8EDC.pf		Regular File	12/4/2024 2:23:50 AM		
Microsoft.NET			Regular File			
Migration	SETUP.EXE-DD2FF2BC.pf		Regular File	12/4/2024 2:23:48 AM		
ModemLogs	THORIUM.EXE-66FB8EE4.pf			12/4/2024 2:23:54 AM		
	SETUP.EXE-DD2FF2B8.pf		Regular File	12/4/2024 2:23:43 AM		
Offline Web Pages	ASPNET_REGIIS.EXE-40E849C6.pf		Regular File	12/4/2024 2:20:58 AM		
B-C Panther	ASPNET_REGIIS.EXE-C5CCF814.pf		Regular File	12/4/2024 2:20:57 AM		
B- C Performance	LINQWEBCONFIG.EXE-5BC12A0E.pf		Regular File	12/4/2024 2:20:56 AM		
🗰 🧰 PLA	LINQWEBCONFIG.EXE-B663A069.pf	5	Regular File	12/4/2024 2:20:56 AM		
PolicyDefinitions	WFSERVICESREG.EXE-57F828F6.pf	6	Regular File	12/4/2024 2:20:56 AM		
Prefetch     PrintDialog	WFSERVICESREG.EXE-1704209B.pf	5	Regular File	12/4/2024 2:20:55 AM		

Prefetch files for Window 10

Data FTK Imager 4.7.1.2 Mode Help					- C	-
	• 🖸 🎙 🗋 🖹 🗎 🐱 🛣 🐮 🤗 🚬					
	File List			Lover and a second seco		
- Downloaded Program Files	Name	Size	Туре	Date Modified		
	MSEDGEWEBVIEW2.EXE-C49DB0EB.pf	56	Regular File	12/4/2024 6:30:32 AM		
en-US	MSEDGEWEBVIEW2.EXE-C49DB0ED.pf	17	Regular File	12/4/2024 6:30:33 AM		
a explorer.exe	MSEDGEWEBVIEW2.EXE-C49DB0F8.pf	10	Regular File	12/4/2024 6:30:33 AM		
🖲 🧰 Fonts	MSEDGEWEBVIEW2.EXE-C49DB0F6.pf		Regular File	12/4/2024 6:30:33 AM		
GameBarPresenceWriter	ASPNET_REGIIS.EXE-E7D16D20.pf		Regular File	12/4/2024 7:02:46 AM		
🔅 🛅 Globalization	ASPNET REGIIS.EXE-8545410E.pf		Regular File	12/4/2024 7:02:45 AM		
🐵 🇀 Help						
HelpPane.exe	LINQWEBCONFIG.EXE-9673412C.pf		Regular File	12/4/2024 7:02:44 AM		
hh.exe	LINQWEBCONFIG.EXE-3DA8D97D.pf		Regular File	12/4/2024 7:02:44 AM		
i IdentityCRL	WFSERVICESREG.EXE-915F757D.pf		Regular File	12/4/2024 7:02:44 AM		
IME     ImmersiveControlPanel	WFSERVICESREG.EXE-6E167515.pf	6	Regular File	12/4/2024 7:02:44 AM		
InboxApps	SMCONFIGINSTALLER.EXE-937DEE55.pf	4	Regular File	12/4/2024 7:02:43 AM		
INF	SMCONFIGINSTALLER.EXE-887C1FF3.pf	5	Regular File	12/4/2024 7:02:43 AM		
InputMethod	MSEDGEWEBVIEW2.EXE-C49DB0EC.pf	36	Regular File	12/4/2024 6:30:33 AM		
🗄 🛅 Installer	WIDGETS.EXE-466E9E5A.pf	14	Regular File	12/4/2024 6:27:32 AM		
1 L2Schemas	MSCORSVW.EXE-16B291C4.pf		Regular File	12/4/2024 7:04:54 AM		
LanguageOverlayCache	DRIVER INSTALLER.EXE-6B175320.pf		Regular File	12/4/2024 6:42:17 AM		
- CiveKemelReports	NZXT CAM.EXE-F7ED1A5F.pf		Regular File	12/4/2024 6:37:17 AM		
🖲 🧰 Logs			Regular File	12/4/2024 6:36:11 AM		
🖲 🧰 Media	REMOTEMOUSE.TMP-61049A7A.pf					
mib.bin	GETUSERPROFILEPATH.EXE-992AB388.pf		Regular File	12/4/2024 6:36:11 AM		
Microsoft.NE1     Migration	VC_REDIST.X64.EXE-D249E4AB.pf		Regular File	12/4/2024 6:36:46 AM		
	NETSH.EXE-8174DA63.pf	12	Regular File	12/4/2024 6:36:10 AM		
notepad.exe	REMOTEMOUSE.TMP-4411C3C2.pf	11	Regular File	12/4/2024 6:36:08 AM		
I CO OCR	REMOTEMOUSE.EXE-7C50500B.pf	8	Regular File	12/4/2024 6:36:10 AM		
Offline Web Pages	SC.EXE-F4E1A8F7.pf	3	Regular File	12/4/2024 6:36:13 AM		
🔅 🧰 Panther	VC REDIST.X64.EXE-C41C90EA.pf	12	Regular File	12/4/2024 6:36:43 AM		
🔅 🧰 Performance	WMIAPSRV.EXE-FC8436DD.pf		Regular File	12/4/2024 6:35:44 AM		
👜 🧰 PLA	CAM HELPER.EXE-0D330F1F.pf		Regular File	12/4/2024 6:35:36 AM		
PolicyDefinitions	NZXT CAM.EXE-F7ED1A56.pf		Regular File	12/4/2024 6:35:31 AM		
Prefetch	NZXT CAM.EXE-F7ED1A60.pf		Regular File	12/4/2024 6:35:37 AM		
regedit.exe						
regedit exe     Registration	NZXT CAM.EXE-F7ED1A57.pf		Regular File	12/4/2024 6:35:27 AM		
rescache	NZXT CAM.EXE-F7ED1A59.pf	6	Regular File	12/4/2024 6:35:27 AM		

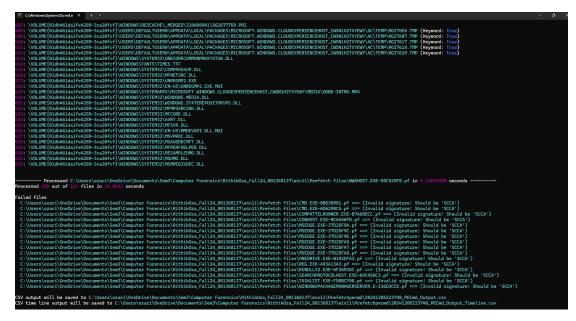
Prefetch for Window 11

			_
∑ C:WindowsSystem32/conde × + ∽			ĸ
Microsoft Windows [Version 10.0.26100.2054] (c) Microsoft Carporation. All rights reserved.			
C:\Users\ozari\OneDrive\Documents\Sem3\Computer Forensics\RithikOza_Fall24_801368137\win10\PECmd>pecmd.exe -d "C:\Users\ozari\OneDrive\Documents\Sem3\Computer Forensics\RithikOza_Fall24_801368137\win10\P s" —csv "C:\Users\ozari\OneDrive\Documents\Sem3\Computer Forensics\RithikOza_Fall24_801368137\win10\Pefetchpecmd'S	refetch	file	
			l
			l

Command for parsing prefetch file in PECmd for Windows 10 (same for Windows 11)

131: VALUE (DIMESCANDIAL-AN
191: Volume (vicuotesva/seda1-aeva1see/swatuotes) sisterista (vicuotes) sioves, vicuotes) vicuotes vicuotes vicuotes vicuotes) vicuotes vi
133: VOLUME (BIdb45c54423eda1-ae443ede1) WINDOWS (SYSTER32) WINDOWS (STREREPOSTIORYDS DLL
194: \VOLUME{81db45c54423eda1-ac443e4e}\wINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOwS\SYSTEM32\WINDOWS\SYTEM32\WINDOWS\SYSTEM32\WINDOWS\SYTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYTEM32\WINDOWS\SYTEM32\WINDOWS\SYTEM32\WINDOWS\SYTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYSTEM32\WINDOWS\SYTEM32\WINDOWS\SYTEM32\WINDOWS\SYTEM32\WINDOWS\SYS
195: \V0LUME{01db45c54423eda1-ae443e4e}\WINDOWS\SYSTEM32\WINDOWS\SYSTEM.PROFILE.PLATFORMDIAGNOSTICSANDUSAGEDATASETTINGS.DLL
196: \VoLUME{01db45c54423eda1-ae443e4e}\\WINDOWS\SYSTEM32\POLICYMANAGER.DLL
197: \VOLUME{01db45c54423eda1-ae443e4e}\WINDOWS\SYSTEM32\MSVCP110_WIN.DLL
198: \VOLUME{01db45c54423edal-ac443e4e}\wINDOwS\SYSTEM32\WINDOWS\SUSTEM32\WINDOWS.UI.WINMD
199: \VOLUME{01db45c54423edal-ae443e4e}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.SECURITY.WINMD
000 : VVUUME (01dbits544023eda1-aed49aede) VXINDONS /SYSTER32/VXINDONS .SECURITY, AUTHENTICATION WEB.CORE.DLL 011 : VVUUME (01dbits544023eda1-aed49aede) VXINDONS /SYSTER32/VXINDONS .SECURITY, AUTHENTICATION WEB.CORE.DLL
201: VoUUME (%10H05CMH23e0a1-ae443e4e3 VAIINUM%) \STS1ED32 (VIECUMELUMINUMPKUXTS1UB-LLD) 202: VOUUME (%10H05CMH23e0a1-ae443e4e3) VARGAME TIELS(%1NOMSENDET MICROSOFTOFFICEHUB_18.1993.1152.9.X64_BMEVHYOFFICE_WINMD
221 VOLUME (2010) COMPACE AND A CONTROL AND
201: VV0LUME[8]dbu5c5u423cda1-ac443c4e]VMIDOWS/SYSTEM32LEN-USVMIDDOWS, SECURITY, AUTHENTICATION, WEB.CORE.DLL.MUI
205: \VOLUME{01db45c54423eda1-ae443e4e}\WINDOWS\SYSTEM32\LOGONCLI.DLL
206: \V0LUME{81db45c54423eda1-ae443e4e}\WINDOWS\SYSTEM32\EN-GB\WINDOWS\STORAGE.DLL.MUI
207: \VOLUME{01db45c54423eda1-ae443e4e}\WINDOWS\SYSTEM32\WEBPLATSTORAGESERVER.DLL
208: \VOLUME{01db45c5u423eda1-ae443e4e}\USERS\VBOXUSER\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D88BWE\AC\INETCACHE\QSZS6HM6\THIRDPARTYNOTICE[1].HTM
209: \VOLUME{01db45c54423eda1-ae443e4e}\wINDOwS\SYSTEM32\CRYPTOWINRT.DLL
210: \VOLUME{01db45c544423eda1-ae443e4e}\USERS\VBOXUSER\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8MEKYB308B8WE\LOCALSTATE\THIRDPARTVNDTICE.HTML.~TMP (Keyword: True)
Processed C:\USers\ozar\UneDrive\Documents\Sem3\Computer Forensics\RithikOza_Fall20_801368137\win10\Prefetch files\WMHHOST.EXE-EDE7CE84.pf in 0.0011c200 seconds Processed 217 out of 229 files in 5.4415 seconds
<pre>Failed files C: Users vara:\/nebrive\Documents\Sem3/Computer Forensics\RithidOza_Fail20_801368137\uinlo\Prefetch files\SEARCHFILTENGST.EXE-AN7ALFDD.pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_801368137\uinlo\Prefetch files\SEARCHFILTENGST.EXE-AN7ALFDD.pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_801368137\uinlo\Prefetch files\SEARCHFILTENGST.EXE-AN7ALFDD.pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_801368137\uinlo\Prefetch files\SETUP_DE-S3786420.pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_801368137\uinlo\Prefetch files\SETUP_DE-S3786420.pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_801388137\uinlo\Prefetch files\SETUP_DE-S3786420.pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_801388137\uinlo\Prefetch files\SETUP_DE-S3786420.pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_801388137\uinlo\Prefetch files\NDBERDE, pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_80138137\uinlo\Prefetch files\NDBERDE, pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_80138137\uinlo\Prefetch files\NDBERDE, pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_80138137\uinlo\Prefetch files\NDBERDE, pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/Computer Forensics\RithidOza_Fail20_80138137\uinlo\Prefetch files\NDBERDE, pf ⇒&gt; (Invalid signature: Should be 'SCCA') C: Users vara:\/nebrive\Document\Sem3/</pre>
CSV output will be saved to C:\Users\ozari\OneDrive\Documents\Sem3\Computer Forensics\RithikOza_Fall24_801368137\win10\Prefetchpecmd\20241205223304_PECmd_Output.csv CSV time line output will be saved to C:\Users\ozari\OneDrive\Documents\Sem3\Computer Forensics\RithikOza_Fall24_801368137\win10\Prefetchpecmd\2024120522304_PECmd_Output_Timeline.csv
C:\Users\ozari\OneDrive\Documents\Sem3\Computer Forensics\RithikOza_Fall24_801360137\PECmd>

Output for Windows 10



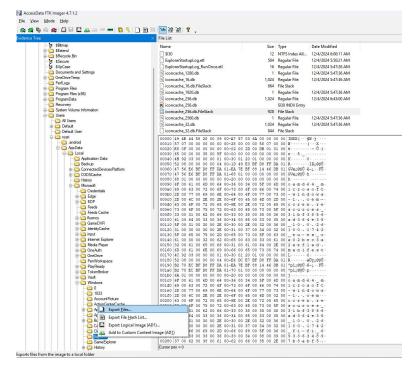
Output for windows 11

## 5. Thumbnail Cache

Description: Windows generates thumbnail cache files for images in the test folder.

Method of Collection:

Extract thumbnail cache files in FTK imager from "win10\_copy.vmdk\Partition 1 [51198MB]\NONAME[NTFS]\[root]\Users\vboxuser\AppData\Local\Microsoft\Windows\Explo rer" and export all the files to "win10/Thumbnail Cache; win11/Thumbnail Cache", after which I have parsed the files using Thumbcache\_viewer\_64 in csv format for further inspection at "win10/Thumbnail Cache/exported; win11/Thumbnail Cache/exported".



Extracting thumbnail cache files in FTK imager Windows 11 (similar for Windows 10)

F	ilename								
	licitatite	<b></b>	Open a Thumbca	ache Databa	ise file				×
		÷	→ ~ 1	N 🛄 «	win10 > Thumbnail Cache	> Explorer ~	C Search Expl		م
		Or	ganise 🔻 🛛 N	lew folder				∎ -	
		>	👝 Rithik - Pers	sona	Name	Status	Date modifie	d i	<sup>Type</sup>
		-		_	🗟 iconcache_16		12/3/2024 9:0	02 PM	Data Base
			🥅 Desktop	*	iconcache_32	C .	12/3/2024 9:(	02 PM	Data Base
		11	🕹 Downloads	*	😼 iconcache_48		12/3/2024 9:0	02 PM	Data Base
			Documents	*	🚯 iconcache_96	<u>.</u>	12/3/2024 9:0	02 PM	Data Base
			🔀 Pictures	*	🔹 iconcache_256	<b>3</b>	12/3/2024 9:0	02 PM	Data Base
		1.0	<b>~</b>		-			-	
				File name	iconcache_32" "iconcache	_48" "iconcache_96" "icon	cacł ~ Thumbca	che Database Fi	iles (*.1 🗸
							Open	Ca	ance

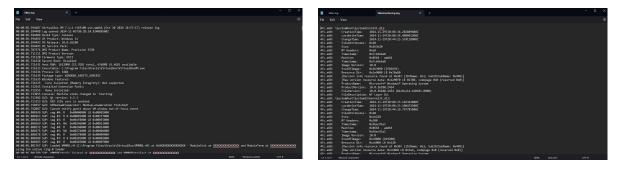
Loading all thumbcache into Thumbcache Viewer to parse and get output into csv file.

# **Findings and Forensics Analysis:**

Observations from the "test" Folder Experiment

## **Event Logs**

All the logs files are saved in "win10/Event logs; win11/Event logs" for Windows 10 and 11 respectively. Here is a preview of those logs:

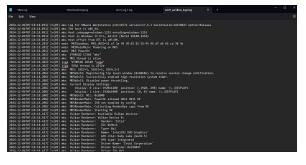


System event log for Windows 10



System event log for Windows 11

Security event log for Windows 10



Security event log for Windows 11

# System Log Analysis:

System Configuration:

- Both logs identify Windows 11 as the host OS.
- Similar build versions suggest the systems are running comparable software updates.

Virtualization Platforms:

• Log 1 pertains to VirtualBox, while Log 2 corresponds to VMware Workstation, showcasing two distinct virtual machine environments.

Activity Focus:

- The VirtualBox log is centered on system setup and hardware configurations.
- The VMware log includes user-specific paths and runtime details, indicating a more dynamic usage profile.

Security and Boot:

- Both logs reflect the use of UEFI firmware, a modern boot standard.
- VirtualBox specifically notes that Secure Boot is turned off.

### Security Log Analysis:

VBoxHardening:

This log is primarily focused on verifying the integrity and security of essential system files to ensure their reliability and protection against tampering.

#### **Purpose and Focus**

- Objective: To validate system-critical files and confirm they remain unaltered and secure.
- Files Examined: Key system libraries, such as ntdll.dll, located in \SystemRoot\System32\.

#### Metadata of Files:

- Example File: \SystemRoot\System32\ntdll.dll.
- Creation Time: 2024-11-29T20:08:34.282889800Z.
- Last Modified: 2024-11-29T20:08:34.408091200Z.
- Last Change: 2024-11-29T20:44:23.524118800Z.
- Size: Approximately 2.5 MB (0x263b20 bytes).

- NT Headers: Offset 0xe8, indicating the location of the Portable Executable (PE) file header.
- Architecture: amd64, confirming compatibility with 64-bit systems.

#### Validation Processes:

- Timestamps: The log cross-verifies file timestamps to detect potential tampering.
- File Attributes: Includes markers like 0x20, signifying the file's archive status.
- Integrity Checks:
- Verifies headers and metadata for anomalies or corruption.
- Ensures the file is correctly aligned with the operating system's architecture.

#### **Security Measures:**

- Ensures compliance with system security policies by thoroughly examining core files.
- Repeated validation steps ensure no unauthorized modifications are present.

#### Observations

- Comprehensive Checks: The log offers meticulous detail, highlighting security and integrity at the file level.
- Structure: Organized for systematic review, making it effective for auditing and identifying system vulnerabilities.
- Relevance: Ideal for ensuring stability and trustworthiness of the system's foundational components.

#### win11\_sandbox\_logs:

This log captures real-time operations, configurations, and processes of a Windows 11 system, offering a dynamic view of its functionality.

#### **Purpose and Focus**

- Objective: To document system activity and operational behaviors, with a focus on runtime processes and configurations.
- Real-Time Tracking: Provides insights into system performance, errors, and host details.

#### Host System Information:

- Architecture: x86\_64 (64-bit).
- Operating System: Windows 11 Pro, 64-bit.
- Build Version: 26100.2454.
- Encoding: windows-1252, denoting the system's character set.
- Time Zone: UTC +05:00, reflecting regional settings.

#### **Runtime Processes:**

Examples:

- MKSRoleMain: Powering on MKS Indicates the initialization of a critical system process.
- MKS thread is alive Confirms successful activation and operation of a thread.

#### **Errors and Warnings:**

- Identifies missing or inaccessible files, such as config.ini, which might impact performance or functionality.
- Logs UUIDs and other unique identifiers for processes to facilitate troubleshooting.

#### **System Interactions:**

- Tracks the relationships and interactions between various processes and threads, offering a dynamic perspective on system activity.
- Provides timestamps and details for system events, aiding in detailed analysis.

#### Observations

- Real-Time Insight: Captures the current state and interactions of the system, making it invaluable for monitoring.
- Error Detection: Highlights configuration issues or missing files, helping administrators address potential problems.
- Operational Emphasis: Focuses on live processes and system behavior rather than static file validation.

The VBoxHardening.log is a specialized tool for ensuring the security and integrity of a system, offering detailed insights into the state of critical files. It is essential for maintaining system reliability and compliance.

On the other hand, the win11\_sandbox\_logs.log provides a dynamic view of the system's performance and operations, capturing runtime activity and errors. It complements the hardening log by offering a broader perspective on the system's health and real-time interactions.

Together, these logs provide a comprehensive understanding of the system, covering both its foundational security and dynamic operations. This dual approach ensures that the system remains secure, stable, and efficient.

# **Registry Entries:**



SOFTWARE registry log for Windows 10 Windows 10

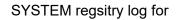
ukritisibuvurgitu X +	o ×
File Edit View	۲
Hive (C:Ubars\zari\dwdriveldocameti\$aab)(coputer formsics\hidda_falld_bH186137\dot1Ubgistry file\S6TM#E_vdct1) is dirty. I' yaa waa to process Nim tomaaction logs, plaase contider using ywg = registryfian.gy Owdan \$Annow (r-slarce (frC: Gumeran).	
urtingenie v.2010120 (offbare, stuer.dt) Get Artine Setup StafPath values MTRE: 11547 (SetIsteck)	
Key path: MicrosoftVctive SetupiInstalled Components	
Nawe INCONCIPTIONO MAILS Player Laricetta tess: Norte-Ad-81 (8) (9):22: StadBate : X0 ptendio031 (ystead) unreged.exe / Noad89 Elizabilio : 8	
Rease : Deams Series : Lincetter time: 2004 6-34 97 25:00 07 Staldard : //downloada 11 Lincetalier : 1	
Intercont History Multi-Player           Exercise the History And ed. 90 (H) 022.           Statistict ::         Statistict ::           Statistict ::         Statistict ::	
Rame i Vilotos (astro (listo) Entrelin time: 2014.04.21 (2):55.42 Statem : U Entrelin 1	
Rease : We Patters Guinedication Limitation teles: 2001-244 05:17:202 Scalara : Childholoc System22Lefalati.cee -UserGeetig Enfektive : 1	
141 Cold AMERICAN AND A COLD AND	

SOFTWARE registry log for Windows 11 Windows 11





wintDaystenreg.tat			- u x
			8
you need to process h	STBf_winil) is dirty. hive transaction logs, please consider using yarg + registryflush.py cm (frif limewam).		
ow upgrade v.2023075 rstem) Check for Allow RE: T1601 (defense ev	wUpgradesWithUnsupportedTPMDrCPU value		
path: Setup\MoSetup LastWrite time: 2024			
lates to be installed	wdogradenWithUnsupportedTPWorCPU' value set to 1 is a hack to allow Windows 11 on systems that did not meet the TPM or CPU checks. This could be interpreted as oursion by upgrading the system image to provide additional capabilities, such as ndroid.		
: https://support.mic			
nching appeartdlls v. RE: T1546.009 (privil	.20200813		
tro15et001\Contro1\Se			
compatcache v. 2022002			
divite Time: 2024-12- nature: 0x34			
Users\ozar1\AppDeta\L NTNDWS\SvsWW64\regs	Sitesittesittisittak_51=4423Movie.ewe 2024-12-04.06109133 LonalWitcrosoft/NombringNombringNombringNombringLater.exe 2024-12-04.05:54:56 Sym23.ce. 2023-12-04.05105114 MOVDTI (M.w.s.2004.051051-105-270		
L Col 1 372.681 characters		100% Windows (CRUP)	UT7-8



## Anaysis:

Active Setup

- Windows 10: Entries include components like "Microsoft Windows Media Player," "Themes Setup," and "Windows Desktop Update." Updates are reflected with timestamps up to December 3, 2024. Some items are inactive, indicated by IsInstalled set to 0.
- Windows 11: Features similar components, with additional entries such as "Microsoft Edge Configuration" and timestamps updated through December 4, 2024. StubPath values point to system-level processes, such as Rundll32.exe.
- Key Difference: Windows 11 includes more recent updates and a broader range of components, reflecting system-level refinements.

### App Paths

• Windows 10: Common paths point to apps like Mozilla Firefox (firefox.exe) and Microsoft Edge (msedge.exe), with some historical entries dating back to 2019 for executables like wmplayer.exe and WORDPAD.EXE.

- Windows 11: Path updates align with modern software, listing newer versions of browsers and tools, including utilities for Internet Explorer (IEDIAGCMD.EXE).
- Key Difference: Windows 11 reflects updates for modern applications and streamlined path configurations.

#### AppInit\_DLLs

- Windows 10: The key, last updated on December 4, 2024, shows AppInit\_DLLs is blank, and LoadAppInit\_DLLs is set to 0, preventing unauthorized DLL injection.
- Windows 11: Maintains the same structure and settings, with recent timestamps suggesting periodic system maintenance.
- Key Difference: Both systems adhere to default security measures, with no active use of AppInit\_DLLs.

#### Authentication (LogonUI)

- Windows 10: The last logged-in user is listed as "vboxuser" with a specific SID. AutoAdminLogon is enabled, allowing automated logins.
- Windows 11: The last user is "ozari," with an updated SID and display name. AutoAdminLogon remains active.
- Key Difference: Windows 11 reflects updated user details, indicative of a new primary user or administrative setup.

#### **File Associations**

- Windows 10: File associations include entries like .evtx linked to eventvwr.exe, with some configurations dating back to 2019.
- Windows 11: Similar associations, but updated for recent system configurations and newer timestamps.
- Key Difference: Windows 11 shows more up-to-date file handling settings.

#### Security and Certificates

- Windows 10: Default certificate trust settings under Microsoft\SystemCertificates and EnterpriseCertificates are intact, with no suspicious values.
- Windows 11: Similar certificate setups, with updates reflecting administrative adjustments.
- Key Difference: Both systems maintain consistent security baselines, with slight refinements in Windows 11.

#### Audio Devices

• Windows 10: Lists standard audio devices, such as "Speakers" and "Microphone," with unique GUIDs per device.

- Windows 11: Updated device list includes newer audio hardware, suggesting hardware or system changes.
- Key Difference: Windows 11 supports more recent audio devices or configurations.

Persistence and Security Configurations

- Windows 10: Critical registry keys, such as Active Setup and AppInit\_DLLs, show no signs of suspicious entries, maintaining default values.
- Windows 11: Similar approach, with refreshed timestamps reflecting ongoing updates.
- Key Difference: Windows 11 demonstrates minor updates in persistence prevention strategies.

System Upgrade and Compatibility

- Windows 10: No registry key for bypassing hardware checks (AllowUpgradesWithUnsupportedTPMOrCPU), aligning with legacy hardware compatibility.
- Windows 11: While the Setup\MoSetup key exists, no evidence of bypassing hardware requirements is present.
- Key Difference: Windows 11 aligns with modern hardware requirements and stricter upgrade policies.

Persistence Mechanisms

- Windows 10: The AppCompatCache logs apps like RemoteMouse.exe and various executables from late 2023. No entries suggest DLL injection.
- Windows 11: Logs include applications like Attack\_SharkX3Mouse.exe and NZXT CAM.exe, reflecting enhanced tracking.
- Key Difference: Windows 11 expands application tracking for improved monitoring.

Registry and Backup Settings

- Windows 10: Excludes standard items, such as %TEMP% and hiberfil.sys, from backups, with minimal changes to default settings.
- Windows 11: Updated registry entries and additional exclusions reflect periodic maintenance.
- Key Difference: Windows 11 incorporates modernized backup configurations.

Security and Logging

- Windows 10: Defender logging is active with no signs of tampering.
- Windows 11: Retains active Defender logging with enhanced entries for system activity tracking.

• Key Difference: Windows 11 improves logging granularity while maintaining similar configurations.

#### Application Compatibility

- Windows 10: The AppCompatCache tracks legacy apps, such as NZXT CAM.exe and RemoteMouse.exe, ensuring compatibility.
- Windows 11: Reflects modern application usage, including tools like Edge helpers and updated OneDrive versions.
- Key Difference: Windows 11 emphasizes compatibility with contemporary applications.

#### **Device Management**

- Windows 10: Minimal Bluetooth configurations, with no active devices in BTHPORT.
- Windows 11: Similar default settings with limited device registration.
- Key Difference: Both systems show default configurations for Bluetooth.

#### Crash and Diagnostic Settings

- Windows 10: Configured for crash dumps and basic diagnostics.
- Windows 11: Maintains the same settings for post-crash data capture.
- Key Difference: No notable changes between versions.

#### Performance and Code Pages

- Windows 10: Uses code page 1252 for legacy encoding compatibility.
- Windows 11: Retains the same setting for continuity.
- Key Difference: Both systems preserve legacy encoding support.

Windows 11 introduces notable updates, including more modern application compatibility, enhanced tracking in AppCompatCache, stricter adherence to hardware requirements, and updated backup and logging configurations. These changes reflect a focus on adapting to newer software and hardware ecosystems while maintaining robust system security

# File Metadata

Report Navigation	Autopsy Forensic Report	Report Navigation	Autopsy Forensic Report
C. Constantin	HTML Report Generated on 2024/12/05 10:50:23	Case Summary	Case 1
Case Summary	Case: win10	Accounts: Email (1)	Case Number: 1
Chromium Extensions (28)	Case Number: 1	🔶 Chromium Extensions (54)	Number of data sources 1
Chromium Profiles (1)	Number of data 2	+ Chromium Profiles (2)	in case:
Tata Source Usage (1)	sources in case: Examiner: Rithik	🔶 Data Source Usage (1)	
EXIF Metadata (3)	Oza	Encryption Suspected (18)	Image Information:
Encryption Suspected (3)			
Extension Mismatch Detected (255)	Image Information:	Extension Mismatch Detected (182)	Windows 11 xS4.vmdk
Favicon (39)	indge monitation.	🔶 Favicon (70)	Timezone: America/New_York
Installed Programs (42)	win10_copy.vmdx	🤘 Installed Programs (06)	Path: D'all/Windows 11 x64.vmdk
<ol> <li>Keyword Hits (2834)</li> </ol>	Timezone: America/New_York	Alexandre (5)	
(A Metadata (79)	Path: C:/Users/ozari/Downloads/win10_copy.vmdk	Operating System Information (1)	Software Information:
g Operating System Information (1)	Windows 11 x54.vttdk	Recent Documents (40)	Autopsy Version: 4 21.0
Recent Documents (18)		🔶 Recycle Bin (4)	Android Analyzer Module: 4.21.0
	Timezone: America/New_York	╈ Shell Bags (14)	Android Analyzer (aLEAPP) Module: 4.21.0
Kun Programs (417)	Path: C./Users/ozari/OneDrive/Documents/Virtual Machines/Windows 11 x64/Windows 11 x64.vmdk	Tapped Files (0)	Central Repository Module: 4.21.0
Shell Bags (5)		Tagged Images (0)	DJI Drone Analyzer Module: 4.21.0
Tagged Files (0)	Software Information:		Data Source Integrity Module: 4.21.0
Tagged Images (0)	Autopsy Version: 4.21.0	Tagged Results (0)	Email Parser Module: 4.21.0
* Tagged Results (0)	Android Analyzer Module: 4.21.0	USB Device Attached (18)	Embedded File Extractor Module: 4.21.0
USB Device Attached (2)	Android Analyzer (aLEAPP) Module: 4.21.0	Web Account Type (194)	Encryption Detection Module: 4.21.0
User Content Suspected (3)	Central Repository Module: 4.21.0	Web Accounts (314)	Extension Mismatch Detector Module: 4.21.0
Web Account Type (1)	DJI Drone Analyzer Module: 4.21.0	/ Web Bookmarks (32)	File Type Identification Module: 4.21.0 GPX Parser Module: 1.2
1 Web Accounts (1)	Data Source Integrity Module: 4.21.0	Web Cache (938)	GPX Parser Module: 1.2 Hash Lookup Module: 4.21.0
/ Web Bookmarks (5)	Email Parser Module: 4.21.0	Web Categories (6)	Interesting Files Identifier Module: 4.21.0
	Embedded File Extractor Module: 4.21.0	Web Cookies (54)	Keyword Search Module: 4.21.0
Web Cache (1023)	Encryption Detection Module: 4.21.0		PhotoRec Carver Module: 7.0
Wab Categories (5)	Extension Mismatch Detector Module: 4.21.0 File Type Identification Module: 4.21.0	Web Downloads (8)	Picture Analyzer Module: 4.21.0
i Web Cookies (125)	GPX Parser Module: 1.2	<ul> <li>Web Form Autofil (234)</li> </ul>	Recent Activity Module: 4.21.0
Web Downloads (7)	Hash Lookup Module: 4.21.0	Web History (48)	Virtual Machine Extractor Module: 421.0
Web Form Autofil (1)	Interesting Files Identifier Module: 4.21.0		YARA Analyzer Module: 4.21.0
Web History (24)	Keyword Search Module: 4.21.0		IOS Analyzer (ILEAPP) Module: 4.21.0
Web Search (2)	PhotoRec Carver Module: 7.0		
	Picture Analyzer Module: 4.21.0		Ingest History:
	Recent Activity Module: 4.21.0		Job 1:
	Virtual Machine Extractor Module: 4.21.0		Data Source: Windows 11 x64.vmdk
	YARA Analyzer Module: 4.21.0		Status: CANCELLED
	IOS Analyzer (ILEAPP) Module: 4.21.0		Enabled Modules: Recent Activity
	Ingest History:		Hash Lookup File Type Identification
	Job 1:		Extension Mismatch Detector

#### Windows 10 Forensics report

Windows 11 Forensics report

### Analysis:

#### **Chromium Extensions**

- Windows 10: Limited use of extensions, primarily for PDF viewing and media, tied to a virtual machine environment.
- Windows 11: Expanded extensions, including Edge-specific tools and Microsoft Store integrations, indicating active and updated use.

#### **Chromium Profiles**

- Windows 10: Single, default profile with no user-specific configurations.
- Windows 11: Detailed profiles linked to user accounts, reflecting personalization and diverse use cases.

#### Data Source Usage

- Windows 10: Logs from a virtualized environment for testing purposes.
- Windows 11: Reflects deployment on a physical system with full installation.

#### Encryption

- Windows 10: Encrypted files primarily include Defender scans and compressed files.
- Windows 11: Broader encryption scope, including system and application components.

#### **Extension Mismatch**

- Windows 10: Mismatched file extensions in test paths under a virtual machine.
- Windows 11: Expanded instances, reflecting a more active and complex application environment.

#### Favicons

- Windows 10: Limited to basic domains like bing.com.
- Windows 11: Broader domain coverage, reflecting diverse browsing activity.

#### **Installed Programs**

- Windows 10: Focused on test tools and utilities.
- Windows 11: Longer history of software use, with re-installations and upgrades.

#### Metadata

- Windows 10: Minimal metadata tied to system files.
- Windows 11: Enhanced metadata with user contributions and structured tracking.

#### **Operating System**

- Windows 10: Virtualized Windows 10 Home with generic setup.
- Windows 11: Upgraded and personalized Windows 11 installation.

#### **Recent Documents**

- Windows 10: Test files with limited activity.
- Windows 11: Broader and more recent document usage.

#### Shell Bags

- Windows 10: Test environment paths with limited user interaction.
- Windows 11: Richer user activity logs with personalized paths.

#### Case Summary

- Windows 10: Simplified forensic case setup.
- Windows 11: Complex workflows with multiple data sources.

#### **USB** Devices

- Windows 10: Minimal USB activity in a virtual environment.
- Windows 11: Broader device interaction, reflecting active usage.

#### Web Accounts

- Windows 10: Single account entry (Google).
- Windows 11: Multiple accounts across platforms like Discord and Spotify.

#### Web Bookmarks

- Windows 10: Default browser entries.
- Windows 11: Personalized bookmarks synced across devices.

#### Web Cache

- Windows 10: Smaller cache focused on test activity.
- Windows 11: Expanded cache with detailed metadata.

#### Web History

- Windows 10: Test-focused browsing activity.
- Windows 11: Broader and more dynamic web usage.

Windows 11 reflects a transition to a fully personalized and actively used system compared to the virtualized, test-focused environment of Windows 10. It exhibits richer metadata, broader encryption scope, enhanced web activity, and improved user interaction across profiles, accounts, and programs.

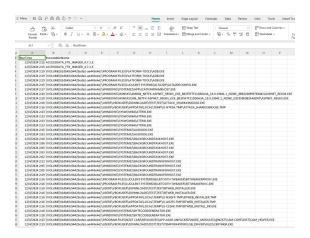
# **Prefetch Files**

2	ra d	6	Calib	ni	~ .	11 ~ A+ A	$\sim - 1$	= _ + +		20	Wrap	Text	Gene	ral	~	Rows	and Columns 🗸	E	₽4 ~	Fi	ill ~ [	]↓ Se
	Paste ~ [	Ġ~	в 2	<u>v</u> .		Q . A . Q .		= = = ⊫			🖽 Merge	and Center ~	8.	%	000 €•0 •00 • •00 →•0	Work:	sheet ~	Conditiona	a ∏ -	ΣA	utoSum ~ 5	74
Painter																		Formatting				
										📩 LA	ST CALL! B	uy 2 years of W	PS Pro, get	15 moi	nths FREE!	Get Now						
B2	~	e	fx fx	C:\Users\	ozari\One	Drive\Documents\S	em3\Cc	mputer Forensi	cs\Rit	hikOza_Fa	all24_8013	368137\win10	)\Prefetch	n files\	ACCESSDATA_	TK_IMAG	ER_4.7.1.E-6B6	A2BBC.pf				
			c	o	8		6	1.8.1.6.1	(a)	x	1	м	N O P	QR	5		т	[ u ]	v w	x	v   z	
SourceFilenan	ne	SourceCn		ourceModified S		ExecutableName ACCESSDATA_FTK_IMAGER_4.7.1.E	Hash 685.0288C	Size Version B 180452 Windows IX	unCount	LastRun 12/4/2004 2:15		PreviousRun1 Previo	ousRun2 Prev Prev		VolumeOName		Volume@Sorial	VolumeOCreated V	olume1Ns Volume1	15e Volume10	VOLUMEN VOLUM	
C\Users\azar	I)DreDrive)Docum					ACCESSOATA FTK MAGER 4.7.1.E		214522 Windows IC		12/4/2024 2:15					\v0LUME[01db43c54425		A0443040	12/3/2024 20:52			(VOLUME)C (VOLUM	
	1),DeeDrive\Docum		5/2024 21:25		12/5/2024 22:33		F4220043	28922 Windows 30	3			12/4/2024 2:19			\v0uums(01db45c54423)		AE443E4E	12/3/2024 20:52			VOLUME (C VOLUM	
	ADeDrive\Docum		5/2024 21:25	12/5/2024 3:58 12/5/2024 3:58		ALTA20PCONFIG.EXE APPUCATIONFRAMEHOST.EXE	3D8076CF	90750 Windows IC 62220 Windows IC	1	12/4/2024 2:15					WOLLIME[01db45c54423/ WOLLIME[01db45c54423/		AE443E4E AE443E4E	12/3/2024 20:52 12/3/2024 20:52			VOLUME): WOLUN	
	(DeeDrive)Docum		5/2024 21:25	12/5/2024 3:58		ASPNET REGISLEXE	40534905	27432 Windows IC	- 1	12/4/2024 2:20					WOLLIME101db45c54423		AE443E4E	12/3/2024 20:52			WOLLWEIC WOLLN	
C\Users\azar	DeeDrive\Docum	× 12/	5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33	ASPNET REGIS.EXE	CSCCF814	25784 Windows IC	1	12/4/2024 2:20	0				WOULME(01db45c54428	da1 ae443e4e)	AE443646	12/3/2024 20:52			WOULDNESS WOULD	eesc.
	(DeeDrive)Docum		5/2024 23:25			ATTACK, SHARKISMOUSE EXE	387AAC19	30506 Windows IC	1	12/4/2024 2:16					\v0UUME(01db45c54425		AE443848	12/3/2024 20:52			/vounsic/voun	
	1)/DeeDrive)/Docum 1)/DeeDrive)/Docum		5/2024 21:25	12/5/2024 3:58 12/5/2024 3:57	12/5/2024 22:33	ATTACK SHARKOMOUSE TMP	9ED17AD0 8E828325	46544 Windows IC 7242 Windows IC				12/4/2024 2:23 12/4/2	024 2:23		WOLUME[01db45c54423		AE443E4E AE443E4E	12/3/2024 20:52 12/3/2024 20:52			(VOLUME)C (VOLUM	
C'Users'azar	NDreDrive\Docum	w 12,	3/2024 21:25	12/5/2024 3:58	12/5/2024 22:53	AUDIODS.EXE	DOD776AC	22600 Windows 30	2	12/4/2024 2:15	12/4/2024 2:03				\v0LUME[01db45c54423	da1 ae443e4e)	AE443848	12/1/2024 20:52			VOLUME C WOULD	rejc
C:\Users\ozar	1)DecDrive)Docum	n: 12/	5/2024 22:25			BADKGROUNDTASKHOST.EXE	3690C537	55372 Windows 30			12/4/2024 2:00				\v0uumt(01db45c54423		AE443E4E	12/3/2024 20:52			(VOLUME): (VOLUM	
	NDneDrive\Docum		5/2024 21:25	12/5/2024 3:58		BACKGROUNDTASKHOST EXE BACKGROUNDTASKHOST EXE	4025F763 8490FF36	43678 Windows IC 68332 Windows IC	2	12/4/2024 2:05	12/4/2024 2:03				WOLLMEID1db45c54423		A5443545	12/3/2024 20:52			(NORTWER: MORTH	
	1)DeDrive)Docum		5/2024 21:25	12/5/2024 3:58		BACKGROUNDTRANSFERHOST.EXE	540E9620	68352 Windows IX 85542 Windows IX	1		12/4/2024 2:00	12/4/2024 2:05			WOULME(018045c54425		AE443E4E	12/3/2024 20:52			(NORDWERC (NORDW	
	UneDrive\Docum		5/2024 21:25	12/5/2024 3:57		BADOGROUNDTRANSFERHOST.EXE	FOFF9666	35644 Windows X	1	12/4/2024 2:19					\v0LUME(01db45c54423		AE443545	12/3/2024 20:52			(VOLUME): (VOLUM	
	()DeeDrive)Dooum		5/2024 21:25	12/5/2024 3:58		BTTWEAKERPROXY.EXE	96804000	54318 Windows IX	1	12/4/2024 2:16					WOULDMEJ03db45c54423		A6443648	12/3/2024 20:52			(voume): (voun	
	1\DecDrive\Docum 1\DecDrive\Docum		5/2024 21:25	12/5/2024 3:58		BTTWEAKERSVCEKE BTWER INSTALLER.EXE	90633879	16350 Windows IC 34996 Windows IC	1		12/6/2024 2:16				WOLUME (01db45c54423		AEAA3EAE	12/3/2024 20:52			(VOLUME): (VOLUM	
	ADreDrive\Docum		5/2024 21:25	12/5/2024 3:58		STWEE INSTALLER.TMP	24898938	62110 Windows IC	1	12/4/2024 2:16					WOLUME[01db45c54423		A8443848	12/3/2024 20:52			WOULDNESS WOULD	
	NDreDrive\Docum		5/2024 21:25	12/5/2024 3:58		STWEE INSTALLER.TMP	65ADZAES	58476 Windows 20		12/4/2024 2:16					\v0LUME(01db43c54423		AE443E4E	12/1/2024 20:52			VOLUME C VOLUM	
	1/DeeDrive/Docum		5/2024 21:25	12/5/2024 3:58		BTWEB INSTALL RREXE BYTECODEGENERATOR FXE	1.235	OR 141982 Windows IC 26668 Windows IC	1	12/4/2024 2:16	12/4/2024 2:18				WOULIME(01db45c54423)		A5443545	12/3/2024 20:52			VOLUME)C (VOLUM	
	ADreDrive Docum		3/2024 21 25	12/5/2024 3:58		CAM HEUPEREXE	C4657305	23878 Windows IC		12/4/2024 2:22					WOLLMEID1db43c34423		ATAAVAT	12/1/2024 20:52			WOULWEST WOULK	
	h/DneDrive/Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33		C796006F	14584 Windows SC	4			12/4/2024 2:19 12/4/20			\v0uuMt(01db45c54423		AE443E4E	12/2/2024 20:52			(VOLUME)C (VOLUM	
	NOneDrive\Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33		89305047	11870 Windows IC							WOLUMEI01db45c54423		AE443E4E	12/3/2024 20:52			(VOLUME): WOLUM	
	(DeeDrive)Docum		5/2024 23:25	12/5/2024 3:57	12/3/2024 22:33	COMPATTE RINNER DVE	EASTEASE EENISCO	13542 Windows IC 11565 Windows IC	8			12/4/2024 2:23 12/4/20			WOULDME(01db45c54423		AE443E4E	12/3/2024 20:52			(VOLUME): (VOLUM	
	\OneDrive\Docum		5/2024 21:25	12/5/2024 3:58		COMPRESSRY EXE	FC36EA77	18612 Windows IC	5			12/4/2024 2:13 12/4/20			\v0tUMF[01db45c54423		AE443646	12/3/2024 20:52			(VOLUME): (VOLUM	
	I/DreDrive/Docum		3/2024 21:25	12/5/2024 3:57	12/3/2024 22:32		32388401	23374 Windows IC							VOLUME(01db45c54423		AE443545	12/3/2024 20:52			(VOLUME)C (VOLUM	
	1/DreDrive/Docum		5/2024 21:25	12/5/2024 3:57	12/5/2024 22:32		65F6206D	314676 Windows 10 34782 Windows 10	10	12/4/2024 2:21 12/4/2024 2:02		12/4/2024 2:17 12/4/20	024 2:17 www eee		VOLUME[03db45c54423 VOLUME[03db45c54423		AE44324E AE44324E	12/3/2024 20:52			VOLUME(C)VOLUM	
	ADreDrive Docum		3/2024 21.25	12/5/2024 3:58		DEFAULT BROWSER AGENT.EXE	38484082	14934 Windows IC		12/4/2024 2:18					WOLUME/01db45c54425		A5443545	12/3/2024 20:52			(voume): (voun	
	i\DeeDrive\Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33		A730F696	33092 Windows 20		12/4/2024 2:19					\v0UUME[01db45c54423		AE443E4E	12/3/2024 20:52			VOLUME C VOLUM	
	NOneDrive\Docum		5/2024 21:25	12/5/2024 3:57	12/5/2034 22:33		5873590	19986 Windows IC	1	12/4/2024 2:19					WOULINE JOI db45c54423		A5443545	12/3/2024 20:52			VOLUME): WOLUM	
	(DeeDrive)Docum		5/2024 21:25		12/5/2024 22:33		P726681 308267A2	17070 Windows IC 32292 Windows IC		12/4/2024 2:18					WOLUME1018645654425		A2443242 A2443242	12/3/2024 20:52			WOLDMER WOLDN	
	\DeeDrive\Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33		63268510	19934 Windows IC	1	12/4/2024 2:04					\v0uum#j01db45c54423		A5443545	12/3/2024 20:52			(VOLUME)C (VOLUM	
	/DreDrive\Docum		3/2024 21:25	12/5/2024 3:58	12/5/2024 22:33		69004068	22446 Windows IC	1	12/4/2024 2:02					\v0UUME(01db45c54423		AE443848	12/3/2024 20:52			(voumetc )voun	
	(Deprive)Docum		5/2024 21:25	12/5/2024 3:57 12/5/2024 3:58	12/5/2024 22:32		71214 74CFC884	27300 Windows 10 28784 Windows 10	11	12/4/2024 2:22 12/4/2024 2:15		12/4/2024 2:16 12/4/2	024 2:15 www.mem		VOLUME[01db45c54423		A2443242 A2443242	12/1/2024 20:52			VOLUME (C VOLUM	
	(OneDrive) Docum		5/2024 21 25		12/5/2024 22:83		SHRDDF55	19826 Windows IC		12/4/2024 2:02					WOLLIMFIO1/045/54423		19413945	12/3/2024 20:52			WOLLMER WOLLS	
	(DeDrive)Docum		5/2024 22:25		12/3/2024 22:33		C3C53689	16582 Windows IC	3			12/4/2024 2:17			\v0LUME[01db45c54423		AE443E4E	12/3/2024 20:52			(voume)c (voum	
	1\DecDrive\Docum		5/2024 21:25	12/5/2024 3:58		DOWNLOAD.EXE	74297FAE	222682 Windows 10	1	12/4/2024 2:17					\v0tum#j01db45c54423		AE443E4E	12/3/2024 20:52			(VOLUME): (VOLUM	
	(DeDrive)Docum		5/2024 21:25	12/5/2024 3:57		DRVER_INSTALLER EXE DRUDCAM_SETUP.6.5.2.EXE	D8DE3856	51534 Windows IC 68828 Windows IC	- 1	12/4/2024 2:23					WOLLMEI01db45c54423		AE443E4E AE443E4E	12/3/2024 20:52 12/3/2024 20:52			(VOLUME): (VOLUM (VOLUME): (VOLUM	
	1)Debrive(Docum		5/2024 22:25	12/5/2024 3:58	12/5/2024 22:33		5F8E77CD	46896 Windows 30	10			12/4/2024 2:22 12/4/2	024 2:19 mm ent		(VOLUME(01db45c54423		AE44364E	12/3/2024 20:52			(vocume)c (vocum	
	NOneDrive\Docum		5/2024 21:25	12/5/2024 3:57		DSMUSERTASK.EXE	E6SECED9	22492 Windows (C	3		12/4/2024 2:23	12/4/2024 2:03			WOLUME(01db45c54428		AE443848	12/3/2024 20:52			WOLLIMES: WOLLIN	
	1/DreDrive/Docum 1/DreDrive/Docum		5/2024 21:25	12/5/2024 3:57 12/5/2024 3:58		EDAD SO28 052C C34F EXE ELEVATION SERVICE EXE	EA05C378 FDD452DA	141534 Windows IX 20182 Windows IX	1	12/4/2024 2:21 12/4/2024 2:10					\v0uumt(01db45c54423 \v0uumt(01db45c54423		AE443E4E AE443E4E	12/3/2024 20:52			VOLUMEIC WOLLIN	
	1\OneDrive\Docum 1\OneDrive\Docum		5/2024 21:25	12/5/2024 3:58		FLEVATION SERVICE.EXE FLESVACEONFIG.EXE	FDD452DA 2540D758	20182 Windows IC 27484 Windows IC	1	12/4/2024 2:10					\v0UUME[01db45c54423		AE443E4E	12/3/2024 20:52			(VOLUME)C (VOLUM	
C/Users/ozar	I)DeeDrive\Docum	w 12/	3/2024 21:25	12/5/2024 3:58	12/5/2024 22:53	FILESYNCCONFIG.EXE	C535779E	28764 Windows IC	- 1	12/4/2024 2:04					\v0LUME(01db45c54425	da1 ac443c4c)	AE443E4E	12/3/2024 20:52			(VOLUME)C (VOLUM	rejc
	i)DecDrive)Docum		5/2024 21:25	12/5/2024 3:57	12/5/2024 22:33		16207658	6746 Windows 10	1	12/4/2024 2:19					\v0uumej01db45c54423		34354354	12/3/2024 20:52			(vounwe)c (vounw	
	ADreDrive\Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:32	FINDSTREXE FIREFOR INSTALLER.EXE	41768665 FOCD3A1A	7500 Windows IC 26525 Windows IC	2	12/4/2024 2:19	12/4/2024 2:35				WOLLMEIDLdb45c54423		A5443646 A5443545	12/3/2024 20:52			(VOLUME): (VOLUM	
	1/DreDrive/Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33		EGOCDAA7	273768 Windows 20	9		12/4/2024 2:18	12/4/2024 2:18 12/4/2	024 2:15 www eee		(VOLUME[01db45c54423		AE443E4E	12/3/2024 20:52			(VOLUME)C (VOLUM	
	(OneDrive)Docum		5/2024 22:25	12/5/2024 3:58	12/5/2024 22:33		96782838	28882 Windows IC	1	12/4/2024 2:17					\vCuUMF(01db45c54423	da1 ac443c4c)	A8443848	12/3/2024 20:52			(vounte): (vount	
	(DeDrive)Docum		5/2024 21:25	12/5/2024 3:57	12/5/2024 22:53		27103050	34788 Windows IX 33728 Windows IX	2	12/4/2024 2:19 12/4/2024 2:03	12/4/2024 2:15				WOLLIME[01db45c54425 WOLLIME[01db45c54425		AE443848	12/3/2024 20:52			VOLUMEIC WOLLN	
	1)Debrive\Docum 1)Debrive\Docum		5/2024 21:25	12/5/2024 3:58 12/5/2024 3:57		FSQUIRT.EXE GETUSERPROFILEPATH.EXE	GEB1AAF1 6F19886	33728 Windows IC 39280 Windows IC	1	12/4/2024 2:03					WOLUME[01db45c54423		AE443E4E AE443E4E	12/3/2024 20:52			(VOLUME): (VOLUM	
C/Users/azar	NDreDrive\Docum	N 12/	3/2024 21:25	12/5/2024 3:58	12/5/2024 22:33	IDENTITY_HELPER.EXE	83C5A303	75458 Windows IC	2	12/4/2024 2:10	12/4/2024 2:06				\v0UUME[01db45c54423	da1 ae443e4e)	AE443848	12/3/2024 20:52			VOLUME (VOLUM	rejc
	ADreDrive\Docum		5/2024 22:25	12/5/2024 3:58	12/5/2024 22:33		11820946	10522 Windows 10	2		12/4/2024 2:35				\v0UUME(01db45c54423		A5443545	12/3/2024 20:52			(VOLUME): (VOLUM	
	1)DeDrive\Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33		75632858	34510 Windows IC 24820 Windows IC	2		12/4/2024 2:17	12/4/2024 2:21 12/4/2	124 2.23 899		\v0cuME[01db45c54428 \v0cuME[01db45c54428		A5443545	12/3/2024 20:52 12/3/2024 20:52			(AORINE): (AORIN	
	1/DreDrive/Docum		5/2024 21:25	12/5/2024 3:58	12/5/2024 22:33	UNOWEBCONFIG.EXE	30C12ACE	22566 Windows 10	1	12/4/2024 2:20	**************	11/4/10/07/2111/04/0			\v0LUME(01db45c54423)	ds1 ac443c4c)	AE443E4E	12/3/2024 20:52			(VOLUME)C (VOLUM	esic
	1/DreDrive),Docum		5/2024 21:25	12/5/2024 3:57		UNDWERDONFIG.EXE	8663/069	22088 Windows IC	1	12/4/2024 2:20					\v0uum#j01db45c54423		AE443E4E	12/3/2024 20:52			(VOLUME): (VOLUM	
	A.D			A 10 No No No No. of August												1.1.1.1.1.1		and the basis a set and			to contract a state to contract	49.54

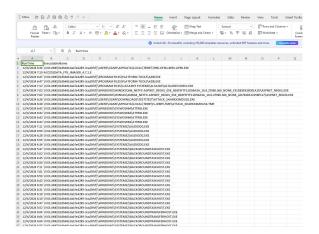
Prefetch extracted csv from PECmd of Windows 10

Menu 日日 P B R もう ママー			Insert Page	Layout Form	ulas Data	Review			rt Toolbox	Q					Share ~	Ð	
🐴 📸 🔏 🔽 Calibri 🔍 11 🔍	A* A -	= = = = =	2 Ew	rap Text	General	~	Rows an	id Columns 👻	E	⊮~	🐨 Fill 🗸	₿↓ Sort ~	🚼 Free	ze Panes 👻	8		
Format Pastev िry B Z ⊔ v A ⊞ v 🕰 v 🖌 Painter	<u>↓</u> • <i>Q</i> • ∃	Ξ Ξ Ξ Ξ 1 <u>9</u>   Ori	ientation ~ 🖽 M	erge and Center 🗸	8 - %	000 €-0 -00 7 -00 9-0	U Workshe	eet ~	Conditional Formatting ~	□.~	∑ AutoSum ~	P AutoFilter	Q Find	i and Replace 、	Smart Toolbox	Settin	ngs ~
		Unlock 80+ Pr	ro benefits, includir	ng 100,000 templat	es resources, unl	imited PDF feat	ures and more.	Upgrade a	1011								
A1 Q fx Note																	
A 8 C D E F G	н	K L	M N	0	P	Q R	S T	U	v w	×	Y Z	AA AB	AC	40 A	LE AF	49	AH
ote SourceFilena SourceOreated SourceModified SourceAccessed ExecutableN Hash St	ze versior RunCa	ount LastRun PreviousRun0 F	PreviousRun1 Previousl	lun2 Previousitun3	Previouskun4 Previo	ushur Previoushur V	olumetiva volumetise	er volume0created v	olume1Na Volume15	er volume10	e Directories FilesLoaded	d ParsingError					
C:\Users\ats 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 7090-0F60-8007EAED	140232	112/4/2024 6:34				1	VOLUMERC BCA20FCF	12/4/2024 7:25			VOLUMEX VOLUMER	C FALSE					
C:\Users\ozs 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 ACCESSIDAT FA385D2E	212200	112/4/2024 7:19				1	VOLUME C 3CA20FCF	12/4/2024 7:25			VOLUME C VOLUME	C FALSE					
C:\Usen\ozs 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 ADB.EXE ADB0F88D	32596	212/4/2024 6:47 12/4/2024 6:47				1	VOLUME C 3CA20FCF	12/4/2024 7:25			VOLUME C VOLUME	C FALSE					
C:\Users\oze 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 ALTA2DPOD 31108909	\$14242	112/4/2024 7:12				1	VOLUME C SCA20FCF	12/4/2024 7:25			VOLUME C VOLUME	C FALSE					
C:\Usen\oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:57 ASPNET_R0 8545410E	29150	112/4/2024 7:02				1	VOLUME C SCA20FCF	12/4/2024 7:25			VOLUME C VOLUME	C FALSE					
C/Users/oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 ASPNET_RD E7D16D2D	32096	112/4/2024 7:02				1	VOLUME C SCA20FCF	12/4/2024 7:25			(VOLUME C VOLUME)						
C:\Users\oza 12/5/2024 21:25 12/5/2024 5:58 12/5/2024 22:57 ATTACK_SH 7125228	45602	112/4/2024 6:28					VOLUME CSCA20PCP				(volume)c/volume)						
C:\User5\oza 12/5/2024 21:25 12/5/2024 3:38 12/5/2024 22:37 ATTACK_SH 47F62EE0	54054	112/4/2024 6:28					VOLUME (C SCA20FCF				\volume(c\volume)						
C1User5\ota 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 ATTRIB.EXE 58407CAF	9324	412/4/2024 6:42 12/4/2024 6:421				1	VOLUME[CBCA20FCF	12/4/2024 7:25			\VOLUME(C\VOLUME)	C FALSE					
C1User51ota 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 AUDIODG E A822E946	30820	512/4/2024 7:11 12/4/2024 6:501	2/4/2024 6:28 12/4/202	4 5:55 12/4/2024 4:34			VOLUME[C 3CA20FCF				(VOLUME)C (VOLUME)						
C1Users/oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 BACKGROUP SEBEDDA	42910	112/4/2024 5:47					VOLUME[C BCA20FCF				/vornweig/vornweig						
C:\Users\oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 &ACKGROUP 51333CCD	38392	212/4/2024 5:52 12/4/2024 4:45					VOLUME (C 3CA20FCF	12/4/2024 7:25			/vornwelc/vornwels						
C:\Users\oze 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 BACKGROUP 64C18432	47006	112/4/2024 5:50					VOLUME (C 3CA20FCF	12/4/2024 7:25			/vornwelc/vornweli						
C:\Users\oze 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:57 8ACKGROUF 6D58042C	62212	2112/4/2024 7:11 12/4/2024 7:011	2/4/2024 6:50 12/4/202	4 6:42 12/4/2024 6:39	12/4/2024 6:31 ####		VOLUME C 3CA20FCF	12/4/2024 7:25			/vornwelc/vornwell						
C:\Users\oze 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 BACKGROUP ASRD92A4	43300	112/4/2024 5:47					VOLUME (CSCA20FCF				/volume(c/volume)						
C/USMIS/0EW 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 BACKGROUF 0085982A	72094	112/4/2024 5:52					VOLUME (CSCA20PCP				/vornweic/vornwei						
C:\Users\ota 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 BACKGROUF E7870877	40652	512/4/2024 6:04 12/4/2024 6:041		4 5:55 12/4/2024 5:55			VOLUME C SCA20PCP				/volume(c/volume)						
C:\Users\dza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 80EUISRV.E78C33651	23770	312/4/2024 7:19 12/4/2024 5:581	2/4/2024 4:38				VOLUME[C3CA20FCF				(volume)c/volume)						
C:\User5\ota 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 8TTWEAKEF E918ADE7	132866	112/4/2024 7:12					VOLUME[C3CA20FCF				/vornweig/vornweig						
C:\Users\ota 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 8TTWEAKEF 03808029	19258	112/4/2024 7:12					VOLUME[C 3CA20FCF				/AOLINESC/AOLINES						
C:\Lisers\oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 8TWE8_INS 19F5517	50982	212/4/2024 6:29 12/4/2024 6:29					VOLUME[C3CA20FCF				/vornweic/vornweij						
C:\Liters\oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 8TWEB_INS 81465686	72378	112/4/20246:29					VOLUME (C 3CA20FCF				(vornwelc/vornwel)						
C:\Usen\oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 8TWEB_ING EE6167F8	60300	112/4/2024 6:29					VOLUME (CSCA20FCF				/vornwelc/vornwels						
C:\Users\oze 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 5TWE5_INS F07A9027							VOLUME (CSCA20PCP	12/4/2024 7:25			(volume)c/volume)						
C/Users/ora 12/5/2024 21:25 12/5/2024 3:35 12/5/2024 22:37 CAM_HELPE0330P1F C/Users/ora 12/5/2024 21:25 12/5/2024 3:35 12/5/2024 22:37 CERTMGR.E 5C855154	97542	212/4/2024 6:35 12/4/2024 6:35 412/4/2024 6:47 12/4/2024 6:35					VOLUME C SCAZOPCP	12/4/2024 7:25			/vocume(c/vocume)						
C105645/028 12/5/2024 21:25 12/5/2024 3 38 12/5/2024 22 37 CERTMGR E 50855154 C105675/028 12/5/2024 21:25 12/5/2024 3 38 12/5/2024 22 37 CLOUDEX/E A826E807	17284	412/4/2024 6:47 12/4/2024 6:471	2/4/2024 6.47 12/4/202	46:47			VOLUME C SCA20FCF				(VOLUME)C(VOLUME) (VOLUME)C(VOLUME)						
	27494	112/4/2024 5:29 712/4/2024 6:01 12/4/2024 6:011															
C1User5/dt8 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 COMPPK0S 4780F0C1 C1User5/dt8 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 CONSENT E 40419367	387276	1312/4/2024 7:11 12/4/2024 6:511					VOLUME[CBCA20FCF				\volume(c\volume) \volume(c\volume)						
Childenhora 12/5/2024 21:25 12/5/2024 3:36 12/5/2024 22:37 CROMINIAIRCEDATE	144292	112/4/2024 5:30	224720240.4412747202	+0.30 Later 200+0.33	12/4/2024 0.54 9999		VOLUME E BOAZOFCF				(VOLUME)C (VOLUME)						
C10585/058 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 CROOM/AISCHARE C10585/058 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 CSRS5.EXE F3C368C8	17974	112/4/2024 5:47					VOLUME (C3CA20FCF				(volume)c/volume)						
C'Users/ore 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 CTFMON D 79578130	42098	1212/4/2024 7:19 12/4/2024 7:111	2/4/2024 6 4442/4/202		1///2014/01/			12/4/2024 7:25			(VOLUME)C/VOLUME)						
C1(Usen)/dds 12/3/2024 21:25 12/3/2024 3:58 12/3/2024 22:37 C17MOR(5) /45/8130 C1(Usen)/dds 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DATAEXCH/ 8566795C	45655	1212/4/2024 4:51		and any stand 0:35			VOLUME C SCA20FCF				(VOLUME)C (VOLUME)						
C/Unam/ora 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DPFAULT-RECARAMENTE	20652	112/4/2024 6:52					VOLUME C SCA20FCF				(volumele (volumele						
C/Users/gea 12/5/2024 21:25 12/5/2024 3 55 12/5/2024 22 37 DEFEAG EXISOREBOTE	15022	112/4/2024 6:12					VOLUME[CSCA20FCF				(VOLUME[C\VOLUME]						
C/USerS/028 12/5/2024 21:25 12/5/2024 5:35 12/5/2024 22:37 DEVCON EX 6FC87C48	15604	112/4/2024 6:46					VOLUME C SCA20FCF				\volumelc\volumeli						
C'UKERDATE 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DEFCORE VIEW	43916	112/4/2024 6:07					VOLUMER SCA20FCF	12/4/2024 7:25			(VOLUME)C (VOLUME)						
C1Uper5/ota 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DISMHOST. 9ED88089	24682	112/4/2024 6:07					VOLUMER BCA20FCF				VOLUMER VOLUMER						
C1Users/ota 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DISMHOST. 88586608	330438	112/4/2024 5:04					VOLUMER BCA20FCF				VOLUMEX VOLUMER		201072 WINDO	WSISTEM 320NT	TOLL DUL WOULD	FIDIdb461da1	1144289-31
Elorande, / normello, / normellorang, / normellorang, / normello.			VOLUME[014 VOLUM	Elosa IVOLUME(01db	VOLUME 014 VOI				VOLUME VOLUME	VOLUME							
C:\Users\oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DLUHDST EX 136EBFED	52774	412/4/2024 6:32 12/4/2024 6:281				1	VOLUME (C 3CA20FCF	12/4/2024 7:25			(VOLUME)C (VOLUME)						
C:\Users\oze 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DLUHDST.E) 18A50688	19692	512/4/2024 6:27 12/4/2024 5:491	2/4/2024 5:47 12/4/202	44:38 12/4/2024 4:34		1	VOLUME C SCA20FCF	12/4/2024 7:25			(VOLUME C VOLUME)	C FALSE					
C\Users\oza 12/5/2024 21 25 12/5/2024 3 55 12/5/2024 22 37 DLUHOST EX478E07DC	47004	212/4/2024 5:47 12/4/2024 4:54				1	VOLUME C SCA20FCF	12/4/2024 7:25			(VOLUME)C (VOLUME)	C FALSE					
C/USerS/018 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DLLHOST EX SECTOR C	54174	212/4/2024 7:19 12/4/2024 6:28				1	VOLUME C SCA20FCF	12/4/2024 7:25			(VOLUME)C(VOLUME)	C FALSE					
C/Users/oza 12/5/2024 21:25 12/5/2024 3:38 12/5/2024 22:37 DLHOST EX 6P625E57	19824	512/4/2024 6:28 12/4/2024 6:001		44:45 12/4/20244:50			VOLUME C SCA20PCP				(volume)c(volume)						
C/USerS/028 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DLHOST.E> 7.428+214	30698	312/4/2024 6:17 12/4/2024 5:531					VOLUME[C SCA20FCF				(VOLUME)C (VOLUME)						
C1User5/008 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DLLHOST EP7050E0CA	17474	2012/4/2024 7:18 12/4/2024 7:181		4 6:56 12/4/2024 6:46	12/4/2024 6:43 #####						(volume)c/volume)						
C1Users/oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DUHOST E/8106688E	45820	312/4/2024 5:18 12/4/2024 4:381	2/4/2024 4:34				VOLUME (C BCA20FCF	12/4/2024 7:25			VOLUME (C VOLUME)						
C:\Users\oza 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DUHOST ID 95797F8F	22094	112/4/2024 5:29					VOLUME[C 3CA20FCF	12/4/2024 7:25			/vornwelc/vornwell						
C:\Users\oze 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DLUHOST EVA18F1D38	22940	112/4/2024 6:51					VOLUME (C 3CA20FCF	12/4/2024 7:25			(vornwelc/vornwel)						
C:\Usen\ccs 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:37 DLUHD5T.EX C7F45418	35062	312/4/2024 5:18 12/4/2024 4:361					VOLUME C SCA2OFCF	12/4/2024 7:25			(VOLUME)C (VOLUME)						
Children/one 12/5/2024 21:25 12/5/2024 3:58 12/5/2024 22:32 DU HOST PL0200FFC3	19764	312/4/2024 6/36 12/4/2024 6/341					CUMPIC SCAZOFCE				WOLLMRIC WOLLMRIN	C RALER					

Prefetch extracted csv from PECmd of Windows 11



Prefetch timeline extracted csv of Windows 10



Prefetch timeline extracted csv of Windows 11

### Analysis

File Metadata (SourceFilename, Created, Modified, Accessed)

- Windows 10: Includes files like ACCESSDATA\_FTK\_IMAGER\_4.7.1.E, ADB.EXE, and ALTA2DPCONFIG.EXE. Timestamps point to frequent access and modifications in December 2024.
- Windows 11: Logs similar files, including ACCESSDATA\_FTK\_IMAGER\_4.7.1.E and ADB.EXE, but also additional entries such as ASPNET\_REGIIS.EXE. Access times are slightly delayed compared to Windows 10.
- Observation: Windows 11 contains more executables, reflecting newer software activity and slight differences in usage patterns.

**Executable Names and Run Details** 

- Windows 10: Logs executables like ApplicationFrameHost.exe and NZXT-CAM-Setup.exe with run counts between 1 and 3, indicating repeated but limited usage.
- Windows 11: Adds files like ASPNET\_REGIIS.EXE and logs broader application coverage with similar run counts.
- Observation: Windows 11 demonstrates more diverse application usage.

#### Hash and Size

- Windows 10: File hashes, such as 6B6A2BBC for ACCESSDATA\_FTK\_IMAGER\_4.7.1.E, and sizes range from small utilities (~30 KB) to larger setups (~214 KB).
- Windows 11: Files like ACCESSDATA\_FTK\_IMAGER\_4.7.1.E have updated hashes (e.g., FA3B5D2E), likely from updates or reinstallation. Larger executables, like ASPNET\_REGIIS.EXE, appear.
- Observation: Differences in hashes and sizes suggest updates or variations in software installations.

Volume Information

- Windows 10: Volume identifier \VOLUME{01db45c54423eda1-ae443e4e} with serial AE443E4E was created on December 3, 2024, indicating recent initialization.
- Windows 11: Volume identifier \VOLUME{01db461da1fe4289-3ca20fcf} with serial 3CA20FCF was created on December 4, 2024.
- Observation: Separate volumes confirm distinct environments or machines.

#### Directories and Loaded Files

- Windows 10: Includes directories like \PROGRAM FILES\ and \WINDOWS\SYSTEM32\. Frequently loaded files include cmd.exe and system DLLs.
- Windows 11: Adds directories for newer tools and logs recent executables like MicrosoftEdgeUpdate.exe.
- Observation: Windows 11 reflects an updated software environment with modern application integrations.

#### Parsing Errors

• Both logs indicate successful data extraction with no parsing errors.

#### **Observations**

#### Windows 11 Features

- Broader application coverage, including newer tools and executables.
- Updated file hashes and sizes, indicating software updates or replacements.
- Consistent directory and volume logging with added modern software directories.

Windows 10 Features

- Core configurations focus on fewer executables and system utilities.
- Older file hashes and limited updates compared to Windows 11.

#### Analysis of Windows 10 and Windows 11 Timeline Logs

#### Structure

• Both logs contain RunTime and ExecutableName columns, tracking execution timestamps and file paths.

#### Windows 10 Timeline

Examples include:

- ACCESSDATA\_FTK\_IMAGER\_4.7.1.E executed at 2:15 AM on December 4, 2024.
- Files stored under \VOLUME{01db45c54423eda1-ae443e4e}, primarily in PROGRAM FILES.

• Logs show concentrated activity over a short period.

Windows 11 Timeline

Examples include:

- ACCESSDATA\_FTK\_IMAGER\_4.7.1.E executed at 7:19 AM on December 4, 2024.
- Files stored under \VOLUME{01db461da1fe4289-3ca20fcf} with paths like USERS\OZARI.
- Activity extends across the day, covering diverse program usage.

Key Comparisons

- Execution Range: Windows 11 logs show extended activity throughout the day, compared to Windows 10's shorter timeline.
- File Scope: Windows 10 logs focus on system directories like PROGRAM FILES, while Windows 11 captures both system-level and user-specific paths.

Windows 10 logs highlight focused, system-oriented activity over a short timeframe, likely indicative of testing or limited usage. In contrast, Windows 11 logs reflect a more dynamic and diverse system environment, with broader application use, updated files, and extended user interaction. These differences suggest that Windows 11 is more actively used and better equipped for modern software needs.

## Thumbnail Cache

0			libri	9 11	~ A+ A-	= =		10.	📰 Wrap Teo	4	General			Rows and Co	lumor	1000	₽, -	Fill +	AL Sort -	97 F	eze Panes +	0	ineri	
Ê								2						U		E			-	0.0		13	4	
Format Painter	Paste ~ [	G~ В	1 0.	≜ ⊞ • <mark>≗</mark> •	<u>A</u> · Q ·			Orientation	· 巴 Merge an	nd Center ~	<del>ସ</del> ~ ୨	6 99 56	0 -20	🖽 Worksheet 🤸		Conditiona Formatting		∑. AutoSum	<ul> <li>W AutoFilter</li> </ul>	Q Fin	d and Replace 👻	Smart Toolbox	Settings	14
A1	~	Q fs	Filename																					
A	В	с	D	E	F G	н	1	J	к	L	м	N	0	р	a	R	S	т	U	V	W	x	Y	
				lata Size (EData				Location																
09dbc2ea5	24	1264	114																er\iconcache_16					
1a4159ec7	1288	1264	1378																er\iconcache_16					
1c494794d4	2552	1264	2642																er\iconcache_16					
5413693b05	3816	1264	3906																er\iconcache_16					
724ce787e3	5080	1264	5170																er\iconcache_16					
:84fefba0fe	6344	1264	6434																er\iconcache_16					
50bdf0b0a	7608	1264	7698																er\iconcache_16					
e7becb22e!	8872	1264	8962																er\iconcache_16					
7a19be3f84	10136	1264	10226																er\iconcache_16					
80a9f016c2	11400	1264	11490																er\iconcache_16					
19ed392401	12664	1264	12754																er\iconcache_16					
acfbf30bb9	13928	1264	14018																er\iconcache_16					
f989800b02	15192	1264	15282																er\iconcache_16					
d0615f984e	16456	1264	16546																er\iconcache_16					
365d195e2f	17720	1264	17810																er\iconcache_16					
a54642f486	18984	1264	19074																er\iconcache_16					
61a34ea9fc	20248	1264	20338																er\iconcache_16					
c027858dbf	21512	1264	21602																er\iconcache_16					
a412f87c0a	22776	1264	22866																er\iconcache_16					
c85a773ab1	24040	1264	24130																er\iconcache_16					
48e6dd71cc	25304	1264	25394	1174 d3e3	a31f219aac07b	ofe0 48e6dd71	c Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer I	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	.db				
df2b595ae8	26568	1264	26658	1174 e03b	665f22 ccf4019	905: df2b595a	e8 Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer l	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	.db				
6e28c27660	27832	1264	27922																er\iconcache_16					
2f62b1e3ae	29096	1264	29186																er\iconcache_16					
d7c37b2b9:	30360	1264	30450																er\iconcache_16					
6eb88a5c6t	31624	1264	31714																er\iconcache_16					
f363234790	32888	1264	32978	1174 54670	5469b c64704b	587 f3632347	0 Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer l	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	.db				
dee5bd3b9	34152	1260	34238																er\iconcache_16					
8fa9bf40ee	35416	1264	35506																er\iconcache_16					
98c5d52d95	36680	1264	36770	1174 553d	b0076e35b8d3	8c1298c5d52d	95 Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer I	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	.db				
e63faf9930!	37944	1260	38030	1174 af9b3	8263e b837f40	Me2 0e63faf9	3 Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer I	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnal	I Cache\Explor	er\iconcache_16	.db				
8a105477e0	39208	1264	39298	1174 67bb	6e223(3e5572	3952 8a105477	et Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer l	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	.db				
5db5e7119	40472	1264	40562	1174 fa4b6	8afd2 a7df47f	807 5db5e711	9 Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer I	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	db				
b7b9e967bi	41736	1264	41826	1174 aaca9	2fbda b752e7	ba4: b7b9e967	b Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer I	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	.db				
aef9cdb60b	43000	1264	43090																er\iconcache_16					
e0c2e84283	44264	1264	44354	1174 1bbb	8eald 4c17ffc	3863 e0c2e842	83 Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	nts\Sem3\C	omputer I	Forensics	RithikOza_Fa	124_8013	58137\win10\	Thumbnai	I Cache\Explor	er\iconcache_16	db				
38fec8ad52	45528	1264	45618	1174 c9cdł	70eec4409695	5de438fec8ad	52 Window:	1 C:\Users\	ozari\OneDriv	ve\Documer	hts\Sem3\C	omputer I	Forensics	RithikOza Fa	124 8013	59127\wint0\	Thumbnai	Carba\Evolor	er\iconcache 16	db				

Win10

		100	<ul><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li></ul>						- 5	Home	Insert	Page Lay	JUL FOR	mulas	Data	Review	View	Tools	Smai	t Toolbox	Q					Share ~	(E) ~	
Ê	r X				11 ×						No.	📰 Wrap		Gene		~		ws and Colu	umns ~	图	₽∦~	😨 Fill 🗸	A↓ Sort ~	🔠 Free	ze Panes ~	G	3	
Format Painter	Paste -	6- B	I ⊻• /	• ⊞•	<u>a</u> .,	<u>A</u> - 6	2* =	ΞΞ	Ξ.	≡ 121	Orientation	- 💾 Merge	and Center	8.	%	000 <del>(+0</del> -00 • -00 <del>-0</del>	tt wa	orksheet 🗸		Conditional Formatting ~	□-	∑ AutoSum ~	AutoFilter •	Q Fin	i and Replace 🗸	Smart Toolbox	Setting	15-
											*	AST CALLIE	uy 2 years of	WPS Pro, get	15 mo	inths FREE!	Get No	w										
A1	~	Q. fx	Filename																									
A	в	c	D	F	F		G	н		1	f a	к	1	M		N	0	р	Q	B	5	т	u	v	w	x	Y	
lename Ca	ache Entry C	ache Entry D	ata Offset Da	ta Size (b	Data Chi				intry Sy	/stem	Location																	
9dbc2ea	24	1264	114	1174	d3e3a31	f21 0c33	39d3335	a09dbc	2eat W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sem	Com	puter Foren	ics\Rithi	kOza Fall2	24 80136	8137\win11\1	humbnai	I Cache\Explore	viconcache 16	.db				
5e40db981	1288	1264	1378																			I Cache\Explore						
54642f486	2552	1264	2642																			I Cache\Explore						
Se6dd6d9	3816	1264	3906	1174	d3e3a31	f21 1ae	e 28aa9	48e6dd	6d9 W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	4 80136	3137\win11\1	humbnai	I Cache\Explore	r\iconcache 16	.db				
9f4a1fb7b	5080	1264	5170																			I Cache\Explore						
aadd7357(	6344	1264	6434	1174	846d271	8dea3b	c307675	eaadd7	357(W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	db				
914343445	7608	1264	7698																			I Cache\Explore						
3d25ea571	8872	1264	8962	1174	26c3872	306 a6a	a55e3ei	43d25e	a571W	findows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sema	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\1	humbnai	I Cache\Explore	r\iconcache 16	.db				
45a779144	10136	1264	10226	1174	0b6abc3	49f 228	36822b2	845a77	9144 W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sema	NCom	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	db.				
od5183556	11400	1264	11490																			I Cache\Explore						
badedf7a7	12664	1264	12754	1174	f1b0e1f	0d0 8f1	dedac85	7baded	f7a7W	indows	1 C:\Users\	ozari\OneD	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\1	humbnai	I Cache\Explore	r\iconcache 16	.db				
ee1c6711b4	13928	1264	14018	1174	134c0337	70b 292	589d8f1	ee1c67	1164 W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sema	\Com	puter Foren:	ics\Rithi	kOza Fall2	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	db.				
55d6c2d8ea	15192	1264	15282	1174	b982833	8aC 959	d40867	55d6c2	d8eaW	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	db				
ab498e6fec	16456	1260	16542	1174	98f4d7e	f8d 7ed	157e67	0ab498	e6feW	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	.db				
591435da77	17720	1264	17810	1174	0690ea7	826 bed	5c1519	591435	da77W	findows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sema	Com	puter Foren	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	.db				
43d25f636b	18984	1264	19074	1174	26c3872	306 9b2	4230041	143d25f6	536b W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sema	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	.db				
845a77a785	20248	1264	20338	1174	0b6abc3	49f e4d	478e11	1845a77	785 W	Indows	1 C:\Users\	ozari\OneD	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	db.				
f1c6e13cb4	21512	1264	21602																			I Cache\Explore						
55d6c2ece5	22776	1264	22866	1174	b982833	BaC aa6	ee92a2	55d6c2	ece5 W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sema	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\7	humbnai	I Cache\Explore	r\iconcache 16	db.				
6ff89ebdaa	24040	1264	24130	1174	aecf28e	Sfd SfSc	17b7536	6ff89eb	idaa W	Indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\T	humbnai	I Cache\Explore	r\iconcache 16	db				
ee1c6740f7	25304	1264	25394	1174	f34c0337	70b da2	1e6291	eelc67	40f7 W	indows	1 C:\Users\	ozari\Onet	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\1	humbnai	I Cache\Explore	r\iconcache 16	.db				
ab49cb032c	26568	1260	26654																			I Cache\Explore						
ccd5185029	29096	1264	29186	1174	ofb56d4	d9£ c9e	979a320	ccd5185	5029 W	indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sem3	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\T	humbnai	I Cache\Explore	r\iconcache 16	db				
d445ed852r	30360	1264	30450																			I Cache\Explore						
e5abca93df	31624	1264	31714																			I Cache\Explore						
1c20226a7c	32888	1264	32978																			I Cache\Explore						
33205a8019	34152	1264	34242	1174	10245a4	195 530	53c83d4	33205a	3019 W	Indows	1 C:\Users\	ozari\OneE	rive\Docun	nents\Sema	Com	puter Foren:	ics\Rithi	kOza Falla	24 80136	3137\win11\1	humbnai	I Cache\Explore	r\iconcache 16	.db				
b961857d8;	35416	1264	35506																			I Cache\Explore						
d39e1d04b;	36680	1264	36770																			I Cache\Explore						
f745234f58(	58168	1264	58258																			I Cache\Explore						
171409bbf8	59432	1264	59522																			I Cache\Explore						
d325f9b78c	60696	1264	60786																			I Cache\Explore						
6824cd62d3	61960	1264	62050																			I Cache\Explore						
55f1080684	63224	1264	63314																			I Cache\Explore						
	64488	1264	64578	1174																								

Win11

# Analysis of Thumbnail Cache CSV Logs

The thumbnail cache logs provide information on cached image files, including details about file attributes, offsets, checksums, and system metadata. Below is a breakdown of the findings:

## 1. Structure of the Logs

#### MetaData

- Filename: The name of the cached image file (e.g., .bmp format).
- Cache Entry Offset (bytes): The starting point of the cache entry in the file.
- Cache Entry Size (bytes): The total size of the cached entry.
- Data Offset and Size (bytes): Indicates where the image data starts and its size.
- Checksums: Includes Data Checksum and Header Checksum for verifying integrity.
- Cache Entry Hash: A unique identifier assigned to each cache entry.
- System: Specifies whether the log is from Windows 10 or Windows 11.
- Location: The directory path where the cached image is stored.

## 2. Key Comparisons

#### Filename and Hash

#### Windows 10:

- Examples: a09dbc2ea5d5218d.bmp, a1a4159ec7d7f66f.bmp.
- Features unique hashes, such as a09dbc2ea5d5218d.
- Files are often found in user directories like C:\Users\ozari\OneDrive\Documents.

#### Windows 11:

- Examples: a09dbc2ea5d5218d.bmp, 35e40db9817c985d.bmp.
- Some filenames match Windows 10 (e.g., a09dbc2ea5d5218d.bmp), while others are unique, indicating the presence of additional files.
- Cached files are stored in similar directories, suggesting consistency in cache management.

Observation: Although some files and hashes are consistent across both systems, Windows 11 introduces additional cached files with unique identifiers, reflecting newer content or more extensive usage.

#### Offsets and Sizes

Windows 10:

- Cache entries typically begin at an offset of 24 bytes and have a size of 1264 bytes.
- Data offsets follow a sequential pattern, increasing by approximately 1264 bytes with each new entry.

Windows 11:

- Maintains the same structure for cache entry offsets and sizes.
- Sequential offsets confirm that the caching approach is consistent with Windows 10.

Observation: Both systems use identical caching structures, but Windows 11 includes additional entries, suggesting broader activity.

Checksums

Windows 10:

Examples:

- Data Checksum: d3e3a31f2101866f.
- Header Checksum: 0c339d3335e58056.

```
Windows 11:
```

Examples:

- Some Data Checksum values match Windows 10, indicating shared content (e.g., d3e3a31f2101866f).
- Others, such as 9e8f164f85967bc5, are unique, reflecting new or updated entries.

Observation: Shared checksums suggest overlapping cached content, while unique checksums in Windows 11 point to newer or updated images.

Location

- Both systems reference similar directories, such as C:\Users\ozari\OneDrive\Documents.
- Cached thumbnails derive from identical user locations, reflecting consistent system behavior and user habits.

## **Overall Observations**

Commonalities:

- Both Windows 10 and Windows 11 utilize the same caching structure, with identical size allocations and offsets.
- Some thumbnails, filenames, and hashes are shared, indicating continuity in cached content.

Differences:

- Windows 11 contains additional thumbnails with unique hashes and checksums, reflecting newer software, expanded user interactions, or increased activity.
- These new entries highlight a more dynamic and updated cache in Windows 11 compared to Windows 10.

Windows 11 retains the caching framework established in Windows 10 while introducing additional cached entries. These updates likely stem from broader system use, newer software integration, or enhanced compatibility with modern applications, demonstrating an evolution in caching behavior.

# Conclusion

The transition from Windows 10 to Windows 11 brings significant changes to how digital artifacts are generated, stored, and accessed, profoundly impacting forensic practices. Windows 11 prioritizes user personalization, compatibility with modern software, and improved security measures, resulting in richer datasets and enhanced artifact tracking. Key observations include:

Windows 11 enhances digital artifact management, offering significant advancements in forensic capabilities. Updates include streamlined registry configurations, detailed event logging, improved prefetch file tracking, and a more dynamic thumbnail cache with additional entries. The system also features enriched metadata and strengthened security measures like TPM 2.0 and UEFI boot standards. With its focus on user personalization, Windows 11 provides new opportunities for forensic investigations, though it demands specialized tools and methodologies to handle the increased complexity.

#### **Implications for Forensic Practices**

The advancements in Windows 11 call for updates in forensic methodologies:

**Tool Updates:** Utilize forensic tools capable of parsing artifacts specific to Windows 11, such as revised registry keys and enhanced security logs.

**Training and Education:** Develop expertise in navigating new file structures, metadata formats, and system behaviors introduced by Windows 11.

**Collaboration with Developers:** Work with software providers to ensure tools are compatible with the latest operating system features.

Windows 11 represents a substantial leap forward in terms of security, usability, and technological advancements. While these improvements enhance the end-user experience, they also introduce challenges for forensic investigators. By adapting their approaches and leveraging updated tools, forensic professionals can continue to conduct thorough and effective analyses, ensuring their ability to uphold justice in an increasingly digital environment.