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:

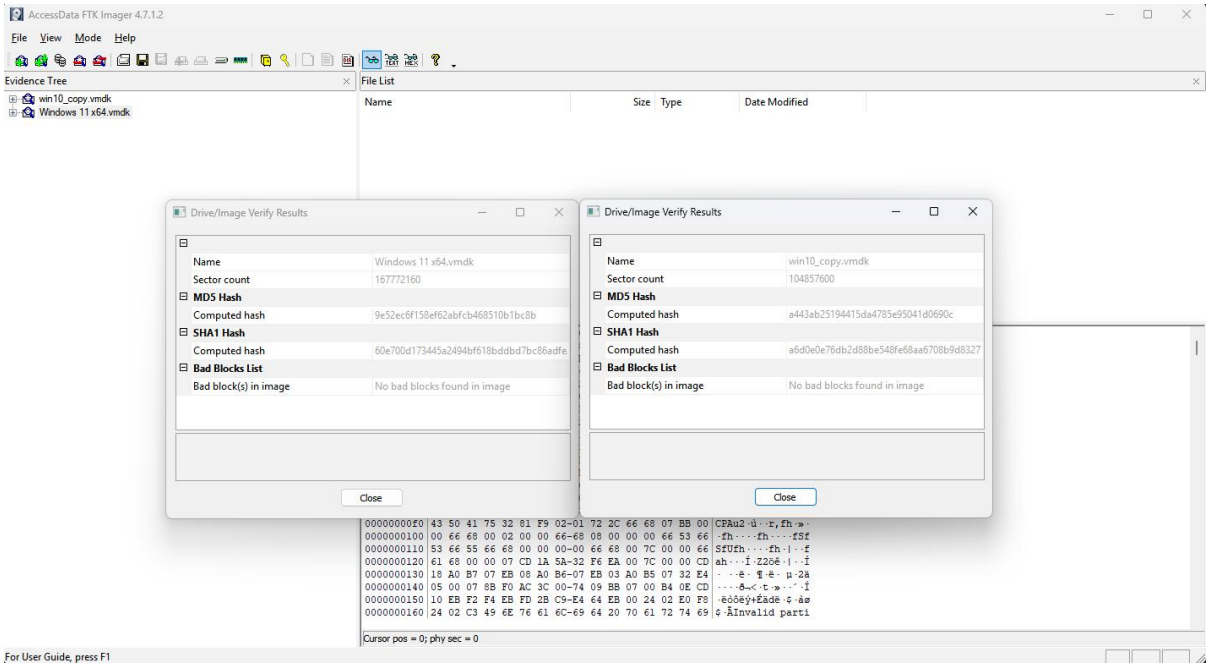
The transition from Windows 10 to Windows 11 brings significant changes to system architecture, artifact handling, and security features, with far-reaching implications for digital forensic investigations. This study explores the effects of these changes on the discovery, extraction, and analysis of 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.

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
    - 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:
    - Dell Precision 5550 laptop
    - Autopsy 4.21.0: To extract and analyze artifacts.
    - 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.



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.

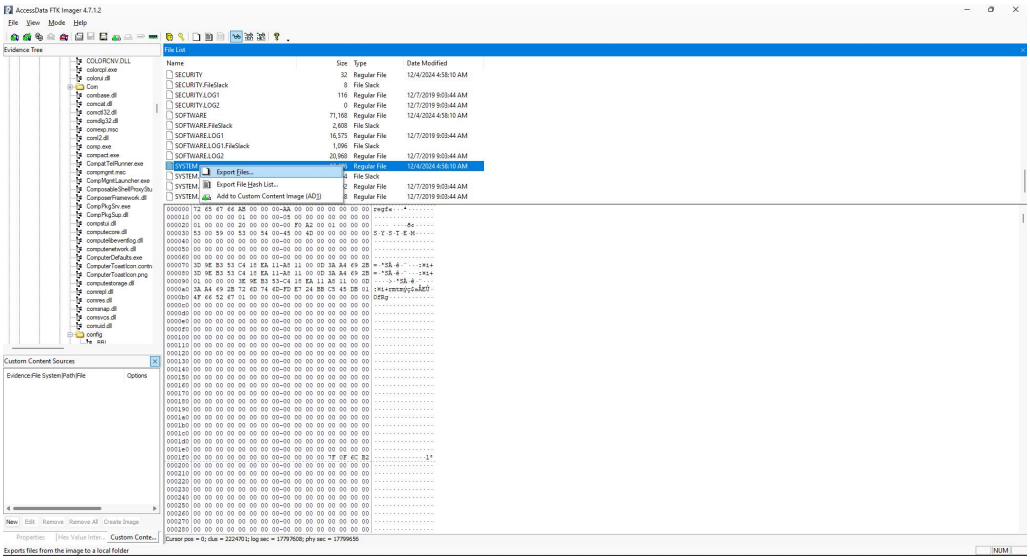
Both types of log files will be examined and compared to the same type of log file of the other operating system. The files are stored in "win10/Event logs" and "win11/Event logs" for windows 10 and 11 respectively.

2. Registry Entries

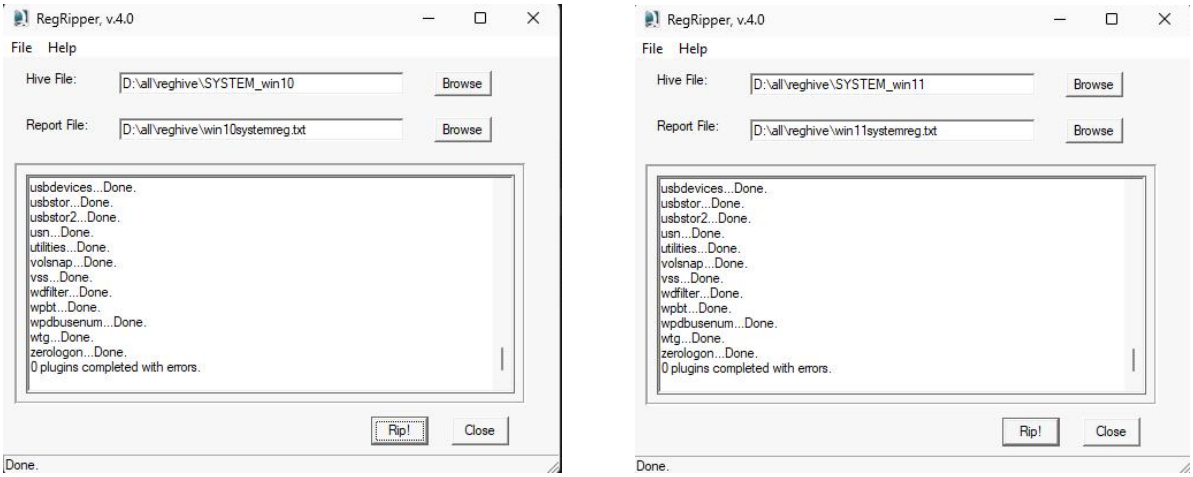
Description: Registry entries record software installations and file interactions.

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)



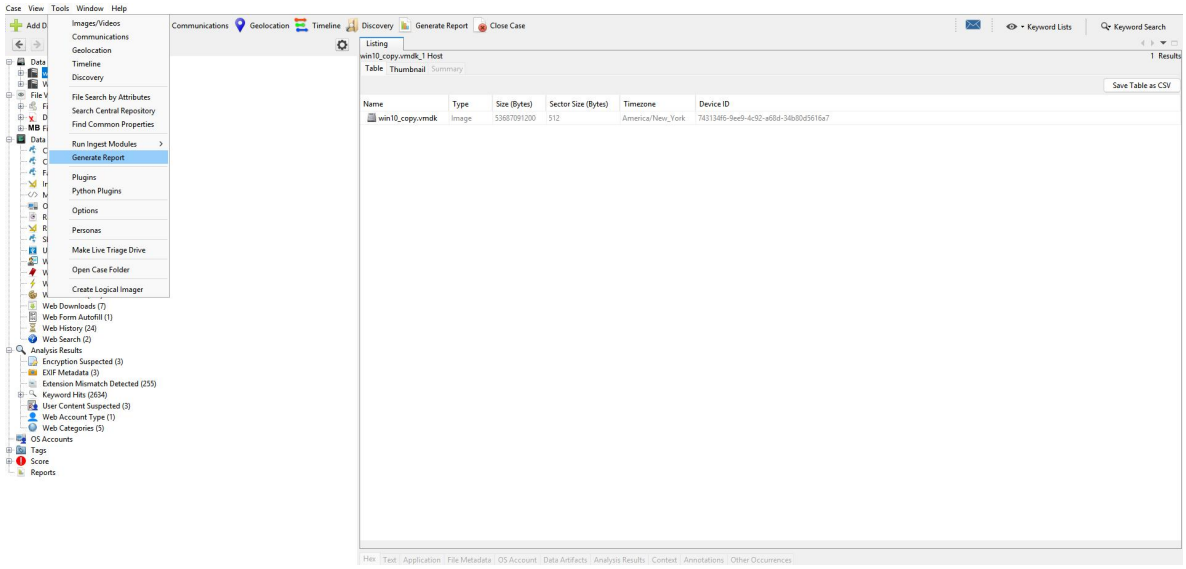
Regripper parsing all the registry files

3. File Metadata

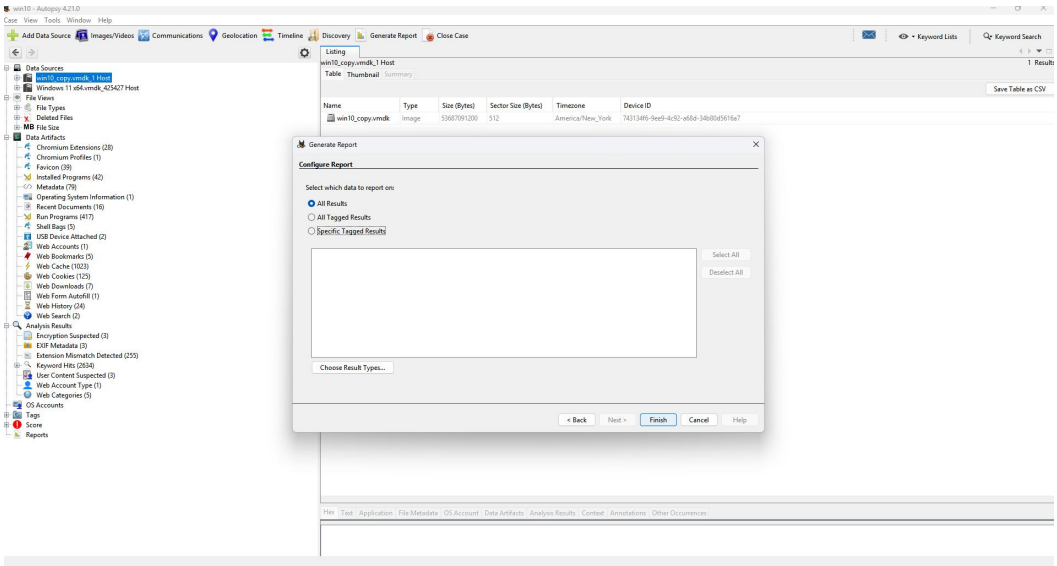
Description: Metadata includes timestamps for file creation, modification, and access.

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).



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

4. Prefetch Files

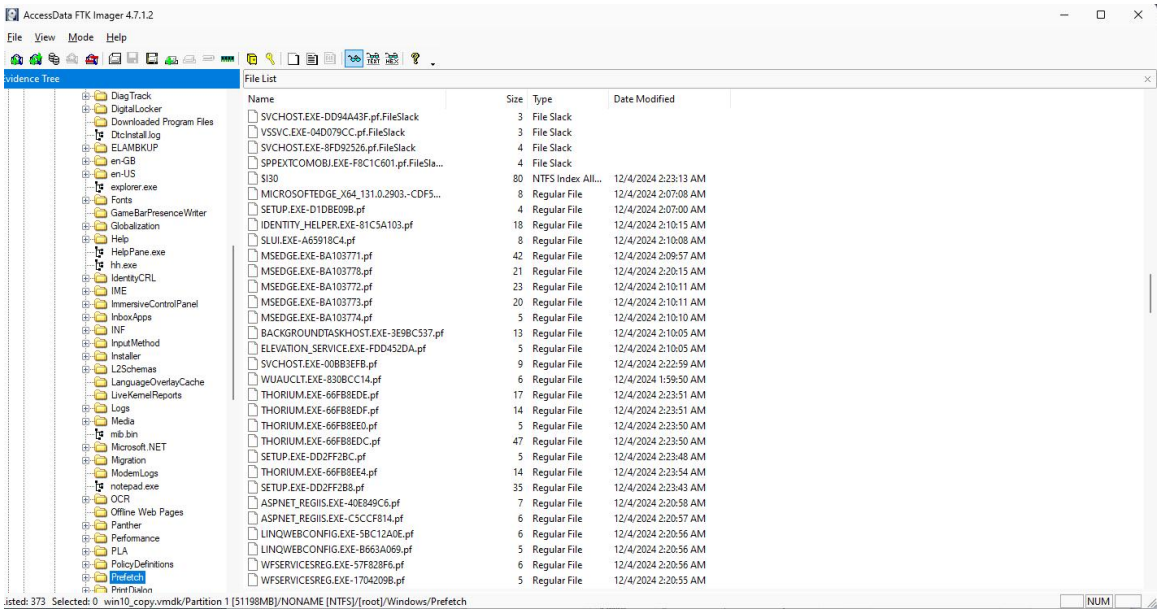
Description: Prefetch files reveal program execution history, including interactions with the test folder's installers.

Method of Collection:

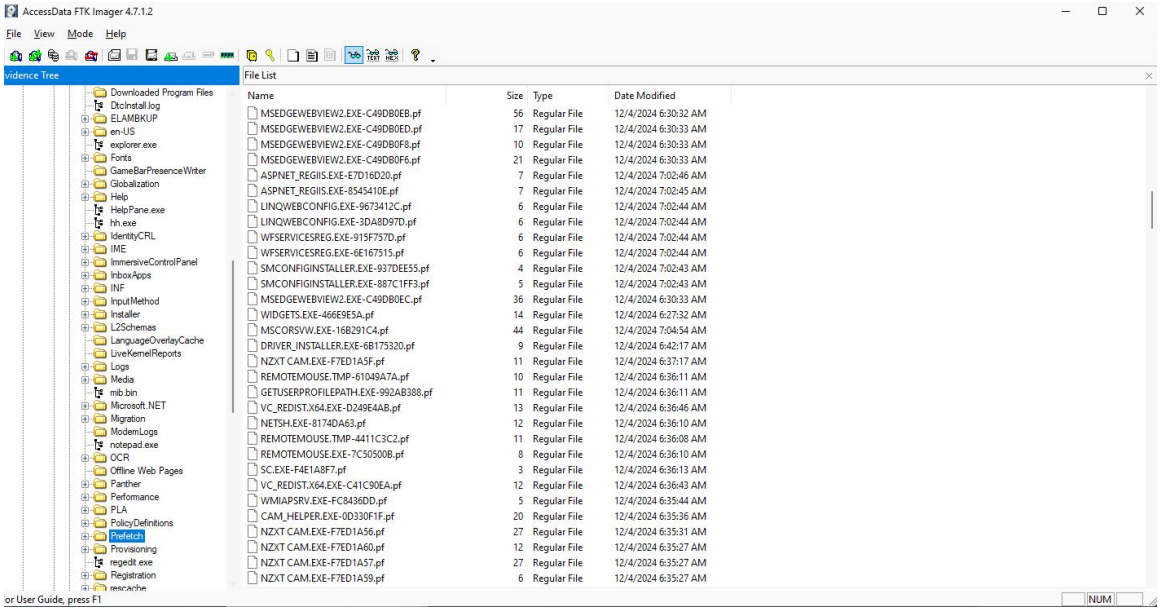
Collect prefetch files, the location in my case is :

win10_copy.vmdk/Partition 1 [51198MB]/NONAME [NTFS]/[root]/Windows/Prefetch

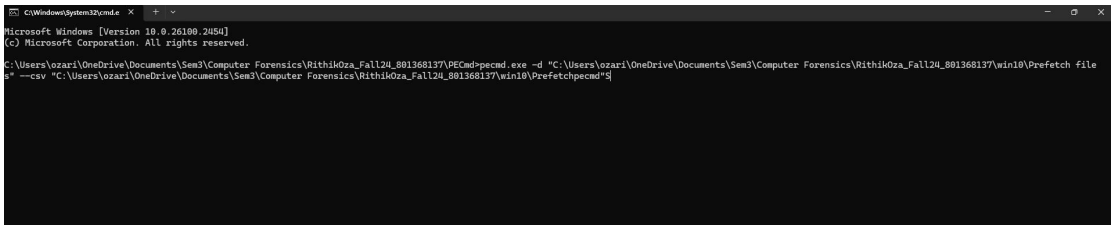
After all the prefetch files have been exported to destination folder using PECmd(win10/Prefetchpecmd; win11/Prefetchpecmd), compare both the csv files.



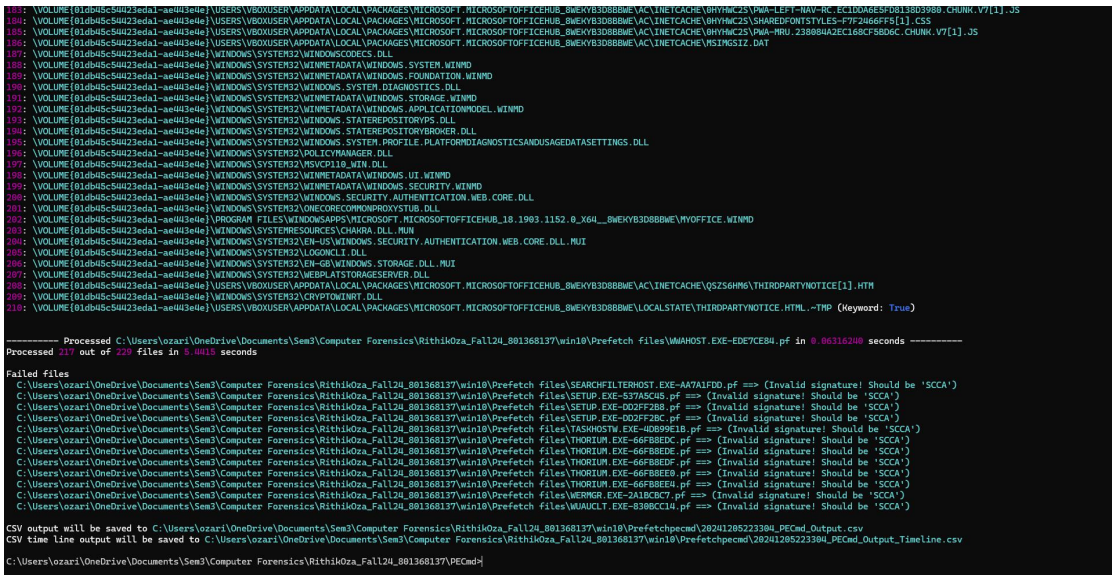
Prefetch files for Window 10



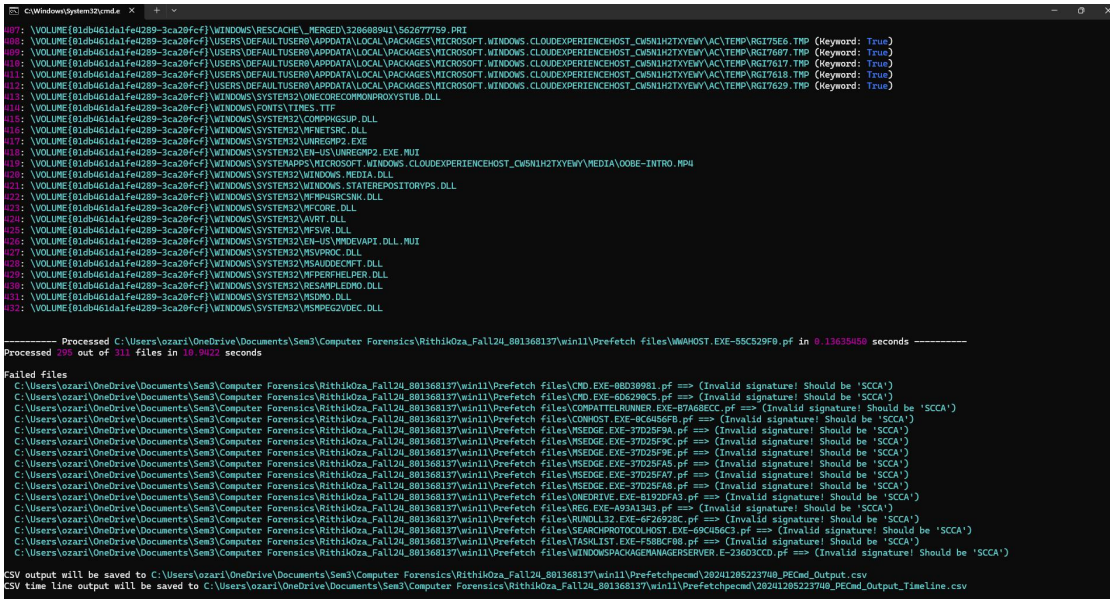
Prefetch for Window 11



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



Output for Windows 10



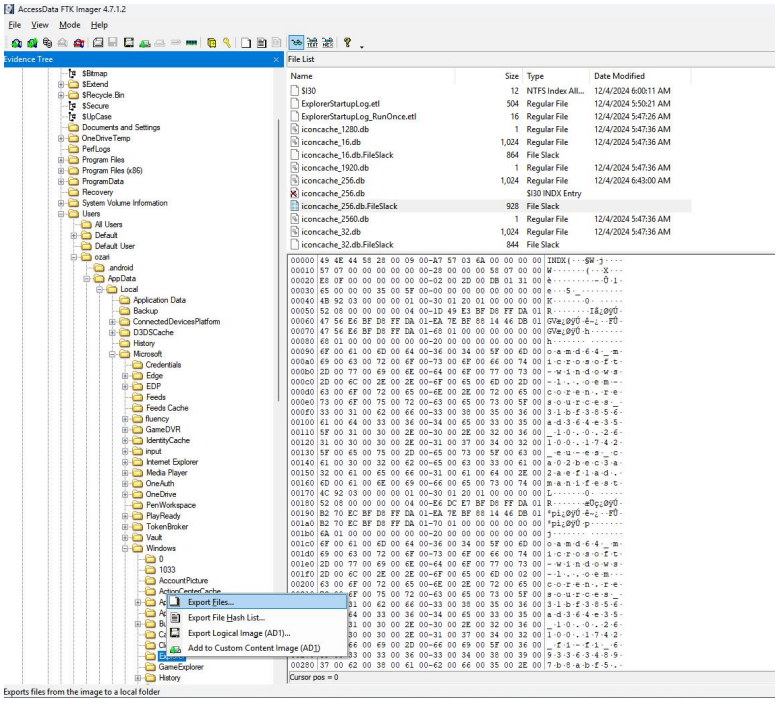
Output for windows 11

5. Thumbnail Cache

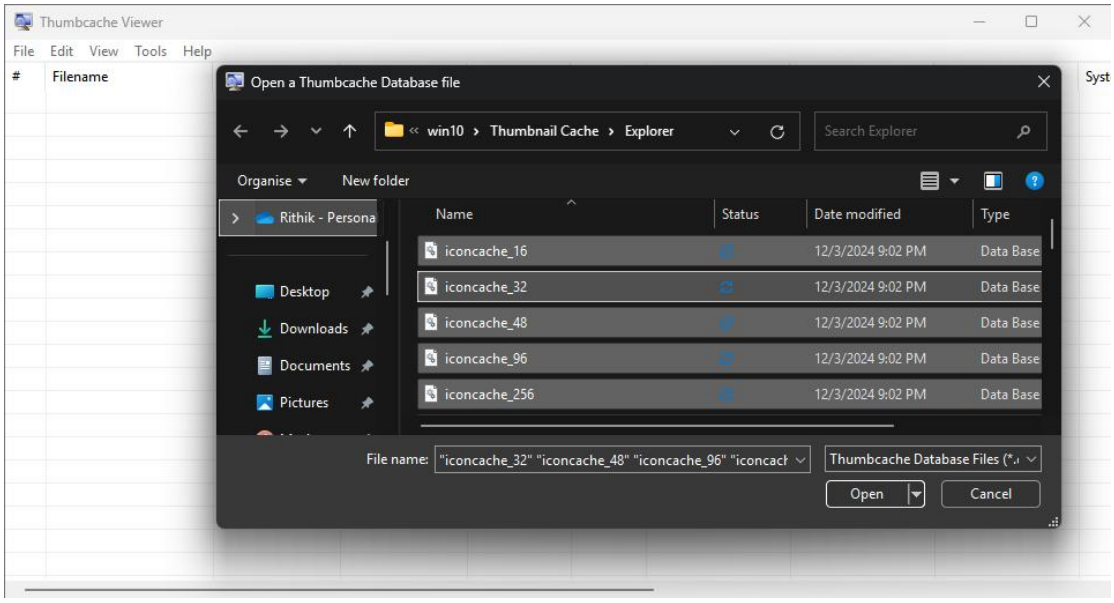
Description: Windows generates thumbnail cache files for images in the test folder.

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\Explorer” 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)



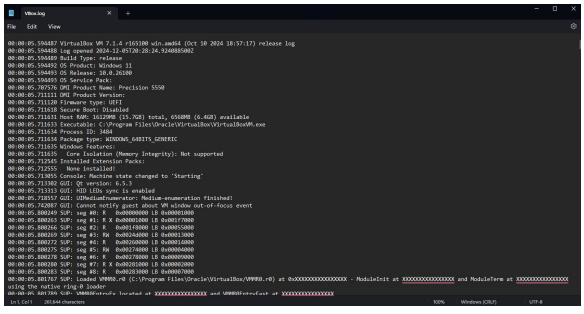
Loading all thumbcache into Thumbcache Viewer to parse and get output into csv file.

Findings and Forensics Analysis:

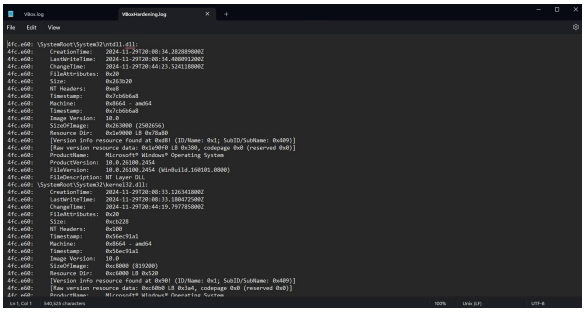
Observations from the “test” Folder Experiment

Event Logs

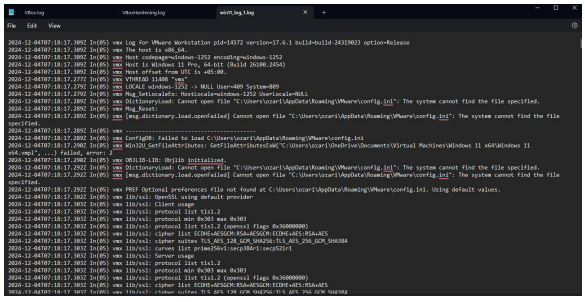
All the logs files are saved in “win10/Event logs; win11/Event logs” for Windows 10 and 11 respectively. Here is a preview of those logs:



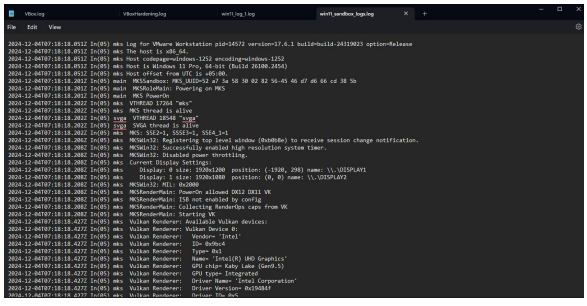
System event log for Windows 10



Security event log for Windows 10



System event log for Windows 11



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

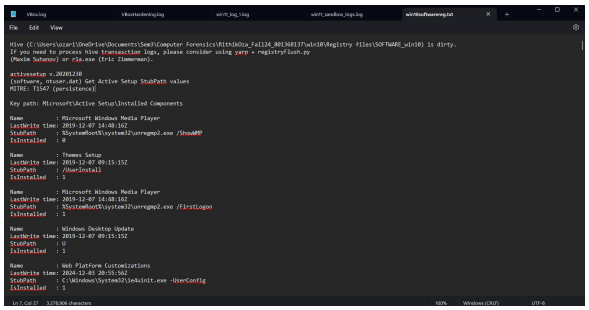
- Real-Time Insight: Captures the current state and interactions of the system, making it invaluable for monitoring.
- Error Detection: Highlights configuration issues or missing files, helping administrators address potential problems.
- Operational Emphasis: Focuses on live processes and system behavior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

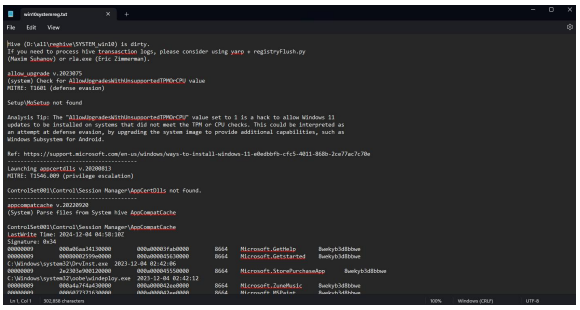
On the other hand, the win11_sandbox_logs.log provides a dynamic view of the system's performance and operations, capturing runtime activity and errors. It complements the hardening log by offering a broader perspective on the system's health and real-time interactions.

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.

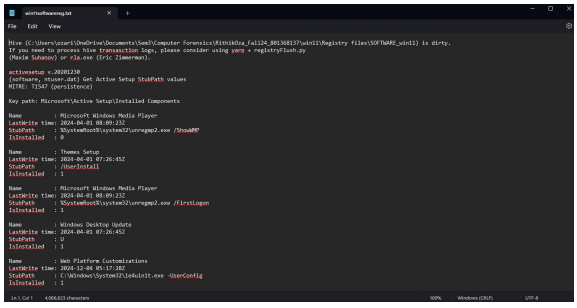
Registry Entries:



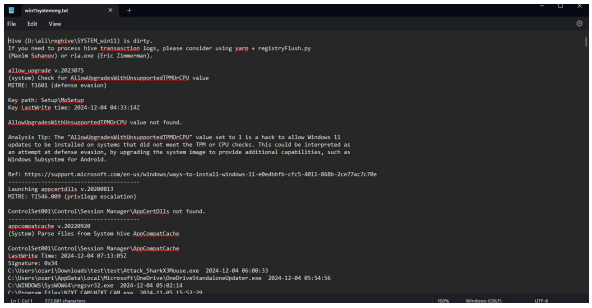
SOFTWARE registry log for Windows 10



SYSTEM regsitry log for Windows 10



SOFTWARE registry log for Windows 11



SYSTEM regsitry log for Windows 11

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

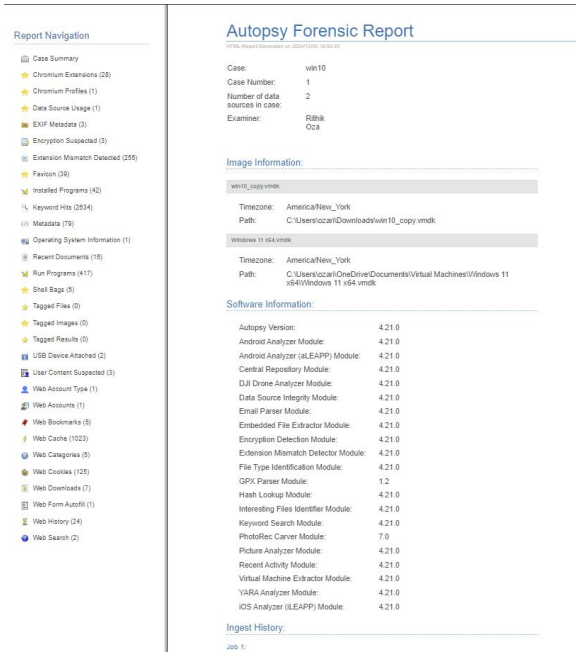
- Windows 10: Configured for crash dumps and basic diagnostics.
- Windows 11: Maintains the same settings for post-crash data capture.
- Key Difference: No notable changes between versions.

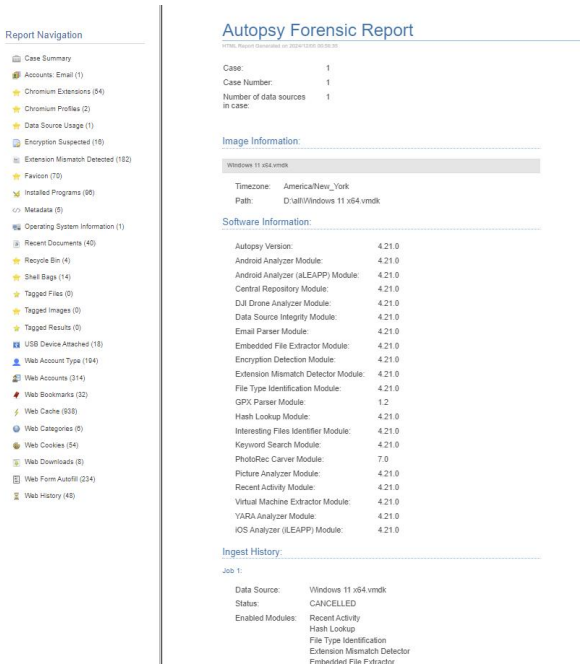
Performance and Code Pages

- 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





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

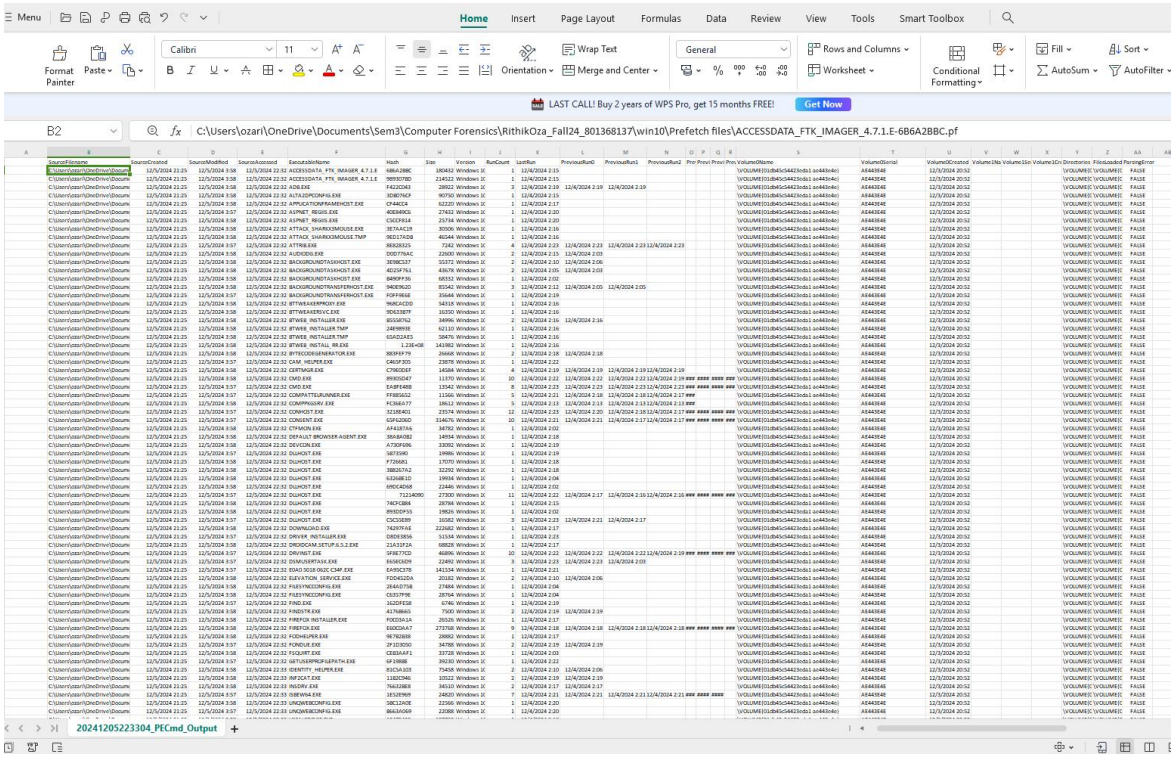
- Windows 10: Smaller cache focused on test activity.
- Windows 11: Expanded cache with detailed metadata.

Web History

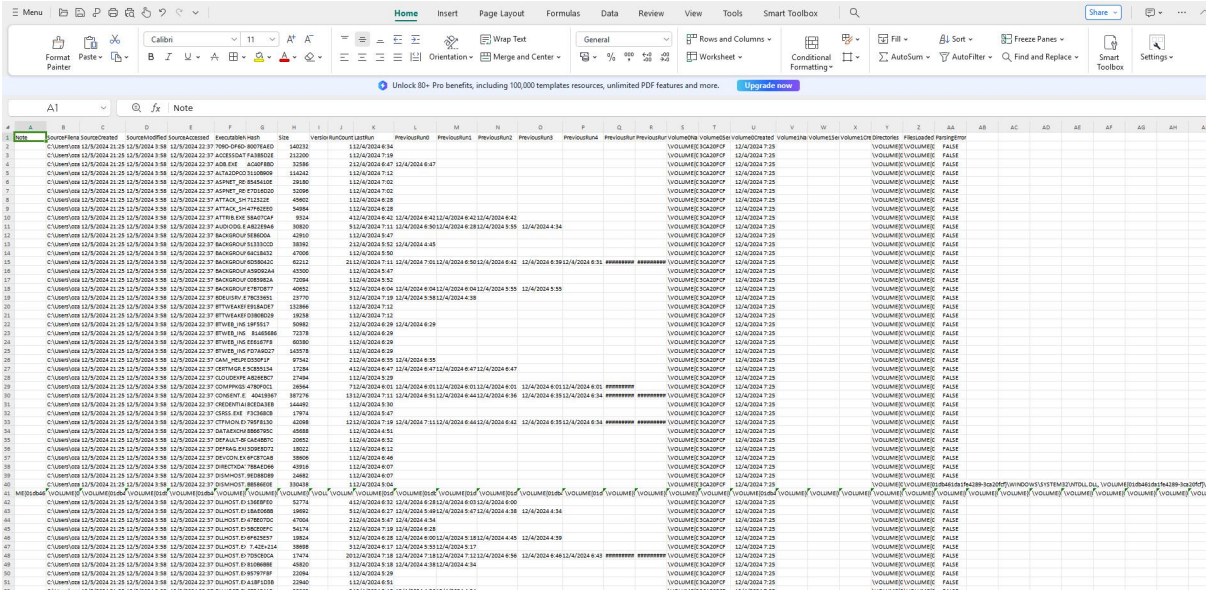
- Windows 10: Test-focused browsing activity.
- Windows 11: Broader and more dynamic web usage.

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.

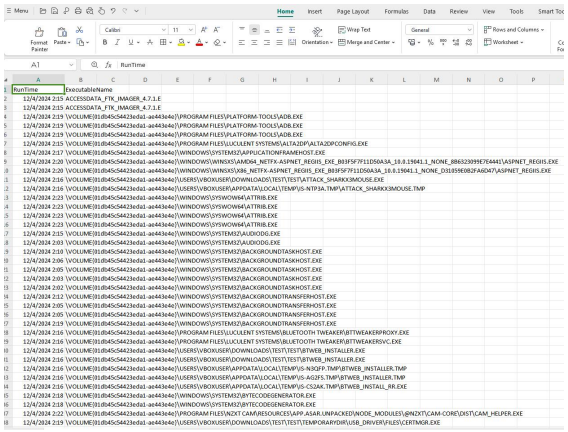
Prefetch Files



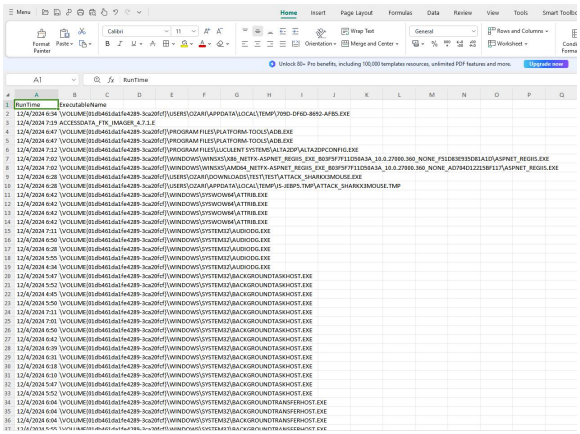
Prefetch extracted csv from PECmd of Windows 10



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:

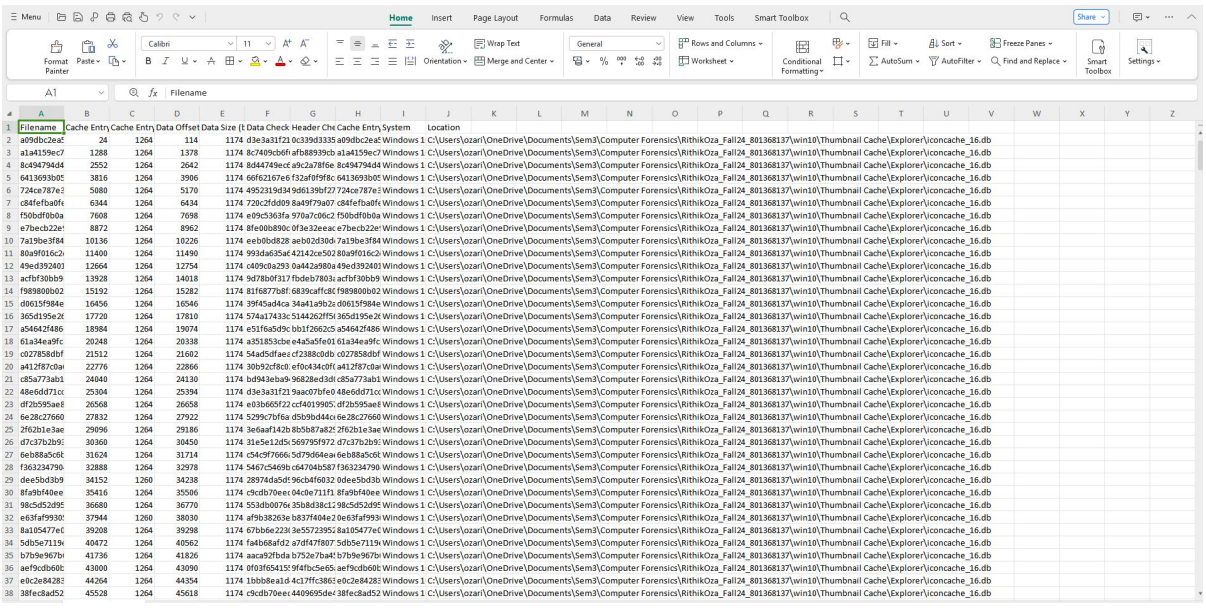
- ACCESSDATA_FTK_IMAGER_4.7.1.E executed at 7:19 AM on December 4, 2024.
- Files stored under \VOLUME{01db461da1fe4289-3ca20fcf} with paths like USERS\OZARI.
- Activity extends across the day, covering diverse program usage.

Key Comparisons

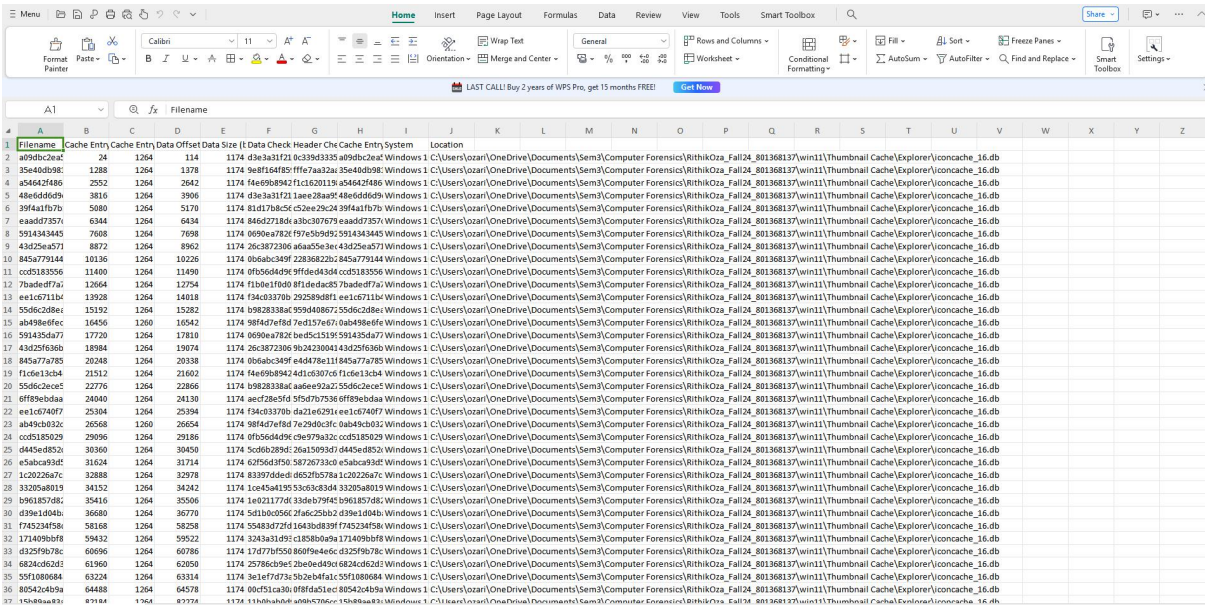
- Execution Range: Windows 11 logs show extended activity throughout the day, compared to Windows 10's shorter timeline.
- File Scope: Windows 10 logs focus on system directories like PROGRAM FILES, while Windows 11 captures both system-level and user-specific paths.

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



Win10



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.