Windows 10 vs. Windows 11, What Has Changed?

GIAC GCFE Gold Certification

Author: Andrew Rathbun, andrew.d.rathbun@gmail.com

Advisor: Christopher Walker.'., MS-ISS, BA CS, CISSP, GSEC, GCED, GCWN, GWEB, C|CISO, CISA

Accepted: July 12, 2022

Abstract

Windows 10 was released on July 29, 2015. It has since become the most installed desktop operating system. More recently, Windows 11 was released to the general public on October 5, 2021, which served as an evolution of Windows 10. At the time of publication, there has not been a peer-reviewed, deep-dive comparison between the well-known artifacts in Windows 10 and what changes Windows 11 have brought. Artifacts come and go with each new version of Windows, requiring a comparative analysis between the most recent version, Windows 10, and the next version, Windows 11. Security features also come and go as threat models evolve. This Gold Paper aims to provide an exhaustive look into the difference between Windows 10 and 11 as it relates to common artifacts and security features to provide actionable takeaways for digital forensic and incident response examiners and IT administrators alike.

1. Introduction

Windows is an operating system created by Microsoft that has become ubiquitous in the world of personal and professional computing since its initial release in 1985. As of March 2022, Windows is the most installed Operating System ("OS") with an overall global market share of 75.7%, making it the most widely used OS in the world by a wide margin (Statcounter, 2022). At the time of publication, Statcounter (2022) states that 74.82% of Windows installations are Windows 10, and 8.45% are Windows 11. Microsoft (2022a) asserts that over 1.4 billion devices are running Windows 10 or 11. With that many devices and users, it should be no surprise that Windows is essential in many people's personal and professional lives.

Microsoft (2022b) states they will support at least one version of Windows 10 until October 14, 2025. Therefore, it is reasonable to project that Windows 11's adoption will experience a marked increase as security updates will no longer be developed for Windows 10 at that time. Understanding the differences between Windows 10 and 11 will be crucial for digital forensic examiners as time goes on and the adoption of Windows 11 increases.

The integration of Microsoft's Windows operating system into so many people's lives worldwide means that digital forensic examiners must understand the nuances in each version of Windows compared to previous, more familiar versions of Windows. This paper aims to detail the differences and similarities between Windows 10 and Windows 11 from two perspectives: investigative artifacts and security features.

For Digital Forensic and Incident Response ("DFIR") examiners, Windows provides a platform to run many commercial and open-source digital forensics tools.

Windows 11 Specs and System Requirements | Microsoft - use this

2. Background

2.1. Assumptions

This paper assumes the reader has already taken SANS FOR500 or has an understanding equivalent to the course objectives of SANS FOR500. As a result, there is minimal discussion about what each artifact signifies in the context of a digital forensic analysis scenario. This expectation of prior knowledge means this paper will not fully explain standard definitions from SANS FOR500 or SANS FOR508.

2.2. Context

Microsoft (2021d) officially announced Windows 11 on June 24, 2021, and released the first version of Windows 11 on October 4, 2021 (Microsoft, 2021c). The research for this paper is based on the most current builds of Windows 10 and Windows 11 (see Appendix A) at the time of Windows 11's release on October 4, 2021 (Microsoft, 2022c and 2022d).

Please note the versions highlighted above will be referred to as "Windows 10" and "Windows 11", respectively, throughout the remainder of this paper. Also, it should be noted that this paper can only provide a "snapshot in time" analysis between Windows 10 and 11. At the time of this paper's publication, new features have surfaced and will continue to emerge beyond the scope of the specific version of Windows 11 covered in this paper. Lastly, all independent research was based on a clean installation of Windows 10 and 11.

2.3. Tools Used During This Research

A variety of tools were used during the general research process. VMware Workstation Pro was used to virtualize Windows 10 and 11 to generate artifacts (VMware, 2022). Kroll Artifact Parser and Extractor (KAPE) was used to acquire artifacts using Targets on artifacts generated from Windows 10 and 11 virtual machines (Kroll, 2022). Eric Zimmerman's tools were leveraged using KAPE's Modules to generate parsed output from the artifacts acquired by KAPE (Zimmerman, 2022). Beyond Compare was used to compare raw artifacts, output from Eric Zimmerman's Tools, and output from artifact-specific tools.

When comparing the raw artifact(s) from Windows 10 with Windows 11, 010 Editor was used to observe differences at the hexadecimal level, often leveraging binary templates (SweetScape Software, Inc, 2021). When comparing Registry hives, NirSoft's RegistryChangesView was used to compare the differences between Keys and Values added or removed from Windows 10 and Windows 11 Registry hives (Sofer, 2021).

2.4. Associated GitHub Repository and Raw Artifacts

A GitHub repository was created in support of this paper to benefit the reader, researchers, and forensic examiners (Rathbun, 2022c). The repository contains raw samples of the artifacts mentioned throughout this paper and are the same artifacts used by the author to draw conclusions made in this paper. Additionally, this repository contains supporting evidence for various artifacts too significant to summarize in the respective artifact's subsection or the Appendix. Therefore, the Appendix for this paper will be extensive and contain many references to this repository, providing the evidence needed to validate the conclusions made in this paper independently. This paper will broadly summarize the findings drawn from the raw artifacts hosted in the GitHub repository, but more can be gleaned from diving into the artifacts yourself. The link to the GitHub repository is here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun.

3. Forensic Artifacts

3.1. Previously Established Artifacts

This section aims to provide a primer on whether previously established artifacts from Windows 10 still exist in Windows 11. Additionally, a comparative analysis was conducted between Windows 10 and 11 artifacts to observe and report similarities and differences between each respective set of artifacts. Some comparisons may be too voluminous to report in this paper reasonably. In those instances, the reader can review the ancillary datasets provided in the associated GitHub repository.

3.1.1. LNK Files/Jump Lists

The Shell Link (.LNK) Binary File Format was revised in June 2021 (Microsoft, 2021e). However, in this most recent revision, no forensically significant changes appear to have been made in the Shell Link (.LNK) Binary File Format. Independent research conducted for this paper (see Appendix B) did not reveal any differences between the Shell Link (.LNK) Binary File Format from Windows 10 and Windows 11. Given that Jump Lists consist of a group of .LNK files as they relate to an application, it is no surprise that independent research conducted for this paper (see Appendix C) did not reveal any differences in the Jump Lists artifact (Rathbun, 2022c).

3.1.2. $Recycle_Bin Metadata Files

Independent research conducted for this paper (see Appendix D) indicates that the Recycle Bin metadata files ($I30) in Windows 10 appear identical to those found in Windows 11. In comparing a $I file from Windows 10 and Windows 11 in 010 Editor, there were no observed differences between the two artifacts at the hex level. Each of the $I files displayed the same version (0x02) at the beginning of the file when examined in hexadecimal (Rathbun, 2022a).

3.1.3. Amcache

Independent research conducted for this paper (see Appendix E) indicates that the Amcache hive in Windows 10 is identical to that found in Windows 11 (Rathbun, 2022c). In comparing a recursive dump from the topmost (root) key of Amcache.hve in Windows 10 and Windows 11, there were no observed differences between the two artifacts on a clean install.

3.1.4. Registry Hives

The Registry hives (see Appendix F) from Windows 10 and 11 were dumped from the topmost (root) key to JSON using KAPE. A comparison between Windows 10 and 11 instances of these Registry hives using NirSoft's RegistryChangesView revealed many Registry Keys and Values were added to or removed from Windows 11. Independent research conducted for this paper (see Appendix G) revealed over 35,000 changes in Keys and Values occurred between Windows 10 and 11 (Rathbun, 2022c). At this time, nothing forensically significant has been discovered in the Windows 11

Registry, but given the number of changes, more granular research needs to be conducted.

3.1.5. Windows Timeline

The Windows Timeline feature was added to Windows 10 in the April 2018 (1804) update (Microsoft, 2021a). Using the Windows logo key + Tab, end-users could view a timeline of applications they had opened for up to 30 days prior. As of July 2021, end-users could no longer sync their timeline activity through their Microsoft accounts. Microsoft (2021a) subsequently removed the Windows Timeline feature from Windows 11. However, independent research conducted for this paper (see Appendix H) confirmed that the Windows Timeline database, ActivitiesCache.db, still exists (Rathbun, 2022c).

3.1.6. Prefetch

Prefetch files require decompression to do a proper comparative analysis between the Windows 10 and Windows 11 versions of the artifact. Independent research conducted for this paper (see Appendix I) did not reveal any difference between the Prefetch (.pf) artifact in Windows 10 and Windows 11 (Rathbun, 2022c).

3.1.7. Event Logs

A GitHub repository, EVTX-ETW Resources (Bencherchali, N and Rathbun, A, 2022), provides XML files for each Provider in clean installs of over 140 versions of the Windows operating system dating back to Windows 7. The repository also provides a CSV for each version of Windows, which will list every Message and Event ID for every Provider present on a clean installation of a given version. Independent research conducted for this paper (see Appendix J) consisted of a comparative analysis between Windows 10 and 11, revealing that multiple Providers were either removed from Windows 10 or added to Windows 11, and multiple event IDs were added or removed from Windows 11. Numerous Event Messages were updated, added, or removed in Windows 11 (Bencherchali, N and Rathbun, A, 2022).

3.1.8. Shellbags

Independent research conducted for this paper (see Appendix K) revealed that Shellbags operated similarly in Windows 10 and 11. A simple scenario of creating multiple new subfolders within a new folder and navigating to each new folder revealed that the artifacts were recorded identically in Windows 10 and 11 (Rathbun, 2022c).

3.1.9. Windows Search Index (.ESE) Database

The Windows Search Index (Windows.ebd) artifact is present in Windows 10 and 11. Independent research conducted for this paper (see Appendix L) revealed that the same columns exist in the SystemIndex_PropertyStore table of Windows.edb. However, the table number for SystemIndex_PropertyStore changed from Table #17 in Windows 10 to Table #15 in Windows 11. Additionally, Windows 11 records one more column than Windows 10 in the SystemIndex_PropertyStore table: System_Setting_SettingsEnvironmentID. Otherwise, the other 598 columns were identical in Windows 10 and 11 (Rathbun, 2022c).

Lastly, the version of the ESE engine in Windows 10 is 9180, and the version in Windows 11 is 9400. The version of the ESE database is important for examiners to consider because ESE databases originating from Windows 10 (9180) are repairable in Windows 11, but Windows 11 ESE databases are not repairable in Windows 10. Examiners will notice this by observing an error when using esentutl.exe to repair an ESE database on an older version of Windows than the database came.

3.1.10. Web Browsers

Independent research conducted for this paper (see Appendix M) confirmed that regardless of which version of Windows 10 or 11 is installed on a computer, the version of the web browser will determine the nature of the artifacts. Edge Chromium 101.0.1210.53 was installed in both Windows 10 and Windows 11. When conducting a test of navigating multiple web pages and downloading a file, the artifacts recorded resulted in identical datasets. It is important to note that changes in artifacts for web browsers should be monitored from version to version of the web browser itself and not based on the version of the operating system it is installed on (Rathbun, 2022c).

3.1.11. ShimCache (AppCompatCache)

Davis (2021) calls the ShimCache the “most misunderstood artifact” that examiners commonly analyze as a part of their everyday investigations. Independent research conducted for this paper (see Appendix K) revealed that the ShimCache artifact operated similarly in Windows 10 and 11 (Rathbun, 2022). Given that the forensic value of ShimCache has shifted multiple times in Windows 10 (Zimmerman, 2017), it would not be surprising if ShimCache continued to evolve as Windows 11 updates over time.

3.2. Other Interesting Observations

Outside of artifacts covered in SANS FOR500, independent research discovered other interesting observations relating to the differences between Windows 10 and 11.

3.2.1. SQLite Databases

Windows ships with many files from various file types, many of which are SQLite Databases. Some artifacts previously mentioned are SQLite Databases as well as many browser artifacts. Independent research conducted for this paper (see Appendix O) revealed that similar SQLite databases exist between Windows 10 and 11 (Rathbun, 2022c).

3.2.2. Directory Listing Comparison

A GitHub repository, VanillaWindowsReference, provides a directory listing in CSV format (see Appendix P). These CSV files include several data points about the files and folders that exist on a clean install of multiple versions of Windows, including but not limited to Windows 10 and 11. The directory listings CSVs are available for public consumption for research purposes. A comparative analysis of the CSV files from Windows 10 and 11 reveals that many files and folders differ (Rathbun, 2022b).

4. Security Features

4.1. New to Windows 11

Windows 11 brings security features exclusive to Windows 11, as well as security features that Windows 10 adopted years after its initial release in 2015. This section aims to give a high-level overview of these security features to bring greater awareness to the security benefits of Windows 11.

4.1.1. Trusted Platform Module 2.0 Requirement

A Trusted Platform Module (TPM) is a firmware root-of-trust "designed to bring hardware-based security-related functions and help prevent unwanted tampering." Starting with Windows 10, "Microsoft's hardware certification required all new Windows PCs to include a TPM 2.0 built-in and enabled by default". Windows 11 takes this one step further by requiring both new and upgraded devices to have TPM 2.0 to strengthen the security posture across all Windows 11 devices using a hardware root-of-trust security model (Microsoft, 2022f).

4.1.2. Passwordless Authentication

Windows 11 provides a secure authentication process to allow end-users to utilize multifactor authentication (MFA) to significantly reduce the risk of compromise. User credentials are secured beneath hardware and software security layers to provide passwordless access to applications and services. TPM 2.0 provisions asymmetric keys to offer the chip-level hardware security used in the passwordless authentication process. The keys stored within the TPM 2.0 never leave the computer itself and, therefore, cannot be used by anyone that does not have physical access to the computer (Microsoft, 2022f).

4.1.3. Hypervisor-protected Code Integrity (HVCI)

Hypervisor-protected Code Integrity, commonly called Memory Integrity, is a virtualization-based security (VBS) feature in Windows 10 and 11 (Microsoft, 2021f). Starting in Windows 11, new installations on compatible systems will have Memory Integrity enabled by default (Microsoft, 2021b). It should be noted that Memory Integrity can still be turned on by configuring various Registry keys even if the required hardware requirements (see Appendix Q) are not met.

4.1.4. Transport Layer Security (TLS) 1.3

Transport Layer Security (TLS) is the most used security protocol on the internet (Cloudflare, 2022). TLS 1.3 is enabled by default in Windows 11 and serves to improve security by eliminating obsolete cryptographic algorithms. TLS 1.3 also encrypts as much of the handshake as possible while reducing the average number of round trips the handshake takes per connection. As a safety net, Windows 11 supports a fallback to TLS 1.2 if a server or client application does not support TLS 1.3 (Microsoft, 2022f).

4.1.5. DNS Over HTTPS

DNS over HTTPS is an encrypted DNS protocol that allows IT administrators to protect their name queries from attackers. Securing the connection to a name resolver can prevent attackers who monitor browsing history or actively redirect clients to malicious sites (Microsoft, 2022). Windows 11 allows IT administrators to implement DNS over HTTPS by default within their organization (Williams, 2022).

4.1.6. SMB Protocol Upgrades

SMB and files services are commonly used by users and applications to access files in commercial and public sector environments. Windows 11 updates the SMB protocol to include AES-256 bits encryption, accelerated SMB signing, Remote Directory Memory Access (RDMA) network encryption, and SMB over QUIC for untrusted networks. Windows 11 will automatically negotiate using the most secure cipher supported when connecting to another computer to reduce common relay and spoofing attacks (Microsoft, 2022).

4.1.7. WPA3

Windows 11 supports WPA3, WPA Enterprise 192-bit Suite B, and Opportunistic Wireless Encryption (OWE) (Microsoft, 2021f). Wi-Fi Protected Access (WPA) is a security standard that provides user authentication and encryption when connecting to Wi-Fi networks (Wi-Fi Alliance, 2018). Microsoft (2021f) states that WPA3 “provides a more secure and reliable connection method and replaces WPA2 and older security protocols”. Microsoft (2021f) says that Opportunistic Wireless Encryption (OWE) is a “technology that allows wireless devices to establish encrypted connections to public Wi-Fi hotspots.”

5. Future Research

5.1. Windows Subsystem for Android (WSA)

Windows Subsystem for Android™ enables users to run Android applications found in the Amazon Appstore on their Windows 11 device (Microsoft, 2022g). This feature did not ship with Windows 11’s initial release and therefore was not researched for this paper. Android applications on Windows 11 provide another vector for potentially malicious activity and another location for various artifacts to exist outside of traditional Windows artifacts.

5.2. Smart App Control

Smart App Control is a feature aimed to provide "significant protection from malware, including new and emerging threats, by blocking malicious or untrusted apps" (Microsoft, 2022e). Once released, this feature will require testing to determine how effectively it serves as a roadblock to malicious actors from accomplishing their mission. This feature did not ship with Windows 11's initial release and therefore was not researched for this paper.

5.3. Secured-Core PC Configuration Lock

Config Lock is a feature that "monitors the Registry keys set by IT administrators to ensure devices in their ecosystem comply with company security policies" (Microsoft, 2022h). Microsoft (2022f) states that Config Lock will detect changes in Registry keys and revert an impacted system's Registry keys to the desired state as set by an IT administrator. Additionally, Config Lock will log the activity of when changes in the Registry configuration were detected. This feature did not ship with Windows 11's initial release and therefore was not researched for this paper. Independent research will need to determine where this activity is logged.

5.4. Artifact Validation

Conventional Windows artifacts mentioned in this paper have evolved with the operating system as new versions and updates are released. As Windows 11 is updated yearly, it will be incumbent upon researchers and forensic examiners to continue to validate that the generally understood functionality of these artifacts remains the same. New findings are encouraged to be reported and shared with the community to benefit the greater good.

6. Conclusion

From the perspective of the DFIR examiner, Windows 11 contains minimal differences relative to what one would expect with a major new version release. However, new features mentioned in this paper and ones yet to be revealed will most certainly provide the potential for new artifacts of relevance for digital forensic examiners. With Microsoft committing to yearly updates for Windows 11, the DFIR community will need to revisit each feature update to revalidate commonly understood artifacts and hunt for new artifacts that can provide reliable evidence of user activity.

7. References

Bencherchali, N., & Rathbun, A. D. (2022, May 19). NASBENCH/EVTX-ETW-resources: Event tracing for windows (ETW) resources. Retrieved May 27, 2022, from https://github.com/nasbench/EVTX-ETW-Resources

Cloudflare. (2022, May 21). What is transport layer security? | TLS protocol | cloudflare. Retrieved May 21, 2022, from https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

Davis, R. (2021, July 19). Let's talk about shimcache - the most misunderstood artifact. Retrieved May 27, 2022, from https://www.youtube.com/watch?v=7byz1dR_CLg

Kroll. (2022). Kroll artifact parser and extractor - kape. Retrieved May 21, 2022, from https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

Microsoft. (2021a). Microsoft. Retrieved May 6, 2022, from https://support.microsoft.com/en-us/windows/get-help-with-timeline-febc28db-034c-d2b0-3bbe-79aa0c501039

Microsoft. (2021b, December 17). Enable virtualization-based protection of code integrity - windows security. Retrieved May 21, 2022, from https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/enable-virtualitzation-based-protection-of-code-integrity

Microsoft. (2021c, June 24). Introducing Windows 11. Retrieved May 14, 2022, from https://news.microsoft.com/windows11-general-availability/

Microsoft. (2021d, June 24). Introducing Windows 11. Retrieved May 7, 2022, from https://news.microsoft.com/june-24-2021/

Microsoft. (2021e, June 24). [MS-SHLLINK]: Shell link (.LNK) binary file format. Retrieved April 14, 2022, from https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-shllink/16cb4ca1-9339-4d0c-a68d-bf1d6cc0f943

Microsoft. (2021f, October 26). Hypervisor-protected code integrity enablement. Retrieved May 21, 2022, from https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-hvci-enablement

Microsoft. (2022a). Microsoft by the numbers. Retrieved May 7, 2022, from https://news.microsoft.com/bythenumbers/en/windowsdevices

Microsoft. (2022b). Windows 10 home and Pro - Microsoft Lifecycle. Retrieved April 16, 2022, from https://docs.microsoft.com/en-us/lifecycle/products/windows-10-home-and-pro

Microsoft. (2022c, April 13). Windows 10 - release information. Retrieved April 16, 2022, from https://docs.microsoft.com/en-us/windows/release-health/release-information

Microsoft. (2022d, April 25). Windows 11 - release information. Retrieved May 7, 2022, from https://docs.microsoft.com/en-us/windows/release-health/windows11-release-information

Microsoft. (2022e, April 5). What is Smart App Control? Retrieved May 14, 2022, from https://support.microsoft.com/en-gb/topic/what-is-smart-app-control-285ea03d-fa88-4d56-882e-6698afdb7003

Microsoft. (2022f, April 5). Windows 11 security book: Powerful security from chip to cloud. Retrieved May 15, 2022, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMyFE

Microsoft. (2022g, March 1). Windows subsystem for Android™. Retrieved May 13, 2022, from https://docs.microsoft.com/en-us/windows/android/wsa/

Microsoft. (2022h, March 14). Secured-core configuration lock - windows client management. Retrieved May 14, 2022, from https://docs.microsoft.com/en-us/windows/client-management/mdm/config-lock

Rathbun, A. D. (2022a, February 25). Add messaging for windows 11 $i files by Andrewrathbun · pull request #5 · Ericzimmerman/RBCMD. Retrieved April 14, 2022, from https://github.com/EricZimmerman/RBCmd/pull/5

Rathbun, A. D. (2022b, May 19). Andrewrathbun/Vanillawindowsreference: A repo that contains recursive directory listings (using PowerShell) of a vanilla (clean) install of every windows OS version to compare and see what's been added with each update. use these CSVS to create your own known good hash sets! Retrieved May 21, 2022, from https://github.com/AndrewRathbun/VanillaWindowsReference

Rathbun, A. D. (2022c, May 27). AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun: A repository containing the output of my research in comparing Windows 10 and Windows 11. (github.com). Retrieved May 27, 2022, from https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun

Scooter Software. (2022). Beyond Compare. Retrieved May 21, 2022, from https://scootersoftware.com

Sofer, N. (2021). Compare Snapshots of Windows Registry. Retrieved May 30, 2022, from https://www.nirsoft.net/utils/registry_changes_view.html

Statcounter. (2022, March). Desktop Operating System Market Share Worldwide. Retrieved April 14, 2022, from https://gs.statcounter.com/os-market-share/desktop/worldwide

Statcounter. (2022, March). Desktop windows version market share worldwide. Retrieved April 16, 2022, from https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/

SweetScape Software Inc. (2021, October 7). 010 editor - pro text/hex editor: EDIT 200+ formats: FAST & powerful: Reverse engineering. Retrieved May 21, 2022, from https://www.sweetscape.com/010editor/

VMware. (2022, May 18). Workstation Pro - VMware Products : Windows Virtualization for everyone. Retrieved May 21, 2022, from https://www.vmware.com/products/workstation-pro.html

Wi-Fi Alliance. (2018, June 25). Wi-Fi Alliance® introduces Wi-Fi certified WPA3™ security. Retrieved May 21, 2022, from https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

Williams, J. (2022, January 7). How SMBs Can Benefit from the Security Protections of Windows 11. Retrieved April 15, 2022, from https://www.sans.org/white-papers/how-smbs-benefit-from-security-protections-windows-11/

Zimmerman, E. R. (2017, March 30). Windows 10 creators update VS shimcache parsers: Fight!! Retrieved May 27, 2022, from https://binaryforay.blogspot.com/2017/03/windows-10-creators-update-vs-shimcache.html

Zimmerman, E. R. (2022, May 20). Eric Zimmerman’s tools. Retrieved May 21, 2022, from https://ericzimmerman.github.io/#!index.md

8. Appendix

Appendix A

Operating System	Version	Build Number	Build Date
Windows 10	Pro (21H1)	19403.1237	2021-09-14
Windows 11	Pro (21H2)	22000.194	2021-09-16

Windows 10 source: https://support.microsoft.com/en-us/topic/september-14-2021-kb5005565-os-builds-19041-1237-19042-1237-and-19043-1237-292cf8ed-f97b-4cd8-9883-32b71e3e6b44

Windows 11 source: https://support.microsoft.com/en-us/topic/windows-11-update-history-a19cd327-b57f-44b9-84e0-26ced7109ba9

Appendix B

Raw .LNK artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/LNKFiles

Appendix C

Raw Jump List artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/Jump Lists

Appendix D

Raw Recycle Bin artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/RecycleBin

Appendix E

Raw Amcache artifacts from Windows 10 and 11 virtual machines created for this research can be found here:

https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/Amcache

Appendix F

The Registry hives affected were the following:

- BCD-Template
- COMPONENTS
- DEFAULT
- DRIVERS
- ELAM
- NTUSER.dat
- SAM
- SECURITY
- SOFTWARE
- SYSTEM
- UsrClass.dat

Appendix G

Raw Registry artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/Registry

Appendix H

Raw Windows Timeline artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/WindowsTimeline

Appendix I

Raw Prefetch artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/Prefetch

Appendix J

Raw Event Log artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/EventLogs

Below is a table that illustrates which Event Log Providers exist in Windows 10 but not 11 or exist in Windows 11 but not 10:

Windows 10 (Not Present in Windows 11)	Windows 11 (Not Present in Windows 10)
Microsoft-Windows-Containers-Wcnfs	Microsoft-Quic
Microsoft-Windows-Diagnosis-PerfHost	Microsoft-System-Diagnostics-DiagnosticInvoker
Microsoft-Windows-Diagnostics-PerfTrack-Counters	Microsoft-Windows-DNS-Client-DiagTrack
Microsoft-Windows-DucUpdateAgent	Microsoft-Windows-EnhancedStorage-ClassDriver
Microsoft-Windows-HomeGroup-ListenerService	Microsoft-Windows-hidcfu
Microsoft-Windows-HomeGroup-ProviderService	Microsoft-Windows-Hyper-V-KMCL-Child
Microsoft-Windows-Hyper-V-Guest-Drivers-IcSvc	Microsoft-Windows-Kernel-Cache
Microsoft-Windows-Mobile-Broadband-Experience-Parser-Task	Microsoft-Windows-Kernel-CPU-Starvation
Microsoft-Windows-MSPaint	Microsoft-Windows-Kernel-Dump
Microsoft-Windows-NetworkStatus	Microsoft-Windows-Kernel-Prm
Microsoft-Windows-OcpUpdateAgent	Microsoft-Windows-MapControls
Microsoft-Windows-PackageStateRoaming	Microsoft-Windows-MosHost
Microsoft-Windows-PerfCtrs	Microsoft-Windows-NtfsLog_2fa848f80350371e48dfc224687745af
Microsoft-WindowsPhone-Net-Cellcore-CellManager	Microsoft-Windows-NvmeDisk

Windows 10 (Not Present in Windows 11)	**Windows 11 (Not Present in Windows 10)**
Microsoft-WindowsPhone-Net-Cellcore-CellularAPI	Microsoft-Windows-Privacy-Auditing-CPSS
Microsoft-Windows-Registry-SQM-Provider	Microsoft-Windows-StorageManagement-PartUtil
Microsoft-Windows-Security-Adminless	Microsoft-Windows-StorageSpaces-Api
Microsoft-Windows-Security-IdentityListener	Microsoft-Windows-StorageSpaces-Parser
Microsoft-Windows-SettingSync	Microsoft-Windows-TenantRestrictions
Microsoft-Windows-SettingSync-Azure	Microsoft-Windows-USB-USB4DeviceRouter-EventLogs
Microsoft-Windows-SettingSync-Desktop	Microsoft-Windows-WerKernel
Microsoft-Windows-SettingSync-OneDrive	Microsoft-Windows-WinHttp-Pca
Microsoft-Windows-Volume	Microsoft-Windows-WinINet-Pca
Microsoft-Windows-WinJson	Microsoft-Windows-Winsock-Sockets
Microsoft-Windows-WinQuic	Microsoft-Windows-WwanClient_ba7d1e0209ba3c1618d0ff4e1b3cc41f
	Microsoft-Windows-ZTraceMaps

Appendix K

Raw Shellbags artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/Shellbags

Appendix L

Raw Windows Search Index Database artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/WindowsSearchIndexDB

Appendix M

Raw Edge Chromium artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/EdgeChromium

Appendix N

Raw ShimCache artifacts from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/ShimCache

Appendix O

A list of SQLite databases located on Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/SANSGoldPaperResearch_FOR500_Rathbun/tree/main/SQLiteDBs

Appendix P

A directory listing from the root of the C drive from Windows 10 and 11 virtual machines created for this research can be found here: https://github.com/AndrewRathbun/VanillaWindowsReference

Appendix Q

For a system to be comp**atible with Memory Integrity, Microsoft (2021) provides the following minimum hardware requirements:**

Processor	Intel 11th generation Core processors and newer AMD Zen 2 architecture and newer Qualcomm Snapdragon 8180 and newer
RAM	Minimum 8GB
Storage	SSD with minimum size of 64GB
Drivers	HVCI-compatible drivers must be installed
BIOS	Virtualization enabled