International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 10 – Issue 02 || Mar - Apr 2025 || PP. 13-19

Uncovering Digital Evidence through Timeline Artifact Analysis in Windows OS Systems

Dija S, Lokeswari K, Shamil Shaji
Resource Centre for Cyber Forensics
Center for Development of Advanced Computing(C-DAC)
Thiruvanathapuram, India

Abstract: With the rapid advancement of technology and the evolution of Cyber Security threats, investigators often struggle to keep pace with the increasing complexity of data collection and analysis. As operating systems undergo frequent updates, the structure and accessibility of key forensic artifacts continuously change, complicating the reconstruction of user activity. Forensic artifacts serve as critical sources of evidence, capturing various aspects of system activity and user interactions. Among them, the Timeline artifact in Windows OS plays a crucial role by collecting and organizing user activity details in a structured database format known as ActivitiesCache.db. This database maintains records of timestamps, application usage, file access, and system interactions, providing valuable insights for forensic investigations. This paper highlights the significance of analyzing the timeline artifact. Unlike registry entries and event logs, timeline artifact analysis offers a more comprehensive and structured representation of system activities, ensuring faster and more efficient forensic investigations.

Keywords: Cyber Forensics, Digital Forensics, Windows Forensics, Timeline Artifact Analysis

1. Introduction

Cyber Forensics involves collecting, examining, and preserving digital evidence to investigate cybercrimes. It plays a vital role in detecting suspicious activities, retrieving lost data, and ensuring compliance with legal standards in digital investigations. Digital artifacts are traces of data left behind by user activities, system processes, and application interactions on a computer or device. These artifacts serve as valuable sources of evidence in forensic investigations, helping analysts understand past actions, recover deleted information, and track unauthorized access. A thorough examination of these artifacts allows forensic professionals to accurately trace digital activities, aiding criminal investigations. Understanding these artifacts is essential for uncovering security breaches, identifying cyber threats, and preserving evidence for legal proceedings.

A significant artifact in Windows operating systems is the Windows Timeline, which logs and records user interactions across applications, documents, and web activities. This artifact offers forensic investigators a structured overview of user behavior, detailing actions taken, timestamps, and context. This paper delves into the significance of Windows timeline artifact analysis in digital forensics. Modern operating systems store vast amounts of critical digital evidence, but the complexity and volume of this data make tracking user activity challenging. This paper also examines the difficulties in retrieving and interpreting these evolving artifacts within modern Windows environments

2. Windows Timeline Artifact Analysis

Windows 10 introduced a new feature called Windows Timeline that stores user activities done by the user in the last 30 days. Windows Timeline artifact is compelling and makes it possible to improve one's productivity and enhance task management across many applications, websites, and documents. This artifact is going to give an elaborate record of the chronological activities, making it easier for users to pick up on where they left off, whether on a project in a document or a website. It traces down all the interactions that might have taken place with files, applications, and websites as part of reconstructing user behavior in any cybercrime-related incidents or malicious activities.

The Windows Timeline artifact helps forensic investigators to trace user activities in detail. This artifact is important in building a user actions narrative, identifying abnormal behavior, and gathering key evidence. Data analysis will enable investigators to build a timeline that captures significant interactions with files, programs, websites, and even connected devices. The more applications and system functionalities interact with the timeline, the richer the evidence becomes for digital forensics. As the artifact continues to evolve with frequent updates on Windows, knowing the underlying structure of the Timeline and the artifacts that it produces is critical in the recovery of accurate data and forensic analysis. Despite this, the Timeline artifact is a

valuable asset for investigators who want to know the full scope of the user's activity. The following section will discuss its location, analysis methods, key fields, forensic relevance and challenges.

2.1 Acquisition of Timeline Artifact

In a Windows OS, the Timeline artifact database can be found in the directory: Users<username>\AppData\Local \ConnectedDevicesPlatform on the OS drive. Within this directory, open the folder corresponding to the user ID. Inside this folder, is the ActivitiesCache.db, which stores activity-related data for the Timeline artifact. Since the data is stored in a SQLitedatabase format, forensic experts can analyze it using forensic tools to extract and examine user activity records.

2.2 Analysis of Timeline Artifact

The Timeline artifact follows a structured format to record and arrange digital activities in the order they occurred. By analyzing theActivitiesCache.db file, investigators can extract critical details such as how frequently applications were used, file access history, website visits, clipboard activity, and system interactions. Key data points include timestamps (Creation Time, Expiration Time), application identifiers (AppId, ActivityId), user actions (Payload, Activity Type), device details (PlatformDeviceId), content access (ContentUri), session duration (ActiveDurationSeconds), event sequence tracking (Etag), and activity status (Active, Updated, Deleted, Ignored). This helps investigators track user actions and analyze events more effectively during forensic investigations.

2.2.1 Structure of ActivitiesCache.db

ActivitiesCache.db, a database of Timeline artifact, contains seven structured tables: Activity, ActivityOperation, ActivityPackageId, AppSettings, DataEncryptionKeys, ManualSequence, and Metadata. Each table serves a specific role in logging, updating, encrypting, and managing user activity related data. Understanding the structure and significance of these tables is crucial for extracting meaningful forensic insights. These insights help reconstruct user behavior, identify unauthorized access, and uncover potential security threats, making the Timeline artifact a valuable artifact in forensic investigations.

Table 1: Overview of Database Tables and Their Functions

SI No	Table Name	Description
1	Activity	Stores records of user activities, including timestamps and actions
2	ActivityOperation	Tracks updates made to activity records
3	Activity_PackageId	Logs deleted activities linked to specific applications
4	AppSettings	Contains configuration settings related to activity tracking
5	DataEncryption Keys	Stores encryption keys used for securing activity data
6	Manual Sequence	Maintains sequencing information for activity records
7	Metadata	Holds additional details about stored activities and system interactions

The Activity table is the first table located in ActivitiesCache.db, which is responsible for storing details about various user activities, including timestamps for when an application was used. It contains fields that capture various time-related tags: LastModifiedTime, ExpirationTime, StartTime, EndTime, and LastModifiedOnClient. StartTime indicates when an application was launched, while EndTime specifies when it stopped being used. ExpirationTime denotes the duration after which a record expires in the database. LastModifiedTime reflects the most recent modification to a record, especially if the activity was repeated. The LastModifiedOnClient field is usually empty and is updated only when users modify files. All timestamps are recorded in UTC format.

The ActivityOperation table in ActivitiesCache.db records user activity details across different devices. It is mainly used to track activity synchronization between multiple devices. If Microsoft Sync is turned off, this table remains empty**.** However, when Sync is enabled, it stores data similar to the Activity table and helps keep user activities updated across devices. This means it plays an important role in syncing and maintaining records of user actions on connected devices.

The Activity_PackageId table in ActivitiesCache.db stores user activities related to executed applications and accessed files. It acts as a cache, maintaining paths and names of executable files along with their expiration times in epoch format. These records are typically kept for up to 30 days. This table may also contain references to files or applications that have been deleted from the system, helping investigators trace past activities and reconstruct user actions.

The AppSettings table in ActivitiesCache.db stores settings and preferences including configurations and synchronization settings ofuser activities and connected applications. It contains key fields such as AppId, a unique identifier for each application, and SettingName, which refers to the specific configuration setting. The SettingValue represents the assigned value for the setting, while SyncEnabled indicates whether synchronization is turned on or off. The LastModifiedTime field records the timestamp of the most recent update. These fields help forensic investigators understand how applications store, update, and sync their data within the Timeline system, ensuring a smooth and accurate reconstruction of user activity.

The DataEncryptionKeys table in ActivitiesCache.db secures Timeline data by managing encryption keys that protect stored user activities. This table contains key fields such as KeyId, which uniquely identifies each encryption key, EncryptionAlgorithm, which specifies the method used for encrypting Timeline data, KeyValue, which stores the actual encryption key in a secure format, and LastModifiedTime, which records the timestamp of the last update to the encryption key. These fields help forensic investigators understand how Timeline data is encrypted and whether any modifications have occurred, ensuring the authenticity and security of stored activity records.

The ManualSequence table in ActivitiesCache.db helps identify changes or deletions in user activities. It includes the maximum ETag value, representing the most recent recorded activity. Investigators rely on this value to detect whether any records, especially recent ones, have been deleted or tampered with. If an expected ETag value is missing or out of sequence, it indicates possible tampering or unauthorized modifications. This field in the table preserves data integrity and aids in detecting unauthorized alterations.

The Metadata table in ActivitiesCache.db is an essential component that stores additional details about recorded activities. It includes fields such as CurrentSettings, which defines activity type configurations, and DatabaseInstanceId, a unique identifier for the database instance. The DatabaseInstanceIdUpdateTime records the last update timestamp, while DatabaseActivityPolicies stores synchronization policies.By checking when the database was last updated and what settings were changed, investigators can identify any unauthorized edits or tampering with user activity records.

2.2.2 Visualizing Timeline User Activity Data

After examining the data stored in ActivitiesCache.db and extracting information from its different tables, the output provides a clear and organized view of user activities. It includes details such as the last modification time, application name, unique application ID, application status and type, ETag values, application usage, and additional metadata. This processed data helps investigators understand user behavior and system interactions. This visual representation organizes all extracted values into a clear and detailed timeline of activities, making it highly useful for forensic investigations.The structure of the Windows 11 Timeline artifact differs from that of Windows 10 in how it records application activity duration. In Windows 10, if ActiveDurationSeconds for an application is zero, the field is absent. However, in Windows 11, there is always an entry as ActiveDurationSeconds: 0 for zero values.

2.3 Important Artifact and its Forensic Relevance

Understanding how and when specific events occurred allows forensic analysts to reconstruct user activity accurately. This section will provide a detailed analysis of the forensic significance of each table. By analyzing the tables in ActivitiesCache.db database, investigators can examine various fields to reconstruct a timeline of user actions and uncover valuable evidence. Here are the key fields stored in the database:

Table 2: Activity Table Fields and Descriptions

SI No	Field Name	Description
1	Creation Time	When an activity was first logged
2	Expiration Time	How long a record stays before deletion
3	AppId	The app that created the activity
4	Application ActivityId	The type of user interaction in an app
5	Payload	User actions like opened files and web pages
6	Activity Type	Categorizes user actions, like opening or copying
7	PlatformDevice Id	Identifies the device where the activity happened
8	ActiveDuration Seconds	Records how long a user spent on an activity
9	ContentUri	Stores links to accessed websites and files

An activity's start time in the system is indicated by the CreationTime timestamp in the Activity table. Because it helps pinpoint the precise moment a file was accessed or a program was launched, this is crucial information for forensic investigators. Investigators can follow the user's actions by examining this timestamp. Since all timestamps in ActivitiesCache.db are stored in EPOCH format, they need to be converted into a standard date and time format for easy understanding.

The Expiration Time field in the Activity table of ActivitiesCache.db shows how long a record stays in the database before it gets deleted automatically. Similar to other timestamps, expiration time is stored in EPOCH format and needs to be converted to a standard date and time format for analysis. Investigators use this field to determine whether a record was intentionally deleted or if it was removed due to expiration.This helps in distinguishing between intentional data deletion and automatic system cleanup.

The AppId field in the Activity table stores a unique identifier for the application that generated a specific activity. Every application has a distinct AppId, which allows forensic analysts to determine which software or service was responsible for creating a particular record. Additionally, for each AppId, there are multiple Application ActivityId entries that define the exact type of user interaction performed within the application. These identifiers help map out different activities associated with an application, such as opening a file, playing a video, or browsing a webpage. The Application ActivityId in the Activity table also contains details like Uniform Resource Identifier (URI) and file path, further aiding in reconstructing user actions.

The Payload field in the Activity table records the details of the files and applications accessed by the user.It gives useful information about user activity, like opened files, visited web pages, and other interactions. By examining this field, investigators can gain a better understanding of user activity over time. With this information, they can analyze how a user interacts with different applications and track usage behavior.The data is stored in a JSON format, making it easy to read and analyze with forensic tools. For example, if a suspect claims they never opened a confidential document, this table can confirm whether the file was accessed and when it happened. Investigators can also use it to establish patterns, such as whether a user regularly accessed a particular file or if there was an unusual spike in activity before an incident.

An integer value called Activity Type in the Activity table indicates the particular kind of action a user has performed on a system. It categorizes interactions, such as opening an application, viewing a document, or browsing a webpage. This classification helps forensic investigators analyze user behavior and track digital footprints. By examining activity types, investigators can determine what operations were executed and how they relate to other recorded events. For example, if a user typically has opened an application (Activity Type 5) or used an application (Activity Type 6) but suddenly shows accessing settings (Activity Type 9), or copying files (Activity Type 10) it may indicate suspicious activity. By tracking Activity Type, forensic investigators can compare it to normal behavior. Such deviations may signal unauthorized access or a security breach.

Table 3: Activity Types and Their Descriptions

SI No	ActivityType	Description
1	5	User opened an application
2	6	User was working with an application
3	10 /11	Copy/Paste

PlatformDeviceId field in the Activity table is a unique identifier that provides details about the host machine where a particular activity was initiated. This information is essential for forensic investigators as it helps determine which device was used to create or modify a file. By analyzing this identifier, investigators can link activities to specific computers and identify the user. This is particularly useful in multi-device environments where the same user may access files or applications from different systems. Correlating PlatformDeviceId with other timeline artifactsstrengthens digital evidence by establishing a clear connection between actions and devices.

The ActiveDurationSeconds field in the Activity table shows how long a user spent on an activity in a human-readable format. It records the duration of each activity at that moment. There can be multiple records for the same activity (Etag) because a user might use the application at different times. Hence by using Etag, ActiveDurationSecond, and EndTime information, the total time used by an application could be calculated.

The ContentUri field in the Activity table of ActivitiesCache.db stores links to websites, cloud documents, or local files accessed by the user. This helps investigators see which web pages were visited, which online files were opened, or which media was played. Unlike browser history, ContentUri tracks activity from different apps, not just web browsers. This gives forensic analysts a clearer picture of user actions, helping them connect different pieces of digital evidence across multiple platforms.

Table 4: Platform IDs and Corresponding Device Names

SI No	Platform Id	Device Name
1	1	Xbox One
2	6	Apple iPhone
3	7	Apple iPad
4	8	Android device
5	9	Windows 10 Desktop
6	11	Windows 10 Phone
7	12	Linux device
8	13	Windows IoT
9	14	Surface Hub
10	15	Windows Laptop

The Etag field, also known as the event ordering integer, is in the ActivityOperation table and assigns a sequential number to events associated with a particular application. When a user interacts with an application multiple times, each interaction is assigned a unique Etag, ensuring that activities are logged in chronological order. This ordering mechanism is essential for forensic investigations, as it helps establish the sequence in which events occurred. By analyzing Etag values, investigators can determine if any records have been deleted or altered. If gaps or inconsistencies appear in the sequence, it may indicate potential data tampering or anti-forensics attempts. This field is crucial in identifying unauthorized actions, such as a user attempting to delete their browsing history or remove traces of a specific file access. For instance, if an individual erases logs related to a suspicious transaction, forensic analysts can examine this field to determine if and when the deletion occurred, helping to reconstruct the missing data.

Table 5: Activity Status Codes and Descriptions

SI No	Activity Status	Description
1	1	Active
2	2	Updated
3	3	Deleted
4	4	Ignored

The Activity Status field in the ActivityOperation table indicates if an application is open, updated, deleted, or ignored. This information is stored in the SQLite database along with a timestamp for each record. This helps forensic investigators track when an application was used or changed and identify the last action the user performed.

The Executable files (EXE) field and their associated metadata are stored in the Activity_PackageId table. This field helps investigators trace which applications were run on a system and for how long. It also records details like the application's name, version, and publisher. The timestamps associated with these records help establish a timeline of events, which is crucial in forensic investigations. Additionally, by analyzing the frequency of execution, forensic experts can identify habitual usage patterns or detect anomalies that may indicate suspicious activity. Investigators use this information to track software usage and identify unauthorized programs. For example, if an investigator finds an application with an unknown publisher and an unusual version number installed on a system, it may indicate unauthorized software. For instance, if a user typically runs Microsoft Word (Version 16.0, Publisher: Microsoft) but a suspicious application named "Word_Pro" (Version 1.0, Publisher: Unknown) appears in the logs, it could signal malware or unauthorized software installation. By analyzing such anomalies, investigators can detect potential security threats. Additionally, analyzing installation timestamps and execution history can help determine if the suspicious software was recently launched.

The AppSettings table contains application specific settings and user preferences, which help forensic investigators understand configuration changes. The SettingsPropertyBag field stores key application settings,

while the AppTitle field indicates the related application. For example, if a suspect modified application settings to disable security features, this table would record such changes, aiding forensic analysis.Investigators can use this data to determine whether security settings were altered before an incident.

The Manual Sequence table provides information about the maximum ETag value in the ActivitiesCache.db file. This table helps forensic investigators determine if the suspect deleted the most recent operation. By analyzing the ETag value, investigators can identify any missing or altered activity data. It is a crucial artifact in tracing user actions and confirming whether certain operations were intentionally removed. By analyzing these records, forensic experts can identify suspicious activity patterns and recover critical evidence even if attempts were made to obscure or erase user actions. Furthermore, these artifacts contribute to legal investigations, providing verifiable insights that strengthen digital evidence in court proceedings.The Metadata table provides crucial information regarding the date and time when the evidence file, specifically ActivitiesCache.db, became active or came into service.

Forensic investigators can use these fields to identify suspicious activity, such as unauthorized access or attempts to erase digital evidence. Even if a suspect tries to delete or modify records, these fields and tables in the database can reveal gaps or inconsistencies in the activity log. This information is crucial in cybercrime cases, fraud investigations, and insider threat analysis. By analyzing these records, investigators can reconstruct events accurately and present strong digital evidence in court.

3. Challenges

While analyzing data from timeline artifacts, investigators face several challenges. Operating system artifacts, which serve as key evidence in digital investigations, are stored in different locations such as databases, logs, and system files. These artifacts often change with system updates, making it difficult to track and extract important information. Investigators must carefully navigate these evolving data structures to ensure no critical details are missed. Recovering data from complex artifacts requires specialized tools and techniques that must stay updated with the latest system changes. Some data in the database is not in a human-readable format, making manual analysis time-consuming and difficult. Investigators often need special tools or custom scripts to interpret raw data and convert it into a usable format. Another challenge is that the exact duration of an activity is not directly recorded and requires further calculations to reconstruct an accurate timeline. Investigators must rely on timestamps and indirect indicators, which can lead to errors if not handled carefully. Additionally, JSON data formats often contain both relevant and irrelevant information, requiring extra effort to filter and extract the necessary details for analysis.

4. Future Work

As technology advances and user activities become more complex, the Windows OS Timeline artifact presents new opportunities and challenges for forensic analysis. Future research should focus on enhancing tools and methodologies to effectively analyze the evolving structure of Timeline artifacts, particularly as Windows OS updates continue to modify data storage and retrieval processes. With the growing integration of cloud synchronization and cross-device activity tracking, forensic analysts must explore advanced techniques to reconstruct user behavior across platforms while addressing potential data fragmentation. Collaboration with operating system developers can aid in documenting changes and ensuring the reliability of extracted evidence. Furthermore, integrating the Timeline artifact with other forensic artifacts such as AmCache, ShimCache, and Prefetch could significantly enhance the ability to detect and investigate data deletion events or tampering, providing a more comprehensive view of system activity. Future work should also assess the reliability and integrity of Timeline data in light of these developments, ensuring it remains a valuable resource for uncovering user activities and supporting digital investigations in an ever-changing technological landscape.

5. Conclusion

Windows Timeline is a crucial OS artifact for forensic investigations in Windows machines, capturing user activity data such as app usage, accessed files, and timestamps. This data is stored in a database format, allowing investigators to analyze and reconstruct user actions.This artifact provides a chronological reconstruction of user interactions, aiding in uncovering critical digital evidence. Compared to other artifacts like shellbags, prefetch files, and registry hives, which offer insights into file access and system behavior, Timeline artifact analysis uniquely consolidates diverse activity records in a structured format, enhancing the efficiency of forensic examinations. While prefetching files primarily track application execution and shellbags record folder navigation, Timeline artifact analysis provides a broader perspective by encompassing detailed activity logs across multiple applications and system events. Unlike event logs, which focus on system-level

operations, Timeline offers a more user-centric view, allowing investigators to reconstruct digital footprints with greater clarity. Its ability to present a detailed and sequential overview of user actions makes it an invaluable artifact for investigators, enabling them to correlate evidence, map out activity sequences, and strengthen case findings with greater accuracy and reliability.

References

[1] P. Nair, S. Mukherjee, and R. Iyer, "Comprehensive analysis of ActivitiesCache.db for advanced forensic investigations," in Proceedings of the International Symposium on Cyber Forensics and Security (ISCF), Bengaluru, India, 2024, pp. 88–94.

[2] D. Patel and A. Sharma, "Forensic evaluation of Windows 10 Timeline and its implications in legal proceedings," in Proceedings of the National Conference on Legal and Digital Evidence (NCLDE), Ahmedabad, India, 2024, pp. 55–60.

[3] S. Kumar, R. Mishra, and V. R. Nair, "Investigating user activity using Windows 10 Timeline: A forensic approach," in Proceedings of the 2020 IEEE International Conference on Forensics and Security (ICFS), Mumbai, India, 2020, pp. 45–50.

[4] A. Gupta, M. Sharma, and P. Iyer, "Analysis of ActivitiesCache.db for reconstructing digital evidence," in Proceedings of the 2021 National Conference on Emerging Trends in Cyber Security (NCETC), Bengaluru, India, 2021, pp. 130–135.

[5] K. D. Roy, S. Verma, and A. Prakash, "Timeline forensics: Decoding user behavior on Windows 10," in Proceedings of the International Symposium on Digital Investigation (ISDI), New Delhi, India, 2022, pp. 78–84.

[6] R. Krishnan, S. Devi, and A. Menon, "Advancements in Timeline analysis for forensic investigations," in Proceedings of the Indian Digital Forensics Conference (IDFC), Chennai, India, 2023, pp. 200–206.

[7] P. S. Reddy, V. Subramanian, and N. Kumar, "Activity reconstruction using Windows Timeline in cybercrime investigations," in Proceedings of the IEEE International Workshop on Forensic Computing (IWFC), Hyderabad, India, 2021, pp. 112–118.

[8] R. Singh, A. Yadav, and V. Gupta, "Leveraging Windows Timeline data for cyber forensic investigations," in Proceedings of the Indian Conference on Digital Evidence and Analysis (ICDEA), Pune, India, 2023, pp. 98–104.

[9] J. Mehta, P. Roy, and K. Sharma, "Enhancing forensic methodologies through Timeline artifact analysis," in Proceedings of the International Conference on Advanced Cybersecurity Techniques (ICACT), Kolkata, India, 2022, pp. 67–73.

[10] M. Bose, S. Kapoor, and N. Agarwal, "A novel approach to extracting user activities from modern OS timelines," in Proceedings of the International Conference on Digital Forensics and Cybersecurity (ICDFC), Hyderabad, India, 2023, pp. 120–126.

[11] A. Banerjee, R. Choudhury, and P. Sen, "Comprehensive analysis of timeline artifacts for forensic investigations," in Proceedings of the National Workshop on Digital Evidence and Security (NWDES), Bengaluru, India, 2024, pp. 35–40.

[12] G. Horsman, A. Caithness, and C. Katsavounidis, "A forensic exploration of the Microsoft Windows 10 Timeline," Journal of Forensic Sciences, vol. 64, no. 2, pp. 577–586, 2019.