Mapping Cyber Incidents with Windows Timeline: The What and When of Digital Forensics

One of the key elements in a successful digital forensic investigation is to accurately analyze the sequence of events. In cases involving computer breaches, malware infections, or data theft, timelines help forensic experts retrace the steps leading to the incident.

Traditionally, temporal analysis during a cyber incident investigation involves two approaches: the basic **Timeline**, which focuses on file system metadata, and the more comprehensive **Super Timeline**, which gathers data from both the file system and the operating system. Both of these approaches typically rely on digital forensics software that allows for comprehensive analysis of file and event timestamps. The Windows 10 Timeline functionality adds one more layer to temporal analysis—a timeline generated by the operating system.

Even though in Windows 11 the timeline feature has been deprecated, the majority of users have yet to make the switch. According to recent data, Windows 11 holds a market share of around 31%, while Windows 10 still dominates with over 64% of users opting to stay with the older operating system.

With more users remaining on Windows 10, features like the Timeline can still be incredibly useful for analysis with computer forensics software, so let us explore how.

Windows 10 Timeline in a Nutshell

The "Timeline" feature allows users to browse through their past activities, including recently opened documents, launched applications, and viewed media such as videos and images. The Timeline can store this activity history for up to 30 days. Users also have the option to delete specific activity records or completely turn off the Timeline feature if desired.

To access the Windows 10 Timeline, you can click the Task View icon, located next to the magnifying glass icon on the taskbar, or use the shortcut by pressing **WinKey + Tab**. Once opened, you will see thumbnails of programs, documents, and websites that were accessed either today or in the past.

Picture 1 of Mapping Cyber Incidents with Windows Timeline: The What and When of Digital Forensics

However, it is not all smooth from there. Investigators have identified two key issues with the Windows 10 Timeline feature:

1. Certain applications do not appear in the Timeline after being used.
2. Some older Timeline data is synced to Microsoft's cloud storage.

As a result, the information gathered from analyzing the Windows 10 Timeline artifact can differ from the traditional Timeline and Super Timeline methods. It is important to note that Windows 10 Timeline is not the same as timelines generated by computer forensics software. Advanced forensic tools for Windows usually extract far more entries than what is included in the Windows 10 Timeline.

Locating the Windows 10 Timeline Database

Windows 10 tracks user activities and stores this information in a file called **ActivitiesCache.db**, located at: C:Users%username%AppDataLocalConnectedDevicesPlatformL.%username%.

Picture 2 of Mapping Cyber Incidents with Windows Timeline: The What and When of Digital Forensics

This **ActivitiesCache.db** file is an SQLite database (version 3), and like other SQLite databases, it is accompanied by two transactional files: **ActivitiesCache.db-shm** and **ActivitiesCache.db-wal**.

To retrieve additional information, particularly data that may have been deleted from the database, investigators can analyze the unallocated space within the database, as well as **Freelist** and the **WAL** (Write Ahead Log) records. By examining these areas during forensic analysis, you can potentially recover up to 30% more data.

Here is a brief explanation of these technical terms in SQLite database analysis:

1. **Freelists**: These are portions of the database that once held records but are now marked as free to be overwritten. However, they may still contain valuable, recoverable information.
2. **Write Ahead Log (WAL)**: This is a temporary file where changes to the database are written before being permanently committed. Analyzing this log can reveal information that has not yet been finalized in the database.
3. **Unallocated Space**: This refers to areas of the database that are no longer in active use but may still contain remnants of previously stored data.

Breaking Down the Windows 10 Timeline

It is time to dig deeper for possible artifacts. The latter can be found in the **ActivitiesCache.db** file, which, in turn, contains several tables:

Picture 3 of Mapping Cyber Incidents with Windows Timeline: The What and When of Digital Forensics

Among these, the **Activity** and **Activity_PackageId** tables hold the most value for investigators who can further employ computer forensics software to analyze user activities and related application package details.

Activity_PackageId Table

Picture 4 of Mapping Cyber Incidents with Windows Timeline: The What and When of Digital Forensics

The **Activity_PackageId** table, usually covering the last 30 days, stores information about executable files and the expiration time for these records. The **Expiration Time** column shows when records related to user activities will be deleted from the database, and these values are in the Unix Epoch format.

Key points about the **Activity_PackageId** table:

1. Stores data for a limited period, usually covering the last 30 days.
2. May include records of executable files or documents that are no longer present on the hard drive.
3. Has an **Expiration Time** column which shows when records related to user activities will be deleted from the database, and these values are in **Epoch Time**

Activity Table

Picture 5 of Mapping Cyber Incidents with Windows Timeline: The What and When of Digital Forensics

The **Activity** table contains five different fields that record timestamps related to user activity:

1. **StartTime**: Marks the time when an application was launched.
2. **EndTime**: Indicates when the application was last used.
3. **ExpirationTime**: Specifies when the record for that user activity will be removed from the database.
4. **LastModifiedTime**: The last time the user activity record was modified. This may occur if the activity has been repeated multiple times.
5. **LastModifiedOnClient**: This field may be empty, as it is only filled when users themselves modify files.

Another important point to consider about the **Activity** table is that the timestamps of deleted files remain unchanged. For modified documents, the time fields do not update instantly but within a 24-hour window.

How Is Windows 10 Timeline Used in Cyber Incident Investigations

When it comes to responding to incidents like data breaches, investigators focus on key activities such as remote desktop protocol (RDP) usage, file sharing events, and any interaction with cloud services, as these can indicate unauthorized access or data transfers.

Additionally, the Timeline can help track when applications were run from external storage devices like USB drives—an essential detail when identifying suspicious activity. One can often spot this by examining the disk name from which an app was executed. Monitoring these patterns allows investigators to reconstruct potential security breaches or data theft events more efficiently.

Conclusion

As one can see, Windows 10 Timeline plays a crucial role by helping reconstruct events from the last 30 days, revealing details about files that were launched, even if they have been deleted.

To analyze Windows Timeline data effectively, reliable forensic tools for Windows are necessary. Advanced digital forensics tools streamline this process with features like automated search, recovery of deleted events, and advanced filters, enhancing both Windows and mobile forensics software investigations.