

Jo

I am a forensic investigator and I need to know if a file I found on a windows 10 computer was downloaded by a particular user, how can I find this out?



As a forensic investigator, you can use various methods to determine if a file was downloaded by a particular user on a Windows 10 computer. Here are some steps you can follow:

1. File Metadata: Check the file's metadata, such as creation, modification, and access timestamps. This information can provide clues about when the file was downloaded and by whom. You can view this data in Windows by right-clicking the file, selecting 'Properties,' and then navigating to the 'Details' tab.
2. Browser History: Examine the browser history of the user in question. If the file was downloaded via a web browser, you should be able to find the download event and associated timestamp in the browser's history. Each browser has its own method to access history. For example, in Google Chrome, press Ctrl+H to open the browsing history.
3. User Account Analysis: Check the user's profile directory to see if the file is present in their 'Downloads' folder or any other folder they might have saved it in. This can help you determine if the file was downloaded by the specific user.
4. Windows Event Logs: Windows records various events on the system, including file-related activities. You can use Event Viewer to check for events related to the file download. Look for event IDs related to file creation and modification, as well as any related to user login/logout events. This may help you correlate the file download with a specific user.
5. Network Logs: If you have access to network logs, review them to find any file transfer events associated with the user's IP address and the time frame in question. This can provide additional evidence linking the file download to the user.
6. Third-party Forensic Tools: You can use specialized forensic software like EnCase, FTK, or X-Ways Forensics to perform a more in-depth analysis of the computer and gather more evidence.

Keep in mind that it's essential to follow proper forensic procedures and maintain a chain of custody to ensure that the evidence you gather is admissible in court.

Jo

I don't think that the file was downloaded using a browser, I think it was downloaded using skype, how can I find out if it was?



If you suspect that the file was downloaded via Skype, you can investigate by examining the following:

1. Skype Chat History: Check the chat history of the user to see if there is any conversation related to the file transfer. Skype stores chat history locally on the computer. You can find the main.db file, which contains the chat history, in the following location:

makefile

C:\Users\<username>\AppData\Roaming\Microsoft\Skype f

Replace `<username>` with the specific Windows user account name. You can use SQLite tools like DB Browser for SQLite to open and analyze the main.db file. Look for messages with a file attachment and verify the file name and timestamp.

2. Skype Received Files: Skype stores received files in a specific folder. Check this folder to see if the file is present:

makefile

C:\Users\<username>\AppData\Roaming\Microsoft\Skype f

Replace `<username>` with the specific Windows user account name. Compare the file name, size, and timestamp to the file you're investigating.

3. Windows Event Logs: Skype activities might be logged in the Windows Event Logs. Use Event Viewer to check for any relevant events related to Skype or file transfers during the timeframe in question.
4. Network Logs: If you have access to network logs, you can analyze them to find any file transfer events related to Skype during the time frame in question. Look for Skype-related traffic (e.g., the IP address and ports used by Skype) and file transfer events.
5. Third-party Forensic Tools: Use specialized forensic software like EnCase, FTK, or X-Ways Forensics to perform a more in-depth analysis of the computer and gather more evidence related to Skype activities.

Remember to follow proper forensic procedures and maintain a chain of custody to ensure that the evidence you gather is admissible in court.

Jo

What Skype activities can I find in the Windows event logs?



Skype activities in Windows Event Logs are limited, as Skype doesn't log detailed application-level activities, such as file transfers or chat messages, in the Event Logs. However, you might find some events related to the general functioning of the Skype application.

Some events you might find in the Windows Event Logs include:

1. Application installation and updates: Look for events related to Skype installation, updates, or uninstallation. These can be found under "Application" or "System" logs in the Event Viewer.
2. Application errors or crashes: You can check for any Skype application errors, crashes, or other issues that might have been recorded in the Event Logs. These events can be found under "Application" logs in the Event Viewer.
3. User login and logout events: You can check for user login and logout events to determine if the user was active during the time frame when the file might have been downloaded. These events can be found under "Security" logs in the Event Viewer.

To search for Skype-related events in the Event Viewer:

1. Press `Win + R`, type `eventvwr.msc`, and press Enter to open the Event Viewer.
2. Expand the "Windows Logs" folder in the left pane and click on "Application," "System," or "Security," depending on which logs you want to review.
3. Use the "Filter Current Log" option in the right pane to filter events based on the event source, event ID, or keywords related to Skype (e.g., "Skype" or "Skype for Desktop").

Keep in mind that these logs might not provide enough information to conclusively determine if the file was downloaded using Skype. Examining the Skype chat history and the received files folder, as mentioned in the previous response, can provide more specific evidence.