

# transcript.txt Analysis Report  
\*\*Folder Name:\*\* raw\_logs  
\*\*File Types:\*\* TXT  
\*\*Collection Date:\*\* 2026-01-25  
\*\*Report Generated:\*\* 2026-01-25

## 1. File Overview and Meaning

### 1.1 What Is the transcript.txt?

The `transcript.txt` file is a log generated by Windows PowerShell, which records the commands executed in a session.

### 1.2 Purpose and Importance

- \* **Credential Discovery:** The log may contain usernames, which could be useful for credential discovery in forensic investigations.
- \* **Forensic Analysis:** The transcript can help investigators understand the sequence of events, identify potential threats, and track user activity.

### 1.3 File Format and Structure

The `transcript.txt` file contains a series of PowerShell commands, their output, and any errors or exceptions that occur during the session.

## 2. Data Types and Structure

### 2.1 Key Attributes or Fields

- \* Start Time
- \* Username
- \* Process ID
- \* Configuration Name
- \* Machine
- \* Host Application
- \* PSVersion
- \* PSEdition
- \* PSCompatibleVersions
- \* BuildVersion
- \* CLRVersion
- \* WSMANStackVersion
- \* PSRemotingProtocolVersion
- \* SerializationVersion
- \* Output File Path
- \* Transcript Start and End Time
- \* Error Messages

### 2.2 Field Descriptions

Field Name	Data Type	Description
Start time	DateTime	The time when the transcript was started
Username	String	The user who initiated the PowerShell session
Process ID	Int	The process ID associated with the PowerShell session
Configuration Name	String	The name of the configuration used in the script or interactive session
Machine	String	The name and operating system version of the machine where the PowerShell session was initiated
Host Application	String	The application that initiated the PowerShell session, such as a script file or interactive console
PSVersion	String	The version of PowerShell being used
PSEdition	String	The edition of PowerShell (Desktop, Server, etc.)
PSCompatibleVersions	String	A comma-separated list of compatible versions of PowerShell
BuildVersion	String	The build number of the operating system
CLRVersion	String	The version of the Common Language Runtime (CLR) being used
WSMANStackVersion	String	The version of the Web Services for Management (WSMAN) stack
PSRemotingProtocolVersion	String	The version of the PowerShell remoting protocol being used