events_filtered_Application.csv Analysis Report
Folder Name: raw_logs
File Types: CSV
Collection Date: 2026-01-25
Report Generated: 2026-01-25

1. File Overview and Meaning
1.1 What Is the events_filtered_Application.csv?
The `events_filtered_Application.csv` is a log file that contains application-related events in a comma-separa

1.2 Purpose and Importance
This log file serves multiple purposes:
* **Credential Discovery:** It may contain sensitive information such as usernames, timestamps, and other s
* **Forensic Analysis:** The events recorded in this log can help investigators understand the behavior of ap

1.3 File Format and Structure
The `events_filtered_Application.csv` file consists of rows with comma-separated fields, each representing d

2. Data Types and Structure
2.1 Key Attributes or Fields
Common fields found in this type of artifact include:
* TimeCreated: Timestamp of when the event occurred
* Id: Unique identifier for the event
* LevelDisplayName: Severity level of the event (e.g., Error, Warning, Information)
* Message: Detailed description of the event

2.2 Field Descriptions
Field Name	Data Type	Description
TimeCreated	DateTime	Timestamp of when the event occurred
Id	Integer	Unique identifier for the event
LevelDisplayName	String	Severity level of the event (e.g., Error, Warning, Information)
Message	String	Detailed description of the event

2.3 Sensitive or Security-Relevant Data Categories
* **Credential Metadata:** Usernames, passwords, or other sensitive information that may be included in the
* **Access Context:** Information about the application, user, and system context in which the event occurre

3. Where This Data Is Used
3.1 Security Operations Use Cases
SOC teams use this data for auditing and monitoring to:
* Identify unusual or suspicious activity patterns related to specific applications.
* Investigate potential security incidents by correlating events with other logs, such as system event logs or f
* Troubleshoot application-related issues and improve overall system performance.

3.2 Incident Response and Threat Hunting
IR teams use this data to find attackers by:
* Analyzing the sequence of events related to a specific application to identify potential malicious activity.
* Investigating failed or unsuccessful installations, updates, or modifications of applications that could indicat

3.3 Correlation With Other Artifacts
This log correlates with other logs such as:
* System Event Logs