# evtx_export_skipped 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 evtx_export_skipped Artifact?
The `evtx_export_skipped` artifact is a text file generated by tools that export Event Tracing for Windows (ET

### 1.2 Purpose and Importance
* **Credential Discovery:** The artifact may contain event data that could potentially reveal sensitive informa
* **Forensic Analysis:** The skipped events may provide valuable context for ongoing investigations or incid

### 1.3 File Format and Structure
The `evtx_export_skipped` artifact is a plain text file with each line representing an event that was skipped d

## 2. Data Types and Structure
### 2.1 Key Attributes or Fields
* Event ID
* Source Name (e.g., Application, Security, System)
* Timestamp

### 2.2 Field Descriptions
| Field Name | Data Type | Description |
| :--- | :--- | :--- |
| Event ID | Integer | A unique identifier for the event. |
| Source Name | String | The name of the source (e.g., Application, Security, System) that generated the eve
| Timestamp | DateTime | The date and time when the event occurred. |

### 2.3 Sensitive or Security-Relevant Data Categories
* **Credential Metadata:** Potentially, if the skipped events contain sensitive information such as user accou
* **Access Context:** Depending on the source of the skipped events, they may provide context about acces

## 3. Where This Data Is Used
### 3.1 Security Operations Use Cases
* SOC teams can use this data for auditing and monitoring by reviewing the skipped events to identify unusu

### 3.2 Incident Response and Threat Hunting
* IR teams can use this data to find attackers by analyzing the skipped events for indicators of compromise (

### 3.3 Correlation With Other Artifacts
* Event Logs
* Firewall logs
* Intrusion Detection System (IDS) alerts

## 4. Data Protection and Security Precautions
### 4.1 Why This Data Is Sensitive
The data contained in the `evtx_export_skipped` artifact can potentially reveal sensitive information, which c

### 4.2 Storage, Access Control, and Handling
* Encryption: The file should be encrypted to protect its contents from unauthorized access.
* Access Control: Access to the file should be restricted to authorized personnel only, with proper permissio