Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

School of Computer Engineering and Technology
Academic Year: 2023-2024 Sem V
Digital Forensics and Investigation

Lab Assignment : 04

Title: Systems Logs analysis using Event Viewer

Prepared By
Saurabh Jitendra Jadhav
Roll No:PA12
Batch A1
September 25,2023

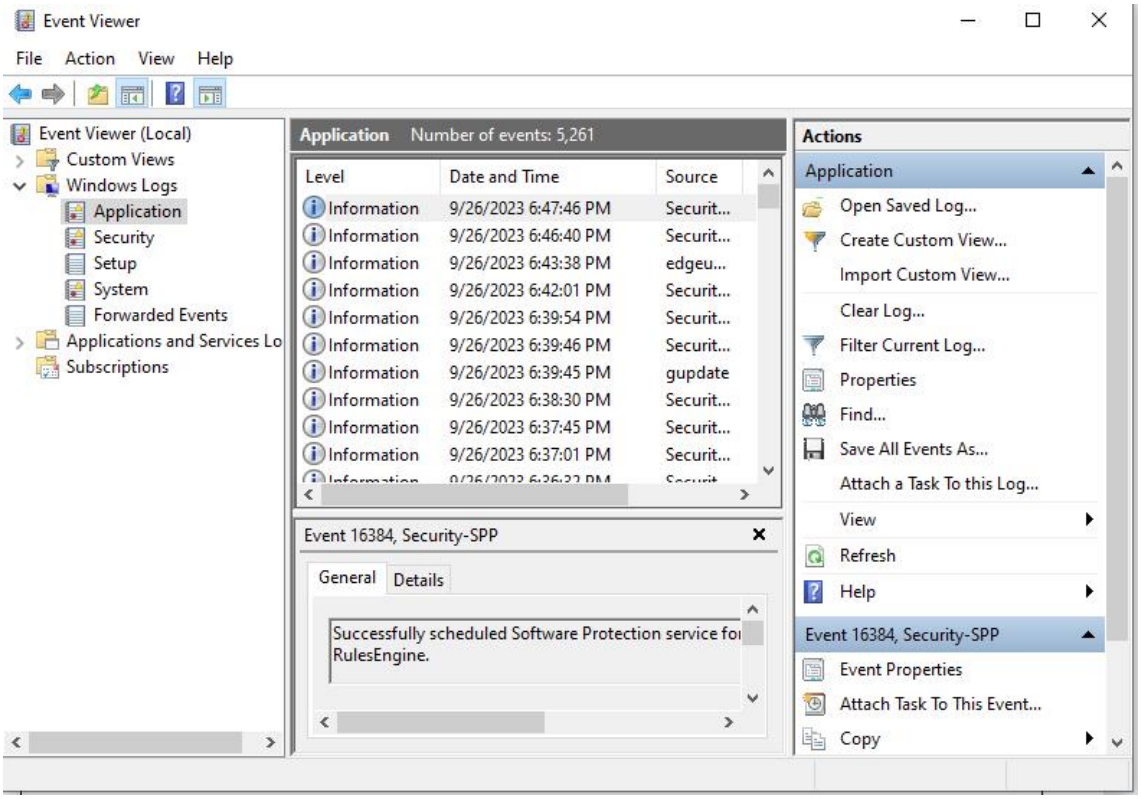
Aim: System Logs analysis Using Event Viewer.

Objective:

1. To understand the significance of system logs in digital forensics and their role in investigating computer-related incidents.
2. To demonstrate the ability to access and navigate Event Viewer on a Windows operating system for the purpose of log analysis.
3. To analyze individual log events, interpreting the information presented, including time stamps, event IDs, and event descriptions.

Theory:-

A) **Event Viewer:** Event Viewer is a built-in Windows tool that provides access to logs and details about events on a Windows computer. It is a valuable resource for digital forensics investigators to examine system and application events.



Event Viewer

B)Types of System Logs:

Application Logs: These logs record events related to applications and services running on the system. They often contain information about application crashes, errors, and warnings.

Security Logs: Security logs are crucial for tracking user logins, logouts, and security-related events. Suspicious activities or unauthorized access attempts can be found in these logs.

System Logs: System logs record events related to the operating system itself, such as hardware failures, driver issues, and system startups and shutdowns.

C)Event Identification:

Event IDs: Each log entry in Event Viewer is associated with an event ID, which categorizes the type of event. Event IDs help investigators quickly identify the nature of an event.
Filtering and Searching:

Filtering: Event Viewer allows users to filter logs based on various criteria, such as time, event type, source, and keywords. This feature is essential for isolating relevant information.

Searching: Event Viewer also provides a search function to find specific events or keywords within logs, making it easier to locate relevant data in extensive log files.

D)Analyzing Events:

Time stamps: Log entries include time stamps, which provide information about when an event occurred. Accurate time stamps are crucial for establishing timeline in digital forensics.

Event Descriptions: Event Viewer provides descriptions for each event, explaining the nature of the event and its potential implications.

E)Event Correlation:

Event Correlation: Investigating digital incidents often requires correlating events from multiple logs to reconstruct a sequence of actions. This helps investigators understand the context and impact of an incident.
Exporting Logs:

Exporting Logs: Event Viewer allows users to export log entries for further analysis, sharing with colleagues, or presentation as evidence in legal proceedings. Common export formats include CSV, XML, and EVT.

Implementation:

```python
import pandas as pd


df = pd.read_csv("systemlog.csv")


print("Summary of the DataFrame:")
print(df.info())


print("\nFirst few rows of the DataFrame:")
print(df.head())

unique_event_ids = df["Event ID"].nunique()
print(f"\nNumber of unique Event IDs: {unique_event_ids}")

# Filter events with a specific Event ID
event_id_to_filter = 1000
filtered_events = df[df["Event ID"] == event_id_to_filter]
print(f"\nEvents with Event ID {event_id_to_filter}:")
print(filtered_events)

```

```
Summary of the DataFrame:
<class 'pandas.core.frame.DataFrame'>
Index: 6695 entries, Warning to Information
Data columns (total 5 columns):
 #   Column         Non-Null Count  Dtype
---  ------         --------------  -----
 0   Level          6695 non-null   object
 1   Date and Time  6695 non-null   object
 2   Source         6695 non-null   int64
 3   Event ID       3324 non-null   object
 4   Task Category  6695 non-null   object
dtypes: int64(1), object(4)
memory usage: 313.8+ KB
None

First few rows of the DataFrame:
                         Level                    Date and Time  Source  \
Warning      9/26/2023 7:19:35 PM  Microsoft-Windows-DistributedCOM   10016
Warning      9/26/2023 7:18:10 PM      Microsoft-Windows-DNS-Client    1014
Warning      9/26/2023 7:03:19 PM      Microsoft-Windows-DNS-Client    1014
Information  9/26/2023 6:50:42 PM           Service Control Manager    7040
Warning      9/26/2023 6:46:51 PM      Microsoft-Windows-DNS-Client    1014

            Event ID                                      Task Category
Warning          NaN  The machine-default permission settings do not...
...
Events with Event ID 1000:
Empty DataFrame
Columns: [Level, Date and Time, Source, Event ID, Task Category]
Index: []
```

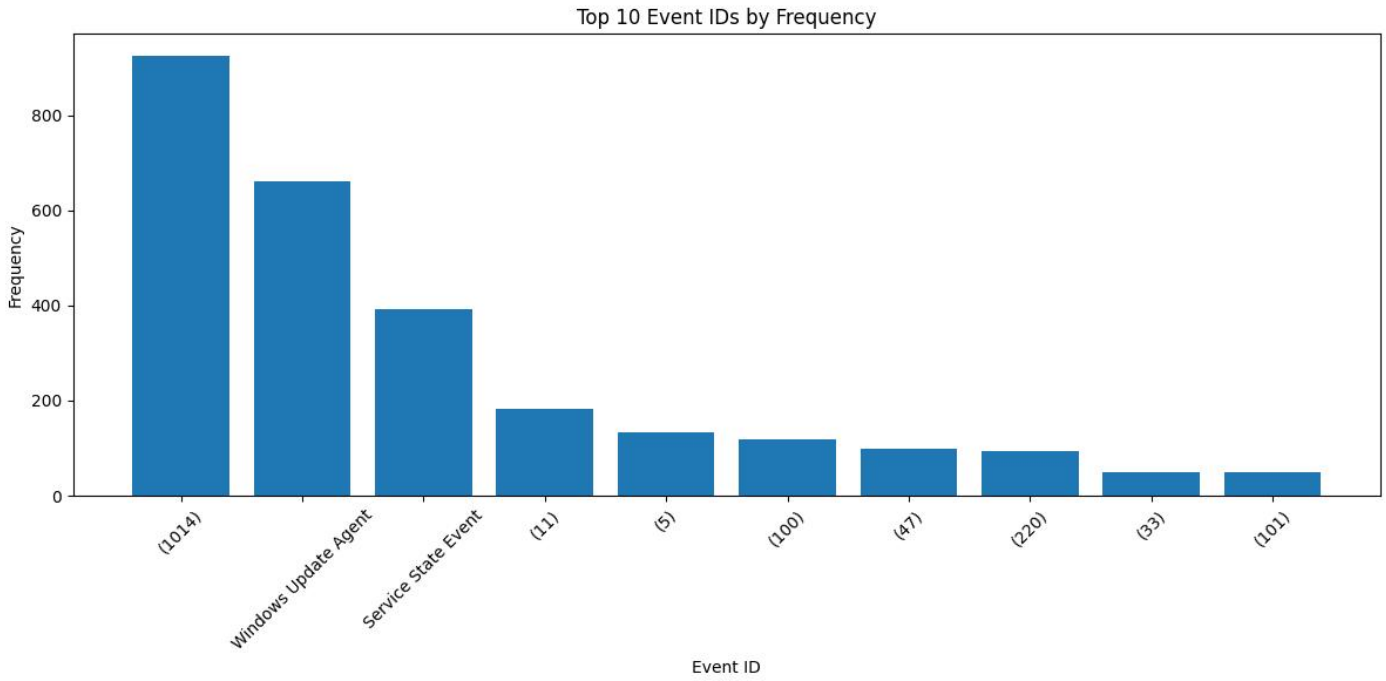
Output Image

```python
import pandas as pd
import matplotlib.pyplot as plt

# Load the "systemlog.csv" file into a DataFrame
df = pd.read_csv("systemlog.csv")

# Event Frequency Analysis
event_frequency = df["Event ID"].value_counts().reset_index()
event_frequency.columns = ["Event ID", "Frequency"]

# Plot the top N events by frequency (adjust N as needed)
top_n_events = 10
plt.figure(figsize=(12, 6))
plt.bar(
    event_frequency["Event ID"][:top_n_events],
    event_frequency["Frequency"][:top_n_events],
    tick_label=event_frequency["Event ID"][:top_n_events].astype(str),
)
plt.title("Top {} Event IDs by Frequency".format(top_n_events))
plt.xlabel("Event ID")
plt.ylabel("Frequency")
plt.xticks(rotation=45)
plt.tight_layout()
plt.show()
```



Conclusion:- Thus we learned to analyze System logs using Event Viewer.We take log from Event viewer in CSV file format and then Analyze logs by using python library named “panda”.