Practical No. 4

Aim : Write a computer forensic application program for Recovering permanent Deleted Files and Deleted Partitions.

Code :

```
import re
from datetime import datetime

def parse_logs(log_file):

    logs = []
    log_pattern = re.compile(r"\[(.*?)\] \[(.*?)\] (.*)")

    with open(log_file, "r") as f:
        for line in f:
            match = log_pattern.match(line)
            if match:
                timestamp_str, level, message = match.groups()
                timestamp = datetime.strptime(timestamp_str, "%Y-%m-%d
%H:%M:%S")
                logs.append({"timestamp": timestamp, "level": level,
"message": message})
    return logs

def correlate_events(logs, keyword=None, time_window=5):

    correlated = []
    n = len(logs)

    for i in range(n):
        for j in range(i+1, n):
            time_diff = abs((logs[j]["timestamp"] -
logs[i]["timestamp"]).total_seconds() / 60)
            if time_diff <= time_window:
                if keyword:
                    if keyword.lower() in logs[i]["message"].lower() and
keyword.lower() in logs[j]["message"].lower():
                        correlated.append((logs[i], logs[j]))
                else:
```

```
                correlated.append((logs[i], logs[j]))
    return correlated

if __name__ == "__main__":
    log_file = input("Enter log file path: ")

    logs = parse_logs(log_file)
    print(f"\nTotal log entries captured: {len(logs)}")

    keyword = input("Enter keyword to correlate (or press Enter to skip): ")
    correlated_events = correlate_events(logs, keyword=keyword if
keyword else None, time_window=10)

    print(f"\nCorrelated Events (within 10 min window):
{len(correlated_events)}\n")
    for e1, e2 in correlated_events:
        print(f"[{e1['timestamp']}] [{e1['level']}] {e1['message']}")
        print(f"[{e2['timestamp']}] [{e2['level']}] {e2['message']}")
        print("---")
```

Output :

sample.log :

```
[2025-09-21 14:30:10] [INFO] System started
[2025-09-21 14:32:15] [ERROR] Disk space low
[2025-09-21 14:34:50] [WARNING] CPU usage high
[2025-09-21 14:36:00] [ERROR] Disk space low
[2025-09-21 14:45:20] [INFO] User login
```

```
Enter log file path: sample.log
Total log entries captured: 5
Enter keyword to correlate (or press Enter to skip): disk

Correlated Events (within 10 min window): 1

[2025-09-21 14:32:15] [ERROR] Disk space low
[2025-09-21 14:36:00] [ERROR] Disk space low
---
```