Introduction to Computer Security

Detection-Phase 5

Team Members:

Pooja Peechara - 11663837

Rachana Reddy Sunki - 11709719

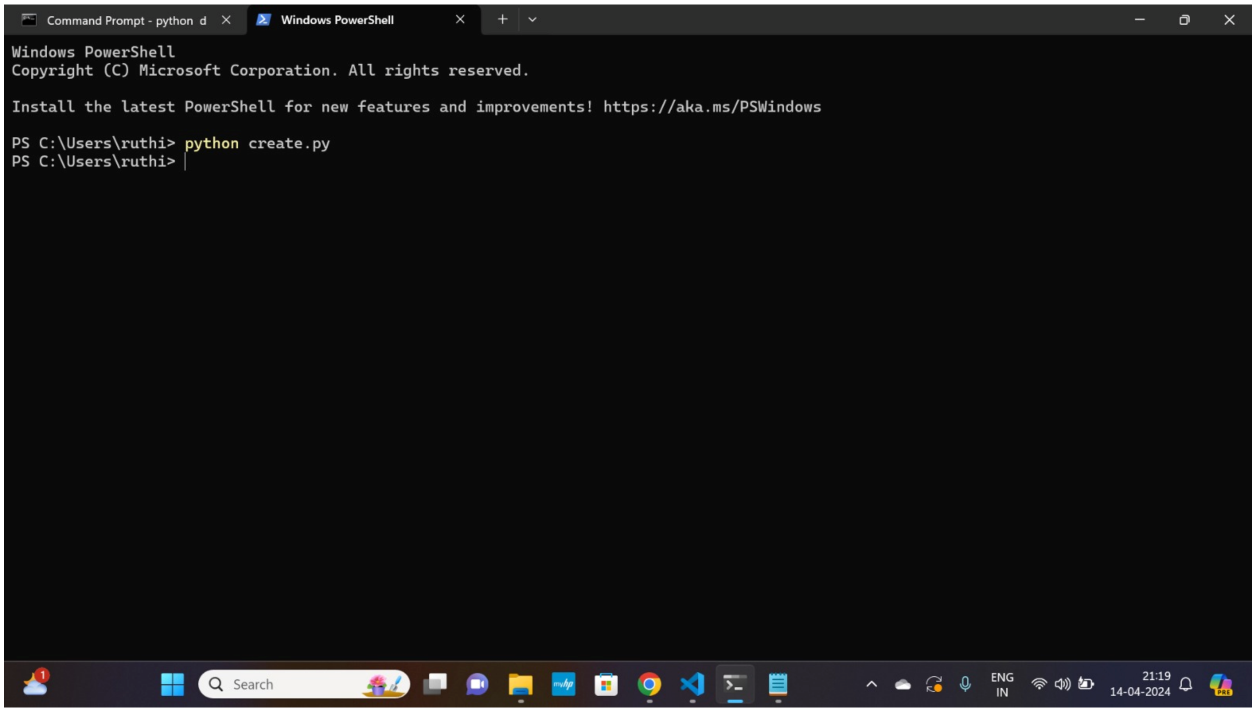
Mounika Nuchu - 11653658

Lagadapati Kondarao - 11661743

Yenugu Ruthiksha Reddy - 11714976

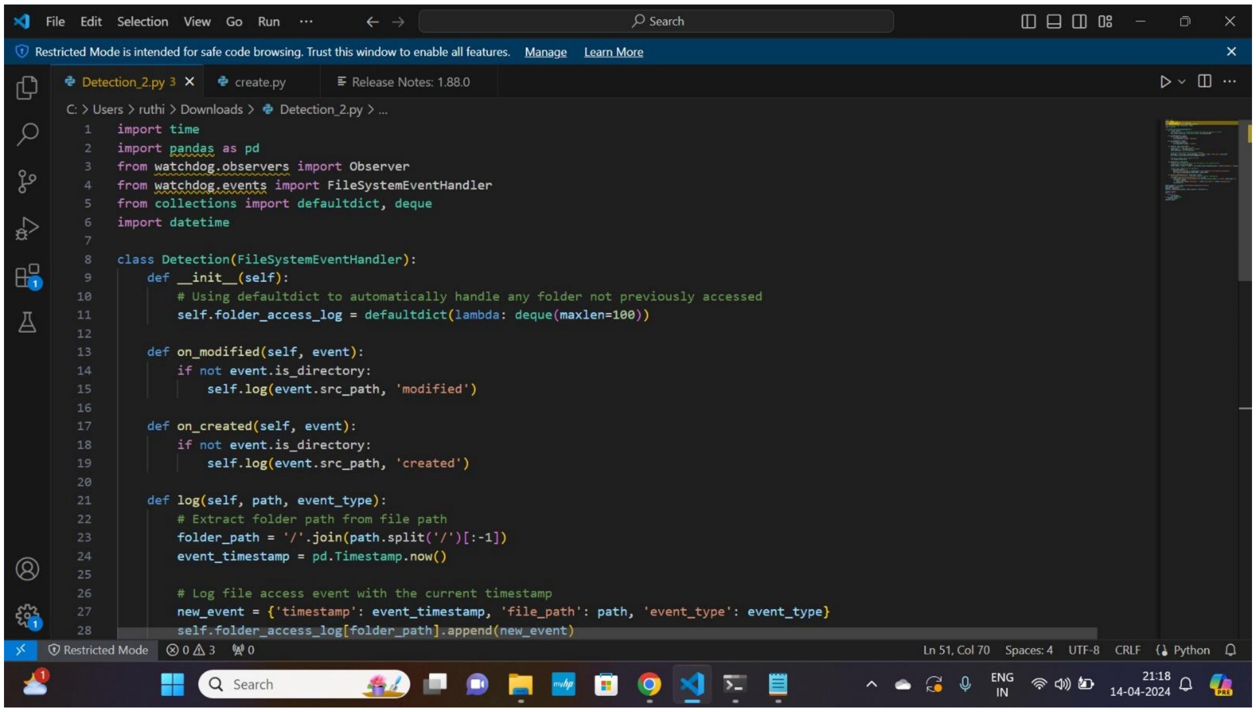
Introduction: In the previous phases we have monitored the logs by using the Python Library Watchdog. Here, We will be detecting the unusual activities based on the investigation performed on the files.

To create an unusual activity from different sources, we have created a file named create.py



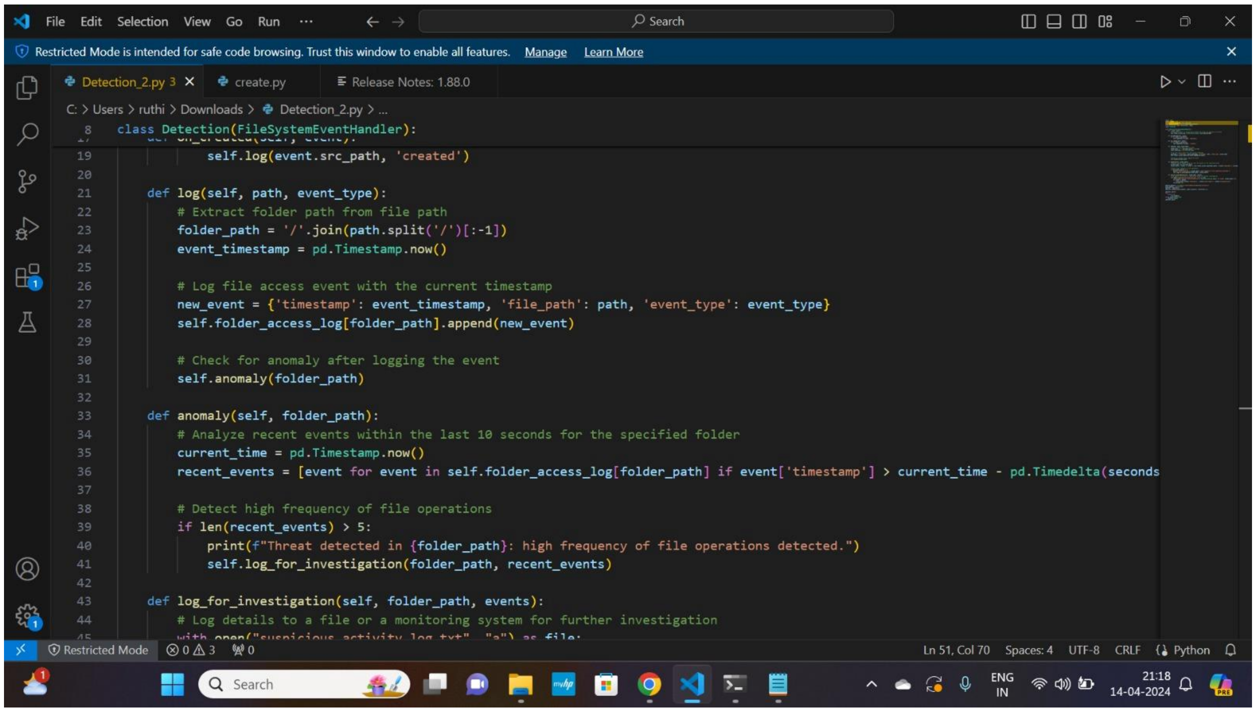
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ruthi> python create.py
PS C:\Users\ruthi>
```

Code:-


Detection_2.py 3
create.py
Release Notes: 1.88.0
C: > Users > ruthi > Downloads > Detection_2.py > ...
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
Ln 51, Col 70 Spaces: 4 UTF-8 CRLF Python

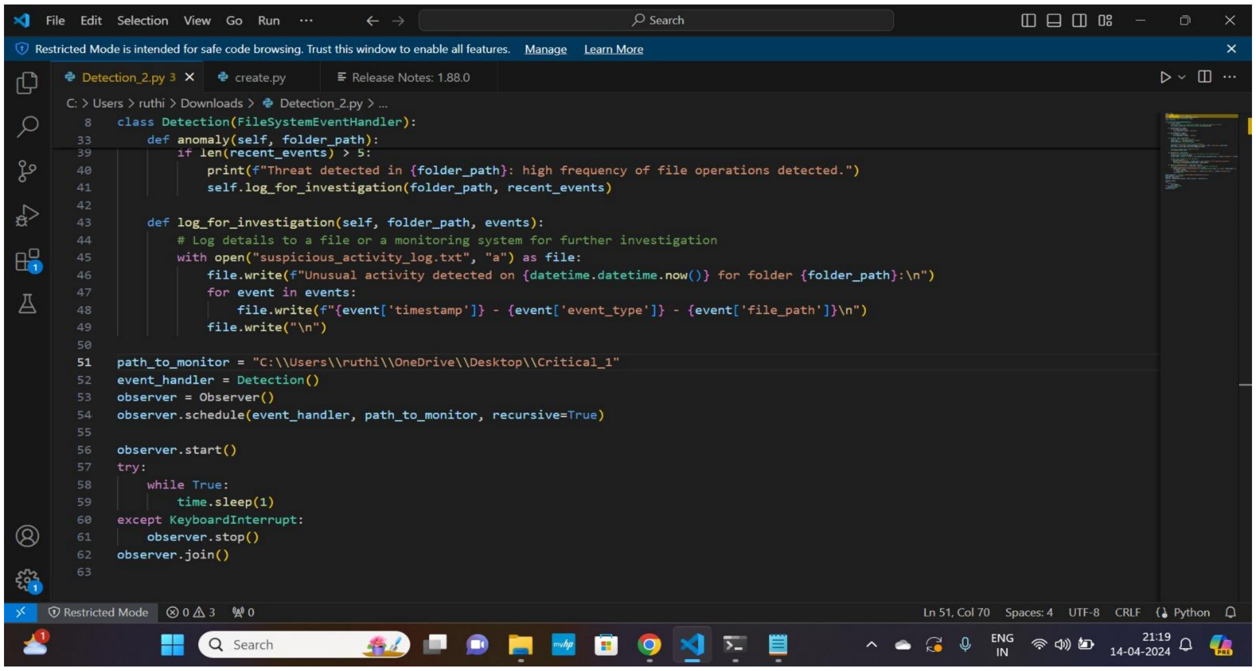
```python
import time
import pandas as pd
from watchdog.observers import Observer
from watchdog.events import FileSystemEventHandler
from collections import defaultdict, deque
import datetime

class Detection(FileSystemEventHandler):
    def __init__(self):
        # Using defaultdict to automatically handle any folder not previously accessed
        self.folder_access_log = defaultdict(lambda: deque(maxlen=100))

    def on_modified(self, event):
        if not event.is_directory:
            self.log(event.src_path, 'modified')

    def on_created(self, event):
        if not event.is_directory:
            self.log(event.src_path, 'created')

    def log(self, path, event_type):
        # Extract folder path from file path
        folder_path = '/'.join(path.split('/')[:-1])
        event_timestamp = pd.Timestamp.now()

        # Log file access event with the current timestamp
        new_event = {'timestamp': event_timestamp, 'file_path': path, 'event_type': event_type}
        self.folder_access_log[folder_path].append(new_event)
```

2)


Detection_2.py 3
create.py
Release Notes: 1.88.0
C: > Users > ruthi > Downloads > Detection_2.py > ...
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
Ln 51, Col 70 Spaces: 4 UTF-8 CRLF Python

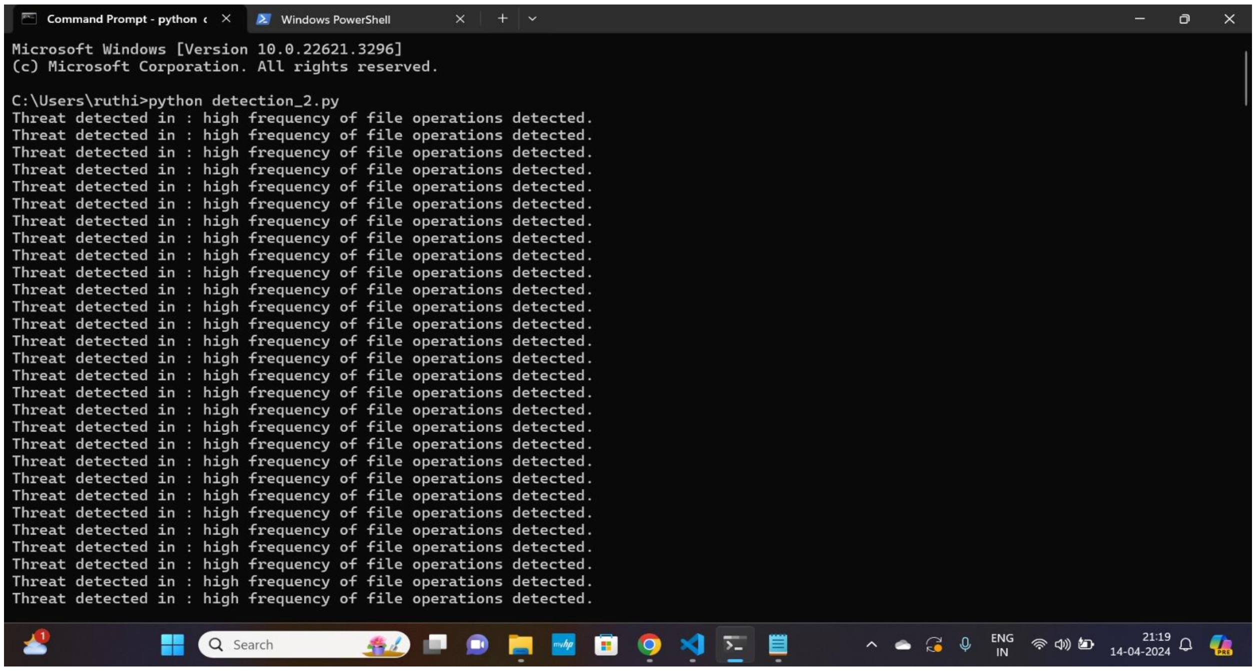
```python
class Detection(FileSystemEventHandler):
            self.log(event.src_path, 'created')

    def log(self, path, event_type):
        # Extract folder path from file path
        folder_path = '/'.join(path.split('/')[:-1])
        event_timestamp = pd.Timestamp.now()

        # Log file access event with the current timestamp
        new_event = {'timestamp': event_timestamp, 'file_path': path, 'event_type': event_type}
        self.folder_access_log[folder_path].append(new_event)

        # Check for anomaly after logging the event
        self.anomaly(folder_path)

    def anomaly(self, folder_path):
        # Analyze recent events within the last 10 seconds for the specified folder
        current_time = pd.Timestamp.now()
        recent_events = [event for event in self.folder_access_log[folder_path] if event['timestamp'] > current_time - pd.Timedelta(seconds

        # Detect high frequency of file operations
        if len(recent_events) > 5:
            print(f"Threat detected in {folder_path}: high frequency of file operations detected.")
            self.log_for_investigation(folder_path, recent_events)

    def log_for_investigation(self, folder_path, events):
        # Log details to a file or a monitoring system for further investigation
        with open("suspicious_activity_log.txt", "a") as file:
```

3)



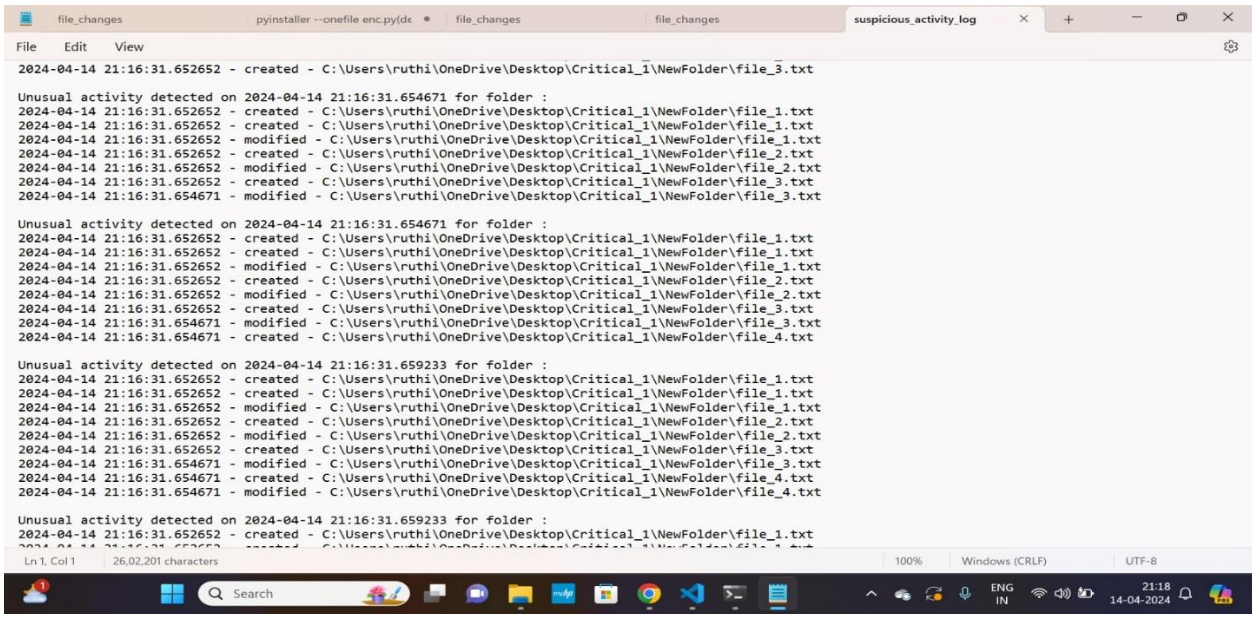
```python
class Detection(FileSystemEventHandler):
    def anomaly(self, folder_path):
        if len(recent_events) > 5:
            print(f"Threat detected in {folder_path}: high frequency of file operations detected.")
            self.log_for_investigation(folder_path, recent_events)

    def log_for_investigation(self, folder_path, events):
        # Log details to a file or a monitoring system for further investigation
        with open("suspicious_activity_log.txt", "a") as file:
            file.write(f"Unusual activity detected on {datetime.datetime.now()} for folder {folder_path}:\n")
            for event in events:
                file.write(f"{event['timestamp']} - {event['event_type']} - {event['file_path']}\n")
            file.write("\n")

path_to_monitor = "C:\\Users\\ruthi\\OneDrive\\Desktop\\Critical_1"
event_handler = Detection()
observer = Observer()
observer.schedule(event_handler, path_to_monitor, recursive=True)

observer.start()
try:
    while True:
        time.sleep(1)
except KeyboardInterrupt:
    observer.stop()
observer.join()
```

In our code, we have imported the watchdog library along with creation of a new class called as Detection from the FileSystemEventHandler present in the watchdog module.



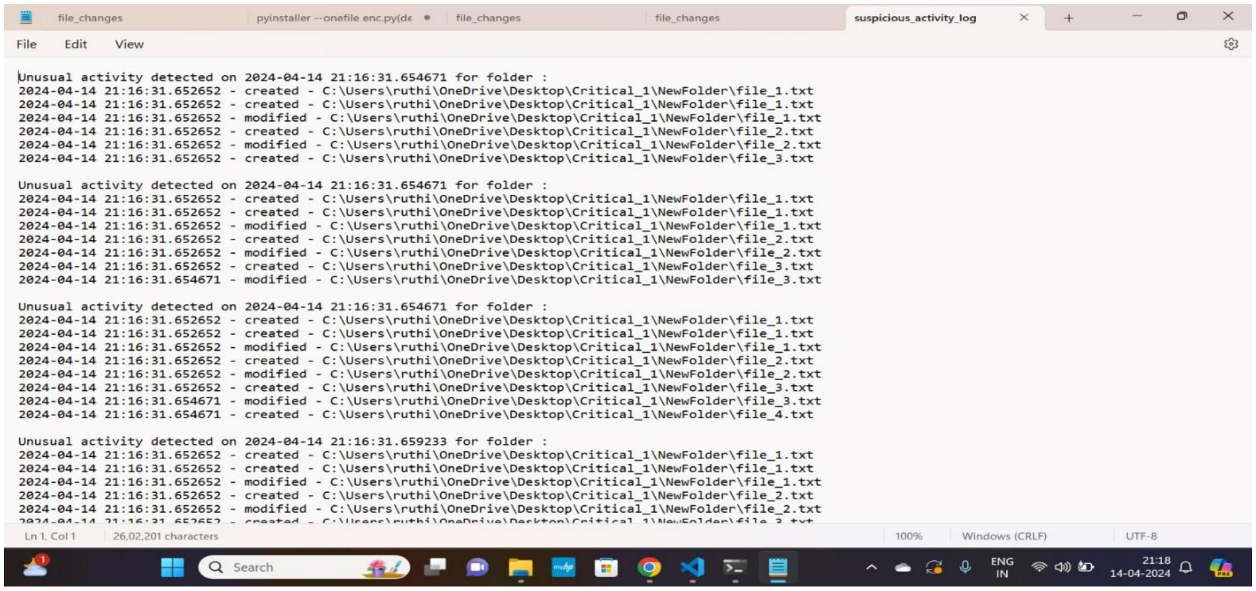
```
Microsoft Windows [Version 10.0.22621.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ruthi>python detection_2.py
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
Threat detected in : high frequency of file operations detected.
```

In the logs, we have initialized a method named as anomaly which checks for any anomalies by scanning the File operations. Based on the conditions which we have given, the high frequency of events is called as a threat to the device and then it calls a method called as log_for_investigation when the frequency of the events are more.



```
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt

Unusual activity detected on 2024-04-14 21:16:31.654671 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt

Unusual activity detected on 2024-04-14 21:16:31.654671 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_4.txt

Unusual activity detected on 2024-04-14 21:16:31.659233 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_4.txt
2024-04-14 21:16:31.654671 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_4.txt

Unusual activity detected on 2024-04-14 21:16:31.659233 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
```

Then, the logs are entered in the Suspicious activity_log.txt file where it has the event type, timestamp, and the file path of the suspicious event.



```
Unusual activity detected on 2024-04-14 21:16:31.654671 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt

Unusual activity detected on 2024-04-14 21:16:31.654671 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt

Unusual activity detected on 2024-04-14 21:16:31.654671 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_3.txt
2024-04-14 21:16:31.654671 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_4.txt

Unusual activity detected on 2024-04-14 21:16:31.659233 for folder :
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_1.txt
2024-04-14 21:16:31.652652 - created - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
2024-04-14 21:16:31.652652 - modified - C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder\file_2.txt
```

Conclusion:- By implementing this phase, we have developed script which displays the logs of the suspicious threats by detecting the high frequency of the files modifications/changes. The log file has the logs of each detected events until the code is run again.