**Step 4**

In this **step4 Monitoring**, we implemented a component designed to detect the ransomware activities within a specified environment. Our goal was to monitor file changes (like creation, modification, deletion) and log the data to a structured file and specifically a SQLite database that to facilitate ransomware detection. We used UTM virtual machine to execute the python code and create sql database.

**Tools and Libraries we used for this step4**

* Python programming
* Watchdog library for monitoring the file system changes.
* SQLite3 database for structured logging.

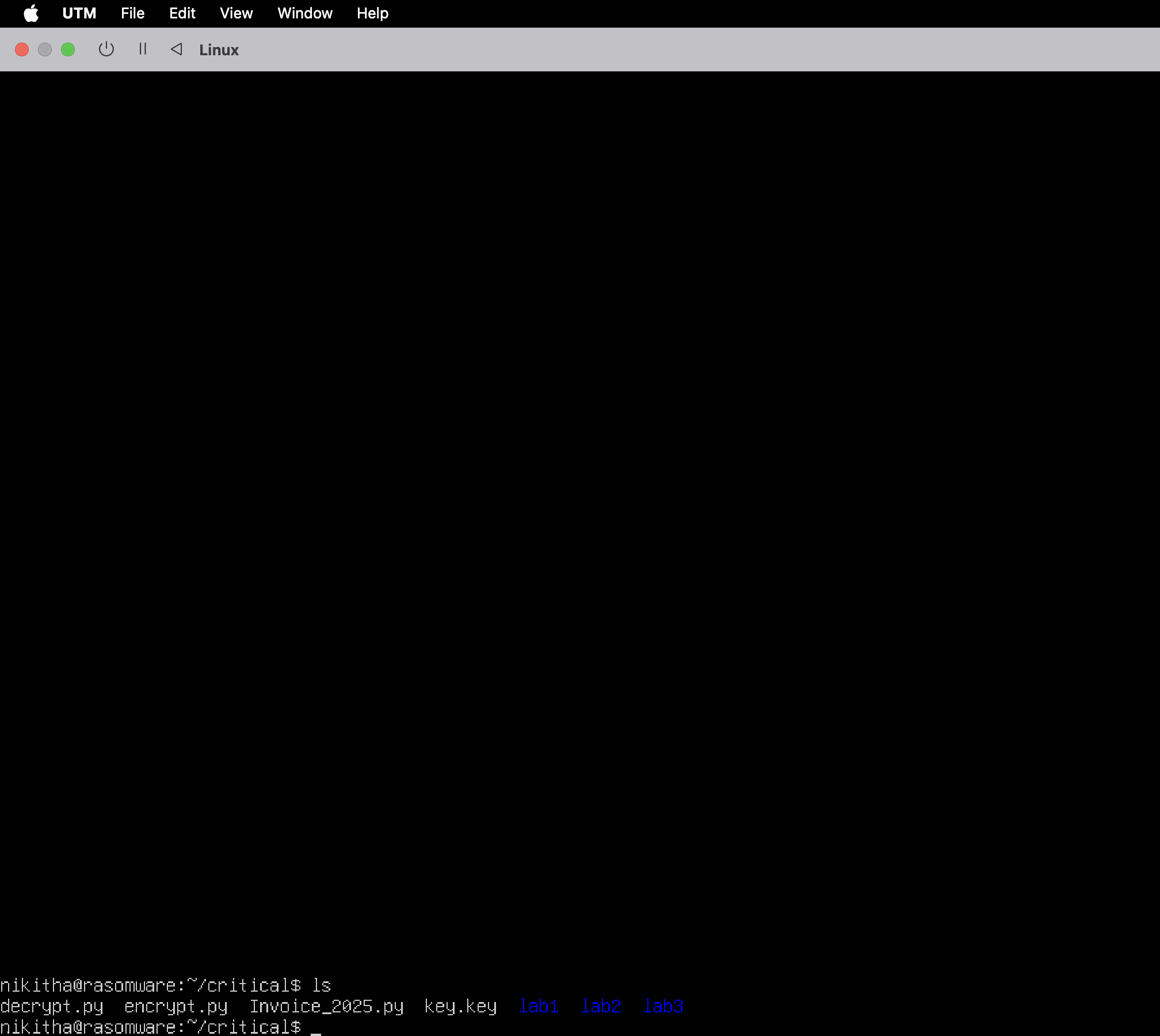
**Implementation Process:**

* The monitoring script continuously watches the specified directory and It also uses a custom file event that detects three types of file events like creation, modification, and deletion to the database.
* And each detected event is logged with a timestamp, event type, and the file path. The data is stored in a Sqlite database (**monitor.db)** for the future analysis and incident response as well.
* Since the file system events that are captured asynchronously and we ensured that the database operations are handled correctly to avoid any threading issues.

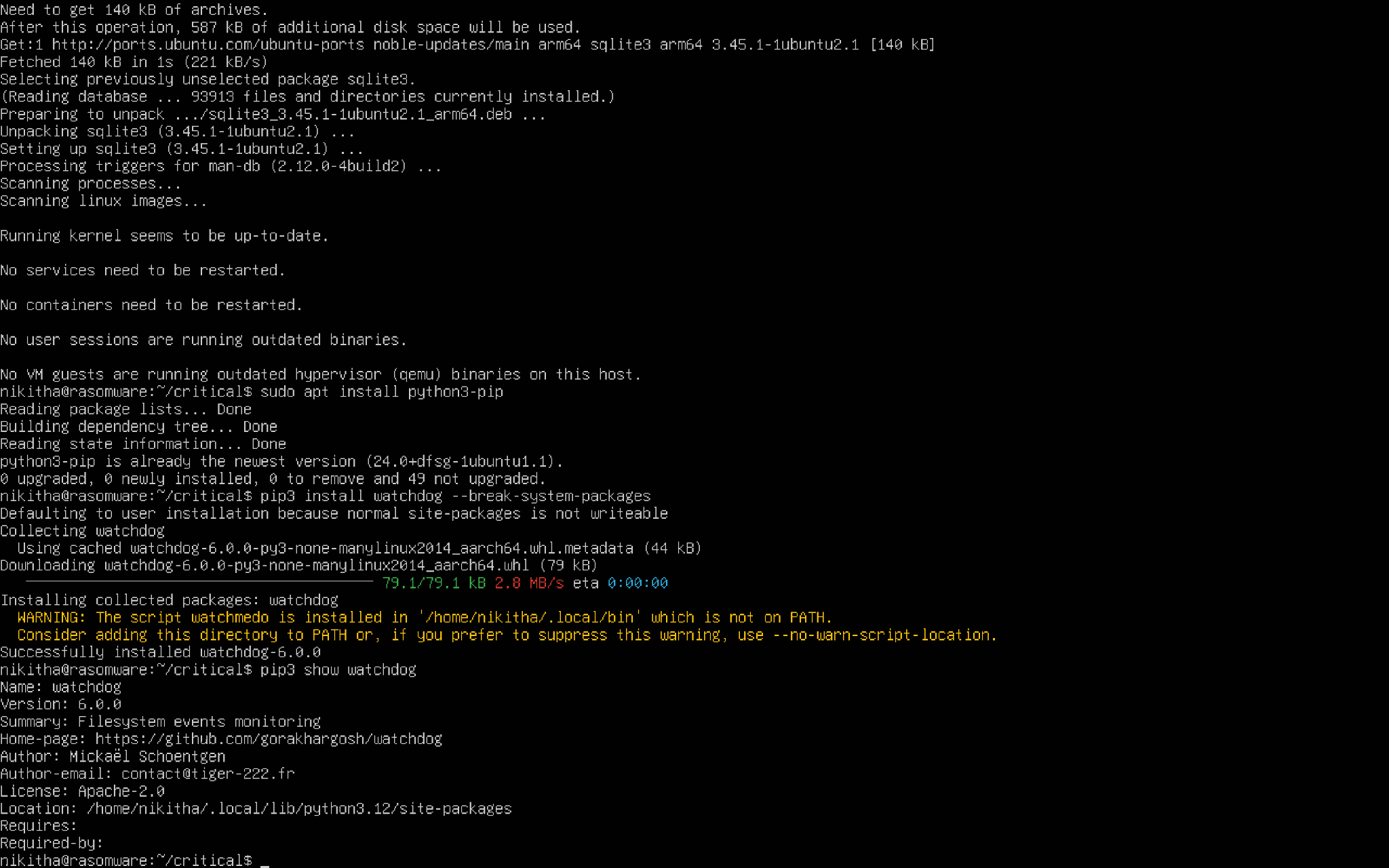
The logs data were verified both in the terminal output and in the database using the below sql command

SELECT \* FROM file\_events;

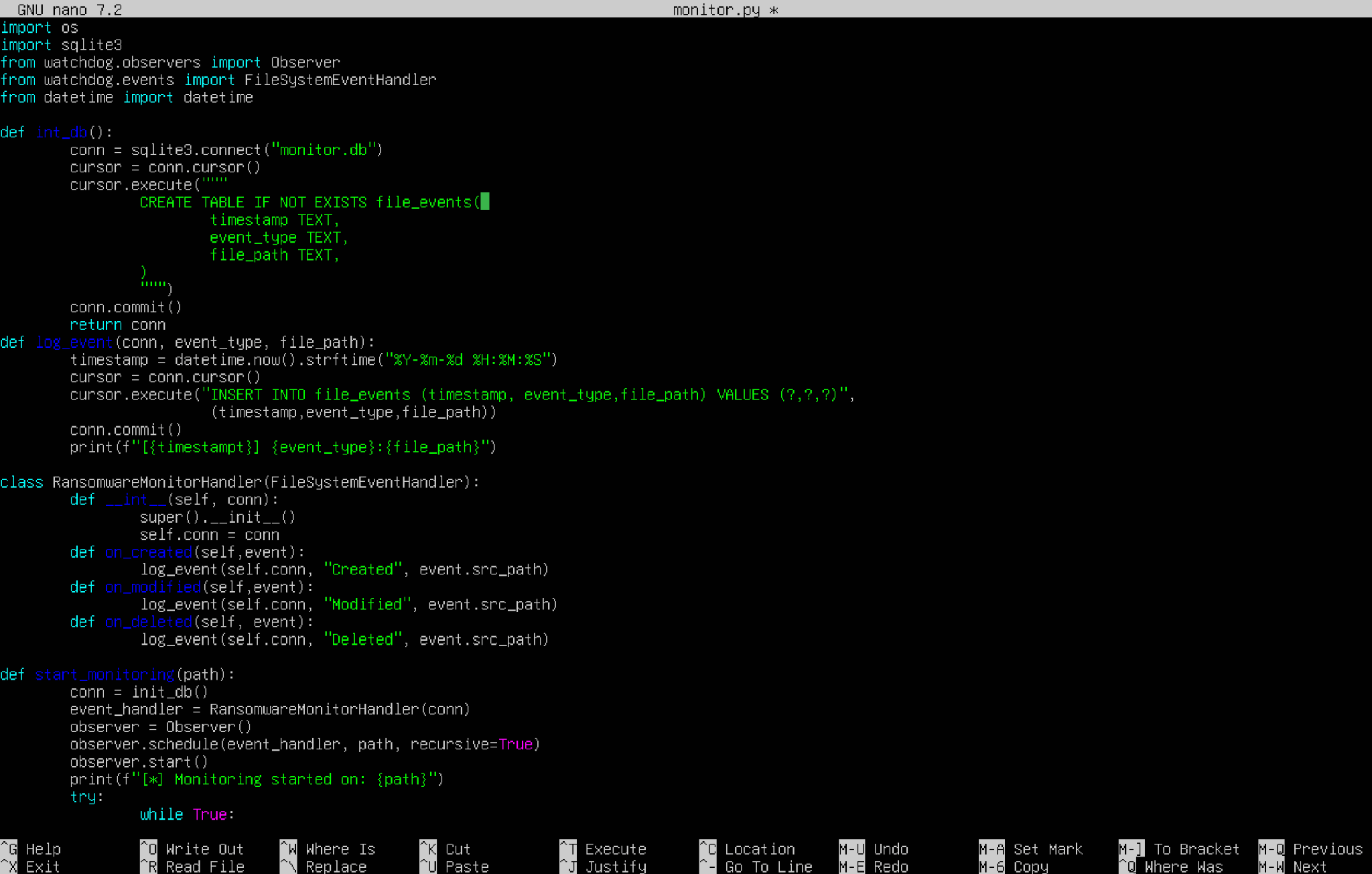
Open UTM to run the python file

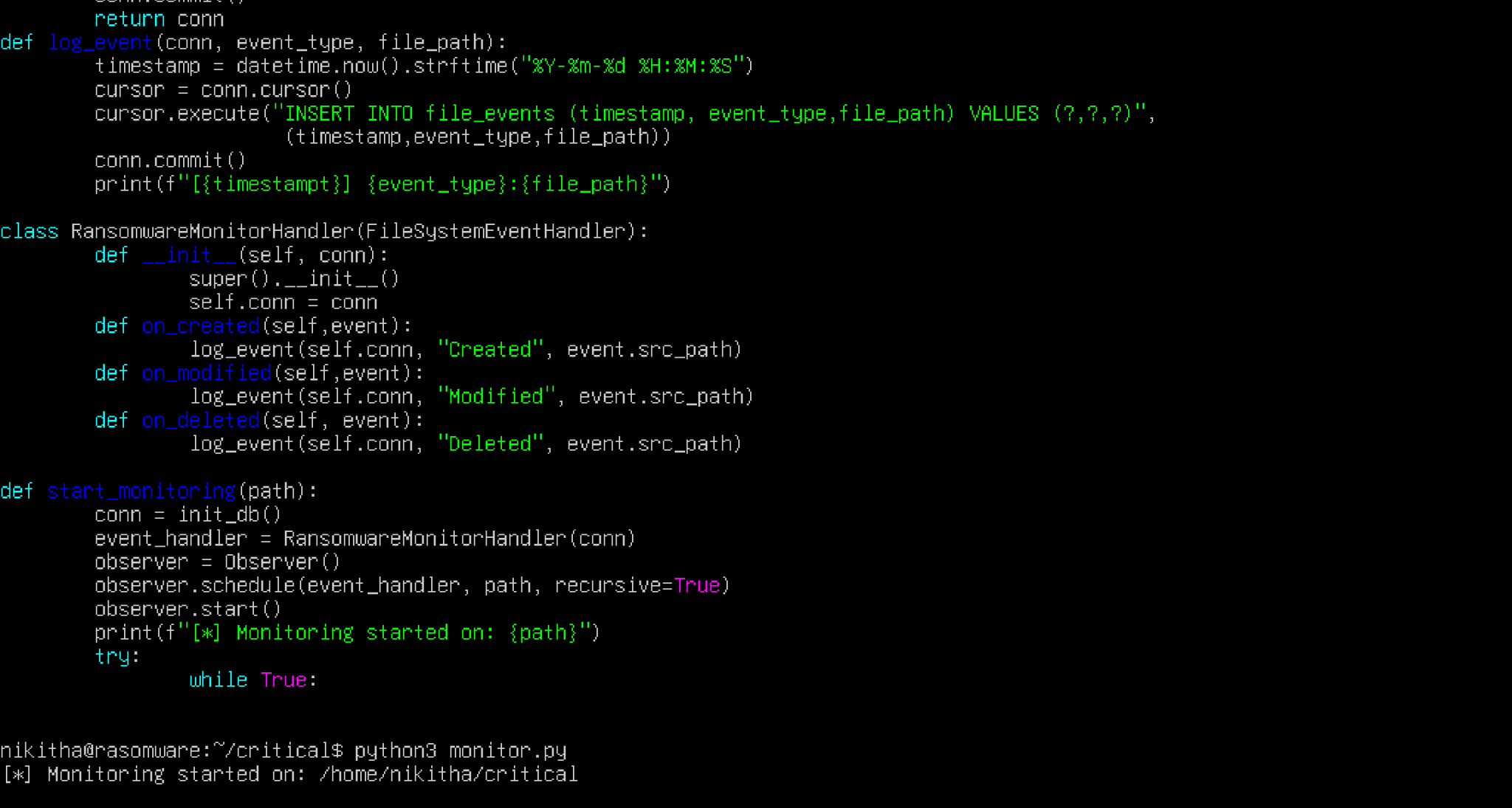


Installed watchdog library

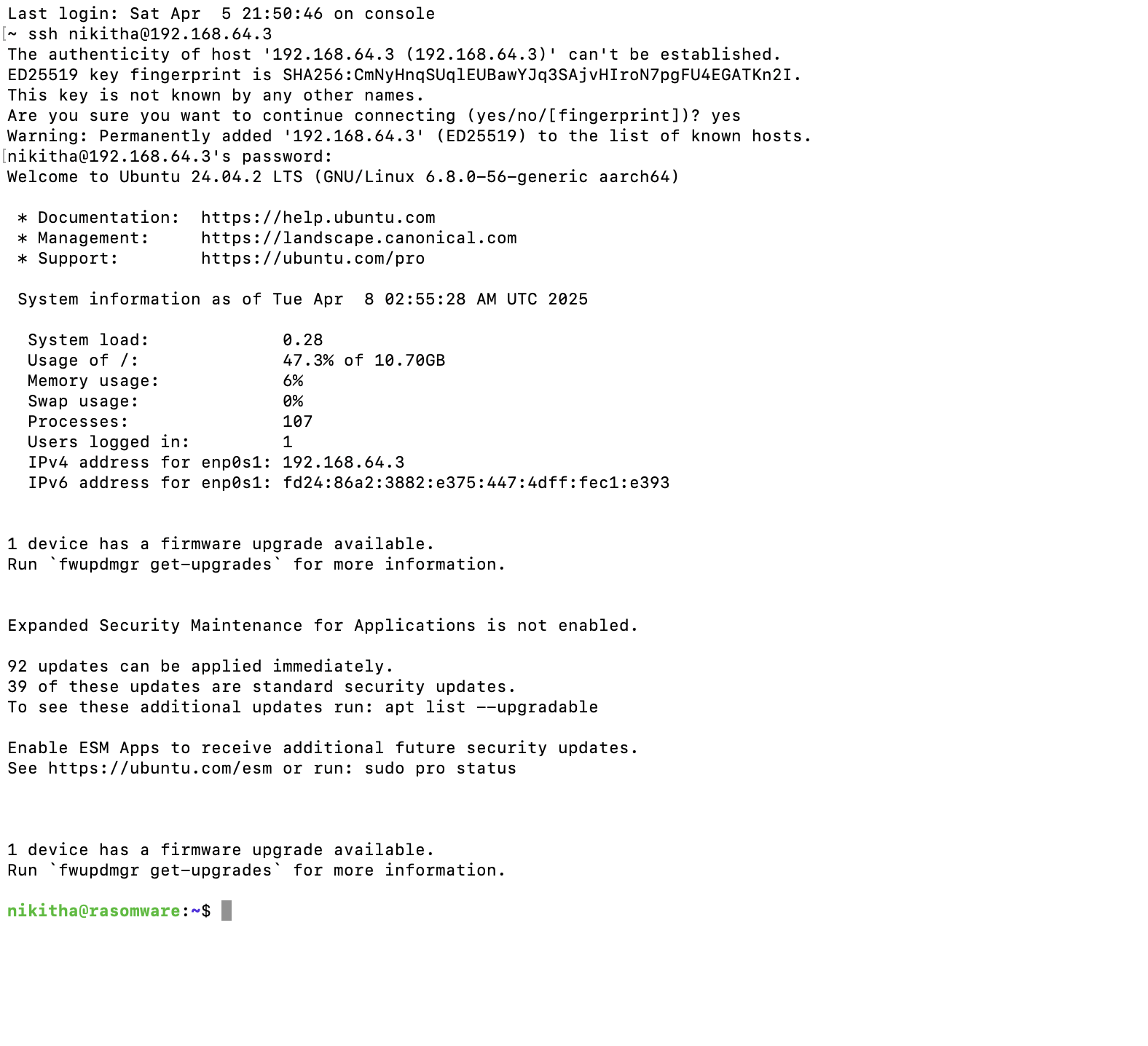


Python code





Connect virtual machine in local and run the text file against to that



Monitoring the logs

