**SUKKUR IBA UNIVERSITY**

**Cyber security**

**LAB# 02**

**Class: BS-VIII Course Instructor: Sir Zakria**

**Candidate Name: Muhammad Yamin CMS: 021-19-0029**

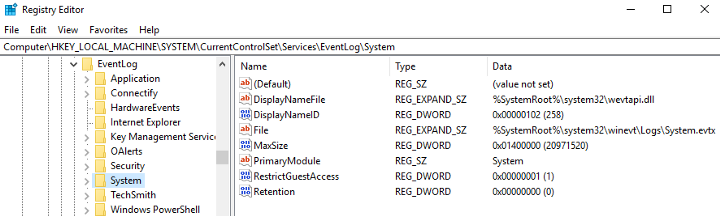
Windows Event Viewer

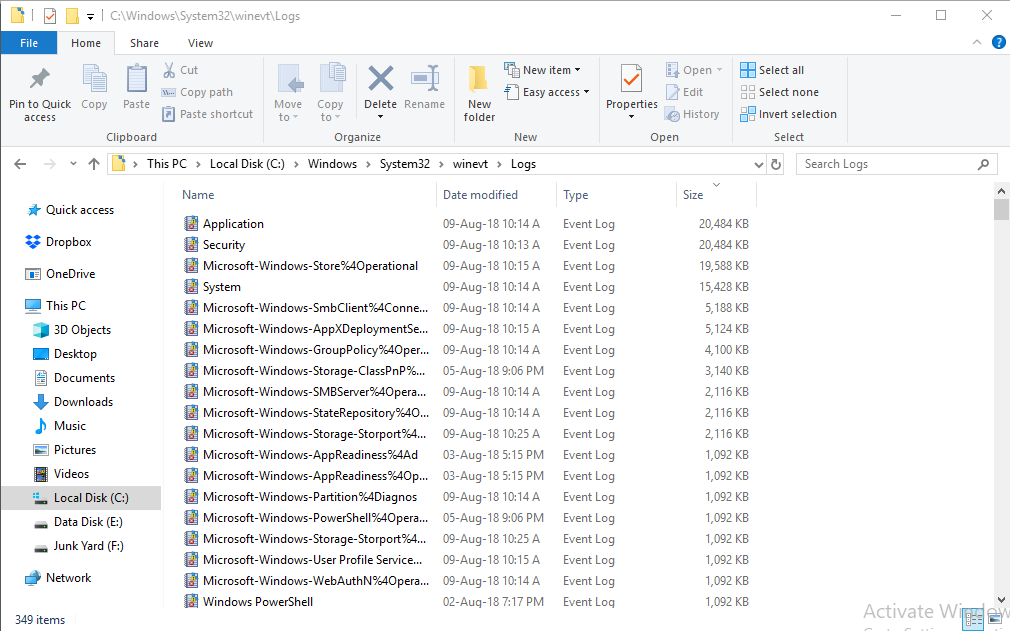
All Windows versions have the Windows Event Viewer as an administrative tool. It enables you to see events, faults, and other crucial data about what's going on inside your operating system. When you use Windows, the operating system maintains a log of significant and helpful data regarding what is occurring on the computer. The Windows Event Log is a collection of many logs that houses this data.

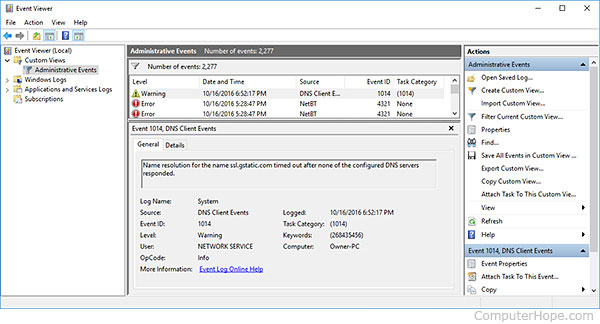
How Windows Event Viewer can be used in cyber forensic?

Windows Event Logs are the main source of evidence in forensic investigations because the operating system records all system operations. An investigator can create a timeline using the logging data and found artefacts by analyzing the Windows Event Log. Event logs can be disabled with administrative access since the information that needs to be logged relies on the audit features being enabled. The Event Logs capture a lot of information from a forensic perspective. In forensics, a history of events is reconstructed using the Windows Event Logs.

Event logs typically consist of these three elements:

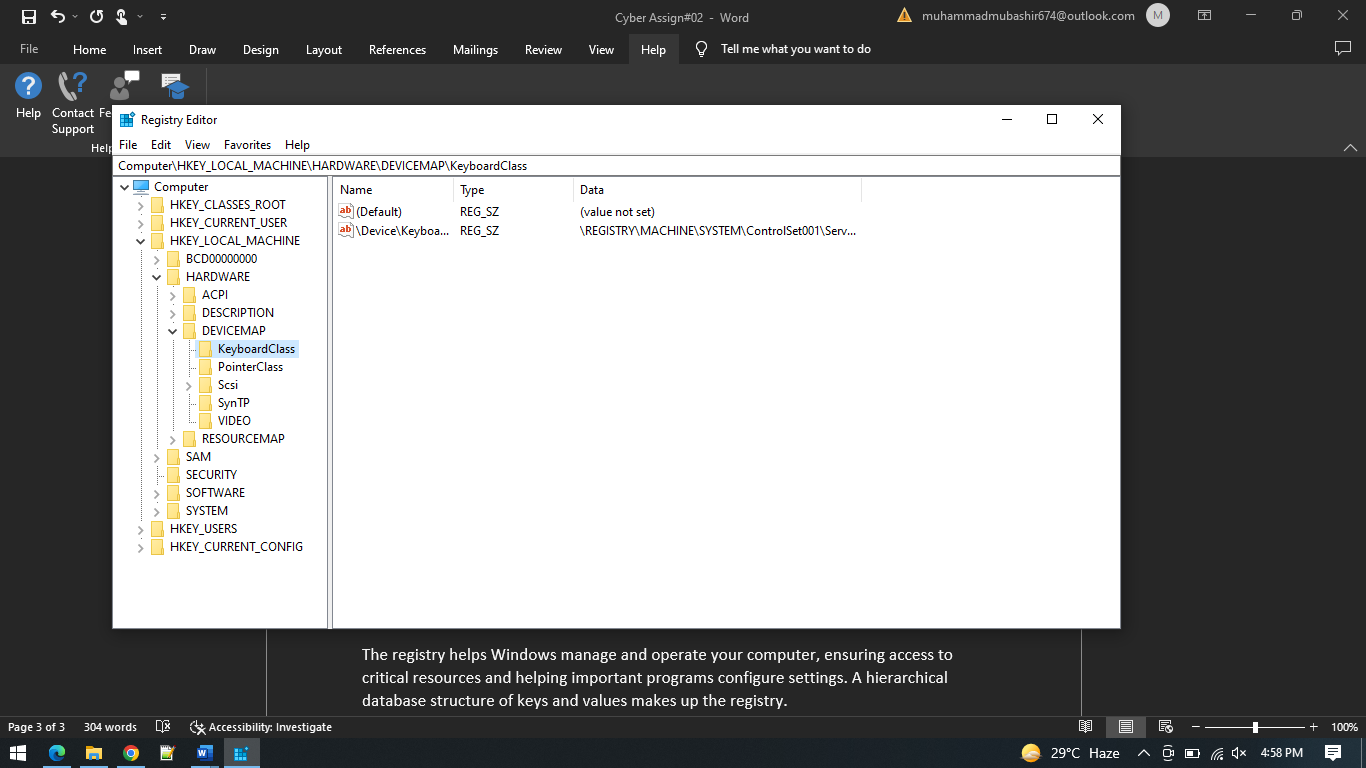
1. Application
2. System
3. Security



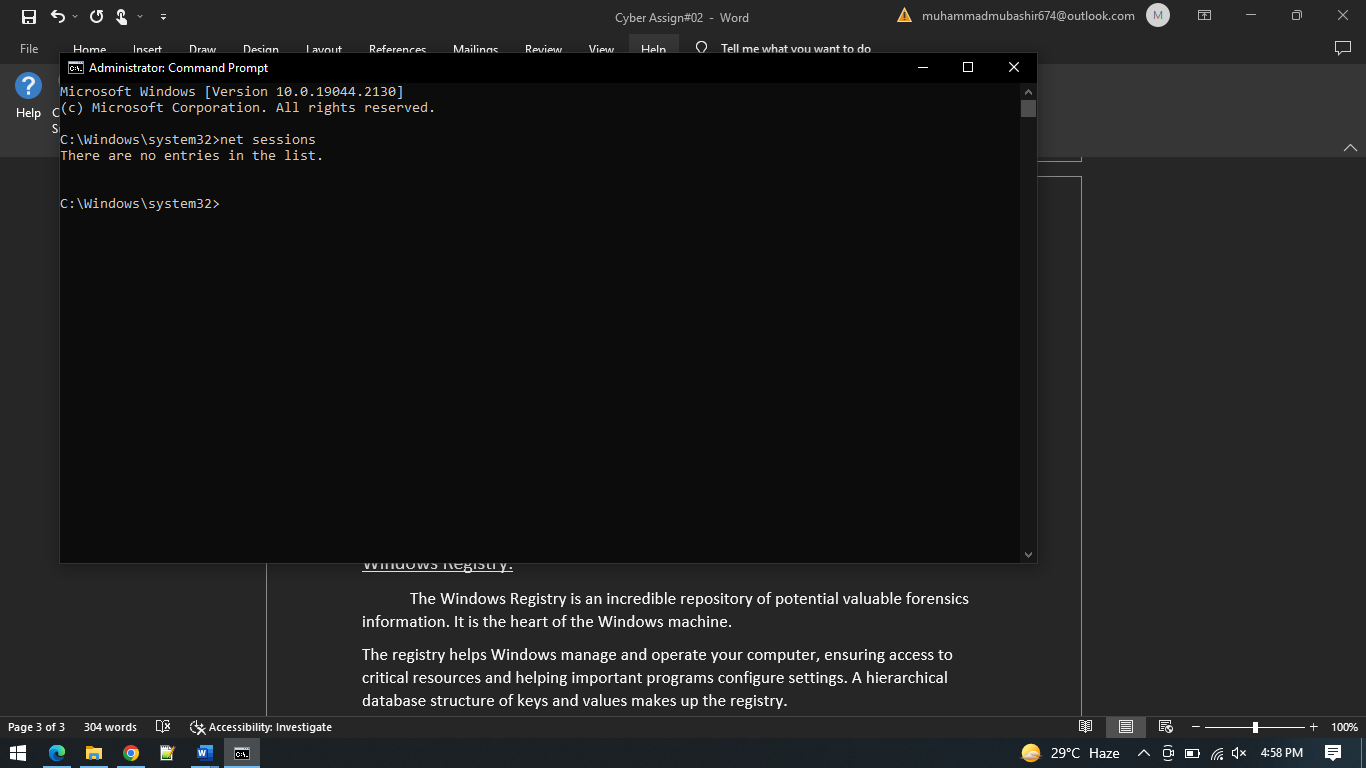


Task 2

Windows registry

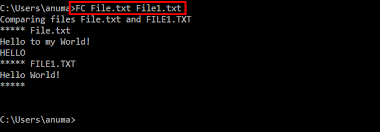


Net Sessions



FC:

You can use the command Fc with a forensic copy of a computer. It contrasts two files and displays the variations. You can contrast a configuration file with a known-good backup if you suspect a change has been made.

****