SysMon Logger (User Interface)

The User Interface (UI) is split into two sections; Events and Data. The

Events

The Events tab shows a unified view of all event types that have occurred. The events are in chronological order, with the most recent first

Data

The Data section is split into a event specific view. Each view shows the events that are specific to one data/event type. The types configured are:

- Process Create
- Process Terminate
- Network Connection
- File Creation Time
- Driver Loaded
- Image Loaded
- Raw Access Read
- Create Remote Thread