Upload Monitor Tool – Design

1. **Event Sources (Windows Kernel ETW Providers)**
    - **File I/O Provider** -> Notifies when a file is read/written.
    - **TCP/IP Provider** -> Notifies when data is sent over network.
2. **Event Collector / Callback**
    - EventCallback function receives real-time events.
    - Separates events into **File events** and **Network events**.
3. **Data Tracking Structures**
    - **FileSlot** -> Stores per-PID file info (path, bytes transferred, timestamp).
    - **NetSlot** -> Stores per-PID network info (remote IP/port, bytes, timestamp).
    - **Hash Table** -> Maps FileObject → file path for quick lookups.
4. **Detection Engine**
    - Correlates **File I/O** and **Network send** events by PID.
    - Applies thresholds:
        Minimum file size: 8 KB
        Time window: 20 seconds
    - Ignores system/junk files.
5. **Output / Logging**
    - Console: prints detected uploads in real-time.
    - File: appends logs to uploads.log.