Analyzing, filtering, and searching event log and syslog output/Collecting and validating digital evidence