

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

The image displays two screenshots of a virtual lab environment, likely running on a web browser. The top screenshot shows a desktop environment with a blue background and the "Security Onion" logo. The desktop contains several icons: "Squid", "Squert", "Kibana", "CyberChef", "Setup", and "README". A taskbar at the bottom shows the time as "Mon 03:56" and the temperature as "2°C Clear". The right sidebar of the browser window shows the lab title "07: Analyzing, Filtering, and Searching Event Log and s" with a progress bar at 100% and a section titled "End Lab" with instructions.

The bottom screenshot shows a desktop environment with a dark blue background. The desktop contains several icons: "Recycle Bin", "Notepad++", "Microsoft Edge", "Autopsy 4.10.0", "PuTTY", "Heavy Load", "SilentEye", "LABFILES", "Webserver Stress", "Microsoft Baseline S...", "WinSCP", "Mozilla Thunderbird", "Wireshark", "NetStress", and "Zenmap - GUI". A taskbar at the bottom shows the time as "22:00" and the temperature as "2°C Clear". The right sidebar of the browser window shows the lab title "08: Collecting and Validating Digital Evidence" with a progress bar at 100% and a section titled "End Lab" with instructions.