Process Flow: Acquisition & Preservation of Sysdiagnose and Apple Unified Log

Category	Sysdiagnose	Apple Unified Log
Purpose	Snapshot of system state	Detailed timeline of events and logging
Initiation	`sudo sysdiagnose` or key combination	`sudo log collect --device --output /path/to/name.logarchive`
File size	300 MB – 1 GB+	100 MB – several GB depending on logging duration
Analysis tools	Forensic license tools, grep, custom scripts, etc.	Forensic license tools, `log` command, custom scripts, Consolation3, etc.
Content	Bundle with log files, crash reports, sysdiagnose, network status, battery, kernel logs, etc.	Detailed, chronological logs of system and app activities, including subsystem events
Time source	System clock (RTC) at snapshot moment	System clock and monotonic time
Timestamps	YYYY-MM-DD HH:MM:SS +0000	YYYY-MM-DD HH:MM:SS.ns (nanoseconds) +0000
Timeline structure	Limited, fragmented	Fully chronological, nanosecond precision
Time analysis	Limited	Excellent
Forensic information	Configuration, app usage, power logs, network diagnostics, crash logs	User interaction, process start/stop, system state changes, authentication events, nanosecond logs
Privacy display	May contain raw strings	Privacy labels visible