Dynamic Analysis Report - Impl14 (SOCP Chat Client)

1. Execution Context

Container: run-impl14
Environment: Non-root Docker sandbox, network disabled (--network=none), Python 3.11 on Debian bookworm slim.
Execution time: 60 seconds (timeout 60s)
Main entry: client.py detected automatically.
Goal: Run client in isolation to inspect system-call, file-activity, and port behavior.

2. File-System Activity (from inotify.log)

During execution, the program compiled several modules under __pycache__ (utils.py, cli_crypto.py, server_keys.py, envelope.py, etc.). The client created and repeatedly modified a local SQLite database socp.db and its journal file socp.db-journal, then cleaned them up (delete + re-create cycles). This indicates message persistence or key-exchange records.

No writes occurred outside /home/auditor/app, ensuring sandbox containment.
No new executables or system directories were touched.
Verdict: File operations confined, behavior expected for local DB caching.

3. Network Activity (from ss.txt)

No established connections or external sockets were observed. Only loopback initialization (127.0.0.1 or ::1) entries appeared transiently. No outbound HTTP/WS/TCP traffic, confirming network isolation (--network=none) was effective.
Verdict: No leakage or unintended external contact.

4. System-Call Trace (from strace_log.18)

Frequent openat() and read() system calls on .py and .pyc files were observed—normal for Python imports. Numerous write() and fsync() operations targeted socp.db and socp.db-journal, consistent with SQLite use.
No connect() calls to external IPs and no fork()/execve() process spawning were detected.
The program terminated cleanly after timeout without errors or zombie processes.
Verdict: Stable I/O behavior, no privilege escalation attempts.

5. Security Observations

Category	Observation	Severity
Execution Control	Program starts & ends normally (timeout clean).	None
File I/O	Only socp.db under app path is modified.	None

Network I/O	No external traffic or listening ports.	None
Process Control	No child processes or shell invocations.	None

6. Overall Assessment

Behavior: Benign — client performs local DB transactions only.

Security posture: Strong — no network leak, no unauthorized writes.

Reliability: Stable — predictable I/O cycle, clean shutdown.

7. Recommendations

1. Keep DB path inside sandbox (./socp.db); avoid absolute paths in production.

2. Add explicit exception handling around SQLite operations to prevent corruption on sudden shutdown.

3. Maintain network isolation for future tests to validate client logic safely.

4. Regularly inspect socp.db schema for sensitive data (potential key storage).