

Part 1 — Lab Answers

Reference solutions for the lab exercises. Use these only after attempting the exercises yourself.

Exercise 1 — Filesystem Timeline

Time zero is usually the first write in `%TEMP%` or `/tmp` of an executable. Timestamp-stomping shows as files with identical nanosecond values or 2000-01-01 defaults. Note the USN journal gaps — those indicate secure-delete attempts.

Exercise 2 — Memory Analysis

Malicious process often has: no parent, unusual path, `malfind` hit showing RWX pages, and a handle to `\Device\PhysicalMemory` or LSASS. Commands: `volatility -f mem.dmp --profile=Win10 malfind` then `procdump` on the suspect PID.

Exercise 3 — Event Log Analysis

Critical: Event 1102 (audit log cleared). Near it: 4688 for a suspicious binary, Sysmon EID 1 with the command line, EID 3 for the C2 connection, 7045 for a newly installed service or 4698 for a new scheduled task.

Exercise 4 — Network Forensics

Beacon interval ~60s, exfil via HTTPS POST to an IP-literal URL. Volume estimate: multiply the POST body size by the count. Detection rule: JA3 fingerprint for the attacker tool + SNI mismatch check.

Final Exercise — Forensic Report

Neutral language. Every finding has an evidence reference. Limitations section lists what you could NOT determine (e.g., data actually read by the attacker).

Part 2 — Homework Answers

Model answers for the homework tasks. Your solution may differ and still be correct.

Task 1 — Mini Evidence Collection

Folder with timestamped files, a manifest with SHA-256 hashes, and a chain-of-custody note. Even on your own system, the discipline matters.

Task 2 — Timeline Template

One sortable table with all sources. The critical minute should be highlighted or bolded. Sources should be identifiable at a glance.

Task 3 — Forensic Report

Court-style tone: no speculation, no adjectives like "obviously", every claim cites a line.