CS-103 · Digital Forensics

Log Analysis

Reading the records systems keep to reconstruct what happened and when.

Executive Summary

Log analysis is the practice of examining the records that systems, applications, and network devices generate to reconstruct events and detect problems. Logs are often the backbone of an investigation because they show who did what and when across many sources. Their value depends on collecting them completely, aligning their timestamps, correlating them, and preserving them so they can be trusted later.

What It Is

A log is a time-stamped record of an event, such as a login, a file access, a configuration change, a firewall decision, or an error. Log analysis brings these records together from operating systems, applications, servers, network devices, cloud services, and security tools, then reads them to understand behavior over time. Because a single event often leaves traces in several logs, analysis usually means correlating sources rather than reading one in isolation. A core output is a timeline that places events in order, which is why consistent, accurate time across systems is so important. Logs are also evidence, so how they are collected and preserved affects whether they can be relied upon.

Why It Matters

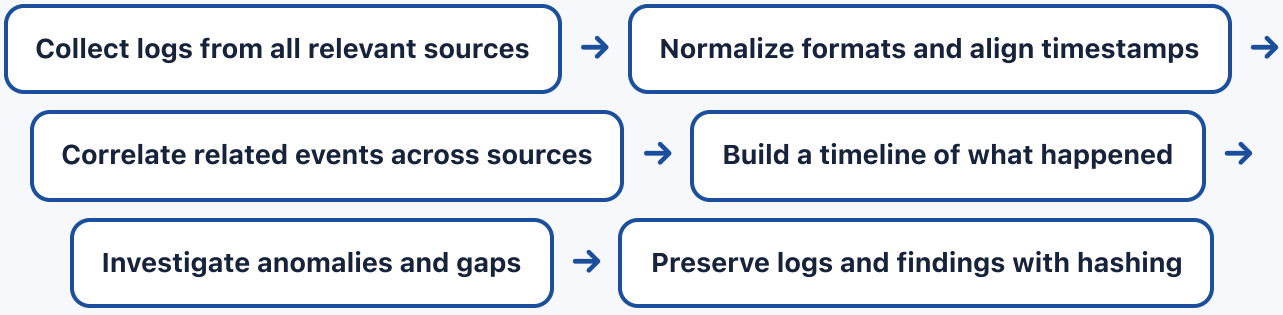
Logs frequently answer the central questions of an investigation: how an attacker got in, what they touched, and how far they moved. They also power detection, letting teams spot suspicious behavior before it becomes a full incident. Without good logging, an organization can be blind to a breach and unable to prove what happened after one. Gaps, inconsistent clocks, or logs that roll over too quickly can leave critical periods undocumented. For professionals, log analysis is

one of the most-used skills in security operations, incident response, and forensics, and fluency with it is expected across many roles.

How It Works

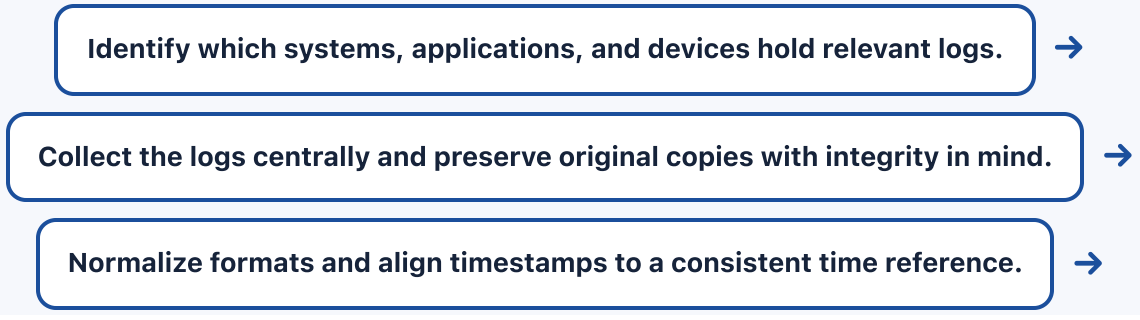
Log analysis works by gathering records, making them comparable, and connecting the dots. Collection centralizes logs from many sources, often into a system such as a SIEM, so they are searchable and retained. Normalization puts different formats into a common structure and, critically, aligns timestamps to a consistent time reference so events from different systems can be sequenced. Correlation then links related events across sources to reveal patterns, such as a login followed by privilege changes and data movement. For forensic use, the logs and the analysis are preserved with integrity in mind, including hashing exported records so they can be shown to be unchanged. Guidance such as NIST SP 800-86 treats log data as important evidence within incident response, and consistent time is emphasized because timelines depend on it.

Architecture Diagram



Logs become a defensible timeline once they are collected, time-aligned, correlated, and preserved with integrity.

Visual Workflow



Correlate related events across sources to surface patterns. →

Build a timeline and investigate anomalies, gaps, and outliers. →

Hash exported records and document the analysis so it can be reproduced.

Common Attacks

- Clearing or deleting logs to erase evidence of intrusion
- Disabling or tampering with logging so activity is never recorded
- Timestamp manipulation to confuse the sequence of events
- Flooding logs with noise to bury malicious activity
- Living-off-the-land techniques that blend in with normal logged behavior

Common Mistakes

- Analyzing one log source in isolation and missing the correlated picture
- Ignoring clock differences so the timeline is out of order
- Letting logs roll over or expire before they can be examined
- Collecting too little, leaving key systems unlogged
- Failing to preserve original logs, so their integrity cannot be shown

Best Practices

- Centralize logs from all relevant sources and retain them long enough
- Synchronize clocks and record time zones so timelines are accurate
- Correlate across sources rather than reading logs in isolation
- Preserve original logs and hash exported copies for integrity
- Monitor for gaps that suggest logging was disabled or cleared
- Document the analysis so another examiner can reproduce the timeline

Quick Checklist

- [x] Relevant sources identified and centrally collected
- [x] Clocks synchronized and time zones recorded
- [x] Logs retained long enough to cover the investigation window
- [x] Events correlated across sources into a timeline
- [x] Original logs preserved and exports hashed
- [x] Analysis documented and reproducible

Recommended Tools

SIEM
Centralizes, searches, and correlates logs from many sources

Log collector or forwarder
Gathers logs from systems and ships them to central storage

Timeline analysis tool
Orders events across sources to reconstruct what happened

Hashing utility
Fixes the integrity of exported log evidence

Industry Standards

NIST SP 800-86
Guide that treats log data as key evidence within incident response

NIST SP 800-92
Guidance on computer security log management

SWGDE best practices
Community guidance on handling and documenting digital evidence

Career Relevance

Log analysis is a daily skill for SOC analysts and incident responders, and it is essential to DFIR analysts and forensic investigators building timelines. It also supports detection engineers, auditors verifying activity, and privacy and AI governance professionals who assess how systems are monitored and how records prove accountability, the audience AI-Governance-Jobs.com serves.

Interview Questions

- Why is correlating multiple log sources more powerful than reading one in isolation?
- How do clock synchronization and time zones affect a forensic timeline?
- What would you look for in logs to investigate a suspected account compromise?
- How do you handle a gap in logs where logging appears to have been disabled?
- How do you preserve log evidence so its integrity can be shown later?

Related Certifications

GIAC Certified Incident Handler (GCIH) **GIAC Certified Forensic Analyst (GCFA)** **CompTIA CySA+**

Further Reading

- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-92: Guide to Computer Security Log Management
- CISA: Incident Response

Key Takeaways

- Logs reconstruct who did what and when across many systems.
- Correlation across sources reveals patterns a single log cannot.
- Accurate, synchronized time is what makes a timeline trustworthy.
- Missing, cleared, or disabled logs are themselves a warning sign.
- Preserve original logs and hash exports so the evidence holds up.

FAQ

▶ **Why is time synchronization so important for log analysis?**

▶ **What does it mean when logs are missing for a time window?**

▶ **How are logs kept defensible as evidence?**

Related Careers

RELATED ROLES

Dfir Analyst · Forensic Investigator · Incident Responder · Soc Analyst

RELATED CERTIFICATIONS

GIAC Certified Incident Handler (GCIH) · GIAC Certified Forensic Analyst (GCFA) · CompTIA CySA+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides · Role roadmaps · Salary data · Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Log Analysis**
3. Go deeper: Digital Evidence
4. Go deeper: Chain of Custody
5. Validate it: work toward **GIAC Certified Incident Handler (GCIH)**
6. Find the role: browse current openings

RELATED SHEETS

CS-099 Digital Evidence | CS-100 Chain of Custody | CS-101 Memory Forensics | CS-102 Disk Imaging | CS-094 Incident Response: Identification | CS-095 Incident Response: Containment | CS-001 Cybersecurity