OT Forensics

Evidence collection and analysis in industrial control system environments

OT Security Learning Series

Document 610 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Digital forensics in OT environments requires specialized approaches that balance evidence preservation with operational continuity. Unlike IT forensics, OT investigators must work with proprietary systems, real-time constraints, and equipment that cannot be easily taken offline.

OT forensics challenges include:

- Systems that cannot be shut down for imaging
- Proprietary file systems and data formats
- Limited or no logging capabilities
- Volatile evidence in controller memory
- Chain of custody across IT and OT boundaries

2 OT vs IT Forensics

Aspect	IT Forensics	OT Forensics
System access	Can often image offline	Must preserve operations
Evidence sources	Disk, memory, logs	Controllers, network, historian
Tools	Standard forensic suites	Vendor-specific, custom tools
File systems	NTFS, ext4, APFS	Proprietary, embedded
Time sensitivity	Hours to days	Minutes to hours
Expertise	IT security analysts	OT engineers + forensics

Table 1: IT vs OT Forensics Comparison

Warning

Critical Difference: In IT, you typically take systems offline for imaging. In OT, shutting down a PLC or HMI may halt production or create safety hazards. Live forensics is often the only option.

3 Evidence Sources

3.1 Network Evidence

- **Packet captures** – Full PCAP from network taps or SPAN ports
- **NetFlow/IPFIX** – Connection metadata and flow statistics
- **Firewall logs** – Allowed and denied connections

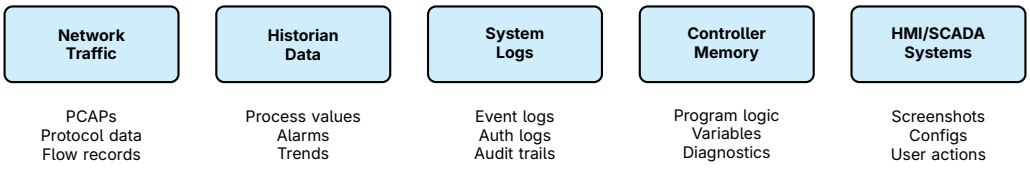

Figure 1: OT Evidence Sources

- **IDS/IPS alerts** – Detection events with packet samples
- **Protocol-specific logs** – Modbus, DNP3, OPC UA transactions

3.2 Historian Data

Key Point

Key Evidence: Historians often contain the best timeline of process anomalies. Sudden setpoint changes, unusual values, or gaps in data collection can indicate compromise.

- Process variable trends (before, during, after incident)
- Alarm and event sequences
- Operator actions and acknowledgments
- System health metrics

3.3 Controller Evidence

- **Program files** – Current logic vs known-good baseline
- **Runtime variables** – Current values in memory
- **Diagnostic buffers** – Error logs, communication stats
- **Firmware version** – Check for unauthorized changes
- **Project files** – Engineering workstation copies

3.4 Endpoint Evidence

- HMI screenshots and session recordings
- Engineering workstation disk images
- USB device connection logs
- Remote access session logs
- Antivirus/EDR detection logs

4 Evidence Collection Process

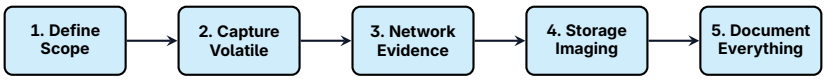

Figure 2: Evidence Collection Workflow

4.1 Order of Volatility

Collect evidence in order of how quickly it may be lost:

1. **Network traffic** – Capture immediately, flows constantly
2. **Controller memory** – Runtime state, may change with process
3. **System memory** – RAM on Windows/Linux systems
4. **Running processes** – Active connections, loaded modules
5. **Historian data** – May be overwritten by retention policies
6. **Disk storage** – Most persistent, collect last

4.2 Live Collection Techniques

Non-Disruptive Collection

- **Network tap** – Passive copy of all traffic
- **SPAN/mirror port** – Switch-based traffic copy
- **Read-only PLC upload** – Extract program without stopping
- **Historian export** – Query historical data via API
- **Log forwarding** – Real-time copy to forensic server

Critical

Do Not:

- Stop or restart controllers during evidence collection
- Install forensic agents on production OT systems
- Run active network scans that may disrupt protocols
- Modify system configurations to enable logging

5 Chain of Custody

Maintain rigorous documentation:

- **Who** collected the evidence

- **What** was collected (hashes, descriptions)
- **When** collection occurred (timestamps)
- **Where** evidence was stored
- **How** collection was performed (tools, methods)

5.1 Evidence Integrity

- Calculate cryptographic hashes (SHA-256) immediately
- Use write-blockers for disk imaging
- Store evidence on encrypted, access-controlled media
- Maintain detailed logs of all access
- Create working copies for analysis

6 Analysis Techniques

6.1 Timeline Analysis

Correlate events across multiple sources:

- Historian timestamps (process anomalies)
- Network capture timestamps (malicious traffic)
- Log timestamps (authentication, errors)
- Normalize all times to UTC

6.2 PLC Program Analysis

- Compare current program to known-good baseline
- Identify unauthorized function blocks or logic changes
- Check for hidden routines or conditional triggers
- Analyze program upload/download history

6.3 Network Traffic Analysis

- Identify unauthorized connections
- Analyze industrial protocol commands
- Look for reconnaissance (scans, enumeration)
- Detect data exfiltration patterns

- Check for C2 communication signatures

7 Tools for OT Forensics

Category	Tools
Network capture	Wireshark, tcpdump, NetworkMiner
Protocol analysis	Wireshark dissectors, custom parsers
Disk imaging	FTK Imager, dd, Guymager
Memory analysis	Volatility, Rekall
Timeline	log2timeline/Plaso, Timesketch
PLC analysis	Vendor tools, custom scripts

Table 2: OT Forensics Tool Categories

8 Summary

Key Takeaways

- **Operational priority** – Evidence collection must not disrupt operations
- **Multiple sources** – Network, historian, controllers, endpoints
- **Order of volatility** – Capture ephemeral evidence first
- **Live forensics** – Often the only option in OT
- **Chain of custody** – Document everything for legal proceedings
- **Baseline comparison** – Compare against known-good configurations
- **Cross-domain expertise** – Requires both OT and forensics skills

9 Further Reading

Standards and Guidelines

- **NIST SP 800-86** – Guide to Integrating Forensic Techniques
  https://csrc.nist.gov/publications/detail/sp/800-86/final
- **IEC 62443-2-1** – Security program requirements
  https://webstore.iec.ch/publication/7030

Resources

- **CISA – ICS Forensics Resources**
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS – Digital Forensics**
  https://www.sans.org/cyber-security-courses/ics-cyber-security-in-depth

Books

- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)
- NIST – *Guide to Industrial Control Systems Security*

Part of the OT Security Learning Series