USE CASE

# Safe Forensic Collection from Compromised Endpoints

## Give forensics teams a hardware-enforced path from compromised endpoint to trusted lab.

### Challenge

→ Connecting a compromised endpoint to a forensics system exposes the trusted environment to threats.

### Solution

→ Hardware-enforced one-way USB transfer with the Owl IRD moves evidence out without any return path to the source.

### Benefits

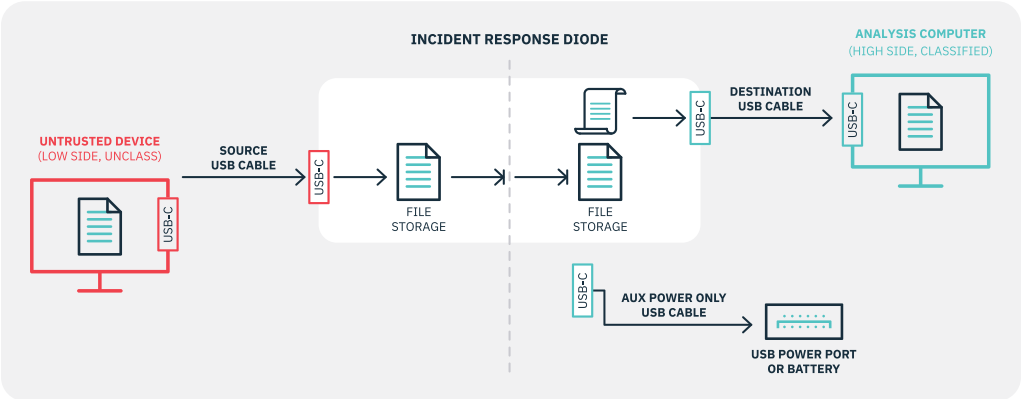
→ Replace improvised, high-risk collection methods with a repeatable, hardware-validated forensic workflow that holds up to scrutiny at every stage.

## **The Challenge:** Evidence Collection puts Clean Systems at Risk

When an endpoint is compromised, incident responders need to collect forensic evidence like logs, memory captures, malware samples, and artifacts that reveal what happened and how far the threat spread – and they need to do it quickly. But every traditional collection method introduces new risk. Connecting a compromised host to a clean analysis system opens a bidirectional path that active malware, callbacks, or hidden payloads can exploit. USB drives carry contamination risk and produce no reliable session record. Ad hoc workarounds are neither repeatable nor defensible in court or compliance reviews. The evidence that responders need most is also the evidence hardest to collect safely.

## **The Solution:** Owl IRD™ Enforces One-Way Evidence Transfer at the Endpoint

The Owl Incident Response Diode™ (IRD) is the industry's first portable Protocol Filtering Diode (PFD) built specifically for incident response and forensics teams. Plug the untrusted end into the compromised endpoint, plug the trusted end into a clean analysis system, copy files as normal. The Owl IRD features FPGA-level PFD technology that moves data forward in one direction only, with no return path ever created. Protocol filtering operates at the hardware level, meeting U.S. Government PFD requirements, so no command, callback, or malicious payload can traverse back from the trusted environment. Built-in session records standardize how evidence moves from field to lab, producing a defensible, auditable chain of custody on every collection, without configuration, training, or complexity.

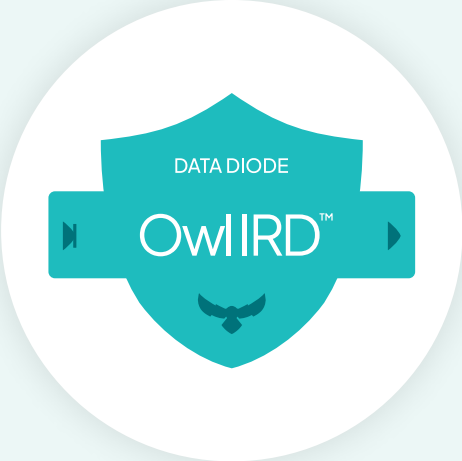





203-894-9342 | owlcyberdefense.com

## **The Result:** Safer Collections. Stronger Evidence. Faster Response.

- **Eliminates reinfection risk:** FPGA-driven and hardware-enforced one-way enforcement ensures no malware, callback, or payload can reach the trusted analysis environment during or after collection.
- **Preserves forensic chain of custody:** Built-in session records provide a consistent, auditable evidence path from field collection to lab intake and legal proceedings.
- **Replaces dangerous workarounds:** Retires contaminated USB drives and ad hoc network connections with a U.S. Government-validated PFD process.
- **Deploys in seconds, anywhere:** Portable and self-contained — responders plug in and collect without network reconfiguration, special training, or additional equipment.
- **Supports low-to-high evidence transfer:** Moves malware samples and forensic files across classification boundaries defensibly, with hardware-enforced one-way transfer at every step.




### Owl IRD

The industry's first pocket-sized Protocol Filtering Diode, the Owl Incident Response Diode (IRD) gives operators a quick, simple, hardware-enforced, one-way USB path to safely extract data from compromised or isolated endpoints, surveillance systems, and air-gapped networks that traditional tools cannot touch. Plug in, drag & drop, done. FPGA-level protocol filtering meets U.S. Government PFD requirements, preserves chain of custody, and eliminates reinfection risk, no configuration, no complexity.

OWL Cyber Defense™

Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, leads the industry in data diode and cross-domain network cybersecurity solutions for faster, safer and smarter decision making. We create solutions tailored for high-risk sectors including the military, government and critical infrastructure. Our advanced technologies enable secure, near-instantaneous collaboration, bridging network barriers to protect critical missions. With a focus on scalability and interoperability, Owl ensures that organizations can maintain secure, reliable, and compliant communication channels against evolving cyber threats.

For more information on Owl, or to schedule a demo, visit **www.owlcyberdefense.com.**



203-894-9342 | owlcyberdefense.com