

Hands-On DFIR Training at

SANS DFIRCON Miami

November 16–22, 2025
Hyatt Regency Coral Gables

SANS | GIAC
CERTIFICATIONS



The most practical, hands-on DFIR experience of the year!

Led by community legends Eric Zimmerman and David Cowen, DFIRCON is built to deliver what investigators need most—real tools, real workflows, and real-world training. Every session is rooted in practical applications, open-source tools, and hands-on exercises you can immediately apply on the job.

Highlights of DFIRCON Miami 2025

- **Community Learning Day (Nov 16):** Free and open to all registered DFIRCON attendees—a full day of guided, hands-on tutorials with open-source DFIR tools
- **EZ Tool Challenge:** Submit your idea for a chance to have it built by Eric Zimmerman and shared globally
- **DFIR NetWars:** Fully updated with new challenges, evidence sets, and scenarios to push your DFIR skills further than ever
- **DFIR Bytes Case Simulation:** Walk through a complete investigation in a two-part, hands-on case simulation
- **14 Tailored DFIR Courses:** Curated to match DFIRCON themes, tools, and investigative challenges
- **Live Support + Virtual Labs:** Reinforce your learning with real-time assistance and secure, interactive practice
- **Networking Receptions and AlumNight:** Connect with DFIR experts, alumni, and peers in a unique community-driven atmosphere

Why Attend?

- Learn directly from the top tool developers and instructors in the DFIR field
- Gain hands-on experience with open-source investigative tools
- Earn GIAC certifications aligned with DFIRCON courses
- Extend your learning with four months of OnDemand recordings
- Build your network and join a one-of-a-kind DFIR community

Agenda

Community Learning Day – Nov 16

- SOF-ELK Workshop (Phil Hagen)
- EZ Tools Masterclass (Eric Zimmerman)
- ArtEx Artifact Research (Ian Whiffin)
- LEAPPs Mobile & Cloud Parsing (Alexis Brignoni)
- SIFT Workshop (Mike Pilkington)
- Velociraptor for IR (Carlos Cajigas)
- SIFT + AI Wrap-Up (Rob Lee)

Welcome Reception – Nov 17

- *Keynote: Code, Community, and the Calling* by Eric Zimmerman
- Live reveal of the winning EZ Tool Challenge tool

DFIR AlumNight/DFIR Bytes – Nov 18–19

- Casual networking for alumni and attendees
- DFIR Bytes: Operation Phantom Thread (Instructor-led case simulation)

DFIR NetWars Tournament – Nov 20–21













- Free for registered 4–6 day course students
- New challenges covering forensics, IR, threat hunting, and malware analysis

“DFIRCON is about building tools, workflows, and skills that actually solve problems investigators face every day. This isn’t theory—it’s what works in the field.”

—Eric Zimmerman

Secure your spot today and be part of the ultimate DFIR community experience!

Confirmed Courses

FOR498: Digital Acquisition and Rapid Triage™	GBFA	GIAC Battlefield Forensics and Acquisition giac.org/gbfa	
FOR500: Windows Forensic Analysis™	GCFE	GIAC Certified Forensic Examiner giac.org/gcfe	
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics™	GCFA	GIAC Certified Forensic Analyst giac.org/gcfa	
FOR509: Enterprise Cloud Forensics and Incident Response™ UPDATED	GCFR	GIAC Cloud Forensics Responder giac.org/gcfr	
FOR518: Mac and iOS Forensic Analysis and Incident Response™	GIME	GIAC iOS and macOS Examiner giac.org/gime	
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™	GNFA	GIAC Network Forensic Analyst giac.org/gnfa	
FOR577: Linux Incident Response and Threat Hunting™	GLIR	GIAC Linux Incident Responder giac.org/glir	
FOR578: Cyber Threat Intelligence™	GCTI	GIAC Cyber Threat Intelligence giac.org/gcti	
FOR585: Smartphone Forensic Analysis In-Depth™	GASF	GIAC Advanced Smartphone Forensics giac.org/gasf	
FOR589: Cybercrime Investigations™			
FOR608: Enterprise-Class Incident Response & Threat Hunting™	GEIR	GIAC Enterprise Incident Responder giac.org/geir	
FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques™	GREM	GIAC Reverse Engineering Malware giac.org/grem	
SEC401: Security Essentials – Network, Endpoint, and Cloud™	GSEC	GIAC Security Essentials giac.org/gsec	
SEC504: Hacker Tools, Techniques, and Incident Handling™	GCIH	GIAC Certified Incident Handler giac.org/gcih	