FOR563: Applied AI for Digital Forensics and Incident Response: Leveraging Local Large Language Models™

1 Day Course	6 CPEs	Laptop Required

Topics

- Introduction to LLMs and their use in DFIR workflows
- Model setup, local hosting, and parameter tuning
- Structured artifact analysis
- Creating and using LLM-powered forensic agents
- Natural language querying at scale
- Introduction to fine-tuning: data prep, formats, and chat templates
- Understanding limitations and validation techniques for AI in DFIR

You Will Be Able To

- Configure and deploy local LLMs through both GUI and programmatic methods
- Build and implement custom AI agents for forensic and incident response use cases
- Analyse structured data—including logs, text messages, and databases—using natural language
- Fine-tune LLMs for specialised DFIR tasks using custom datasets

Business Takeaways

- Reduce the risk of data exposure by enabling AI-assisted analysis without sending sensitive data to third-party cloud services
- Improve incident response workflows by equipping DFIR teams to use natural language interfaces for analysis
- Lower reliance on proprietary AI platforms by training analysts to deploy and manage local, self-hosted LLMs
- Expand investigative capabilities with custom AI agents tailored to your organisation's specific forensic needs
- Accelerate adoption of AI-driven workflows without compromising internal security or compliance requirements
- Support knowledge retention and skill development by standardising repeatable, scalable AI-driven forensic processes
- Future-proof DFIR operations by preparing staff for integrating AI solutions across evolving data sources and forensic tooling

Who Should Attend

- Digital Forensics and Incident Response (DFIR) professionals
- Security analysts and forensic examiners
- Threat hunters and detection engineers
- Investigators interested in AI and data automation
- Cybersecurity researchers and lab developers
- Security professionals wanting to explore LLM use cases

NICE Framework Work Roles

- Cyber Defense Forensics Analyst (IN-FOR-002)
- Cyber Defense Analyst (PR-CDA-001)
- Cyber Defense Incident Responder (PR-CIR-001)
- Law Enforcement/Counterintelligence Forensics Analyst (IN-FOR-001)
- Threat Analyst (AN-TWA-001)
- Cyber Defense Analyst (PR-CDA-001)
- Security Architect (SP-ARC-002)
- Research and Development Specialist (SP-RD-001)
- Data Analyst (OM-DTA-001)

FOR563™ is a one-day, hands-on course designed to help DFIR professionals harness the power of Artificial Intelligence (AI) through the use of local Large Language Models (LLMs). As organisations increasingly explore AI in investigative workflows, they must do so without compromising the sensitive nature of forensic data. This course bridges that gap by showing practitioners how to operationalise LLMs in a fully self-hosted environment, giving them full control over their data while still benefiting from powerful, cutting-edge AI capabilities.

Students will learn to configure and deploy local LLMs, build custom forensic agents, and analyse large volumes of data found across DFIR artifacts using AI. This includes logs, forensic artifacts, databases, and files containing proprietary or undocumented formats often unique to specific applications or operating systems.

The course also dives into the practical challenges of using LLMs in DFIR, such as context limitations and model fine-tuning, giving students real-world experience through four technical labs. While the course emphasises private, local AI implementations, the concepts can easily be extended to API-based or cloud-hosted LLMs, offering flexible options for organisations at different stages of AI adoption.

FOR563™ enables DFIR teams to accelerate investigations, automate repetitive analytical tasks, and tailor AI tools to their specific forensic needs—all without sending sensitive data outside their controlled environment. By the end of the course, students will be equipped with both foundational knowledge and practical skills to confidently integrate AI into modern DFIR workflows.

Hands-On Training

FOR563™ emphasises practical, real-world applications of Large Language Models in DFIR through a full day of guided, interactive labs. Students will use a cloud-based platform that provides access to GPU-powered development environments—similar to notebook-style coding interfaces—without requiring expensive local hardware. This allows students to start building and running local LLMs immediately, using a free-to-create account, no matter their workstation specs.

Each lab is designed to reinforce key concepts through hands-on tasks such as configuring models, analysing forensic data, building custom agents, and fine-tuning an LLM. By the end of the course, students will have deployed, tested, and interacted with LLMs in a fully private, local setup that mirrors real-world DFIR use cases.

Author Statement

"In my own work, I've seen how going beyond the basic GUI experience and truly understanding how tools work under the hood leads to greater automation and efficiency. This course is about showing digital forensic examiners how Large Language Models can help them work smarter—not by replacing expertise, but by enhancing it. Much like scripting in Python, LLMs are a force multiplier: that can streamline repetitive tasks, speed up analysis, and surface new insights. But they aren't magic. We'll also explore the limitations of these models, how to trust but verify their output, and how to integrate them thoughtfully into real-world DFIR workflows."

—Mari DeGrazia