

FOR498: Digital Acquisition and Rapid Triage™



GBFA
Battlefield Forensics
and Acquisition
giac.org/gbfa

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Collect data from PCs, Macs, tablets, smartphones, RAM, virtual machines, and cloud environments
- Perform evidence acquisition while maintaining forensic soundness and chain of custody
- Execute rapid triage workflows to generate actionable intelligence in 90 minutes or less
- Capture volatile data and memory from live systems during active investigations
- Manage scenes efficiently to preserve and prioritize critical data
- Acquire evidence from enterprise environments including Exchange, SharePoint, and network repositories
- Utilize industry-standard open-source tools and SANS-provided environments for hands-on collection and analysis

Business Takeaways

- Preserve digital evidence effectively to support regulatory, legal, and internal investigations
- Accelerate incident response with rapid data triage and reduced analysis time
- Confidently operate across diverse platforms, storage types, and user environments
- Improve collaboration between technical teams, investigators, and legal stakeholders
- Prevent data loss or mishandling during high-pressure incidents
- Reduce dependency on external digital forensics resources by building in-house capability
- Stay current with evolving acquisition challenges across cloud, mobile, and large-scale storage systems

“In DFIR, things rarely go as planned. This course teaches you about the options to control when things aren’t working as expected.”

— J-Michael Roberts, *Corvus Forensics*

THE CLOCK IS TICKING. YOU NEED TO PRIORITIZE THE MOST VALUABLE EVIDENCE FOR PROCESSING. LET US SHOW YOU HOW.

The FOR498: Digital Acquisition and Rapid Triage course will help you to:

- Acquire data effectively from:
 - PCs, Microsoft Surface, and Tablet PCs
 - Apple Devices, Mac, and Macbooks
 - Random Access Memory (RAM)
 - Smartphones and portable mobile devices
 - Cloud storage and services
 - Network storage repositories
 - Virtual Machine environments
- Produce actionable intelligence in 90 minutes or less

The first step in any investigation is the gathering of evidence. Digital forensic investigations are no different. The evidence used in this type of investigation is data, and this data can live in many varied formats and locations. You must be able to first identify the data that you might need, determine where that data resides, and, finally, formulate a plan and procedures for collecting that data.

With digital forensic acquisitions, you will typically have only one chance to collect data properly. If you manage the acquisition incorrectly, you run the risk of not only damaging the investigation, but more importantly, destroying the very data that could have been used as evidence.

With the wide range of storage media in the marketplace today, any kind of standardized methodology for all media is simply untenable. Many mistakes are being made in digital evidence collection, and this can cause the guilty to go free and, more importantly, the innocent to be incarcerated. The disposition of millions and millions of dollars can rest within the bits and bytes that you are tasked with properly collecting and interpreting.

An examiner can no longer rely on “dead box” imaging of a single hard drive. In today’s cyber sphere, many people utilize a desktop, laptop, tablet, and cellular phone within the course of a normal day. Compounding this issue is the expanding use of cloud storage and providers, and the proper collection of data from all these domains can become quite overwhelming.

This in-depth digital acquisition and data handling course will provide first responders and investigators alike with the advanced skills necessary to properly respond to, identify, collect, and preserve data from a wide range of storage devices and repositories, ensuring that the integrity of the evidence is beyond reproach. Constantly updated, FOR498 addresses today’s need for widespread knowledge and understanding of the challenges and techniques that investigators require when addressing real-world cases.

Numerous hands-on labs throughout the course will give first responders, investigators, and digital forensics teams practical experience needed when performing digital acquisition from hard drives, memory sticks, cellular phones, network storage areas, and everything in between.

During a digital forensics response and investigation, an organization needs the most skilled responders possible, lest the investigation end before it has begun. FOR498: Digital Acquisition and Rapid Triage will train you and your team to respond, identify, collect, and preserve data no matter where that data hides or resides.

Section Descriptions

SECTION 1: Introduction, Basic Concepts, and Device Identification

Section 1 introduces foundational forensic concepts and tools, as well as common file systems an examiner may encounter. We also explore a myriad of different device and interface types, adapters, and identification for data-informed decision making, as well as multi-drive storage scenarios.

TOPICS:

- Introduction to SIFT and Digital Forensic Concepts
- Understanding the Data; Device and Interface Identification
- Multi-Drive Storage
- Timeline Explorer

SECTION 2: Online Asset Ownership, Scene Management, File Systems, Memory Acquisition, and Encryption Detection

Section 2 emphasizes the importance of proper digital evidence collection, focusing on procedures including evidence handling and scene management. We also highlight the need for proper training to ensure data integrity in high-pressure investigative environments. Further to this, we cover acquisition methodologies, memory capture, analysis, and triage techniques. Importantly, we will also address online attribution, tracing digital artifacts to their sources, and legal considerations.

TOPICS:

- Identifying Online Asset Ownership
- Preparing Destination Media
- Scene Management and Evidence Collection
- Acquisition Methodology
- File Systems Revisited
- Memory Acquisition and Encryption Checking

SECTION 3: Triage and Data Acquisition

Section 3 covers "Quick Win Forensics," focusing on rapidly identifying and acquiring key evidence through write blocking, live response, and Volume Shadow Copies using tools like KAPE for rapid triage and remote collection. It emphasizes speed and efficiency, especially in cases involving encryption or file-less malware.

TOPICS:

- Conducting Host-Based Live Acquisition
- Image Mounting
- Triage Acquisition
- Rapid Triage With KAPE
- Write Blocking

SECTION 4: Dead Box Acquisition, Virtual Machines, and Apple Preparation

Section 4 covers acquiring data using traditional methods. It also prepares investigators to quickly access critical evidence from complex modern systems like Virtual Machines, and dealing with little understood areas such as the BIOS/UEFI. We also focus on the unique challenges of acquiring data from Apple devices. It covers macOS-specific tools, encryption hurdles, and alternative imaging methods due to hardware constraints.

TOPICS:

- Dead Box Acquisition
- Virtual Machines
- macOS Security Layers
- macOS Device Preparation

SECTION 5: Apple Acquisition, Data Carving, and Remote Acquisition

Section 5 continues the battle of acquiring Apple data, then moves on to file and stream carving to recover deleted or corrupted data. We also dive into advanced data recovery techniques when traditional tools fall short. Emphasis is placed on understanding tool limitations and applying manual recovery methods. We round out this section discussing remote acquisition including email.

TOPICS:

- Apple Acquisition
- File and Stream Recovery
- Data Carving and Rebuilding
- Remote Acquisition

SECTION 6: Portable Device Acquisition, Analysis, and the Internet of Things

Section 6 focuses on acquiring and analyzing data from portable devices emphasizing proper handling. We will also explore how to analyze IoT device communication and collect related network traffic for forensic purposes.

TOPICS:

- Portable Device Acquisition
- Portable Device Analysis
- Internet of Things

Who Should Attend

- Federal agents and law enforcement personnel
- First responders
- Digital forensic analysts
- Information security professionals
- Incident response team members
- Media exploitation analysts
- Department of Defense and intelligence community professionals
- Anyone interested in an understanding of the proper preservation of systems

NICE Framework Work Roles

- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)



GBFA

Battlefield Forensics
and Acquisition
giac.org/gbfa

GIAC Battlefield Forensics and Acquisition

GIAC Battlefield Forensics and Acquisition (GBFA) Certification. The GIAC Battlefield Forensics and Acquisition (GBFA) certification demonstrates that an individual is trained and qualified in the proper collection, acquisition, and rapid triage analysis of many forms of data storage.

- Efficient data acquisition from a wide range of devices
- Rapidly producing actionable intelligence