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

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where they are stored
- Handle and process a scene properly to maintain evidentiary integrity
- Perform data acquisition from at-rest storage, including both spinning media and solid-state storage
- Identify the numerous places that data for an investigation might exist
- Perform Battlefield Forensics by going from evidence seizure to actionable intelligence in 90 minutes or less
- Assist in preparing the documentation necessary to communicate with online entities such as Google, Facebook, Microsoft, etc.
- Understand the concepts and usage of large-volume storage technologies, including JBOD, RAID storage, NAS devices, and other large-scale, network-addressable storage
- Identify and collect user data within large corporate environments where they are accessed using SMB
- Gather volatile data such as a computer system's RAM
- Recover and properly preserve digital evidence on cellular and other portable devices
- Address the proper collection and preservation of data on devices such as Microsoft Surface/ Surface Pro, where hard-drive removal is not an option
- Address the proper collection and preservation of data on Apple devices such as MacBook, MacBook Air, and MacBook Pro, where hard-drive removal is not an option
- Properly collect and effectively target email from Exchange servers, avoiding the old-school method of full acquisition and subsequent onerous data culling
- Properly collect data from SharePoint repositories
- Access and acquire online mail stores such as Gmail, Hotmail, and Yahoo Mail accounts

"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
  - RAM and memory
  - Smartphones and portable mobile devices
  - Cloud storage and services
  - Network storage repositories
- 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: Battlefield Forensics & Acquisition 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: Scene Prep, Management, and Storage Interfaces

Investigators often respond in high-stress environments where many different entities are critically scrutinizing the collection process. Personnel need to be properly trained and equipped to work in less-than-optimal surroundings, and they must be confident that they have managed the scene, identified all necessary data, collected it in a properly defensible manner, and maintained its integrity. One of the most common scenarios that can cause headaches is receiving an evidence file (usually an E01), and being expected to provide answers immediately. The common approach is to mount the image and then start running carving and other tools against it. These automated tasks can take many hours (and sometimes days) just by themselves!

TOPICS: SIFT Introduction; Introduction to Digital Forensic Acquisition; Understanding the Data; Scene Management and Evidence Acquisition; Device and Interface Identification

SECTION 3: Triage and Data Acquisition

Given that 99 percent of the necessary evidence typically will exist in 1–2 percent of the data acquired, it is easy to see how a great deal of time can be wasted following the normal procedures in today's digital forensics world. Instead, let's focus on this 1–2 percent and perform a very rapid triage collection that can be used to start our investigation sooner! Far too often, computers are seized in an "on" state, and immediately powered down because "that is how we've always done it." With today's computers this means you are throwing away (essentially destroying) many gigabytes of data. The RAM in a computer holds an incredibly important treasure trove of data, from keystrokes to network connections, running services, and, quite importantly, passwords and decryption keys. With the vastly increasing spread of file-less malware, in many cases the only place that evidence will exist is in memory. Another often-overlooked factor is full disk encryption. In cases like this, "live" acquisition will be your only hope.

TOPICS: Beginning the Collection Process; Mounting Evidence; Triage Acquisition; Memory Acquisition and Encryption Checking; Host-Based Live Acquisition; Dead Box Acquisition

SECTION 5: Apple Acquisition and Internet of Things

This course section will explore the fundamentals of acquiring data from Apple devices. Compared to Windows, there are very few tools and techniques available when it comes to acquisition of Apple products. The tools that exist can be quite expensive, and free tools are simply few and far between. In this course section, will acquire memory and identify systems that are running CoreStorage technology and full disk encryption. We will also visit the challenges posed by APFS. Many of the Apple systems are closed systems, in that you simply cannot remove the hard drive because it is soldered directly to the motherboard. The uniqueness of the data storage demands alternative methods of acquisition. In this course section, you'll learn how to access and forensically image iPads, MacBooks, and other HFS+ devices, working at the command line, as well as how to build a free acquisition boot disk to image even the latest macOS versions on current hardware. Not to be left out, the pervasive Internet of Things is controlling our fridges, thermostats, security cameras, and door locks. It is listening passively and waiting patiently for an instruction to perform. In this course section, you will learn how these devices communicate, and more importantly, who is controlling them.

TOPICS: Apple MacOS Device Overview and Acquisition; Internet of Things (IoT)

SECTION 2: Portable Devices and Acquisition Processes

Portable devices bring their own set of challenges to the table. These devices are more ubiquitous than computers. Seldom is the case today that does not include a cellular device. Unfortunately, there is no standard for cellular operating systems. Even within brands, there can be vastly different data storage. This course section will introduce students to several devices and the tools that will acquire them. We will also explore the myriad of acquisition hardware and software, not to mention adapters and identification, so that you can make the best decisions about the data.

TOPICS: Smartphone Acquisition; Smartphone Analysis; Android; Acquisition Hardware and Software; Acquisition Methodology; Discovering and Interacting with Data

SECTION 4: Non-Traditional and Cloud Acquisition

When we think about acquisition, it usually involves opening the side of the computer, removing the hard drive, connecting to a write blocker or imaging equipment, and completing the task. While this does not necessarily result in an inaccurate assessment, it does not address a great deal of the access and acquisition questions surrounding so much data today. If full disk imaging is necessary, then it is certainly easier and quicker to do it directly from the storage itself. But what happens with devices such as iPads, Surface Books, and other equipment held together by glue instead of screws? This course section will teach you how to identify and access data in non-traditional storage areas. In today's world, so much data live off site, and there are very few methods in place to access and properly acquire those data. We will identify these locations, including SharePoint, Exchange, webmail, network locations, cloud storage, and social media, not to mention Dropbox, Google Drive, and the Internet of Things. This also includes RAID storage and how to best collect these devices regardless of configuration. Moving to the forefront of most Enterprise investigations, we will be examining vSphere and virtual machine collections as well!

TOPICS: File Systems Revisited; Battlefield Forensics with KAPE; Multi-Drive Storage; EMC/Non-traditional Formats; Remote Acquisition

SECTION 6: Beyond the Forensic Tools: The Deeper Dive

You have traced an artifact back to an IP, email, or web address. Now what? In this course section you'll learn the best methods to determine attribution, from proper collection to legal documentation. The usefulness of file and stream carving cannot be overstated. Some data simply do not live in the defined file space that can be readily accessed by a viewer. From partially overwritten to deleted data, we will explore techniques you can employ when traditional tools fail. Data carving is an increasingly important skill. Once the reference to a file is destroyed, how can the data still be recovered? File carving tools will assist in this, but examiners must understand the limitations of their tools. Without the proper pieces of the original file, a carver is useless.

TOPICS: Identifying Online Asset Ownership; File and Stream Recovery; Advanced Data Carving and Rebuilding; Where Do We Go From Here

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

"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. Certified GBFA professionals can traverse each point from arriving at a scene, through determining and establishing the "quick wins" necessary to rapidly move an investigation forward. They have shown skill and excellence in the use of a wide variety of tools and techniques across a vast spectrum of media storage repositories from portable devices, servers, and endpoints, through to IoT and Cloud data. This industry certification will convey that the holder is prepared to handle every facet of the collection and rapid triage process."
– Kevin J Ripa, FOR498 Course Co-Author

- Efficient data acquisition from a wide range of devices
- Rapidly producing actionable intelligence
- Manually identifying and acquiring data