NEW!

FOR498

| **6**
Day Program | **36**
CPEs | Laptop
Required |

Battlefield Forensics & Data Acquisition

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 and who has a background in information systems, information security, and computers.

You Will Be Able To

❚ Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where it is 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 it is 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

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

FOR498: Battlefield Forensics & Acquisition Course will help you to:

❚ Acquire data effectively from:

❚ PCs, Microsoft Surface, and Tablet PCs

❚ Apple Devices, and 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.

SANS

Course Day Descriptions

498.1 | Hands On

Evidence File Quick Wins and Dealing with Smartphones

Investigators will often be responding 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 be confident that they have managed the scene, identified all necessary data, collected the data 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!

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 the cellular operating systems. Even within brands, there can be vastly different data storage. Today will introduce the student to several devices and the tools that will acquire them.

Topics: SIFT Introduction; Introduction to Digital Forensic Acquisition; Understanding the Data; Smartphone Acquisition; Smartphone Analysis; Android

498.2 | Hands On

Evidence Acquisition and Collection

Investigators and first responders should be armed with the latest tools, digital container access techniques, and enterprise methodologies to identify, access, and preserve evidence across a vast range of devices and repositories. Personnel must also be able to scale their identification and collection across thousands of systems in their enterprise. Enterprise and cloud storage collection techniques are now a requirement to track activity that has been intentionally and unintentionally spread across many devices. Responding to these many systems cannot be accomplished using the standard "pull the hard drive" forensic examination methodology. Such an approach will cause frustration and result in lost opportunities due to the time it takes to forensically image entire hard drives. Furthermore, investigators need actionable intelligence as quickly and responsibly as possible. This section lays the foundation for evidence collection, from initial arrival on a scene to the fundamentals of understanding data at rest and properly identifying devices, interfaces, and tools that will be necessary to affect a successful collection. This course section will explore the myriad of acquisition hardware and software, not to mention adapters and identification, so we can make the best decisions about the data.

Topics: Scene Management and Evidence Acquisition; Device and Interface Identification; Acquisition Hardware and Software; Acquisition Methodology; Discovering and Interacting with Data

498.3 | Hands On

Quick Win Forensics

Given that 99% of the necessary evidence typically will exist in 1-2% 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% 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

498.4 | Hands On

Non-Traditional and Cloud Acquisition

Battlefield forensics is considered the bleeding edge of digital forensics. It requires in-depth knowledge of where the most valuable data resides on the computer and how to get at it as fast as possible. An effective battlefield forensicator needs to be extracting actionable intelligence in 90 minutes or less, butthe clock does not start when the forensic imaging is done. Rather. it starts from the moment you lay your hands on the device.

Learn how to identify and access data in non-traditional storage areas. In today's world so much data lives off site, and there are very few methods in place to access and properly acquire it. In this section, 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.

Topics: Dead Box Acquisition; File Systems Revisited; Battlefield Forensics with KAPE; Multi-Drive Storage; EMC/non-traditional formats; Remote Acquisition

498.5 | Hands On

Apple Acquisition, Internet of Things, and Online Attribution

There are very few tools and techniques available when it comes to acquisition of Apple products, as compared to Windows. The tools that exist can be quite expensive, and free tools are simply few and far between. In this section, we will explore the fundamentals of acquiring data from Apple devices. We 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, as 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. You have traced an artifact back to an IP, email, or web address. Now what? We will learn the best methods for determining attribution, from proper collection to legal documentation. Not to be left out, the Internet of Things is pervasive. It is controlling our fridges, thermostats, security cameras, and door locks. It is listening passively and waiting patiently for an instruction to perform. Today you will learn how these devices communicate, and more importantly, who is controlling them.

Topics: Identifying Online Asset Ownership; Apple MacOS Device Overview and Acquisition; Internet of Things (IoT)

498.6 | Hands On

Beyond the Forensic Tools: The Deeper Dive

The usefulness of file and stream carving cannot be overstated. Some data simply does 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 a skill that is increasingly important. 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. At some point, you will be faced with non-functioning media. Learn about the inner workings of hard drives, and what you can (and cannot) do to revive them to a point where you can then create your forensic image. We will also be looking at the "best of breed" data recovery tools, from those that are free to those that cost many thousands of dollars.

Topics: File and Stream Recovery; Advanced Data Carving and Rebuilding; Data Recovery; Where Do We Go From Here

*Courses are subject to change.