Who Should Attend

- Federal agents and law enforcement officers who want to learn the fundamentals of digital forensics, or who are starting out in digital forensics, or who are responsible for managing digital forensics units, or who want to know how digital evidence can be used in investigations and other law enforcement operations.
- Digital forensic analysts who want to consolidate and expand their understanding of the fundamentals of digital forensics as a discipline.
- Information security professionals who want to understand the fundamentals of digital forensics and how to leverage this in their operational environments.
- Legal professionals who need to understand digital forensics, the role it can play in proving a matter in court, the various uses of digital evidence, and the relationship between digital forensics and digital evidence.
- Military and intelligence operators who need to understand the role of digital investigation and intelligence gathering, and how digital forensics can enhance their missions.
- HR professionals that may have to rely on digital forensics and evidence in internal investigations of staff misconduct.
- Managers and executives who need to understand what digital forensics can do for their organizations and the critical role that it can play in securing their organization.
- Anyone interested in digital forensics, whether or not they are considering a career in this field.

You Will Be Able To

- Effectively use digital forensics methodologies.
- Ask the right questions in relation to digital evidence.
- Understand how to conduct digital forensics engagements compliant with acceptable practice standards.
- Develop and maintain a digital forensics capacity.
- Understand incident response processes and procedures and when to call on the team.
- Describe potential data recovery options in relation to deleted data.
- Identify when digital forensics may be useful and understand how to escalate to an investigator.
- If required, use the results of your digital forensics in court.

IT’S NOT JUST ABOUT USING TOOLS AND PUSHING BUTTONS

FOR308: Digital Forensics Essentials course will help you understand:

- What digital forensics is.
- What digital evidence is and where to find it.
- How digital forensics can assist your organization or investigation.
- Digital forensics principles and processes.
- Incident response processes and procedures.
- How to build and maintain a digital forensics capacity.
- Some of the key challenges in digital forensics and incident response.
- Some of the core legal issues impacting on digital evidence.

Digital forensics has evolved from methods and techniques that were used by detectives in the 1990’s to get digital evidence from computers, into a complex and comprehensive discipline. The sheer volume of digital devices and data that we could use in investigative ways meant that digital forensics was no longer just being used by police detectives. It was now being used as a full forensic science. It was being used in civil legal processes. It was being used in the military and intelligence services to gather intelligence and actionable data. It was being used to identify how people use and mis-use devices. It was being used to identify how information systems and networks were being compromised and how to better protect them. And that is just some of the current uses of digital forensics.

However digital forensics and incident response are still largely misunderstood outside of a very small and niche community, despite their uses in the much broader commercial, information security, legal, military, intelligence and law enforcement communities.

Many digital forensics and incident response courses focus on the techniques and methods used in these fields, which often do not address the core principles: what digital forensics and incident response are and how to actually make use of digital investigations and digital evidence. This course provides that. It serves to educate the users and potential users of digital forensics and incident response teams, so that they better understand what these teams do and how their services can be better leveraged. Such users include executives, managers, regulators, legal practitioners, military and intelligence operators and investigators. In addition, not only does this course serve as a foundation for prospective digital forensics practitioners and incident responders, but it also fills in the gaps in fundamental understanding for existing digital forensics practitioners who are looking to take their capabilities to a whole new level.
Course Day Descriptions

308.1 | Hands On
Introduction to Digital Investigation
The volume of digital information in the world is growing at a scary fast rate. In fact, 90 percent of the digital data that exists worldwide today was created within the last two years and it’s not slowing down with 25 quintillion bytes of new data created each and every day. If you are investigating any matter, whether it is a crime, an administrative or civil issue, or trying to figure out how your network was compromised, you need evidence. If you are gathering intelligence you need information. The simple reality is that these days the vast majority of potential evidence or information that we can use, whether it is for investigations, court, or intelligence purposes, is digital in nature. To effectively conduct digital investigations, one needs to understand exactly what digital evidence is, where to find it, the issues affecting digital evidence, and the unique challenges facing digital evidence. This will allow one to understand the crucial role that digital forensics plays with regards to digital evidence.

308.3 | Hands On
Incident Response
Digital forensics deals with the preservation, examination and analysis of digital evidence. However, Incident Response is often the preceding activity that leads to the requirement to conduct a forensic investigation. If not executed properly, the Incident Response processes and team have the ability to inadvertently disrupt or damage subsequent forensic activities. It is therefore a vital important aspect of an investigation. The Incident Response team must be adept at recognizing incidents and responding appropriately to collect and preserve evidence, whilst identifying and containing the incident. This same team are also usually involved in Forensic Readiness planning, which defines what evidence may be useful in a number of attack scenarios and ensures that systems are configured to collect and retain this evidence. Evidence that is collected in advance of an investigation can provide vital clues to a digital forensic investigator and when used in addition to subsequently acquired data, can provide insights into what data may have changed during specified periods of time that may be pertinent to the case. Digital Forensics and Incident Response therefore go hand-in-hand and are often referred to by the acronym DFIR. If you are a prospective or current digital forensics practitioner, understanding exactly how incident response works will enable you better leverage these teams before, during and after investigations to obtain the best and most useful evidence and improve reporting. If you do not plan to build a career in digital forensics, understanding exactly how incident response works will enable you better leverage these teams before, during and after investigations to obtain the best and most useful evidence and improve reporting. If you suspect an incident may have occurred and the types of actions on your part that may assist (or impede) any potential investigation, to provide you with the best possible outcome.

Digital Forensic Readiness
Digital forensic readiness acknowledges and defines the tools, processes and resources that must be in place to allow an organization to suitably deal with Digital Forensic investigations and Incident Response cases. If Readiness policies and processes are not defined properly, digital evidence may be unsuitable or may not be available when required, which can hinder or entirely prevent an investigation. It is therefore a vitally important aspect of pre-investigation planning.

308.2 | Hands On
Digital Forensics
CSI and similar television shows has popularized forensics in the public consciousness and increased awareness of forensics. Digital forensics is the forensic discipline that deals with the preservation, examination and analysis of digital evidence. However, television and movies have created misunderstandings about exactly what digital forensics is and does. As a result, many people interested in forensics have no real understanding about what it entails. These misperceptions have also seen lawyers that make use of digital evidence in court, investigators that need digital evidence to solve cases, information security practitioners responding to security incidents, and even people conducting digital forensics; making mistakes in relation to digital evidence, which can have negative consequences.

Digital forensics is crucial to ensure accurate and usable digital evidence, but is it important to understand exactly what it is, what it can do, and how it can be used. If you are a user of digital forensics and digital evidence, understanding exactly how digital forensics works will enable you to better make use of digital forensics and digital evidence. If you are a manager or supervisor of a digital forensic capacity, this will help you understand exactly how it should be functioning and how to build and maintain it. Finally, if you are a prospective digital forensics practitioner or an existing one, this will equip you with the fundamental knowledge and skills that form the core of the digital forensic profession.

308.4 | Hands On
Digital Evidence Acquisition Essentials
Acquiring digital evidence is a crucial component in any investigation. Digital forensics is about finding answers, and if we cannot get to the evidence that we need, which is often stored on devices, in memory, on the wire or wireless, or in the Cloud, then we will never be able to get the answers we seek. Getting the digital evidence and selecting the appropriate method to obtain it can mean the difference between success and failure in an investigation. The acquisition of digital evidence has evolved over the years and the old way of doing it may not always be the best or most effective way of getting the evidence and may actually compromise an investigation. By understanding the various strategies and methods that we have available to us to acquire digital evidence means that informed decisions can be made as to the best method to use to acquire evidence in a given situation or environment.

Digital Forensics Analysis
The key purpose of digital forensics is to find answers, and it is through the analysis process that digital forensics transforms raw data into either evidence or intelligence that we can use to answer the questions that we need answered. The use of technology is so integral to our day to day activities that it allows us an unprecedented opportunity to reconstruct what has happened in the past, to learn what is happening in the present, and even predict what may happen in the future. Based on the data available to us. By understanding digital forensic analysis, we can see how we can answer the true questions in our investigations and intelligence efforts, how we can critically examine and analyze the data at hand in a manner that can withstand scrutiny and finally, understand the types of answers we can get.

308.5 | Hands On
Documenting and Reporting in Digital Forensics
Digital forensics is at its core about getting answers to questions, whether as evidence or intelligence. So, it is important that we can get the answers that we find in our investigations to the right people so that they can make decisions and act on what is found in the digital forensics process. It is crucial that we are able to effectively communicate these answers to those people who need them, in a manner that is useful to them, and to be able to effectively support our answers. Not only must we be able to effectively communicate, but it is important that the users of these answers understand what our various reports means and how they can use them effectively. Without effective communication and understanding of what is communicated, all effort expended in the digital forensic process is lost.

Going to Court
Digital investigations can often end up in court. In certain instances, a criminal prosecution may be desired where your digital evidence will be used in a criminal court to prosecute an offender using the digital evidence you have gathered and analyzed. In other instances, you may use your digital evidence in a civil court claiming damages or other relief or defending your organization against claims for damages arising from a breach or other incident.

While laws differ around the world, there are some common principles that apply which digital forensic practitioners need to know. They need to understand the legal requirements for evidence to be acceptable for a court to use. They also need to understand how to present that evidence if they are called upon to testify in court. These two fundamentals can mean the difference between success and failure.

*Courses are subject to change.*