FOR308: **Digital Forensics Essentials**

6 Day Program	36 CPEs	Laptop Required

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

Course Topics

- Introduction to digital investigation and evidence
- Where to find digital evidence
- Digital forensics principles
- Digital forensics and incident response processes
- Digital forensics acquisition
- Digital forensics examination and analysis
- Presenting your findings
- Understanding digital forensic reports
- Challenges in digital forensics
- Building and developing digital forensics capacity
- Legality of digital evidence
- How to testify in court

More than half of jobs in the modern world use a computer. The vast majority of people aged 18-30 are 'digitally fluent'; accustomed to using smartphones, smart TVs, tablets and home assistants, in addition to laptops and computers, simply as part of everyday life. Yet, how many of these users actually understand what's going on under the hood? Do you know what your computer or smartphone can tell someone about you? Do you know how easy it might be for someone to access and exploit that data? Are you fed up with not understanding what technical people are talking about when it comes to computers and files, data and metadata? Do you know what actually happens when a file is deleted? Do you want to know more about Digital Forensics and Incident Response? If you answered 'yes' to any of the above, this course is for you. This is an introductory course aimed at people from non-technical backgrounds, to give an understanding, in layman's terms, of how files are stored on a computer or smartphone. It explains what Digital Forensics and Incident Response are and the art of the possible when professionals in these fields are given possession of a device.

This course is intended to be a starting point in the SANS catalogue and provide a grounding in knowledge, from which other, more in-depth, courses will expand.

IT'S NOT JUST ABOUT USING TOOLS AND PUSHING BUTTONS

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.

Section Descriptions

SECTION 1: Introduction to Digital Investigation

The volume of digital information in the world is growing at a scarily 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, 2.5 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.

TOPICS: Introduction to Digital Investigation; Digital Forensics Fundamentals; Incident Response Fundamentals Response Fundamentals; Digital Forensics Management

SECTION 2: Digital Forensics

Digital forensics is the core set of principles and processes necessary to produce usable digital evidence and uncover critical intelligence. Digital forensics is crucial to ensure accurate and usable digital evidence, but it is 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.

TOPICS: Digital Forensics Management; Digital Evidence Acquisition Essentials; Concepts of Digital Forensic Analysis; Digital Forensics Challenges

SECTION 3: Incident Response and Digital Forensic Readiness

INCIDENT RESPONSE
Incident Response is the core set of principles and processes necessary to allow an organization to successfully respond, react and remediate against potential attack scenarios.

TOPICS: Documentation and Reporting in Digital Forensics; Legal Aspects of Digital Forensics; Incident Response Challenges

DIGITAL FORENSICS MANAGEMENT
Good management of a digital forensic or incident response team is key in allowing an organization to successfully respond to potential attack scenarios and investigate digital evidence.

TOPICS: Introduction to Forensic Readiness; The need for Forensic Readiness; Building and Managing a DFIR Capacity

SECTION 4: 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.

TOPICS: Forensic Acquisition Principles and Standards; Understanding Forensic Images; Forensic Acquisition Processes; Acquisition Challenges

SECTION 5: Digital Forensic 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, all based on the data available to us. By understanding digital forensic analysis, we can see how we can ask the right 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.

TOPICS: What Can Forensic Analysis Prove; Planning the Examination; The Art and Science of Forensic Analysis; Forensic Examination and Analysis Standards; Forensic Examination and Analysis Challenges

SECTION 6: Documenting and Reporting and Going to Court

DOCUMENTING AND REPORTING IN DIGITAL FORENSICS
It doesn't matter how good your technical skills are, if you are not able to effectively document what you have done and report on your findings in a manner that non-technical people understand, your investigation is on shaky ground.

TOPICS: Ongoing Documentation; Presenting your Findings

GOING TO COURT
While not all digital forensics matters end up going to court, some do, and when that is the case it is important to at least have some understanding of the law of evidence and going to court.

TOPICS: Legal Evidence; Testifying in Court

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 what 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.