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 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.

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 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: Understanding Digital Investigation; Digital Evidence; Sources of Digital Evidence; Digital Evidence Challenges

 SECTION 2: Digital Forensics
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: Introduction to Digital Forensic; Digital Forensics Principles; Digital Forensics and Incident Response Processes; Building and Maintaining a Digital Forensics Capacity

 SECTION 3: 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 vitally important aspect of an investigation.
TOPICS: Introduction to Incident Response; Incident Response Challenges; Building and Maintaining an Incident Response Capacity

 SECTION 4: 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.
TOPICS: Introduction to Forensic Readiness; The need for Forensic Readiness

 SECTION 5: Digital Acquisition Evidence 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.
TOPICS: Forensic Acquisition Principles and Standards; Understanding Forensic Images; Forensic Acquisition Processes; Acquisition Challenges

 SECTION 6: Digital Forensic Analysis
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.
TOPICS: What Can Forensic Analysis Prove; Planning the Examination; The Art and Science of Forensic Analysis; Forensic Examination and Analysis Standards

 SECTION 7: 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.
TOPICS: Ongoing Documentation; Presenting Your Findings; Reports and Presentations

 SECTION 8: 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.
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.