FORENSICS 585

Hands On | Six Days | Laptop Required | 36 CPEs

NEW

FOR585: Advanced Smartphone Forensics

It is rare to conduct a digital forensic investigation that does not include a smartphone or mobile device. Often, the smartphone may be the only source of digital evidence tracing an individual's movements and motives and may provide access to the who, what, when, where, why, and how behind a case. FOR585 teaches real-life, hands-on skills that enable digital forensic examiners, law enforcement officers, and information security professionals to handle investigations involving even the most complex smartphones available today.

FOR585: Advanced Smartphone Forensics focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. ***Don't miss the NEW FOR585!***

The hands-on exercises in this class cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones. This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensic professionals. ***It's time to get smarter!***

Who Should Attend

- Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and files they accessed
- Information security professionals who respond to data breach incidents and intrusions.
- Incident response teams tasked with identifying the role that smartphones played in a breach
- Law enforcement officers, federal agents, and detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- IT auditors who want to learn how smartphones can expose sensitive information
- SANS SEC575, FOR408, and FOR508 graduates looking to take their skills to the next level

You Will Be Able To

- Extract and use information from smartphones and mobile devices, including Android, iOS, Blackberry, Windows Phone, Symbian, and Chinese knock-off devices
- Understand how to detect hidden malware and spyware on smartphones and extract information related to security breaches, cyber espionage, and advanced threats involving smartphones
- Prevent loss or destruction of valuable data on smartphones by learning proper handling of these devices
- Learn a variety of acquisition methods for smartphones with an understanding of the advantages and limitations of each acquisition approach
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Recover artifacts of user activities from third-party applications on smartphones
- Recover location-based and GPS information from smartphones
- Perform advanced forensic examinations of data structures on smartphones by diving deeper into underlying data structures that many tools do not interpret
- Analyze SQLite databases and raw data dumps from smartphones to recover deleted information
- Perform advanced data-carving techniques on smartphones to validate results and extract missing or deleted data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (who communicated with whom, locations at particular times)
- Decrypt locked backup file and bypass smartphone locks
- Apply the knowledge you acquire during the six days to conduct a full-day smartphone capstone event involving multiple devices and modeled after real-world smartphone investigations

DFIR

digital-forensics.sans.org

585.1 HANDS ON: Smartphone Overview and Malware Forensics

Although smartphone forensic concepts are similar to those in digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. Today you will apply what you already know to smartphone forensic handling, device capabilities, acquisition methods, and data encoding concepts of smartphone components. You will also become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures.

Topics: Introduction to Smartphones; Smartphone Handling; Forensic Acquisition of Smartphones; Smartphone Forensics Tool Overview; Smartphone Components

585.2 HANDS ON: Android Forensics

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. Without honing the appropriate skills for bypassing locked Androids and correctly interpreting the data stored on the devices, you will be unprepared for the rapidly evolving world of smartphone forensics. Malware affects not only Androids, but also a plethora of smartphone devices. This section will examine various types of malware, how it exists on smartphones, and how to identify it.

Topics: Android Forensics Overview; Android File System Structures; Android Evidentiary Locations; Handling Locked Android Devices; Traces of User Activity on Android Devices; Malware and Spyware Forensics

585.3 HANDS ON: iOS Forensics

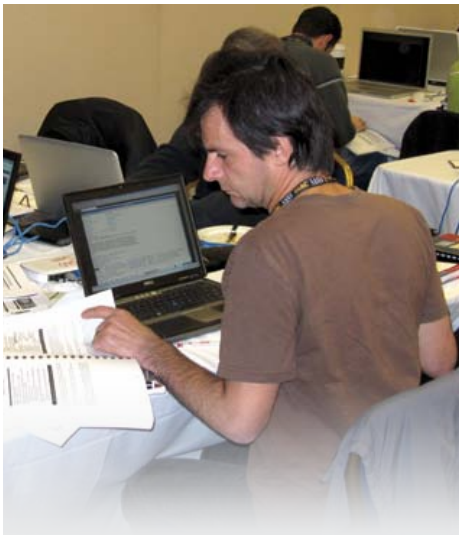
Apple iOS devices are no longer restricted to the United States, but are in use worldwide. iOS devices contain substantial amounts of data, including deleted records, that can be decoded and interpreted into useful information. Proper handling and parsing skills are required for bypassing locked iOS devices and correctly interpreting the data. Without the iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

Topics: iOS Forensics Overview and Acquisition; Handling Locked iOS Devices; iOS File System Structures; iOS Evidentiary Locations; Traces of User Activity on iOS Devices

585.4 HANDS ON: Blackberry and Backup File Forenics

Blackberry smartphones are designed to protect user privacy, but techniques taught in this section will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of the file system of Blackberry devices. Backup files are commonly found on external media and can be the only forensic acquisition method for newer iOS devices that are locked. Learning how to access and parse data from encrypted backup files may be the only lead to smartphone data relating to your investigation.

Topics: Backup File Forensics Overview; Creating and Parsing Backup Files; Evidentiary Locations on Backup Files; Locked Backup Files; Blackberry Forensics Overview; Blackberry Forensic Acquisition and Best Practices; Blackberry File System and Evidentiary Locations; Blackberry Forensic Analysis



FOR585 Training Formats

(subject to change)

Live Training
sans.org/security-training/by-location/all

OnSite
sans.org/onsite

vLive Events
sans.org/vlive

Simulcast
sans.org/simulcast

SelStudy
sans.org/selfstudy

585.5 HANDS ON: Third-Party Application and Other Smartphone Device Forensics

Given the prevalence of other types of smartphones around the world, it is critical for examiners to develop a foundation of understanding about data storage on multiple devices. Nokia smartphones running the Symbian operating system may no longer be manufactured, but it doesn't mean that they do not exist in the wild. You must acquire skills for handling and parsing data from uncommon smartphone devices. This day of instruction will prepare you to deal with "misfit" smartphone devices and provide you with advanced methods for decoding data stored in third-party applications across all smartphones.

Topics: Third-Party Applications on Smartphones Overview; Third-Party Application Locations on Smartphones; Decoding Third-Party Application Data on Smartphones; Knock-off Phone Forensics; Nokia (Symbian) Forensics; Windows Phone/Mobile Forensics

585.6 HANDS ON: Smartphone Forensic Capstone Exercise

This section will test all that you have learned during this week. In small groups, you will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.