

FOR585: Smartphone Forensic Analysis In-Depth



GASF
Advanced Smartphone
Forensics
giac.org/gasf

6
Day Program

36
CPEs

Laptop
Required

You Will Be Able To

- Select the most effective forensic tools, techniques, and procedures to effectively analyze smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device - we'll teach you how to know if the user created the data, if it was AI created or synced data which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover unparsed data stored on smartphones
- Tie a user to a smartphone on a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and crack iOS backup files that were encrypted with iTunes
- Extract and use information from smartphones and their components from Android, iOS, application directories, and SD cards
- 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
- Apply the knowledge you acquire during the course to conduct a full-day smartphone capstone event involving multiple devices and modeled after real-world smartphone investigations

SMARTPHONES HAVE MINDS OF THEIR OWN. DON'T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE, AI CREATED DATE, INCORRECT LOCATIONS, SMARTPHONE SUGGESTIONS, OR APPLICATION CACHE AS USER ACTIVITY. IT'S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Smartphone Forensic Analysis In-Depth will teach you those skills.

Every time the smartphone "thinks" or makes a suggestion, the data is saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You must understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data was put on the device. Consider AI vs human - how can a tool determine that level of granularity from a data set? Examination and interpretation of the data is your job, and this course will provide you and your organization with the capability to find and examine the correct evidence from smartphones with confidence.

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 23 hands-on labs, a forensic challenge, bonus labs, and a bonus take-home case that allows students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools. The course will also introduce community created tools that are designed to parse specific artifacts that compliment commercial tools.

FOR585 is continuously updated to keep up with the latest smartphone operating systems, third-party applications, acquisition short-falls, extraction techniques (jailbreaks and roots), file format changes, malware and encryption. This intensive six-day course offers the most unique and current instruction on the planet, and it will arm you with mobile device forensic knowledge you can immediately apply to cases you're working on the day you leave the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's time for the good guys to get smarter and for the bad guys to know that their smartphone activity can and will be used against them!

SMARTPHONE DATA CAN'T HIDE FOREVER – IT'S TIME TO OUTSMART THE MOBILE DEVICE!

Section Descriptions

SECTION 1: Smartphone Overview, Fundamentals of Analysis, and SQLite Forensics

Although smartphone forensic concepts are similar to those of digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. On this first course day, students will apply what they know to smartphone forensic handling, device capabilities, smartphone components, common file formats used for data storage, SQLite database examination, and query development. Students will become familiar with the most popular forensic tools required to complete comprehensive examinations of smartphone data structures.

TOPICS: Course Resources; The FOR585 VM; Smartphone Fundamentals; Smartphone Handling and Acquisition Terminology; Cellebrite Physical Analyzer Fundamentals; AXIOM Fundamentals; File Formats Overview; SQLite Overview; Bonus Materials

SECTION 3: iOS Device Forensics

Apple iOS devices contain substantial amounts of data that can be decoded and interpreted into useful information. Proper handling and parsing skills are needed to extract information from iOS devices and correctly interpret the data. This course section will cover extraction techniques using jailbreaks and exploits to obtain a Full File System acquisition. Without 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 Overview and Device Acquisition Considerations; Basic Device Information; Native Applications; Native Logs; Location Artifacts; Advanced Analysis; Bonus Materials

SECTION 5: Third-Party Application Analysis

This course day starts with third-party applications across all smartphones and is designed to teach students how to leverage third-party application data and preference files to support an investigation. The rest of the day focuses heavily on secure chat applications, recovery of deleted application data and attachments, mobile browser artifacts, and knock-off phone forensics. The skills learned in this section will provide students with advanced methods for decoding data stored in third-party applications across all smartphones. We will show you what the commercial tools miss and teach you how to recover these artifacts yourself.

TOPICS: Forensic Challenge Prep; Third-Party Application Overview; Geolocation Artifacts; MDM and MAM; File Sharing Artifacts; Payment Apps and Mobile Wallets; Messaging Applications; Mobile Browsers; AI Applications and Related Artifacts; Dissecting Python Code for Mobile App Parsing

SECTION 2: Android Forensics

Android devices are among the most widely used smartphones in the world, which means they surely will be part of an investigation that comes across your desk. Unfortunately, gaining access to these devices isn't as easy as it used to be. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills to acquire the best dataset and correctly interpret the data stored on them, you will be unprepared for the rapidly evolving world of smartphone forensics. Android data acquired using tools may exist in various formats. Often data will be missing if a Full File System acquisition is not obtained. Smartphone examiners need to understand the file structures and how to parse the data.

TOPICS: Android Overview and Acquisition Considerations; Basic Device Information; Native Applications; Location Artifacts; Native Logs and Advanced Analysis; Android Fitness and Health Applications; Bonus Materials

SECTION 4: Backups and Cloud Data, Malware and Spyware Forensics, and Detecting Evidence Destruction

iOS backups are extremely common and are found in the cloud and on hard drives. Users create backups, and we often find that our best data can be derived from creating an iOS backup for forensic investigation. Android backups differ a bit as users do not commonly backup outside of Network Service Providers and Google. This section will cover methodologies to extract backups and cloud data and analyze the artifacts for each. Malware affects a plethora of smartphone devices. We will examine various types of malware, how it exists on smartphones, and how to identify and analyze it. Most commercial smartphone tools help you identify malware, but none of them will allow you to tear down the malware to the level we cover in this class. We'll conduct five labs on this day alone! The day ends with students challenging themselves using tools and methods learned throughout the week to recover user data from intentionally altered smartphone data (deleting, wiping, and hiding of data).

TOPICS: Backup and Cloud Considerations; Google Backups; Apple Backups; Locked iOS Backup Files; iCloud Backups; Malware and Spyware Forensics; Detecting Evidence Destruction; Bonus Materials

SECTION 6: Smartphone Forensic Capstone Exercise

This final course day will test all that you have learned during the course. Working in small groups, students will examine three smartphone devices and solve a cold case 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.

TOPICS: Identification and Scoping; Forensic Examination; Forensic Reconstruction; Bonus Materials

Who Should Attend

- Experienced digital forensic examiners
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- Accident reconstruction investigators
- IT auditors
- Graduates of SANS SEC575, FOR308, FOR498, FOR563, FOR500, FOR508, FOR572, FOR526, FOR610, or FOR518 who want to take their skills to the next level

NICE Framework Work Roles

- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)

“Mobile phones have become increasingly prevalent in digital investigations, and this course equips examiners with the latest techniques to perform a holistic examination.”

—Bilal Malik, Stroz Friedberg



GASF

Advanced Smartphone Forensics
giac.org/gasf

GIAC Advanced Smartphone Forensics

The popularity of mobile devices in our work and personal lives has become increasingly broad and complex. The volume and type of data that these devices carry such as contact lists, email, work documents, SMS messages, images, internet browsing history and application specific data make them important for the individual who carries the device and allows for a rich source of data for forensic examinations.

- Fundamentals of mobile forensics and conducting forensic exams
- Device file system analysis and mobile application behavior
- Event artifact analysis and the identification and analysis of mobile device malware