SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

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

- Locate critical evidence on iOS and Android and determine exactly how data got there
- Recover deleted, unparsed, and obfuscated mobile data that commercial tools miss
- Manually decode third-party application artifacts when tools provide zero support
- Validate location artifacts and confidently identify false positives before court
- Detect, isolate, decompile, and analyze mobile malware and commercial spyware apps
- Leverage AI assistants safely to build Python scripts and SQL queries for analysis
- Extract evidence from locked devices, encrypted containers, and secure messaging

Business Takeaways

- In-house smartphone forensic capability eliminates outsourcing delays and reduces costs
- Time to evidence is critical—volatile mobile data can purge within hours of seizure
- Open-source tools taught in class supplement or replace expensive commercial licenses
- Examiners who validate findings produce court-ready reports that withstand scrutiny
- Mobile malware analysis skills prepare incident response teams for emerging threats
- Staff trained on manual recovery techniques extract evidence when tools fail entirely

Hands-On Labs and Practical Application

FOR585 includes 22 hands-on labs, two optional bonus labs, and a comprehensive capstone CTF exercise. Every lab teaches a technique you will apply to real casework the week you return to your organization.

Labs cover the full spectrum of smartphone forensic challenges:

- Android and iOS artifact recovery from full file system extractions, not filtered tool outputs
- Third-party application parsing when commercial tools provide no support whatsoever
- Location artifact validation including identification of false positives before you report them
- Mobile malware detection, isolation, decompilation, and behavioral analysis
- Evidence destruction detection on devices where users attempted to delete, wipe, or hide data
- AI-generated content identification using operating system metadata and multi-tool validation
- AI-assisted forensic scripting to accelerate analysis without compromising case integrity

Each lab uses real device extractions with complete file systems. You will work with the same messy, complex data you encounter in actual investigations, not sanitized training datasets designed to make tools look good.

Why Artifact Interpretation Changes Everything

A smartphone lands on your desk. Commercial forensic tools extract gigabytes of structured data and present GPS coordinates placing the device at your crime scene on the date in question. The timestamps align. The location data looks solid. Case closed?

Not yet. That location artifact might be a traffic prediction the operating system cached; one the user never acted on and may never have seen. The timestamp could reflect when iOS or Android wrote data to the database, not when the user was physically present. The "user activity" your tool flagged with high confidence might be AI-generated content from a third-party app, data synced automatically from another device, cloud-cached information, or application prefetch that never involved human interaction at all.

Commercial forensic tools parse what exists on the device. They extract, decode, and present data in readable formats. What they cannot do is determine intent, context, or origin. They cannot tell you whether a human being created that artifact or whether the smartphone's operating system generated it autonomously. That interpretation is your job and making that determination correctly is what separates competent examiners from expert witnesses whose testimony withstands cross-examination.

This course teaches you how to make those determinations with confidence and defend them in court.

What Makes FOR585 Different from Other Mobile Forensics Training

Most mobile forensics courses teach tool operation: push buttons, generate reports, trust the output. FOR585 takes a fundamentally different approach. We prioritize interpretation over extraction because extraction without understanding produces dangerous conclusions.

You will learn which artifacts on iOS and Android devices you can actually trust, and which one's forensic tools routinely misinterpret. You will build test datasets to validate your tools against known ground truth. You will discover when commercial products report data incorrectly, misattribute system activity to users, or miss critical evidence entirely.

We cover the file formats that commercial tools struggle with most: protobuf structures in Android applications, levelDB key-value stores, iOS SEGB files, SQLite WAL journals containing deleted records, and REALM databases used by secure messaging applications. When your commercial tools fail to parse these formats—and they will fail regularly—you will know how to recover and decode the data manually.

You will write SQLite queries from scratch, joining tables across databases to surface relationships tools don't expose. You will leverage Python scripts and open-source parsers including ALEAPP, iLEAPP, and ArtEx to validate commercial tool output and recover artifacts those tools never found. You will learn to use AI assistants safely to generate custom parsing scripts without exposing sensitive case data to public systems.

Commercial Tool Licenses Included with Course Registration

Students receive substantial commercial tool access to continue learning after the course concludes. Your registration includes a 120-day Cellebrite Inseyets Physical Analyzer license, a 90-day Magnet AXIOM license, and Elcomsoft licenses for cloud data extraction and password recovery. These tools complement the open-source solutions taught throughout the course.

sans.org/for585

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

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

Build the foundation for advanced smartphone analysis: proper device handling for hot and cold acquisition states, acquisition terminology explained, and SQLite query development from scratch. Write complex table joins, parse databases manually, and learn exactly when tools report data incorrectly. Labs cover SD cards, Physical Analyzer, AXIOM, and SQL.

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 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. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills to 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 to ensure files containing the truth of the device usage are not overlooked.

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 3: iOS Device Forensics

Apple iOS devices contain substantial amounts of data that can be decoded and interpreted into useful information. Proper examination 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. With proper iOS instruction, you will be prepared 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 4: AI Impact on Mobile Forensics, Malware/Spyware Forensics, and Detecting Evidence Destruction

Generative AI is on the rise, and mobile devices are often the origin of many of these artifacts, thanks to the popularity and availability of AI capable applications in our application stores. As mobile examiners, we are often tasked with determining the authenticity of the artifacts that we have come to rely upon for investigations, so this section aims to explore our current tool capabilities combined with artifacts generated by the operating system to best identify the true source of the data. This section covers malware and evidence destruction as well, as no smartphone platform is immune to malware. 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: AI Applications and Related Artifacts; Malware and Spyware Forensics; Detecting Evidence Destruction; 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: Third-Party Application Overview; Geolocation Artifacts; MDM and MAM; File Sharing Artifacts; Payment Apps and Mobile Wallets; Messaging Applications; Mobile Browsers; Forensic CTF/Capstone Prep

SECTION 6: Smartphone Forensic Capstone Exercise

Apply every technique learned throughout the week in a gamified CTF environment using prior lab datasets plus new cold case evidence from multiple smartphone devices. Work individually or in teams answering investigation questions covering identification, attribution, timeline, and motive. Prove that you can decode complex data under real pressure. By requiring students to answer a variety of questions at different skill levels, this capstone exercise will test the students' understanding of the techniques taught during the week. OnDemand students have the opportunity to participate in the CTF just as students in Live classes do.

TOPICS: Identification and Scoping; Forensic Examination; Forensic Reconstruction

Continuous Updates Reflecting Current Device Behavior

FOR585 undergoes continuous revision to address new iOS and Android releases, emerging third-party applications, and evolving file format structures. The artifacts that mattered two years ago may be deprecated today. The applications dominating current investigations may not have existed when other courses were written.

When you take FOR585, you learn current device behavior from instructors who actively work cases and contribute to the forensic research community. Your training reflects what devices do today, not outdated assumptions from legacy course 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, FOR498, FOR500, FOR508, FOR528, FOR572, FOR577, FOR589, 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)

> **"This class has been amazing. I've learned so much in such a short amount of time. I'm ready to go back to work and use these new skills."**
>
> —Stephen W., **Seminole County**

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