2024 COURSE UPDATE

FOR585

SMARTPHONE FORENSIC ANALYSIS IN-DEPTH

FOR585 builds in-depth digital forensics knowledge of artifacts and application data existing on Android and iOS devices. Learn how to analyze and validate smartphone artifacts, track individual user activity on the device, and organize findings for use in accident reconstruction, incident response, internal investigations,, and civil or criminal litigation. New skills provide the means to validate smartphone findings, speak intelligently to how the data was created on the device, and uncover artifacts not parsed by popular smartphone tools.

US Court Orders Pegasus-Maker NSO to Provide Documents on Its Products to WhatsApp

Source: FBI PSA I-050422-PSA

Spring 2024 Update

The new update focused on testing and documenting significant changes across iOS, Android, third-party application storage formats, malware, and AI applications. Brand new hands-on labs were created, taking advantage of the latest tool advancements to help you understand the new formats and new artifacts.

NEW CONTENT

- File formats have changed on iOS and Android devices. The course material has been updated to reflect the most common data formats, methods for analyzing each format, and the expected content for each.
- A complete re-structure of Android and iOS forensics, logs and files of interest, and methods for diving below the surface to conduct forensic examinations.
- Updated cloud and backup data from multiple sources to include extraction and analysis. Cloud data may be the only source of evidence if the smartphone is locked or inaccessible.
- AI is being used everywhere and data on the smartphone may help you identify how an artifact was created. AI applications are starting to play an important role in investigations.
- LevelDB is playing a major role in application and Browser storage. Understanding how to analyze these data formats is required.

UPDATED FEATURES

- Methods for carving and identifying location artifacts have improved and community research has led to a better understanding of trusted locations you can rely upon for investigations on iOS and Android devices.
- As we rely more and more on AI, traces are left behind of these interactions with apps, such as ChatGPT. Determining if a chat was created by a human or AI is possible when you deep-dive into the application.
- Smartphone components, such as SD cards, are often overlooked during a forensic extraction. The data stored on these components often contain application data relevant to investigations. Method for proper acquisition and analysis matter for SD and SIM cards.
- Android 14 and iOS 17 introduced changes in files and new features that can be examined for relevance to an investigation. These key files and how the data exists were researched and added to the sections of this course.

LAB REFRESH

- Nearly every lab was re-written along with new datasets to showcase new OS version, tool updates and capabilities.
- New labs on SQLite forensics focuses on complex time conversions and table joins.
- A new lab focusing on AI chat apps, ephemeral apps, and deletion teaches on methods to uncover the hidden content.
- Multiple labs focusing on Full File System extractions from iOS and Android datasets to teach methods for places devices in locations when specific applications were used.
- Datasets are provided without a forensic extraction to encourage examiners to learn the file structures, methods for searching and understanding the application data.

GIAC ADVANCED SMARTPHONE GASF FORENSICS

GIAC Advanced Smartphone Forensics (GASF)

The global forensic technology market is expected to expand at a “stunning” compound annual growth rate of 10.9%, generating almost 28 billion dollars per year by 2028. Source: Vantage Market Research

For more information:
sans.org/FOR585

SANS | GIAC CERTIFICATIONS