I recently had the opportunity to beta test the soon to be released SANS 585 Smartphone Forensics course and I wanted to share some thoughts about the course content and the labs.

The course page on the SANS website (http://www.sans.org/event/for585-advanced-smartphone-mobile-device-forensics/course/advanced-smartphone-mobile-device-forensics) provides an accurate overview of each day's topics so I'll focus more on thoughts and opinions than lists.

Overview

The course starts with an overview of cellular technology and networks and quickly moves on to explore advanced topics. The jump from the basics into topics like wear leveling, garbage collection and so on is an earmark of a SANS forensics course, which is one of the reasons why I love these courses so much. The refresher of the basics is nice, but the integration of advanced issues – which is where many of us need the help – is nothing short of awesome. Throughout all five days, the course provides full-page examples that demonstrate the concepts explained within the content.

The initial section on parsing the contents of a SIM in hex is a smooth introduction into a course that delivers a healthy dose of hex each day. It's important to understand that the emphasis on hex is never "hex for the sake of using hex."

Hex is used to locate and parse artifacts that commercial programs will not automatically parse and for digging for deleted artifacts not present in the tools' reporting mechanisms. One lab shows a tool reporting six entries in an application. Analyzing the underlying sqlite database confirms that the table does indeed have six entries. You can then look at the sqlite database in hex to uncover how many messages were not picked up in the report. This course is full of tricks of the trade that can make huge differences in efficacy in real world settings.

Also, the labs are all incredible and the 'answers' sections at the back of each lab are perfect. They don't just give an answer; they give detailed walkthroughs with plenty of screenshots. It's another testament as to how meticulous, knowledgeable and detail-oriented the course – and its designers – are.

Day One

The core concepts section covers the basics and continues with the overview of smartphone handling and acquisition and a tool overview. The course moves on to using FTK imager to examine an SD card and to parsing SIM card data at the hex level. The first day ends with a section on general mobile device repair that provides an overview of resources, tools, and tips.

Day One's appendix is a step-by-step guide to acquire data utilizing Cellebrite, XRY and Oxygen. Students who already perform mobile device forensics on a daily basis may not crack open this section of the book, but it contains great walkthroughs with plenty of pictures and is a great reference for those who are new to these tools.

Day Two

Day Two provides a detailed look at the Android file system, including where certain types of evidence may be located. While this section makes up the bulk of the day, the section at the end is where I'd like to share my observations.

The last part of Day Two starts off with a talk about malware and using Cellebrite PA to scan devices for malware. It also includes a few slides that introduce various Android spyware programs, available for purchase on the internet, and then show artifacts that these different applications could leave on a device. Mobile device spyware applications aren't something that I look for on a regular basis, but this will be a fantastic resource for those times when I am in need of this information.

The appendix contains a guide to examining an image in Internet Evidence Finder and using XRY to parse a Samsung Kies backup.

Day Three

Day Three is for iOS devices and provides an in-depth look at the iOS file system and where certain types of evidence may be located. It also includes information on how to identify if a device has been jailbroken or wiped, how to recover data from third-party communication applications, and so on. In addition, there is some tool-specific content, including keyword searches and timeline generation.

Day Four

Day Four is split in half, with the first portion covering Blackberry devices and the second covering forensics on backup files.

The Blackberry device presentations are extremely in depth and include familiarization with Blackberry artifacts at the hex level.

Several of the 585 labs do a solid job of reinforcing the concept that an examiner should use multiple tools to examine a device. However, one of the Day Four labs takes it to the next level by having the student examine a Blackberry device using four different methods. The student is given a list of questions to answer, and every one of the four examination methods used in the lab will reveal artifacts that the other three do not.

Day Five

Day Five is a grab bag day that covers Windows mobile, Nokia & Symbian, knock-off devices and third party applications.

The Nokia & Symbian section does a great job covering the file system and artifacts down to the hex level. The next time I have a question concerning a device running these operating systems, this book will be the first thing I reach for.

The Windows Mobile forensics section covers several topics including Windows Mobile registry analysis and usage artifacts.

The knockoff section provides both a good overview of dealing with clones and some specific guidance and examples for artifact parsing.

The final section discuses different types of third party applications on iOS and Android devices and parsing these types of applications.

The Day Five appendix gives a step-by-step walkthrough for using a Cellebrite PA with CHINEX to examine a clone phone.

Conclusion

I've taken multiple mobile device forensics courses, including the SANS 563, and can say with the utmost confidence that this course is phenomenal. The books will be an invaluable desk reference the next time I'm poking around inside a file system, and the labs do a great job re-enforcing lessons taught in the course.

The topics covered in the course can be considered advanced but are also very practical. Topics such as parsing and searching devices not supported by commercial tools and digging in hex for deleted artifacts are extremely important and not incredibly intuitive to try to learn through trial and error.

In closing, this course is a much needed – and valuable addition – to the SANS forensics course lineup.

Reviewed by

Matthew Edmondson,
CISSP, GCFA, GCIH, CEH, GWAPT, GSEC, GCFE
Website: www.DigitalForensicsTips.com
Email: Matt0177@gmail.com