

## Course Review: Digital Mobile Forensics Deep Dive

David Caissy, CISSP, GPEN, GSEC, CEH, PMP, B.Sc.A.

Digital Mobile Forensics Deep Dive is a 3-day course written and taught by Wayne Burke of Securit. I decided to take this course to expend my knowledge into a field I barely knew. Being a penetration tester with a background in web application development, I was completely new to the forensic world. Since the official web site stated that this was a "highly advanced and technical course," I honestly expected to be completely lost. I thought I would learn more from home after the class, trying to slowly digest what the instructor said. With the site also stating that "about 80% of the course is focused on practical REAL WORLD hands-on lab scenario exercises," I decided to buy an airplane ticket and give it a try.

I received the lab requirements by email directly from the instructor, Wayne Burke. The email included the laptop specifications and software that had to be installed such as VMware Workstation. The instructor also mentioned needing Backtrack 5 and CAINE (Computer Aided INvestigative Environment) virtual machines. So I cleaned up some space on my laptop, downloaded what I needed and installed the two VMs. I was eager to start the class.

Discuss in Forums {mos\_smf\_discuss:/root}

## Day 1

Arriving early in the classroom, I had plenty of time to get settle and talk a bit with Wayne. My first impression was very good: nice room, plenty of space, detailed course notes and a motivated teacher.

After a short introduction, the course started on the &ldquo;Digital Forensics Fundamentals and Legal Practices&rdquo; module. We were introduced to the differences between criminal and civil incidents, the evolution of digital forensics, computer fraud and various laws around the world. This section wasn't specifically directed at mobile devices, but I felt it was a necessary introduction to the course. The pace was good, and, although experienced forensic investigators would not have learned much, it prepared us well for the remainder of the class.

We then moved to our first exercise: Installing and Running CAINE in VMware Workstation. As mentioned earlier, I had already installed the VM at home prior to the class, and I didn't understand why we had to spend 20 minutes doing it in the class. But to my surprise, a few students were not prepared and therefore struggled to complete the exercise. I asked myself, isn't this a highly advance and technical course? Hmmm...

The second module was &ldquo;Mobile Hardware Design for iPhone, BlackBerry, Android and Other Devices.&rdquo; We started by looking at the hardware evolution of the iPhone and a few other phones. It was interesting to see the difference between each generation of devices with manufacturers making them more and more secure. We then proceeded to download the Android System Development Kit (SDK) and Eclipse, an open source IDE. In addition to this massive download, the Android SDK was itself downloading many components. Twelve students sharing one Internet connection didn't make the download very effective. In fact, it took several hours before we all had the tools downloaded. I found it strange that we didn't have the software already on our course DVD. Or better yet, how about having it already installed in a virtual machine? But since we were only to use these tools on Day 2, I thought this wasn't a big deal. For the subsequent downloads, we started sharing USB thumb drives to save time (you've got to trust your neighbour!). I honestly felt disappointed spending a couple of hours on a task that we could have easily done at home. But again, some people in the class found this to be a challenge.

In the third module, &ldquo;Mobile Software Design and the Typical Boot Process for Smart Devices,&rdquo; we started by analyzing common boot processes. At this point, the course started to be technical. We looked at the differences between the Recovery Mode and Device Firmware Update (DFU) mode and how an attacker could leverage them to access the device's data. We then looked at the Zdziarski technique and how to perform a bit-by-bit copy of an iPhone device. This was an interesting module for those new to the forensic field. The lab was about launching and troubleshooting the Android SDK. But since many people were not done downloading and installing it, it was postponed to Day 2. So maybe with a little more stress by the instructor before the course, there could have been much less time wasted.

All and all, I felt disappointed by the first day. While I learned a few good concepts, I expected a lot more hands-on exercises. And by exercises, I don't mean downloading and installing software for about 3 hours, but performing actual forensics on mobile devices. I was hoping for a lot more on the second day.

## Day 2

We started the second day with the module titled "Mobile Device Storage and Evidence Acquisition Techniques." We went deeper in data copy techniques and explored various disk partitioning concepts (from Windows to the iPhone). We also learned how to acquire evidence properly, so it can be admissible in court. While some of these concepts related to forensic investigation in general and not just mobile devices, other sections were dedicated to the iPhone.

In the lab, we learned how to use dd to create an exact image of a file system partition and how to combine it with netcat to add network capabilities. Overall, this was an excellent module. Not only did I learn a lot of new theory, but I got to practice new techniques in the lab. So far, Day 2 was much better than the previous day.

We went over the short Module 5: "Mobile Forensic Hardware and Software Field Kits DIY" rather quickly. It was a succession of both commercial and open source digital forensic toolkits, focusing on the pros and cons of each. Instead of working on the lab (which we can always do at home), the instructor gave us a real demo with an iPhone 3G. I found it very interesting to see a live example, with the usual problems associated with demos and the way the instructor solved them. The instructor was quite entertaining and gave us lots of little tricks through the demonstration. At this point, it became clear to me that a professional digital mobile forensic investigator can get a lot of data from a mobile device. Another good module, thanks to the demo.

After learning how to collect data from mobile devices, we moved to Module 6: "Forensic Software, Evidence Analysis and Reporting." Like the previous module, we quickly went from one product to another while the instructor highlighted the differences between them. This was a gold mine for those looking to acquire forensic tools. In the lab, we installed Access Data Forensic Toolkit (FTK) and learned how to use its basic functionalities. The instructor finished the day with a demo of a commercial product.

The second day felt a lot better than the first one. I was starting to understand how digital forensic investigations were conducted. After the class, I left for a walk outside and came back an hour later to find that Wayne was still in the class trying to help two students catch up. It is only then that I realized the huge gap between the students: one was extremely knowledgeable and probably in the top 10 guys in the world doing mobile forensics (I learned a lot from him during the breaks!!), while others had problems installing and running VMware workstation. Because of that, the instructor seemed to have a hard time keeping everyone interested. At this point, I understood why we spent so much time installing software the first day. While I personally think that since those who registered knew it was going to be a technical course, the teacher should have kept it like that. I can't blame Wayne for slowing down to keep everyone on board, but levelling from the bottom wasn't a great idea. This surely didn't make the best students happy.

## Day 3

The last day of the class felt more relaxed than the second one. We started with Module 7: "Cryptography, Steganography, Malware and Password Recovery Techniques." We went over it pretty quickly, since we all knew quite a lot about cryptography before the class. Wayne did a demo of SET, the Social Engineering Toolkit. He showed us how easy it was today to launch phishing attacks and install malware on mobile devices. It was interesting to see his demo and everyone seemed to enjoy it.

After this, the instructor started to update all of his tools to the latest version, while we were waiting. This was a poor decision as the process took a lot of time and created problems later during the demos. Tools should have been updated and tested before the class.

We went over the last 2 modules very quickly. Module 8: "Court Approved Non-Standard Evidence Collection Deviations" and Module 9: "Final Report - Evidence Documentation" were both covered in less than 30 minutes.

At this point, you may have caught what was the biggest problem of this class: we spent a lot of time installing tools that we didn't even end up using in the labs! Many hours were lost, especially on day one, which made the modules in this 3rd day rushed due to time constraints. I felt that the time would have been much better spent on more hands-on experience. In the end, we didn't even use Backtrack and CAINE. This poor management of time is a mortal sin in a course that is only 3 days.

## Conclusions

I had mixed feelings about this class. Being new to the forensics field, I learned many good concepts and understood the basic methodologies. But I also felt that I could have learned a lot more from the class. While the instructor took the time to explain forensic concepts very well, most students felt that it was less technical than what the brochure suggested. While beginners will learn the concepts very well, experts in forensics would gain little from this class which lacks advanced hands-on exercises. In fact, an advanced forensic investigator who also took the course told me that he didn't learn a single thing. Seeing as though it was billed as an advanced course, I'm compelled to give this class a 5/10. However, it could easily be a 9/10 with a marketing focus on less advanced students and only a few slight adjustments from the instructor such as:

- Having a pre-built virtual machine distributed and set up in advance with all the tools installed would have saved almost a full day of class.
- A dedicated exercise on each of the main mobile devices (iPhone, Blackberry and Android) would have been a great addition.
- Stressing to students beforehand the importance of being fully prepared for a short 3-day course.

Mr. Burke is extremely knowledgeable in this field with many years of experience performing forensic investigations and penetration tests, so there were absolutely no problems there. And on the bright side, Wayne seems to be currently updating his class, because the name recently changed from "CAST 612: Digital Mobile Forensic Deep Dive" to "CAST 612: Advanced Mobile Hacking & Forensics"; I am sure the new version will be better.

Digital Mobile Forensics Deep Dive is a decent course for those new to forensic investigations taught by an energetic instructor who is undeniably an expert in the field. Topics that were introduced such as digital forensic fundamentals, mobile device boot process and storage, evidence acquisition techniques and forensic field kits were well covered. The same thing can be said about evidence analysis and reporting software. It's was disappointing that the claimed 80% hands-on exercises turned out to be much less, but this fact was partially saved by very good demonstrations by Wayne Burke. All in all, this course is on the cusp. Look for great things in the near future.

Mr. Caissy has 7 years of experience as an Information Security Specialist and 12 years as a Java Web Application Architect. He has performed security audits, web application penetration tests and designed several secure systems. In addition, he has handled multiple information security incidents, reducing data lost and minimizing impacts on compromised systems. Mr. Caissy also has significant experience in providing functional and technical solutions in Multi-Tier systems and Service Oriented Architectures. His experience ranges from creating architectures, analyzing existing systems, designing and maintaining relational databases to gathering requirements and writing specifications. He has implemented SOAP and REST web services and AJAX communications schemes. This mix of web application development experience with up-to-date security knowledge has lead Mr. Caissy to test several applications and systems for security vulnerabilities. He has the perfect background to perform web application vulnerability assessments, penetration testing and code reviews.