CS 444/544 Spring 2018 Lab 4

Lab 4 is due by 11:59pm on Friday, May 4th, 2018. University policy prevents me from having things due during finals week, so there will not be any extensions.

Send your writeup as a PDF attachment to crandall@cs.unm.edu.

Lab 4 is worth 100 points. You should try to answer the questions below, but the quality of your writeup and the investigative work you do are what the grade will be based on (*i.e.*, the questions are just to give you ideas what to look for and write about, and don't represent a grading rubric).

I will provide a single Android nonvolatile storage image. The uncompressed version is just under 32GB, so plan accordingly. "I didn't realize how much time/space it would take to download/unzip/carve the file" is not grounds for an extension. As always, start early and plan ahead. **YOU CANNOT PERFORM THIS LAB ON CS LAB MACHINES.** You need to be root and have a Linux machine (or virtual machine) of your own with enough hard drive space for not only the image but also the results. If you haven't already followed my advice of getting your own Linux machine (or virtual machine) to use, now is the time. The tools may or may nor work on Macs, they definitely will not work on Windows.

The backstory is that a rabbit poop beer smuggler (alias McLovin) was arrested here in Albuquerque, and you've been hired as a consultant by the ATFRP (Beureau of Alcohol, Tobacco, Firearms, and Rabbit Poop) to perform a forensic analysis of an image of the non-volatile storage on the alleged smuggler's phone. The alleged smuggler is from the Tamil region of India, and the accusation is that he is somehow smuggling rabbit poop beer into the country and then distributing it to rabbit poop beer fiends in Albuquerque.

As a starting point, I would perform file carving on the image. Then you can investigate any images (JPEGs, *etc.*), web histories, *etc.* found by the file carving process. Most chat applications will store chats unencrypted in SQLite databases. I can't guarantee that this will be the case, but parsing SQLite databases is a good second step after file carving. File carving will also show you images, and you can use apk files to infer which apps are installed on the phone. You should be able to find web histories and things of that nature via file carving, as well.

If you want to do something advanced, you can set the image up as a loopback device and mount it. File carving has the advantage of being able to recover deleted files, but it flattens all files by type and doesn't present to you the file system hierarchy. Mounting the image read-only can make it easier to explore the files that haven't been deleted.

You should have fun and explore the image, Lab 4 is not as formal as Labs 1 and 2 were. Here are some questions to guide you, but don't get caught up on trying to answer each one...

What applications are installed on the phone? Which ones were used to commit crimes?
Who are the major players in the rabbit poop beer smuggling and dealing ring? Where do they live and/or operate? Can you identify any rabbit poop beer fiends within our jurisdiction here in New Mexico? (Be sure to anonymize any real-world identifying information from the phone, such as phone numbers)
Are there other potential crimes in other jurisdictions that should be investigated? Where should those investigations begin?

What is the timeline of events that can be discerned from the image?
Were there any deleted messages?
Is there anything that could be use to “flip” others against the rabbit poop beer smuggler? *E.g.*, if he lied about the quality of his product or the source of an image or anything like that, that can be used to erode trust of the smuggler and help convince a fiend to testify against him.

You should produce a writeup (submitted as a single PDF) that is at least 5 pages, but can be more. You should have lots of visual aids in the writeup, most of it should be screenshots, figures, graphs or whatever and not too much text. The text is just to give context to what you found.

http://www.forensicswiki.org/wiki/Tools
scalpel and foremost (ext4 file carvers) are a good place to start, then you'll probably want to find a good SQLite parser/viewer, and perhaps check out the EXIF data on images.

You are expected to do your own work. From analyzing the image to writing the answers, for all phases of this project you should do your own work. Any instance of not doing your own work will be considered cheating. For your submission, if you copy even a single screencap or result from a classmate that will be considered cheating. If you're not sure whether something will be considered cheating or not, ask me before you do it. You are encouraged to discuss the assignment with your classmates at a high level. Exchanging tools, source code (which is not required for this assignment), and general thoughts about approaches to specific problems is okay. As a reminder of the course policy, if you cheat on any assignment in this class including this assignment (cheating includes, but is not limited to, representing somebody else's work as your own or having someone else do the assignment for you) you will receive an F in the class.

DO NOT share the phone's nonvolatile storage image with anybody outside the class, or make any use of real-world phone numbers contained in the image. It's simply not feasible to scrub all phone numbers from the image, so I have to trust that you guys will not save, store, report, share, call, message, or do anything with any of the phone numbers in the image. **In your report, you should anonymize the phone numbers and real identities** of anybody who was communicating with the phone or using the phone that the image is from.