CCSI460 Final Forensic Lab Report

Investigator’s Name: Matt Ferry

Date of Investigation: 9/12/2013

Lab Number and Title: Lab 2 – Current Issues in Digital Forensics

Summary of Findings:

For part one of this week’s lab assignment I chose to read an article entitled “Android forensics: Automated data collection and reporting from a mobile device”[[1]](#endnote-1). This particular paper focused very heavily on bring your own device (BYOD) device policies, and how companies need to have total monitoring abilities over these devices without requiring root access to the device itself, in particular through the use of an application currently in development called DroidWatch.

While I can understand the need for this type of monitoring because the growth of BYOD uses continue to grow, at the same time this type of software just screams total paranoia and zero trust. Maybe we are finally at that stage, where you can no longer trust anyone with anything, but the software covered in this paper tracks everything, even down to whether or not the devices screen is locked or unlocked.

In fact, because of what the software tracks, I can actually see this killing BYOD. Once a user fully understands the level of monitoring that will occur with the use of this software they will begin to consider BYOD devices as “work devices” that should be supplied by the employer rather than them bringing their own.

I say this because in section 4.1.2 of the paper it is specifically talking about User consent to monitoring, and how “The option to reject the user consent terms is also presented for the purposes of this research, although organizations may wish to omit this option in real deployments.”. I read this as by not allowing your employee’s an option to “Opt-Out” that they are also consenting to allowing their device to continue to be monitored for “Proper work usage” even when they are no longer at work.

A more appropriate form of implementation for this type of monitoring software would be to integrate this software as an application with network authentication functions and protocols so that in order to connect to the work network this software has to be installed and running. Then when the individual is no longer using the network they can disconnect from the network by closing this application.

This software package did have a couple of things that I did appreciate, and thought were good about it. One is that it does not require elevated user access (root) in order to function properly. This is because while some people may feel comfortable with “rooting” their phone, this is something that should not be done by everyone, and thus should not be a requirement for the software to function properly. And two, the software has the ability to be configured to start during the phone boot process, which prompts the user for consent to monitor. The article even mentions this as an advantage as there are other monitoring applications out there that are classified as spyware because they give the user zero notification of the program being run.

Details of Investigation:

9/12/2013

11:10 AM – Beginning part 1, reading a session paper from [www.dfrws.org](http://www.dfrws.org) and writing a report on the topic. Report chosen: Android Forensics: Automated data collection and reporting from a mobile device.

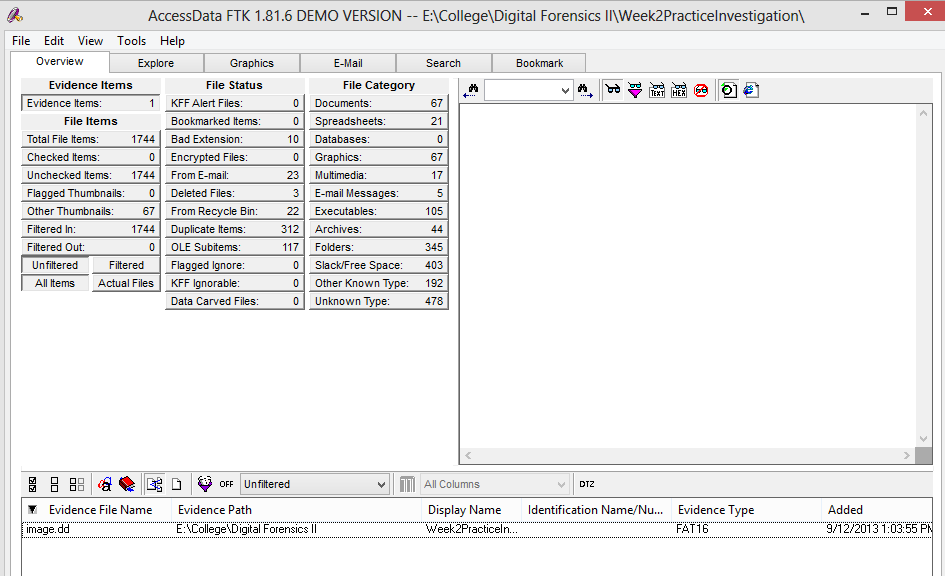
<http://www.dfrws.org/2013/proceedings/DFRWS2013-1.pdf>

12:10 PM – Wrote the summary report on my thoughts on this article.

01:00 PM – Finished with the rough draft of part 1, proceeding to part 2 and analyzing the image.dd file that was located downloaded for this weeks assignments.

01:00PM – Added the image.dd file as evidence to FTK.

01:07PM – Taking the requested screenshot of FTK after the image.dd evidence file has been processed by FTK.



9/15/13

1:30PM – Reviewed the assignment and made minor editing changes to the summary of the paper that I read.

1. <http://www.dfrws.org/2013/proceedings/DFRWS2013-1.pdf> [↑](#endnote-ref-1)