Ryan Lockman – Essay 1

A Trip to RMRCFA

On the day of March 3rd 2014 our class took a trip to the Federal Bureau's Rocky Mountain Regional Computer Forensic Agency. This essay will be an overview of my experience there and the impressions it left on me.

I arrived at ten in the morning and soon after we made our way to one of the back computer labs. We found out that our day consisted of a tour and presentation by supervising special agent Sean O' Brian. Over the coarse of the presentation special agent O' Brian explained many facts about the establishment. I learned that they specialized in digital forensics and digital forensics training via CART. At the top of the list on their agenda was terrorism and counter intelligence, but computer intrusion was a hot topic at the moment. The department also has a separate cyber investigation service and are the main place for investigating child exploitation. Special agent O' Brian stated that much of their work on investigating child exploitation was lurking through peer to peer traffic. We learned in class that this was one additional computer related crime that Colorado enforced besides the main three. Another important job for them is also expert witness testimony.

The whole RCFL network has 16 labs and 14 participating agencies. The one we were currently at was created in 2006. This location is an accredited lab which requires a standard operation of procedures, quality assurance policy, and expert witness. One of their specialties is the FTK toolkit, which we are going to be starting soon, and the Access Data lab tools, even offering a certification in EnCase. They do most of their work on Macintosh, Windows, Unix/Linux, Cellular Phone, PDA and surprisingly, camera related devices. A pie chart presented explained that ICAC involved 47 percent of their time, violent crimes 23 percent, white collar 17 percent, and an additional 13 percent divided out among the remaining crimes, computer related etc. You can tell they only have a small percentage of all crimes being investigated as computer related. Special agent O' Brian actually stated that one of the trends going around is that data is going up but cases are going down.

Once the presentation and talk by special agent O' Brian was over he kindly led us on a tour of the facility. The first thing, and one of the coolest I thought, was their triages. These kiosk machines, two of them, consisted of a loose media kiosk and a cellular phone kiosk. The phone kiosk was created by Cellebrite and I didn't get who made the loose media kiosk. The reason these caught my attention was the fact that it did a handful of tasks related to saving and analyzing your data. The loose media accepted many types of mediums for storage. The machine would organize the files by type and provided a very user friendly environment that you could use after a half hour of training. The Cellebrite kiosk had many phone hookups and allowed the transfer of data off of a device to another medium. Another nice aspect of these machines were the write blocks built directly in as to not accidentally overwrite or damage your sensitive data.

Next we had a quick view of the evidence room and a brief explanation of their chain of custody routine and case priority. We also got a nice look at the server room they

use. This was a very nice setup and consisted of two hot aisles and two cold aisles. After giving us a walk around the individual work stations of the employees special agent O' Brian took us back to the image processing room. He told us that they actually image everything over a network and that they used to do it on HDD but prefer the new method. The network has two parts, the examiner network and the decaf network which is used state and locally. One fact that astonished me was the size of the data analyzed each year which estimated out to 143 terrabytes last year. A pretty high amount considering special agent O' Brian said earlier that cases were going down.

The last part of the tour was a view of the cell phone examination station. This particular station served all of Colorado and all of Wyoming on the subject. The room even had a separate station just for the iPhone. One cool piece of equipment they used was called a fair day box/room. This was a special environment set up specifically to block RF signals form leaving or entering.

Sadly this was the end of our tour. After a quick round of applause for supervising special agent Sean O' Brian we were led back to the entrance. Overall the experience was great and gave a wonderful view of the everyday operations of a forensic lab. I leaned many facts, some obscure about the facility; such as the red and blue lights on the ceilings signaling who's present. My favorite part of the tour consisted of learning about each of the rooms they did their processing in and the main equipment used. Hopefully someday another chance will arise for another tour like this, or who knows, a job may be in the future somewhere.