Bowie Seniors Computer Club Minutes for Aug 21, 2008

Dan Lee presiding.

The minutes for Aug 7th were reviewed and accepted.

Dan announced that Baltimore Gas & Electric's IT department, is tentatively scheduled to provide a presentation at the Oct 16th meeting. Nothing yet scheduled for the Sept meetings.

Dan then introduced our guest speakers: Sgt John Boesman and Cpl Justin Brackett of the Computer Forensics Unit, Prince George's County Police Department.

We learned that Sgt Boesmana and Cpl Brackett are the Computer Forensics Unit and work on cases not only for Prince George's but also other nearby jurisdictions.

Cpl. Brackett related that there were only 879 certified computer investigative specialists in the United States and only 8 have been certified so far this year. He was formally trained at a school in Florida called IASIS, which stands for International Association of Computer Investigative Specialists.

As forensic specialists they must be able to get evidence from all sorts of devices in such a manner that they do not destroy the evidence and can explain in court exactly what they did and how so that the defense cannot successfully challenge it. They are certified experts in court.

They work on all kinds of devices that have memory--computers, PDAs, cell phones, IPods, GPS and even Playstations and X-boxs. If it has memory, a suspect may have stored information there. Usually they have to copy off whatever is in memory so as to reserve the original for vidence. They then go thru the records looking for evidence, 40-50% of the time they are looking for images in child pornography cases. Their other cases involve many kinds of crimes and in some they are not sure just what evidence they can expect to find. These are the toughest cases, for then they have to go through everything looking for any kind of clues to the crime.

In answer to a question, they believe that the Russians probably performed cyber attacks on the Georgians, and probably used a lot of computers all over the world, including in the United States to do this. This would have been done by using a Bot program to insert a program into unprotected computers, which under command would bombard computers, in this case Georgian government computers, with requests for service that overload and often shut down the server they run on.

In answer to another question, they say they spend about 2 days in any three month period in court. They said that the child pornography cases are usually plead out--for they can show thousands of images recovered from the suspect's computer and the evidence is thus overwhelming.

A typical raid/seizure is carried out early in the morning. Ten to twelve policemen usually secure the house. The Forensic Unit then goes in with the primary investigator and find the devices with memory, and document what they did. They take the devices back to their lab, and make forensic copies to a hard drive and then "hash" them so that the copy cannot be changed without leaving evidence that it was done. They then go thru a read only device so that they don't accidentally write anything to the copy.

With this copy they go looking for evidence, usually graphic files. They have a lot of equipment that will help them recover data from many different devices. For computers, they know to look in the registry for information. For

Bowie Seniors Computer Club Minutes for Aug 21, 2008

cell phones--each one is different. An additional problem with cell phones is that they are set to hold a limited number of messages and each new message wipes out the oldest message. They have tried to keep new messages from arriving, but it is difficult. They are now working on getting a shielded room where they can store and/or work on cell phones without losing the old messages.

When asked about encrypted information, the answer was they can decrypt many times and that they can call on Federal help if necessary. The question was raised about Steganography. This is a way of hiding images by slightly modifying bits describing a picture in such a minor way that it is not visible to the eye. A decoding program is used to search for the modifications to assemble an image that is being hidden. This of course would be a pretty sophisticated cloaking program and require some extremely good work to be able to detect that an image had been so stored and then to be able to recover it.

In answer to a question about using Kill Disk to overwrite once (with all 1s or 0s) on the hard drive of a home computer that is being disposed of, Cpl. Brackett said that this would ordinarily be sufficient-- it is possible to reconstruct the data but the cost would be more that the criminal would get by doing this.

We were reminded that anything that goes out to the web will be copied and archived so that we shouldn't put anything out there we don't want to come back to haunt us.

This was a very long program with lots of Q & A so when the presenters were done, we thanked them and adjourned.

BSCC Meeting Minutes submitted by Dale Grant