My First Autopsy

March 22, 2008 – 7:15 PM

I have a System Forensics class this quarter at ITT Technical Institute and this was my first true lab where I actually got to use the tools and resources against "real" data. We are doing a simulated case from The HoneyNet Project and here was the documented police report:

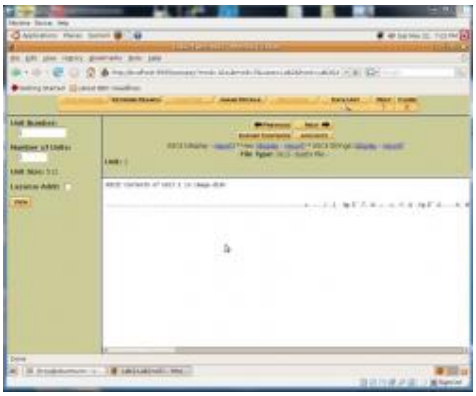
> The scenario is: Joe Jacobs, 28, was arrested yesterday on charges of selling illegal drugs to high school students. A local police officer posed as a high school student was approached by Jacobs in the parking lot of Smith Hill High School. Jacobs asked the undercover cop if he would like to buy some marijuana. Before the undercover cop could answer, Jacobs pulled some out of his pocket and showed it to the officer. Jacobs said to the officer "Look at this stuff, Colombians couldn't grow it better! My supplier not only sells it direct to me, he grows it himself."
>
> Jacobs has been seen on numerous occasions hanging out at various local high school parking lots around 2:30pm, the time school usually ends for the day. School officials from multiple high schools have called the police regarding Jacobs' presence at their school and noted an increase in drug use among students, since his arrival.
>
> The police need your help. They want to try and determine if Joe Jacobs has been selling drugs to students at other schools besides Smith Hill. The problem is no students will come forward and help the police. Based on Joe's comment regarding the Colombians, the police are interested in finding Joe Jacob's supplier/producer of marijuana.
>
> Jacobs has denied selling drugs at any other school besides Smith Hill and refuses to provide the police with the name of his drug supplier/producer. Jacobs also refuses to validate the statement that he made to the undercover officer right before his arrest. Upon issuing a search warrant and searching of the suspect's house the police were able to obtain a small amount of marijuana. The police also seized a single floppy disk, but no computer and/or other media was present in the house.
>
> The police have imaged the suspect's floppy disk and have provided you with a copy. They would like you to examine the floppy disk and provide answers to the following questions. The police would like you to pay special attention to any information that might prove that Joe Jacobs was in fact selling drugs at other high schools besides Smith Hill. They would also like you to try and determine if possible who Joe Jacob's supplier is.

> Jacob's posted bail set at $10,000.00. Afraid he may skip town, the police would like to get him locked up as soon as possible. To do so, the police have asked that you have the results fully completed and submitted by October 25, 2002. Please provide the police with a strong case consisting of your specific findings related to the questions, where the findings are located on the disk, processes and techniques used, and any actions that the suspect may have taken to intentionally delete, hide and/or alter data on the floppy disk. Good Luck!
>
> Any names, locations, and situations presented are completely made up. Any resemblance to any name, locations and/or situation is purely coincidence.

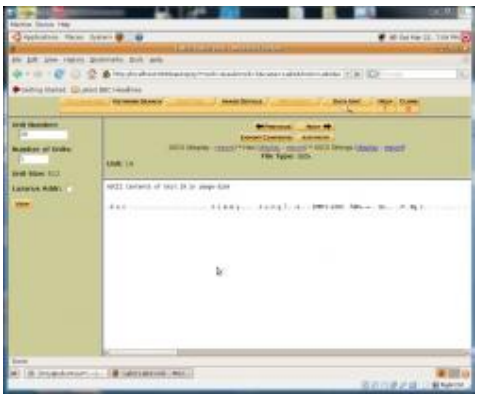
I am using Ubuntu 7.10 Linux and the Sleuth Kit/Autopsy forensics program. I was given the image of a 1.44MB floppy disk and asked to obtain as much information as I could get from it. I wasn't sure at first if the files were still intact or if they have been deleted from the disk to try and hide the evidence. I launched the Autopsy engine from a Terminal:

(each picture below is a thumbnail. Click for the full screenshot in a new window)

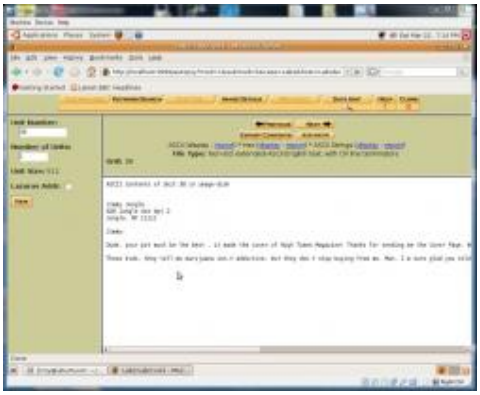
I then launched Firefox and browsed to the Autopsy home page and pointed the program to my image file. Having never used the program before, I fumbled around for a few minutes until I started to figure it out. I was then looking at the raw data that was on the floppy:



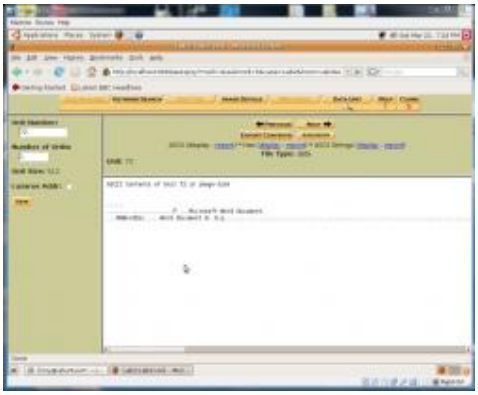
Browsing through the different data units (sectors of the disk) I stumbled upon something that caught my eye. At data unit 19 I started to see what looks to be filenames and possible extensions:



The next few units were empty so I knew that must have just been some kind of index of the files to come. I continued on sector by sector until I got to sector 38. I saw what appears to be a letter:

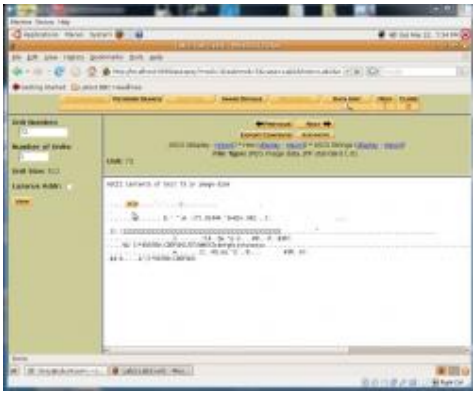


I backed up a few sectors until I saw the start of “something” and noted the sector number. It seemed to start at sector 33. I continued on until I saw what looked like the end of one thing and the start of another and documented that ending sector. That was sector 72. It also stated in the footer of the file that it was a Microsoft Word Document:

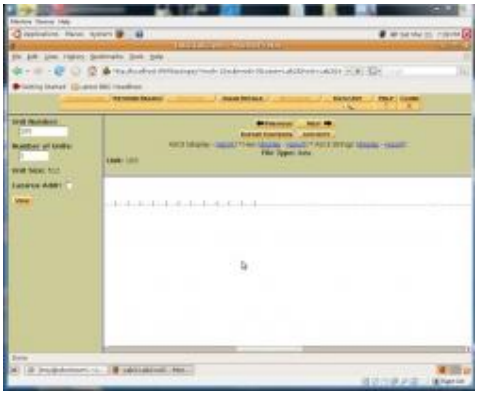


I knew this document spanned from sector 33-72 of the disk. I used Autopsy’s built-in export feature and exported sectors 33-72 as raw data and saved it to my desktop. I then renamed this raw export file to a .doc file and re-saved it. Sure enough, it opened up in OpenOffice and I could read it just fine:

First piece of evidence has been recovered from the disk. I moved on to the next sector and I saw another chunk of code starting with JFIF:

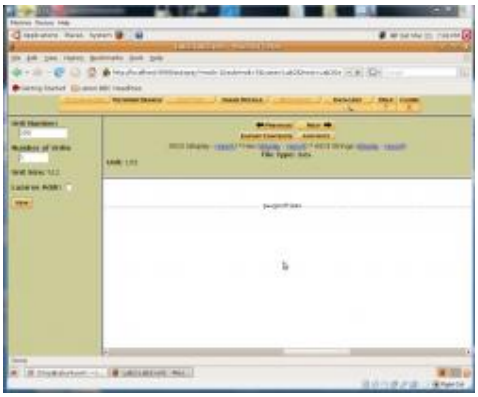


A quick Google search for JFIF revealed that this is in the header of all .jpg files. I knew then I had an image starting at sector 73. I continued on trying to find the end of the file. I came across what appeared to be the end of it at sector 103:

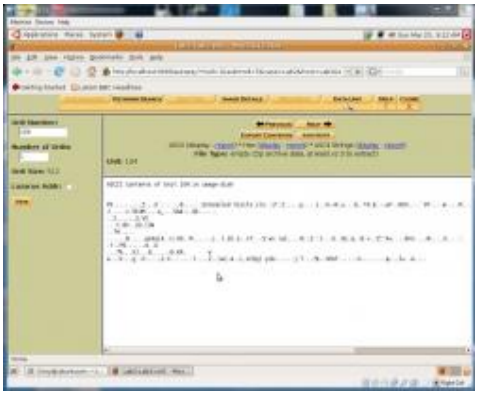


So again, I knew I had something – this time a jpg image – between sectors 73-103. I exported that raw data and renamed to a .jpg file. It then opened up with GIMP and showed me the image:

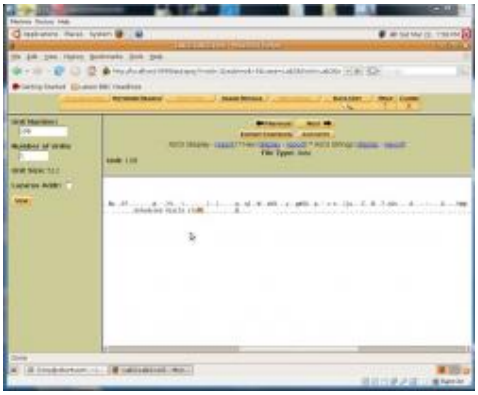
Two files successfully recovered. But I saw something else at the end of sector 103 that really stuck out. It doesn't take an expert to know that this is a password for something:



The next sector was 104 and this sector started with a PK. Again, a search or two or three on Google revealed that this is the header for a PKZip file. A few characters down it explicitly states a filename of Scheduled Visits.xls.

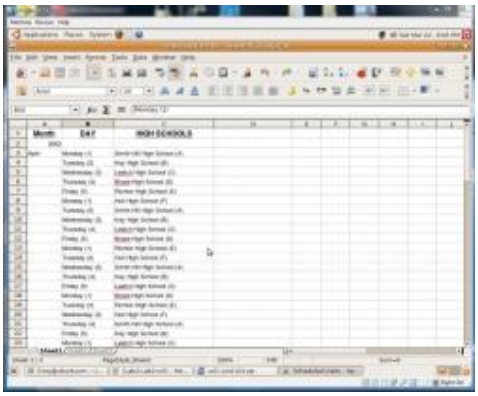


Putting two and two together to get five, I had a hunch that he had a password protected spreadsheet zipped up to easily send or distribute to somebody. I kept going through the sectors and finally saw the ending PK at sector 108:



I exported the raw data from sectors 104-108 and renamed it with a .zip extension. I tried to open it with the Archive Manager in Ubuntu and sure enough, it exposed the above named spreadsheet showing it as being password protected:

It prompted me for the password when I tried to open it and I keyed in the “goodtimes” password that I found at the end of sector 103 and it let me right in. Bingo. I found a spreadsheet of all his scheduled drug-selling “visits” at other high schools:



Continuing through the remainder of the sectors found nothing. The rest of the disk was blank. Three pieces of good evidence have been recovered against Jimmy Jungle.

Case closed.

You must be logged in to post a comment.

- Subscribe

Related Posts

- Repartition your hard disk on-the-fly with Vista
- Beginners Guides: Back up and Restore Data in WinXP
- Used Hard Drives Retain Data in eBay Sale
- Darik's Boot and Nuke Securely Wipes Your System in an Emergency
- High-Security Flash Storage
- Linux Shootout: 7 Desktop Distros Compared
- A Faster, Denser Hard Drive Debuts
- Dealing With Hard Drive Problems
- New Compression Tool Triples Network Storage
- Seagate ships world's most secure hard drive

Search PC Sympathy

Search

Site Links

- Log in
- Entries RSS
- Comments RSS
- WordPress.org