**EXPERIMENT 1**

**Greg Schardt Case Study**

Download the image files of Greg Schardt Case Study On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, Greg Schardt. Schardt also goes by the online nickname of “Mr. Evil” and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords. Find any hacking software, evidence of their use, and any data that might have been generated.

Attempt to tie the computer to the suspect, Greg Schardt.

1. What is the image hash? Does the acquisition and verification hash match?

2. What operating system was used on the computer?

3. When was the install date?

4. Who is the registered owner?

5. What is the computer account name?

We will use the forensics tool **Autopsy** for this experiment.

Autopsy is an open source digital forensics tool developed by Basis Technology, first released in 2000. It is a free to use and quite efficient tool for hard drive investigation with features like multi-user cases, timeline analysis, registry analysis, keyword search, email analysis, media playback, EXIF analysis, malicious file detection and much more.

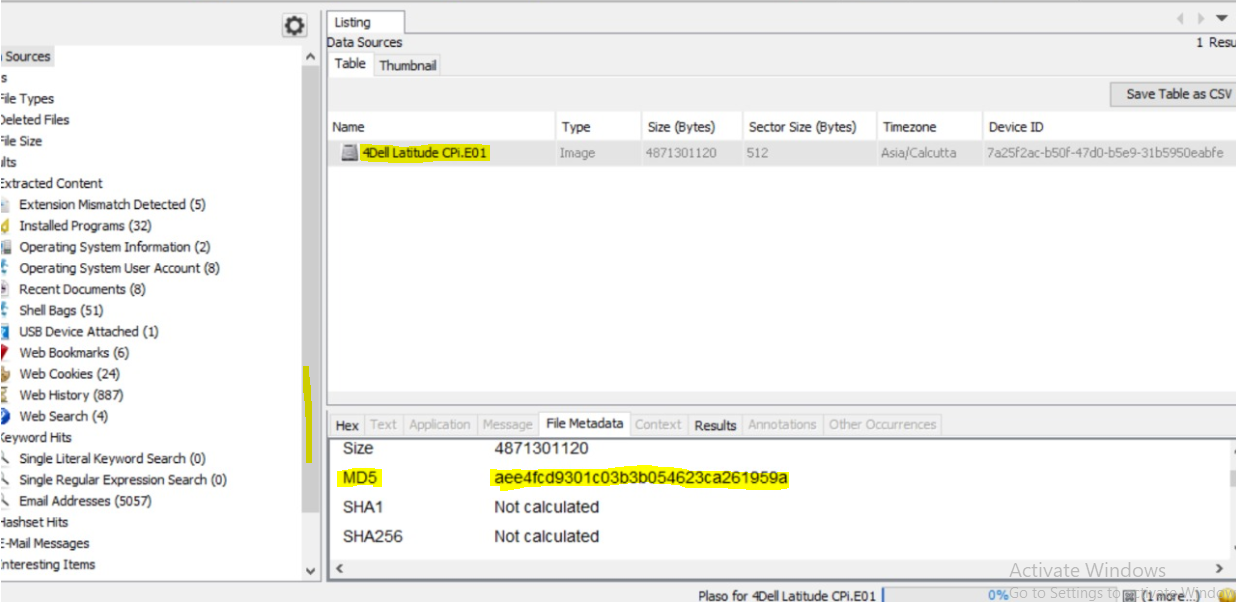
**Steps**

* First we will run Autopsy and select new case.
* Next step is to provide the Case name and the directory to store the case file. Then click on next.
* Add case number and Examiner’s details, then click on Finish.
* Now we will choose the required data source type, in this case Disk Image and click on Next.
* Select the path of the data source and click on next.
* Add the data source click on finish.
* Now we can start investigating

**Q1.** What is the image hash? Does the acquisition and verification hash match?

* **AEE4FCD9301C03B3B054623CA261959A.**

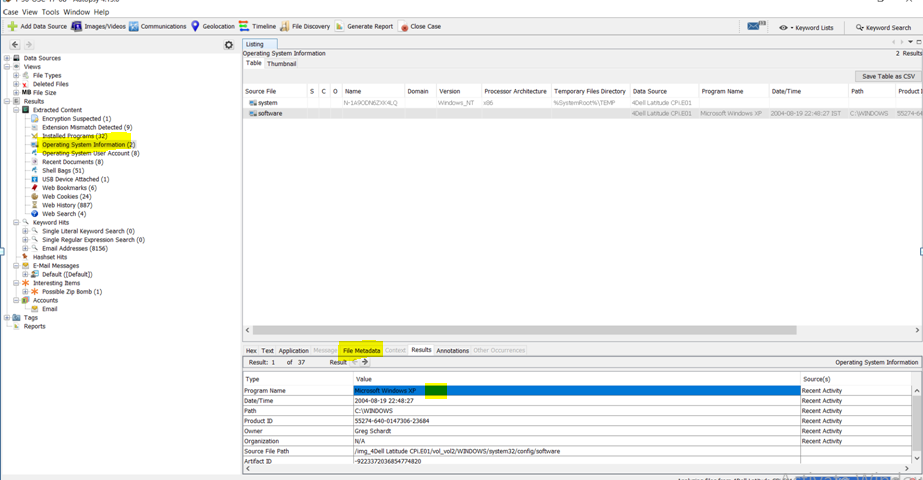
Found in metadata of the file



**Q2:** What operating system was used on the computer?

* **Microsoft Windows XP.**

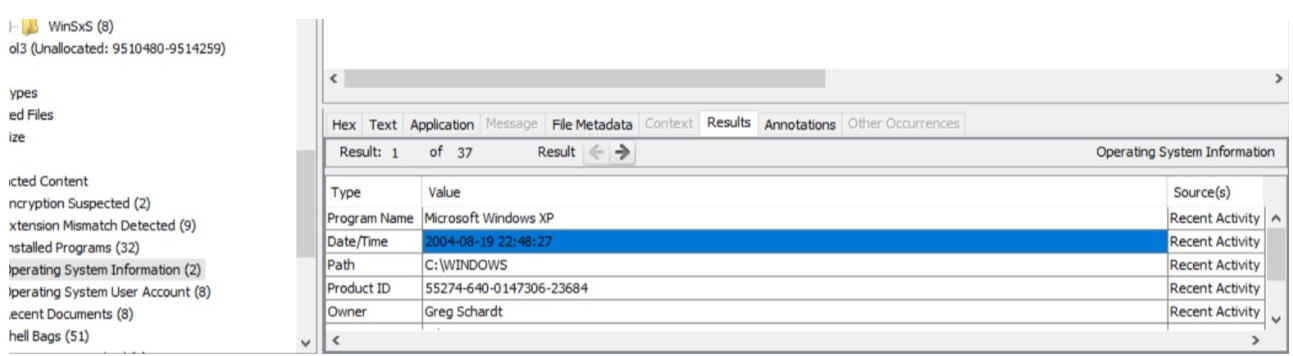
Steps: **For this, in the left side panel, we go to**Results > Extracted Content > Operating System Information**.**



**Q3:** When was the install date?

* **GMT**: **Thursday, August 19, 2004 10:48:27 PM**

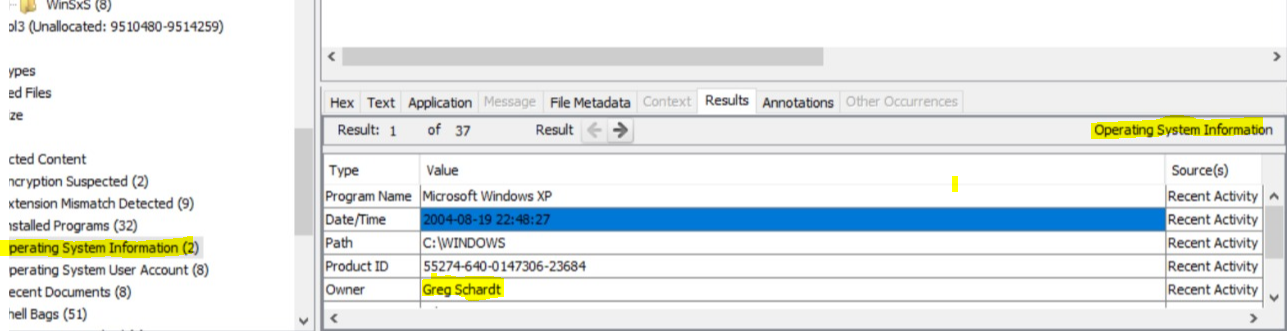
Similar to above: Results>Extracted Content>Operating System Information.



**Q4.** Who is the registered owner?

* **Greg Schardt**

Similar to above: Results>Extracted Content>Operating System Information.



**Q5.** What is the computer account name?

* **N-1A9ODN6ZXK4LQ**

Steps: It is a system information.

Go to Results(In the Left Pane)> Operating SystemInformation>select 'System'> resultstab> Name

