**Greg Schardt Case Study Part 2**

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.

Q1. When was the last recorded computer shutdown date/time?

Q2. How many accounts are recorded (total number)?

Q3.Who was the last user to logon to the computer?

Q4. List the network cards used by this computer?

Q5. What is the IP address and MAC address of the computer?

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

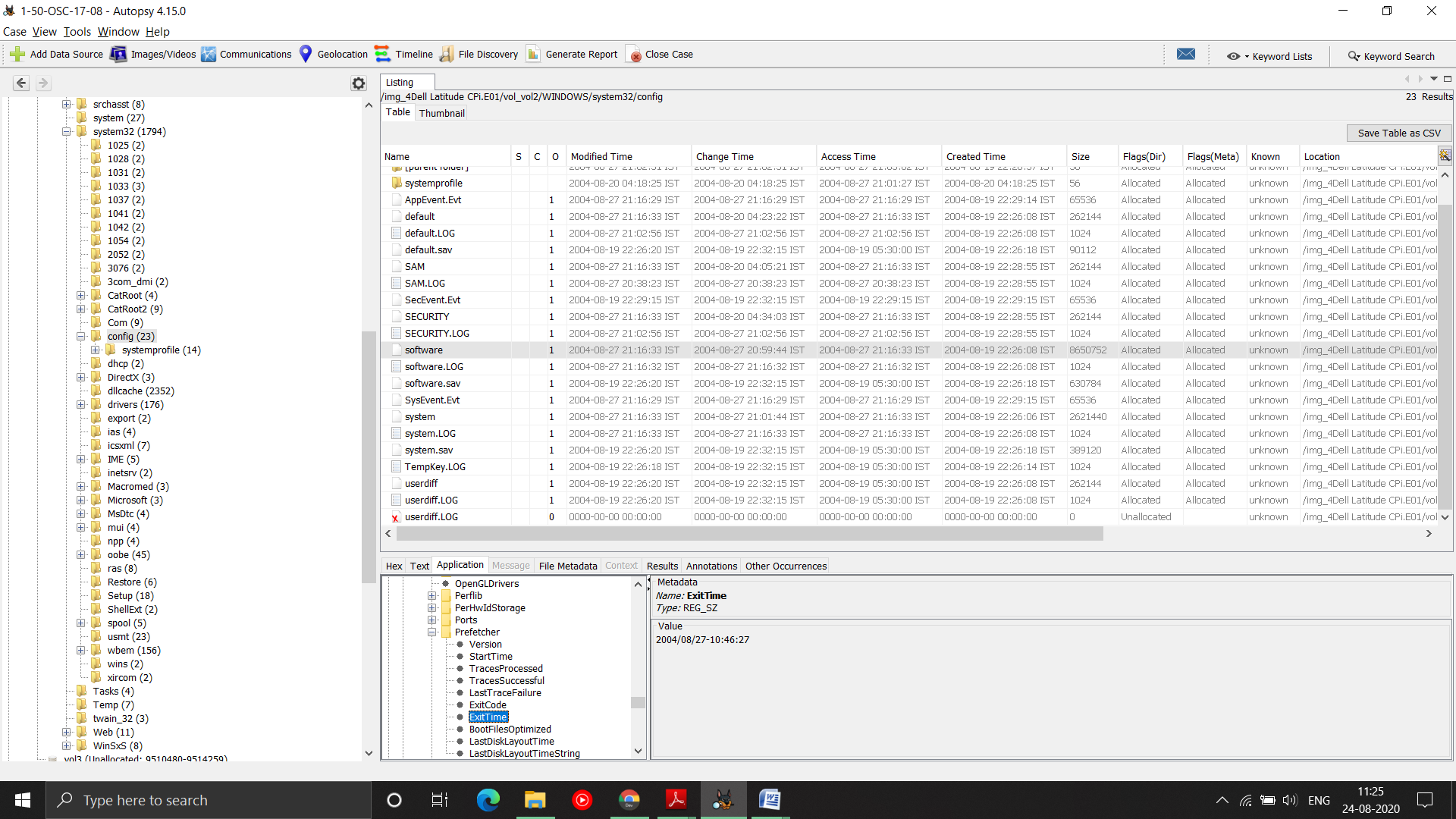
Autopsy is an open source digital forensics tool developed by Basis Technology, first released in 2000. It is a free to use and quite efficient tool for hard drive investigation with features like multi-user cases, timeline analysis, registry analysis, keyword search, email analysis, media playback,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

**Q1.** When was the last recorded computer shutdown date/time?

**Soln. 2004/08/27–10:46:27**

**Steps: C:\WINDOWS\system32\config\software\Microsoft\WindowNT\CurrentVersion\Prefetcher\ExitTime**

Screenshot:

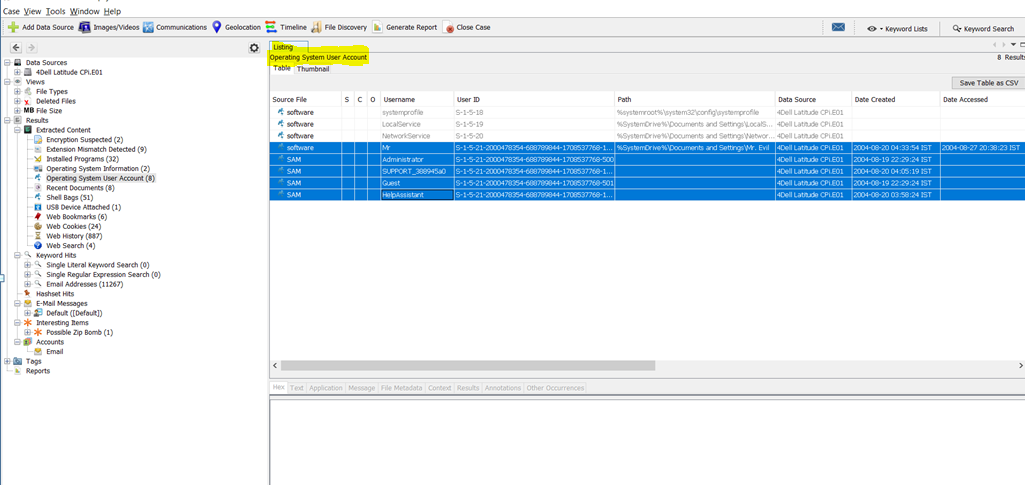
­­­­­­­

**Q2.** How many accounts are recorded (total number)?

**Soln.** 5 accounts: Administrator, Guest, HelpAssistant, Mr. Evil, and SUPPORT\_388945a0 (Look at the Account Type column).

**In the left side panel, we go to Results > Extracted Content > Operating System User Account**

Screenshot:

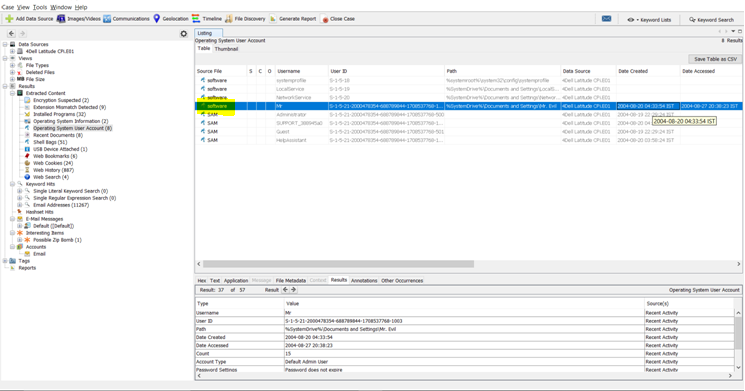


**Q3**. Who was the last user to logon to the computer?

**Soln. Mr. Evil**

**Mr. Evil was the last user to logon to the computer on 2004-08-20 at 04:33:54 IST.**

**It can be checked through Date Accessed column**



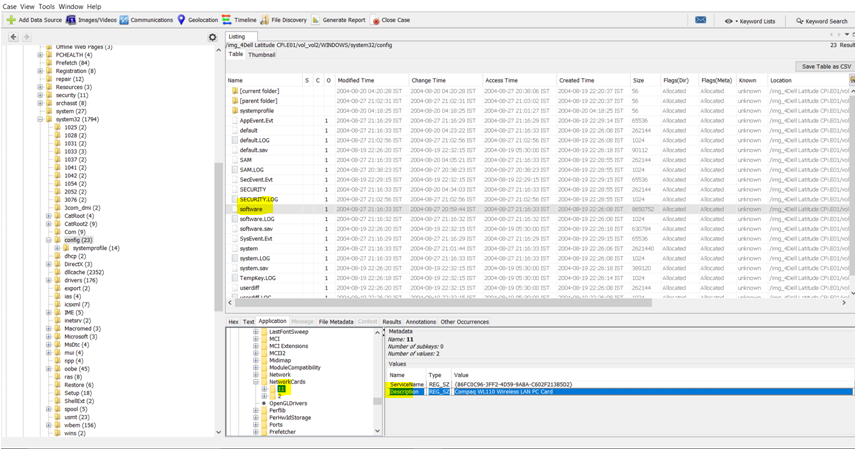
**Q4.** List the network cards used by this computer?

Soln. **Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)**

**Compaq WL110 Wireless LAN PC Card**

**Steps: at C:\WINDOWS\system32\config\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\**

**Screenshot:**

****

**Q5.** What is the IP address and MAC address of the computer?

**Soln.** **IP=192.168.1.111 and MAC=00:10:a4:93:3e:09**

**Steps: We go to C:/Program Files/Look@LAN/irunin.ini**

