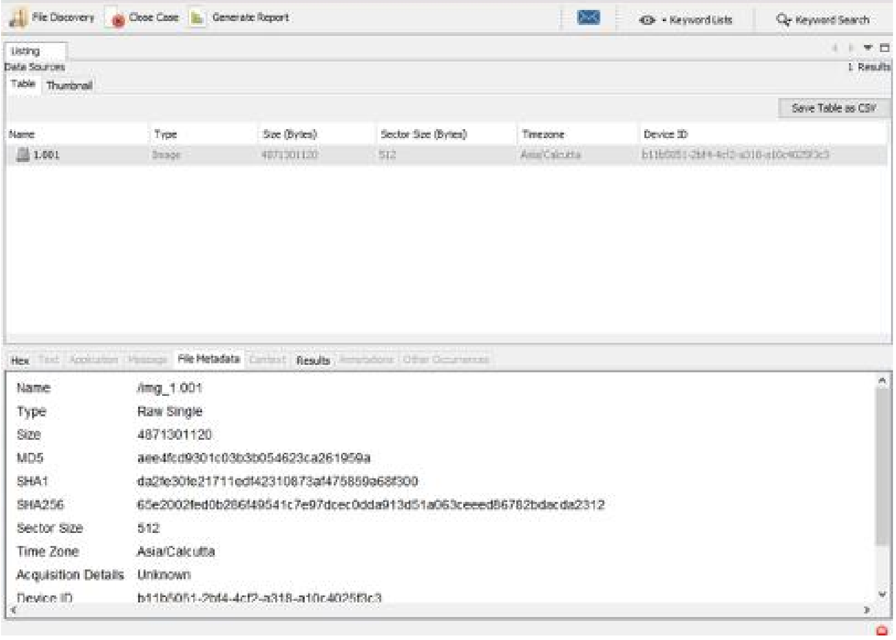
Kashish Srivastava
500067405

LAB EXPERIMENT 1 - AUTOPSY

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

Questions:

1 . What is the image hash? Does the acquisition and verification hash match?
Ans:
Image hash is : AEE4FCD9301C03B3B054623CA261959A.



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
1.001	Image	4871301120	512	Asia/Calcutta	b11b5051-2bf4-4cf2-a318-a10c4025f3c3

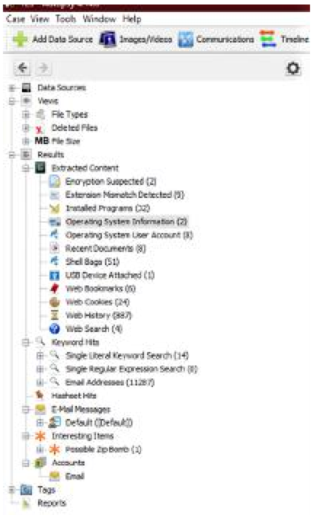
Name	/img_1.001
Type	Raw Single
Size	4871301120
MD5	aee4fcd9301c03b3b054623ca261959a
SHA1	da2fe30fe21711edf42310873af475859a68f300
SHA256	65e2002fed0b286f49541c7e97dcec0dda913d51a063ceeed86782bdacda2312
Sector Size	512
Time Zone	Asia/Calcutta
Acquisition Details	Unknown
Device ID	b11b5051-2bf4-4cf2-a318-a10c4025f3c3

For finding the image hash we need to click on the image.
After clicking on the image , we go tothe file metadata tab.

We get MD5 hash : ***AEE4FCD9301C03B3B054623CA261959A***
We also verify the images by checking their hashes

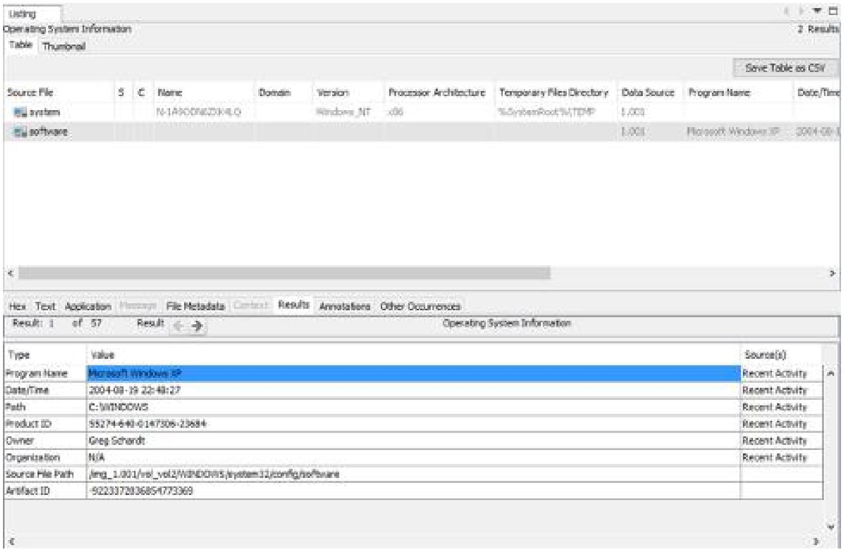
2. What operating system was used on the computer?

Ans:
Windows XP



In the left hand panel we find an option as results:
In results we have to click on extracted content
Then click on Operating system information:

We get two options in the right hand “System” and “Software”
We click on software


Listing
Operating System Information
2 Results
Table Thumbnail
Save Table as CSV
Hex Text Application Message File Metadata Context Results Annotations Other Occurrences
Result: 1 of 57 Result
Operating System Information

Source File	S	C	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Date/Time
system			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	1.001		
software								1.001	Microsoft Windows XP	2004-08-1

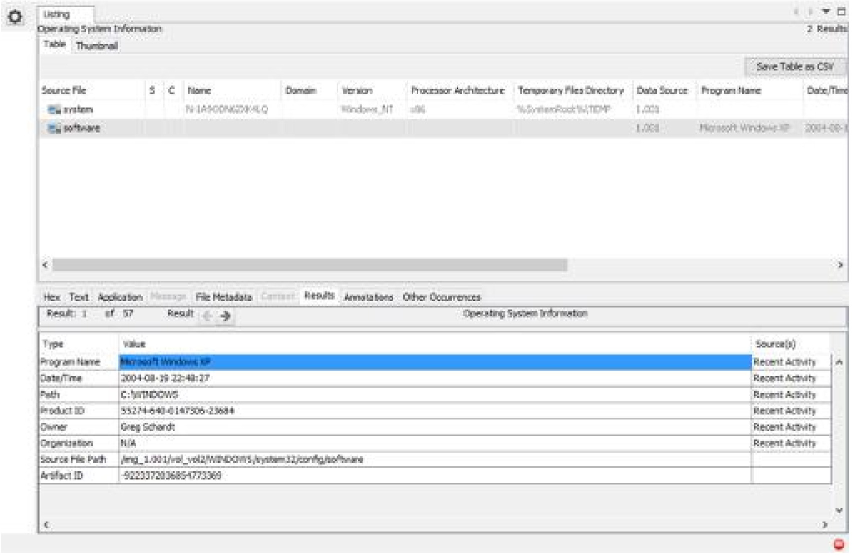
Type	Value	Source(s)
Program Name	Microsoft Windows XP	Recent Activity
Date/Time	2004-08-19 22:48:27	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_1.001/vol_vol2/WINDOWS/system32/config/software	
Artifact ID	-9223372036854773369	

In the bottom tab we see program name mentioned as ***Microsoft Windows XP***

3. When was the install date?

Ans:

August 19, 2004 22:48:27



Listing

Operating System Information

2 Results

Table | Thumbnail

Save Table as CSV

Source File	S	C	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Date/Time
system			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	1.001		
software								1.001	Microsoft Windows XP	2004-08-1

Hex | Text | Application | Message | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 1 of 57 Result

Operating System Information

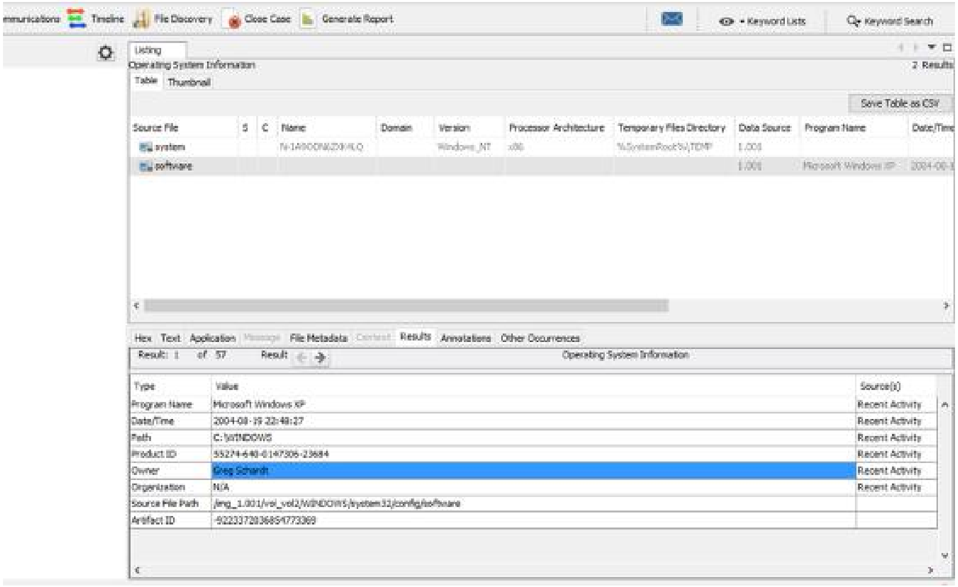
Type	Value	Source(s)
Program Name	Microsoft Windows XP	Recent Activity
Date/Time	2004-08-19 22:48:27	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_1.001/vol_vol2/WINDOWS/system32/config/software	
Artifact ID	-9223372036854773369	

Similary as above, below program name we have Date and Time mentioned *__2004-08-19 and 22.48.27__*

4. Who is the registered owner?

Ans:

Greg Schardt



mmunications | Timeline | File Discovery | Close Case | Generate Report | Keyword Lists | Keyword Search

Listing

Operating System Information

2 Results

Table | Thumbnail

Save Table as CSV

Source File	S	C	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Date/Time
system			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	1.001		
software								1.001	Microsoft Windows XP	2004-08-1

Hex | Text | Application | Message | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 1 of 57 Result

Operating System Information

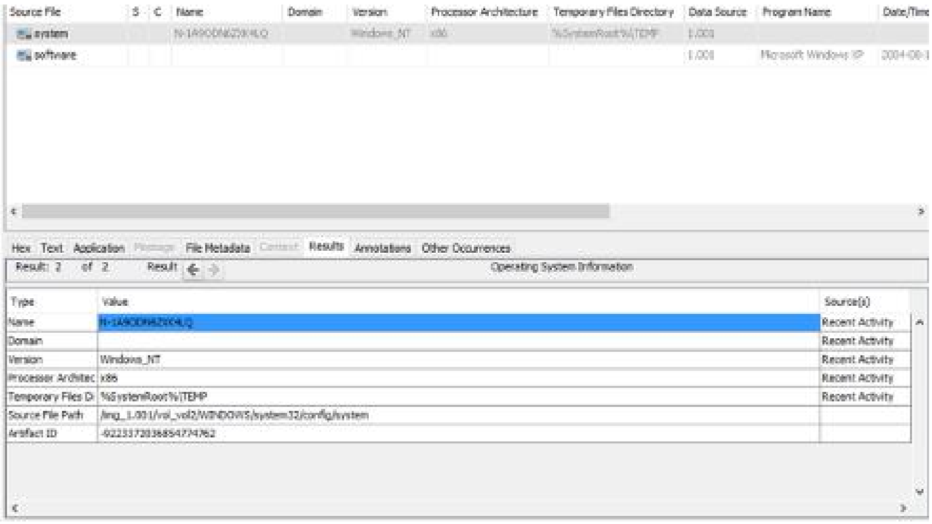
Type	Value	Source(s)
Program Name	Microsoft Windows XP	Recent Activity
Date/Time	2004-08-19 22:48:27	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_1.001/vol_vol2/WINDOWS/system32/config/software	
Artifact ID	-9223372036854773369	

Below date and time we have path, product-id and owner

In the owner it is mentioned as *__Greg Schardt__*

5. What is the computer account name?

Ans: N-1A9ODN6ZXK4LQ (In System file above Software file)



Source File	S	C	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Date/Time
system			N-1A9ODN6ZXK4LQ		Windows_NT	x86	%SystemRoot%\TEMP	1.001		
software								1.001	Microsoft Windows XP	2004-08-1

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Result: 2 of 2 Result

Operating System Information

Type	Value	Source(s)
Name	N-1A9ODN6ZXK4LQ	Recent Activity
Domain		Recent Activity
Version	Windows_NT	Recent Activity
Processor Architec	x86	Recent Activity
Temporary Files Di	%SystemRoot%\TEMP	Recent Activity
Source File Path	/img_1.001/vol_vol2/WINDOWS/system32/config/system	
Artifact ID	-9223372036854774762	

We had 2 files in operating system information tab:

The first was sytem containing system information, second is software containing software information.

In system information we get the bottom panel that has Name of the system which is the computer account name as: ***N-1A9ODN6ZXK4LQ***