# Solving Computer Forensic Case Using Autopsy

Computer Forensics is the well-planned series of procedures and techniques used for obtaining evidence from computer systems and storage media. This evidence can then be analyzed for relevant information that is to be presented in a court of law.

This article focused on a particular case and a forensic tool to give you a ‘feel’ of what computer forensics investigations are like. However, it is in no way comprehensive enough to cover the variety of problems and complications faced by the investigator.

## Scenario

A complaint was made to the authorities describing alleged Wi-Fi hacking activity. When the authorities reached the spot, they found an abandoned Dell computer which is suspected that this computer was used for hacking purposes. Schardt uses "Mr.Evil" nickname when he goes online.

He is also accused of parking his car in wireless range (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords. We're going to solve 20 important questions that will be related to this case by examining the images of his computer.

## Tasks performed:

During the course of investigation, analysis of the evidence would require performing the 12 basic tasks of computer forensics:

1. Generating an image hash and confirming the integrity of the image
2. Determining the Operating System used on the disk
3. Determining the date of OS installation
4. Determining the registered owner, account name in use and the last recorded shut down date and time
5. Determining the account name of the user who mostly used the computer and the user who last logged into it
6. Determining the hacker handle of the user and tying the actual name of the user to his hacker handle
7. Determining the MAC and last allocated IP address of this computer
8. Locating the programs installed in this computer that could have been used for hacking purposes
9. Collecting information regarding the IRC service that was used by the owner
10. Searching the Recycle Bin for relevant information
11. Listing the Newsgroups that the owner of the computer has registered to
12. Determining the SMTP email address in use

My Blog:

https://qaishussainy.blogspot.com/

Video tutorial for this investigation

https://youtu.be/0TUHpYIscBA

**Seized Laptop's Disk Image:**

Part 1: http://www.cfreds.nist.gov/images/4Dell%20Latitude%20CPi.E01

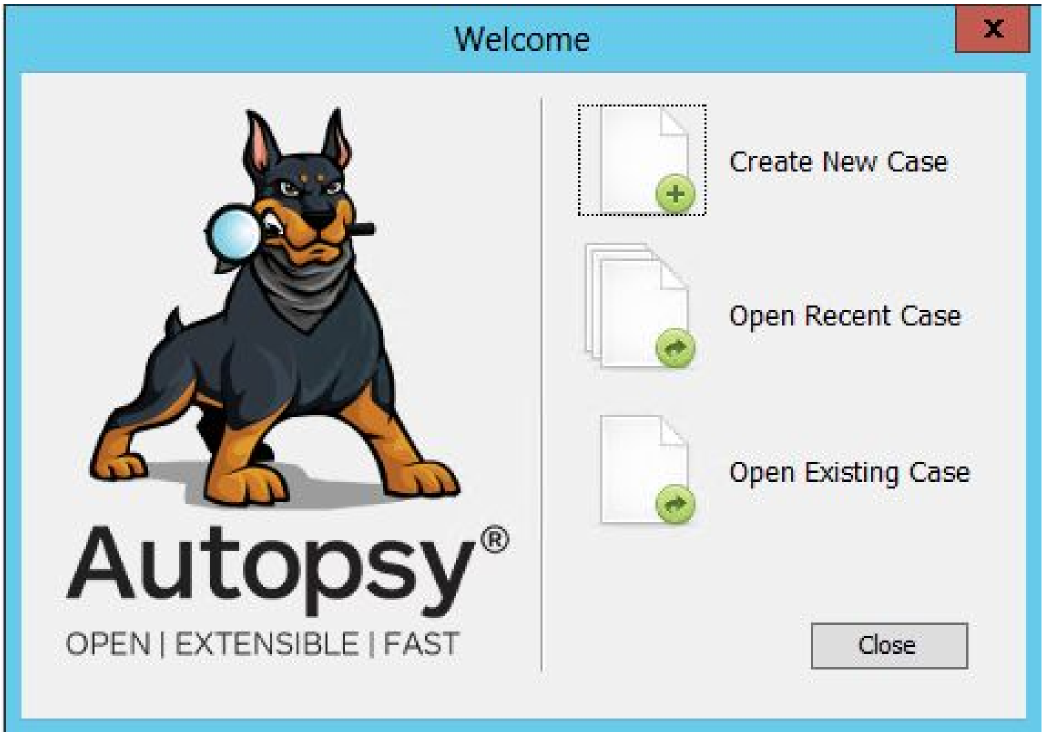
Part 2: http://www.cfreds.nist.gov/images/4Dell%20Latitude%20CPi.E02

Autopsy download link:

https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.14.0/autopsy-4.14.0-64bit.msi

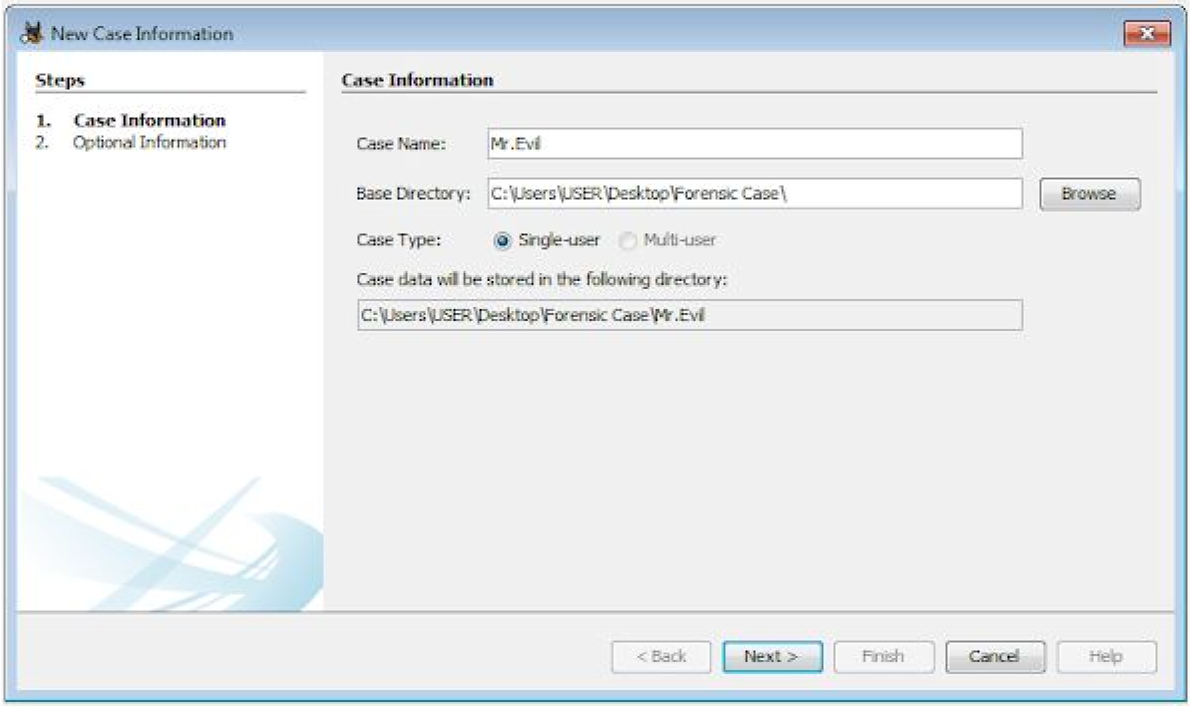
**Step 1**:

After downloading the evidence disk and installing Autopsy, run Autopsy it and select New Case



**Step 2:**

Set a name for this case as i have set Mr.Evil and also set the location where you want to save your forensic investigation data. click next and provide information but it's optional. click finish.



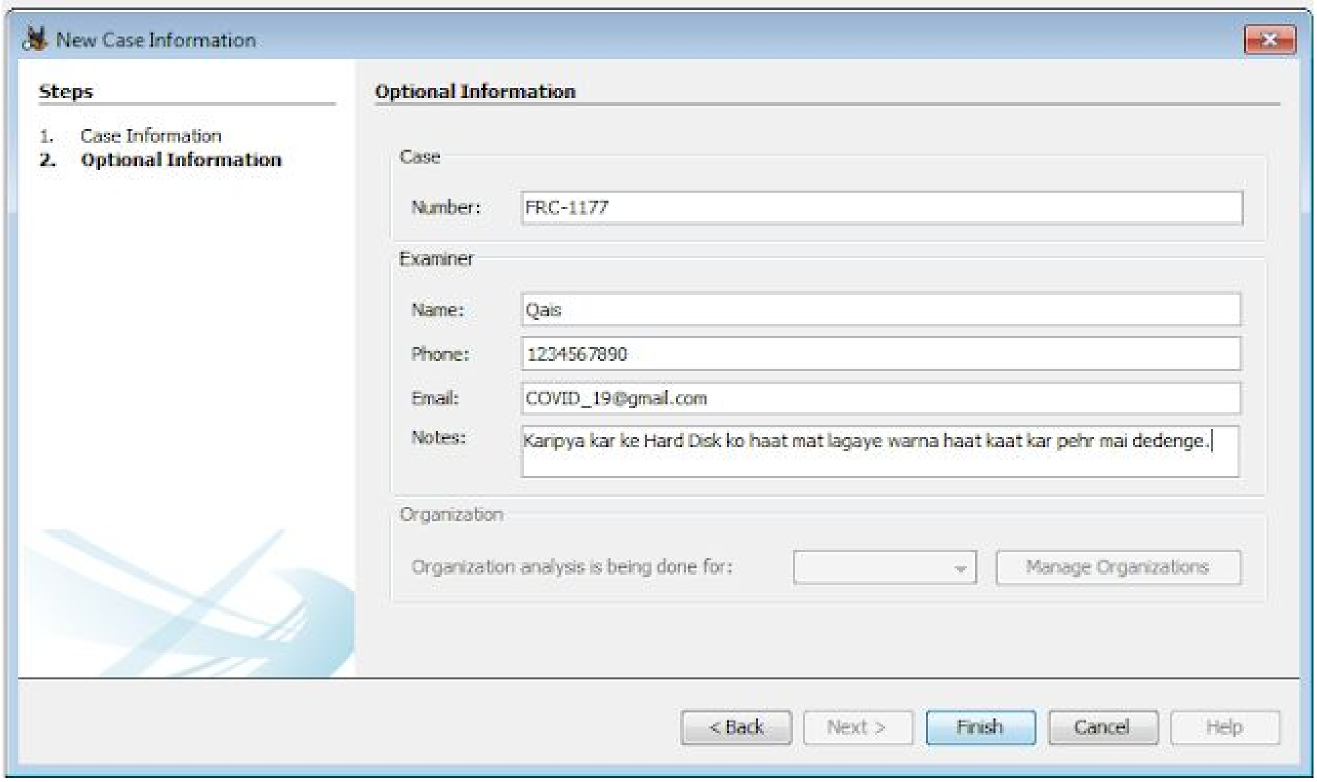
Case Name: Mr.Evil

Base Directory: C:\Users\USER\Desktop\Forensic Case\

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\USER\Desktop\Forensic Case\Mr.Evil



New Case Information

Steps

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number: FRC-1177

Examiner

Name: Qais

Phone: 1234567890

Email: COVID_19@gmail.com

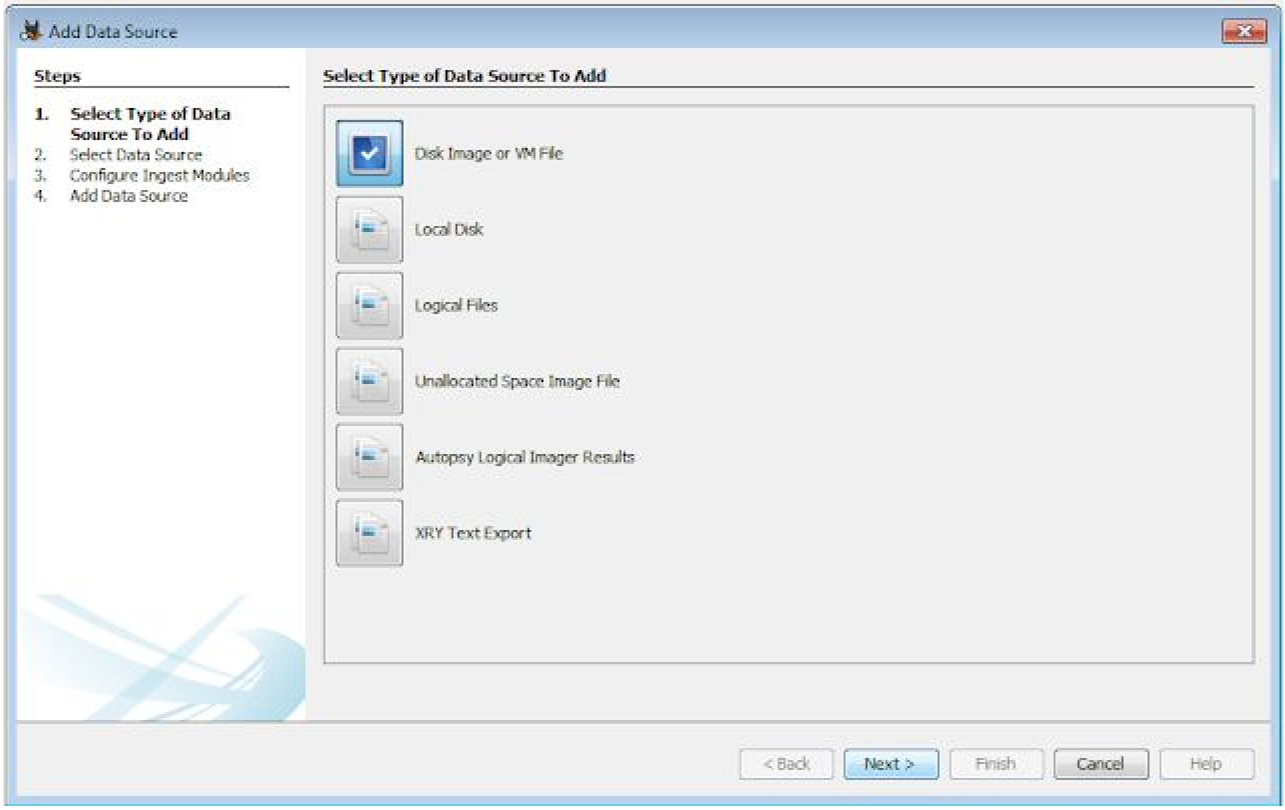
Notes: Karipya kar ke Hard Disk ko haat mat lagaye warna haat kaat kar pehr mai dedenge.

Organization

Organization analysis is being done for:

**Step 3:**

Select the first options Disk Image



Add Data Source

Steps

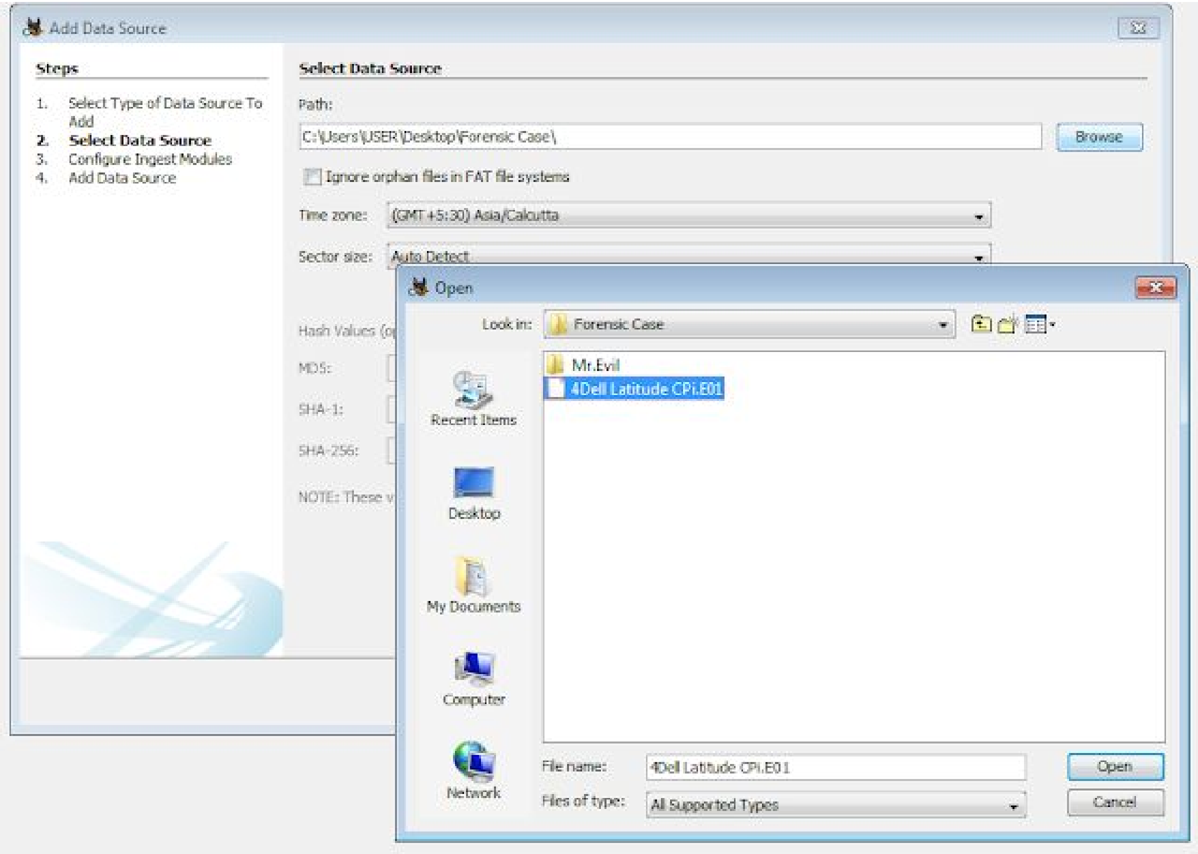
1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

**Select Type of Data Source To Add**

- ☑ Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

Select the evidence disk image which you have downloaded before. i have created a separate folder by the name of Forensic Case and pasted the disk images into it.

**Note:** Although both parts of the downloaded image are there in this folder, you will only see the first part to select. Autopsy will automatically take the second part of the downloaded image.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: C:\Users\USER\Desktop\Forensic Case\

☐ Ignore orphan files in FAT file systems

Time zone: (GMT +5:30) Asia/Calcutta

Sector size: Auto Detect

Open

Look in: Forensic Case

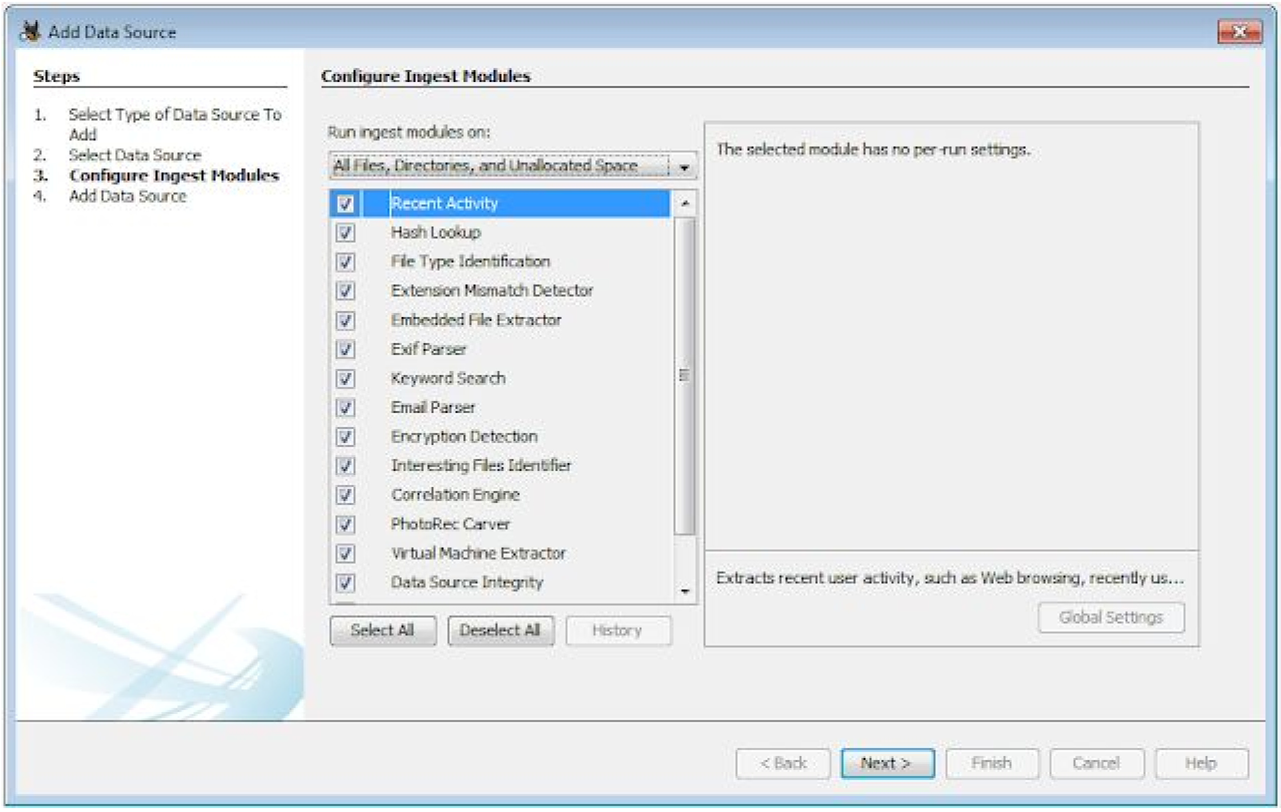
Mr.Evil

4Dell Latitude CPi.E01

File name: 4Dell Latitude CPi.E01

Files of type: All Supported Types

Click next and let all options as default.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

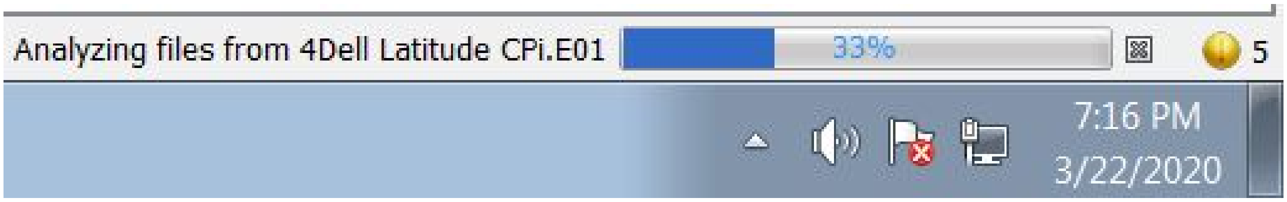
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Correlation Engine
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Wait until all steps of analysis and integrity check loads completely.

make sure you have sufficient storage minimum 1GB otherwise the modules will not completely load and the investigation will be incomplete.



Analyzing files from 4Dell Latitude CPi.E01

## So now let's start our investigation

We will find the solution for these given tasks from the disk image of the suspect.

Q1. What is the image hash?

Q2: What operating system was used on the computer?

Q3: When was the install date?

Q4. Who is the registered owner?

Q5. What is the computer account name?

Q6. When was the last recorded computer shutdown date/time?

Q7. How many accounts are recorded (total number)?

Q8.Who was the last user to logon to the computer?

Q9. List the network cards used by this computer?

Q10. What is the IP address and MAC address of the computer?

Q11. Search for programs/tools that aided in the crime (Wireless Hacking)

Q12. Which Email client is used by Mr. Evil?

Q13. What is the SMTP email address for Mr. Evil?

Q14. How many executable files are in the recycle bin?

Q15. Are there any malware on the computer?

Q16. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the userid,

Q17. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

Q18. Which internet browser was used?

Q19. What websites victim was accessing?

Q20. What is the web-based email address for the main user?

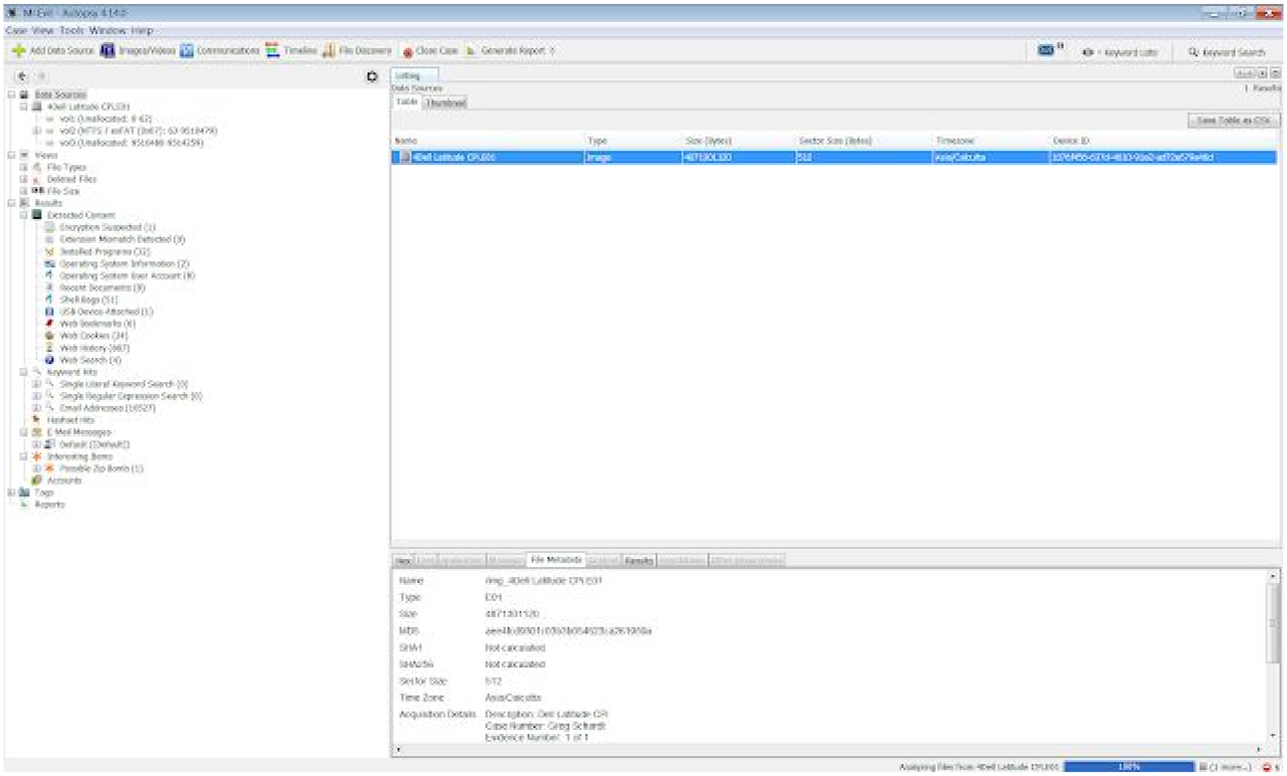
**Q1**. What is the image hash?

Ans1: The HASH of image is AEE4FCD9301C03B3B054623CA261959A.

**How?**

Click on Data source --> Select the image Dell Latitude CPi, E01 --> Click on Metadata

MD5: AEE4FCD9301C03B3B054623CA261959A



| Name | Type | Size (Bytes) | Sector Size (Bytes) | Timezone | Device ID |
|---|---|---|---|---|---|
| 4Dell Latitude CPi.E01 | Image | 4871301120 | 512 | Asia/Calcutta | [illegible] |

| | |
|---|---|
| Name | /img_4Dell Latitude CPi.E01 |
| Type | E01 |
| Size | 4871301120 |
| MD5 | aee4fcd9301c03b3b054623ca261959a |
| SHA1 | Not calculated |
| SHA256 | Not calculated |
| Sector Size | 512 |
| Time Zone | Asia/Calcutta |
| Acquisition Details | Description: Dell Latitude CPi<br>Case Number: Greg Schardt<br>Evidence Number: 1 of 1 |

We check hash to see if the image is not altered or something is not added or not deleted from the activities. It's very important because a single tamper to data would make an accused, guilty or innocent.

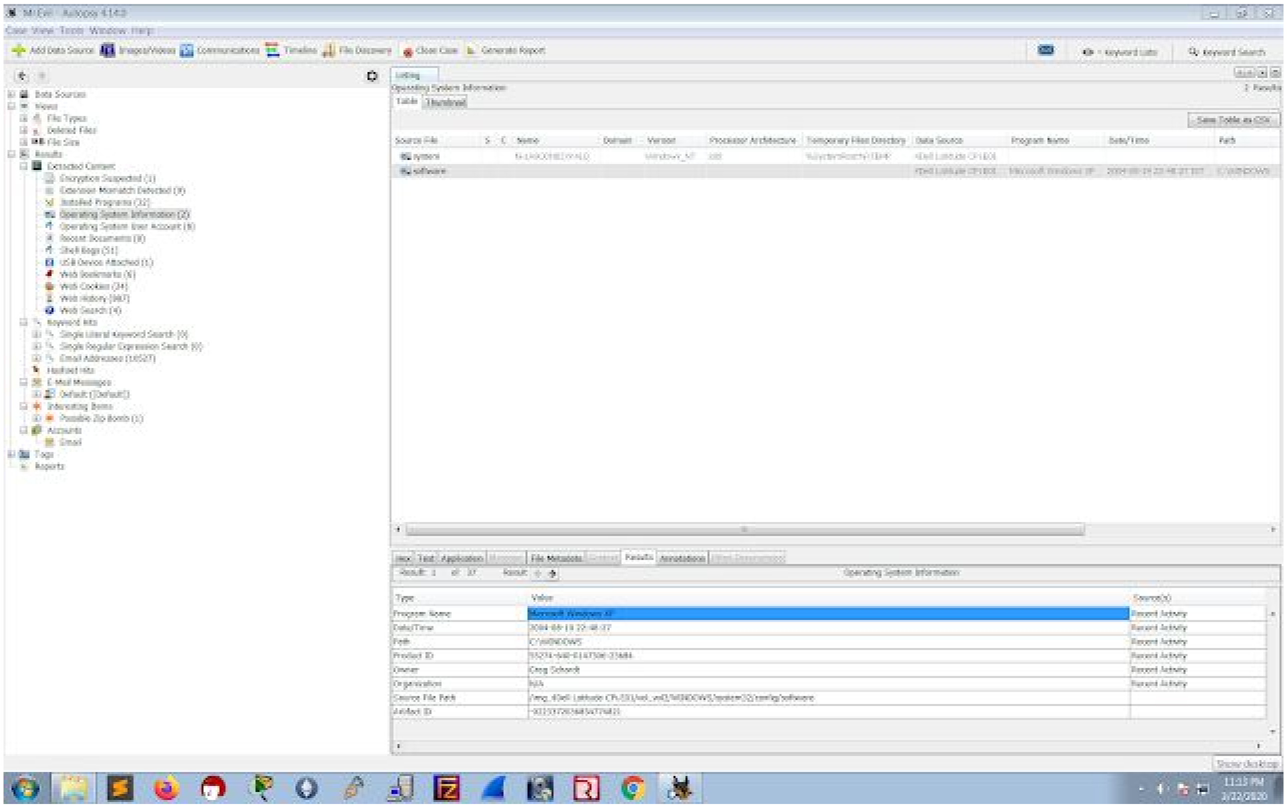
**Q2**: What operating system was used on the computer?

Ans2: Microsoft Windows XP was used.

**How**?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on software you can see the under Program Information tab which is written Microsoft Windows XP.



Operating System Information

| Source File | S | C | Name | Domain | Version | Processor Architecture | Temporary Files Directory | Data Source | Program Name | Date/Time | Path |
|---|---|---|---|---|---|---|---|---|---|---|---|
| system | | | N-1A9ODN6ZXK4LQ | | Windows_NT | x86 | %SystemRoot%\TEMP | 4Dell Latitude CPi.E01 | | | |
| software | | | | | | | | 4Dell Latitude CPi.E01 | Microsoft Windows XP | 2004-08-19 22:48:27 EDT | C:\WINDOWS |

Result: 1 of 37 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_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software | |
| Artifact ID | [illegible] | |

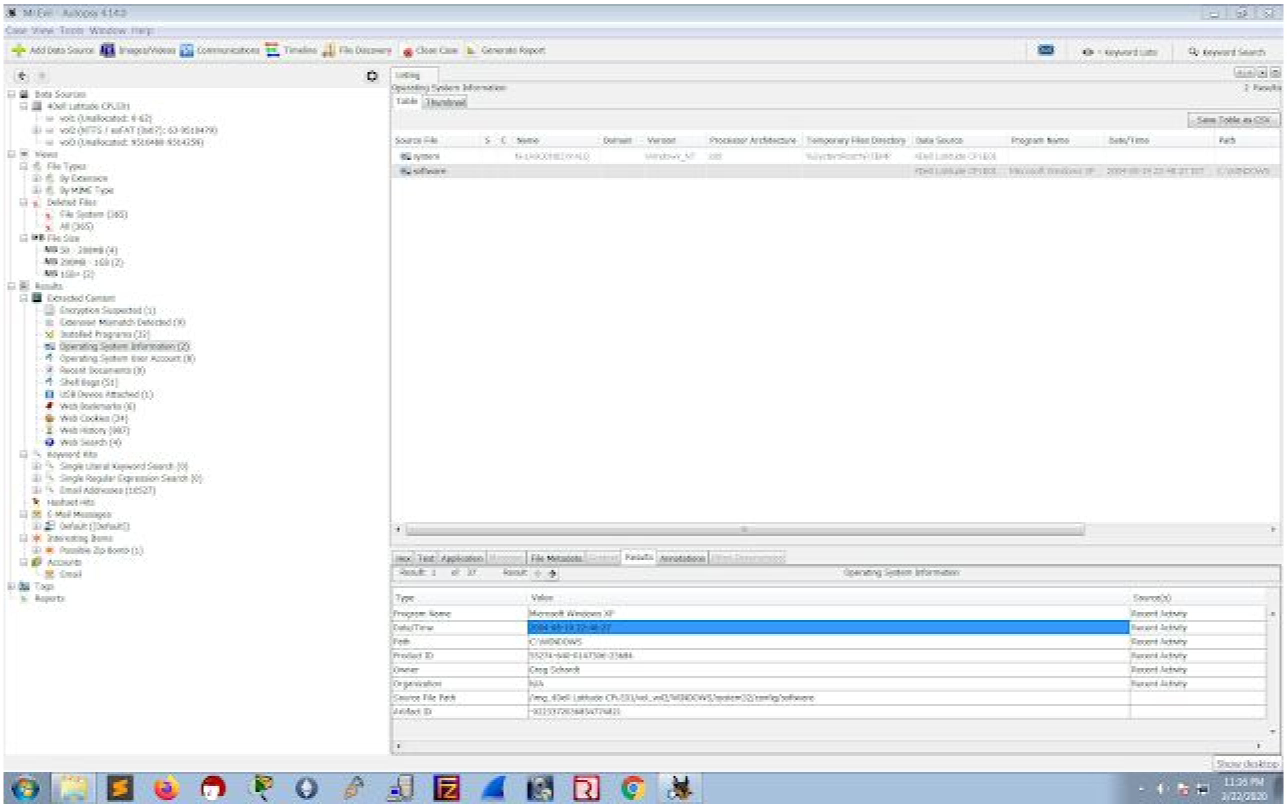
**Q3**: When was the install date?

Ans3: 2004-08-19 22:48:27

How?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on software you can see under the Date Time tab which is written Microsoft Windows XP.



| Source File | S | C | Name | Domain | Version | Processor Architecture | Temporary Files Directory | Data Source | Program Name | Date/Time | Path |
|---|---|---|---|---|---|---|---|---|---|---|---|
| system | | | N-1A9ODN6ZXK4LQ | | Windows_NT | x86 | %SystemRoot%\TEMP | 4Dell Latitude CPi.E01 | | | |
| software | | | | | | | | 4Dell Latitude CPi.E01 | Microsoft Windows XP | 2004-08-19 22:48:27 EDT | C:\WINDOWS |

| 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_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software | |
| Artifact ID | -9223372036854775831 | |

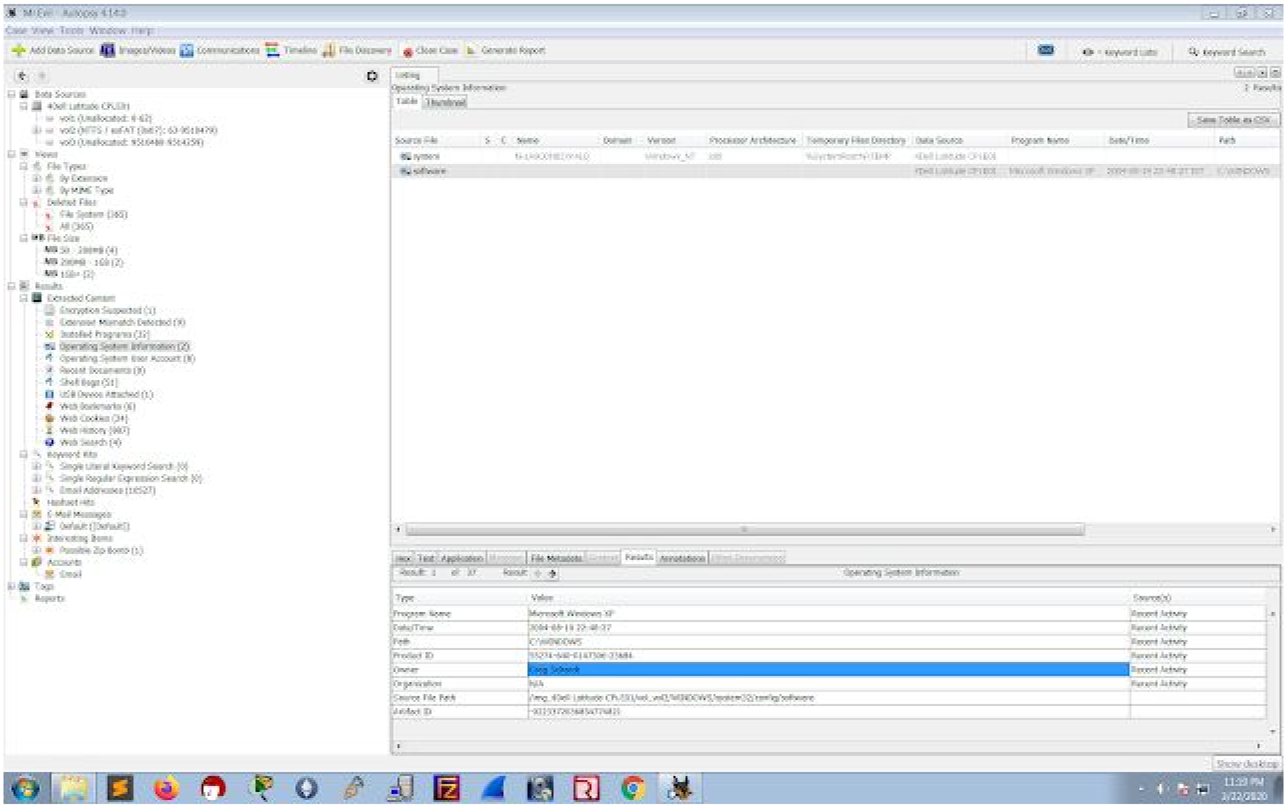
**Q4**. Who is the registered owner?

Ans4: The owner is Greg Schardt

How?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on software you can see the under Owner tab which shows Greg Schardt.



Operating System Information

| Source File | S | C | Name | Domain | Version | Processor Architecture | Temporary Files Directory | Data Source | Program Name | Date/Time | Path |
|---|---|---|---|---|---|---|---|---|---|---|---|
| system | | | N-1A9ODN6ZXK4LQ | | Windows_NT | x86 | %SystemRoot%\TEMP | 4Dell Latitude CPi.E01 | | | |
| software | | | | | | | | 4Dell Latitude CPi.E01 | Microsoft Windows XP | 2004-08-19 22:48:27 EDT | C:\WINDOWS |

Result: 1 of 37

| 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_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software | |
| Artifact ID | -9223372036854775821 | |

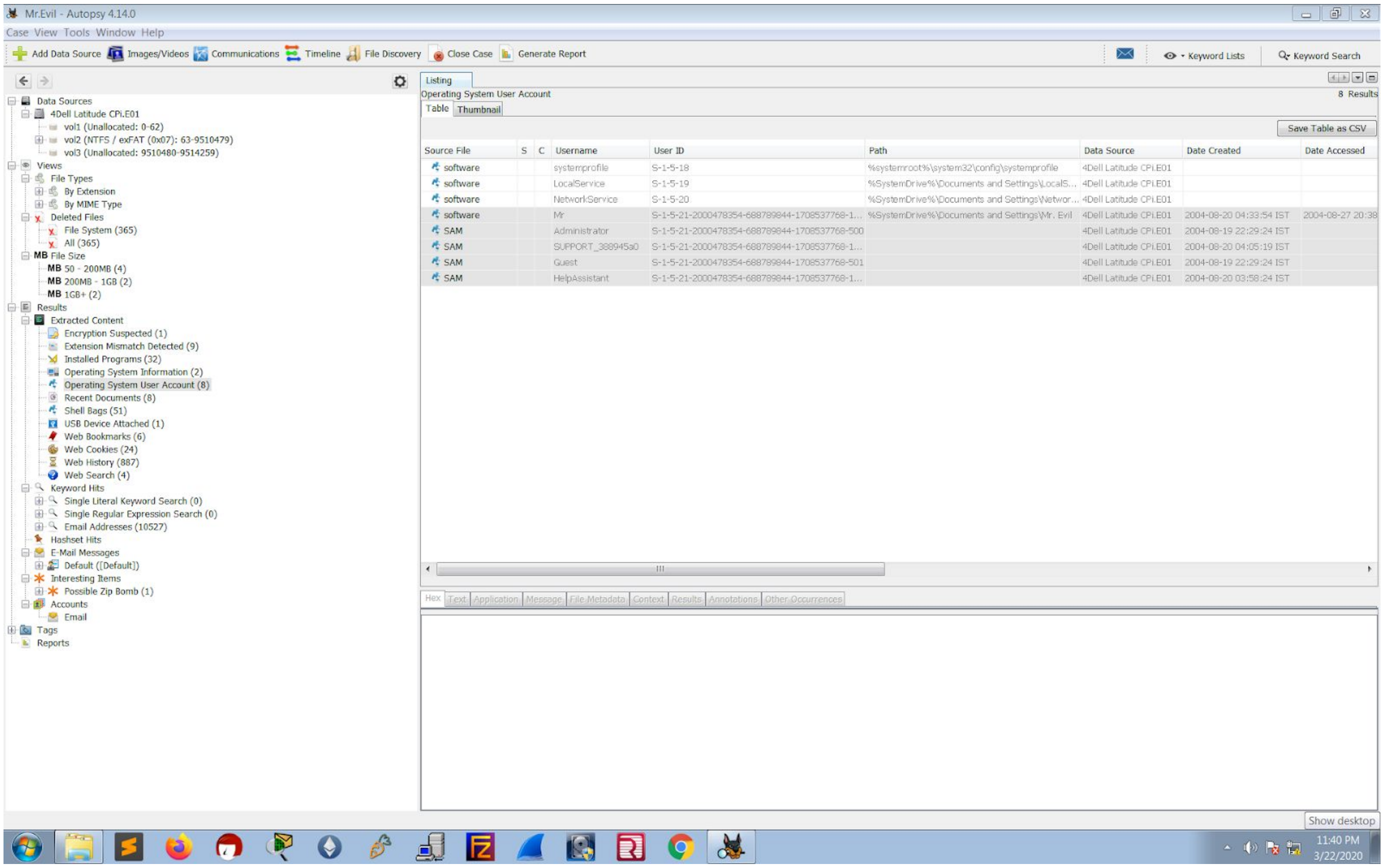
**Q5**. What is the computer account name?

Ans5: The account name is N-1A9ODN6ZXK4LQ

How?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on System you can see the under Name which it shows N-1A9ODN6ZXK4LQ



Operating System User Account

8 Results

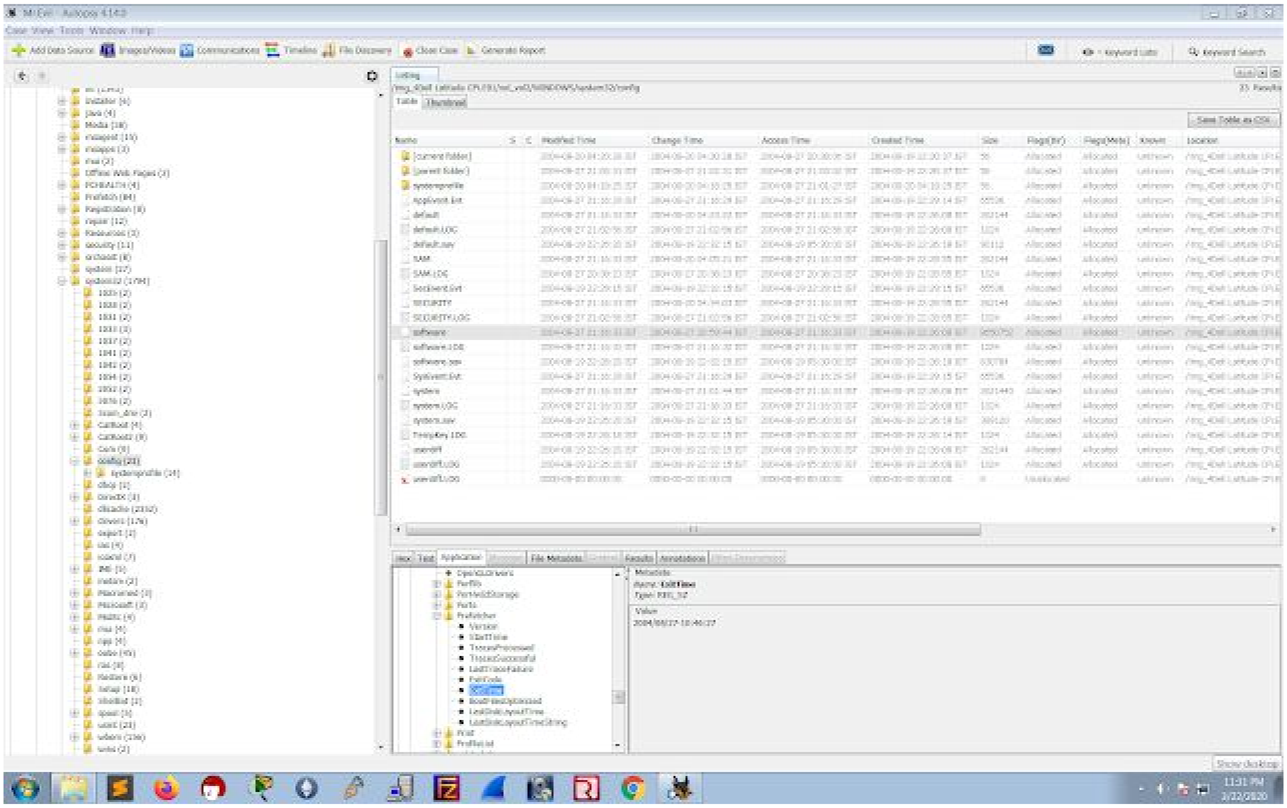
| Source File | S | C | Username | User ID | Path | Data Source | Date Created | Date Accessed |
|---|---|---|---|---|---|---|---|---|
| software | | | systemprofile | S-1-5-18 | %systemroot%\system32\config\systemprofile | 4Dell Latitude CPi.E01 | | |
| software | | | LocalService | S-1-5-19 | %SystemDrive%\Documents and Settings\LocalS... | 4Dell Latitude CPi.E01 | | |
| software | | | NetworkService | S-1-5-20 | %SystemDrive%\Documents and Settings\Networ... | 4Dell Latitude CPi.E01 | | |
| software | | | Mr | S-1-5-21-2000478354-688789844-1708537768-1... | %SystemDrive%\Documents and Settings\Mr. Evil | 4Dell Latitude CPi.E01 | 2004-08-20 04:33:54 IST | 2004-08-27 20:38 |
| SAM | | | Administrator | S-1-5-21-2000478354-688789844-1708537768-500 | | 4Dell Latitude CPi.E01 | 2004-08-19 22:29:24 IST | |
| SAM | | | SUPPORT_388945a0 | S-1-5-21-2000478354-688789844-1708537768-1... | | 4Dell Latitude CPi.E01 | 2004-08-20 04:05:19 IST | |
| SAM | | | Guest | S-1-5-21-2000478354-688789844-1708537768-501 | | 4Dell Latitude CPi.E01 | 2004-08-19 22:29:24 IST | |
| SAM | | | HelpAssistant | S-1-5-21-2000478354-688789844-1708537768-1... | | 4Dell Latitude CPi.E01 | 2004-08-20 03:58:24 IST | |

**Q6**. When was the last recorded computer shutdown date/time?

Ans6: The last recorded shutdown time of the computer is 2004/08/27-10:46:27

How?

Click on Data Sources select 4Dell Latitude --> vol2 --> WINDOWS\system32\config\software\Microsoft\WindowNT\CurrentVersion\Prefetcher\ExitTime



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

Metadata
Name: ExitTime
Type: REG_32

Value
2004/08/27-10:46:27

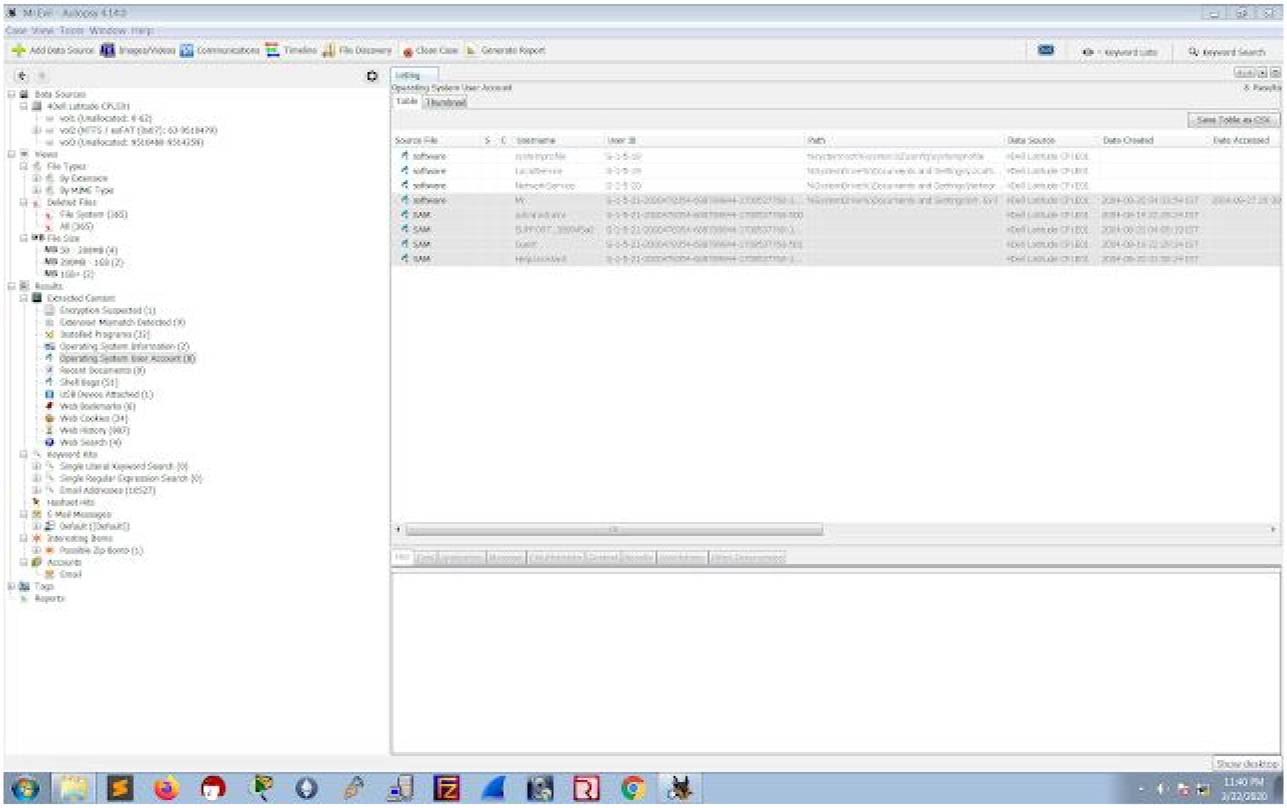
**Q7**. How many accounts are recorded (total number)?

Ans7: There are 5 accounts

Mr, Administrator, Guest, Support388945a0, HelpAssistant

How?

Click on Results --> Operating System User Accounts



Operating System User Account

8 Results

| Source File | S | C | Username | User ID | Path | Data Source | Date Created | Date Accessed |
|---|---|---|---|---|---|---|---|---|
| software | | | systemprofile | S-1-5-18 | %systemroot%\system32\config\systemprofile | 4Dell Latitude CPi.E01 | | |
| software | | | LocalService | S-1-5-19 | %SystemDrive%\Documents and Settings\LocalS... | 4Dell Latitude CPi.E01 | | |
| software | | | NetworkService | S-1-5-20 | %SystemDrive%\Documents and Settings\Networ... | 4Dell Latitude CPi.E01 | | |
| software | | | Mr | S-1-5-21-2000478354-688789844-1708537768-1... | %SystemDrive%\Documents and Settings\Mr. Evil | 4Dell Latitude CPi.E01 | 2004-08-20 04:33:54 EDT | 2004-08-27 [illegible] |
| SAM | | | Administrator | S-1-5-21-2000478354-688789844-1708537768-500 | | 4Dell Latitude CPi.E01 | 2004-08-19 22:28:24 EDT | |
| SAM | | | SUPPORT_388945a0 | S-1-5-21-2000478354-688789844-1708537768-1... | | 4Dell Latitude CPi.E01 | 2004-08-20 04:05:22 EDT | |
| SAM | | | Guest | S-1-5-21-2000478354-688789844-1708537768-501 | | 4Dell Latitude CPi.E01 | 2004-08-19 22:28:24 EDT | |
| SAM | | | HelpAssistant | S-1-5-21-2000478354-688789844-1708537768-1... | | 4Dell Latitude CPi.E01 | 2004-08-20 03:58:24 EDT | |

**Q8**.Who was the last user to logon to the computer?

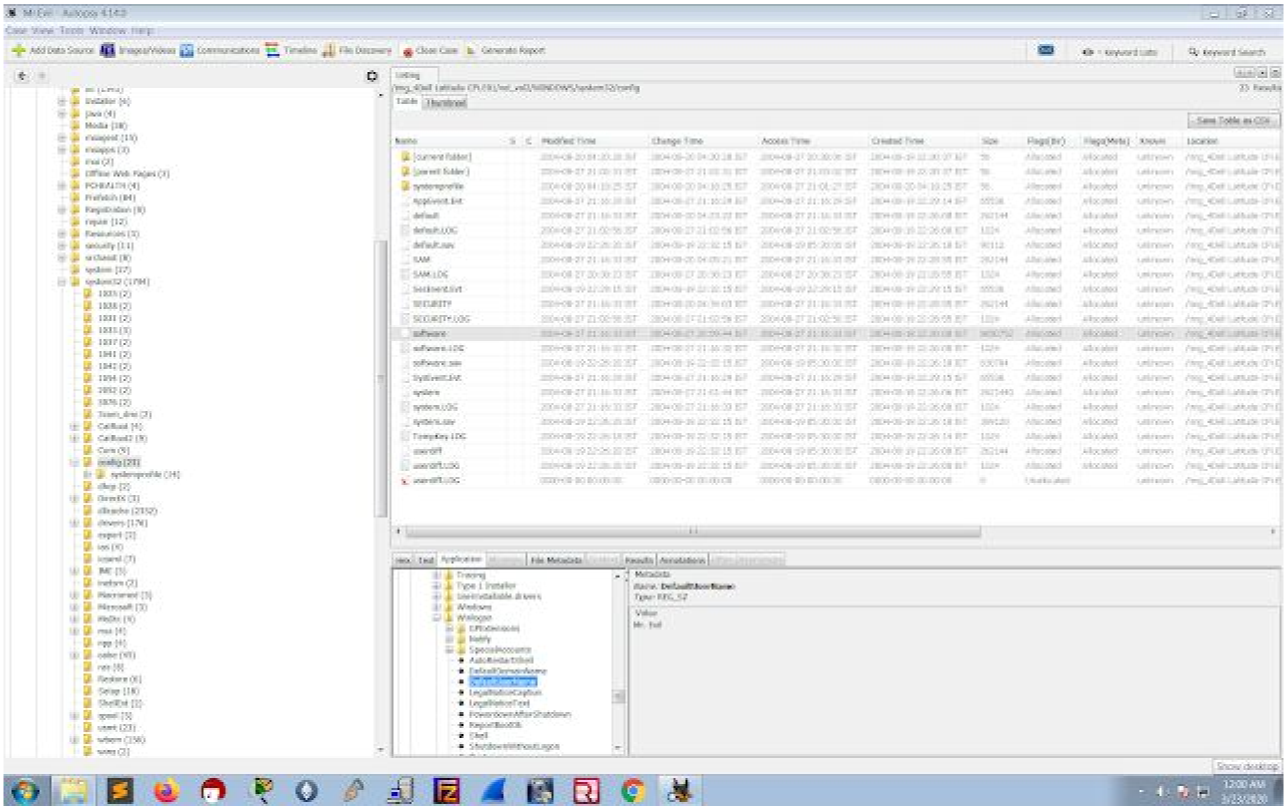
Ans8: Mr. Evil

The system will obtain the last user who logged on from the key ‘DefaultUserName’. This information can be uncovered from the following path

How?

Click on Data Sources select 4Dell Latitude --> vol2 -->

WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/WINLOGON/DEFAULT USER NAME



Metadata
Name: DefaultUserName
Type: REG_SZ

Value
Mr. Evil

**Q9**. List the network cards used by this computer?

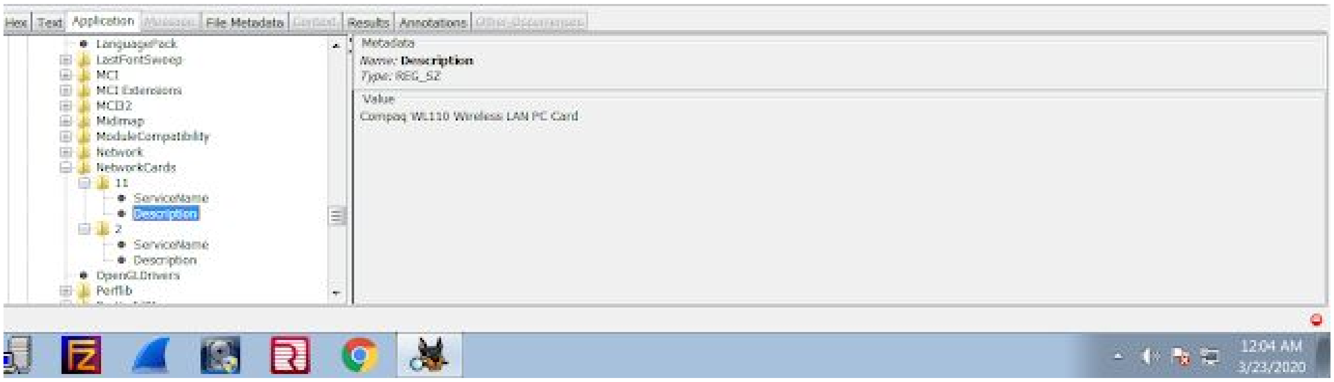
Ans9: Compaq WL110 Wireless LAN PC Card, Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface).

**How**?

Click on Data Sources select 4Dell Latitude --> vol2 -->

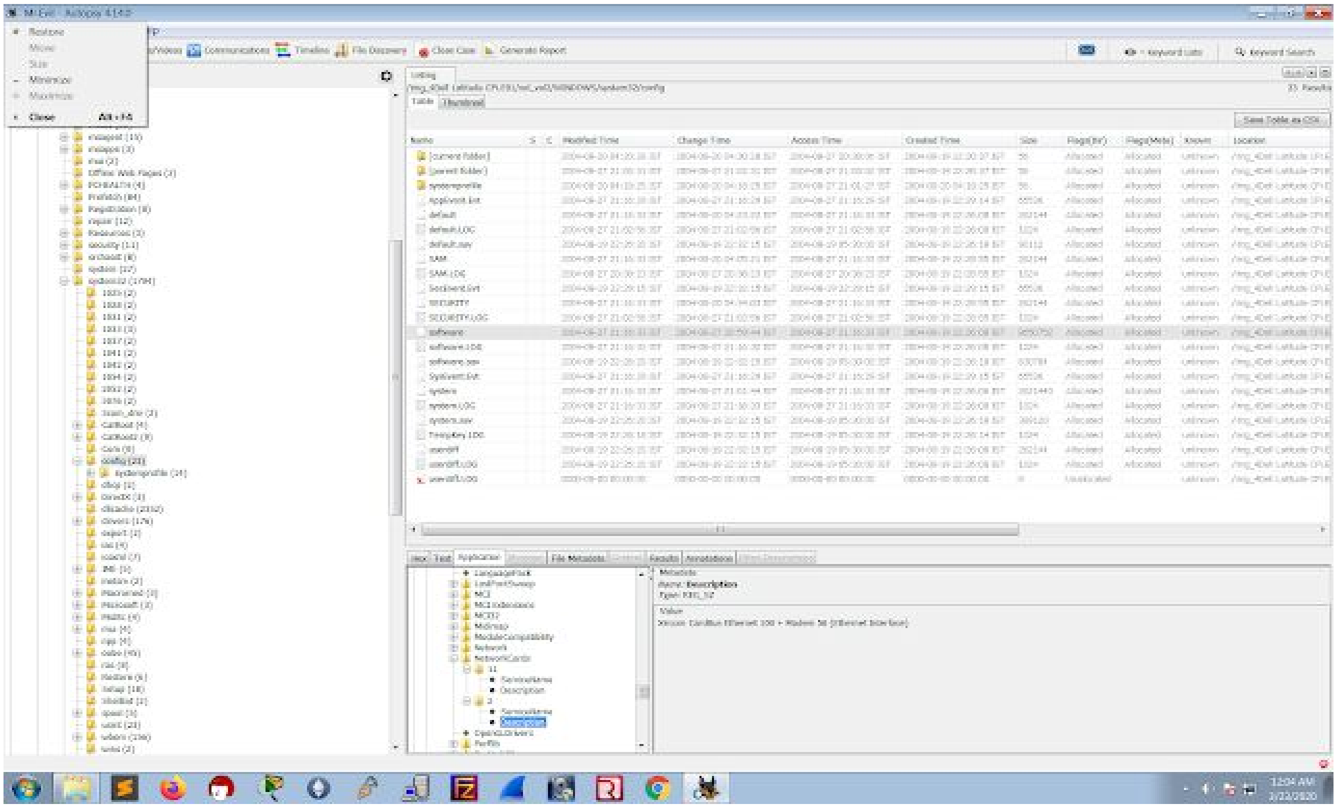
WINDOWS\system32\config\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\

click on descriptions



Metadata
Name: **Description**
Type: REG_SZ

Value
Compaq WL110 Wireless LAN PC Card



Metadata
Name: **Description**
Type: REG_SZ

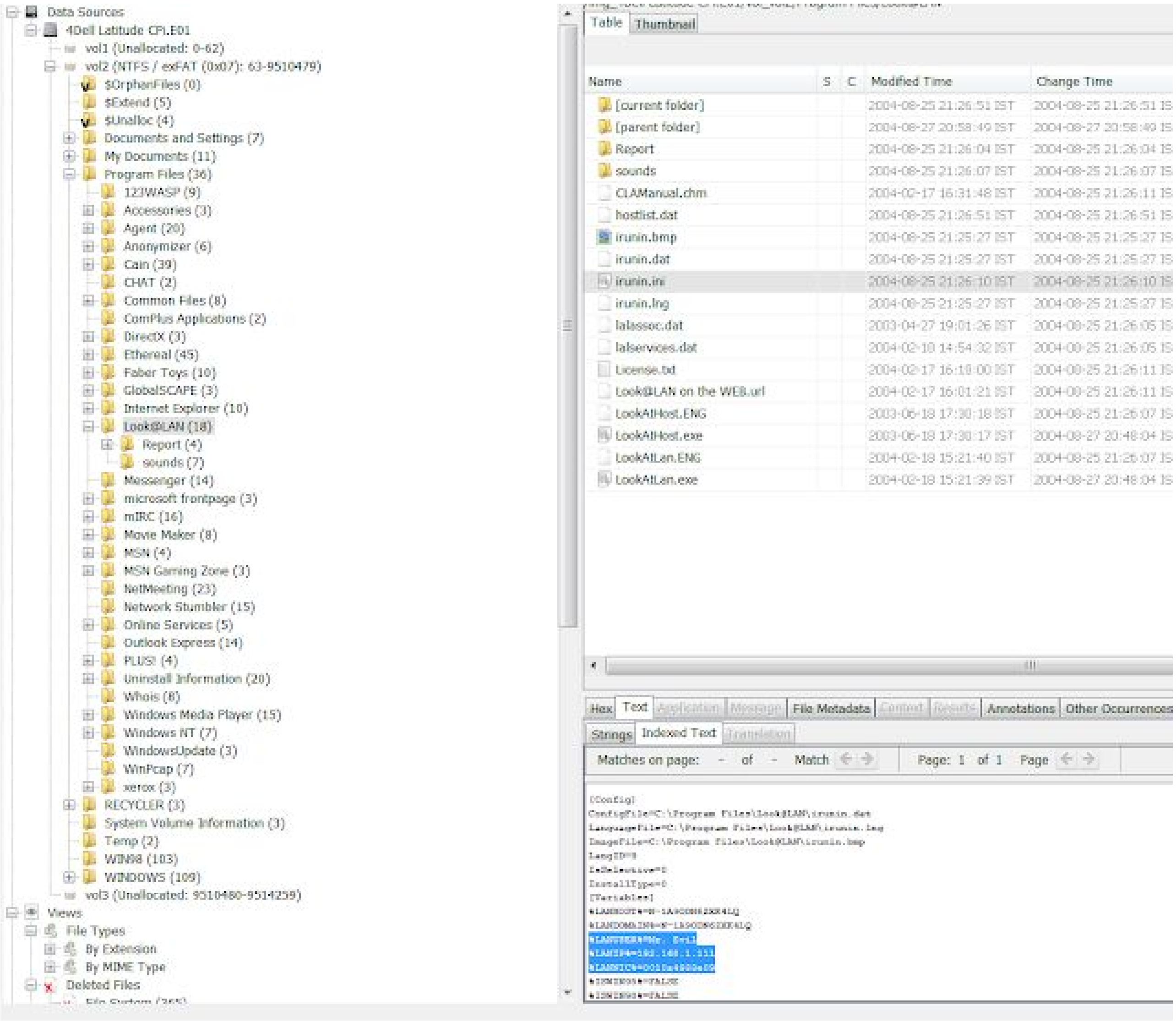
Value
Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

## **Q10**. What is the IP address and MAC address of the computer?

Ans10: IP=192.168.1.111,  MAC=00:10:a4:93:3e:09

**How?**

Click on Data Sources select 4Dell Latitude --> vol2 --> Program Files/Look@LAN/irunin.ini



```
Data Sources
  4Dell Latitude CPi.E01
    vol1 (Unallocated: 0-62)
    vol2 (NTFS / exFAT (0x07): 63-9510479)
      $OrphanFiles (0)
      $Extend (5)
      $Unalloc (4)
      Documents and Settings (7)
      My Documents (11)
      Program Files (36)
        123WASP (9)
        Accessories (3)
        Agent (20)
        Anonymizer (6)
        Cain (39)
        CHAT (2)
        Common Files (8)
        ComPlus Applications (2)
        DirectX (3)
        Ethereal (45)
        Faber Toys (10)
        GlobalSCAPE (3)
        Internet Explorer (10)
        Look@LAN (18)
          Report (4)
          sounds (7)
        Messenger (14)
        microsoft frontpage (3)
        mIRC (16)
        Movie Maker (8)
        MSN (4)
        MSN Gaming Zone (3)
        NetMeeting (23)
        Network Stumbler (15)
        Online Services (5)
        Outlook Express (14)
        PLUS! (4)
        Uninstall Information (20)
        Whois (8)
        Windows Media Player (15)
        Windows NT (7)
        WindowsUpdate (3)
        WinPcap (7)
        xerox (3)
      RECYCLER (3)
      System Volume Information (3)
      Temp (2)
      WIN98 (103)
      WINDOWS (109)
    vol3 (Unallocated: 9510480-9514259)
Views
  File Types
    By Extension
    By MIME Type
  Deleted Files
    File System (265)
```

| Name | S | C | Modified Time | Change Time |
|---|---|---|---|---|
| [current folder] | | | 2004-08-25 21:26:51 IST | 2004-08-25 21:26:51 IS |
| [parent folder] | | | 2004-08-27 20:58:49 IST | 2004-08-27 20:58:49 IS |
| Report | | | 2004-08-25 21:26:04 IST | 2004-08-25 21:26:04 IS |
| sounds | | | 2004-08-25 21:26:07 IST | 2004-08-25 21:26:07 IS |
| CLAManual.chm | | | 2004-02-17 16:31:48 IST | 2004-08-25 21:26:11 IS |
| hostlist.dat | | | 2004-08-25 21:26:51 IST | 2004-08-25 21:26:51 IS |
| irunin.bmp | | | 2004-08-25 21:25:27 IST | 2004-08-25 21:25:27 IS |
| irunin.dat | | | 2004-08-25 21:25:27 IST | 2004-08-25 21:25:27 IS |
| irunin.ini | | | 2004-08-25 21:26:10 IST | 2004-08-25 21:26:10 IS |
| irunin.lng | | | 2004-08-25 21:25:27 IST | 2004-08-25 21:25:27 IS |
| lalassoc.dat | | | 2003-04-27 19:01:26 IST | 2004-08-25 21:26:05 IS |
| lalservices.dat | | | 2004-02-10 14:54:32 IST | 2004-08-25 21:26:05 IS |
| License.txt | | | 2004-02-17 16:10:00 IST | 2004-08-25 21:26:11 IS |
| Look@LAN on the WEB.url | | | 2004-02-17 16:01:21 IST | 2004-08-25 21:26:11 IS |
| LookAtHost.ENG | | | 2003-06-18 17:30:18 IST | 2004-08-25 21:26:07 IS |
| LookAtHost.exe | | | 2003-06-18 17:30:17 IST | 2004-08-27 20:48:04 IS |
| LookAtLan.ENG | | | 2004-02-18 15:21:40 IST | 2004-08-25 21:26:07 IS |
| LookAtLan.exe | | | 2004-02-18 15:21:39 IST | 2004-08-27 20:48:04 IS |

```
[Config]
ConfigFile=C:\Program Files\Look@LAN\irunin.dat
LanguageFile=C:\Program Files\Look@LAN\irunin.lng
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
```

**Q11**. Search for programs/tools that aided in the crime (Wireless Hacking)

Ans11: The programs which will be used for hacking purpose

**1. Look@LAN**

Look@Lan is an advanced network monitor that allows you to monitor your net in few clicks.

**2. Cain**

Cain and Abel is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks.

**3. Network Stumbler**

NetStumbler is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP.

**4. mIRC**

mIRC is an Internet Relay Chat client for Windows, created in 1995.

5. Ethereal/Wireshark

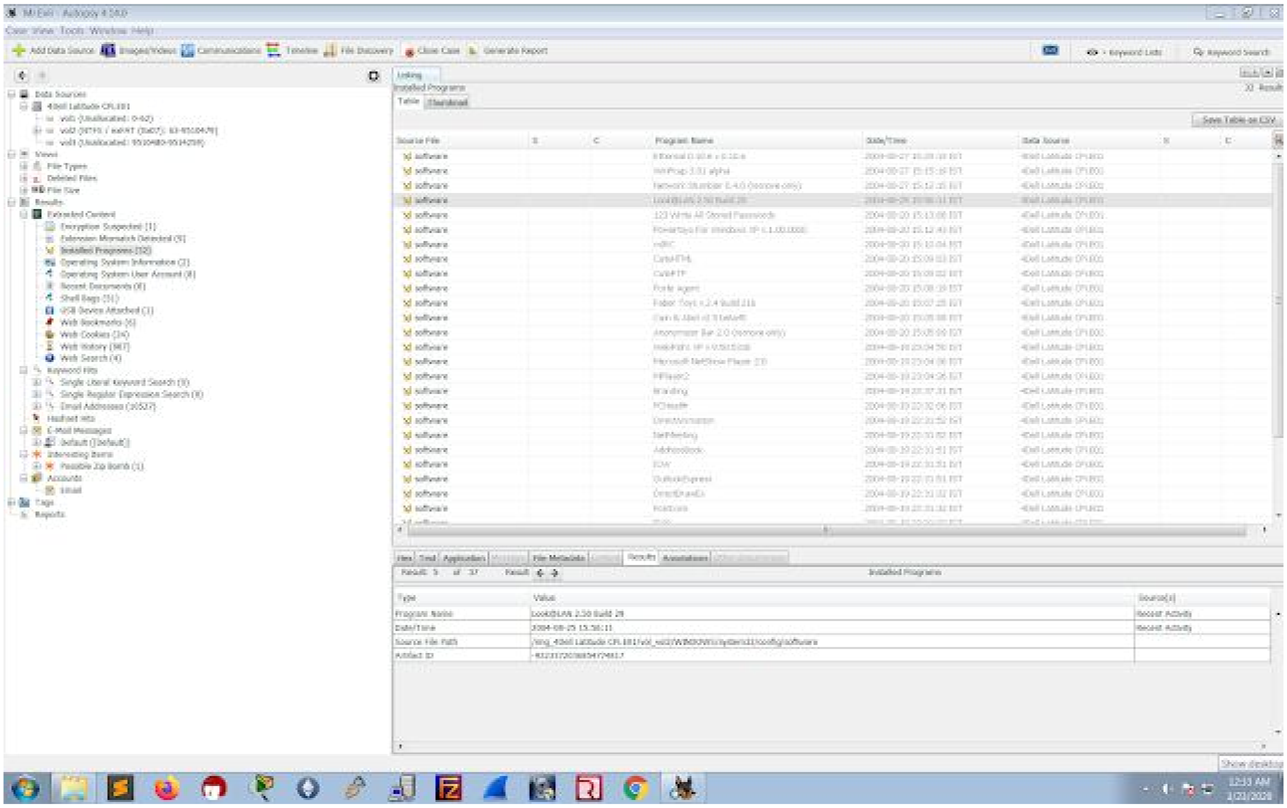
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

**6. 123WASP**

WASP will display all passwords of the currently logged in user that are stored in the Microsoft PWL file.

How?

Click on Results --> Extracted Content --> Installed Programs



| Source File | S | C | Program Name | Date/Time | Data Source | S | C |
|---|---|---|---|---|---|---|---|
| software | | | Ethereal 0.10.6 v.0.10.6 | 2004-08-27 15:28:18 EST | 4Dell Latitude CPi.E01 | | |
| software | | | WinPcap 3.01 alpha | 2004-08-27 15:15:18 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Network Stumbler 0.4.0 (remove only) | 2004-08-27 15:12:35 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Look@LAN 2.50 Build 29 | 2004-08-25 15:56:11 EST | 4Dell Latitude CPi.E01 | | |
| software | | | 123 Write All Stored Passwords | 2004-08-20 15:13:06 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Powertoys For Windows XP v.1.00.0000 | 2004-08-20 15:12:40 EST | 4Dell Latitude CPi.E01 | | |
| software | | | mIRC | 2004-08-20 15:10:04 EST | 4Dell Latitude CPi.E01 | | |
| software | | | CuteHTML | 2004-08-20 15:09:03 EST | 4Dell Latitude CPi.E01 | | |
| software | | | CuteFTP | 2004-08-20 15:09:02 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Forte Agent | 2004-08-20 15:08:18 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Faber Toys v.2.4 Build 211 | 2004-08-20 15:07:25 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Cain & Abel v2.5 beta45 | 2004-08-20 15:05:08 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Anonymizer Bar 2.0 (remove only) | 2004-08-20 15:05:00 EST | 4Dell Latitude CPi.E01 | | |
| software | | | WebFldrs XP v.9.50.5318 | 2004-08-19 23:04:50 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Microsoft NetShow Player 2.0 | 2004-08-19 23:04:38 EST | 4Dell Latitude CPi.E01 | | |
| software | | | MPlayer2 | 2004-08-19 23:04:36 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Branding | 2004-08-19 22:37:31 EST | 4Dell Latitude CPi.E01 | | |
| software | | | PCHealth | 2004-08-19 22:32:06 EST | 4Dell Latitude CPi.E01 | | |
| software | | | DirectAnimation | 2004-08-19 22:31:52 EST | 4Dell Latitude CPi.E01 | | |
| software | | | NetMeeting | 2004-08-19 22:31:52 EST | 4Dell Latitude CPi.E01 | | |
| software | | | AddressBook | 2004-08-19 22:31:51 EST | 4Dell Latitude CPi.E01 | | |
| software | | | ICW | 2004-08-19 22:31:51 EST | 4Dell Latitude CPi.E01 | | |
| software | | | OutlookExpress | 2004-08-19 22:31:51 EST | 4Dell Latitude CPi.E01 | | |
| software | | | DirectDrawEx | 2004-08-19 22:31:32 EST | 4Dell Latitude CPi.E01 | | |
| software | | | Fontcore | 2004-08-19 22:31:32 EST | 4Dell Latitude CPi.E01 | | |

Result: 5 of 32 Result ← →

Installed Programs

| Type | Value | Source(s) |
|---|---|---|
| Program Name | Look@LAN 2.50 Build 29 | Recent Activity |
| Date/Time | 2004-08-25 15:56:11 | Recent Activity |
| Source File Path | /img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software | |
| Artifact ID | -9223372036854774817 | |

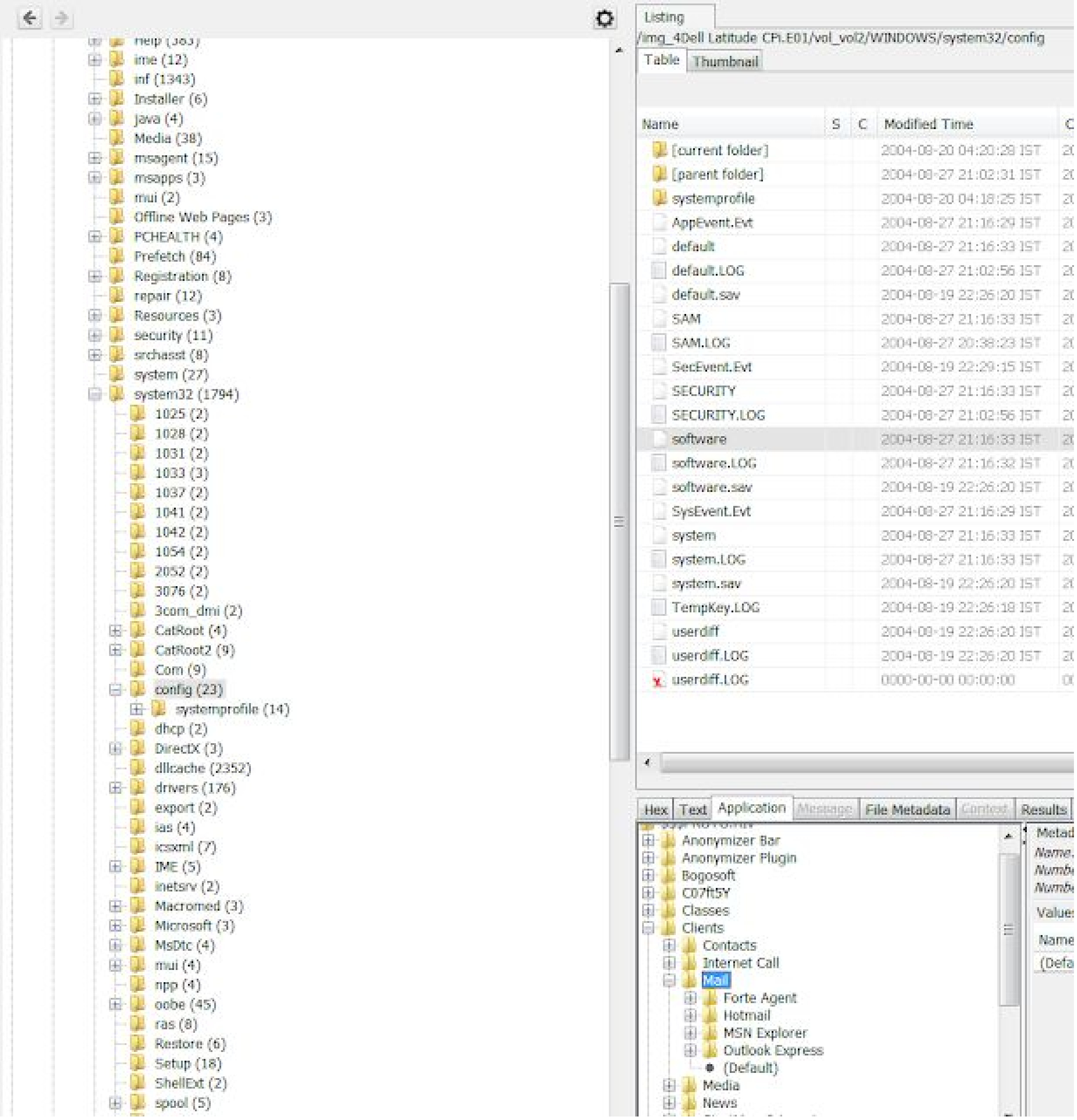
**Q12**. Which Email client is used by Mr. Evil?

Ans12: Outlook Express, Forte Agent, MSN Explorer, MSN (Hotmail) Email

**How?**

Click on Data Sources select 4Dell Latitude --> vol2 -->

WINDOWS\system32\config\software\clients\Mail



```
ime (12)
inf (1343)
Installer (6)
java (4)
Media (38)
msagent (15)
msapps (3)
mui (2)
Offline Web Pages (3)
PCHEALTH (4)
Prefetch (84)
Registration (8)
repair (12)
Resources (3)
security (11)
srchasst (8)
system (27)
system32 (1794)
    1025 (2)
    1028 (2)
    1031 (2)
    1033 (3)
    1037 (2)
    1041 (2)
    1042 (2)
    1054 (2)
    2052 (2)
    3076 (2)
    3com_dmi (2)
    CatRoot (4)
    CatRoot2 (9)
    Com (9)
    config (23)
        systemprofile (14)
    dhcp (2)
    DirectX (3)
    dllcache (2352)
    drivers (176)
    export (2)
    ias (4)
    icsxml (7)
    IME (5)
    inetsrv (2)
    Macromed (3)
    Microsoft (3)
    MsDtc (4)
    mui (4)
    npp (4)
    oobe (45)
    ras (8)
    Restore (6)
    Setup (18)
    ShellExt (2)
    spool (5)
```

/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

| Name | S | C | Modified Time | C |
|---|---|---|---|---|
| [current folder] | | | 2004-08-20 04:20:28 IST | 20 |
| [parent folder] | | | 2004-08-27 21:02:31 IST | 20 |
| systemprofile | | | 2004-08-20 04:18:25 IST | 20 |
| AppEvent.Evt | | | 2004-08-27 21:16:29 IST | 20 |
| default | | | 2004-08-27 21:16:33 IST | 20 |
| default.LOG | | | 2004-08-27 21:02:56 IST | 20 |
| default.sav | | | 2004-08-19 22:26:20 IST | 20 |
| SAM | | | 2004-08-27 21:16:33 IST | 20 |
| SAM.LOG | | | 2004-08-27 20:38:23 IST | 20 |
| SecEvent.Evt | | | 2004-08-19 22:29:15 IST | 20 |
| SECURITY | | | 2004-08-27 21:16:33 IST | 20 |
| SECURITY.LOG | | | 2004-08-27 21:02:56 IST | 20 |
| software | | | 2004-08-27 21:16:33 IST | 20 |
| software.LOG | | | 2004-08-27 21:16:32 IST | 20 |
| software.sav | | | 2004-08-19 22:26:20 IST | 20 |
| SysEvent.Evt | | | 2004-08-27 21:16:29 IST | 20 |
| system | | | 2004-08-27 21:16:33 IST | 20 |
| system.LOG | | | 2004-08-27 21:16:33 IST | 20 |
| system.sav | | | 2004-08-19 22:26:20 IST | 20 |
| TempKey.LOG | | | 2004-08-19 22:26:18 IST | 20 |
| userdiff | | | 2004-08-19 22:26:20 IST | 20 |
| userdiff.LOG | | | 2004-08-19 22:26:20 IST | 20 |
| userdiff.LOG | | | 0000-00-00 00:00:00 | 00 |

```
Anonymizer Bar
Anonymizer Plugin
Bogosoft
C07ft5Y
Classes
Clients
    Contacts
    Internet Call
    Mail
        Forte Agent
        Hotmail
        MSN Explorer
        Outlook Express
        (Default)
    Media
    News
```

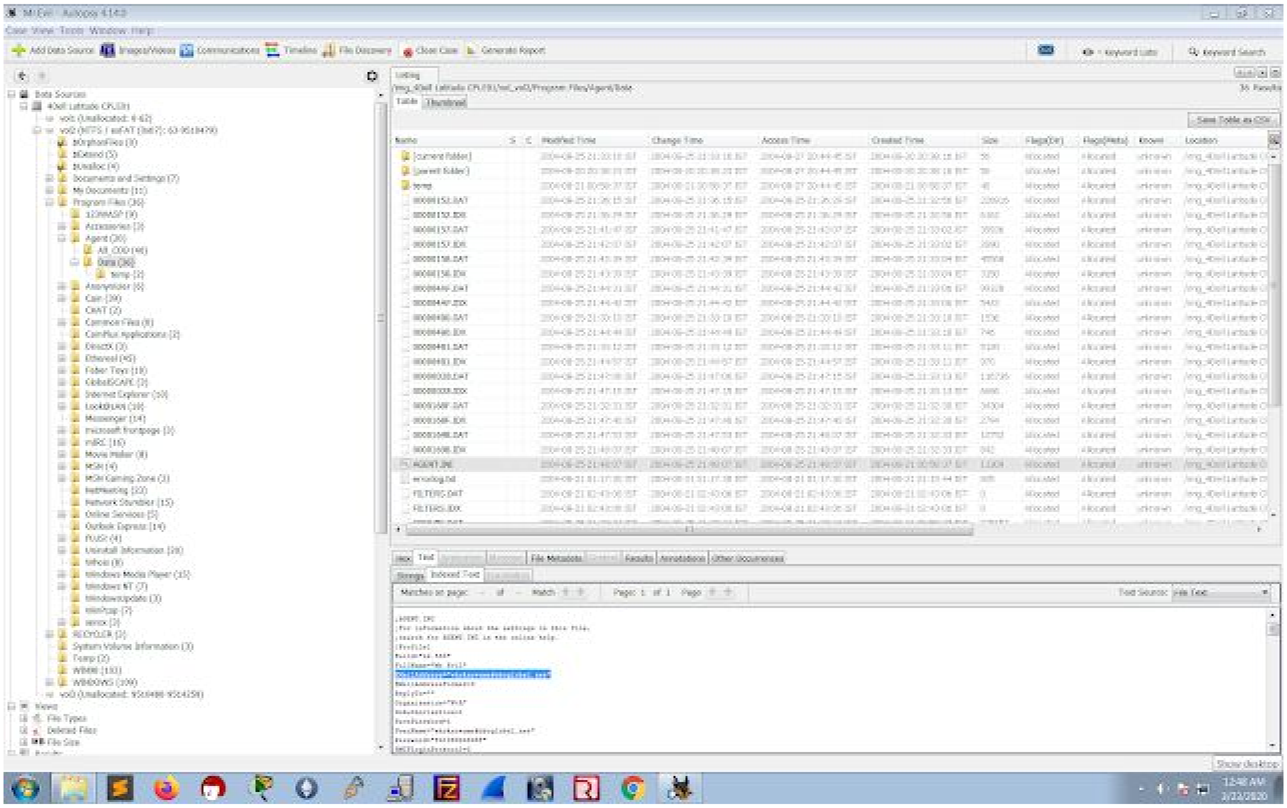
**Q13**. What is the SMTP email address for Mr. Evil?

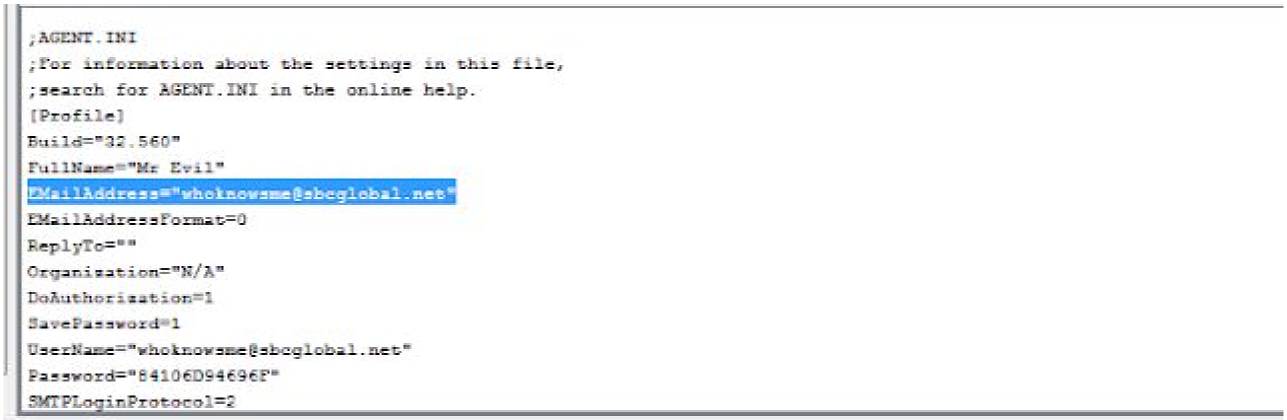
Ans13: The SMTP email address iswhoknowsme@sbcglobal.net

**How**?

Click on Data Sources select 4Dell Latitude --> vol2 -->

Program Files\Agent\Data\Agent.ini





```
;AGENT.INI
;For information about the settings in this file,
;search for AGENT.INI in the online help.
[Profile]
Build="32.560"
FullName="Mr Evil"
EMailAddress="whoknowsme@sbcglobal.net"
EMailAddressFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sbcglobal.net"
Password="84106D94696F"
SMTPLoginProtocol=2
```

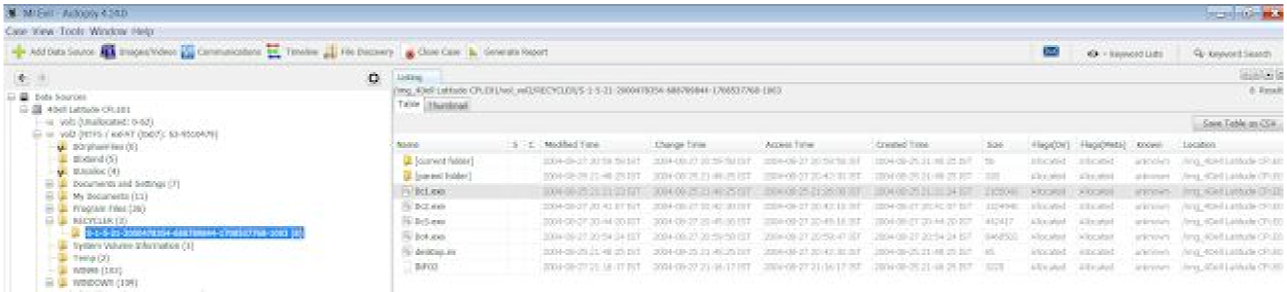
**Q14**. How many executable files are in the recycle bin?

Ans14: There are 4 files in recycle bin

**How?**

Click on Data Sources select 4Dell Latitude --> vol2 -->

Recycler



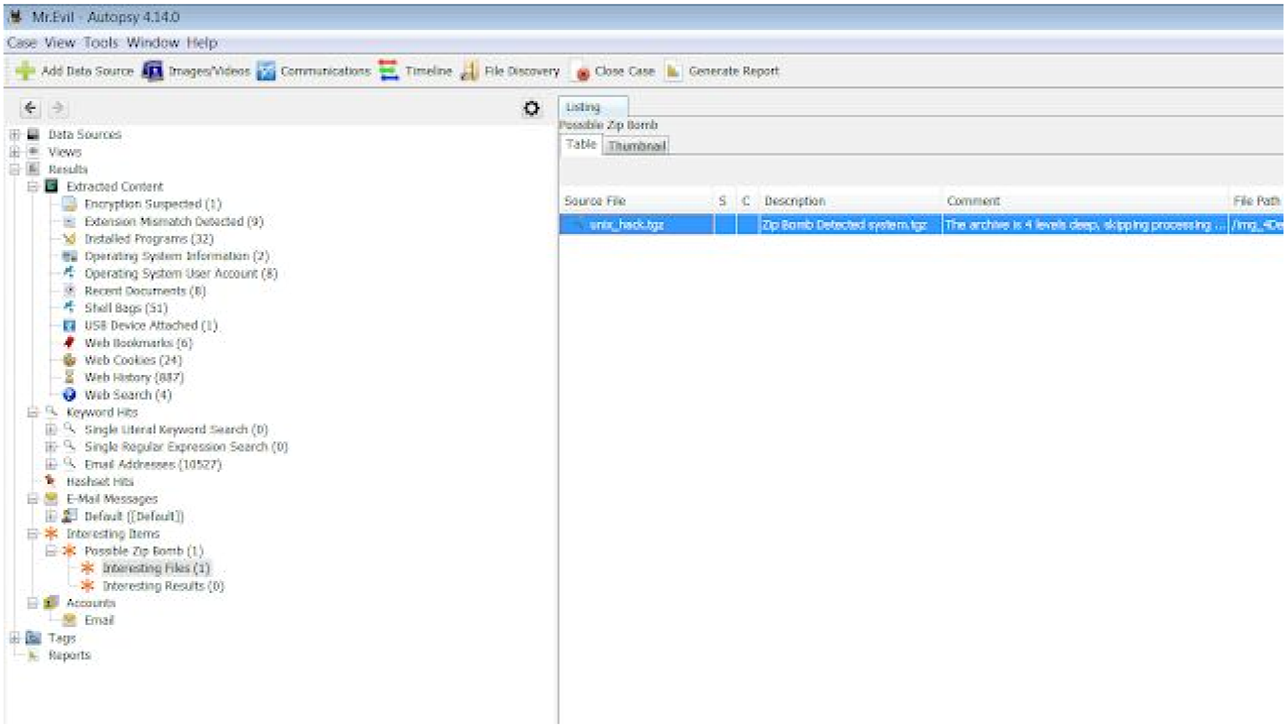
/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

| Name | S | C | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [current folder] | | | [illegible] | [illegible] | [illegible] | [illegible] | 56 | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |
| [parent folder] | | | [illegible] | [illegible] | [illegible] | [illegible] | 320 | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |
| Dc1.exe | | | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |
| Dc2.exe | | | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |
| Dc3.exe | | | [illegible] | [illegible] | [illegible] | [illegible] | 412417 | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |
| Dc4.exe | | | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |
| desktop.ini | | | [illegible] | [illegible] | [illegible] | [illegible] | 65 | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |
| INFO2 | | | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | Allocated | Allocated | unknown | /img_4Dell Latitude CPi.E0 |

**Q15**. Are there any malware on the computer?

Ans15: Yes there is a zip bomb malware by the name of unix_hack.giz in this system.
**How**?

Click on Results --> Extracted Content --> Interesting Items --> Possible Zip Bomb -->Interesting Files



Possible Zip Bomb

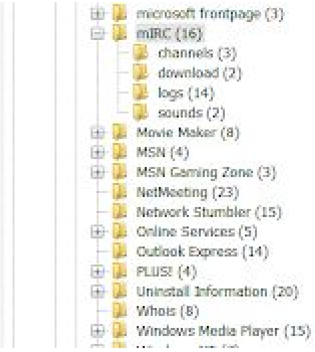
| Source File | S | C | Description | Comment | File Path |
|---|---|---|---|---|---|
| unix_hack.tgz | | | Zip Bomb Detected system.tgz | The archive is 4 levels deep, skipping processing ... | /img_4De |

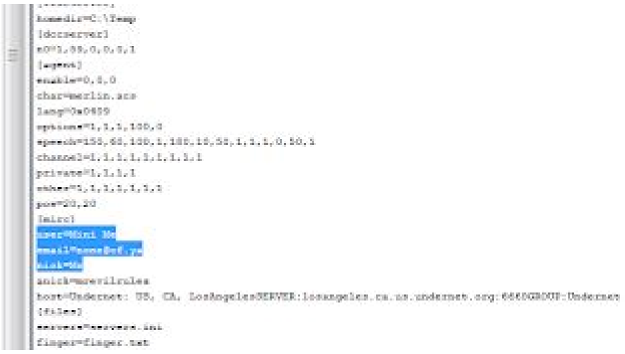
**Q16**. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the userid,

Ans16: user=Mini Me, email=none@of.ya, nick=Mr, anick=mrevilrulez
**How**?

Click on Data Sources select 4Dell Latitude --> vol2 -->

Program Files\mIRC\mirc.ini





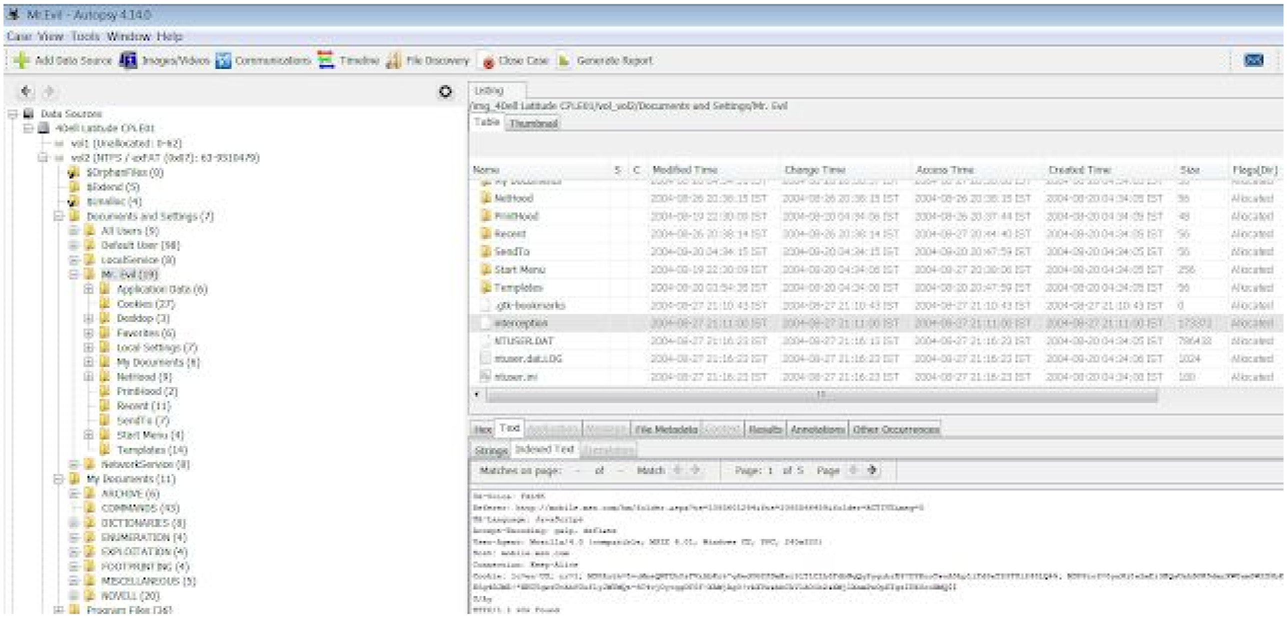
```
homedir=C:\Temp
[docserver]
n0=1,88,0,0,0,1
[agent]
enable=0,0,0
char=merlin.acs
lang=0x0409
options=1,1,1,100,0
speech=150,60,100,1,180,10,50,1,1,1,0,50,1
channel=1,1,1,1,1,1,1,1,1
private=1,1,1,1
other=1,1,1,1,1,1,1
pos=20,20
[mirc]
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
host=Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
[files]
servers=servers.ini
finger=finger.txt
```

**Q17**. Ethereal, a popular “sniffing” program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

Ans17: File name is Interception

**How?**

Click on Data Sources select 4Dell Latitude --> vol2 --> Document and Settings\Mr.Evil\intercerption



/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

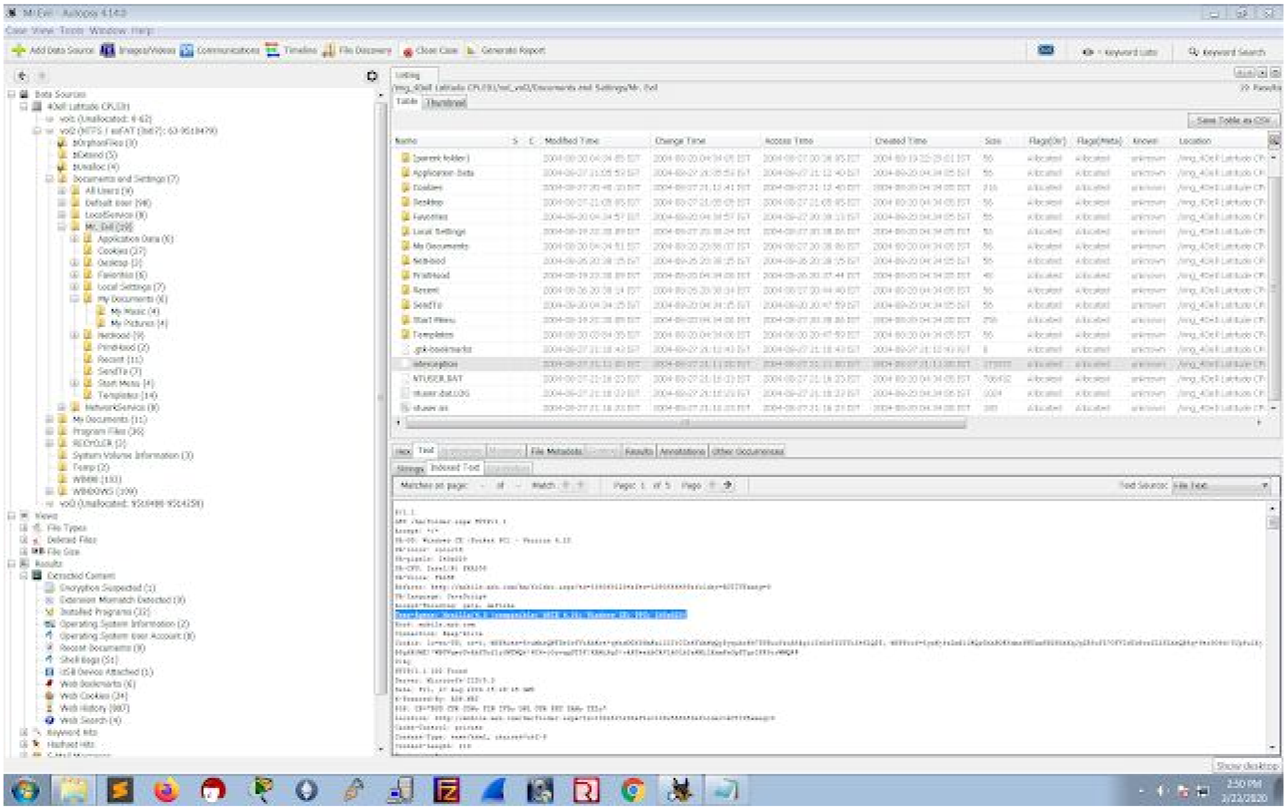
| Name | S | C | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) |
|---|---|---|---|---|---|---|---|---|
| NetHood | | | 2004-08-26 20:38:15 IST | 2004-08-26 20:38:15 IST | 2004-08-26 20:38:15 IST | 2004-08-20 04:34:05 IST | 56 | Allocated |
| PrintHood | | | 2004-08-19 22:30:09 IST | 2004-08-20 04:34:08 IST | 2004-08-26 20:37:44 IST | 2004-08-20 04:34:09 IST | 48 | Allocated |
| Recent | | | 2004-08-26 20:38:14 IST | 2004-08-26 20:38:14 IST | 2004-08-27 20:44:40 IST | 2004-08-20 04:34:05 IST | 56 | Allocated |
| SendTo | | | 2004-08-20 04:34:15 IST | 2004-08-20 04:34:15 IST | 2004-08-20 20:47:59 IST | 2004-08-20 04:34:05 IST | 56 | Allocated |
| Start Menu | | | 2004-08-19 22:30:09 IST | 2004-08-20 04:34:08 IST | 2004-08-27 20:38:06 IST | 2004-08-20 04:34:05 IST | 256 | Allocated |
| Templates | | | 2004-08-20 03:54:38 IST | 2004-08-20 04:34:08 IST | 2004-08-20 20:47:59 IST | 2004-08-20 04:34:05 IST | 56 | Allocated |
| .gtk-bookmarks | | | 2004-08-27 21:10:43 IST | 2004-08-27 21:10:43 IST | 2004-08-27 21:10:43 IST | 2004-08-27 21:10:43 IST | 0 | Allocated |
| interception | | | 2004-08-27 21:11:00 IST | 2004-08-27 21:11:00 IST | 2004-08-27 21:11:00 IST | 2004-08-27 21:11:00 IST | 173391 | Allocated |
| NTUSER.DAT | | | 2004-08-27 21:16:23 IST | 2004-08-27 21:16:13 IST | 2004-08-27 21:16:23 IST | 2004-08-20 04:34:05 IST | 786432 | Allocated |
| ntuser.dat.LOG | | | 2004-08-27 21:16:23 IST | 2004-08-27 21:16:23 IST | 2004-08-27 21:16:23 IST | 2004-08-20 04:34:06 IST | 1024 | Allocated |
| ntuser.ini | | | 2004-08-27 21:16:23 IST | 2004-08-27 21:16:23 IST | 2004-08-27 21:16:23 IST | 2004-08-20 04:34:08 IST | 180 | Allocated |

```
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093584918&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: [illegible]
[illegible]
0/hy
HTTP/1.1 [illegible] Found
```

**Q18**. Which internet browser was used?

Ans18: Internet explorer
**How?**

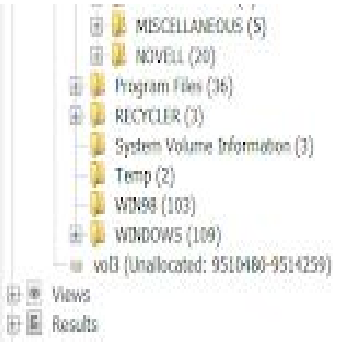
Click on Data Sources select 4Dell Latitude --> vol2 --> Document and Settings\Mr.Evil\interceprtion
scroll down and see User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)

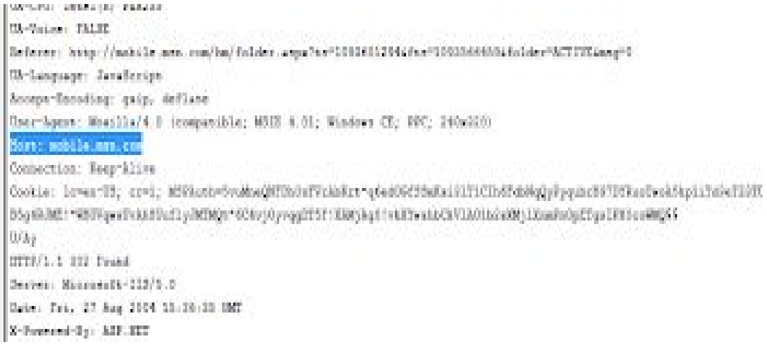


**Q19**. What websites victim was accessing?

Ans19: login.passport.com, mobile.msn.com, [www.passportimages.com](http://www.passportimages.com)
How?

you can also copy all texts from ***intercept*** file and search for the .com it will show you the websites which were visited.





```
UA-CPU: [illegible]
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=[illegible]&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; [illegible]
[illegible]
U/A;
HTTP/1.1 302 Found
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:28:33 GMT
X-Powered-By: ASP.NET
```

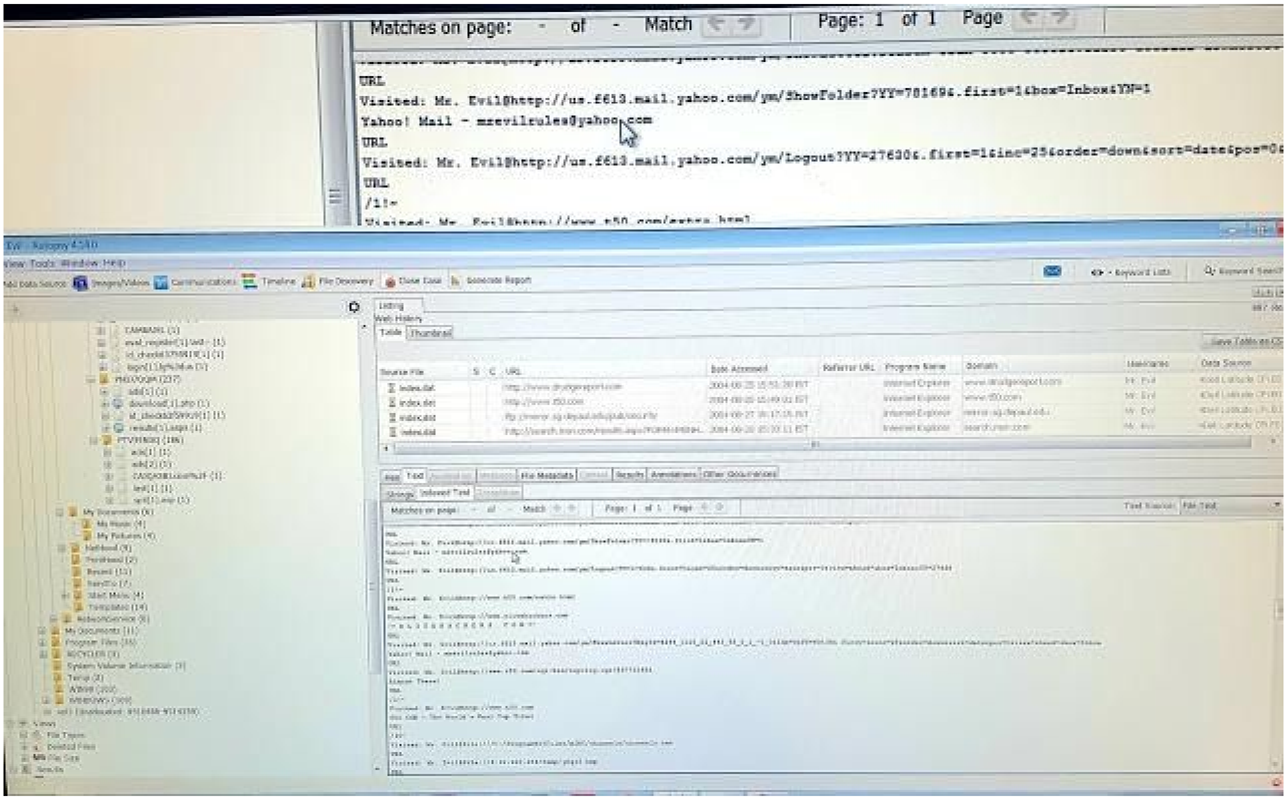
**Q20**. What is the web-based email address for the main user?

Ans20:  mrevilrulez@yahoo.com was found in web history.

**How**?

Click on Results --> Extracted Content --> Web History

I have used Windows 7 Magnifier to zoom in



```
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowFolder?YY=78169&.first=1&box=Inbox&YN=1
Yahoo! Mail - mrevilrulez@yahoo.com
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/Logout?YY=27630&.first=1&inc=25&order=down&sort=date&pos=0
URL
/1!-
Visited: Mr. Evil@http://www.t50.com/extra.html
```

## Conclusion

Computers Forensics is a vast field of study and includes topics like Processing Crime Scenes, Operating Systems and File Structures, Recovering Graphic Files and Defeating Steganography, Email Investigations, Mobile Device Investigations, Report Writing.