

**Kashish Srivastava**  
**500067405**  
**R134218079**

## LAB EXPERIMENT 3 - AUTOPSY

### Questions:

#### Q1. Search for programs/tools that aided in the crime (Wireless Hacking)

**Ans:**

Ethereal

WinPcap

NetStumbler

Look@LAN

123 Write all sorted passwords

Cain&Abel

CuteFTP

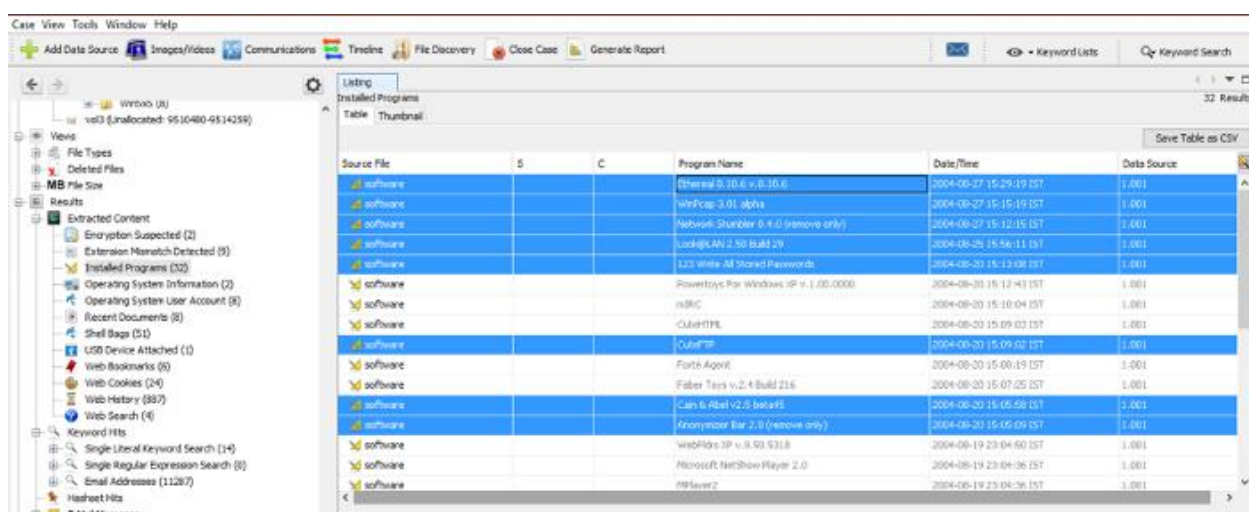
Anonymizer

As provided by the hint Results>Extracted Content

We find several files such as operating system user account, operating system information, web cookies and more. For the tools to be used in the crime they have to be installed in the system hence. We look into installed system.

We find that it has several softwares listed by the name and we need to focus on the ones that are used for wireless hacking.

Path: **Results>Extracted Content>Installed Programs>Program Names**



Source File	S	C	Program Name	Date/Time	Data Source
software			Ethereal 3.10.6 v.3.10.6	2004-08-27 15:29:19 IST	1.001
software			WinPcap 3.01.alpha	2004-08-27 15:15:19 IST	1.001
software			NetStumbler 0.4.0 (remove only)	2004-08-27 15:12:15 IST	1.001
software			Look@LAN 2.50 Build 29	2004-08-26 15:56:11 IST	1.001
software			123 Write All Stored Passwords	2004-08-20 15:13:08 IST	1.001
software			PowerToys For Windows XP v.1.00.0000	2004-08-20 15:12:43 IST	1.001
software			nsIRC	2004-08-20 15:10:04 IST	1.001
software			CuteFTP	2004-08-20 15:09:03 IST	1.001
software			Anonymizer	2004-08-20 15:09:02 IST	1.001
software			Forti Agent	2004-08-20 15:08:19 IST	1.001
software			Fiber Task v.2.4 Build 216	2004-08-20 15:07:25 IST	1.001
software			Cain & Abel v2.0 beta05	2004-08-20 15:05:59 IST	1.001
software			Anonymizer 2.0 (remove only)	2004-08-20 15:05:09 IST	1.001
software			WebPids XP v.0.93 5318	2004-08-19 23:04:50 IST	1.001
software			Microsoft NetShow Player 2.0	2004-08-19 23:04:36 IST	1.001
software			MPViewer2	2004-08-19 23:04:36 IST	1.001

#### Q2. Which Email client is used by Mr. Evil?

**Ans:**

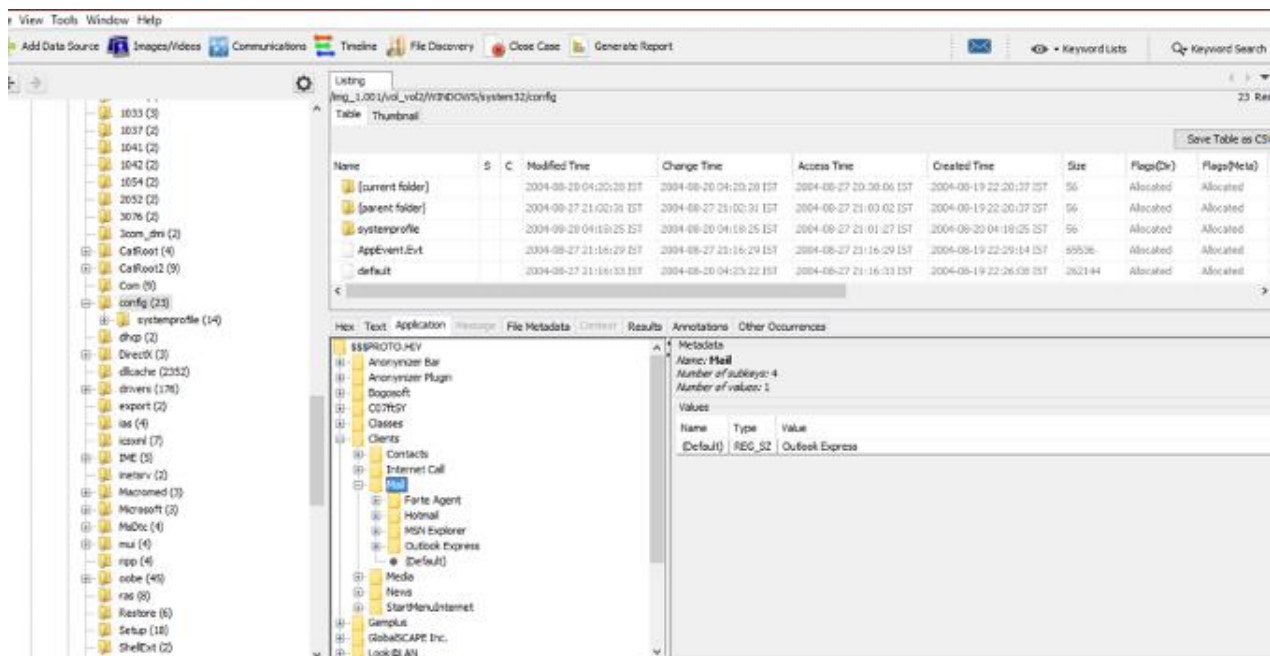
Outlook Express  
Forte Agent  
MSN Explorer  
MSN (Hotmail) Email

In previous experiment we observed that the email details are mostly present in system32 folder.

Hence I traverse on the path C:Windows/system32/config/

In config in the applications section we find Clients and then Mail and find 4 folders named as Outlook Express, Forte Agent, MSN Explorer & MSN (Hotmail) Email.

The path is **C:Windows/system32/config/Clients/Mail/(4 folders)**



**Q3. What is the SMTP email address for Mr. Evil?**

**Ans:**

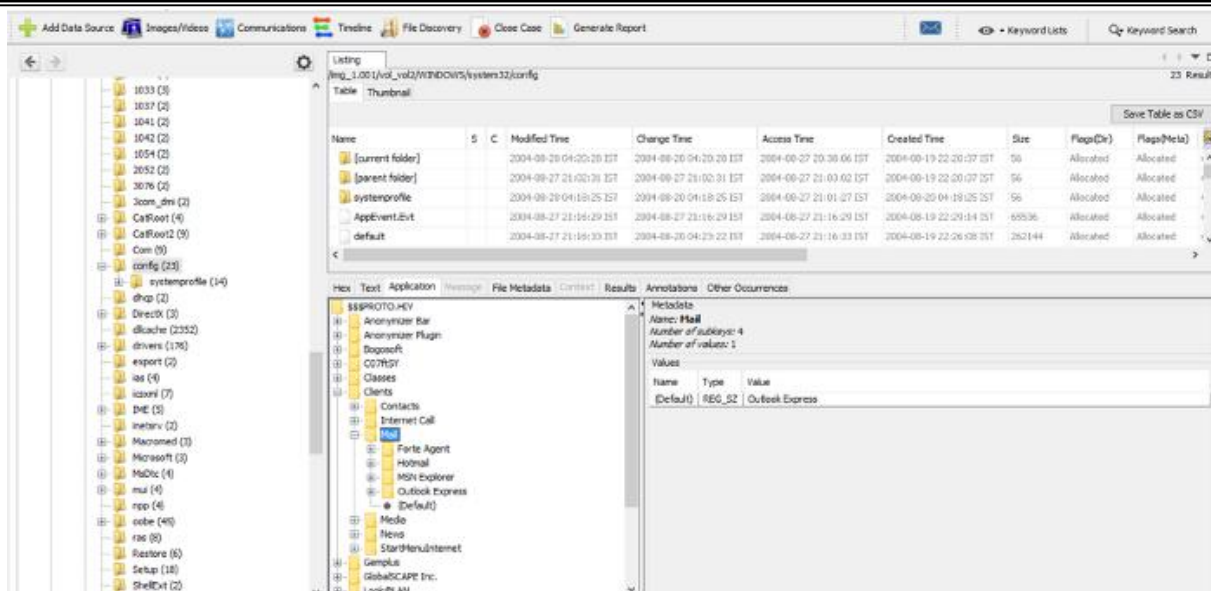
Whoknowsme@sbcglobal.net

As provided in the hint we traverse for Program files and agent.

In agent after finding I found AGENT.INI in data.

SMTPUserName: Whoknowsme@sbcglobal.net is mentioned in Data in agent.ini file

The path is : **C:\Program Files\Agent\Data\AGENT.INI**



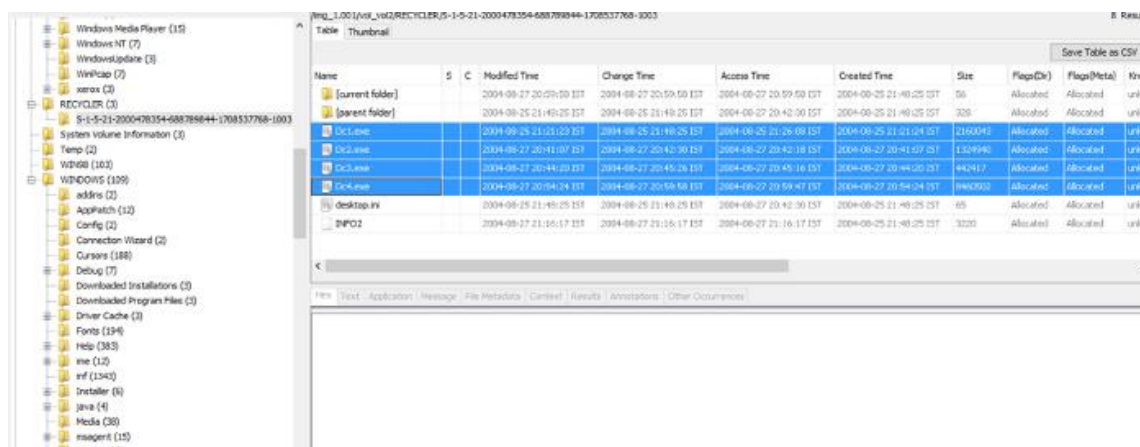
#### Q4. How many executable files are in the recycle bin?

**Ans:**

Dc1.exe  
Dc2.exe  
Dc3.exe  
Dc4.exe

For finding executable files in recycle bin, we check a folder names as Recycler in C:  
After opening the folder, several files are present. We need to look for the executable files. We find 4 files with .exe extension.

The path is : **C:\Recycler/sub-folder(long name)/.exe extension files**

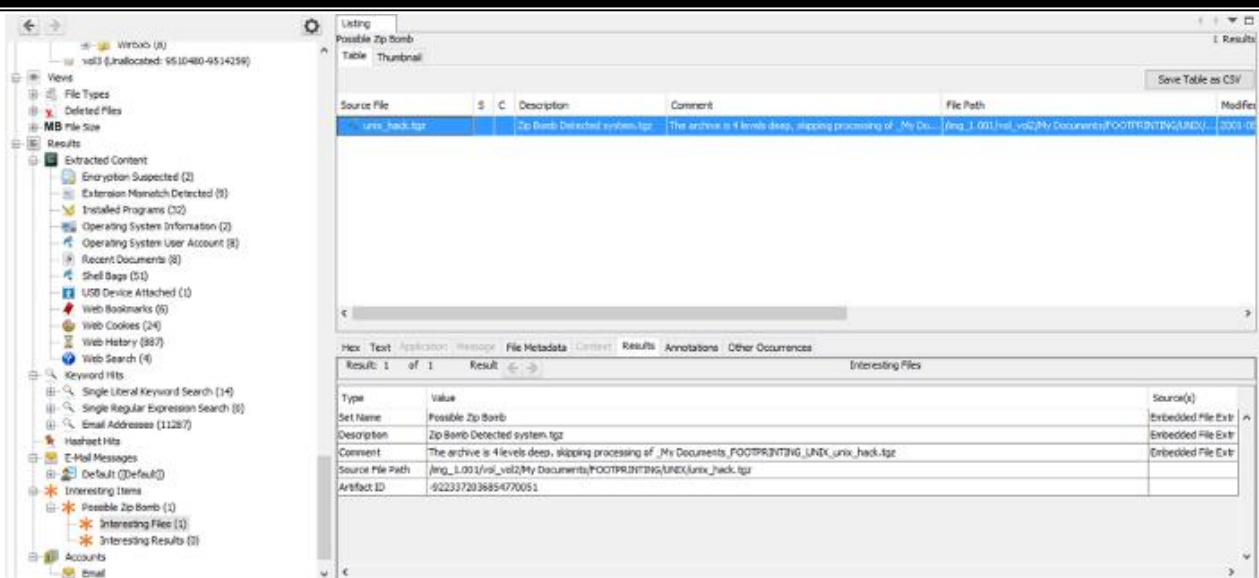


#### Q5. Is there any malware on the computer?

**Ans:** Unix\_Hacz.tgz

I searched google for malware files in autopsy and it explained that Interesting files has all the malwares present.

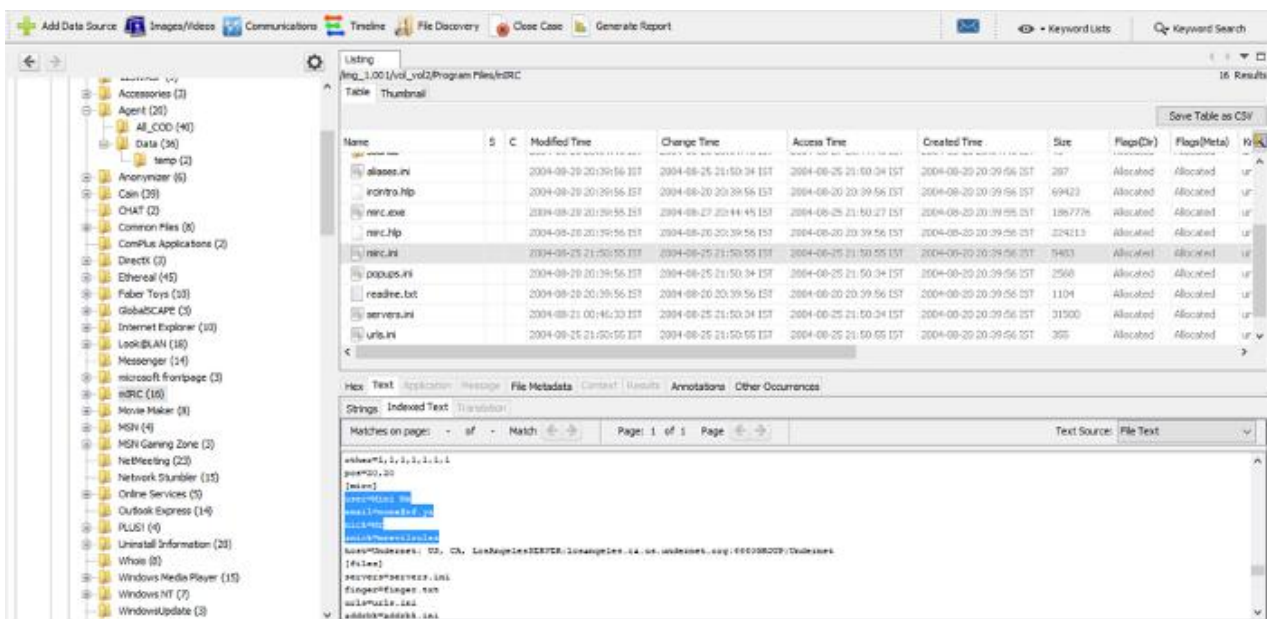
The path was direct : **Results/Interesting Items/Possible Zipbomb/Interesting files**



**Q6. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the userid?**

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

The path is **C:\Program Files\mIRC\mirc.ini**



## BONUS Questions

**Q7. 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?**



**Ans:** File name is 'Interception'

As hinted we need to go to through My Documents which in this case would be Documents and then Setting and we explore the folder Mr.Evil, since it contains intercepted data it is interception file

The path is: *Documents and Settings/Mr.Evil/Interception file*

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)
Recent			2004-08-26 20:38:14 IST	2004-08-26 20:38:14 IST	2004-08-27 20:44:40 IST	2004-08-28 04:34:05 IST	56	Allocated	Allocated
SendTo			2004-08-26 04:34:15 IST	2004-08-26 04:34:15 IST	2004-08-28 20:47:59 IST	2004-08-28 04:34:05 IST	56	Allocated	Allocated
Start Menu			2004-08-19 22:30:09 IST	2004-08-20 04:34:06 IST	2004-08-27 20:36:06 IST	2004-08-28 04:34:05 IST	256	Allocated	Allocated
Templates			2004-08-20 03:54:35 IST	2004-08-20 04:34:06 IST	2004-08-28 20:47:59 IST	2004-08-28 04:34:05 IST	56	Allocated	Allocated
.gk-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	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	173372	Allocated	Allocated
NTUSER.DAT			2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-28 04:34:05 IST	766432	Allocated	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	2004-08-28 04:34:06 IST	1024	Allocated	Allocated
ntuser.ini			2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-28 04:34:06 IST	180	Allocated	Allocated

Name	/img_1.001/vol_2/Documents and Settings/Mr. Evil/Interception
Type	File System
MIME Type	application/vnd.tcpdump.pcap
Size	173372
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2004-08-27 21:11:00 IST
Accessed	2004-08-27 21:11:00 IST
Created	2004-08-27 21:11:00 IST

**Q8. Which internet browser was used?**

**Ans:** Internet Explorer 4

I had opened the interception file in the previous question. Where I directly found the internet browser - Internet Explorer 4

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)
Recent			2004-08-26 20:38:14 IST	2004-08-26 20:38:14 IST	2004-08-27 20:44:40 IST	2004-08-28 04:34:05 IST	56	Allocated	Allocated
SendTo			2004-08-26 04:34:15 IST	2004-08-26 04:34:15 IST	2004-08-28 20:47:59 IST	2004-08-28 04:34:05 IST	56	Allocated	Allocated
Start Menu			2004-08-19 22:30:09 IST	2004-08-20 04:34:06 IST	2004-08-27 20:36:06 IST	2004-08-28 04:34:05 IST	256	Allocated	Allocated
Templates			2004-08-20 03:54:35 IST	2004-08-20 04:34:06 IST	2004-08-28 20:47:59 IST	2004-08-28 04:34:05 IST	56	Allocated	Allocated
.gk-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	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	173372	Allocated	Allocated
NTUSER.DAT			2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-28 04:34:05 IST	766432	Allocated	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	2004-08-28 04:34:06 IST	1024	Allocated	Allocated

Strings	Indexed Text	Translation
Matches on page: 1 of 5	Match	Page: 1 of 5
Text Source: File Text		
HTTP/1.1 200 Found		

**Q9. What websites victim was accessing?**

**Ans:** Mobile.msn.com, MSN (Hotmail) Email

The websites are mentioned in the same interception file. Under the browser.

The screenshot displays the XactiView application window. On the left, a file tree shows a hierarchy of folders and files, including 'vol1' and 'vol2'. The 'vol2' folder is expanded, showing subfolders like 'Documents and Settings' and 'My Documents'. The main pane on the right shows a table of files. The table has columns: Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), and Flags(Meta). The file 'ntuser.datLOG' is highlighted in the table. Below the table, there is a section for 'Hex Text Application Message File Metadata Content Results Annotations Other Occurrences'. The 'Text' tab is selected, showing a preview of the file's content, which appears to be a Windows registry file.