Kashish Srivastava
500067405
R134218079

LAB EXPERIMENT 2 - AUTOPSY

Questions:

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

Ans: ***2004/08/27–10:46:27***

The path followed for identifying the time :

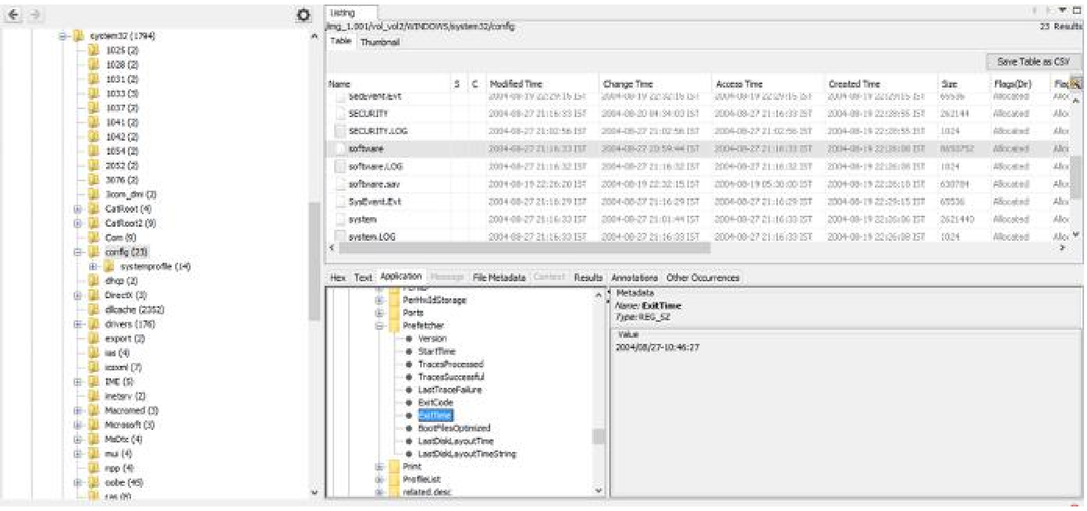
After the image, we need to click on C:\Windows\System32\Config in the left hand pannel it consists of all the configuration files.

In the centre pannel, after config we find out the software column that includes Microsoft\WindowNT\Currentversion

After that we can click on Prefetcher exploring all the folders as in prefetcher we find several time mentioned and we have to look for exit time:

Prefetcher\ExitTime - that denotes the last decorded shut down time.

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



/img_1.001/vol_vol2/WINDOWS/system32/config

23 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Fla
secevent.evt			2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allo
SECURITY			2004-08-27 21:16:33 IST	2004-08-20 04:34:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allo
SECURITY.LOG			2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allo
software			2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	[illegible]	Allocated	Allo
software.LOG			2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allo
software.sav			2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:10 IST	630784	Allocated	Allo
SysEvent.Evt			2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allo
system			2004-08-27 21:16:33 IST	2004-08-27 21:01:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:06 IST	2621440	Allocated	Allo
system.LOG			2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allo

Metadata

Name: **ExitTime**

Type: REG_SZ

Value

2004/08/27-10:46:27

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

Ans: ***5 accounts***

Administrator

Guest

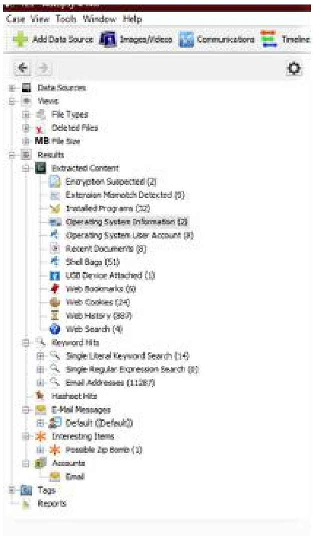
HelpAssistant

Mr. Evil

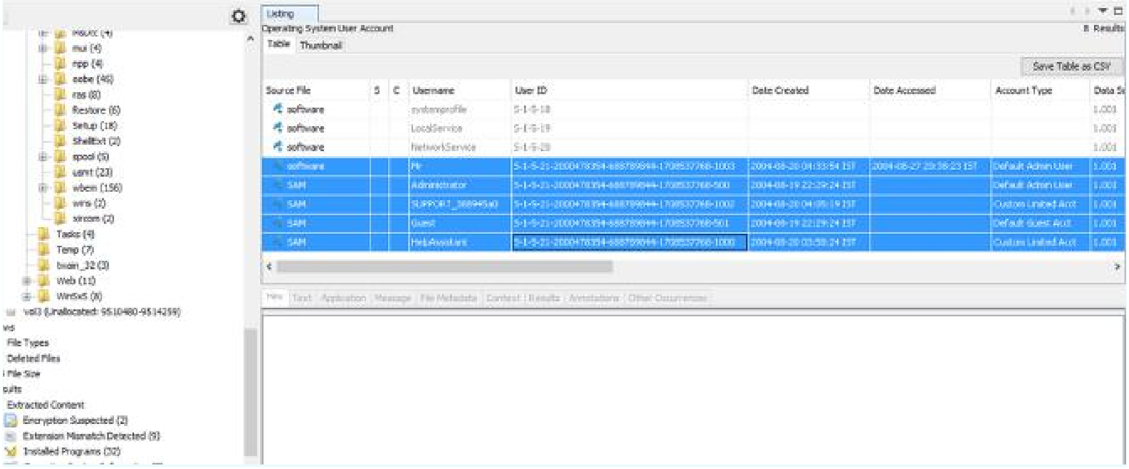
SUPPORT_388945a0

<<Looking at the Account Type as it says " default admin user">>

In the results , extracted content has the OS user accounts. We found OS information in last lab activity , similarly we find OS User Account tab.



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



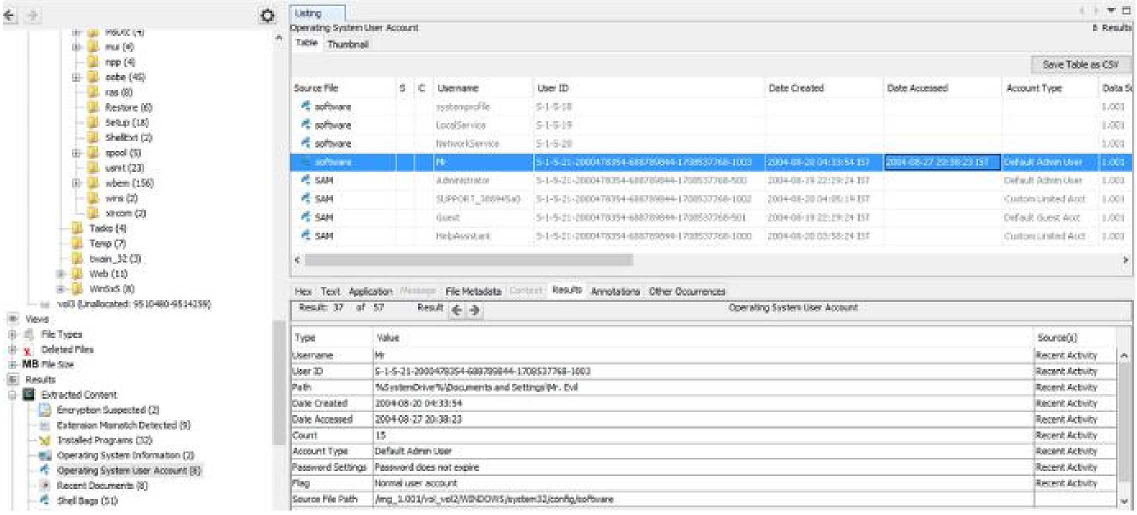
Operating System User Account

Source File	S	C	Username	User ID	Date Created	Date Accessed	Account Type	Data S
software			systemprofile	S-1-5-18				1.001
software			LocalService	S-1-5-19				1.001
software			NetworkService	S-1-5-20				1.001
software			Mr	S-1-5-21-2000478354-688789844-1708537768-1003	2004-08-20 04:33:54 IST	2004-08-27 20:38:23 IST	Default Admin User	1.001
SAM			Administrator	S-1-5-21-2000478354-688789844-1708537768-500	2004-08-19 22:29:24 IST		Default Admin User	1.001
SAM			SUPPORT_388945a0	S-1-5-21-2000478354-688789844-1708537768-1002	2004-08-20 04:05:19 IST		Custom Limited Acct	1.001
SAM			Guest	S-1-5-21-2000478354-688789844-1708537768-501	2004-08-19 22:29:24 IST		Default Guest Acct	1.001
SAM			HelpAssistant	S-1-5-21-2000478354-688789844-1708537768-1000	2004-08-20 03:58:24 IST		Custom Limited Acct	1.001

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

Ans: Mr. Evil

(Check via *Date Accessed* column, beside Acount Type similarly in Q7. above) Inbottomwe look for results and beside its mentioned as recent activity



Operating System User Account

Source File	S	C	Username	User ID	Date Created	Date Accessed	Account Type	Data S
software			systemprofile	S-1-5-18				1.001
software			LocalService	S-1-5-19				1.001
software			NetworkService	S-1-5-20				1.001
software			Mr	S-1-5-21-2000478354-688789844-1708537768-1003	2004-08-20 04:33:54 IST	2004-08-27 20:38:23 IST	Default Admin User	1.001
SAM			Administrator	S-1-5-21-2000478354-688789844-1708537768-500	2004-08-19 22:29:24 IST		Default Admin User	1.001
SAM			SUPPORT_388945a0	S-1-5-21-2000478354-688789844-1708537768-1002	2004-08-20 04:05:19 IST		Custom Limited Acct	1.001
SAM			Guest	S-1-5-21-2000478354-688789844-1708537768-501	2004-08-19 22:29:24 IST		Default Guest Acct	1.001
SAM			HelpAssistant	S-1-5-21-2000478354-688789844-1708537768-1000	2004-08-20 03:58:24 IST		Custom Limited Acct	1.001

Result: 37 of 57 Result

Operating System User Account

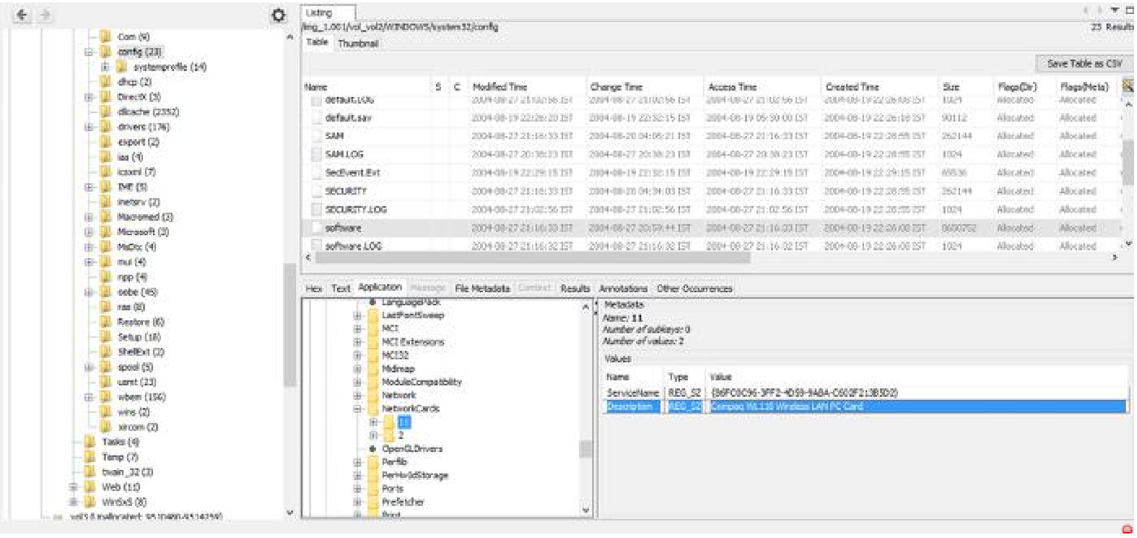
Type	Value	Source(s)
Username	Mr	Recent Activity
User ID	S-1-5-21-2000478354-688789844-1708537768-1003	Recent Activity
Path	%SystemDrive%\Documents and Settings\Mr. Evil	Recent Activity
Date Created	2004-08-20 04:33:54	Recent Activity
Date Accessed	2004-08-27 20:38:23	Recent Activity
Count	15	Recent Activity
Account Type	Default Admin User	Recent Activity
Password Settings	Password does not expire	Recent Activity
Flag	Normal user account	Recent Activity
Source File Path	/img_1.001/vol_vol2/WINDOWS/system32/config/software	

Q9. List the network cards used by this computer?

Ans: Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

Compaq WL110 Wireless LAN PC Card

The details we need to find out belongs to configuration system files hence we follow the same path as in the Q6. *C:\WINDOWS\system32\config\software\Microsoft\Windows NT\CurrentVersion\* and since we need to find network cards we get a folder named as network cards and we explore it.



/img_1.001/vol_vol2/WINDOWS/system32/config

23 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
default.LOG			2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated
default.sav			2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 06:30:00 IST	2004-08-19 22:26:18 IST	90112	Allocated	Allocated
SAM			2004-08-27 21:16:33 IST	2004-08-20 04:08:21 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated
SAM.LOG			2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated
SecEvent.Evt			2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated
SECURITY			2004-08-27 21:16:33 IST	2004-08-20 04:34:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated
SECURITY.LOG			2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated
software			2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	8650752	Allocated	Allocated
software.LOG			2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated

Metadata

Name: **11**

Number of subkeys: 0

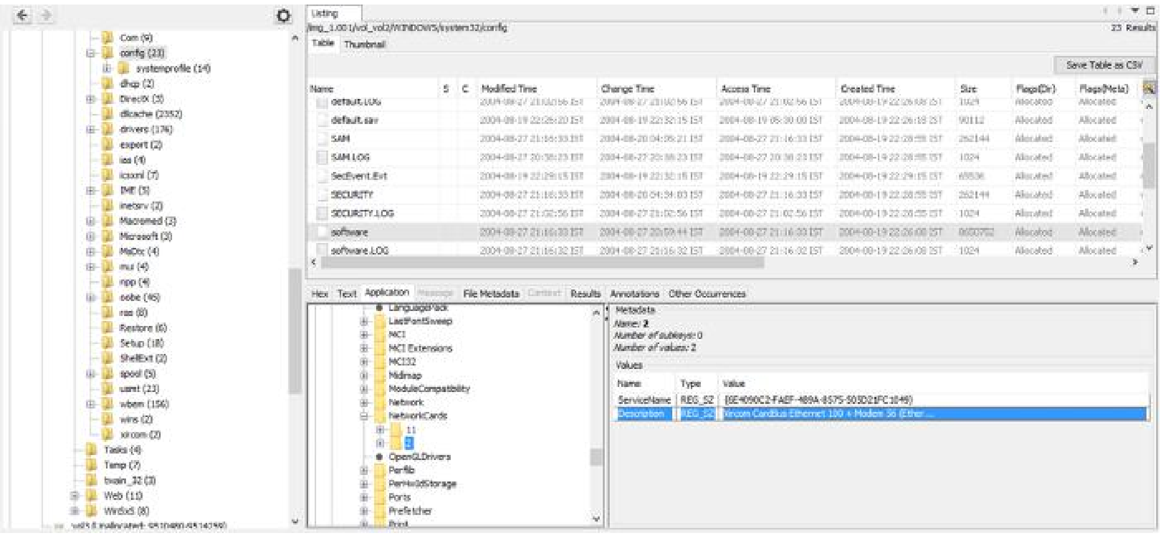
Number of values: 2

Values

Name	Type	Value
ServiceName	REG_SZ	{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}
Description	REG_SZ	Compaq WL110 Wireless LAN PC Card

After clicking on network cards we find two folders

We explore both of them and find the details



/img_1.001/vol_vol2/WINDOWS/system32/config

23 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
default.LOG			2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated
default.sav			2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 06:30:00 IST	2004-08-19 22:26:18 IST	90112	Allocated	Allocated
SAM			2004-08-27 21:16:33 IST	2004-08-20 04:08:21 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated
SAM.LOG			2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated
SecEvent.Evt			2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated
SECURITY			2004-08-27 21:16:33 IST	2004-08-20 04:34:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated
SECURITY.LOG			2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated
software			2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	8650752	Allocated	Allocated
software.LOG			2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated

Metadata

Name: **2**

Number of subkeys: 0

Number of values: 2

Values

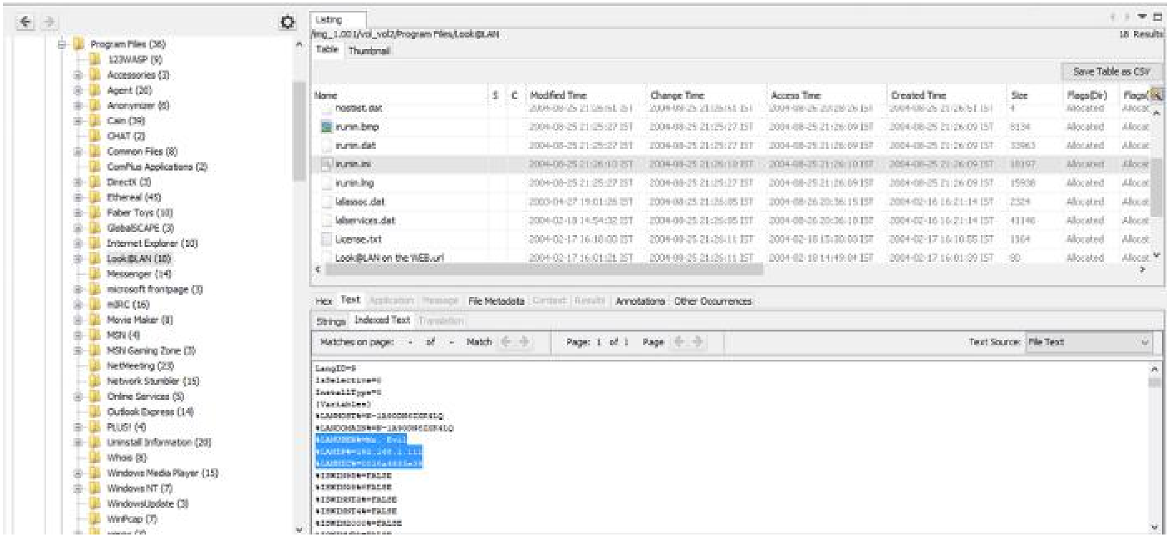
Name	Type	Value
ServiceName	REG_SZ	{6E4090C2-FAEF-489A-8575-505D21FC1049}
Description	REG_SZ	Xircom CardBus Ethernet 100 + Modem 56 (Ether...

We find answer at *C:\WINDOWS\system32\config\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\<<we get 2 cards>>*

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

Ans: IP=192.168.1.111

MAC=00:10:a4:93:3e:09



- Program Files (36)
  - 123WASP (9)
  - Accessories (3)
  - Agent (26)
  - 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)
  - 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)

Listing

/img_1.001/vol_vol2/Program Files/Look@LAN

18 Results

Table Thumbnail

Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(
hosttest.dat			2004-08-25 21:26:51 IST	2004-08-25 21:26:51 IST	2004-08-26 20:28:26 IST	2004-08-25 21:26:51 IST	4	Allocated	Allocat
irunin.bmp			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 IST	2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST	8134	Allocated	Allocat
irunin.dat			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 IST	2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST	33963	Allocated	Allocat
irunin.ini			2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:09 IST	18197	Allocated	Allocat
irunin.lng			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 IST	2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST	15938	Allocated	Allocat
lalassoc.dat			2003-04-27 19:01:26 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:15 IST	2004-02-16 16:21:14 IST	2324	Allocated	Allocat
laservices.dat			2004-02-18 14:54:32 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:10 IST	2004-02-16 16:21:14 IST	41146	Allocated	Allocat
License.txt			2004-02-17 16:10:00 IST	2004-08-25 21:26:11 IST	2004-02-18 15:30:00 IST	2004-02-17 16:10:55 IST	1564	Allocated	Allocat
Look@LAN on the WEB.url			2004-02-17 16:01:21 IST	2004-08-25 21:26:11 IST	2004-02-18 14:49:04 IST	2004-02-17 16:01:39 IST	80	Allocated	Allocat

```
LangID=9
IsSelection=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
%ISWIN2000%=FALSE
```

Mostly the ip addresses are found in domain areas, in program files we find out several folders since we need to look for IP and Mac address after exploring most of the folders I find Look@LAN

In that we find several options after exploring them I land into irunin.ini file that contains IP and MAC address

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