NIST Hacking Case Writeup

1. **What is the image hash? Does the acquisition and verification hash match?**

The md5 value is aee4fcd9301c03b3b054623ca261959a.

```
root@kali:~/Desktop# md5sum SCHARDT
aee4fcd9301c03b3b054623ca261959a  SCHARDT
```

2. **What operating system was used on the computer?**

Windows XP. (I loaded the image in Autopsy, and then checked the Image Details.)

FILE SYSTEM INFORMATION

File System Type: NTFS
Volume Serial Number: B26CB1CE6CB18D9B
OEM Name: NTFS
Version: Windows XP

3. **When was the install date?**

The install date info lies in the "HKLM\Software\Microsoft\Windows NT\CurrentVersion\InstallDate". We can run RegRipper on EnCase image to get this info. However, I did this in another way. I checked MFT Entry and found the install date is 2004-08-19 12:57:43.694987200 (EDT).

4. **What is the timezone settings?**

TimeZoneInformation key

ControlSet001\Control\TimeZoneInformation

LastWriteTime Thu Aug 19 17:20:02 2004 (UTC)

DaylightName -> Central Daylight Time

StandardName -> Central Standard Time

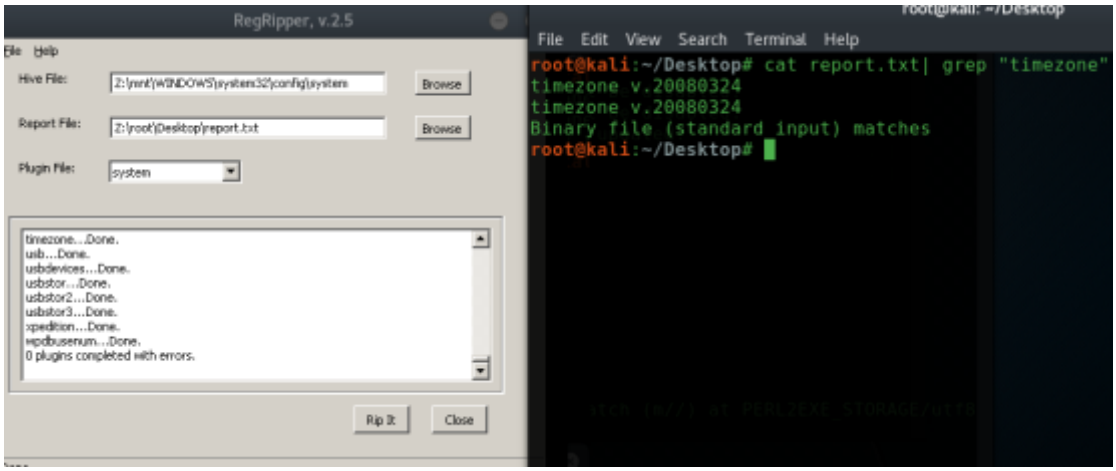
Bias -> 360 (6 hours)

ActiveTimeBias -> 300 (5 hours)

First, mount dd image on /mnt with command:

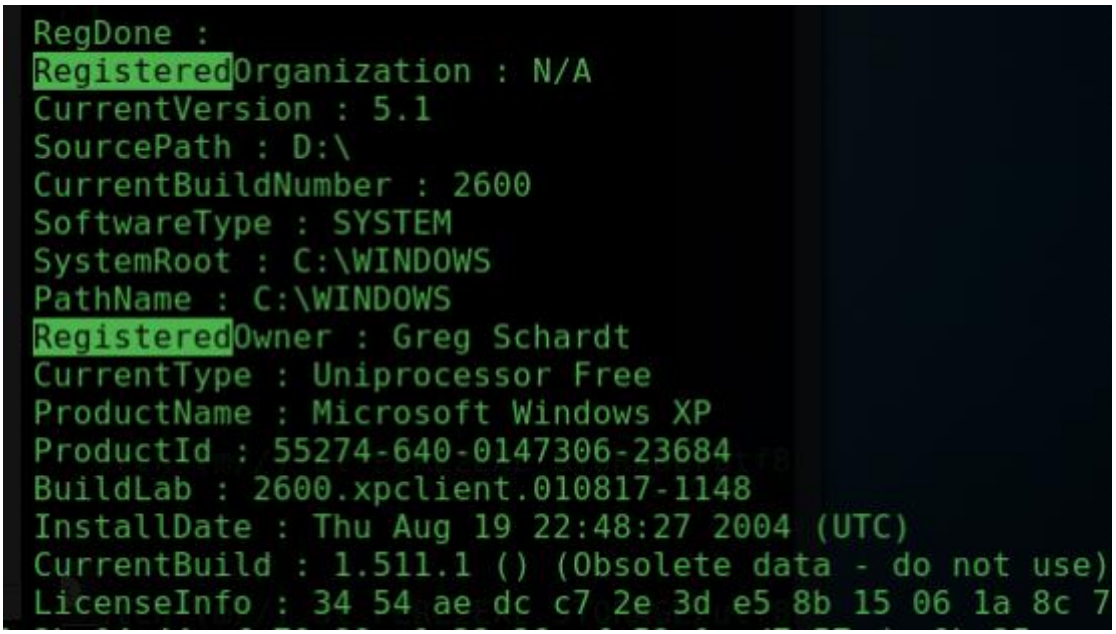
```
mount SCHARDT / mnt -o, offset =32256,l oop
```

Then user RegRipper to load “\mnt\WINDOWS\system32\config\system” as Hive File and generate report.txt which contains all the information in System Hive. The same, software.txt is generated with Software Hive. We can now get bunch of system info by searching keyword in these two report files.



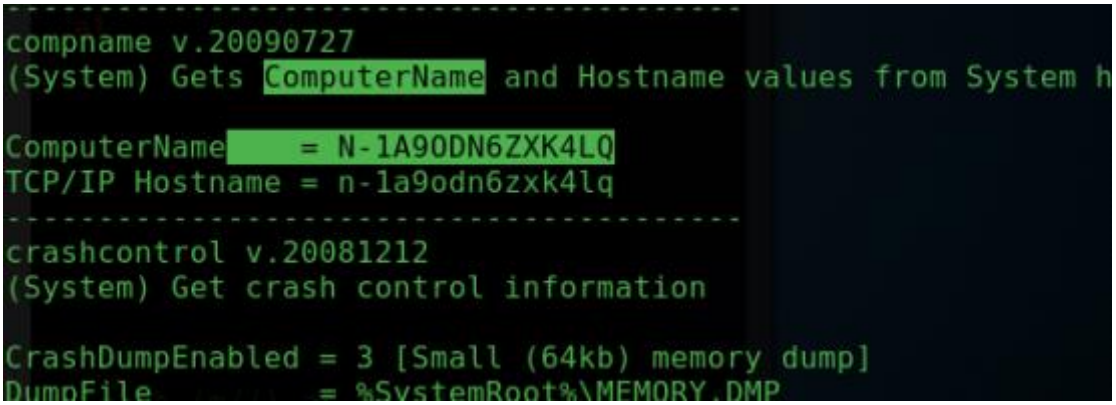
5. Who is the registered owner?

Greg Schardt. It’s in software hive.



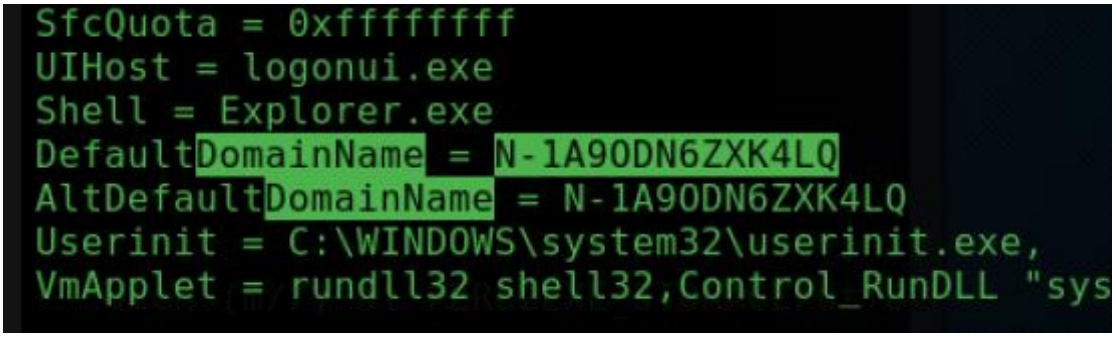
6. What is the computer account name?

ComputerName = N-1A9ODN6ZXK4LQ



7. What is the primary domain name?

N-1A9ODN6ZXK4LQ



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

ShutdownTime = Fri Aug 27 15:46:33 2004 (UTC)

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

There are 5. Users' information is stored in SAM (Security Account Manager) Hive. All the user accounts can be found here.

```
Login Count     : 0
  --> Password does not expire
  --> Normal user account

Username        : SUPPORT_388945a0 [1002]
Full Name       : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
User Comment    : This is a vendor's account for the Help and Support Service
Account Type    : Custom Limited Acct
Account Created : Thu Aug 19 22:35:19 2004 Z
Last Login Date : Never
Pwd Reset Date  : Thu Aug 19 22:35:19 2004 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Account Disabled
  --> Normal user account

Username        : Mr. Evil [1003]
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Aug 19 23:03:54 2004 Z
Last Login Date : Fri Aug 27 15:08:23 2004 Z
Pwd Reset Date  : Thu Aug 19 23:03:54 2004 Z
Pwd Fail Date   : Never
Login Count     : 15
  --> Password does not expire
  --> Normal user account
```

10. What is the account name of the user who mostly uses the computer?

We can also find the Login Count value in SAM Hive. Mr. Evil has the most uses which is 15.

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

Mr. Evil. We can get this answer by comparing the Last Login Date.

12. A search for the name of "Greg Schardt" reveals multiple hits. One of these proves that Greg Schardt is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

Look@LAN

```
root@kali:/mnt# grep -R "Greg Schardt" .
./Program Files/Look@LAN/irunin.ini:%REGOWNER%=Greg Schardt
./Program Files/Look@LAN/irunin.ini:%USERNAME%=Greg Schardt
./WINDOWS/Look@LAN Setup Log.txt:Value data = Greg Schardt
```

13. List the network cards used by this computer

It's in the Software Hive.

14. This same file reports the IP address and MAC address of the computer. What are they?

I didn't find the IP address and MAC Address in the same file.

15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?

I didn't find the MAC address. But according to the answer of Q13, it should be Xircom.

16. Find 6 installed programs that may be used for hacking.

WinPCap, Whois, Network Stumbler, Look@LAN, Anonymizer, 123WASP

Use Autopsy to check the Program Files directory.

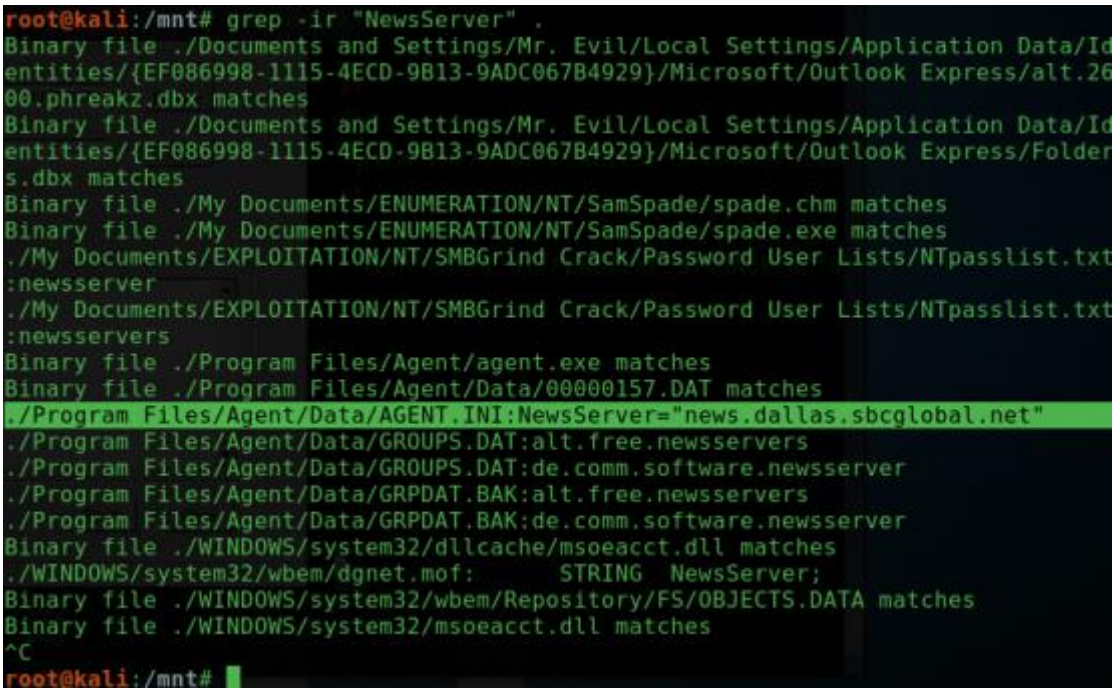
17. What is the SMTP email address for Mr. Evil?

whoknowsme@sbcglobal.net

Use RegRipper to rip the ntuser.dat in Document and Settings directory.

18. What are the NNTP (news server) settings for Mr. Evil?

news.dallas.sbcglobal.net.



19. What two installed programs show this information?

Outlook and Agent. Use grep command to search this server address in the mount point. According to the directory name of the search result, we can get these two programs.

20. List 5 newsgroups that Mr. Evil has subscribed to?

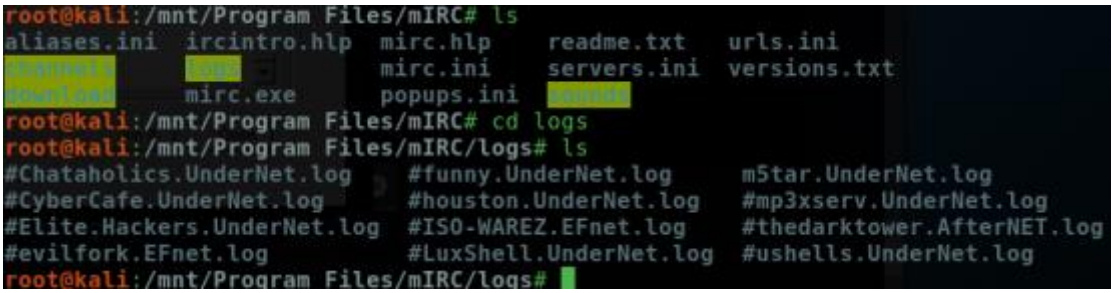
Can't find it.

21. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?

The mIRC can be found in "Program Files" directory, and there are some .ini files in this directory. First, I tried to find some clues in readme.txt. However, there is nothing helpful. Then I examed the mirc.ini, which seems to be the main configuration file. And the user information can be found here.

22. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.

It is obviously that the log files are in “logs” directory. We can find several logs here.



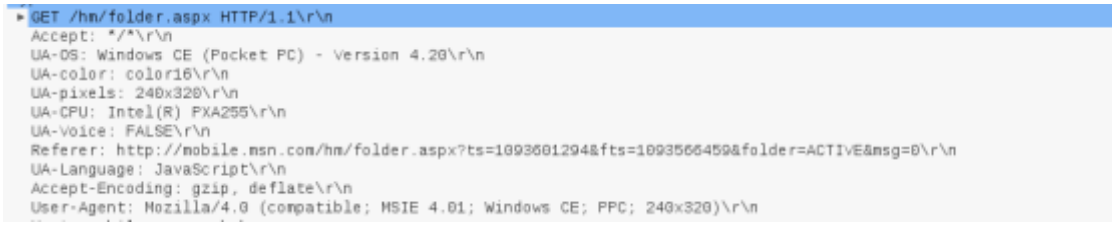
23. Ethereal, a popular “sniffing” program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the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

In Mr. Evil’s “My Documents” directory, there are only two default directories. But I find that in its parent directory, I find a file called interception. I use file command to check this file. It is a tcpdump file.

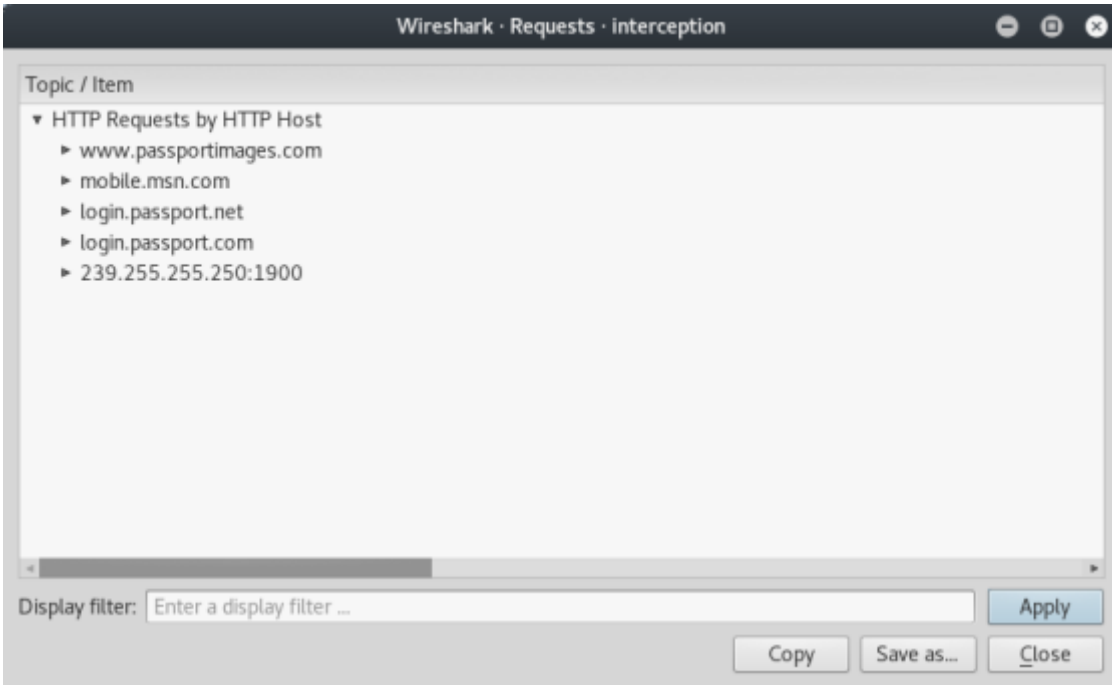
24. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet surfing recorded) using?

The victim is using Windows CE v4.20.

Open the file with Wireshark. Select one of the HTTP packets. The information can be found in the HTTP headers.

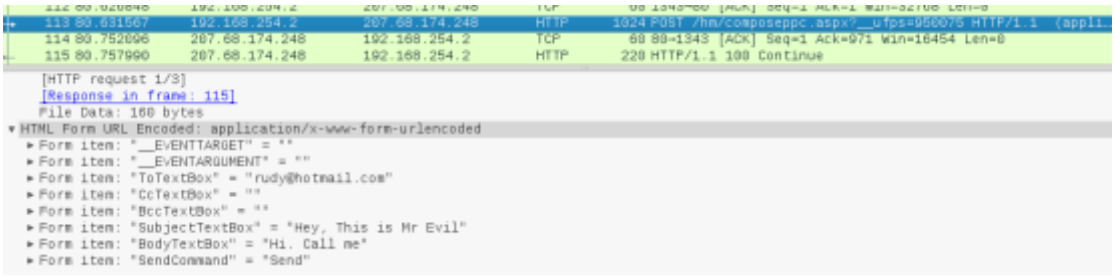


25. What websites was the victim accessing?



Wireshark -> Statistics -> HTTP -> Requests

26. Search for the main users web based email address. What is it?



I found a http packet like this. And try to trace the tcp stream. But didn't find out the Sender's address.

27. Yahoo mail, a popular web based email service, saves copies of the email under what file name?

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

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

```
root@kali:/mnt# ls
AUTOEXEC.BAT  Documents and Settings  ntdetect.com  System Volume Information
boot.ini      FRUNLOG.TXT             ntldr         Temp
BOOTLOG.PRV   hiberfil.sys            pagefile.sys  VIDEOROM.BIN
BOOTLOG.TXT   IO.SYS                  Program Files WIN98
BOOTSECT.DOS  MSDOS.---               RECYCLER      WINDOWS
COMMAND.COM   MSDOS.SYS               SETUPLOG.TXT
CONFIG.SYS    My Documents            SUHDLOG.DAT
DETLOG.TXT    NETLOG.TXT              SYSTEM.1ST
root@kali:/mnt# cd RECYCLER/
root@kali:/mnt/RECYCLER# ls
S-1-5-21-2000478354-688789844-1708537768-1003
root@kali:/mnt/RECYCLER# file S-1-5-21-2000478354-688789844-1708537768-1003/
S-1-5-21-2000478354-688789844-1708537768-1003/: directory
root@kali:/mnt/RECYCLER# cd S-1-5-21-2000478354-688789844-1708537768-1003/
root@kali:/mnt/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003# ls
Dc1.exe  Dc2.exe  Dc3.exe  Dc4.exe  desktop.ini  INFO2
root@kali:/mnt/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003#
```

29. Are these files really deleted?

No. Still in the file system.

30. How many files are actually reported to be deleted by the file system?

Four. Check the INFO2 in the directory.

```
root@kali:/mnt/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003# strings
INFO2
C:\Documents and Settings\Mr. Evil\Desktop\lalsetup250.exe
C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
C:\Documents and Settings\Mr. Evil\Desktop\WinPcap_3_01_a.exe
C:\Documents and Settings\Mr. Evil\Desktop\ethereal-setup-0.10.6.exe
```

31. Perform a Anti-Virus check. Are there any viruses on the computer?

Yes. There are 22 infected files.

Use clamav to scan the /mnt:

clamscan -r /mnt

```
----------- SCAN SUMMARY -----------
Known viruses: 4858042
Engine version: 0.99.2
Scanned directories: 766
Scanned files: 11234
Infected files: 22
Total errors: 71
Data scanned: 1469.89 MB
Data read: 1768.03 MB (ratio 0.83:1)
Time: 293.478 sec (4 m 53 s)
```