

# Digital Forensic Analysis of a Suspected Hacker's Notebook: The Case of Greg Schardt, Alias 'Mr. Evi'

Leen Sharab - Reema Abdallah - Sarah Alshumayri

May 1, 2024

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Background . . . . .	1
1.2	Objectives . . . . .	2
1.2.1	Tasks . . . . .	2
1.2.2	Hypotheses . . . . .	31

### Abstract

As a group of digital forensics students, we were assigned to investigate a Dell CPi notebook suspected of being used for hacking, to determine if it was associated with the alleged hacker, Greg Schardt, also known as "Mr. Evil." Equipped with academic knowledge and training in cybercrime investigation techniques, our group embarked on this complex forensic task. The project began with the examination of the notebook, which included a wireless interception setup. Using a comprehensive array of forensic tools, we conducted a thorough analysis of the device's hard drive, system files, and network configurations. Our findings revealed the presence of multiple hacking tools, evidence of intercepted internet traffic, and personal data such as credit card numbers and usernames. These artifacts conclusively linked Greg Schardt to the device and directly implicated him in various illegal activities including identity theft and fraud. The structured approach adopted by our team, combining both automated and manual forensic methods, ensured a detailed and reliable investigation, leading us to conclude with high confidence that Greg Schardt was indeed utilizing this notebook for hacking purposes.

## 1 Introduction

### 1.1 Background

The proliferation of wireless technology has dramatically transformed the computing and internet access landscape. However, this technological advancement

also presents significant security challenges, notably in the form of unauthorized access and data interception. Hacking through wireless networks has become a common attack vector, posing threats to personal and organizational security [1].

The present case involves the examination of a Dell CPi notebook, equipped with a wireless PCMCIA card and an external homemade 802.11b antenna, suspected to have been used in hacking activities. The device was found abandoned and is linked to Greg Schardt, alias "Mr. Evil," who is suspected of using this equipment to intercept wireless communications and engage in identity theft activities [2].

Forensic investigations of digital devices require a robust understanding of both the hardware involved and the software used by potential criminals. Digital forensics tools enable investigators to recover data that users have attempted to delete, hide, or encrypt. These tools are crucial in uncovering the truth behind the digital facades created by malicious entities [3].

The focus of this investigation was to determine if the notebook was used for hacking activities, specifically to intercept internet traffic, and to gather sensitive information such as credit card numbers, usernames, and passwords. Our investigation methods included the use of specialized software to analyze the hard drive, review system logs, and retrieve hidden or deleted data [1].

## 1.2 Objectives

This section specifies what you are being asked to do, including your hypothesis.

### 1.2.1 Tasks

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

The hash is an MD5, its value is AEE4FCD9301C03B3B054623CA261959A. This is a unique identifier from an MD5 algorithm calculation applied to the file content. It allows a unique identification of the source file

```
(kali㉿kali)-[~]
$ mkdir hacking_case
```

Figure 1

```
(kali㉿kali)-[~]
$ cd hacking_case
```

Figure 2

```

└─(kali㉿kali)-[~/hacking_case]
└─$ wget -q https://www.cfreds.nist.gov/images/hacking-dd/SCHARDT.001

└─(kali㉿kali)-[~/hacking_case]
└─$ wget -q https://www.cfreds.nist.gov/images/hacking-dd/SCHARDT.002

└─(kali㉿kali)-[~/hacking_case]
└─$ wget -q https://www.cfreds.nist.gov/images/hacking-dd/SCHARDT.003

└─(kali㉿kali)-[~/hacking_case]
└─$ wget -q https://www.cfreds.nist.gov/images/hacking-dd/SCHARDT.004

└─(kali㉿kali)-[~/hacking_case]
└─$ wget -q https://www.cfreds.nist.gov/images/hacking-dd/SCHARDT.005

└─(kali㉿kali)-[~/hacking_case]
└─$ wget -q https://www.cfreds.nist.gov/images/hacking-dd/SCHARDT.006

└─(kali㉿kali)-[~/hacking_case]
└─$ wget -q https://www.cfreds.nist.gov/images/hacking-dd/SCHARDT.007

```

Figure 3: Disk Image Installation and Combination

- **What operating system was used on the computer ?**

The operating system used in the computer was **Microsoft Windows**. Indicated by the NTFS and exFAT file systems which belong to Windows.

```

└─(kali㉿kali)-[~/hacking_case]
└─$ mmfs SCHARDT.dd

DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start          End          Length        Description
000: Meta    000000000000  000000000000  000000000001 Primary Table (#0)
001: _____  000000000000  00000000062    00000000063 Unallocated
002: 000:000  00000000063   0009510479   0009510417 NTFS / exFAT (0x07)
003: _____  0009510480   0009514259   0000003780 Unallocated

```

Figure 4: Displaying the Partition information of SCHARDT.dd

```

└─(kali㉿kali)-[~/hacking_case]
$ fls -rF -o 63 SCHARDT.dd | grep -i software
File System
r/r 9895-128-4: Program Files/Anonymizer/Toolbar/Images/software-A.bmp
r/r 9896-128-4: Program Files/Anonymizer/Toolbar/Images/software-D.bmp
r/r 9897-128-4: Program Files/Anonymizer/Toolbar/Images/software-M.bmp
r/r 6375-128-5: WINDOWS/PCHEALTH/HELPCTR/System/sysinfo/sysSoftwareInfo.htm
r/r 6376-128-5: WINDOWS/PCHEALTH/HELPCTR/System/sysinfo/sysSoftwareInfo.js
r/r 9742-128-4: WINDOWS/repair/software
r/r 336-128-4: WINDOWS/system32/config/software
r/r 466-128-5: WINDOWS/system32/config/software.LOG
r/r 471-128-3: WINDOWS/system32/config/software.sav

└─(kali㉿kali)-[~/hacking_case]
$ icat -o 63 SCHARDT.dd 336 > software

└─(kali㉿kali)-[~/hacking_case]
$ ls software -l
-rw-r--r-- 1 kali kali 8650752 Apr 24 07:20 software

```

Figure 5: The First command is to list files and directory entries within a disk image file, and then filters the output to show lines containing the word "software". The second command is to extracts the contents of a file with 336 inode number from the disk image and redirects it to a file named "software". The third command is to list the details of the extracted file "software", showing its permissions, size, and other information.

- When was the OS install date?
- The install date was on **2004-08-19 22:48:27Z**.

```

└─(kali㉿kali)-[/usr/lib/regripper]
$ /usr/lib/regripper/rip.pl -l | grep -i winver
111. winver v.20200525 [Software]
+index/runonce/100 grys : Permission denied

```

Figure 6: Extracts and analyzes data from the Windows registry, specifically using a plugin that retrieves the version and installation information of the Windows operating system.

```
(kali㉿kali)-[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r software -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName           Microsoft Windows XP
BuildLab              2600.xpclient.010817-1148
RegisteredOrganization N/A
RegisteredOwner        Greg Schardt
InstallDate           2004-08-19 22:48:27Z
```

Figure 7: Displays information about the Windows version, build number, owner, and etc.

- **What is the timezone settings ?**

The time zone setting according to the image is **"Central Standard Time"** with a standard bias of **360 minutes (6 hours)** and an active time bias of **300 minutes (5 hours)**.

```

[(kali㉿kali)-[~/hacking_case]
$ fls -rF -o 63 SCHARDT.dd | egrep -i config/system$

r/r 334-128-4:  WINDOWS/system32/config/system
/usr/lib/regripper/rip.pl

[(kali㉿kali)-[~/hacking_case]
$ icat -o 63 SCHARDT.dd 334 > system
]

[(kali㉿kali)-[~/hacking_case]
$ rip.pl -r system -p timezone
rip.pl: command not found

[(kali㉿kali)-[~/hacking_case]
$ /usr/lib/regripper/rip.pl -r system -p timezone

Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2004-08-19 17:20:02Z
    DaylightName → Central Daylight Time
    StandardName → Central Standard Time
    Bias           → 360 (6 hours)
    ActiveTimeBias → 300 (5 hours)

```

Figure 8: Begins by filtering the file named "config/system", then extracting its contents to a file named "system", and then extracting info about the system's time zone settings from the registry data.

- **Who is the registered owner ?**  
The registered owner of the Windows XP system is **Greg Schardt**.
- **What is the computer account name ?**  
The computer account name is **N-1490DN62XK4LQ**.

```
(kali㉿kali)-[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r software -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName           Microsoft Windows XP
BuildLab              2600.xpclient.010817-1148
RegisteredOrganization N/A
RegisteredOwner        Greg Schardt
InstallDate           2004-08-19 22:48:27Z
```

Figure 9: Extracts Windows version and build information from the "software" file.

```
(kali㉿kali)-[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r system -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName      = N-1A9ODN6ZXK4LQ
TCP/IP Hostname  = n-1a9odn6zxk4lq
```

Figure 10: Extracts the computer name and hostname values from the system hive.

- **What is the primary domain (workgroup) name?**  
The workgroup name is "**EVIL**".

```

└─(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | egrep -i config/sysevent
r/r 3678-128-1: WINDOWS/system32/config/SysEvent.Evt

└─(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 3678 > SysEvent.Evt

└─(kali㉿kali)-[~/hacking_case]
└─$ ls -l SysEvent.Evt
-rw-r--r-- 1 kali kali 65536 Apr 24 09:34 SysEvent.Evt

```

Figure 11: Searches for workgroup in the system event log and extracts the event log.

```

└─$ git clone https://github.com/keydet89/Tools.git
Cloning into 'Tools' ...
remote: Enumerating objects: 193, done.
remote: Counting objects: 100% (27/27), done.
remote: Compressing objects: 100% (20/20), done.
remote: Total 193 (delta 13), reused 16 (delta 7), pack-reused 166
Receiving objects: 100% (193/193), 8.37 MiB | 3.26 MiB/s, done.
Resolving deltas: 100% (108/108), done.

└─(kali㉿kali)-[~/hacking_case]
└─$ perl Tools/source/evtparse.pl

evtparse [option]
Parse Event log (Win2000, XP, 2003)

-e file.....Event log (full path)
-d dir.....Directory where .evt files are located
-s .....Output in sequential format (record number and time
        generated values ONLY - use to see if system time may
        have been tampered with)
-t .....TLN output (default .csv)
-h .....Help (print this information)

Ex: C:\>evtparse -e secevent.evt -t > timeline.txt
    C:\>evtparse -e sysevent.evt -s

**All times printed as GMT/UTC

copyright 2012 Quantum Analytics Research, LLC

```

Figure 12: Uses a tool to parse the event log.

- When was the last recorded computer shutdown date/time ?  
The last Recorded computer was **2004-08-27 15:46:33Z**.

```

└─(kali㉿kali)-[~/hacking_case]
└─$ perl Tools/source/evtparse.pl -e SysEvent.Evt -t > SysEvent.txt

└─(kali㉿kali)-[~/hacking_case]
└─$ ls -l SysEvent.*
-rw-r--r-- 1 kali kali 65536 Apr 24 09:34 SysEvent.Evt
-rw-r--r-- 1 kali kali 14183 Apr 24 09:41 SysEvent.txt

```

Figure 13: Parsing the event log.

```

└─(kali㉿kali)-[~/hacking_case]mission denied
└─$ cat SysEvent.txt
1092934732|EVT|MACHINENAME|N/A|Serial/2;Info;\Device\Serial0,\Device\Serial0
1092934755|EVT|MACHINENAME|N/A|EventLog/6009;Info;5.01.,2600,,Uniprocessor F
ree
1092934755|EVT|MACHINENAME|N/A|EventLog/6005;Info;
1092935246|EVT|MACHINENAME|N/A|Serial/2;Info;\Device\Serial1,\Device\Serial1
1092954012|EVT|N-1A90DN6ZKX4LQ|N/A|EventLog/6011;Info;MACHINENAME,N-1A90DN6Z
XK4LQ
1092954111|EVT|N-1A90DN6ZKX4LQ|N/A|Dhcp/1007;Warn;0010A4933E09,169.254.242.
13
1092954197|EVT|N-1A90DN6ZKX4LQ|N/A|Workstation/3260;Info;workgroup,EVIL
1092955778|EVT|N-1A90DN6ZKX4LQ|N/A|Setup/60054;Info;2600
1092955914|EVT|N-1A90DN6ZKX4LQ|N/A|EventLog/6009;Info;5.01.,2600,,Uniprocess
or Free

```

Figure 14: Displays domain info, PC name, etc.

```

└─(kali㉿kali)-[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r system -p shutdown

Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2004-08-27 15:46:33Z
ShutdownTime : 2004-08-27 15:46:33Z

```

Figure 15: Extracts information about system shutdown events.

- **How many accounts are recorded (total number) ?**

A total of **five** accounts are recorded. The accounts listed are: Administrator, Guest, HelpAssistant, SUPPORT 388945a0 and Mr. Evil.

```
(kali㉿kali)-[~/hacking_case]
$ /usr/lib/regrripper/rip.pl -r SAM -p smparse
[+] Reading file /tmp/WindowsSAM.sam...
Launching smparse v.20220921
smparse v.20220921
(SAM) Parse SAM file for user & group mbrshp info

User Information
-----
Username      : Administrator [500]
SID          : S-1-5-21-2000478354-688789844-1708537768-500
Full Name    :
User Comment  : Built-in account for administering the computer/domain
Account Type  : Default Admin User
Account Created: Thu Aug 19 16:59:24 2004 Z
Name         :
Last Login Date: Never
Pwd Reset Date: Thu Aug 19 17:17:29 2004 Z
Pwd Fail Date: Never
Login Count   : 0
    → Normal user account
    → Password does not expire

Username      : Guest [501]
SID          : S-1-5-21-2000478354-688789844-1708537768-501
Full Name    :
User Comment  : Built-in account for guest access to the computer/domain
Account Type  : Default Guest Acct
Account Created: Thu Aug 19 16:59:24 2004 Z
```

Figure 16: All Windows user account names, SIDs (Security Identifiers), login counts, creation dates, last password change dates, groups, and much more can be found in the Windows Registry SAM.

- **What is the account name of the user who mostly uses the computer ?**  
The account name of the user who most likely uses the computer is "Mr. Evil".
- **Who was the last user to log on to the computer ?**  
The last user to log on to the computer was "Mr. Evil", as indicated by the last write timestamp of 2004-08-27 15:46:23Z for his user profile directory.

```

Pwd Reset Date : Never
Pwd Fail Date : Never
Login Count : 0
    → Normal user account
    → Password not required
    → Password does not expire
    → User does not have "script" permission denied

Auston@Auston-OptiPlex-5090 MINGW32 [~] ~ % net user /domain

Username : HelpAssistant [1000]
SID : S-1-5-21-2000478354-688789844-1708537768-1000
Full Name : Remote Desktop Help Assistant Account
User Comment : Account for Providing Remote Assistance
Account Type : Custom Limited Acct
Account Created : Thu Aug 19 22:28:24 2004 Z
Name :
Last Login Date : Never
Pwd Reset Date : Thu Aug 19 22:28:24 2004 Z
Pwd Fail Date : Never
Login Count : 0
    → Normal user account
    → Password does not expire

Username : SUPPORT_388945a0 [1002]
SID : S-1-5-21-2000478354-688789844-1708537768-1002
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
Name :
Last Login Date : Never
Pwd Reset Date : Thu Aug 19 22:35:19 2004 Z

Username : Mr. Evil [1003]
SID : S-1-5-21-2000478354-688789844-1708537768-1003
Full Name :
User Comment :
Account Type : Default Admin User
Account Created : Thu Aug 19 23:03:54 2004 Z
Name :
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
    → Normal user account
    → Password does not expire

_____
Group Membership Information
_____

Group Name : Backup Operators [0]
LastWrite : Thu Aug 19 16:59:24 2004 Z
Group Comment : Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Users : None

Group Name : Administrators [2]
LastWrite : Thu Aug 19 23:03:54 2004 Z
Group Comment : Administrators have complete and unrestricted access to the computer/domain

```

Figure 17

```
Username      : Mr. Evil [1003]
SID          : S-1-5-21-2000478354-688789844-1708537768-1003
Full Name    :
User Comment  :
Account Type   : Default Admin User
Account Created : Thu Aug 19 23:03:54 2004 Z
Name          :
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
    → Normal user account
    → Password does not expire
```

Figure 18: Account name

```
[kali㉿kali] -[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r software -p profilelist
Launching profilelist v.20200518
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : 2004-08-19 22:48:26Z

Path      : %SystemDrive%\Documents and Settings\LocalService
SID       : S-1-5-19
LastWrite : 2004-08-27 15:08:21Z

Path      : %SystemDrive%\Documents and Settings\NetworkService
SID       : S-1-5-20
LastWrite : 2004-08-27 15:08:20Z

Path      : %SystemDrive%\Documents and Settings\Mr. Evil
SID       : S-1-5-21-2000478354-688789844-1708537768-1003
LastWrite : 2004-08-27 15:46:23Z

Domain Accounts
```

Figure 19: Method 1 of finding the last logged-in user by displaying the profile list from the software file.

- Proves that Greg Schardt is Mr. Evil

```

└─(kali㉿kali)-[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r SAM -p sampaarse_tln
Launching sampaarse_tln v.20200826
1092934764|SAM||Administrator|Acct Created (Default Admin User)
1092935849|SAM||Administrator|Password Reset Date
1092934764|SAM||Guest|Acct Created (Default Guest Acct)
1092954504|SAM||HelpAssistant|Acct Created (Custom Limited Acct)
1092954504|SAM||HelpAssistant|Password Reset Date
1092954919|SAM||SUPPORT_388945a0|Acct Created (Custom Limited Acct)
1092954919|SAM||SUPPORT_388945a0|Password Reset Date
1092956634|SAM||Mr. Evil|Acct Created (Default Admin User)
1092956634|SAM||Mr. Evil|Password Reset Date
1093619303|SAM||Mr. Evil|Last Login (15)

└─(kali㉿kali)-[~/hacking_case]
└─$ date -d @1093619303

Fri Aug 27 11:08:23 AM EDT 2004

```

Figure 20: Method 2 of finding the last logged-in user.

```

└─(kali㉿kali)-[~/hacking_case]
└─$ sudo mount /dev/loop0p1 /mnt/loop
Error opening '/dev/loop0p1' read-write
Could not mount read-write, trying read-only

└─(kali㉿kali)-[~/hacking_case]
└─$ ls /mnt/loop
AUTOEXEC.BAT          hiberfil.sys      RECYCLER
boot.ini               IO.SYS           SETUPLOG.TXT
BOOTLOG.PRV            MSDOS.---       SUHDLOG.DAT
BOOTLOG.TXT            MSDOS.SYS        SYSTEM.1ST
BOOTSECT.DOS           'My Documents'   'System Volume Information'
COMMAND.COM            NETLOG.TXT       Temp
CONFIG.SYS              ntdetect.com    VIDEOROM.BIN
DETLLOG.TXT             ntldr            WIN98
'Documents and Settings' pagefile.sys  WINDOWS
FRUNLOG.TXT             'Program Files'

└─(kali㉿kali)-[~/hacking_case]
└─$ grep -rn '/mnt/loop/' -e 'Greg Schardt'
/mnt/loop/Program Files/Look@LAN/irunin.ini:29:%REGOWNER%=Greg Schardt
/mnt/loop/Program Files/Look@LAN/irunin.ini:396:%USERNAME%=Greg Schardt
/mnt/loop/WINDOWS/Look@LAN Setup Log.txt:42:Value data = Greg Schardt

```

Figure 21: Finds all instances where the name "Greg Schardt" appears within the files of the mounted directory.

```
(kali㉿kali)-[~/hacking_case]
└─$ cat "/mnt/loop/WINDOWS/Look@LAN Setup Log.txt" | grep -i 'evil'
C:\Documents and Settings\Mr. Evil\Desktop\Look@LAN.lnk
C:\Documents and Settings\Mr. Evil\Desktop\Look@Host.lnk
```

Figure 22: Lines containing the string "evil" were found, which appears to be a part of a file path indicating that a user named "Mr. Evil" has a directory on the desktop with shortcuts related to "Look@LAN", which is likely a network monitoring tool.

```
(kali㉿kali)-[~/hacking_case]
└─$ cat "/mnt/loop/Program Files/Look@LAN/irunin.ini" | grep -i 'evil'
%LANUSER%="Mr. Evil"
%DESKTOP%=C:\Documents and Settings\Mr. Evil\Desktop
%STARTMENU%=C:\Documents and Settings\Mr. Evil\Start Menu
%STARTMENUPROGRAMS%=C:\Documents and Settings\Mr. Evil\Start Menu\Programs
%STARTUP%=C:\Documents and Settings\Mr. Evil\Start Menu\Programs\Startup
%MYDOCUMENTSDIR=C:\Documents and Settings\Mr. Evil\My Documents
%SRCFILE%=C:\Documents and Settings\Mr. Evil\Desktop\lalsetup250.exe
%SRCDIR%=C:\Documents and Settings\Mr. Evil\Desktop
```

Figure 23: Shows that "Mr. Evil" has various user-specific paths set up on the system, likely indicating that this account was actively customizing or using the Look@LAN program.

```
(kali㉿kali)-[~/hacking_case]
└─$ strings '/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/index.dat' | grep -i greg
Visited: Mr. Evil@http://edit.yahoo.com/config/id_check?.fn=Greg&ln=Schardt
&.id=mrevil20006.u=b568cfp0ic6g0

(kali㉿kali)-[~/hacking_case]
└─$ strings '/mnt/Loop/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/MSHist012004081620040823/index.dat' | grep -i 'greg'
:2004081620040823: Mr. Evil@http://edit.yahoo.com/config/id_check ?.fn=Greg&
ln=Schardt&.id=mrevil20006.u=b568cfp0ic6g0
```

Figure 24: Indicates that the user searched for or visited pages related to the name "Greg" or that "Greg" was part of some credential or identifier used during the sessions saved in the history files

- List the network cards used by this computer
- This same file reports the computer's IP address and MAC address. What are they ?  
IP Address: 192.168.1.111 - MAC Address: 0010a4933e09.

```
(kali㉿kali)-[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r software -p networkcards
Launching networkcards v.20200518
networkcards v.20200518
(Software) Get NetworkCards Info

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Description Key LastWrite time
Compaq WL110 Wireless LAN PC Card 2004-08-27 15:31:44Z
Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface) 2004-08-19 17:07:19Z
```

Figure 25: Identifying the Computer's Network Cards

```
(kali㉿kali)-[~/hacking_case]
└─$ egrep -rIl '\b[0-9]{1,3}\.\b[0-9]{1,3}\.\b[0-9]{1,3}\.\b[0-9]{1,3}\b' '/mnt/loop'
oop/ > ip.txt

(kali㉿kali)-[~/hacking_case]
└─$ egrep -rIl '[^-/]\b[0-9a-fA-F]{12}\b' '/mnt/loop' > mac.txt
comm -12 ip.txt mac.txt

comm: file 1 is not in sorted order
/mnt/loop/Program Files/Look@LAN/irunin.ini
/mnt/loop/Program Files/mIRC/channels/channels.txt
comm: file 2 is not in sorted order
comm: input is not in sorted order
```

Figure 26: Searches recursively for IP and MAC address patterns within the /mnt/loop/ directory.

```
(kali㉿kali)-[~/hacking_case]
└─$ grep -rP '\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b' '/mnt/loop/Program Files/Look@LAN/irunin.ini'
%LANIP%=192.168.1.111

(kali㉿kali)-[~/hacking_case]
└─$ egrep -r '[^-/]\b[0-9a-fA-F]{12}\b' '/mnt/loop/Program Files/Look@LAN/irunin.ini'
%LANNIC%=0010a4933e09
```

Figure 27: Searches for Ip and MAC address patterns within the same irunin.ini file and prints the matched lines.

- Which NIC card was used during the installation and set-up for LOOK@LAN?  
The NIC card is **XIRCOM**.
- Find 6 installed programs that may be used for hacking  
Ethereal 0.10.6 v.0.10.6, WinPcap 3.01 alpha, Network Stumbler 0.4.0

(remove only), 123 Write All Stored Passwords, CuteFTP, Cain Abel v2.5 beta45, and Anonymizer Bar 2.0 (remove only).

```
(kali㉿kali)-[~/hacking_case]
└─$ /usr/lib/regripper/rip.pl -r software -p uninstall
Launching uninstall v.20200525
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER
.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2004-08-27 15:29:19Z
    Ethereal 0.10.6 v.0.10.6

2004-08-27 15:15:19Z
    WinPcap 3.01 alpha

2004-08-27 15:12:15Z
    Network Stumbler 0.4.0 (remove only)

2004-08-25 15:50:17
```

Figure 28: Displays the installed Programs in the software file.

```
2004-08-20 15:09:02Z
    CuteFTP

2004-08-20 15:08:19Z
    Forté Agent

2004-08-20 15:07:25Z
    Faber Toys v.2.4 Build 216

2004-08-20 15:05:58Z
    Cain & Abel v2.5 beta45

2004-08-20 15:05:09Z
    Anonymizer Bar 2.0 (remove only)
```

Figure 29: Displays the installed Programs in the software file.

- **What is the SMTP email address for Mr. Evil ?**  
Email Address: `whoknowsineedhelp@sbeglobal.net`

```
(kali㉿kali)-[~/hacking_case]
$ fls -rF -o 63 SCHARDT.dd | grep -i 'ntuser.dat'

r/r 7324-128-4: Documents and Settings/Default User/NTUSER.DAT
r/r 391-128-4: Documents and Settings/LocalService/NTUSER.DAT
r/r 418-128-4: Documents and Settings/LocalService/ntuser.dat.LOG
r/r 345-128-4: Documents and Settings/Mr. Evil/NTUSER.DAT
r/r 9798-128-4: Documents and Settings/Mr. Evil/ntuser.dat.LOG
r/r 350-128-4: Documents and Settings/NetworkService/NTUSER.DAT
r/r 377-128-4: Documents and Settings/NetworkService/ntuser.dat.LOG
r/r 9746-128-4: WINDOWS/repair/ntuser.dat

(kali㉿kali)-[~/hacking_case]
$ icat -o 63 SCHARDT.dd 345 > NTUSER_Evil.DAT
```

Figure 30: To filter and find instances of NTUSER.DAT files, which are Windows Registry hive files associated with individual user accounts.

```
(kali㉿kali)-[~/hacking_case]
$ strings NTUSER_Evil.DAT | grep -iP '\b^[\w\.-]+@[\\w-]+\.\w{2,4}\b'

whoknowsme@sbcglobal.net
xeashdoclc.dll,-866
Look@LAN.lnk
Look@LAN.lnk
Look@LAN.lnk
```

Figure 31: To filter out email addresses with a regex pattern that matches a typical email address format.

- What are the NNTP (news server) settings for Mr. Evil ?  
Forte Agent, OutlookExpress, AddressBook, and ICW.

```
2004-08-20 15:08:19Z
Forté Agent
```

```
2004-08-19 22:31:51Z
AddressBook
ICW
OutlookExpress
```

```
(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i 'forte'

(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i 'agent' | head

r/r 10064-128-1:      Documents and Settings/Mr. Evil/Desktop/Tools/Agent.
lnk
r/r 10065-128-4:      Documents and Settings/Mr. Evil/Start Menu/Programs/
Agent Newsreader/Agent Help.lnk
r/r 10066-128-1:      Documents and Settings/Mr. Evil/Start Menu/Programs/
Agent Newsreader/Readme.lnk
r/r 10210-128-3:      My Documents/ARCHIVE/Arj/AGENTS.TXT
r/r 10055-128-3:      Program Files/Agent/8859-1.cod
r/r 10057-128-3:      Program Files/Agent/8859-15.cod
r/r 10056-128-3:      Program Files/Agent/8859-1w.cod
r/r 10013-128-3:      Program Files/Agent/agent.cnt
r/r 10009-128-3:      Program Files/Agent/agent.exe
r/r 10012-128-3:      Program Files/Agent/agent.hlp
```

Figure 32: To find evidence of installation or use of Forté Agent on the system.

```
r/r 11797-128-3:      Program Files/Agent/Data/000004B1.IDX
r/r 11798-128-3:      Program Files/Agent/Data/00000D28.DAT
r/r 11799-128-3:      Program Files/Agent/Data/00000D28.IDX
r/r 11415-128-3:      Program Files/Agent/Data/0000168F.DAT
r/r 11730-128-3:      Program Files/Agent/Data/0000168F.IDX
r/r 11731-128-3:      Program Files/Agent/Data/0000169B.DAT
r/r 11732-128-3:      Program Files/Agent/Data/0000169B.IDX
r/r 11406-128-4:      Program Files/Agent/Data/AGENT.INI
r/r 11416-128-1:      Program Files/Agent/Data/errorlog.txt
r/r 11420-128-1:      Program Files/Agent/Data/FILTERS.DAT
r/r 11423-128-1:      Program Files/Agent/Data/FILTERS.IDX
r/r 11727-128-3:      Program Files/Agent/Data/GROUPS.DAT
r/r 11728-128-3:      Program Files/Agent/Data/GROUPS.IDX
r/r 11417-128-3:      Program Files/Agent/Data/GRPDAT.BAK
r/r 11418-128-3:      Program Files/Agent/Data/GRPIDX.BAK
r/r 11419-128-1:      Program Files/Agent/Data/RANGES.BAK
```

Figure 33: Data/AGENT.INI was found.

```
[(kali㉿kali)-[~/hacking_case]]$ icat -o 63 SCHARDT.dd 11406 | more

;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
SMTPUsePOPLogin=0
SMTPUserName="whoknowsme@sbcglobal.net"
SMTPSavePassword=1
SMTPPPassword="84106D94696F"
IsRegistered=0
IsRegistered19=0
IsLicensed=3
Key=""
EnableSupportMenu=0
```

Figure 34: News server Configuration.

```
[Servers]
NewsServer="news.dallas.sbcglobal.net"
MailServer="smtp.sbcglobal.net"
POPServer=""
NNTPPort=119
SMTPPort=25
POPPort=110
SMTPServerPort=25
```

```
(kali㉿kali)-[~/hacking_case]
$ fls -rF -o 63 SCHARDT.dd | grep -i 'outlook'

r/r 11431-128-3:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/cleanup.log
r/r 11443-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.cardz.dbx
r/r 11444-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.codez.dbx
r/r 11445-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.crackz.dbx
r/r 11442-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.dbx
r/r 11539-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.hackerz.dbx
r/r 11446-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.moderated.dbx
r/r 11536-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.phreakz.dbx
r/r 11523-128-4:      Documents and Settings/Mr. Evil/Local Settings/Application
```

Figure 35: Lists all the files that are associated with OutlookExpress.

```
(kali㉿kali)-[~/hacking_case]
└─$ strings '/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.cardz.dbx' | grep -i 'news.dallas.sbcglobal.net' | head
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
```

Figure 36: Finds the new server:news.dallas.sbcglobal.net in the .dbx

- **What two installed programs show this information ?**  
Forte Agent and OutlookExpress.

- **List 5 newsgroups that Mr. Evil has subscribed to ?**

Based on the file names, here are five newsgroups that Mr. Evil has subscribed to:

1. alt.binaries.hackers
2. alt.2600
3. alt.2600.codez
4. alt.2600.phreakz
5. alt.2600.programz

```
└─(kali㉿kali)-[~/hacking_case]
$ ls '/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express'
alt.2600.cardz.dbx
alt.2600.codez.dbx
alt.2600.crackz.dbx
alt.2600.dbx
alt.2600.hackerz.dbx
alt.2600.moderated.dbx
alt.2600.phreakz.dbx
alt.2600.programz.dbx
alt.binaries.hacking.beginner.dbx
alt.binaries.hacking.computers.dbx
alt.binaries.hacking.utilities.dbx
alt.binaries.hacking.websites.dbx
alt.dss.hack.dbx
alt.hacking.dbx
alt.nl.binaries.hack.dbx
alt.stupidity.hackers.malicious.dbx
cleanup.log
'Deleted Items.dbx'
Folders.dbx
free.binaries.hackers.malicious.dbx
free.binaries.hacking.beginner.dbx
free.binaries.hacking.computers.dbx
free.binaries.hacking.talentless.troll-haven.dbx
free.binaries.hacking.talentless.troll_haven.dbx
free.binaries.hacking.utilities.dbx
free.binaries.hacking.websites.dbx
Inbox.dbx
```

Figure 37: Mr. Evil's Newsgroup Subscriptions Exposed

- Investigate an Internet Relay Chat program

```
(kali㉿kali)-[~/hacking_case]
$ fls -rF -o 63 SCHARDT.dd | grep -i 'mirc'

r/r 10087-128-4:      Documents and Settings/All Users/Start Menu/Programs
/mIRC/IRC Intro.lnk
r/r 10086-128-4:      Documents and Settings/All Users/Start Menu/Programs
/mIRC/mIRC Help.lnk
r/r 10088-128-4:      Documents and Settings/All Users/Start Menu/Programs
/mIRC/Readme.txt.lnk
r/r 10089-128-4:      Documents and Settings/All Users/Start Menu/Programs
/mIRC/Versions.txt.lnk
r/r 10085-128-1:      Documents and Settings/Mr. Evil/Desktop/Tools/mIRC.l
nk
r/r 10081-128-1:      Program Files/mIRC/aliases.ini
r/r 11072-128-6:      Program Files/mIRC/channels/channels.txt
r/r 10077-128-3:      Program Files/mIRC/ircintro.hlp
r/r 11315-128-4:      Program Files/mIRC/logs/#Chataholics.UnderNet.log
r/r 11316-128-4:      Program Files/mIRC/logs/#CyberCafe.UnderNet.log
r/r 11276-128-1:      Program Files/mIRC/logs/#Elite.Hackers.UnderNet.log
r/r 11074-128-1:      Program Files/mIRC/logs/#evilfork.EFNet.log
r/r 11401-128-1:      Program Files/mIRC/logs/#funny.UnderNet.log
r/r 11306-128-1:      Program Files/mIRC/logs/#houston.UnderNet.log
r/r 11073-128-1:      Program Files/mIRC/logs/#ISO-WAREZ.EFnet.log
r/r 11272-128-4:      Program Files/mIRC/logs/#LuxShell.UnderNet.log
r/r 11273-128-4:      Program Files/mIRC/logs/#mp3xserv.UnderNet.log
r/r 11327-128-4:      Program Files/mIRC/logs/#thedarktower.AfterNET.log
r/r 11275-128-1:      Program Files/mIRC/logs/#ushells.UnderNet.log
r/r 11317-128-1:      Program Files/mIRC/logs/mStar.UnderNet.log
r/r 10074-128-6:      Program Files/mIRC/mirc.exe
```

Figure 38: Tracing IRC activity: A hacker's chat logs

```
(kali㉿kali)-[~/hacking_case]
$ icat -o 63 SCHARDT.dd 10080 | grep -iE 'user|email|log|ip|server'

n46=#mIRCScripts
n75=#UserGuide,"The official Undernet help channel"
n76=#UserHelp
accept=*.bmp,*.gif,*.jpg,*.log,*.mid,*.mp3,*.png,*.txt,*.wav,*.wma,*.zip
logdir=log\
userid=Mrevil
useip=yes
status=/users
ServerStatus=on
[fileserver]
[dccserver]
user=Mini Me
email=none@of.ya
host=Undernet: US, CA, LosAngeles$ERVER:losangeles.ca.us.undernet.org:6660GR
OUP:Undernet
servers=servers.ini
```

Figure 39: Config clues: IRC user details revealed

- List 3 IRC channels that the user of this computer accessed.

Three IRC channels that the user accessed are:

1. Chataholics.UnderNet
2. CyberCafe.UnderNet
3. Elite.Hackers.UnderNet

```
(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i 'Program Files/mIRC/logs'
Home
r/r 11315-128-4: Program Files/mIRC/logs/#Chataholics.UnderNet.log
r/r 11316-128-4: Program Files/mIRC/logs/#CyberCafe.UnderNet.log
r/r 11276-128-1: Program Files/mIRC/logs/#Elite.Hackers.UnderNet.log
r/r 11074-128-1: Program Files/mIRC/logs/#evilfork.EFNet.log
r/r 11401-128-1: Program Files/mIRC/logs/#funny.UnderNet.log
r/r 11306-128-1: Program Files/mIRC/logs/#houston.UnderNet.log
r/r 11073-128-1: Program Files/mIRC/logs/#ISO-WAREZ.EFnet.log
r/r 11272-128-4: Program Files/mIRC/logs/#LuxShell.UnderNet.log
r/r 11273-128-4: Program Files/mIRC/logs/#mp3xserv.UnderNet.log
r/r 11327-128-4: Program Files/mIRC/logs/#thedarktower.AfterNET.log
r/r 11275-128-1: Program Files/mIRC/logs/#ushells.UnderNet.log
r/r 11317-128-1: Program Files/mIRC/logs/m5tar.UnderNet.log
```

Figure 40: 3 IRC channels that the user accessed

- Investigate Ethereal

```
(kali㉿kali)-[~/hacking_case]
└─$ ls /mnt/loop/Documents\ and\ Settings\Mr.\ Evil
'Application Data'  interception  NTUSER.DAT  Recent
Cookies             'Local Settings' ntuser.dat.LOG SendTo
Desktop             'My Documents'  ntuser.ini   'Start Menu'
Favorites           NetHood        PrintHood  Templates

(kali㉿kali)-[~/hacking_case]
└─$ file /mnt/loop/Documents\ and\ Settings\Mr.\ Evil/interception
/mnt/loop/Documents and Settings\Mr. Evil/interception: pcap capture file, m
icrosecond ts (little-endian) - version 2.4 (Ethernet, capture length 65535)
```

Figure 41: Investigate Ethereal

- **What type of device was the victim (person who had his internet surfing recorded) using?**

The victim appears to have been using a Windows CE operating system device. "PPC" suggests that it was a Pocket PC, a handheld, touchscreen personal digital assistant that ran Windows CE.

```
(kali㉿kali)-[~/hacking_case]
└─$ tshark -r /mnt/loop/Documents\ and\ Settings\Mr.\ Evil\interception -Y http.request -T fields -e http.user_agent -e http.host

Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320) mobile.msn.com
```

Figure 42: The type of device the victim was using

- **What websites was the victim accessing?**

The websites that the victim accessed are:

1. mobile.msn.com
2. www.passportimages.com
3. login.passport.net
4. login.passport.com

- Search for the main user's web-based email address. What is it?  
It's mrevilrulez@yahoo.com

```
(kali㉿kali)-[~/hacking_case]
└─$ grep -EiorhI '([[:alnum:]]_.-]+@[[:alnum:]]_.-]+?\.[[:alpha:]].{2,6})' '/mnt/loop/Documents and Settings/Mr. Evil/'

mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mailbot@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
nightwolf@confine.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
seabachashaw.ca
J06.42522@pd7tw2no ...
NOSPAM-fredawarddriving.com
jim@mcmahon.cc
jim@mcmahon.cc
hacked@2600.com
webmaster@2600.com
you@your-name.com
LmTomarijuana.com
chris@splitinfinity.com
NOSPAM-fredawarddriving.com
```

Figure 43: Sifting through data: Email patterns in focus

```
(kali㉿kali)-[~/hacking_case]
└─$ grep -EiorhI 'b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,6}\b' '/mnt/loop/Documents and Settings/Mr. Evil/'

mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mailbot@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
nightwolf@confine.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
seabachashaw.ca
NOSPAM-fredawarddriving.com
jim@mcmahon.cc
jim@mcmahon.cc
hacked@2600.com
webmaster@2600.com
you@your-name.com
LmTomarijuana.com
chris@splitinfinity.com
NOSPAM-fredawarddriving.com
123@123.com
info@mosnews.com
info@mosnews.com
Rating@Mail.ru
```

Figure 44: Email extraction: Mining addresses from Mr. Evil's files

```
(kali㉿kali)-[~/hacking_case]
└─$ grep -EiorhI '([[:alnum:]]_[-]+@[[:alnum:]]_[-]+?\.[[:alpha:]].{2,6})' '/mnt/loop/Documents and Settings/Mr. Evil/' | sort | uniq -c | sort -nr

      12 mrevilrulez@yahoo.com
      6 info@mosnews.com
      4 jim@mcmahon.cc
      3 webmaster@2600.com
      3 --Rating@mail.ru
      3 PASSCODE@HOTMAIL.COM
      3 PASSADMINBOT@HOTMAIL.COM
      3 NOSPAM-fred@wardriving.com
      3 HERE@HOTMAIL.COM
      2 suckme@oyea.lick
      2 slim532@hotmail.com
      2 248e504e.0408150655.a30aac9@posting.google.com...
      1 you@your-name.com
      1 tmt3i0tnq18gm819ecv27r73vm6hnoddcm@4ax.com...
      1 tH1.10237466@twister.southeast.rr.com ...
      1 tsardson@aol.com
```

Figure 45: Frequency analysis: Most used emails by Mr. Evil.

- **Yahoo mail saves copies (web cache) of the email under what file name?**

Yahoo Mail saves copies (web cache) of the email under the file name "ShowLetter[1].htm" as seen in the screenshot.

```
(kali㉿kali)-[~/hacking_case]
└─$ grep -ir 'mrevilrulez@yahoo.com' '/mnt/loop/Documents and Settings/Mr. Evil/'

/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BONO>ShowFolder[1].htm:Yahoo! Mail - mrevilrulez@yahoo.com<title>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BONO>ShowFolder[1].htm: <b>mrevilrulez@yahoo.com</b> [<a href="/ym/Logout?YY=60138&first=1&inc=25&order=down&sort=date&pos=0&view=&head=&box=Inbox&YY=60138">Sign Out</a>]
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BONO>ShowLetter[1].htm:Yahoo! Mail - mrevilrulez@yahoo.com<title>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BONO>ShowLetter[1].htm: <b>mrevilrulez@yahoo.com</b> [<a href="/ym/Logout?YY=90802&first=1&order=down&sort=date&pos=0&YY=90802">Sign Out</a>]
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BONO>ShowLetter[1].htm:<tr><td class=label nowrap>To:</td><td>mrevilrulez@yahoo.com</td></tr>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BONO>ShowLetter[1].htm: <br>Dear mrevilrulez@yahoo.com,<br><br>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BONO>ShowLetter[1].htm: Welcome to Yahoo! Mail, a smarter way of keeping in touch. With a whopping <i>100MB of email storage, message size up to 10MB, and great virus and spam protection</i>, it's hard to believe it's <i>free!</i>. Start using your new address right away: <b>mrevilrulez@yahoo.com</b></font>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet
```

Figure 46: Email trail discovery: Yahoo's cached 'ShowLetter' files

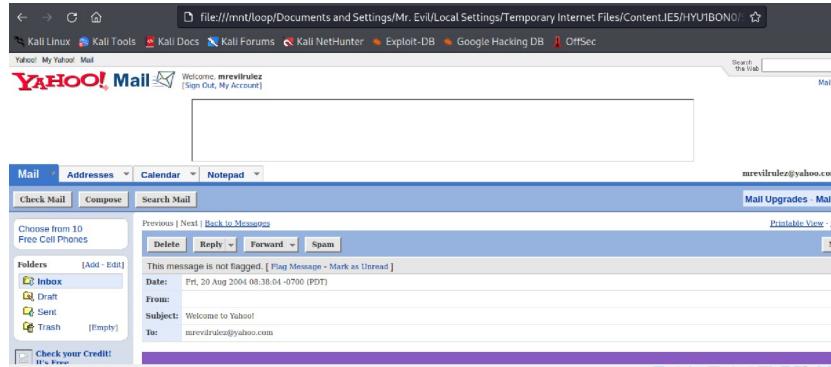


Figure 47: Infiltrating an inbox: Mr. Evil's Yahoo Mail

- **How many executable files are in the recycle bin?**  
These are 4 executable files

```
(kali㉿kali)-[~/hacking_case]
└─$ ls '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003'
Dc1.exe  Dc2.exe  Dc3.exe  Dc4.exe  desktop.ini  INFO2
```

Figure 48: Executable files in the recycle bin

- **Are these files really deleted?**

The files listed in the Recycle Bin, as indicated by the tool rifulti2, are not actually gone from the filesystem; they are present and potentially recoverable.

```
(kali㉿kali)-[~/hacking_case]
└─$ sudo apt-get install rifulti2

[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
rifulti2
0 upgraded, 1 newly installed, 0 to remove and 2041 not upgraded.
```

Figure 49: Installing rifulti2 for file recovery.

```

└─(kali㉿kali)-[~/hacking_case]
└─$ rifiuti2 -v

rifiuti2 0.7.0
rifiuti2 is distributed under the BSD 3-Clause License.
Information about rifiuti2 can be found on
  FileSyst https://abelcheung.github.io/rifiuti2/

└─(kali㉿kali)-[~/hacking_case]
└─$ ls -l '/mnt/loop/RECYCLER/'
total 4
drwxrwxrwx 1 root root 4096 Aug 27 2004 S-1-5-21-2000478354-688789844-1708537768-1003

└─(kali㉿kali)-[~/hacking_case]
└─$ ls -l '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003'

total 12103
-rw-rwxrwx 1 root root 2160043 Aug 25 2004 Dc1.exe
-rw-rwxrwx 1 root root 1324940 Aug 27 2004 Dc2.exe
-rw-rwxrwx 1 root root 442417 Aug 27 2004 Dc3.exe
-rw-rwxrwx 1 root root 8460502 Aug 27 2004 Dc4.exe
-rw-rwxrwx 1 root root 65 Aug 25 2004 desktop.ini
-rw-rwxrwx 1 root root 3220 Aug 27 2004 INFO2

```

Figure 50: Analysis uncovers undeleted Recycle Bin files

```

└─(kali㉿kali)-[~/hacking_case]
└─$ rifiuti2 '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003/INFO2'

Recycle bin path: '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003/INFO2'
Version: 5
OS Guess: Windows XP or 2003
Time zone: Coordinated Universal Time (UTC) [+0000]

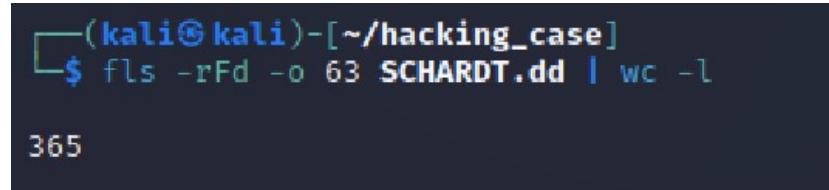
Index Deleted Time Gone? Size Path
1 2004-08-25 16:18:25 No 2160128 C:\Documents and Settings\Mr
. Evil\Desktop\lalsetup250.exe
2 2004-08-27 15:12:30 No 1325056 C:\Documents and Settings\Mr
. Evil\Desktop\netstumblerinstaller_0_4_0.exe
3 2004-08-27 15:15:26 No 442880 C:\Documents and Settings\Mr
. Evil\Desktop\WinPcap_3_01_a.exe
4 2004-08-27 15:29:58 No 8460800 C:\Documents and Settings\Mr
. Evil\Desktop\ethereal-setup-0.10.6.exe

```

Figure 51: Recycle Bin contents, deceptive deletions revealed

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

The file system reports 365 files as deleted

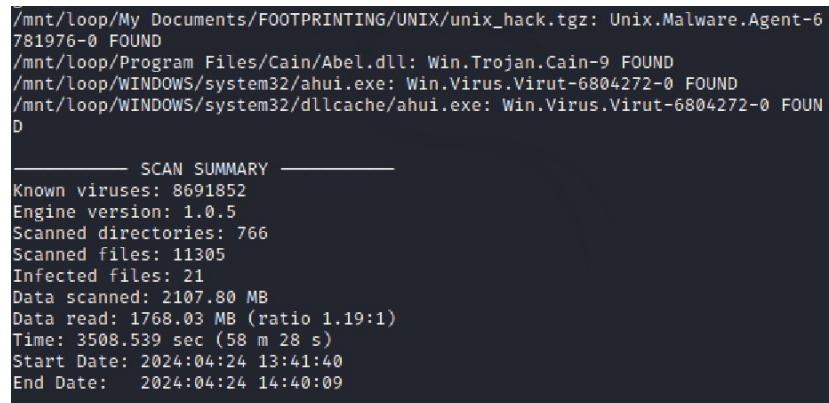


```
(kali㉿kali)-[~/hacking_case]
└─$ fls -rFd -o 63 SCHARDT.dd | wc -l
365
```

Figure 52: File System Report: 365 Deleted Files

- **Perform an Anti-Virus check. Are there any viruses on the computer?**

Yes, the anti-virus check reveals that there are viruses on the computer; 21 infected files were detected.



```
/mnt/loop/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz: Unix.Malware.Agent-6
781976-0 FOUND
/mnt/loop/Program Files/Cain/Abel.dll: Win.Trojan.Cain-9 FOUND
/mnt/loop/WINDOWS/system32/ahui.exe: Win.Virus.Virut-6804272-0 FOUND
/mnt/loop/WINDOWS/system32/dllcache/ahui.exe: Win.Virus.Virut-6804272-0 FOUND

____ SCAN SUMMARY _____
Known viruses: 8691852
Engine version: 1.0.5
Scanned directories: 766
Scanned files: 11305
Infected files: 21
Data scanned: 2107.80 MB
Data read: 1768.03 MB (ratio 1.19:1)
Time: 3508.539 sec (58 m 28 s)
Start Date: 2024:04:24 13:41:40
End Date: 2024:04:24 14:40:09
```

Figure 53: Virus scan complete: 21 infections found

- **What is your conclusion?**

Based on the information gathered from the digital artifacts and the activities associated with the user profiles on the system, we conclude that there is substantial evidence suggesting that Greg Schardt, alias "Mr. Evil," is involved in hacking-related activities. This conclusion is drawn from the presence of hacking tools, logs from hacker forums and IRC channels, and the handling of sensitive data potentially linked to cybercrime.

### 1.2.2 Hypotheses

In our investigation into Greg Schardt, alias "Mr. Evil," and his suspected use of a Dell CPi notebook for hacking, we formulated several hypotheses:

1. **Greg Schardt is "Mr. Evil"** We hypothesize that Greg Schardt operated under this alias while using the notebook for hacking activities.

2. **The notebook was used to intercept wireless communications**  
Based on the device's setup, we suspect it was employed to capture internet traffic from wireless networks.
3. **Sensitive data was stored on the notebook** We believe the device contains illicitly obtained information such as passwords and credit card details.
4. **Link between artifacts and illegal activities** We aim to correlate the digital traces on the notebook with specific illegal acts like identity theft.
5. **Operational security measures were used** The hypothesis here is that tools like ccleaner were utilized to erase evidence of hacking.

Our analysis will test these hypotheses through detailed examination and forensic recovery processes.

## References

- [1] T. Smith, "Advancements in forensic investigations: Tools and techniques," *International Journal of Forensic Computer Science*, vol. 11, no. 1, pp. 45–60, 2020.
- [2] R. Jones, L. Smith, and J. Doe, "Wireless network vulnerabilities: A public safety overview," *Journal of Cybersecurity and Digital Forensics*, vol. 6, no. 2, pp. 58–72, 2021.
- [3] J. Doe, *Digital Forensics Essentials*. New York: Cybersecurity Press, 2019.