On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. (The equal signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, G=r=e=g S=c=h=a=r=d=t.

A DD image and a EnCase image of the abandoned computer have already been made.

---

1. What is the image hash? Does the acquisition and verification hash match?
   AEE4FCD9301C03B3B054623CA261959A
   Yes

2. What operating system was used on the computer?
   Windows XP

3. When was the install date?
   08/19/04 05:48:27PM

4. What is the timezone settings?
   Central Daylight Time (-05hrs GMT)

5. Who is the registered owner?
   G=r=e=g S=c=h=a=r=d=t

6. What is the computer account name?
   N-1A9ODN6ZXK4LQ

7. What is the primary domain name?
   Evil

8. When was the last recorded computer shutdown date/time?
   08/27/04 10:46:33AM

9. How many accounts are recorded (total number)?
   5

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

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

Mr. Evil

12. A search for the name of “G=r=e=g S=c=h=a=r=d=t” (The equal signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

C:\Program Files\Look@LAN
\irunin.ini Look@LAN

13. List the network cards used by this computer

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

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

```
192.168.1.111
0010a4933e09
```

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?

Xircom

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

Cain & Abel v2.5 beta45 (password sniffer & cracker)
Ethereal (packet sniffer)
123 Write All Stored Passwords (finds passwords in registry)
Anonymizer (hides IP tracks when browsing)
CuteFTP (FTP software)
Look&LAN_1.0 (network discovery tool)
NetStumbler (wireless access point discovery tool)

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

whoknowsme@sbcglobal.net

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

News.dallas.sbcglobal.net

19. What two installed programs show this information?

MS Outlook Express
Forte Agent

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

Alt.2600.phreakz
Alt.2600

Alt.2600.cardz
Alt.2600codez
Alt.2600.crackz
Alt.2600.moderated
Alt.binaries.hacking.utilities
Alt.stupidity.hackers.malicious
Free.binaries.hackers.malicious
Free.binaries.hacking.talentless.troll_haven
Free.binaries.hacking.talentless.troll-haven
alt.nl.binaries.hack
free.binaries.hacking.beginner
free.binaries.hacking.computers
free.binaries.hacking.utilities
free.binaries.hacking.websites
alt.binaries.hacking.computers
alt.binaries.hacking.websites
alt.dss.hack
alt.binaries.hacking.beginner
alt.hacking
alt.2600.programz
alt.2600.hackerz

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?

user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez

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

Ushells.undernet.log
Elite.hackers.undernet.log
Mp3xserv.undernet.log
Chataholics.undernet.log
Cybercafé.undernet.log
M5tar.undernet.log
Thedarktower.afternet.log
Funny.undernet.log
Luxshell.undernet.log
Evilfork.efnet.log
Iso-warez.efnet.log
Houston.undernet.log

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?

Interception

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?

Windows CE (Pocket PC)

25. What websites was the victim accessing?

Mobile.msn.com
MSN (Hotmail) Email

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

mrevilrulez@yahoo.com

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

Showletter[1].htm

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

4

29. Are these files really deleted?

No

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

3

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

Yes