BOSTON UNIVERSITY
2-14-2021

Katie Barnes

MET CJ 710 01

Professor Choi

February 14, 2021

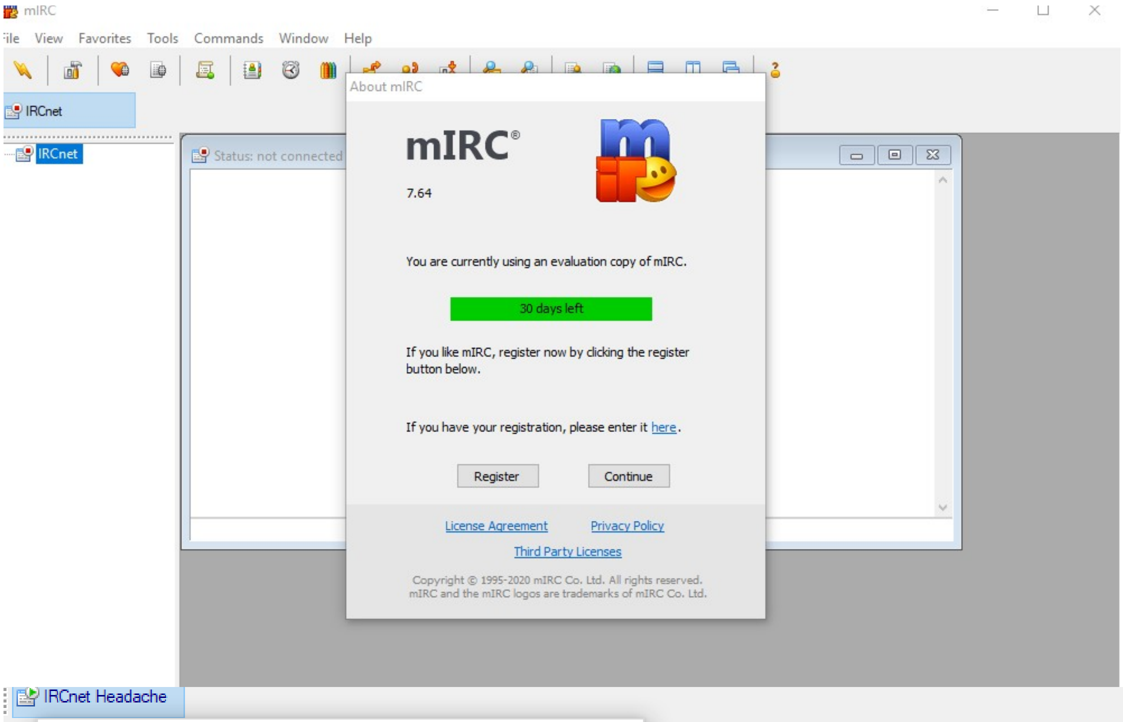
Lab Assignment 3-1: mIRC

Mr. Evil Noodle could infect Curry’s computer system within the mIRC chatroom because at this point Curry has granted access somewhat comparable to an open channel or tunnel. The mIRC software essentially opens a port to send and a port to receive data. Since Curry allowed the app download onto his computer it is now vulnerable to hackers, Mr. Evil Noodle can now spam him, send a virus, even hijack his computer. This means he can take control of the entire computer. He can attempt a worm-based DOS attack which could provide a broad-spectrum of damages (Choi, 2015). Moreover, Botnets could be awaiting opportunity to attack Curry’s computer. A bot is a malicious application that can be used to control a computer (Module 4, 2021).

A zombie computer, which is a computer that is under the hacker’s command executes an attack on the computer, and a Botnet is a group of computers that are controlled by a bot (Module 4). Ultimately these bots are ready to gain access as soon as the computer becomes vulnerable for attack. Once Mr. Evil Noodle has acquired Curry’s data, he can share his information over the dark web with other cyber criminals. He can expose personal photographs, his email address, his identity. Basically, anything that he can come across in Curry’s device. Mr. Evil Noodle could even install malicious software in the system or pornographic pictures, audio, or videos. In addition, he could find credit card or bank account information as well. These are only a few examples of what that can happen when a hacker is given direct access to a device.

If Mr. CIC and Mr. Hero investigated the case, first and foremost they would need to find out where the IP address leads them to. They need to find the exact location that the crime was committed so that they can investigate who the device or computer involved in the crime belongs to. After tracing the device to an actual person or company Mr. CIC and Mr. Hero can attain a search warrant to seize items that are involved in the crime. For starters, they need information as a contraband or fruits of the crime, information as an instrument, information as evidence (Choi. 2015). Mr. CIC and Mr. Hero must make sure that they follow the search warrant requirement and that is to respect the Fourth Amendment of the United States which protects the privacy of all citizens unless probable cause is given to move forward with a search warrant. After a search warrant is approved by a judge prior to seizing anything. Once the warrant is granted Mr.CIC and Mr. Hero shall only seize computers that are covered in their search warrant (Choi, 2015). The search warrant application provided to the judge should include all items that MR.CIC and Mr. Hero are looking for to prove their case which could include but are not limited to digital; evidence such as photographs, documents, databases, spreadsheets, financial sheets, financial records, emails, etc. (Choi, 2015). Additionally, devices, hacking tools, MS office, Fox Prodata etc., fingerprints, DNA, Network, ISP, OS, or other usernames or passwords (Choi, 2015). Afterwards, secure the evidence, document the evidence, tag it, bag it, and transport it to the forensic lab (Choi, 2015).

If any person decides to enter mIRC chat that individual would need to be careful what type of information they are sharing and make sure they are not exposing their computer to the hacker world. If for instance I decided to chat in mIRC I would hide personal information such as my email address that could be exposed to the dark web. I would need to keep all personal information private and not reveal my real identity or my address. I would not exchange any of my personal information with other users also would not click on anything or accept files from other users in the chatroom. In addition, I should not chat on unknown platforms or click on questionable chats such as porn chats or anything that seems illegal, I should not interact in those types of chats. If I were the victim of a hacker, I would secure my device with software such as Norton 360 other Virus scanners. I would be sure that I had a Malware or malicious software removal tool as well. I would be more careful about who I interact with and what types of chats I join. I personally would have no need to use mIRC but if I were a user, I would be more cautious about my activities. I would be making sure I do not continue to make my computer vulnerable for hackers to steal my information or invade my privacy or devices. If need be, I would contact the proper authorities and report crimes, secure my credit report for discrepancies, and report fraudulent charges to my credit cards. I would change all my passwords to my email addresses and other secure websites that need my attention such as my login credentials for school or work.



mIRC®

7.64

You are currently using an evaluation copy of mIRC.

30 days left

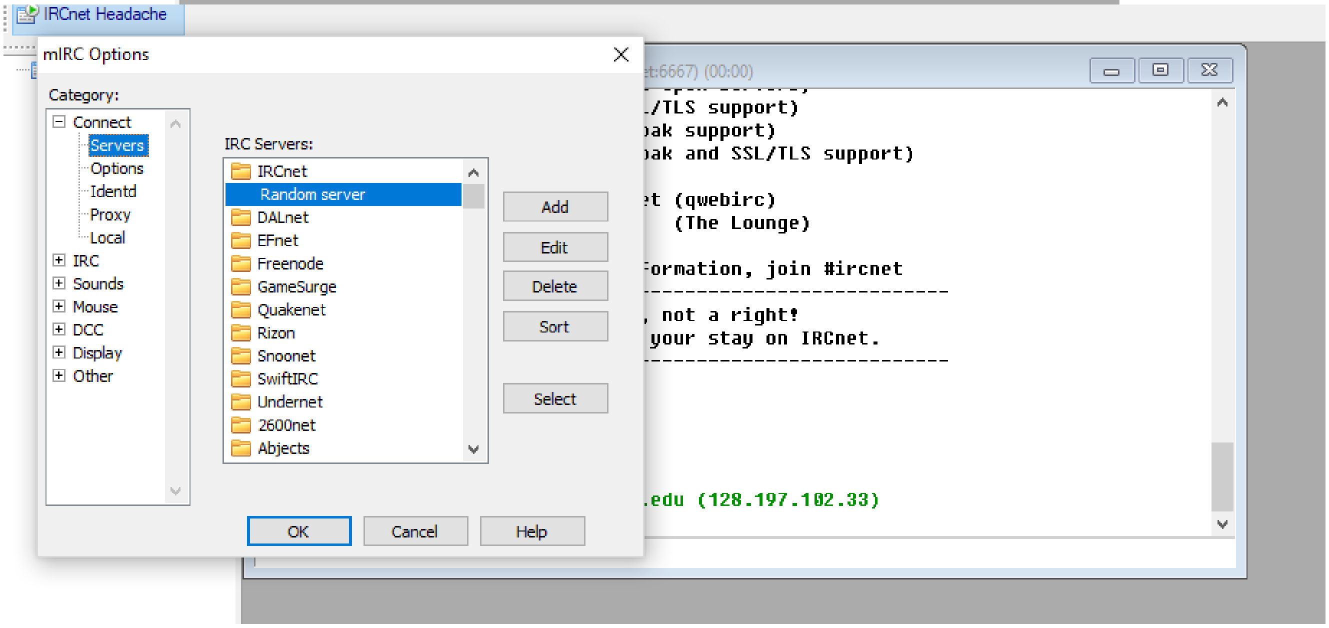
If you like mIRC, register now by clicking the register button below.

If you have your registration, please enter it here.

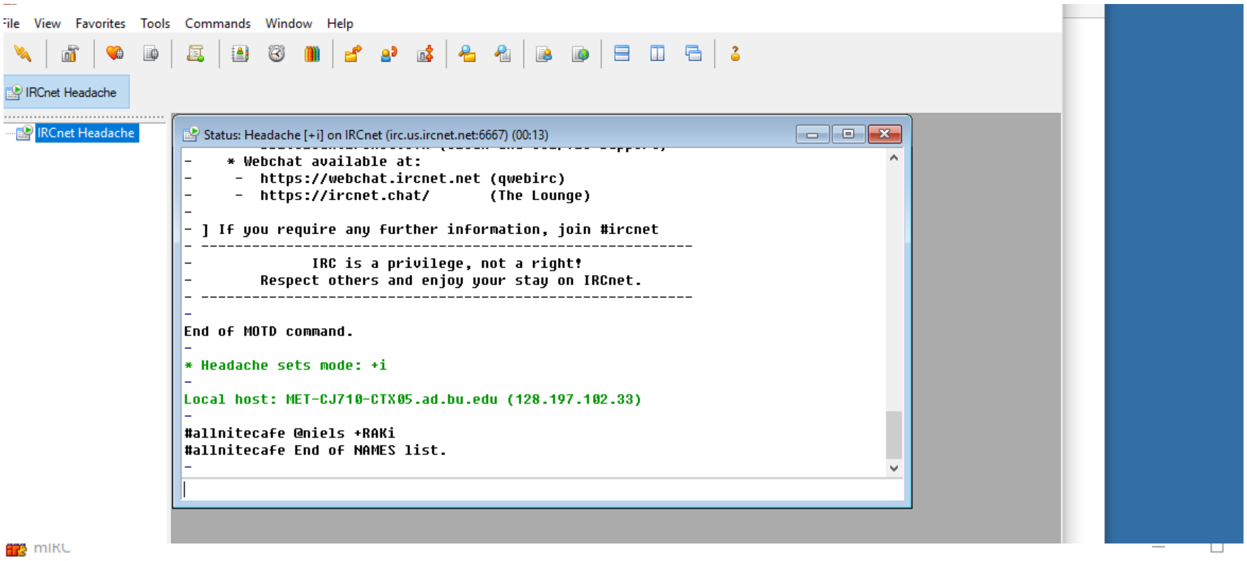
License Agreement Privacy Policy

Third Party Licenses

Copyright © 1995-2020 mIRC Co. Ltd. All rights reserved.
mIRC and the mIRC logos are trademarks of mIRC Co. Ltd.

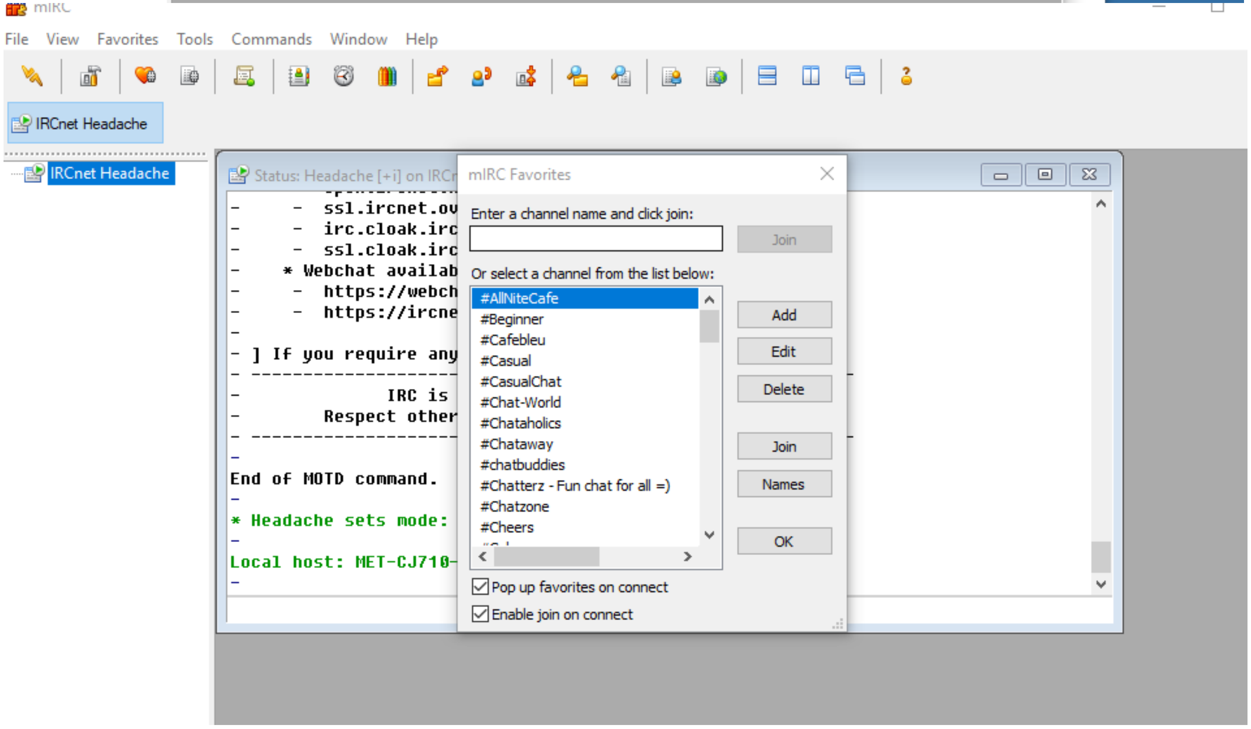


```
/TLS support)
ak support)
ak and SSL/TLS support)

t (qwebirc)
  (The Lounge)

formation, join #ircnet
---------------------------
, not a right!
your stay on IRCnet.
---------------------------




.edu (128.197.102.33)
```



Status: Headache [+i] on IRCnet (irc.us.ircnet.net:6667) (00:13)

```
-     * Webchat available at:
-      -  https://webchat.ircnet.net (qwebirc)
-      -  https://ircnet.chat/       (The Lounge)
-
- ] If you require any further information, join #ircnet
- ----------------------------------------------------------
-              IRC is a privilege, not a right!
-        Respect others and enjoy your stay on IRCnet.
- ----------------------------------------------------------
-
End of MOTD command.
-
* Headache sets mode: +i
-
Local host: MET-CJ710-CTX05.ad.bu.edu (128.197.102.33)
-
#allnitecafe @niels +RAKi
#allnitecafe End of NAMES list.
-
```



```
-      -  ssl.ircnet.ov
-      -  irc.cloak.irc
-      -  ssl.cloak.irc
-    * Webchat availab
-      -  https://webch
-      -  https://ircne
-
- ] If you require any
- ----------------------
-              IRC is
-       Respect other
- ----------------------
-
End of MOTD command.
-
* Headache sets mode:
-
Local host: MET-CJ710-
-
```

Enter a channel name and click join:

Or select a channel from the list below:

- #AllNiteCafe
- #Beginner
- #Cafebleu
- #Casual
- #CasualChat
- #Chat-World
- #Chataholics
- #Chataway
- #chatbuddies
- #Chatterz - Fun chat for all =)
- #Chatzone
- #Cheers

☑ Pop up favorites on connect

☑ Enable join on connect

The above screenshots are a display of the chat app that Curry installed on his computer. Curry accessed the mIRC chat with other users and unknowingly let hackers into his devices when he joined a chatroom and clicked on links provided by other users in the chat. At this point a hacker gained access to his device. mIRC is esentially a platform that anyone can use to share expertise, you for fun like gaming. Unfortunately, hackers also use this app to take advantage of other users who leave their device open for attack.

Examination Report

Case Information

Case Number	001
Case Date	6-6-2017
Examiner Name	BARNES
Examiner I.D. #	CJ-710--01
Agency	BU
Description	Computer Forensic Investigation

Examination Report

Summary of Findings

This is a complete investigation for a Dell Latitude laptop that was involved in a series of hacking cybercrimes. The owner of the Dell laptop is Greg Schardt is believed to be involved in these crimes as his named is listed under all the evidence provided in this examination report. All evidence links Greg Schardt to the alias name Mr. Evil. Enclosed in this report is the evidence to be used in the case and they are as follows:

- Evidence Dell Latitude Laptop
- A snapshot of Greg Schardt's yahoo email that links both Greg and Mr. Evil as the same person
- A login by a Drwtsn32.log that directly links both Greg Schardt to Mr. Evil.
- 11 installed hacking software programs/ hacking tools
- 2 downloaded multimedia videos about hacking

Examination Tools

The following tools and equipment were used to process the submitted items of evidence:

Evidence

Each item was individually inventoried, cataloged and photographed. As part of the cataloging procedures, each submitted item is assigned a unique Bar Code Number (BCN). Additionally, for each piece of Evidence submitted, I created a physical "image" which was then saved to forensically prepared media.
The following devices were examined (for further information, see the enclosed worksheets):

Name	Acquisition MD5	Verification MD5	Evidence Number	Examiner Name
Dell Latitude CPi	aee4fcd9301c03b3b054623ca261959a	aee4fcd9301c03b3b054623ca261959a	1 of 1	

Registered Owner of Device

These items listed below are cached Microsoft files that display the identity of the owner of the Dell Latitude computer device. It not only demonstrates that the user is Greg Schardt but links the suspect to multiple usernames within the device.

1) RegisteredOwner

Item Path	$$$PROTO.HIV\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
File Created	
Last Written	
Last Accessed	
MD5	ecd3569cc8603aa6f1ea7e8a1daa9523
Start Sector	15,523
Sector offset	108
File Offset	0
Length	26
Comment	

```
    G r e g   S c h a r d t
```

2) RegisteredOwner

Item Path	$$$PROTO.HIV\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
File Created	
Last Written	
Last Accessed	
MD5	ecd3569cc8603aa6f1ea7e8a1daa9523
Protected	
Comment	Registered user

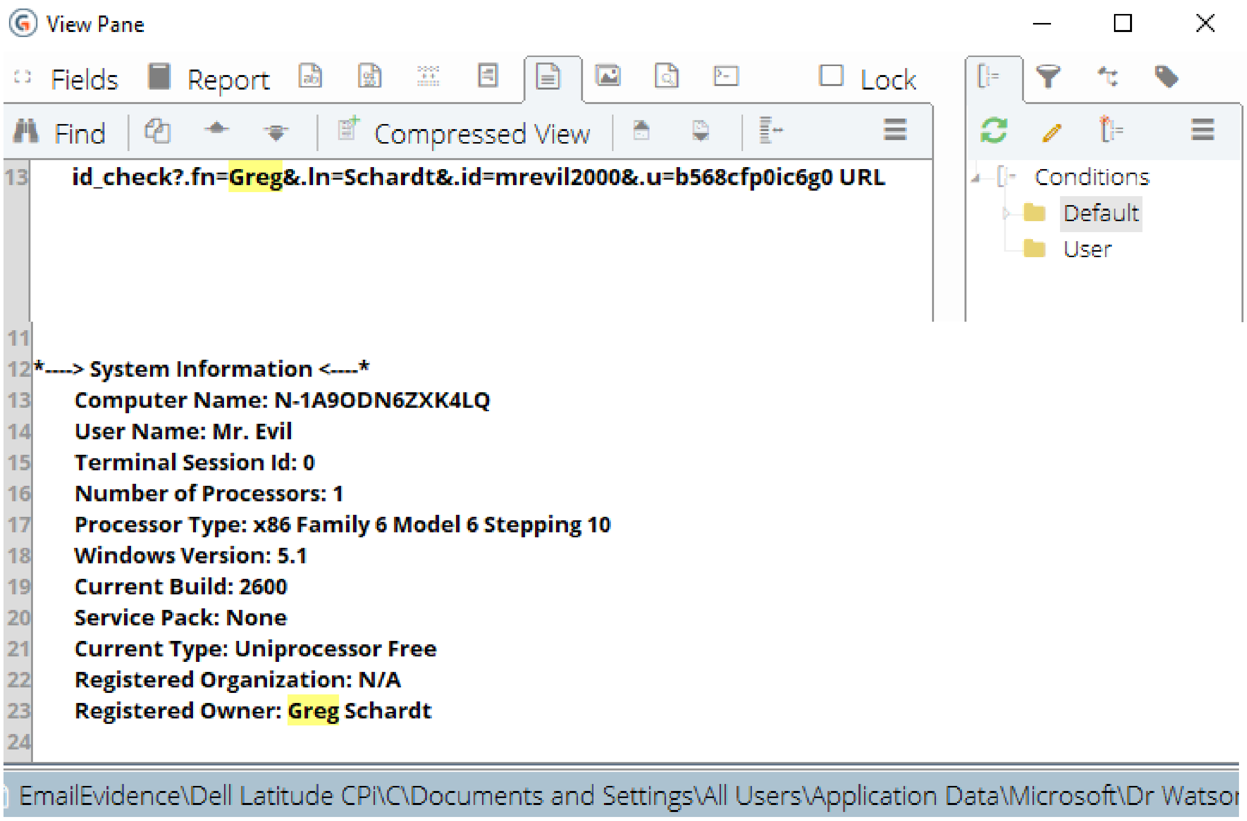
3) drwtsn32.log

Item Path	Dell Latitude CPi\C\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\drwtsn32.log
File Created	08/20/04 10:25:45 AM
Last Written	08/20/04 10:25:48 AM
Last Accessed	08/20/04 10:25:48 AM
MD5	1f6aa0e6768d1393861f8c551840309f
Start Sector	
Sector offset	
File Offset	0

Length	706
Comment	Registered Owner Gred is Mr. Evil and Dr.Watsn32

```
Microsoft (R) DrWtsn32
Copyright (C) 1985-2001 Microsoft Corp. All rights reserved.



Application exception occurred:
        App: C:\Program Files\Internet Explorer\iexplore.exe (pid=1140)
        When: 8/20/2004 @ 10:25:46.165
        Exception number: c0000005 (access violation)

*----> System Information <----*
        Computer Name: N-1A9ODN6ZXK4LQ
        User Name: Mr. Evil
        Terminal Session Id: 0
        Number of Processors: 1
        Processor Type: x86 Family 6 Model 6 Stepping 10
        Windows Version: 5.1
        Current Build: 2600
        Service Pack: None
        Current Type: Uniprocessor Free
        Registered Organization: N/A
        Registered Owner: Greg Schardt
```

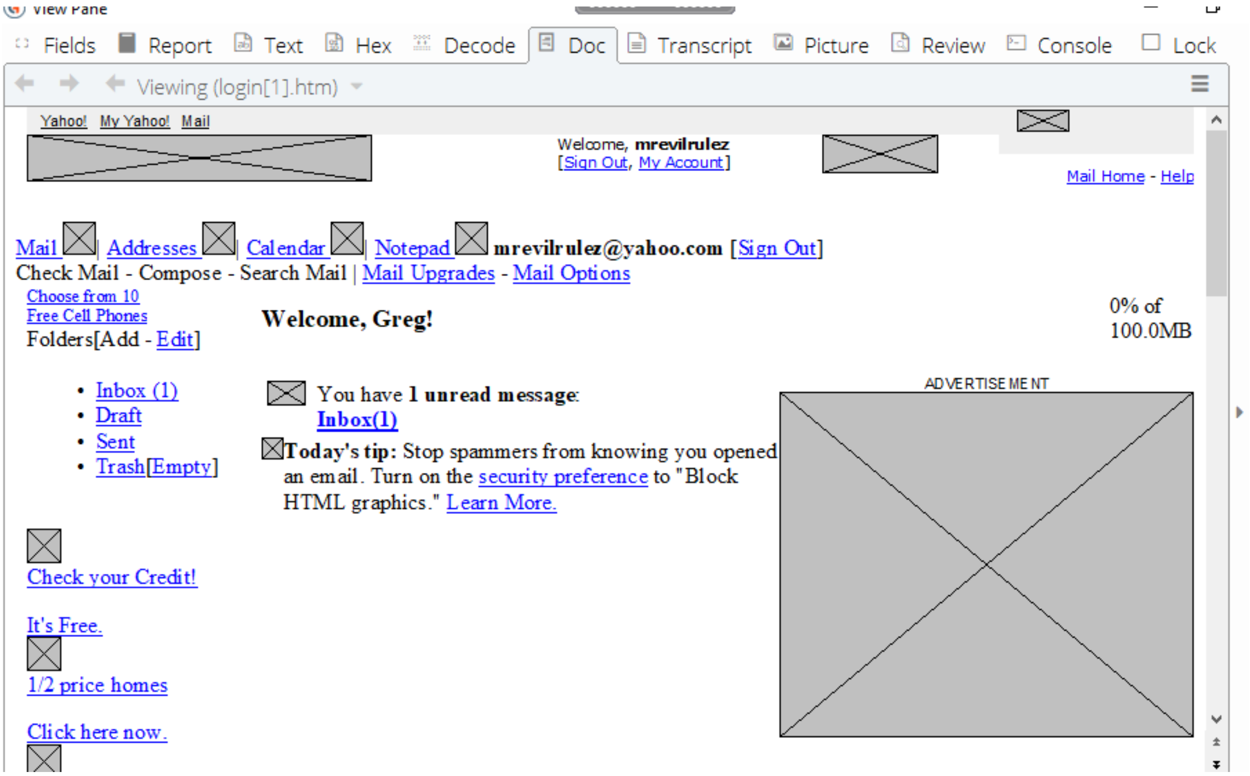
Email Evidence



```
   id_check?.fn=Greg&.ln=Schardt&.id=mrevil2000&.u=b568cfp0ic6g0 URL
```

```

*----> System Information <----*
    Computer Name: N-1A9ODN6ZXK4LQ
    User Name: Mr. Evil
    Terminal Session Id: 0
    Number of Processors: 1
    Processor Type: x86 Family 6 Model 6 Stepping 10
    Windows Version: 5.1
    Current Build: 2600
    Service Pack: None
    Current Type: Uniprocessor Free
    Registered Organization: N/A
    Registered Owner: Greg Schardt

```

EmailEvidence\Dell Latitude CPi\C\Documents and Settings\All Users\Application Data\Microsoft\Dr Watsor



Yahoo! My Yahoo! Mail

Welcome, **mrevilrulez**
[Sign Out, My Account]

Mail Home - Help

Mail | Addresses | Calendar | Notepad **mrevilrulez@yahoo.com** [Sign Out]
Check Mail - Compose - Search Mail | Mail Upgrades - Mail Options

Choose from 10
Free Cell Phones
Folders[Add - Edit]

Welcome, Greg!

0% of
100.0MB

- Inbox (1)
- Draft
- Sent
- Trash[Empty]

You have **1 unread message**:
Inbox(1)

Today's tip: Stop spammers from knowing you opened an email. Turn on the security preference to "Block HTML graphics." Learn More.

Check your Credit!

It's Free.

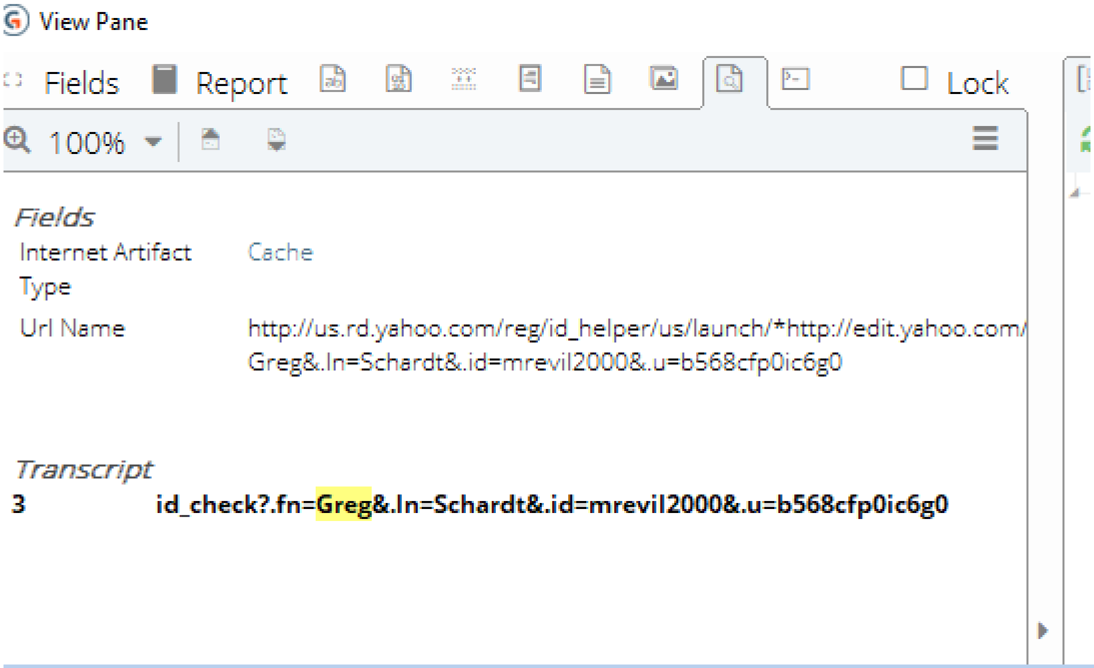
1/2 price homes

Click here now.

The email snapshots provided demonstrate that the alias Mr. Evil belong to Greg Schardt.

Internet Artifacts

The following artifacts were found in the Internet Explorer Cache.



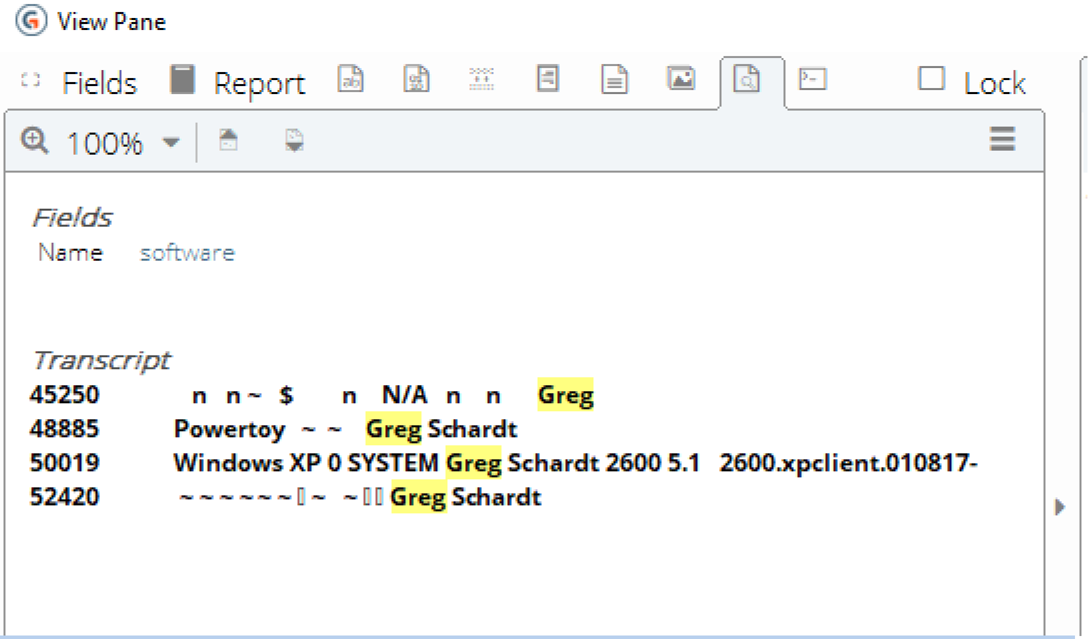
Fields

Internet Artifact Type	Cache
Url Name	http://us.rd.yahoo.com/reg/id_helper/us/launch/*http://edit.yahoo.com/ Greg&.ln=Schardt&.id=mrevil2000&.u=b568cfp0ic6g0

Transcript

```
3          id_check?.fn=Greg&.ln=Schardt&.id=mrevil2000&.u=b568cfp0ic6g0
```

This cache displays the registered user of a yahoo account (Greg Schardt) which is listed in email evidence as mrevilrulez@yahoo.com. The user Greg Schardt and alias Mr. Evil are the same person.



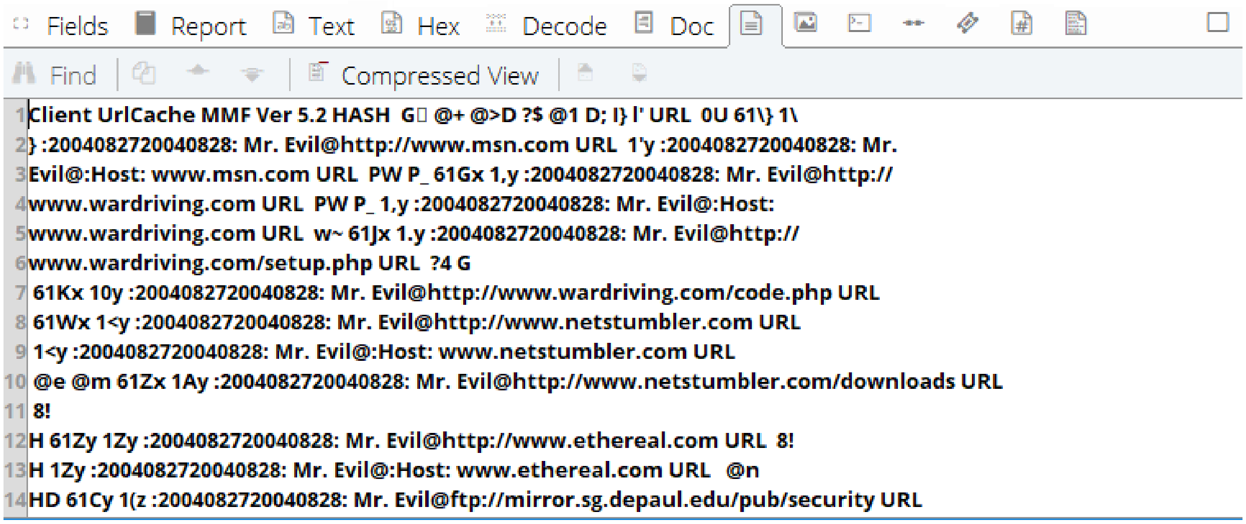
Fields

Name	software

Transcript

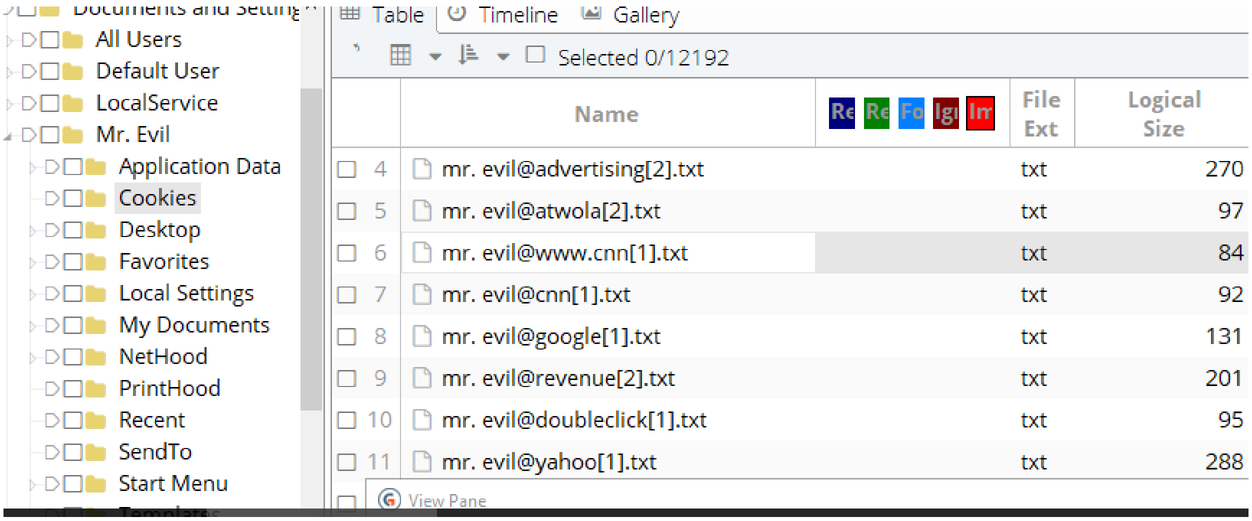
```
45250     n  n ~  $     n   N/A  n   n     Greg
48885    Powertoy  ~ ~   Greg Schardt
50019    Windows XP 0 SYSTEM Greg Schardt 2600 5.1   2600.xpclient.010817-
52420     ~ ~ ~ ~ ~ ~ ~ ▯ ~   ~ ▯▯ Greg Schardt
```

This snapshot is a transcript of illegal hacker software also found in cache.



```
Client UrlCache MMF Ver 5.2 HASH  G @+ @>D ?$ @1 D; l} l' URL  0U 61\} 1\
} :2004082720040828: Mr. Evil@http://www.msn.com URL  1'y :2004082720040828: Mr.
Evil@:Host: www.msn.com URL  PW P_ 61Gx 1,y :2004082720040828: Mr. Evil@http://
www.wardriving.com URL  PW P_ 1,y :2004082720040828: Mr. Evil@:Host:
www.wardriving.com URL  w~ 61Jx 1.y :2004082720040828: Mr. Evil@http://
www.wardriving.com/setup.php URL  ?4 G
 61Kx 10y :2004082720040828: Mr. Evil@http://www.wardriving.com/code.php URL
 61Wx 1<y :2004082720040828: Mr. Evil@http://www.netstumbler.com URL
 1<y :2004082720040828: Mr. Evil@:Host: www.netstumbler.com URL
 @e @m 61Zx 1Ay :2004082720040828: Mr. Evil@http://www.netstumbler.com/downloads URL
 8!
H 61Zy 1Zy :2004082720040828: Mr. Evil@http://www.ethereal.com URL  8!
H 1Zy :2004082720040828: Mr. Evil@:Host: www.ethereal.com URL   @n
HD 61Cy 1(z :2004082720040828: Mr. Evil@ftp://mirror.sg.depaul.edu/pub/security URL
```

The above snapshot demonstrates a transcript from software programs installed used for hacking tools. The software listed is Ethereal, net stumbler mirroring, and wardriving set up. These programs are all illegal hacker software tools. These items were saved into the cache from previously installed software.



	Name	Re	Re	Fo	Igı	Im	File Ext	Logical Size
4	mr. evil@advertising[2].txt						txt	270
5	mr. evil@atwola[2].txt						txt	97
6	mr. evil@www.cnn[1].txt						txt	84
7	mr. evil@cnn[1].txt						txt	92
8	mr. evil@google[1].txt						txt	131
9	mr. evil@revenue[2].txt						txt	201
10	mr. evil@doubleclick[1].txt						txt	95
11	mr. evil@yahoo[1].txt						txt	288

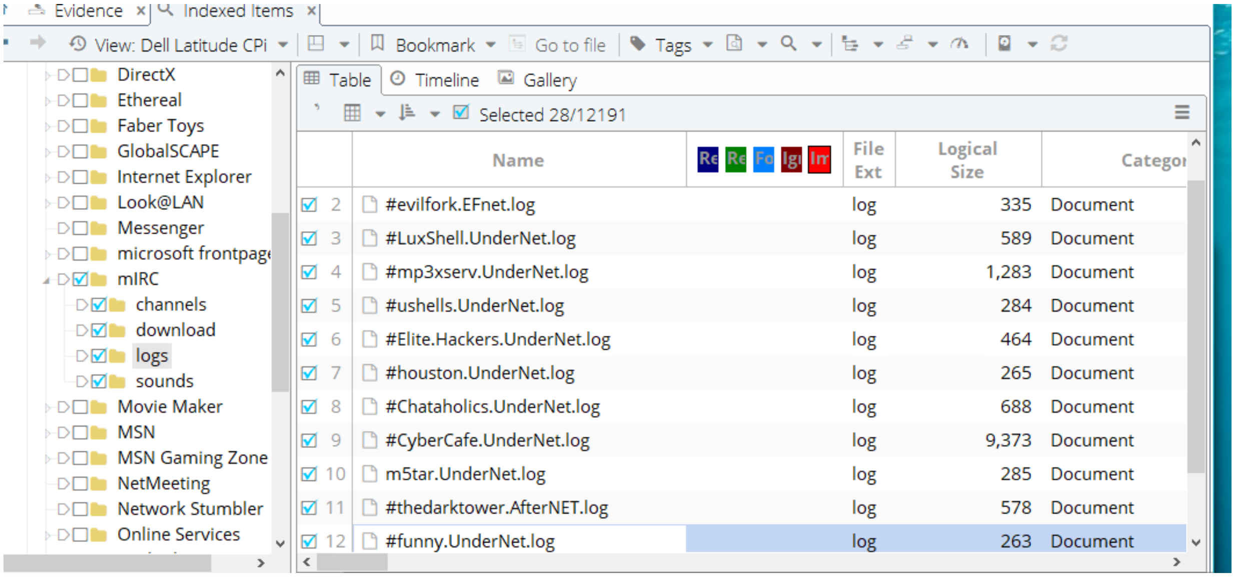
This photo displays cookies which are essentially a memory for the internet. Cookies remember websites that are visited frequently over the web.

[Subscribed Hacker websites

elitehackers[1]

Item Path	Internet Explorer (Windows)\Cache\HTML\elitehackers[1]
File Created	
Last Written	
Last Accessed	
MD5	526e61cda18e658965439ef7392fe530
Start Sector	
Sector offset	
File Offset	0
Length	203
Comment	hacker website

```
Night Wolf
-= E L I T E H A C K E R S . C O M =-


http://www.t50.com/cgi-bin/topvlog.cgi?897731691


http://www.blackcode.com/top50/gateway.php?id=1646


http://www.progenic.com/vote/?id=elitehackers
```



- ▷☐ DirectX
- ▷☐ Ethereal
- ▷☐ Faber Toys
- ▷☐ GlobalSCAPE
- ▷☐ Internet Explorer
- ▷☐ Look@LAN
- ▷☐ Messenger
- ▷☐ microsoft frontpage
- ◢☑ mIRC
  - ▷☑ channels
  - ▷☑ download
  - ▷☑ logs
  - ▷☑ sounds
- ▷☐ Movie Maker
- ▷☐ MSN
- ▷☐ MSN Gaming Zone
- ▷☐ NetMeeting
- ▷☐ Network Stumbler
- ▷☐ Online Services

		Name	Re Re Fo Igi Im	File Ext	Logical Size	Categor
☑	2	#evilfork.EFnet.log		log	335	Document
☑	3	#LuxShell.UnderNet.log		log	589	Document
☑	4	#mp3xserv.UnderNet.log		log	1,283	Document
☑	5	#ushells.UnderNet.log		log	284	Document
☑	6	#Elite.Hackers.UnderNet.log		log	464	Document
☑	7	#houston.UnderNet.log		log	265	Document
☑	8	#Chataholics.UnderNet.log		log	688	Document
☑	9	#CyberCafe.UnderNet.log		log	9,373	Document
☑	10	m5tar.UnderNet.log		log	285	Document
☑	11	#thedarktower.AfterNET.log		log	578	Document
☑	12	#funny.UnderNet.log		log	263	Document

In the above snapshot these are Greg Schardt's logs of hacker chats that he is subscribed to.

Examination

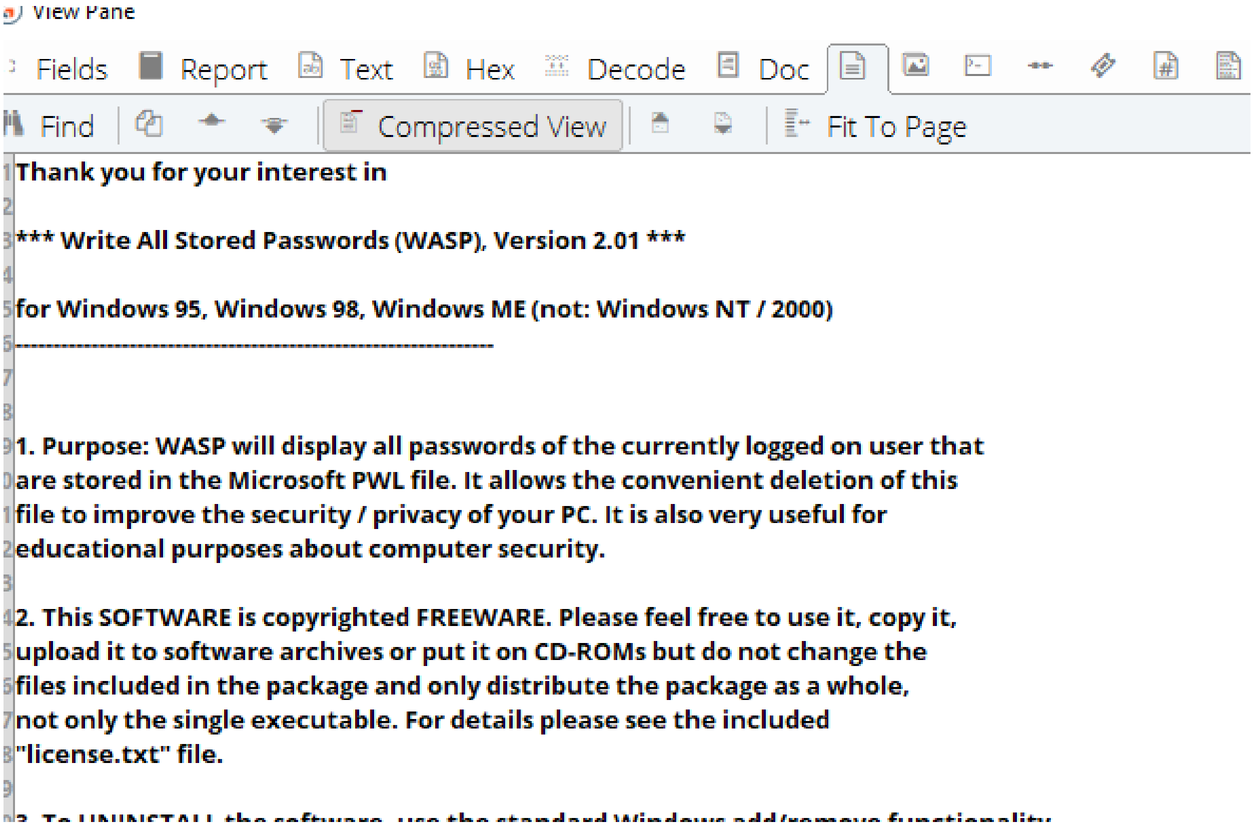
Installed Hacking Software

ALL ITEMS LISTED BELOW CAN BE FOUND IN PROGRAMS FILES OF THE DELL LATITUDE COMPUTER.

1) 123WASP

Item Path	Dell Latitude CPi\C\Program Files\123WASP

File Created	08/20/04 10:13:08 AM
Last Written	08/20/04 10:13:12 AM
Last Accessed	08/27/04 10:14:44 AM
MD5	6a78648419df8db554adada318a30612
Protected	
Comment	wasp123



Thank you for your interest in

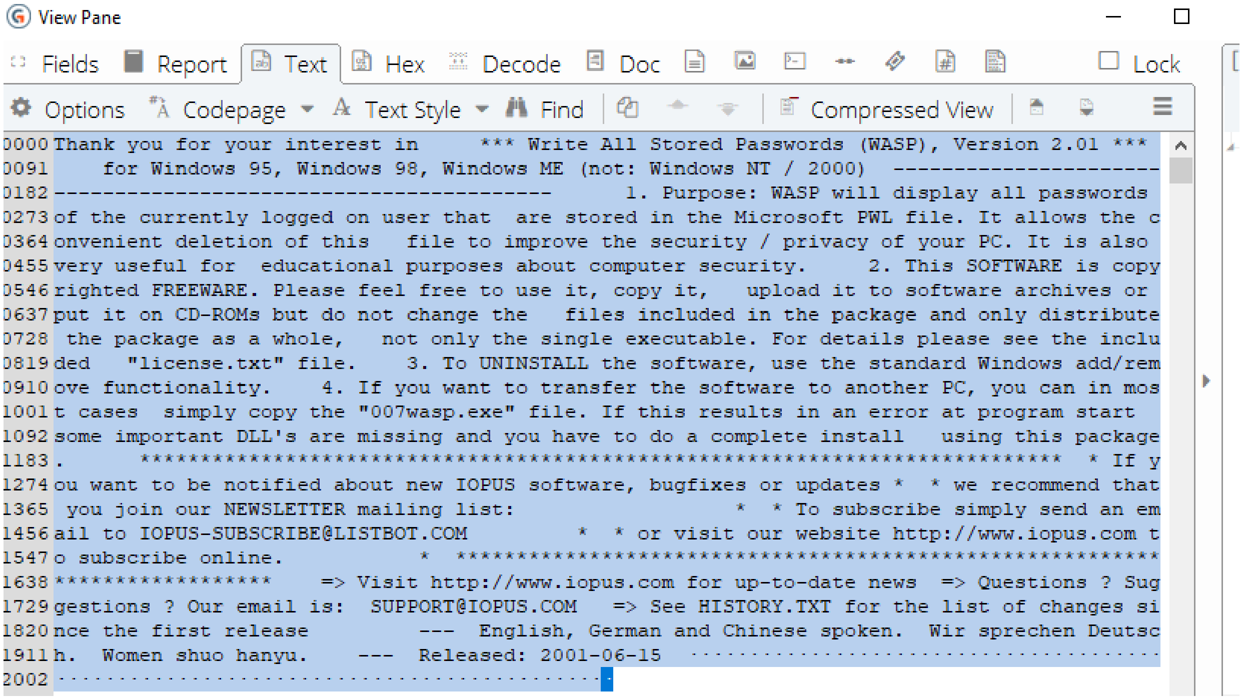
***** Write All Stored Passwords (WASP), Version 2.01 *****

for Windows 95, Windows 98, Windows ME (not: Windows NT / 2000)
--

1. Purpose: WASP will display all passwords of the currently logged on user that are stored in the Microsoft PWL file. It allows the convenient deletion of this file to improve the security / privacy of your PC. It is also very useful for educational purposes about computer security.

2. This SOFTWARE is copyrighted FREEWARE. Please feel free to use it, copy it, upload it to software archives or put it on CD-ROMs but do not change the files included in the package and only distribute the package as a whole, not only the single executable. For details please see the included "license.txt" file.

3. To UNINSTALL the software, use the standard Windows add/remove functionality



```
0000 Thank you for your interest in     *** Write All Stored Passwords (WASP), Version 2.01 ***
0091     for Windows 95, Windows 98, Windows ME (not: Windows NT / 2000)  -----------------------
0182 ----------------------------------------      1. Purpose: WASP will display all passwords
0273 of the currently logged on user that  are stored in the Microsoft PWL file. It allows the c
0364 onvenient deletion of this   file to improve the security / privacy of your PC. It is also
0455 very useful for  educational purposes about computer security.     2. This SOFTWARE is copy
0546 righted FREEWARE. Please feel free to use it, copy it,   upload it to software archives or
0637 put it on CD-ROMs but do not change the   files included in the package and only distribute
0728  the package as a whole,   not only the single executable. For details please see the inclu
0819 ded   "license.txt" file.    3. To UNINSTALL the software, use the standard Windows add/rem
0910 ove functionality.    4. If you want to transfer the software to another PC, you can in mos
1001 t cases  simply copy the "007wasp.exe" file. If this results in an error at program start
1092 some important DLL's are missing and you have to do a complete install   using this package
1183 .      ****************************************************************************  * If y
1274 ou want to be notified about new IOPUS software, bugfixes or updates *  * we recommend that
1365  you join our NEWSLETTER mailing list:                         *  * To subscribe simply send an em
1456 ail to IOPUS-SUBSCRIBE@LISTBOT.COM         *  * or visit our website http://www.iopus.com t
1547 o subscribe online.            *  **********************************************************
1638 ******************    => Visit http://www.iopus.com for up-to-date news  => Questions ? Sug
1729 gestions ? Our email is:  SUPPORT@IOPUS.COM   => See HISTORY.TXT for the list of changes si
1820 nce the first release         ---  English, German and Chinese spoken.  Wir sprechen Deutsc
1911 h.  Women shuo hanyu.    ---  Released: 2001-06-15  ·······································
2002 ·············································
```

2) README.txt

Item Path	Dell Latitude CPi\C\Program Files\123WASP\README.txt
File Created	08/20/04 10:13:08 AM
Last Written	06/13/01 02:33:28 PM
Last Accessed	08/20/04 10:13:08 AM
MD5	cea129eb7f2ca894011c162d847ecd2e
Start Sector	
Sector offset	
File Offset	220
Length	288
Comment	Wasp Software

```
1. Purpose: WASP will display all passwords of the currently
logged on user
that
are stored in the Microsoft PWL file. It allows the
convenient deletion of this

file to improve the security / privacy of your PC. It is
also very useful for
educational purposes about computer security.
```

3) Cain

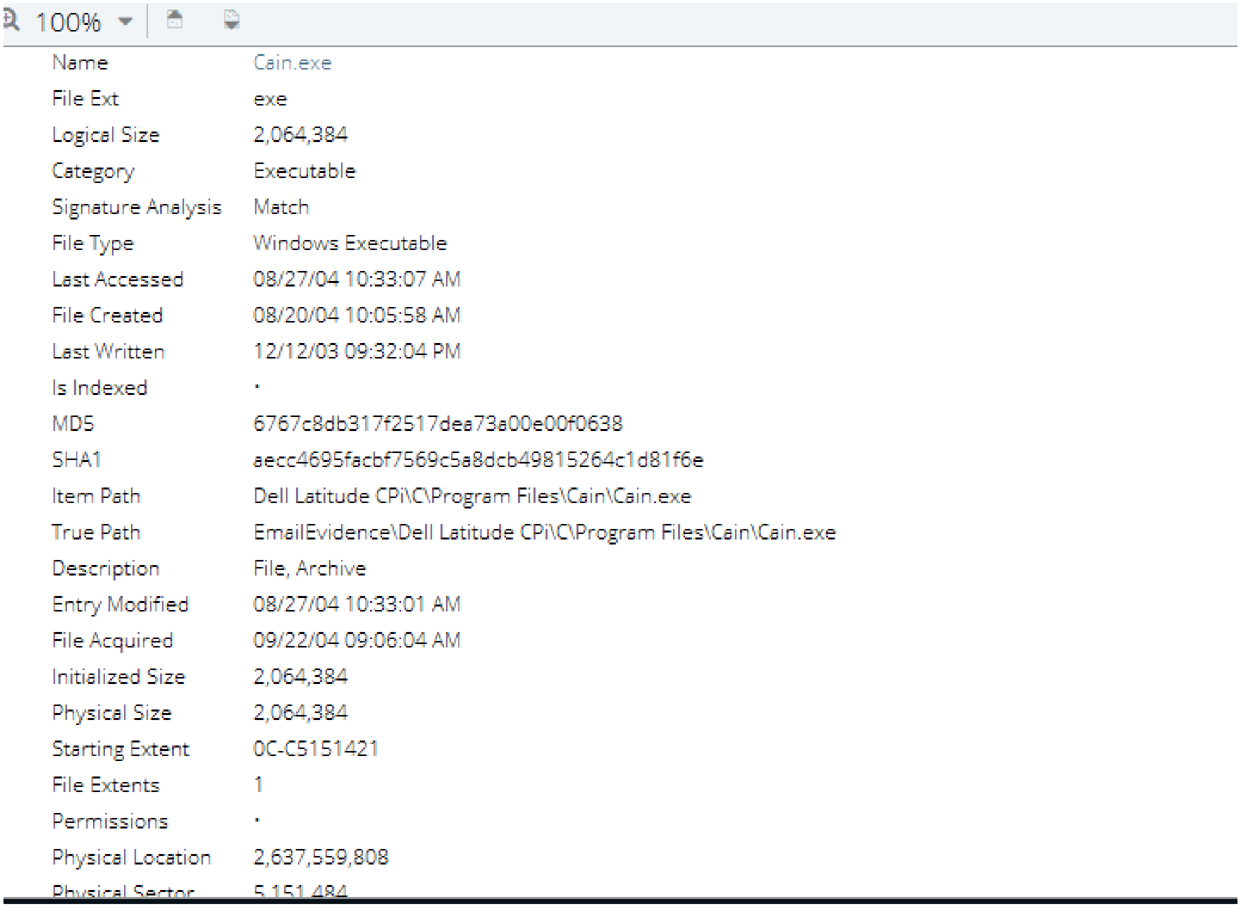
Item Path	Dell Latitude CPi\C\Program Files\Cain
File Created	08/20/04 10:05:58 AM
Last Written	08/25/04 11:20:19 AM
Last Accessed	08/27/04 10:14:45 AM
MD5	4b463522e1f3c186f9a1d87fffab99ce

Protected
Comment

4) Cain v2.5.lnk

Item Path	Dell Latitude CPi\C\Documents and Settings\Mr. Evil\Desktop\Tools\Cain v2.5.lnk
File Created	08/20/04 10:06:01 AM
Last Written	08/20/04 10:06:01 AM
Last Accessed	08/27/04 10:34:52 AM
MD5	61aa7bac7db3da50b0ee53da442d6d64
Start Sector	389,093
Sector offset	261
File Offset	261
Length	331
Comment	Cain hacker software

```
 Cain.exe  (     ï¾ 1Àx    C a i n . e x e       M              -       L
›±l     C:\Program Files\Cain\Cain.exe    C a i n   v 2 . 5 $ . . \ . . \ . . \ P r o g r
 a m   F i l e s \ C a i n \ C a i n . e x e   C : \ P r o g r a m   F i l e s \ C a i n
 C : \ P r o g r a m   F i l e s \ C a i n \ C a i n . e x e
```



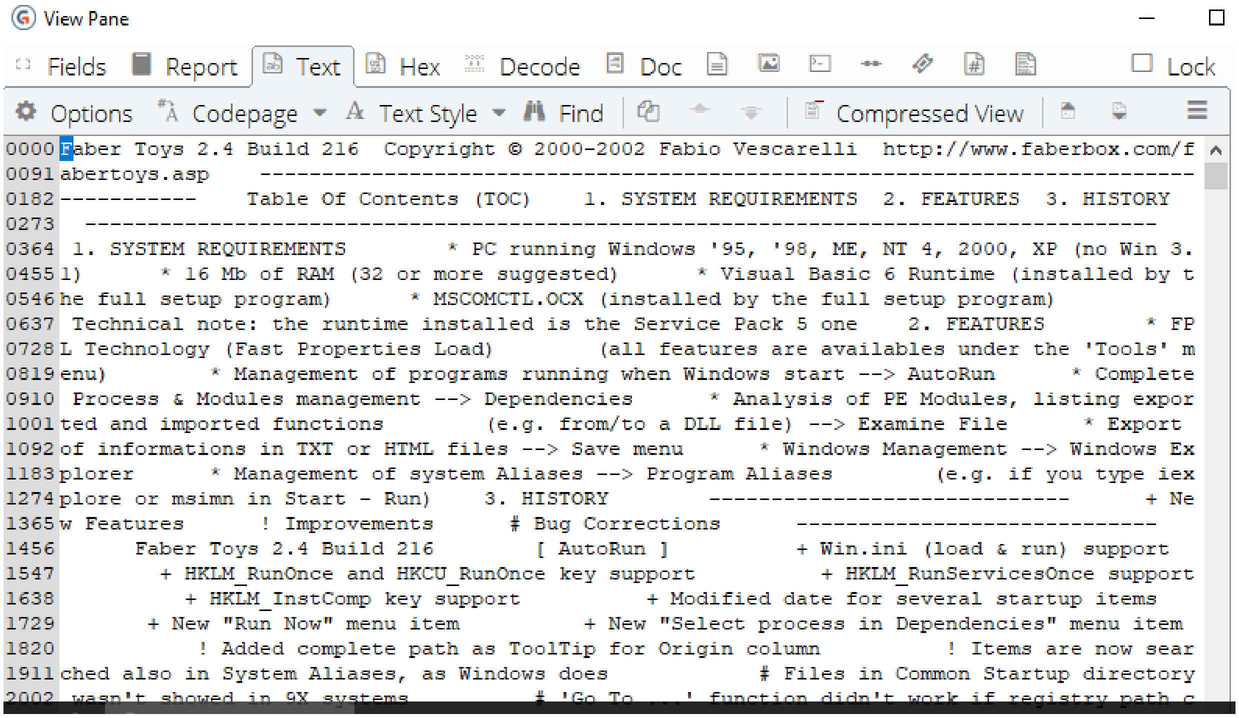
Name	Cain.exe
File Ext	exe
Logical Size	2,064,384
Category	Executable
Signature Analysis	Match
File Type	Windows Executable
Last Accessed	08/27/04 10:33:07 AM
File Created	08/20/04 10:05:58 AM
Last Written	12/12/03 09:32:04 PM
Is Indexed	·
MD5	6767c8db317f2517dea73a00e00f0638
SHA1	aecc4695facbf7569c5a8dcb49815264c1d81f6e
Item Path	Dell Latitude CPi\C\Program Files\Cain\Cain.exe
True Path	EmailEvidence\Dell Latitude CPi\C\Program Files\Cain\Cain.exe
Description	File, Archive
Entry Modified	08/27/04 10:33:01 AM
File Acquired	09/22/04 09:06:04 AM
Initialized Size	2,064,384
Physical Size	2,064,384
Starting Extent	0C-C5151421
File Extents	1
Permissions	·
Physical Location	2,637,559,808
Physical Sector	5,151,484

5) Faber Toys.lnk

Item Path	Dell Latitude CPi\C\Documents and Settings\Mr. Evil\Desktop\Tools\Faber Toys.lnk
File Created	08/20/04 10:07:24 AM
Last Written	08/20/04 10:07:24 AM
Last Accessed	08/25/04 10:27:30 AM
MD5	65dfc6bcfa5f304166333d6d5f2a1886

Start Sector	686,555
Sector offset	379
File Offset	379
Length	330
Comment	Fabor Toys Hacker Software

```
    ›±l     C:\Program Files\Faber Toys\Faber Toys.exe  0 . . \ . . \ . . \ P r o g r a m
   F i l e s \ F a b e r   T o y s \ F a b e r   T o y s . e x e   C : \ P r o g r a m   F
 i l e s \ F a b e r   T o y s           &   w   `        X       n-1a9odn6zxk4lq f¼Mv¿Îá@ %f
‹ù ½‰ôžÒSºòØ °ù  ¤“> f¼Mv¿Îá@ %f‹ù ½‰ôžÒSºòØ °ù  ¤“>
```

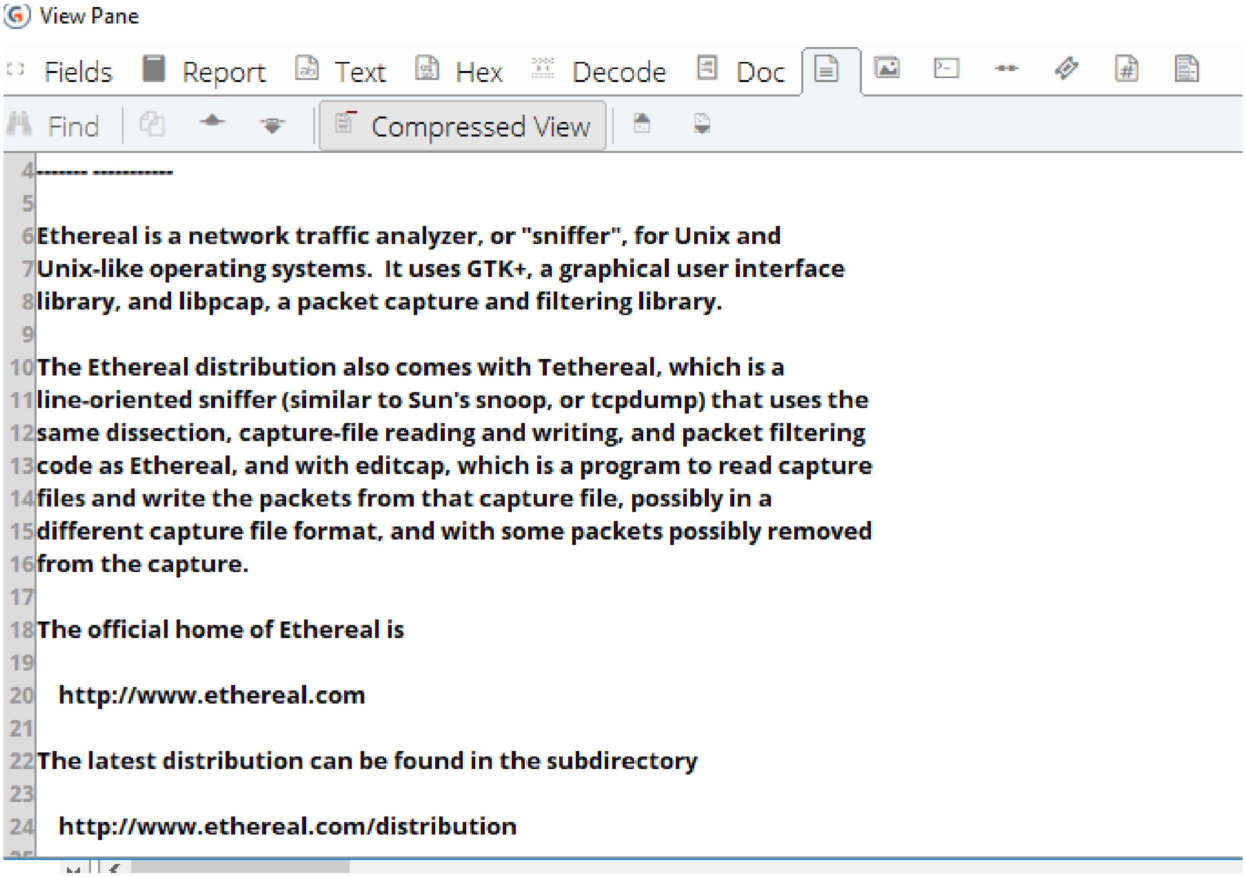


```
0000 Faber Toys 2.4 Build 216  Copyright © 2000-2002 Fabio Vescarelli  http://www.faberbox.com/f
0091 abertoys.asp    --------------------------------------------------------------------------
0182 -----------    Table Of Contents (TOC)    1. SYSTEM REQUIREMENTS  2. FEATURES  3. HISTORY
0273  ---------------------------------------------------------------------------------------
0364  1. SYSTEM REQUIREMENTS        * PC running Windows '95, '98, ME, NT 4, 2000, XP (no Win 3.
0455 1)       * 16 Mb of RAM (32 or more suggested)      * Visual Basic 6 Runtime (installed by t
0546 he full setup program)      * MSCOMCTL.OCX (installed by the full setup program)
0637  Technical note: the runtime installed is the Service Pack 5 one    2. FEATURES        * FP
0728 L Technology (Fast Properties Load)        (all features are availables under the 'Tools' m
0819 enu)       * Management of programs running when Windows start --> AutoRun       * Complete
0910  Process & Modules management --> Dependencies      * Analysis of PE Modules, listing expor
1001 ted and imported functions        (e.g. from/to a DLL file) --> Examine File      * Export
1092 of informations in TXT or HTML files --> Save menu      * Windows Management --> Windows Ex
1183 plorer       * Management of system Aliases --> Program Aliases        (e.g. if you type iex
1274 plore or msimn in Start - Run)    3. HISTORY       -----------------------------      + Ne
1365 w Features       ! Improvements      # Bug Corrections      -----------------------------
1456       Faber Toys 2.4 Build 216        [ AutoRun ]          + Win.ini (load & run) support
1547         + HKLM_RunOnce and HKCU_RunOnce key support         + HKLM_RunServicesOnce support
1638           + HKLM_InstComp key support          + Modified date for several startup items
1729        + New "Run Now" menu item          + New "Select process in Dependencies" menu item
1820            ! Added complete path as ToolTip for Origin column          ! Items are now sear
1911 ched also in System Aliases, as Windows does           # Files in Common Startup directory
2002  wasn't showed in 9X systems          # 'Go To ...' function didn't work if registry path c
```

6) Ethereal.lnk

Item Path	Dell Latitude CPi\C\Documents and Settings\Mr. Evil\Desktop\Tools\Ethereal.lnk
File Created	08/27/04 10:29:44 AM
Last Written	08/27/04 10:29:44 AM
Last Accessed	08/27/04 10:34:54 AM
MD5	9a5f7343c4660695f9a3aba02bcc41ba
Start Sector	2,123,208
Sector offset	168
File Offset	384
Length	202
Comment	Ethereal Hacker Software

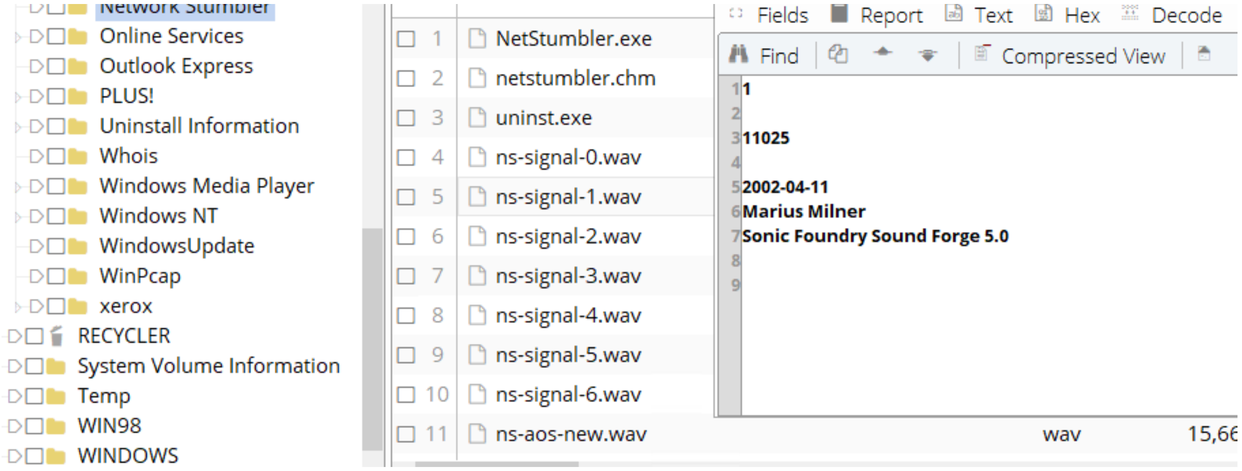
```
C:\Program Files\Ethereal\ethereal.exe  , . . \ . . \ . . \ P r o g r a m   F i l e s \ E
t h e r e a l \ e t h e r e a l . e x e " C : \ D o c u m e n t s   a n d   S e t i n g
s \ M r .   E v i l
```



```
------- -----------

Ethereal is a network traffic analyzer, or "sniffer", for Unix and
Unix-like operating systems.  It uses GTK+, a graphical user interface
library, and libpcap, a packet capture and filtering library.

The Ethereal distribution also comes with Tethereal, which is a
line-oriented sniffer (similar to Sun's snoop, or tcpdump) that uses the
same dissection, capture-file reading and writing, and packet filtering
code as Ethereal, and with editcap, which is a program to read capture
files and write the packets from that capture file, possibly in a
different capture file format, and with some packets possibly removed
from the capture.

The official home of Ethereal is

   http://www.ethereal.com

The latest distribution can be found in the subdirectory

   http://www.ethereal.com/distribution
```

7) Network Stumbler

Item Path	Dell Latitude CPi\C\Program Files\Network Stumbler
File Created	08/27/04 10:12:15 AM
Last Written	08/27/04 10:12:16 AM
Last Accessed	08/27/04 10:14:45 AM
MD5	e0a166447fcd10c4102fa78430147916
Protected	
Comment	



1	NetStumbler.exe	
2	netstumbler.chm	
3	uninst.exe	
4	ns-signal-0.wav	
5	ns-signal-1.wav	
6	ns-signal-2.wav	
7	ns-signal-3.wav	
8	ns-signal-4.wav	
9	ns-signal-5.wav	
10	ns-signal-6.wav	
11	ns-aos-new.wav	wav 15,66

```
1

11025

2002-04-11
Marius Milner
Sonic Foundry Sound Forge 5.0
```

8) README.DOC

Item Path	Dell Latitude CPi\C\My Documents\ARCHIVE\Pkzip\README.DOC

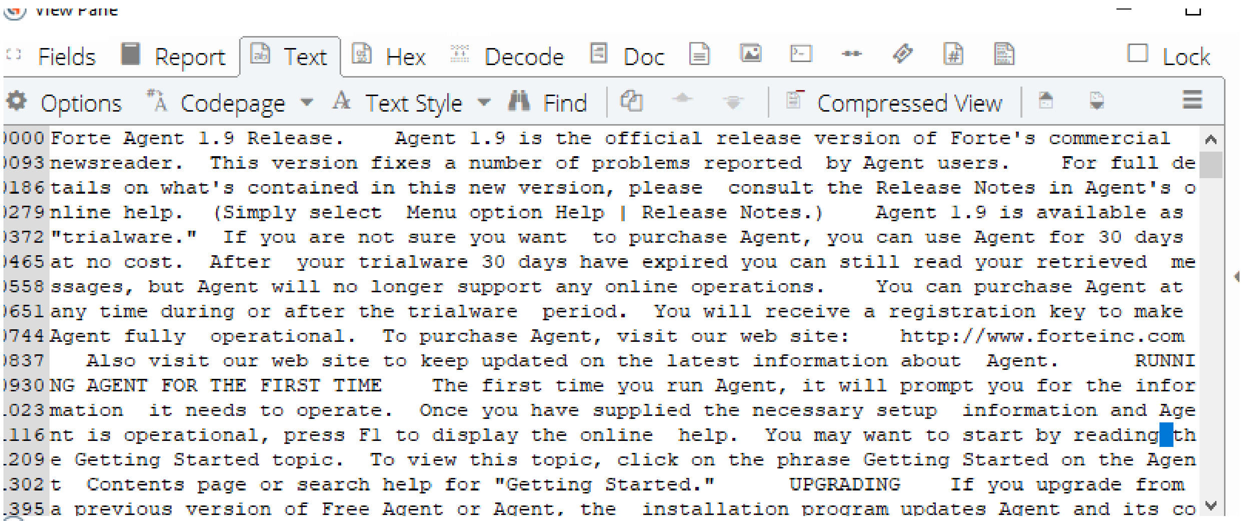
File Created	08/20/04 10:18:09 AM
Last Written	02/01/93 11:04:16 PM
Last Accessed	08/20/04 10:18:09 AM
MD5	a582843d97d6b40cdd1cd64f1c1491f2
Start Sector	
Sector offset	
File Offset	2
Length	709
Comment	hacker software

```
This diskette contains the file PKZ204g.EXE.  Type

PKZ204g

followed by pressing the Enter key to create the program and
documentation files for PKUNZIP, PKZIP, and PKSFX version 2.04g
To print the documentation files after running PKZ204g, type

COPY *.DOC PRN
COPY *.NEW PRN
COPY *.204 PRN
COPY *.TXT PRN

following each line by the return key.


See the files V204G.NEW, WHATSNEW.204 and ADDENDUM.DOC for more
information about features and changes made in this version of
the software.

If you distribute PKUNZIP, PKZIP, and PKSFX to friends, associates,
or to a computer bulletin board system (BBS), please distribute the
file PKZ204g.EXE rather than the individual files for PKUNZIP, PKZIP
and PKSFX.
```

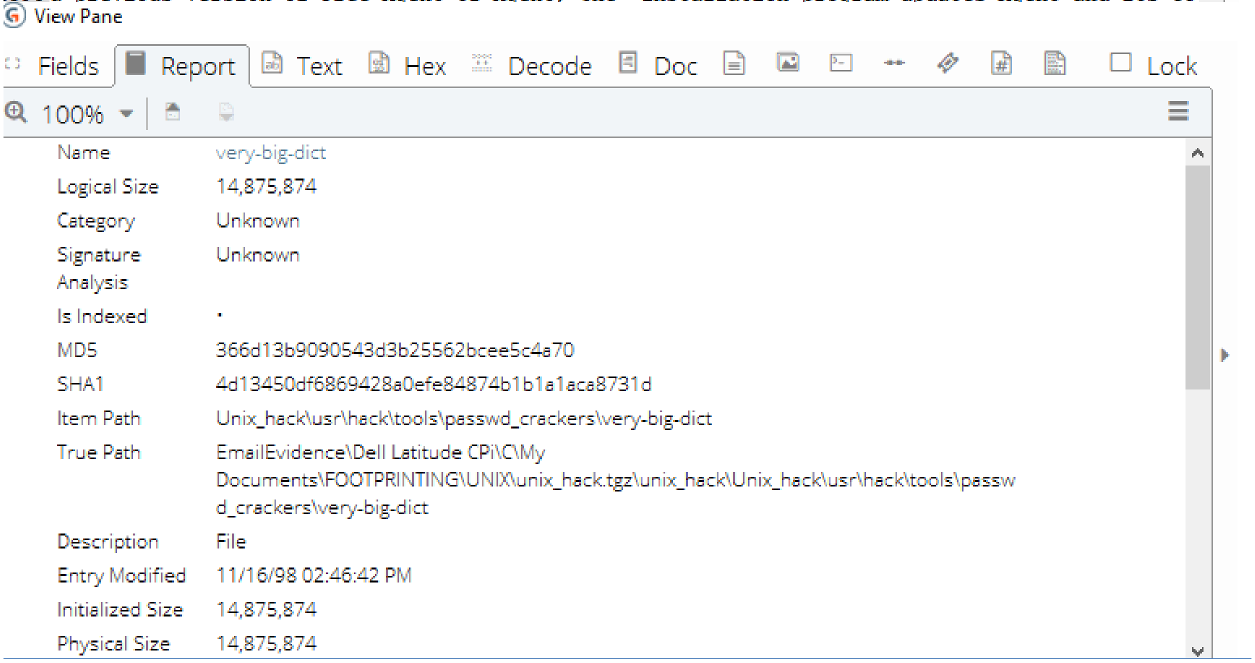
9) SHAREWAR.DOC

Item Path	Dell Latitude CPi\C\My Documents\ARCHIVE\Pkzip\SHAREWAR.DOC
File Created	08/20/04 10:18:09 AM
Last Written	02/01/93 11:04:16 PM
Last Accessed	08/20/04 10:18:09 AM
MD5	c5b0569e869325a1d7f798b17dde8e41
Start Sector	
Sector offset	
File Offset	0
Length	444
Comment	shareware

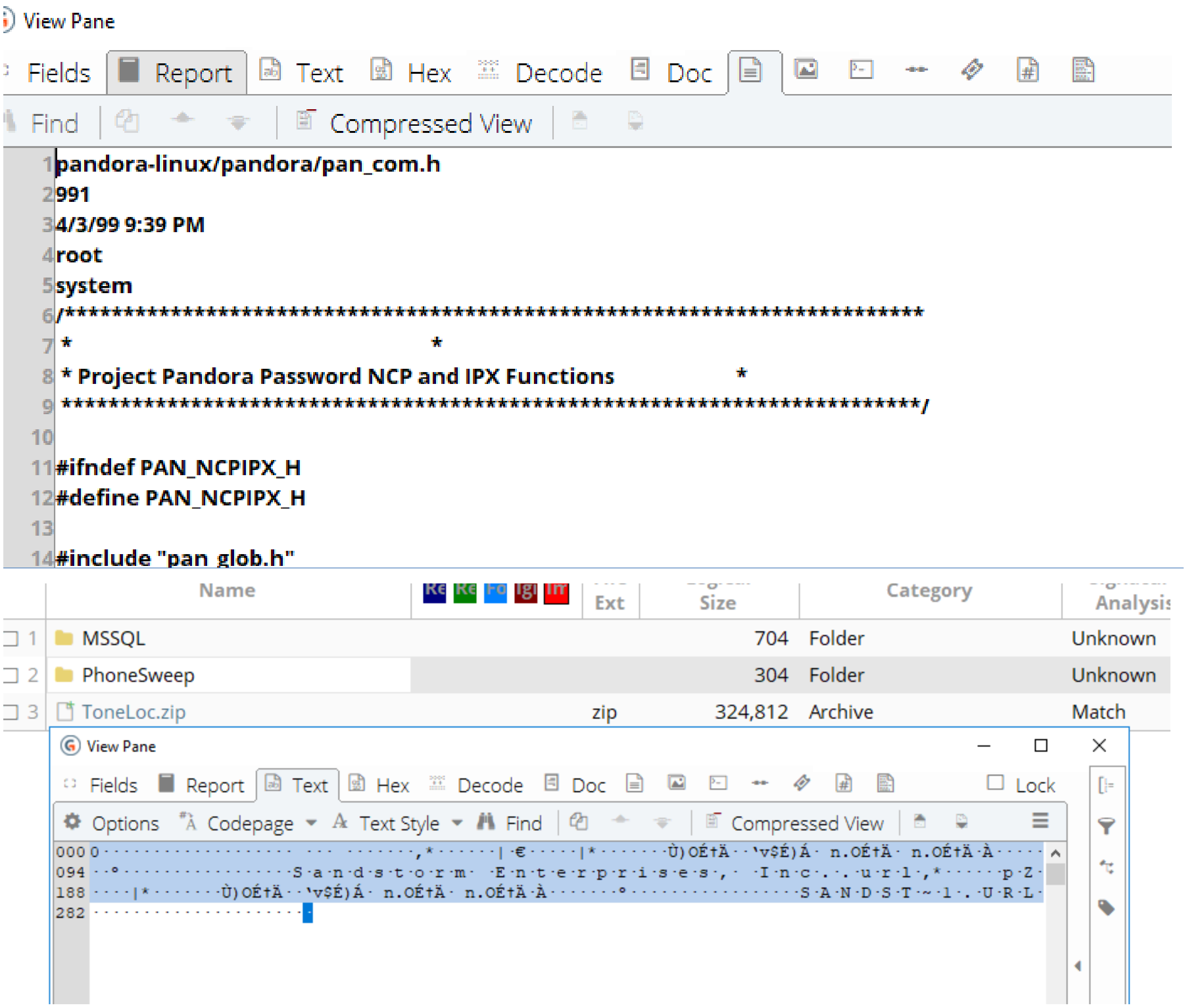
```
 BENEFITS OF REGISTRATION
 --------------------------------------------------------------

 PKZIP is Shareware, and if you use PKZIP regularly we strongly
 encourage you to register it.  With registration you will receive
 the latest version of the software, a comprehensive printed manual,
 one free upgrade of PKZIP, PKUNZIP & PKSFX, premium access to
 the PKWARE Support BBS and an optional Authenticity Verification
 Name and Serial Number.
```



```
000 Forte Agent 1.9 Release.    Agent 1.9 is the official release version of Forte's commercial
093 newsreader.  This version fixes a number of problems reported  by Agent users.    For full de
186 tails on what's contained in this new version, please  consult the Release Notes in Agent's o
279 nline help.  (Simply select  Menu option Help | Release Notes.)    Agent 1.9 is available as
372 "trialware."  If you are not sure you want  to purchase Agent, you can use Agent for 30 days
465 at no cost.  After  your trialware 30 days have expired you can still read your retrieved  me
558 ssages, but Agent will no longer support any online operations.    You can purchase Agent at
651 any time during or after the trialware  period.  You will receive a registration key to make
744 Agent fully  operational.  To purchase Agent, visit our web site:    http://www.forteinc.com
837    Also visit our web site to keep updated on the latest information about  Agent.      RUNNI
930 NG AGENT FOR THE FIRST TIME    The first time you run Agent, it will prompt you for the infor
023 mation  it needs to operate.  Once you have supplied the necessary setup  information and Age
116 nt is operational, press F1 to display the online  help.  You may want to start by reading th
209 e Getting Started topic.  To view this topic, click on the phrase Getting Started on the Agen
302 t  Contents page or search help for "Getting Started."      UPGRADING    If you upgrade from
395 a previous version of Free Agent or Agent, the  installation program updates Agent and its co
```



Name	very-big-dict
Logical Size	14,875,874
Category	Unknown
Signature Analysis	Unknown
Is Indexed	·
MD5	366d13b9090543d3b25562bcee5c4a70
SHA1	4d13450df6869428a0efe84874b1b1a1aca8731d
Item Path	Unix_hack\usr\hack\tools\passwd_crackers\very-big-dict
True Path	EmailEvidence\Dell Latitude CPi\C\My Documents\FOOTPRINTING\UNIX\unix_hack.tgz\unix_hack\Unix_hack\usr\hack\tools\passwd_crackers\very-big-dict
Description	File
Entry Modified	11/16/98 02:46:42 PM
Initialized Size	14,875,874
Physical Size	14,875,874



```
pandora-linux/pandora/pan_com.h
991
4/3/99 9:39 PM
root
system
/*************************************************************************
 *                                          *
 * Project Pandora Password NCP and IPX Functions               *
 *************************************************************************/

#ifndef PAN_NCPIPX_H
#define PAN_NCPIPX_H

#include "pan_glob.h"
```

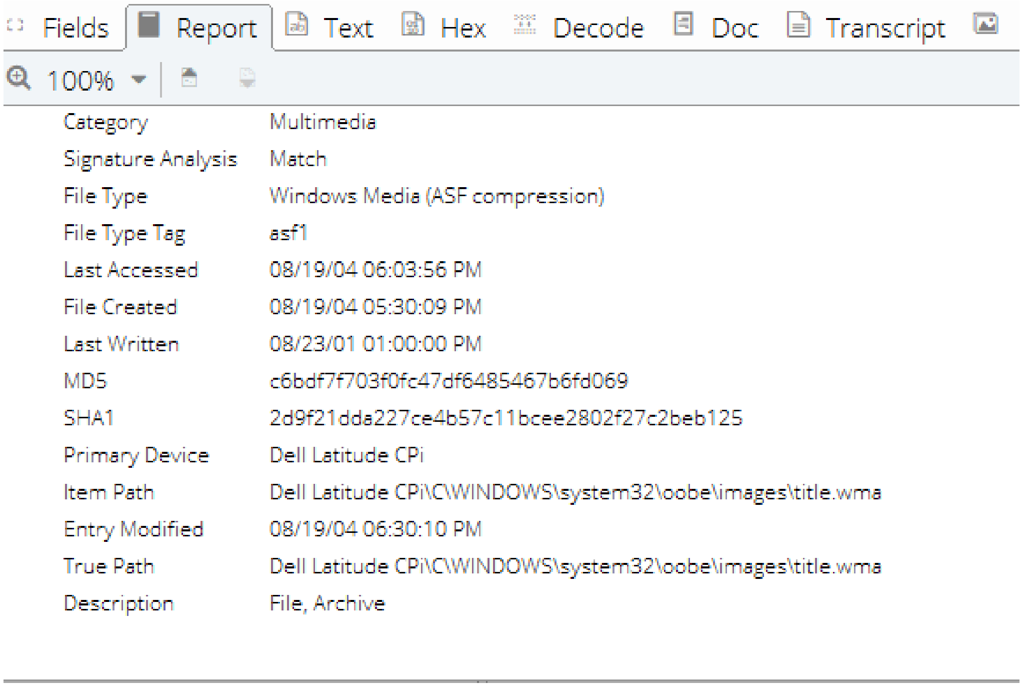
	Name	Ext	Size	Category	Analysis
1	MSSQL		704	Folder	Unknown
2	PhoneSweep		304	Folder	Unknown
3	ToneLoc.zip	zip	324,812	Archive	Match

```
000 0·················· ··· ·······,*······|·€·····|*·······Ù)OÉ†Ä··'v$É)Á· n.OÉ†Ä· n.OÉ†Ä·À·····
094 ··°·················S·a·n·d·s·t·o·r·m· E·n·t·e·r·p·r·i·s·e·s·,· I·n·c·.·.·u·r·l·,*······p·Z·
188 ····|*·······Ù)OÉ†Ä··'v$É)Á· n.OÉ†Ä· n.OÉ†Ä·À·······°··················S·A·N·D·S·T·~·1·.·U·R·L·
282 ······················
```

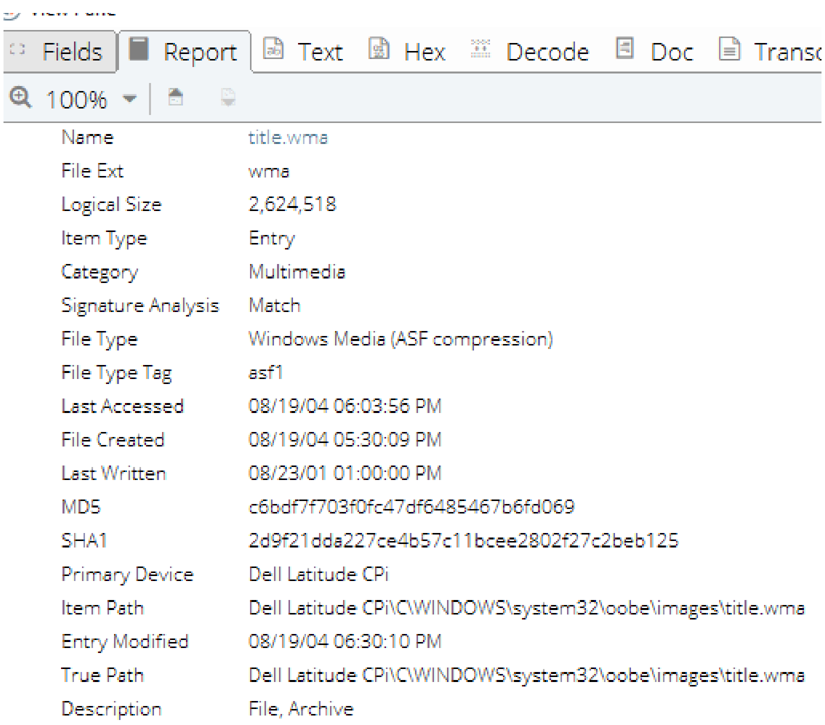
The phoneSweep program is a hacker tool that can steal all data from a cell phone device. This application was found under programs files stored in the computer

The multimedia snapshots below are video files that can be retrieved through the user’s personal files such as downloaded video content or personal folders such as images. Specifically, these files were found in images and the link is Windows media wma.

Multimedia Content



Category	Multimedia
Signature Analysis	Match
File Type	Windows Media (ASF compression)
File Type Tag	asf1
Last Accessed	08/19/04 06:03:56 PM
File Created	08/19/04 05:30:09 PM
Last Written	08/23/01 01:00:00 PM
MD5	c6bdf7f703f0fc47df6485467b6fd069
SHA1	2d9f21dda227ce4b57c11bcee2802f27c2beb125
Primary Device	Dell Latitude CPi
Item Path	Dell Latitude CPi\C\WINDOWS\system32\oobe\images\title.wma
Entry Modified	08/19/04 06:30:10 PM
True Path	Dell Latitude CPi\C\WINDOWS\system32\oobe\images\title.wma
Description	File, Archive



Name	title.wma
File Ext	wma
Logical Size	2,624,518
Item Type	Entry
Category	Multimedia
Signature Analysis	Match
File Type	Windows Media (ASF compression)
File Type Tag	asf1
Last Accessed	08/19/04 06:03:56 PM
File Created	08/19/04 05:30:09 PM
Last Written	08/23/01 01:00:00 PM
MD5	c6bdf7f703f0fc47df6485467b6fd069
SHA1	2d9f21dda227ce4b57c11bcee2802f27c2beb125
Primary Device	Dell Latitude CPi
Item Path	Dell Latitude CPi\C\WINDOWS\system32\oobe\images\title.wma
Entry Modified	08/19/04 06:30:10 PM
True Path	Dell Latitude CPi\C\WINDOWS\system32\oobe\images\title.wma
Description	File, Archive

References

Choi, K. (2015). *Cybercriminology and Digital Investigation.* LFB Scholarly Publishing LLC.

Choi, K. (2015). Module 4 *Electronic Vandalism Criminal Patterns and Countermeasures.* [Lecture Notes]. MET CJ 710 01: Applied Digital Forensic Investigation (2021 Spring 1) https://onlinecampus.bu.edu.