

Lecture 5: Data Hiding Forensics and Anti Forensics

INTRODUCTION

- ❑ Over the last years, al-Qaeda manuals have been found to contain techniques for covert communications using steganography programs and techniques.
- ❑ On May 16th, 2011, an Austrian was questioned for hiding a digital storage device and memory cards that contains a video with over 100 files hidden in it using steganography techniques and protected with a password.

ANTI-FORENSICS HIDING YOUR TRACKS

- ❑ Anti-forensics include **all techniques related to hiding the truth** of using a **steganography tool** on the suspect machine.

- ❑ It also **includes all the protective measures** that can be used in **order to delete user traces on the target's** machine like
 - Internet activities,
 - IP addresses,
 - last-used programs



Users Of Computer Anti-Forensics

❑ we cannot say that this branch of computer security is dedicated only to criminals.

❑ Legitimate users of computer anti-forensics tools are:

1. Diplomats
2. Journalists
3. Human rights activists
4. Military and defense personnel

ANTI-FORENSICS HIDING YOUR TRACKS

- ☐ Do not leave the original carrier
- ☐ Do not leave the carrier file with the hidden message (Stego)
- ☐ Remove evidence of the data hiding program
- ☐ Use a strong password in the data hiding program
- ☐ Storing the data hiding program and carrier files **on removable storage.**
- ☐ choose a custom-made digital photograph (not Google)

Data Hiding Passwords

- ❑ Use strong passwords when hiding a message within a carrier file.

- ❑ Common recommendations include:

- Use a password different from the operating system password, not stored passwords in the browser, or passwords used for network services.

- Use a combination of upper/lower alphanumeric characters and special characters.

- Use a program to secure your passwords
E.g, PasswordSafe: <https://pwsafe.org/>

Data Hiding Passwords

Using one or more **special characters** in your password will allow you to avoid many types of brute force password cracking programs.

–Examples:

–[CTRL]+[ALT]+[C] gives ©

–[CTRL]+[ALT]+[R] gives ®

–[CTRL]+[ALT]+[T] gives ™

Hiding Your Tracks

- ❑ In Windows, you can use the **cleanmgr** utility to wipe **your system clean of any remaining evidence of data hiding software.**

From the command line, simply run: `c:\cleanmgr2`

- ❑ This will prompt **the user to pick a drive to cleanse.**

Hiding Your Tracks







The **command** will clean the following:

- Temporary Internet Files.
- Temporary Setup Files.
- Temporary Offline Files.
- Downloaded Program Files.
- Empty the Recycle Bin.

Hiding Your Tracks

Windows also keeps track of every program that you run and places the most frequently run programs in the Start Panel.

- ☐ clear this list of programs
- ☐ –Right click on the taskbar
- ☐ –Uncheck :
 - Show recently added apps
 - Show most used apps
 - Show recently opened items

 HomeFind a setting **Personalization** Background Colors Lock screen Themes Fonts Start Taskbar

Start

Show more tiles on Start

☐ Off

Show app list in Start menu

☒ On

Show recently added apps

☐ Off

Show most used apps

☐ Off

Show suggestions occasionally in Start

☒ On

Use Start full screen

☐ OffShow recently opened items in Jump Lists on Start or the taskbar
and in File Explorer Quick Access☒ On[Choose which folders appear on Start](#)

Digital FORENSICS

- ❑ **Digital forensics** is a branch of forensic science that uses scientific knowledge for collecting, analyzing, and presenting evidence for use in a court of law.
- ❑ The term “digital forensics” has expanded to cover investigating all devices that are capable of storing digital data such as mobile phones, cameras, and magnetic media like CDs and DVDs for offline storage

Data Hiding FORENSICS

- ❑ There are a variety of ways to detect if a suspect system contains data hiding software.
- ❑ These options may include:
 - Data hiding software applications still exist on the suspect computer.
 - Cached website pages indicate the suspect accessed web pages that provide data hiding software.
 - Remaining artifacts indicated that data hiding software was once installed or used on the system.

Looking for Data Hiding Software

- ❑ Everything from viewing the installed programs to searching directories may reveal installed packages.
- ❑ For example, in Ubuntu Linux you can obtain a list of installed packages by running:

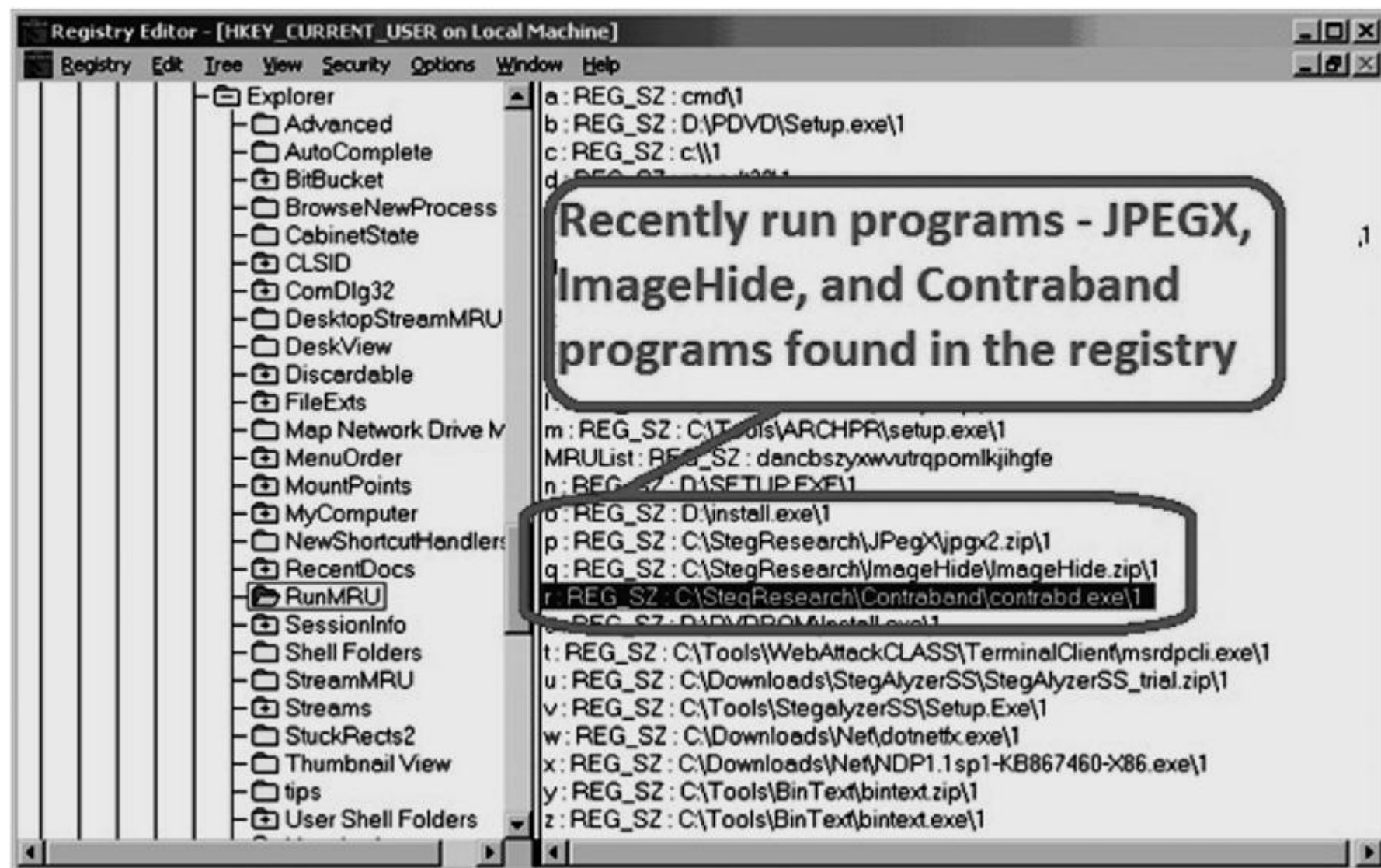
```
# sudo dpkg --get-selections > listofpkgs
```

Looking for Data Hiding Software

- ❑ Some data hiding programs don't require any installation whatsoever, and as a result can be run from a CD, floppy, thumb drive etc.
- ❑ To view the Most Recently Used (MRU) programs in Windows, simply run **regedit** and view the following key:

User Key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU



Finding Remaining Artifacts

- ❑ experienced **users delete** the data hiding program after use, **or run it from removable** media.
- ❑ Both may **leave trace evidence** that can be extremely useful during an investigation.

Finding Remaining Artifacts

Various organizations such as the **Department of Defense (DoD)** and **National Institute of Standards and Technology (NIST)** have created **file hashes** for common *.dll's and other files created during the installation of the data hiding software.

Finding Remaining Artifacts

- ❑ Software packages now exist that allow an investigator to scan a machine for these files and compare the hashes to determine if a data hiding program was once installed.
- ❑ These programs can sometimes also look for artifacts left behind in the registry, even after the data hiding program has been removed.

WetStone Technologies StegoHunt™

❑ **StegoHunt**Software provides investigators with:

- The ability to search for known Steganography / Data Hiding programs
- The ability to identify carrier files (images, audio, video, and documents) that contain hidden information.



StegoHunt

Your Price: \$2,100.00

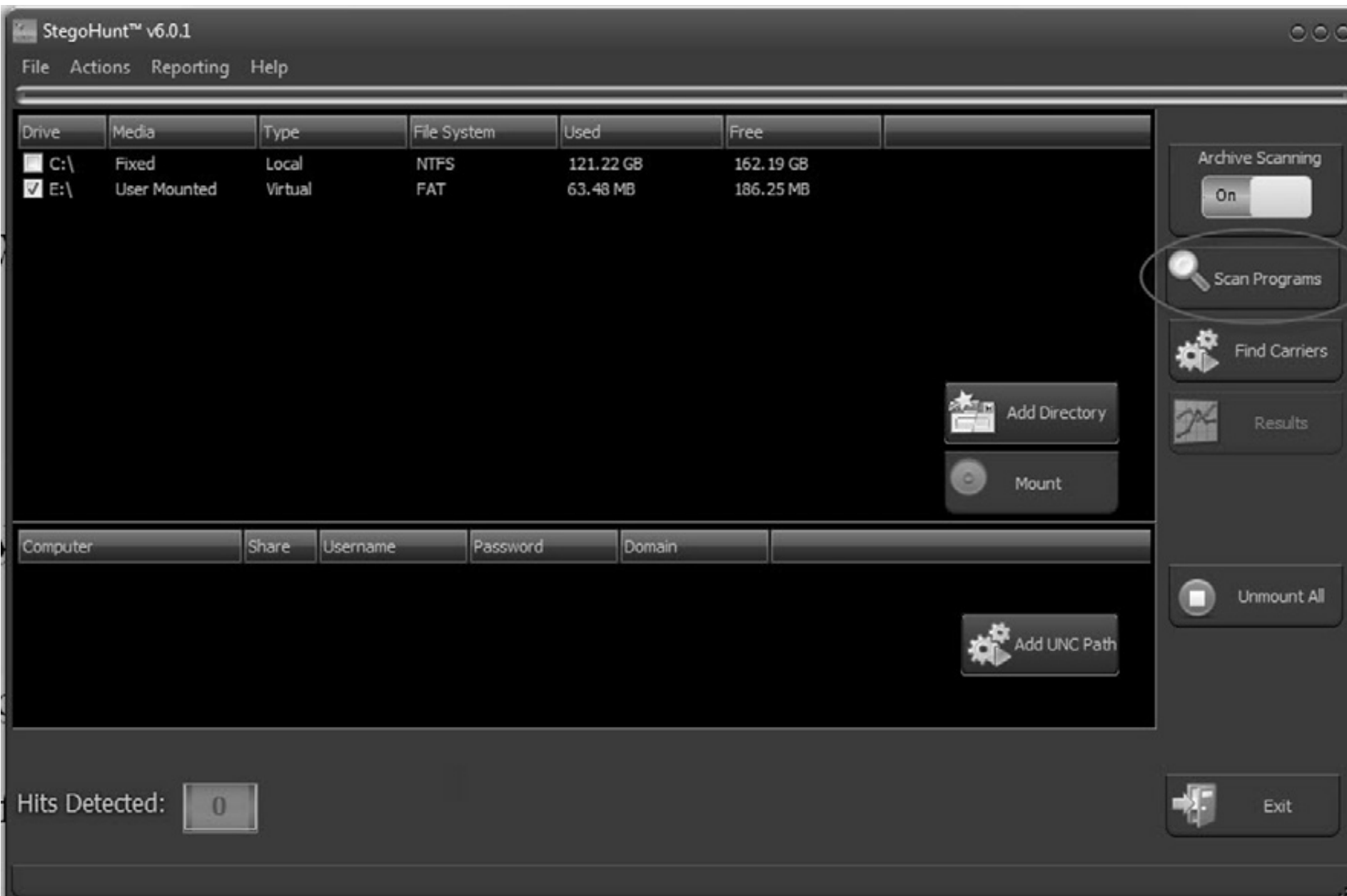
Part Number: STGOHNT

Availability: This item is currently in stock. Free Shipping.

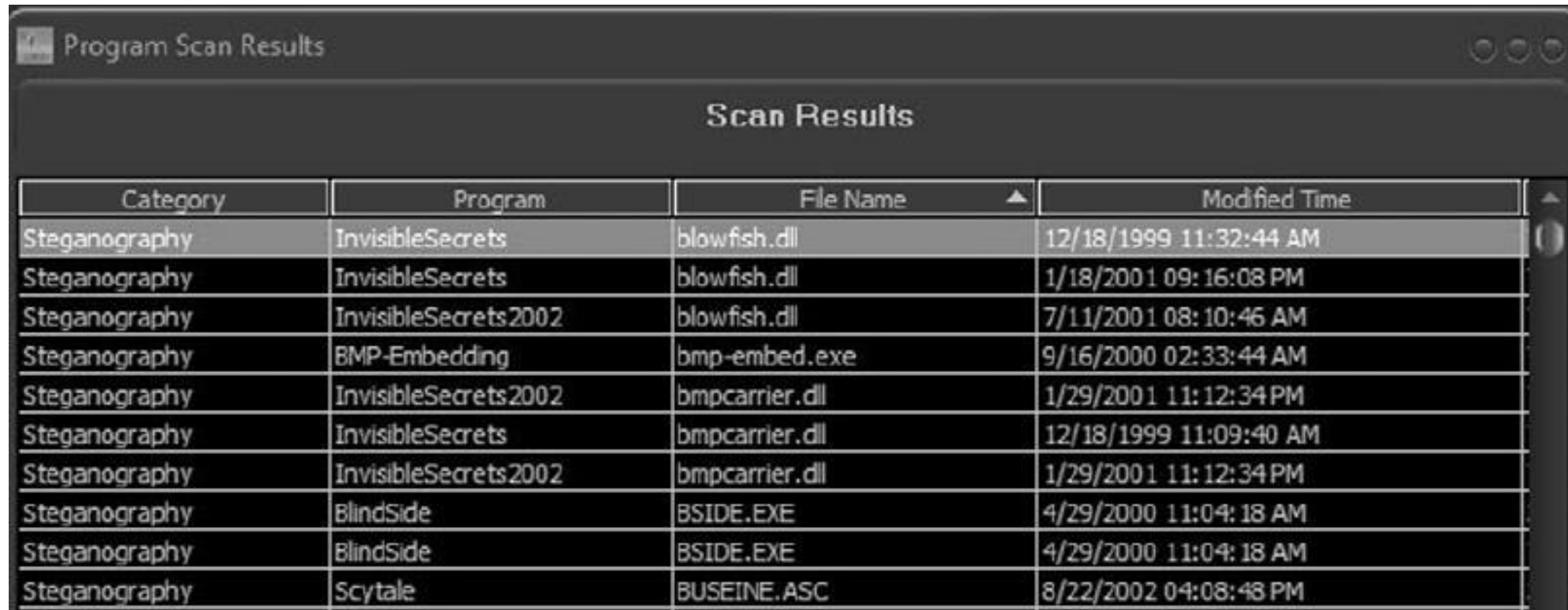
Quantity

1	+
	-

 ADD TO CART



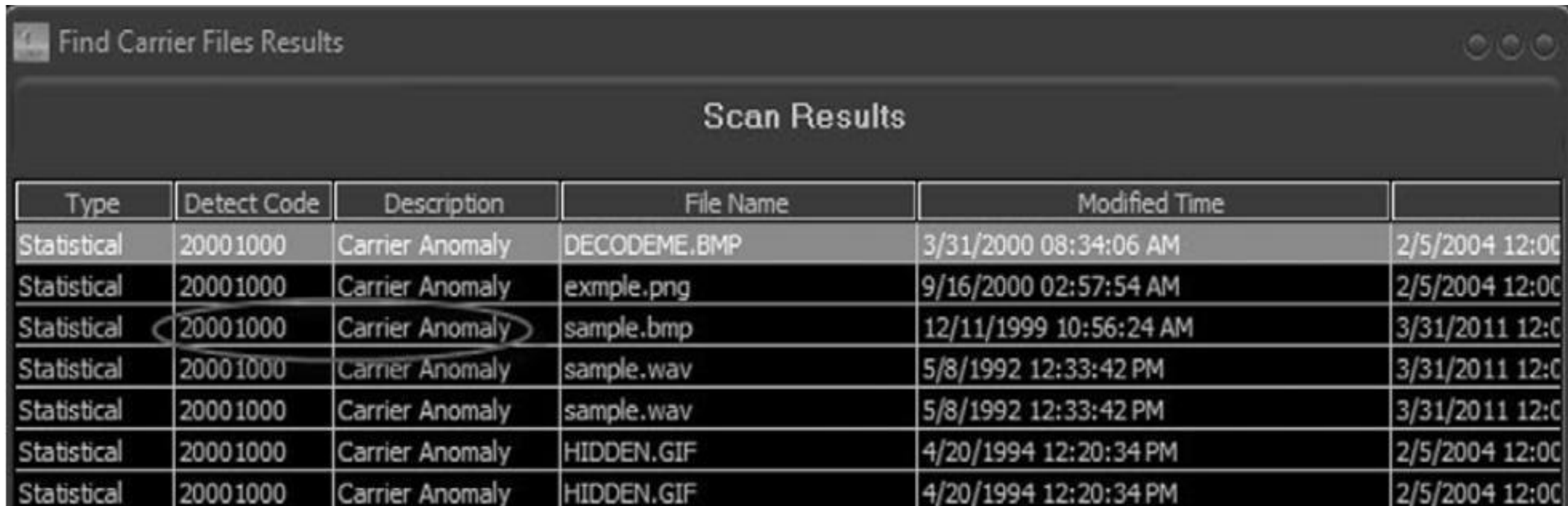
Once the scan completes, StegoHunt provides detailed results either in printable reports or a results grid



The screenshot shows a window titled "Program Scan Results" with a sub-header "Scan Results". Below the header is a table with four columns: "Category", "Program", "File Name", and "Modified Time". The table contains ten rows of data, all categorized as "Steganography". The programs listed are InvisibleSecrets, BMP-Embedding, InvisibleSecrets2002, BlindSide, and Scytale. The file names include blowfish.dll, bmpcarrier.dll, BSIDE.EXE, and BUSEINE.ASC. The modified times range from 1999 to 2002.

Category	Program	File Name	Modified Time
Steganography	InvisibleSecrets	blowfish.dll	12/18/1999 11:32:44 AM
Steganography	InvisibleSecrets	blowfish.dll	1/18/2001 09:16:08 PM
Steganography	InvisibleSecrets2002	blowfish.dll	7/11/2001 08:10:46 AM
Steganography	BMP-Embedding	bmp-embed.exe	9/16/2000 02:33:44 AM
Steganography	InvisibleSecrets2002	bmpcarrier.dll	1/29/2001 11:12:34 PM
Steganography	InvisibleSecrets	bmpcarrier.dll	12/18/1999 11:09:40 AM
Steganography	InvisibleSecrets2002	bmpcarrier.dll	1/29/2001 11:12:34 PM
Steganography	BlindSide	BSIDE.EXE	4/29/2000 11:04:18 AM
Steganography	BlindSide	BSIDE.EXE	4/29/2000 11:04:18 AM
Steganography	Scytale	BUSEINE.ASC	8/22/2002 04:08:48 PM

This function invokes a search **for images**, audio, video, and document files that may contain hidden information.















Type	Detect Code	Description	File Name	Modified Time	
Statistical	2000 1000	Carrier Anomaly	DECODEME.BMP	3/31/2000 08:34:06 AM	2/5/2004 12:00
Statistical	2000 1000	Carrier Anomaly	exmple.png	9/16/2000 02:57:54 AM	2/5/2004 12:00
Statistical	2000 1000	Carrier Anomaly	sample.bmp	12/11/1999 10:56:24 AM	3/31/2011 12:00
Statistical	2000 1000	Carrier Anomaly	sample.wav	5/8/1992 12:33:42 PM	3/31/2011 12:00
Statistical	2000 1000	Carrier Anomaly	sample.wav	5/8/1992 12:33:42 PM	3/31/2011 12:00
Statistical	2000 1000	Carrier Anomaly	HIDDEN.GIF	4/20/1994 12:20:34 PM	2/5/2004 12:00
Statistical	2000 1000	Carrier Anomaly	HIDDEN.GIF	4/20/1994 12:20:34 PM	2/5/2004 12:00

Identifying and View Cached Images

- ❑ An investigator can attempt to **identify websites** commonly known for providing data hiding software.
- ❑ It is also **important to determine** if the suspect was a member of **any online chat** groups to determine posts that may be relevant to the investigation.

STG Cache Audit

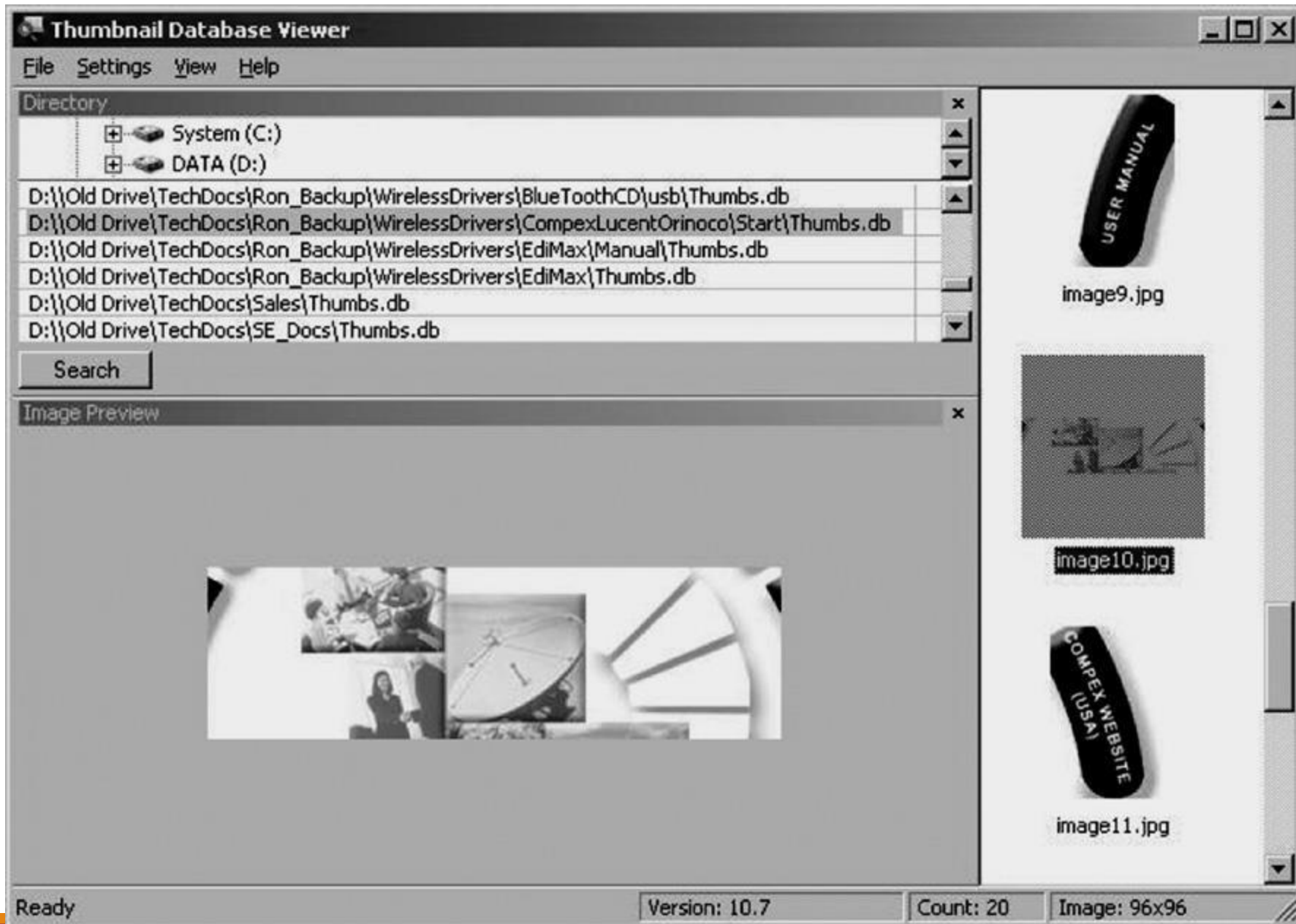
- ❑ STG Cache Audit is an advanced cache, cookie, and history viewer that runs on Windows and that allows you to investigate web surfing habits of a suspect machine.
- ❑ The “Site View” allows one to see which sites were visited how often.

STG Cache Audit					
File Edit View Mode Options Reports Help					
           					
Sites Found in OBLIVION cache: 40 (10/18/2006 10:13:24 PM)					
URL	Hits	Size (Bytes)	Last Modified	Last Access	
http://us.bc.yahoo.com	10	430		10/18/2006 10:06:03 ...	
http://us.i1.yimg.com	1713	167597	10/18/2006 12:19:55 ...	10/18/2006 10:06:02 ...	
http://us.js2.yimg.com	404	1240131	10/16/2006 5:07:48 PM	10/18/2006 10:06:02 ...	
http://address.mail.yahoo.com	2	13629		10/18/2006 10:06:01 ...	
http://us.f337.mail.yahoo.com	13	401122	10/18/2006 9:03:08 PM	10/18/2006 10:05:55 ...	
http://cdn2.adsdk.com	1	27364	9/7/2005 10:13:03 AM	10/18/2006 10:05:36 ...	
http://us.a2.yimg.com	57	128487	10/16/2006 3:39:32 PM	10/18/2006 10:05:36 ...	
http://m1.2mdn.net	1	12255	6/29/2006 12:02:37 PM	10/18/2006 10:05:33 ...	
http://spe.atdmt.com	13	33873		10/18/2006 10:05:10 ...	
http://content.yieldmanager.com	2	35114	9/7/2006 2:24:28 PM	10/18/2006 10:05:06 ...	
http://csc3-2004-crl.verisign.com	1	39115	10/18/2006 6:00:29 AM	10/18/2006 10:05:04 ...	
http://fpdownload2.macromedia.com	1	1056028	6/22/2006 7:45:08 PM	10/18/2006 10:05:02 ...	
https://login.yahoo.com	1	43	6/22/2006 3:10:07 PM	10/18/2006 10:04:47 ...	
https://a248.e.akamai.net	20	72503	8/25/2006 3:55:40 PM	10/18/2006 10:04:42 ...	
http://p.www.yahoo.com	2	672		10/18/2006 10:04:40 ...	
http://www.yahoo.com	71	102783		10/18/2006 10:04:33 ...	

Evidence in Thumbnails

- ❑ When you open a folder like your My Pictures folder, you can view the files in a thumbnail format, like a bunch of small pictures. These small pictures or thumbnails are stored in a special file called a thumbnail cache database. These thumbnail databases can be read using special software and used as evidence in both civil and criminal cases.
- ❑ Thumbnails are another type of cached information that can be analyzed on a suspect computer.
- ❑ Thumbnails are found in Windows Operating Systems and are intended to allow a quick view of files residing in a folder.

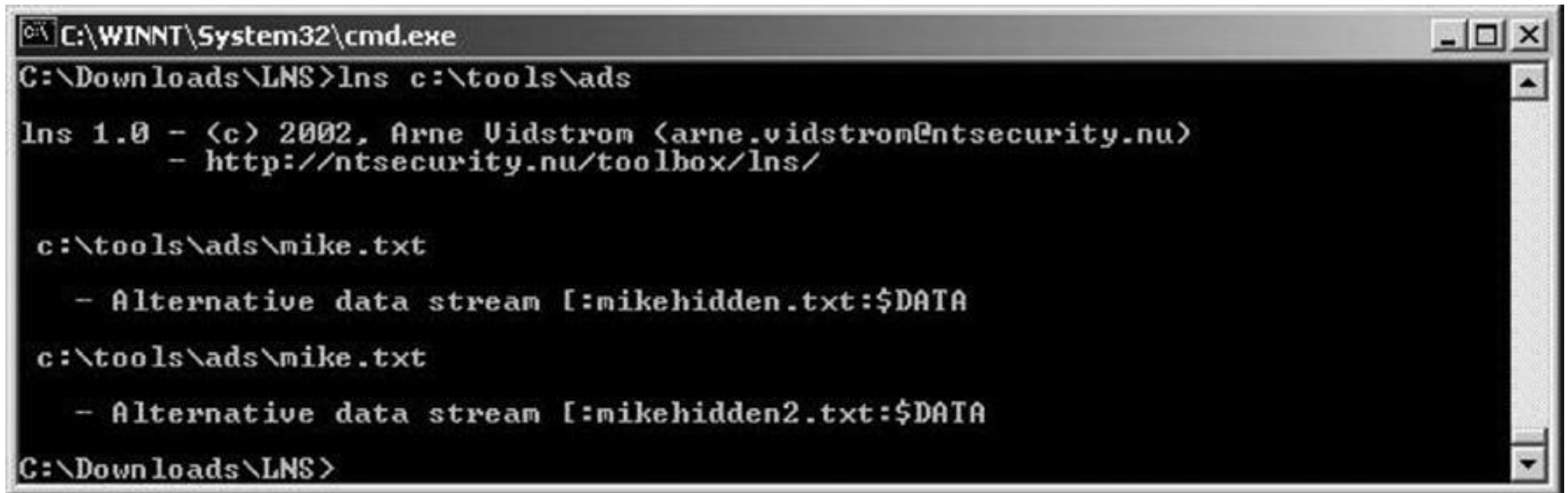
- ❑ To view the thumbnails database, one must first go into Folder Options, select View, and deselect “Hide protected operating system files”.
- ❑ Windows Explorer will then display thumbs.db in the current folder.
- ❑ There are a number of freeware and commercial tools for viewing and analyzing thumbs.db files.



Searching for Hidden Directories and Files

There are a handful of other tools that do allow one to identify files hidden in Alternate Data Streams.

- Let's take a look at LNS.



```
C:\WINNT\System32\cmd.exe
C:\Downloads\LNS>ls c:\tools\ads

ls 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
        - http://ntsecurity.nu/toolbox/ls/

c:\tools\ads\mike.txt
        - Alternative data stream [:mikehidden.txt:$DATA]
c:\tools\ads\mike.txt
        - Alternative data stream [:mikehidden2.txt:$DATA]
C:\Downloads\LNS>
```