Exhibit 1

Crackers are classed as those who break into systems to do damage whereas hackers are those who enjoy taking programs apart just to see how they work. The original description of a hacker was somebody who made furniture with an axe. Like most computer viruses, this method of furniture making was very crude but nonetheless effective.

Viruses are in reality a certain type of computer malware, which is a common term covering all types of malicious software. The most common types of malware are viruses, worms and Trojans.

Viruses

A Computer Virus is normally concealed inside another program such as an installation program delivered via an email attachment. The term Computer Virus came about because of the similarity with biological viruses that require a host organism to live and reproduce, When the host program is run, the Computer Virus program runs at the same time. Once the Computer Virus is in memory it is able to do its dirty work which normally includes infecting other programs on the host computer.

After the infection stage of the Computer Virus, there's a destructive stage. The Computer Virus waits for a pre-determined trigger (such as a specific date or a certain number of times the Computer Virus has replicated itself) before delivering its 'payload'. Payloads range from basic messages to file deletion commands to destruction of the core operating system.

When viruses were first developed they were commonly distributed on floppy disks. However, with the evolution of the Internet, downloaded files and email are now the preferred delivery mechanisms. email can also contain attachments which can be any type of computer file. Any executable file can be infected with a Computer Virus, and should never be run unless you are absolutely certain they are virus free.

Worms

Worms are very much the same to viruses in that they are self replicating. Unlike a Computer Virus a worm does not need another executable program to be distributed. They reproduce themselves across networks by email sending and without any human assistance.

Worms usually affect networks more than particular computers on the network. Because of their self replicating behavior, worms can overload network resources very quickly which in turn causes slowdowns in data transmission due to massive bandwidth consumption.

Worms can also be designed to carry a payload which can create a 'backdoor' on the infected computer. Two of the more infamous worms that did this were Sobig and Mydoom. A backdoor is a hidden access point to a computer system that effectively bypasses any normal login procedures. The backdoor allows access to the infected computer by spammers to send junk email from that system.

Trojans

Trojans or Trojan Horses are the third common type of malware. A trojan is a program that pretends to do one thing but actually does something different. The term comes from the story of the Trojan Horse. During the siege of Troy, the Greeks left a large wooden horse outside the gates, supposedly as a peace offering. The Trojans took the horse inside the city walls only to find it was full of Greek soldiers who quickly overrun the city.

Trojans on a computer is very much the same. It looks like a harmless or useful program but in reality contains concealed code that can erase data, corrupt files, install backdoors and log keystrokes so that hackers can steal information such as credit card numbers and passwords.

Although frequently referred to as a type of Computer Virus, Trojans cannot replicate themselves like a Computer Virus or worm.. It is purely designed to gain access to your computer system and wreak havoc, just like the legendary Greek soldiers.

Malware: spyware, adware, viruses, trojan horses, malicious dialers and other nasties are the current scourge of the Internet.

Is your computer running slow? Do pop up windows frequently annoy you (even at times when you are not logged on? Does your dial up connection suddenly pop up out of nowhere and you *didn't* click on it? Has your start page suddenly changed? Chances are very good that you are the victim of malware.

Even if none of these things happen to you, you'ld be surprised at what you might find lurking on your computer!

What is it?

Malware (short for "malicious software") is any software developed for the purpose of doing harm to a computer system.

The threat of malicious software can easily be considered as the greatest threat to Internet security. Earlier, viruses were, more or less, the only form of malware. Nowadays, the threat has grown to include network-aware worms, trojans, spyware, adware and so on.

There are many different types of Malware:

- *Viruses & Worms*: Spread through e-mail, web pages or networks, these can self replicate and spread to other computers. They can often cause great damage to a computer
- *Trojan Horse*: A trojan horse program is a harmful piece of software that is disguised as legitimate software. Trojan horses cannot replicate themselves, in contrast to viruses or worms. A trojan horse can be deliberately attached to otherwise useful software by a programmer, or it can be spread by tricking users into believing that it is useful. To complicate matters, some trojan horses can spread or activate other malware, such as viruses. These programs are called droppers.
- *Back Door*: A backdoor is a piece of software that allows access to the computer system bypassing the normal authentication procedures. Based on how they work and spread, there are two groups of backdoors. The first group works much like a Trojan, i.e., they are manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload.
- *Spyware*: Spyware consists of computer software that gathers information about a computer user (such as browsing patterns in the more benign case or credit card numbers in more serious ones) and then transmits this information to an external entity without the knowledge or informed consent of the user.
- *Adware*: Adware or advertising-supported software is any software application in which advertisements are displayed while the program is running. These

applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen.

Every computer that connects to the Internet should have a good virus-scanner and spyware/adware scanning software installed on it and these should be used regularly to scan the system to rid it of malware. There is one very important thing to keep in mind:

None of these will work for you unless you keep them updated!!!

Exhibit 2

bandy_cd1

This is a list of all of the folders copied to the CD on November 4, 2004 at 10:31 pm.

```
└bandy_cd1
  └(1) JPE
    ├Comix
    │ ├Alice
    │ │ └xtream
    │ ├Chipets
    │ ├Digy
    │ ├Eco
    │ │ ├1
    │ │ ├2
    │ │ ├3
    │ │ └4
    │ ├Ho comix
    │ ├Mickey
    │ ├PAPA
    │ │ ├2
    │ │ ├3
    │ │ └4
    │ ├Pokimon
    │ ├TTA
    │ ├Tomcat
    │ │ └Albert temple
    │ ├barmaid
    │ ├kthanid
    │ ├simp
    │ └tt
    │ └New Folder
    ├Disny
    ├Horse
    │ ├El
    │ └toon
    ├Rita
    ├Tabitha
    ├Tail
    ├Zimmerman
    ├chip
    ├fatalis
    ├good stuff
    │ ├Girl
    │ └pink
    ├hh
    ├kid
    │ ├Animated
    │ ├Nudist
    │ └lolita
    │   └Good ones
    ├lelo
    ├lohan
    ├neo
    ├poke
    ├tight
    ├tiny toons
    └velma
```

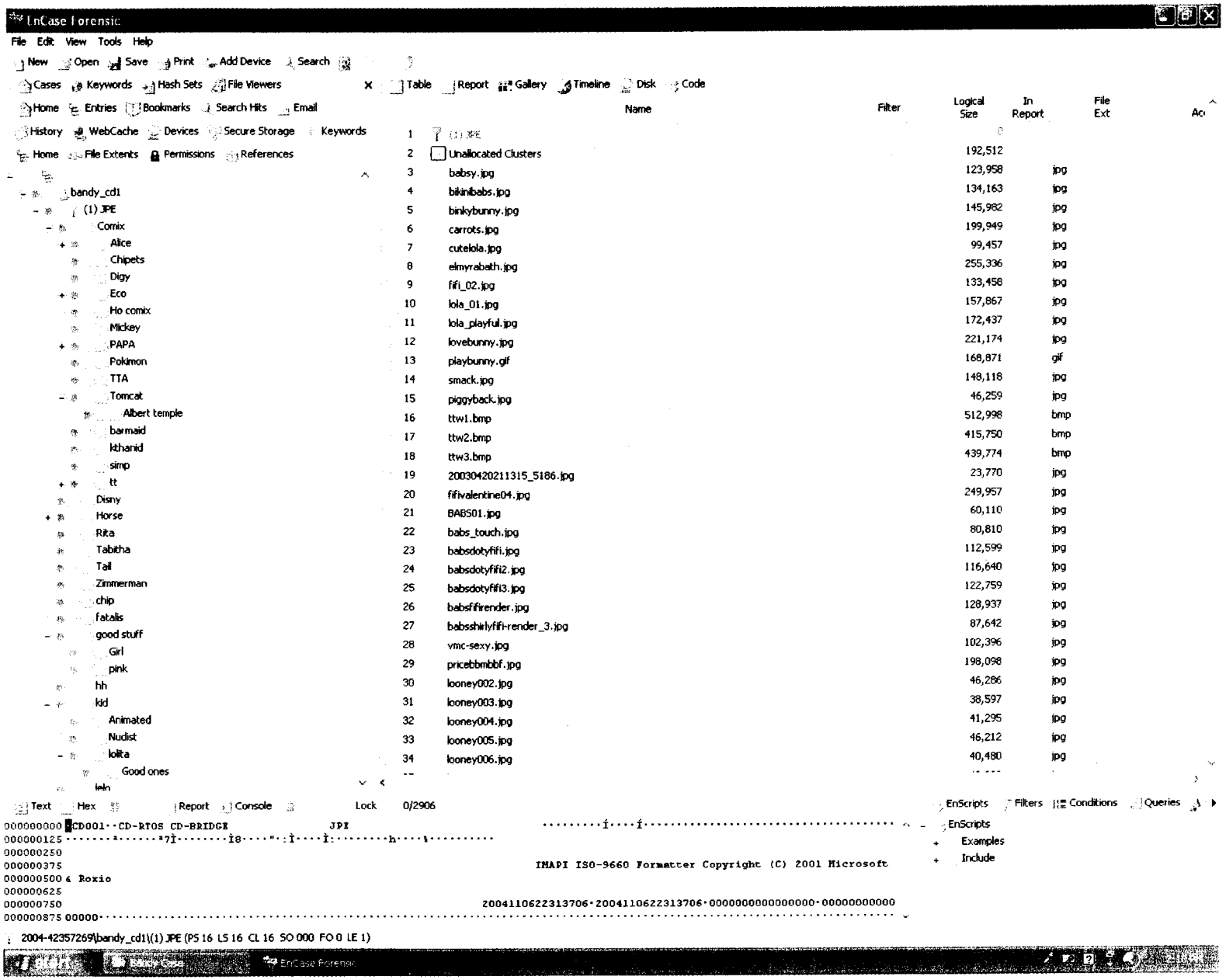

EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search
Cases Keywords Hash Sets File Viewers
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks Search Hits Email
History WebCache Devices Secure Storage Keywords
Home File Extents Permissions References
bandy_cd1
(1) JPE
Comix
Alice
Chipets
Digy
Eco
Ho comix
Mickey
PAPA
Pokimon
TTA
Tomcat
Albert temple
barmaid
kthanid
simp
tt
Disny
Horse
Rita
Tabitha
Tail
Zimmerman
chip
fatalis
good stuff
Girl
pink
hh
kid
Animated
Nudist
lolita
Good ones
Name
Filter
Logical Size
In Report
File Ext
1 (1) JPE
2 Unallocated Clusters 192,512
3 babsy.jpg 123,958 jpg
4 bikinibabs.jpg 134,163 jpg
5 binkybunny.jpg 145,982 jpg
6 carrots.jpg 199,949 jpg
7 cutelola.jpg 99,457 jpg
8 elmyrabath.jpg 255,336 jpg
9 fifi_02.jpg 133,458 jpg
10 lola_01.jpg 157,867 jpg
11 lola_playful.jpg 172,437 jpg
12 lovebunny.jpg 221,174 jpg
13 playbunny.gif 168,871 gif
14 smack.jpg 148,118 jpg
15 piggyback.jpg 46,259 jpg
16 ttw1.bmp 512,998 bmp
17 ttw2.bmp 415,750 bmp
18 ttw3.bmp 439,774 bmp
19 20030420211315_5186.jpg 23,770 jpg
20 fifivalentine04.jpg 249,957 jpg
21 BABS01.jpg 60,110 jpg
22 babs_touch.jpg 80,810 jpg
23 babsdotyfifi.jpg 112,599 jpg
24 babsdotyfifi2.jpg 116,640 jpg
25 babsdotyfifi3.jpg 122,759 jpg
26 babsfifirender.jpg 128,937 jpg
27 babsshirlyfifi-render_3.jpg 87,642 jpg
28 vmc-sexy.jpg 102,396 jpg
29 pricebbmbbf.jpg 198,098 jpg
30 looney002.jpg 46,286 jpg
31 looney003.jpg 38,597 jpg
32 looney004.jpg 41,295 jpg
33 looney005.jpg 46,212 jpg
34 looney006.jpg 40,480 jpg
Text Hex Report Console Lock 0/2906
EnScripts Filters Conditions Queries
EnScripts
Examples
Include
000000000 CD001··CD-RTOS CD-BRIDGE JPE
000000125
000000250
000000375
000000500 & Roxio
000000625
000000750
000000875 00000
IMAPI ISO-9660 Formatter Copyright (C) 2001 Microsoft
2004110622313706·2004110622313706·0000000000000000·00000000000
2004-42357269\bandy_cd1\(1) JPE (PS 16 LS 16 CL 16 SO 000 FO 0 LE 1)
EnCase Forensic

Exhibit 3

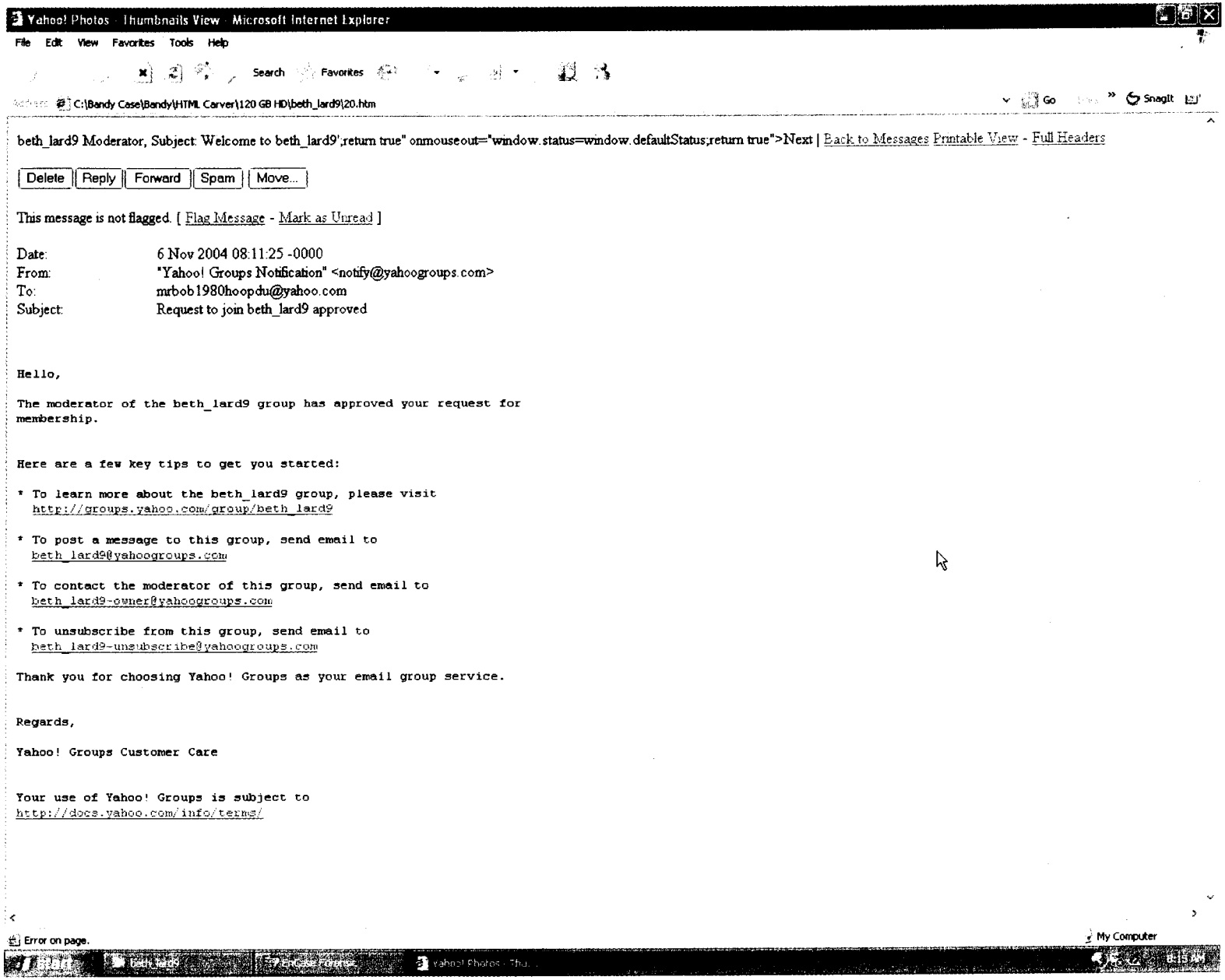

Yahoo! Photos - Thumbnails View - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites
C:\Bandy Case\Bandy\HTML Carver\120 GB HD\beth_lard9\20.htm
Go
SnagIt
beth_lard9 Moderator, Subject: Welcome to beth_lard9',return true" onmouseout="window.status=window.defaultStatus;return true">Next | Back to Messages Printable View - Full Headers
Delete Reply Forward Spam Move...
This message is not flagged. [Flag Message - Mark as Unread]
Date: 6 Nov 2004 08:11:25 -0000
From: "Yahoo! Groups Notification" <notify@yahoogroups.com>
To: mrbob1980hoopdu@yahoo.com
Subject: Request to join beth_lard9 approved
Hello,
The moderator of the beth_lard9 group has approved your request for membership.
Here are a few key tips to get you started:
* To learn more about the beth_lard9 group, please visit
http://groups.yahoo.com/group/beth_lard9
* To post a message to this group, send email to
beth_lard9@yahoogroups.com
* To contact the moderator of this group, send email to
beth_lard9-owner@yahoogroups.com
* To unsubscribe from this group, send email to
beth_lard9-unsubscribe@yahoogroups.com
Thank you for choosing Yahoo! Groups as your email group service.
Regards,
Yahoo! Groups Customer Care
Your use of Yahoo! Groups is subject to
http://docs.yahoo.com/info/terms/
Error on page.
My Computer

Exhibit 4

msn Hotmail

az_core@hotmail.com Printed: Monday, January 22, 2007 12:41 PM

From : Hill, Michael (BER) <Michael.Hill@state.ma.us>
Sent : Monday, January 22, 2007 12:16 PM
To : <az_core@hotmail.com>
Subject : RE: [IACIS-L] Statement by Defense Expert

Attachment : image001.jpg (< 0.01 MB)

I've been doing this for almost ten years and have never come across a case where this occurred. Never heard of an actual case where this happened either.

Sergeant Michael Hill - EnCE, CFCE
Berkshire Detective Unit
Massachusetts State Police
413-499-1112 x313
michael.hill@state.ma.us

From: iacis-l@cops.org [mailto:iacis-l@cops.org] **On Behalf Of** greg.allinich@phoenix.gov
Sent: Monday, January 22, 2007 11:42 AM
To: IACIS-L@cops.org
Subject: [IACIS-L] Statement by Defense Expert

I was asked to forward this question to the list.

Please respond directly to Det. Larry Core,

Maricopa County Attorney's Office.

A Computer Forensic Expert, testifying for the Defense, made a public statement

as to:

It is well known that a person that views Child Pornography on the Internet

will hack into a personal computer belonging to an innocent party, and store their

Child Pornography on that person's hard drive without the owner's knowledge.

1) Has anyone heard of or had any "actual" case of this happening?

If so, please respond "ASAP" to:

Det. Larry Core, CFCE, Maricopa County Attorneys Office

az_core@hotmail.com (az_core)

Thank you

msn Hotmail

az_core@hotmail.com Printed: Monday, January 22, 2007 11:57 AM

From : Mayott Michael J <Michael.Mayott@ci.irs.gov>
Sent : Monday, January 22, 2007 10:29 AM
To : <az_core@hotmail.com>
Subject : As requested

Been doing this 15 plus years and have never seen this. Also, note that anyone who calls themselves an expert is not one.

There is simply too much to know to be an expert.

FWIW

Mike

I was asked to forward this question to the list.

Please respond directly to Det. Larry Core,

Maricopa County Attorney's Office.

A Computer Forensic Expert, testifying for the Defense, made a public statement

as to:

It is well known that a person that views Child Pornography on the Internet

will hack into a personal computer belonging to an innocent party, and store their

Child Pornography on that person's hard drive without the owner's knowledge.

1) Has anyone heard of or had any "actual" case of this happening?

If so, please respond "ASAP" to:

Det. Larry Core, CFCE, Maricopa County Attorneys Office

az_core@hotmail.com (az_core)

Thank you

Mike Mayott
SA
912.577.6086

msn Hotmail

az_core@hotmail.com Printed: Monday, January 22, 2007 12:06 PM

From : Jefford Englander <englander.iacis@gmail.com>
Sent : Monday, January 22, 2007 10:38 AM
To : az_core@hotmail.com
Subject : Expert witness

Larry, I saw a posting regarding CP and hacking on the IACIS list posted on your behalf. While I have NEVER seen that accomplished, I am curious if this statement was made by one of our "local" experts? If so, I would be most interested in who that person is. I still have many of my old Law Enforcement cases going to trial, and I would love to know if any of the defense experts in those cases are so foolish as to have made a statement like the one posted on your behalf. Thanks, and good luck.
–

Jefford L. Englander, CFCE, EnCE

Computer Forensic Investigator

LSS Spinelli Corporation

7702 E Doubletree Ranch Road Suite 300

Scottsdale, AZ 85258

(480) 607-1700 Voice

(480) 607-0100 Fax

www.spinellicorp.com

msn Hotmail®

az_core@hotmail.com Printed: Wednesday, January 24, 2007 7:36 AM

From : <greg.allinich@phoenix.gov>
Sent : Tuesday, January 23, 2007 3:55 PM
To : <az_core@hotmail.com>
Subject : FW: [IACIS-L] Statement by Defense Expert

-----Original Message-----
From: iacis-l@cops.org [mailto:iacis-l@cops.org] On Behalf Of Jim Willingham
Sent: Tuesday, January 23, 2007 9:53 AM
To: iacis-l@cops.org; az_core@hotmail.com
Subject: RE: [IACIS-L] Statement by Defense Expert

Never. Not once. Ever. I've been doing this since 1999, worked TONS o' cases, and this has never occurred at all. Guess y'all can add me to the
"moron" list since, according to this "expert", it happens all the time.

- Jim Willingham, CFCE/SCERS -

-----Original Message-----
From: iacis-l@cops.org [mailto:iacis-l@cops.org] On Behalf Of Greg Norman
Sent: Tuesday, January 23, 2007 06:49
To: iacis-l@cops.org
Subject: Re: [IACIS-L] Statement by Defense Expert

Greg,

Who is the defense expert? I think it would be of great benefit to the list to know who it was that made such an erroneous statement.

I have been working in computer forensics for over eight years and it is not "well known" to me. In fact I have never had a CP case in which there was any evidence at all that a CP computer had been hacked.

If every pedophile is capable of being a computer hacker than hacking computers must be really easy and we (those working in law enforcement and forensics) are just plain morons.

Greg

Gregory N. Norman, CFCE
Digital Evidence Examiner
U.S. Army Criminal Investigation Laboratory
4930 North 31st St
Forest Park, GA 30297-5205
(404) 469-3490; DSN 797-3490
gregory.n.norman@us.army.mil

On 1/22/07, greg.allinich@phoenix.gov <greg.allinich@phoenix.gov> wrote:
>
>
>
>
>
>
> I was asked to forward this question to the list.

> Please respond directly to Det. Larry Core,
>
> Maricopa County Attorney's Office.
>
>
>
>
>
> A Computer Forensic Expert, testifying for the Defense, made a public
> statement
>
> as to:
>
>
>
> It is well known that a person that views Child Pornography on the
Internet
>
> will hack into a personal computer belonging to an innocent party, and
store
> their
>
> Child Pornography on that person's hard drive without the owner's
knowledge.
>
>
>
> 1) Has anyone heard of or had any "actual" case of this happening?
>
> If so, please respond "ASAP" to:
>
> Det. Larry Core, CFCE, Maricopa County Attorneys Office
>
> az_core@hotmail.com (az_core)
>
>
>
> Thank you

-

msn Hotmail

az_core@hotmail.com Printed: Wednesday, January 24, 2007 7:38 AM

From : <greg.allinich@phoenix.gov>
Sent : Tuesday, January 23, 2007 3:54 PM
To : <az_core@hotmail.com>
Subject : FW: [IACIS-L] Statement by Defense Expert

-----Original Message-----
From: iacis-l@cops.org [mailto:iacis-l@cops.org] **On Behalf Of** WILLIAMS Steve E
Sent: Tuesday, January 23, 2007 9:05 AM
To: iacis-l@cops.org
Subject: RE: [IACIS-L] Statement by Defense Expert

I had a defense expert on the stand say that right-clicking on a file to check properties is the sign of a master computer user! It comes down to someone who's "ethics" allow them to say whatever their paying client wants them to say.

Steve

Detective Steve Williams CFCE

Eugene Police Department

Financial Crimes Unit

777 Pearl St. Room 107

Eugene OR 97401

(541) 682-2682 office

(541) 682-8337 fax

From: iacis-l@cops.org [mailto:iacis-l@cops.org] **On Behalf Of** Elise Feetham
Sent: Tuesday, January 23, 2007 7:52 AM
To: iacis-l@cops.org

Subject: RE: [IACIS-L] Statement by Defense Expert

My experience in over 10 years of looking at these cases indicates that most pedophiles want to keep their stash close at hand--- (I see) printed copies, multiple copies in different folders, or stored on floppies or other removable media -including Internet free storage.

They may encrypt or otherwise try to hide their images (FSpro Hide Folders is one such utility, there are many more)-- but most often when they find an image on the Internet, they can't resist saving a copy for themselves to view at random.... For those who are smart enough understand they can be "outted" and try to avoid storing locally- they tend to save the porn sites URL's somewhere for return access. (in favorites, spreadsheets, even in paper notebooks at the scene, etc.)

It doesn't make sense that they would store it somewhere where they don't have complete control, or may be traceable, or may lose it by losing access at some point.

It is possible and probable one would see a case where someone tries to frame a "known" associate by putting illegal items on their targets PC (but not a stranger)--- thank God they leave footprints for us to follow and analyze....

All-in-all that blank statement is ridiculous and unable to substantiate (at least as of today).

Of course in this business-- there is always something new and stranger than the last around the corner.

Off my soapbox...

Good luck!

-----Original Message-----
From: iacis-l@cops.org [mailto:iacis-l@cops.org] On Behalf Of Greg Norman
Sent: Tuesday, January 23, 2007 7:49 AM
To: iacis-l@cops.org
Subject: Re: [IACIS-L] Statement by Defense Expert

Greg,

Who is the defense expert? I think it would be of great benefit to the list to know who it was that made such an erroneous statement.

I have been working in computer forensics for over eight years and it is not "well known" to me. In fact I have never had a CP case in which there was any evidence at all that a CP computer had been hacked.

If every pedophile is capable of being a computer hacker than hacking computers must be really easy and we (those working in law enforcement and forensics) are just plain morons.

Greg

Gregory N. Norman, CFCE
Digital Evidence Examiner
U.S. Army Criminal Investigation Laboratory
4930 North 31st St
Forest Park, GA 30297-5205
(404) 469-3490; DSN 797-3490
gregory.n.norman@us.army.mil

On 1/22/07, greg.allinich@phoenix.gov <greg.allinich@phoenix.gov> wrote:

>

>

>
>
>
>
> I was asked to forward this question to the list.
>
> Please respond directly to Det. Larry Core,
>
> Maricopa County Attorney's Office.
>
>
>
>
>
> A Computer Forensic Expert, testifying for the Defense, made a public
> statement
>
> as to:
>
>
>
> It is well known that a person that views Child Pornography on the Internet
>
> will hack into a personal computer belonging to an innocent party, and store
> their
>
> Child Pornography on that person's hard drive without the owner's knowledge.

>

>

>

> 1) Has anyone heard of or had any "actual" case of this happening?

>

> If so, please respond "ASAP" to:

>

> Det. Larry Core, CFCE, Maricopa County Attorneys Office

>

> az_core@hotmail.com (az_core)

>

>

>

> Thank you

-

msn Hotmail

az_core@hotmail.com Printed: Monday, January 22, 2007 12:08 PM

From : Dave_on_the_run <dave@davekleiman.com>
Sent : Monday, January 22, 2007 10:59 AM
To : <az_core@hotmail.com>
Subject : RE: [IACIS-L] Statement by Defense Expert

Is you D expert by any chance Jason Combs? That is a typical statement by him. I have an entire public dialogue from him on various security lists where he makes many outrageous claims similar to that.

The answer is no.

I hope your DA hit him with "well known by whom?"
Could you please give us a list of cases this has been identified in..

FROM DAVES PHONE!!
HTTP://WWW.DAVEKLEIMAN.COM

-----Original Message-----
From: greg.allinich@phoenix.gov
To: IACIS-L@cops.org
Sent: 22-Jan-07 11:42
Subject: [IACIS-L] Statement by Defense Expert

I was asked to forward this question to the list.

Please respond directly to Det. Larry Core,

Maricopa County Attorney's Office.

A Computer Forensic Expert, testifying for the Defense, made a public statement

as to:

It is well known that a person that views Child Pornography on the Internet

will hack into a personal computer belonging to an innocent party, and store their

Child Pornography on that person's hard drive without the owner's knowledge.

1) Has anyone heard of or had any "actual" case of this happening?

If so, please respond "ASAP" to:

Det. Larry Core, CFCE, Maricopa County Attorneys Office

az_core@hotmail.com (az_core)

Thank you

msn Hotmail

az_core@hotmail.com Printed: Monday, January 22, 2007 11:55 AM

From : <Paulvan2@aol.com>
Sent : Monday, January 22, 2007 11:13 AM
To : az_core@hotmail.com
Subject : Defense Expert`

I am a recently retired law enforcement officer who conducted criminal investigations for over ten years and five years of computer crime investigations.
I am a Cetified Forensic Computer Examiner and now conduct private civil examinations. I am a member of IACIS (International Association of Copmputer Investigative Specialists) for six years as well as a member of HTCIA (High Technology Crime Investigation Association) and regualrly read the message boards
of those organizations. Several thousand experts, from around the world in the field of computer forensics, belong to these message boards and routinely discuss criminal cases involving computer forensics. It is my expert opinion that the defense experts statement, in your case, is completely incorrect. Although this defense is often brought up, I do not know of a case where it has ever been shown to have occurred. That is not to say it has never occurred, but surfice to say if it was "common" the experts in the field would certainly be discussing it.

Statement Reference:

"It is well known that a person that views Child Pornography on the Internet
will hack into a personal computer belonging to an innocent party, and store their
Child Pornography on that personâ€™s hard drive without the ownerâ€™s knowledge."

Lt. Paul Van Steenhuyse Ret. CFCE
Cell 563-940-8209
Bettendorf, Iowa

msn Hotmail

az_core@hotmail.com Printed: Monday, January 22, 2007 11:56 AM

From : Scot Bradeen <sbradeen@ci.lewiston.me.us>
Sent : Monday, January 22, 2007 11:06 AM
To : <az_core@hotmail.com>
Subject : Statement by defense "expert"

Not here in Maine. I've been with our unit since the inception in 1999.

Det. Scot Bradeen, CFCE
Lewiston Police Department
171 Park Street
Lewiston, Maine 04240
(207) 795-9000 ext 256
Fax (207) 784-2384

msn Hotmail

az_core@hotmail.com Printed: Monday, January 22, 2007 3:25 PM

From : john davis <johntdavis2001@yahoo.com>
Sent : Monday, January 22, 2007 2:02 PM
To : az_core@hotmail.com
Subject : Defense Expert Statement-Re Hacking

I saw your question on the IACIS list serve. Prior to leaving LE a little over a year ago, I was the Operations Manager of the Colorado Computer Forensics Lab. We performed computer forensics for federal, state and local law enforcement throughout Colorado for 4 years.

I know of no documented case where a person specifically hacked into the system of another to download child porn. I now own my own computer forensics company and one of my clients is the probation department where I monitor and examine the computers of convicted sex offenders. I've yet to meet a probationer who asserts that his computer was hacked.

Though it is possible to hack other computers or their wireless access points, it is not sufficient that the "expert" make this statement without being called to task to provide case facts and the specific evidence he/she found where a computer had been hacked in such a way. Much less the statement that it happens all the time. The expert should be able to provide the specific evidence if it exists.

Hopefully, your computer forensics expert can provide the information you need to overcome this statement (e.g. link analysis, examination for virus signatures (or the lack thereof), time line analysis, typed URLs, and Internet history analysis (if applicable).

I almost don't have to ask, but could you please provide the name of this expert? There's one here in Colorado who gets around to other states who has made similar statements in court. These statements have been exposed during cross examination, but it doesn't seem to stop him from making them still.

John Davis, EnCE, CFCE
Colorado Computer Forensics
14501 E. Alameda Ave., Ste 1
Aurora, Co 80012
303.524.4589

msn Hotmail®

az_core@hotmail.com Printed: Tuesday, January 23, 2007 6:41 AM

From : Mike Parks <mikeaparks@cox.net>
Sent : Tuesday, January 23, 2007 5:29 AM
To : az_core@hotmail.com
Subject : Statement by Defense Expert

Larry,

While there is the remote possibility such a thing could happen, In the 5 years I have been investigating these cases I have never found this to have happened. I would speculate your expert is not much of an expert if he is making blanket statements like that. While I have on several occasions had someone CLAIM the CP was the result of a virus, those investigations have ultimately revealed the virus to be the person behind the keyboard. In the end, all of those who claimed it was a virus, admitted they were responsible for the images.

Just curious..... Who is this expert?

Detective Mike Parks, CFCE
Fayetteville Police Department
Special Investigations Unit
280 N. College Avenue, Suite 100
Fayetteville, AR 72701
Office (479) 587-3535
e-mail:mparks@ci.fayetteville.ar.us

msn Hotmail

az_core@hotmail.com Printed: Tuesday, January 23, 2007 10:10 AM

From : <ryawn@hiwaay.net>
Sent : Tuesday, January 23, 2007 8:03 AM
To : az_core@hotmail.com
Subject : Re: [IACIS-L] Statement by Defense Expert

Detective Core,

I'm replying off list to your inquiry. I've been involved in computer forensics since 1994 and this is not "well known" to me either. In all of the cases that I've worked over the years, there has been evidence other than the images themselves that refute this statement.

Again, I know of no case, worked myself or by others, that would support such a statement.

hth,

Russell

> Greg,
>
> Who is the defense expert? I think it would be of great benefit to
> the list to know who it was that made such an erroneous statement.
>
> I have been working in computer forensics for over eight years and
> it is not "well known" to me. In fact I have never had a CP case in
> which there was any evidence at all that a CP computer had been
> hacked.
>
> If every pedophile is capable of being a computer hacker than
> hacking computers must be really easy and we (those working in law
> enforcement and forensics) are just plain morons.
>
> Greg
>
> Gregory N. Norman, CFCE
> Digital Evidence Examiner
> U.S. Army Criminal Investigation Laboratory
> 4930 North 31st St
> Forest Park, GA 30297-5205
> (404) 469-3490; DSN 797-3490
> gregory.n.norman@us.army.mil
>
>
> On 1/22/07, greg.allinich@phoenix.gov <greg.allinich@phoenix.gov>
> wrote:
> > >
> > >
> > >
> > >
> > >
> > >
> > > I was asked to forward this question to the list.
> > >
> > > Please respond directly to Det. Larry Core,
> > >
> > > Maricopa County Attorney's Office.
> > >
> > >
> > >
> > >
> > >
> > > A Computer Forensic Expert, testifying for the Defense, made a public

> > statement
> >
> > as to:
> >
> >
> >
> > It is well known that a person that views Child Pornography on the
> Internet
> >
> > will hack into a personal computer belonging to an innocent party, and
> store
> > their
> >
> > Child Pornography on that person's hard drive without the owner's
> knowledge.
> >
> >
> >
> > 1) Has anyone heard of or had any "actual" case of this happening?
> >
> > If so, please respond "ASAP" to:
> >
> > Det. Larry Core, CFCE, Maricopa County Attorneys Office
> >
> > az_core@hotmail.com (az_core)
> >
> >
> >
> > Thank you
>
>
>
> -
>

Russell Yawn, CFCE
Office of Prosecution Services
515 South Perry Street
Montgomery, Alabama 36104
(334) 242-4191

Exhibit 5

OS Information

Product Name:	Microsoft Windows XP
Current Version:	5.1
Registered Owner:	
Registered Organization:	
System Root:	C:\WINDOWS
Current Build Number:	2600
Path Name:	C:\WINDOWS
Product ID:	55277-OEM-0011903-00106
Last Service Pack:	Service Pack 1
Product Key:	
VersionNumber:	
Source Path:	D:\i386
Install Date:	12/04/04 05:41:52PM
Last Shutdown Time:	12/06/04 07:27:08PM

Exhibit 6

Folder Named (')

This is the list of folders copied back onto the hard drive on December 4, at 5:49 pm.

└'
- ├chip
- ├Comix
  - ├Alice
    - └xtream
  - ├barmaid
  - ├Chipets
  - ├Digy
  - ├Eco
    - ├1
    - ├2
    - ├3
    - └4
  - ├Ho comix
  - ├kthanid
  - ├Mickey
    - └CD
  - ├PAPA
    - ├2
    - ├3
    - └4
  - ├Pokimon
  - ├PPG
  - ├simp
    - ├L7SM
    - ├Mos R
    - └sleep
  - ├Tomcat
    - └Albert temple
  - ├tt
    - └New Folder
  - └TTA
- ├Disny
- ├fatalis
- ├good stuff
  - ├Girl
  - └pink
- ├hh
- ├Horse
  - ├Beastility
  - ├El
  - └toon
- ├kid
  - ├Animated
  - ├lolita
    - └Good ones
  - └Nudist
- ├lelo
- ├lohan
- ├neo
- ├poke
- ├Rita
- ├Tabitha
- ├Tail
- ├tight
- ├tiny toons
- ├velma
- └Zimmerman

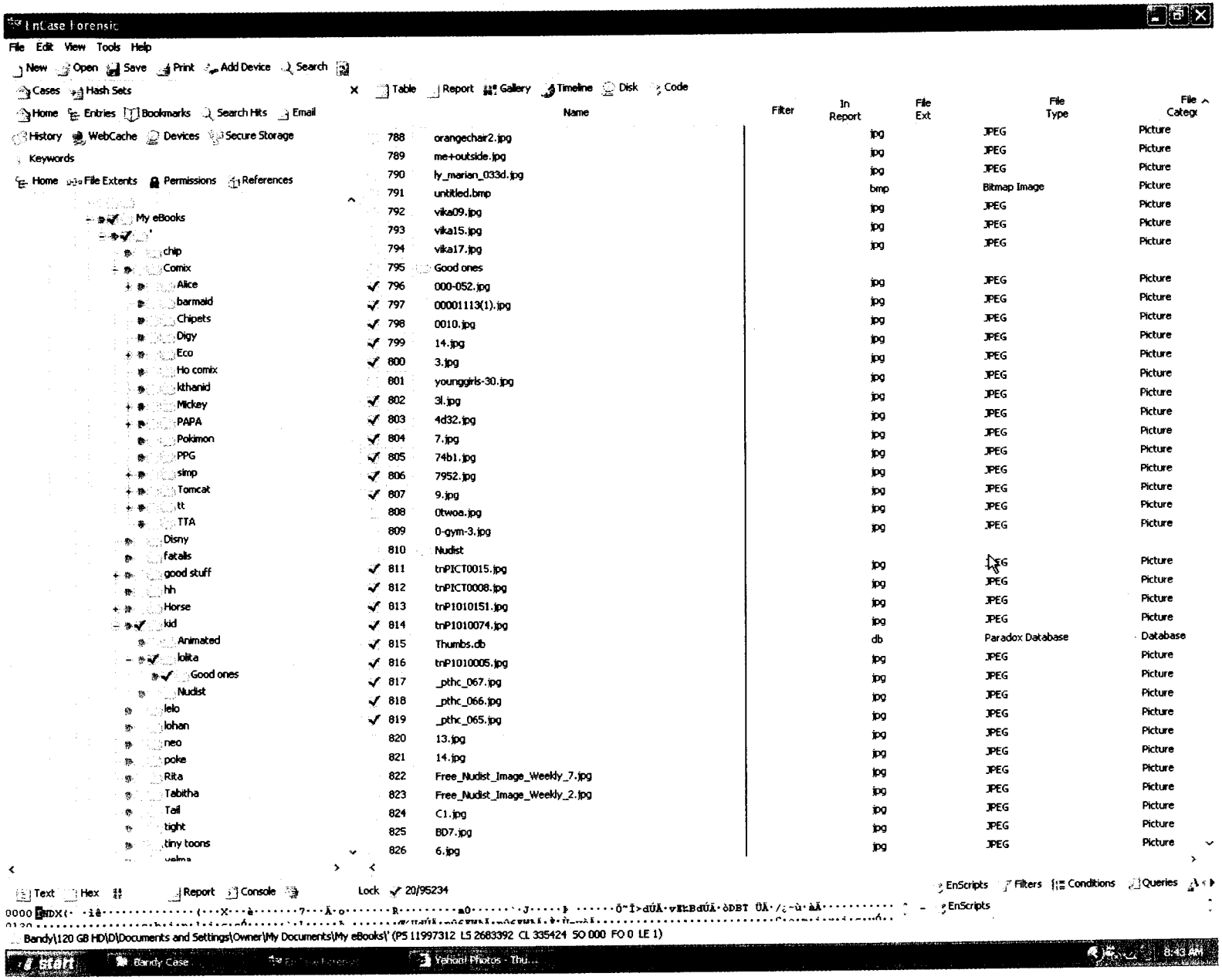

EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search
Cases Hash Sets
Home Entries Bookmarks Search Hits Email
History WebCache Devices Secure Storage
Keywords
Home File Extents Permissions References
Table Report Gallery Timeline Disk Code
Name
Filter
In Report
File Ext
File Type
File Categ
My eBooks
chip
Comix
Alice
barmaid
Chipets
Digy
Eco
Ho comix
kthanid
Mickey
PAPA
Pokimon
PPG
simp
Tomcat
tt
TTA
Disny
fatalls
good stuff
hh
Horse
kid
Animated
lolita
Good ones
Nudist
lelo
lohan
neo
poke
Rita
Tabitha
Tail
tight
tiny toons
788 orangechair2.jpg
789 me+outside.jpg
790 ly_marian_033d.jpg
791 untitled.bmp
792 vika09.jpg
793 vika15.jpg
794 vika17.jpg
795 Good ones
796 000-052.jpg
797 00001113(1).jpg
798 0010.jpg
799 14.jpg
800 3.jpg
801 younggirls-30.jpg
802 3l.jpg
803 4d32.jpg
804 7.jpg
805 74b1.jpg
806 7952.jpg
807 9.jpg
808 0twoa.jpg
809 0-gym-3.jpg
810 Nudist
811 tnPICT0015.jpg
812 tnPICT0008.jpg
813 tnP1010151.jpg
814 tnP1010074.jpg
815 Thumbs.db
816 tnP1010005.jpg
817 _pthc_067.jpg
818 _pthc_066.jpg
819 _pthc_065.jpg
820 13.jpg
821 14.jpg
822 Free_Nudist_Image_Weekly_7.jpg
823 Free_Nudist_Image_Weekly_2.jpg
824 C1.jpg
825 BD7.jpg
826 6.jpg
jpg JPEG Picture
bmp Bitmap Image
db Paradox Database Database
Text Hex Report Console Lock 20/95234
EnScripts Filters Conditions Queries
EnScripts
Bandy\120 GB HD\D\Documents and Settings\Owner\My Documents\My eBooks\' (PS 11997312 LS 2683392 CL 335424 SO 000 FO 0 LE 1)
Start
Bandy Case
Yahoo! Photos - Thu...
8:43 AM

Exhibit 7

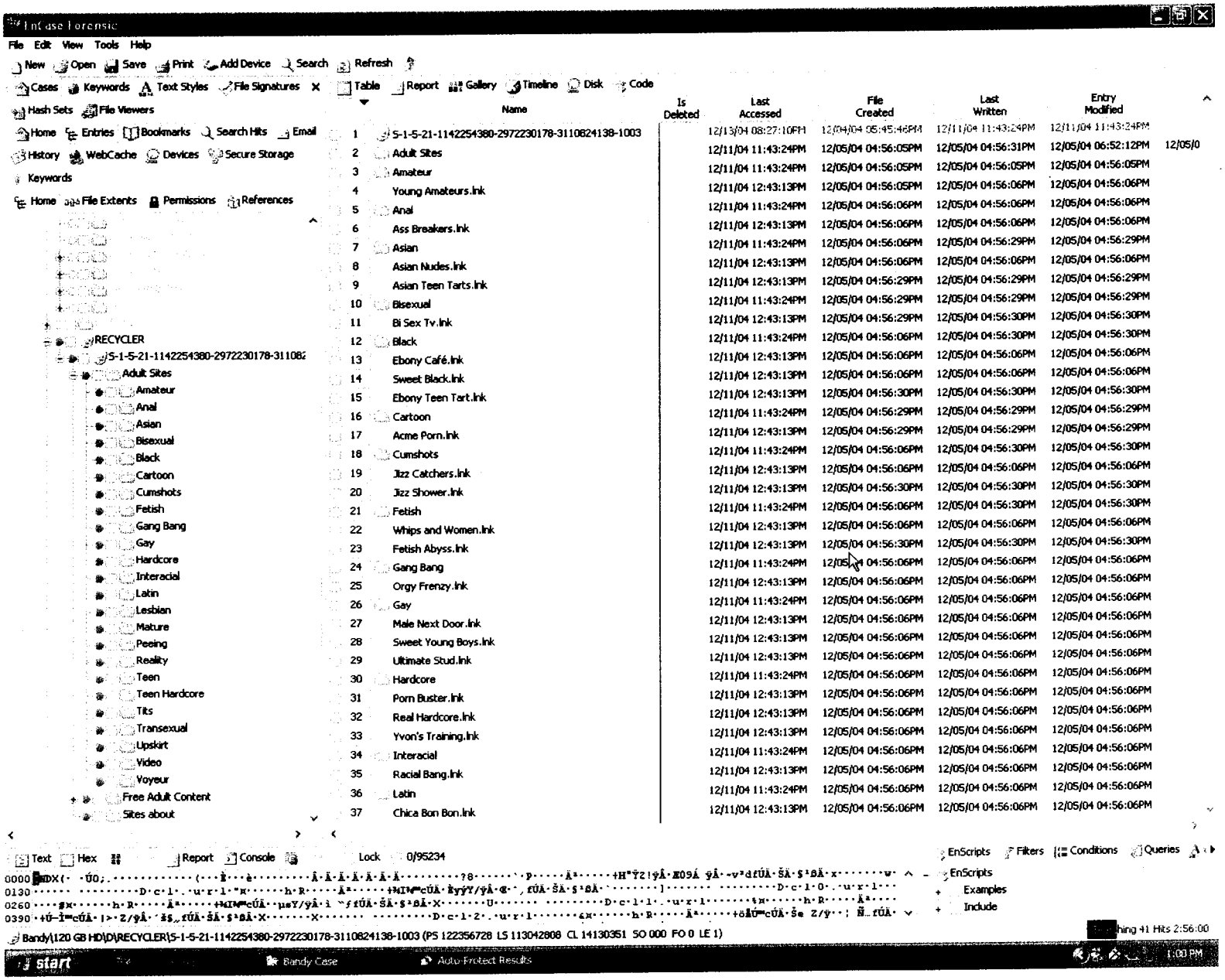

EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases Keywords Text Styles File Signatures
Hash Sets File Viewers
Home Entries Bookmarks Search Hits Email
History WebCache Devices Secure Storage
Keywords
Home File Extents Permissions References
RECYCLER
S-1-5-21-1142254380-2972230178-311082
Adult Sites
Amateur
Anal
Asian
Bisexual
Black
Cartoon
Cumshots
Fetish
Gang Bang
Gay
Hardcore
Interacial
Latin
Lesbian
Mature
Peeing
Reality
Teen
Teen Hardcore
Tits
Transexual
Upskirt
Video
Voyeur
Free Adult Content
Sites about
Table Report Gallery Timeline Disk Code
Name
Is Deleted
Last Accessed
File Created
Last Written
Entry Modified
1 S-1-5-21-1142254380-2972230178-3110824138-1003
2 Adult Sites
3 Amateur
4 Young Amateurs.lnk
5 Anal
6 Ass Breakers.lnk
7 Asian
8 Asian Nudes.lnk
9 Asian Teen Tarts.lnk
10 Bisexual
11 Bi Sex Tv.lnk
12 Black
13 Ebony Café.lnk
14 Sweet Black.lnk
15 Ebony Teen Tart.lnk
16 Cartoon
17 Acme Porn.lnk
18 Cumshots
19 Jizz Catchers.lnk
20 Jizz Shower.lnk
21 Fetish
22 Whips and Women.lnk
23 Fetish Abyss.lnk
24 Gang Bang
25 Orgy Frenzy.lnk
26 Gay
27 Male Next Door.lnk
28 Sweet Young Boys.lnk
29 Ultimate Stud.lnk
30 Hardcore
31 Porn Buster.lnk
32 Real Hardcore.lnk
33 Yvon's Training.lnk
34 Interacial
35 Racial Bang.lnk
36 Latin
37 Chica Bon Bon.lnk
12/13/04 08:27:10PM 12/04/04 05:45:46PM 12/11/04 11:43:24PM 12/11/04 11:43:24PM
12/11/04 11:43:24PM 12/05/04 04:56:05PM 12/05/04 04:56:31PM 12/05/04 06:52:12PM 12/05/0
12/11/04 11:43:24PM 12/05/04 04:56:05PM 12/05/04 04:56:05PM 12/05/04 04:56:05PM
12/11/04 12:43:13PM 12/05/04 04:56:05PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM
12/11/04 11:43:24PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM
12/11/04 12:43:13PM 12/05/04 04:56:29PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM
12/11/04 11:43:24PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM
12/11/04 12:43:13PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM 12/05/04 04:56:29PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM 12/05/04 04:56:30PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 11:43:24PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
12/11/04 12:43:13PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM 12/05/04 04:56:06PM
Text Hex Report Console Lock 0/95234
EnScripts Filters Conditions Queries
EnScripts
Examples
Include
Bandy\120 GB HD\D\RECYCLER\S-1-5-21-1142254380-2972230178-3110824138-1003 (PS 122356728 LS 113042808 CL 14130351 SO 000 FO 0 LE 1)
start
Bandy Case
Auto-Protect Results
1:00 PM

Exhibit 8

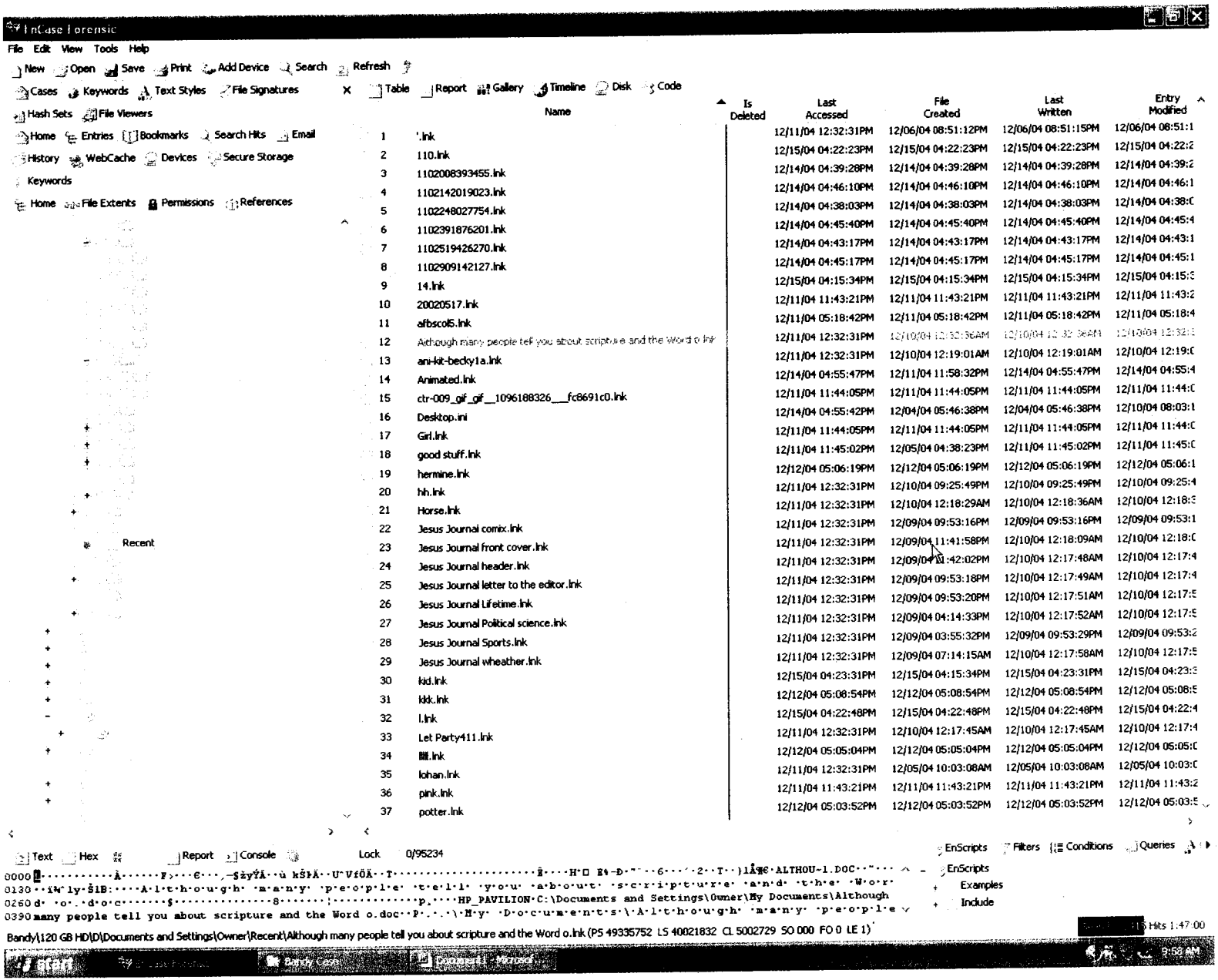
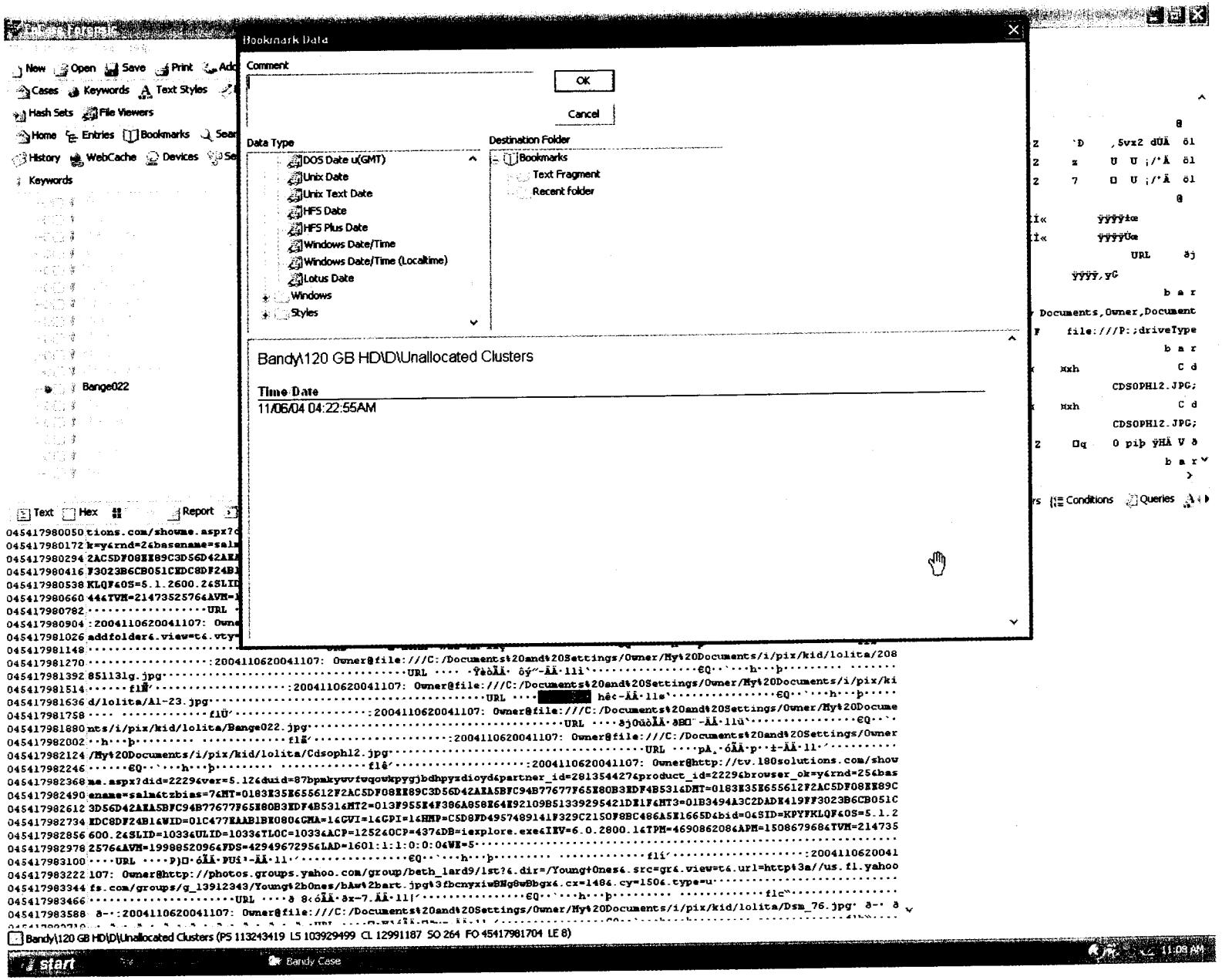
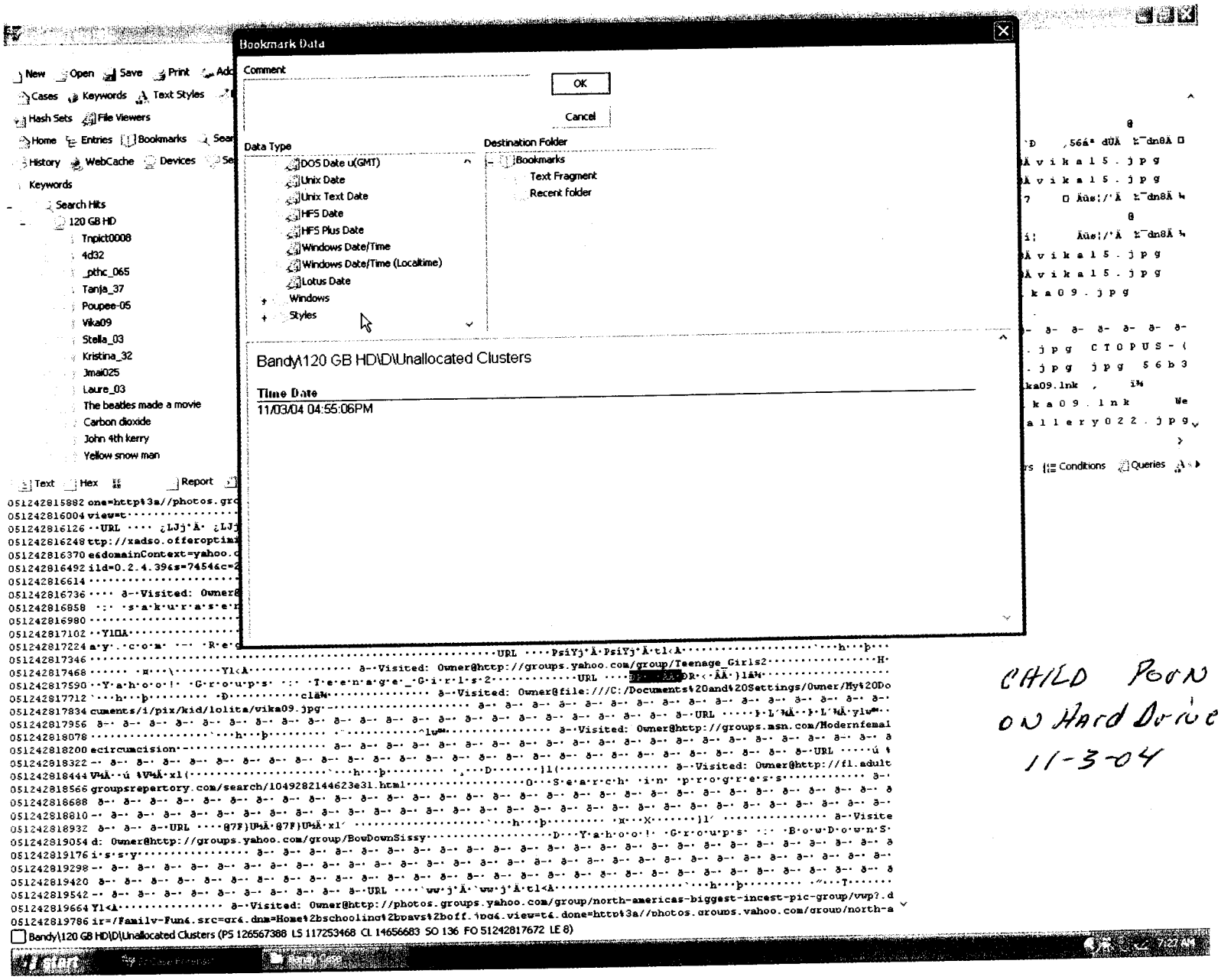
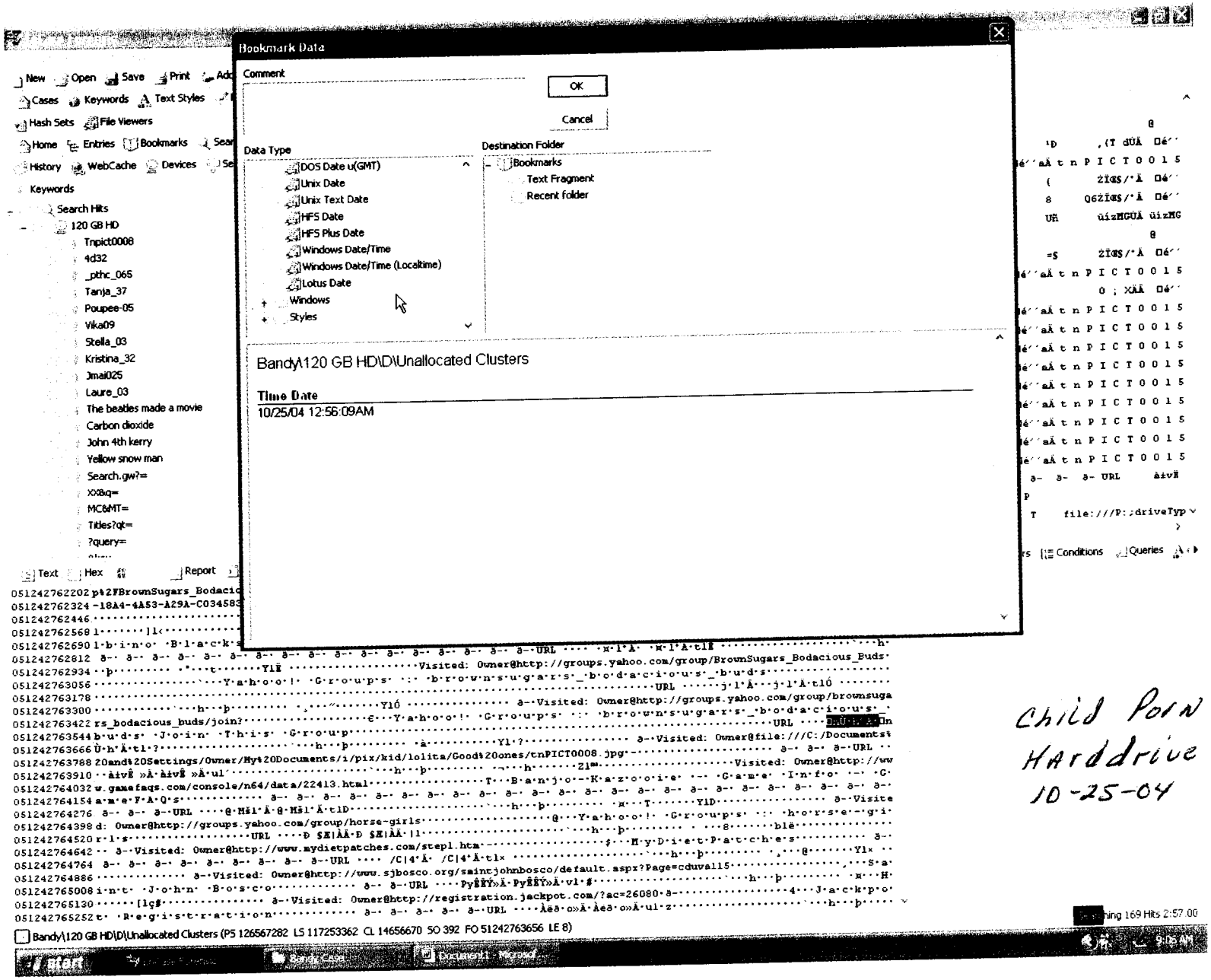

EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases Keywords Text Styles File Signatures
Hash Sets File Viewers
Home Entries Bookmarks Search Hits Email
History WebCache Devices Secure Storage
Keywords
Home File Extents Permissions References
Table Report Gallery Timeline Disk Code
Name
Is Deleted
Last Accessed
File Created
Last Written
Entry Modified
1 '.lnk
2 110.lnk
3 1102008393455.lnk
4 1102142019023.lnk
5 1102248027754.lnk
6 1102391876201.lnk
7 1102519426270.lnk
8 1102909142127.lnk
9 14.lnk
10 20020517.lnk
11 afbscol5.lnk
12 Although many people tell you about scripture and the Word o.lnk
13 ani-kit-becky1a.lnk
14 Animated.lnk
15 ctr-009_gif_gif__1096188326___fc8691c0.lnk
16 Desktop.ini
17 Girl.lnk
18 good stuff.lnk
19 hermine.lnk
20 hh.lnk
21 Horse.lnk
22 Jesus Journal comix.lnk
23 Jesus Journal front cover.lnk
24 Jesus Journal header.lnk
25 Jesus Journal letter to the editor.lnk
26 Jesus Journal Lifetime.lnk
27 Jesus Journal Political science.lnk
28 Jesus Journal Sports.lnk
29 Jesus Journal wheather.lnk
30 kid.lnk
31 kkk.lnk
32 l.lnk
33 Let Party411.lnk
34 [redacted].lnk
35 lohan.lnk
36 pink.lnk
37 potter.lnk
Recent
Text Hex Report Console Lock 0/95234
EnScripts Filters Conditions Queries
EnScripts
Examples
Include
Hits 1:47:00
Bandy\120 GB HD\D\Documents and Settings\Owner\Recent\Although many people tell you about scripture and the Word o.lnk (PS 49335752 LS 40021832 CL 5002729 SO 000 FO 0 LE 1)
9:58 AM

Exhibit 9

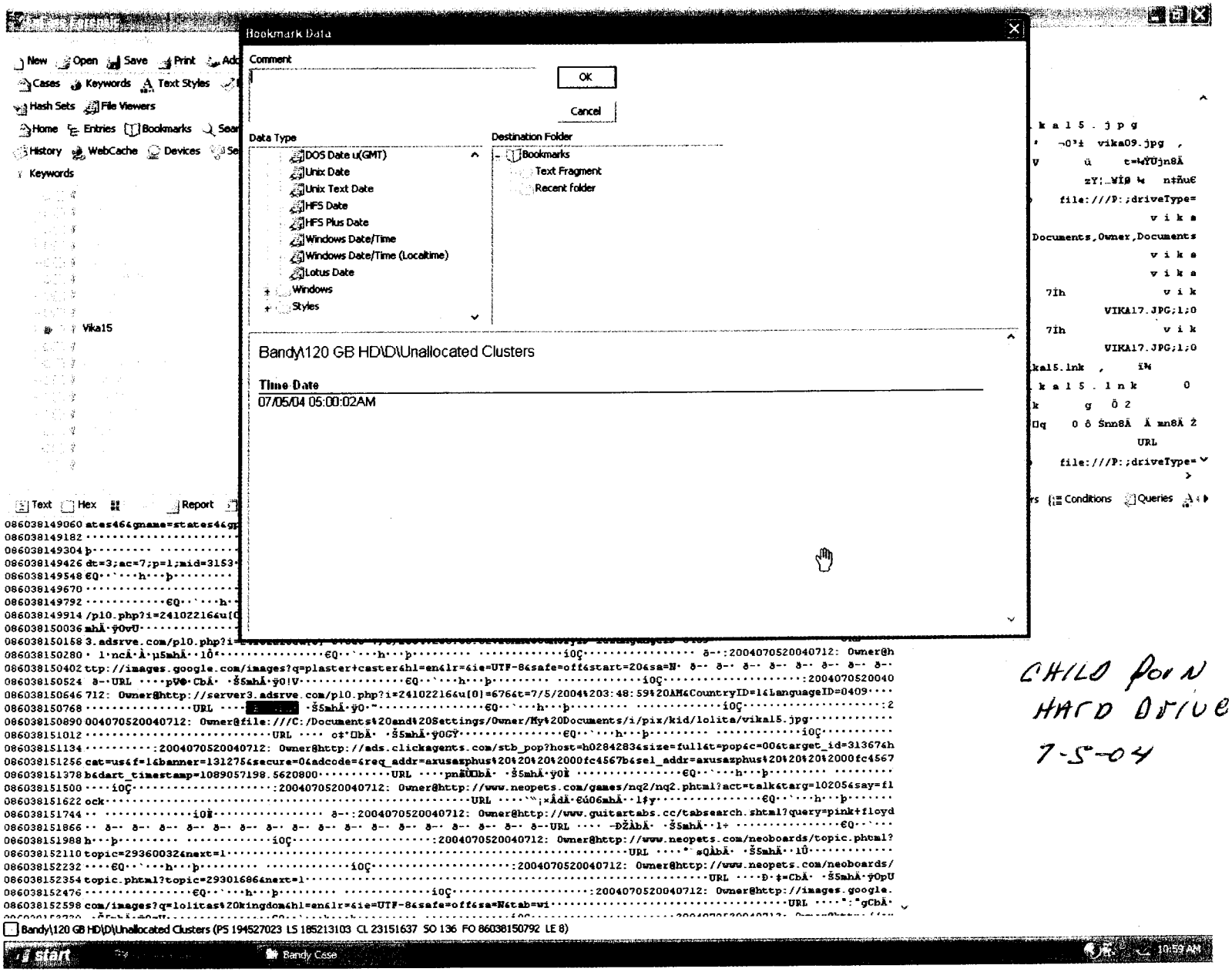

Bookmark Data
Comment
OK
Cancel
Data Type
DOS Date u(GMT)
Unix Date
Unix Text Date
HFS Date
HFS Plus Date
Windows Date/Time
Windows Date/Time (Localtime)
Lotus Date
Windows
Styles
Destination Folder
Bookmarks
Text Fragment
Recent folder
Bandy\120 GB HD\D\Unallocated Clusters
Time Date
11/06/04 04:22:55AM
New
Open
Save
Print
Cases
Keywords
Text Styles
Hash Sets
File Viewers
Home
Entries
Bookmarks
History
WebCache
Devices
Keywords
Bange022
Text
Hex
Report
Conditions
Queries
Bandy\120 GB HD\D\Unallocated Clusters (PS 113243419 LS 103929499 CL 12991187 SO 264 FO 45417981704 LE 8)
start
Bandy Case
11:08 AM



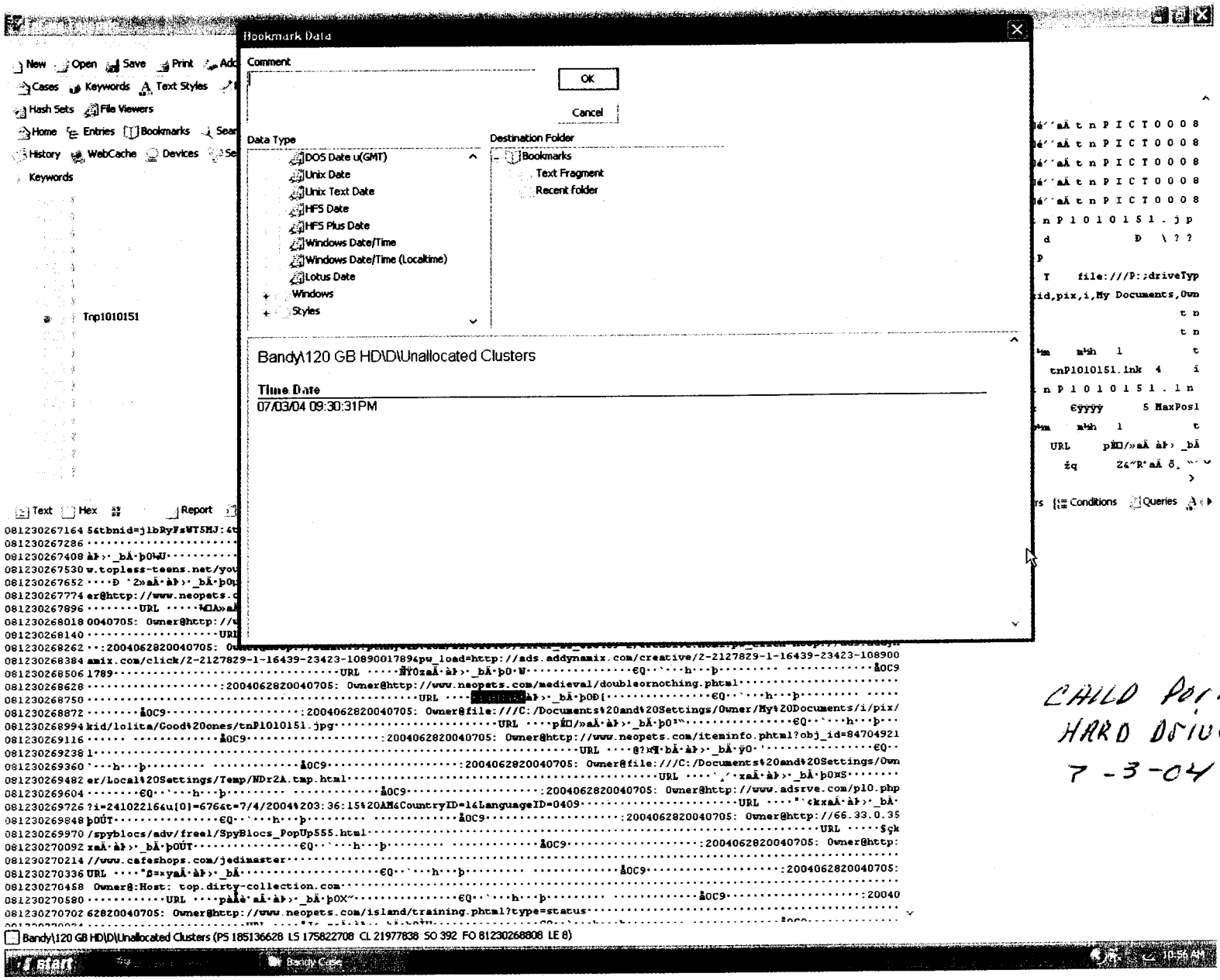
CHILD PORN
ON Hard Drive
11-3-04



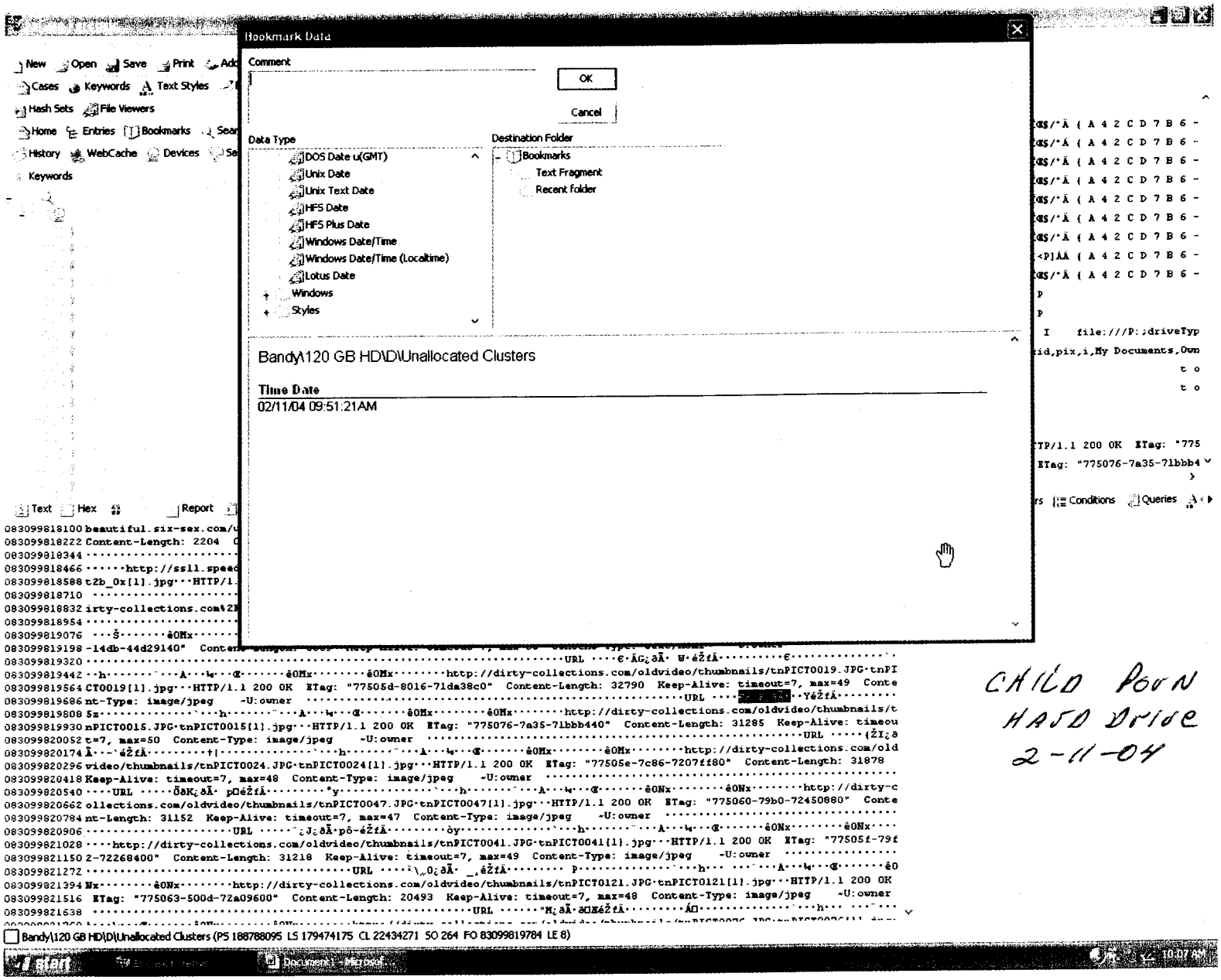
Child Porn
Harddrive
10-25-04



CHILD PORN
HARD DRIVE
7-5-04



CHILD PORN
HARD DRIVE
7-3-04



CHILD PORN
HARD DRIVE
2-11-04

Exhibit 10

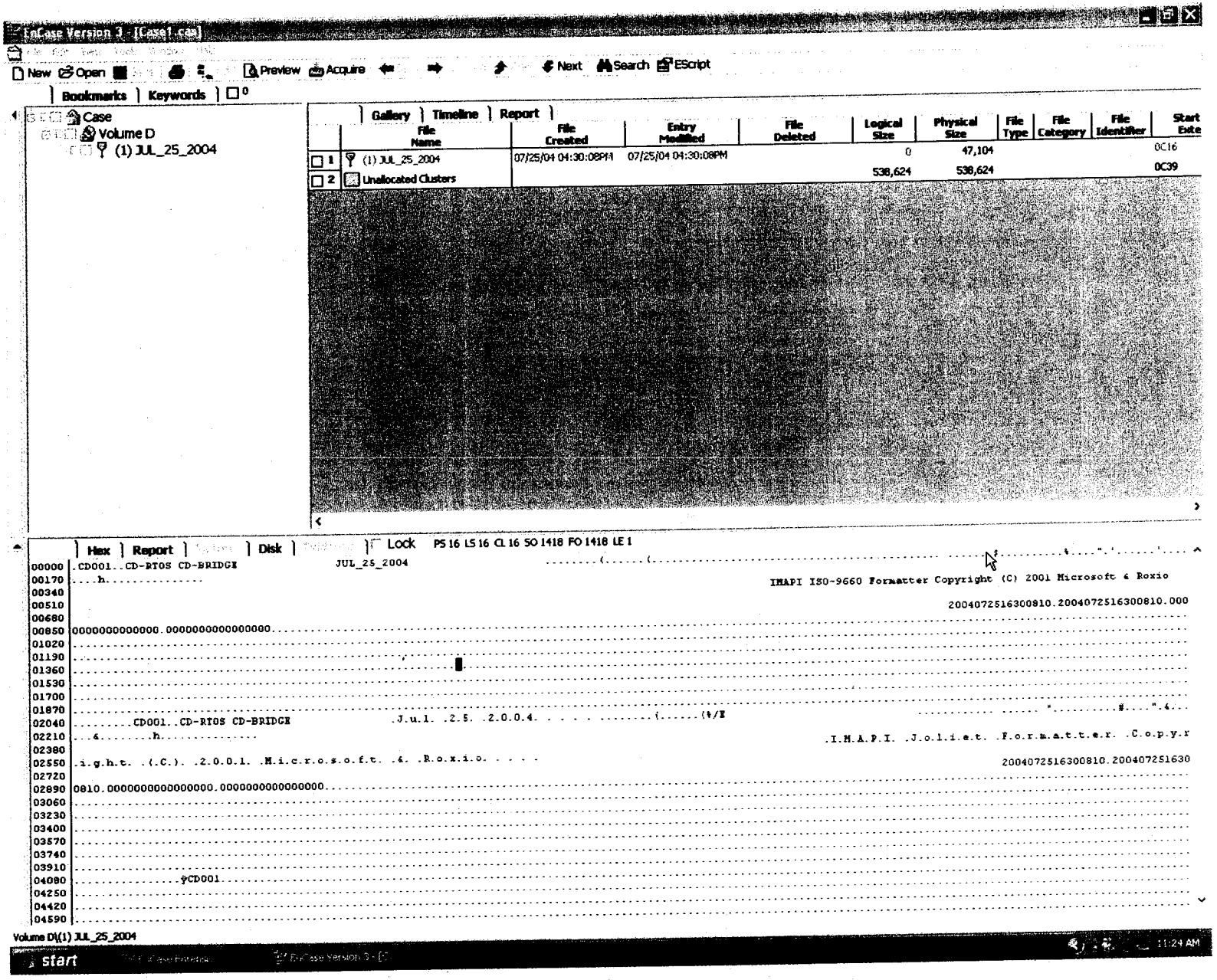

EnCase Version 3 - [Case1.cas]
New
Open
Preview
Acquire
Next
Search
EScript
Bookmarks
Keywords
Case
Volume D
(1) JUL_25_2004
Gallery
Timeline
Report
File Name
File Created
Entry Modified
File Deleted
Logical Size
Physical Size
File Type
File Category
File Identifier
Start Exte
1 (1) JUL_25_2004 07/25/04 04:30:08PM 07/25/04 04:30:08PM 0 47,104 0C16
2 Unallocated Clusters 538,624 538,624 0C39
Hex
Report
Disk
Lock
PS 16 LS 16 CL 16 SO 1418 FO 1418 LE 1
00000 .CD001..CD-RTOS CD-BRIDGE JUL_25_2004
00170 ....h.
IMAPI ISO-9660 Formatter Copyright (C) 2001 Microsoft & Roxio
00340
00510
20040725163008l0.2004072516300810.000
00680
00850 0000000000000.0000000000000000
01020
01190
01360
01530
01700
01870
02040 .CD001..CD-RTOS CD-BRIDGE .J.u.l. .2.5. .2.0.0.4.
02210 ...&.....h.
.I.M.A.P.I. .J.o.l.i.e.t. .F.o.r.m.a.t.t.e.r. .C.o.p.y.r
02380
02550 .i.g.h.t. .(.C.). .2.0.0.1. .M.i.c.r.o.s.o.f.t. .&. .R.o.x.i.o.
2004072516300810.200407251630
02720
02890 0810.0000000000000000.0000000000000000
03060
03230
03400
03570
03740
03910
04080 .CD001
04250
04420
04590
Volume D\(1) JUL_25_2004
start
11:24 AM

Exhibit 11

TROJANS
LISTED BY
TAMI LOEHRS

Discovered: April 15, 2004

Updated: April 17, 2004 03:04:28 PM ZE9

Type: Trojan Horse

Infection Length: variable

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows XP

When Backdoor.IRC.Zcrew.C is executed, it performs the following actions:

1. Creates the following files in the %System%\instsrv folder:

- 001.config
- Configure
- COPYING
- cygregex.dll
- cygwin1.dll
- firedaemon.exe
- foxdg.exe
- hideapp.exe
- ident.exe
- inst.bat (detected as Backdoor.IRC.Zcrew.C)
- iroffer.cron
- KILL.EXE
- irs.reg (detected as Backdoor.IRC.Zcrew.C)
- Makefile.config
- mybot.ignl
- mybot.ignl.bkup
- mybot.ignl.tmp
- new.txt
- README
- rn.bat
- secure1.bat (detected as Backdoor.IRC.Zcrew.C)
- secure2.bat
- startsecure.bat
- test.bat
- WHATSNEW

Notes:

- %System% is a variable. The Trojan locates the System folder and copies the files to that location. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

- Unless otherwise stated, these files are nonmalicious, so Symantec antivirus programs will not detect them.

Discovered: January 15, 2004

Updated: January 15, 2004 03:26:44 PM PST

Also Known As: Worm.Win32.Randon.o [Kaspersky]

Type: Trojan Horse

Infection Length: varies

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

When Backdoor.IRC.Aladinz.G is executed, it performs the following actions:

1. Creates the folder %Program Files%\Common Files\OOBE\DivX Player 7.0, and drops the following files into the folder:

- sample.bin (detected as Backdoor.Trojan)
- DivXinstall.bat (detected as Trojan Horse)
- DecodeDivX.exe (detected as Hacktool.DoS)
- nacs.exe (detected as Hacktool)
- DrDivXRegistration.exe (detected as Hacktool.HideWindow.)
- Dr.DivX.exe (mIRC client software. It is detected as IRC.Backdoor.Trojan.)
- DelDivX.exe (Process viewer. This utility is not viral by itself.)
- Divx.exe (Remote execution utility. It is not viral by itself)
- helptoo.txt (Text file that includes username.It is not malicious itself.)
- helpuse.txt (Text file that includes username and password. It is not malicious itself.)
- DivX.ini (Ini file that the Trojan uses to load other IRC scripts. It is not malicious itself.)

Updated: December 13, 2005 04:37:48 PM PST

Type: Adware

Risk Impact: High

File Names: Winshow.dll

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows XP

Behavior

Adware.Winshow is an adware component that modifies the Web browser's default home page and search settings without your permission.

Symptoms

The files are detected as Adware.Winshow.

Transmission

This adware component must be manually installed, or installed as a component of another program that you install.

Protection

- **Virus Definitions (LiveUpdate™ Weekly)** October 1, 2003
- **Virus Definitions (Intelligent Updater)** September 30, 2003

Discovered: April 29, 2005

Updated: June 29, 2005 04:09:27 PM PDT

Also Known As: Win32.Rbot.CKU [Computer Associates], Backdoor.Win32.Rbot.gen [Kaspersky Lab], W32/Sdbot.worm.gen [McAfee], W32/Rbot-Fam [Sophos], WORM_RBOT.GEN [Trend Micro]

Type: Worm

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

W32.Spybot.OFN is a network-aware worm that has distributed denial of service and back door capabilities. The worm spreads through network shares protected by weak passwords and by exploiting vulnerabilities. W32.Spybot.OFN may be downloaded by W32.Kelvir.AZ.

Protection

- **Virus Definitions (LiveUpdate™ Weekly)** May 4, 2005
- ***Virus Definitions (Intelligent Updater)*** *April 30, 2005*

Threat Assessment

Wild

- **Wild Level:** Low
- **Number of Infections:** 0 - 49
- **Number of Sites:** 0 - 2
- **Geographical Distribution:** Low
- **Threat Containment:** Easy
- ***Removal:*** Moderate

Damage

- **Damage Level:** Medium
- **Payload:** Opens a back door.

Distribution

- **Distribution Level:** Medium
- **Ports:** TCP ports 8080, 1433, and 445.
- **Target of Infection:** Exploits vulnerabilities.

Discovered: June 6, 2005

Updated: July 7, 2005 03:14:01 PM PDT

Also Known As: Win32.Rbot.CRX [Computer Associates], Backdoor.Win32.Rbot.rx [Kaspersky Lab], W32/Sdbot.worm.gen.y [McAfee], W32/Rbot-Fam [Sophos], WORM_RBOT.BJF [Trend Micro]

Type: Worm

Infection Length: 121,504 bytes.

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

W32.Spybot.PKC is a network-aware worm that has distributed denial of service and back door capabilities. The worm spreads through network shares protected by weak passwords and by exploiting vulnerabilities.

Note: Definitions dated prior to June 6, 2005 detect this threat as W32.Spybot.Worm.

Protection

- **Virus Definitions (LiveUpdate™ Weekly)** June 8, 2005
- **Virus Definitions (Intelligent Updater)** June 6, 2005

Threat Assessment

Wild

- ***Wild Level:*** *Low*
- **Number of Infections:** 0 - 49
- ***Number of Sites:*** 3 - 9
- **Geographical Distribution:** Low
- **Threat Containment:** Easy
- **Removal:** Moderate

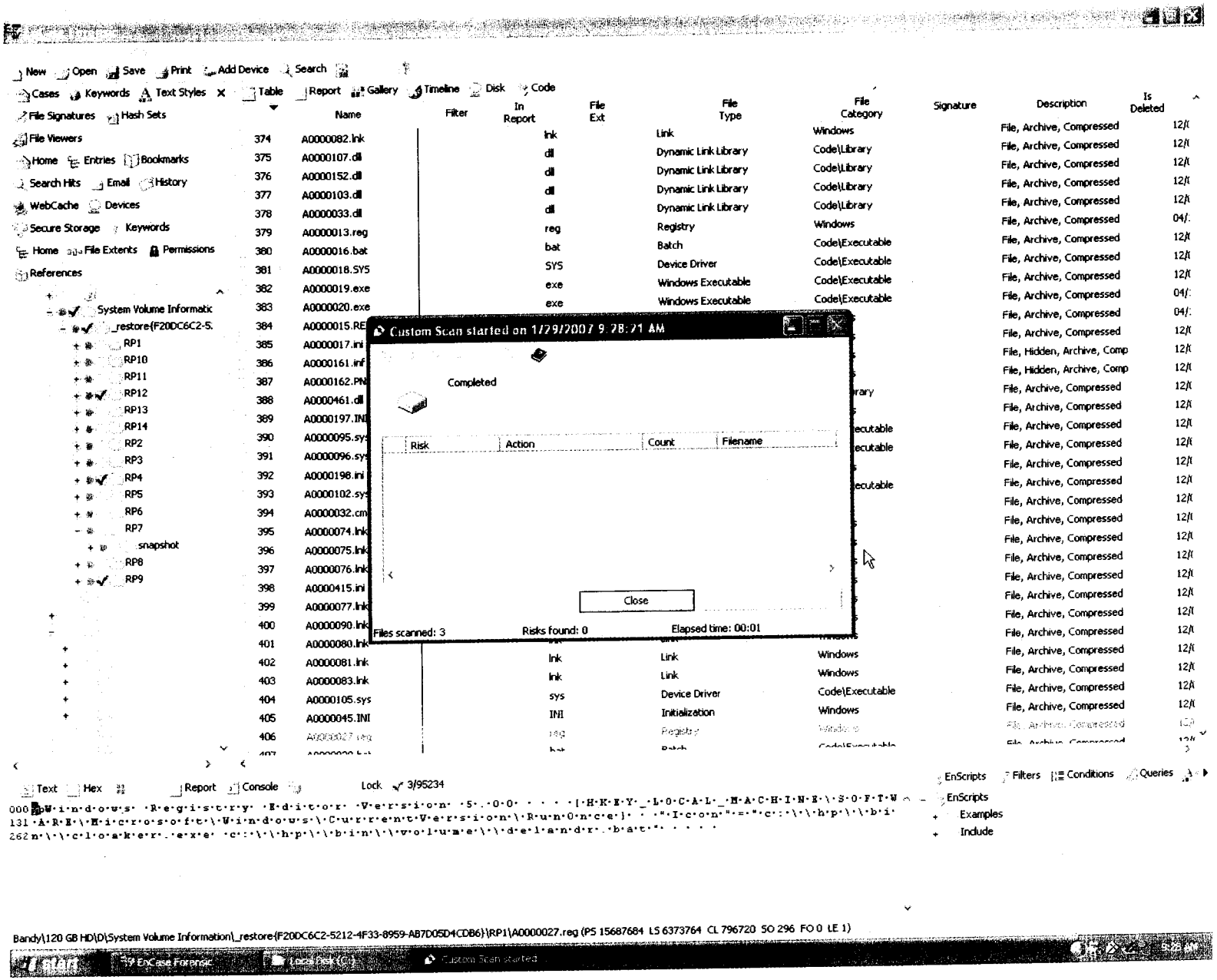
Damage

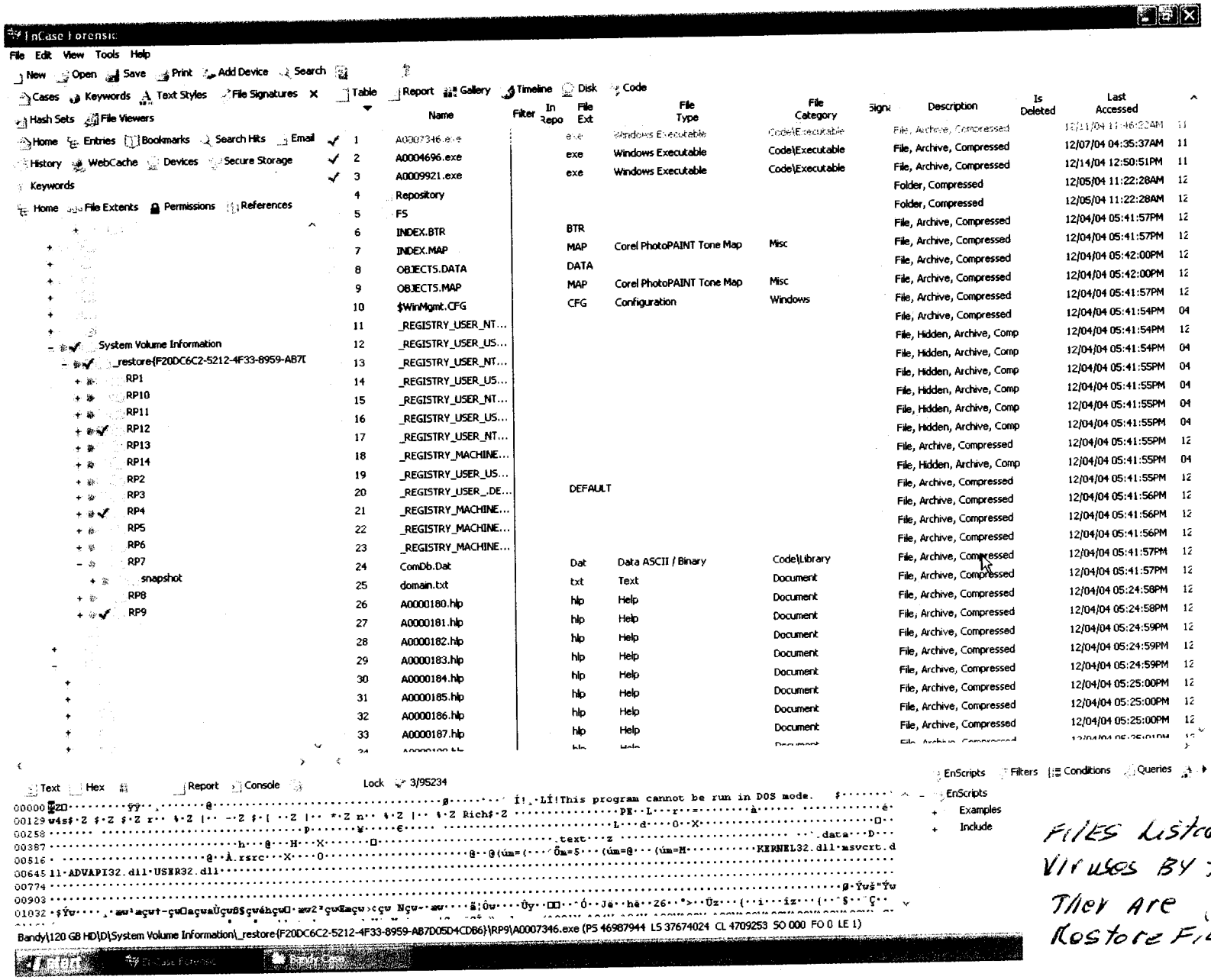
- **Damage Level:** Medium
- **Payload:** Opens a back door.
- **Releases Confidential Info:** Installed keylogger may steal confidential information.

Distribution

- **Distribution Level:** Medium
- **Ports:** TCP ports 6394 and 445; UDP port 1433.
- **Target of Infection:** Exploits vulnerabilities.

Exhibit 12


Custom Scan started on 1/29/2007 9:28:21 AM
Completed
Risk
Action
Count
Filename
Close
Files scanned: 3
Risks found: 0
Elapsed time: 00:01



FILES Listed AS VIRUSES BY TAMI THEY ARE RESTORE FILES

Virus Report

Initialization of Chest files

Program will try to load all Chest files from the following server: (null)
FileID: 0000000001 Original file name: C:\WINDOWS\system32\kernel32.dll File category: 0
FileID: 0000000002 Original file name: C:\WINDOWS\system32\winsock.dll File category: 0
FileID: 0000000003 Original file name: C:\WINDOWS\system32\wsock32.dll File category: 0
FileID: 0000000004 Original file name: D:\Documents and Settings\Owner\Local Settings\Temp\76.tmp File category: 1
FileID: 0000000005 Original file name: D:\Documents and Settings\Owner\Local Settings\Temp\bb.exe File category: 1
FileID: 0000000006 Original file name: D:\Documents and Settings\Owner\Local Settings\Temp\GLFA3GLFA3.EXE File category: 1
FileID: 0000000007 Original file name: D:\Documents and Settings\Owner\Local Settings\Temp\GLFD2GLFD2.EXE File category: 1
FileID: 0000000008 Original file name: D:\Documents and Settings\Owner\Local Settings\Temp\tsinstall_4_0_3_7.exe File category: 1
FileID: 0000000009 Original file name: D:\Program Files\BullsEye Network\bin\adv.exe File category: 1
FileID: 0000000010 Original file name: D:\Program Files\BullsEye Network\bin\adx.exe File category: 1
FileID: 0000000011 Original file name: D:\Program Files\BullsEye Network\bin\bargains.exe File category: 1
FileID: 0000000012 Original file name: D:\Program Files\Common Files\tsa\rainbow\classify.dll File category: 1
FileID: 0000000013 Original file name: D:\Program Files\Common Files\tsa\ts2.exe File category: 1
FileID: 0000000014 Original file name: D:\Program Files\Common Files\tsa\ts1.exe File category: 1
FileID: 0000000015 Original file name: D:\Program Files\Common Files\tsa\ts12.exe File category: 1
FileID: 0000000016 Original file name: D:\Program Files\Common Files\tsa\tsm2.exe File category: 1
FileID: 0000000017 Original file name: D:\Program Files\Common Files\tsa\tsp2.exe File category: 1
FileID: 0000000018 Original file name: D:\Program Files\Common Files\tsa\tsuninst.exe File category: 1
FileID: 0000000019 Original file name: D:\Program Files\Internet Explorer\cdrjbovd.exe File category: 1
FileID: 0000000020 Original file name: D:\Program Files\Web_Rebates\WebRebates0.exe File category: 1
FileID: 0000000021 Original file name: D:\Program Files\Windows ControlAd\WinCtlAd.exe File category: 1
FileID: 0000000022 Original file name: D:\Program Files\Windows ControlAd\WinCtlAdAlt.exe File category: 1
FileID: 0000000023 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP10\A0008125.exe\zetzd:$DATA File category: 1
FileID: 0000000024 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP10\A0008128.ini\uypxb:$DATA File category: 1
FileID: 0000000025 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP10\A0008129.exe\mzzdv:$DATA File category: 1
FileID: 0000000026 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP10\A0008129.exe File category: 1
FileID: 0000000027 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP10\A0008182.exe\wofbo:$

DATA File category: 1
FileID: 0000000028 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0008797.ini\uypxb:$DATA File category: 1
FileID: 0000000029 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0008798.exe\mzzdv:$DATA File category: 1
FileID: 0000000030 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0008798.exe File category: 1
FileID: 0000000031 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0008799.exe\zetzd:$DATA File category: 1
FileID: 0000000032 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0008865.exe\wofbo:$DATA File category: 1
FileID: 0000000033 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009462.exe File category: 1
FileID: 0000000034 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009463.exe File category: 1
FileID: 0000000035 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009464.exe File category: 1
FileID: 0000000036 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009466.srg File category: 1
FileID: 0000000037 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009468.exe File category: 1
FileID: 0000000038 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009469.ini\uypxb:$DATA File category: 1
FileID: 0000000039 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009470.vxd File category: 1
FileID: 0000000040 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009471.exe File category: 1
FileID: 0000000041 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009472.exe File category: 1
FileID: 0000000042 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009473.exe\zetzd:$DATA File category: 1
FileID: 0000000043 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009482.exe File category: 1
FileID: 0000000044 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009483.exe File category: 1
FileID: 0000000045 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009484.vxd\C:\WINDOWS\System32\exdl.exe File category: 1
FileID: 0000000046 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009484.vxd\C:\WINDOWS\System32\mqexdlm.srg File category: 1
FileID: 0000000047 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009484.vxd\C:\WINDOWS\System32\exul.exe File category: 1
FileID: 0000000048 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009484.vxd\C:\WIND

OWS\System32\javexulm.vxd File category: 1
FileID: 0000000049 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009484.vxd\C:\WIND
OWS\System32\msexreg.exe File category: 1
FileID: 0000000050 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009484.vxd\C:\WIND
OWS\System32\instsrv.exe File category: 1
FileID: 0000000051 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009484.vxd\C:\WIND
OWS\System32\exclean.exe File category: 1
FileID: 0000000052 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009485.exe\mzzdv:$
DATA File category: 1
FileID: 0000000053 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009485.exe File
category: 1
FileID: 0000000054 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP11\A0009505.exe\wofbo:$
DATA File category: 1
FileID: 0000000055 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0009834.ini\uypxb:$
DATA File category: 1
FileID: 0000000056 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0009835.exe\mzzdv:$
DATA File category: 1
FileID: 0000000057 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0009835.exe File
category: 1
FileID: 0000000058 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0009836.exe\zetzd:$
DATA File category: 1
FileID: 0000000059 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010009.exe\wofbo:$
DATA File category: 1
FileID: 0000000060 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010148.exe File
category: 1
FileID: 0000000061 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010149.exe File
category: 1
FileID: 0000000062 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010150.vxd\C:\WIND
OWS\System32\exdl.exe File category: 1
FileID: 0000000063 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010150.vxd\C:\WIND
OWS\System32\mgexdlm.srg File category: 1
FileID: 0000000064 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010150.vxd\C:\WIND
OWS\System32\exul.exe File category: 1
FileID: 0000000065 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010150.vxd\C:\WIND
OWS\System32\javexulm.vxd File category: 1
FileID: 0000000066 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010150.vxd\C:\WIND
OWS\System32\msexreg.exe File category: 1
FileID: 0000000067 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010150.vxd\C:\WIND
OWS\System32\instsrv.exe File category: 1
FileID: 0000000068 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP12\A0010150.vxd\C:\WIND
OWS\System32\exclean.exe File category: 1
FileID: 0000000069 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010490.ini\uypxb:$

DATA File category: 1
FileID: 0000000070 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010491.exe\mzzdv:$DATA File category: 1
FileID: 0000000071 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010491.exe File category: 1
FileID: 0000000072 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010492.exe\zetzd:$DATA File category: 1
FileID: 0000000073 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010655.exe\wofbo:$DATA File category: 1
FileID: 0000000074 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010780.exe File category: 1
FileID: 0000000075 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010782.exe File category: 1
FileID: 0000000076 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010783.vxd\C:\WINDOWS\System32\exdl.exe File category: 1
FileID: 0000000077 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010783.vxd\C:\WINDOWS\System32\mqexdlm.srg File category: 1
FileID: 0000000078 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010783.vxd\C:\WINDOWS\System32\exul.exe File category: 1
FileID: 0000000079 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010783.vxd\C:\WINDOWS\System32\javexulm.vxd File category: 1
FileID: 0000000080 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010783.vxd\C:\WINDOWS\System32\msexreg.exe File category: 1
FileID: 0000000081 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010783.vxd\C:\WINDOWS\System32\instsrv.exe File category: 1
FileID: 0000000082 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP13\A0010783.vxd\C:\WINDOWS\System32\exclean.exe File category: 1
FileID: 0000000083 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP14\A0010850.exe\wofbo:$DATA File category: 1
FileID: 0000000084 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP14\A0010853.exe\zetzd:$DATA File category: 1
FileID: 0000000085 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP14\A0010855.ini\uypxb:$DATA File category: 1
FileID: 0000000086 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP14\A0010856.exe\mzzdv:$DATA File category: 1
FileID: 0000000087 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP14\A0010856.exe File category: 1
FileID: 0000000088 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP14\A0010917.exe File category: 1
FileID: 0000000089 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001420.exe\zetzd:$DATA File category: 1
FileID: 0000000090 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001421.dll File

category: 1
FileID: 0000000091 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001422.exe File category: 1
FileID: 0000000092 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001423.dll File category: 1
FileID: 0000000093 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001424.exe File category: 1
FileID: 0000000094 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001426.exe File category: 1
FileID: 0000000095 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001432.ini\uypxb:$DATA File category: 1
FileID: 0000000096 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001433.exe\mzzdv:$DATA File category: 1
FileID: 0000000097 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001433.exe File category: 1
FileID: 0000000098 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001435.exe\wofbo:$DATA File category: 1
FileID: 0000000099 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001679.exe File category: 1
FileID: 0000000100 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP2\A0001680.exe File category: 1
FileID: 0000000101 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0001751.exe\wofbo:$DATA File category: 1
FileID: 0000000102 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0001760.exe\zetzd:$DATA File category: 1
FileID: 0000000103 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0001764.ini\uypxb:$DATA File category: 1
FileID: 0000000104 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0001765.exe\mzzdv:$DATA File category: 1
FileID: 0000000105 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0001765.exe File category: 1
FileID: 0000000106 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002317.dll File category: 1
FileID: 0000000107 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002421.exe File category: 1
FileID: 0000000108 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002422.exe File category: 1
FileID: 0000000109 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002423.exe File category: 1
FileID: 0000000110 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002424.srg File category: 1
FileID: 0000000111 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002425.exe File

category: 1
FileID: 0000000112 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002426.vxd File category: 1
FileID: 0000000113 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002427.exe File category: 1
FileID: 0000000114 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002428.exe File category: 1
FileID: 0000000115 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002429.exe\zetzd:$DATA File category: 1
FileID: 0000000116 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002434.ini\uypxb:$DATA File category: 1
FileID: 0000000117 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002435.exe\mzzdv:$DATA File category: 1
FileID: 0000000118 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002435.exe File category: 1
FileID: 0000000119 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002437.exe File category: 1
FileID: 0000000120 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002438.exe File category: 1
FileID: 0000000121 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002439.vxd\C:\WINDOWS\System32\exdl.exe File category: 1
FileID: 0000000122 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002439.vxd\C:\WINDOWS\System32\mqexdlm.srg File category: 1
FileID: 0000000123 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002439.vxd\C:\WINDOWS\System32\exul.exe File category: 1
FileID: 0000000124 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002439.vxd\C:\WINDOWS\System32\javexulm.vxd File category: 1
FileID: 0000000125 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002439.vxd\C:\WINDOWS\System32\msexreg.exe File category: 1
FileID: 0000000126 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002439.vxd\C:\WINDOWS\System32\instsrv.exe File category: 1
FileID: 0000000127 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002439.vxd\C:\WINDOWS\System32\exclean.exe File category: 1
FileID: 0000000128 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002440.exe File category: 1
FileID: 0000000129 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0002481.exe\wofbo:$DATA File category: 1
FileID: 0000000130 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003419.exe File category: 1
FileID: 0000000131 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003420.srg File category: 1
FileID: 0000000132 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003421.exe File

category: 1
FileID: 0000000133 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003422.vxd File category: 1
FileID: 0000000134 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003424.exe File category: 1
FileID: 0000000135 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003425.exe File category: 1
FileID: 0000000136 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003426.exe\zetzd:$DATA File category: 1
FileID: 0000000137 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003431.ini\uypxb:$DATA File category: 1
FileID: 0000000138 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003432.exe\mzzdv:$DATA File category: 1
FileID: 0000000139 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003432.exe File category: 1
FileID: 0000000140 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003434.exe\wofbo:$DATA File category: 1
FileID: 0000000141 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003437.exe File category: 1
FileID: 0000000142 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003499.exe File category: 1
FileID: 0000000143 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003500.srg File category: 1
FileID: 0000000144 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003501.exe File category: 1
FileID: 0000000145 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003502.vxd File category: 1
FileID: 0000000146 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003504.exe File category: 1
FileID: 0000000147 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003505.exe File category: 1
FileID: 0000000148 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003506.exe\zetzd:$DATA File category: 1
FileID: 0000000149 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003511.ini\uypxb:$DATA File category: 1
FileID: 0000000150 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003512.exe\mzzdv:$DATA File category: 1
FileID: 0000000151 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003512.exe File category: 1
FileID: 0000000152 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003514.exe File category: 1
FileID: 0000000153 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003535.exe\wofbo:$DATA

ATA File category: 1
FileID: 0000000154 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0003552.exe File category: 1
FileID: 0000000155 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004460.exe File category: 1
FileID: 0000000156 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004461.exe File category: 1
FileID: 0000000157 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004462.exe File category: 1
FileID: 0000000158 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004463.srg File category: 1
FileID: 0000000159 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004464.exe File category: 1
FileID: 0000000160 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004465.vxd File category: 1
FileID: 0000000161 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004466.exe File category: 1
FileID: 0000000162 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004467.exe File category: 1
FileID: 0000000163 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004468.exe\zetzd:$D
ATA File category: 1
FileID: 0000000164 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004472.ini\uypxb:$D
ATA File category: 1
FileID: 0000000165 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004473.exe\mzzdv:$D
ATA File category: 1
FileID: 0000000166 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004473.exe File category: 1
FileID: 0000000167 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004475.exe File category: 1
FileID: 0000000168 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP3\A0004478.exe\wofbo:$D
ATA File category: 1
FileID: 0000000169 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0004544.ini\uypxb:$D
ATA File category: 1
FileID: 0000000170 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0004545.exe\mzzdv:$D
ATA File category: 1
FileID: 0000000171 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0004545.exe File category: 1
FileID: 0000000172 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0004546.exe\zetzd:$D
ATA File category: 1
FileID: 0000000173 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005009.exe File category: 1
FileID: 0000000174 Original file name: D:\System Volume Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005010.exe File

category: 1
FileID: 0000000175 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005011.vxd\C:\WINDO
WS\System32\exdl.exe File category: 1
FileID: 0000000176 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005011.vxd\C:\WINDO
WS\System32\mqexdlm.srg File category: 1
FileID: 0000000177 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005011.vxd\C:\WINDO
WS\System32\exul.exe File category: 1
FileID: 0000000178 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005011.vxd\C:\WINDO
WS\System32\javexulm.vxd File category: 1
FileID: 0000000179 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005011.vxd\C:\WINDO
WS\System32\msexreg.exe File category: 1
FileID: 0000000180 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005011.vxd\C:\WINDO
WS\System32\instsrv.exe File category: 1
FileID: 0000000181 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP4\A0005011.vxd\C:\WINDO
WS\System32\exclean.exe File category: 1
FileID: 0000000182 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005160.ini\uypxb:$D
ATA File category: 1
FileID: 0000000183 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005161.exe\mzzdv:$D
ATA File category: 1
FileID: 0000000184 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005161.exe File
category: 1
FileID: 0000000185 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005162.exe\zetzd:$D
ATA File category: 1
FileID: 0000000186 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005563.exe\wofbo:$D
ATA File category: 1
FileID: 0000000187 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005596.exe File
category: 1
FileID: 0000000188 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005598.exe File
category: 1
FileID: 0000000189 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005600.vxd\C:\WINDO
WS\System32\exdl.exe File category: 1
FileID: 0000000190 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005600.vxd\C:\WINDO
WS\System32\mqexdlm.srg File category: 1
FileID: 0000000191 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005600.vxd\C:\WINDO
WS\System32\exul.exe File category: 1
FileID: 0000000192 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005600.vxd\C:\WINDO
WS\System32\javexulm.vxd File category: 1
FileID: 0000000193 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005600.vxd\C:\WINDO
WS\System32\msexreg.exe File category: 1
FileID: 0000000194 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005600.vxd\C:\WINDO
WS\System32\instsrv.exe File category: 1
FileID: 0000000195 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP5\A0005600.vxd\C:\WINDO

WS\System32\exclean.exe File category: 1
FileID: 0000000196 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0005773.exe\zetzd:$D
ATA File category: 1
FileID: 0000000197 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0005775.ini\uypxb:$D
ATA File category: 1
FileID: 0000000198 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0005776.exe\mzzdv:$D
ATA File category: 1
FileID: 0000000199 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0005776.exe File
category: 1
FileID: 0000000200 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0005806.exe File
category: 1
FileID: 0000000201 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006180.exe\wofbo:$D
ATA File category: 1
FileID: 0000000202 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006224.exe File
category: 1
FileID: 0000000203 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006233.exe File
category: 1
FileID: 0000000204 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006334.vxd\C:\WINDO
WS\System32\exdl.exe File category: 1
FileID: 0000000205 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006334.vxd\C:\WINDO
WS\System32\mqexdlm.srg File category: 1
FileID: 0000000206 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006334.vxd\C:\WINDO
WS\System32\exul.exe File category: 1
FileID: 0000000207 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006334.vxd\C:\WINDO
WS\System32\javexulm.vxd File category: 1
FileID: 0000000208 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006334.vxd\C:\WINDO
WS\System32\msexreg.exe File category: 1
FileID: 0000000209 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006334.vxd\C:\WINDO
WS\System32\instsrv.exe File category: 1
FileID: 0000000210 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP6\A0006334.vxd\C:\WINDO
WS\System32\exclean.exe File category: 1
FileID: 0000000211 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006448.ini\uypxb:$D
ATA File category: 1
FileID: 0000000212 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006449.exe\mzzdv:$D
ATA File category: 1
FileID: 0000000213 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006449.exe File
category: 1
FileID: 0000000214 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006450.exe\zetzd:$D
ATA File category: 1
FileID: 0000000215 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006941.exe File
category: 1
FileID: 0000000216 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006942.exe File

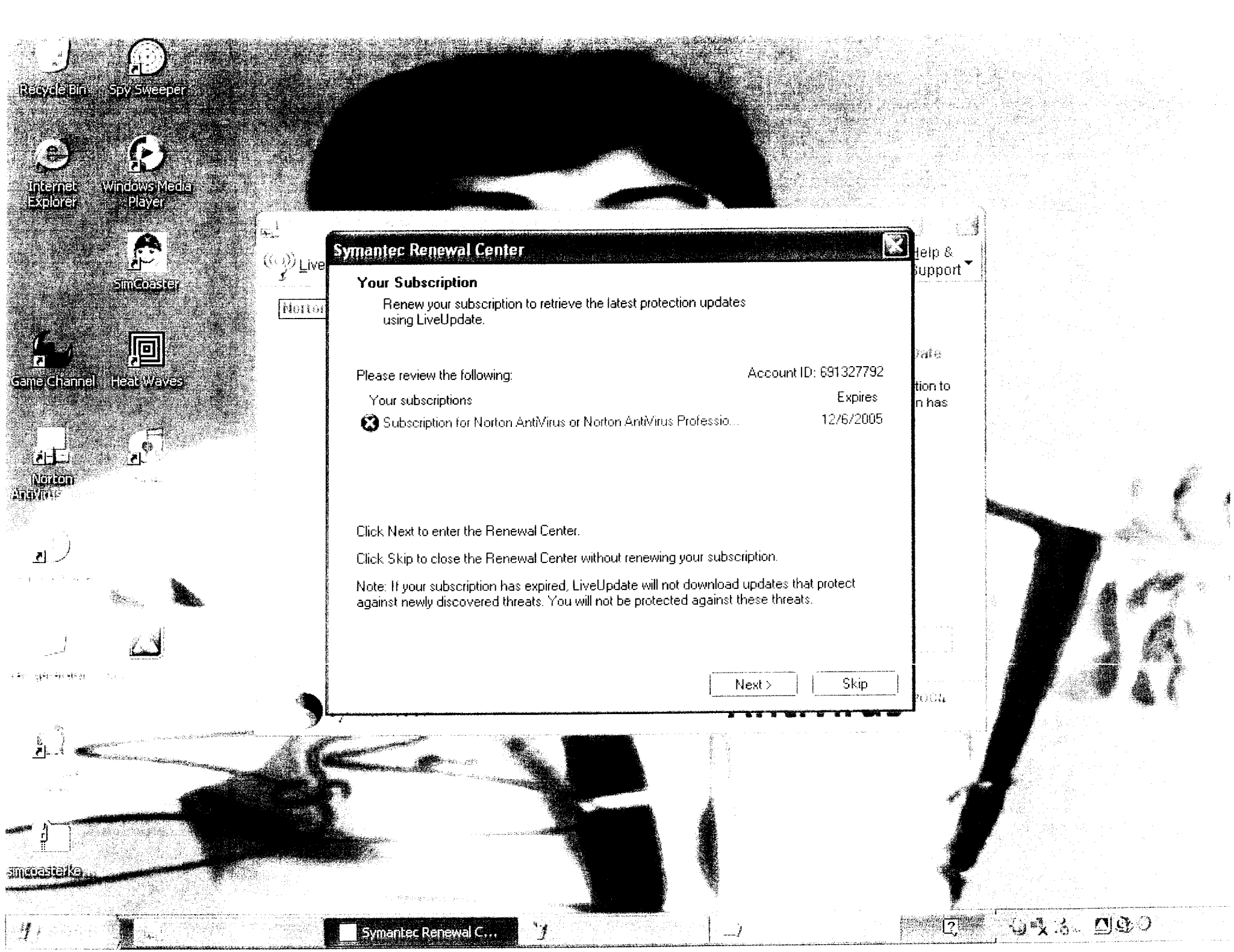
category: 1
FileID: 0000000217 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006944.vxd\C:\WINDO
WS\System32\exdl.exe File category: 1
FileID: 0000000218 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006944.vxd\C:\WINDO
WS\System32\mqexdlm.srg File category: 1
FileID: 0000000219 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006944.vxd\C:\WINDO
WS\System32\exul.exe File category: 1
FileID: 0000000220 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006944.vxd\C:\WINDO
WS\System32\javexulm.vxd File category: 1
FileID: 0000000221 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006944.vxd\C:\WINDO
WS\System32\msexreg.exe File category: 1
FileID: 0000000222 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006944.vxd\C:\WINDO
WS\System32\instsrv.exe File category: 1
FileID: 0000000223 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006944.vxd\C:\WINDO
WS\System32\exclean.exe File category: 1
FileID: 0000000224 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006948.exe File
category: 1
FileID: 0000000225 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006949.exe File
category: 1
FileID: 0000000226 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006950.exe File
category: 1
FileID: 0000000227 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006951.dll File
category: 1
FileID: 0000000228 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006952.exe File
category: 1
FileID: 0000000229 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006953.exe File
category: 1
FileID: 0000000230 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006955.dll File
category: 1
FileID: 0000000231 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006956.exe File
category: 1
FileID: 0000000232 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006958.dll File
category: 1
FileID: 0000000233 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP7\A0006959.exe\wofbo:$D
ATA File category: 1
FileID: 0000000234 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP8\A0007093.ini\uypxb:$D
ATA File category: 1
FileID: 0000000235 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP8\A0007094.exe\mzzdv:$D
ATA File category: 1
FileID: 0000000236 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP8\A0007094.exe File
category: 1
FileID: 0000000237 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP8\A0007095.exe\zetzd:$D

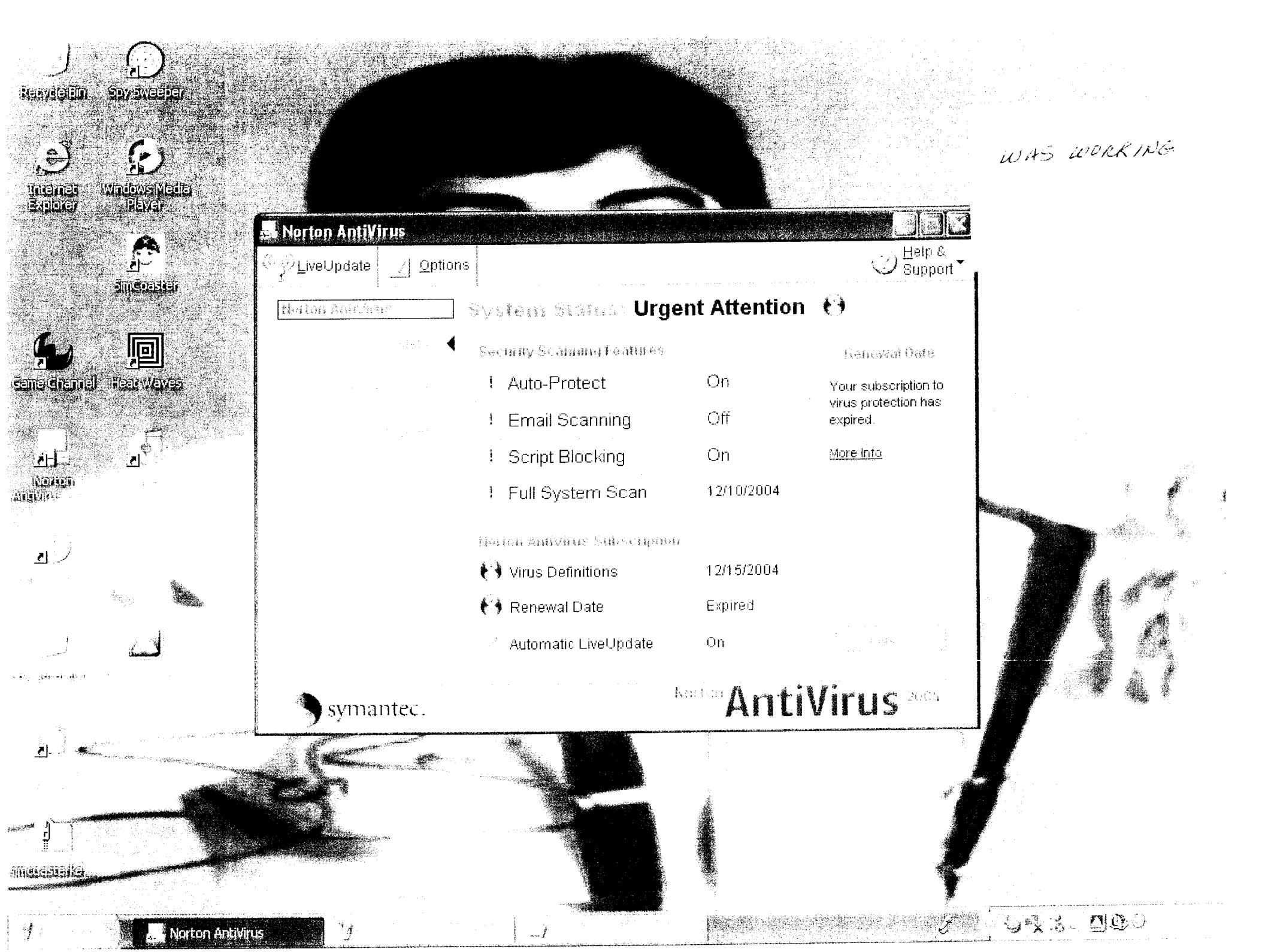
ATA File category: 1
FileID: 0000000238 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP9\A0007259.exe\zetzd:$D
ATA File category: 1
FileID: 0000000239 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP9\A0007261.ini\uypxb:$D
ATA File category: 1
FileID: 0000000240 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP9\A0007262.exe\mzzdv:$D
ATA File category: 1
FileID: 0000000241 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP9\A0007262.exe File
category: 1
FileID: 0000000242 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP9\A0007477.exe\wofbo:$D
ATA File category: 1
FileID: 0000000243 Original file name: D:\System Volume
Information_restore{F20DC6C2-5212-4F33-8959-AB7D05D4CDB6}\RP9\A0007685.exe File
category: 1
FileID: 0000000244 Original file name: D:\temp\NCasePackage.exe File category: 1
FileID: 0000000245 Original file name: D:\temp\pootz_58.exe File category: 1
FileID: 0000000246 Original file name: D:\temp\powersetup.exe\powerscan.exe File
category: 1
FileID: 0000000247 Original file name: D:\temp\salm.exe File category: 1
FileID: 0000000248 Original file name: D:\temp\salmhook.dll File category: 1
FileID: 0000000249 Original file name: D:\WINDOWS\COM+.log\dlxpd:$DATA File
category: 1
FileID: 0000000250 Original file name: D:\WINDOWS\Downloaded Program
Files\webdlg32.dll File category: 1
FileID: 0000000251 Original file name: D:\WINDOWS\hh.exe\zetzd:$DATA File
category: 1
FileID: 0000000252 Original file name: D:\WINDOWS\mfsngd.exe File category: 1
FileID: 0000000253 Original file name: D:\WINDOWS\msdfmap.ini\uypxb:$DATA File
category: 1
FileID: 0000000254 Original file name: D:\WINDOWS\msxmidi.exe File category: 1
FileID: 0000000255 Original file name: D:\WINDOWS\netzd32.exe\mzzdv:$DATA File
category: 1
FileID: 0000000256 Original file name: D:\WINDOWS\netzd32.exe File category: 1
FileID: 0000000257 Original file name: D:\WINDOWS\n_bukeoc.log File category: 1
FileID: 0000000258 Original file name: D:\WINDOWS\n_kxevvk.log File category: 1
FileID: 0000000259 Original file name: D:\WINDOWS\syscr.dll File category: 1
FileID: 0000000260 Original file name: D:\WINDOWS\system32\angelex.exe File
category: 1
FileID: 0000000261 Original file name: D:\WINDOWS\system32\crkz.exe File category:
1
FileID: 0000000262 Original file name: D:\WINDOWS\system32\exclean.exe File
category: 1
FileID: 0000000263 Original file name: D:\WINDOWS\system32\exdl.exe File category:
1
FileID: 0000000264 Original file name: D:\WINDOWS\system32\exdl0.exe File
category: 1
FileID: 0000000265 Original file name: D:\WINDOWS\system32\exdl1.exe File
category: 1
FileID: 0000000266 Original file name: D:\WINDOWS\system32\exul.exe File category:
1
FileID: 0000000267 Original file name: D:\WINDOWS\system32\exul1.exe File
category: 1
FileID: 0000000268 Original file name: D:\WINDOWS\system32\instsrv.exe File
category: 1
FileID: 0000000269 Original file name: D:\WINDOWS\system32\javexulm.vxd File
category: 1
FileID: 0000000270 Original file name: D:\WINDOWS\system32\mac80ex.idf\C:\Program
Files\BullsEye Network\bin\bargains.exe File category: 1

Virus Report

FileID: 0000000271 Original file name: D:\WINDOWS\system32\mac80ex.idf\C:\Program Files\BullsEye Network\bin\adv.exe File category: 1
FileID: 0000000272 Original file name: D:\WINDOWS\system32\mac80ex.idf\C:\Program Files\BullsEye Network\bin\adx.exe File category: 1
FileID: 0000000273 Original file name: D:\WINDOWS\system32\mqexdlm.srg File category: 1
FileID: 0000000274 Original file name: D:\WINDOWS\system32\msexreg.exe File category: 1
FileID: 0000000275 Original file name: D:\WINDOWS\system32\netbm32.dll File category: 1
FileID: 0000000276 Original file name: D:\WINDOWS\system32\netut80ex.vxd\C:\WINDOWS\System32\exdl.exe File category: 1
FileID: 0000000277 Original file name: D:\WINDOWS\system32\netut80ex.vxd\C:\WINDOWS\System32\mqexdlm.srg File category: 1
FileID: 0000000278 Original file name: D:\WINDOWS\system32\netut80ex.vxd\C:\WINDOWS\System32\exul.exe File category: 1
FileID: 0000000279 Original file name: D:\WINDOWS\system32\netut80ex.vxd\C:\WINDOWS\System32\javexulm.vxd File category: 1
FileID: 0000000280 Original file name: D:\WINDOWS\system32\netut80ex.vxd\C:\WINDOWS\System32\msexreg.exe File category: 1
FileID: 0000000281 Original file name: D:\WINDOWS\system32\netut80ex.vxd\C:\WINDOWS\System32\instsrv.exe File category: 1
FileID: 0000000282 Original file name: D:\WINDOWS\system32\netut80ex.vxd\C:\WINDOWS\System32\exclean.exe File category: 1
FileID: 0000000283 Original file name: D:\WINDOWS\system32\sdkiu.exe File category: 1
FileID: 0000000284 Original file name: D:\WINDOWS\system32\trkgif.exe File category: 1
FileID: 0000000285 Original file name: D:\WINDOWS\tsoc.log\zzyhx:$DATA File category: 1
FileID: 0000000286 Original file name: D:\WINDOWS\weffo.dll File category: 1
FileID: 0000000287 Original file name: D:\WINDOWS\winhlp32.exe\wofbo:$DATA File category: 1
FileID: 0000000288 Original file name: D:\WINDOWS\WINNT32.LOG\opygi:$DATA File category: 1
FileID: 0000000289 Original file name: D:\WINDOWS\zeta.exe File category: 1

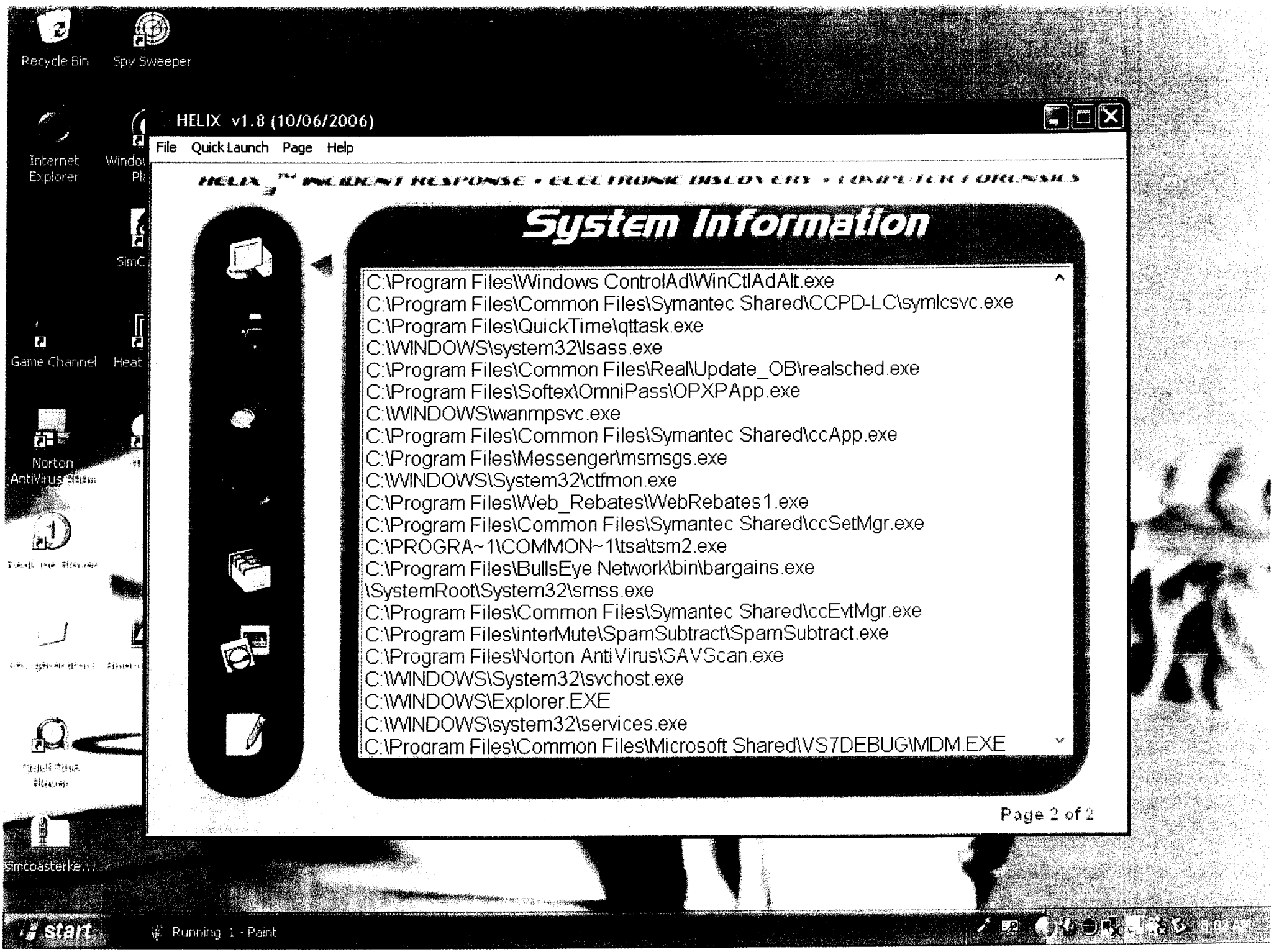
Exhibit 13

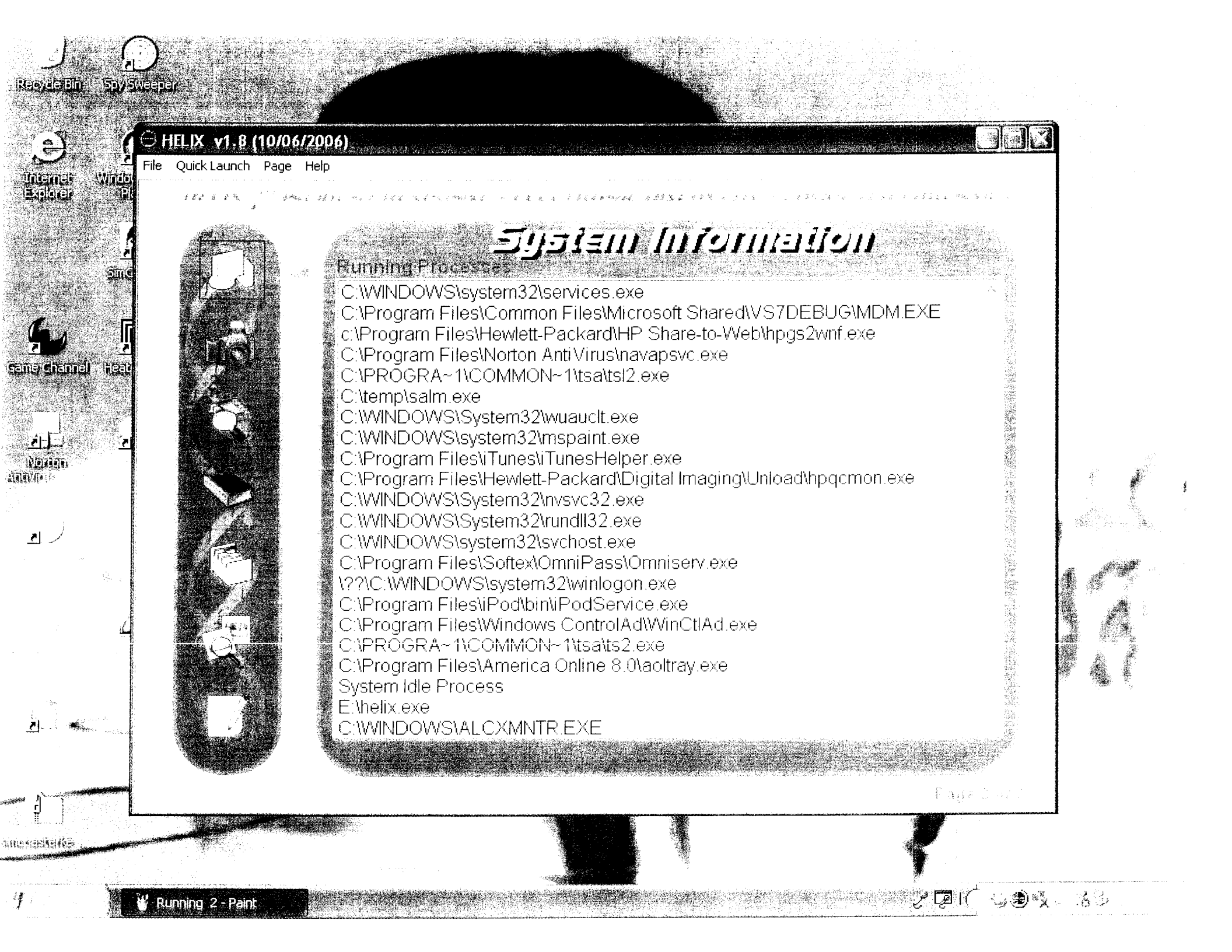

Recycle Bin
Spy Sweeper
Internet Explorer
Windows Media Player
SimCoaster
Game Channel
Heat Waves
Norton AntiVirus
simcoaster.ke
Symantec Renewal Center
Your Subscription
Renew your subscription to retrieve the latest protection updates using LiveUpdate.
Please review the following:
Account ID: 691327792
Your subscriptions
Expires
Subscription for Norton AntiVirus or Norton AntiVirus Professio...
12/6/2005
Click Next to enter the Renewal Center.
Click Skip to close the Renewal Center without renewing your subscription.
Note: If your subscription has expired, LiveUpdate will not download updates that protect against newly discovered threats. You will not be protected against these threats.
Next >
Skip
Help & Support
Symantec Renewal C...


Recycle Bin
Spy Sweeper
Internet Explorer
Windows Media Player
SimCoaster
Game Channel
Heat Waves
Norton AntiVirus
LiveUpdate
Options
Help & Support
System Status: Urgent Attention
Security Scanning Features
Renewal Date
! Auto-Protect On
! Email Scanning Off
! Script Blocking On
! Full System Scan 12/10/2004
Your subscription to virus protection has expired.
More Info
Norton AntiVirus Subscription
Virus Definitions 12/15/2004
Renewal Date Expired
Automatic LiveUpdate On
symantec.
Norton AntiVirus
Norton AntiVirus

WAS WORKING

Exhibit 14


Recycle Bin
Spy Sweeper
Internet Explorer
HELIX v1.8 (10/06/2006)
File
Quick Launch
Page
Help
System Information
C:\Program Files\Windows ControlAd\WinCtlAdAlt.exe
C:\Program Files\Common Files\Symantec Shared\CCPD-LC\symlcsvc.exe
C:\Program Files\QuickTime\qttask.exe
C:\WINDOWS\system32\lsass.exe
C:\Program Files\Common Files\Real\Update_OB\realsched.exe
C:\Program Files\Softex\OmniPass\OPXPApp.exe
C:\WINDOWS\wanmpsvc.exe
C:\Program Files\Common Files\Symantec Shared\ccApp.exe
C:\Program Files\Messenger\msmsgs.exe
C:\WINDOWS\System32\ctfmon.exe
C:\Program Files\Web_Rebates\WebRebates1.exe
C:\Program Files\Common Files\Symantec Shared\ccSetMgr.exe
C:\PROGRA~1\COMMON~1\tsa\tsm2.exe
C:\Program Files\BullsEye Network\bin\bargains.exe
\SystemRoot\System32\smss.exe
C:\Program Files\Common Files\Symantec Shared\ccEvtMgr.exe
C:\Program Files\interMute\SpamSubtract\SpamSubtract.exe
C:\Program Files\Norton AntiVirus\SAVScan.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\services.exe
C:\Program Files\Common Files\Microsoft Shared\VS7DEBUG\MDM.EXE
Page 2 of 2
start
Running 1 - Paint


Recycle Bin
Spy Sweeper
Internet Explorer
HELIX v1.8 (10/06/2006)
File
Quick Launch
Page
Help
System Information
Running Processes
C:\WINDOWS\system32\services.exe
C:\Program Files\Common Files\Microsoft Shared\VS7DEBUG\MDM.EXE
c:\Program Files\Hewlett-Packard\HP Share-to-Web\hpgs2wnf.exe
C:\Program Files\Norton AntiVirus\navapsvc.exe
C:\PROGRA~1\COMMON~1\tsa\tsl2.exe
C:\temp\salm.exe
C:\WINDOWS\System32\wuauclt.exe
C:\WINDOWS\system32\mspaint.exe
C:\Program Files\iTunes\iTunesHelper.exe
C:\Program Files\Hewlett-Packard\Digital Imaging\Unload\hpqcmon.exe
C:\WINDOWS\System32\nvsvc32.exe
C:\WINDOWS\System32\rundll32.exe
C:\WINDOWS\system32\svchost.exe
C:\Program Files\Softex\OmniPass\Omniserv.exe
\??\C:\WINDOWS\system32\winlogon.exe
C:\Program Files\iPod\bin\iPodService.exe
C:\Program Files\Windows ControlAd\WinCtlAd.exe
C:\PROGRA~1\COMMON~1\tsa\ts2.exe
C:\Program Files\America Online 8.0\aoltray.exe
System Idle Process
E:\helix.exe
C:\WINDOWS\ALCXMNTR.EXE
Running 2 - Paint

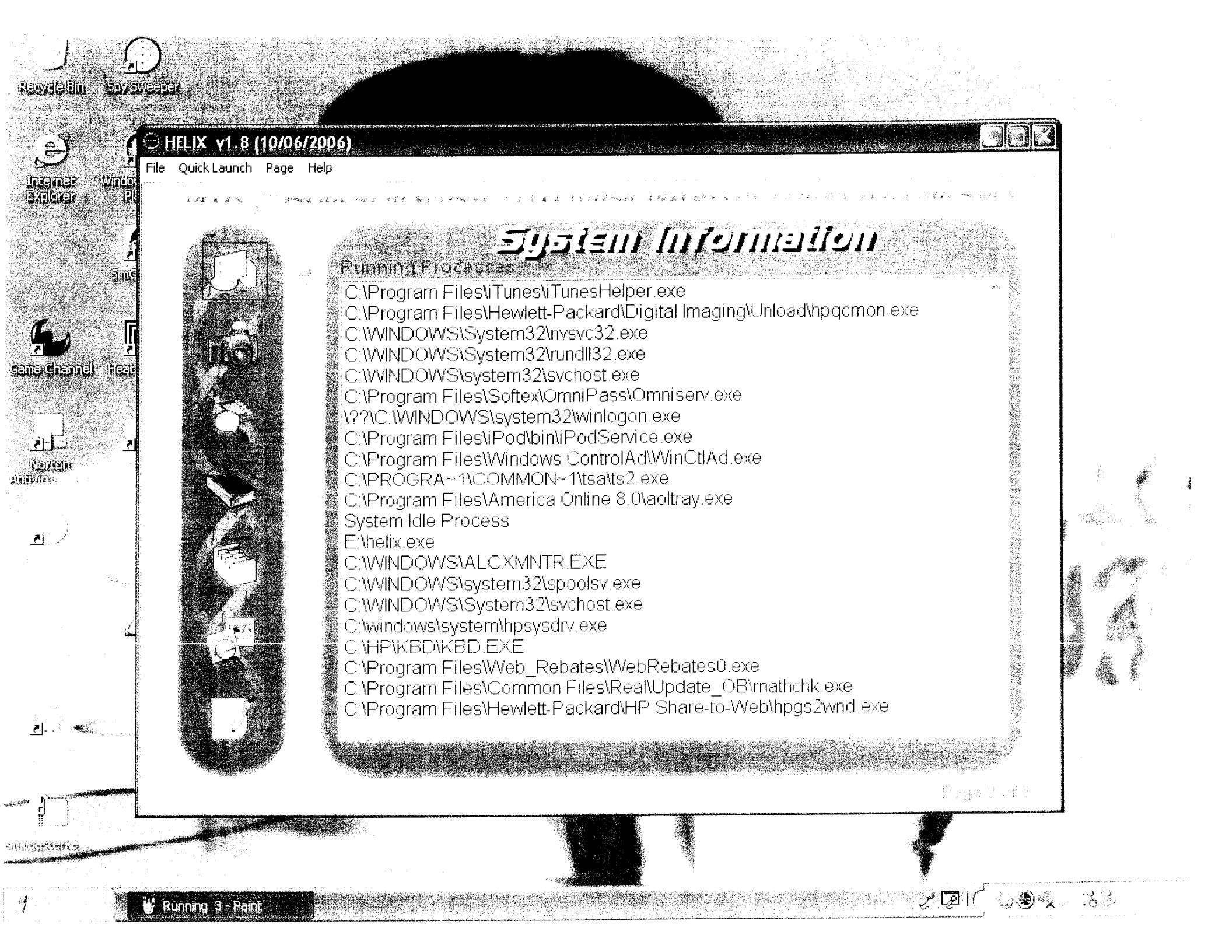
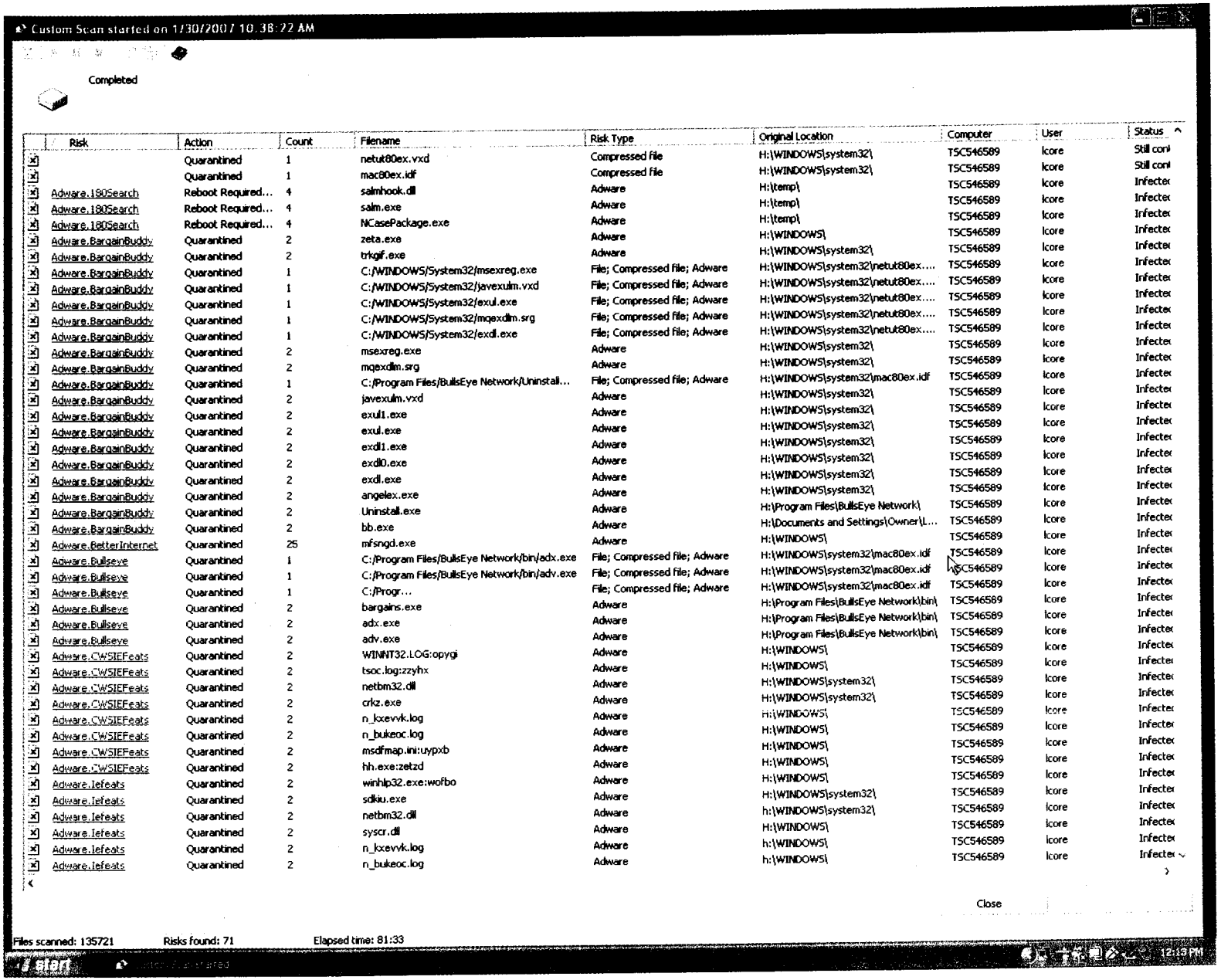
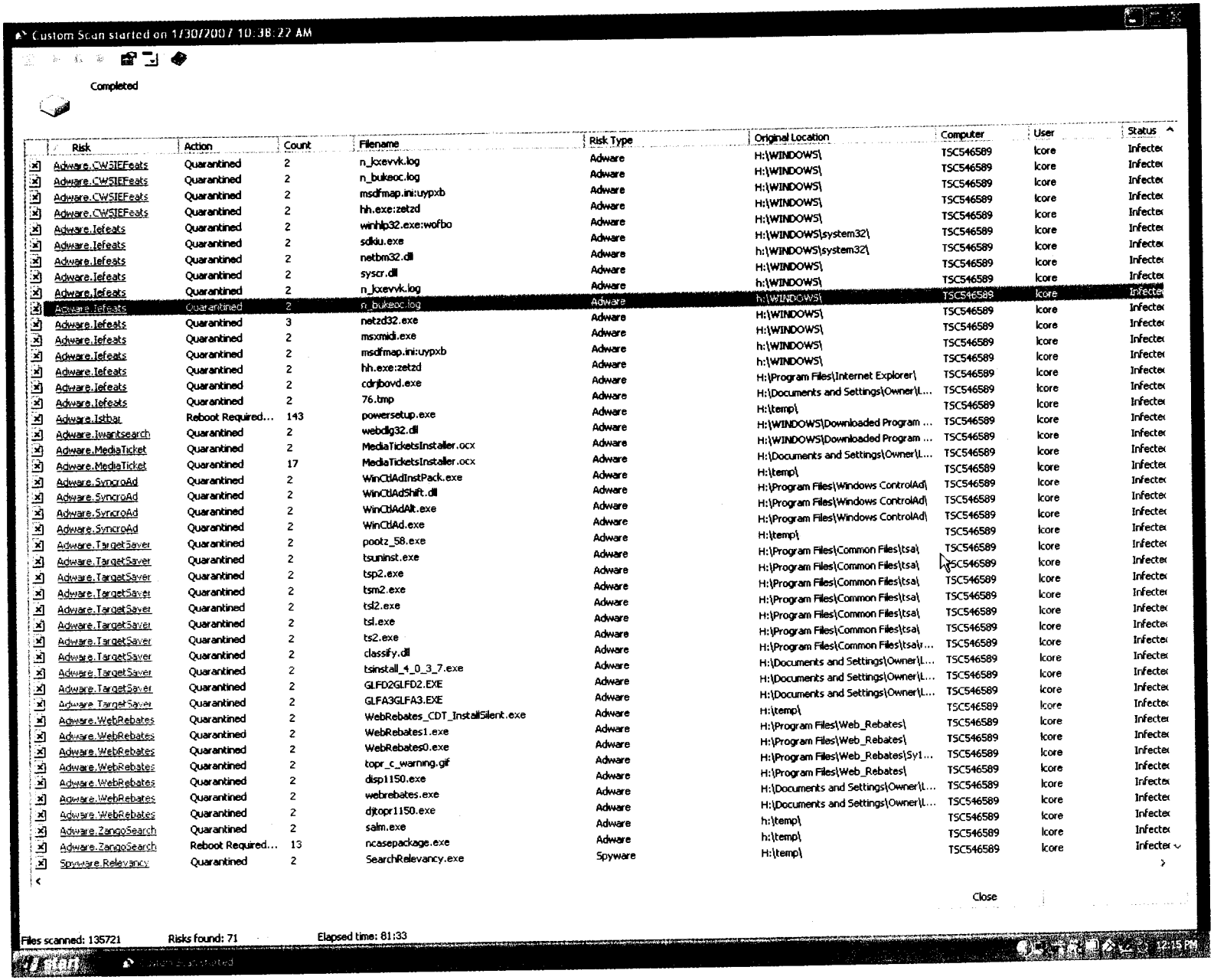

Recycle Bin
Spy Sweeper
Internet Explorer
Game Channel
HELIX v1.8 (10/06/2006)
File
Quick Launch
Page
Help
System Information
Running Processes
C:\Program Files\iTunes\iTunesHelper.exe
C:\Program Files\Hewlett-Packard\Digital Imaging\Unload\hpqcmon.exe
C:\WINDOWS\System32\nvsvc32.exe
C:\WINDOWS\System32\rundll32.exe
C:\WINDOWS\system32\svchost.exe
C:\Program Files\Softex\OmniPass\Omniserv.exe
\??\C:\WINDOWS\system32\winlogon.exe
C:\Program Files\iPod\bin\iPodService.exe
C:\Program Files\Windows ControlAd\WinCtlAd.exe
C:\PROGRA~1\COMMON~1\tsa\ts2.exe
C:\Program Files\America Online 8.0\aoltray.exe
System Idle Process
E:\helix.exe
C:\WINDOWS\ALCXMNTR.EXE
C:\WINDOWS\system32\spoolsv.exe
C:\WINDOWS\System32\svchost.exe
C:\windows\system\hpsysdrv.exe
C:\HP\KBD\KBD.EXE
C:\Program Files\Web_Rebates\WebRebates0.exe
C:\Program Files\Common Files\Real\Update_OB\rnathchk.exe
C:\Program Files\Hewlett-Packard\HP Share-to-Web\hpgs2wnd.exe
Running 3 - Paint

Exhibit 15


Custom Scan started on 1/30/2007 10:38:22 AM
Completed
Risk
Action
Count
Filename
Risk Type
Original Location
Computer
User
Status
Quarantined 1 netut80ex.vxd Compressed file H:\WINDOWS\system32\ TSC546589 lcore Still cont
Quarantined 1 mac80ex.idf Compressed file H:\WINDOWS\system32\ TSC546589 lcore Still cont
Adware.180Search Reboot Required... 4 salmhook.dll Adware H:\temp\ TSC546589 lcore Infected
Adware.180Search Reboot Required... 4 salm.exe Adware H:\temp\ TSC546589 lcore Infected
Adware.180Search Reboot Required... 4 MCasePackage.exe Adware H:\temp\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 zeta.exe Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 trkgif.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 1 C:/WINDOWS/System32/msexreg.exe File; Compressed file; Adware H:\WINDOWS\system32\netut80ex.... TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 1 C:/WINDOWS/System32/javexulm.vxd File; Compressed file; Adware H:\WINDOWS\system32\netut80ex.... TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 1 C:/WINDOWS/System32/exul.exe File; Compressed file; Adware H:\WINDOWS\system32\netut80ex.... TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 1 C:/WINDOWS/System32/mqexdlm.srg File; Compressed file; Adware H:\WINDOWS\system32\netut80ex.... TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 1 C:/WINDOWS/System32/exdl.exe File; Compressed file; Adware H:\WINDOWS\system32\netut80ex.... TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 msexreg.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 mqexdlm.srg Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 1 C:/Program Files/BullsEye Network/Uninstall... File; Compressed file; Adware H:\WINDOWS\system32\mac80ex.idf TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 javexulm.vxd Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 exul1.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 exul.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 exdl1.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 exdl0.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 exdl.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 angelex.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 Uninstall.exe Adware H:\Program Files\BullsEye Network\ TSC546589 lcore Infected
Adware.BargainBuddy Quarantined 2 bb.exe Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.BetterInternet Quarantined 25 mfsngd.exe Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Bullseye Quarantined 1 C:/Program Files/BullsEye Network/bin/adx.exe File; Compressed file; Adware H:\WINDOWS\system32\mac80ex.idf TSC546589 lcore Infected
Adware.Bullseye Quarantined 1 C:/Program Files/BullsEye Network/bin/adv.exe File; Compressed file; Adware H:\WINDOWS\system32\mac80ex.idf TSC546589 lcore Infected
Adware.Bullseye Quarantined 1 C:/Progr... File; Compressed file; Adware H:\WINDOWS\system32\mac80ex.idf TSC546589 lcore Infected
Adware.Bullseye Quarantined 2 bargains.exe Adware H:\Program Files\BullsEye Network\bin\ TSC546589 lcore Infected
Adware.Bullseye Quarantined 2 adx.exe Adware H:\Program Files\BullsEye Network\bin\ TSC546589 lcore Infected
Adware.Bullseye Quarantined 2 adv.exe Adware H:\Program Files\BullsEye Network\bin\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 WINNT32.LOG:opygi Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 tsoc.log:zzyhx Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 netbm32.dll Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 crkz.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 n_kxevvk.log Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 n_bukeoc.log Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 msdfmap.ini:uypxb Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 hh.exe:zetzd Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 winhlp32.exe:wofbo Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 sdkiu.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 netbm32.dll Adware h:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 syscr.dll Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 n_kxevvk.log Adware h:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 n_bukeoc.log Adware h:\WINDOWS\ TSC546589 lcore Infected
Close
Files scanned: 135721
Risks found: 71
Elapsed time: 81:33
start
12:19 PM


Custom Scan started on 1/30/2007 10:38:27 AM
Completed
Risk
Action
Count
Filename
Risk Type
Original Location
Computer
User
Status
Adware.CWSIEFeats Quarantined 2 n_lxcevvk.log Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 n_bukeoc.log Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 msdfmap.ini:uypxb Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.CWSIEFeats Quarantined 2 hh.exe:zetzd Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 winhlp32.exe:wofbo Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 sdiku.exe Adware H:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 netbm32.dll Adware h:\WINDOWS\system32\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 syscr.dll Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 n_lxcevvk.log Adware h:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 n_bukeoc.log Adware h:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 3 netzd32.exe Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 msxmidi.exe Adware H:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 msdfmap.ini:uypxb Adware h:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 hh.exe:zetzd Adware h:\WINDOWS\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 cdnjbovd.exe Adware H:\Program Files\Internet Explorer\ TSC546589 lcore Infected
Adware.Iefeats Quarantined 2 76.tmp Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.Istbar Reboot Required... 143 powersetup.exe Adware H:\temp\ TSC546589 lcore Infected
Adware.Iwantsearch Quarantined 2 webdlg32.dll Adware H:\WINDOWS\Downloaded Program ... TSC546589 lcore Infected
Adware.MediaTicket Quarantined 2 MediaTicketsInstaller.ocx Adware H:\WINDOWS\Downloaded Program ... TSC546589 lcore Infected
Adware.MediaTicket Quarantined 17 MediaTicketsInstaller.ocx Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.SyncroAd Quarantined 2 WinCtlAdInstPack.exe Adware H:\temp\ TSC546589 lcore Infected
Adware.SyncroAd Quarantined 2 WinCtlAdShift.dll Adware H:\Program Files\Windows ControlAd\ TSC546589 lcore Infected
Adware.SyncroAd Quarantined 2 WinCtlAdAlt.exe Adware H:\Program Files\Windows ControlAd\ TSC546589 lcore Infected
Adware.SyncroAd Quarantined 2 WinCtlAd.exe Adware H:\Program Files\Windows ControlAd\ TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 pootz_58.exe Adware H:\temp\ TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 tsuninst.exe Adware H:\Program Files\Common Files\tsa\ TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 tsp2.exe Adware H:\Program Files\Common Files\tsa\ TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 tsm2.exe Adware H:\Program Files\Common Files\tsa\ TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 tsl2.exe Adware H:\Program Files\Common Files\tsa\ TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 tsl.exe Adware H:\Program Files\Common Files\tsa\ TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 ts2.exe Adware H:\Program Files\Common Files\tsa\r... TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 classify.dll Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 tsinstall_4_0_3_7.exe Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 GLFD2GLFD2.EXE Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.TargetSaver Quarantined 2 GLFA3GLFA3.EXE Adware H:\temp\ TSC546589 lcore Infected
Adware.WebRebates Quarantined 2 WebRebates_CDT_InstallSilent.exe Adware H:\Program Files\Web_Rebates\ TSC546589 lcore Infected
Adware.WebRebates Quarantined 2 WebRebates1.exe Adware H:\Program Files\Web_Rebates\ TSC546589 lcore Infected
Adware.WebRebates Quarantined 2 WebRebates0.exe Adware H:\Program Files\Web_Rebates\Sy1... TSC546589 lcore Infected
Adware.WebRebates Quarantined 2 topr_c_warning.gif Adware H:\Program Files\Web_Rebates\ TSC546589 lcore Infected
Adware.WebRebates Quarantined 2 disp1150.exe Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.WebRebates Quarantined 2 webrebates.exe Adware H:\Documents and Settings\Owner\L... TSC546589 lcore Infected
Adware.WebRebates Quarantined 2 djtopr1150.exe Adware h:\temp\ TSC546589 lcore Infected
Adware.ZangoSearch Quarantined 2 salm.exe Adware h:\temp\ TSC546589 lcore Infected
Adware.ZangoSearch Reboot Required... 13 ncasepackage.exe Adware H:\temp\ TSC546589 lcore Infected
Spyware.Relevancy Quarantined 2 SearchRelevancy.exe Spyware
Close
Files scanned: 135721
Risks found: 71
Elapsed time: 81:33