



Enter your e-mail address to get a free subscription.



We **guarantee your privacy**: 1. We will never sell, rent, or give away your address to any outside party, ever. 2. We will never send you any unrequested e-mail, besides newsletter updates. 3. All unsubscribe requests are honored immediately, period. [Privacy policy](#)

[Home](#) [Newsletter](#) [WinFind](#) [Reviews](#) [Polls](#) [Contact](#)
[This issue](#) [Past issues](#) [Upgrade](#) [Prefs](#) [Unsubscribe](#)

Windows Secrets Newsletter • Issue 97 • 2007-02-22 • Circulation: over 265,000



Get the tips you need, before you need 'em

It's great to see the reviews that ordinarily hard-nosed critics are giving to the latest Secrets book. "To really appreciate what is in Vista, you almost need to read through the leading book on the product, *Windows Vista Secrets*, by Brian Livingston and Paul Thurrott," writes Rob Enderle, principal analyst of the Enderle Group, in [TechNewsWorld](#). "It's 595 pages of things you can do with this product — most of which you probably wouldn't have discovered for some time, let alone right at first." Check the book out now for tips you can use. — *Brian Livingston, Editorial Director*

For more information: [United States](#) / [Canada](#) / [Elsewhere](#)

TOP STORY	Pop-up ads can land you in jail
LANGALIST TIPS	Make more space by deleting log files
USEFUL LINKS	Now, rechargeable batteries you can rely on
WACKY WEB WEEK	Gollum and Smeagol get their groove on
LANGALIST PLUS	Avoid firewall confusion with insider secrets
WOODY'S WINDOWS	Vista Timesaver #4 — the Windows Experience Index
PATCH WATCH	Don't install drivers from Microsoft Update
YOUR SUBSCRIPTION	How to change your address or unsubscribe

For links to every subtopic in this issue, scroll down to the [Index](#)

External links open in a new window

ADS



Simplify Windows server backup & restore

Easy to install, use & maintain Windows backup software. Supports Exchange, Active Directory, MS-SQL, and Open Files. Client/server solution designed for small business, disk-based storage with drive spanning to grow with you. Free download.

www.Backup-for-Workgroups.com



Keep your surfing safe

Block threats permitted through your firewall & secure vulnerable applications. LinkScanner Pro ensures data passing through your firewall is checked for exploits & other security breaches. Stop attacks while you search & browse the Web. Only 2.95MB

www.explabs.com



Free PC performance scan

Run PC Pitstop's free optimize scan to automatically diagnose problems with your computer and receive a custom report detailing how you can speed up your system without the expense or hassle of adding new hardware.

www.pcpitstop.com

[See your ad here](#)

TOP STORY

Pop-up ads can land you in jail



By Ryan Russell

If you find yourself the victim of pop-up ads on a computer, with children in the vicinity, you could face decades in prison.

I wish that I was exaggerating or being sensationalistic, but for Julie Amero this is far too real.

Meet Julie Amero, substitute teacher

There's a good chance that you've already heard something about Julie. She's perhaps better known as the Connecticut substitute schoolteacher who's been convicted of "child endangerment." She now faces a sentence of up to 40 years in prison because porn pop-ups appeared on a school computer.

For background on the case, you can read articles from the [New York Times](#), [MSNBC](#), or [SecurityFocus](#). (Full disclosure: WSN editorial director Brian Livingston is quoted in the New York Times piece supporting Julie. The article at the MSNBC site is also a good read, but I don't recommend the accompanying video, which starts out with a falsehood and goes downhill from there.)

Let me begin by saying that I'm biased when it comes to Julie's innocence. I'm doing my best to

spread the word about her case, and have offered my technical skills to support her defense. I have access to some technical experts who are reviewing the trial transcripts and computer forensic evidence. I can't point to a public reference to support all of my positions yet, so you'll just have to take my word, for the time being.

There are many points I could make about what's wrong with her case. But I'll stick with my core competency and just point out some of the technical flaws.

Flawed technology condemns an educator

The key issues were set in motion before Julie ever arrived to substitute-teach on the day in October 2004 that the pop-ups occurred. The school district had allowed its Web-filtering software support contract to expire, preventing the software from receiving updates. The computer in question was running Windows 98, and the browser in use was IE 6.

According to evidence analysis performed by Alex Shipp, an independent malware researcher, the antivirus software was a trial version of Cheyenne Antivirus (CA). That product had been discontinued by Computer Associates on Mar. 17, 2004. It appears that CA issued a last courtesy update on June 30. Julie taught the class on Oct. 19. The computer had no antispysware software.

In other words, this computer had almost no protection and an unsecurable operating system. This is the machine Julie was given to use.

On the day in question, the regular teacher was there before class to log Julie into the computer. Substitutes didn't have their own accounts, and were ordered not to log out or shut down the computer. Julie left briefly and, when she returned, the regular teacher was gone. She found students, some of whom didn't even belong in the upcoming class, Web surfing on the teacher's computer.

Experts now analyzing the hard-drive image have confirmed that the computer had been infected with adware days before Julie's arrival. Unfortunately, in this case, that means that when a student tried to visit a hairstyle Web site, he or she was instead redirected to a different site that had adult products advertised. When Julie tried to close the site down, this started a pop-up cascade.

One thing I should mention about Julie: She's a total "computerphobe." She can perform basic computing functions, but that's about it.

So what did she do when she couldn't get rid of the pop-ups? She turned the screen away from the students. It was at the front of the room, where the students would have had to be essentially at the teacher's desk in order to see. She did her best to get rid of the images without making it obvious to the students that something was wrong. If a student approached, she reportedly chased them away.

During a break, Julie went for technical help to get rid of the pop-ups, which reappeared as fast as she tried to close them, but she received no help. No one would return to the classroom with her. She was told not to worry about it. However, she **was** worried about it, and it turns out she had reason to worry — she was later arrested for "child endangerment."

Legal system fails pop-up victim

When law enforcement became involved, sanity should have prevailed. Instead, the technical flubs continued, and the case sped downhill. A detective was assigned to take a forensic image of the computer and perform a technical analysis.

Let me briefly tell you what I know about taking a proper forensic image of a computer that will be involved in a criminal case. Keep in mind that I'm not a forensics expert; these standards are just common knowledge in the computer security field.

If you're going to image a drive for evidence, you have to use special write-blocking hardware that helps take a sector-by-sector image of the entire hard drive, including the "empty" space. The image is then hashed so that any tampering will be evident, and you always work from copies.

Typically, only software tools with support from existing case law are used. Otherwise, questions can arise over the soundness of the tools and techniques. The imaging tools that have case law behind them are [EnCase](#) and the Unix **dd** utility.

The detective in this case took an "image" of the hard drive with Norton Ghost. Norton Ghost is a tool used to back up a computer's hard drive in order to restore it to a known state after people have modified the configuration. It is often used on training or lab machines. There is nothing wrong with Ghost for what it does, but it is not a forensic tool.

So what did the detective use to examine the "image"? He used a program called ComputerCOP Pro. It appears that the program displays a version of the Internet Explorer history, which shows the URLs that were visited. At trial, this ended up translating to the prosecutor telling the jury that this means that Julie "physically clicked" those links. In fact, pop-ups show up in the history the same way as a link you click on.

In truth, the software also cannot tell you who was in front of the computer, who typed in a URL, or who saw the pictures displayed. It's clear that someone who lacks the technical background to properly interpret the results, and is not willing to put in the time to figure it out, can jump to some very wrong conclusions. The detective never even looked for spyware on the computer.

This is the kind of technical evidence on which Julie was convicted.

An innocent teacher awaits sentencing

Julie is now awaiting sentencing, which is scheduled for Mar. 2. I could discuss jail-time possibilities, but many of us are still refusing to accept any possibility other than someone coming to their senses and throwing the verdict out.

To that end, the experts I mentioned are frantically preparing their report on the technical information. The hope is that the prosecution or court will recognize that there has been a basic mistake in the facts presented at trial before a sentence is handed down.

Despite my bias that I told you about, do you have reasonable doubt about Julie's guilt? For more information, see the [Julieamer blog](#) at Blogspot, which is largely maintained by Julie's husband.

There's a PayPal button at the top of that blog so people can contribute to help pay Julie's defense costs, which are reported to be over \$20,000 so far.

Ryan Russell is quality assurance manager at [BigFix Inc.](#), a configuration management company. He moderated the vuln-dev mailing list for three years under the alias "Blue Boar." He was the lead author of [Hack-Proofing Your Network, 2nd Ed.](#), and the technical editor of the [Stealing the Network](#) book series. His Perimeter Scan column appears twice a month in the paid version of the newsletter.

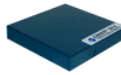
[Contents](#) [Index](#)

ADS



Remotely monitor your PC from anywhere

SnoopStick is a USB device that allows you to securely monitor activity on your PC from any Windows-based computer, anywhere. Monitor IM, browser activity, e-mail, and control access to Internet services. Great for parents and employers.
www.snoopstick.com



Deep Six your spam problems

Unique, next generation technology: Affordable, easy to deploy, simple to maintain. Patent-pending technology rejects junk e-mail before messages can be sent. Improved and updated. Buy now and get pending major release free. Newly available overseas.
www.tyrnstone.com



Backup your data with ZipBackup

Finally, a backup program that is easy to use. ZipBackup's Wizard makes backups a snap for beginners. Filtering, scheduling, and disk spanning make it a powerful tool for experts. For a limited time, Windows Secrets readers receive 25% off.
www.zipbackup.com

[See your ad here](#)

LANGALIST TIPS

Make more space by deleting log files



By Fred Langa

Log files can be useful, but they mainly just take up space.

Trim away your useless log files to gain space and make your backups and restores smaller and faster!

Hidden log files eat your disk space

Log files can be useful: They're usually plain-text records of actions taken by software as it runs — changes made, files added or deleted, and so on. When something goes wrong, it may be possible to examine the appropriate log file to see what the software was trying to do when it encountered trouble. That, in turn, can be a valuable troubleshooting clue.

But over the years, log files have moved from front-line troubleshooting to a rarely used and obscure tool tucked away on your PC. Log files can be like weeds, growing in the quiet corners of your hard drive.

Try this experiment in order to see just how many log files are taking up space on your hard drive:

Click Start, Search, then search **All files and folders** on your hard drive for any files named ***.log**. Odds are, you'll find hundreds of log files you probably never knew existed. (The **Windows** folder tree alone is a rich repository of log files.) My system currently has almost 900 of the suckers!

With today's large disks, a passel of small log files isn't worth worrying about. But sometimes log files can become huge, or a single active program may create a large quantity of log files. Karen Cleveland found one such instance in the ZoneAlarm Security Suite, which practically logs every heartbeat. Let's take a look at her example, but keep in mind that the log-file proliferation caused by other programs can often be cured in similar ways:

- "I've installed ZoneAlarm (ZA) Internet Security Suite 6.5, which I purchased in the box off-the-shelf at a major computer store. I'm having a problem with ZA writing multiple files to the **c:\WINNT\Internet Logs** directory. These files are continually modified by ZA and quickly become very large (i.e., many MBs).

"I stumbled upon this phenomenon because I noticed the free space on my hard disk kept decreasing day after day. Another problem is that the storage space used by System Restore is also consumed, because these files are backed up when a restore point is created. The restore directory in **c:\System Volume Information** was also growing by leaps and bounds. My hard disk is/was being cannibalized.

"Do you know how to fix these problems? I don't want to get rid of ZA, but I can't continue using it the way it is now."

First and foremost, log files are usually simple plain-text files. You can open them in Notepad and see what they contain. You can delete them if you're sure that neither you nor the application that created them will need the information inside. (Tip: Copy the log files to a CD or other safe place before you delete them from your hard drive. Then, if it turns out you need the information, it's still recoverable.)

You also can use various disk-cleaning utilities to delete log files automatically, if you're sure you no longer need them. For example, the free do-it-yourself [CleanAll](#) tool can easily be modified to delete any or all of the log files on your system each time it runs.

But sometimes, software will lock a log file while it's in use, making it difficult to remove by normal

means. A tool like the free and excellent [MoveOnBoot](#) (a more powerful paid version is also available) can delete files that are normally locked, in-use, or otherwise unable to be deleted from inside Windows.

The above steps can take care of log files after they're created. But, of course, it's best to keep unneeded log files from being generated in the first place. Most log-creating software, including the ZoneAlarm Security Suite, lets you turn off the log file function, if you're sure you don't need it.

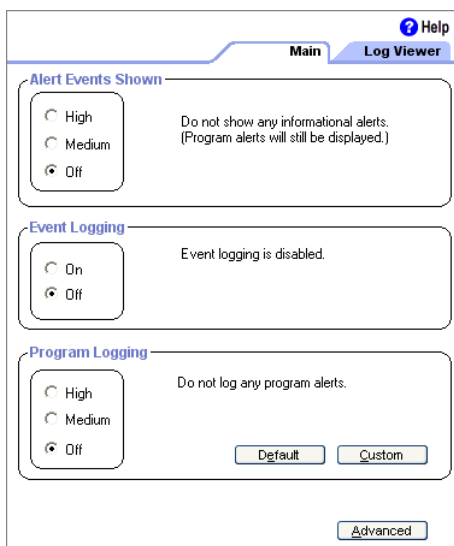


Figure 1. This example shows how the ZoneAlarm Pro firewall lets you control its log keeping. The "Advanced" button allows even finer control.

For example, to enable, disable, or alter event logging and program logging in the ZoneAlarm Security Suite and in the stand-alone Zone Alarm Pro firewall, follow these steps:

Step 1. Select **Alerts & Logs**.

Step 2. In the **Event Logging** area, select the desired setting. **On** creates a log entry for all events. **Off** means no events are logged.

Step 3. In the **Program Logging** area, specify the log level. **High** creates a log entry for all program alerts. **Med.** creates a log entry for high-rated program alerts only. **Off** means no program events are logged.

So, if you're drowning in log files — even hidden log files you never knew existed — you can easily get your head above water. Back up and delete the log files you don't want or need, and then adjust your software so that it doesn't create new unnecessary log files in the first place.

Running floppy-based tools with no floppy drive

Some software still legitimately needs to boot from a floppy drive. Reader Chris Henshaw asks what to do when your PC no longer has a floppy to boot from:

- "I was about to purchase Symantec Ghost for use as ghosting [imaging] software. In the [Feb. 8, 2007](#), issue, you wrote that [BootItNG](#) was your favorite. So, after reading the Terabyte Web site, I purchased a copy. When I tried to install it, I found that it required a floppy disk drive. Nowhere was this mentioned — either in your article or on the Terabyte Web site. I have not had a floppy disk drive for some years. Buyer beware!"

Your immediate problem is easily solved, Chris. BootItNG will run happily from any bootable medium, including bootable CDs, and even some Flash drives (depending on your hardware). You can use Terabyte's free [MakeDisk](#) utility, or any number of third-party tools and techniques to convert bootable floppy disk images into CDs or other bootable media. There's a good tutorial at [Ultimate Boot CD](#).

The reason why BootItNG requires a floppy is also the main reason why I personally like and recommend it: BootItNG is 100% self-contained. When it's running from its boot medium, Windows is entirely inert. No files are open or in use. Nothing is "live" on the hard drive.

This means that BootItNG's partition work and imaging work has no competition from other programs while it's running. Instead, the self-booting utility completely "owns" the PC and so is not likely to run into any problems with locked or in-use files, or files that change during the imaging process.

Most other disk-imaging tools that run from inside Windows (including Terabyte's own [Image for Windows](#)) rely on software sleight-of-hand; features like [shadowing](#) to create reliable backups and images of in-use and locked files.

This usually works, but is not 100% certain, as is booting from an external medium. In fact, this is also why some tools that use shadowing and similar techniques still recommend that you close all other programs before making an image or backup. That's the only way to get the reliability on par with that of externally bootable tools.

Admittedly, it's less convenient to use a tool that requires a separate boot. To me, it's worth it for the extra certainty of the imaging/backup process. But, it may not be for you. Indeed, BootItNG has a free trial period in which you can experiment to see if it fits your needs. If it doesn't, you haven't lost a dime.

CD-Rs don't survive freezing temperatures

It's midwinter here in the northern hemisphere, while our friends on the bottom half of the Earth swelter through summer. Either extreme can be deadly for CDs you create yourself, as reader Dalton Seymour found out:

- "Just had a look at your [Feb. 8, 2007](#), newsletter comments on how long CDs will last, which referenced McFadden's FAQ on the subject of CDs. This struck a chord with me because this year, I had the occasion to transport my computer system and collection of CDs from Michigan to Missouri in the dead of winter. Everything was packed up in the back of a pickup truck and covered with a tarp to make the trip. CDs were all in jewel cases packed in cardboard boxes.

"When they finally arrived, many of the home-grown CDs containing music transferred from vinyl to CD had died. Most were of the gold variety. My guess is that subfreezing temperatures may actually crystallize the dyes embedded in the plastic. These were all CD-R, not CD-RW. I had this happen to me once a long, long time ago with floppy media, but the phenomenon there was related to the lack of hysteresis [persistence of magnetism] at freezing temps."

Right you are, Dalton. CD-Rs last longest in dark and cool (but not cold) environments. If you burn CDs to carry data between work to home, or to rip your own music mixes, or for any other reason, don't leave them exposed to extreme hot or cold. If you leave a CD-R sitting in your car in subfreezing temperatures or baking in the summer sun, you'll run the risk of losing the data on that CD in a remarkably short period of time.

Another look at HijackThis

Reader Chris DeWitt's note focuses on an old favorite antimalware tool:

- "I've done some PC housecleaning for various people and found that some of the common tools I've used (Ad Aware, Spybot, NAV) don't always do the job. After I've used them, I turn to **HijackThis.exe**. It does a scan of your system and gives you a listing and log file of lots of potential malware files. It takes pains to tell you that these are not guaranteed to be malware, but could be. It's up to you to then go through each line, research the item, and determine for yourself if it is a culprit.

"If you then redo the scan, you can check the appropriate lines in the list and click the **Fix Checked** button. It will then remove most of these. Some of the remaining items may need more sophisticated removal techniques. If you send the log file to one of the many online forms, you can get help both in determining which of these is malware and in removing the more stubborn ones. It's a lot of work, but it can be done. Here is a link to one of the places you can get [HijackThis](#)."

HijackThis is indeed an excellent and powerful tool. It produces so much information that it can actually be intimidating the first time you run it! Windows Secrets has discussed and recommended HijackThis on several occasions, including in the [March 10, 2005](#), issue. The advice given then still stands today:

- "Several online forums provide free help to interpret the technical output from HijackThis. These forums are described in the [HijackThis log recommendations](#), provided by anti-advare guru Eric Howes. You'll also want to read the [HijackThis Quick Start](#) and the [HijackThis tutorial](#)."

Thanks, Chris!

[Fred Langa](#) edited the LangaList e-mail newsletter from 1997 to 2006, when it merged with Windows Secrets. Prior to that, he was editor of Byte Magazine and editorial director of CMP Media, overseeing Windows Magazine and others.

[Contents](#) [Index](#)

ADS



Get your product seen by 265,000 readers

Does your company offer a product or service? Now you can place an ad in the Windows Secrets Newsletter and be seen by more than 265,000 active buyers of PC hardware and software. Bid as much or as little as you like to get the ideal ad placement.
www.WindowsSecrets.com

[See your ad here](#)

TELL A FRIEND

How you can share this information

We love it when you send your friends links to our articles. But please don't forward your copy of our e-mail newsletter to people, which subjects us to spam complaints. Instead, simply suggest that your friends visit this issue's permanent Web address, shown below. A complete index at the bottom of the Web page provides you with hyperlinks to any article you'd like to recommend.

The address of this issue is <http://WindowsSecrets.com/comp/070222>

USEFUL LINKS

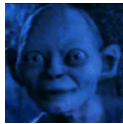
Now, rechargeable batteries you can rely on

A new technology is about to change your opinion of rechargeable batteries, and products that take advantage of the new technique are already showing up in shops. (By [Brian Livingston, Datamation](#)) [More info](#)

[Contents](#) [Index](#)

WACKY WEB WEEK

Gollum and Smeagol get their groove on



A hilarious new video that appeared on the Web recently is a creative, creepy, and delightful duet version of a Barry White classic. It's performed by none other than those loveable Lord of the Rings creatures, Gollum and Smeagol.

The characters do a great job of lip-syncing the song, at least as edited by a director who goes by the handle of **amds**. This definitely puts a new twist on the old soul classic. [Watch the video](#)

[Contents](#) [Index](#)

INDEX

The following topics appear in the free version

- TOP STORY** [Pop-up ads can land you in jail](#)
[Meet Julie Amero, substitute teacher](#)
[Flawed technology condemns an educator](#)
[Legal system fails pop-up victim](#)
[An innocent teacher awaits sentencing](#)
- LANGALIST TIPS** [Make more space by deleting log files](#)
[Hidden log files eat your disk space](#)
[Running floppy-based tools with no floppy drive](#)
[CD-Rs don't survive freezing temperatures](#)
[Another look at HijackThis](#)
- USEFUL LINKS** [Now, rechargeable batteries you can rely on](#)
- WACKY WEB WEEK** [Gollum and Smeagol get their groove on](#)

You get all of the following in the paid version

- LANGALIST PLUS** [Avoid firewall confusion with insider secrets](#)
[How to uninstall the Comodo firewall](#)
[What 'stateful inspection' means for you](#)
[Stateful inspection can slow down your system](#)
[How to track down and report the bad guys](#)
[Make Registry key files run when clicked](#)
[Running Vista in a virtual machine](#)
[Launching programs with and without DropMyRights](#)
[Adding icons to the IE 7 toolbar](#)
- WOODY'S WINDOWS** [Vista Timesaver #4 — the Windows Experience Index](#)
[The trouble with Vista's benchmarks](#)
[How to understand your computer's WEI](#)
[The index maxes out at 5.9](#)
[A critical look at WEI's scoring components](#)
[Don't overestimate Microsoft's performance ratings](#)
- PATCH WATCH** [Don't install drivers from Microsoft Update](#)
[VIA storage driver causes constant rebooting](#)
[Don't leave documents unsaved when auto-patching](#)
[Ads infect users via Windows Live Messenger](#)
[Hotfixes allow Office patches to install](#)
[New releases for SQL and WSUS](#)
[IE 7 conflicts with ZoneAlarm, Outlook 2003](#)
[Have SVChost issues? Hotfix is now downloadable](#)
[What you need to know about Vista patches](#)
[Windows Genuine Advantage gets an update](#)
[Moving dates in public folders](#)

Paid subscribers can access all old and new paid newsletter content

Make a contribution to support our research into Windows and you'll immediately be able to read and search through scores of valuable articles. In addition, paid subscribers are entitled to download valuable content that we license for you at least once every calendar quarter.

To upgrade, simply make a contribution of any amount you choose.

If you do this by Feb. 28, 2007, you'll instantly be sent the full, paid version of today's newsletter.

To upgrade to the paid version of the Windows Secrets Newsletter, please visit our [upgrade page](#). Thanks in advance.

[Contents](#) [Index](#)

YOUR SUBSCRIPTION

The **Windows Secrets Newsletter** is published weekly on the 1st through 4th Thursdays of each month, plus occasional news updates. Vacation breaks occur in late August, Thanksgiving Week, and Christmas/New Year's.

Publisher: WindowsSecrets.com LLC, 300 Queen Anne Ave. N. #456, Seattle, WA 98109 USA. Vendors, please send no unsolicited packages to this address (readers' letters are fine).

Editorial Director: Brian Livingston. Editor: Fred Langa. Contributing Editors: Susan Bradley, Scott Dunn, Mark Edwards, Woody Leonhard, Chris Mosby, Ryan Russell. Research Director: Vickie Stevens. Program Director: Brent Scheffler. Managing Editor: Jody Braverman.

Trademarks: Microsoft and Windows are registered trademarks of Microsoft Corporation. The Windows Secrets series of books is published by [Wiley Publishing Inc.](#) The Windows Secrets Newsletter, WindowsSecrets.com, LangaList, LangaList Plus, WinFind, Security Baseline, Patch Watch, Perimeter Scan, Wacky Web Week, the Logo Design (W, S or road, and Star), and the slogan Everything Microsoft Forgot to Mention all are trademarks and service marks of WindowsSecrets.com LLC. All other marks are the trademarks or service marks of their respective owners.

HOW TO SUBSCRIBE: Anyone may subscribe to this newsletter by visiting our [free signup page](#).

WE GUARANTEE YOUR PRIVACY:

1. We will never sell, rent, or give away your address to any outside party, ever.
2. We will never send you any unrequested e-mail, besides newsletter updates.
3. All unsubscribe requests are honored immediately, period. [Privacy policy](#)

HOW TO UNSUBSCRIBE: To unsubscribe from the Windows Secrets Newsletter,

- Visit our [Unsubscribe page](#).

Copyright © 2007 by WindowsSecrets.com LLC. All rights reserved.

[Contents](#) [Index](#)
