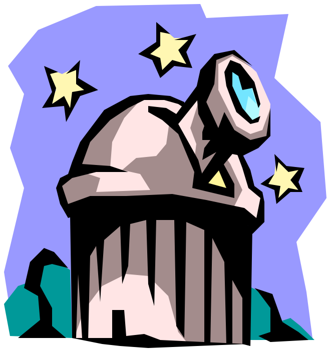
STAR Watch

Statewide Technology Assistance Resources Project

A publication of the Western New York Law Center, Inc.



Volume 9 Issue 1

January/February 2005

USB Hard Drive Enclosures:

An Inexpensive Way to Recycle That Old Hard Drive

In the early days of personal computers, floppy diskettes were the only storage medium. The computer was booted up from a floppy and all of the data files were saved on floppies. As internal hard drives started to become affordable, users continued to keep data files on floppies because of their portability. A floppy disk would easily fit in a shirt pocket, purse, or briefcase. It was easy to keep copies of one's prized briefs, spreadsheets, etc. close at hand. Every personal computer had at least one floppy disk drive on it, making it easy to create or access files on floppy disks. Other than the almost inevitable read and write errors on those floppies, it was the only way to keep an electronic copy of a document in a transportable format. But over time, things began to change.

When computer applications began to allow users to spice up their documents with graphics and/or create multimedia presentations, users were no longer able to fit the files on a floppy diskette. The sizes of these new files greatly exceeded the 1.44 Megabyte storage capacity of a floppy disk. Many storage devices that had adequate capacity became available, but none were as prevalent as floppy disks and weren't always compatible with one another. Many of these new devices were designed to be portable, but they all shared a common issue: They cost a lot of money.

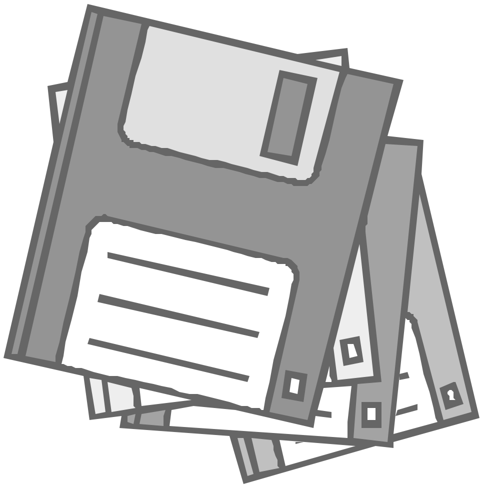
...

Are there any retired desktop computers just lying around the office collecting dust? Are they so old that no one will even accept them as a donation? Maybe the hard drives from

In this issue…

those computers could be used to create a storage device that is high-capacity, portable, and inexpensive. If you have $30 - $40, know how to use a screwdriver and possess basic computer literacy, you can create a large capacity, portable storage device.

There are literally dozens of USB hard drive enclosure kits that can be purchased for $25 - $40. The kit contains an enclosure in which to place the salvaged hard drive, a USB cable to connect the unit to a computer, and documentation. The drive is hooked up to a power and data connection inside the box. Put the cover back on the enclosure and tighten up the screws. That's it. The device will have a capacity equal to the capacity of the hard drive.



But how will it perform?

According to most product reviews, the performance of these units is not as fast as an internally-installed hard drives. Generally, internally-installed hard drives can read or write data at 35 – 50 Megabytes/sec. These units can move data at up to 1 Megabyte/sec on a USB 1.1 connection or up to 25 Megabytes/sec on a USB 2.0 connection. Almost all computers manufactured in the last 2 years have USB 2.0 ports on them.

Are all of the enclosures the same?

Besides the enclosure kits for 3.5" hard drives from desktop computers, there are hard drive enclosures that will accept 2.5" hard drives from laptop computers. In addition to kits that use USB, there are others that use a Firewire (also known as IEEE 1394A or i.Link) connection. Some have both USB and Firewire on the same unit. Pick the unit that best meets your needs.

Who makes them?

Here are some makes and models of hard drive enclosures.

- Apricorn EZGXC
- Highpoint Rocket Mate 1100
- Icybox IB-355-U
- Icybox IB-350UE-BL
- Icybox IB-350US
- Kingwin KH-350U
- Lindy ME-720U2SI
- MaPower Combo MAP-H31C2
- MaPower Warps MAP-KC31U2G
- Sharkoon Rocketpod
- PCT 29155
- PCT 29162
- PCT 29159
- PCT 29158
- Vantec Nexstar NST-350UF

Anatomy of Computer Problems: Patience and Perseverance

In a perfect world, there would be no computer problems. But if there were any problems, the solutions to them would be simple. Unfortunately, most of us live in the real world where solutions to computer problems involve more than one step. As soon as the issue at hand is resolved, we are confronted with another. We begin to think that the problem is too big for us to handle and we give up. But a lot of seemingly complex computer problems can be solved by patience and perseverance—because they are really simple.

...

We knew that there was a virus on the computer. It had all kinds of quirky behaviors, ran very slowly, and spontaneously tried to connect to the Internet via a dialup connection. The solution should be reasonably simple: Run the antivirus program to eliminate the virus.

Unfortunately, the computer told us that it could not connect to the vendor's site to get the latest antivirus update. The update program kept telling us that we should check our settings for the Internet because it could not connect to the update site. Since we were able to get to every other site that we could think of, it did not seem to be a configuration issue, but we still weren't sure. Was it possible that the antivirus web site was down? It seemed very suspicious.

In order to find out, we opened an MD-DOS command window on the computer and typed in:

```
PING WWW.SYMANTEC.COM
```

Ping verifies connections to remote computers. It sends echo packets to a computer and listens for echo reply packets. The computer reported that each of our pings was answered. At first blush, it looked like there was nothing wrong with the Symantec site. But a couple of items seemed strange.

According to Ping, the Symantec web site responded to each of our requests in less than 1 millisecond. That isn't just fast, it's too fast of a response from any remote site. The usual response times range from 70 to 150 milliseconds when connected to the Internet via a broadband connection. This computer was connected through a dialup connection operating at 21.6 Kbps (very slow).

Then we saw it: According to the Ping utility, the IP address of the Symantec web site was 127.0.0.1. That IP address has a special meaning to any computer that encounters it. It is the IP address that each computer uses to identify itself. If that IP address is used in any message, the message is “sent” to the computer that originated it. We weren’t pinging Symantec, we were pinging ourselves. If this was true for a simple Ping, could it be that this computer was receiving its own requests for updates? It seemed like a plausible situation. But how?

When any Windows computer tries to access any web site, it tries to resolve the host name into an IP address by following a protocol.

1. NetBIOS Name Cache
2. WINS Server
3. B-Node Broadcast
4. LMHOSTS file
5. HOSTS file
6. DNS server

The first 5 steps in the protocol involve attempts to resolve the IP address from information stored on the computer itself or the local area network on which the computer resides. The last step is to contact a “Domain Name Server” (DNS) on the Internet and ask for the IP address of the named site. Contacting a DNS for IP address resolution is slower that resolving the name locally, so the local resolution methods are preferred. If any of the first 5 steps yield an IP address, the DNS is not contacted.

We could make a lot of important sounding statements about why we didn’t investigate items 1 through 3 in the list above, but the truth is we would have had to research each one to find out more about it and it was getting late, we were getting tired, and we knew something about items 4 and 5.

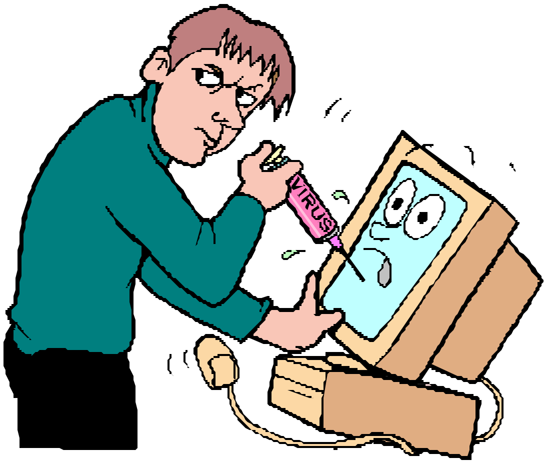
The HOSTS and LMHOSTS files contain mappings of IP addresses to host names. While their intended uses are slightly different, their basic function is the same. These files on the local computer are referenced before the name resolution request goes to the DNS. Since they are used before the name resolution request goes to a Domain Name Server, these files can be used to override host name to IP address relationships.

We searched the C: drive on the misbehaving computer for all occurrences of files named “HOSTS” and “LMHOSTS” and found multiple copies of each. Both of these files are ASCII text files that can be opened and/or modified by any text editor such as Notepad (Word or WordPerfect should never be used on these files). We found several copies of each of the files. Several of the copies contained nothing remarkable in them. They looked like they were installed by Microsoft and contained a great deal of explanatory text in them. Those files were not modified.

Pay Dirt!

Eventually, we opened a HOSTS file that contained a Who’s Who of antivirus web sites. And for every web site named, the IP address that it pointed to was the same: 127.0.0.1. Any attempt to update virus definitions or go to the vendor’s web site for help would point everything back to this computer and cause the request to fail. The virus that infected the computer loaded the HOSTS file with bogus web site information causing all requests for updates or help to be misdirected.

The correction procedure was simple: Remove every web site name from the list that couldn't possibly be located on the local computer and save the updated list.



At last...

After fixing all of the copies of HOSTS and LMHOSTS, we were finally able to contact the real Symantec site and update the virus definitions. Once the virus definitions were updated, the virus scan found all of the copies of the viruses and removed them.

...

In retrospect, only two things happened:

1. A virus managed to infect the computer before the virus definitions were updated that would have identified it.
2. To prevent its discovery by the antivirus program, the virus loaded the HOSTS file with incorrect IP information for all of the antivirus web sites.

Whenever an attempt was made to update the virus definitions, it would fail and present the user with an error message that he/she could not figure out because they couldn't get to the Symantec web site for an explanation. At a loss to explain the problem, the user had no idea what to do to correct the problem as long as they continued to think "inside the box". The hacker was hoping that the virus would remain undetected while the user remained focused on the antivirus update problem. The longer it took, the longer the virus remained viable.

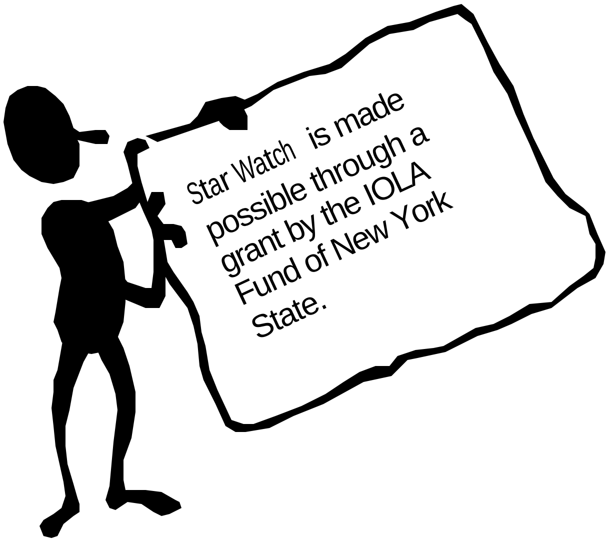
Updating the virus definitions would ultimately rid the computer of the virus, but questioning why the update failed was the key to solving the problem. Ethics aside, a small part of us respects how a low-life hacker could create such a wildly confusing situation with so little effort. But, there isn't any admiration. After all, we beat them at their game through patience and perseverance.

Most computer problems are like that. We don't see the forest because the trees are in the way. We prevent ourselves from solving the problem. Examine the little problems that make up the big problem. One of them will provide you with the information you seek.

WNYLC Web Statistics For December 2004

Total Hits	284,567
Total User Sessions	38,543
Average Hits/Day (Monday – Friday)	11,430
Average user Sessions/Weekday	1,456
Number of Pages Viewed	98,899
Average Number of Pages Viewed Per Day	3,190
Number of Documents Viewed	67,202

Accessed Using Internet Explorer	87%
Accessed Using Netscape	5%
Operating Systems Used:	
Windows 98	20%
Windows 2000	18%
Windows XP	46%
Windows 95	<1%
Windows ME	1%
Windows NT	1%
Macintosh	<1%
Linux/Unix	<1%


Star Watch is made possible through a grant by the IOLA Fund of New York State.

WHO WE ARE

Joe Kelemen - Attorney
Kathleen Lynch - Attorney
Tom Karkau - Programmer
Carly Bouchard - Administrative Assistant

Wnylc@wnylc.com

716-855-0203

www.wnylc.net

Western New York Law Center, Inc.
237 Main Street, Suite 1030
Buffalo, New York 14203