WindoWatch

MAY 1996
Vol 2 No. 4

NEXT

ww

WHAT'S INSIDE

Vol.2 No. 4 May 1996

ww

WindoWatch **The Electronic Windows Magazine of the Internet**
Volume 2 No. 4 **May 1996**

It was just a year ago, that some of us were deeply involved with the Windows95 beta What a difference a year makes!

To their credit, Microsoft with its marketing genius has been guiding its customers into the 32 bit world of computers and operating systems. Windows 95 is king, at least for now. However, anyone who has used NT 3.51 must acknowledge the superiority of this OS. Finally there are 32 bit applications in sufficient quantity and diversity, to allow NT to strut its stuff. The heir apparent is waiting to grab center stage after being on the side lines for several years.

There was massive hand holding for millions of customers as Windows 95 was brought to market. With much help, customers developed a taste for what a 32 bit operating system can deliver. Because technical support was available, cheap and/or free, efficiency and speed long taken for granted in the 32bit world of business have changed the face of computing for everyone. There is no going back! More importantly, who wants to return?

Unhappily there is a hole in the Microsoft plan. Tech support for NT is priced for corporate customers. The NT operating system is sufficiently different to require free and/or low cost tech support for its users. Individuals and small business cannot afford to become proficient given the extremely high price tag for hourly services. It doesn't really matter that support for competitive operating systems is more expensive. The competition has never been committed to technical support for ordinary users. It is the ordinary user who will want to network their home computers, access the corporate office, and provide the advantages of the online world to their families. It is no longer acceptable to define a robust operating system like NT as just a corporate product. Further, support for the large and ever growing installed base of DOS-Windows users, must begin to reorder and redefine issues of backward compatibility.

Recently one of the Microsoft spokesmen made the statement that it was not the company's intention to foist NT upon the world of Windows. From where I sit, little encouragement will be required! Concerns about the cost of hardware are diminishing daily.

It seems to me that we have a classic chicken-egg dilemma.
As the pool of experienced Windows users increases, including NT, the demand for NT software at the corporate level will increase as well. (NEXT)

EDITORIAL

Editor Lois B. Laulicht
Contributing Editor: Herb Chong
Home Page Editor Paul Kinnaly
Ascii Edition Editor Lin Sprague
Contributing Writer s: Derek Buchler, John M. Campbell, Leonard Grossman, Gregg Hommel , Stan Kanner, Jerry Laulicht, Phil Leonard, Bob Miller, Frank McGowan, Peter Neuendorffer, Jim Plumb, Ben Schorr, Paul Williamson

SUBMISSIONS and REQUESTS
Email using Internet
lois.laulicht@channel1.com
windowatch@ins.infonet.net
winwatch@user1.channel1.com
Editor WindoWatch
Valley Head, WV 26294
Submissions remain the intellectual property of the author. Manuscripts will NOT be returned if not used.
Electronic File Access
FTP>ftp.channel1.com/pub/WindoWatch
FTP>oak.oakland.edu/pub3/Simtel-win3/winwatch
WindoWatch is found on Channel One in several formats by calling
617-354-3137 (28800) or
617-354-3230 (9600 and 14.400).

We publish in a Windows compatible format and in HTML on our home page. The DOS format uses ReadRoom (*.TOC) One can also read online from the Reader Room itself - Door 48. Non-members of Channel One can download the latest WindoWatch issue by typing J Free from the main board prompt
Annual shareware subscriptions at $20 per year for electronic delivery of the ASCII or Acrobat edition. Sponsorship and contributions at various levels.
Comments, letters, and requests can be sent to us at various locations. Postlink to Lois Laulicht ->15 tagging the message "receiver only" and on the Internet
lois.laulicht@channel1.com

How to Design, Implement, and Manage your own Webspace

There is little doubt that the Internet is currently the hottest topic in all of personal computing! Suddenly, Internet software development conferences are being held regularly, as well as an upcoming Java Development Conference, the first for the programming language of web browsers. A small start-up called Netscape has seemingly come from out of nowhere to give Microsoft arguably their strongest competition in years. The talk of the industry has suddenly shifted from Microsoft Windows, and focused on something called the Netscape Navigator. And to prove this is gospel, the industry's resident wunderkind is no longer Bill Gates, but the boy wonder of Netscape, Marc Andressen.

And, of all the areas of the Internet, there is also little doubt that the hottest at the moment is the World Wide Web. By modest estimates, there are somewhere between ten and twenty million pages currently posted to the World Wide Web. Where having a cell phone might have been bleeding edge five years ago, today's technologically savvy post their home page addresses on their business cards.

With all those pages on the Web, some are excellent examples of content and design, while others are completely devoid of taste and are almost impossible to look at without damaging your eyes. I have

been told that virtually anyone can learn HTML (Hypertext Markup Language), but few can turn its' lines of code into a stunning visual representation.

So, one of the side-bets in this, the age of the Web, is whether that home page you have been working on is GOLD or garbage.

A web page is essentially a printed page in a book, displayed on a computer screen. What looks pleasing to the eye, transcends the media. But, the true challenge is to create an environment that is at once, both rich with content and tantalizing visually. This is much harder than it would appear to be. My fifteen years as a graphic design specialist in the commercial printing industry allows a certain authority as to what should and what should not go on a World Wide Web home page.

So, it is at this point we begin. Here, I will reveal to you, the secrets of a Web Master. Beginning with this first article, I will take you by the hand, and give you all the tips you'll need to make your home page one of those *Cool Site Of The Day* pages. In addition, I'll do my level best to help keep your page off of "Mirsky's Worst Of The Web."

There is an old saying that if you took fifty monkeys, and sat them at fifty typewriters for fifty years, that they would type the complete works of Shakespeare. While some claim that is true, I'll bet that the completed document would still look like fifty monkeys typed it. You might say the same for this latest craze of publishing home pages on the Internet's World Wide Web. The trick is to prevent your finished product from looking like fifty monkeys typed it. That is why I am here with you today, to hopefully prevent that from happening.

Recently, I had a discussion with a friend of mine, who is also a designer. He commented how most people who put up a home page don't have any idea of what they're doing. Their pages are filled with typing, spelling and grammatical errors. In this day and age, when every word processor worth its' salt contains the very tools to prevent this. And, it doesn't end there. Inappropriate use of graphics is another area greatly abused. Background textures are supposed to compliment the page, not completely overwhelm it. But, that is exactly what happens on page after page. I could go on and on and on . . . . my friend hit the proverbial nail right on the head!

My response to that discussion begins this series of articles, which, when finished, should be a good jumping-off point for any would-be Web Master. This is a work in progress, so you'll have to bear with me. As of today, I don't know how many parts there will be to this series, it'll end when I have told you everything that you should know. Seems pretty fair, wouldn't you say? So, let's begin . . .

So, you want to publish your own Web Page?

You've decided that you have to join the millions who have already posted their home pages all over the World Wide Web. Everyone from Joe Schmoe to Disney have already staked out their own corner of cyberspace. But what is leaving you baffled is the content of your page. Should you publish the definitive home page relating to Windows 95? Nah, a quick search of the Web on C/Net's Search.com spits back over 15,000 pages already dedicated to Windows 95. The first quest in your journey to publish a home page is to *do something original*.

ww

That guy who has the CRUNCH site, devoted to cereal box art of the 1950's to the 1990's isn't going to foster world peace with his page, but at the very least, it is original content. Sure enough, Search.com brings up one single link when you type in the words *cereal box art* into the search engine. If Mr. Crunch hasn't succeeded in anything else, at least he has created something no one else has thought of.

***The next thing that you should consider are any hobbies or interests that you may have.* You might find the choices for your web page content quickly resolved by the existence of your beer mug collection. If you happen to be rather well read on a particular subject, such as *18th Century Snuff Boxes*, or *Doorknobs Through The Ages*, you just might find yourself introducing those particular topics to the potential audience for your web page.**

In discovering subject matter for a web page, I can only speak from my own experience. During the summer of 1995, as I stress tested the final BETA of Windows 95 before its' release, I began to write a FAQ on the single aspect of the operating system that seemed to be perplexing to even the most seasoned programmers and power users. And, on the very day that Microsoft introduced Windows 95 to the world, August 24, 1995, I released my little FAQ on the Windows 95 Registry. In the seven months since, I have calculated that almost 100,000 people have either read or downloaded my FAQ.

I had stumbled over the answer to what I should publish on my own web page. The Windows 95 Registry FAQ was the perfect thing for me to put up for the world to lay witness to. So, as I write this, I am also distilling an update to the Windows 95 Registry FAQ into an OFFICIAL web site. That was the answer for me, it was the one that made the most sense. True, I could have published the first site in

cyberspace dedicated exclusively to PEPSI and Pop Tarts, as I live on ‘em! But, that would appeal only to those who share similar dietary propensities.

This brings me to the third bit of advice that I have for you on the issue of selecting web page subject matter; *select a topic or topics that others will find valuable!* Every single successful web site has triumphed because its’ visitors found value in the content. Whether it was a national directory of Zip Codes, or Hollywood gossip, these sites have not only existed, but thrived on the World Wide Web. While you may have a passion for mangoes is it a passion that is widely shared? Will the visitors to your site leave happy that they stopped in for a visit? More importantly, will they return? Believe it or not, one of the most successful sites on the Web is one called *The Big Red Button That Does Nothing!*

Okay! Okay! I have a subject ... Now What?

Even though the Web seems chaotic at times, in reality, it is highly organized. And so should your home page. The physical structure of the individual pages in a web site must be logically organized. Because of the non-linear nature of the Web, people who visit your page must be able to jump from link to link, without any trouble or hassles. Otherwise, they will never return, no matter how intriguing or useful the content really is.

So, the next little bit of advice I have for you is to *prepare an outline of your sites’ pages, as well as of the intended hypertext links.* I know, I know, you hated doing that for your English professor in college. I can hear all of you moaning and groaning .

Actually, there are several ways that you could put together a thumbnail representation of your intended web site. If you already have such a program, Visio - the flow chart program, can help you complete this task. If you are currently a registered user of OFFICE 95, there is a program installed in the *Shared Files* folder called Microsoft Organization Chart. That could also do the trick.

However, the program that I am using, that can accomplish this and so much more, is a free (until 6/30/96) download called Microsoft FrontPage 1.1, available at their corporate website. Tightly integrated with the user interfaces of both Windows 95 and Office 95 Professional, FrontPage creates a thumbnail view of your entire website, in several useful views. But, more on this and my other software recommendations a bit later.

If you doubt the value of preparing a thumbnail view of your web pages, let me tell you that this is the only way that you are going to keep things together and organized if you plan on publishing more than a handful of pages. To use my Registry FAQ as an example, the update that I recently completed is twice the size of the original edition. And, with fifteen separate sections, the thumbnail view of my web site is the only possible way that I am going to keep the 130 pages of text properly organized with the associated hyperlinks.

You can attempt to bypass the thumbnail stage of web page creation, and you may even get away with few or no problems along the way. But, if you try to save time in this way, it is entirely probable that you will waste much more time trying to fix the broken hyperlinks than whatever time spent creating a thumbnail map. The choice is yours, however. But, if you don’t heed my warning, and get into a deep jam, don’t say that I didn’t warn you!

ww

Service Providers - National versus Local

In deciding the type of Internet Service Provider you will use as the server for your website, your selection criteria should be based on a mix of technical and economic issues. If you look closely at the marketing campaigns of the national proprietary online services like America Online, CompuServe, and Microsoft Network, it should become immediately apparent that they avoid precisely those issues.

Instead, they focus on the exclusivity of their content, pitching their wares to certain demographic segments of the potential audience. While they play up how cool it will be for you when you become a member, the fact that they are charging up to ten times what a local provider might charge, is completely ignored. Until, that is, until you get your first bill, and its' over one hundred dollars!

While the national online services all provide direct Internet access, and heavily market that fact, the truth is that access is anything but. What happens when you log onto America Online for example, is you are piped into their proprietary server structure. Your Windows swap file fills with their GUI shell, which usually chews up considerable amounts of user resources. Then, if you want to use their browser to surf the web, America Online then becomes what is known as a *PROXY SERVER*.

By definition, a proxy server routes outside network content through another proprietary server behind their own firewall. There, the proprietary network can gain control of the flow and of the content of the outside data. This is how CompuServe and America Online can block access to certain newsgroups that they deem unsuitable for their membership. Many view this as nothing more than censorship, and a

direct violation of the first amendment right of free speech. To this, I couldn’t agree more, but, that is a matter for a future column.

The problem with this Proxy Server structure for the user is simple to define, and nearly impossible to solve. When you use a service like America Online to access the Internet, you have to load all of their GUI shell into your system resources, RAM, and Windows swap file before you even get to the Internet itself. Once there, the data flows through many hubs and routers along the Internet, and through the firewall back to the proxy server, which then directs the data back to your browser, placing further demands on your system resources. This can literally choke a Pentium system into behaving like a 386, which is not the kind of performance I want to pay $3.00 an hour for.

To exemplify this, let me give you an example right from my desktop. I have online accounts at both America Online and a local service provider here in Buffalo, NY called BuffNET. I connect to both at 28,000 BPS, which is the fastest service I can buy at the moment from either. My favorite site on the entire World Wide Web is C/Net (www.cnet.com), which is in my opinion, the single best online resource for up to the minute computer news. In fact, I have C/Net as my home page on both the America Online browser, and the Netscape Navigator GOLD 2.01 browser that I use while on BuffNET. But, logging onto C/Net is quite different when I am on America Online, then it is on BuffNET.

While logging onto C/Net by using the convoluted proxy server structure of America Online, it takes *up to three minutes* to load their front door. And, this is at 28,000 BPS!!! Considering that I pay $3.00 an hour for the privilege of being an America Online member, I am being billed fifteen cents to twiddle my thumbs while I wait for the

overworked America Online network to send C/Net to my desktop. This can be not only be a very expensive way to surf the web, but it is also a pain in the ass!

With BuffNET, surfing the web was like finding religion. C/Net loads in *fifteen seconds*, more than ten times as fast as when I am on America Online. The other main advantage to my local ISP is the cost of membership. After paying a one-time $25.00 start-up fee, I am paying $39.95 for three full months of UNLIMITED access to the Internet. Better still, I can log on for all the time that I want, without feeling like my budget is controlling my online activities.

So, unless I have unlimited funds, or I am just plain foolish, this really isn't a difficult decision. I was paying well over $100 per month for Internet access through America Online. Now, I pay less than half of that for three months!! Finally, if the national proprietary online services want to stay competitive, and in business, they are going to have to seriously retool their business models. America Online just isn't all that cool!!

I just signed up, now what?

Before you do anything at all, please take the time to contact the technical support department of your local ISP. It is vital to the success of your Web Site, that you have these following questions answered. This way, you'll know what your limitations are, in terms of space on the server, extra charges, etc.

Webspace ISP Checklist:

- ***How much space on the server will I have for my web page(s)?***

Obviously, the more space that the ISP allows its' members, the more you can publish in your allotted webspace. America Online allows only 2 mb per member ID, which allows for only the most basic of websites. My local service provider, BuffNET, allows me 5 mb. This gives me much more flexibility and allows me to put the kind of site I want on the Web.

So, if the amount of allotted server space is important to you . . .

- ***What is the fee per additional megabyte if I exceed that limit?***

Every ISP has a fee schedule for additional space, should you require it. The prices vary, but a dollar per megabyte is a fair price to pay per billing period. Ask about this before you discover your local ISP is charging you America Online prices.

- ***Is there a web page, FAQ, or help document that will give me the needed instructions to publish my web page(s)?***

With the typical Web Server running on GOD knows what platform, make sure that you find out where the specific instructions that you will need to get your files onto to the server. With Windows 95 having its' own self-contained solution for accessing the Internet via Dial-Up

Networking, you may still need further instruction on how to use their system.

- *Will I be able to set up my page(s) to allow visitors to download right from the page(s), without having to go to a separate FTP site?*

ISP's have varying policies on the posting of software on their members' web pages. Make sure that you find out what your ISP's specific policy is, before you get yourself in trouble. And, without exception, it is absolutely forbidden to post any commercial software. This is a violation of federal copyright law, punishable by heavy fines and jail time . . . know this before you post your warez!

- *How much FTP space will I have available for my own use?*

Most ISP's will also make a certain amount of FTP space available to you for your own public and/or private use. Make sure that you ask about this, and whether your FTP space is monitored by any of their staff. As with the question immediately above, make sure you understand what the rules are, before you break them!

- *Can you provide CGI scripts needed for counting "hits" on my site?*

You might want to keep track of the number of people who visit your site, and with HTML, the only way to do this is with something called CGI (Common Gateway Interface) scripts. CGI is a method of running programs on the web server based upon input from a web browser

anywhere on the Internet. The most common uses of CGI scripts are fill-in forms, visitor counters, and search engines.

Ask if you have to write the script yourself, or if the ISP’s WebMaster provides this to you, as part of your membership privileges . . .

- ***What Webpage content is allowed? What is forbidden?***

As I mentioned earlier, you should be aware of the rules before you break them. With the recent runaway popularity of the Internet, the cybercops have begun to seriously hassle certain people who are posting objectionable content on their webpages. You should know the standards of the community in which you live.
After having been warned, what you then do , is your own business !

- ***Is there a personal rate versus business rate, and if so, what is it?***

If you are an individual, you will most likely qualify for a personal membership, which is usually considerably cheaper than the price of a business membership, as it should be. A business gets the write off, I don’t! Here, it is crucial that you understand what your local ISP considers personal content from what they consider business content.

This is the perfect place to trip yourself up; where you suddenly find out that just because you posted an announcement that you want to sell your old copy of Office for Windows 3.1, your ISP is suddenly charging you the business rate for your webpage.

It would be pointless for me to go any further into this subject. Every Internet service provider has their own set of guidelines, rules and requirements. Hopefully, this will be enough o start thinking about

when you talk to your ISP's technical people regarding the posting of your very own webpage.

Getting Your Toolbox Together

At this point, we'll assume that you have an ISP, you've called them and discussed their requirements concerning the posting of your own page on the World Wide Web. I am also assuming that you have never done anything like this before.

"So, what now, oh, fearless leader?" You ask, pounding your fists on the keyboard.

The very next step involves getting a toolbox together. By this, I don't mean to suggest that you head on out to the local hardware store and pick up a black metal box filled with screwdrivers and hammers. But, what I do mean is that you've got to get your World Wide Web toolbox together. Even if you already have Corel DRAW! or Adobe Photoshop, chances are that you are ill-equipped to create and edit the highly specialized images and text that is the foodstuff of Webpages the world over.

Here's the scoop . . .

Your World Wide Web toolbox will consist of the following:

- **the web browser of your choice**
- **assortment of browser plug-ins**

- **various editing tools (text and graphics)**
- **a well stocked reference library**

Above is a quick overview of the major components that you will need to create and maintain a successful webpage. The specifics as to which browser to use, or which word processor you will need to edit your HTML tags, is entirely a matter of personal preference. I don’t have anything to gain by recommending one piece of software over another; and I don’t care what you use, as long as you have something in your toolbox that gives you the following capabilities.

However, I *will* tell you which pieces of software are accepted industry standards. Knowing that a particular browser is the standard of the industry will result in the users of that software having added features and abilities sooner than the users of another browser that isn’t a standard in the industry. These secondary competitors usually trail the leader in the development cycle. So, there is a direct advantage to having one piece of software over another. In spite of all of this, you must make that decision on your own.

Rather than have a long listing of every browser available today, and every HTML editor, and graphic editor, and the like, I will let you in on the real skinny, as it is out there on the Web itself.

Web Browsers

Web Browser (Netscape Navigator GOLD 2.01)

File - g32e201.exe (3,616,768 bytes)
Registration Fee - $89 (FREE for Educational/Non-Profit)
Publisher - Netscape Communications
WWW - http://www.netscape.com

The Web Browser is far and away the hottest piece of software available on the market today. With Netscape commanding an unreal 89% share of the Web Browser market, this is the standard by which everyone else is measured. This even includes Microsoft, which for once, *isn't* the domineering force in this particular market.

By my own count, there are twenty-eight different browsers available today. If you want to compare them all, be my guest, and head to the BrowserWatch website. There you can compare them all, but, I promise that you will agree that the Netscape Navigator is the best, and why not have the very best in this life?

Web Browser (Netscape Navigator GOLD 3.0 ATLAS BETA)

File - atls32s1.exe (5,907 K)
Registration Fee - Free BETA
Publisher - Netscape Communications
WWW - http://www.netscape.com

There is a saying ... *If it's not broke, don't fix it* .. which doesn't apply to Netscape Communications. On a breakneck product development cycle, this BETA of what eventually may become Navigator 3.0

GOLD, is until further notice (or an update), a free download. Code named ATLAS, this browser adds many features that were until now, available only as third party plug-ins. Downloading the ATLAS beta will allow you to peek into the future, and believe me, it is a sight worth seeing!

Web Browser (Microsoft Internet Explorer 2.0)

File - msie20.exe (1,194,496 bytes)
Registration Fee - Free Download
Publisher - Microsoft Corporation
WWW - http://www.microsoft.com

How could Netscape, whose browser dominates the Internet just like Microsoft dominates the Desktop, fear that their stranglehold on the nascent Web Browser market will succumb to their formidable foes' perseverance? They have nearly 90% of the market, and more than that, they have what is known as mindshare. When you think of surfing the Web, you think of Netscape . . . when you see a screen shot of a browser either in an advertisement, or in a review, it almost always bears the unmistakable Netscape logo.

Nonetheless, Microsoft's Internet Explorer is the greatest threat to the Netscape supremacy. It will probably erode some of Netscape's lead, as the Internet Explorer is being heavily marketed as a free download. Quick to point out that the Netscape Navigator costs $49, and Netscape GOLD costs $89, Microsoft is currently gaining ground with deals recently inked with America Online and CompuServe.

Notwithstanding the big plus of the Internet Explorer soon to be bundled free inside the Windows 95 operating system, it is slightly

overshadowed by the fact that it is slightly less capable than the Netscape offering. Even so, this browser is certainly worth the download and your consideration.

Web Browser (Microsoft Internet Explorer 3.0 BETA)

File - msie30.exe (2,151,424 bytes)
Registration Fee - Free Download
Publisher - Microsoft Corporation
WWW - http://www.microsoft.com

Not to be outdone by anyone, Bill Gates' company also has a version 3.0 BETA of their web browser to download from their corporate website. Between the release of 2.0 and this current BETA offering, Microsoft has licensed Java, which virtually insures compatibility for this browser with the hundreds of Java-able applets that are multiplying like rabbits all over the Internet these days.

This 3.0 BETA provides some insight into Microsoft's plan of fully integrating the web browser into the Windows UI. Furthermore, they have recently released the last of the Internet Assistant plug-ins for the Office 95 applications suite. When all are installed, it provides further clues into what we should expect from the next iteration of Office, which is due sometime in 1997.

Downloading this BETA, and running it side by side with the Netscape 3.0 BETA is certainly the best way to stress test the two. That way, at least you'll know for sure which of the two is more suited to your style and personality.

Required Plug-Ins

Before I get into the list of which plug-ins are required these days, let me tell you about a web site that you should keep a regular eye on. It is called the Browser Watch Plug-In Plaza, and it is at the following address on the World Wide Web:

http://www.browserwatch.com/plug-in.html

Every single plug-in made for either Windows 3.x, Windows 95/NT, MAC, or UNIX can be found there. They list each plug-in, which are all linked to their original home pages, so you can get more information on the companies that made them. They also graphically display which platforms each particular plug-in are made for. If you are serious about the Web, then, get serious about BrowserWatch!

Java ... a/k/a - JavaScript

This is the programming language that breathes life into static web pages, which spring to life when a little Java is added. More importantly, Java is a platform-independent development language, a true alternative to Microsoft's offerings. One downside is that, because it is based on the interpretive language C++, it isn't the easiest to understand.

Java is included in all Netscape Navigator browsers beginning with 2.0, and will be included in all Microsoft Internet Explorer browsers beginning with 3.0

The real skinny: An absolute must-have!! If you are using one of the browsers that doesn’t already have Java – add some! For more information, visit Sun Microsystems: http://java.sun.com/

RealAudio 2.0 BETA

File - ra32_2b4.exe (510,790 bytes)
Registration Fee - Free BETA
Publisher - ConnectSoft
WWW - http://www.realaudio.com

This is the plug-in that brings streamed audio to your desktop from any web page that contains embedded RealAudio files. Streaming allows the user to listen to the audio file at the same time it is being downloaded to a temporary file on the hard drive. Once the RealAudio player is shut down, and the browser exited, the streamed audio file automatically deletes itself.

RealAudio is one of several audio formats, but, it is far and away the most widely used. Not a standard yet, but it is destined to be, soon.

Shockwave 4.0

File - n32d40.exe (1,104,264 bytes)
Registration Fee - Free Download
Publisher - Macromedia
WWW - http://www.macromedia.com

Shockwave brings animation to the Web in a big way. If you have ever visited a web page that contained animated cursors, and well, animated anything, it was quite possibly, the work of Shockwave. In fact, there has been such a response to Shockwave, that I would dare say that this is one of the required plug-ins that you should definitely have set-up for use with your browser.

Acrobat Amber Document Viewer BETA

File - ambr32a1.exe (2,436,096 bytes)
Registration Fee - Free BETA
Publisher - Adobe Systems
WWW - http://www.adobe.com

Since the United States government decided to make Acrobat their preferred electronic document format, the Acrobat document viewer has found itself elevated to must-have status. The *Amber* beta is the latest version, and it is well worth checking out.

Live 3D BETA (VRML)

File - 3dns32a.exe
Registration Fee - Free BETA
Publisher - Netscape Communications
WWW - http://www.netscape.com

If you want to check out those 3D chat worlds that the computer press has been raving about, then you are going to have to have a VRML (Virtual Reality Modeling Language) plug-in for your browser. There are a few caveats, however. If you have anything less than a 28.8 modem, then forget about VRML for now. The response of the caching of the artwork requires the fattest pipe available. The first application of VRML has been chat, so don’t expect to see it used anywhere until several issues regarding bandwidth are resolved.

VDOLive

File - plgply32.exe (433,275 bytes
Registration Fee - Free Download
Publisher - VDOnet Corporation
WWW - http://www.vdolive.com

Every once in a while an application comes along that captures the attention of the power user. Because it features some exciting new application of a technology, VDOLive is one of the handful of plug-ins that has created a bit of a stir. VDOLive is essentially the video equivalent of the streaming technology that is also featured in RealAudio. Because it brings us video that can be viewed as it is being downloaded, VDOLive is the last of the recommended plug-ins that I will be talking about today.

Epilogue

This concludes the first bunch of WebMaster secrets. There are many more to follow, as there is lots more to say and know about designing home pages for the World Wide Web. Next month, I'll continue with the tools that you are going to need for Web Page creation. Although I am not in the business of recommending one software vendor over another, I will be talking about some of the most popular software packages, and hopefully that will point you into the right direction.

Next month, we'll continue to fill your Web toolbox and will be talking about the pros and cons of using a word processor instead of a dedicated HTML editor. We'll try to help you decide which is the path for you. A well stocked library will help you succeed in learning the craft of web page design, so we will also discuss the must-have reference titles that every good WebMaster must have. Finally, I will

talk about graphics on the Web. Everything from which file types to use, to why World Wide Web clip art needs to be different from the many other clip art libraries on the market.

Until next month... maybe we'll see each other on the surf . . . . .

This is the first in a series of HTML articles from Kent Daniel Bentkowski who has been a long time computer user and computer graphics designer. An exper-ienced BETA tester, Kent has participated with betas representing top software products on the market today. He is the author of the Windows 95 Registry FAQ, written during his stint as a Windows95 BETA tester and prior to the public release of '95. His article THE WINDOWS95 Registry FAQ was published in December of 1996 by WindoWatch (Vol.1 No. 9) He is also an active member of the Microsoft Developer Network.

Editorial Continued... **All of this will be assured if the cost of the Workstation version of NT becomes competitive with both Windows95 and OS/2.**

It is not just the glitz of graphics and music; sound for games or voice for the office and the Internet that will fuel this market. The way we work and play is placing an increasing pressure upon the operating systems we want to use. The winning marketing formula has been developed and tested. It is now a matter of dusting off the strategies that have worked in the past, updating them and finding and replacing the name NT 4 for Win95. And voila., another Microsoft success story.

ww

WEB BASED CONFERENCING:
COLLABORATION FOR THE NEXT CENTURY

AN ALLAIRE WHITE PAPER

As companies and organizations continue to adopt and deploy Internet-based technology solutions, it is increasingly important to reflect critically on the direction of Web application development (WAD). At the center of emerging Internet technologies is a new generation of Web applications which go beyond information publishing and distribution to enable collaboration and information exchange. This new generation of applications will redefine the way organizations use the Internet for both internal and external operations. The most exciting new application is Web-based conferencing.

How is the Web changing?

Until very recently the Web has been a system for distributing static information, rather than a true platform for dynamic data access and distributed applications - hallmarks of the early 1990s client/server revolution. Because of technical limitations and a lack of awareness about the potential for the technology, the Web has primarily been used to provide employees, customers, and the general public one-way information access to static documents.

The introduction of a new set of WAD tools is changing the way competitive companies and organizations use the Web. Increasingly, serious organizations are creating dynamic Web sites which fuse the Web with information in relational databases, document archives, and even legacy mainframe systems. WAD tools like Allaire's Cold Fusion make these dynamic Web sites possible.

More importantly, this new generation of WAD tools is giving companies and organizations the means to quickly develop and deploy sophisticated client/server Web applications on Intranets and the Internet. These applications are the foundation of a Web-based collaborative computing system which will transform the workplace of the future.

What is Conferencing?

Conferencing is a core application for computer networks. Conferencing systems enable groups of individuals to communicate electronically, and they have existed in a variety of forms for decades. In recent years they have grown in popularity as more and more organizations link their employees with networked computers.

In their simplest form, public conferences on Bulletin Board Systems (BBSs) and USENET News have provided a forum for public dialogue and exchange since the mid-1970s. Recently, more sophisticated services such as America On-Line and CompuServe have thrived with a variety of active public conferences at the center of their activities. Within organizations, private conferences have grown in popularity because they enable on-going collaboration and communication.

Internal conferencing systems range in complexity and integration with other desktop technologies. The most popular system is based on the proprietary client technology in Lotus Notes.

Because of its traditionally static structure, the Web has not been a platform for conferencing until now. As the Web browser becomes the universal client, conferencing is the most logical next step in Web applications. Web-based conferencing will provide a seamless link between public and private conferencing systems. Web conferences will become a core component to collaborative computing and groupware solutions.

What is Web Conferencing?

Web conferencing provides the foundation for true inter-networking between organizations and individuals by creating a unified platform for collaboration and group communication. Web conferencing overcomes many of the problems which have plagued other approaches to both public and private computer conferencing.

Web conferencing is easy to deliver because it does not depend on custom client software. Users or customers can use their Web browsers to access the conferencing system in the convenient and familiar environment of the Web page.

As more and more organizations adopt Web technology for both internal and external applications, it will soon become possible to tie together the internal systems of two distinct organizations to create an *inter-networked application*. Imagine the following scenario.

An engineering team in a firm is considering the use of a new line of production tools from a vendor they have worked with in the past. The new line will very likely have a huge impact on how their work evolves. Instead of following the traditional path - phone calls, paper literature, an onsite sales trip, perhaps even a full team-to-team meeting - they opt to invite several members of the vendor to join them

in a private conference on their quasi-public Web system. The teams then participate in an on-going conversation over a week, sharing thoughts, documents, visuals, and pointing to data and infor-mation on other public and private Web servers. This rich inter- action allows them to assess the tools in a strategic and thoughtful fashion without the huge expense (for the buyer or the seller) of travel, sending documents, missed phone calls, etc.

On the Internet, web conferencing can be a way to provide much richer interaction with constituencies and customers. Custom conferencing delivered via the Web is an incredible way to build customer loyalty and branded communities.

The Web is becoming the universal information interface. WAD tools are enabling a new generation of Internet applications which are transforming the nature of work and the structure of business, politics, and the global economy. As the first significant manifestation of these applications, Web conferencing overcomes the problems of other conferencing systems and lays the foundation for a new class of web-based collaborative computing systems.

Advantages of Web Conferencing in Internal Applications

Provide a uniform, easy-to-use interface to users

Integrate data access and information systems

Allow groups or teams to communicate privately or publicly

Create a space for organization wide communication and feedback

Eliminate the need for unproductive meetings

Exist in the context of the standard information interface - the Web browser

Advantages of Web Conferencing in External Applications

Allow for public and private interaction with customers.

Create a rich space for feedback and suggestions.

Enliven a static and information-centric Web page.

Provide a low-cost and manageable foundation for customer support.

Doesn't require any additional software for users - just a Web browser.

Overcome limitations of time and location.

Digital ID’s

Published with permission of VeriSign, Inc
A susidiary of RSA Data Security Corp.
July 15, 1995

VeriSign, Inc. was formed by RSA Data Security, Inc. and several major industry leaders to focus on building a seamless, global Digital ID (digital certificate) infrastructure. The foundation of services and products that has become VeriSign originated as part of RSA Data Security, the industry leader in providing public-key cryptography solutions going back to 1989. An updated version of this document is being prepared as this one is published.

Digital IDs are currently being used in products like Netscape's Commerce Server, Terisa System's Secure HTTP tool kit, and Apple's Mac OS 7.5.Sun, Open Market, CyberCash, Premenos, National Semiconductor and Lotus are all planning on implementing VeriSign's Digital ID services. VeriSign products are being used internally in many institutions, including branches of the U.S. government, major corporations, national laboratories, and universities.

DIGITAL IDs

What are Digital IDs (digital certificates)?

Digital IDs or digital certificates are the binding mechanism of a public key to an individual or other entity. They allow verification of the claim that a given public key does in fact belong to a given individual. Digital IDs help prevent someone from using a phony key to impersonate someone else.

In their simplest form, Digital IDs contain a public key and a name. As commonly used, they also contain the expiration date of the key, the name of the Certifying Authority that issued the Digital ID, the serial number of the Digital ID, and perhaps other information. Most importantly, it contains the digital signature of the Digital ID issuer. A Digital ID is issued by a Certifying Authority and signed with the Certifying Authority's private key.

Why do I need a Digital ID?

A Digital ID is an electronic ID file that notarizes the connection between an RSA public key and its purported owner, just as your driver license notarizes the connection between your photo and the rest of your identifying information (name, address, birth date, etc.) And just as you wouldn't go anywhere without your ID, users of secured applications and networks always need to *carry* their Digital Ids with them.

How do I get a Digital ID and what do I do with it?

Generating an *ID request* is part of the initial installation or setup procedures for many applications that use RSA public key cryptography. For example, Apple's implementation of Digital ID issuing capability allows Mac users to generate a *Signer Approval Request* from their DigiSign desktop.

After properly filling out the Digital ID request, the applicant follows the necessary procedures outlined in the request which includes attaching their public key and sending the proper documentation to the given Certifying Authority. The Certifying Authority will process the request and if it meets the requirements, a Digital ID will be forwarded back to the individual or organization.

What is authentication? What is a digital signature?

Authentication in a digital setting is a process whereby the receiver of a digital message can be confident of the identity of the sender and the integrity of the message. Authentication protocols can be based on either conventional secret-key cryptosystems like DES or on public-key systems like RSA.

In this document, authentication will generally refer to the use of digital signatures, which function like handwritten signatures for printed documents: the signature is an unforgable piece of data asserting that a named person wrote or otherwise agreed to the document to which the signature is attached. The recipient, as well as a third party, can verify both that the document did indeed originate from the person whose signature is attached and that the document has not been altered since it was signed. A secure digital signature system thus consists of two parts: a method of signing a document such that forgery is not feasible, and a method of verifying that a signature was actually generated by whomever it represents. Furthermore, secure digital signatures cannot be repudiated; i.e., the signer of a document cannot later disown it by claiming it was forged.

Unlike encryption, digital signatures are a recent development, the need for which has arisen with the proliferation of digital communications.

How is a digital signature used for authentication?

Suppose Alice wishes to send a signed message to Bob. She uses a hash function on the message to create a message digest, which serves as a *digital fingerprint* of the message. She then encrypts the message digest with her RSA private key; this is the digital signature, which she sends to Bob along with the message itself. Bob, upon receiving the message and signature, decrypts the signature with Alice's public key to recover the message digest. He then hashes the message with the same hash function Alice used and compares the result to the message digest decrypted from the signature. If they are exactly equal, the sig-nature has been successfully verified and he can be confident that the message did indeed come from Alice. If, however, they are not equal, then the message either originated elsewhere or was altered after it was signed, and he rejects the message. Note that for authentication, the roles of the public and private keys are converse to their roles in encryption where the public key is used to encrypt and the private key to decrypt.

In practice, the public exponent is usually much smaller than the private exponent; this means that the verification of a signature is faster than the signing. This is desirable because a message or document will only be signed by an individual once, but the signature may be verified many times.

One or more Digital IDs may accompany a digital signature. A Digital ID is a signed document attesting to the identity and public key of the person signing the message. Its purpose is to prevent someone from impersonating someone else, using a phony key pair. If a Digital ID is present, the recipient (or a third party) can check the authenticity of the public key, assuming the Certifying Authority's public key is itself trusted.

A digital signature is superior to a handwritten signature in that it attests to the contents of a message as well as to the identity of the signer. As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter the signed message in any way. The slightest change in a signed document will cause the digital signature verification process to fail. Thus, authentication allows people to check the integrity of signed documents. Of course, if a signature verification fails, it may be unclear whether there was an attempted forgery or simply a transmission error.

How are Digital IDs used?

A Digital ID is used to generate confidence in the legitimacy of a public key. Someone verifying a signature can also verify the signer's Digital ID to insure that no forgery or false representation has occurred. These steps can be performed with greater or lesser rigor depending on the context.

The most secure use of authentication involves enclosing one or more Digital IDs with every signed message. The receiver of the message would verify the Digital ID using the Certifying Authority's public key and, now confident of the public key of the sender, verify the message's signature. There may be two or more Digital IDs enclosed with the message, forming a hierarchical chain, wherein one Digital ID testifies to the authenticity of the previous Digital ID. At the end of a Digital ID hierarchy is a top-level Certifying Authority, which is trusted without a Digital ID from any other Certifying Authority. The public key of the top-level Certifying Authority must be independently known, for example by being widely published.

The more familiar the sender is to the receiver of the message, the less need there is to enclose, and to verify, Digital IDs. If Alice sends messages to Bob every day, Alice can enclose a Digital ID chain on the first day, which Bob verifies. Bob thereafter stores Alice's public key and no more Digital IDs or Digital ID verifications are necessary. A sender whose company is known to the receiver may need to enclose only one Digital ID (issued by the company), whereas a sender whose company is unknown to the receiver may need to enclose two Digital IDs. A good rule of thumb is to enclose just enough of a Digital ID chain so that the issuer of the highest level Digital ID in the chain is well-known to the receiver.

According to the PKCS standards for public-key cryptography, every signature points to a Digital ID that validates the public key of the signer. Specifically, each signature contains the name of the issuer of the Digital ID and the serial number of the Digital ID. Thus even if no Digital IDs are enclosed with a message, a verifier can still use the Digital ID chain to check the status of the public key.

What are the compelling uses of Digital IDs?

Digital IDs can be used in a variety of ways including e-mail, electronic commerce, groupware and electronic funds transfers. Netscape's popular Commerce Server requires a Digital ID for each secure server. Electronic commerce customers shopping at an electronic mall being run by Netscape's server software will request the Digital ID of the server to authenticate the identity of the mall operator and the content provided by the merchant. Without authenticating the server, the shopper would not be able to trust the operator or merchant with sensitive information like a credit cards number. The Digital ID is then instrumental in establishing a secure channel for communicating any sensitive information back to the mall operator.

What applications support Digital IDs today?

Users of Apple Computer's DigiSign application in Mac OS 7.5 can generate their own Digital ID requests and verify Digital IDs from other users. Netscape's popular Commerce Server software requires a server Digital ID. Sun, Open Market, Fischer International, Security Dynamics, CyberCash, Mitsubishi and National Semiconductor are all committed to making their products Digital ID capable.

Who issues Digital IDs and how?

Digital IDs are issued by a Certifying Authority (CA), which can be any trusted central administration willing to vouch for the identities of those to whom it issues Digital IDs. A company may issue Digital IDs to its employees, a university to its students, a town to its citizens. In order to prevent forged Digital IDs, the CA's public key must be trustworthy: a CA must either publicize its public key or provide a Digital ID from a higher level CA attesting to the validity of its public key. The latter solution gives rise to hierarchies of CAs.

Digital ID issuance proceeds as follows. Alice generates her own key pair and sends the public key to an appropriate CA with some proof of her identification. The CA checks the identification and takes any other steps necessary to assure itself that the request really did come from Alice, and then sends her a Digital ID attesting to the binding between Alice and her public key, along with a hierarchy of Digital

IDs verifying the CA's public key. Alice can present this Digital ID chain whenever desired in order to demonstrate the legitimacy of her public key.

Since the CA must check for proper identification, organizations will find it convenient to act as a CA for its own members and employees. There will also be CA’s that issue Digital IDs to unaffiliated individuals.

Different CAs may issue Digital IDs with varying levels of identification requirements. One CA may insist on seeing a driver's license, another may want the Digital ID request form to be notarized, yet another may want fingerprints of anyone requesting a Digital ID. Each CA should publish its own identification requirements and standards, so that verifiers can attach the appropriate level of confidence in the certified name-key bindings.

An example of a Digital ID-issuing protocol is Apple Computer's Open Collaborative Environment (AOCE). AOCE users can generate a key pair and then request and receive a Digital ID for the public key; the Digital ID request must be notarized.

What are alternatives to VeriSign?

There may be many entities that will eventually participate in issuing Digital IDs, creating Certifying Authorities, and or maintaining Certification Revocation Lists. The US Postal Service has already announced their intent to enter this business.

How can signatures remain valid beyond the expiration dates of their keys? Or, how do you verify a 20-year-old signature?

Normally, a key expires after, say, two years and a document signed with an expired key should not be accepted. However, there are many cases where it is necessary for signed documents to be regarded as legally valid for much longer than two years; long-term leases and contracts are examples. How should these cases be handled? Many solutions have been suggested but it is unclear which will prove the best. Here are some possibilities.

One can have special long-term keys as well as the normal two-year keys. Long-term keys should have much longer modulus lengths and be stored more securely than two-year keys. If a long-term key expires in 50 years, any document signed with it would remain valid within that time. A problem with this method is that any compromised key must remain on the relevant CRL until expiration; if 50-year keys are routinely placed on CRLs, the CRLs could grow in size to unmanageable proportions. This idea can be modified as follows. Register the long-term key by the normal procedure, i.e., for two years. At expiration time, if it has not been compromised, the key can be recertified, that is, issued a new Digital ID by the Certifying Authority, so that the key will be valid for another two years. Now a compromised key only needs to be kept on a CRL for at most two years, not fifty.

One problem with the previous method is that someone might try to invalidate a long-term contract by refusing to renew his key. This problem can be circumvented by registering the contract with a digital time-stamping service at the time it is originally signed. If all parties to the contract keep a copy of the time-stamp, then each can prove that the contract was signed with valid keys. In fact, the time-stamp can prove the validity of a contract even if one signer's key gets compromised at some point after the contract was signed. This time-stamping solution can work with all signed digital documents, not just multi-party contracts.

What is the legal status of documents signed with digital signatures?

If digital signatures are to replace handwritten signatures they must have the same legal status as handwritten signatures, i.e., documents signed with digital signatures must be legally binding. NIST has stated that its proposed Digital Signature Standard should be capable of "proving to a third party that data was actually signed by the generator of the signature." Furthermore, U.S. federal government purchase orders will be signed by any such standard; this implies that the government will support the legal authority of digital signatures in the courts. Some preliminary legal research has also resulted in the opinion that digital signatures would meet the requirements of legally binding signatures for most purposes, including commercial use as defined in the Uniform Commercial Code . A Government Accounting Office decision requested by NIST also opines that digital signatures will meet the legal standards of hand-written signatures.

However, since the validity of documents with digital signatures has never been challenged in court, their legal status is not yet well-defined. Through such challenges, the courts will issue rulings that collectively define which digital signature methods, key sizes, and security precautions are acceptable for a digital signature to be legally binding. Digital signatures have the potential to possess greater legal authority than handwritten signatures. If a ten page contract is signed by hand on the tenth page, one cannot be sure that the first nine pages have not been altered. If the contract was signed by digital signatures, however, a third party can verify that not one byte of the contract has been altered.

Currently, if two people wish to digitally sign a series of contracts, they may wish to first sign a paper contract in which they agree to be bound in the future by any contracts digitally signed by them with a given signature method and minimum key size.

Currently several efforts are underway to legislate the legality and use of digital signatures. Utah has implemented laws qualifying digital signatures. California and New York are being legislated with other states following.

CERTIFYING AUTHORITIES

Are Certifying Authorities susceptible to attack?

One can think of many attacks aimed at the Certifying Authority, which must be prepared to defend against said attacks.

Consider the following attack. Suppose Bob wishes to impersonate Alice. If Bob can convincingly sign messages as Alice, he can send a message to Alice's bank saying "I wish to withdraw $10,000 from my account. Please send me the money." To carry out this attack, Bob generates a key pair and sends the public key to a Certifying Authority saying "I'm Alice. Here is my public key. Please send me a Digital ID." If the CA is fooled and sends him such a Digital ID, he can then fool the bank, and his attack will succeed. In order to pre-vent such an attack the CA must verify that a Digital ID request did indeed come from its purported author, i.e., it must require sufficient evidence that it is actually Alice who is requesting the Digital ID. The CA may, for example, require Alice to appear in person and show a birth certificate. Some CAs may require very little identification, but the bank should not honor messages authenticated with such low-

assurance Digital IDs. Every CA must publicly state its identification requirements and policies; others can then attach an appropriate level of confidence to the Digital IDs.

An attacker who discovers the private key of a Certifying Authority could then forge Digital IDs. For this reason, a Certifying Authority must take extreme precautions to prevent illegitimate access to its private key. The private key should be kept in a high-security box, known as a Certificate Signing Unit, or CSU.

The Certifying Authority's public key might be the target of an extensive factoring attack. For this reason, CAs should use very long keys, preferably 1000 bits or longer, and should also change keys regularly. Top-level Certifying Authorities are exceptions: it may not be practical for them to change keys frequently because the key may be written into software used by a large number of verifiers.

In another attack, Alice bribes Bob, who works for the Certifying Authority, to issue to her a Digital ID in the name of Fred. Now Alice can send messages signed in Fred's name and anyone receiving such a message will believe it authentic because a full and verifiable Digital ID chain will accompany the message. This attack can be hindered by requiring the cooperation of two (or more) employees to generate a Digital ID; the attacker now has to bribe two employees rather than one. For example, in some of today's CSUs, three employees must each insert a data key containing secret information in order to authorize the CSU to generate Digital IDs.

Unfortunately, there may be other ways to generate a forged Digital ID by bribing only one employee. If each Digital ID request is checked by only one employee, that one employee can be bribed and slip a false request into a stack of real Digital ID requests. Note that a corrupt employee cannot reveal the Certifying Authority's private key, as long as it is properly stored.

Another attack involves forging old documents. Alice tries to factor the modulus of the Certifying Authority. It takes her 15 years, but she finally succeeds, and she now has the old private key of the Certifying Authority. The key has long since expired, but she can forge a Digital ID dated 15 years ago attesting to a phony public key of some other person, say Bob; she can now forge a document with a signature of Bob dated 15 year ago, perhaps a will leaving everything to Alice. The underlying issue raised by this attack is how to authenticate a signed document dated many years ago.

Note that these attacks on Certifying Authorities do not threaten the privacy of messages between users, as might result from an attack on a secret-key distribution center.

What if the Certifying Authority's key is lost or compromised?

If the Certifying Authority's key is lost or destroyed but not compromised, Digital IDs signed with the old key are still valid, as long as the verifier knows to use the old public key to verify the Digital ID to prevent compromise.

In some CSU designs, encrypted backup copies of the CA's private key are kept. A CA which loses its key can then restore it by loading the encrypted backup into the CSU, which can decrypt it using some unique information stored inside the CSU; the encrypted backup can only be decrypted using the CSU. If the CSU itself is destroyed, the manufacturer may be able to supply another with the same internal information, thus allowing recovery of the key.

A compromised CA key is a much more dangerous situation. An attacker who discovers a Certifying Authority's private key can issue phony Digital IDs in the name of the Certifying Authority, which would enable undetectable forgeries; for this reason, all precautions must be taken to prevent compromise.

If a compromise does occur, the CA must immediately cease issuing Digital IDs under its old key and change to a new key. If it is suspected that some phony Digital IDs were issued, all Digital Ids should be recalled, and then reissued with a new CA key. These measures could be relaxed somewhat if Digital IDs were registered with a digital time-stamping service. Note that compromise of a CA key does not invalidate users' keys, but only the Digital IDs that authenticate them. Compromise of a top-level CA's key should be considered catastrophic, since the key may be built into applications that verify Digital IDs.

Why are there multiple trust hierarchies?

Several Digital ID hierarchies (domains) have been established to ensure a common level of identity and confidence for all Digital IDs within the domains. Two of the most popular domains with thousands of existing customers, are the Commercial Hierarchy (Digital IDs for individual users) and the Secure Server Hierarchy (Digital IDs for specific servers used in Electronic Data Interchange and Electronic Commerce). Universities, corporations, and other entities may find it useful to establish their own hierarchies.

What is a Certificate Issuing System (CIS)?

With a purchase of CIS, your organization is granted the right to issue its own Digital IDs for employees and affiliates. The CIS includes the most secure, tamper resistant hardware made anywhere in the world, CIS software and documentation and your company's unique *distinguished name* to become a Certification Authority. You can establish your organization as a Certification Authority within VeriSign's Commercial Certification Authority or establish your own *custom* hierarchy. The CIS is also pre-loaded with Digital ID serial numbers (like postage in a postage meter) and can be replenished by contacting VeriSign at any time.

What is a CSU?

It is extremely important that private keys of Certifying Authorities are stored securely, because compromise would enable undetectable forgeries. One way to achieve the desired security is to store the key in a tamperproof box; such a box is called a Certificate Signing Unit, or CSU. The CSU would, preferably, destroy its contents if ever opened, and be shielded against attacks using electromagnetic radiation. Not even employees of the Certifying Authority should have access to the private key itself, but only the ability to use the private key in the process of issuing Digital IDs.

There are many possible designs for CSUs; here is a description of one design found in some current implementations. The CSU is activated by a set of data keys, which are physical keys capable of storing digital

information. The data keys use secret-sharing technology such that several people must all use their data keys to activate the CSU. This prevents one disgruntled CA employee from producing phony Digital IDs.

Note that if the CSU is destroyed, say in a fire, no security is compromised. Certificates signed by the CSU are still valid, as long as the verifier uses the correct public key. Some CSUs will be manufactured so that a lost private key can be restored into a new CSU.

Bolt, Beranek, and Newman (BBN) currently sells a CSU, and RSA Data Security sells a full-fledged Digital ID issuing system built around the BBN CSU.

CERTIFICATE REVOCATION LIST

What are Certificate Revocation Lists (CRLs)?

A Certificate Revocation List (CRL) is a list of Digital IDs that have been revoked before their scheduled expiration date. There are several reasons why a key might need to be revoked and placed on a CRL. A key might have been compromised. A key might be used profession-ally by an individual for a company; for example, the official name associated with a key might be "Alice Avery, Vice President, Argo Corp." If Alice were fired, her company would not want her to be able to sign messages with that key and therefore the company would place the key on the CRL.

When verifying a signature, one can check the relevant CRL to make sure the signer's key has not been revoked. Whether it is worth the time to perform this check depends on the importance of the signed document.

CRLs are maintained by Certifying Authorities (CAs) and provide information about revoked keys originally certified by the CA. CRLs only list current keys, since expired keys should not be accepted in any case; when a revoked key is past its original expiration date it is re-moved from the CRL. Although CRLs are maintained in a distributed manner, there may be central repositories for CRLs, that is, sites on networks containing the latest CRLs from many organizations. An institution like a bank might want an in-house CRL repository to make CRL searches feasible on every transaction.

KEY MANAGEMENT

What key management issues are involved in public-key cryptography?

Secure methods of key management are extremely important. In practice, most attacks on public-key systems will probably be aimed at the key management levels, rather than at the cryptographic algorithm itself. The key management issues mentioned here are discussed in detail in later questions.

Users must be able to securely obtain a key pair suited to their efficiency and security needs. There must be a way to look up other people's public keys and to publicize one's own key. Users must have confidence in the legitimacy of others' public keys; otherwise an intruder can either change public keys listed in a directory, or impersonate another user. Digital IDs are used for this purpose.

Digital IDs must be unforgable, obtainable in a secure manner, and processed in such a way that an intruder cannot misuse them. The issuance of Digital IDs must proceed in a secure way, impervious to attack. If someone's private key is lost or compromised, others must be made aware of this, so that they will no longer encrypt messages under the invalid public key nor accept messages signed with the invalid private key. Users must be able to store their private keys securely, so that no intruder can find it, yet the keys must be readily accessible for legitimate use. Keys need to be valid only until a specified expiration date. The expiration date must be chosen properly and publicized securely. Some documents need to have verifiable signatures beyond the time when the key used to sign them has expired.

Although most of these key management issues arise in any public-key crypto system, for convenience they are discussed here in the context of VeriSign.

Who needs a key?

Anyone who wishes to sign messages or to receive encrypted messages must have a key pair. People may have more than one key. For example, someone might have a key affiliated with his or her work and a separate key for personal use. Other entities will also have keys, including electronic entities such as modems, workstations, and printers, as well as organizational entities such as a corporate depart-ment, a hotel registration desk, or a university registrar's office.

How does one get a key pair?

Each user should generate his or her own key pair. It may be tempting within an organization to have a single site that generates keys for all members who request one, but this is a security risk because it involves the transmission of private keys over a network as well as catastrophic consequences if an attacker infiltrates the key-generation site. Each node on a network should be capable of local key generation, so that private keys are never transmitted and no external key source need be trusted. Of course, the local key generation software must itself be trustworthy. Secret-key authentication systems, such as Kerberos, often do not allow local key generation but instead use a central server to generate keys.

Once generated, a user must register his or her public key with some central administration, called a Certifying Authority. The Certifying Authority returns to the user a Digital ID attesting to the veracity of the user's public key along with other information. Most users should not obtain more than one Digital ID for the same key, in order to simplify various bookkeeping tasks associated with the key.

Should a public key or private key be shared among users?

In the RSA public-key cryptosystem, each person should have a unique modulus and private exponent, i.e., a unique private key. The public exponent, on the other hand, can be common to a group of users without security being compromised. Some public exponents in common use today are 3 and 216+1; because these numbers are relatively small, the public-key operations (encryption and signature verification) are fast relative to the private key operations (decryption and signing). If one public exponent becomes a standard, software and hardware can be optimized for that value.

In public-key systems based on discrete logarithms, such as ElGamal, Diffie- Hellman, or DSS, it has often been suggested that a group of people should share a modulus. This would make breaking a key more attractive to an attacker, however, because one could break every key with only slightly more effort than it would take to break a single key. To an attacker, therefore, the average cost to break a key is much lower with a common modulus than if every key has a distinct modulus. Thus one should be very cautious about using a common modulus; if a common modulus is chosen, it should be very large.

What happens when a key expires?

In order to guard against a long-term factoring attack, every key must have an expiration date after which it is no longer valid. The time to expiration must therefore be much shorter than the expected factoring time, or equivalently, the key length must be long enough to make the chances of factoring before expiration extremely small. The validity period for a key pair may also depend on the circumstances in which the key will be used, although there will also be a standard period. The validity period, together with the value of the key and the estimated strength of an expected attacker, then determines the appropriate key size.

The expiration date of a key accompanies the public key in a Digital ID or a directory listing. The signature verification program should check for expiration and should not accept a message signed with an expired key. This means that when one's own key expires, everything signed with it will no longer be considered valid. Of course, there will be cases where it is important that a signed document be considered valid for a much longer period of time.

After expiration, the user chooses a new key, which should be longer than the old key, perhaps by several digits, to reflect both the performance increase of computer hardware and any recent improvements in factoring algorithms. Recommended key length schedules will likely be published.

A user may recertify a key that has expired, if it is sufficiently long and has not been compromised. The Certifying Authority would then issue a new Digital ID for the same key, and all new signatures would point to the new Digital ID instead of the old. However, the fact that computer hardware continues to improve argues for replacing expired keys with new, longer keys every few years. Key replacement enables one to take advantage of the hardware improvements to increase the security of the cryptosystem. Faster hardware has the effect of increasing security, perhaps vastly, but only if key lengths are increased regularly.

How do I find someone else's public key?

Suppose you want to find Bob's public key. There are several possible ways. You could call him up and ask him to send you his public key via e-mail; you could request it via e-mail as well. Certifying authorities may provide directory services; if Bob works for company Z, look in the directory kept by Z's Certifying Authority. Directories must be secure against unauthorized tampering, so that users can be confident that a public key listed in the directory actually belongs to the person listed. Otherwise, you might send private encrypted information to the wrong person.

Eventually, full-fledged directories will arise, serving as on-line white or yellow pages. If they are compliant with CCITT X.509 standards, the directories will contain Digital IDs as well as public keys; the presence of Digital IDs will lower the directories' security needs.

What is a digital time-stamping service?

A digital time-stamping service (DTS) issues time-stamps which associate a date and time with a digital document in a cryptographically strong way. The digital time-stamp can be used at a later date to prove that an electronic document existed at the time stated on its time-stamp. For example, a physicist who has a brilliant idea can write about it with a word processor and have the document time-stamped. The time-stamp and document together can later prove that the scientist deserves the Nobel Prize, even though an arch rival may have been the first to publish.

Here's one way such a system could work. Suppose Alice signs a document and wants it time-stamped. She computes a message digest of the document using a secure hash function and then sends the mess-age digest (but not the document itself) to the DTS, which sends her in return a digital time-stamp consisting of the message digest, the date and time it was received at the DTS, and the signature of the DTS. Since the message digest does not reveal any information about the content of the document, the DTS cannot eavesdrop on the documents it time-stamps. Later, Alice can present the document and time-stamp together to prove when the document was written. A verifier computes the message digest of the document, makes sure it matches the digest in the time-stamp, and then verifies the signature of the DTS on the time-stamp.

To be reliable, the time-stamps must not be forgeable. Consider the requirements for a DTS of the type just described. First, the DTS itself must have a long key if we want the time-stamps to be reliable for, say, several decades. Second, the private key of the DTS must be stored with utmost security, as in a tamperproof box. Third, the date and time must come from a clock, also inside the tamperproof box, which cannot be reset and which will keep accurate time for years or perhaps for decades. Fourth, it must be infeasible to create time-stamps without using the apparatus in the tamperproof box.

A cryptographically strong DTS using only software has been implemented by Bellcore; it avoids many of the requirements just described, such as tamperproof hardware. The Bellcore DTS essentially combines hash values of documents into data structures called binary trees, whose *root* values are periodically published in the newspaper. A time-stamp consists of a set of hash values which allow a verifier to recompute the root of the tree. Since the hash functions are one-way the set of validating hash values cannot be forged. The time associated with the document by the time- stamp is the date of publication.

The use of a DTS would appear to be extremely important, if not essential, for maintaining the validity of documents over many years. Suppose a landlord and tenant sign a twenty-year lease. The public keys used to sign the lease will expire after, say, two years; solutions such as recertifying the keys or resigning every two years with new keys require the cooperation of both parties several years after the original signing. If one party becomes dissatisfied with the lease, he or she may refuse to cooperate. The solution is to register the lease with the DTS at the time of the original signing; both parties would then receive a copy of the time-stamp, which can be used years later to enforce the integrity of the original lease.

In the future, it is likely that a DTS will be used for everything from long-term corporate contracts to personal diaries and letters. Today, if an historian discovers some lost letters of Mark Twain, their authenticity is checked by physical means. But a similar find 100 years from

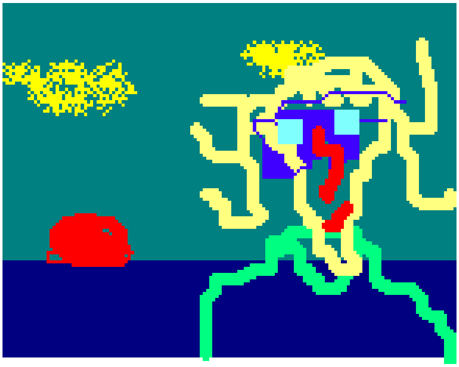
now may consist of an author's computer files; digital time-stamps may be the only way to authenticate the find.

Part Two which we'll publish next time will cover how the federal government is dealing with these concerns and what parts of the technology are ready to be implemented.

We thank Verisign, Inc. for permission and assistance in reproducing their valuable white paper.

ww

Unplugged Alice



I got a handwritten note in the mail from Alice, my friend and person of letters. She was taking the lead set by Kurt Vonnegut, who announced he does not believe in writing on the computer.

Alice now tells time by the height of the sun in the sky and ties string to trees on her walks so she may find her way back. She shops for food at the bazaar where there are no cash registers to impede her socially.

Alice does not answer the phone, as she does not have a phone. It turns out that there is no federal law that says you must have a phone. Since she is beyond all cellular grids, she has retired her cellular phone as well. She sends no faxes, she receives no faxes.

She brings up her water from a well, and cooks over an open hearth. Since she does not believe in automobiles any more, she must carry everything on her head. She washes her clothes by a stream, stone washing her jeans. Although it takes her easily a hundred hours a week to do all the chores, she feels the peace of mind is worth it.

She charges up a few thousand a month on the American Express, and pays it in full at the end of each month. Since she took with her a number of patents upon leaving Green Line Software, she can well afford the cash flow. She does not leave home without her card. As soon as she perfects her paper IOU system with the local merchants, she will dispense with the card forever.

Alice has donated all her computer equipment to me, and has begun singing in an acapella group on her island. They swing through the sleepy town serenading the populace, who pause briefly in their telecommute to salute them.

Last month, though, Alice contracted a rare disease, and after screening by managed care, was medivaced to the mainland for treatment.

She says she is feeling much better, and has gotten a bicycle to get around a little faster. She has decided to give up writing with a quill pen, and now has several packages of ball-points to draw from.

Alice says the quiet life is getting her down, and she may come back to computer land sooner than originally thought.

Peter Neuendorffer is a Windows programmer and the inventor of Alice. Included in his list of programs is a Windows program to sweep away office clutter: Petmt31.zip, available on his WEB page at http://channel1.com/users/petern or write to Peter at petern@channel1.com

ww

OFFICE 95: WORD V 7.0

Copyright 1996 by Frank McGowan

Okay! I finally gave in and started using Win95. How else was I going to review the Office 95 suite? Much to my surprise, I think I like it, at least what I've seen of Word, so far. The first thing that impresses me is the built-in Spell facility which underlines my typographical errors in wavy red. Now I can see the errors as I go along, rather than waiting until I've finished the file. Nice! No one can claim not see the errors unless they're color blind. To make the correction, click the right mouse button on the indicated word and a list of suggestions appears, just as though you'd been using the Spell program from the menu bar or the toolbar.

I suspect the main reason I like Word 7 so much is that it so closely resembles Word 6. There's been no radical makeover from one to the other. The changes are significant but subtle, with major emphasis on ensuring that Word files are ready to be zapped across the Internet with as little additional processing as necessary. Thus the File menu looks pretty much the same, except for the inclusion of the Send and Add Routing Slip options. Other than that, you'll have nothing to adjust relating to choices on the menu bar.

The same holds true for the Standard Toolbar, which has an array of pushbuttons virtually identical to the 6.0 toolbar. There is the addition of an Insert Address button, presumably to a file to be sent via Email, though I was not able to confirm this. When I clicked on it, I got a dialog box telling me to enter a logon name for

a schedule I wanted to work with. Taking the cowards' way out, I canceled the request.

The Formatting toolbar has a really neat feature, new to 7.0: the highlighter, which lets you set selected text to a different color. For example, you might have made changes to a file and want your reader to be able to see them quickly. Just select the text, click the highlighter button (the one with the little yellow square in it) and zap! The selection is a different color (yellow, unless you choose another). You could do this before, but only by using the Format, Font option and dealing with the dialog box.

Likewise, the status bar contains our old V6.0 friends (the three View option buttons for Normal, Page Layout View and Outline View) and the usual indicators telling you where you are and what's what.

On of Word's best features, AutoCorrect, has been improved through significant additions to its list of automatic corrections. For example "alot" becomes "a lot," which warms the cockles of my heart. Why "noone" was omitted is a mystery; and "potatoe," remains unrecognized as well, so I guess Dan Quayle will have to rely on his staff for the correct spelling. Nor have they figured out a way to get people to stop using "loose" when they mean "lose."

In keeping with the slant towards Internet-compatibility, AutoCorrect also provides Email-friendly characters, which let you put in emoticons like smiley faces and have them appear as special symbols. Thus, the :-) combination comes out as its symbolic counterpart, if you have the appropriate symbols in your arsenal of typefaces.

Maybe this would be a good time to create a little table, so I can use that feature to summarize what I liked/didn't like about Word 7.

Feature	Liked	Disliked
AutoCorrect	Y	
File menu	Y*	
Spell	Y	
Table	Y	
Insert	Y	
Autotext	Y	
Tip Wizard		Y
* There's still no Delete option, which continues to annoy me. Why should I have to use the File Manager to nuke an old Word file?		

As you can plainly see, the Table features still work quite nicely, and in the same way they did in the earlier version (always a good feature, in my opinion). My one complaint about Word 7 is similar to the one I had about Word 6: get rid of the Tip Wizard. All it does is take up space on the screen without providing an iota of information to the user. At least I didn't see that stupid "If you run with pointed objects, you can hurt yourself," or whatever it was. I suspect it's still there, however.

Switching from one open Word file to another is still pretty straightforward (once you've been told how): click the Window menu, then click the name of the file that appears in the pulldown menu. The Window menu still contains the Split and Arrange options, as before. Nothing too startling there.

Now I’ll try using the Section break and Column features to see if there are any major new breakthroughs to report. So far, nothing alarming. I’ll just fill with a bunch of repeated X’s to see what happens. Stand by.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Okay, it looks just about as I expected it would. Let’s switch back to single-column format.

Ah, that's more like it.

I wonder what they did to the Header/Footer feature? No time like the present to find out. Much to my relief, I don't have to be retrained! Everything looks "normal," i.e., just as it did in V6. I hope all this similarity to the old version means they meant to design it this way, not that they didn't have time to make all the changes they wanted to.

After more than a quarter of a century in the business, I know how hard it is to prevent software types from redesigning everything from the ground up, especially if they weren't the original designers. That's the price of putting so much stress on being innovative, I suppose. Maybe it's time to start rewarding people for knowing when to leave well enough alone, - or is that too radical a concept?

The topic of tabs, for some reason, has been a bugaboo for me and my students. I can't be sure whether it's because tabs are inherently confusing or that I'm not very good at teaching people how to use them. Whichever it is, apparently I'm going to get no help from the new version of Word: tab formatting remains unchanged. With all my sermonizing about leaving things alone, I guess I shouldn't complain. Still…

The other feature that unfailingly gets me and my students in trouble is Indenting via the Ruler. I've gotten so gun-shy, I'm ready to turn the Ruler off, rather than let people drag those damned indents around. In the usual case, they drag them so far left, they're off the sheet! I spend most of my time getting them back where they were (you can't imagine the hue and cry that arises when this happens).

Summing up, I can say that Word 7 seems to be an excellent follow-on to its Windows 3.1 predecessor, which is my way of saying it was no trouble to learn and use, having once learned Word 6. In this respect, at least, the transition from 3.1 to 95 is silky smooth.

ww

Next month, I hope to have a review of Excel 7.0. Based on what I've seen of the Office 95 package , I'm looking forward to it.

McGowan has been contributing articles to WindoWatch for quite sometime where he most recently has reviewed the Suites from both Lotus and Microsoft. Frank McGowan has the experience, as both a user and teacher, to authoritatively evaluate and review Microsoft Office for Windows95. When he's not doing fine things for the magazine, he is a trainer, computer consultant and college teacher.

A Ferry Tale...

A helicopter pilot, whose job was to ferry VIP's from Seattle's airport downtown, one day found himself with a passenger in thick fog somewhere over downtown Seattle. No landmarks were visible and the passenger became panicky. The pilot said, "Don't worry" and very gradually let the helicopter down until it was hovering opposite the window of a large and unknown building.

The pilot motioned to a woman working in the building to roll down her window and asked her "Where are we?"

The woman responded "You're in a helicopter."

The pilot immediately lifted the helicopter above the buildings, flew a mile and a half, let it down through the fog, and hit the landing pad dead center.

Amazed and relieved, the passenger said, "How on earth did you do that?"

The pilot said: "It was simple! The information the woman gave me was precisely correct and totally useless. I knew that she had to be working at the Microsoft Customer Support Center."

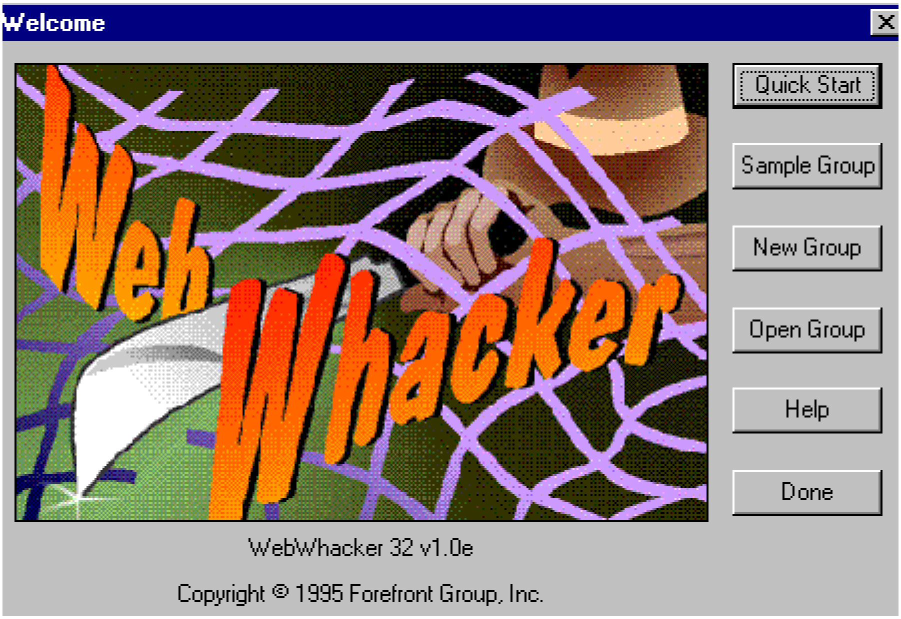
ww

WebWhacker ***A Product Review***

Browsing Web Sites at Leisure

Copyright 1996 by John M. Campbell

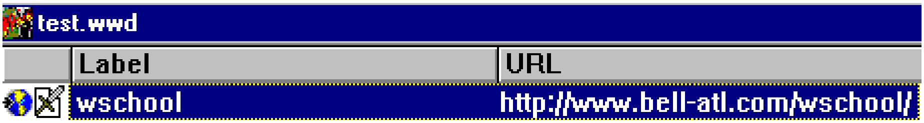
In the last issue, I described Milktruck Delivery, one of the new breed of Web Browser *enhancements*. Now, let's look at a competing product, WebWhacker 32, from the ForeFront Group, Inc. These programs are designed to download an entire Web site, or a selected portion(s), for offline viewing. While both serve the same end, the manner in which each goes about its task is rather different.



ww

WEbWhacker 32 is, as the name implies, a 32-bit program. It requires either Windows 95, or Windows NT 3.5 or later. Windows 3.1 and Mac versions of the program are also available. For viewing *whacked* pages, any browser that meets the Spyglass SDI standard will do. WebWhacker costs $49.50, but a free demo version is available. I will be talking about the demo in this review.

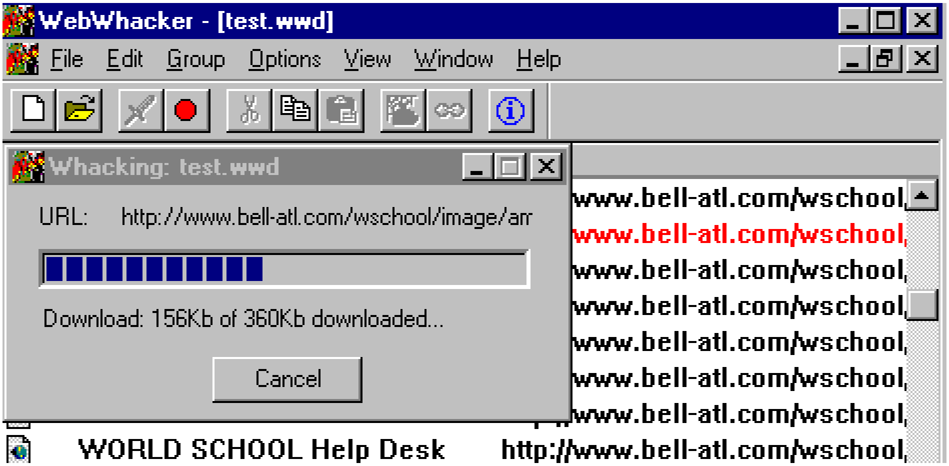
WebWhacker's opening screen contains six large buttons: Quick Start, Sample Group, New Group, Open Group and Done. The Quick Start choice brings up an overview of the program's operation in sufficient detail for the user to do just what the name implies.
The sample group included with the program contains four pages from ForeFront's own Web site. By the way, the term *group* is used here to mean pages organized as the user sees fit. All of the pages on a site might constitute a group, or the user can collect pages from different sites that share something in common, such as Education Related or Schools as seen below.



test.wwd

Label	URL
wschool	http://www.bell-atl.com/wschool/

I began by creating a new group. I simply dragged a URL from my Netscape Bookmarks menu into the WebWhacker Group List Window. I chose the Bell Atlantic Schools Home Page URL. This URL displayed as the full HTTP address, with two symbols to its left; a globe (site not yet whacked), and a dagger (site ready for whacking). I next pulled down the Options menu and chose the desired whack level. One can choose levels from 0 to 100, or all levels. Levels refer to how far down one wishes to go when following links on the start page. For example, whacking down two levels would retrieve all pages (first level) referenced on the start page (zero level), and all pages referenced on each of first level pages. Normally, the program will not pick up pages external to the site where the start page is located. However, there is a dialog box choice that, if checked, will permit retrieval of one level of external links.



URL: http://www.bell-atl.com/wschool/image/arr

Download: 156Kb of 360Kb downloaded...

www.bell-atl.com/wschool,
www.bell-atl.com/wschool,
www.bell-atl.com/wschool,
www.bell-atl.com/wschool,
www.bell-atl.com/wschool,
www.bell-atl.com/wschool,
www.bell-atl.com/wschool,
WORLD SCHOOL Help Desk http://www.bell-atl.com/wschool,

The next step is the actual "whacking" process. I clicked the dagger icon at the top of the window, and WebWhacker immediately went online to the designated site. At this point, a dialog box popped up to display the download process. Note that WebWhacker downloads independently of one's Web browser. A browser doesn't even need to be loaded while the program is retrieving information. The browser is only used to display pages that have been retrieved by WebWhacker.

ww

After the desired levels of a site are retrieved, the symbols at the left of the page name in the Group List window, change. The dagger disappears, and the globe changes to a page symbol, meaning the page has been retrieved. Now, one can invoke an add-links feature to see what lies at the next lower level for each page that was retrieved. Clicking the add-links icon displays a dialog box that shows the name and URL addresses for all links that appear on a chosen page in the Group List window. From this dialog, one can pick and choose pages to add to the Group List window. These pages can then be whacked.

This makes it possible to go back online and selectivly download only those links that are of interest, rather than being forced to retrieve all links several levels deep on the first download of an unfamiliar site, in the hope that most of the material will be worth viewing. It can take considerable time to download every page referenced in two or three levels of a site.

If WebWhacker is unable to get a linked page, that URL is displayed red in the Groups List window. One can check the Properties for any URL either by clicking an icon, or, if using Windows 95, with a right-mouse click. For problem pages, the properties sheet will indicate why the download failed. When one of the linked page could not be retrieve from Bell Atlantic, the Properties Error tab showed "Request not found - invalid URL."

WebWhacker includes a number of bells and whistles. A Table of Contents feature loads an entire whacked group into one's browser as a html document, making it possible to follow links online just as one would if the displayed page had been retrieved by the browser. Extensive use of cut-and-paste permits moving pages among groups

at will. URLs in WebWhacker windows can be dragged into a browser, or from browser to WebWhacker. Multiple groups can be whacked at the same time.

I found that the program worked pretty much as advertised. It does have some deficiencies, though. There is no way to disable the download of graphics content. Graphics add considerable overhead, and not everyone wants to see them. Also, there is no way to retrieve sites that require a password for access. Image maps are not supported. And the program, at least for me, won't work with the 32-bit Trumpet Winsock. Also be aware that the evaluation version will only whack 10 times, and that the software disables thirty days following installation. For extended use, one must purchase the permanent version from ForeFront.

In my opinion, the most serious deficiency is that WebWhacker replaces, without asking permission, several key DLLs in the Windows/System directory by substituting older versions. The only clue one has that this is taking place is a dialog advising that a DLL is read-only, overwrite Y or N? Worse, regardless of how one answers the question, uninstalling WebWhacker completely removes these DLLs. In my installation, this botched uninstall routine effectively killed both Netscape and my Internet dialler.

So, how does WebWhacker compare with its main competitor, Milktruck Delivery? I found Milktruck to be the better program, overall. It does retrieve password-protected sites, and offers an option to bypass graphics elements when downloading pages.

Also, Milktruck will visit some popular subscription sites, such as ESPN's SportsZone and CNN Interactive. Further, it has the ability

ww

to update selected sites, delivering only changed information. WebWhacker lacks this feature. Finally, Milktruck has a more intuitive interface and costs about $20 less.

John Campbell continues to provide articles of interest and quality about the Internet and Internet tools created for the various Windows platforms. In real life, as opposed to his virtual one, John is the manager of the Elkins, WV local office of the WV Unemployment Compensation Board. He is also the Co-Host of the Browsers conference found on Ilink.

ww

Are You Ready for NT?

WindoWatch is participating in the NT beta program and over the next months we will be reporting our experiences. Even though Paul Kinnaly, Linda Rosenbaum and Jim Plumb are our official beta testers, others will be looking at the current version 3.51 to develop experience with the operating system.

Given the more general renewed interest in WindowNT we decided to do some digging for NT resources on the Internet and found some bona fide goodies.

There are many specialized areas from RAS (remote access service) to discussions of BackOffice. Others will follow with lists and links pages covering the NT waterfront. Nonetheless this bejewled offering will stay the course as a bibliography for those of us learning the new terrain. The following are solid general information sites done with remarkable authority and skill. You will find a certain amount of duplication from site to site but each has its unique flavor and emphasis.

INFO NEDERLAND from Edwin Drieesens
http://nt.info.nl/default.htm

Sam Houston State University
http://coba.shsu.edu/messages/nt-list.htm

Rick's Information Center
http://rick.wzl.rwth-aachen.de/rick

ww

University of Michigan at Dearborn
http://www.umd.umich.edu/~cwilli

InterGreat Software
http://intergreat.com/winnt/ftpsites.htm

Beverly Hills Software
http://www.bhs.com/

A neat (and free) networking utility for NT, '95 and Windows for Workgroup connectivity from the Aquia Company.
WindowsGroup95
http:/www.aquia.com/web/wingroup.html

And finally a pair of "new to us" pages...

http://www.foxnet.de/ntsoft00.htm

http://www.webwriter.com/winnt.htm

Windows NT Workstation 4.0 (Beta)

A First Look...

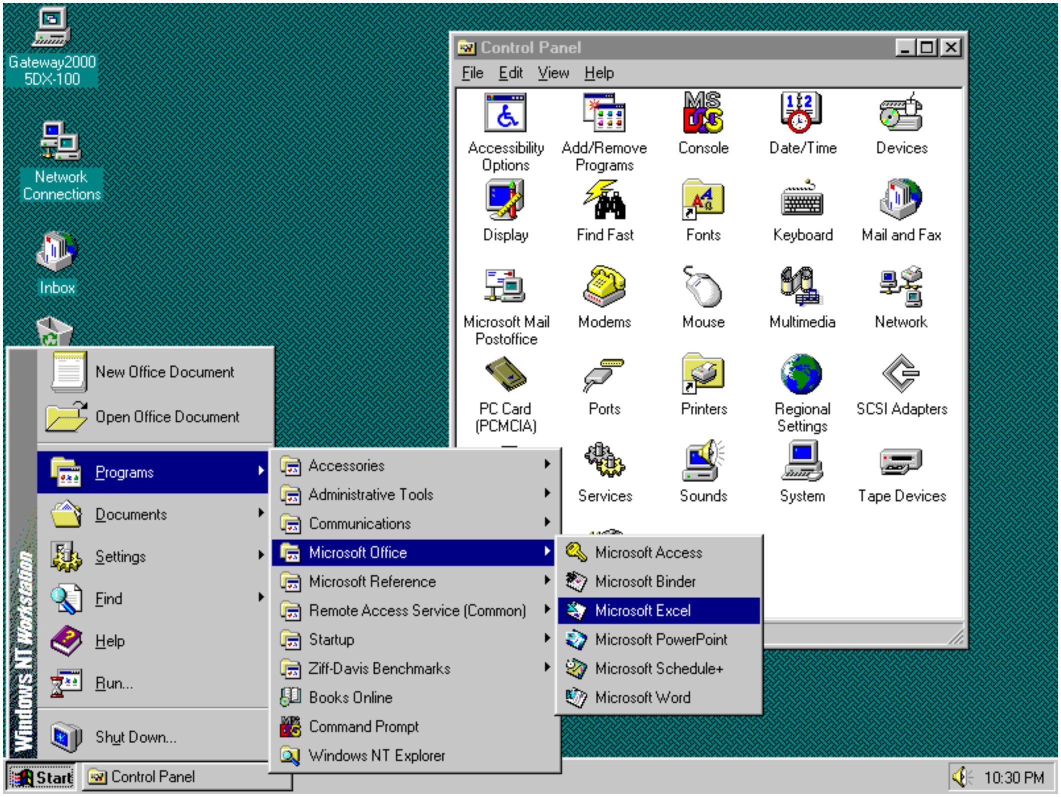
I guess I've always been a bit of an OpSystem junkie. I started computing with an Apple][, graduated to an Apple IIGS, then played with an Amiga. Using an add-on board, I even ran IBM PC software on my IIGS (and you thought an 8088 was slow?) and Mac software on my Amiga. Eventually, I migrated to a PC and have since used MS-DOS, DR-DOS, Windows 3.0, Windows 3.1, OS/2 2.1, Windows for Work-groups 3.11, and Windows95. So I guess it should be no surprise that when I was offered a chance to look at the *WindoWatch* beta copy of Microsoft's new Windows NT Workstation 4.0 beta, I jumped at it!

I knew I'd be pushing the limits some. My old Gateway 4DX-33V had been upgraded to 16mb of RAM and had a new Cyrix 5x86-100 CPU, but everything I had read about current versions of NT Workstation said they would run in 12mb, but if you wanted them to *run*, you needed 24mb or more and a Pentium CPU. However, the Microsoft publicists had been touting that NT 4.0 would be less demanding of memory, so it seemed worth a shot.

I was also concerned that I might lose my current Win95 setup. While NT can dual-boot with some OpSystems, I wasn't sure the new beta could peace-

fully co-exist with ‘95. But, what the heck... If this was to be Microsoft’s business/power-user OS of choice, I knew I had to give it a try.

In a coming issue of *WindoWatch*, we’ll be bringing you many more details on NT 4.0, both the Server and Workstation versions, as well as other NT related articles, but for now, I’d like to give you my first impressions...



ww

Microsoft is now referring to NT 4.0 as the *Shell Update Release*. Somehow, one expects more than just a single feature upgrade to mark an “X.0” release of software, even if a total redo of the shell and user interface is that feature. Even though there is more to 4.0 than just that, the changed interface is the most readily obvious and apparent.

Once booted and logged on, there are but two tiny clues that the desktop you are seeing comes from NT rather than 95: The Explorer icon is labeled “NT Explorer” and the Start Menu displays “Windows NT” along its side - rather than Windows95. Even in the early Press Beta I am testing (Build 1234), the shell update is uncanny in its resemblance to that of 95. From the *Auto-Hide* of the toolbar, to the context menus available with a right-click of the mouse, the practices one is familiar with from 95 carry over to NT 4.0 exactly. Certainly, for the average user, NT 4.0 and Windows 95 will be virtually indistinguishable - with one significant difference, speed.

This *is* still a beta. And -hopefully- the release version will be further tweaked for performance. But, NT does require more memory for smooth operation than even Windows95. While the speed difference is minimal with single, simple tasks, for anything complex or for true multitasking, even a 16mb machine is too little. I’ll be presenting some numeric results in my follow-up article, but if you are considering NT, I would urge you to take advantage of the current low prices on memory! We’ve all joked about Microsoft’s assertion that Windows95 will run with 4 mb of RAM; power users know that even 8 mb causes considerable system-slowing swapping and that 16 mb is about right. Microsoft’s equivalent claim for NT Workstation (or Server!) 4.0 is 12 mb; I can see why most users say 24 mb is a more practical figure.

I am an NT novice - at best. Even so, I have not been gentle with the 4.0 beta. I have played with the Registry, played with the Network settings, toyed with the desktop, rights, permissions, services, and more. And -while not

everything is working properly anymore- I have yet to crash it. That's not to say it's crash proof, but its stability is superb. Just as Windows95 is substantially more stable than its 16bit predecessor was, NT 4.0 lives up to NT's rock-solid reputation in this area.

One last note for this "First Impression": NT 4.0 will very nicely set up a Dual-Boot capability with Windows95. This will allow a user to maintain their current *compatibility oriented* Windows95 system while also having the *stability oriented* option of running NT. Although it has not been implemented in this beta, there are strong indications that in the release version, NT 4.0 will have the capability of installing over -and thus replacing- Windows95. Here, however, Microsoft faces a significant problem in that the Windows95 and Windows NT system Registries vary - considerably. Thus, it does not appear that such an installation will migrate desktop settings, installed software, etc. Rather, reinstallation will be necessary. Perhaps Microsoft will find a way around this situation prior to final release, but for now installing NT 4.0 will mean reinstalling all software for 95 users.

We'll be talking more about NT very soon. But in the interim, if your PC has more than 16 mb of RAM and a Pentium processor, I would encourage you to read everything you can about NT 4.0; I really think you may want to seriously consider it as a supplement to, if not an alternative for, Windows95.

Paul Kinnaly is a member of the WindoWatch Editorial board, our WebMaster, chief of the Eagle Eyes department and general right hand of the magazine. He with Linda Rosenbaum and Jim Plumb are beta testing NT for both Microsoft and WindoWatch. He is a Management Analyst for the Veterans Administration.

ww

Windows NT File System Security

An Overview and Comparison

By Dennis Martin
Rocky Mountain Windows NT User Group
November 1994

Internet: 76314.1441@compuserve.com

http://budman.cmdl.noaa.gov/RMWNTUG/RMWNTUG.HTM
ftp://budman.cmdl.noaa.gov/RMWNTUG/White_papers/NTFSSEC1.DOC

ww

Introduction

One of the important and popular features of Windows NT is the file security built into the file system known as "NTFS." This paper primarily presents basic file security information about NTFS, and compares this to other well-known computer operating systems.

These other operating systems include MVS/ESA, OS/2, OS/400, and VM/ESA from IBM, VAX/VMS from Digital, MS-DOS and Windows from Microsoft, and a variant of UNIX.

This document is not intended to be a comprehensive security guide for Windows NT systems. Rather, this is an overview of the file security for the Windows NT file system, NTFS.

The material presented here has been obtained from the author's personal experience, or from the references cited in the technical references list.

Send comments and questions regarding this document to:

Dennis Martin
CompuServe: 76314,1441
Internet: 76314.1441@compuserve.com

NTFS Feature Overview

As the *network becomes the computer*, the need for security in the file system becomes increasingly important for desktop computers, even (especially) in the commercial sector. Windows NT provides fully integrated networking capabilities and supports several network protocols natively. One of these, TCP/IP, provides services such as "ftp" that are available on UNIX systems, mainframe systems, and the Internet. Because of this interoperability with existing networks, the user of a Windows NT system needs to be aware of the relatively easy to use security features available with Windows NT.

Security features are built into the Windows NT operating system. Microsoft has applied for U.S. Government Class C2 security compliance for Windows NT. Windows NT provides a secure logon facility, discretionary access control, auditing and memory protection, which are features required for Class C2 security. Security attributes are defined for all system resources (objects) within the Windows NT operating system. These objects include processes, threads, memory, files and other items. Many of the security features can be "tuned" to fit into your environment.

Windows NT currently provides three file systems. These are known as File Allocation Table (FAT), High-performance File System (HPFS) and Windows NT File System (NTFS). The FAT file system is used by MS-DOS and was introduced in 1981. In 1990, HPFS was introduced as part of OS/2. In 1993, Windows NT became generally available, and introduced NTFS.

NTFS is designed to perform the basic operations of a file system and provide advanced features not found on other systems. The advanced features include file system recovery, data access control and ownership privileges, long Unicode filenames and other features. The server versions of Windows NT also support uninterruptible power supplies, disk mirroring, disk duplexing, and disk striping with parity. Some of the advanced features require a small computer standard interface (SCSI) controller, for which Windows NT provides native support.

These are the kinds of features mainframes and mini-computers have used for some time. It's a good thing that these kinds of features are now available on desktop computer operating systems.

NTFS Security Features

Security in Windows NT was designed into the system, from the ground up. Although the security model works through all the components of Windows NT, NTFS offers data security that is unavailable with FAT or HPFS systems.

Class C2 Security

The Windows NT security model is designed to meet U.S. Government Class C2 security. Some of the C2 requirements are listed here.

Secure Logon Facility. Each user must logon to the system with a unique userid and password. The system must track all activities of the user with the unique identification.

Discretionary Access Control. The owner of a resource must be able to determine and control who has access to that resource, and what they can do with that resource.

Auditing. System administrators must be able to detect and record security-related events. This includes attempts to create, access or delete system resources.

Memory Protection (Object Reuse). When a resource (such as memory or a file) is released back to the operating system, that resource's contents are not available for re-use by other processes.

NTFS uses security attributes available at logon time to allow or disallow access to files and directories. The Windows NT Resource Kit provides a detailed description of the Windows NT security id, security access token, access control list, access control entry, and related security components. This paper will simply describe at a high level, the kinds of file and directory permissions that can be set using NTFS.

Auditing A variety of levels of file security auditing can be enabled or disabled, depending on your preferences. These are set using the User Administrator tools and the File Manager security menus. If you want no auditing of any security-related events having to do with files and directories, you can turn it all off.

You can audit nothing, successes, failures or both successes and failures for any file or directory access. You can also audit activities involving things other than file or directory access.

Memory Protection Memory protection for files means that when you delete a file, the area used by the data is not recoverable by any process. To restore the data, you must restore from your regular backup media, such as floppy disk, tape, etc.

Groups Part of the security profile for a user is the group or groups to which that user belongs. There are several default groups included with Windows NT, such as *administrator, power user, tape backup operator, guest* and others. You can also create new groups. A user may be a member of more than one group. The Windows NT Resource Guide explains the process of granting access to a particular resource for users that belong to more than one group.

Security Privileges The kinds of privileges that can be granted are listed below. These are found in the Security/Permissions menu of the File Manager. In the following definitions, a resource is a file or directory, unless specifically indicated.

No Access. No access to the resource. You do not even see the name of the resource.

List. You may see the name of the resource, but not access it contents.

Read. You may see the name and read (or copy) the contents of the resource.

Read and Add. You may see the name, read the resource or append new data to the resource. Change. You may see the name, read, append or change the resource (read and write).

Delete. You may see the name, read, append, change or delete the resource.

Execute. You may execute the program, but not read (copy) it.

Permissions. You may grant a specific user or group of users the privilege to alter the security permissions of a resource that you currently own.

Take Ownership. You may grant a specific user or group of users the right to become the owner of a resource that you currently own.

Full Control. You have all the above privileges.

Special. A special combination of the individual security attributes. Many systems, including Windows NT, have a feature known as hidden files (or directories). These are files that are present, but do not normally appear in a listing of files. You simply have to know that these files are present. Any of the above security privileges can be applied to hidden files. You can change permissions on a file or directory. When you change permissions on a directory, you may optionally change the permissions of it's existing subdirectories and their contents.

You may give different privileges to different users or groups for the same file or directory. For example, you might give *No Access* to members of the Guests group to all the files in the C:\XYZ directory, while granting "Read" access to members of the Power Users group for the same directory, while granting *Full Control* to members of the Administrators group.

The following table compares NTFS to the file systems of other operating systems, for the security privileges listed above. This is not an attempt to discuss all the security features available for any given

operating system. There are many other security features available which are beyond the scope of this document.

File Security Features Table

	NTFS	MSDOS	MVS	OS/2	OS/400	UNIX	VAX	VM
No Access	X		X		X	X	X	X
List	X						X	
Read	X	X	X		X	X	X	X
Read&Add	X				X			
Change	X	X	X	X	X	X	X	X
Delete	X		X		X		X	X
Execute	X		X		X	X	X	
Permissions	X		X		X		X	X
Take Ownership	X					*		

*** Some variants of UNIX have limited versions of Take Ownership.**

Technical References

The following is a list of publications used in preparing this document. The ISBN or other document numbers are included.

Baritz, Tony & Dunne, David. *AS/400 Concepts And Facilities*. McGraw-Hill, 1991. ISBN 0-07-018301-5.

Custer, Helen. *Inside Windows NT*. Microsoft Press, 1993

ISBN 1-55615-481-X.

Digital Equipment Corporation. ***VMS User's Manual,***
VMS Version 5.2. Digital Equipment Corporation, 1989.
Order No. AA-LA98B-TE.

IBM Corporation. ***Resource Access Control Facility*** **(RACF)**
Command Language Reference**. IBM Corporation, March 1993.**
SC28-0733-14.

IBM Corporation. ***Resource Access Control Facility*** **(RACF)**
General User's Guide**. IBM Corporation, March 1993.**
SC28-1341-08.

IBM International Technical Support Centers. ***AS/400 Security and***
Auditing Considerations**. IBM Corporation, 1988.**
GG24-3322-00.

Microsoft Corporation. ***Microsoft MS-DOS 6 User's Guide*****.**
Microsoft Corporation, 1993. Doc. No. MS55892-1193.

Microsoft Corporation. ***Microsoft MS-DOS 6.2 Technical Reference*****.**
Microsoft Corporation, 1993. Doc. No. MS55879-1193.

Microsoft ***CorporationWindows NT Resource Guide, Volume 1.***
Microsoft Press, 1993. ISBN 1-55615-598-0.

National Computer Security Center. ***Department of Defense Trusted***
Computer System Evaluation Criteria**. National Computer Security**
Center, December 1985. DOD 5200.28-STD. Also known as the
Orange Book.

National Computer Security Center. *Trusted Network Interpretation, Version I*. National Computer Security Center, 31 July 1987. NCSC-TG-005. Also known as the Red Book.

Picking Everyone’s Brains!

Anyone following the operating system buzz around the Microsoft planning for Nashville, Memphis, or Cairo must keep in mind earlier forays into geographic punditry like Chicago and all points every where.

Nonetheless, given the long standing and public disdain of the FAT, primarily from UNIX users of all dialects, the OS/2 bunch and what's left of the Apple camp, Microsoft has ignored the slurs from the noisy competition and is planning for FAT32.

The File Allocation Table or FAT is simply a method of organizing space on a hard drive. It has been said that FAT16 is inefficient and doesn't use every bit of available hard drive real estate. That debate will rage some where else....depend on it! However, that is not our mission.

We have collected commentary about FAT32 from as many available sources to be found through a simple YAHOO search on FAT32. The following represents what we uncovered. We have done some limited editing (really translating from computereeze into English) from the several dozen YAHOO citations from news services and tech reports.

The 32 Bit FAT File System removes restrictions inherent in the standard 8.3 file system upgrading it to be compatible (long file names) with various software applications. Basically the FAT entries

will be 32 bits wide giving it more room to expand over the next few years. Keep in mind, there is still an unclear time frame for release of both 32bit Windows operating systems after major upgrades. This last has to be the raison d'etre for the FAT32 move amid the aforementioned criticism, - some of which is legitimate.

It is said that it is almost impossible to fill a 32 bit FAT table before exhausting the maximum partition space. The important reason not to dump the FAT file system is backward compatibility. The reason to upgrade to FAT32 is accommodation for the larger hard drive partitions even though the NTFS (NT File System and other 32bit file systems) perform more efficiently on large partitions.

FAT32 will change the data structures that inventory the entries of a hard disk. It certainly gives those of us renewing interest in NT to carefully reconsider converting to the NTFS because one is unable to reconvert to either of the FAT systems after NTFS is installed. Further, FAT32 will, obviously not be compatible with Fat16 utility software.

The new FAT32 file system, will be an important feature in the newest Windows service pack release. The primary motivator is that FAT32 will support hard disks beyond the present 2GB ceiling. Additionally it will eliminate cranky cluster size problems we've heard about ad nauseum. I for one am never sure whether this public beefing is an excuse to bash Bill Gates or memorialize him for inventing FAT16.

In truth FAT16 is old and should be updated to handle the huge hard drives coming to market. Presently formatted drives have a maximum cluster size of 32K bytes. A 1K-byte file throws away 31K bytes of disk space. FAT32, allows clusters be as small as 512 bytes.

ww

It is expected that Microsoft will release the Windows Service Pack 2, just to PC manufacturers. The upgrade promises support of the 32-bit PC Card standard, IRQ sharing on PCI systems, and the big new storage devices.

"Major overhauls of both systems are scheduled for 1997. Windows 95 is code-named Memphis, and Windows NT is code-named Cairo."

These new Windows service pack features were previously referred to as Nashville, but Microsoft has not yet settled on a name for the final release. My nomination is West Virginia!

According to the April 15th issue of PCWeek, Microsoft will release Service Pack 2 for Windows 95 late in the summer of 1996.

ww

Cartoon Laws of Physics

Contributed by Derek Buchler

Cartoon Law I

Any body suspended in space will remain in space until made aware of its situation.

Daffy Duck steps off a cliff, expecting further pastureland. He loiters in mid-air, soliloquizing flippantly, until he chances to look down. At this point, the familiar principle of 32 feet per second takes over.

Cartoon Law II

Any body in motion will tend to remain in motion until solid matter intervenes suddenly.

Whether shot from a cannon or in hot pursuit on foot, cartoon characters are so absolute in their momentum that only a telephone pole or an outsize boulder retards their forward motion absolutely. Sir Isaac Newton called this sudden termination of motion the stooge's surcease.

Cartoon Law III

Any body passing through solid matter will leave a perforation conforming to its perimeter.
Also called the silhouette of passage, this phenomenon is the specialty

of victims of directed-pressure explosions and of reckless cowards who are so eager to escape that they exit directly through the wall of a house, leaving a cookie- cutout-perfect hole. The threat of skunks or matrimony often catalyzes this reaction.

Cartoon Law IV

The time required for an object to fall twenty stories is greater than or equal to the time it takes for whoever knocked it off the ledge to spiral down twenty flights to attempt to capture it unbroken.

Such an object is inevitably priceless, the attempt to capture it inevitably unsuccessful.

Cartoon Law V

All principles of gravity are negated by fear.

Psychic forces are sufficient in most bodies for a shock to propel them directly away from the earth's surface. A spooky noise or an adversary's signature sound will induce motion upward, usually to the cradle of a chandelier, a treetop, or the crest of a flagpole. The feet of a character who is running or the wheels of a speeding auto need never touch the ground, especially when in flight.

Cartoon Law VI

As speed increases, objects can be in several places at once.

This is particularly true of tooth-and-claw fights, in which a character's head may be glimpsed emerging from the cloud of altercation at several places simultaneously. This effect is common as well among bodies that are spinning or being throttled. A *wacky* character has the option of self- replication only at manic high speeds and may ricochet off walls to achieve the velocity required.

Cartoon Law VII

Certain bodies can pass through solid walls painted to resemble tunnel entrances; others cannot.

This trompe l'oeil inconsistency has baffled generations, but at least it is known that whoever paints an entrance on a wall's surface to trick an opponent will be unable to pursue him into this theoretical space.

The painter is flattened against the wall when he attempts to follow into the painting. This is ultimately a problem of art, not of science.

Cartoon Law VIII

Any violent rearrangement of feline matter is impermanent.

Cartoon cats possess even more deaths than the traditional nine lives might comfortably afford. They can be decimated, spliced, splayed, accordion-pleated, spindled, or disassembled, but they cannot be destroyed. After a few moments of blinking self pity, they reinflate, elongate, snapback, or solidify.

Corollary: A cat will assume the shape of its container.

Cartoon Law IX

Everything falls faster than an anvil.

Cartoon Law X

For every vengeance there is an equal and opposite revengeance.

This is the one law of animated cartoon motion that also applies to the physical world at large. For that reason, we need the relief of watching it happen to a duck instead.

Cartoon Law Amendment A

A sharp object will always propel a character upward. When poked, usually in the buttocks with a sharp object (usually a pin),a character will defy gravity by shooting straight up, with great velocity.

Cartoon Law Amendment B

The laws of object permanence are nullified for "cool" characters.

Characters who are intended to be "cool" can make previously non-existent objects appear from behind their backs at will. For instance, the Road Runner can materialize signs to express himself without speaking.

Cartoon Law Amendment C

Explosive weapons cannot cause fatal injuries.
They merely turn characters temporarily black and smoky.

Cartoon Law Amendment D

Gravity is transmitted by slow-moving waves of large wavelengths.

Their operation can be witnessed by observing the behavior of a canine suspended over a large vertical drop. Its feet will begin to fall first, causing its legs to stretch. As the wave reaches its torso, that part will begin to fall, causing the neck to stretch. As the head begins to fall, tension is released and the canine will resume its regular proportions until such time as it strikes the ground.

Cartoon Law Amendment E

Dynamite is spontaneously generated in *C-spaces* (spaces in which cartoon laws hold).

The process is analogous to steady-state theories of the universe which postulated that the tensions involved in maintaining a space would cause the creation of hydrogen from nothing. Dynamite quanta are quite large (stick-sized) and unstable (lit). Such quanta are attracted to psychic forces generated by feelings of distress in "cool" characters (see Amendment B, which may be a special case of this law), who are able to use said quanta to their advantage. One may imagine C-spaces where all matter and energy result from primal masses of dynamite exploding. A big bang indeed.

Derek Buchler is a Systems Administrator and regularly contributes to WindoWatch.

Hardware Notes

Upgrading the Display

Bob, Doesn't one select the monitor first and then find a card that shows off the special features of the monitor in the best way?

Actually, one can buy the graphics card first and benefit from some performance gains with the old monitor. Here's some information to demystify the subject...

First, ask yourself how big of a monitor you might want in the near term future. You see, the bigger the screen, the greater the chance of eye fatiguing flicker. That's because there's so much area to "paint" that the first part of screen being scanned (i.e., "painted") is fading out before it's refreshed (i.e., "repainted"). Note the use of the term, refreshed... you just learned a fundamental technical term for graphics cards.

When one speaks of Refresh Rate, they're talking about how quickly the graphics card can send a new screen-full of information to "refresh" the image.

The higher the refresh rate, the better. When we all had 13-14" monitors, refresh rates of 60 Hz were fast enough to keep the screen bright and flicker free. But step up to a 17" monitor, and the graphics card better be able to handle a refresh rate of 70 Hz or better (some say 90 Hz).

ww

So, you now know a little about refresh rates. Take comfort that virtually all modern graphics cards can handle the higher refresh rates that larger monitors want... at least at typical screen resolutions... which takes us to the next technical item.

If one gets a bigger monitor, it's probably because they want to see more information on the screen. The standard resolution for a 13-14" monitor is 640x480 pixels or the number of paint dots across the screen times the number of paint rows top to bottom. With a 17" monitor, a popular resolution is 1024 x 768 pixels. This lets you, for example, see more of a document at one time.

Ah, but more pixels means the graphics card has to pass along more *paint* for each screen-full of information. That's more work. To make matters worse, we just discussed the importance of refresh rates. We're not only asking for more paint per screen, that is, higher resolution, we're also asking that it be delivered faster or at a higher refresh rate. As if that weren't enough to give the graphics card a headache, we haven't decided how many potential colors we want to see... known as color depth.

Shall we draw each screen-full of information selecting from only 16 differently colored cans of paint? That would be ok for text and simple graphics and it's still the color depth used for a standard Windows VGA display. But selecting from 256 different colors, known as 8-bit color, gives a more life-like image. I remember when

that was considered photo quality1 Not any more. Today there is 15-bit High Color (32,768 colors), 16-bit High Color (65,536 colors) and 24-bit True Color (16.7 million colors).

ww

By now you should be gaining some respect, if not sympathy, for what some people expect from their graphics card.. pick from tens of thousands of individual paint cans (color depth), paint more on the screen (screen resolution), and be quick about it (refresh rate).

But isn't video memory one of the keys?

Bingo! That's where the above three factors come together. If I'm a graphics card and you ask me to paint a 640x480 screen-full of information using 16 colors, I can probably remember to do that without a tremendous tax on my "memory". Ask me to do a 1024x768 picture using 16.7 million colors and I may *run out of memory* before I've even formulated in my mind what the picture is supposed to look like! And, even if I had that much memory, if you want it drawn quickly, I'd better be able to *think fast,* i.e., be able to process the information quickly. I'd better have some specialized Video memory to work with known as VRAM.

The real life of a graphics card is no different than my simple analogy. It has to formulate in memory what the screen-full of information is going to look like... before it sends it to the monitor. With a limited amount of memory, one makes tradeoffs... high resolutions, less colors... or low resolution and more colors. Some people are greedy and want both which is fine,- just add more memory!

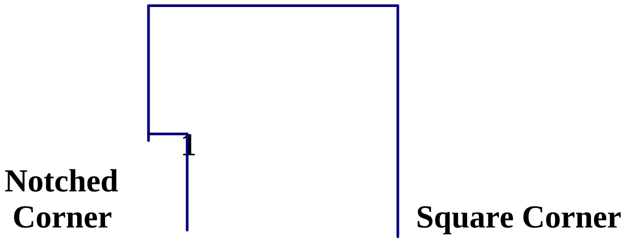
Well, that's enough of the basics for one session. The technical gurus are already wincing at the liberties I've taken. Any more, and a few of them will be more than just "looking" at their monitors.

ww

Another Hardware Notes

When I asked my friend Bob Blow how one knows which end is which when installing simms to a motherboard he come up with this:

Regarding where pin #1 is on memory modules, if you look along the bottom edge of the simm (the edge that plugs in to the socket), you'll see that one of the outside corners has a notch shaved out of it. Hold the simm with the notch to the left and pin 1 will be the first pin on the left.



Because of this notch, the simms won't properly seat in the mother-board sockets if you try to install them incorrectly. In other words, if the simms lock in place, you've done it correctly.

If you can't get the little locking arms to snap in place, you've got the simm turned around, end for end.

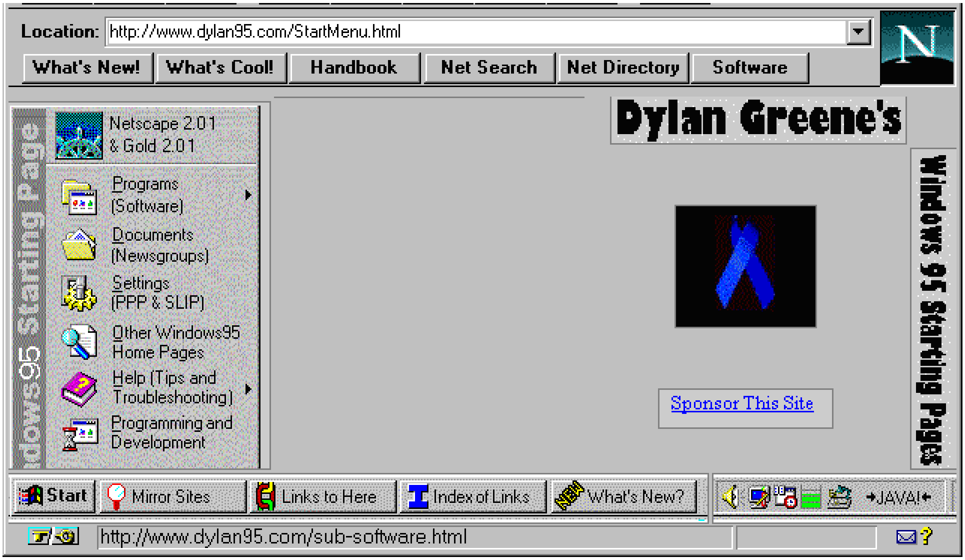
Bob Blow is a very versatile computer user and hardware maven. His messages to Ilink conferees are always worth publishing. He has tentatively promised us a sound board piece...

ww

The Dylan Greene Windows95 Starting Pages

Dylan Green has one of the most useful Windows95 resource pages on the WEB. He presents a wide variety of Windows information and organizes it in ways that make the goodies he offers easily accessible.

This is not the usual *List and Links* pages we are used to seeing. The attractive Start Page is uncluttered notwithstanding the menued items available for selection.



Location: http://www.dylan95.com/StartMenu.html

http://www.dylan95.com/sub-software.html

.

http://www.dylan95.com

Some of Greene's other accomplishments include:

Interface design and construction of the user interface to three AEGIS missile encounter simulators created by other people. His program adds bounds and error checking, default values, the ability to save input values, and an extensive batch-run process which permits the program to run several sets of data overnight. The intuitive Windows based interface also makes the program easier to use because the data controls were logically placed and are automatically enabled and disabled based upon values of other controls.

As a computer consultant and advisor, he maintain the latest versions of Internet software, and I has taught others how to use different Internet tools, including composing HTML. Working with others, they created WITS (Windows Internet Tool Set) for the Computer Science Center. WITS sets up installs and configures several Internet programs, as well as a PPP Winsock stack for Windows 3.x users. With WITS, users do not have to know or understand what their DNS, SNTP, NNTP, and other Internet addresses are. WITS is used by the majority of students, staff, and faculty at Maryland who use Windows 3.x. Served as a computer consultant for the University of Maryland, servicing questions with various hardware and software problems.

AND!

Rated Number 5 Computer Site by Iway Magazine
Selected as WLYN Special Link of the Year.
Rated among the "Top 5% of All Web Sites" by Point Survey.
PC WEEK: "Probably the most complete site of this type..."
Boardwatch Magazine's "Best Of Reader-Submitted Web Sites."
PCsense "Web Site of the Month" for December 1995.
Guest on Info Snack, 640 AM, Toronto, Ontario
First Place in the 1994 ACM/Robotics Club Lego Competition ‘94

ww

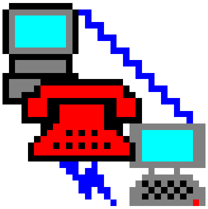
Fourth Place in the 1994 ACM RobotWars. (10/27/94)

Programming:

WebMatic: HTML Automation by Dylan Greene

WebMatic is a program written for creating his extensive set of Windows 95 web pages. In addition to automatically creating Netscape and MSIE enhanced versions of the site, it also creates the "What's New" page, the site index, adds a NEW or UPDATED icon next to new links *which is removed by WebMatic after the link is one week old* and does global search and replaces throughout the entire site over multiple files and directories. Even tho' WebMatic is Greene's creation it has been structured in such a way that it can be split into parts so that others can work on and enhance different sections of the program. Examples of Dylan Greene's work can be found at: http://dylan.thru.net

Presently Dylan Greene is a Sophomore in the University of Maryland's Computer Science Department.



Reflections of a ModemJunkie

A World Grown Smaller . . .

The Internet is changing the ways we think. Categories that once made sense are losing their meaning. Sometimes that is a gain while other times, a loss. When thinking about the last six years on line, I remember the excitement of communicating with someone from Europe or visiting an online friend while on vacation in Washington, D.C. I remember a wonderful dinner in my home with friends from Brooklyn, Utah and the Midwest, all of whom I met online.

Part of the excitement was learning about each other. Then the other day something happened. Regular readers know that I am always looking for new software that doesn't require new hardware; applications that are conservative in their use of resources, so that end users with other places to put their money (like the mortgage or their children's education) can continue to take full advantage of the many expanding opportunities.

A week or so ago I spotted an announcement about a new HTML editor. I sent the author an e-mail and he sent me a copy of his latest beta. It was small, fast, opened like lightening, and left memory available to run other applications while it was open-- even on this old 386/40. The author mentioned in a note that at the moment he didn't have access to a web site and he wondered if I could put a link to his file on my home page. That was a good trade off -- he would have a way to distribute his file and I would get increased hits on my page from people wanting to download his file. Some might even glance at my page before clicking on the link.

I asked the author to send me a short paragraph about the file and another about himself. He did so and I made the necessary changes to my home page, including a reference to his place of birth and his current home -- both of which happen to be half way around the world, more or less.

Soon, I got another e-mail. The author said that he thought nationality was not relevant on the Internet and would I, please, remove the biographical information. I did as he asked.

And I understand the point. Since a simple click takes me from Chicago to Tokyo and then another can jump me to Israel, what difference does it make where the author lives or comes from. I really do understand. But isn't something lost as well?

When Washington's birthday merged with Lincoln's and became President's Day and when Columbus Day was moved to Monday, I began to mourn the loss of meaningful distinctions -- each became just another three day weekend. Are we not about to lose more as we take away the wonder of just how marvelous the Internet really is? Or am I just hopelessly old fashioned?

By the way, the editor I am referring to, DiDa, is available on my home page http://www.mcs.net/~grossman Try it out. The author keeps sending me updates and improvements.

ww

Browser Software Grown Bloated

One of the reasons I need a small HTML editor is that I frequently want to run it while Netscape is open and, sometimes, while I am online as well. If other applications were as conservative with resources it would not be a problem, but Netscape is growing so fat so fast it is frightening. When I first downloaded Netscape it was a little over a meg. By last winter Netscape 2.0 had grown to over two megs. Now the preview of Atlas, the latest Netscape beta is out. Its over six megabytes.

SIX !! Forgive me for shouting. Netscape is in a battle with Microsoft and others to maintain dominance in the browser wars, so they think they have to add every bell and whistle to every version. It should be called the Netscape Suite, by now. I understand the current version even has an HTML editor built in. When will they add a spell checker and a Diet Coke dispenser??

I understand: make a full featured application, but do it with options. One of the biggest jokes is Netscape's built in news reader. Click and my whole machine slows down as a giant news reading application sucks resources like a starving pig -sorry, Babe! And its not even a good news reader. The news groups related to browsers are full of questions as to how to do this or that under Netscape's new reader. The most common response is a recommendation to use another reader. This has been going on since last summer, but Netscape doesn't seem to be able to take the hint.

Like many others, I do use another news reader-- NewsXpress. But the old simple, and generally inadequate news reader in Netscape versions 1.x did have some good features. It let you bookmark a particular news group and open that group directly with a single click.

ww

That was my favorite way of browsing. I clicked on News:comp.infosystems.www.announce and began my late night surfing seamlessly from there... Can't do that with Netscape 2.x And you need 2.x for all those new Netscape features-- frames, moving banners, coffee --oh, I mean Java.

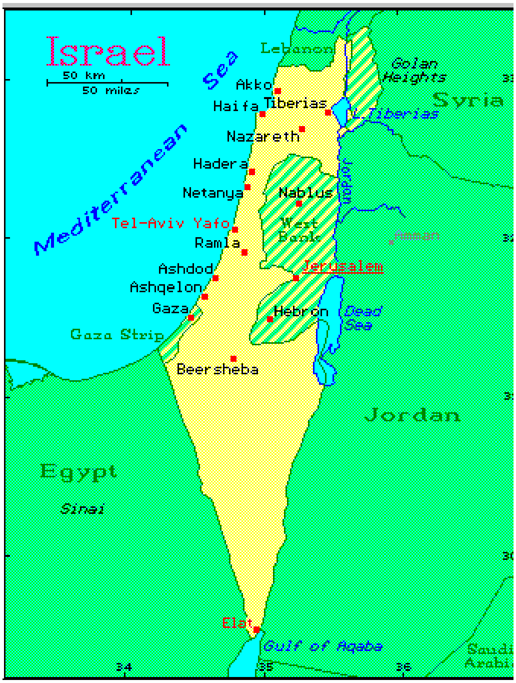
So I thought, I'll just keep two copies of Netscape on my machine--1.x for surfing and 2.x just for sites (and there are more and more of them) that demand 2.x or better and even tell you so in strong language if you don't have it. But Netscape is particularly nasty about coexisting with its earlier versions. It can be done but it is anything but seamless . . . and if you surf late at night one false click will destroy your preferences or your carefully acquired bookmarks. So for now, I'll skip the Java.

See you later, I'm going down for another Diet Coke.

Leonard Grossman in an attorney who works for the government. He is a WindoWatch regular and has been contributing "Reflections" for some time.
Comments can be sent to grossman@mcs.com or leonard.grossman@syslink.mcs.com
To visit his home page go to http://www.mcs.net/~grossman

What? No Hebrew Edition of Windows95

Copyright 1996 by *Stan Kanner*



No surprise that computers continue to be popular here in Jerusalem. I recently made the rounds with a friend to help him buy one. It is interesting to compare prices and styles to the American market. I have been In Israel since September and seven months can be a very long time using computer marketing standards. I admit to not knowing the current hot computer config-uration in the States. I can tell you however, what the systems are like here in Israel.

The base system that computer stores want to sell is the following. A Pentium 75mhz, 8 megs of ram, and an 850 meg hard drive with a VGA monitor. Sounded fair enough to me. The initial price looked pretty reasonable too at $1300 (given in dollars, so it sounds like less I think). But, that

price is a bit deceptive. In Israel, most of the taxes are collected in the form of a sales tax called VAT (value added tax). The tax is a whopping 17%. Adding the cost of a modem and then the tax the price can very quickly jump up to $1,700 and then some, - in dollars.

The sales pitch for the Pentium is based completely upon what you might need in the future. This is a point of view that I have never personally bought. My philosophy is that technology increases so quickly that whatever you buy will be obsolete too soon. I always try to base my purchases on what I expect to realistically use, along with the toys I might want to play with. As a result Window's 95 and Pentiums have never really interested me. Perhaps one day when there is a real shift in technology and I can have a star trek type computer. When I can simply say *Computer, - I want to do this,* then I will be happy to upgrade.

Until then my word processor and spread sheet programs happily move along on a 486 processor. Since I use my computer mainly for the Internet, deciding whether a 486 or a 586 is better at sitting and waiting for the data to come in, is an easy choice. The 486 can wait for data a lot more cheaply. But, I digress.

Presently in Israel, people cannot use Windows 95. There is no Hebrew version. So, the hardware is being geared up for software that does not yet exist in this market. My friend needed a connection to the Internet primarily for email. He needed an English/Hebrew word processor, available for Windows 3.1, and probably will run some other household programs at some point. So, in keeping with my philosophy we found a used 486, 8 meg of ram, computer for about 1,000 (VAT included). The cost difference can be used for buying toys for the computer like a color inkjet printer, multimedia, and a video

capture board. These are all nice add -ons which can be purchased for less than the difference in price.

I'm sure he will enjoy it as much as I enjoy my low end but formerly high end 486 computer.

I did upgrade my computer recently by buying Snappy, a video capture tool that allows you to do all kinds of neat photo doctoring. Some of the *artistic* work I have done by doctoring images would surely get me into big trouble with at least three of the worlds major religions. When you live in Jerusalem there are just too many tempting things you can super-impose upon each other.

Stan Kanner is spending the year in Israel. He is the creator of Compuhigh an accredited online high school. He is a regular WindoWatch contributor!

ww

Internet Gems: The Editor's Picks

They may not hear but you can certainly say what you think to your Congresssional delegation! If the Congress ever listens it has to be in an election year! So speak your mind to Congress On the Net
The House Members: http://www.house.gov
The Senate: http://www.senate.gov
The President: http://www.whitehouse.gov

Learn HTML online. ***Helping Newbies Become Knowbies !***
The owners call it CyberCourse. A $5 shareware registration fee. Check out the curriculum at
http://www.newbie.net/CyberCourse/00index.html

Humanities Online from Michigan State Universities! A marvelous source of information from demography to zen. It's called H-Net!
http://h-net.msu.edu

Are you a Desk Potato? Do you have *the* ten characteristics? Visit The Desk Potato Home Page to find out.
http://trance.helix.net/~lekei/deskpota.html

On this very select list, the last is never least. Need a CGI script? A no-cost source for a variety of routines for the budding Webmaster. Matt Wright has a very useful site. Visit him at
http://worldwidemart.com/scripts

ww

Editorial Note:

A couple of our regular writers are absent this time.

Herb Chong is busy building and configuring a huge system for very sophisticated programming projects.

Ben Schorr is physically moving his company and residence to another location. The computer with his copy for this month's LastWord is buried amid boxes and plastic popcorn.

Gregg Hommel was tied up with the Canadian federal tax deadline of April 30th fullfilling his annual committment to the many seniors he assists.

Sadly, we have lost Phil Leonard to a new business. He will be missed and has an open invitation to return whenever possible.

lbl

ww