

September Meetings:

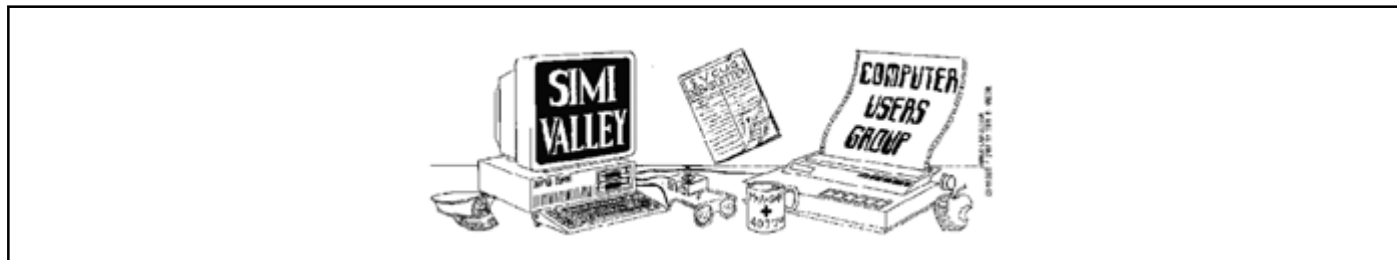
Thursday, 9/9/99: Windows 2000 by Microsoft Corp.

Wednesday, 9/22/99: Tracker - Gary Saxer of Enfish

Simi Valley Computer User Group:

BBS Numbers: 805-526-6196 or 805-522-9127

website: www.svcug.org or email: svcug@wgn.net



Volume XV, Issue XIX

"The "All Types of Computers" Club

September, 1999

9/9/99 - OFFICE 2000 PRESENTATION BY MICROSOFT CORP

Power Users' Top 10 Office 2000 Features and Enhancements

From the Microsoft Office 2000 Preview Tour Around the country, network administrators, Webmasters, and information technology (IT) professionals are getting their first peek at Microsoft® Office 2000, so we asked these computer enthusiasts to comment on their favorite new features and enhancements. They're finding out how Office 2000 connects the traditional desktop tools —Microsoft Word, Microsoft Excel, PowerPoint®, Outlook®, and Microsoft Access — to the World Wide Web, and they're previewing two applications that have joined the team: the Microsoft FrontPage® 2000 Web site creation and management tool and new PhotoDraw™ 2000 business graphics software.

The Crowd Pleasers

1. Saving files directly to the Web Preview Tour attendees were impressed with the ease by which they can move between Microsoft Office application files and the Web. All Office applications now allow automatic save in hypertext markup language (HTML) format, which simplifies publishing Office documents to an intranet or Internet site.

2. Threaded discussions Network users saw immediate uses for threaded discussions that allow workgroup members to collaborate on projects across intranets and the Web. You can insert a threaded discussion in any part of a document that can be viewed by coworkers in the original application or in a Web browser.

continued on page 2

ENFISH TRACKER PRESENTATION BY GARY SAXER - 9/22/99

Never worry about naming, filing, or manually organizing anything ever again. Saves you time by putting the exact information you need at your fingertips... in seconds.

Enfish Tracker works like an intelligent assistant, organizing and filing everything on your computer, helping you find exactly what you need, when you need it.

Automatically groups your related emails, files and Web pages by project, people, companies, topics... whatever is important to you. Quickly finds specific phrases and subjects in hundreds (even thousands) of documents and files. It even searches the Web. Lets you view the contents of your emails, files and Web pages instantly, without launching any other program. Works "virtually" so it's totally safe! your actual files are never touched!

Adds network drive integration

Offers enhanced Internet features

Provides Act!, Goldmine and Outlook PIM support

Track and view over 100 applications, including all major word processing, email, spreadsheet and graphics programs. Even track information on removable media!

Enfish Tracker's patented technology combines the power of four existing software types, giving you the finding capabilities of a search engine, the organization of a filing system, the navigation of a browser, and the sorting ability of a database program!

continued on page 2

Bring a whole group up to speed on a project with the background discussion that's already taken place. With Office 2000, you can insert a threaded discussion into any part of a document.

3. Collect and paste The Office 2000 Clipboard lets you copy up to 12 different pieces of text or graphics from any Office application and paste any or all of them into any other application.

4. WYSIWYG font management The drop-down font management window—available in all Office applications—shows a line of text in each available font, and was mentioned as a new favorite almost as often as the Clipboard feature. You can quickly preview what your documents will look like before applying the fonts.

5. Floating tables Improvements in the ability to format Word tables were well received. Now users can place and move a table anywhere within a document, wrap text around it, and use diagonal lines inside table cells.

No more time-intensive formatting problems. Now you can move a Word table, and automatically wrap the text around it.

6. Save for Use In Wizard Another feature that audiences liked is the option in the new PhotoDraw application that allows users to save a file automatically for different uses, without worrying about the file format. For example, you can save designs that are customized for the Web — and preview what the design will look like before you import it into your Web program — so that you have control over image-quality vs. download time.

7. Language Pack proofing tool Users in bilingual areas, such as the U.S. Southwest, were excited to discover that Office 2000 can detect the language that they're typing and automatically use proofing tools (such as Spelling and Grammar checker and AutoCorrect) in the correct language.

8. PowerPoint Tri-Pane view Presentation builders loved this one: The slide, outline, and notes views are combined into a single, framed screen — no more time-consuming switching back and forth between views.

Save time switching views: slide, outline, and notes views are combined into a single, framed screen in Microsoft PowerPoint.

9. FrontPage Explorer and Editor in a single view Webmasters were happy to discover that the views in FrontPage have been brought together (similar to the same improvement in PowerPoint) for easier use and management.

10. The Office 2000 doctor is always in Everyday PC users and administrators alike were impressed with the self-repairing installation that simplifies information system support. For example, if someone inadvertently deletes essential files from a hard disk and tries to run an Office application that requires the files, Office 2000 automatically finds the files from the network — or prompts you for the CD — and quickly reinstalls them, then launches the application as requested. A window shows progress as the file quickly loads.

The computer professionals interviewed for this article were Cara Cawfield, Board Member, Houston Area League of PC Users; John Kamper, Computer Training and Education Consultant; and Les Stein, Program Director, Tucson Computer Society.

Enfish Tracker and Enfish Tracker Pro are loaded with useful features!

Cover Notes - These electronic "sticky" notes can be added to any email, file or Web page for instant cross-referencing to other information. Great for tracking graphics files!

Highlighted Words - Clicking on any highlighted word link pulls up the information associated with it. Cross-referencing becomes easy and intuitive.

Adding and excluding items - Adjust your Results List manually, so you see exactly the information you want to work with, regardless of how you found it.

Categorize your Trackers - Group related Trackers together for easy reference.

Web site tracking - Incorporate any Web site into your tracked information, schedule when to update specific sites, and even specify how many levels of pages you wish to track.

Speaker Info

Gary Saxer can be seen at Trade Shows and Press Events. Many people remember him from his days at Quarterdeck Corporation. In his 14 years there he was a programmer, a marketing specialist, Vice President of Technical Services, and Vice President of Product Promotion. He is well known for his spirited presentations, especially at major industry trade shows, user groups, and seminars. Considered an expert in Memory Management, he has published a book, "Total Recall: The Ultimate Guide to Memory Management." Mr. Saxer holds a BS in Computer Science from California State University, Northridge.

MICROSOFT, THE NSA, AND YOU

Here is the press release; for the full details, look [here](#).

A sample program which replaces the NSA's key is here, at the bottom of the page.

Microsoft Installs US Spy Agency with Windows

Research Triangle Park, NC - 31 August 1999 - Between Hotmail hacks and browser bugs, Microsoft has a dismal track record in computer security.

Most of us accept these minor security flaws and go on with life. But how is an IT manager to feel when they learn that in every copy of Windows sold, Microsoft may have installed a 'back door' for the National Security Agency (NSA - the USA's spy agency) making it orders of magnitude easier for the US government to access their computers?

While investigating the security subsystems of WindowsNT4, Cryptonym's Chief Scientist Andrew Fernandes discovered exactly that - a back door for the NSA in every copy of Win95/98/NT4 and Windows2000. Building on the work of Nicko van Someren (NCipher), and Adi Shamir (the 'S' in 'RSA'), Andrew was investigating Microsoft's "CryptoAPI" architecture for security flaws. Since the CryptoAPI is the fundamental building block of cryptographic security in Windows, any flaw in it would open Windows to electronic attack. Normally, Windows components are stripped of identifying information. If the computer is calculating "number_of_hours = 24 * number_of_days", the only thing a human can understand is that the computer is multiplying "a = 24 * b". Without the symbols "number_of_hours" and "number_of_days", we may have no idea what 'a' and 'b' stand for, or even that they calculate units of time.

In the CryptoAPI system, it was well known that Windows used special numbers called "cryptographic public keys" to verify the integrity of a CryptoAPI component before using that component's services. In other words, programmers already knew that windows performed the calculation "component_validity = crypto_verify (23479 237498234 ...,crypto_component)", but no-one knew exactly what the cryptographic key "23479237498234..." meant semantically.

Then came Windows NT4's Service Pack 5. In this service release of software from Microsoft, the company crucially forgot to remove the symbolic information identifying the security components. It turns out that there are really two keys used by Windows; the first belongs to Microsoft, and it allows them to securely load CryptoAPI services; the second belongs to the NSA. That means that the NSA can also securely load CryptoAPI services... on your machine, and without your authorization.

The result is that it is tremendously easier for the NSA to load unauthorized security services on all copies of Microsoft Windows, and once these security services are loaded, they can effectively compromise your entire operating system. For non-American IT managers relying on WinNT to operate highly secure data centers, this find is worrying. The US government is currently making it as difficult as possible for "strong" crypto to be used outside of the US; that they have also installed a cryptographic back-door in the world's most abundant operating system should send a strong message to foreign IT managers.

There is good news among the bad, however. It turns out that there is a flaw in the way the "crypto_verify" function is implemented. Because of the way the crypto verification occurs, users can easily eliminate or replace the NSA key from the operating system without modifying any of Microsoft's original components. Since the NSA key is easily replaced, it means that non-US companies are free to install "strong" crypto services into Windows, without Microsoft's or the NSA's approval. Thus the NSA has effectively removed export control of "strong" crypto from Windows. A demonstration program that replaces the NSA key can be found on Cryptonym's website.

Cryptonym: Bringing you the Next Generation of Internet Security, using cryptography, risk management, and public key infrastructure.

Interview Contact:

Andrew Fernandes

Telephone: +1 919 469 4714

email: andrew@cryptonym.com

Fax: +1 919 469 8708

Cryptonym Corporation
1695 Lincolnshire Boulevard
Mississauga, Ontario
Canada L5E 2T2

<http://www.cryptonym.com>

###

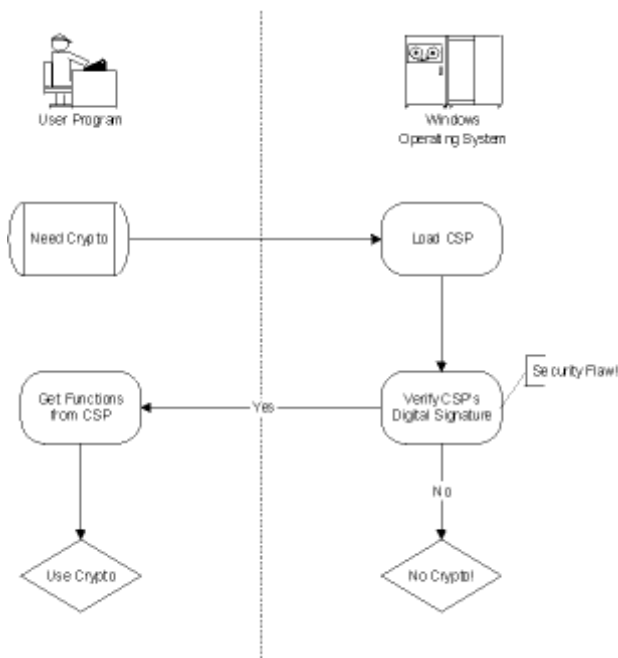
NSA's cryptographic "back door" into MS Windows (all versions):

The Full Details These details are essentially the contents of the "Rump Session" talk that Andrew Fernandes gave at the Crypto'99 Conference, on 15 August 1999, in Santa Barbara, California.

Note 1: many people have written us and assumed that we "reverse engineered" Microsoft's code. This is not true; we did not reverse engineer Microsoft code at any time. In fact, the debugging symbols were found using standard Microsoft-purchased programmer's tools, completely by accident, when debugging one of our own programs.

Note 2: many reporters have stated that Andrew studied computer science at the University of Waterloo and was a classmate of Ian Goldberg of Zero Knowledge Systems. In fact, Andrew studied biochemistry and mathematics at Waterloo for his undergraduate, and mathematics at McGill for his graduate work. He and Ian graduated in the same year, but really did not know each other at the time.

An Overview of the Microsoft's CryptoAPI Microsoft's CryptoAPI allows independent software vendors (ISVs) to dynamically load Cryptographic Service Providers (CSPs) as in the following diagram:



This arrangement of having Windows verify the CSP signature is what allows Microsoft to add cryptographic functionality to Windows. They will not digitally sign a CSP unless you first agree to abide by US export rules. Translation: Microsoft will not allow non-US companies to add strong crypto functions to Windows.

Fortunately, the verification of the CSP's digital signature opens up a security flaw in this picture.

Observations Using NT4 Server, SP5 (domestic, 128-bit encryption version), and Visual C++ 6, SP3. These same results have been found in Win95osr2, Win98, Win98gold, WinNT4 (all versions), and Win2000 (up to and including build 2072, RC1).

Many people have emailed us to say that these debugging symbols are actually present in NT4-Workstation, and are in the original CD's debugging symbols! Thanks, people!

Before CSP loading

in ADVAPI32.DLL

Address 0x77DF5530 -> A9 F1 CB 3F DB 97 F5

Address 0x77DF55D0 -> 90 C6 5F 68 6B 9B D4

After RC4 encryption using we see

A2 17 9C 98 CA => R S A 1 ... 00 01 00 01 ... (looks like an RSA public key)

A0 15 9E 9A CB => R S A 1 ... 00 01 00 01 ... (looks like an RSA public key)

Looking at SP5 debugging symbols

in "_CProvVerifyImage@8"

Address 0x77DF5530 <- has data tag "_KEY"

Address 0x77DF55D0 <- has data tag "_NSAKEY"

Screenshots One, Two, Three, Four, and Five showing the actual debugging information.

The Flaw

An attack: Replace "_KEY" with your own key...

...but Windows will stop working since it cannot verify it's own security subsystem!

An better attack: Replace "_NSAKEY" with your own key... .. Windows keeps working, since Microsoft's key is still there - stops the NSA - works because Windows tries to verify the CSP first using "_KEY", and then silently fails over to "_NSAKEY"

The Result:

Windows CryptoAPI system still functional
 the NSA is kicked out - the user can load an arbitrary CSP,
 not just one that Microsoft or the NSA signed!

Implications

1. What is the purpose of "_NSAKEY"? Espionage? Or do they simply not want to rely on Microsoft when installing their own CSPs?
2. Using RSA's Data Security's (now Security Dynamics) "BSafe" toolkit actually makes analysis of a program easier.
3. We do not need to modify the "advapi32.dll" file in order to remove the NSA key, nor do we need special privileges on the machine.
 - a. use self-modifying code
 - b. needs undocumented vxd calls under Win95 and Win98
 - c. needs special memory features under WinNT and Win2k
4. It is easy for any process to bypass any CSP and substitute its own.
5. Export controll is effectively dead for Windows.
6. Note for Win2k - there appear to be three keys in Win2k; Microsoft's, the NSA's, and an unknown third party's.

Thanks to Nicko van Someren for bringing this to our attention.

Removing the NSA

A sample program which replaces the NSA key with a test key, and leaves the rest of the CryptoAPI system intact, can be downloaded by clicking this link (currently only for WinNT and Win2k). For legal reasons, source code will be provided for free, but only be available through a Nondisclosure Agreement with Cryptonym. These files are provided for demonstration purposes only, and may not be redistributed or used for any purpose other than demonstration without the written authorization and license of Cryptonym Corporation. For more information, please contact:

Andrew Fernandes email: andrew@cryptonym.com
Phone +1 919 469 4714 Fax +1 919 469 8708

Win95/98 Programmers: we could use help in porting the software to Win95/98. If you have a strong background in Win95/98 virtual memory management, virtual device writing, and Windows 'internals', and don't mind volunteering your time, please contact Andrew at the addresses above!

SIX INTERNET SEMINARS AT WARP EXPO WEST

These six free Internet seminars have been carefully scheduled so none are at the same time. If your interest, your job or your business revolves around the Internet, you'll get the knowledge you need at Warp Expo West.

Web Server Performance and Scalability

Presented by Robert Chapman, Institute of Advanced Development Strategies and SCOUG Member.

Mr. Chapman will lecture on intranet and internet response times, file I/O bottlenecks, communication bottlenecks, operating system constraints, platform issues and the use of programs, Active Server Pages and Dynamic HTML and the effect they have on performance, and the new Application Server architectures and their current and future ramifications. Be prepared with your own questions about your current or planned Internet servers, because Mr. Chapman will take questions from the floor.

Quick Start for Netscape Composer

Presented by Virginia R. Hetrick, Ph.D., Senior Consultant for CIBER Custom Solutions Group and SCOUG Member.

Dr. Hetrick will demonstrate how to design award-winning web pages using the Composer portion of Netscape Communicator, including all of its tools and capabilities, the tricks that add "the look" to your pages, how to properly organize your page information for maximum impact, color selection, designing for the multiple resolutions that visitors may use, layout styles, and headlining. Bring printouts of your favorite web pages and learn how their look and impact can be further improved.

Technology Overview: Why XML Is Important

Presented by Bill Schindler, Editor In Chief of Extended Attributes, the award-winning OS/2 magazine published by POSSI. Mr. Schindler will present the reasons that XML is important to web businesses, web designers and web users, the history of web languages, the relationship between XML and the alternatives, the purpose of XML in web page design, and the business and casual considerations that must be analyzed when deciding on its usage. All persons who manage or design web pages should attend this seminar.

Managing Your Website

Presented by Virginia R. Hetrick, Ph.D., Senior Consultant for CIBER Custom Solutions Group and SCOUG Member.

Dr. Hetrick's background in managing web sites for UCLA and other organizations has led to a successful overall strategy for designing and running any web site, from avoiding the "web wall" to planning your expansion, handling traffic, tracking usage, what to look for when analyzing server logs, reorganizing the web site, budgeting the resources, and handling each of the certain problems as they occur. Web site administrators and future administrators need the training and insights included in this lecture.

Internet Communication Methods

Presented by Dave Watson, SCOUG Member and Internet SIG Leader.

Mr. Watson will cover the full complement of Internet communication methods, from traditional asynchronous protocols to live interactive sessions, email, mail lists, newsgroups, Internet relay chat, instant messaging, CUSeeMe, sending to many individuals simultaneously, the programs which supply these functionalities, the current OS/2 resources, the importance these capabilities will have in our everyday lives as bandwidth and processing power increase, and a changed future as connectivity becomes truly universal. Most web users have heard of these capabilities but are unaware of many of the business and personal uses, and this presentation will give all attendees the major new insights into how these technologies are just beginning to affect our lives and our pocketbooks.

An Introduction to XML Basics

Presented by Bill Schindler, Editor In Chief of Extended Attributes, the award-winning OS/2 magazine published by POSSI. Mr. Schindler will present a somewhat technical introduction to XML (eXtensible Markup Language), including how XML is different from HTML, how to create a well-formed XML document, parsing and validating an XML document, creating your own "tags", using DTDs, vector graphics, data transformations, fast XML design, and design considerations. XML is the new future language of the web and those who control web sites need this information to stay ahead of the competition.

You'll learn a lot about the Internet when you attend Warp Expo West!

Warp Expo West is free. The show will be held on September 18 near Disneyland in sunny Southern California.

All the info is at www.scoug.com/warpexpowest

Sponsored by The Southern California OS/2 User Group.

SOCIAL SECURITY DATABASE POST-EMS.

Now you can attach a message to any of the more than 61 million records in the Social Security Death Index (SSDI) at RootsWeb by using a "post-em," developed by RootsWeb's own Randy Winch. Some suggested uses: attach notes to the records of your relatives, providing researchers with a direct link to you; add background information on an individual in the database, such as pointers to other records relating to that individual; or add a correction to an incorrect record. Check the records of individuals of interest to you often. Someone recently might have left a note there for you. To add a note to a record, do a search and click on "Post-em" at the end of a record at: <http://ssdi.genealogy.rootsweb.com/cgi-bin/ssdi.cgi>

CA-CVGS-CIG Mailing List

The CVGS~CIG meets at 7:00 PM on the first Tuesday of every month in the main meeting room at the Grant R. Brimhall Library 1401 E. Janss Road, Thousand Oaks, CA

LOCAL COMPUTER CLUBS NEED HELP?

Appleholics Anonymous 2nd Sat 9:30 am

3169 Telegraph Road, Ventura

Chuck Baca 805-650-7503 Tony Pizza 805-482-3453

Conejo Valley Genealogical Society 1st Tues

Herb Berger, 805-497-7307 herbberger@aol.com

CVMUG sherrera@vcnet.com

Westminster Presbyterian Church, Camarillo

General Meeting: 1st Thursday, 7 pm

Novice SIG: 4th Monday Internet SIG: Quarterly

Susie Herrera 805-484-2259

Commodore 64/128 Users

General Meetings: 1st Sat., 10 am @ Cal Fed Bank

430 Arneill Road, Camarillo

Tech Meeting: 2nd Sat, 10 am @ Boys-Girls Club

126 E. 7th Street, Oxnard

BBS: 805-382-1125 Loyd Couch: 805-483-9200

Channel Islands PC Group

General Meeting: 1st Sat, 9 am @ Camarillo Airport

OS/2 Corner: 2nd Sat, 9:30 am

www.cipcug.org Toby Scott, 805-981-1212

Gold Coast CUE of Ventura County

Days vary, 4 pm Camarillo area or local school

Tim Rainville, 805-525-3873 rainvilt@vcss.k12.ca.us

Leisure Village Club

1st Friday, 10am Camarillo 1st Monday, MAC group

2nd Friday, Communications 3rd Wednesday, Novice

Neil Iven, 805-383-0016 iniven1@juno.com

Simi Conejo Linux User Group

Meets every other Saturday at 6 pm at Nortel, 4100 Guard-

ian Street, Simi Valley www.psilord.com/sclug

MacValleyUsers Group

1st Wednesday Wilkinson Senior Center

8956 Vanalden Street (one light east of Tampa,

just south of Nordhoff), Northridge

Daphne Gruberman (818) 998-7025

Simi Valley Computer User Group

Main meeting: 2nd Thurs 7:30 pm

Hardware/Software Meeting: 4th Wed, 7:30 pm

at Simi Valley Library - SVCUG web: www.svcug.org

Barbara Cott 805-581-2495 bobbie@wgn.net

Thousand Oaks Personal Computer Club

4th Thurs: 6:30pm Jan-Oct 3rd Thurs: 6:30 Nov-Dec

Goebbel Sr Ctr or T.O. Library

Harry Isaman 805-405-8323 www.vcnet.com/topcc

TUGNET meets every Tues, 7pm Granada Pavilion

11128 Balboa.Granada Hills. www.tugnet.org

Ventura Beginners PC Users' Group

3rd Sat, 10 am Club House, Bena Ventura

Mobile Home Estate 11407 Darling Road

Howard Wilson 805-647-0360

Ventura Windows Publisher User Group

3rd Tuesdays, 7 pm Cal Fed Bank Bldg

430 Arneill Road, Camarillo

Bob Tracy 482-7092 bobtracy@vcnet.com

Dennis Atherton

hardware - any, networking , WIN95 setups

dennis_atherton@yahoo.com 7-11 evenings

Steve Carter

OS/2 - scarter@vcnet.com 805-598-8455 til 9 pm

Barbara Cott desktop publishing, word processing,

Internet, Excel, Photoshop, web pages bobbie@wgn.net

805-581-2495 any time

Howard Engel

Word 6, programming in PASCAL or ADA

engelh@gte.net 805-523-7602 9 am - 10 pm

Will Fiske

Win95/3.11/3.1, DOS 6.2 and down to 5

wfiske@juno.com after 6 pm

Roger Freeman

online researching

update1@ez2.net 805-579-8426 before 10

Spencer Hartman Digital Research DOS 6, Novell

DOS 7.0 WordPerfect 6.1 for DOS, batch files

805-522-7212 if no answer, lv msg 10 am - 10 pm

Gordon Huff modems, Telix, FDISK

ghuff@vcnet.com 805-499-3494

Lucy Lediaev Basic Windows & Office, Basic

HTML & graphics concepts

lucyl@cnmnetwork.com evenings 6-9:30 pm & wknds

David Ringwood

hardware - jolyon@mail.westworld.com

Oliver Stockton

MS Word , Wndows 95, Beginners

SimiClown@aol.com 805-581-2991 24 hours / 7 days

Robert Sully

Hardware Questions, OS's (Win95 and OS/2)

BASIC Programming, Beginning Visual Basic

rsully@earthlink.net

Dee Tillman

Office 97 Word & Excel, WordPerfect, Commodore,

Apple II dtillman@juno.com 805-526-1395, after 4 pm

Gaylord Trubey

DOS internet, WIN 3.x, WIN 95, software hardware

gaylordt@juno.com 805-526-2077

Dick Uhlman

XTree (1-3), Windows, DOS Excel

computerwizard@juno.com

805-583-2174 & 805-583-2804 5pm - 8pm

Karleen Volz

BASIC questions, DOS WIN 3.11, WIN 95 WIN NT,

basic hardware questions

kvolz@juno.com 7pm - 9:30pm & weekends

Simi Valley Computer User Group Officers

President	Barbara Cott	805-581-2495	bobbie@wgn.net
Vice President	Gaylord Trubey	805-526-2077	gaylordt@juno.com
Secretary	Gerry Scott	818-341-7107	gerry@wgn.net
Treasurer	Howard Engel	805-523-7602	engelh@gte.net
M.C.	Dennis Atherton	805-581-2495	dennis_atherton@yahoo.com
SYSOP	Lee Barton	805-527-0181	leeb@rain.org
Warp Zone BBS	1st line 805-526-6196 2nd line, 805-522-1927 (member line)		

NEWSLETTER ADVERTISING

Small member ads (business card size) are free.

1/4 pg - \$25/mo 1/2 pg - \$50/month full pg - \$100/month

Send camera ready art to Editor by mail /e-mail or call 805-581-2495.

Should be in ASCII. Deadline is near the end of the month.



www.wgn.net

Ask for User Group Rate

Simi Valley Computer User Group

2718 Kadota Street
Simi Valley, CA 93063

September Meetings

Thursday, September 9th
Presentation: Windows 2000
by Microsoft Corporation

Wednesday, September 22nd
Presentation: Tracker
by Gary Saxer of
Enfish Technologies