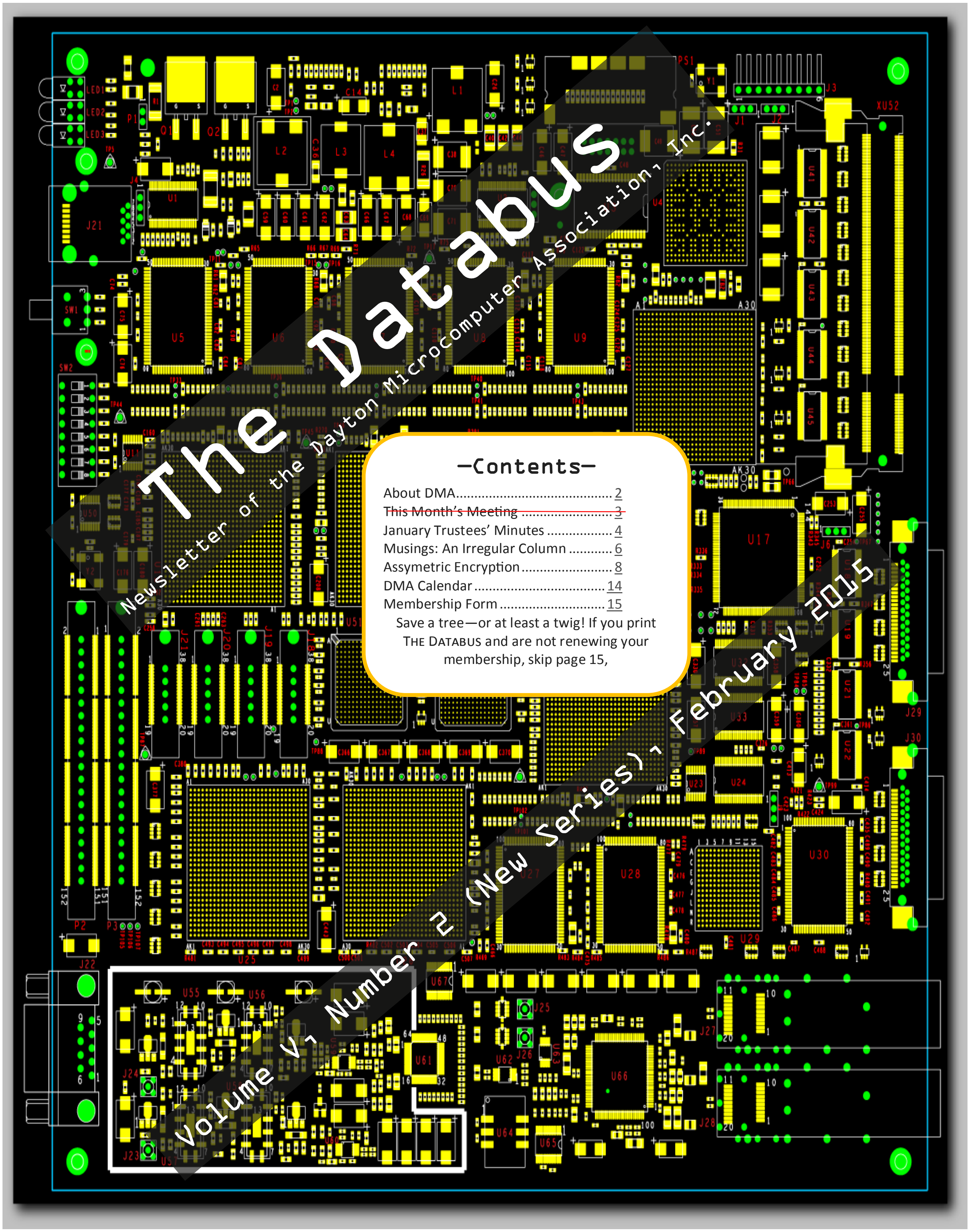


The Databus

Newsletter of the Dayton Microcomputer Association, Inc.

Volume V, Number 2 (New Series), February 2015

—Contents—

Save a tree—or at least a twig! If you print THE DATABUS and are not renewing your membership, skip page 15,

DMA

Post Office Box 4005
Dayton, Ohio 45401
Telephone:
(937) 222–4DMA
(937) 222-4362

Visit us at:

DMA1.org

Established in 1976, DMA is a group of Dayton–area professionals and hobbyists in the field of computing and information technology. General membership meetings are usually on the last Tuesday of each month. DMA has a number of Special Interest Groups (SIGs) in areas ranging from digital photography and genealogy to the Linux operating system. Each SIG meets according to its own schedule. DMA is a member of Association of Personal Computer Users' Groups (APCUG) and the Affiliated Societies Council (ASC). Click on any of the logos — including our own — to go to that organization's Web site.

Submissions …

The Databus welcomes compliments, complaints, suggestions, and especially articles. We can accept articles in ASCII, or as attachments in Microsoft Word or Works, Open Office Writer, Word Perfect, or, yes, even WordStar (a word–processing program that goes all the way back to the 1980s!). No PDF files, please. Send e–mails to:

Editor@DMA1.org

All articles are subject to editing for spelling, grammar, usage, and space. Always retain a copy of your work, as The Databus cannot be responsible for loss. When articles are of roughly equal quality, those by paid–up DMA members usually receive preference.

All registered trademarks, for example: DMA or Radio Shack, are the property of their respective owners. However, for better readability, the Registered Trade Mark symbols (® or TM) have been omitted. The Editor occasionally inserts comments into articles. Such comments are always in square brackets [like these] and are preceded by the phrase: "Editor's Note."

The Databus is written and published by volunteers. We do not give professional advice on computer, network, or software installation, troubleshooting, or repair. If you need professional advice or other expert assistance, please seek the services of a competent professional.

By Jove, Harrington ! We appear to have lost our way to the Regional Center.
You fool—this is the Regional Center! The February meeting has been canceled !

Bing Images

The February DMA meeting has been canceled because of the weather!

MINUTES are usually published almost *two months late.* This is because the Minutes for, say, the January Board meeting must be approved by the Trustees at the following month's meeting—in this case, early February. The corrected and approved January Minutes will thus appear in this (February) issue of THE DATABUS, which comes out just before the General Membership Meeting at the end of the month.

DMA Board of Trustees' Meeting of Monday, January 5, 2015

CALL TO ORDER

The meeting was called to order at 7:02 P.M. by Gary Coy. **Trustees present**: Martin Arbagi, Glady Campion, Gary Coy, Debra McFall, Eric Ottoson, Wynn Rollert, Jim Ullom, Gary Turner, Ken Phelps and Ed Skuya.

OFFICERS' REPORTS

President-Gary Coy

We had a good turnout at the Christmas Party with about sixty people in attendance. The concept of the $5 ticket was popular and we sold fourteen extra tickets.

Vice President-Eric Ottoson

We are in the process of getting the insulation in our storage locker repaired.

Secretary-Debra McFall

Debra presented the Minutes for the December Board meeting as corrected. Jim Ullom moved the Minutes be accepted. Eric Ottoson seconded and the motion passed.

Treasurer-Glady Campion

Glady presented a revenue and expense report for January 1-December 31, 2014. Our Fifth Third Checking Account has a balance of $20,911.80. Our Fifth Third Savings Account has a balance of $11,218.14. Our Dayton Foundation Account has a balance of $76,693.07. This gives us a total of $109,226.11.

COMMITTEE REPORTS

Audit-Glady Campion

The spreadsheet clean-up is nearly complete.

Bylaws Review-Eric Ottoson

We will have a rough draft by the end of the week.

Funding-Open

No report.

Membership-Dave Lundy, Glady Campion

No report.

(Continued on page 5)

Net Administration Team-Ken Phelps, Gary Turner

We are coordinating with Google to switch our mail to dma1.org.

Programs-Jim Ullom

We are planning a program on internet security for January and a program on fiberoptics for February.

Publications-Martin Arbagi

The December DATABUS will go on the DMA website with photos from the Christmas Party.

OLD BUSINESS

Holiday Dinner-Glady Campion

No report.

Storage Locker Clean-Up Committee-Debra McFall, Glady Campion

We are still trying to contact Dan Forshaw about items in the Apple cabinet. Old office supplies will be brought to the January meeting to sell. Jim Ullom may know someone who will do our shredding free. Monco Industries is also being considered for shredding.

Board Meetings-Glady Campion

The next Board Meeting will be held on Monday, February 2, 2015 at 7pm. If you would like to eat dinner, please come at 6 pm. The location will be announced.

WSU Archives-Martin Arbagi, Glady Campion

Martin and Glady are in the process of having THE DATABUS archived at WSU.

VOLUNTEER OF THE MONTH/QUARTER/YEAR

No report.

ADJOURNMENT

Jim Ullom moved to adjourn at 7:56 P.M. Eric Ottoson seconded and the motion passed.

Respectfully Submitted,

Debra McFall, Secretary

Trustees' meetings are open to all DMA members—think about attending once in a while.

In Memoriam

MILDRED HAND BIAWITZ, wife of longtime DMA member
STEVE BIAWITZ

Musings: An Irregular Column

By Steven M. Schoemann, Dayton Microcomputer Organization, Inc.
Steve (at) Gemair.com
DMA1.org

February 2015

It is with sad heart that I view the massive downsizing of Radio Shack. As I had previously predicted, the company had to file for reorganization under the current bankruptcy regulations. From its insignificant origins in the amateur radio world, Tandy's Radio Shack became one of the microcomputer world's retail behemoths in the 1980s and early 1990s. Its line of TRS 80 computers helped lead the way to the world of microcomputers that we have today. I can't speak for others, but it was always a comfort to me, knowing that there was a Radio Shack on a nearby corner, where I could go and purchase a device that I needed for some electronic project that I was working on. In today's world of pre-made, off-the-shelf computer gadgets, I have little use for my old friend, the soldering iron.

The ability to take computer classes at a local Radio Shack led many a mainstream youth and adult (young and old) to take one small step at a time into the new age, to a world previously limited to the collegiate, corporate computer scientist, the geeky nerd, and the science fiction aficionado. In some ways, I miss those past days and, in some ways, I don't. Life is a mixed bag of reminisces located in a modern setting. Still, it was a comfort to have Radio Shack there, holding your hand, and answering many of what we would call today, naïve questions.

It was Radio Shack's misfortune that it could not hang on to the main stream and its grip on the frivolities of public fashion. Even though it tried, the company could not keep up with the fast changing world and current technologies as its market share slowly declined over the years. Goodbye, old friend, and good luck in your new and reduced guise.

It is a shame that the banks and other financial institutions continue to flaunt their lack of security when it comes to their and our cash holdings. As I have mentioned in other articles, it seems that they do not even attempt to maintain up-to-date security. According to today's news, banks around the world have lost over a billion dollars to cyber thieves attacking their ATMs. Evidently, this world wide theft has been going on for a couple of years and even though they are aware of this ongoing theft, it still continues with no end in sight. Don't these financial institutions do accounting and have audits? According to the evening news, much of this could have been prevented if the institutions would have taken the simple step of running updates and security patches on their software, as well as running

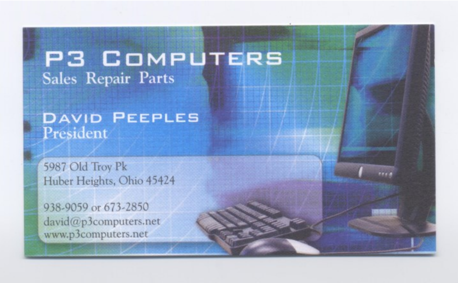
(Continued on page 7)

(Continued from page 6)

anti-malware software. Most of us who use computers and have access to the Internet routinely do updates, and run a variety of scans on our computer systems. It should be a routine thing for businesses that have access to highly trained computer technicians to do this sort of maintenance on a very regular basis. Who is guilty of this negligence: The banking hierarchy or the banks' IT departments? TDB

Have a business card? Are you a DMA member?

ANY PAID–UP MEMBER of the Dayton Microcomputer Association is entitled to a *free* business card–sized advertisement in THE DATABUS. Give your card to Editor **Martin Arbagi** to be scanned, or send a good–quality image to Editor@DMA1.org A link to your Web site (if you have one) can be embedded in the image of your card. Under weird IRS regulations, your site may not include discount coupons, although discount offers may be included in the advertisement itself. See the examples just below, both of which include discounts to DMA members.



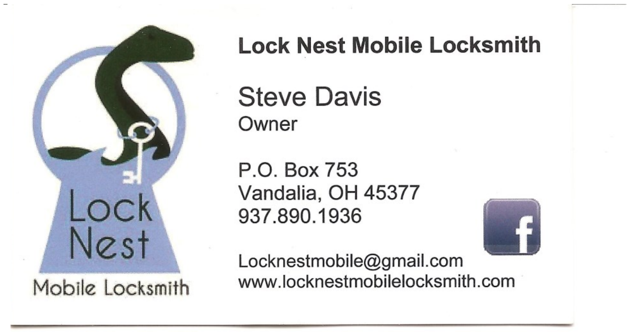
P3 COMPUTERS
Sales Repair Parts

DAVID PEEPLES
President

5987 Old Troy Pk
Huber Heights, Ohio 45424

938-9059 or 673-2850
david@p3computers.net
www.p3computers.net

5% Discount to DMA members!
(Special orders excluded.)



Lock Nest Mobile Locksmith

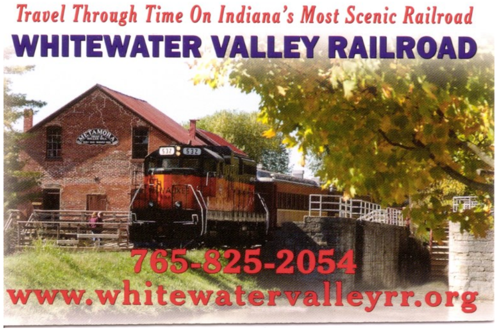
Steve Davis
Owner

P.O. Box 753
Vandalia, OH 45377
937.890.1936

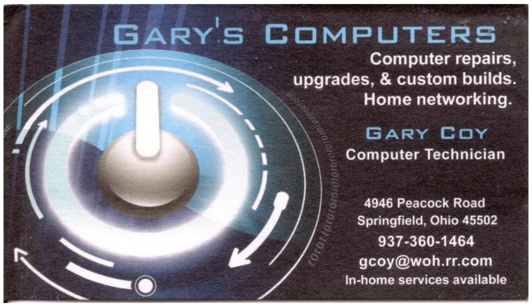
Locknestmobile@gmail.com
www.locknestmobilelocksmith.com

Lock
Nest
Mobile Locksmith

10% Discount to DMA members!



Travel Through Time On Indiana's Most Scenic Railroad
WHITEWATER VALLEY RAILROAD
765-825-2054
www.whitewatervalleyrr.org



GARY'S COMPUTERS
Computer repairs,
upgrades, & custom builds.
Home networking.

GARY COY
Computer Technician

4946 Peacock Road
Springfield, Ohio 45502
937-360-1464
gcoy@woh.rr.com
In-home services available

—Asymmetric Encryption—

By Dick MAYBACH, Member, Brookdale Computer Users' Group, NJ
July 2014 issue, *BUG Bytes*
www.bcug.com
n2nd (at) att.net

ASYMMETRIC OR PUBLIC-KEY ENCRYPTION uses a pair of keys, a private one that you keep secure and a public one that you publish. A file encrypted with one of the key pair can be decrypted only by using the other. It is difficult (that is, it would require many years of computer time) to find the private key even if you know the public one. This technique is used to exchange information securely with others using an insecure communication system, such as the Internet. Anyone who has your public key can encrypt a message with it that only you can decrypt, since only you have the corresponding private key. Conversely, if you encrypt a message using your private key, anyone who successfully decrypts it using your public key knows that it must have come from you. Commonly, this latter technique is used to send a digital signature. For example, you would send someone a message encrypted with his or her public key and include a signature encrypted with your private key.

Clearly, the tricky part of this method is to be sure that a public key really belongs to the person you think it does. This is especially important if you obtain a key from a Website. Most encryption techniques used by private individuals conform to the OpenPGP standard (http://www.openpgp.org/), which has been subjected to many rigorous audits by experts in security. This standard includes features to help you verify that a public key belongs to the person you think it does.

A complication of this method is that you must keep track of many keys, made up of long sequences of random characters: your own private key, your own public key, and the public keys of everyone to whom you wish to send encrypted files. These are stored in a file, called a "keyring," which you encrypt with a pass-phrase and keep on your computer. Because you must remember the pass-phrase, it's not as secure as the message keys, but a keyring is not exposed to as many threats as messages sent over public media.

The standard open-source asymmetric encryption program is GNU Privacy Guard (GnuPG), http://www.gnupg.org/. Although GnuPG is a Linux program, there are related ones for OS X (https://gpgtools.org/) and Windows (http://www.gpg4win.org/). I'll use the Windows variant as an example of how to use this type of encryption, but this won't be a detailed user's manual as one is available on the developer's Website.

Gpg4win includes the following programs:

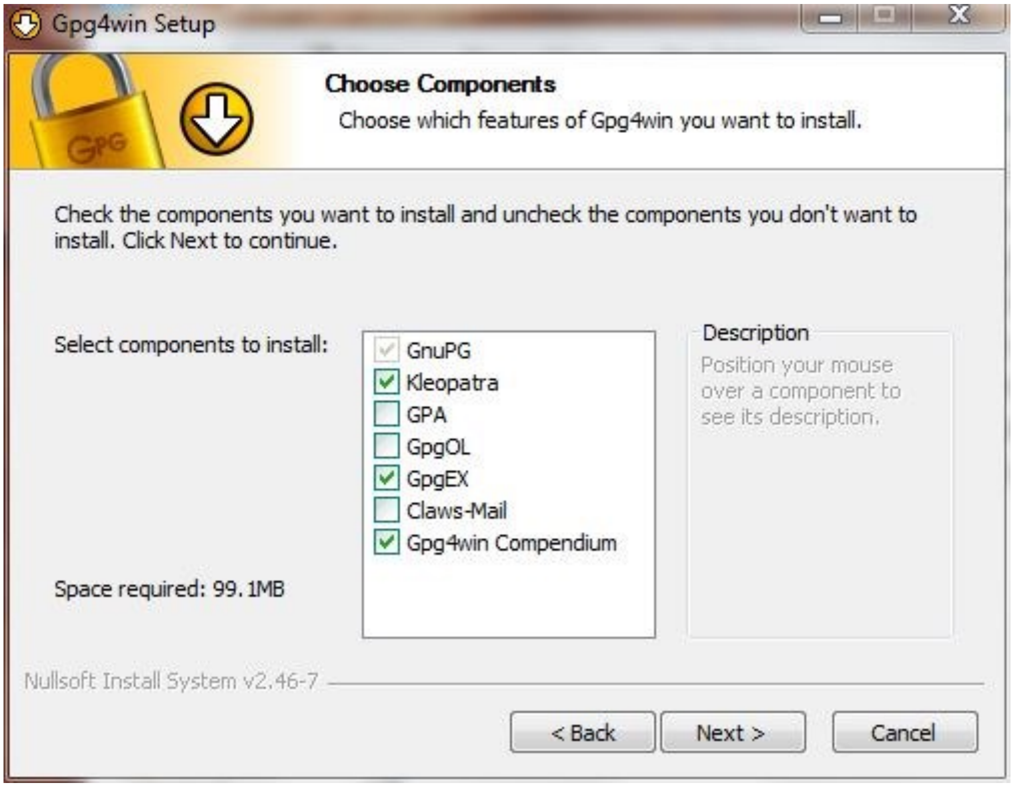
- GnuPG - GnuPG forms the heart of Gpg4win—the actual encryption software.

(Continued on page 9)

- Kleopatra - The central certificate administrator of Gpg4win, which ensures uniform user navigation for all cryptographic operations.
- GNU Privacy Assistant (GPA) - is an alternative program to Kleopatra that manages certificates.
- GnuPG for Outlook (GpgOL) - is an extension for Microsoft Outlook 2003 and 2007, which is used to sign and encrypt messages.
- GPG Explorer eXtension (GpgEX) - is an extension for Windows Explorer which can be used to sign and encrypt files using the context menu.
- Claws Mail - is a full e-mail program that offers very good support for GnuPG.

You download only those components that you need.

Thus, Gpg4win provides a complete suite of cryptography tools to manage keys, encrypt e-mail, and encrypt individual files on your PC. Installation is quite easy: just download the installation file and run it. You will soon see a Window that lets you select the components to install.



Choose Components

Choose which features of Gpg4win you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ GnuPG
☑ Kleopatra
□ GPA
□ GpgOL
☑ GpgEX
□ Claws-Mail
☑ Gpg4win Compendium

Description

Position your mouse over a component to see its description.

Space required: 99.1MB

Nullsoft Install System v2.46-7

The core program is GnuPG, which you must install. You will also need Kleopatra (to manage keys), GpgEX (an extension to Windows Explorer that aids in encrypting and decrypting files), and Gpg4win Compendium (documentation). GPA is an alternative program to Kleopatra, and you need only one of the two. GpgOL is an extension to Outlook; download it only if you have MS Outlook (not Outlook Express). Claws is an e-mail client, but unfortunately the current version has a bug that prevents it from working with encryption. After you complete the installation, you should read over the Compendium, located in C:\Program Files\Gpg4win; I find the HTML version the easiest to navigate. Most users will need only the components checked in the screen-shot.

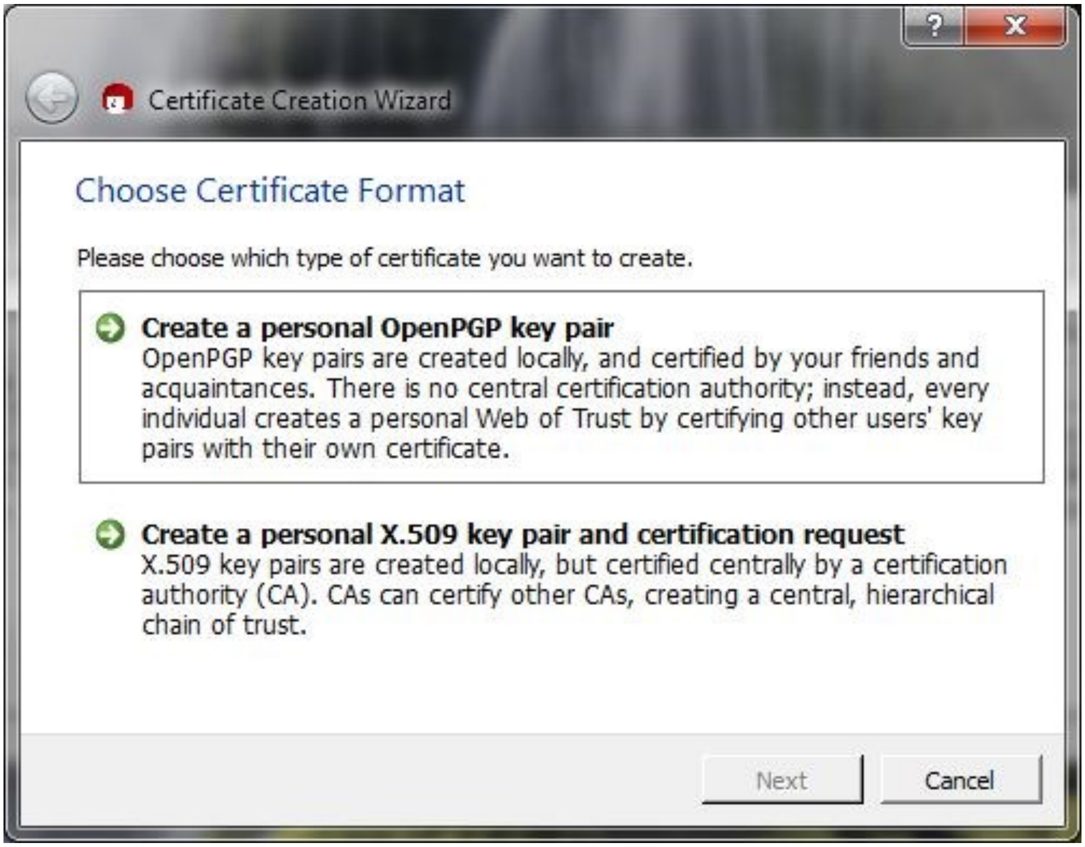
(Continued on page 10)

Using public-key encryption requires that you have a different key for each person with whom you communicate, plus at least two for yourself. You will first create a keyring and generate your own public and private key, after which you can add the public keys of those to whom you wish to send messages. Start Kleopatra, click on **Files,** then on **New Certificate** to open the Certificate Creation Wizard. You will want a personal OpenPGP key pair; you'll keep the private key and send the public one to others who wish to send you encrypted e-mail. You could use the second option shown in the screen-shot to publish your public key, but this also publishes your e-mail address and would probably increase the spam you receive.

Keys are identified by your name and e-mail address, so you next would enter these. For this article, I generated two keys, one for each of my major e-mail accounts. Both are temporary, so I set them to expire after just a week.

Right-click on a key and select **Properties** to learn more about it. In the screen-shot, note the fingerprint. This lets you quickly verify that a key you own really belongs the person it claims. For example, You could call that person and ask: "What are the last five characters in the fingerprint?" In this case, the correct answer is 38E90. The fingerprint is a checksum, and if any five characters are correct, the odds you have an invalid key are infinitesimal.

(Continued on page 11)



Certificate Creation Wizard

Choose Certificate Format

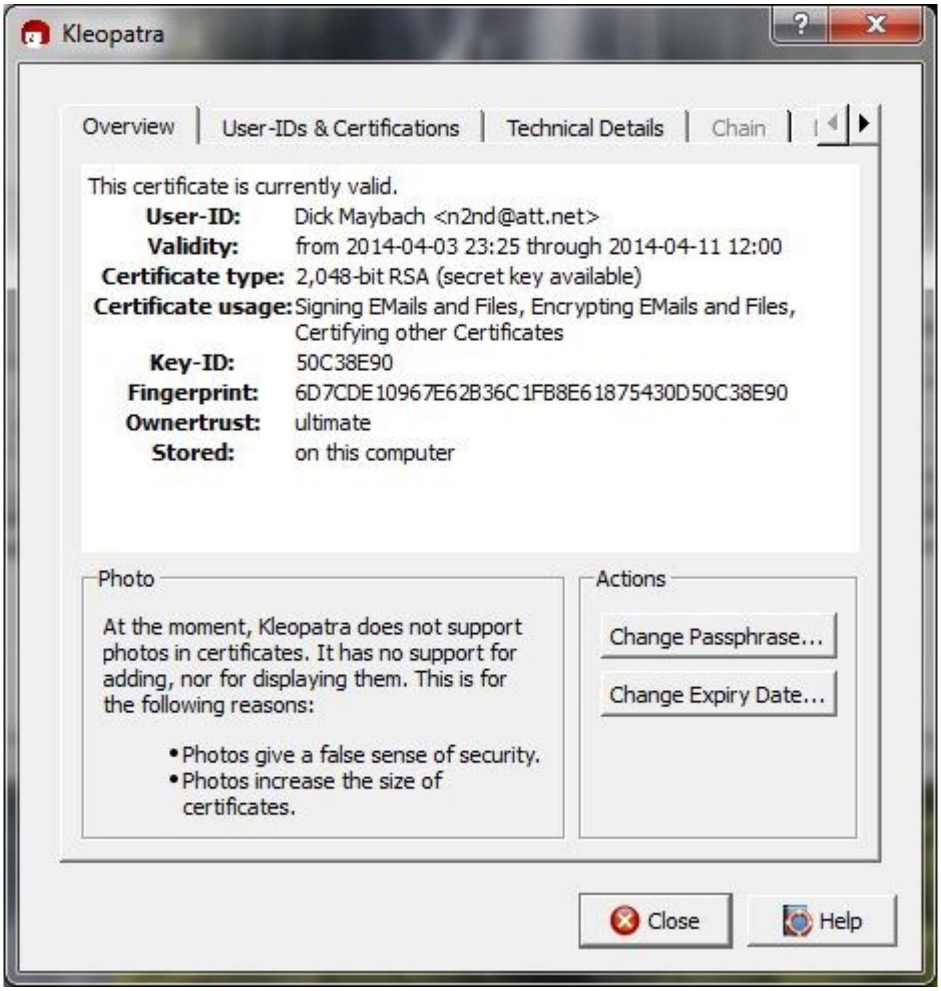
Please choose which type of certificate you want to create.

Create a personal OpenPGP key pair
OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every individual creates a personal Web of Trust by certifying other users' key pairs with their own certificate.

Create a personal X.509 key pair and certification request
X.509 key pairs are created locally, but certified centrally by a certification authority (CA). CAs can certify other CAs, creating a central, hierarchical chain of trust.

The procedure to add someone's public key is similar. Put the file containing his certificate somewhere on your PC, in Kleopatra click on **File,** then on **Import certificate,** and follow the instructions.

Select a file for encryption with Windows Explorer (assuming you have installed GpgEX) by right-clicking on the file and selecting **Sign** and encrypt. See the compendium for other options. You then select the key, which will always be a public key, your own if the encrypted file stays on your computer or someone else's if you will e-mail it to him. You can select as many keys as you like, which makes it convenient to send encrypted files to several people. It's a good idea to include your own key to files you send to others, since if a file is encrypted only with someone else's public key, you can't decrypt it. In many cases, you will have to enter your pass-phrase to access the keys on your keyring.



This certificate is currently valid.

User-ID: Dick Maybach <n2nd@att.net>
Validity: from 2014-04-03 23:25 through 2014-04-11 12:00
Certificate type: 2,048-bit RSA (secret key available)
Certificate usage: Signing EMails and Files, Encrypting EMails and Files, Certifying other Certificates
Key-ID: 50C38E90
Fingerprint: 6D7CDE10967E62B36C1FB8E61875430D50C38E90
Ownertrust: ultimate
Stored: on this computer

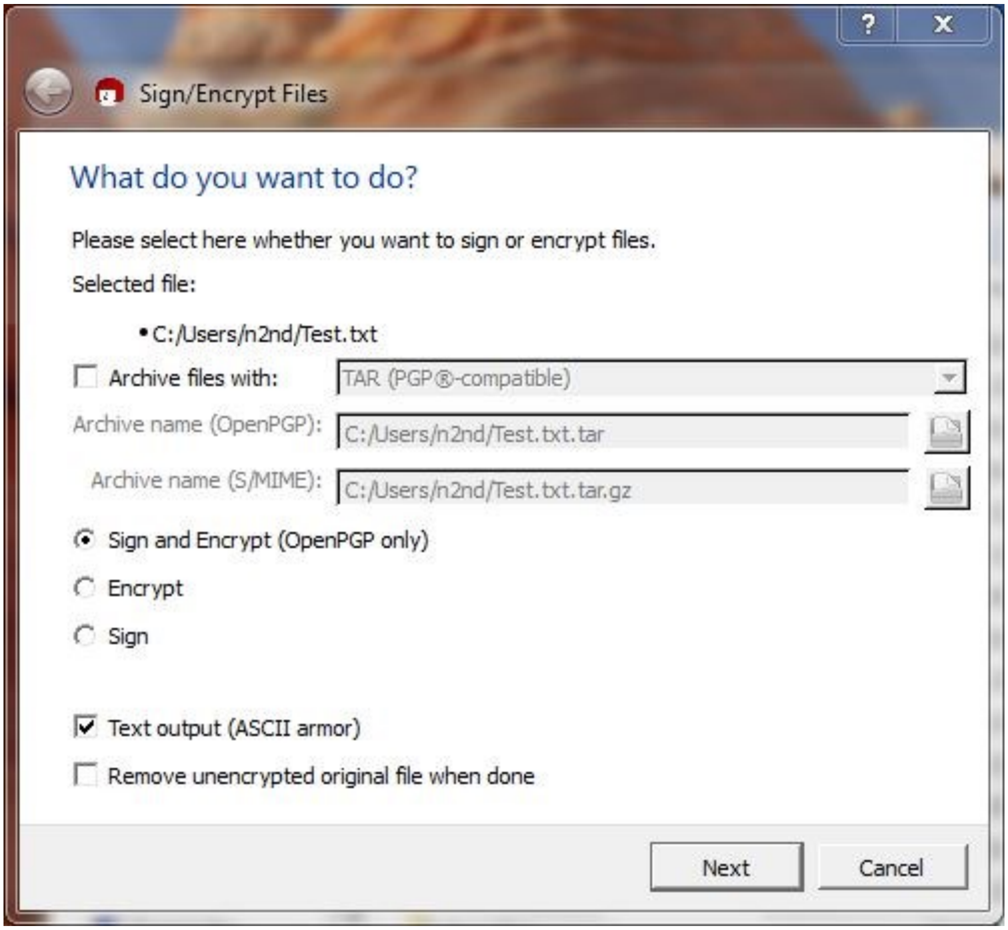
At the moment, Kleopatra does not support photos in certificates. It has no support for adding, nor for displaying them. This is for the following reasons:

- Photos give a false sense of security.
- Photos increase the size of certificates.

As the next screen-shot *(see page 12)* shows, you have a second chance to decide whether you want both to sign and encrypt the file, and you also can decide whether the encrypted file will consist of binary or ASCII digits. Use the former for files that stay on your computer and the latter for e-mail.

(Continued on page 12)

The last (January) issue of THE DATABUS carried photographs of our 2014 Holiday Dinner. These pictures should have been credited to staff photographer **Bruce Murphy**. We apologize for the omission.


Sign/Encrypt Files

What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- C:/Users/n2nd/Test.txt

□ Archive files with: TAR (PGP®-compatible)

Archive name (OpenPGP): C:/Users/n2nd/Test.txt.tar

Archive name (S/MIME): C:/Users/n2nd/Test.txt.tar.gz

● Sign and Encrypt (OpenPGP only)

○ Encrypt

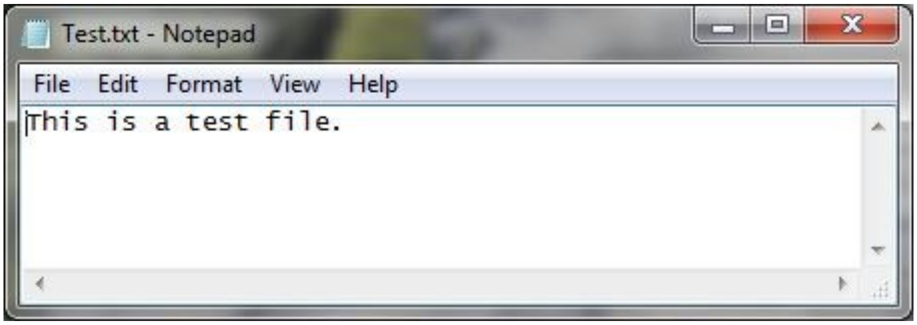
○ Sign

☑ Text output (ASCII armor)

□ Remove unencrypted original file when done

The next two screen-shots show the contents of a test file and its ASCII-coded encrypted counterpart. *(Second screen-shot is on page 13.)*

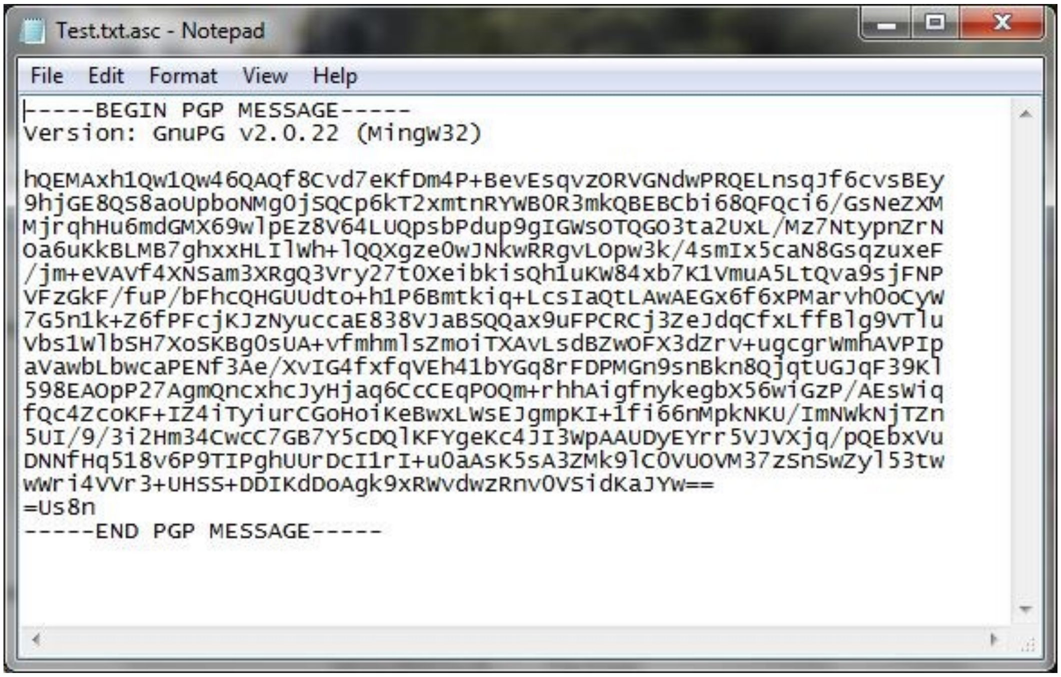
ASCII-coded files have *.asc* appended to their names, while binary-coded ones have *.pgp*. The encrypted version is larger, because it has preambles, each containing the key to decrypt the body of the file, in turn encrypted with the recipient's public key, and probably the sender's signature, encrypted with his private key. If there are several recipients, there will be several preambles.


Test.txt - Notepad

```
This is a test file.
```

To decrypt a file, use the same procedure as when encrypting it, but select **Decrypt** and verify after you right-click on the file name.

(Continued on page 13)



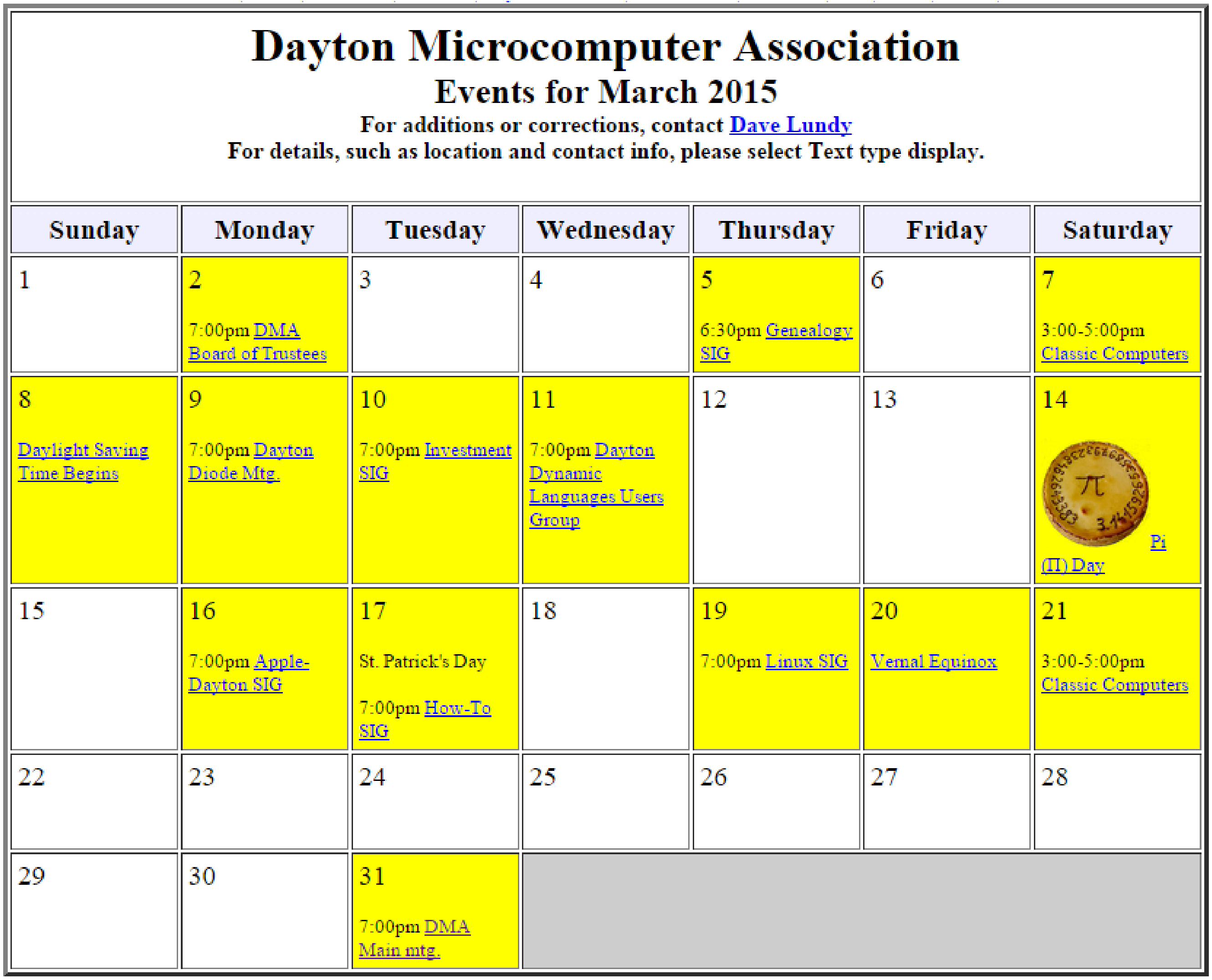
```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.22 (MingW32)

hQEMAxh1Qw1Qw46QAQf8Cvd7eKfDm4P+BevEsqvzORVGNdwPRQELnsqJf6cvsBEy
9hjGE8QS8aoUpboNMg0jSQCp6kT2xmtnRYWBOR3mkQBEBCbi68QFQci6/GsNeZXM
MjrqhHu6mdGMX69wlpEz8V64LUQpsbPdup9gIGWsOTQGO3ta2UxL/Mz7NtypnZrN
Oa6uKkBLMB7ghxxHLIlWh+lQQXgze0wJNkwRRgvLOpw3k/4smIx5caN8GsqzuxeF
/jm+eVAVf4XNSam3XRgQ3Vry27t0XeibkisQh1uKW84xb7K1VmuA5LtQva9sjFNP
VFzGkF/fuP/bFhcQHGUUdto+h1P6Bmtkiq+LcsIaQtLAWAEGx6f6xPMarvhOoCyW
7G5n1k+Z6fPFcjKJzNyuccaE838VJaBSQQax9uFPCRCj3ZeJdqCfxLffBlg9VTlu
Vbs1WlbSH7XoSKBg0sUA+vfmhmlsZmoiTXAvLsdBZwOFX3dZrv+ugcgrWmhAVPIp
aVawbLbwcaPENf3Ae/XvIG4fxfqVEh41bYGq8rFDPMGn9snBkn8QjqtUGJqF39Kl
598EAOpP27AgmQncxhcJyHjaq6CcCEqPOQm+rhhAigfnykegbX56wiGzP/AEsWiq
fQc4ZcoKF+IZ4iTyiurCGoHoiKeBwxLWsEJgmpKI+1fi66nMpkNKU/ImNWkNjTZn
5UI/9/3i2Hm34CwcC7GB7Y5cDQlKFYgeKc4JI3WpAAUDyEYrr5VJVXjq/pQEbxVu
DNNfHq518v6P9TIPghUUrDcI1rI+u0aAsK5sA3ZMk9lC0VUOVM37zSnSwZyl53tw
wWri4VVr3+UHSS+DDIKdDoAgk9xRWvdwzRnv0VSidKaJYw==
=Us8n
-----END PGP MESSAGE-----
```

The easiest way to send encrypted e-mail is to create a file on your PC, encrypt it with both your and the recipient's public key, sign it with your private key, and use text output. Then open the file and transfer its contents to the e-mail message using copy-and-paste (Ctl-C, Ctl-V). This works with any e-mail client program and also with e-mail accounts you access with your Web browser. The recipient opens the e-mail and an editor, transfers the information in the same way, and decrypts the resulting file as usual. You could also send the encrypted file as an attachment, but dealing with attachments is inconvenient with some Web-based e-mail services.

The process is easier if you have an e-mail client program that can encrypt and decrypt directly, as this avoids the copy-and-paste operation, but these are rare in the Windows world. Gpg4win does include Claws-mail, which has optional add-ons that are intended to provide this service. Unfortunately, the version available at this writing has a fatal bug. (The window that asks you for your pass-phrase never appears, and the program waits forever for you to enter it.) If you install the add-on, you will completely disable gpg4win, including the file operations we've been discussing here. I was able to regain these functions only after I went back to a Windows restore point and uninstalled then reinstalled gpg4win. Hopefully, this problem will be corrected soon. In the meantime, the copy-and-paste operations are not that inconvenient.

Gpg4win and its Linux and Mac counterparts provide a secure, standard, and convenient method of encrypting individual files and e-mail. They deserve much wider use than they have. Perhaps as the headlines about privacy violations continue, more people will realize how foolish it is to ignore the security risks of digital storage and communications. TDB



Dayton Microcomputer Association

Events for March 2015

For additions or corrections, contact Dave Lundy
For details, such as location and contact info, please select Text type display.

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2 7:00pm DMA Board of Trustees	3	4	5 6:30pm Genealogy SIG	6	7 3:00-5:00pm Classic Computers
8 Daylight Saving Time Begins	9 7:00pm Dayton Diode Mtg.	10 7:00pm Investment SIG	11 7:00pm Dayton Dynamic Languages Users Group	12	13	14 Pi (Π) Day
15	16 7:00pm Apple-Dayton SIG	17 St. Patrick's Day 7:00pm How-To SIG	18	19 7:00pm Linux SIG	20 Vernal Equinox	21 3:00-5:00pm Classic Computers
22	23	24	25	26	27	28
29	30	31 7:00pm DMA Main mtg.				

Click anywhere on the DMA Calendar (above) to go to the original at DMA1.org.

DMA Membership Application/Renewal

PLEASE ALLOW UP TO THREE WEEKS FOR APPLICATION PROCESSING AND INTERNET SET–UP

Name: ____Birth date:_____/_____/_____
mo. day year

Associate Name: ____Birth date:_____/_____/_____
mo. day year

Address: ____

City: ____ State: ________ Zip: __________

Phone: (Home) (________) ___________-_____________ (Work) (________) _________–______________x___________

I wish to have my name and address published in the club roster: YES □ NO □

E–mail address: ____@____

Name of DMA member who recruited me: _______________________________________ (only new regular memberships)

Are you a current or recent DMA Member? Yes q No q Change of Address only? q Today's date: _____/_____/_____

If you are renewing, please give your Membership Number (from your membership card) _________________________

Type of Membership

Application is for: New Membership □ Membership Renewal □ Associate Membership* □

If applying for free student membership, please give school name and student ID number: Available only for students under 22 years old. (Student Members *cannot* vote in DMA elections.)

School Name: ____ Student ID#: ______________________________

* A family or associate membership is an additional membership for a member of your immediate family or someone else who is living in the member's household. If this is a family or associate membership, give name of regular member:

Dues/Fees (Dues and Fees are subject to change without prior notice):

Membership (one year — New or Renewal)	1.) □ $25.00
Family or Associate Membership (must live at same address as regular member)	2.) □ $12.50
Free Student Membership for students under 22 yrs of age. (Student Members *cannot* vote in DMA elections.)	3.) □ FREE
Please assign me a user ID for E–mail and Usenet news access one–time setup fee for new E–mail accounts.	4.) □ $10.00
Total — Lines 1 and 2 (+ 4 if checked)	5) $____________

□ Cash
□ Check

Check # _____

Make your check payable to Dayton Microcomputer Association, Inc. (DMA), and then send the check and application to:
PO Box 340402
Beavercreek, OH 45434–0402

DMA Use only: Membership # __________________
Exp. Date: __________/_________/______________
Processed by: ________________________________
REV: 25 November 2013

Click here to pay your dues using PayPal. Simplified Membership Form, too!