25 Years DACS

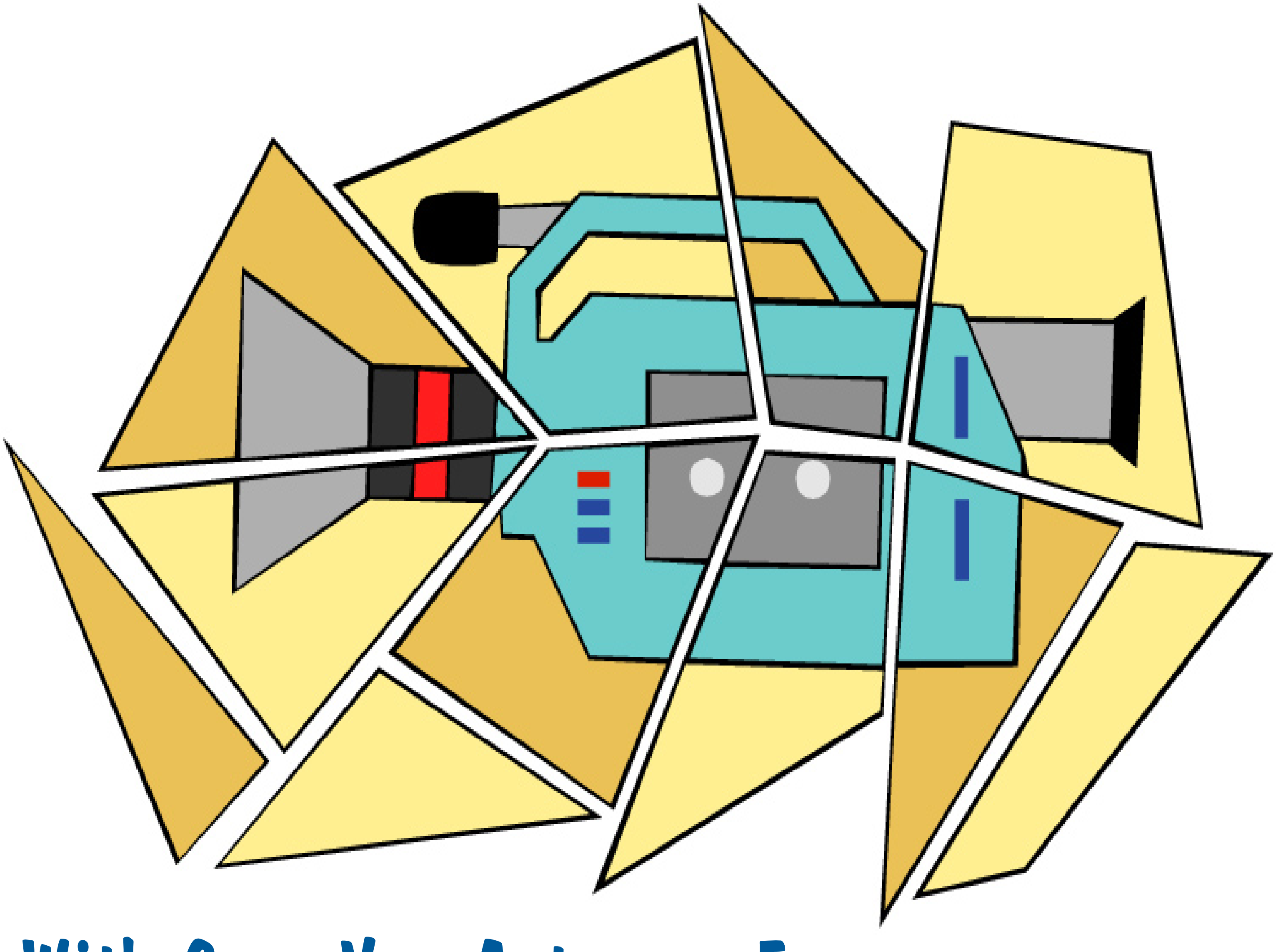
DACS.doc

A Computer & Technology Newsletter

June 2015 Volume 26, Issue 6 $2.00

Next Event: June 2, 7:30 PM

Video Production Basics For Home or the Superhighway



With Greg Van Antwerp, Franny Hannigan and Mark Ingram of Charter Community Access TV

President's File

THERE IS SO MUCH going on this month that it is difficult to know where to begin. So I would like to start by sharing with you some of the great things we accomplished last month. **Andy Woodruff** made a huge effort planning and setting up our general meeting, featuring John Patrick's excellent presentation, panel discussion, and book launch, for which the first 25 DACS members received John's new book, "Health Attitude". In addition to that, Andy supplied all the video recording equipment, speakers, and mixers. He recorded the video of the entire event (still editing), combining video from 3 camera angles to produce a very professional presentation for everyone who visits our website. **Tom Zarecki** also deserves a lot of credit for an excellent job, preparing and moderating the panel discussion, as well as **Lisa Leifels** and **Steve Harkness,** who helped set up and record video for the entire meeting.

The **video recording** of Tom's April presentation on Social Media should be available on Charter Cable community access channel 192 by the time you read this. Check Charter's link in the June meeting preview article on Video Production for the schedule. It may also soon **appear on Comcast and as a YouTube video**. I encourage everyone to attend the June meeting. You may (hopefully) want to get involved in video production of DACS meetings. It might be a nice creative sideline for you to enjoy and Charter will train you for free. With enough support from DACS members, I hope to produce recordings of our meetings as a regular occurrence.

IN THIS ISSUE

Tell us which **new presentations** you would like to see, or email us directly at *programs@dacs.org*. If you like what we are doing, **please help to spread the word about DACS**, our excellent presentations each month, our new video productions, and the growing list of workshops we run and co-sponsor with other groups throughout the month. **Use social media** to spread the word. Speaking of which …

The **new Social Media workshop series** will begin on Wednesday, May 27th at our Resource Center. The first workshop will be a hands-on boot camp to get you started using a few of the popular sites. Later workshops will explore more in depth how to use and benefit from each of the popular social media applications. I am looking forward to this!

DACS co-sponsored Workshops and Events – We have just finished an excellent series of three workshops which we co-sponsored with SCORE and Microsoft on using **Microsoft Office**. These workshops were well attended by DACS and I expect to see new DACS members as a result. There is a limit to how much can be covered in 3 sessions but there was a lot of interest in extending these into a series of DACS workshops. Stay tuned.

We are co-sponsoring another workshop, with the Danbury Library and SCORE, on Running a Restaurant. This is scheduled for Saturday, May 30th at the Danbury Library and described elsewhere on our website.

Excellent student presentation at WCSU – Lisa Leifels and I attended the last Marketing 315 class of the semester run by Professor Tom Zarecki. This class focused on Advertising and Social Media. Two teams of his students presented their class projects on how we might increase awareness of DACS and attract new members. Lisa and I were so impressed that I invited both teams to present their findings to the Board.

New interns coming to DACS – I have identified two areas where we can use some help – Marketing and IT Support. I must admit that I was so inspired by the capability and preparation of the student presentations that I was motivated to seek help from the University. Tom got me in touch with the Career Development Center at WestConn and I made my case for two student interns who will receive college credits. I will be reviewing resumes and will

Membership Information

dacs.doc, ISSN 1084-6573, is published monthly by the Danbury Area Computer Society, 65 Legion Rd, New Milford, CT 06776. Annual subscription rates: $60 to regular members, $40 electronic access (included in dues).

Postmaster

Send address changes to Danbury Area Computer Society, Inc., 4 Gregory Street, Danbury, CT 06810-4430.

Editorial Committee

Managing Editor:	Richard Teasdale
Production Editor:	Allan Ostergren

Contributors

Charles Bovaird
Drew Kwashnak
Dave Mawdsley
Bill Saturno
Annette van Ommeren
Richard Corzo
Lisa Leifels
Bruce Preston
Jim Scheef
Andy Woodruff

DACS, its officers and directors assume no liability for damages arising out of the publication or non-publication of any article, advertisement, or other item in this newsletter.

The editors welcome submissions from DACS members. Contact Richard Teasdale (*dacseditor*@dacs.org). Advertisers, contact Charles Bovaird at (203) 792-7881 *(aam@mags.net)*

Copyright

Bill Saturno APCUG Liaison
wsaturno@dacs.org

Officers

DACS GENERAL NUMBER: (203) 744-9198
PRESIDENT: Richard Gingras *dacsprez@dacs.org*
VICE PRESIDENT PROGRAMS: *vpprograms@dacs.org*
SECRETARY: Bert Goff • **TREASURER:** Bert Goff

Directors

dacsboard@dacs.org

Richard Corzo	(203) 797-1518	*rcorzo@dacs.org*
Richard Gingras	(203) 426-1780	*rgingras@dacs.org*
Bert Goff	(860) 355-8895	*bgoff@dacs.org*
Lisa Leifels	(203) 416-6642	*lleifels@dacs.org*
Jim Scheef	(860) 355-0034	*jscheef@dacs.org*
Bill Saturno	(203) 437-0611	*wsaturno@dacs.org*
Cathy Quaranta		*cquaranta@dacs.org*
Andy Woodruff	(203) 744-9588	*awoodruff@dacs.org*
Tom Zarecki		*ZareckiT@wcsu.edu*

Committees

NEWSLETTER: Richard Teasdale: *dacseditor@dacs.org*,
PROGRAM: *vpprograms@dacs.org*
WEB MASTERS: Richard Corzo (*rcorzo@dacs.org*), (203) 797-1518
Annette van Ommeren (*avanommeren@dacs.org)*, (914) 232-0149
PRESS RELEASES: Richard Teasdale (*pr@dacs.org*)
APCUG LIAISON: Bill Saturno (203) 437-0611
MARKETING: Cathy Quaranta *(cquaranta@dacs.org)*
MEMBERSHIP COORDINATOR: Charles Bovaird: *aam@mags.net*
RESOURCE CENTER: (203) 748-4330 • **WEB SITE:** *http://www.dacs.org*

HelpLine

Our former telephone HelpLine has been replaced by our web-based DACS Community Forum at *http://forum.dacs.org*. We have topic-specific forums where DACS members can post questions. Questions may be answered by Workshop leaders or other DACS members. If none of the categories fit your question, just post it to the Ask DACS forum.

Topic	Forum
.NET Programming	ASP.Net and C#VB.Net Workshop
Digital cameras/scanners/image processing	Digital Imaging Workshop
Content Management Systems	Drupal Workshop
Linux	Linux Workshop
Mac and iPhone/iPad/iPod touch	Apple Workshop
PC maintenance	PC Maintenance Workshop
Smartphones & Tablets	Mobile Devices Workshop
Virtual machine software	Virtual Computing Workshop
Desktop publishing and website design	Web Site Design Workshop
Windows	Windows Workshop

hopefully have the privilege of working with these students, starting in June.

25th anniversary – Let's make this year-long celebration a success. We want to create a much broader awareness of DACS as we participate in new activities, and create collectables of interest to DACS members and the general public. Talk about your ideas with Cathy Quaranta at the check-in table at our next general meeting, or let her know by email.

***From mobile to desktop, we inform, enlighten, and educate*.**

- Dick Gingras, President

Directors' Notes

Danbury Area Computer Society
DACS headquarters – 198 Main Street, Danbury, CT – Thursday, May 7, 2015

Board Meeting Minutes

Meeting called to order at 7:26 PM by president Dick Gingras.

In attendance: Bert, Lisa Liefels, Richard Corzo, Jim Sheef, Dick Gingras, Tom Zarecki, and special guest Rob Willard

Meeting topics:

1. Minutes approved from last meeting. Passed w/one abstention.
2. Membership report. See Bert's submitted worksheet.
3. Attendance report: 69 people were at last Tuesday's monthly meeting.
4. Treasurer's report, submitted separately by Bert.
5. $400 in donations total the night of the healthcare seminar last Tuesday.
6. Program Committee report (Lisa): no meeting last month. Next month's general meeting on Tuesday, June 2. The topic will be video production. Charter cable will be sponsoring an upcoming workshop, plus their own internship program.
7. Webcast virtual technology conference on Internet security.
8. Workshop discussion of which day of week is best…no decision reached.
9. Discussion of posting on DACS website, topic: "how to start a workshop"
10. Tom Z to get publicity to Richard Teasdale, get last year's as an example.
11. Two more 9AM to 10:30 AM Saturday workshops at Microsoft on May 9 and May 16. Attendance at last Saturday's workshop was 13.
12. Ongoing workshops still being debated.

Directors' Notes, *Cont. on page 11*

Meeting Review

John Patrick: Health Attitude

By Richard Corzo

THE MAY GENERAL MEETING was heavily publicized and well attended—it generated DACS's highest attendance in several years. It was designed to promote John Patrick's important new book, *Health Attitude: Unraveling and Solving the Complexities of Healthcare*. John received a doctorate in healthcare administration last year. One thing the book tries to explain is how the Internet and mobile devices are going to change healthcare in the United States.

John started the meeting with an overview of the health care system in this country. A big problem is cost. Factoring into this is fraud—payer systems that are being billed for procedures not performed. Doctors may order unnecessary tests and procedures, although sometimes this is due to the risk of being sued. Costs are twice as high in the U.S. compared to other developed countries, indicating inefficiency in our system. "Big Pharma," the nickname for the vast pharmaceutical industry and its lobbying group, charges prices in this country way beyond what they charge in other countries, and it's illegal to buy drugs from overseas.

John offered solutions in three areas, which are covered in more detail in his book. The first is that a change in attitude is required. Patients need to take more responsibility and ask questions about their medications and procedures that are ordered. Of course they have a role in developing healthful habits, to prevent problems from developing in the first place. Attitudes of physicians are already changing, but the system needs to change so that it compensates for wellness and not just sickness. Payers need to provide motivations for cost savings. Politicians' attitudes need to change as well, but John admitted he didn't have time to go into that area.

Technology is a key area that will help change the healthcare system. The Cray supercomputer developed in the 1970s filled a large room and cost $5,000,000, but smartphones today are 150 times more powerful. The motion coprocessor on recent iPhones can constantly monitor your steps, position, and posture, and the Health app in iOS 8 on your iPhone has 900 apps that feed information to it. Attachments to a smartphone camera can analyze a blood test strip for cholesterol. Electronic health records (EHRs) can be tied into the Health app and monitor, for example, heart irregularities, potentially alerting a physician. A CellScope is an iPhone otoscope that can take a picture and detect an infection in someone's ear. Another sensor attachment can provide a 30-second EKG. The Isabel differential diagnostic tool can ask a few questions about symptoms and come up with some probable diagnoses, prior to coming in for a doctor's visit. The new field of regenerative medicine is doing experiments where tissues can be 3D-printed from pluripotent stem cells and used to repair organs.

The last area is policy. Big data and analytics can look at population health. The accountable care organization (ACO) concept means payers pay based on population health, which breaks the old model.

After John's introductory talk, the meeting moved on to a panel discussion moderated by Tom Zarecki, adjunct professor in the Communication and Media Arts department at Western Connecticut State University. The panelists were:

- Dawn Myles, APRN, Vice President , Quality and Patient Safety at Western Connecticut Health Network
- Aparna Oltikar, MD, Chairman of the Department of Medicine for Danbury and New Milford Hospitals
- Cary Passik, MD, Chief of Cardiothoracic Surgery at The Praxair Regional Heart and Vascular Center at Danbury Hospital
- John Patrick, DHA, President, Attitude LLC

Left to right: Dawn Miles, Aparna Oltikar, Cary Passik, John Patrick, Tom Zarecki

Tom started off with a question, "How do you measure the quality of health care?"

Panelist answers were—

- The best possible outcome for a patient
- Did the patient get what they came for?
- Longitudinal tracking of quality, across time—not just the initial outcome
- The quality of life for both patient and family. (John mentioned Atul Gawande's book *Being Mortal: Medicine and What Matters in the End*.)

Dr. Oltikar explained her role as a hospitalist—a specialist who manages a patient's inpatient care.

The panelists mentioned communication between doctors as a problem, and John mentioned ways to automate communication, e.g. using a tool as simple as e-mail. However, until we move to an accountable care model, physicians are not compensated for their time spent reading e-mails or making Skype calls. Dr. Passik mentioned the distraction of typing in patient notes into an EHR during a patient visit. John asked why we couldn't capture voice recordings and have the system translate them so data is properly entered in the electronic health record. The discussion next veered into the problem of so many different systems being incompatible, sometimes requiring the entry of the same data multiple times.

John contrasted the health care systems in Europe with that in the United States. Doctors in Europe do not have to pay for the liability insurance that American doctors must have, and they don't have the huge medical school debts to pay off that American doctors do. Administrative costs are lower overseas, but not because they have a single payer system. Germany has 200 payers. Canada with thirteen provinces has thirteen payers.

Other topics brought up by the panelists ranged from minimally invasive procedures, telemedicine (robots examining a patient, controlled remotely by a physician), and physician training that involves practicing procedures on patient simulators as well as practicing communication with patients. Hospitals are experimenting with hospitalizing patients in their own homes. Touching on policy, John mentioned the United States is the only developed country that doesn't pay for health care for everyone. Dr. Passik mentioned that everyone wants access to health care, but no one wants to pay for it. Our taxes pay for police, fire, schools, and a military, so why not health services? Also what is the responsibility of people for their own health, with the health habits they choose?

The meeting concluded with a question and answer session with audience members who were either physicians or who shared their experience as patients. Some of the questions and topics were:

- Why is the U.S different from Europe?
- How patient care can transition from being focused on physician efficiency to being patient centered.
- Defensive medicine practiced to defend against possible lawsuits.
- The cost of drugs. It's a felony to buy drugs more cheaply overseas and resell them.
- Direct to consumer—We're the only country in the world that permits advertising drugs to consumers

The entire meeting was videotaped and it is expected to be broadcast on Charter cable systems, possibly Comcast, and made available online. Watch for future announcements on the DACS website.

Meeting Preview

Video Production Basics
For Home or the Superhighway

By Lisa Leifels

Date: Tuesday, June 2, 7:30 p.m.
Location: Danbury Hospital CreasyAuditorium
Presenters: Greg Van Antwerp, Franny Hannigan, Mark Ingram
Topic: Video Production

ARE YOU ONE OF the growing number of people spending more of your time online watching digital videos? Instead of just watching, would you like to learn how to create and share your own digital videos? This is the topic that will be covered on June 2nd, at the next DACS general meeting, by Greg Van Antwerp, Franny Hannigan and Mark Ingram, who all work at Charter Community Access TV.

The three-person panel will start off with a brief introduction to public-access television including the history of it and where it is today. They will go over the three different types of training that Charter CTV offers to the public at their studio, and they will also talk about what equipment is necessary for the training class.

Greg is the Charter CTV supervisor, and has been with the company since 1988. He is constantly learning more about multi-media presentations, marketing, and social media content distribution. Franny is the Community Access Coordinator for Charter and is in charge of the video production training department at CTV. Mark has been a coordinator with Charter since 1998 and specializes in equipment management and training. The majority of their presentation will be spent demonstrating how to create a video and how to upload it to YouTube and then share it, both on Facebook and Twitter.

This will be a great opportunity to learn more about Charter CTV's training course that will be starting soon - the good news is that it is free and no prior experience is necessary. This presentation is also free and open to DACS members and the general public, starting at 7:30 pm on Tuesday, June 2nd, in the Creasy Auditorium at the Danbury Hospital. There is plenty of free parking in the guest parking garage adjacent to the auditorium. After the meeting, everyone is invited to the Danbury Hospital Praxair Café for additional networking.

Franny Hannigan

Greg Van Antwerp

Mark Ingram

Workshops

Workshop NOTES: June 2015

Apple. Focuses on all aspects of the Mac and iPhone operating systems.

Contact: Richard Corzo (*macsig@dacs.org*).

Meets 2nd Tuesday, 7 p.m. at DACS Resource Center.

Next Meeting: June 9

Digital Imaging. All about digital cameras, retouching, and printing using various programs.

[Note: SIG is suspended until further notice

Drupal. Covers all things on Drupal, the open source content management system (CMS) .
Contact: Jim Scheef (*jscheef@dacs.org*).

Go to the DACS Community Forum - (*http://www.dacs.org/forum/*) within the Members only area.

Next meeting: Look for future announcements.

Jobs. Networking and jobs search

Contact: Charles Bovaird, 203-792-7881 (*aam@ mags.net*). Go to DACS Community Forum (*http://forum.dacs.org for job listings*.

Linux. Helps in installing and maintaining the Linux operating system. Also of interest to Apple owners using OS X.

Contact: Dave Mawdsley, linuxsig@dacs.org
Meets 3rd Wednesday, 7:30 p.m. at the DACS Resource Center.

Next Meeting: June 17

Mobile Devices/Windows 8. Smartphones, tablets, and e-readers of all makes and models.

Contact: Richard Corzo and Jim Scheef (*Mobilesig@dacs.org*)

Meets fourth Thursday 7 p.m. at the DACS Resource Center

Next Meeting: Workshop Suspended

PC Maintenance. Review of PC hardware and OpSys maintenance and use.

Contact: Charles Bovaird, 203-792-7881 (*aam@ mags.net*).
Go to DACS Community Forum (*http://forum.dacs.org*).

Single Board Computers Workshop. Explores various small cheap computers like Raspberry Pi, Arduino, Netduino, Beaglebone, and more. Meets on third Thursday at the DACS Resource Center.

Contact: Jim Scheef (*jscheef@dacs.org*), or go to the DACS Community Forum: *http://www.dacs.org/forum/,* within the Members-only area

Next Meeting: June 18

Social Media: Master the basics of Facebook, Twitter, LinkedIn, and Instagram.

Contact: Tom Zarecki 914-548-4948; email tomZshow@gmail.com.

Meets on the 4th Wednesday of the month at 6:30pm, usually at the DACS Resource Center, but check the monthly schedule.

Next Meeting: June 24

Web Design and DTP. Learn how to work with HTML, CSS, CMS Systems, WordPress, SEO and more.
Contact: Annette van Ommeren (*avo@annagraphics.com*).

Meets 3rd Tuesday, 7-9 p.m. at the DACS Resource Center.

Next Meeting: July 21

Workshops News & Events

Apple. We got a question from one of our Apple Workshop members, “Can you suggest a good way to record videos I play from the internet? Then later I can burn a DVD.” In the meeting we’ll do some online research to try to answer this question. We could look for an application, or a how-to on YouTube, or maybe even a Firefox or Safari plugin.

He had a similar question about recording audio and burning a CD. That should be an easier question to answer.
—Richard Corzo

Social Media (Preview). After last month’s social media talk, many DACS members said YES to an ongoing social media workshop where Mr. Z could work with everyone.

Well, here it is! In just 90 minutes, you’ll learn…

- THE TOP 4 FORMATS: Facebook, Twitter, LinkedIn & Instagram
- HOW TO TALK TO MILLIONS, no matter how few followers you have!
- HOW HASHTAGS say “hi” while HANDLES find followers/friends
- HOW TO GET MORE EYEBALLS than the original by re-writing posts quickly
- HOW TO AVOID “THE BIG TIME SUCK”; stop losing hours w/social media

Join Mr. Tom Zarecki, MBA, who will spend time answering YOUR questions. Just show up at DACS’ Resource Center in Danbury (address below).

LEARN FROM EXPERTS: Tom Z is a DACS board member, radio announcer, advertising expert and lifetime media pro who teaches radio, marketing and social media at Western CT State University. PLUS: Tom is bringing his best social media students, too, to help you get going or advancing to the next level.

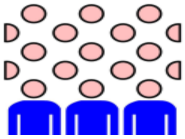
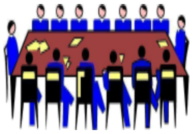
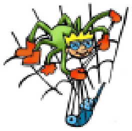
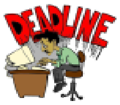
BRING YOUR OWN MOBILE DEVICE (smartphone, tablet, or laptop) so you can practice while you learn. The workshop is FREE.

Wednesday, May 27, 6:30 to 8PM. Don’t be late! Bring your own device (and plug) to the DACS Resource Center, 198 Main Street in Danbury.

Interested? Questions? Text Tom Z 914-548-4948; email *tomZshow@gmail.com*.

June 2015

Danbury Area Computer Society

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1	2  **General Meeting** 6:30 PM	3  **Board of Directors** 7:00 PM	4	5	6
7	8	9 **Apple** 7:00 PM Richard Corzo *macsig@dacs.org*	10	11 **Membership Committee** 7:00 PM Jim Scheef 860-355-0034	12	13
14	15	16  **Web Design& DTP** Annette van Ommeren 7:00 - 9:00 PM *avanommeren@dacs.org* **Cancelled**	17 **Linux** 7:30 -9:30 PM Dave Mawdsley *linuxsig@dacs.org*	18 **Single Board Computers Workshop** 7:00 PM Jim Scheef 860-355-0034	19	20  **DACS.DOC Deadline**
21	22 **PR & Marketing Committee** 6:30 - 8:30 PM	23	24 **Social Media** Tom Zarecki 6:30 - 8:00 PM *tomZshow@ gmail.com*	25	26	27
28	29	30				

May 2015

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Jul 2015

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Secure Computing

Asymmetric Encryption

By Dick Maybach

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 one. 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 their 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 which 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.
- 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.

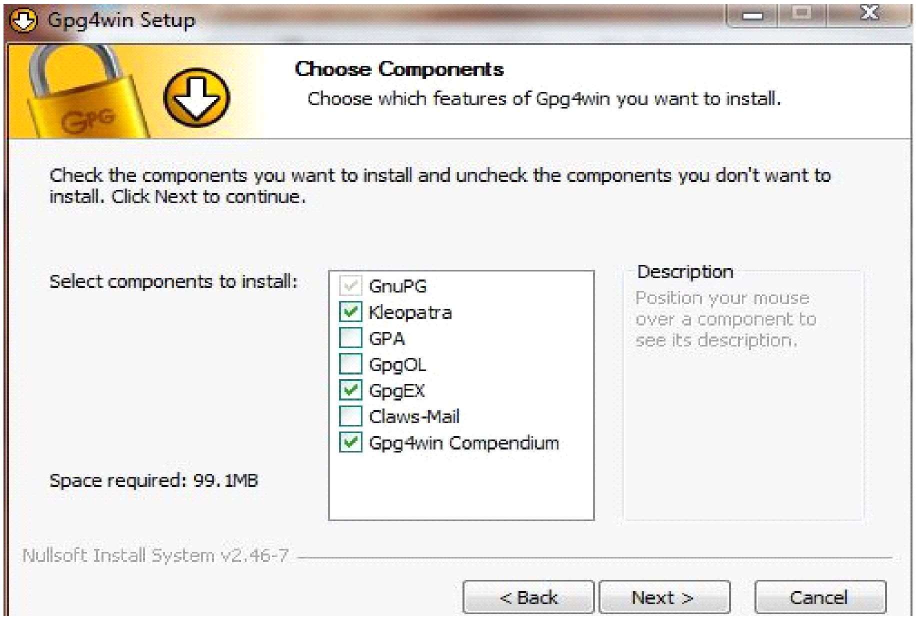
You download only those components that you need.

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 (Figure 1, below).

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.

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 (Figure 2,).

Keys are identified by your name and e-mail address, so you next would enter



Gpg4win Setup

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

Space required: 99.1MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.46-7

Figure 1

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 about 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. You could call that person and ask, "What are the last 5 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 (Figure 3).

The procedure is similar to add someone's public key is similar. Put the file containing their certificate somewhere on your PC, in Kleopatra click on File, then on Import certificate, and follow the instructions. (Figure 4)

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 them. 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 passphrase to access the keys on your keyring.

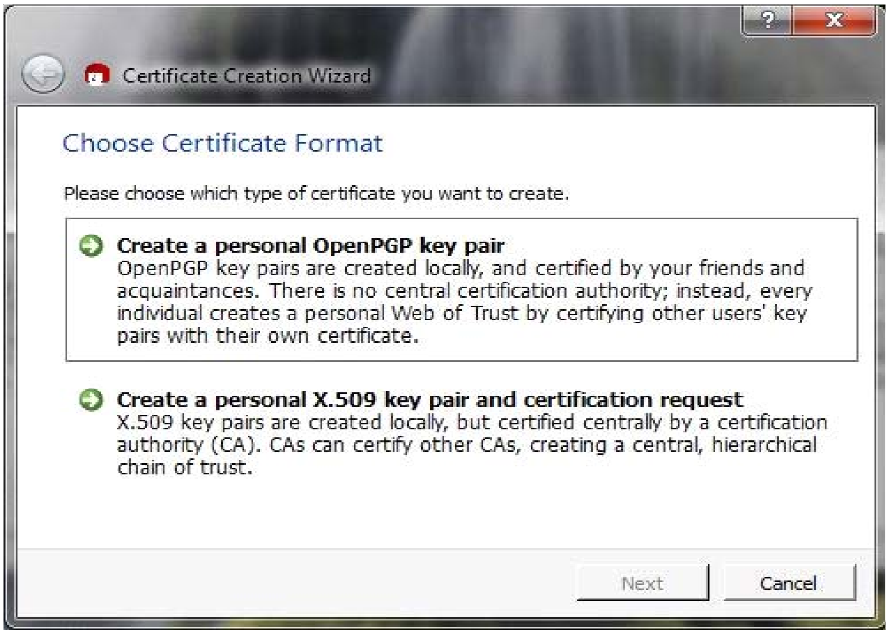
As the next screen-shot shows you have a second chance to decide whether you want to both sign and encrypt the file, and you also can decide whether the encrypted file will consist of binary or ASCII digits. Use the former for files that stay on your computer and the latter for e-mail (Figure 5.

The next two screen-shots show the contents of a test file and its ASCII-coded encrypted counterpart (Figure 6).

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.

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

The easiest way to send encrypted e-mail is to create a file on your PC, encrypt it



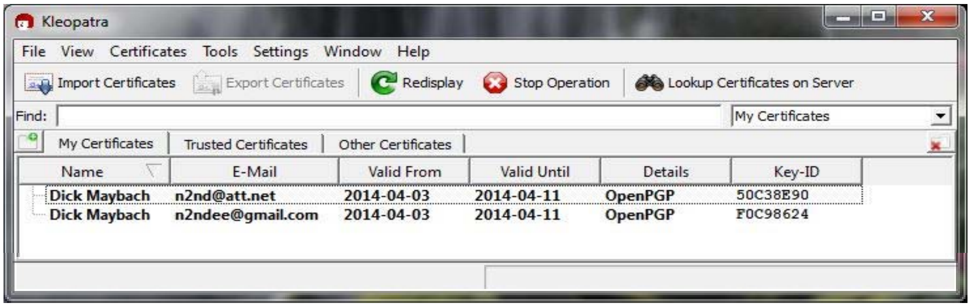
Choose Certificate Format

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.

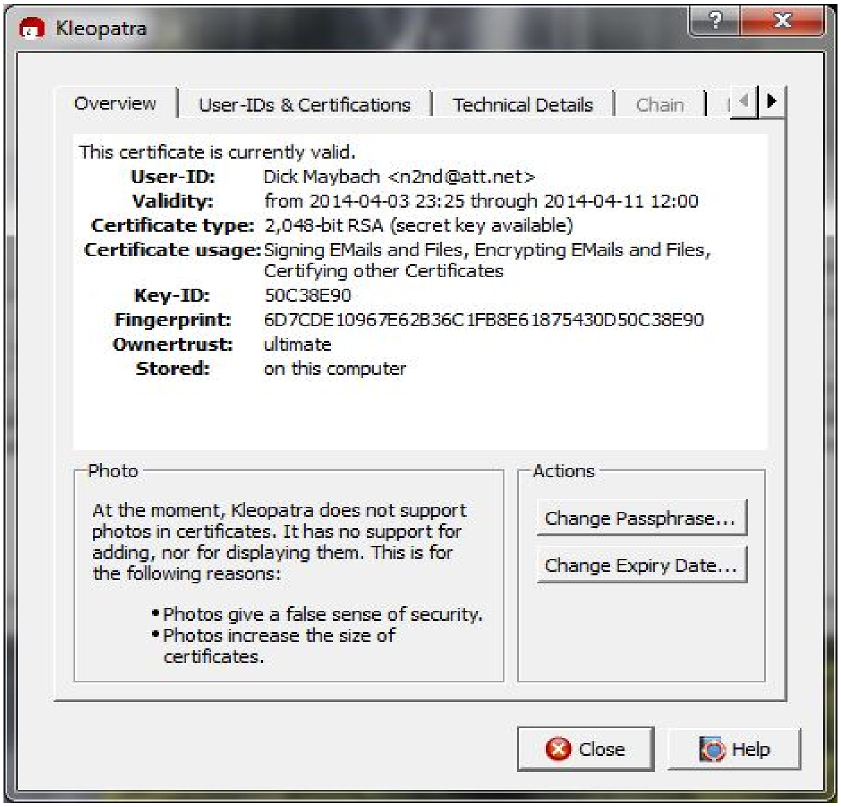
Create a personal X.509 key pair and certification request
X.509 key pairs are created locally, but certified centrally by a certification authority (CA). CAs can certify other CAs, creating a central, hierarchical chain of trust.

Figure 2



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Dick Maybach	n2nd@att.net	2014-04-03	2014-04-11	OpenPGP	50C38E90
Dick Maybach	n2ndee@gmail.com	2014-04-03	2014-04-11	OpenPGP	F0C98624

Figure 3



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.

Figure 4

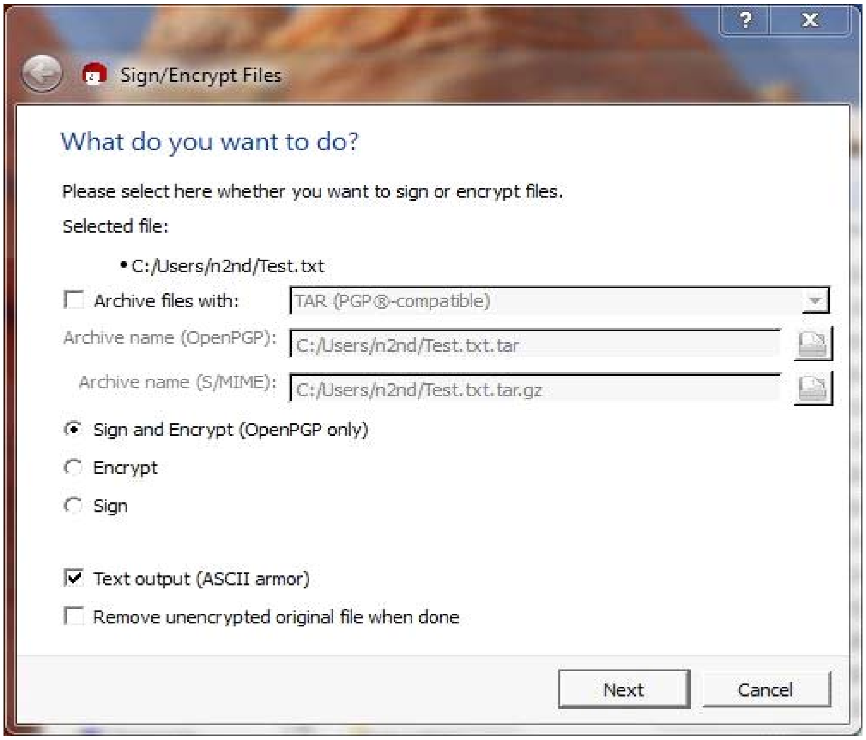
with both your and the recipient's public key, sign it with your private key, and use text output. Then open the file and transfer its contents to the e-mail message using copy-and-paste (Ctl-C, Ctl-V). This works with any e-mail client program and also with e-mail accounts you access with your Web browser. 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 passphrase 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.

Dick Maybach *is a member of Brookdale Computer Users' Group (*NJ n2nd (at) att.net; www.bcug.com*).*

This article appeared in the July 2014 issue, BUG Bytes, and is reprinted by permission for APCUG user groups.



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)

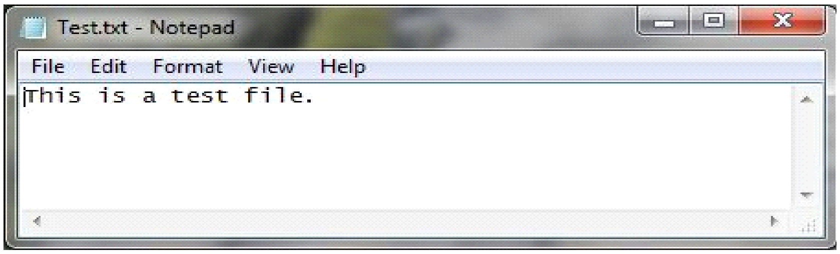
○ Encrypt

○ Sign

☑ Text output (ASCII armor)

☐ Remove unencrypted original file when done

Figure 5



Test.txt - Notepad

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

Figure 6

There are Many Ways to Join DACS

An easy way to join DACS is to attend one of the monthly general meetings. General meetings are normally held on the first Tuesday of each month at Danbury Hospital. Or join right on our Website via the PayPal link, where you may also pay by credit card without a PayPal account.

General meetings are always free to the public, but only members benefit fully from DACS' many other events, activities, and publications. As a member you become part of a dynamic computer group in the Greater Danbury Area.

You will receive a subscription to *dacs.doc*, our award-winning monthly newsletter, packed with news and information pertinent to computer users of all levels. In addition to interesting feature stories, the newsletter contains a monthly calendar of events and a recap of the the previous general meeting and last month's workshops. Members may also post questions to the DACS Community Forum.

Members may also attend the monthly workshops, where topics relating to computers, peripherals, software, and operating systems are discussed. Workshops meet throughout the month at our Resource Center in downtown Danbury unless mentioned otherwise in the calendar. Occasionally, special topic sessions are also offered to members.

Individual/Family Memberships

Annual membership dues are $40.00 for individuals or for each family living at the same address. Annual memberships which include a printed newsletter are available for $60.00 a year.

Operating Systems

"systemd" - A Replacement for "init"

by Cal Esneault

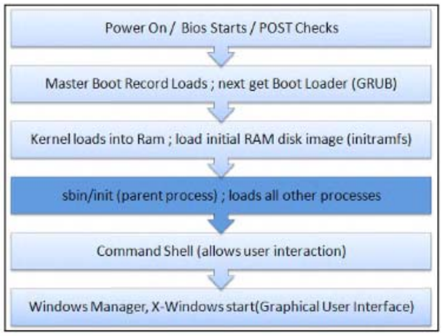
EVERY X-86 COMPUTER running Linux follows a typical boot process to initialize the operating system. After power-up, software stored on a ROM chip (the BIOS) initializes the hardware (screen, keyboard, memory test - known as the power-on self-test or POST). Next the boot loader software is located and put into memory (for example, location stored in Master Boot Record section at start of drive). GRUB, the Grand Unified Boot Loader, is commonly used for Linux. It has a text interface which allows selection of a kernel and is responsible for loading the kernel image and initramfs, the initial RAM disk (it contains critical files and device drivers needed to start the system). When the kernel is loaded into RAM, it immediately initializes and configures the computer's memory and also configures all the hardware attached to the system, such as processors, I/O subsystems, storage devices, etc. The initramfs system mounts the root file system onto the main drive, launches the init program, and clears itself from memory.

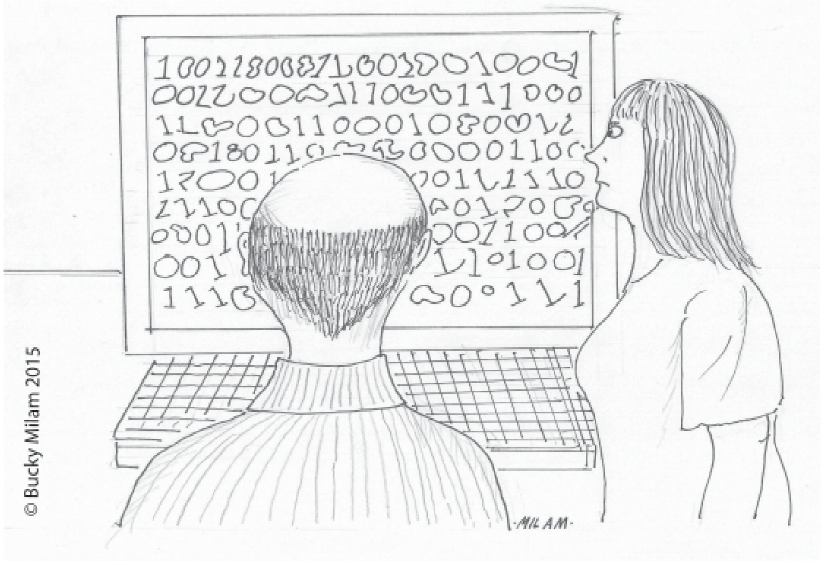
The init process is the parent process for all subsequent processes and runs until shutdown. Dating back to early Unix methodology, the system goes through a number of "run levels" where various "services" can be started and stopped. For example, text-based interfaces allow user interaction via a command-line interface (CLI), and then a "windows manager" loads X-windows and other configuration details to make a graphical user interface (GUI).

With increasing operating system complexity, the systemd daemon was developed to replace init beginning in 2011. This approach bundled several other supporting daemons including journald, logind, and networkd. Systemd has been adopted by many popular distros (see partial list below). The GNOME project is further integrating systemd, and Ubuntu has committed to changing from its current system (upstart) to systemd.

There has been pushback from some Linux distributions claiming that it is too complicated (224,000 lines of code vs. 15,000 lines for init) and does not put everything in one place. They say this violates the Unix principle of using lots of small independent programs that "do one thing and do it well." Currently Gentoo and Slackware have refused to adopt systemd, and some community members are boycotting distros that use it.

Such resistance to change is common with programmers who dislike changing from a tested system which has a long history of successfully working. Expect the next series of complaints to occur when new windows managers, such as Wayland, replace X-windows for GUI. Computer operating systems must constantly change to keep up with the progress in hardware.

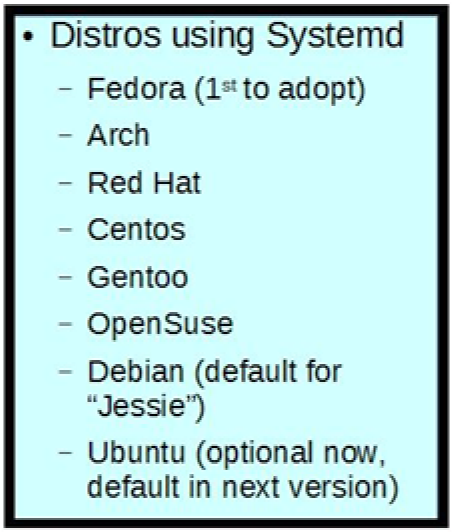

Power On / Bios Starts / POST Checks
Master Boot Record Loads ; next get Boot Loader (GRUB)
Kernel loads into Ram ; load initial RAM disk image (initramfs)
sbin/init (parent process) ; loads all other processes
Command Shell (allows user interaction)
Windows Manager, X-Windows start(Graphical User Interface)



“Your problem appears to be that some of the ones and zeroes in your Windows code are switching their orientation”

CAL ESNEAULT is former president of CCCC; leader of many Open Source Workshops & SIGs.

This article was published in the October 2014 issue, CCCC Computer News (Newsletter (at)clickers.org;www.clickers.org)


- Distros using Systemd
  - Fedora (1st to adopt)
  - Arch
  - Red Hat
  - Centos
  - Gentoo
  - OpenSuse
  - Debian (default for “Jessie”)
  - Ubuntu (optional now, default in next version)

Directors' Notes*, Cont. from page 3*

13. Tom will be soon announcing date for monthly social media workshops.

14. Guest: Rob Willard’s presentation that he and his team of interactive marketing students of Tom Zarecki’s class at WestConn last week.

a. Need to increase links to DACS.org from
b. Google mobility test
c. Google analytics
d. Topics from various people to build resumes, need diversification
e. Aggregate web sites are winning these days
f. Huge discussion on social media
g. Needs to be an outreach to people to teach future workshops

15. Tracking student membership, ideas discussed. Simply allow all student IDs.

16. Half price for student ID for membership – Vote: unanimous $20 half price

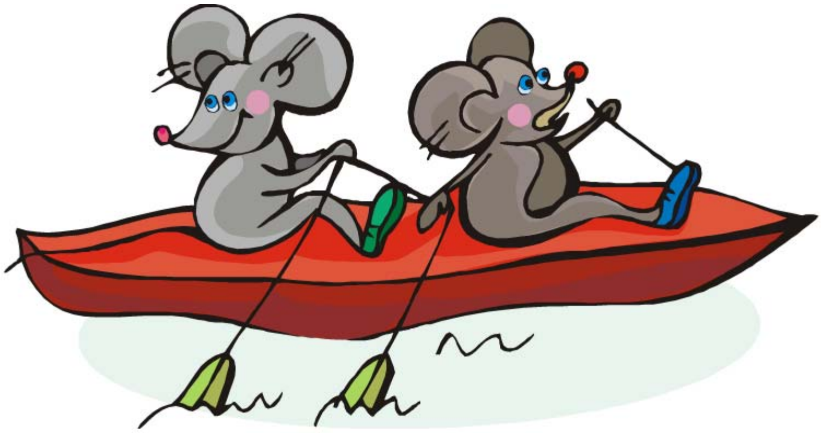
17. Richard proposed changing board meetings to Thursday after gen. meeting Voted down.

18. Bert suggests thank you note for donations.

9:44 PM - meeting adjourned.

—Dick Gingras

dacs.doc
Danbury Area Computer Society
65 Legion Rd
New Milford, CT 06776



When you come to the next DACS meeting, why not bring a friend?

Voice for Joanie

Help give the
gift of speech
Call Frank Ruiz
at 203 770-6203
and become a
Voice for Joanie
volunteer
www.voiceforjoanie.org

Future Events:

June 2

Video Production Basics
For Home or the
Superhighway

July 7

Ira Wilsker
Internet Security

August 4

TBA

September 1

TBA