HAPPY THANKSGIVING!!!
The Villages Computer Club - NO meeting Friday Nov 23rd.

Have a great Thanksgiving and safe travels should you be leaving The Villages for the holiday. There will be NO meeting on Friday Nov. 23rd.

Our next meeting will be Nov. 30th at Lake Miona it will be a workshop with lots of interesting subjects and informative discussions. More on this in my next announcement.

Paul Rabenold
TVCC.Pres@gmail.com
www.thevillagescomputerclub.com
****

Kindle for PC

A free download from *www.amazon.com/gp/**kindle/pc***

You'll be able to download ebooks and read them on your own PC.

You will also be able to sync books from your PC to your handheld Kindle

****

Email Settings Centurylink.net

Domain	Incoming POP	Outgoing SMTP	Username
embarqmail.com centurylink.net Email Server Limits	pop.centurylink.net Port 995 SSL	smtp.centurylink.net Port 587 TLS if available	Email Address

****

Restore Points Deleted in Win 7 Vista & XP

Restore Points may be deleted to safe hard disk space.

1. Open the START menu, rightclick Computer...click Properties.
2. Select System Protection and click Configure.
3. Choose Delete under Disk Space Usage and then click OK.

You may use Disk cleanup to delete all but the most recent restore point in Win XP/Vista/Win7.

1. Open Start menu and click All Programs. Under Accessories, choose System Tools and click Disk Cleanup.

2. Choose the drive you wish to clean. Select Clean Up System Files from dialog box and click Ok.

3. Under More Optios tab (in Win XP) choose Clean Up under System Restore. (In Vista and Win 7, this is listed under System Restore And Shadow Copies) Click Yes (Win XP) or Delete (Vista and Win 7) and when prompted click OK.

****

How to Read Email Headers

The email header is the info that travels with every email, containing details about the sender, the route and the receiver. It is like a flight ticket. It can tell who sent the email, when the email was sent,from where it was sent and how it arrived to you. It also has arrival details, who is the receiver and when it was received.

As with a booked flight, someone can send an email with false identity, pretending the email was sent from a different account,etc. This is a common practice of spammers.

1. In the return email, you will see paragraphs starting with Received tag: each of them was added to the email header by email servers, as the email travelled from the sender to the receiver. The last Received tag shows who sent the email (blue lines).

2. By reading the Receiving From tag, you can tell the ISP domain of the sender, and the IP address.

3. The Originating-IP shows the IP address of the sender.

4. The X-Mailer tag says what email client was used to send the email.

Note: When an email is returned to you, it will be sent to you by YOUR own server. Example if you are using AOL, then the returned email will come to you from the AOL server. This does NOT mean there is a problem with your email program or with AOL. If you sent the email to someone using Comcast.net and comcast.net does not find that email address in it's log, it will reject the email as sender unknown and return it via AOL. When it reaches the AOL server, AOL then will have to send it on to you as the original sender. This means the problem is with the address you're using or with Comcast.net as that is the server that rejected the email.

****

How to read email headers

- *see also: How to analyze and read a SPAM header...*

What is an email header?

The email header is the information that travels with every email, containing details about the sender, route and receiver. It is like a flight ticket: it can tell you who booked it (who sent the email), the departure information (when the email was sent), the route (from where it was sent and how did it arrive to you) and arrival details (who is the receiver and when it was received). As when you would book a flight ticket with a false identity, the same goes for emails: the sender can partially fake these details, pretending that the email was sent from a different account (common practice for spammers or viruses).

How do I see an email header?

It depends on your email client. Here is a comprehensive list of email client programs and methods to see the email headers.

How to interpret email headers?

Starting from the assumption that you want to read an email header because you want to know who really sent it, let's take an example (we will ignore the header tags that do not give precise information about the sender).
The following email was received by support@emailaddressmanager.com and we want to see who the sender is. Here is the email header of the message:

1.As you may already noticed, there are three paragraphs starting with the Received tag: each of them was added to the email header by email servers, as the email travelled from the sender to the receiver. Since our goal is to see who sent it, we only care about the last one (the blue lines).

By reading the **Receving From** tag, we can notice that the email was sent via corporate2.fx.ro, which is the ISP domain of the sender, using the IP 193.231.208.28. The email was sent using SMTP ("**with ESMTP id**") from the mail server called mail.fx.ro.

2.Looking further into the message, you will see the tag called **X-Originating-IP**: this tag normally gives the real IP address of the sender. The **X-Mailer** tag says what email client was used to send the email (on our case, the email was sent using FX Webmail).

How to analyze and read a SPAM header...

Analysis: Spam Header

Email header: where the spam starts

Here is the starting part of the header of a junk email (spam), which includes information about the transfer of the email between the sender and the receiver:

Let's analyze the red highlighted lines:

• **Return-path**: the header tells that if you reply to this email message, the reply will be sent to ydcdd...@yahoo.com. Would you use such an email address for real?

• **Received tags**: as on web blogs, read them from the bottom to top. The header says the email was originally sent from 206.85... and it was sent to 217.225... (which is the name/IP of the first mail server that got involved into transporting this message). Then suddenly, the next **Received** tag says the message was received from root@localhost, by mailv.fx.ro. You can also notice that so far, the **Received** tags do not contain any information about how the email was transmitted (the **"with"** tag is missing: this tag tells the protocol used to send the email).

In reality, this is the common case of a spammer pretending to be the root user of mailv.fx.ro and sending the email from 206.85..., through 217.225... and telling 217.225... to act as the root user of mailv.fx.ro, in order to use the SMTP server of mailv.fx.ro to send the email. Since more and more mail servers are not allowing open-relay connections, the spammer can only use the mail server of the receiver, in order to send the message. If the spammer will try to send the email to support@emailaddressmanager.com, through exactly the same route as above, it wouldn't work, because support@emailaddressmanager.com is not a network user of mailv.fx.ro. This is the reason why you may have received spam emails appearing to be sent through an email address of your own ISP.

Going deeper with the analysis, you can use an IP tracing tool, like Visual Route, in order to see to whom the IP belongs to. As in most of the spamming cases, the starting IP (206.85...) is unreachable, which means that the spammer could have routed the real IP or he could have used a dynamic IP (a normal case for dial-up users). However, by tracing 217.225..., you will get to the ISP used by the spammer, a German provider. The ISP has nothing to do with the spam itself, but it was simply used by the spammer to connect to the Internet.

Let's look further into the email header:

• The **Message-ID** field is a unique identifier of each email message. It is like the tracing ID of an express postal mail. The rule says the ID is composed by the name of the server that assigned the ID and a unique string (for example, QESADJHO@emailaddressmanager.com). Hmm, this is strange, because on our case, the ID belongs to hotmail.com, while the sender appears to belong to yahoo.com. In fact, this difference mainly shows that the sender is forged (fake address or someone pretending to own that email address).

• The **X-IP tag (also named X-Originating-IP)** is probably the most important one and it should give precise information about the sender (from where the email was actually sent). Unfortunately, this tag is optional for email protocols, so some spam messages will not include it. As you can see, the originating IP is not even close to the sender's IP, from the Received tags.

• The **X-UIDL** tag is another unique ID, but this one is used by the POP3 protocol when your email client is receving the email. This is an optional email tag, but the rule of thumb says spammers love to include it.

****

Jmax

Jmax's Website http://www.jmaxbits.com/

Jmax Bits Newsletter is now posted each Monday & Thursday on the website. You have the option for a .pdf or a .rtf file.

1.For help with a computer problem, put HELP in the subject line and give me info about the computer you're using, if you know it.

2.To view or print Jmax Bits Good Services List in the Villages area, click link www.jmaxbits.com

3. To sign up for the non-computer newsletter, send an email to VLGSClassifieds@aol.com. Put SUBSCRIBE in the subject line. To send an Ad, place AD in the subject line.

4. The Villages Computer Club's web page: