The Rochester Computer Society, Inc.
Since 1982

MONITOR

Vol. 31, No. 10 October 2013

Next Meeting

Tuesday, October 8

New Users Group

Contents

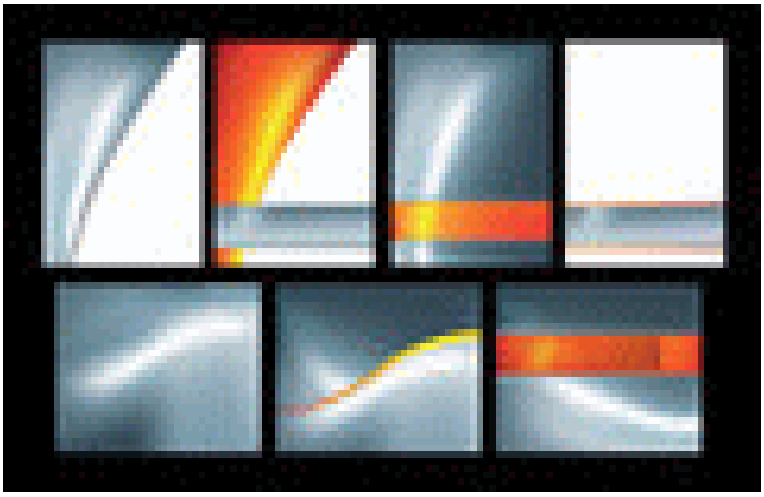
Alternative Streaming Video Sources

by Ira Wilsker

Isn't rapidly evolving technology wonderful? While we can still watch a handful of free TV channels over the air with a simple antenna, relatively few people still do. Stores that rent DVDs still exist in relatively small numbers compared to just a few years ago, and VHS rentals have just about gone the way of the dinosaur. There are still thousands of limited selection kiosk type vending machine video rental boxes, typically adjacent to supermarkets, convenience stores, and fast food restaurants, but they still require time

and mileage to rent and return videos. Most cable and satellite TV providers offer some form of video streaming on demand at varying prices, but they are now facing significant competition from alternative streaming video services that send TV and movies over the internet directly to the consumer.

On a recent visit to see my grandkids in Georgia, my daughter had full length movies from Netflix streaming on her internet connected flat screen TV in her living room; my three year old granddaughter had an inexpensive Android tablet connected to the home Wi-Fi, and expertly manipulated the screen selecting movies and cartoons on the child-safe "Kids Netflix." For the few who may be totally unaware, Netflix (netflix.com) is currently the industry leader in streaming movies and TV to computers, smart devices (phones and tablets), TVs, and other network connected devices. According to the Netflix website, "For only $7.99 a month, you get unlimited movies and TV episodes instantly over the Internet to your TV or computer. There are no commercials, and you can pause, rewind, fast forward, or rewatch as often as you like. It's really that easy!"



As of June 30, 2013, Netflix had 29.8 million subscribers to its streaming service in the U.S. (an increase of 633,000 in the second quarter of 2013), and another 7.75 million outside the U.S. While originally an online DVD rental company, Netflix has seen dramatic decreases in its DVD members as they mostly switch to streaming videos and TV; as of June 30, Netflix was down to 7.51 million DVD subscribers, a loss of 475,000 subscribers in the same quarter (Source: news.yahoo.com/numbers-netflix-subscribers-205626746.html.)

While Netflix is the premier streaming video provider, it is by no means the only provider, as other powerhouses including Amazon, Google's YouTube, Google TV, Walmart, hulu, VUDU, iTunes, and now Target join the fray. Amazon claims to have, "Over 150,000 top movies and TV shows to rent or buy, including thousands available to Amazon Prime members at no additional cost." While most of the 150,000 movies and TV shows are available for streaming at modest prices, Amazon offers a $79 per year "Prime" account which includes the streaming of over 15,000 full length movies and 3100 TV shows at no additional charge. The $79 annual fee for Amazon prime also includes several non-video related services including thousands of "free" Kindle books to "borrow," and free second day shipping of Amazon products with no minimums.

For the past few years, Google has been quietly offering both free and nominally priced full length movies and TV episodes over its extremely popular YouTube service. As Google expands its "Google TV" (google.com/tv) offerings, there is much buzz in the media that Google TV will incorporate the paid YouTube movies, as well as other content into its streaming TV service. According to Google, "As well as making it easier to find stuff to watch from your existing TV service, Google TV enhances the TV you're used to with over 100,000 movies and TV episodes on demand, thousands of YouTube channels, apps, & more content coming all the time."

At present Google TV requires a fast broadband internet connection along with a compatible connected TV or a converter box, several of which are available from a variety of manufacturers, ranging from the tiny $35 Google Chromecast HDMI Streaming Media Player, to a variety of more powerful and sophisticated devices that are mostly in the $75 - $150 range.

Hulu has been around for several years, initially offering thousands of free commercially sponsored TV episodes (still available), and is now offering its $7.99 per month Hulu Plus service as a direct competitor to Netflix, with a heavy emphasis on TV shows. Hulu Plus (hulu.com/plus) can stream directly to almost all smart devices, including phones and tablets, as well as almost any internet connected or networked HDTV,

most modern game consoles, Kindle, Nook, Nintendo, computers, and other streaming media devices.

In recent days, the Target department store chain announced the limited "beta" (pre-release) availability of "Target Ticket" (target ticket.com). While still in its early stages, and not yet available to the public, it is currently only available to employees and customers who are part of the store's REDCard program. Target Ticket has, "... instant access to 15,000 titles, new releases, classic movies and next-day TV, there's always something new to watch and love." Target Ticket allows the user to, "... stream or download movies and shows in your library for playback on your PC, Mac, iOS, & Android pro-ducts." Members will be able to purchase or rent digital content that can be viewed on smart phones, tablets, TVs, Blu-ray players, and game consoles. At present, Target Ticket offers network TV content from ABC, AMC, CBS, CW, Fox, FX, HBO, The WB, NBC, Showtime, Starz, and USA. As a bonus, Target Ticket will allow users to access some of the newer DVDs before their official release date. Being a commercial service, new movies will be available for purchase, projected to be in the $12 - $15 range, with movie rentals around $4. TV episodes can be rented for about $3, with entire seasons available for purchase after the end of a season at around $35.

Walmart has also joined the streaming media craze by partnering with the established streaming provider VUDU (walmart.com/cp/Video-On-Demand-by-VUDU/1084447). With this partnership (or a personal membership directly with vudu.com), members can rent or purchase the latest videos for immediate streaming that can be viewed on a variety of devices including iPad, PlayStation 3, computers, VUDU-enabled TVs, and compatible Blu-ray disc players. VUDU claims to offer the largest library of HD movies where the users only pay for what they watch, with no subscription or late fees. In its partnership with VUDU, Walmart is selling VUDU enabled TVs and Blue-ray players from Mitsubishi, Vizio, LG, Magnavox, Philips, Samsung, and Sony. Walmart also offers specials and deals on VUDU movies, including a "99-cent Movie of the Day" over a thousand $2 - two day rentals.

Obviously going after industry leader Netflix, VUDU claims to offer most major studio, newly released DVDs to its customers long before they are available to Netflix' streaming customers. Specifically, VUDU claims that "Almost all of our movies are available the same day they come out on DVD and Blu-ray" compared to Netflix' 28 day delay on physical DVDs mailed to rental subscribers, and up to seven years after release to be streamed on Netflix!

Apple is also offering streaming TV and movies through iTunes (apple.com/itunes/charts/movies). iTunes members can purchase or rent TV shows and movies thru their existing iTunes account and stream them to TV, a computer, iPod, or iPhone. Apple also offers a $100 hardware device, Apple TV, which allows streaming and downloaded content from iTunes, Netflix, Vimeo, and other sources to be played in 1080p HD on most HD TVs. The Apple TV device can also stream video and games from Apple (iOS) devices, PCs and Macs to TVs. The Apple TV device has HDMI and digital optical output, and can be connected to home networks running 802.11n (also called wireless-N or WiFi-N) or with a traditional Ethernet cable.

With these reasonably priced alternatives to the more traditional sources of electronic entertainment, consumers have some excellent choices. Some (VUDU, Walmart, iTunes, YouTube) offer free membership, where the user only pays for downloaded content, while others such as Netflix and Hulu Plus offer a flat rate of $7.99 per month, with Amazon Prime available at $79 per year. With choices like these, anyone with a decent broadband connection has quite a bit to choose from.

Websites:

http://www.targetticket.com/home/premium
http://www.hulu.com/
http://www.hulu.com/plus
http://netflix.com
http://www.amazon.com/Instant-Video/b?ie=UTF8&node=2858778011
http://www.walmart.com/cp/Video-On-Demand-by-VUDU/1084447
http://www.vudu.com
http://www.youtube.com/movies

http://www.youtube.com/user/movies/videos?flow=grid&view=26 (FREE MOVIES)
http://www.google.com/tv
http://www.apple.com/itunes/charts/movies

When Fine-Tuning Fails

Q. My grandson offered to "fine-tune" my Windows 7 computer to make it run better, though it wasn't really having any problems. He installed several programs and now I'm having problems where none existed before. Could the programs he installed be causing this?

A. I would like to cite a world-renowned, authoritative treatise in responding to your question, that being Mr. Modem's Computing Rule 47-A: "With very few exceptions, never let a spouse, friend, neighbor or computing-genius child fine-tune your computer. The outcome will rarely be satisfactory."

Let's examine the facts: Your computer was running fine. Your well-intentioned, semi-gifted grandchild was then granted permission for what? To make your computer run finer? The result of his diligent effort:

Problems where none previously existed. I'm no Sherlock Holmes, but I'm thinking that there just might be a causal connection here.

I would suggest requesting your grandson do a bit more fine-tuning and uninstall whatever he installed. If that doesn't resolve the problem, run System Restore which you can do on your Win 7 system by clicking Start > Search and type "System Restore," (without the quotes), then select System Restore. Select a date to restore to from the calendar that appears. In this way you should be able to turn back the clock to a time prior to the occasion when your grandson worked his magic.

Q. I have an age-old question, Mr. M: Should I turn my computer off when I'm finished using it or leave it on 24/7?

A. If you use your desktop computer daily, I recommend leaving it on. I leave my computers on for a number of reasons, not the least of which is that most catastrophic failures occur during power up when a surge of electricity hits the cold, static computer components. Leaving a computer on maintains a stable, internal operating temperature which is desirable. I have 11 computers here (Mrs. Modem is destined for sainthood) and all of them run 24/7.

Space constraints do not permit an exhaustive discussion of this topic, but in general, though my computers run 24/7, I have my monitors configured to go dark after two hours of non-use. Depending on your version of Windows, you can generally configure that by going to Power Management in the Control Panel > Display > Screen Saver > Monitor Power. You will see settings for the Monitor, Hard Drive and Standby. I have my desktop computers set to 2 hours, Never and Never. In other words, the hard drives never shut down, nor does any system go into Hibernation or Sleep mode. (There are no moving parts with solid-state or SS drives, so "always-on" is a natural state -- not unlike my Cousin Norbert, the Insomniac.

Hard drives are rated by hours between failures and a typical new hard drive today is rated at 200,000 hours. Even at 100,000 hours, that's a little over 11 years of 24/7 operation, so it is extremely unlikely that your drive is going to self-destruct as a result of being on. You do need to pay attention to any strange noises emanating from the drive, its cooling fan(s), or your gastrointestinal tract. If a fan starts to make unusual noises, you can have it replaced for approximately $20.

If you do decide to leave your computer on, restart it once a week to clear out the memory and refresh system resources, but that's all you really need to do. By leaving my computers on, I have my anti-virus and

anti-spyware programs configured to update and scan in the middle of the night.

Mr. Modem's DME (Don't Miss 'Em) Sites of the Month

Not in My Food

Hosted by a Consumers Union team of food safety advocates, this site operates on the premise that everyone has a right to know what's in the food they eat. That means knowing what foods contain carcinogens, what ingredients might be dangerous or of concern, and even if the packaging should be approached with caution. This is an excellent and informative site, particularly for those who never want to eat again.

www.NotInMyFood.org

Rat Race Rebellion

If you have ever searched for a work-from-home job, you probably know that there are oodles of scams, all too eager to separate you from your hard-earned dollars. This site wants to change that by offering approved, qualified leads for legitimate jobs. Start your visit by reviewing the FAQ that explains how the site works, then under Start Here, check out Today's Screened Job Leads which will take you to the newest job listings.

www.ratracerebellion.com

Vehicle Fixer

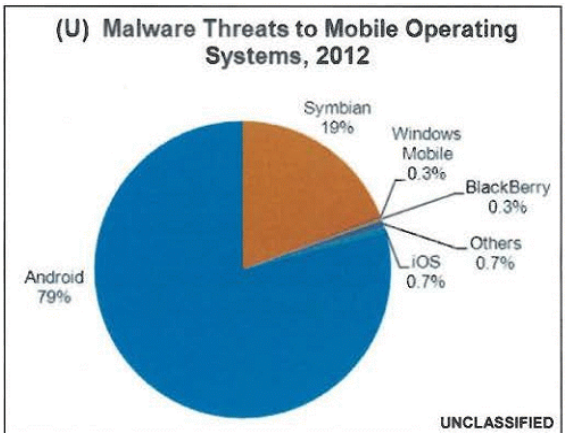
Here you can release your inner mechanic and watch videos that will help you repair your vehicle. That's the theory, anyway. Start by selecting the type of vehicle or the type of repair required. The site will then display your video search results. If you scroll past the explanation of the site, you can click links to videos about the site, a link to the site's blog, news and interviews.

www.vehiclefixer.com

For more information about Mr. Modem's eBooks and award-winning computer-help newsletter featuring personal answers to your questions by email, visit www.MrModem.com

DHS, FBI, Warn About Threats to Android Mobile Devices

by Ira Wilsker



In a document labeled "U//FOUO (Unclassified For Official Use Only) Roll Call Release for Police, Fire, EMS and Security Personnel," dated July 23, 2013 the Department of Homeland Security (DHS) and the FBI issued a warning about security threats to Android powered mobile devices.

According to recently published industry figures, mobile devices powered by Google's Android operating system currently comprise about 75% of all mobile smart devices, making Android the world's most widely used mobile operating system. Even though Google designed Android to be secure, and have each running "app" or program run in a closed memory space or "sandbox" in order to protect one bad app from infecting the entire device, Android devices have become a primary target for malware authors. Because the Android operating system is released as "open source," and the program has much in common with the well known Java operating system, Android has become the targeted operating system of choice for creators of malware.

While Google has frequently released updates and upgrades to Android, many of which have improved and increased the security of the operating system, 44% of Android users are still using the out-of-date (2011) "Gingerbread" or versions 2.3.3 to 2.3.7 of the operating sys-tem. These older versions of Android, which were once thought to be secure, are now known to have several known security vulnerabilities; Google repaired

and patched these vulnerabilities in later versions of Android. In this "Roll Call Release," the DHS and FBI warned that, "The growing use of mobile devices by federal, state, and local authorities makes it more important than ever to keep mobile OS patched and up-to-date." It only seems logical that this warning would equally apply to privately owned Android devices as well. Personally, as the owner of several Android powered mobile devices, I can attest to the fact that many of the "older" Android devices running some form of Gingerbread, many of which are still currently available in the marketplace as "new" devices, cannot be readily upgraded to the newer versions of Android. The latest version of Android released by Google is "Jelly Bean," a tweak to version 4.3, released on August 23, 2013. It is important that, in terms of security, the latest Android updates available be installed and updated again as appropriate.

According to this DHS-FBI warning, there are three primary security threat types currently targeting mobile devices running the Android operating system. Almost one-half of the current threats are called "SMS (Text Messaging) Trojans." Targeting predominately the older, unpatched versions of Android, such as Gingerbread, these trojans send text messages, unknown by the user, to premium rate numbers owned or operated by the hackers; these financial charges, often unreasonably high, appear on the monthly bills of the victim user, with the bulk of the proceeds going to the criminal enterprise. While Android devices are essentially immune from traditional computer viruses, the DHS-FBI warning suggests that this threat can be reduced with the simple installation of a comprehensive app. While almost all of the commercial security software companies offer a paid Android security suite, there are also several excellent Android security suites available for free. An updated list (revised August 8) of the top rated free Android security suites is available from Gizmo's TechSupportAlert.com at www .techsupportalert.com/content/best-free-antivirus-app-android.htm. According to the Gizmo reviews, the current top-rated free Android security suite is 360 Mobile Security – Antivirus by Qihu Software, closely followed by what I have on my personal Android phone, TrustGo Antivirus & Mobile Security. These, and all of the other free security suites listed by Gizmo are available from the Google Play Store, accessible directly through the device, or from Android web store at play.google.com.

The second major type of threat to Android powered devices are generically called "Rootkits," which are a type of malware that hides itself from traditional forms of detection. In 2011, a controversial rootkit, that had likely been intentionally installed on the phone by its manufacturer or carrier, was found to be running on millions of mobile devices. According to Wikipedia (en.wikipedia.org/wiki/Carrier_IQ), an intentionally installed rootkit, Carrier IQ, has been installed on over 150 million Android phones. Wikipedia says that Carrier IQ, "is software, typically pre-installed on mobile devices by handset manufacturers or network operators, designed to gather, store and forward diagnostic measurements on their behalf. Data available can include metrics on the device itself (e.g., firmware, battery levels, application performance, web performance) and performance data on voice and data connectivity between the device and radio towers."

While this may seem innocent enough, as the phone carriers need to monitor system performance, there is also substantial evidence that this Carrier IQ software "phones home" with a lot more than basic performance information. On December 1, 2011, CNN broke the story "Carrier IQ: Your phone's secret recording device" (money.cnn .com/2011/12/01/technology/carrier_iq/index.htm). According to the CNN report, "Carrier IQ is a piece of software installed on millions of mobile phones that logs everything their users do, from what websites they browse to what their text messages say." CNN was referring to an earlier study by Android expert Trevor Eckhart who first published concerns that Carrier IQ was transmitting more than just system data, followed up by a YouTube video (http://youtu.be/T17XQI_AYNo) de-tailing the personal data being captured and sent to the carriers.

In his YouTube video, Trevor Eckhart showed how the Carrier IQ software factory installed on his Android phone recorded every key stroke, every text message, and the URL (internet address) of every website that he visited, including websites that are encrypted to prevent tracking. Immediately following the CNN report, the publisher of Carrier IQ announced, "While a few individuals have identified that there is a great deal of information available to the Carrier IQ software inside the handset, our software does not record, store or

transmit the contents of SMS messages, email, photographs, audio, or video." (*Wikipedia*).

There are several free (and paid) Android apps in the Google Play Store that can detect Carrier IQ, and notify the user of its presence; simply search the Google Play Store (play.google.com) for "Carrier IQ." While it is free and simple to detect the Carrier IQ rootkit software on Android phones, it is extremely difficult to remove, with some published reports that many phones that have had the Carrier IQ software removed lost functionality, and were no longer covered by warranty (source: *Wikipedia*). There are also some apps that can cripple some of the Carrier IQ reporting, without actually removing it from the phone. The DHS-FBI warning recommends that Android devices used by first responders should have Carrier IQ removed. For the record, all of my Android devices tested positive for the Carrier IQ software.

The third security threat mentioned was "Fake Google Play Domains." These websites were created by cyber crooks to trick innocent users into downloading and installing malicious apps. These malicious apps, which often appear as legitimate music, books, magazines, movies, TV programs, and other applications, are designed to steal sensitive information, financial data, user names, and passwords. While not perfect, as some malicious apps have been slipped through and been posted, the genuine Google Play Store (play.google.com) is probably the safest resource for Android apps. The DHS-FBI warning also advises that security software, such as some of those mentioned above, should be installed on the Android devices and frequently updated. If any malicious software is found, it should be removed immediately, followed by an immediate change in any possibly compromised user names and passwords.

If the Department of Homeland Security (DHS) and the FBI believe that the security threat to Android devices is serious enough to post a "Roll Call" message to first responders, perhaps the same warnings should be considered by private citizens.

Just in case that Apple iOS device users think that their smart devices are immune from security threats, do not be complacent; your devices are at risk as well.

How to Sell Your Cell Phone (or Other Gadget)

by Bob Rankin
askbobrankin.com

Smartphones become obsolete almost as fast as the news these days. If you like to stay on the bleeding edge, you'll upgrade your tech gadgets at every opportunity. But what's the best way to get cash for your used electronics, without getting scammed? Here several ways you can sell an unwanted mobile phone, tablet, computer, or other gear...

Selling Your Used Electronics

Are looking to sell your smartphone or tablet? Some carriers take old models as trade-ins, but sometimes you're stuck with a piece of electronics you can no longer use. Fortunately, there are several ways to turn your old phone into cash. If you have an unwanted tablet, Kindle, laptop, game console, or digital camera, you can sell those too. Here are some options to find out how much your items are worth, and sell them to the highest bidder.

Gazelle is one such option. Answer a few simple questions about your phone and get an offer for it. Mail your phone to Gazelle using their postage-paid label delivered to you electronically. When it passes Gazelle's inspection, you receive money via check, Amazon gift card, or Paypal. Note that Paypal will take a cut of the money sent to you.

Gazelle takes tablets as well as phones of all operating systems. It accepts Apple computers and iPods. It does not accept Windows PCs, Linux x86 boxes, or basically anything made by Intel. I sold a used Motorola Droid via Gazelle, and got a check in the mail 10 days later, for the agreed amount. You can buy used electronics from Gazelle, too. The company resells and re-buys a gadget until it cannot be sold anymore, then sends it off to a recycling center to be torn apart for its useable components. Gazelle is into both kinds of green: Money and Mother Earth.

Usell deals in used phones, especially iPhones and Samsung models, and also deals in iPods, iPads, game consoles, video games, and even non-electronics such as textbooks, kids' clothing, women's clothing, and gift cards. I say "deals" because Usell doesn't buy anything; it acts as a broker between device owners and a network of resellers. Usell takes information about your device; puts it out to resellers on its private network; and gets back to you with a list of offers, if there are any. If you accept an offer, you ship your phone to Usell and it's forwarded to the reseller-buyer. You get paid when Usell gets paid by the reseller-buyer.

If the reseller-buyer pays, that is. There are reports online of long-delayed checks; checks for a fraction of the agreed upon amount; and checks that never arrived. While ultimate culpability for such scams lies with the reseller-buyer, Usell may not be exercising sufficient due diligence in choosing its partners. They do have a rating system for the buyers, so be sure to choose one that has at least four stars and lots of positive reviews.

NextWorth is a similar service that buys used electronics for cash. They will purchase smartphones, tablets, e-readers, digital cameras, mp3 players, video games, game consoles, Apple and PC laptops, and even calculators. Aside from the wide variety of items, a few things that differentiate NextWorth are their 30-day price lock on quoted offers, and the option to get paid instantly by bringing your device to a participating Target department store.

With services like Gazelle, Usell, and NextWorth, it's important to be honest and realistic about the condition of your device. If you say it's "like new" and send them a scratched-up phone with no accessories, you're likely to be unhappy with the payment you receive. I suspect that a large portion of the unhappy customers of these services are those with unrealistic opinions about the condition of their gear.

Which Way Is Best?

By way of comparison, I got quotes from all three of these services on a Verizon Samsung Galaxy S3 (White, 16GB) smartphone, in good but used condition. NextWorth offered $144, Gazelle $145, and Usell $150. Next, I tried an AT&T iPhone 5 (16GB). NextWorth offered $320, Gazelle $300, and Usell $305. For some reason, the mobile carrier to which your phone is assigned makes a big difference. In the cases above, Sprint phones were usually quoted at about 60% of the offers for the same phone on AT&T or Verizon. In a few cases, T-Mobile phones got significatly higher offers. Usell was the only one of these three that offered to buy feature phone (non-smartphone) cell phones.

Of course, you can always sell the device directly yourself. Craigslist is free; just post an ad in your local market, watch the offers flow in, pick a buyer and – go meet a stranger in a strange place with a few hundred bucks worth of gear in your hand? Yeah, you have to be careful. Stick to public places to make exchanges. I'd go with the police station parking lot, or someplace where there are obvious video cameras rolling. NEVER give a stranger your home address! Some people bring a large friend or two along. Under no circumstances should you deal in anything other than cash handed over in person; counterfeit check and money order scams abound on Craigslist. But thousands of phones and other electronic devices change hands safely via Craigslist every day.

If you don't know what your used device is worth, eBay can help you find out even before you put an item up for auction. Among the many search parameters found on eBay, "sold items" is probably the most valuable. It will show you the true market value of items like yours that actually sold. With a good feel for what's realistic, you can set your starting price low but not too low, high but not too high.

Cracked or scratched display? A chipped case corner? A phone that does not work at all? Not a problem; list it anyway and take what you can get. A lot of people buy damaged and non-working electronics for parts, or something.

Just don't be like the Australian woman who posted an online ad looking to buy two iPhones. She got a

response, and met in a McDonald's restaurant with a seller offering "two Apples." She paid $1,200, took the iPhone boxes home, and only later discovered they contained actual apples, instead of iPhones. Yes, it's a true story!

And then there's Kelly Filkin, who got slammed by Judge Judy for taking hundreds of dollars for a phone advertised on Craigslist, and mailing the buyer just a PICTURE of the phone. Watch this classic Judge Judy episode for the greatest barbecuing of a dumb crook in the history of television. Incidentally, I looked up Ms Filkin a couple of years after this episode aired. Sure enough, she was in jail on fraud charges.

Read more: http://askbobrankin.com/howto_sell_your_cell_phone_or _other_gadget .html#ixzz2emkqRmVh

Holy Cow! Is this a Virus?

by Linda Gonse
Editor/Webmaster, Orange County PC Users' Group, CA

I recently added a second external hard drive to my computer system. I use one for backups of InDesign files and the other one for Acronis True Image system backups.

As I browsed through the files I'd saved to the drives, I ran into something peculiar. Both drives had folders with names that were long strings of random letters. And each folder contained one file: mrtstub.exe at 89KB on the Iomega drive, and MPSigStub.exe at 227KB on the Seagate drive.

Fearing these might be malware or a virus, I quickly did a Google search. Interestingly, the search turned up conflicting opinions in different forums. Some people said it was a virus and highly dangerous, some said the folder and file(s) inside were benign, some said the files were leftover from when Microsoft Malicious Software Removal Tool (MRT) was run and had not been deleted automatically, and some said Windows created them.

Although I only found one file in the folders, other people have seen as many as four at one time: mrtstub.exe, mrt.exe._p, MRT.exe, and $shtdwn$.req.

I found a link to information about the Malicious Software Removal Tool at http://support.microsoft .com/kb/890830#Faq. In particular, it gave instructions on how to remove the Malicious Software Removal Tool.

The Malicious Software Removal Tool does not use an installer. Typically, when you run the Malicious Software Removal Tool, it creates a randomly named temporary directory on the root drive of the computer. This directory contains several files, and it includes the Mrtstub.exe file. Most of the time, this folder is automatically deleted after the tool finishes running or after the next time that you start the computer. However, this folder may not always be automatically deleted. In these cases, you can manually delete this folder, and this has no adverse effect on the computer.

I also learned that MRT is not a substitute for a resident antivirus for various reasons: 1. MRT only removes malware *after* infection, it doesn't *block* malware like an antivirus does; 2. MRT is designed to target a small set of malware only, while an antivirus takes care of most malware in the wild; and 3. MRT can only detect actively running malware – an antivirus can also detect dormant malware.

Microsoft's Knowledge Base (http://support.microsoft.com/kb /890830) also said a new version of the Microsoft Malicious Software Removal Tool is released every month. After you download the tool, the tool runs one time to check your computer for infection by specific prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection it finds.

This Knowledge Base article contains information about how you can download and run the tool, and what happens when the tool finds malicious software on your computer.

Even though I did not intentionally download the Removal Tool or run it, I read that Windows Update may do that when it downloads automatic updates. Further, it uses the largest hard drive on the system to create the temp folders; and in my case, the external hard drives are the largest with each being 2TB.

The upshot of this was I checked each file's Properties and confirmed Microsoft had signed them. Then I deleted the folders and files manually and nothing bad happened. In the future, I'll disconnect the external

drives before downloading or installing Windows Update.

From the March 2013 issue of nibbles & bits*, newsletter of the Orange County PC Users' Group, CA. Courtesy of APCUG.*

A Versatile Android Email Client, Watching Movies in Hotels

by Steve Baer
Hilton Island Computer Club, FL

Aqua Mail – A Versatile Android Email Client

I have been using and traveling with an Asus Transformer Infinity TF700 Android Tablet (running Jelly Bean 4.1.1) for several months now and still love it. (I also still use and travel with a borrowed Ipad2, and also find it quite good.) One thing I like about the Asus Tablet is that it comes with an included tablet based email client (from a Company called XCome) that can collect email from all my mail systems (2 ISP and 1 Gmail). This very nicely emulates the way the various Microsoft email clients that I use work in XP, Vista, and Windows 7. It has one problem however – when you are sending an email it is not possible (on the fly) to change the mailbox that you are sending an email from. For example, if you receive an email on a Hargray account and hit reply, the tablet mail client will automatically send it from that same Hargray account, and not let you change it. (It appears that the original XCome client had the ability to change sending accounts at this point, but it was disabled in bringing it to the Asus tablet.)

That is OK at home. But because of the way Hargary operates their email system, they will bounce the reply if you are traveling and located in a non-Hargray domain such as a distant hotel. Hence, I have to switch senders before I can reply to that incoming mail and use a non-Hargray account.

I spent some time searching for Android Email clients that permitted dynamic sender selection and found several well reviewed ones. After a bit of looking, including user comments, documentation and support, I decided to try the top one resulting from my Search - Aqua Mail (https://play.google.com/store/apps/details?id =org.kman.AquaMail&hl=en).

The almost full version is available free. It is limited to 2 email systems and has a small advertisement in the signature line. For $4.95, you can upgrade to the Pro version, which eliminates the limit of two systems, and the advertisement.

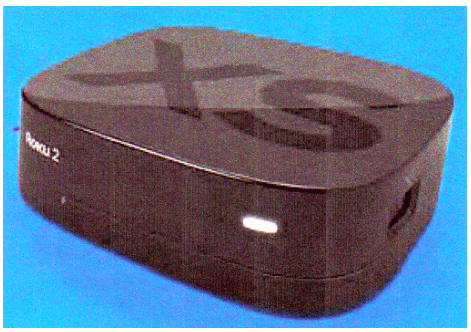
After about a week of use, I have found that it does everything I want. It installs and sets up easily, can POP3 or IMAP mail from existing servers, permits dynamically changing the sending email system (the feature I needed), and works intuitively.

One thing I really like is that it is useful almost immediately with good default settings, yet has a vast array of controls for when you get more confident and really want to tinker.

There is a very good video on Youtube (www.youtube.com/watch?v =U2vzuElEBXA) showing many of its features in operation on a Galaxy S3 phone. That video helped me decide to try this system. I am currently using the Pro version with 2 Hargray and 1 Gmail accounts.

By the way: Whenever I am in search of new hardware or software gadgets I usually check the reviews and comments on Amazon, and search for any videos on Youtube. These are both tremendous research tools.

Second by the way: The 4.8" Galaxy S3 phone in the video above looks awesome! Over the holidays I used a Galaxy Note II phone with a 5.5" screen, and can now see that my next phone will be large! A 6.1" version is rumored. These things, which seem to be an emerging cross breed between a phone and a tablet, are called Phablets.



Watching Movies in Hotels

We did a lot of traveling recently, and I noticed that frequently we are back in our hotel room by 8-9 pm, staring at a large flat screen TV with

dozens of channels of junk to watch. I thought to myself: "All those new hotel TVs have accessible HDMI ports. I should be able to plug my tablet into it and watch movies of my choice." As with many facets of entertainment video however, the technology part of the problem is the easy part. There are many other things that will impede your goal. To explore the topic, I started to try to find answers to the simple question: Given that I usually carry a tablet and a bit of electronics on a trip, how could I legally watch movies of my choice on the hotel TV?

When I work on a complex topic like this, I find it useful to assemble everything I know and don't know in some sort of organized table, and then try to fill in the blanks. The table on the next page - a work in progress, is my second draft attempt at this. In reviewing an earlier version via email and at an HHICC Geeks lunch, several methods that I had missed were suggested. Hopefully this early version of the table will be useful and stimulate additional data and ideas. While my focus was hotel TVs, many of the techniques below will also be useful in home setups. I hope to update this chart later in the year based on your inputs and new industry developments.

As I indicated, there is no easy solution, but there seem to be lots of interesting gadgets to watch. I'll plan to update this table later in the year.

* Some interesting devices and rumors have come out of the CES show. For example, the Panasonic DMP-MS10 and DMP-MST60 have Roku-like capabilities while being able to use Miracast, which lets Android mobile devices (some devices using Android 4.2 or higher), stream content directly to the box like Airplay. It is my estimate that Roku will not give up this market. [See following page for chart.]

Table 1 – Overview of Methods for Watching a Movie of Your Choice on a Hotel TV

Method	Comments
1. Pack a small DVD player to hook to hotel TV.	**Pros:** Easy and requires low preparation – just throw discs in suitcase at last minute. Low cost players start around $25. Simple. Independent of bad or no Wi-Fi connection at hotel or on a ship or airplane. **Cons:** Adds 1-3 pounds plus some bulk to suitcase.
2. Rip your own movie to memory and watch on tablet, or pipe from tablet to hotel TV.	**Pros:** No extra weight or bulk since tablet is on trip anyway. Should be legal under fair use of your own disc. Independent of bad or no Wi-Fi connection at hotel or on a ship or airplane. **Cons:** More time and pre-preparation steps before trip to decode and assemble selected DVD to memory. In an experiment run by Harold Hauer, using a 3.4 GHz Intel Core i7 Mac and Handbrake software, it took a total of 43 minutes to decode and move a 2 hour and 7 minute commercial DVD to his iPad 2. Unless tablet has HDMI output, additional hardware will be needed to get to TV.
3. Google Play or iTunes rental, etc.	**Pros:** 30 days from the time of rental to watch your movie, and 24 hours (in the US) or 48 hours (elsewhere) after you've started viewing to finish it. If pre-download, independent of bad or no Wi-Fi connection at hotel or on a ship or airplane. **Cons:** Must watch within 24 hours from start - a potential problem for long movies that you might want to watch over 2 nights. Unless tablet has HDMI output, additional hardware (i.e. Apple TV) will be needed to get to TV. Somewhat limited choices of movies.
4. Small portable DVD optical drive for tablet.	**Pros:** None. Small USB connected DVD drives available, BUT, see Cons below. **Cons:** Will not work for encrypted commercial movie DVD's per rules of the DVD Forum. (My guess is that the issue is a fear of piracy.) Thus, requires method 2 to decrypt. In that case, use of a memory stick or pre-load takes less bulk/weight than an optical drive.
5. Media Hub/Player (E.G. Samsung SE 208 BW, a DVD Player that WI-FI streams content to tablet or phone.)	**Pros:** Easy and requires low preparation – just throw discs in suitcase at last minute. Independent of bad or no Wi-Fi connection at hotel or on a ship or airplane. Software for Android and IOS available. **Cons:** Small, but adds weight and bulk to suitcase. Reported complex setup. WI-FI may not be useable in airplanes.
6. Roku or equivalent*	**Pros:** Independent of tablet and can stream from online services (see method 3 above) if reasonable speed WI-FI is available. Higher end Roku model can accept USB stick and hence also use method 2 above. **Cons:** Weight, Bulk

From the February 2013 issue of Island Computing*, newsletter of the Hilton Island Computer Club, FL.*

New Crop of Security Suites for 2014 - Review of Trend Micro 2014

by Ira Wilsker

It is that time of year when the major security software publishers start to release the new or updated versions of their security software. Under a "non disclosure agreement" I have had the opportunity to evaluate and test some of the pre-release or "beta" versions of a few of the 2014 suites, and found them generally improved over the previous 2013 dated versions, released last fall.

One of the first of the 2014 security families that has now been publically released is Trend Micro's Titanium Antivirus+, Titanium Internet Security, and Titanium Maximum Security. My personal preference in security software is for comprehensive security suites, rather than just the less expensive but traditional antivirus software; my rationale is that since viruses now only make up a small minority of security threats, traditional antivirus software is woefully inadequate in providing comprehensive protection from contemporary threats. For this reason, the first of the newly released 2014 security products that I installed and tested is Trend Micro Titanium Maximum Security 2014.

Since I currently had a valid software license for the 2013 version of Titanium Maximum 2013, I downloaded the 2014 version from the Trend Micro download website at downloadcenter.trendmicro.com and clicking on the link "Trend Micro Titanium Maximum Security 2014". The link opened another page with the download choices consisting of a 32-bit download, a 64-bit download, or a single download with both 32 and 64-bit downloads (this single download will automatically install the correct version for the computer). The single downloads were about 82mb in size.

Since I have a 64-bit system, I downloaded the 64-bit version, and then opened the file. The installation software first checked my computer for compatibility, and notified me that I had to uninstall my MalwareBytes before I could continue with the installation; Trend offered to perform the removal of the MalwareBytes, which I allowed. After the removal, it was required to reboot the computer, and then detected the 2013 version of Trend Micro Titanium Maximum Security, which it also offered (required) to be uninstalled, which it did quickly after I gave it the OK; another automatic reboot and the 2014 version installed itself in just a few minutes. What is interesting is that in 2013, the installation also required the removal of SuperAntiSpyware and WinPatrol, neither of which is impacted by the 2014 version. Just for interest, I reinstalled my MalwareBytes after the 2014 successfully installed, and I cannot find any apparent conflicts. The installation process detected my valid 2013 license key and by default activated the software with that key, giving full validation for the remaining balance of my license; it also offered the option to use a new activation key.

After the installation, the software immediately went online to download and install the latest updates, which only took a few seconds. A small window opened that said, "Do you own a Mac, Android Phone, or Android Tablet? Your subscription includes them as well." Since many of the Trend Micro Titanium Maximum packages are sold including three licenses, and the Premium Security package includes five licenses (I have the Premium package) I can also install the Windows version on my laptop computers, as well as an Android version on both of my Android devices. Since the security needs of Android devices is quite different from Windows needs, when installed on an Android device (phone or tablet), the Trend Micro for Android (downloaded for free from play.google.com and registered using the provided activation key) can be used to locate the device if it is lost or stolen, can identify mobile apps that may try to steal the users' data (identity theft), automatically provides a secure backup and restore service for the Android device, and could be used to remotely lock and wipe a stolen or lost device. While I am not currently a Mac user, the Mac version provides comprehensive security services designed explicitly for Mac systems. A nice feature of the three or five license packages is that they can be used for any number of devices in any combination (Windows, Android, Mac) up to the limit of the number of licenses.

Opening the "Main Console" and opening the "PC/Mobile" tab offers some of the many additional features

incorporated in the Maximum and Premium versions. The first icon opens the PC and Internet Security options; the second icon opens a comprehensive "System Tuner" that can be used to improve system performance, and the third icon can be used to create a bootable rescue disc that opens a browser window that walks the user through the process. According to Trend Micro, "Trend Micro Rescue Disk lets you use a CD, DVD, or USB drive to examine a computer without launching Microsoft Windows. It finds and removes persistent or difficult-to-clean security threats that can lurk deep within your operating system." Also on that same web page are a variety of other useful tools. These free tools include Trend Micro RootkitBuster which can detect, identify, and remove a type of malware called a "RootKit" which hides itself from traditional detection; Trend Micro Anti-Threat Toolkit (ATTK) with Cleanboot which identifies and destroys many of the difficult to remove threats, restoring and correcting affected registry entries; and a Ransomware Removal Tool that can detect and remove the very troubling "FBI Ransomware" and its many variants that hijack the computer until a ransom is paid to the hijackers claiming to be FBI agents.

The System Tuner included with the Maximum and premium versions can be used to clean junk files from the hard drive, freeing up valuable storage space; manages the startup process, which may decrease the time it takes to boot the computer; a system registry cleaner; an "Internet Privacy" feature that deletes browsing history, cookies, and other content that may be used to violate your personal privacy; and features to protect the user from cyber spies that want to track computer usage and instant messages.

Another tab on the main console opens the integral privacy feature that provides services different from the privacy services in the System Tuner. This utility incorporates a personal privacy feature that works with most social networking services, such as Facebook and Twitter. For example, Trend Micro installs a small window on the top of the Facebook window that monitors the privacy and security settings used on Facebook, and recommends changes to improve the privacy of the user.

Other tabs on the console include options for data protection, secure encryption of sensitive files, secure deletion of sensitive files, an effective and secure password manager (DirectPass), and SafeSync which allows the secure sharing of files across platforms including mobile devices. Families with young children may appreciate the comprehensive, but easy to configure, "Parental Controls" feature that allows the parents to control access to questionable websites, dangerous social networking services, and even a schedule that controls when the child can access the internet or the computer itself. The Maximum version also includes 5 GB of free, secure online storage for critical data files, while the Premium version includes 25 GB of free storage.

All of these frills are nice, and useful, but not the primary reason for having a security suite. What really counts is protection form malware and threats of all types. The 2013 and 2014 versions of Trend products have been tested and rated by several reputable security testing and evaluation services, and have scored the best or very high among the competitors. In the "NSS Labs 2013 – "Average Time to Block – Endpoint Protection Products Testing," TTrend Micro products are the fastest in protecting the user from new web threats, when compared to the likes of McAfee, Kaspersky, AVG, Sophos, and others. Another extremely common threat is Phishing, a sophisticated type of identity theft where a cyber crook tries to trick the user into revealing personal and financial information. In these NSS Labs 2013 tests (nsslabs .com/reports/2013-consumer-avepp-comparative-analysis-phishing-protection), "Trend Micro Titanium Security is #1 in detecting phishing threats, a leading cause of identity theft. It detects spam emails containing phishing scams that can trick you into revealing private personal information."

In terms of active malware protection, Trend Micro products protect the user from opening malicious websites that may be used for phishing or suspected of loading malware on to visitors' computers, as well as email and instant messaging based threats. Trend uses a continuously updated "Cloud Based" system of maintaining updated threat files, as well as automatically downloading frequent updates to users' computers. Trend's cloud claims to detect and block over 250 million threats per day that try to infect users, blocking these threats before they reach users' computers or other devices. Trend Micro also has a cloud based "Smart Protection Network" that processes over 16 billion requests for internet address (URL) inquiries,

potential email threats and file queries (suspicious files), analyzing over 15 terabytes of data every day. Trend Micro employs an international team of over 1200 security experts, in many different global time zones, whose job is "surveillance and prevention."

While there are many excellent commercial or free comprehensive security suites available, I have been very impressed by this 2014 version of Trend Micro Titanium Maximum (or Premium) Security.

Websites:

http://downloadcenter.trendmicro.com
https://www.nsslabs.com/reports/2013-consumer-avepp-comparative-analysis-phishing-protection
http://www.trendmicro.com/us/home/products/titanium/index.html #what-it-does

My PC Backup

Here's a great solution for backing up your files and keeping them backed up. You download an application (mypcbackup.exe) and install it. It will start to back up your documents as soon as the install is completed.

No action is required on your part. Not only are the files saved in the cloud, they are automatically backed up when changes are made. You have 10 GB of storage available, and it's free!

Society News

President's note:

When our scheduled speaker didn't turn up at our last meeting we extended Help's Half Hour. We discovered that there were people in the room who would appreciate a New Users Group and we initiated it right then. If you think that would be helpful to you by all means come to our next meeting.

Jan Rothfuss' Help's Half Hour notes will reappear when Dan has regained his health. We miss them all (Jan, Dan, and the notes ;).

–Steve Staub

The Lighter Side

Don't you wish when life is blah
and things just don't compute,
That all we really had to do
was stop and hit reboot?

Things would all turn out ok,
life could be so sweet
If we had those special keys
Ctrl, Alt, and Delete

Your boss is mad, your bills not paid,
your wife, well she's just mute.
Just stop and hit those wonderful keys
that make it all reboot.

You'd like to have another job
but you fear living in the street?

You solve it all and start a new,
Ctrl, Alt, and Delete.

I recently had a problem setting the video resolution on a new laptop.
Me: "It seems that the resolution is supposed to be 1900x1200. It's set to that, but it's not displaying right."
Tech Support: "Yes, that is 1900x1200."
Me: "No, I have my old computer up here, and it's also set to that resolution, and the icons are much smaller."
Tech Support: "Well, so what? Don't you want a bigger resolution?"
Me: "Um, no, a bigger resolution means that the icons get smaller. I think I should reinstall the drivers."
Tech Support: "No. How long have you been experiencing this problem?"
Me: "Since the computer started, remember?"
Tech Support: "Just on this startup?"
Me: "Yes, this is the only startup."
Tech Support: "OK, what did you change on the computer since the last startup?"
Me: "What? Nothing. Listen, this is a new comp. . . ."
Tech Support: "No, I mean, what have you done with your computer recently?"
Me: "I took it out of the box."
Tech Support: "Why was your computer in a box?"
... and a great gnashing of teeth was heard in the land.

**"I'm trying to be more active.
Which one burns more calories,
Twittering, Blogging or Googling?"**