Issue 199

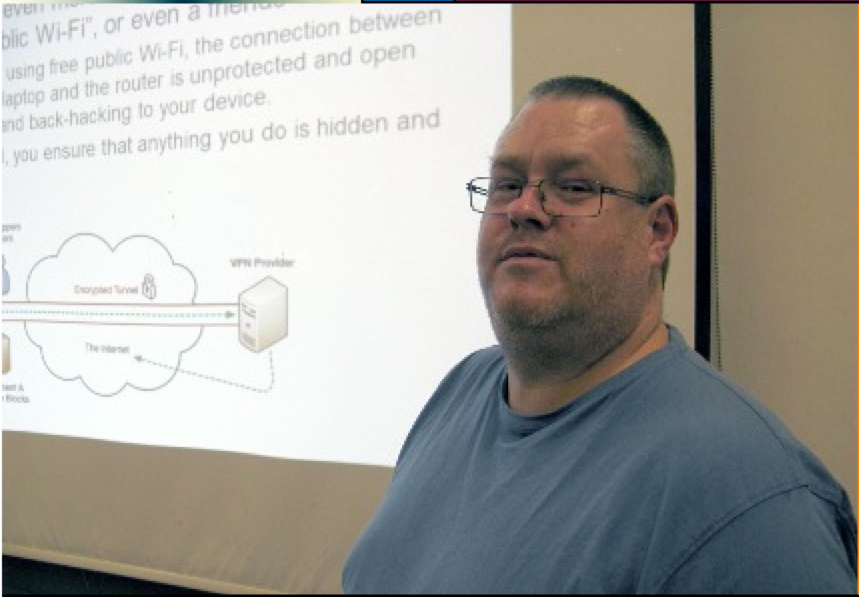
OCTOBER 2017

ISLE OF WIGHT PC USER GROUP

IWPCUG

HOT KEY

OCTOBER 2017


blic Wi-Fi", or even a friend
using free public Wi-Fi, the connection between
laptop and the router is unprotected and open
and back-hacking to your device.
, you ensure that anything you do is hidden and
VPN Provider
Encrypted Tunnel
The Internet

In September Jonathan Burt gave us a talk entitled "Security tweaks and what are the real risks?"

In this Issue

The Isle of Wight Personal Computer User Group

We welcome anyone who has an interest in computers and related technology and what you can do with them.
We are a group which seeks to exchange ideas and new information.
Membership is £12 per annum

Our meetings are normally held on the first Wednesday of each month at
The Riverside Centre, Newport from 7.30 to 9.30 pm
Visitors are always welcome.

A charge of £2 is made per meeting, which includes tea or coffee during the break.

If you would like to know more about us, you are most welcome to come along to one of our meetings, or you can contact one of our Committee Members listed on page 3.

The Club web site address is **www.iwpcug.org**
We also have an e-group discussion area on
Yahoo groups: **iwpcusers@yahoogroups.com.**
Details of how to join are on page 4.

FUTURE MEETINGS

Date	Subject	Speaker
4 October	**Multi-core Coding & Other Stories**	**Richard Burkill**
1 November	**TBA**	
6 December	**TBA**	

ISLE OF WIGHT PC USER GROUP COMMITTEE

Chairman : David Groom

Treasurer : Phil Rogers

Secretary : Susanne Bone

Membership and Database Secretary : Roger Skidmore

Committee Member : Steve Sutters

Committee Member : Soren Johanson

HotKey Editor : Bob Groom

Committee Member : Mike Hoar

Note:

Contact details removed prior to publishing to the internet.

Suggestions for new events, topics or speakers for talks are always welcome.
Please contact Steve Sutters, or any committee member, with your ideas.
If necessary we may be able to find a speaker for your subject.

Chairman's Report

Sadly our annual summer BBQ did not go ahead this year. Originally planned for the first week in August the weather forecast on the day before was not promising, so we decided to postpone the event until the following week. Then on the following week the forecast was again unfavourable and we cancelled the BBQ. Unfortunately those two Wednesdays were the only wet days in either of those two weeks!

The committee continue to meet frequently, our main task being to plan the speakers for the coming months, though this is becoming an increasingly difficult task as many of the pool of speakers from, which we used to draw, are no longer available. We are of course grateful to those speakers who do give up their time to plan a talk and then come along on the night. As you can see from the calendar on page 2 we currently have no speakers arranged for the next two meetings, but hopefully we will find someone to talk, so keep an eye on the web site and your emails.

We have included with this issue of HotKey a reminder of subscriptions due. It helps cut down on the administration if these are sent at the same time as the magazine.

David Groom

Joining the Yahoo Group

Send an email to: **iwpcusers-subscribe@yahoogroups.com** with "join" in the subject line.

All members are encouraged to join this group (it's free and private to club members) so you can keep in touch with events and join in with the discussions.

You can also keep in touch by regularly visiting **www.iwpcug.org**

How to Get a Server for Free

Last year I started to develop a new web site for myself, it was purely out of interest, and would never generate any money. On part of this web site I wanted to have a file which visitors to the site could download, and I wanted this file to be automatically created everyday. I have various web hosting accounts, so the obvious choice would have been to have the file created on one of those web servers. Unfortunately the program which generated the daily file was written in Java, and none of the web hosting accounts I use allow Java programs to be run.

I could run the Java program on my own server in my office, but I would have to remember to run it every day, and then to upload the file to the web server. This would be possible, but it would require me to turn that server on everyday, and if I were on holiday to leave the server running continuously - not something I wanted to do.

Having previously read up on the subject my next thought was that I needed a virtual private server ("VPS"). This is a virtual machine sold as a service by an Internet hosting service. A VPS runs its own copy of an operating system, and customers have superuser-level access to that operating system instance, so they can install almost any software that runs on that OS. Just what I needed! But last year the cheapest VPS I could find was about £15 (plus VAT) per month, or over £200 per year. So not really an option for generating the file for my hobby server.

The solution to my problem came from Amazon. Or more specifically Amazon Web Services ("AWS"). AWS are a range of cloud computing products available from Amazon - Amazon provide all the hardware and infrastructure, and anyone can rent some of this for their own use.

My first problem was that AWS has so many different products it was difficult to immediately know what I wanted, but after a little research it became clear I needed the Amazon Elastic Compute Cloud (Amazon EC2). Clicking on the pricing page I found the words "Amazon EC2 is free to try", Amazon would give me limited usage for 12 months for free. Specifically I could get 750 hours per month of a virtual machine with 1Gb of memory, running a 1Ghz processor, with a choice of operating systems which I could install. This would be enough for my requirements.

Setting up my EC2 instance was very straightforward, just a few clicks on a web form. Understanding how to use it was more complicated, but there is a lot of documentation on the AWS site, its just a case of ploughing through it. All commands are implemented on the command line in a terminal window (this is a server environment after all) running on your own a computer at home, so my familiarity with the Linux command line came in handy.

My AWS instance has been running without problems for over eight months, and in fact most of the time I have simply forgotten it is there. It does its job of producing one file every day, and then sending that to my web server. More importantly it allowed me to experiment with the use of a VPS to see if it suited my needs, and if I was able to understand how to use one, without incurring any costs.

My current problem is that in a few months I will be at the end of my twelve months free usage. It looks like if I keep my current EC2 instance going twenty four hours a day, every day, with AWS it will cost me in excess of £100 per year. It should be noted that Amazon don't force you to have the server running twenty four hours a day, you could start and stop it as your needs require, in which case you only get charged by the hour (it just happens that in my instance I needed the server to run continuously).

Things have moved on in a year, and now I can find a VPS priced at about £36 per year (from OVH), so AWS is more expensive, but likely to be more reliable. One option would be to stop the AWS instance so the server is not running (and therefore I don't get charged) but keep it as a backup in case a VPS I purchase elsewhere fails.

I said earlier that AWS has so many different products it was difficult to immediately know what I wanted, and I| choose the EC2 product. Even looking at the names of the other services confuses me! I have no idea have most of them do.

David Groom

Why can't we have the Internet of Nice Things?

Off-the-shelf, consumer home automation has fallen into a pretty standard pattern. You have a smart device (like a lightbulb or door lock) that talks to some kind of hub that you put on your network. It communicates with a cloud service owned by the device vendor, and you interface with that service via a mobile app. This provides an easy out-of-the-box experience and lets the vendor iterate on its service both in the cloud and on mobile; however, this model has a lot of weaknesses and is extremely limiting with what it can do.

This model depends on the cloud for some of its logic, a cloud you aren't paying for upkeep on, which means the economics are entirely based on selling more devices to keep up this cloud. It also means that internet disruptions now degrade your home. You may lose functions inside your house if any part of the path from your home to that cloud service is disrupted. Also, you are taking inbound commands from the internet-at-large that determine how your home functions. Although doing this securely is possible, it creates added risk. And when it's done poorly, you end up with things like the Mirai botnet, which disrupted large chunks of the internet in the United States last fall.

This model also depends on a mobile app, which means your choice of products might be dictated by your choice of mobile device. The kind of automation you can build is dictated by the vendor and what they expose in their mobile app. Having any real integration between different platforms is unlikely. For example, if opening your door triggered your lamps to turn on that would be nice but, more likely than not, your connected doors and connected lights are on entirely different ecosystems.

Why can't it be seamless?

One of the main reasons we have this pattern is that last-foot networking and device discovery are fragmented. There are real reasons for that. At first, we thought Wi-Fi everywhere might be a great idea, but Wi-Fi is terrible in crowded environments. Also, secure Wi-Fi assumes there is someone able to type a Wi-Fi password into every device coming onto the network. That works great for a mobile phone or a laptop, but poorly for a lightbulb. The various workarounds to make that possible include having the lightbulb run a Wi-Fi access point that you attach to. Wi-Fi is also power hungry compared to other technology choices, so it isn't suitable for sensors running on AA batteries. Further, most home routers are configured for no more than 250 devices, which becomes a real consideration when rolling out connected devices.

Alternatives include X10 RF, Zigbee, Z-Wave, and even Bluetooth. All of them have different tradeoffs for security, discoverability, range, power consumption, and networking. Almost all are better than Wi-Fi. Some will do mesh networking out of the box. Some have active acknowledgment of messages, which is extremely important for building automation systems on top of them. To make any of these things accessible to consumers, you need something that bridges them back to the home network, so you must have a hub.

At that point, the vendor's option is writing all the logic into the hub and hoping that consumers upgrade their hubs regularly—which they won't—or keeping as much logic someplace offsite that lets the vendor continue iterating and improving the platform. It all makes a ton of sense from the vendor's perspective. But it extremely limits what you can do with these devices, and honestly, it makes them less appealing.

Enter Home Assistant (https://home-assistant.io)

This is where Home Assistant comes into play. Home Assistant is an open source home automation hub that can be installed on a variety of devices—from full Linux systems to some network-attached storage (NAS) environments or even a Raspberry Pi. The project made great early decisions, such as writing in Python, which has made it easy for hundreds of people to add device support to the platform. The UI is based on Polymer, the Google library implementing the Web Components standard, so it looks clean and attractive out of the box. The internal state and event model is clean, which makes automating interactions between different components easy.

Out of the box, you get integrations with more than 700 different components, ranging from extremely popular platforms such as Hue, Nest, and Sonos, to a ton of platforms you've never heard of before. As much as possible, the project tries to auto-discover devices on your network and integrate them, using UPnP and other discovery protocols.

Automation in Home Assistant

To get a flavor of the kinds of automations you might have in Home Assistant, consider the following. I've got a screened porch that we use six months of the year as our dining room. I put Hue bulbs in the ceiling, have an Aeotec Z-Wave MultiSensor 6, and run my AV receiver's zone 2 for my outdoor speakers out there. I want the lights to turn on when people go into the porch at night, but not during the day, as that would be a pointless waste of energy. I also sometimes forget to turn off the stereo, so I would really like it if, when no one is out there, zone 2 would shut off as a courtesy to our neighbors.

The complexity of this scenario definitely strains the YAML model a bit, but bear with it, as this complicated example shows a number of things.

Automations are triggered by an event, but in my case, I've got two potential triggers: that the motion sensor is tripped, and that it's late enough to turn on the lights. As such, I need to look for either event, and check that other one is in the expected state. I must also check that the lights are currently off, so that if I've manually turned them on, this automation won't randomly change their color or brightness.

The automation calls a scene, which turns on the deck lights (controlled by a Z-Wave switch), and calls a script that uses a scene name embedded in the Hue controller to turn on the lights. That same Hue scene is exposed to my Hue's tap switches and mobile app, so Home Assistant acts like a tap on that scene in either situation. In the off-automation rule, you can see the shutdown of the lights, the switch, and the receiver.

Note that this automation is integrating devices made by five different manufacturers—the Philips Hue light bulbs/hub, the Z-Wave hub, the Z-Wave switch, the Z-Wave sensor, and the audio receiver—and talking over three different networks—Zigbee, Z-Wave, and Ethernet—into one consistent feel. It's all done in a format that I can commit into a Git repository, so that when I make a change, I can easily revert if it breaks my house (which is really critical, because home automation bugs are some of the hardest things to debug and diagnose).

The ecosystem

The Home Assistant community is vibrant and growing. The project does a release every two weeks and continues to gather contributors. Some of the challenges of complicated automation scenarios (like the one above) are being addressed by ecosystem projects like App Daemon, which let you write your automation code in Python. Because the Home Assistant daemon exposes the entire event and state structure as a web service, it's really easy to build these kinds of custom add-ons or even your own specialized UI for the environment.

If you are thinking about dipping your toes into the home automation space, make sure to check out the Home Assistant project. Putting open source at the heart of your home automation will let you build it at your pace, adapt over time, and ensure you have control over critical resources like your own home.

Sean Dague

The above is based on an article published under a CC=BY-SA licence at https://opensource.com/article/17/7/home-automation-primer

TreeSize

In the last edition of HotKey, in the article titled “Power Failures and Lessons Learned” I said that I was now using Acronis True Image to back up my system. It soon became apparent that even though I had only chosen to back up certain directories of my hard drive I was backing up an awful lot of data. I needed to find what was taking up all the space!

Using Windows Explorer you can click on any directory and find the size of all its files, but this would be time-consuming, there must be a better way. A quick search on the internet led me to TreeSize Free.

This free software can be started either form the start menu, or from the context menu of a folder or drive, and shows you the size of this folder, including its subfolders in an Explorer-like fashion. Large folders can be identified at a glance thanks to the gradient bar displayed in the background. All scan results can be drilled down to file level and filters, e.g. for files of a certain type, can be applied. See the image on the back cover of this issue.

The column view presents more detailed information for each file and folder. Here you will find the size or number of files as well as the last access date and the owner (and other useful facts).

Scan results can be broken down with the flexible filter feature. You can use the filters, for example, to find files of a certain type, such as temporary files, text files or images and use this information to clean up your hard disks.

Running this program on the whole of my user directory (see image on back page) identified that I had over 190,000 files in the AppData folder using 25Gb of data, and 36 files in a directory called VirtualBox VM’s using 20Gb of data. I could then quickly expand the tree for AppData, and I saw that the largest folder here was named “Android SDK”. Two years ago I had installed this but never used it, there certainly was no need to include this in my Acronis backup. However the Folder called “Microsoft Live Mail” had 128,007 files totalling 7.25Gb, these obviously did need to be backed up.

Overall this free program is very useful and I can recommend it to anyone who wants to know what is using the most space on their hard drive.

The TreeSize freeware program can be downloaded from this location:
www.jam-software.com/treesize_free/

David Groom

The Increasing Threat of Ransomware

Can you imagine a worse fate, digitally? A bad guy has taken control of your PC, Mac, or company network, and the only way to get it back and begin doing work again is to pay him. Except if you do, you may not get it back.

Welcome to the world of ransomware, which many experts today regard as the worst of the dangers on the Internet that a typical individual or small business has any reasonable likelihood of encountering.

Ransomware is increasing. Over the past two months the worldwide computing community has been the victim of two big ransomware attacks, dubbed WannaCry and Petya. The number of ransomware attacks jumped from 3.8 million in 2015 to 638 million in 2016, an increase of 167 times, according to Sonicwall, a security provider. More than 400 different types of ransomware exist, according to Intel Security, and this number is also increasing.

Ransomware has been around since 1989. It's becoming much more common because the bad guys are figuring out more effective ways to monetize it.

Individuals as well as organizations can fall victim of ransomware, with organizations typically getting hit by larger ransom demands. Organizations that have been victims include schools, city councils, and churches. Ransoms paid include $17,000, $8,500, and $2,300. The sum of
$300 is common for individuals.

With ransomware attacks no one seems immune, whether users of Microsoft Windows PCs, Macs, Linux, or other platforms. Because acknowledging an attack involves owning up to vulnerabilities or mistakes, it's believed that only a small fraction of them are reported.

But it's not all doom and gloom. You can take steps to prevent ransomware attacks, and you can take other steps now to recover later if you're attacked. None are guaranteed, but they can significantly reduce the risks.

* Practice safe computing. Ransomware is commonly introduced through email attachments, rogue websites that install software on your system without

your consent, "dark web" file- sharing services, or breaches in networks.

You should never click on an email attachment unless you know the sender, and you should be careful even if you do. If anything seems strange, phone the sender ensure he or she actually sent the attachment.
Clicking on such attachments can launch a ransomware program.

* Keep up to date. Older operating systems and programs are more vulnerable to attack. Enable automatic updates if available. With programs that don't offer this option, periodically check for updates, which can often be done through the Help menu.

* Use good security software. Top consumer security suites include Symantec's Norton Security (www.symantec.com) and Kaspersky Internet Security (usa.kaspersky.com/internet- security). Fee-based security suites are typically more robust than free tools, including those that come with operating systems such as Windows or Mac OS.

If you connect using public wi-fi at places such as coffee shops or airports, use virtual private network (VPN) software such as Hotspot Shield (www.hotspotshield.com) or TunnelBear (www.tunnelbear.com).

Use a password manager. Typing in the same password at multiple sites means that if one site is breached, all of the sites you visit, for you, are breached. Instead of using a different password for each site, you can use a password manager.

A password management program lets you use one password for it, then it fills in your passwords for sites you visit automatically and behind the scenes. Two recommended password managers are Lastpass
(www.lastpass.com) and KeePass (www.keepass.info).

* Dispense with extras if not needed. Two commonly mentioned vulnerabilities are Adobe Flash in your browser and macros in Microsoft Word. Google Chrome automatically turns off Adobe Flash, and you can turn it off manually. You can turn off macros through Microsoft Word's Trust Center.

* Back up critical files. Data, whether it's your family photos or your customer database, can be much more valuable than your hardware or software. The often repeated solution is to back up irreplaceable files.

Options include using a cloud backup service such as Mozy (www.mozy.com), a cloud storage service such as Dropbox (www.dropbox.com), an external hard drive, a USB flash drive, a rewritable optical disc, or a backup tape.

If you've been hit with a ransomware attack, sometimes the best recovery option is to start afresh. You simply wipe your hard drive clean, reinstall your operating system and programs, and restore your data from your most recent, usable backup. If everything works as planned, all you'll have lost is time.

The FBI and other government organizations around the world are trying to combat ransomware. In the meantime, you need to be vigilant.

First published in Purchase Area family Magazine
https://issuu.com/purchasefamilymag

The Car Hacker's Handbook - An Introduction

In 2014, Open Garages—a group of people interested in sharing and collaborating on vehicle security—released the first Car Hacker's Manual as course material for car hacking classes. The original book was designed to fit in a vehicle's glove box and to cover the basics of car hacking in a one- or two-day class on auto security. Little did we know how much interest there would be in that that first book: we had over 300,000 downloads in the first week. In fact, the book's popularity shut down our Internet service provider (twice!) and made them a bit unhappy with us. (It's okay, they forgave us, which is good because I love my small ISP. Hi SpeedSpan.net!)

The feedback from readers was mostly fantastic; most of the criticism had to do with the fact that the manual was too short and didn't go into enough detail. This book aims to address those complaints. The Car Hacker's Handbook goes into a lot more detail about car hacking and even covers some things that aren't directly related to security, like performance tuning and useful tools for understanding and working with vehicles.

Why Car Hacking Is Good for All of Us

If you're holding this book, you may already know why you'd want to hack cars. But just in case, here's a handy list detailing the benefits of car hacking:

Understanding How Your Vehicle Works

The automotive industry has churned out some amazing vehicles, with complicated electronics and computer systems, but it has released little information about what makes those systems work. Once you understand how a vehicle's network works and how it communicates within its own system and outside of it, you'll be better able to diagnose and troubleshoot problems.

Working on Your Vehicle's Electrical Systems

As vehicles have evolved, they've become less mechanical and more electronic. Unfortunately, automotive electronics systems are typically closed off to all but the dealership mechanics. While dealerships have access to more information than you as an individual can typically get, the auto manufacturers themselves outsource parts and require proprietary tools to diagnose problems. Learning how your vehicle's electronics work can help you bypass this barrier.

Modifying Your Vehicle

Understanding how vehicles communicate can lead to better modifications, like improved fuel consumption and use of third-party replacement parts. Once you understand the communication system, you can seamlessly integrate other systems into your vehicle, like an additional display to show performance or a third-party component that integrates just as well as the factory default.

Discovering Undocumented Features

Sometimes vehicles are equipped with features that are undocumented or simply disabled. Discovering undocumented or disabled features and utilizing them lets you use your vehicle to its fullest potential. For example, the vehicle may have an undocumented "valet mode" that allows you to put your car in a restricted mode before handing over the keys to a valet.

Validating the Security of Your Vehicle

As of this writing, vehicle safety guidelines don't address malicious electronic threats. While vehicles are susceptible to the same malware as your desktop, automakers aren't required to audit the security of a vehicle's electronics. This situation is simply unacceptable: we drive our families and friends around in these vehicles, and every one of us needs to know that our vehicles are as safe as can be. If you learn how to hack your car, you'll know where your vehicle is vulnerable so that you can take precautions and be a better advocate for higher safety standards.

Helping the Auto Industry

The auto industry can benefit from the knowledge contained in this book as well. This book presents guidelines for identifying threats as well as modern techniques to circumvent current protections. In addition to helping you design your security practice, this book offers guidance to researchers in how to communicate their findings.

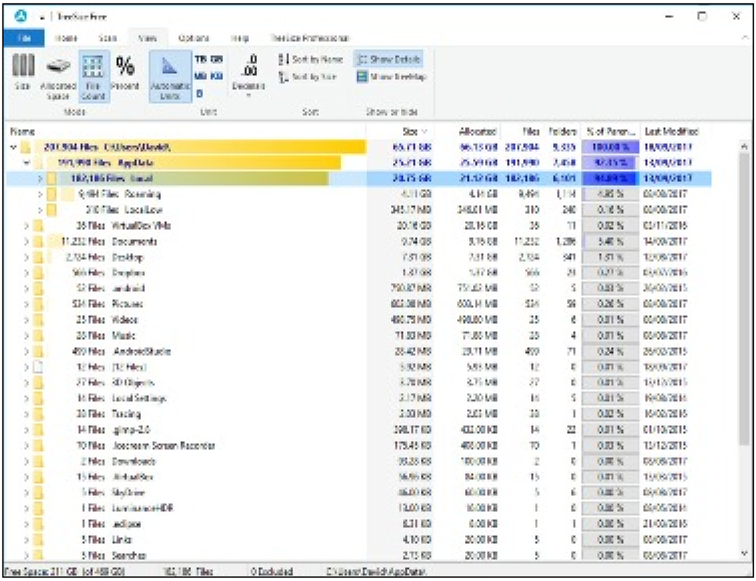
Today's vehicles are more electronic than ever. In a report in IEEE Spectrum titled "This Car Runs on Code," author Robert N. Charette notes that as of 2009 vehicles have typically been built with over 100 microprocessors, 50 electronic control units, 5 miles of wiring, and 100 million lines of code. Engineers at Toyota joke that the only reason they put wheels on a vehicle is to keep the computer from scraping the ground. As computer systems become more integral to vehicles, performing security reviews becomes more important and complex.

WARNING

Car hacking should not be taken casually. Playing with your vehicle's network, wireless connections, onboard computers, or other electronics can damage or disable it. Be very careful when experimenting with any of the techniques in this book and keep safety as an overriding concern. As you might imagine, neither the author nor the publisher of this book will be held accountable for any damage to your vehicle.

The above is the introduction from the book "The Car Hackers Handbook" By Craig Smith, details of how to read or download the full book can be found at http://opengarages.org/handbook/

A photo of Ron Keeler who gave us a talk in July entitled "Selling on Ebay"



Name	Size	Allocated	Files	Folders	% of Paren...	Last Modified
207,904 Files C:\Users\David\	65.71 GB	66.15 GB	207,904	9,335	100.00 %	18/09/2017
191,990 Files AppData	25.21 GB	25.59 GB	191,990	7,458	92.75 %	13/09/2017
182,186 Files Local	23.75 GB	21.12 GB	182,186	6,101	93.89 %	13/09/2017
9,494 Files Roaming	4.11 GB	4.16 GB	9,494	1,114	4.85 %	03/09/2017
310 Files LocalLow	345.17 MB	348.01 MB	310	240	0.78 %	03/09/2017
38 Files VirtualBox VMs	20.16 GB	20.16 GB	38	11	0.02 %	03/11/2016
11,232 Files Documents	9.74 GB	9.15 GB	11,232	1,296	5.40 %	14/09/2017
2,734 Files Desktop	7.51 GB	7.51 GB	2,734	541	1.31 %	12/09/2017
566 Files Dropbox	1.67 GB	1.67 GB	566	28	0.27 %	03/07/2016
52 Files .android	750.87 MB	751.22 MB	52	5	0.03 %	26/03/2015
534 Files Pictures	602.38 MB	600.14 MB	534	59	0.26 %	03/09/2017
23 Files Videos	490.75 MB	490.80 MB	23	6	0.01 %	03/09/2017
20 Files Music	71.83 MB	71.86 MB	23	4	0.01 %	03/09/2017
409 Files AndroidStudio	28.42 MB	28.71 MB	409	71	0.24 %	26/02/2015
12 Files [12 Files]	5.92 MB	5.93 MB	12	0	0.01 %	19/09/2017
27 Files 3D Objects	4.70 MB	4.75 MB	27	6	0.01 %	13/12/2015
16 Files Local Settings	2.17 MB	2.20 MB	16	5	0.01 %	16/08/2016
33 Files Tracing	2.20 MB	2.23 MB	33	1	0.02 %	10/02/2016
14 Files .gimp-2.8	398.17 KB	432.00 KB	14	22	0.01 %	01/10/2015
70 Files Icecream Screen Recorder	179.45 KB	400.00 KB	70	1	0.03 %	13/12/2015
2 Files Downloads	99.26 KB	100.00 KB	2	0	0.00 %	03/09/2017
15 Files .VirtualBox	56.66 KB	84.00 KB	15	0	0.01 %	13/06/2015
5 Files SkyDrive	46.00 KB	60.00 KB	5	6	0.00 %	03/09/2017
1 Files LuminanceHDR	13.00 KB	16.00 KB	1	0	0.00 %	03/05/2016
1 Files .eclipse	6.31 KB	8.00 KB	1	1	0.00 %	21/03/2016
5 Files Links	4.10 KB	20.00 KB	5	0	0.00 %	03/09/2017
5 Files Searches	2.13 KB	20.00 KB	5	0	0.00 %	03/09/2017

Free Space: 211 GB (of 459 GB) 182,186 Files 0 Excluded C:\Users\David\AppData\

The TreeSize program quickly identifies where hard disk space is being used. See article on page 10.

We try to publish HOTKEY quarterly in April, July, October and January
This edition was produced using Serif PagePlus X9
and printed by Island Digital Printers, East Street, Ryde.

No responsibility can be accepted with respect to any advice or suggestions in this journal, and the views expressed are those of the contributors.