**John Loop <pccitizen@gmail.com>**

# John Loops' 8-1-2024 "imonitorg/iotsnoop" newsletter

**John D Loop** <jdloop@imonitorg.com> Mon, Jul 22, 2024 at 7:17 PM
To: "pccitizen@gmail.com" <pccitizen@gmail.com>

Dear imonitor[g] users, potential users, former users, and interested parties: [and NOW potential iotsnoop users!]

Apologies if you do not want to receive this newsletter, sent 3,4 times per year [just reply to remove your address]. I have collected email addresses from some of my friends in hopes you might be interested.

*Summary for those of you new to this newsletter:**

I am working on a project to perform Internet/Local Network/IOT monitoring, using a small device [raspberry pi3B, pi3B+ or pi4B] placed on the network, along with custom scripts to perform this service. Trial pis were deployed to 25+ partners across the country representing many different access technologies and ISPs. As of 2024 I now have Virtual Machine [VirtualBox] images, so you do not even need a separate pi device! Following the "trial" with my partners, I created a "generic" version of the pi which is completely standalone -there is no cloud server which you must access to collect your info- it is all on the pi webserver, accessed by browsing to the pi from your local network! Download an image for a microSD card [you can get it from me if you want], plug it into your pi3B, 3B+, or 4B, connect the ethernet and learn all about your networks. It comes up running. Emphasizing again: There is no cloud connection used! You can configure a daily email status report using your gmail account as a relay. I posted these generic images on sourceforge.net.

/*As of Aug 2024*/, I have completed the initial work on an extension of imonitorg, called "IOT [The Internet of Things] monitoring" and I call this "iotsnoop." It will require a raspberry pi 4B. "Iotsnoop" also contains the previous "imonitorg" functionality! The pi3B, 3B+, ova, only contain the imonitorg function.

## 8-1-2024 Newsletter topics

## 1. IOT "snooping" work

The advances in Internet technology and devices is truly mind boggling. We have absolutely no idea where this is going, especially with "AI" capabilities. What is also interesting/concerning is the explosion in data/AI centers around the world by the world's tech giants. They are even buying up power plants. Every OS is incorporating an "AI" assistant, which will need the cloud power to pull this off. More and more stuff is moving to the cloud.

A MOST dangerous aspects of this AI/cloud Internet blitz continues to be the IOT gadgets you put in your home. These IOT gadgets will gradually be upgraded to increasingly leverage the AI/cloud, and you have almost no clue/ control of what they are doing. The first line of defense we have is to put all these IOT gadgets on their separate network, isolated from your main PCs, phones. Most routers have a "guest" network available to accomplish this.

To address this concern I have been working on additions to the "imonitorg" project, deciding to transition to a raspberry pi4 because of the added capability needed. This is "iotsnoop" and it allows you to use the pi4 as a guest wifi "access point" on your network to terminate all the IOT gadgets. [It has its own wifi SSID/key, just like other wifi APNs.] The added functions on the pi4 gobble up the packets originating from the IOT devices and analyzes them to monitor the IOT network, much as imonitorg monitors your Internet/home network.

The characteristics of "iotsnoop" are as follows:

1. The wifi to which your IOT connects is purposely limited to 802.11g -50Mb/s. [do not let your IOT gobble up all your bandwidth!]

2. All IOT DNS queries are captured for interrogation -this is a main information reservoir about what the IOT gadgets are doing.

3. All packets are captured using up to a 2GB storage buffer [representing avg about 8Mbs rcv/tmt over the hour] in a round robin fashion on hourly boundaries. Each hour the packets are interrogated for DNS/hosts/TCP/UDP info, and

statistics are listed and plotted. Attachment 1 is a snapshot of the overall IOT stats plot. Attachment 2 is a screenshot of this webpage hosted on the pi4, which allows for more detailed interrogation. ***My next work on iotsnoop will enable lifting the communications details of a selected IOT for the previous hour using the wireshark "statistics" which will let you actually see what the IOT was "doing" the last hour, in addition to just monitoring its overall network activity. This will show IP addresses, names, ports and protocols. Maybe I can even submit this to an AI for interpretation.. So much power can be garnered using these tools! Should be neat!!***

4. A 32 bit raspberry pi4 is used, with a recommended min of 4GB RAM, and must be ethernet-attached to your router/switch. The pi4 wifi is put in guest APN mode to enroll your IOT gadgets. You login your IOT gadgets to iotsnoop SSID just like to your regular wifi network.

5. The "iotsnoop" functionality is ***in addition*** to the "imonitorg" functionality provided on previous pi3B, pi3B+, ovas! pi4B has it all!

6. I am restricting this application to a "generic" capability and not providing a "trial subscriber" capability. There is no connection to my server! We can turn the pi4B into a trial subscriber if you wish by exchanging keys and setting a few parameters.

7. Go to https://iotsnoop.com for information and a sourceforge link for the raspberry pi4 image to download.

8. If you feel challenged about all this, just ask me -I will send you an imaged SDcard and order info for a pi4.

9. I have attached two images. The first is the overall IOT statistics plot, which updates hourly. In my own IOT network, I have about 20 gadgets, including a Fire TV. The second pdf shows the main web subpage [hosted on the raspbery pi] with all IOT stats and the ability to query the recorded data. You can even command a plot showing IOT destinations. All this information should help you understand what is going on with your IOT gadgets

10. The present implementation of iotsnoop is passive -you must interpret the data. I hope to add some intelligence and configuration to watch/alert for questionable activities.

PLEASE let me know of suggestions. Needless to say, I am "desperate" for testers for the gadget. Please join our club!

## *some other topics encountered this summer>*

### 2. Cellular broadband Internet access -offered in some parts of country by T-mobile, Verizon, ATT

Two trial pis - pi14 and pi9 are using cellular broadband - the subscriber's Internet access is cellular. It is becoming increasingly apparent that traditional layer 3 monitoring of the cellular network [pings/traceroutes] is becoming more difficult. The cellular broadband is it's own network and you will need layer 2 tools to monitor. pi9's network does not even process TTL flags to enable tracerouting. Pings are not returned by any router in the cellular infrastructure. This means all your normal layer 3 tools such as ping/traceroute may not help you troubleshoot problems. If anybody has information which can help with cellular broadband, let me know.

### 3. Mass migration to the cloud

With AI features being silently incorporated into PCs like Windows recall and Apple's Spotlight, more and more invisible cloud functions are becoming integral to our PCs. Windows even discourages/obfuscates local login now, trying to get you to live with the OneDrive login only. I am less familiar with Apple icloud. ChromeOS is almost totally cloud based. Google of course has their own cloud infrastructure which runs behind your gmail login.

Soon it may be impossible to access your PC if you don't have an Internet connection? "All your machines our ours." Just look at what happened with the crowdstrike disaster last week. Enterprise windows PCs were not even able to boot since they depended on a crowdstrike kernel file -which was botched!

My approach with the generic pi3B, 3B+ and pi4B is to provide all collected information directly on the pi - hosted on a web server running on the pi. You simply browse to your pi's IP address to access all the information. There is no cloud requirement, like with all existing IOT gadgets I am familiar with.

### 4. Passwords managers and the cloud, passkeys

Many of you no doubt use password managers for all your passwords/important data.  LastPass, bitwarden, 1password etc are all cloud based, multiplatform, allowing you to sync across PCs/OSs.  KeePassXC is the last holdout running without integral cloud backup.  I am holding out with KeePassXC and keeping all my secrets off the cloud, tho I have a simpler situation of not having to sync across multiple PCs/sites.

And then we have "Passkeys" which eliminates passwords for web logins!  It uses private/public keys for web servers that support it, but which has questionable cross platform support [how do you get those keys between your PC and your Apple or your cloud manager?] to negate the necessity of mountains of different passkeys for your websites]. And now you get to worry about private keys.  These are "passwords" which are -of necessity- managed by you PC.

The cloud basis of all these password managers can be risky.  Just look what happened to LastPass last year!  If the [cloud] servers get compromised, you are in serious trouble.  Cloud servers are getting compromised/hacked routinely.

### 5. Separation into the universes of Microsoft/Apple/Linux/Google/Amazon.  East/West

The world seems to be transitioning into separate technical universes and they rarely interoperate except at the Internet level.  My knowledge emphasis has always been on networking and Linux, and my knowledge of Windows/ Apple continues to deteriorate.  I feel lost at a Windows screen anymore! At least there is a recognizable command line in MACos.  And the world now seems to be separating into East and West, and maybe not even operating at the Internet level -at least the firewalling/filtering at the border is aggressive.  So much for the desire of global world order.

### 6. AI prognosis/search

Have you noticed how unusable google search is becoming?  It was always necessary to parse results, but now you have to wade thru other stuff. Personally I have transitioned to chatgpt/gemini and just ask as specific a question as I can, sometimes pestering it to come up with better answers, cross referencing different AIs.  We have silently transitioned from search and parse for our answers to asking specific questions of an AI and getting an answer, all within the space of a year!  No more manuals to dig thru, no need for simple coding!  There will be a massive data center on every corner to handle this new use.  So much for saving the planet from CO2.

I have no clue where this technology will take us, and the rest of the world doesn't either it seems.

John

Previous newsletter:  https://imonitorg.com/3-17-2024Newsletter.pdf

Main website:  https://imonitorg.com

**2 attachments**

**iotplot.png**
32K

**iothostinfo.pdf**
317K