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

John Loops' 4-1-2025 "imonitorg/iotsnoop" news: IOT monitoring raspberry pi4 APN - connect to your home router and sub your IOT to watch them -examples!

1 message

John D Loop <jdloop@imonitorg.com> Thu, Mar 27, 2025 at 1:35 PM
To: "pccitizen@gmail.com" <pccitizen@gmail.com>

Youtube intro to imonitorg and iotsnoop: https://youtu.be/v-NOPoMh860

Imonitorg/iotsnoop information: https://imonitorg.com

Dear imonitor[g]*/iotsnoop users, potential users, former users, and interested parties:*

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 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 your 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 2025 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 the iotsnoop pi4 image on sourceforge.net. The others are on my google drive.

As of 3-1-2025 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, images only contain the imonitorg function.

"Iotsnoop" has been undergoing QA for some months now, checking for quirks/bugs/ failures/inconsisencies/nonsense, and it has reached an "interim" stable point.

I have actually made no changes for a month! And I use it for all my wifi.
This 4-1-2025 newsletter recapitulates the work and updates it status and introduces
the next level of work./

4-1-2025 newsletter

The last few months I have concentrated on working out bugs and inconsistencies in the iotsnoop pi4 application. I have especially cleaned up the section which enables extraction of IOT connection information -for a specific IOT device. This allows you to specify one of your IOT devices, and the scripts will extract its packets from the last hour and display statistics about IP addesses, URLs and ports used. It is also possible to display a map of the URLs the IOT visits.

There are two main index pages for the imonitorg/iotsnoop pi4 application:

The home index page, accessed by browsing to the IP address of your iotsnoop pi on your home network [this is http, so you will have to except the location in your browser. It is safe, it is on your home network]
--links for all main pages for the imonitorg and iotsnoop functions
--the previous "imonitorg" function provided in all previous pis is available on the pi4 iotsnoop -except for pihole and wifi stats.
--two separate plots, representing the imonitorg near real time data about pings, plus a rotating plot showing IOT statistics
--quick data showing ping and host stats for your home network and the IOT network
--links for further info: configuration, management, further stats on local/IOT network.

The second main page -iotsnoop functions- is accessed by the link on the above index page: "MAIN IOT" This consists of 5 sections:
--status and alerts for the iotsnoop functions
--overall stats, DNS queries, packet counts per IOT
--IOT DHCP lease table and archive
--Last hour IOT traffic query facility, including -selectable- map of IOT URL visits
--miscellaneous data, such as off network access, non-DHCP IPs

I purposely limit the IOT network to 802.11g 2.4GHz wifi which has a max bandwidth of 50+Mb/s. I do this to throttle the IOT and provide for greater range [5GHz wifi has less range]. ***Why would you allow your IOT devices to monopolize your Internet bandwidth!*** You can always use a wifi extender/mesh routers to extend the range and allow for the use of 5GHz, tho the connection to the pi4 is only 2.4GHz. In addition, I have disabled ipv6 on the IOT. The IOT SSID is "iotsnoopg" and the password is "iotsnoop." You connect the pi4 via ethernet to your router, or a downstream switch, and subscribe your IOT device to the "iotsnoopg" APN just like you do with any wifi device to your home wifi [hopefully guest network]. The iotsnoop acts exactly like your home router in providing a "guest" network which is isolated from your home network. The IOT devices are NAT'd to your pi4 address, and thus not reachable from your home network. You can however browse to the pi4 home index page [on the ethernet side of the pi4] and perform a lot of data extraction on the IOT activity. This is not possible if you use the wifi on your router [except for very advanced routers].

I have been running three pi4 iotsnoop devices on my home network, including one with typically 12 IOT devices, including my Roku and my Amazon FireTV. It is not recommended that you place streaming devices like these on the iotsnoop, but I do this to stress them. They do readily support non 4K streaming devices. I recommend the 4GB or 8GB version of the 32bit pi4, but a 1GB pi4 seems to suffice for normal IOT devices which don't stream. 4K streaming which you will encounter occasionally will saturate the iotsnoop after 30 min or so. The iotsnoop does alert for this, and seems to recover successfully.

I have been experimenting with investigating the activity of some of my IOT devices using the extraction panel. If you run a streaming device like your roku and extract the activity over the last hour, it may take 15-30 minutes to extract and then display the data. Non streaming devices will take much less time, maybe 5-10 minutes. The extraction action uses tshark [command line wireshark] to extract the IOT specific data from the complete tshark file captured and saved over the last hour. The extraction lists all the IP/port activity, the DNS activity and the URL visits by the IOT. It is also possible to display a map of the IOT URL visits, tho this may not be as useful, but it does show the worldwide location of the URL. These are typically just CDNs or cloud appearances of the URLs, but it

is occasionally revealing.

I have found it interesting to use the "URL visit list" for a specific IOT and submit this to an online AI such as chatgpt or grok. [I provide a link on the IOT page for the URL visit file], or you can just copy/paste it from the display]. They are very good about describing exactly the activity, and usually ID amazon/etc specific sites and their purposes. It is very interesting. I have attached three files where I have done this. I used both chatgpt and grok.

1. My FireTV actively tuned, probably to Foxnews
2. My Amazon alexa -note the connections [and the map] to Bahrain, Indonesia and Mexico. grok says these are just load balancing URLs
3. My Samsung android tablet

I wish there some way to attach more intelligence to the iotsnoop function, and I am thinking up all kinds of possibilities. Any ideas are welcome! The pi4 does not seem to be stressed at all by this packet capture [and NAT] function, especially if not encountering streaming. Right now, I am operating it as "collect for an hour, then analyze for the last hour" while collecting for the present hour. The IOT analysis section is done in paralled with this, using tshark again to extract data. I could probably shift some functions to "real time" by interrogating the active packet capture file rather than the "last hour" file. ***What patterns could I check for in the packet captures?*** I am capturing ALL IP packets on the IOT interface. It would probably be possible to trigger on data patterns in the packets, but this is probably not that useful since most al connections use SSL. The pi4 certainly does not have visibility inside the SSL packets. Nevertheless the "meta data" can be very revealing.

I do see occasional non DHCP activity which is not explained. I think it is all the amazon devices discovering and talking amongst themselves, but have not quantified it yet. Slightly annoying and SNEAKY that they are not using assigned addresses!!!

I only have about 20 IOT devices on my home and none of them is particularly interesting.

I would love some of my friends who have literally hundreds of IOT devices to try this out and provide further guidance and ideas.

pi4 images are provided on sourceforge or on my google drive. Or ask me and I can provide a microSD card which will come up running! All you have to do is authenticate to the "iotsnoopg" SSID [password iotsnoop] the same way you do it for your router. ***I can also actually provide a pi4 to somebody who has a particularly rich IOT network, and is willing to give me remote ssh access [like the original pi subscribers] so I can interrogate these further!*** Let me know. All you have to do is plug it into your router/switch and switch some of your IOT to the iotsnoopg SSID -and then, after waiting an hour or more, browse to the pi4 index page at its IP address. It is important to remember that imonitorg/iotsnoop is a longer term monitoring device, and hours, days, and weeks are necessary to accumulate interesting info.

Many thanks to my existing "subscribers" who have supported me in this imonitorg work!! I am eternally grateful.

John Loop

Previous 11-2024 newsletter:

```
*     11-20-2024 Newsletter topics *

      1. IOT "snooping" work  raspberry pi4 image/manual links available at imonitorg.com

--check the three attachments for a quick peek at the iotsnoop capabilities...
```

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" pi4 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!]. It uses the 2GHz 802.11g band because this frequency can reach further, and because the transmitter in the pi4 is less powerful than in normal routers. Ideally, you can use a wifi extender with the pi4, and can even allow its use of the 5GHz band using this extender on the same iotsnoop SSID -"iotsnoopg."

2. All IOT DNS queries are captured for interrogation -this is a main information reservoir about what Internet connections IOT are performing.

3. All packets are captured using up to a 2GB storage buffer [representing avg about 6Mbs 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 iotsnoop index page, showing IOT stats plot, plus overall info and links, including imonitorg info. Attachment 2 is a screenshot of iothost detail showing lots of detail and allowing for interrogation of DNS/contact map, which allows for more detailed interrogation. Attachment 3 is a closer look at the IOT activity plot -hourly points of varying IOT activity.

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 APN mode to allow logging your IOT gadgets. Login your IOT gadgets to iotsnoopg SSID APN just like to your regular wifi network. In fact, if you don't put streaming devices on the IOT APN [like your Fire and Roku TVs], a 1GB RAM pi4 will perform quite well for dozens of IOTs.

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!
However, 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 three images. The first is the IOT index page, including the IOT statistics plot,
which updates hourly. In my own IOT network, I have varied the composition from
10-20 gadgets, and have even added my Fire and Roku TVs to stress its
performance. The second pdf shows the main web subpage [hosted on the pi4 raspberry
pi] with all IOT stats and the ability to query the recorded data. You can even
request a map showing IOT targets. 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.

11. The latest version of iotsnoop adds a plot of the number of IOT devices, as
well as an archive of all the IOT gadgets that have appeared on the APN [all the
leased DHCP addresses]. "Anomalies" are reported, such as the "illegal" use of
IP addresses [surprising!] and off-network access to the IOT APN. The last hour
pcap is always available for independent investigation using wireshark on your
main PC. The IOT DHCP lease time is reduced to 1 hour to more accurately assess
IOT presence.

12. The next version of iotsnoop will incorporate an mqtt broker server in the
pi4 and an mqtt client [meant for your android or iphone] to allow it to receive
info and alerts from the iotsnoop pi. This will be a new venture for me into
IOT and qtt and phone apps!! [all help appreciated]. Till now, all information
was retrieved via a web client to the web server on the pi4.

13. I will be making a short youtube explanatory "film" to explain the
essentials of imonitorg/iotsnoop. The link is https://youtu.be/v-NOPoMh860
The initial attempt may not be very "professional" but I will work to improve it, and
add other shorts to explain email, other topics. T

The draft youtube script is attachment 4 as a pdf

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

As always I am eternally grateful to those of my original trial subscribers. We
still have a network of imonitorg users and I continue to monitor their performance, and we have occasional discussions about all
kinds of networking issues!

John Loop

https://johnloop.com
https://imonitorg.com Network Performance monitoring
https://iotsnoop.com wifi IOT monitoring
Links for pi3B, 3B+, 4B images are on imonitorg.com
minute-by-minute iot activity plot available on iotsnoop pi4

---

3 attachments

FireTVIOTreport.pdf
98K

AlexaURLmapchatgpt.pdf
219K

SamsungTabURLtrack.pdf
53K