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

John Loop's 2-1-2026 "imonitorg/iotsnoop" news: network/IOT monitoring using raspberry pi - NO CLOUD account!!

1 message

John D Loop <jdloop@imonitorg.com>
To: "pccitizen@gmail.com" <pccitizen@gmail.com>

Mon, Feb 2, 2026 at 7:55 AM

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

Apologies if you do not want to receive this newsletter, sent 2,3 times per year [just reply and ask me to remove your address]. I have collected email addresses of friends in hopes you might be interested.

Please forward to friends whom you think might be interested! Thanks!

*****imonitorg/iotsnoop Project Summary:**   --> 2-1-2026 newsletter below***

I am working on a project to perform Internet/Local Network/IOT monitoring, using a small dedicated device [raspberry pi3B, pi3B+ or pi4B] placed on your network, to perform this service. Trial pis were deployed to 25+ partners across the country representing many different access technologies and ISPs. Following the "trial" with my partners, in 2022 I created a "generic" version of the pi which is completely standalone -No Cloud Account needed. 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 for the generic! You can access stats via a browser on your network pointed to the pi, and/or configure a daily email status report using your gmail account as a relay.

As of 2-1-2026 I have completed the work on an extension of the original imonitorg, called "IOT [The Internet of Things] monitoring" and I call this "iotsnoop." It will require a raspberry pi 4B ethernet-connected to your router. "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/inconsisiencies/nonsense, and it has reached a "finished" point. I have actually made no changes for a month! I use it for all my IOT devices [and other wifi],

about 20 in my house so far.

This 2-1-2026 newsletter updates iotsnoop status.

2-1-2026 newsletter [including attached AI interpretations of data, web screenshots of interface]

It has been a busy 4+ months. I started "iotsnoop" in Jan 2024 using a pi4b instead of a pi3b, and I have been challenged mightily. Work on the previous "imonitor[g]" extended 5 years, but this was on and off. Iotsnoop has been a full time project [well -for a retired person!] for 2 years. It is noteworthy that chatgpt, gemini and grok have come of age in these 2 years and have helped me in crafting scripts I needed to do the IOT snooping. My challenge was to prompt VERY specifically what I wanted and ask for the bash/perl/python scripts. The trick is specific prompting and verifying. The capabilities of these AI systems is astonishing! Syntax problems are no more at the very least!!!

I think I have reached a "semi" finished state with iotsnoop [imonitorg is "finished" and I am not actively working on it. It is INCLUDED in the iotsnoop pi4!]. There were earlier "finished" states, but I kept thinking of things to add, and was challenged in the architecture and coding. The challenge of the last 4 months has been the "real time" capture and analysis of a selected IOT, extending the interrogation capabilities for IOTs on my network.

There have been several capability extensions since the last benchmark late summer 2025:

1. Tshark [terminal wireshark program used to capture network traffic] is changed to capture only the first 128 packet bytes ["MED" mode] instead of the entire packet ["MAX" mode]. The pi4 sits in the middle of the data path and cannot decrypt the largely TSL-encrypted packets in any case [no "real" snooping]. All the needed info is in the first 128/64 bytes of the packet! Even streaming is pretty reliable now, HD or 4K, tho I still don't recommend doing streaming on iotsnoop. You can still put iotsnoop in "MAX [full packet capture]" mode still, but I don't see the advantage and unless you setup a "man in the middle." But getting the keys out of the IOTs I have no clue how to do -necesary to decrypt the traffic.

You don't want the IOT gadgets stealing your bandwidth -esp if they are doing malicious bot activity! The IOT APN of the iotsnoop is restricted to 2.4GHz and probably 35Mbs max. 2.4GHz is used instead of 5GHz because it works for longer ranges and thru obstructions better, and the pi4 used as an APN is weak compared to most routers. You would need to use a wifi extender for much bigger than small/house/room coverage. You can configure the extender to use 5GHz on that APN even if it is 2.4GHz.

IPv6 is also disabled for the IOT devices. IPv6 would be difficult to get to work behind this "second" router. The pi4 itself is fully ipv6 capable on its WAN side [your home network LAN].

Remember, the iotsnoop is intended for IOT gadgets, not for your main wifi network --tho that is certainly possible!! Just use the "iotsnoopg" SSID [and password "iotsnoop"] like any other wifi network. It can only be ethernet connected to your main router -the IOT gadgets all appear on wifi. It will be "double NATting" but this is no problem at all. A future project is to enable it as a main router, and the iotsnoop APN would be a "guest" network. SImple enough, and I would enable 5GHz and the "MIN" capture mode. You could do it now OK -just connect iotsnoop WAN port to your cable/fiber modem. Use the iotsnoopg SSID for your wifi. It is performing NAT like any router and has a simple firewall which can be enhanced. Its bandwidth would be limited to the 35MHz however.

2. I added a 10 hour "follow" for the selected IOT traffic analysis ***--the main addition to this release***
This was the hardest project to get working correctly!! Each hour iotsnoop performs a capture of **ALL** IOT traffic, placing it in a file for the next hour analysis. The analysis is thus "quantized on an hourly basis." The **previous** release enabled you to "snapshot" -a single IP address specified- IOT device's activity within that last hour. The subsequent analysis lists IP traffic/ports/DNS queries/etc. For **this** release I have added ***following*** this specified IOT for 10 hours [9 additional hours] to give a feel for what it is up to, giving the same analysis each hour. ***So this is now working*** and appears consistent as far as I have been able to debug with my networks here. I have four iotsnoop pi4s configured in various ways [SDcard, usb stick, usb SSD, 1GB RAM, 4/8 GB RAM] and coded and pointed to different IOTs. So it is not really "real time"..... That would be difficult but not impossible. I may consider a "real" "real time" option as well for

the next release. I would just need to run a crafted "tcpdump" with immediate flushing of the capture to a file and parallel watch of the file.

Attached are three AI interpretations of the IOT data: a FireTV report, an Amazon Alexa, and a Samsung TV report. I added a "visit" map [generated by iotsnoop] for one of the Alexa dumps. Also attached is a screen capture of the main iot stat web page, accessed by browsing to the pi4 iotsnoop on your home network. It would be really neat in a future release to automate this AI interpretation via an API.

The "following" of the IOT is a great way to see what the IOT is doing. "Interpreting" what it is doing is another matter, but can be hinted at by using chatgpt, etc to interpret the IP and DNS visits, as shown in the attached files.

3. I have included instructions for how to configure the firewall on the iotsnoop.
When you have wifi clients connected to your main router, especially IOT devices, you should connect them using a "guest" network to keep them from discovering your main wired and wifi network and compromising them! There are increasingly more malware agents showing up on your IOT. You can lookup "kimwolf" which has shown up recently:

See https://krebsonsecurity.com/2026/01/kimwolf-botnet-lurking-in-corporate-govt-networks/ ***There are at last count 2 million of these compromised devices used in bot attacks.*** This is the dark underbelly of the Internet, along with the ransomware enterprises which threaten our whole Internet.   Don't let them on your network!! To help with detection of these using iotsnoop, I have added a couple links to diagnostic sites which will check your Internet IP against an Internet database. I am working on an "auto" check in the next release.

The thing about the pi4 iotsnoop is that it is NAT'd like everything else on your home networks, but there is actually a route from pi4 IOT devices to your home network [via the WAN interface of the iotsnoop], in the same way that there is a route from your NAT'd PC to the Internet and back. Even tho there is a route between the IOT network and your home LAN, it is a different broadcast network, so not easily discoverable.

So we can add a firewall rule to prevent IOT from ever contacting your home network [except necessarily the Internet gateway!]. You can also block the "DNS over TLS" -DOT- which is a way that IOT devices, or their embedded malware, may hide their DNS queries. Iotsnoop relies on DNS queries for a lot of info! DNS queries are increasingly being "hidden" via DOH, DOT and encrypted DNS, tho IOT devices rarely use these. This is explained in a "README" in the /etc/iptables directory. It has to be done manually, tho I may consider making this automatic in a future release.

4. I made a venture onto youtube..
I created a 30 minute intro to imonitorg and iotsnoop. This does not include the enhancements discussed here. Please, no comments on the professional appearance of this! This would be a universe I would not look forward to mastering right now!! ......maybe an AI to read my script? But how would I sync with the screenshots.
Youtube intro to imonitorg and iotsnoop: https://youtu.be/v-NOPoMh860
Imonitorg/iotsnoop information: https://imonitorg.com
5. I would love some new participants on different [IOT] networks! And I would love comments and suggestions for future work. Please.
John Loop
https://imonitorg.com is the main info page.

interim 8-16-2025 newsletter

This is an interim newsletter on my latest project - adding the "orb" service to raspberry pi4 imonitorg/iotsnoop project. It represents a "short term" network performance monitoring which compliments the longer term imonitorg monitoring. [imonitorg/iotsnoop info here: https://imonitorg.com , with orb info to follow.]

I have successfully installed orb on iotsnoop raspberry pi4. You access it via a phone app pointed to the pi4 iotsnoop APN [or ethernet side on your LAN] , OR just the orb internet third party servers [speedtest founders project].   --I save you the trouble of installing it on your PC/MAC!

You can check out the orb app at orb.net .

"Orb" runs as a service, so it has to be installed on a PC/MAC/raspberryPi/Windows. The orb "service" connects to the orb.net Internet servers.
The orb phone "app" is needed to display results. The phone can connect directly to the orb service, over ethernet or wifi as long as it is on the same LAN.
In addition [or instead of], the orb service connects to the orb.net Internet servers, much like about ANY IOT gadget these days.
And it does NOT need an account on the third party server!

When you install the orb application on the PC/MAC/Windows, you need a user "orb" and you must supply a password. When you start the orb app on the phone, you initially have to supply this passwd. The ID of the orb instance is passed to the orb.net Internet server when the app checks in so it can correlate your orb service with your orb app.

The app grossly simplifies the network characterization, but in this day and age.... the closer our Interconnections get to "clear channels" -much like the old switched network connection-oriented/PVC connections- the closer it resembles reality.
E.g. they have a "time to Internet" which is completely dependent on the target.
And the latency, jitter and packet loss are likely with respect to this target.
--Looks like they are using simple pings to 8.8.8.8 and 1.1.1.1 for their "Internet" tests. Given that those appear on the edge of virtually every ISP, it is probably not a bad guess.

But it is a nice friendly phone app which seems everybody wants these days. Imonitorg/iotsnoop plots and stats are much more specific and configurable, tho not performed at the frequency of the orb app.

Now you have another reason to get a pi4 and get the iotsnoop image -just wait till July. The orb update will be in that release to come].
I will have a newsletter to announce updates and this feature.

I attached a screenshot showing the orb app running on my phone, connected to third party orb server, and reporting on my orb service running on my local pi4.
John

previous 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

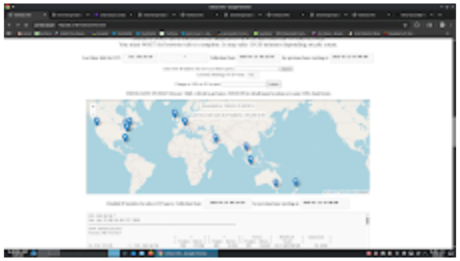
PLEASE let me know of suggestions. Needless to say, I am "desperate" for more testers for the iotsnoop. Please join our club!

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

5 attachments



AmazonEcho1-25-2026.png
299K

FireTVIOTreport.pdf
98K

AlexaURLmapchatgpt.pdf
219K

SamsungTabURLtrack.pdf
53K

iothostinfoWebPage.pdf
235K