Gmail

John Loop <pccitizen@gmail.com>

John Loops' 8-1-2026 "imonitorg/iotsnoop/ispsnoop" newsletter: network performance/IOT/ISP monitoring using raspberry pis

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

Wed, Aug 5, 2026 at 10:37 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 to remove your address]. I have collected email addresses from some of my friends in hopes you might be interested.

Summary for all newsletters [skip to below for current newsletter]:*

I am working on a project to perform Internet/Local Network/IOT monitoring/ISP monitoring, using a small device [raspberry pi3B, pi3B+, pi4B, or pi5] 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 3-1-2026 I have completed the 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 reached a stable point. I have actually made no changes for 8 months!

This 8-1-2026 newsletter introduces the next level of work - an "ISPsnoop" monitor which sits between your Internet modem and your Internet router, utilizing an ethernet switch with a mirror port to capture ALL your Internet traffic. I am developing plots and statistics to

characterize this. This is ongoing, but I have reached a "capture" stable point, and am carefully QA'ing and "finalizing" this pi5 image.

Here is the wikipedia page on raspberry pi if you have no clue: https://en.wikipedia.org/wiki/Raspberry_Pi
Here is my website about my projects: https://imonitorg.com

8-1-2026 newsletter

Dear friends

I have been working on "ispsnoop" since January and have made great progress. ICYMI, **ispsnoop is my next raspberry pi project** [image] that uses a raspberry pi5 [a 64 bit monster!] and is placed between your cable/fiber/etc modem and your router, and uses a mirror port on a switch placed there to mirror all external traffic [the WAN side of your router] and make it available for inspection by the pi5. I use many of the same scripting techniques I used with imonitor[g] and iotsnoop to collect the packets and generate plots and selected/selectable statistics on the traffic. I must say, as you might, that claude and chatgpt are wonderful helpers in generating and diagnosing scripts once I specify my algorithms. No more syntax problems -syntax is very difficult in many of these languages, particularly bash, which I use a lot!

"Iotsnoop" was the last image finished this Jan, and "imonitor[g]" before that, started in 2018. See the website for some history.

For ispsnoop, the necessary plots and statistics to be collected was not a foregone conclusion. Like iotsnoop before it, I made it a work in progress. I am using my own WAN traffic, which I presume may be "representative." It is a Spectrum ISP in Hernando, FL. I do provide port mapped services so as to generate inbound TCP traffic as well as the normal outbound TCP traffic. I especially make it capable for ipv6 as well as ipv4 analysis, and I have learned a lot about ipv6 in this adventure.

As with imonitor[g] and iotsnoop, I would seriously like some -other person/other ISP- experience in data collection and interpretation. While I do consider my ISP appearance "normal," there is no end of data and information I might learn with a different appearance.

All the data is available on a web server run by the pi5, as in previous imonitor[g] and iotsnoop. The user simply browses to the pi5 on their local network. It is a simple http page, so it will require the user to grant an http exception to view it -I don't provide a cert for the page. It is perfectly safe on your own network. ***There is absolutely no cloud connection to these scripts*** like there is with every other application these days.

Some details about ispsnoop. It runs on an 8GB Raspberry pi5, which is a 64 bit ARM small PC.

On the first division [see sample attached], there are several general sections. Simply browse to your pi5 once you establish connectivity to it on your network. This will have to be via wifi since the ethernet port is used for the mirror. [I will have instructions as to how to configure the wifi SSID/passwd, or you can attach a KVM and do this in the normal manner -there is no ethernet connection available for DHCP!]
1. An alerts scroll and a traffic summary scroll window. The scripts are traffic sensitive, but the pi5 should be able to handle sustained 50-100 Mb/s activity. I will be quantifying this soon. Exceeding this rate for longer periods, it is necessary to cap the capture and alert. -and survive!
2 Display of the current IPv4, ipv6, MAC address, etc used on the WAN, router
3. A DNS archive showing month long DNS queries, plus a form you can search this archive.
4. A DNS summary for each hour
5. A traffic summary for each hour showing total packets and showing script takeup time.

The plots and statistics I accumulate is the following:

1. A plot which accumulates hourly, showing several values: This is meant as a longer term visual record of the WAN side of your router.

    -the total [rcv+tmt] data rate [Mbits/sec] and packet count on the WAN link
    -the total out-going originating TCP sessions [normal browsing/etc]
    -the total in-coming TCP sessions [blocked and accepted]
    -the total accepted input-coming TCP sessions [accepted]
    -the total UDP packets in and out
    -the total DNS queries generated

2. Two more plots which are generated **each minute**:

    -the out-going TCP activity showing sessions [SYN-ACK TCP packets] plus ACK packets to indicate traffic intensity
    -the in-coming TCP sessions [blocked and accepted], plus ACK packets and blocked in-coming TCP sessions

The 3 plots rotate at a 5 sec interval on the home page.

A summary of the hourly data, listing

    -links showing the last hour TCP out and in, UDP activity, both blocked and allowed
    -quick counts of these packets [hourly total]
    -a form to submit to query name information for the IP addresses

Clicking on the links will list the traffic indicated. This may be hundreds, thousads of packets.
It is obvious that since I am viewing packets as a "man in the middle" most of these packets are encrypted. Also I have no name to associate with the IP address, and this is VERY difficult in general to do with the use of CDNs, cloud servers, etc. It is possible to do reverse lookups on the IP and garner some info, as well as the TLS certs carried by the IP. That is provided by the "form" which attempts to do this. I will be providing the option of running wireshark on the pi5 [accessible on the PC], and if you can provide the TLS key from the LAN device, you can decrypt traffic.

A section where the minute to minute data can be displayed. The user is expected to submit IP addresses to filter the minute to minute data. Providing a DNS name would not be a surefire way, since there are typically multiple "names" serving a DNS domain. There are four sections provided -still being developed

    -**TCP attempts to connect to my router/LAN**, both blocked and successful. The user will specify the ipv4 or the ipv6 address of their router. It is noticeable that if you specify the ipv6 of your LAN device [typically using the ipv6 netprefix+] you can actually track packets to individual LAN devices. This is not possible with IPv4 addresses.
    -normal outgoing TCP connects. The user can specify an Internet ipv4 or IPv6 address, and the pi5 will find this address in the WAN data and list its occurences.
    -**TCP attempts to my router/LAN which are successful** [SYN-ACK return detected on WAN]. You can specify either end IP of the connection to follow it. It is almost like having a "wireshark" on your ISP connection to summarize the packet activity.
    -A way for the user to **specify a TCP port** and find this in any packet. The details, possibilites of this are still under investigation.
    -**normal TCP connections to the Internet** -specify the IP address

The "ispsnoop" is still a work in progress, and I am not ready to release the image. I am still looking for important data to monitor and analyze on my WAN. I would definitely welcome any input on ideas for this project. I can give you the details on my setup. Right now I am using a managed 5 port netgear switch and assigning ports 1 and 2 to mirror traffic to port 5. I am connecting port 5 to a raspberry pi5 ethernet port, and removing any IP address on the ethernet port. This requires me to connect to the pi5 via wifi, so I the wifi SSID and password needs to be specified before this can be used. Right now, the user can use a utility "rpiimager" to insert this data. The alternative is for the user to connect up KVM to the pi5 initially [or leave it if desired], where the user can enter this information in the normal way [upper right corner, same idea as windows]. Amazingly enough, the insertion of the switch/mirror port does not slow down my

Gbs connection! I have tested the speeds and they hold. Amazing stuff, these modern switches.

A couple things going forward b4 I release this image

1. I will provide a way to use "wireshark," running on the pi5 to allow you to fully investigate the captured traffic. **I save the last hour traffic**, which can be several hundereds of megabytes of data! Wireshark can provide unsurpassed inspection of network traffic, esp if you can provide the TLS keys.
2. I need to **evaluate the capability of the pi5 for heavy traffic**. My "typical" traffic is maybe 1-20 Mb/s of traffic on my Spectrum downlink speed of 1Gbs. My uplink is still 40Mbs until Spectrum gets the "high split" completed for my area. Most of the fiber ISPs provide symmetrical 1Gbs up/down these days. During prolonged stressing of the pi5 when I generate heavy traffic -downloads, HD streaming, etc, the pi5 is a marvelous beast, and barely hiccups so far. But I have not characterized it. I use a 2GB buffer for an hour of data, so I cap the actual data that I do capture so as not to "overrun" the pi5. So far so good. **I do not intend to keep up with sustained speeds >100 Mb/s**. But I don't know the top end before it crashes the pi5. I was able to crash the pi4 iotmonitor with multiple HD streams.
3. I am using the included SDcard for all this activity, and it has shown no problems so far. **It is vitally important to use a good SDcard** -I use Sandisk extreme pro 128GB for the pi5. I also have an NVME "hat" for the pi5 and I can transfer the image there and it should run even faster and more reliably..... Hoping to do that soon.
4. As I mentioned, **I would desperately like feedback for the "ispsnoop" -as well as the iotsnoop**. I have many images of the imonitor[g] in "production", a few tens of the "iotmonitor" images and I sincerely appreciate the feedback.
5. I stopped the capability I started on imonitor which allowed me to **remotely access the device** and monitor it in real time [using a reverse ssh], in place. "Imonitorg," "iotsnoop," and "ispsnoop" do not have this feature. Both imonitor[g], and iotsnoop allow you to send daily emails if you use your gmail account as a relay [setting up the parameters on the piX webpage] I want to add this capability to the ispsnoop as well.
6. characterize the switch used for the **mirror port**
7. characterize details of configuring the **wifi SSID for your wifi network**
8. Closer examination of the UDP data, possibly IDing the **QUIC/UDP** component [all modern web servers use this instead of https]

I have attached several images to give you a feel for what is going on:

1. The **pi5 home index page** for ispsnoop [when you browse to the IP of ispsnoop]. This is the -only- access provided to data. A single web page which you browse to on the pi5 for all the plots/stats. Links to files and stats on the same pi5 server. -it is a long web page which I copied as a pdf. Scroll up and down and note the divisions and plots and stats. I want to add a daily email using your gmail as a relay, like with imonitorg and iotsnoop.
2. **An hourly plot**, showing long term trends [days] on different stats.
3. **The TCP out plot** [notice the spikes in activity]. Minute to minute activity. Normal web browsing/etc activity on your LAN. My wife has been on the Internet for about an hour. Increased total data, Lots of TCP out, some data.
4. **The TCP in plot**. [Notice the spikes in "rogue" -blocked- probes, various attempts to connect to my router/network -yellow.] This is also a minute to minute plot I turned my server on about an hour before. There should be no connections [blue line], unless you have ports open/ forwarded to your network [like me]. . Same total data plot. You can see imonitorg clients checking in [every 15 min], and some web requests to my server.
--these 3 plots rotate at 5 second intervals on the index page [typing "shift-P"] will make a copy in a separate tab. The right scale of plots 2 and 3 auto adjust with scale.

5 I also attached a **plot of my home network** showing just how complex these environments are getting to do all this work. Your networks are getting complicated too!

-**Spectrum modem and alternate Starlink modem** on the right [I can switch to Starlink by putting it in "bridge" mode and replace my Spectrum modem with the Starlink modem. I can also use the Starlink modem simultaneously on my LAN by placing it at a different IP, and changing gateway on my PCs if I want to use it simultaneously [I have to use static IPs to avoid the DHCP problems]

-The **netgear router** between the modem and the router with the mirror port feeding the pi5 ispsnoop
-the **"friendlyWrt" router**, replacement for the Spectrum router, running "openwrt" allowing me total "linux-like" access to the "ISP" router
-the **cisco switch** making basic splits in my home LAN
-the **16 port netgear** which is my main home switch. Notice I do not have a "mesh" system like the Eero, Ubiquiti. No need here. I have several wifi extenders on my main guest network and my iotsnoop networks. I do NOT have a wifi on my main LAN network. Not a good idea to tempt your neighbors.
-**My LAN**, showing my main server running http, https and sshd on ports 22 and 3313. 3313 is port forwarded from the internet. I am running an application level firewall on the server as well as the "firewall" on the router -almost necessary in this day and age [apache modsecurity and fail2ban].
-I have **specific ACLs** in my router allowing Internet acces to an iotsnoop and ispsnoop pi to allow external access. I can give you temp access if you want to experiene a live iotsnoop or my existing ispsnoop! -These are shown as <Niel> on the diagram.
-My **guest network** wifi APN, running openwrt and providing miscellaneous wifi access
-my **iotsnoop devices**, "pi4iotsnoop" providing the "iotsnoop" SSID for my IOT devices
-my **legacy pi3B and pi3B**+ running imonitor[g].
-my **pi5 running ispsnoop**, which I access over my guest wifi network.
-notice all the **port forwards** allowing access
-I am not showing any of my main LAN devices, which are several Linux, windows, even a MAC M1.

I really appreciate any advice going forward for the "ispsnoop" before i release it.
As always I appreciate all the versions of imonitor[g], iotsnoop, and soon to be ispsnoop in the "wild" and the feedback I have received.
It has been a wonderful learning adventure. There really is no "ready made" tool like this that I have found. They all come up running without config [except the ispsnoop wifi] once you plug them into your LAN, and it is as simple as browsing to their IP address. LOTs of configuration/tuning is available for the data collection.

I will report back when I have reached the "conclusion" of the ispsnoop and the pi5 image is ready.

John Loop

Youtube intro to imonitorg and iotsnoop: https://youtu.be/v-NOPoMh860
ispsnoop youtube intro to come!

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

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

isphost-info-webpic8-3-2026.pdf
167K

Hourly8-5-2026.pdf
108K

TCPout8-5-2026.pdf
64K

TCPin8-5-2026.pdf
67K

HomeNetwork_nopasswd_noname.pdf
89K