

Hello,

My name is John Loop, a retired digital system designer, now linux/network hobbyist. This will be a 10-15 minute introduction to "imonitorg" and iotsnoop." A perfect use for your old raspberry pi3B, 3B+ and now 4B!!

Youtube intro: <https://youtu.be/v-NOPoMh860>

If you want iotsnoop only, skip to about halfway, tho you may not understand all of iotsnoop if you skip the imonitorg intro.

Like many of you I am sure, early on, and even today I was/even am plagued by my family, friends and neighbors to make sense of their PCs and network connections, especially their Internet connections, and was called on routinely to diagnose problems -esp in the "early" days, maybe 10-20 years ago. "The Internet doesn't work" was a familiar refrain. Sound familiar? Such a momentous declaration with so little revealing information, right! Trying to debug these home environments and make sense of my friends networks and their problems led me to a years long effort to develop linux tools and scripts to address this. It very often required longer range captures and analyzing than was readily available by simple pings and DNS queries. Internet/network problems are notoriously transient! And there just weren't any good tools available at layer 3 -IP packets- that I could find. No hope for layer 2 unless the modem had a layer 2 stats interface. There was almost nothing which would help me diagnose a problem "at that instant" if the problem occurred previously, intermittently or slowly, over the longer term. So.... longer term tool! How to do this?

So was born "imonitor," its derivative "imonitorg" and later the "iotsnoop" "appliance." I made a decision to use linux & bash scripting on a separate device [not using the user's PC to separate myself from that rat's nest -another story entirely!] such as raspberry pi since I knew the linux OS and some bash, and I wanted to start using the raspberry pi, and I figured I would probably need all the tricks in the linux scripting and command universe to diagnose networks and problems. Running a quick script or two on the user's PC was just not going to get the job done for longer term analysis.

I call imonitorg/iotsnoop an "appliance" because it uses a raspberry pi and hundreds of scripts, mostly bash and python and some perl -no chance of making available a single script or program available on github! Plus, of course the linux cmd line and all the linux goodies developed over the years. The result of all this monitoring and analysis web pages of statistics and some plots, from which we can more readily diagnose much longer term problems, or at least confirm them! So basically, one gadget you can plug into your network, let it run and then go look for problems in the stats it collected. An appliance.

The web pages which give the stats and plots is provided by a web server enabled and configured on the raspberry pi. The raspberry pi "appliance" of course is placed on your network and connected to your ISP router, much like your PC. It runs from startup and requires essentially, no initialization, other than an email address if you

OBJ

want a daily email. You can then point your favorite browser to the pi and see all the stats and plots and results of the scripts ---once it has had time to analyze! -- remember this is longer term monitoring!

It is vitally important to recognize that this is a longer term tool. You rarely start the pi, go look at the stats and plots and immediately conclude much of anything. Wait an hour, more likely a day, or weeks, or months!

Here are a few screenshots of the imonitor.org.

First shown here is the home project web page where a lot of education and links reside.

--scroll down, describing info

Second let us go to the actual pi imonitor/imonitor.org web page

--scroll

The main -index- page - you must enable http because most browsers don't like non https pages, but it is perfectly safe - it is on your private network.

There are links to a manual [contained on the pi]

Scrolling down the page you can see each of these areas -Quick Data, Detailed data, configuration, counts, mgmt showing lots of detail about the network performance, hosts, services. There are archives of the data and plots as well.

Basically, various ICMP [ping to newbies], TCP syn [web stuff], and DNS activities are performed to IP addresses and DNS names and the response times are plotted. ICMP targets are automatically detected based on a traceroute to connected points. TCP targets are drawn from the 100 top web sites. In addition, DNS queries are performed and a curl is executed to a known target. The results of these "pings" are plotted. Algorithms are used to declare "offline" "no ipv6" "router used as ping target [which means actual Internet perf may be less meaningful].

There are many other stats collected about your network, including Details about hosts and services, and changes. There is an historical arp table and archives of previous plots and stats. You can look at your ping plot for any day in the last year. The config page allows variations on these activities, tho the imonitor.org will operate with default config out of the box!

The most useful overall info is probably the plot link at top, which is a link to a near real time display of the stats collected and plotted [opening in a new page], which will be updated each minute. You can call this up anytime and it will display the running stats which began at 2AM for that day. There is a link at the top to go back to the index page.

--the near real time plot- go back to main page.

Here are a few plots showing some unique occurrences on different friends links to show problems which can be easily displayed since we have a longer term record of

[OBJ]

the connection.

Plot 1 Clean

Plot 2 GraduallyWorsening

Plot 3 WindstreamTOSTarlink Very flaky all around

Plot 4 HardFail

Plot 5 VerizonTOSpectrum notice delay and ping problems

Plot 6 SpectrumTOVerison

Plot 7 Fascinating

Plot 8 GREATdebuggingplot

This project has been ongoing and fine tuned for almost 7 years and used many of my friends and neighbors across the US in many different ISPs to allow development, customization, and of course debugging. There were 25 of these at one time, and I had a connection to these pis for monitoring and management. I am forever grateful to my friends allowing me to do this! Later, I released "imonitorg" which is a standalone version of "imonitor" - I have no connection to the "imonitorg" [g for generic] pis. Completely standalone, NO cloud services either.

Most importantly, the imonitorg pis use no connection to any Internet server, i.e there is no cloud connection, which is used by almost all gadgets these days. You typically have to register to the cloud server and the cloud server communicates with the device and stats, and you actually connect to the cloud server to get the stats for your network. That is not the case for imonitorg, all the data is on the pi3B or 3B+ appliance, accessible by browsing to the pi [or by setting up a daily email] from your local network.

Since there are hundreds of scripts tied closely to the pi and the OS, I do not release individual scripts. The release, the "appliance" is an image for the raspberry pi 3B or the 3B+, which is easily burned into a 32GB or larger micro SDcard. These images are available on sourceforge or my google drive, linked on the imonitorg.com web site.

After burning the microSD card and inserting into the 3B or 3B+ pi, simply connect the pi to your router via Ethernet. Everything is automatic after that, except for setting email parameters. Browse to the pi IP address [look in your router typically] and go into config and you can setup email config - it uses your gmail account as a relay. You must use 2FA on gmail, and get a key to use. Instructions are linked there.

You can also use the pi3B or 3B+ if you only have wifi access to your router. You will need a KVM to access the pi and setup the wifi SSID and passwd. You can then operate headless, and the imonitorg will use the wifi as the connection to the Internet. This capability is removed for the iotsnoop pi.

 *plot of iotsnoop pi home page.*

Now we can talk about the "iotsnoop" appliance -my project this year 2024. Watching our IOT gadgets should be very important to us, but there is currently no easy way to do this!!! that I know of.

This tab shows the main iotsnoop web page, an upgrade of the imonitorg page.

At the beginning of 2024, I realized that the wifi of the raspberry pi could be converted into an APN and used as an SSID for wifi clients, in exactly the way your wifi router performs. Thus was born "iotsnoop" -I developed more scripts to extend the functionality of the imonitorg to perform host and network analysis of the wifi APN. I advanced to a raspberry pi4 for this function, but I carried over all of the imonitorg functions onto the pi4 [except pihole and wifi monitoring]. A pi4 must be used for iotsnoop, but you can actually turn iotsnoop "off" and it performs like an "imonitorg" only version, resembling the 3B or 3B+ The iotsnoop must also be connected via ethernet to your router [or a downstream switch] - you cannot use the wifi since it is used for the APN [and I don't reprogram it on the pi4 for client use].

I am targeting this pi4 iotsnoop for IOT gadgets. The IOT gadgets, like your Amazon echo, your doorbell, your security cameras, your alarm system, your thermostat, and a thousand other wifi gadgets are devices that you typically have absolutely no idea what they are doing in your network. Once you assign them your wifi SSID and password, they connect to servers across the world [using your Internet connection] to perform their functions. In the modern world, the danger of these IOT servers being compromised is especially present because the IOT gadgets tend to use an outdated, often insecure OS, and it is often **never** updated. They connect to the outside world, and if they, or the servers become compromised, the outside world can connect to your IOT gadgets. If your IOT gadgets sit on the same network as your important clients like your PCs, this can be dangerous. Malware can -easily- often hop from the IOT to your important PCs, or at the very least scan your network for vulnerabilities. How secure are your PCs inside your router? Do you auto login? This is why they have "guest" networks in routers, to separate the IOT from your important PCs. The "iotsnoop" represent a "guest" network intended for the little tended-to, suspect IOT devices.

Iotsnoop is thus a set of scripts to capture all the wifi traffic -at layer 3- on the APN, perform analysis of the traffic, such as identifying DNS requests, TCP and UDP connections, number of IOT hosts, appearance and disappearance of said hosts, and the time activity of the hosts. Iotsnoop SSID can be used to terminate IOT gadgets within your home, all your ancillary gadgets -except for the streaming devices like TVs- discussed in a minute. This info is collected for an hour and then analysed, the stats displayed and a running plot of this info is displayed. I use the tshark version of wireshark to do this with a 2GB buffer, and run this for one hour at a time. The script repeats each hour updating data for display.

The capability of the pi4 scripts at present is about 6-8Mbps average bandwidth, up and down, so you should not put streaming devices like your TV here - leave them on



your router's "guest" network. In addition, the pi4 wifi APN is limited to 2.4GHz to further limit bandwidth [but has the advantage of greater range]. Why would you want the IOT to monopolize your bandwidth -restrict it!/put it on the lowest speed but greatest range 2.4GHz. And the bandwidth usage is mostly upstream, unlike your main and guest networks. Beware that the wifi on the pi4 is not as powerful as that in your router, so you may need a wifi extender to make it accessible as widely as possible. The extenders also let you garner 5GHz as well as the 2GHz bandwidths for the APN upstream of the extender, but they are throttled by the 2.4GHz APN.

Access to the stats and plots generated by iotsnoop is in the same manner as imonitorg. Just point your browser to the pi4 web server -there is an index page at the pi's IP. The web pages are a little different from the imonitorg pages, but they include all the imonitorg stats and plots.

This is the iotsnoop index page, which contains the quick links to the manual, Quick Data, management config and IOT wifi APN config.
iotsnoop index page -scroll

These actually page down to an additional link -showing instructions- where the referenced page is then called up. The default SSID is "iotsnoopg" and the password is "iotsnoop" so you can use this if you want. You can also change the creds to that of your existing guest network, turn off your existing guest network, and all the guest network gadgets should appear on the iotsnoop. Like I said, be careful of streaming devices like TVs, esp 4K. These should be left on your existing guest network. -- Testing these on my network, the streaming still works when the pi4 iotsnoop scripts "break" and recover on the next hour.

I would recommend gradually walking your IOT gadgets onto the default iotsnoopg SSID one at a time, do some evaluation, and walk the rest. Leave the streaming TVs on your guest wifi.

The index page contains a rolling display of the imonitorg near real time plot/speedtest archive plot, plus a rolling display [max 250 entries -250 hours or 24+ days] of the iotplot, both log and non log. This one shows about 10 days of activity on my IOT network, about 13 hosts, actually including one streaming TV [avoid 4K].

Paging down further shows the Quick data and the hosts info for both imonitorg and iot. Recall that the imonitorg hosts will be those on your main/PC network, whereas the IOT hosts are on your IOT APN. An attempt is made to ID host "changes" and "persistent" hosts for BOTH. Scrolling down further you can see the links for the additional stats and management and config pages.

The "MAIN IOT page contains all the IOT stats.
Email config and wifi creds [if you want to change] are on the 3rd and 4th links

 *tab to IOT page, scroll*

Looking at the MAIN IOT page we see the following sections:

Alerts and script summaries and DNS assignments and SSID assignment. Note the time the script takes in the hour, #packets

IOT statistics and packet counts, including avg bit rate for last hour. The DNS archive for the last month is listed and is searchable. The bottom panels show the last hour scan summary and an archive of the scans [scroll down to see latest]

The next section shows the IOT DHCP lease table info. The DHCP lease time is 1 hour; the table is updated every 5 minutes. The bottom panel is an archive of every device that has ever acquired a DHCP lease on your APN - rolling max 500 entries.

The next section allows you to query the last hour data for info for a specific host, and even plot a map of the servers contacted [actually the DNS queries of the IOT]. Beware that it could take 5-10 minutes to perform this recall, so you have to wait until the page tab completes. The bottom two panels show the last hour and the month archive of DNS queries for the selected IOT

The last section lists actual data files with details, as well as detections of non-DHCP addresses detected and off-network addresses detected. Pcap files are made available for these instances. The entire last hour pcap file is also made available.

Here are a few iotplots. These represent 250 hrs/24+ days of data. Remember you will see NOTHING on your plots when you first start iotsnoop. You have to wait for data to accumulate. Each hour data is added.

plot with one host iotplot1host.png

plot with 13 hosts ~100Kb/s traffic iotplot13hosts.png

plot with 13 hosts and a streaming TV [you should not put hosts > 6Mb/s. This is normal HD. 4K would be maybe 10Mb/s and may saturate iotsnoop]


plot of htop showing pi4 working hard

EXAMPLE

Let's do a deep dive into the activity of an IOT over the last hour. Find the IP address of the IOT you want to monitor, and enter it here, submit and WAIT, esp if you are asking for a map.

This pretty much summarizes the imonitor and iotsnoop. This is a wonderful use for an older pi4 [they are up to pi5 now!].

They give the user wonderful statistics and plots of what is going on in their home network and their IOT network thru a combination of statistics and plots, maybe even shining light on what is going on! It's all a mystery right!

 The next project will attempt to implement an mqtt server on the pi4 and develop a phone app to query the pi4 for imonitorg and iotsnoop specifics.

Links for the appliances are at imonitorg.com

Comments are solicited! John Loop jdloop@imonitorg.com