John Loop <pccitizen@gmail.com>

John Loops' 12-10-2024 imonitorg/iotsnoop news: IOT monitoring raspberry pi4 -"iotsnoop" update; Youtube Intro!

1 message

John D Loop <jdloop@imonitorg.com> Wed, Dec 11, 2024 at 5:51 PM
To: "pccitizen@gmail.com" <pccitizen@gmail.com>, John Loop <jdloop@johnloop.com>

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

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 those of you new to this newsletter:

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

As of 12-10-2024 I have completed the initial work on an extension of imonitorg, called "IOT [The Internet of Things] monitoring" and I call this "iotsnoop." It will require a raspberry pi 4B. "Iotsnoop" also contains the previous "imonitorg" functionality! The pi3B, 3B+, ova, 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. This 12-10-2024 newsletter recapitulates the work and updates it status and introduces the next level of work./*

*** 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

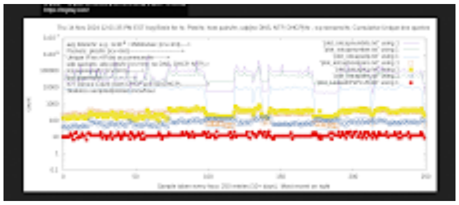
PLEASE let me know of suggestions. Needless to say, I am "desperate" for more testers for the iotsnoop. Please join our club!

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
https://sourceforge.net/projects/iotsnoop

4 attachments



iotplot-103-11-14-2024.png
108K

iotmain.pdf
209K

iothostinfo.pdf
153K

YouTubeScript.pdf
69K