STATUS: IOTfindhosts script alerts/status/hourly finish/total pkts

NOTE! Statistics are done hourly! There will be no initial data until an hour has been crossed and data analyzed. This is 10-50min after the hour depending on #hosts. Thereafter it will accumulate. Always refresh your browser [shift+click browser refresh icon] for latest data. Browser page update is hourly otherwise.

Findiothosts enabled? YES **Must be YES for IOT collection <- "NO" means base imonitorg function**

Tshark environment: MAX **Defined by "/root/DEFtshark.txt" <-NOT SELECTABLE in first versons!**

[left]Findiothosts alert log; [right]Findiothosts follow: script record: date/finish/total pkts captured last hour

```
2024-11-13 02:01 PM: Added DHCP host[s]: 192.168.50.130
192.168.50.77
2024-11-13 02:01 PM: Removed DHCP host[s]: 192.168.50.128
2024-11-13 04:10 PM: NON dhcp addresses used! -see panel below
2024-11-13 05:10 PM: NON dhcp addresses used! -see panel below
2024-11-13 07:10 PM: NON dhcp addresses used! -see panel below
2024-11-13 08:01 PM: Added DHCP host[s]: 192.168.50.128
2024-11-13 08:01 PM: Removed DHCP host[s]: 192.168.50.130
2024-11-14 01:10 AM: NON dhcp addresses used! -see panel below
2024-11-14 10:11 AM: NON dhcp addresses used! -see panel below
2024-11-14 11:10 AM: NON dhcp addresses used! -see panel below
```

```
Mon 04 Nov 2024 01:10:31 AM EST 25232
Mon 04 Nov 2024 02:10:43 AM EST 42031
Mon 04 Nov 2024 03:10:35 AM EST 32907
Mon 04 Nov 2024 04:10:42 AM EST 35352
Mon 04 Nov 2024 05:10:49 AM EST 53581
Mon 04 Nov 2024 06:10:34 AM EST 30938
Mon 04 Nov 2024 07:10:47 AM EST 31243
Mon 04 Nov 2024 08:10:31 AM EST 30859
Mon 04 Nov 2024 09:10:31 AM EST 30904
Mon 04 Nov 2024 10:10:42 AM EST 31183
Mon 04 Nov 2024 11:11:02 AM EST 75154
```

Tshark uses a 2GB ring buffer -this will handle up to 6Mb/s avg [rcv+tmt] over 1 hour b4 tshark capture is stopped -note timestamp b4 EOH.
Capture is per hour... At the end of the hour, assuming 2GB not exceeded, tshark is restarted and analysis/statistics are performed for last hour.
You should avoid putting streaming devices like smart TVs, Dish, DirectTV on iotsnoop. These are not IOT. They may exceed 6Mb/s avg the hour.
4K streaming will overrun the 2GB buffer in about 30min, for tshark MAX env. Happens frequently on youtube, amazon prime, etc.

Current DNS assigned to iotsnoop: 9.9.9.9 Quad9 9.9.9.9 is default [change with caution!]
The DNS assigned to individual IOT gadgets is their gateway -the iotsnoop pi4: 192.168.50.10

Enter new iotsnoop dns server: ________ Submit

DNS cache is set=0 in dnsmasq.conf so all FQDNs require DNS query

Current iotsnoop wifi APN SSID:
```
iotsnoop
```
iotsnoop pi4 uses 2.4GHz wifi band for greatest range. However, the 2.4GHz radio on the pi4 is less capable than most APN/routers.
Use an extender such as Netgear EX6100 to provide access to both 2.4 and 5GHz bands, and extend range.
This is the pcap of the wifi APN for the last hour. Download and investigate via wireshark [could be up to 2GB!!]: pcap file

IOT statistics, packet counts, Overall [rcv+tmt] bit rates

[Left]Cumulative -unique- IOT host dns query archive; [Right]Unique Last hour queries: Total/LastHour ->should be "stable"
Ideally these queries should not deviate/grow significantly over time, except as your IOT gadgets increase.
If the number grows significantly, then there is likely questionable activity on your IOT network!
The "queries" in the right panel will be typically >2 actual list on left because of identicals.
The LEFT FULL DNS query archive is one month long, and is cleared at beginning of month.

```
169.254.205.86  DESKTOP-UGCHF53.local
169.254.234.170 170.234.254.169.in-addr.arpa,apn-pi0.local
169.254.234.170 64.50.168.192.in-addr.arpa,apn-pi0-2.local
169.254.234.170 64.50.168.192.in-addr.arpa,apn-pi0.local
169.254.234.170 64.50.168.192.in-addr.arpa,apn-
pi0.local,e.1.8.9.3.a.6.5.a.e.1.8.0.a.5.b.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.a
rpa
169.254.234.170
e.1.8.9.3.a.6.5.a.e.1.8.0.a.5.b.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa,apn-
pi0-2.local,170.234.254.169.in-addr.arpa
169.254.234.170
```

```
13:01:PM queries: 868  67
14:01:PM queries: 872  108
15:01:PM queries: 874  59
16:01:PM queries: 874  56
17:01:PM queries: 875  87
18:01:PM queries: 876  81
19:01:PM queries: 877  91
20:01:PM queries: 877  68
21:01:PM queries: 877  68
22:01:PM queries: 878  105
23:01:PM queries: 878  64
```

You may submit individual URL [copy from above, then paste into this website]: Virustotal.com query for malicious URL <-Separate tab!
You may submit individual URL [copy from above, then paste into this website]: Overall site info <-Separate tab!
Enter DNS [sub]domain to search in above Month-to-date archive: Submit

[Left] Last Hour /DHCP host?/hosts/pkt count. [Right] Archive listing of /DHCP host?/hosts/pkts[both rcv/tmt]/mdns name: ->SCROLL DOWN for recent!
Each dated block represents iot hosts/pkt counts/names for previous hour [rcv+tmt]

```
11:10: Last hour: Pkts: 29354,
Avg bits/sec: 35830
 DHCP: 192.168.50.104: 132
 DHCP: 192.168.50.108: 12275
 DHCP: 192.168.50.112: 5013
 DHCP: 192.168.50.124: 706
 DHCP: 192.168.50.128: 1331
 nonDHCP: 192.168.50.129: 172
 DHCP: 192.168.50.144: 28
 DHCP: 192.168.50.145: 31
 DHCP: 192.168.50.170: 1661
```

```
 nonDHCP: 192.168.50.129: 172
 DHCP: 192.168.50.144: 28       orig-pi0
 DHCP: 192.168.50.145: 31       Johns-Mac-mini
 DHCP: 192.168.50.170: 1661       ecoflow
 DHCP: 192.168.50.179: 2923       Emporia
 DHCP: 192.168.50.191: 2192       amazon-93f3dcfa9
 DHCP: 192.168.50.64: 32       apn-pi0
 DHCP: 192.168.50.77: 1342       *
 DHCP: 192.168.50.82: 1001       TSTAT-4360
There are likely 169.x, 0.0.0.0 and multicast addresses adding to host counts
```

IOT DHCP lease table, IOT DHCP lease archive [lease time 1 hr]

IOT DHCP leases assigned by dnsmasq -infer device from mdns name. Updated every 5 minutes ->refresh browser.
Left fields show lease expiration time, plus Y or N for host online or offline at last hour scan
Right fields show MAC address, IP address, mdns name [if available].
Some DHCP hosts may not have renewed IP addresses due to reboot... May not show until 1/2 lease time expired.

```
Snapshot at: Thu 14 Nov 2024 11:45:15 AM EST ->DHCP Lease does NOT imply host is present!
Expires: Thu 14 Nov 2024 12:18:03 PM EST Active:  N YourName:X  34:6f:24:6f:43:60 192.168.50.82 TSTAT-4360 *
Expires: Thu 14 Nov 2024 12:20:44 PM EST Active:  N YourName:X  9c:c9:eb:10:e9:e7 192.168.50.124 EX6100v2 01:9c:c9:eb:10:e9:e7
Expires: Thu 14 Nov 2024 12:27:20 PM EST Active:  N YourName:X  b8:27:eb:02:b9:d3 192.168.50.144 orig-pi0 01:b8:27:eb:02:b9:d3
Expires: Thu 14 Nov 2024 12:27:51 PM EST Active:  N YourName:X  b8:27:eb:ab:ef:45 192.168.50.64 apn-pi0 01:b8:27:eb:ab:ef:45
Expires: Thu 14 Nov 2024 12:29:16 PM EST Active:  N YourName:X  58:32:77:1a:02:91 192.168.50.104 * 01:58:32:77:1a:02:91
Expires: Thu 14 Nov 2024 12:31:15 PM EST Active:  N YourName:X  b8:5f:98:eb:b3:d9 192.168.50.77 * 01:b8:5f:98:eb:b3:d9
Expires: Thu 14 Nov 2024 12:34:10 PM EST Active:  N YourName:X  fc:a1:83:2f:e7:5a 192.168.50.191 amazon-93f3dcfa9 *
Expires: Thu 14 Nov 2024 12:34:37 PM EST Active:  N YourName:X  cc:f7:35:03:c4:14 192.168.50.108 amazon-9c739f3aa 01:cc:f7:35:03:c4:14
Expires: Thu 14 Nov 2024 12:36:36 PM EST Active:  N YourName:X  10:52:1c:b9:49:40 192.168.50.179 Emporia 01:10:52:1c:b9:49:40
Expires: Thu 14 Nov 2024 12:38:11 PM EST Active:  N YourName:X  80:6a:10:05:bb:5f 192.168.50.112 Tina-55-BR *
```

Some IP addresses may have expired in above cumulative record ^ -Lease time is 1 hour!
host IOT leases can OUTLIVE their appearance on network! --host can move network, appear there, still have lease here ^
Lookup MAC addresses: [copy from above, then paste into this website]: MAC address Lookup <-Separate tab
You can create a "home_devices.txt" to replace the "X" in "YourName:X" in the above list^: See iotsnoop configuration on main page."

This is the archive of IOT -any IOT and their details that have appeared. Cumulative, max 500 entries -clear via button:

Clear

```


Expires: Fri 01 Nov 2024 YourName:X  00:03:7f:55:5c:7c 192.168.50.128 blink-sync-module *
Expires: Fri 01 Nov 2024 YourName:X  00:03:7f:55:5c:7c 192.168.50.129 blink-sync-module *
Expires: Fri 01 Nov 2024 YourName:X  10:52:1c:b9:49:40 192.168.50.179 Emporia 01:10:52:1c:b9:49:40
Expires: Fri 01 Nov 2024 YourName:X  10:52:1c:b9:49:40 192.168.50.181 Emporia 01:10:52:1c:b9:49:40
Expires: Fri 01 Nov 2024 YourName:X  34:6f:24:6f:43:60 192.168.50.82 TSTAT-4360 *
Expires: Fri 01 Nov 2024 YourName:X  4c:20:b8:ac:48:0a 192.168.50.145 Johns-Mac-mini 01:4c:20:b8:ac:48:0a
Expires: Fri 01 Nov 2024 YourName:X  58:32:77:1a:02:91 192.168.50.104 * 01:58:32:77:1a:02:91
Expires: Fri 01 Nov 2024 YourName:X  74:4d:bd:bd:3a:6c 192.168.50.170 ecoflow 01:74:4d:bd:bd:3a:6c
Expires: Fri 01 Nov 2024 YourName:X  7c:61:66:99:71:95 192.168.50.50 * *
Expires: Fri 01 Nov 2024 YourName:X  80:6a:10:05:bb:5f 192.168.50.112 Tina-55-BR *
```

IP-specific IOT Traffic, IOT contact map

Use DHCP [or non-DHCP] addresses [Lease table above] to display traffic for last hour.

Last Hour DNS queries/pkts for host: 192.168.50.179 Emporia

Enter new IP Address to extract [Normally: leased IP address]: Submit

You can also use non-dhcp assigned addresses [rogue IOTs?] ^ to see what these IOT are up to!

Are we plotting IOT coordinates: NO **See manual to change to YES|NO [as root: echo YES|NO > /root/DEFplotmap.txt]**

Submit, then -WAIT- 5 minutes to extract traffic and 5-10 to construct map of IOT targets [maybe hundreds of DNS queries!!!!]
-WAIT for tab to complete, refresh browser and come here for map!

Results -from "submit"- will display upon refresh of browser [There must be a capture from the LAST hour to display pkts]
FQDNs may not produce Last hour dns queries if locally cached -see file below "file192.168.50.x.txt" for IP URL list.

Last IOT contact map for above "submit" selected IOT IP address. Only LAST HOUR contacts, as selected, are shown!!
Many, multiple IP addresses may be returned for each DNS query, and NOT used by IOT! [and not shown on listing]

No
Map
Created

IP stats/ports/FQDNs/on-net<->on-net from previous IOT query -selected above

```
192.168.50.179 Emporia
Fri Nov  8 18:55:33 EST 2024
================================================================================
IPv4 Conversations
Filter:<No Filter>
                                               |       <-      | |       ->      | |     Total     |    Relative    |   Duration   |
                                               | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      Start     |              |
192.168.50.10        <-> 192.168.50.179          2664    204156       4       880    2668    205036     2.903165232      3584.3610
192.168.50.124       <-> 192.168.50.179             1        70       1        92       2       162  1556.521676106        0.0303

IP address:port  reverse DNS for above tcp/udp conversations
the "reverse DNS" is how the ISP identifies the IP.  DNS queries, listed below, likely map to these

DNS queries by host 192.168.50.179 -cumulative since start of month/reboot
fwsrv.emporiaenergy.com
pool.ntp.org
prod-mqtt.emporiaenergy.com
time.google.com

Fri Nov  8 18:55:37 EST 2024
Intra-network traffic! tcp/udp listed separately -->DNS queries to/nmap scans from 192.168.50.10 are not listed
THIS TRAFFIC IS ENTIRELY BETWEEN IOT hosts, often without dhcp assigned addresses
```

The first iframe below represents the Last Hour DNS queries of the IOT selected above.
The second iframe represents the Archive [month-to-date OR since last boot] DNS queries of the IOT selected above.
MULTIPLE IP addresses may be returned for each FQDN DNS query! See "[Long]ip192.168.50.x.txt" files below.

```
fwsrv.emporiaenergy.com
pool.ntp.org
prod-mqtt.emporiaenergy.com
time.google.com
```

Last Hour:

Copy/paste last hour screen above into google gemini and ask to interpret! Gemini Lookup

```
fwsrv.emporiaenergy.com
pool.ntp.org
prod-mqtt.emporiaenergy.com
time.google.com
```

Month-to-date/since boot:

This is the pcap of the wifi APN for the last hour -all packets/IPs. Download and investigate via wireshark [could be up to 2GB!!]: pcap file

Details/anomalies/misc

[On Left]: [fqdn|Longfqdn].txt shows [LastHour|Month-to-date] DNS queries per IP? [ip|Longip.txt shows [LastHour|Month-to-date] ip addresses
[Center] IOT addresses which are NOT leased in last hour. [Why is the IOT not participating in DHCP?]
[Right] Private addresses which appear on IOT. Latched to last occurrence. [??]
These may also be addresses that are SCANNED by IOT hosts [Why would they do that?]
This is a rolling archive with dated entries. Max 100 entries.

Index of /dnswork/

```
Name↓                      Last Modified:         Size:  Type:
../                                                 -    Directory
dnswork5X/                 2024-Nov-05 15:12:19    -    Directory
fqdn192.168.50.104.txt     2024-Nov-14 11:10:39   0.1K  text/plain; charset=utf-8
fqdn192.168.50.106.txt     2024-Sep-25 21:10:33   0.0K  text/plain; charset=utf-8
fqdn192.168.50.108.txt     2024-Nov-14 11:10:32   1.4K  text/plain; charset=utf-8
fqdn192.168.50.109.txt     2024-Sep-14 20:10:32   0.0K  text/plain; charset=utf-8
fqdn192.168.50.110.txt     2024-Sep-25 21:10:33   0.0K  text/plain; charset=utf-8
```

```
192.168.50.129
```

404 Not Found

Non DHCP host pcap files from last hours are located at /home/pi/tests/iothosts/<IPaddress>.pcap.nodhcp
Pcap files for hour which contains Home Netwk address are located at /home/pi/tests/iotcapture.pcap.last.HomeNetwk

NXDOMAIN and SERVFAIL DNS responses encountered last hour by IOT hosts

Scan of IOTs using non DHCP leases. What are these unallocated devices serving?

This is only for the last hour^ The archive of scans is at /home/pi/tests/iothosts/archiveSCANiotNONdhcpleases.txt

Any hour which reports 5X number of pkts from previous hour saves the pcap as "iotcapture.pcap.5X"
Any hour which reports 5X number of pkts from previour hour saves the DNS query file as "iotcapdns.txt.5X"
These files are in /home/pi/tests/iothosts and allow interrogation of the pcap file.
Host/dns queries are saved in /home/pi/tests/iothosts/dnswork/dnswork5X directory for interrogation
Caution: the [Left] files only work currently for the default iotsnoop network 192.168.50