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

NOTE! Statistics are updated hourly. There will be no data until an hour has elapsed and analysis completes (10–50min delay).

[Left] Alerts | [Right] Hourly Script termination time/packets: finish before hour!

```
Sun Jun 21 07:35:30 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:36:31 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:37:31 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:38:31 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:39:31 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:40:30 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:41:30 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:42:30 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:43:30 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:44:29 AM EDT 2026: checkfile1-file2.sh at end done
Sun Jun 21 07:45:30 AM EDT 2026: checkfile1-file2.sh at end done
```

```
Sun Jun 14 12:02:02 AM EDT 2026 165874
Sun Jun 14 01:04:07 AM EDT 2026 604496
Sun Jun 14 02:02:11 AM EDT 2026 198471
Sun Jun 14 03:02:19 AM EDT 2026 214712
Sun Jun 14 04:06:05 AM EDT 2026 939893
Sun Jun 14 05:01:52 AM EDT 2026 129351
Sun Jun 14 06:01:44 AM EDT 2026 104939
Sun Jun 14 07:06:40 AM EDT 2026 1423467
Sun Jun 14 08:10:10 AM EDT 2026 2349417
Sun Jun 14 09:10:12 AM EDT 2026 2134268
Sun Jun 14 10:08:23 AM EDT 2026 1557132
```

Tshark uses a 2GB ring buffer. This should yield ~100-200Mb/s collection rate. Check script termination time to monitor!

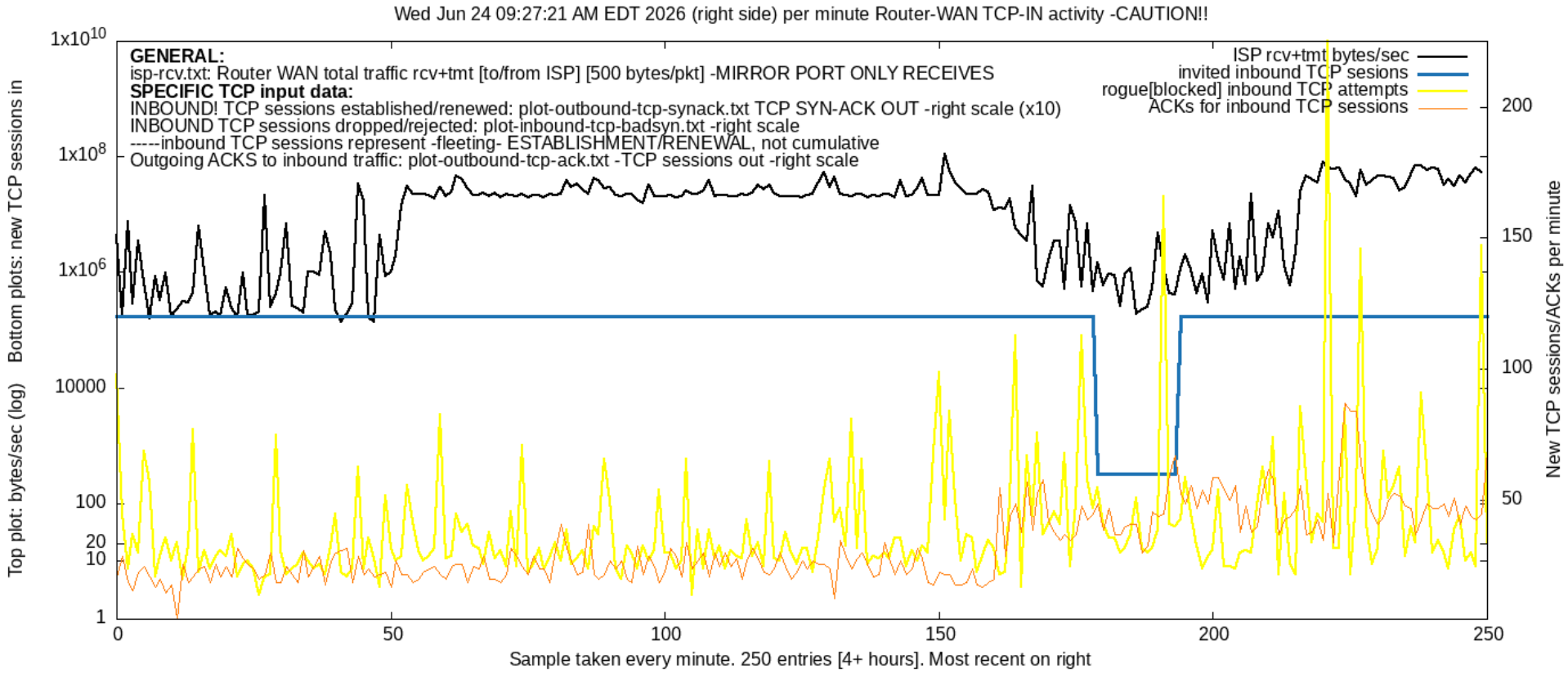
Router WAN MAC address: `5e:32:39:05:61:4d` Router WAN IPv4 address:: `35.137.208.94` Assigned IPv6 prefix [not WAN IPv6]: `2603:900b:b840:2b6e::/64`

Router WAN MAC address and IP address can be automatically determined, via "AUTO."
Set them at /home/ispsnoop/DEFs/DEFmacadd.txt, DEFIPadd.txt, DEFIPv6prefix.txt if necessary [there may be cases]..

(for mgmt access) WiFi SSID: `SSID: OpenWrt2G` Pi5 Memory: `8256592 kB`

Download capture file (last hour): pcap file Could be <=2GB! "bits/sec" are estimates bases on 1000bytes/pkt.

Rolling display of ISP activity on router WAN port: data gathered each hour/each minute
----> press "P" to copy this plot [pick one] to a new tab [thus preserving it]



Scale the plots for your own network [files in /home/ispsnoop/mainfind/]:
Overall: ispplot_options.py: complicated!
IN activity: fastISPgnuplot_optionsTCPin: sety2range [0:YourRange], sety2tics (.....):wq
OUT activity: fastISPgnuplot_optionsTCPout: currently automatic
Adjust "sleep 58" in checkfile1-file2.sh to achieve 1 minute cycle time.

ISP statistics, packet counts, overall bit rates

[Left] Cumulative DNS queries this month | [Right] Unique queries/last hour

```
0.disk.mechanicallydrug.com
       0.html-load.cc
       1.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.4.0.0.7.4.6.0.6.2.ip6.arpa
       1.0.0.1.in-addr.arpa
100.29.192.100  _services._dns-sd._udp.local
100.29.192.103  VERSION.BIND
100.29.192.110          VERSION.BIND
100.29.192.114  VERSION.BIND
100.29.192.123          VERSION.BIND
100.29.192.30   VERSION.BIND
```

```
04:02:AM queries: 14243 590
05:01:AM queries: 14243 660
06:01:AM queries: 14243 659
07:01:AM queries: 14244 663
08:01:AM queries: 14247 917
09:01:AM queries: 14257 1003
10:02:AM queries: 14269 781
11:02:AM queries: 14272 838
12:01:PM queries: 14284 790
13:02:PM queries: 14301 712
14:02:PM queries: 14309 753
```

VirusTotal URL check | Google URL check | Netcraft site info

Search DNS [sub]domain in month archive above: Submit

Last Hour Hosts Bits, Pkts

```
09:02: Last hour Pkts: 345962 Avg bits/sec: 1638399 IP&IPv6 host pairs -tmt&rcv: 533
```

Archive Summary -each hour [scroll down for latest]

```
Mon Mar 16 10:04:34 AM EDT 2026 Pkts last hour: 541237 Avg bits/s: 1704184 IP&IPv6 host pairs -tmt&rcv: 620
Mon Mar 16 11:04:24 AM EDT 2026 Pkts last hour: 671868 Avg bits/s: 2258944 IP&IPv6 host pairs -tmt&rcv: 720
Mon Mar 16 12:03:31 PM EDT 2026 Pkts last hour: 283384 Avg bits/s: 1078436 IP&IPv6 host pairs -tmt&rcv: 686
Mon Mar 16 01:04:07 PM EDT 2026 Pkts last hour: 415046 Avg bits/s: 3218529 IP&IPv6 host pairs -tmt&rcv: 583
Mon Mar 16 02:04:38 PM EDT 2026 Pkts last hour: 542831 Avg bits/s: 4230750 IP&IPv6 host pairs -tmt&rcv: 661
Mon Mar 16 03:04:51 PM EDT 2026 Pkts last hour: 598151 Avg bits/s: 4452042 IP&IPv6 host pairs -tmt&rcv: 773
Mon Mar 16 04:08:14 PM EDT 2026 Pkts last hour: 1298742 Avg bits/s: 8240886 IP&IPv6 host pairs -tmt&rcv: 725
Mon Mar 16 05:04:17 PM EDT 2026 Pkts last hour: 450495 Avg bits/s: 3743508 IP&IPv6 host pairs -tmt&rcv: 719
Mon Mar 16 06:04:23 PM EDT 2026 Pkts last hour: 472500 Avg bits/s: 3860901 IP&IPv6 host pairs -tmt&rcv: 734
Mon Mar 16 07:04:14 PM EDT 2026 Pkts last hour: 454787 Avg bits/s: 3879252 IP&IPv6 host pairs -tmt&rcv: 679
```

ISP TCP/UDP/DNS IP Lists. Click on Link to Download [could be MB of data]

Wed Jun 24 2026 8 AM (Eastern Daylight Time)

NOTE THIS APPLICABLE HOUR FOR BELOW DATA: refresh browser if necessary to sync browser. HOUR evaluated is PREVIOUS HOUR!

1: NORMAL+ABNORMAL: Last Hour ALL Inbound TCP SYN connection Attempts Count: 657 Unique: 388 [tcpsyn_TOrouter.txt]

Some of these Inbound TCP SYN connection attempts may succeed, most [unsolicited] are blocked by the router or LAN device.
1: NORMAL+ABNORMAL: Last Hour -unique- Inbound TCP SYN connection attempts NAME/PTR List. Submit and WAIT for list.

Run Unique Inbound TCP SYN connection ATTEMPT Report

#1-> Wait for tab to complete. Result: NAME/PTR List
These are Internet attempts to connect to your router or LAN [see end of list, or 3 below for successful attempts]

2: NORMAL: Last Hour TCP -total- session established TO INTERNET Count: 3038 [out_tcpsyn-ack.txt]

2: NORMAL: Last Hour -unique- TCP session established TO INTERNET Unique: 686 [explain_uniq_addr_out_tcpsyn-ack.txt]

2:NORMAL: Last Hour -unique- Outbound TCP SYN connection NAME/PTR List. Submit and WAIT for list.

Run Unique Outbound TCP SYN connection Report

#2-> Wait for tab to complete. Result: NAME/PTR List
This is normal "Internet access/browsing"

3: NORMAL?: Last Hour TCP sessions established TO ROUTER OR LAN DEVICE Count: 42 [count_in_tcpsyn-ack.txt] Unique: 12 [uniq_count_in_tcpsyn-ack.txt]

3: Last Hour TCP connections to my router, or my LAN DEVICE
IPv6 packets will show if a LAN IPv6 prefix and IPv6 port forwarding are configured. [uniq_addr-ports_in_tcpsyn-ack.txt]
TCP-SYNs represent ALL TCP SYNs from router, LAN. Normally corresponds to port forwards in your router.

```
Jun 24, 2026 08:15:02.164535569 EDT 108.144.11.81 35.137.208.94 5277 3313
Jun 24, 2026 08:30:01.731614553 EDT 2600:1700:111c:3270::49 2603:900b:b840:2b6e::254 37904 3313
Jun 24, 2026 08:30:01.571790753 EDT 2600:1702:4440:79c0::48 2603:900b:b840:2b6e::254 35096 3313
Jun 24, 2026 08:30:01.794206521 EDT 2600:382:b9f8:9675::48 2603:900b:b840:2b6e::254 32776 3313
Jun 24, 2026 08:15:02.150546694 EDT 2601:280:4900:142b:a946:b4b8:b451:a6fb 2603:900b:b840:2b6e::254 56046 3313
```

Legend: [Time SrcIP DestIP(me) SrcPort DstPort(me)!]
Time record/Archive of connections

4: NORMAL: Last Hour DNS queries Count[unique]: 1522 DNS queries this month [large file!]

Search DNS [sub]domain in Last Hour above: Submit

Search DNS [sub]domain in Month Archive above: Submit

5. NORMAL: Last Hour UDP unique outbound packets [not incl DNS, normal] Total Count: 31142 [Lispcapudp_out.txt]]

5. NORMAL+ABNORMAL: Last Hour UDP unique inbound packets [not incl DNS, normal] Total Count: 27399 [Lispcapudp_in.txt]

6. NORMAL: Last Hour UDP -UNIQUE- solicited packets [not incl DNS, normal] Count: 47 [solicited_keys.txt]

6. NORMAL: Last Hour UDP solicited packets List NAME/PTR recovery attempt. Submit and WAIT for list.

Run Unique -solicited- UDP Address Report

#6-> Wait for tab to complete. Result: NAME/PTR List
This is normal UDP traffic: QUIC, streaming.....

7: ABNORMAL: Last Hour unsolicited inbound UDP packets [not incl DNS,NTP responses] Count [unique]: 28 [unsolicited_keys.txt]

7. Last Hour -unique- inbound unsolicited UDP packets List NAME/PTR recovery attempt. Submit and WAIT for list.

Run Unique -unsolicited-INPUT UDP Address Report

#7-> Wait for tab to complete. Result: NAME/PTR List
This is unexpected/uninvited UDP traffic in, normally just dropped.

CAUTION: invoking the "Run Unique" scripts generate traffic that winds up in the traffic which is collected [assuming you access ispsnoop over the same ISP that you are watching it with!] This of course represents a loopback of sorts!!

Last Hour ISP Traffic Snapshot & Visit Map -including following 10 hour tracking of ISP

Submit an IP address to view its last hour/last 10 hour activity.
You must WAIT for browser tab to complete. It may take 10-20 minutes depending on pkt count.

Last Hour Info for ISP IP: Error Error **Collection Date:** Error **for previous hour starting at:** Error

Enter ISP IP address for new Last Hour query: Submit

Currently Plotting IP visits: Error

Change to YES or NO to plot: Submit

CHECK DATE ON MAP: Browser -Shift- refresh to get latest. ZOOM IN for detail:many locations are same CDN, cloud farms

404 Not Found

Detailed IP statistics for above IP query: Collection Date: Error **for previous hour starting at:** Error

Error

Download bSNI file for AI analysis Download [last hour] full pcap: pcap file Could be <=2GB!

[this] IP visits: Collection Date: Error **for previous hour starting at:** Error

Error

[this] IP DNS queries Collection Date: Error **for previous hour starting at:** Error

Month-to-date [this] IP DNS queries [device IP address constant?]:

10 Hour IP Tracking of above IP selection [or cutoff at 11PM collection].
This hourly tracking follows the IP traffic snapshot specified above. [restarted with a new capture]

10 hour tracking of IP visits -or stopped at 11AM collection: Start Tracking Date: Error **Tracking hour n of 10 Active?** **>0 is active**

Error

10 hour tracking of IP dns queries -or stopped at 11AM collection: Start Tracking Date: Error **Tracking hour Iteration: n of 10**

Error

Interpreting "diff -y" output: example Left column File A, right column File B
Apple Apple
Banana | Blueberries
Cherry <
> Dragonfruit
Row 1: Identical (no symbol).
Row 2 (|): Both files have a second line, but "Banana" was changed to "Blueberries".
Row 3 (<): "Cherry" exists in File A but was deleted in File B.
Row 4 (>): "Dragonfruit" does not exist in File A but was added to File B.

Daily GreyNoise Check -> this is a site that checks if your IP has been sighted doing bot activity!
This may or may not be useful. If you have a "static" or "quasi" static IP, it can signify bot activity along with the plots.

Note when your Internet -ipv4- IP last changed. IP address archive:

Error

NOTE: This -Force Refresh- button is not working ! as of 12-6-2025. Use this direct link: [greynoise bot check page]

GreyNoise check already performed today. Use Force Refresh to reload.

Force Refresh

Synthient.com check: This is another website that will check your IP for malicious activity, specifically the use of your IP address for proxying!
Enter your IP or domainname in the Lookup box.
[synthient proxy check page]

Details / Anomalies: [nonDHCP addresses][LAN on IOT!]

404 Not Found

Error | Error | Error

<-Scan of non-DHCP IOTs

5X packet spike captures saved as "iotcapture.pcap.5X" and "iotcapdns.txt.5X".

These are in /home/pi/tests/iothosts or its dnswork subfolder.