# Computer Networks: Assignment 1

Students Astha Meena (2021CS10122), Bhupesh (2021CS10101)

## Network Analysis

- a) **Traceroute from mobile hotspot to www.iitd.ac.in via wifi .**

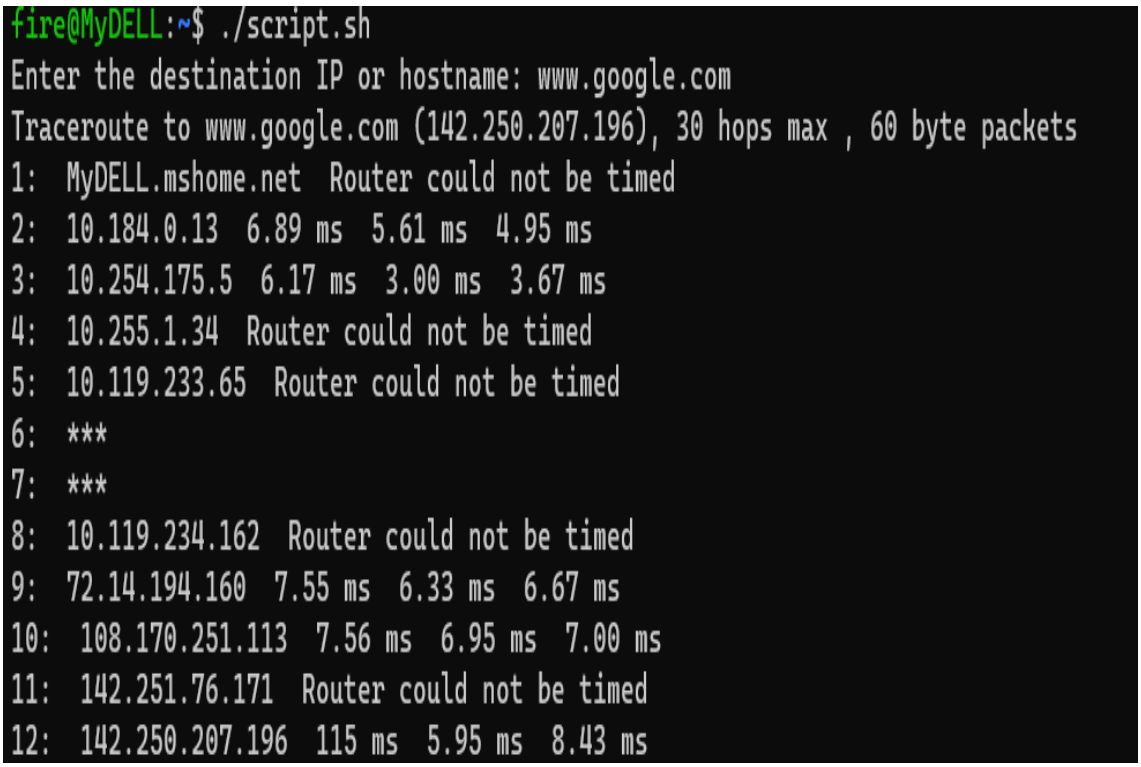
```
C:\Users\bhupe>tracert www.iitd.ac.in

Tracing route to www.iitd.ac.in [2001:df4:e000:29::212]
over a maximum of 30 hops:

  1    52 ms     7 ms     3 ms  2409:4050:2d90:c421::e2
  2     *        *        *     Request timed out.
  3    48 ms   177 ms    72 ms  2405:200:331:eeee:20::808
  4   181 ms    57 ms    79 ms  2405:200:801:300::e78
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8   127 ms    49 ms    52 ms  2405:203:982:68d::6
  9    79 ms    43 ms    55 ms  2405:203:982:68d::e
 10    90 ms    68 ms    60 ms  2405:8a00:a:1::3
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13    36 ms    58 ms    62 ms  2001:4408:a::1
 14    73 ms    41 ms    54 ms  2405:8a00:a:2::c5
 15    65 ms    54 ms    56 ms  2405:8a00:a:2::c6
 16    85 ms    34 ms    59 ms  2001:df4:e000:108::2
 17    47 ms    63 ms   168 ms  2001:df4:e000:26::24
 18    61 ms    43 ms    50 ms  2001:df4:e000:29::212

Trace complete.
```

- b) **Curious things noted during the traceroute.**
  - Trace route by default performs maximum 30 hops and sends 3 packets each hop.
  - Traceroute might use IPv6 due to network settings, but you can force IPv4 with "-4" flag (e.g., traceroute -4 destination).
  - Traceroute passing through 10.x.x.x, 172.x.x.x, or 192.168.x.x in the same hop of traceroute suggests internal networks before the public internet.
  - Missing Routers or Unresponsive Nodes were encountered where Request timed out was received as output. Gaps in traceroute indicate non-responsive routers due to firewalls, congestion, etc.
  - Different times between hops indicate network congestion, routing variations, or performance differences.
- c) **Maximum size of packet over ping**
  - **1472** . The maximum packet size allowed for transmission is 1500 bytes, with 28 bytes allocated for the header.
  - As a result, our ping command operates by sending individual packets. The actual size of the largest packet that can be utilized is determined by the specific link layer. Consequently, the effective limit is calculated to be 1472 bytes.
  - The ping command uses the ICMP Echo Request Packets. The typical maximum packet size for ICMP Echo Request packets is determined by the Maximum Transmission Unit (MTU) of the network, which is often around 1500 bytes for standard Ethernet networks.
  - Each such packet sent over has IP and ICMP headers mandatorily of 28 bytes in them, Hence our observed packet limit of 1472 in this context is around the network constraints of ethernet network which we used.

# Traceroute Using ping

- **Script Functionality** We created a shell script to replicate traceroute using the ping command. The script utilizes the *"ping -t ttl destination"* command, allowing us to set a *Time-to-Live (TTL)* value for reaching the destination. The TTL value is incremented from 1 to a maximum of 30, mirroring traceroute's default hop limit.
- **Documentation Process**

  For each TTL value, we recorded the reached IP address. Using another ping command with the current intermediate IP address as the destination, we measured the time taken to reach that point.
- **Handling Secured or Untraceable Intermediates**

  Intermediate IP addresses that were secured and untraceable were marked with "***". Some intermediate routers couldn't be timed due to unresponsiveness to ping command.
- **Reproduced Traceroute Functionality** Our script successfully emulates the traceroute functionality by monitoring various router IP addresses along the path to the destination.
- 


# Internet architecture

- **AS Number for the IP addressess**

| AS | AS Number | IP address |
|---|---|---|
| UTAH | 17055 | 155.98.186.21 |
| UCT | 36982 | 137.158.159.192 |
| Indian Institute of technology | 132780 | 103.27.9.24 |
| google | 15169 | 142.250.207.196 |
| Facebook | 32934 | 157.240.16.35 |

- **A) Table for the Number of Hopes from Different Source to the Destination**

– Traceroute Source is Equinix New York(NY9) IP address of the source 216.218.252.22

| Destination | Number of Hopes |
|---|---|
| www.utha.edu | 15 |
| www.uct.ac.za | 11 |
| www.iitd.ac.in | 17 |
| www.google.com | 11 |
| www.facebook.com | 8 |

– Traceroute Source is Equinix Osaka (OS1) IP address of the source (216.218.252.58), Japan

| Destination | Number of Hopes |
|---|---|
| www.utha.edu | 16 |
| www.uct.ac.za | 17 |
| www.iitd.ac.in | 15 |
| www.google.com | 10 |
| www.facebook.com | 9 |

– Traceroute form my Mobile Network via Wifi

| Destination | Number of Hopes |
|---|---|
| www.utha.edu | 28 |
| www.uct.ac.za | 29 |
| www.iitd.ac.in | 17 |
| www.google.com | 9 |
| www.facebook.com | 9 |

– **Some Key points observed during the traceroute.**

* **Effect of Geographical distance of the source from the destination on Hops**: If the sources and destinations of the traceroute are near together, there may be fewer hops overall. As there will be fewer routers, gateways, and subnets to pass, there are more likely to be fewer network nodes and routers in between. We cannot, however, generalize this assertion because other elements, such as network coverage, traffic, and routing regulations, can also affect the number of hops. For instance, because the University of Utah is nearer to New York than Osaka, Japan, the traceroute from New York required less hops.
* Google and Facebook both use networks and data centers spread across the world. Google and Facebook exhibit notable uniformity in the amount of hops, typically fewer hops, across many traceroute providers. This is because their provider uses dedicated paths, sound network protocol policies, and efficient routing; however, hops counts may vary depending on factors including traffic volume, network congestion, and changes in routing.

- **B) Latencies between the traceroute sources and the web servers**
  **Equinix New York(NY9) IP address of the source 216.218.252.22**

| Destination | Range of Latenices(RTT) |
|---|---|
| www.utha.edu | 72.812 ms-76.926 ms |
| www.uct.ac.za | 233.000 ms- 240.326 ms |
| www.iitd.ac.in | 227.831 ms-227.951 ms |
| www.google.com | 63.980 ms- 71.135 ms |
| www.facebook.com | 79.227 ms-81.606 ms |

**Source is Equinix Osaka (OS1) IP address of the source (216.218.252.58)**

| Destination | Range of Latenices(RTT) |
|---|---|
| www.utha.edu | 110.988 ms - 112.187 ms |
| www.uct.ac.za | 353.935 ms- 354.040 ms |
| www.iitd.ac.in | 256.705 ms-257.048 ms |
| www.google.com | 113.399 ms - 113.746 ms |
| www.facebook.com | 140.007 ms -140.417 ms |

**Source is cellular mobile network via wifi**

| Destination | Range(RTT) |
|---|---|
| www.utha.edu | 299ms - 358ms |
| www.uct.ac.za | no packet received |
| www.iitd.ac.in | 28ms - 82ms |
| www.google.com | 52ms - 89ms |
| www.facebook.com | 30.ms - 52.9ms |

  - Yes, the latency in a traceroute can related to the number of hops, and it generally increases as the number of hops increases. This phenomenon is due to the delays introduced at each intermediate network device (router or gateway) that the packets pass through which increasing the number of hops Here are some of the reasons for the delays:-
    * Network Congestion and Queueing of packets
    * which Routing Protocol is used
    * time taken by the network device to process the packets
    * Load Balancing at a particular server.

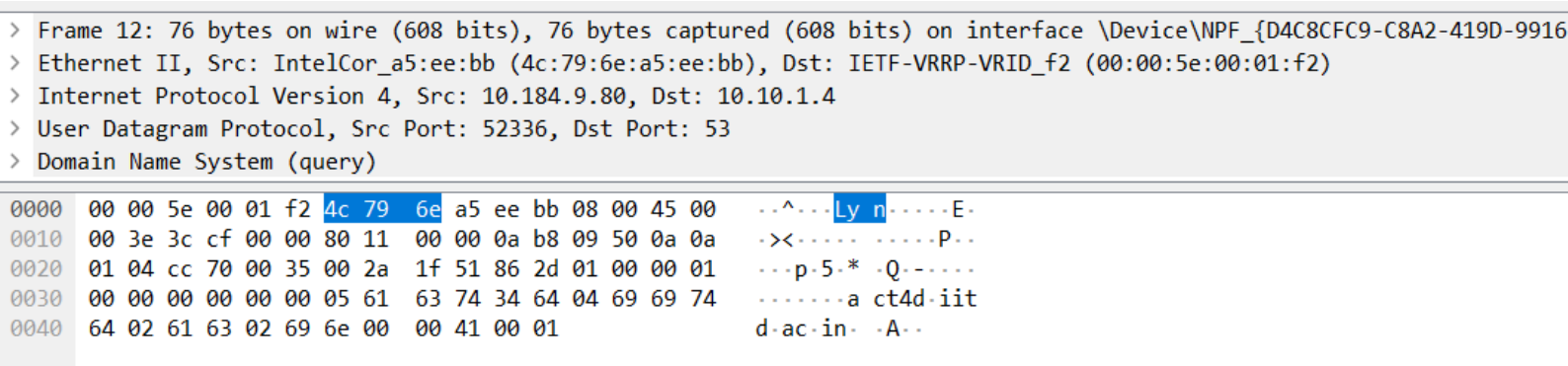
- **C)**The same IP address is used to resolve the destinations www.utah.edu, www.uct.ac.za, and www.iitd.ac.in in tracer-oute from several sources. When accessed from several sources, websites like www.google.com and www.facebook.com display multiple IP addresses. This may be because some businesses maintain many data centers around the globe to guarantee high availability, lessen server load, and provide redundancy across various routes. Users are routed to the closest location when they submit inquiries from several places, which results in distinct IP addresses.

- **D)** Facebook and Google provide distinct IP addresses on the traceroute from the same starting point for my traceroute. Due to the intricacy of routing protocols, network congestion, server load, and load balancing, the pathways can appear different when traceroutes are done from the same starting point.Large web servers are typically where this kind of problem appears. The longest path will be taken if our traceroute was mapped to an IP address that is geographically the most remote from the source.

- **E)** Greece, Sweden, and China are some of countries whose local ISPs are not directly peered with Google and Facebook. Traceroute form this country to Google and Facebook have some other intermediate IP addresses also.

## Packet Analysis

- **a) DNS Queries and Responses**:




**DNS Query to http://act4d.iitd.ac.in**

```
Frame 14: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface \Device\NPF_{D4C8CFC9-C8A2-419D-9916
Ethernet II, Src: Cisco_1b:48:73 (5c:3e:06:1b:48:73), Dst: IntelCor_a5:ee:bb (4c:79:6e:a5:ee:bb)
Internet Protocol Version 4, Src: 10.10.1.4, Dst: 10.184.9.80
User Datagram Protocol, Src Port: 53, Dst Port: 52336
Domain Name System (response)
```

```
0000  4c 79 6e a5 ee bb 5c 3e  06 1b 48 73 08 00 45 00   Lyn···\> ··Hs··E·
0010  00 73 4b 13 40 00 3d 11  d3 51 0a 0a 01 04 0a b8   ·sK·@·=· ·Q·····
0020  09 50 00 35 cc 70 00 5f  d0 15 86 2d 81 80 00 01   ·P·5·p·_ ···-····
0030  00 00 00 01 00 00 05 61  63 74 34 64 04 69 69 74   ·······a ct4d·iit
0040  64 02 61 63 02 69 6e 00  00 41 00 01 c0 12 00 06   d·ac·in· ·A······
0050  00 01 00 01 51 80 00 29  06 69 6e 74 64 6e 73 c0   ····Q··) ·intdns·
0060  12 06 73 79 73 61 64 6d  02 63 63 c0 12 78 95 c4   ··sysadm ·cc··x··
0070  29 00 00 2a 30 00 00 0e  10 00 05 7e 40 00 01 51   )··*0··· ···~@··Q
0080  80                                                 ·
```

**DNS Response from www.iitd.ac.in**

After doing DNS packet analysis using wireshark while visiting http://act4d.iitd.ac.in we got a DNS query and response of Type A (which is used to figure out the IP address of the website) and a DNS query and response related to HTTPS . All these DNS request and response took 5.239 ms in execution.
We also did DNS packet analysis using wire shark while visiting www.iitd.ac.in which took comparatively more DNS queries and response due to redirection happening to home.iitd.ac.in All these DNS requests and responses took 74.842 ms in execution

- **b)HTTP Requests in Packet Trace**:

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 40 | 12.620126 | 10.184.9.80 | 10.237.26.108 | HTTP | 458 | GET / HTTP/1.1 |
| 52 | 13.101338 | 10.237.26.108 | 10.184.9.80 | HTTP/X… | 574 | HTTP/1.1 200 OK |
| 54 | 13.138451 | 10.184.9.80 | 10.237.26.108 | HTTP | 472 | GET /act4d/media/system/js/mootools.js HTTP/1.1 |
| 61 | 13.143815 | 10.184.9.80 | 10.237.26.108 | HTTP | 491 | GET /act4d/templates/beez/css/template.css HTTP/1.1 |
| 73 | 13.148430 | 10.184.9.80 | 10.237.26.108 | HTTP | 491 | GET /act4d/templates/beez/css/position.css HTTP/1.1 |
| 74 | 13.148626 | 10.184.9.80 | 10.237.26.108 | HTTP | 489 | GET /act4d/templates/beez/css/layout.css HTTP/1.1 |
| 75 | 13.148779 | 10.184.9.80 | 10.237.26.108 | HTTP | 490 | GET /act4d/templates/beez/css/general.css HTTP/1.1 |
| 76 | 13.148923 | 10.184.9.80 | 10.237.26.108 | HTTP | 471 | GET /act4d/media/system/js/caption.js HTTP/1.1 |
| 83 | 13.159795 | 10.237.26.108 | 10.184.9.80 | HTTP | 99 | HTTP/1.1 200 OK (text/css) |
| 93 | 13.161377 | 10.184.9.80 | 10.237.26.108 | HTTP | 466 | GET /wiki1-bak/wiki1/statf0e.php HTTP/1.1 |
| 119 | 13.167756 | 10.237.26.108 | 10.184.9.80 | HTTP | 323 | HTTP/1.1 200 OK (text/css) |
| 123 | 13.168117 | 10.237.26.108 | 10.184.9.80 | HTTP | 68 | HTTP/1.1 404 Not Found (text/html) |
| 132 | 13.170697 | 10.237.26.108 | 10.184.9.80 | HTTP | 290 | HTTP/1.1 200 OK (application/javascript) |
| 141 | 13.171762 | 10.237.26.108 | 10.184.9.80 | HTTP | 153 | HTTP/1.1 200 OK (text/css) |
| 155 | 13.176114 | 10.237.26.108 | 10.184.9.80 | HTTP | 165 | HTTP/1.1 200 OK (application/javascript) |
| 163 | 13.180087 | 10.237.26.108 | 10.184.9.80 | HTTP | 558 | HTTP/1.1 200 OK (text/css) |
| 165 | 13.181445 | 10.184.9.80 | 10.237.26.108 | HTTP | 537 | GET /act4d/templates/beez/images/act4d.png HTTP/1.1 |
| 166 | 13.186463 | 10.184.9.80 | 10.237.26.108 | HTTP | 526 | GET /act4d/images/balazahir.jpg HTTP/1.1 |
| 168 | 13.190129 | 10.184.9.80 | 10.237.26.108 | HTTP | 488 | GET /act4d/templates/beez/css/print.css HTTP/1.1 |
| 190 | 13.195231 | 10.237.26.108 | 10.184.9.80 | HTTP | 254 | HTTP/1.1 200 OK (text/css) |
| 830 | 13.290510 | 10.237.26.108 | 10.184.9.80 | HTTP | 529 | HTTP/1.1 200 OK (PNG) |
| 1305 | 13.364602 | 10.237.26.108 | 10.184.9.80 | HTTP | 161 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 1307 | 13.429646 | 10.184.9.80 | 10.237.26.108 | HTTP | 532 | GET /act4d/templates/beez/favicon.ico HTTP/1.1 |
| 1310 | 13.434817 | 10.237.26.108 | 10.184.9.80 | HTTP | 462 | HTTP/1.1 200 OK (image/x-icon) |

**HTTP requests for http://act4d.iitd.ac.in**

| | | | | | |
|---|---|---|---|---|---|
| 39 | 13.071339 | 10.184.9.80 | 10.10.211.212 | HTTP | 456 GET / HTTP/1.1 |
| 41 | 13.077066 | 10.10.211.212 | 10.184.9.80 | HTTP | 495 HTTP/1.1 302 Found (text/html) |

**HTTP requests for http://act4d.iitd.ac.in**

- Upon applying the "HTTP" filter to the packet trace in Wireshark, it was observed that 24 HTTP-related entries were captured for http://act4.d.iitd.ac.in and 2 HTTP-related entries were captured for www.iitd.ac.in
- In each case , half of the entries were GET requests and their acknowledgments,which were replied with a 200 status code.
- One of the request was also reported as not found. While the only HTTP response for www.iitd.ac.in was replied with a status code "302 Modified Temporarily" suggests a temporary modification of the requested resource.
- The website http://act4d.iitd.ac.in also reported Additional resources like images, stylesheets, scripts, and other assets, which initiate only after the initial HTML request. Web browsers initially process the provided HTML content, and subsequently, they pursue included links and references to retrieve extra resources(images, CSS, JavaScript). This collective effort leads to the comprehensive display of a webpage. This tells the process through which browsers render complex webpages with images and various other style-based files.

- c) **Investigating TCP Connections**

gs.syn == 1 and tcp.flags.ack== 0

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 15 | 10.551895 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57501 → 443 [SYN] Seq=0 Win=64240 |
| 17 | 10.804973 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57502 → 443 [SYN] Seq=0 Win=64240 |
| 19 | 11.054871 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57501 → 443 |
| 21 | 11.318502 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57502 → 443 |
| 23 | 11.568472 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57501 → 443 |
| 25 | 11.833581 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57502 → 443 |
| 27 | 12.081359 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57501 → 443 |
| 29 | 12.347735 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57502 → 443 |
| 31 | 12.596858 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57501 → 443 |
| 37 | 12.613793 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57503 → 80 [SYN] Seq=0 Win=64240 |
| 42 | 12.863309 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | [TCP Retransmission] 57502 → 443 |
| 55 | 13.139736 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57504 → 80 [SYN] Seq=0 Win=64240 |
| 56 | 13.141690 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57505 → 80 [SYN] Seq=0 Win=64240 |
| 60 | 13.143522 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57506 → 80 [SYN] Seq=0 Win=64240 |
| 62 | 13.144169 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57507 → 80 [SYN] Seq=0 Win=64240 |
| 63 | 13.144472 | 10.184.9.80 | 10.237.26.108 | TCP | 66 | 57508 → 80 [SYN] Seq=0 Win=64240 |

**TCP requests monitored while visiting http://act4d.iitd.ac.in**

The above TCP requests were filtered about allowing only SYN requests using "tcp.flags" filter. The TCP ports are displayed at the ends of arrows in the Info of the requests. The first 10 TCP requests shown here which have a TCP port numbered 443 do not have a TCP port catering to http requests and are most probably TCP requests not related to the exchange of data.

- **http://act4d.iitd.ac.in**
  - A total of **six** distinct TCP connections were identified between the browser and the web server which cater to the HTTP requests.
  - These TCP connections are distinguished by one TCP port number being 80 for the HTTP requests.The HTTP requests are specifically fetched from the connections of other port numbers being 57503-57508.

    * Comparing the number of TCP connections with the number of HTTP requests, the number of HTTP requests was much more than the number of TCP requests. This is because a single TCP connection was used to fetch multiple HTTP requests. This enhances efficiency by minimizing the need to create new connections for every resource.
    * Furthermore, it was observed that some content objects were indeed fetched over the same TCP connection.

- d) **Absence of traceable data of webpage**
  - On doing HTTP filter in Wireshark, there was no HTTP traffic coming from www.indian.express.com. No traffic of html and javascript files was also not encountered when we browsed through the entire trace without any filters.
  - The reason for this could be that HTTP traffic is encrypted, so Wireshark won't be able to decipher the payload of the packets unless we have administrative rights or SSL encryption key. We won't be able to see content of HTML and javascript files being transferred as explained above content of the packets will be encrypted and we constantly get encryption alerts in the trace. This is a security feature that ensures data privacy during transmission.