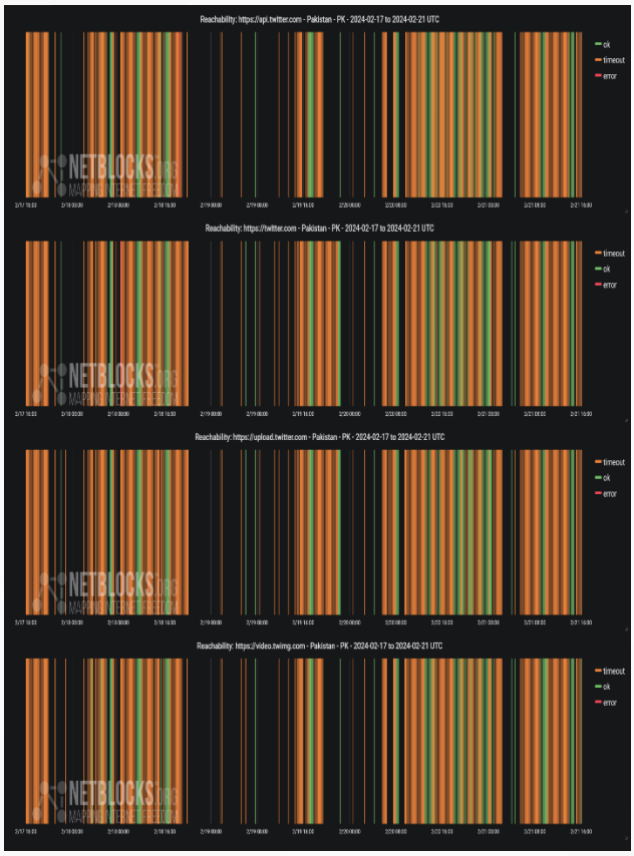
# PTA's Geo-Blocking

## HTTP Interception Tactics to Bar "X"

## Via possible Akamai's Infrastructure


**Authors**
Anees Qureshi, OSINT Analyst, Bytes for All (B4A)
Haroon Baloch, Sr. Program Manager, Bytes for All (B4A)

www.bytesforall.pk

**Disclaimer**

The conclusions drawn in this report are based on analysis conducted using available network traffic data and Open-Source Intelligence (OSINT) tools for network troubleshooting and tracing middleboxes, etc. While efforts were made to ensure accuracy, false positives may occur due to the complexity of the internet censorship techniques and limitations in data collection and analysis.

**Introduction**

X (formerly Twitter) a prominent social media platform has been inaccessible in Pakistan as of February 17, 2024. This report aims to analyze the blocking mechanism employed by the Pakistan Telecommunication Authority (PTA) to restrict access to X within the country. Through a detailed analysis of network traffic data and traceroute examinations, this study aims to understand the methods employed by PTA for censorship, their implications, and the broader context of internet censorship in Pakistan. Analysis of network traffic captured during attempted access to X reveals the blocking mechanism utilized by the PTA, which are discussed below in the results section.

*Figure 1*
*An internet scanning tool confirms blocking of X by means of HTTP*

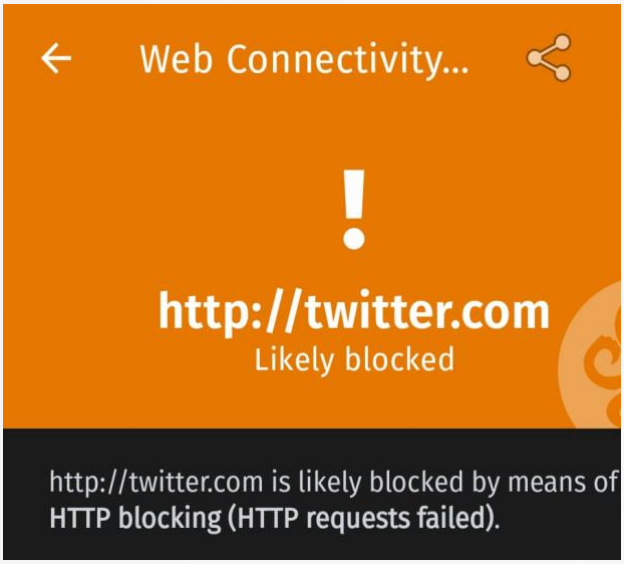
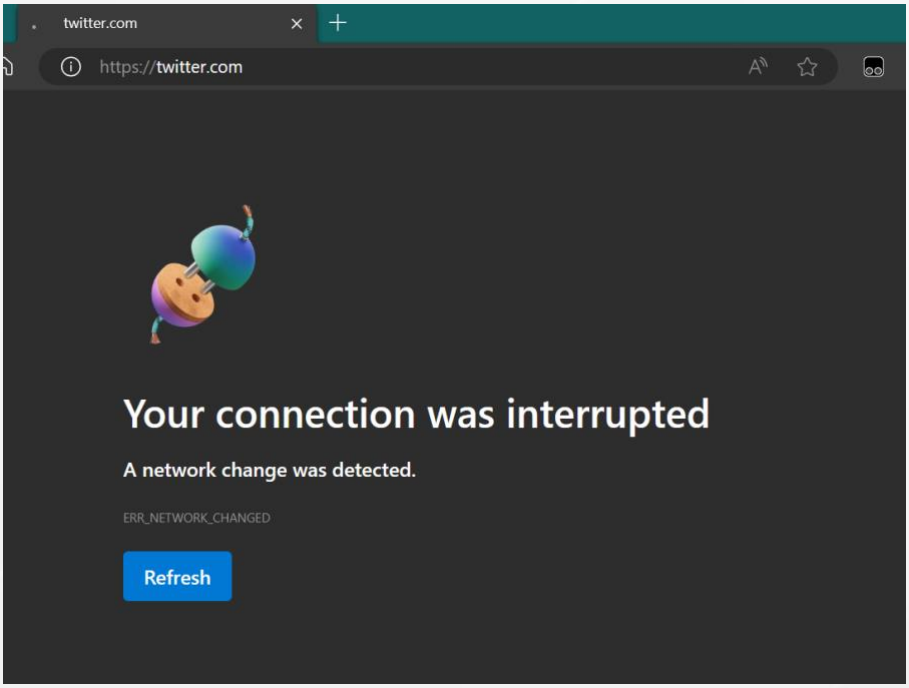



*Figure 2*
*Accessing X through browser confirms traffic interruption*



**Methodology:**

Network examination was performed with the help of OSINT tools available through GitHub to reveal blocking mechanisms. The captured packets provide insights into the network behavior, including source and destination IP addresses, port numbers, and TCP flags, allowing for a comprehensive understanding of the blockage technique.

**Results:**

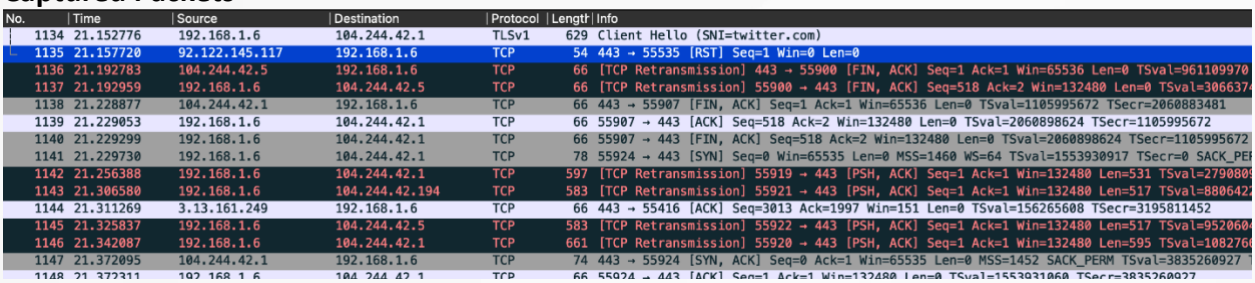
The results of the analysis detailing the methods of censorship deployed by authorities to block access to X in Pakistan. This includes the identification of TCP Reset (RST) packets deployed by Content Delivery Networks (CDNs) to terminate connections to X servers, effectively blocking access to the platform within the country.

Below discussed sequence of packets indicate attempts to establish a connection with X's servers (twitter.com; 104.244.42.1) in packet 1134 and was refused to connect in packet 1135 by RST flag deployed by Akamai CDN (92.122.145.117).

**What is CDN?**

A content delivery network (CDN) is a geographically distributed group of servers that caches content close to end users. A CDN allows for the quick transfer of assets needed for loading Internet content, including HTML pages, JavaScript files, stylesheets, images, and videos. Akamai Content Delivery Network (CDN) is a network of servers that speeds up the delivery of web content to users around the world. It is used to deliver websites, applications, and media files.

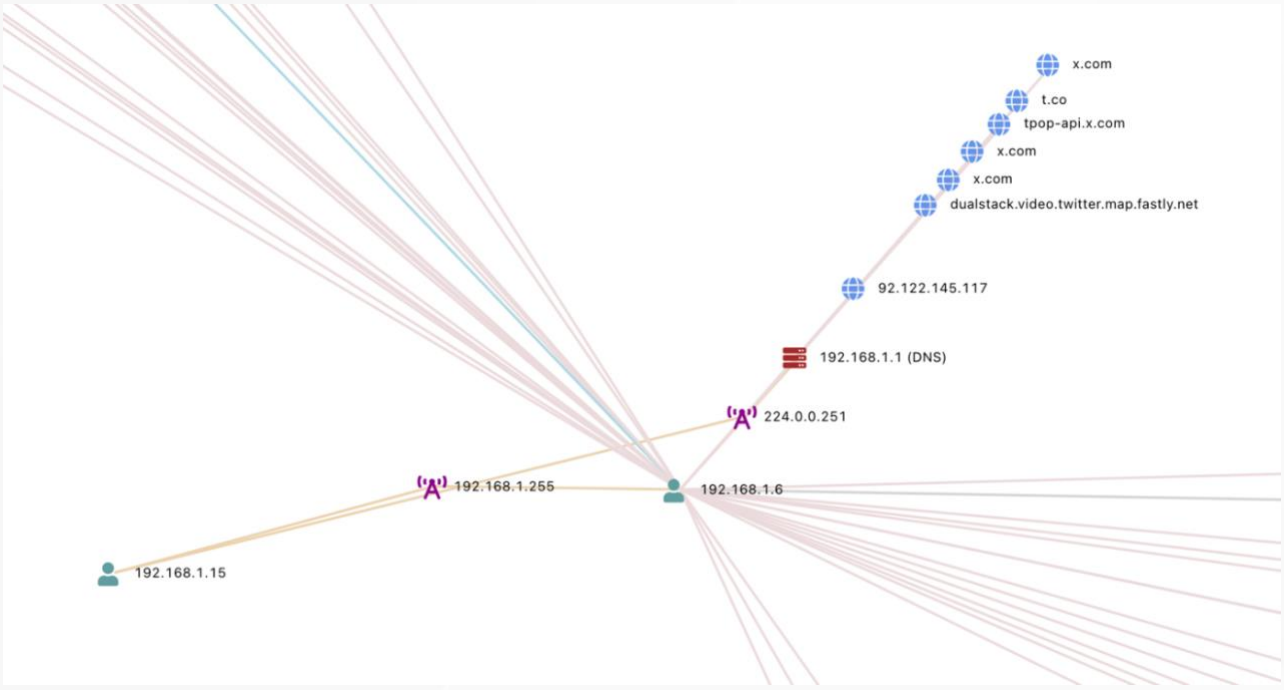
**Captured Packets**



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1134 | 21.152776 | 192.168.1.6 | 104.244.42.1 | TLSv1 | 629 | Client Hello (SNI=twitter.com) |
| 1135 | 21.157720 | 92.122.145.117 | 192.168.1.6 | TCP | 54 | 443 → 55535 [RST] Seq=1 Win=0 Len=0 |
| 1136 | 21.192783 | 104.244.42.5 | 192.168.1.6 | TCP | 66 | [TCP Retransmission] 443 → 55900 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=961109970 |
| 1137 | 21.192959 | 192.168.1.6 | 104.244.42.5 | TCP | 66 | [TCP Retransmission] 55900 → 443 [FIN, ACK] Seq=518 Ack=2 Win=132480 Len=0 TSval=306637 |
| 1138 | 21.228877 | 104.244.42.1 | 192.168.1.6 | TCP | 66 | 443 → 55907 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1105995672 TSecr=2060883481 |
| 1139 | 21.229053 | 192.168.1.6 | 104.244.42.1 | TCP | 66 | 55907 → 443 [ACK] Seq=518 Ack=2 Win=132480 Len=0 TSval=2060898624 TSecr=1105995672 |
| 1140 | 21.229299 | 192.168.1.6 | 104.244.42.1 | TCP | 66 | 55907 → 443 [FIN, ACK] Seq=518 Ack=2 Win=132480 Len=0 TSval=2060898624 TSecr=1105995672 |
| 1141 | 21.229730 | 192.168.1.6 | 104.244.42.1 | TCP | 78 | 55924 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1553930917 TSecr=0 SACK_PE |
| 1142 | 21.256388 | 192.168.1.6 | 104.244.42.1 | TCP | 597 | [TCP Retransmission] 55919 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=531 TSval=2790809 |
| 1143 | 21.306580 | 192.168.1.6 | 104.244.42.194 | TCP | 583 | [TCP Retransmission] 55921 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=517 TSval=8806422 |
| 1144 | 21.311269 | 3.13.161.249 | 192.168.1.6 | TCP | 66 | 443 → 55416 [ACK] Seq=3013 Ack=1997 Win=151 Len=0 TSval=156265608 TSecr=3195811452 |
| 1145 | 21.325837 | 192.168.1.6 | 104.244.42.5 | TCP | 583 | [TCP Retransmission] 55922 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=517 TSval=952060 |
| 1146 | 21.342087 | 192.168.1.6 | 104.244.42.1 | TCP | 661 | [TCP Retransmission] 55920 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=595 TSval=1082760 |
| 1147 | 21.372095 | 104.244.42.1 | 192.168.1.6 | TCP | 74 | 443 → 55924 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM TSval=3835260927 |

- 1134 21.152776 192.168.1.6 104.244.42.1 TLSv1 629 Client Hello (SNI=twitter.com)
- 1135 21.157720 92.122.145.117 192.168.1.6 TCP 54 443 → 55535 [RST] Seq=1 Win=0 Len=0
- 1136 21.192783 104.244.42.5 192.168.1.6 TCP 66 [TCP Retransmission] 443 → 55900 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=961109970 TSecr=306621919
- 1137 21.192959 192.168.1.6 104.244.42.5 TCP 66 [TCP Retransmission] 55900 → 443 [FIN, ACK] Seq=518 Ack=2 Win=132480 Len=0 TSval=306637453 TSecr=961109570
- 1138 21.228877 104.244.42.1 192.168.1.6 TCP 66 443 → 55907 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1105995672 TSecr=2060883481
- 1139 21.229053 192.168.1.6 104.244.42.1 TCP 66 55907 → 443 [ACK] Seq=518 Ack=2 Win=132480 Len=0 TSval=2060898624 TSecr=1105995672
- 1140 21.229299 192.168.1.6 104.244.42.1 TCP 66 55907 → 443 [FIN, ACK] Seq=518 Ack=2 Win=132480 Len=0 TSval=2060898624 TSecr=1105995672
- 1141 21.229730 192.168.1.6 104.244.42.1 TCP 78 55924 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1553930917 TSecr=0 SACK_PERM
- 1142 21.256388 192.168.1.6 104.244.42.1 TCP 597 [TCP Retransmission] 55919 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=531 TSval=279080990 TSecr=618325165
- 1143 21.306580 192.168.1.6 104.244.42.194 TCP 583 [TCP Retransmission] 55921 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=517 TSval=880642292 TSecr=6971897
- 1144 21.311269 3.13.161.249 192.168.1.6 TCP 66 443 → 55416 [ACK] Seq=3013 Ack=1997 Win=151 Len=0 TSval=156265608 TSecr=3195811452
- 1145 21.325837 192.168.1.6 104.244.42.5 TCP 583 [TCP Retransmission] 55922 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=517 TSval=952060457 TSecr=1659474569

- 1146 21.342087 192.168.1.6 104.244.42.1 TCP 661 [TCP Retransmission] 55920 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=595 TSval=1082766194 TSecr=2314919247
- 1147 21.372095 104.244.42.1 192.168.1.6 TCP 74 443 → 55924 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM TSval=3835260927 TSecr=1553930917 WS=256
- 1148 21.372311 192.168.1.6 104.244.42.1 TCP 66 55924 → 443 [ACK] Seq=1 Ack=1 Win=132480 Len=0 TSval=1553931060 TSecr=3835260927
- 1149 21.372829 192.168.1.6 104.244.42.1 TLSv1 629 Client Hello (SNI=twitter.com)
- 1150 21.417930 104.244.42.1 192.168.1.6 TCP 66 [TCP Retransmission] 443 → 55906 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2264484376 TSecr=3642718608
- 1150 21.417930 104.244.42.1 192.168.1.6 TCP 66 [TCP Retransmission] 443 → 55906 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2264484376 TSecr=3642718608
- 1151 21.418030 192.168.1.6 104.244.42.1 TCP 66 [TCP Retransmission] 55906 → 443 [FIN, ACK] Seq=532 Ack=2 Win=132480 Len=0 TSval=3642734140 TSecr=2264483977
- 1152 21.517371 192.168.1.6 104.244.42.1 TCP 629 [TCP Retransmission] 55923 → 443 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=563 TSval=1017934956 TSecr=3835260707
- 1153 21.593759 104.244.42.5 192.168.1.6 TCP 66 [TCP Retransmission] 443 → 55900 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=961110371 TSecr=306621919

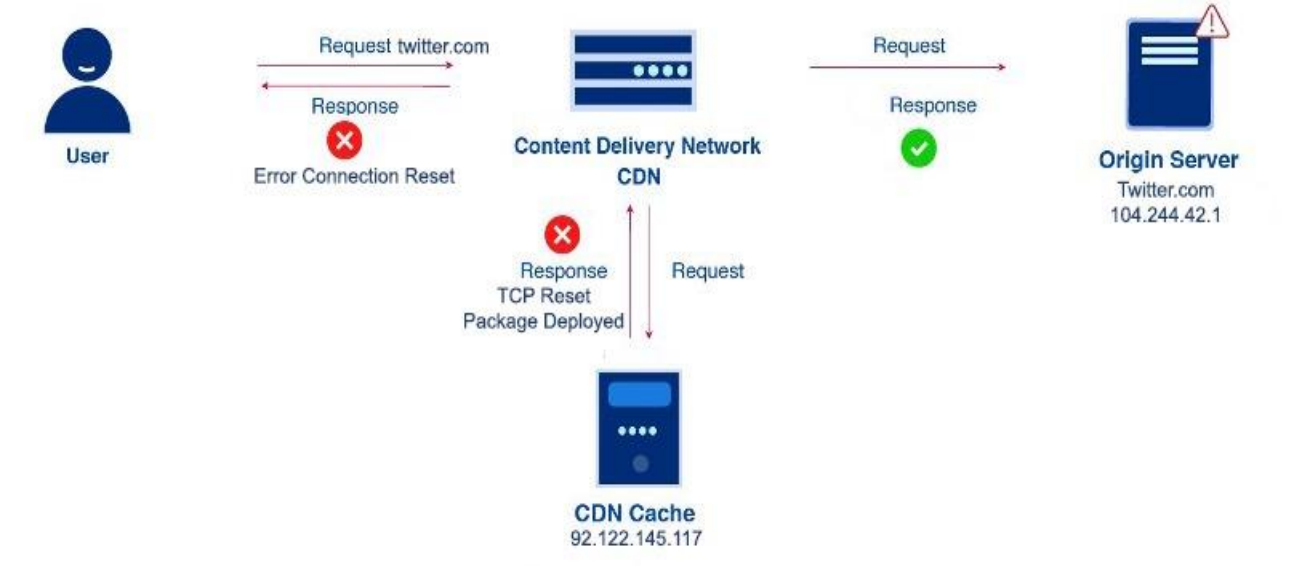



**Packets 1134 and 1149:**
These packets contain a Client Hello message indicating an attempt to initiate a TLS handshake with the server for the domain twitter.com.
**Packets 1135:**
This packet is a TCP packet with a [RST] flag, indicating a reset sent by the remote host Akamai CDN (92.122.145.117) to terminate the connection abruptly.
**Packets 1136 and 1137:**
These are TCP retransmissions of a FIN-ACK packet indicating attempts to close the connection gracefully between the client and the server.
**Packets 1138 and 1139:**
These packets show another attempt to close the connection between the client and the server.
**Packet 1141:**
This packet is a TCP SYN packet sent from the client to the server, indicating an attempt to establish a new connection.

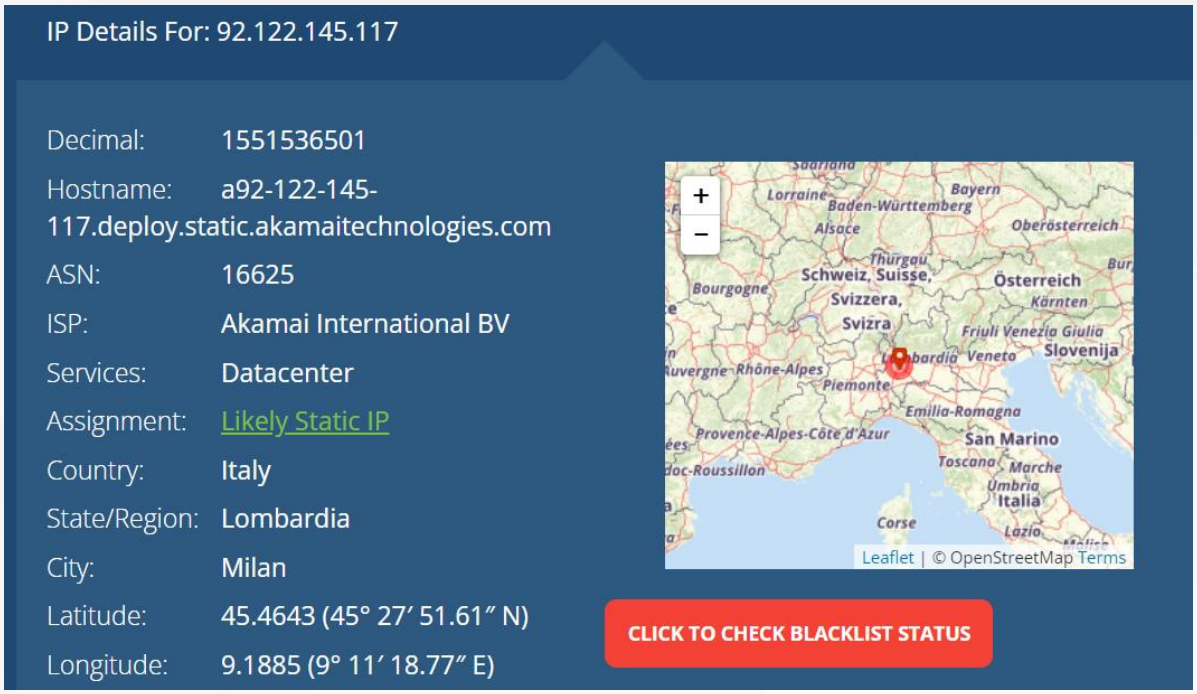
**Packet 1142:**
This packet is a TCP retransmission of a PSH-ACK packet indicating an attempt to push data to the server.
**Packets 1143, 1145, and 1146:**
These are TCP retransmissions indicating repeated attempts to push data to the server.
**Packet 1147:**
This packet is a TCP SYN-ACK packet sent from the server to the client in response to the SYN packet indicating acknowledgment and agreement to establish a connection.
**Packet 1148:**
This packet is a TCP ACK packet sent from the client to the server, acknowledging the SYN-ACK packet and agreeing to establish a connection.
**Packets 1150 and 1153:**
These packets are TCP retransmissions of a FIN-ACK packet, indicating attempts to close the connection gracefully.
**Packets 1151 and 1152:**
These packets are TCP retransmissions indicating repeated attempts to push data to the server.

**Discussion**
The above results from network analysis reveal the following key findings regarding the blockage of X in Pakistan:

1. **HTTP Blocking Technique:** The PTA employs HTTP blocking utilizing Geo-blocking technique to prevent users from accessing X. HTTP requests made to X servers are intercepted and disrupted resulting in failed connections and denied access to the platform.




2. **Identification of Blocking Method:** Through packet inspection, it is evident that the PTA utilizes HTTP blocking, as indicated by the disruption of HTTP requests and the absence of successful TCP connections to X's servers.
3. **Identification of Akamai IP Address:** The source IP address (92.122.145.117) identified in the captured packets belongs to Akamai Technologies, a prominent content delivery network (CDN) provider. This suggests that the PTA is implementing the blockage of X through Akamai' infrastructure.




4. **TCP Reset (RST) Flags:** The captured packets include TCP Reset (RST) flags indicating that the PTA resets TCP connections initiated by users attempting to access X. This reset prevents the establishment of a successful connection and effectively blocks access to the platform. **443 → 55535 [RST]**
5. **Potential Involvement of CDN Providers:** Given that Akamai Technologies hosts content for various online platforms, including X, Facebook, Youtube, and Netflix, it is feared that the PTA has instructed Akamai to reject access requests being generated from Pakistan. This collaboration enables the PTA to implement content filtering at the CDN level denying access to X's services.

The blockage of Twitter in Pakistan has significant civil, political and economic implications. Particularly, at a time when post-election phase is yet in progress, the protesting political parities have actively been using X for freedom of expression, access to information, assemble online and for other associated rights within the country. By censoring a prominent social media platform, the PTA restricts citizens' ability to engage in online discourse, share information, and express dissenting opinions. Despite X being restricted for more almost 5 days, the Pakistan Telecommunication Agency (PTA) has not released any official statement regarding the reasons to this censorship.

**Conclusion:**

The blockage of X in Pakistan is implemented through HTTP blocking with the PTA disrupting HTTP requests to prevent access to the platform. The involvement of Akamai Technologies suggests possible collaboration between the PTA and CDN providers to enforce content restrictions. This blockage raises concerns about censorship and a set of digital rights violations underscoring the importance of preserving freedom of expression, access to information, online assemblies, etc. While it's possible for the Pakistan Telecommunication Authority (PTA) to block access to Twitter using methods such as DNS filtering, IP blocking, or Deep Packet Inspection (DPI), blocking content from a specific CDN provider like Akamai Technologies can be more challenging and less common.

**Recommendations:**

1. **Progressive Judicial Interventions:** Higher judiciary, assuming its constitutional role of being custodian of fundamental freedoms enshrined in the constitution, should progressively take up this online censorship as a test case to decide on the legitimacy of such arbitrary state measures.
2. **Advocacy for Digital Rights:** Digital rights, and other civil society organizations and human rights defenders should advocate for the protection of digital rights and constitutional freedoms, including unrestricted access to online platforms.
3. **Transparency and Accountability:** The PTA should exhibit transparency regarding content blocking measures and ensure accountability for any restrictions imposed on online access.
4. **Technological Countermeasures:** Internet users can explore technological countermeasures such as virtual private networks (VPNs) and proxy services to circumvent content blocking and access restricted platforms.
5. **International Engagements:** The international community should monitor and address instances of online censorship and engage with the government of Pakistan to uphold freedom of expression and digital rights of the citizens.

**References:**

https://www.goclickchina.com/blog/technical-methods-behind-internet-censorship/
https://www.omscs-notes.com/computer-networks/internet-surveillance-and-censorship/
https://www.irtf.org/anrp/IETF118-ANRP-Raman.pdf
https://www.dawn.com/news/1577659