Performance and Privacy Analysis of Encrypted DNS Protocols (UDP, DoT, DoH)

A Comparative Study on Latency, Reliability, and Privacy

Umang Shikarvar Tejas Lohia Mohit Zainab Kapadia Tanishq Chaudhari

Overview & Motivation: Securing the Digital Frontier

Traditional DNS transmits queries in plaintext, making them susceptible to eavesdropping, tracking, and tampering. This inherent vulnerability underscores the critical need for enhanced security measures in modern internet communications.

DNS over UDP(Plaintext DNS)

Vulnerable to tracking and tampering, exposing user activity.

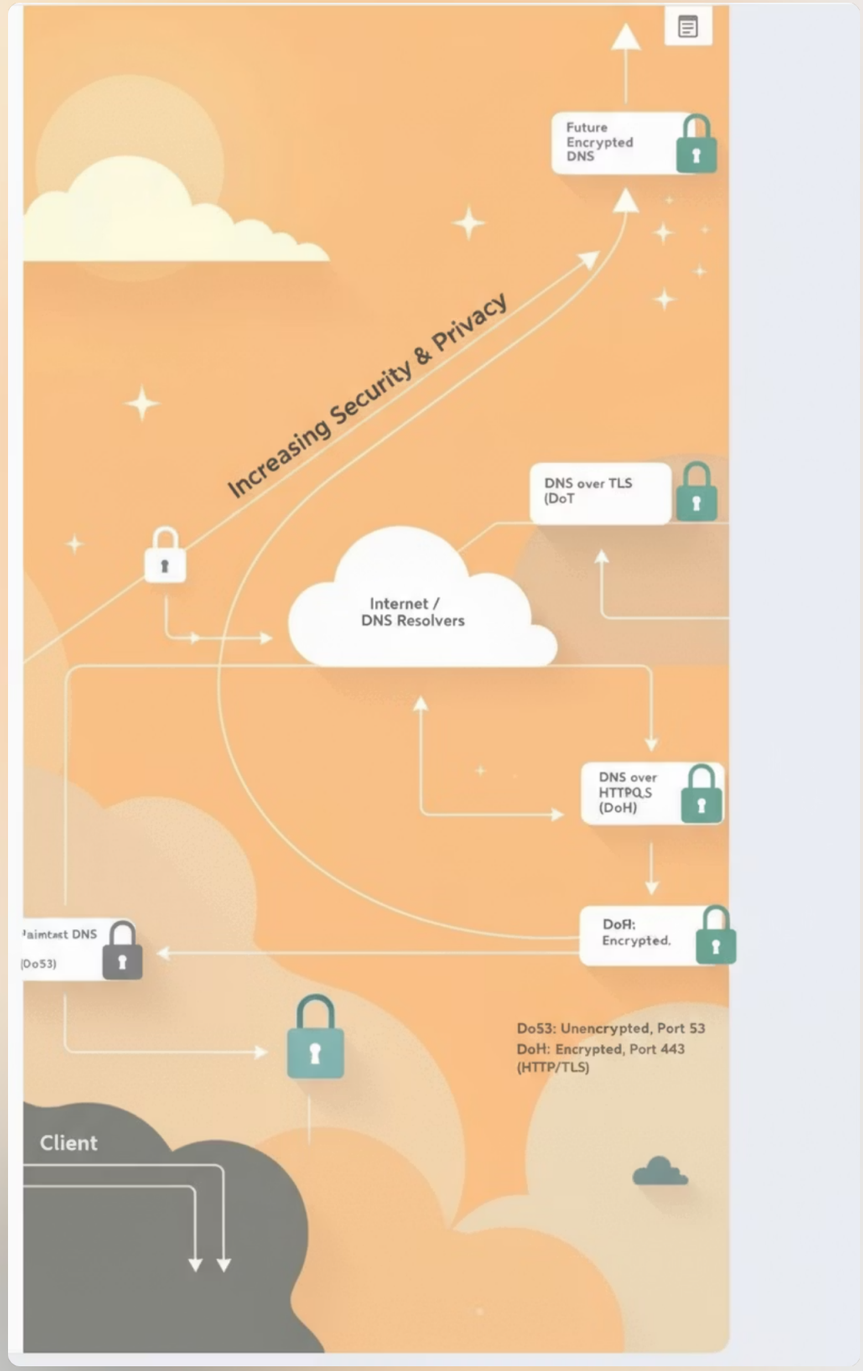
DoT (Encrypted DNS)

Encrypts queries via TLS, enhancing privacy and data integrity.

DoH (Encrypted DNS over HTTPS)

Encapsulates DNS within HTTPS traffic for maximum privacy and resilience.

We aim to quantify the **performance vs. privacy trade-offs** of these protocols using experimental data.

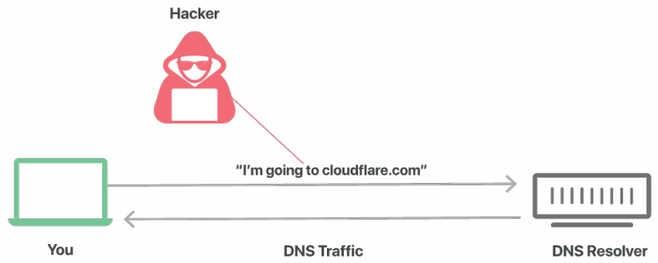


Background & Evolution of DNS Security Protocols

1

Do53 (Traditional DNS)

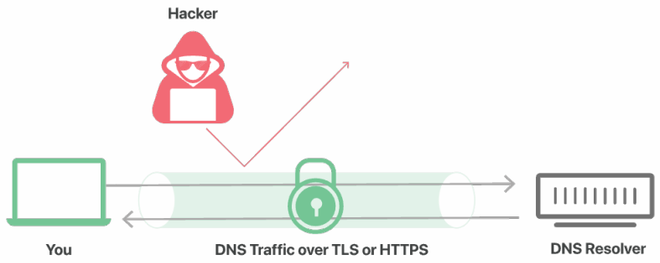
The original DNS protocol, using UDP/TCP port 53. Unencrypted and widely susceptible to attacks.



2

DoT (DNS-over-TLS)

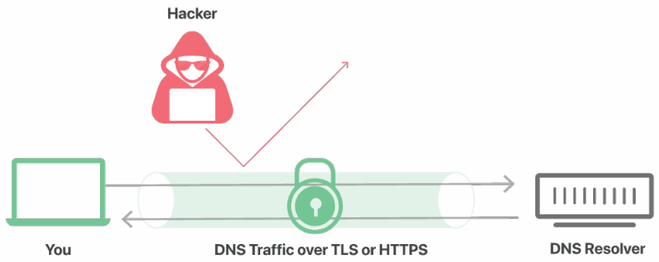
Introduced to encrypt DNS traffic using TLS over TCP port 853. Offers confidentiality and integrity.



3

DoH (DNS-over-HTTPS)

Further enhances privacy by encapsulating DNS queries within HTTPS traffic, typically over port 443. This blends DNS traffic with regular web traffic.



While both DoT and DoH significantly enhance security, they inherently introduce varying levels of latency due to the encryption and protocol overheads.

Controlled Testing Environment

Our experimental setup was meticulously designed to simulate real-world conditions while allowing for precise measurement and control.

Hardware Configuration

Two MacOS machines served as client and server, connected via a dedicated WiFi network to minimise external interference.

Custom Resolver Implementations for DNS, DoT, DoH

A Python application, leveraging `dnslib` and `cryptography`, managed DNS query encryption, decryption, and iterative resolution.

Network Traffic Simulation

`Iperf` was employed to generate realistic background network traffic, simulating a busy network environment.

Browser-based Testing

Firefox, automated with `Selenium` and routed through Proxy, allowed for controlled, browser-specific DNS queries.

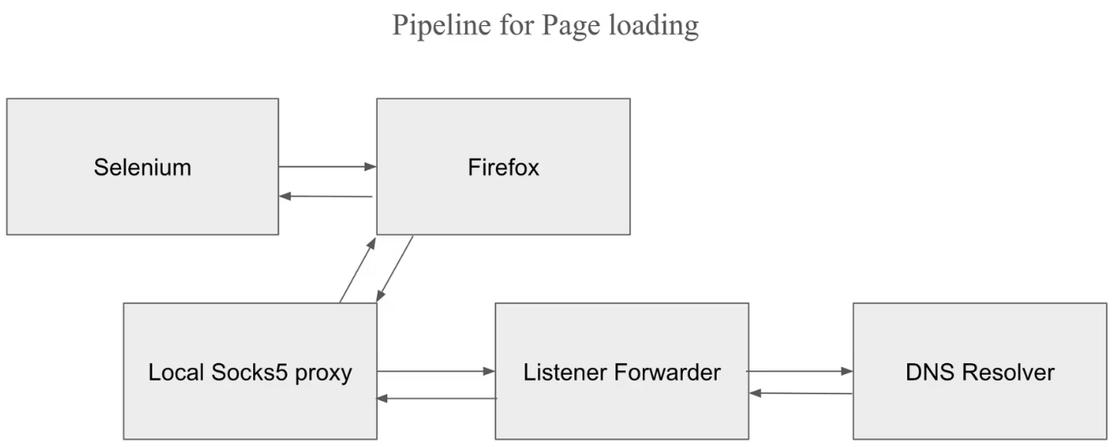


Fig 1. *Pipeline for page loading over all the protocols*

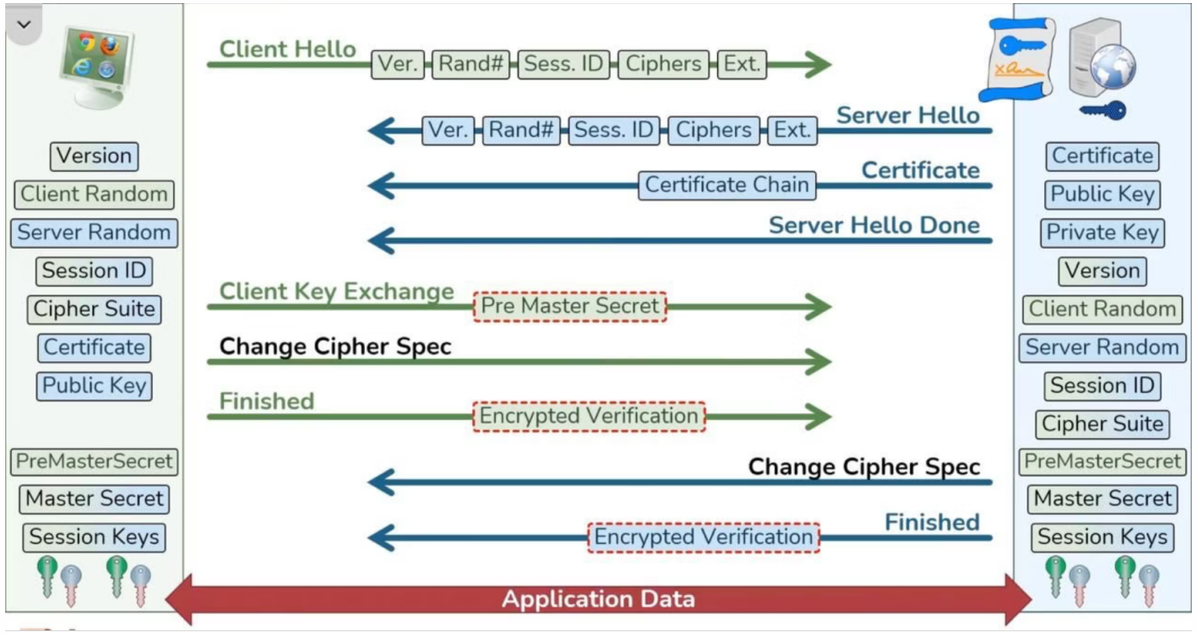


Fig 2. *Handshake architecture*

Measurement Methodology: Quantifying Protocol Performance

To provide a comprehensive comparison, we employed a rigorous methodology, focusing on critical performance indicators.

Website Selection

Utilised the Top 50 and Bottom 50 websites from the Tranco list to ensure a diverse range of popular and less-frequented domains.

Key Metrics Logged

Recorded response times, query status, Response Codes (RCODE), and bytes in/out for each DNS query.

Protocols

Measurements were systematically conducted across all three protocols: DNS over UDP, DoT, and DoH, for direct comparison in two classes of websites, i.e., top and bottom 50 websites.

Data Visualisation

Generated detailed plots for comparisons to illustrate performance trends.

Baseline Analysis using Google- DNS over UDP

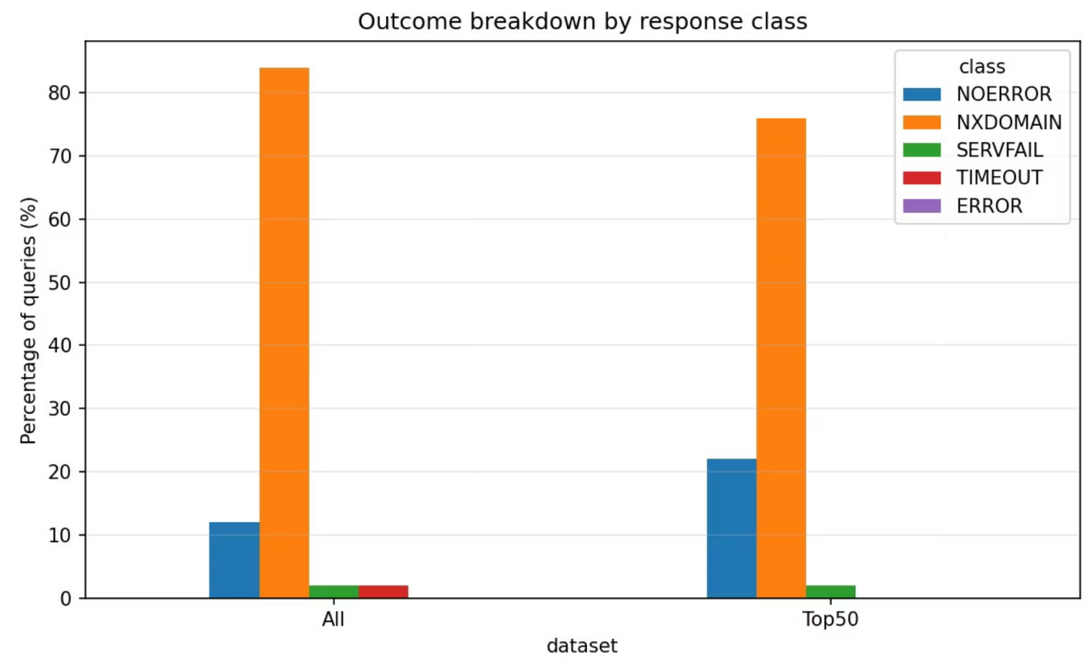


Fig 3: *Outcome Breakdown by Response Code*

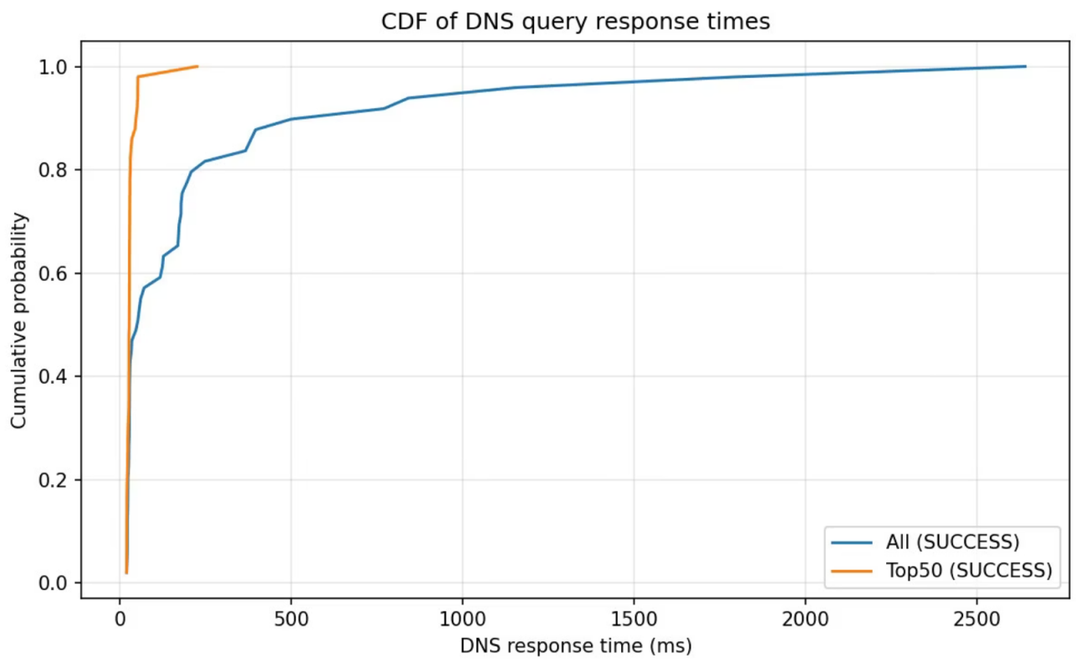


Fig 4: *Cumulative Distribution of DNS Response Times (Success Only)*

Baseline Analysis using Google- DNS over UDP

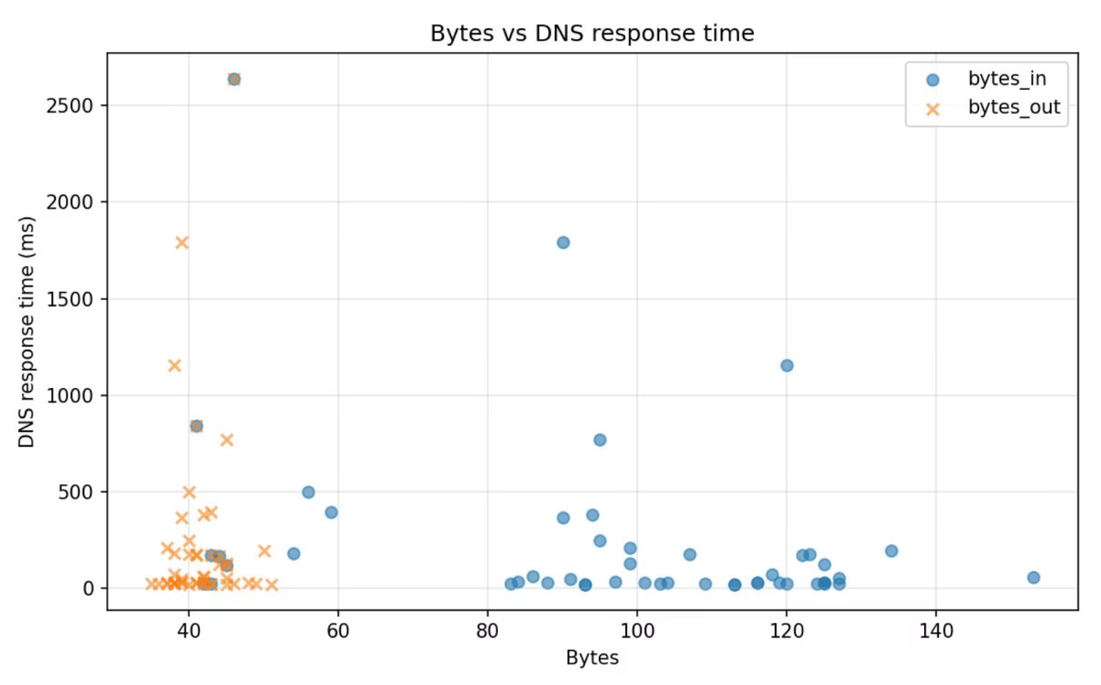


Fig 5: *Correlation Between Query Size and DNS Latency*

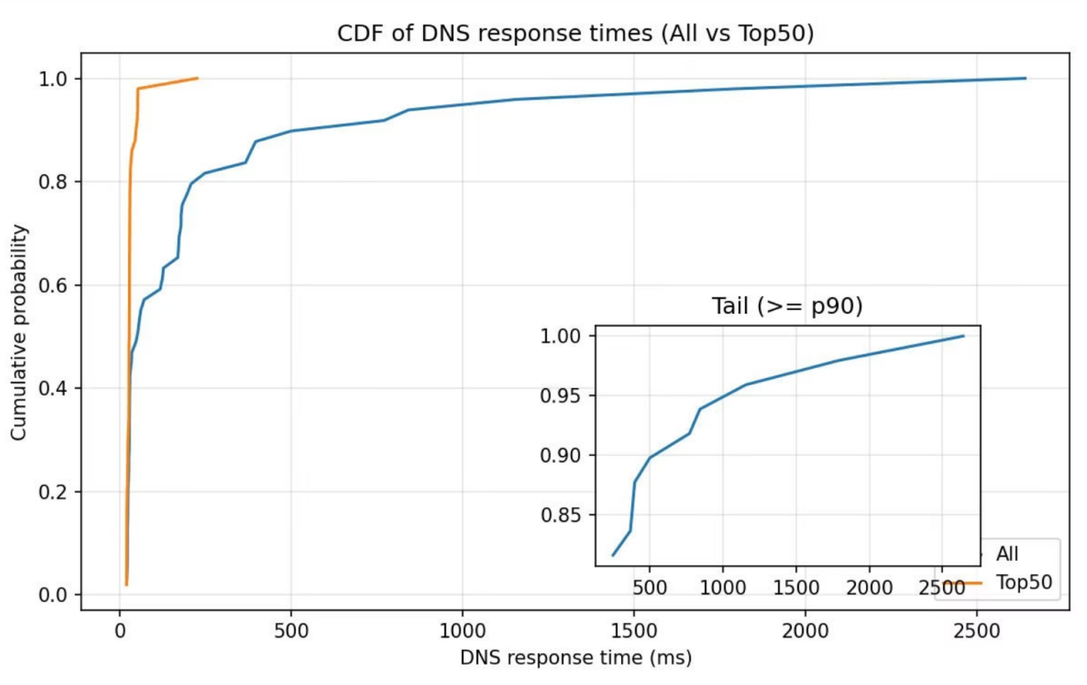


Fig 6: *CDF of DNS Response Times (Tail ≥ p90)*

Baseline Analysis using Google- DoH

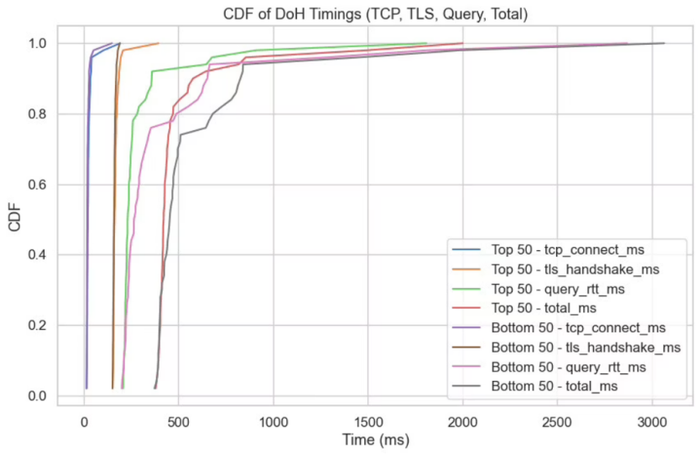


Fig 7: *CDF of DoH Timings(TCP,TLS,Query, Total)*

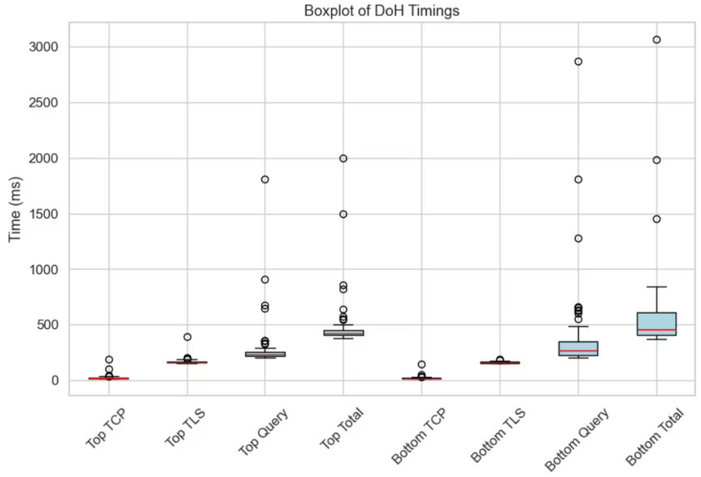


Fig 8: *Boxplot of DoH Timings*

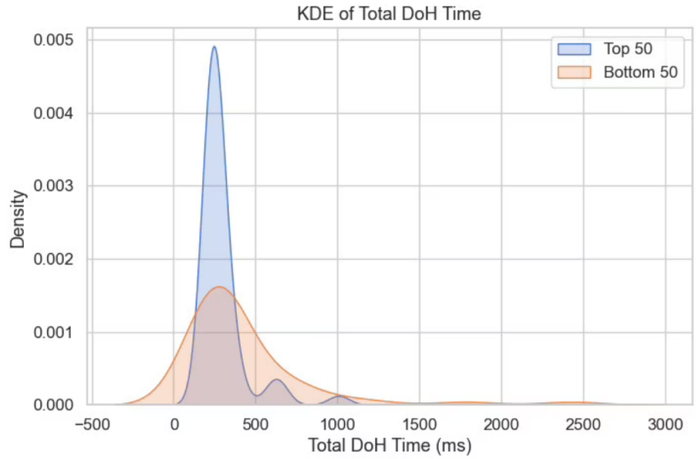


Fig 9: *KDE of total DoH time*

Baseline Analysis using Google- DoH

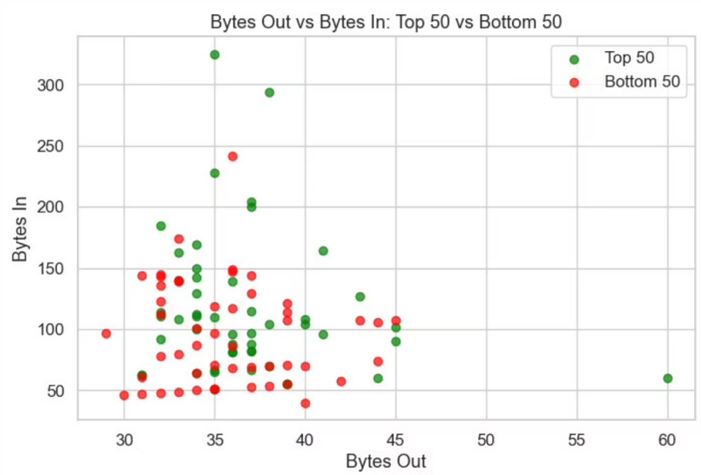


Fig 10: *Scatter: Bytes Out vs Bytes In (Top50 vs Bottom50)*

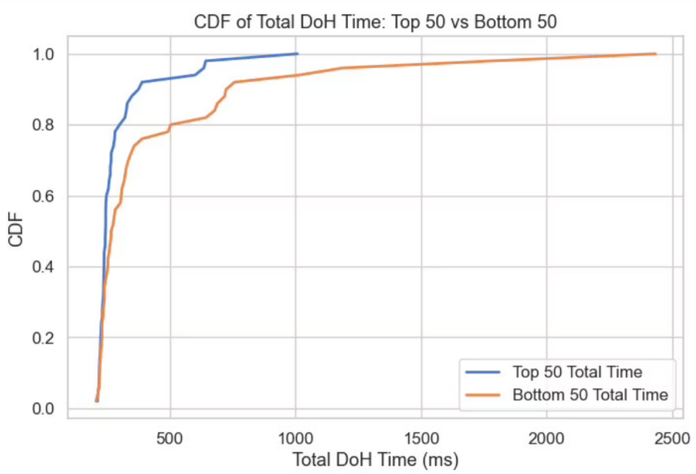


Fig 11: *CDF of DoH Response Time: Top50 vs Bottom50*

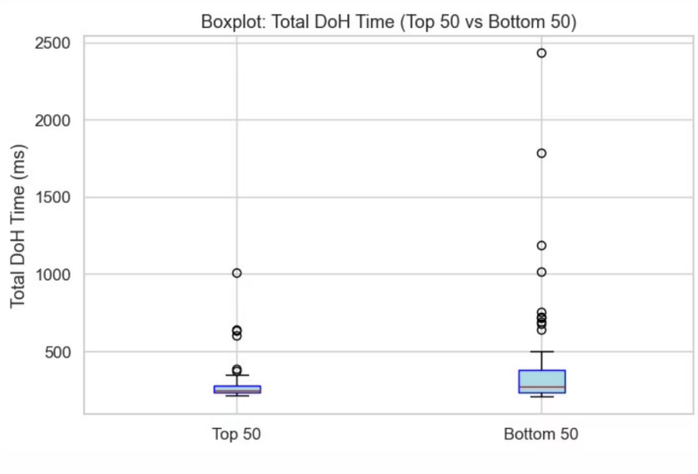


Fig 12: *Boxplot of total DoH Timings*

Baseline Analysis using Google- DoT

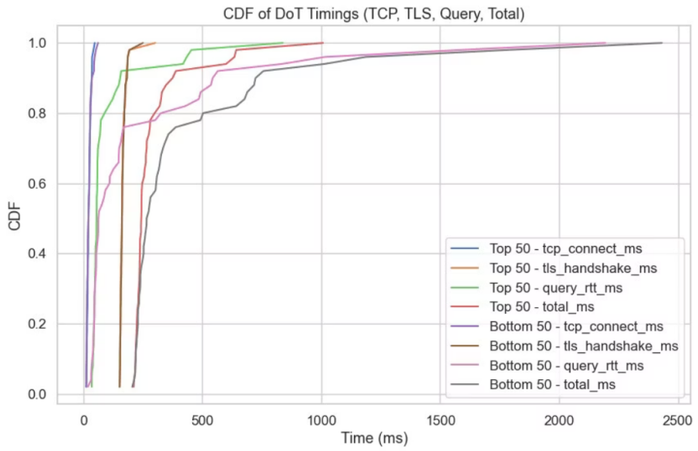


Fig 13: *CDF of DoT Timings(TCP,TLS,Query, Total)*

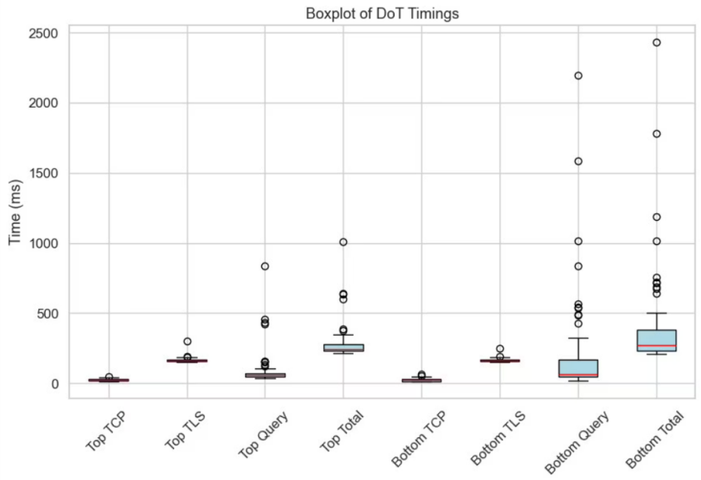


Fig 14: *Boxplot of DoT Timings*

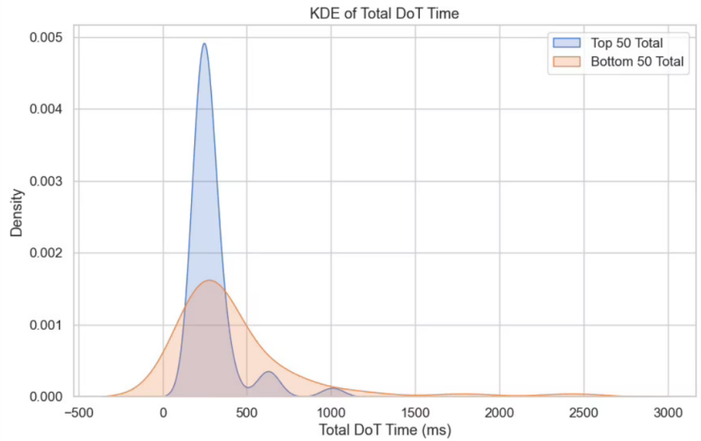


Fig 15: *KDE of total DoH time*

Baseline Analysis using Google- DoT

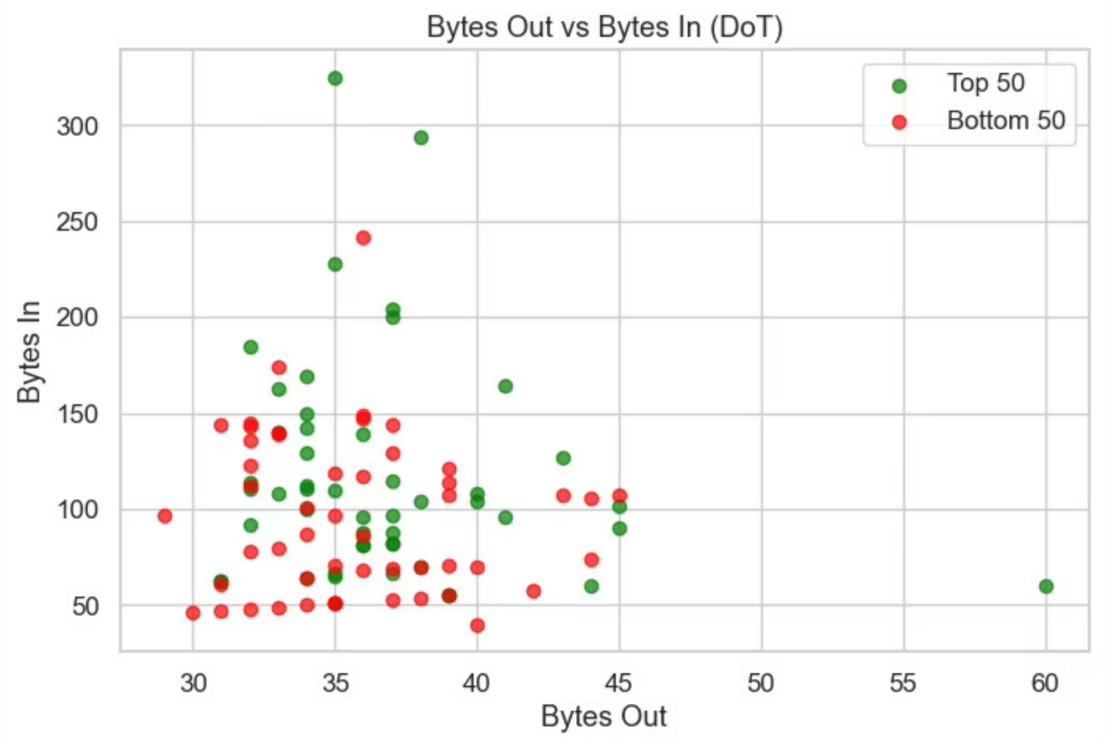


Fig 16: *Scatter: Bytes Out vs Bytes In (Top50 vs Bottom50)*

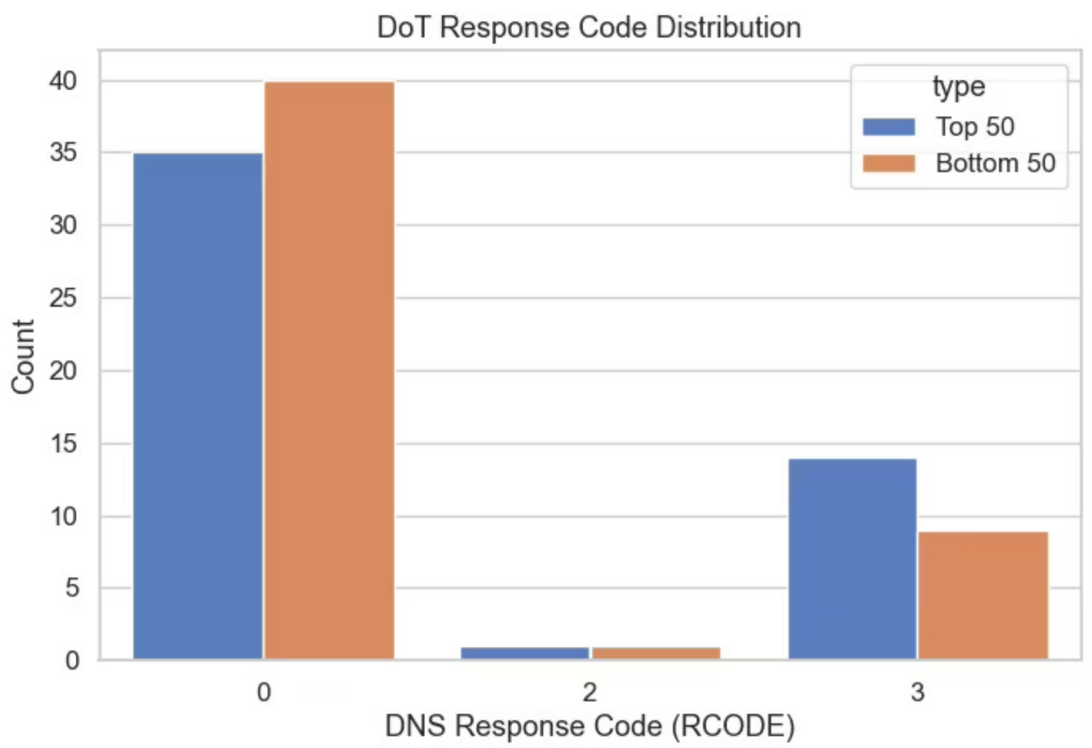
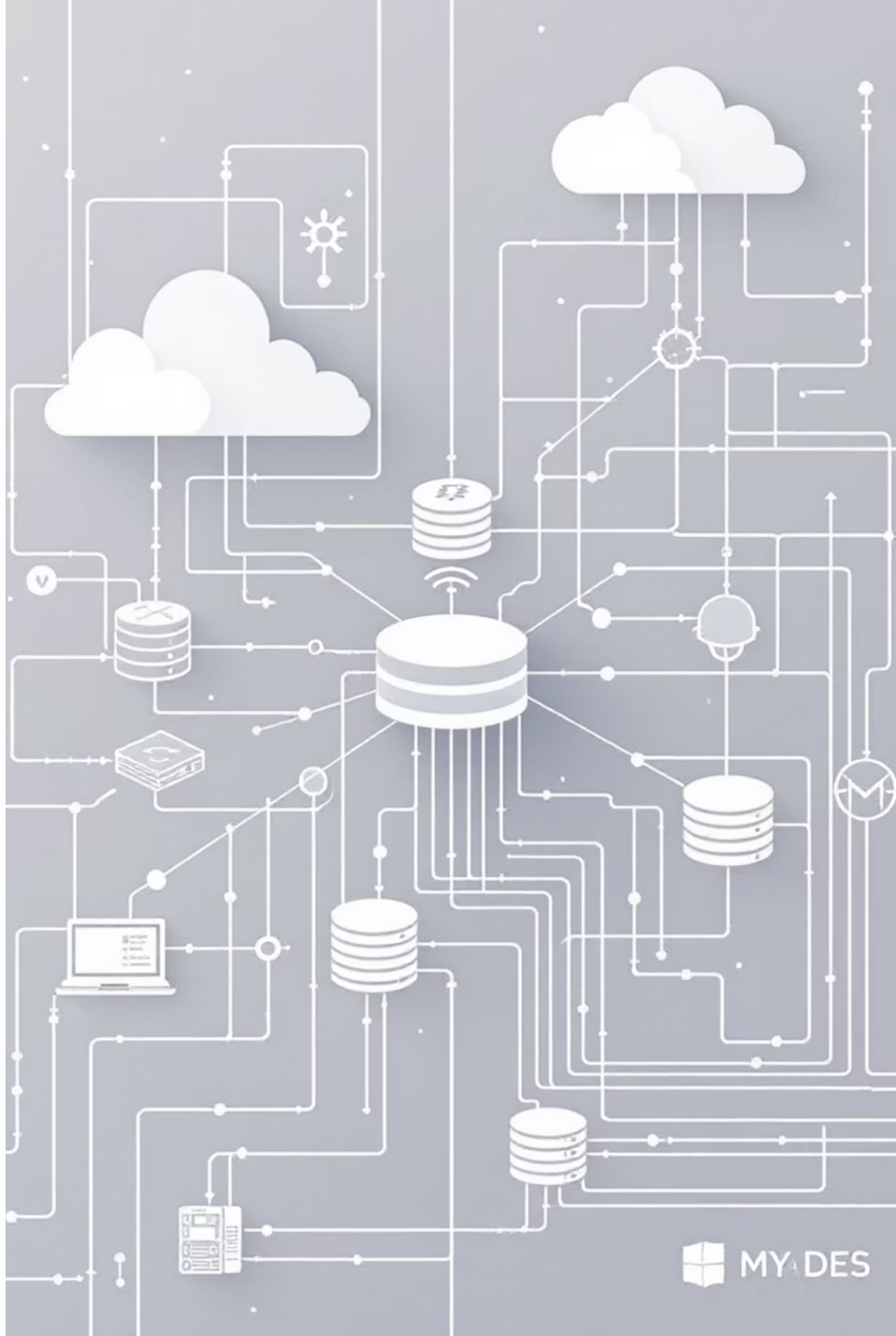


Fig 17: *DoT response code distribution*

Testing and Comparing using the Custom Resolvers- without browser



Latency Comparision

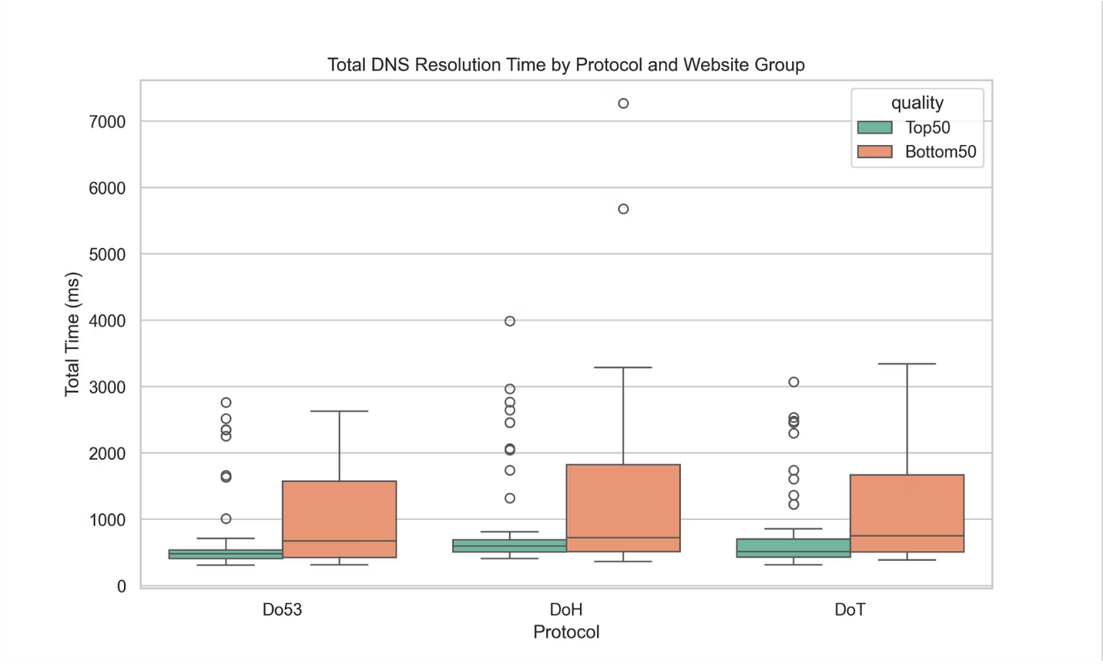


Fig 18: *Box plot of resolution time*

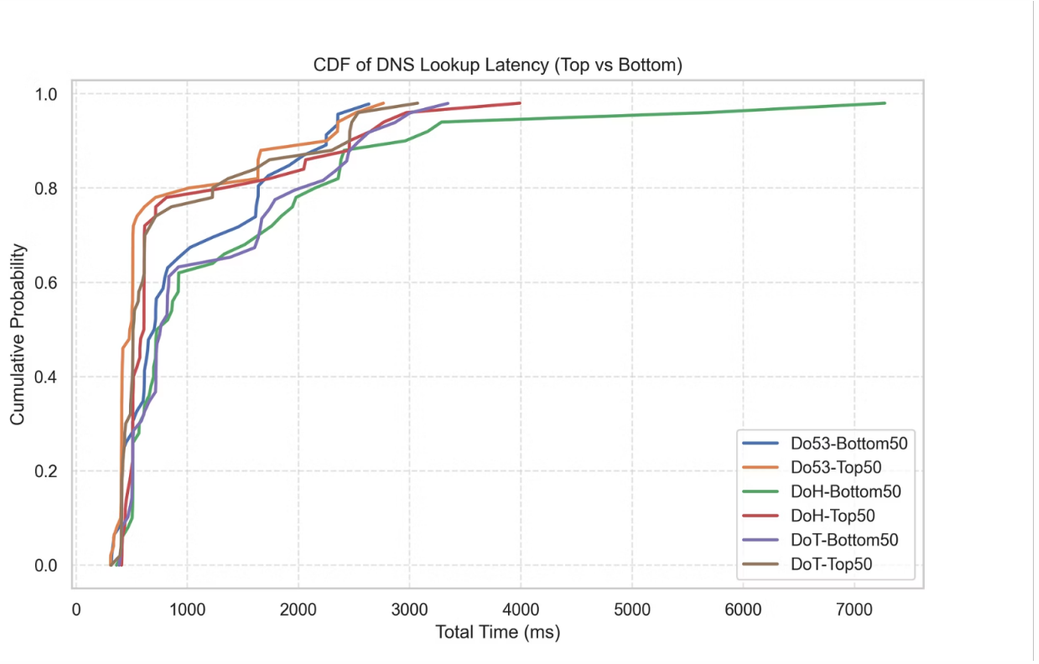


Fig 19: CDF of DNS *Lookup Latency*

Latency Breakdown

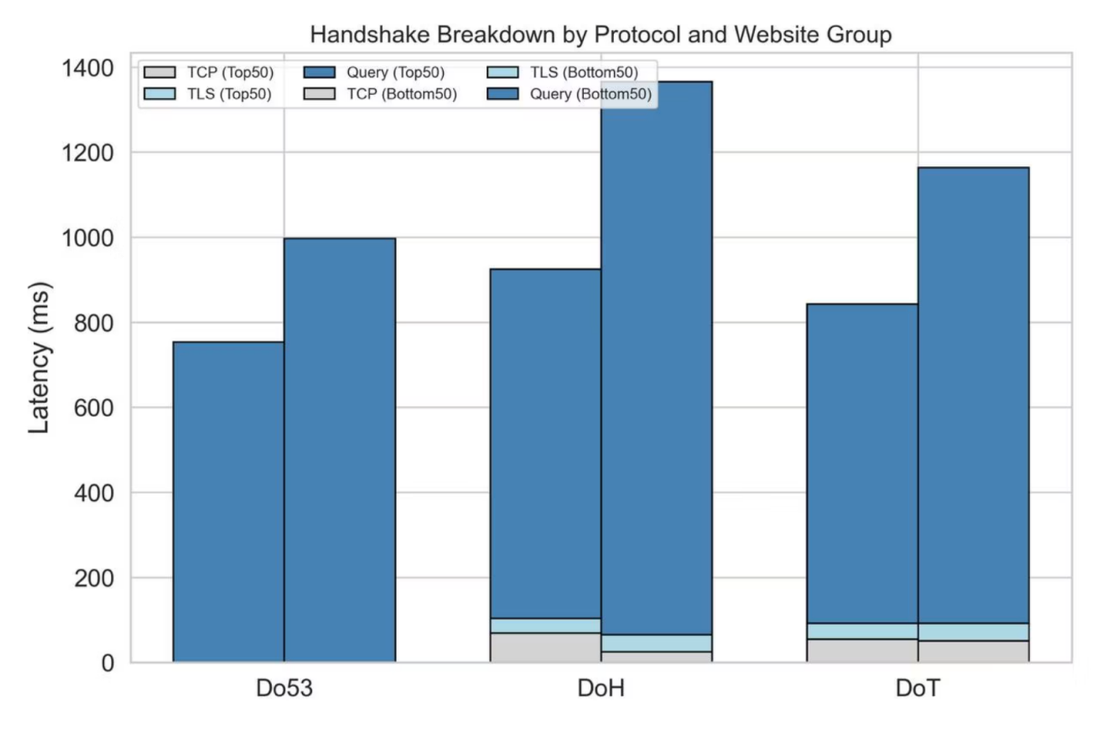


Fig 20: *Handshake latency breakdown*

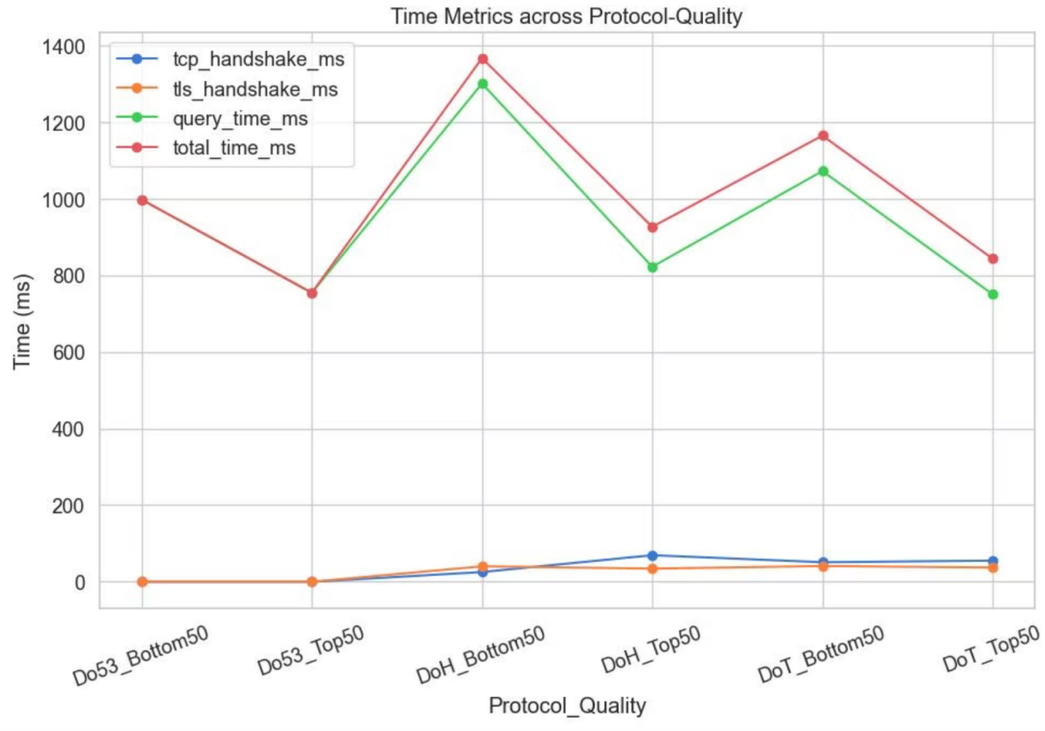


Fig 21: *Time taken across various phases amongst different protocols*

Overhead and Throughput Analysis

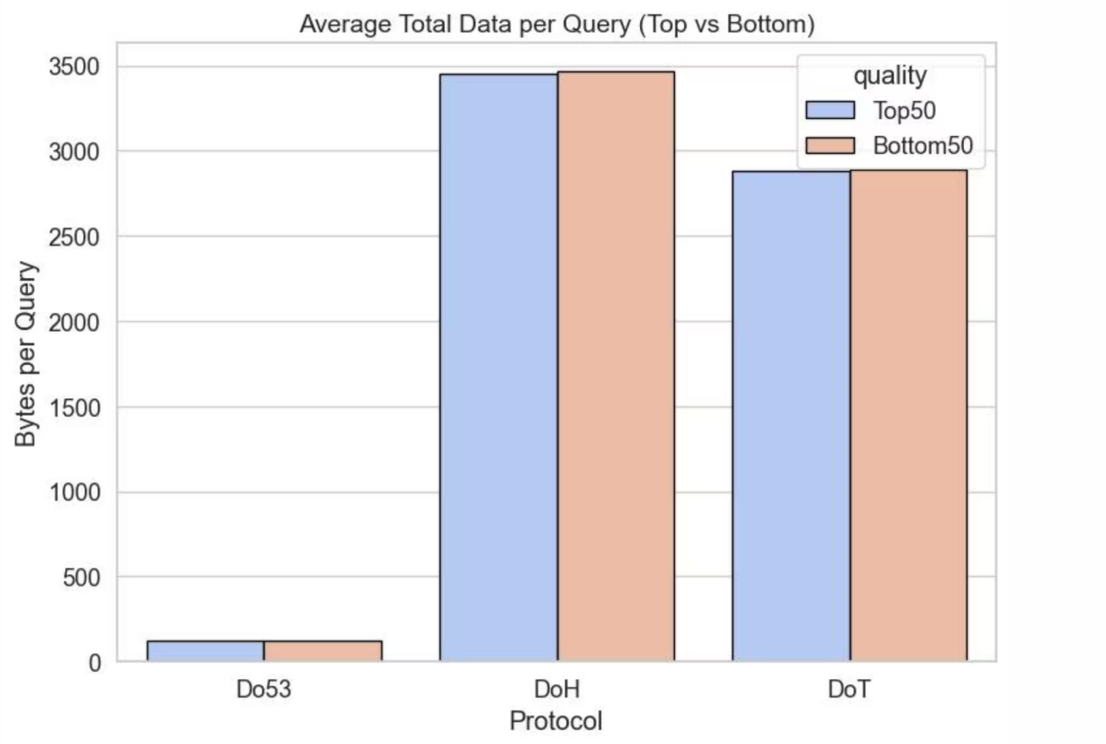


Fig 22: *Average total data per query comparison*

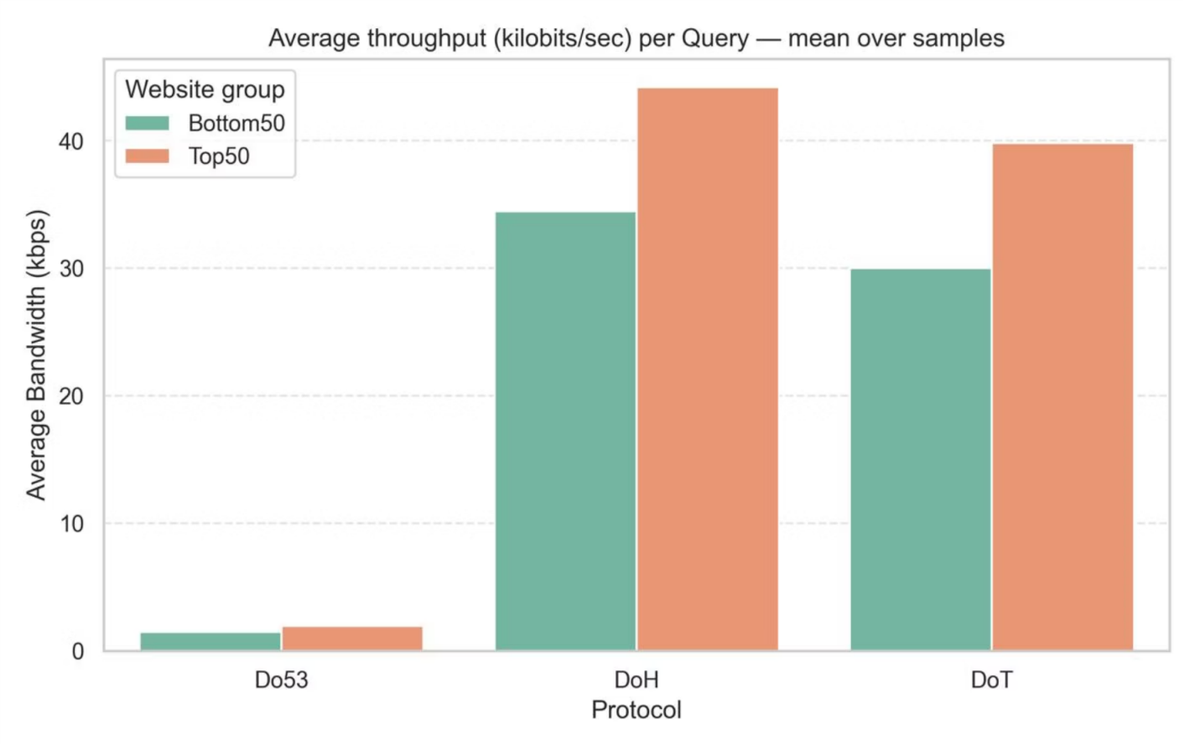
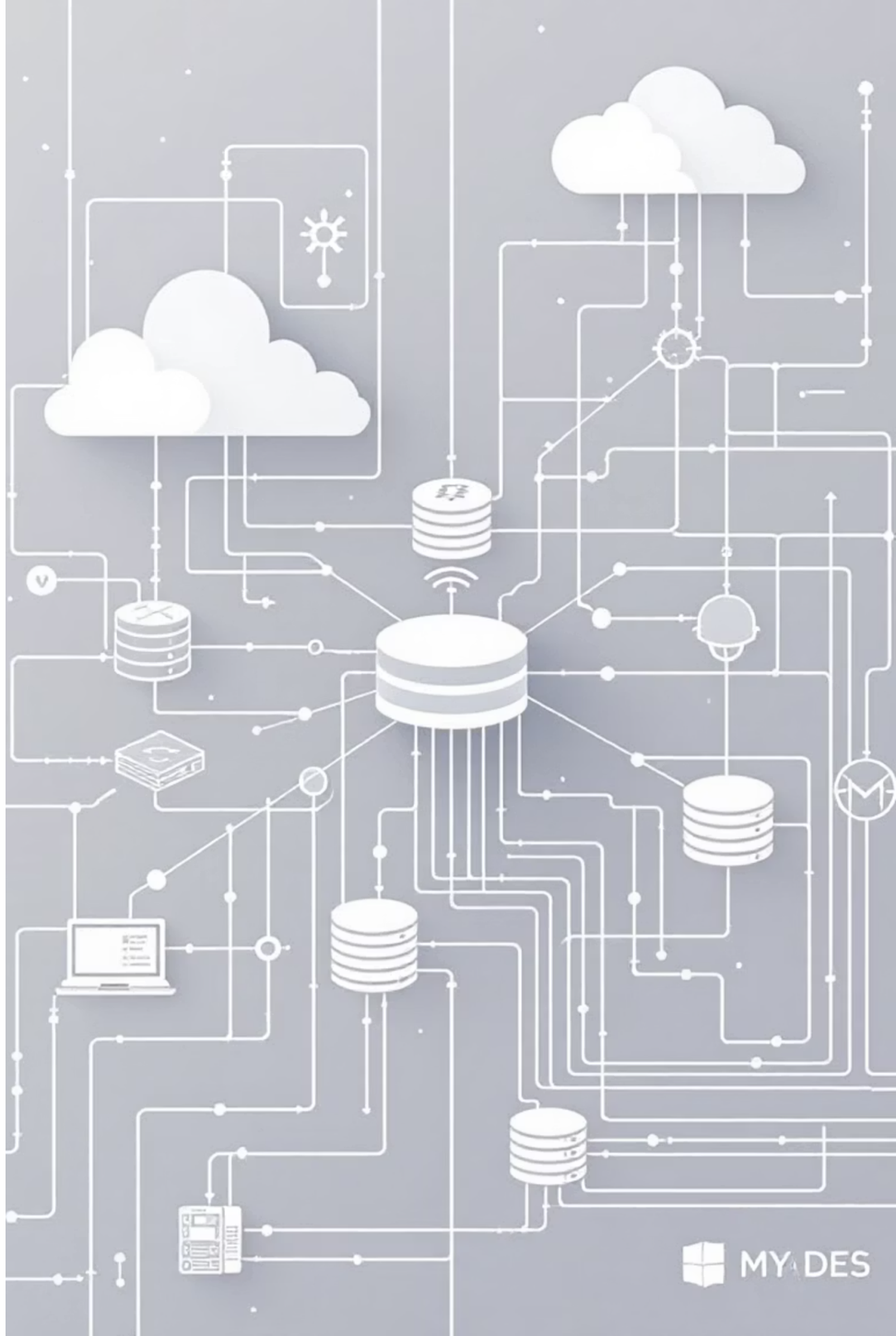


Fig 23: *Average throughput(kb/s) per query*

Testing and Comparing using the Custom Resolvers- using Firefox



Page load

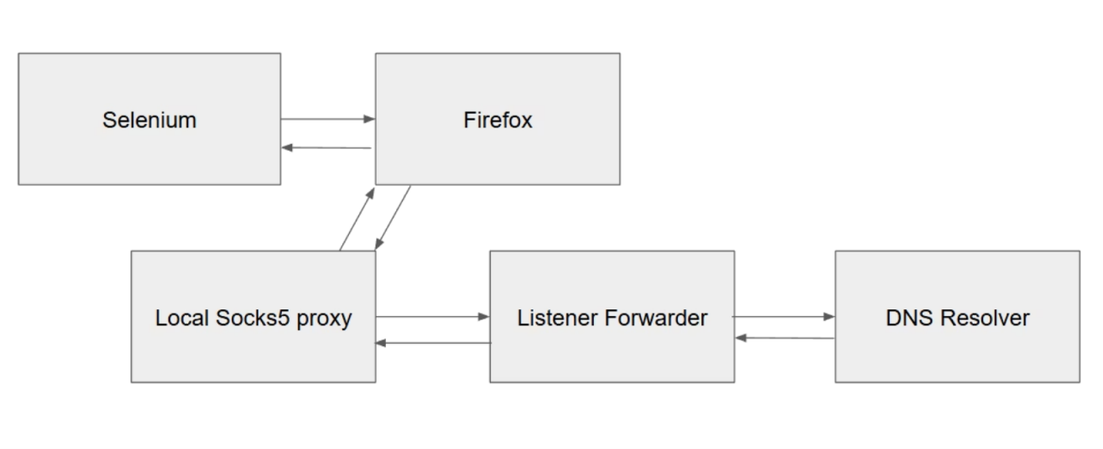


Fig 24: *Pipeline for Page Loading using Selenium*

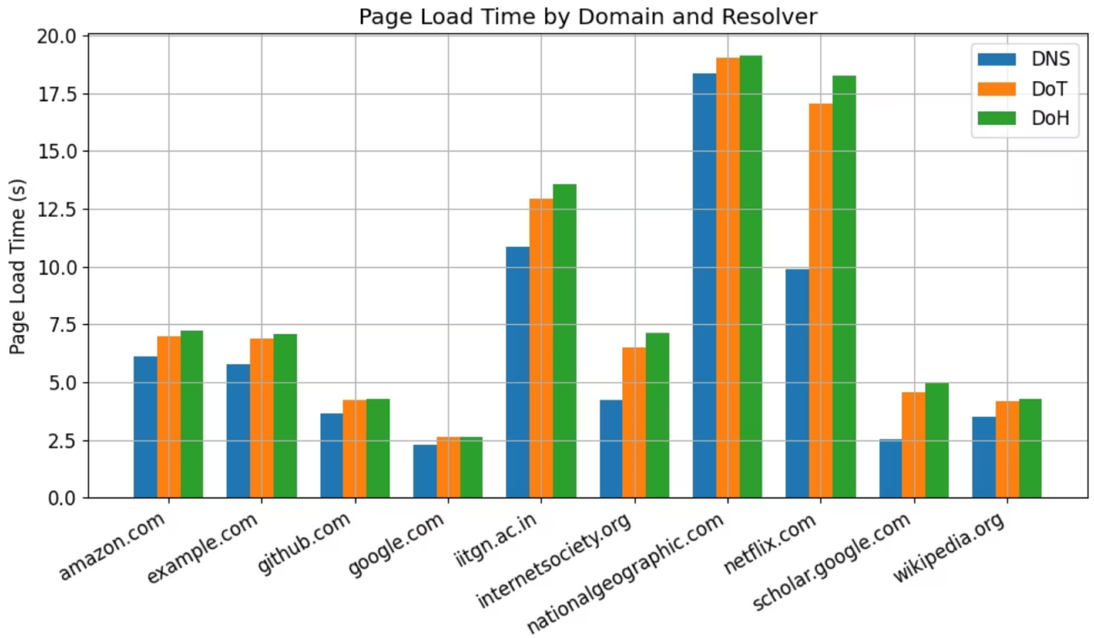


Fig 25: *Page Load Time by Domain and Resolver*

Privacy Evaluation

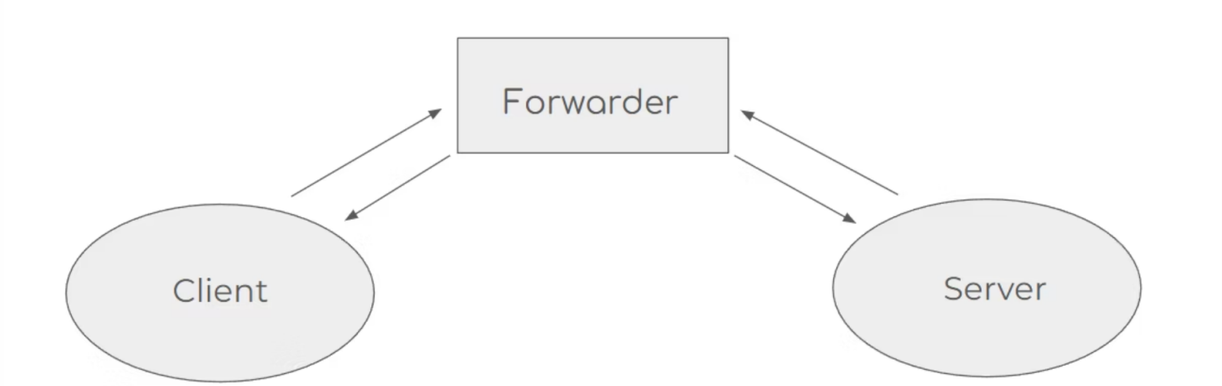
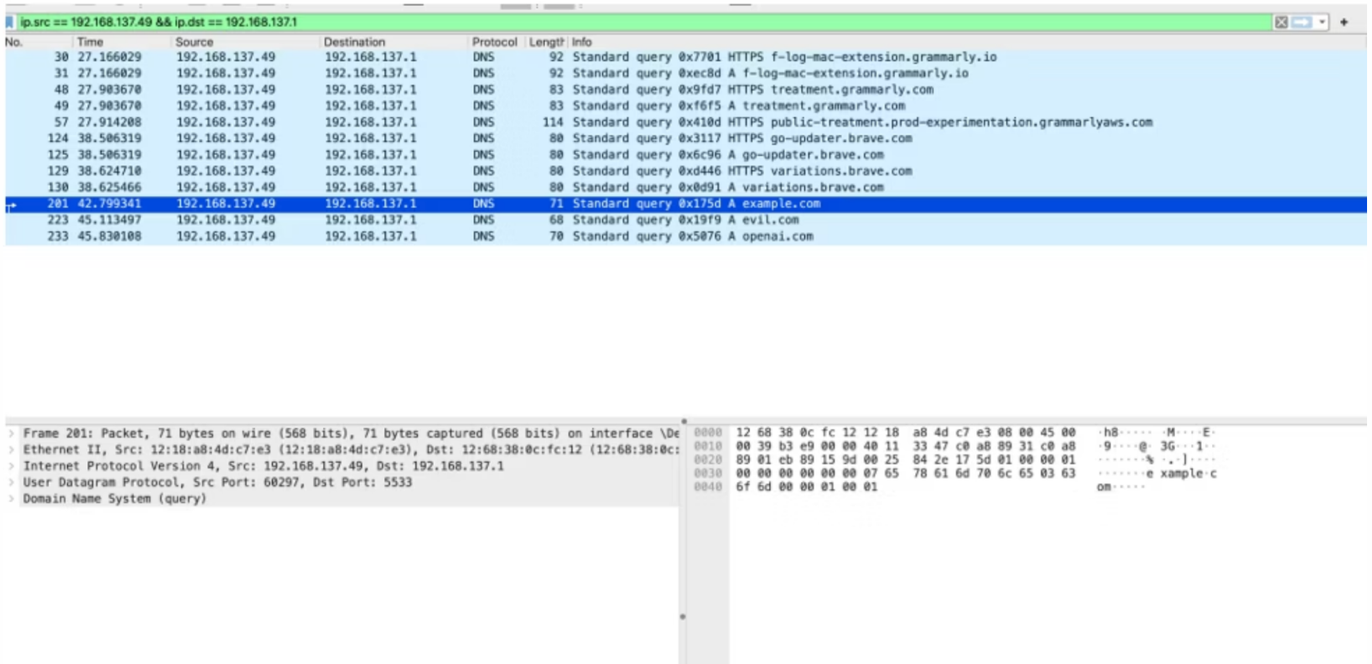
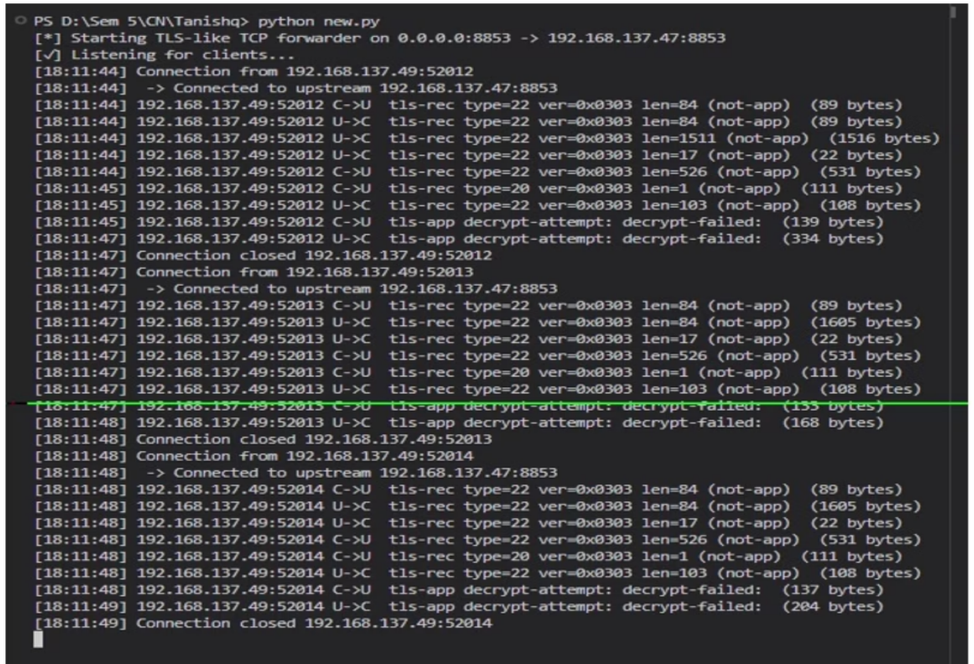


Fig. 26: *Network Pipeline*





Results

Our comprehensive analysis reveals distinct profiles for each DNS protocol, emphasizing the trade-offs between speed, security, and privacy.

DNS over UDP

Achieved the fastest response times due to its unencrypted nature, but offers virtually no privacy or security against interception and tampering.

DoT

Provides a strong balance with robust encryption via TLS and minimal latency impact. Its TCP foundation ensures better reliability in challenging network conditions.

DoH

Offers the highest level of privacy by cloaking DNS traffic as standard HTTPS. This comes with a moderate increase in latency, but excels in bypassing censorship.

For the bottom 50 percentile of websites (those with higher initial latency), DoT and DoH demonstrated superior stability and reliability compared to DNS over UDP, due to their connection-oriented protocols handling lossy network conditions more effectively.

Protocol	Latency	Security	Stability
Do53	Very High (Fastest)	None (Vulnerable)	Low (Unstable)
DoT	High (Minimal Overhead)	High (Encrypted)	High (Stable)
DoH	Moderate (Slight Latency)	Very High (Obfuscated)	High (Stable)

Fig 28: *DNS Protocol Comparison Matrix*

Key Insights: Balancing Performance and Privacy

Our comprehensive analysis provides critical insights into the real-world trade-offs between the speed, security, and privacy offered by Do53, DoT, and DoH protocols.

- ## Enhanced Network Stability

  TCP-based protocols, DoT and DoH, demonstrate superior resilience in handling packet loss and unstable network conditions, ensuring more consistent performance compared to plaintext DNS.

- ## Minimal Encryption Overhead

  In stable network environments, the latency overhead introduced by DoT and DoH encryption is often minimal, making their security benefits highly accessible without significant performance penalties.

- ## Consistent Trade-offs

  Cumulative Distribution Function (CDF) plots consistently highlight the inherent compromises i.e., Do53 offers raw speed at the cost of security, while DoT and DoH prioritize security and privacy with slight latency increases.

- ## DoH for Privacy-Sensitive Scenarios

  DoH emerges as the preferred choice for applications and users where privacy and censorship circumvention are paramount, despite its slightly higher latency due to HTTPS encapsulation.