Jhannes Ernesto Reimann

Note on Data Availability and Scope

The following analysis is based on DNS over UDP measurements conducted using RIPE Atlas probes located exclusively in Germany. It's important to note certain limitations encountered during the data collection phase. Due to API restrictions imposed by the RIPE Atlas platform – specifically,

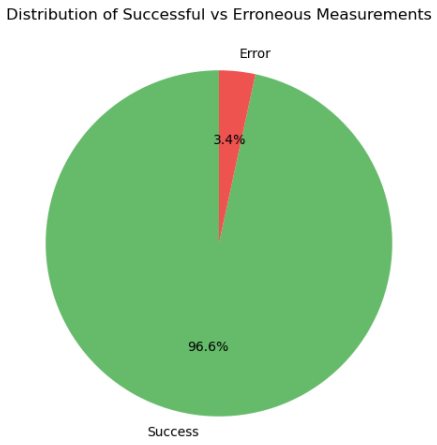
"*We do not allow more than 25 concurrent measurements to the same target...*" – it was not possible to gather data for all initially planned resolver-domain combinations.

Consequently, the dataset for the "*local*" and "*q9*" resolvers includes measurements for all five targeted domains. However, for the "*cloudflare*" resolver, data could only be successfully collected for two domains (*google.com* and *facebook.com*). All measurement attempts targeting the "*google*" public resolver (*8.8.8.8*) failed due to these platform limitations.

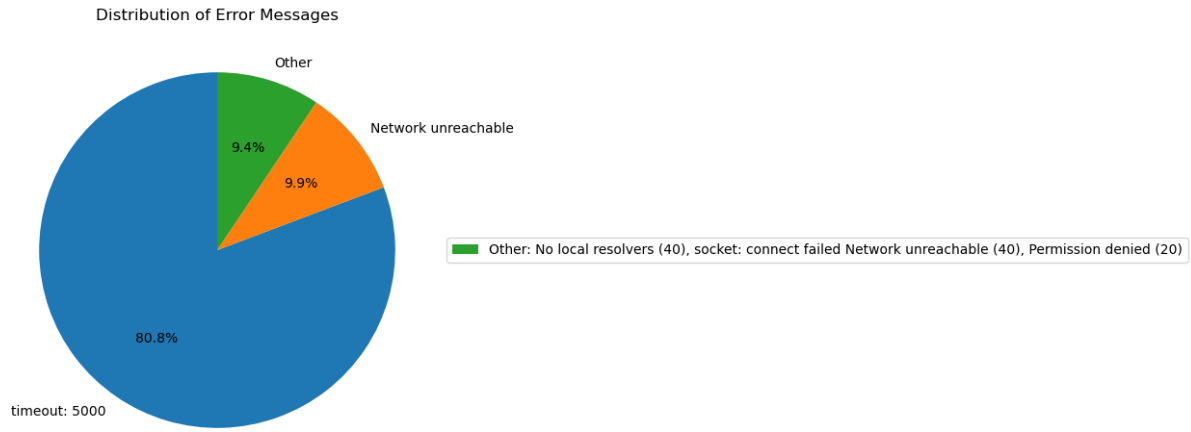
Given these constraints, and the difficulty in finding suitable publicly available RIPE Atlas measurements that used only German probes for the exact same domains and missing resolvers, the decision was made to proceed with the analysis based on the successfully collected data. This context should be kept in mind when interpreting the results, particularly for resolvers with incomplete domain coverage.

Task 1: DNS over UDP (15 points)

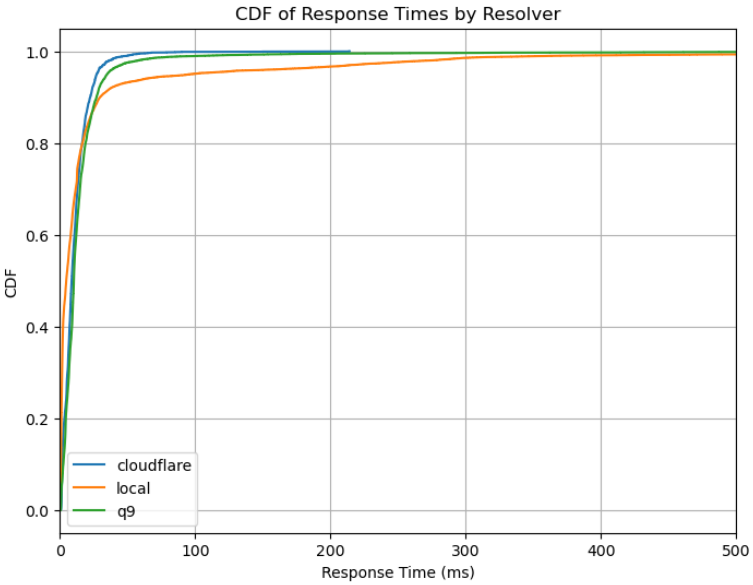
Interpret the plots you just created. What can you infer from the distributions? What differences between distributions in a figure can you spot?



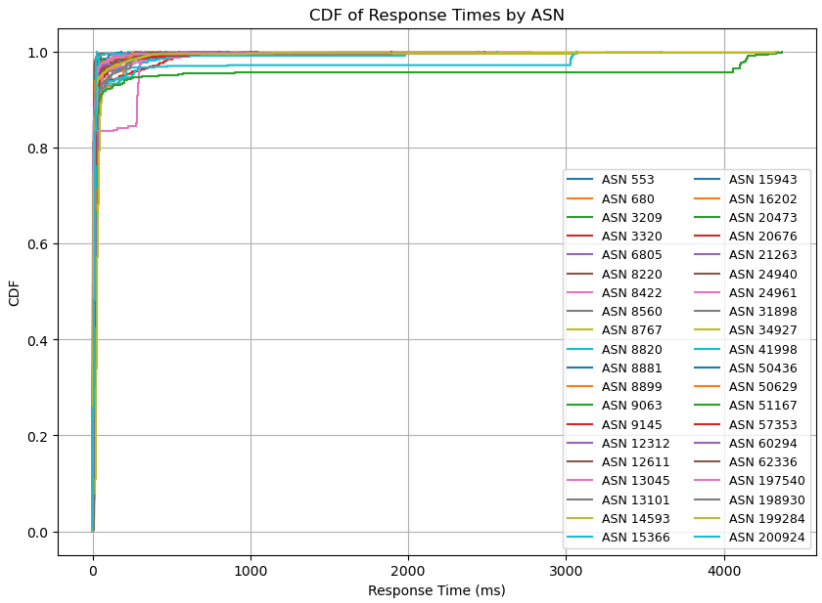
The pie chart illustrates a high overall success rate for the DNS measurements that were actually initiated, with 96.6% completing successfully. Only a small fraction (3.4%) resulted in errors, which correspond to issues like timeouts or network unreachability as detailed in the error distribution plot. This indicates good reliability for the measurements that could be executed.



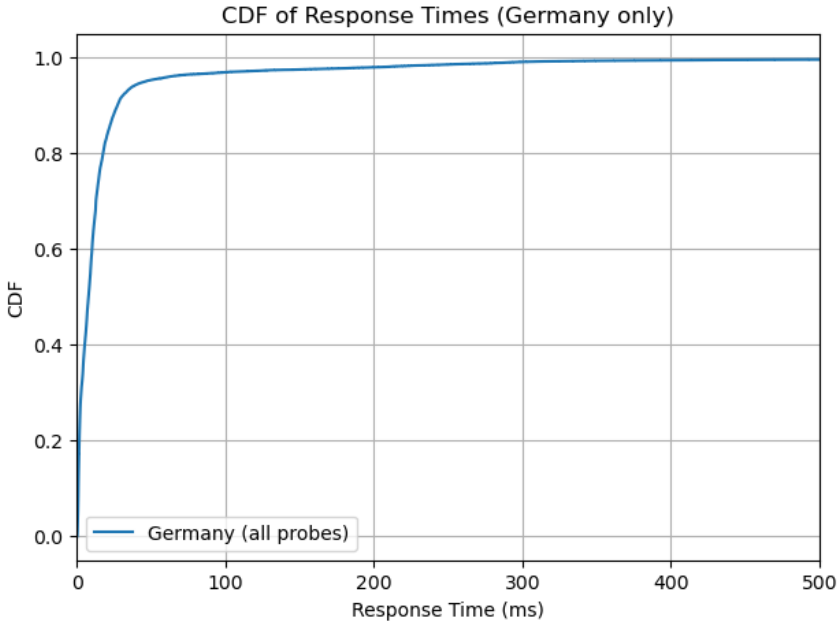
This chart reveals that the vast majority of measurement failures (80.8%) were due to 5-second timeouts, indicating that probes often did not receive a DNS response within this window. "Network unreachable" errors accounted for nearly 10% of failures, with a smaller "Other" category capturing miscellaneous issues like local resolver problems or permission denials. Overall, timeouts were the predominant cause of unsuccessful measurements.



The CDF plot shows that "local" and "q9" resolvers exhibited very similar and fast response times, resolving about 95% of queries in under 30ms. "Cloudflare" also performed well, though its curve suggests slightly more varied response times, reaching 95% resolution closer to 50ms. However, it's important to recall that the "cloudflare" data is limited to only two domains, which might affect direct comparability with the more complete datasets for "local" and "q9".



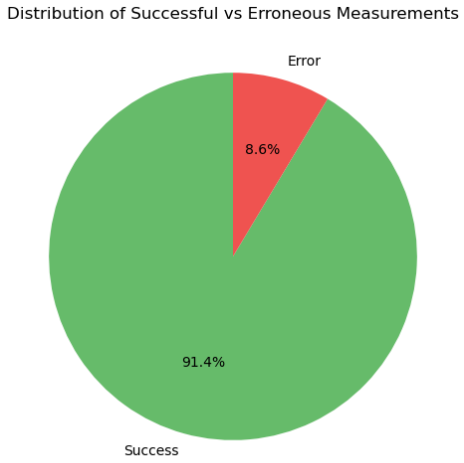
This plot demonstrates that DNS resolution performance varies significantly across different Autonomous System Numbers (ASNs) where the German probes are located. While many ASNs show consistently fast resolution times, others display more gradual CDF curves or longer tails, indicating greater variability or slower performance for probes within those networks. This highlights the influence of network infrastructure on DNS query latency.



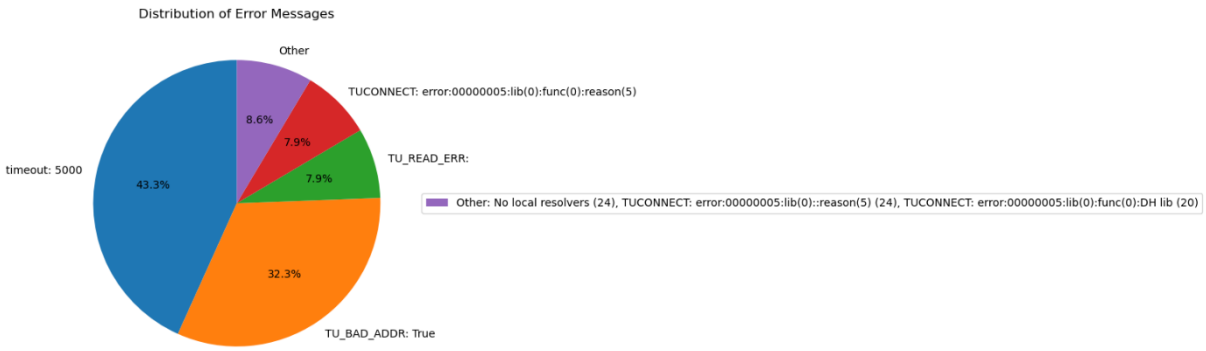
This aggregated CDF for all successful measurements within Germany shows efficient DNS performance, with approximately 90% of queries resolved in under 50ms and nearly 98% by 100ms. The curve rises sharply, indicating that most DNS queries from the German probes in this dataset were answered very quickly. This provides a general overview of quick DNS resolution within the tested scope in Germany.

Task 2: DNS over TLS (5 points)

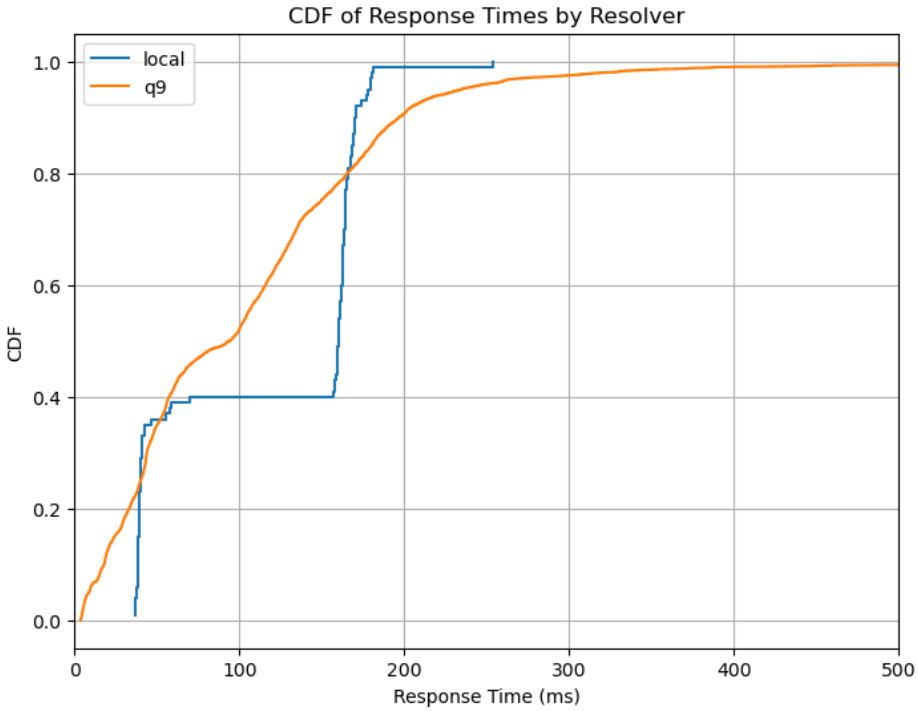
Interpret the plots you just created. What can you infer from the distributions? What differences between distributions in a figure can you spot?



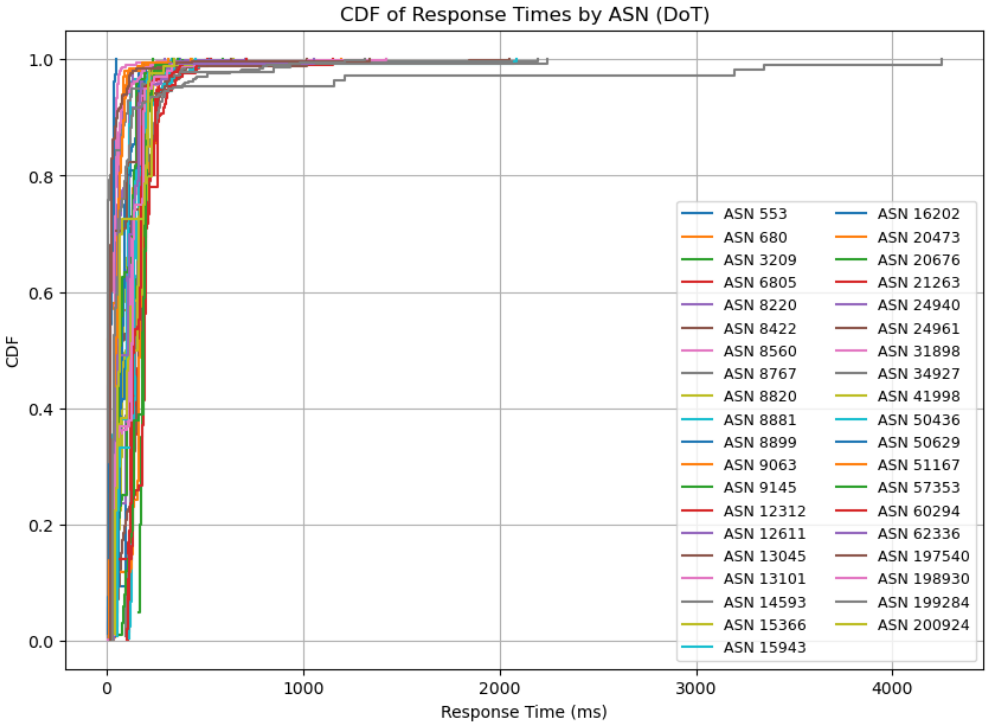
This chart indicates that 91.4% of the initiated DoT measurements were successful, a high rate, though slightly lower than the UDP success rate. The 8.6% of erroneous measurements correspond to the issues detailed in the error distribution plot, such as timeouts, address problems, and TLS connection errors. Overall, while still largely successful, DoT measurements experienced a slightly higher error rate in this dataset compared to UDP.



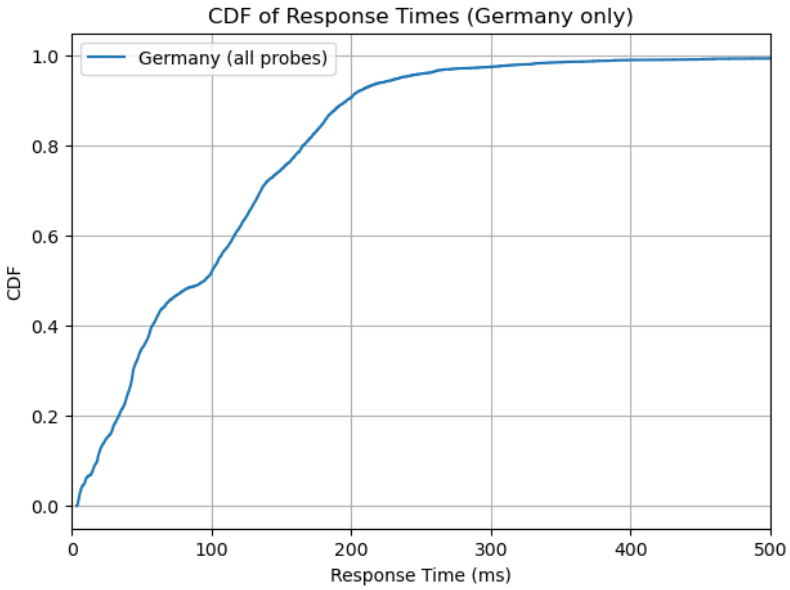
For the DoT measurements, timeouts (43.3%) were a major cause of errors, indicating probes often didn't receive a response within the 5-second window. A significant portion of errors (32.3%) were "TU_BAD_ADDR: True," which can point to issues resolving the target resolver's address or problems with the address itself. "TU_READ_ERR" and "TUCONNECT" errors, along with "Other" (including no local resolvers or TLS library issues like DH lib errors), represent smaller fractions, highlighting various connection or TLS handshake problems.



This CDF plot compares the DoT response times for the "local" and "q9" resolvers. The "q9" resolver shows a smoother, more conventional CDF curve, resolving a high percentage of queries relatively quickly, with most responses under 200ms. The "local" resolver's CDF curve is more step-like, indicating clusters of response times; it shows a rapid resolution for about 40% of queries under 50ms, then another jump around 150-170ms. This step-like behavior for "local" DoT could suggest different underlying resolution paths or caching effects.

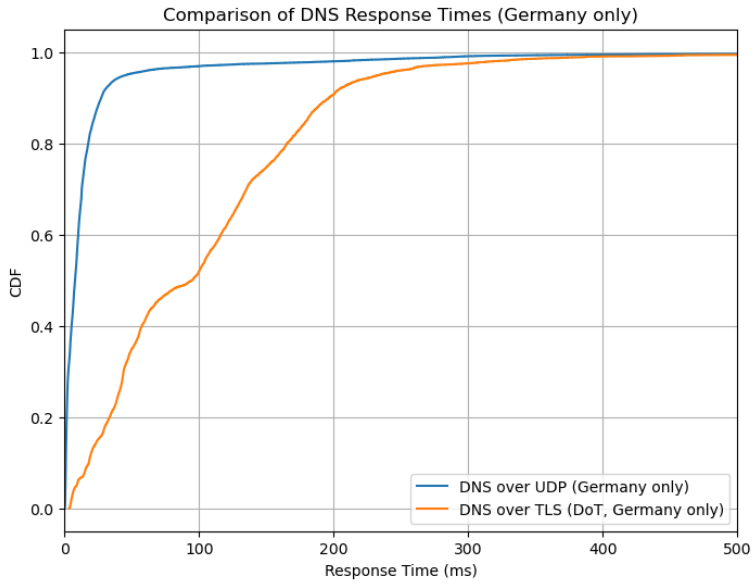


Similar to UDP, this plot for DoT shows variability in DNS resolution performance across different ASNs. Most ASNs demonstrate relatively quick DoT resolutions, but the initial rise of the CDFs is generally less steep than their UDP counterparts, and the "tails" often extend further, indicating higher latencies. Some ASNs exhibit more pronounced delays or greater variability, reflecting the combined impact of network conditions and the additional overhead of establishing secure TLS connections for DNS queries.



The aggregated CDF for all successful DoT measurements in Germany shows a generally slower and more spread-out distribution compared to UDP. While some queries are resolved quickly (around 50% under 100ms), the curve rises more gradually, indicating a wider range of response times. Reaching close to 90% resolution takes approximately 200-250ms, suggesting that the overhead of TLS handshake contributes to higher latencies for DoT compared to UDP.

Choose one CDF of your choice from Task 1 showing DNS over UDP and compare it to the corresponding CDF showing DoT. Describe similarities and differences you can see when comparing regular DNS and DoT.



The provided plot offers a direct comparison of aggregated DNS response time distributions for standard DNS over UDP and the more secure DNS over TLS (DoT) protocol, based on measurements from RIPE Atlas probes located in Germany. This analysis reveals key similarities and significant differences in their performance characteristics.

Shared Characteristics

Despite their protocol differences, both DNS over UDP and DoT demonstrate an ability to eventually resolve most queries. The Cumulative Distribution Function (CDF) curves for both protocols ultimately approach 100% within the 500ms timeframe depicted, suggesting that persistent resolution failures are not the primary distinguishing factor in this context. Furthermore, both protocols show that some queries can be resolved very rapidly, as indicated by the immediate upward trend of their respective CDF curves from 0ms. This implies that under optimal conditions, such as when responses are served from a very local cache or network latency is minimal, both UDP and DoT can deliver quick answers.

Key Performance Differences and Latency Impact

The most striking distinction lies in the overall latency profiles. DNS over UDP exhibits a significantly faster performance, characterized by a much steeper initial rise in its CDF curve and a consistent leftward shift compared to DoT. This visual disparity underscores that UDP resolves the vast majority of queries more quickly. For example, UDP achieves approximately 90% query resolution in under 50ms, a milestone that DoT only reaches at around 200-220ms. Consequently, median and other percentile response times are considerably lower for UDP. The median response time for UDP is estimated to be in the 10-20ms range, whereas for DoT, it is substantially higher, likely between 80-100ms.

The Overhead of TLS in DoT

This pronounced difference in speed is primarily due to the inherent overhead associated with the TLS protocol used by DoT. Establishing a secure TLS session necessitates a handshake procedure involving multiple network round trips between the client and the DoT resolver before the actual DNS query can

be transmitted and answered. This initial handshake latency directly contributes to the increased overall resolution time for DoT, particularly for new connections. While TLS session resumption mechanisms can reduce this overhead for subsequent queries to the same resolver, the aggregated nature of these CDFs likely includes a significant number of initial connections, thus reflecting this setup cost.

Distribution Shape and Variability

The shapes of the CDF curves also highlight differences in performance consistency. The UDP curve rises sharply and then quickly flattens, indicating a tight clustering of response times at the lower end, signifying more consistent, fast responses. In contrast, the DoT curve displays a more gradual ascent and a more pronounced "S" shape, suggesting a wider distribution and greater variability in its response times. The less smooth, somewhat "stepped" appearance of the DoT curve might also allude to distinct phases or potential bottlenecks within the TLS establishment or query resolution process affecting different subsets of measurements. Even at the fastest end of the spectrum, UDP maintains an advantage, with a notable portion of queries resolving in under 10ms, a feat that takes DoT longer to achieve due to the baseline time required for the TLS handshake.

Conclusion: The Performance-Security Trade-off

In summary, the empirical data strongly indicates that DNS over UDP offers significantly lower latency compared to DNS over TLS. The enhanced privacy and security features of DoT, such as encryption and authentication of the DNS resolver, come at a tangible cost of increased response times. This latency penalty is a direct result of the cryptographic operations and additional network communication inherent in establishing a secure TLS channel. Therefore, the choice between standard DNS and DoT involves a clear trade-off: while DoT fortifies DNS communications against eavesdropping and manipulation, users and applications highly sensitive to DNS resolution speed may experience a noticeable performance degradation compared to the traditional, albeit less secure, UDP-based approach.