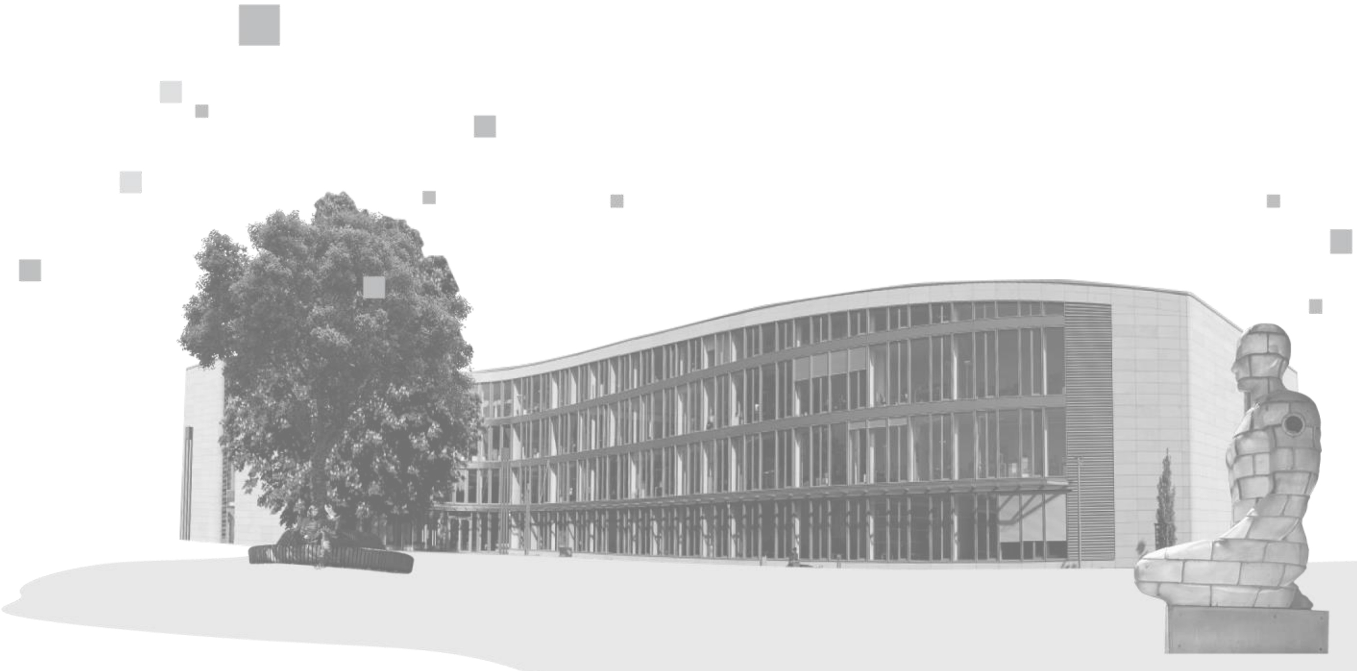
The Future of DNS Privacy

A Comparison of DNS over QUIC and DNS over HTTP/3

Philipp Bielefeld, Felix Hoffmann, Steffen Sasalla, vasilis ververis, and Vaibhav Bajpai

Presenter: **Newton Masinde**

PAM Conference, March 23-25, 2026



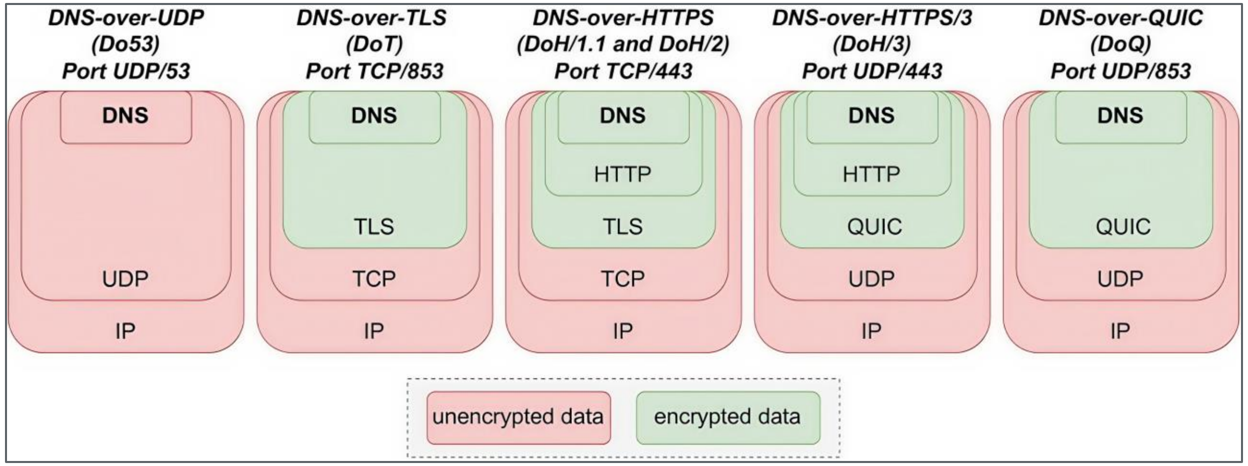
Design IT.
Create Knowledge.

www.hpi.de

Structure of Presentations

1. DNS over Encryption (DoE) Protocols
   - ***DoT, DoQ, DoH***
2. Key Considerations
   - ***Privacy & Security***
   - ***DNS Resolution on Webpage Load Time***
3. Research Questions
4. Methodology Overview
5. Results & Discussion
6. Conclusions

DNS over Encryption (DoE) Protocols


DNS-over-UDP (Do53) Port UDP/53
DNS-over-TLS (DoT) Port TCP/853
DNS-over-HTTPS (DoH/1.1 and DoH/2) Port TCP/443
DNS-over-HTTPS/3 (DoH/3) Port UDP/443
DNS-over-QUIC (DoQ) Port UDP/853
DNS
UDP
IP
DNS
TLS
TCP
IP
DNS
HTTP
TLS
TCP
IP
DNS
HTTP
QUIC
UDP
IP
DNS
QUIC
UDP
IP
unencrypted data
encrypted data

- DoT, DoH and DoQ
  - **DoT**
    - Encrypts DNS over TLS
    - Operates on TCP/853
    - Primary use --> Stub-to-recursive communication
  - **DoH**
    - Encapsulates DNS in HTTPS traffic
    - Supports multiple HTTP versions
    - Operates on TCP/443 with specific URI configurations
  - **DoQ**
    - Uses QUIC for low-latency, high-performance queries
    - Integrates TLS 1.3.
    - Operates on UDP/853

Features under Considerations

- **TLS Connections:**
  - Involves several steps essential for security
    - Cipher suite negotiation, key exchange and certificate verification.
    - Introduces latency and consumes CPU cycles
    - Problematic for high-traffic servers with resource limits.
- Solutions for performance enhancement
  - **Session Resumption (SR)**
  - **Zero round-trip time (0-RTT)**

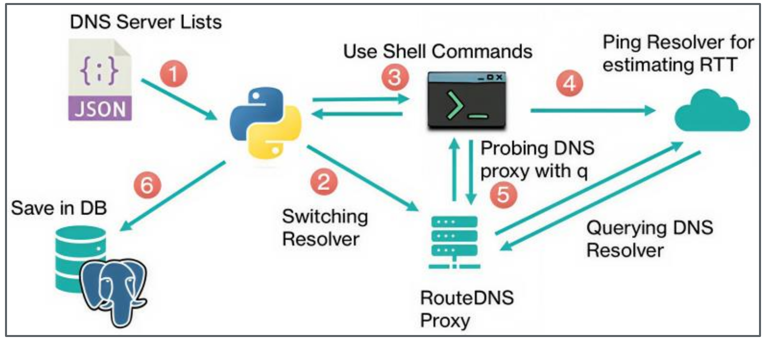
- **Session Resumption (SR)**
  - Introduced in 2008 – **RFC 5077**
  - How it works: Allows skipping parts of the handshake process if parties have recently communicated.
  - Effect: Faster connections and reduced overhead.
- **Zero round-trip time (0-RTT)**
  - Also referred to as Early Data – **RFC 8470**
  - How it works: Allows sending data to server during the handshake process
  - Effect: Eliminates initial latency penalty for establishing encrypted connection.

Research Question 1

What percentage of resolvers support performance-enhancement features for DoQ and DoH/3?

- **Motivation**
  1. **Understand the efficiency gap** → Do53 is highly efficient but unencrypted
     - To what extent do performance enhancement features (like SR & 0-RTT) improve efficiency (reduction of latency)?
  2. **Track maturity and productive use**
     - Measuring support for advanced features is needed to characterize the ecosystem maturity
  3. **Comparative evaluations of performance enhancement features in DoQ and DoH/3 are lacking**

- **Methodology**
  - Large-scale resolver discovery
    - **IPv4** → ZMap scans
    - **IPv6** → Hitlist service
  - Controlled DNS infrastructure
    - **Unique QNAME** → used for resolver behavior tracking.
    - **Authoritative servers (DoT/DoH)** → Docker setup
  - Evaluation Metrics
    - Round-trip times (RTT)
    - Session resumption
    - 0-RTT



RQ1 – Support for Performance Features

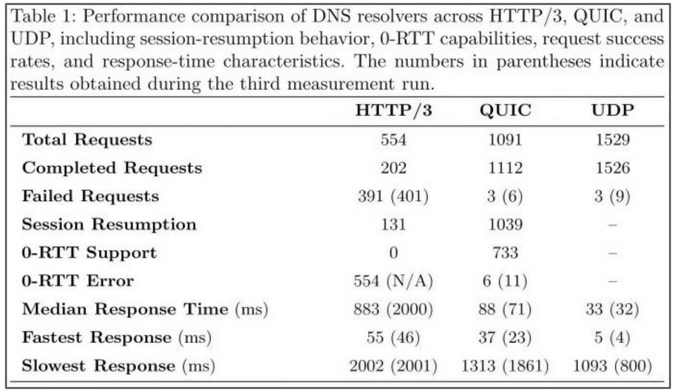


Table 1: Performance comparison of DNS resolvers across HTTP/3, QUIC, and UDP, including session-resumption behavior, 0-RTT capabilities, request success rates, and response-time characteristics. The numbers in parentheses indicate results obtained during the third measurement run.

	HTTP/3	QUIC	UDP
Total Requests	554	1091	1529
Completed Requests	202	1112	1526
Failed Requests	391 (401)	3 (6)	3 (9)
Session Resumption	131	1039	–
0-RTT Support	0	733	–
0-RTT Error	554 (N/A)	6 (11)	–
Median Response Time (ms)	883 (2000)	88 (71)	33 (32)
Fastest Response (ms)	55 (46)	37 (23)	5 (4)
Slowest Response (ms)	2002 (2001)	1313 (1861)	1093 (800)

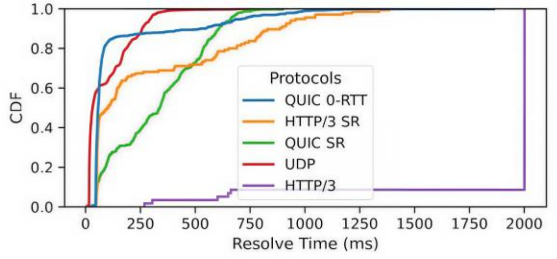
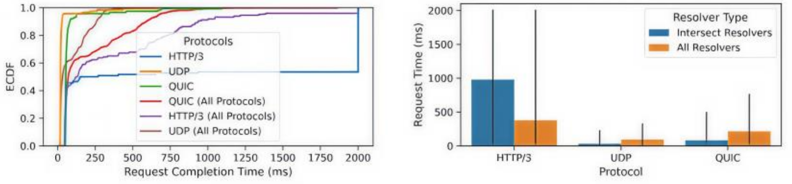


Fig. 9: CDF of DNS resolve times comparing resolvers with and without 0-RTT and session resumption.



(a) CDF of DNS resolution times

(b) Mean and 95th percentile of resolution times

Fig. 10: Comparison of DNS resolve times between the subset of resolvers supporting all DoE protocols and the complete resolver set.

- **Session Resumption and 0-RTT**
  - Session Resumption (SR) support
    - **DoQ resolvers** → ~94% (1039/1112)
    - **DoH/3 resolvers** → ~65% (131/202)
    - Suggests improved DoE efficiency
  - 0-RTT support
    - **DoQ resolvers** → Supported.
    - **DoH/3 resolvers** → No measured support
  - Impact of SR + 0-RTT support
    - Makes it possible for DoQ resolvers to approach Do53 round-trip efficiency
- **Latency Outcomes**
  - Median latency
    - **DoQ resolvers** → 88 ms
    - **DoH/3 resolvers** → 883 ms
    - DoH/3 response values → skewed by slower AdGuard resolvers
- **AdGuard Resolvers Influence**
  - AdGuard DNS resolvers → **~85% of the measured DoH/3 dataset**
  - AdGuard resolvers include slow outliers
    - Heavily skews DoH/3 values
    - **If removed** → ~50% of DoH/3 resolvers w/o SR can match DoQ's performance
- **Reliability**
  - DoH/3 found highly unreliable
    - 391 → fail measurements in certain tests
- **"Intersect subset"** (DoQ+DoH/3+Do53)
  - DoQ outperforms average Do53
  - There are lower latency percentiles
    - 95% of Do53 response < 30ms
    - 60% of Do63 response < 50ms
  - DoH/3 median response → heavily affected by slower AdGuard outliers.

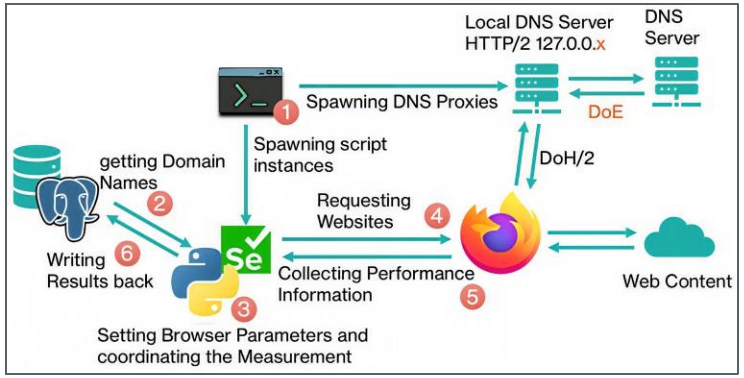
Research Question 2

What is the performance penalty of DoE protocols on website loading speed?

- **Motivation**

1. **Understand the critical role of DNS in Web Browsing** → Modern websites are complex.
   - They resolve from at least 20 different background domains per visit
   - Latency due to encryption has a cumulative effect
2. **Understand the impact on user experience**
   - Most studies compare network-level metrics and do not consider user-centric metrics

- **Methodology**
  - Setup
    - **Firefox + Selenium** with local local DNS proxy (Do53, DoQ, DoH/3)
    - Tranco top websites dataset
  - Procedure
    - Cache warm-up requests.
    - Controlled navigation and failure logging
  - Evaluation Metrics
    - First Contentful Paint (FCP)
    - Largest Contentful Paint (LCP)
    - Page Load Time (PLT)



RQ2 – Impact of DNS on Website Performance

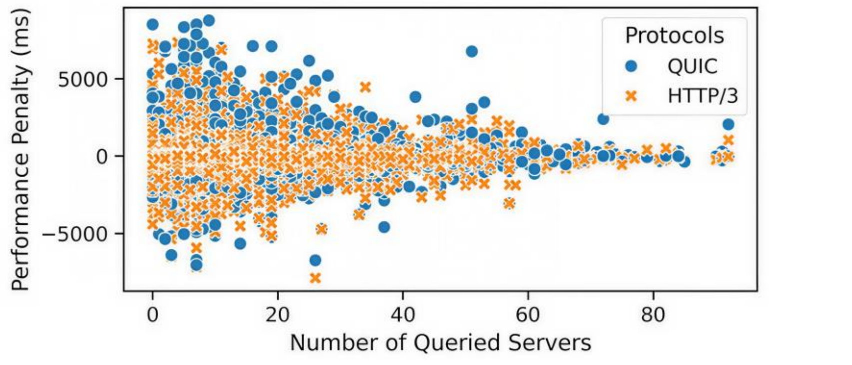
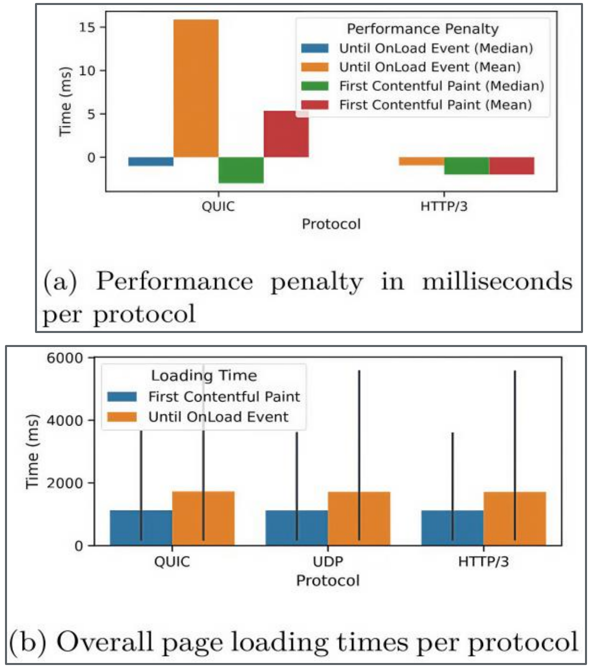


Fig. 11: Impact of the number of DNS queries on webpage FCP experience.



(a) Performance penalty in milliseconds per protocol

(b) Overall page loading times per protocol

Fig. 12: Website performance metrics for successfully measured cases across all protocols.

- **Minimal performance penalty**
  - Average page load time differences across protocols
    - ≤±1% of load time (~2ms to 16ms)
- **Protocol consistency and outliers**
  - DoQ has a slight edge in terms of raw speed
  - DoH/3 offers a more consistent UX with fewer extreme latencies

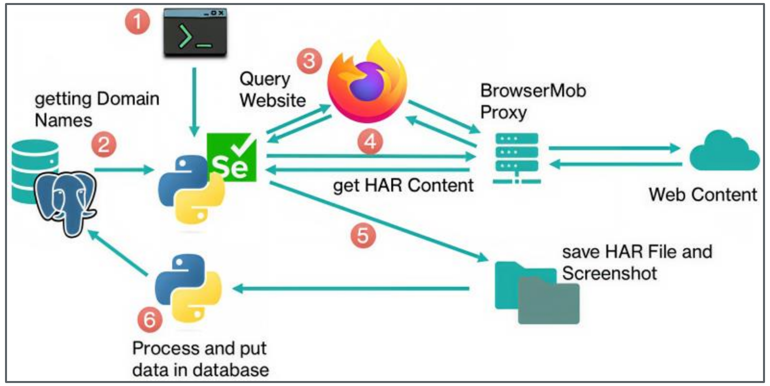
- **Takeaways**
  - DoE protocols do introduce measurable network-level overheads
  - There is no meaningful degradation of the end-to-end browsing experience under typical low-latency conditions

Research Question 3

Do certain website categories experience greater or lesser impacts from DoE resolvers, and what factors influence these variations?

- **Motivation**
  1. **Identification of performance sensitivities**
     - Understand why some websites experience greater impacts than others.
  2. **Identification of the technical and architectural factors that influence how website performance react to DoE protocols**

- **Methodology**
  - ○ Data Collection
    - **Parallel Python Scripts + BrowserMob Proxy**
    - Capture HAR network traces and screenshots
  - ○ Goal
    - Effect of site complexity on DNS performance and DoE protocols
  - ○ Evaluation Metrics
    - Object counts and total bytes
    - MIME types and DNS request counts
    - Distinct & 3rd party queried servers



RQ3 – Impact of Website Complexity

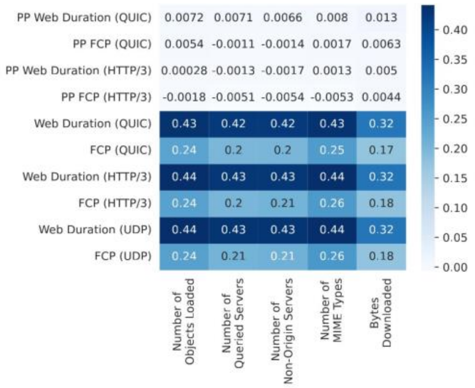


Fig. 13: Heatmap of the correlation between website complexity and performance across different DNS protocols.

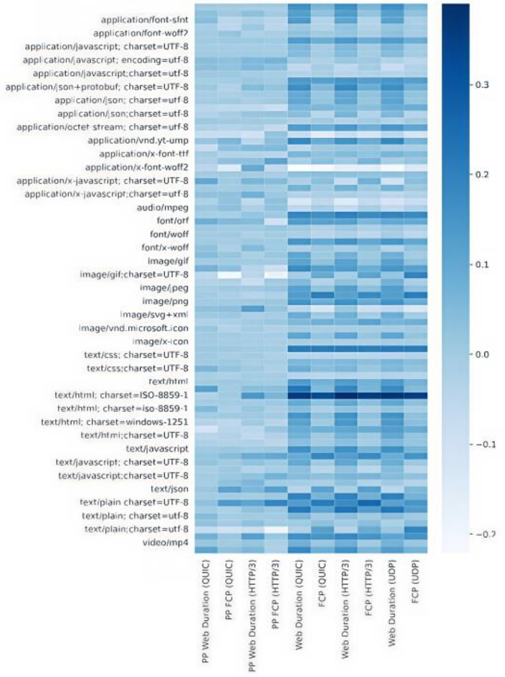


Fig. 14: Heatmap of the correlation between MIME types, DNS performance, and website loading times (*PP* stands for performance penalty).

- **Dataset & Characteristics**
  - ~572k active websites analyzed from 1M domains
  - Median: 1.2MB, 42 resources, 7 servers (~5 external), ~0.9s load time
- **Webpage complexity independence**
  - No statistically significant correlation with weak correlation coefficient (≤0.45)
    - No predictable or meaningful increase in performance penalty due to increased complexity
  - **Important**: complexity does correlate with page load time
- **Other insights**
  - MIME types → no significant or consistent impact on performance
  - DNS protocol influence → minimal across different website types

- **Takeaway**
  - DNS has limited effect on performance in low-latency environments

Conclusions

- **RQ1: What %age of resolvers support performance enhancement features for DoQ and DoH/3?**
  - DoQ Resolvers: SR support → ~94%; 0-RTT support → ~66%
  - DoH/3 resolvers: SR support → 65%; 0-RTT support → **Not observed**
  - **Strong indicator of adoption of QUIC features in DoQ since 2022**
- **RQ2: What is the performance penalty of DoE protocols on website loading speed?**
  - Longer DNS query times → **Does NOT generally imply slow page loads**
  - DoH/3 → **shows more consistent median and average load times than DoQ**
  - There is **minimal impact on performance under low-latency conditions** → Queries run concurrent with other browser tasks.
  - **Best performance → Resolvers supporting all DoE protocols; DoQ outperforms average Do53 speeds**
- **RQ3: Do certain website categories experience greater or lesser impacts from DoE resolvers, and what factors influence these variations?**
  - Number of objects, queried servers, website size & MIME types → **No significant effect on DoE performance penalties**
  - DoE overhead exists at DNS level → **Does not degrade overall webpage load performance**
  - **Complexity supports adoption of privacy-preserving DoE protocols without degrading user experience**

Dataset: https://doi.org/10.5281/zenodo.17860118