

Benchmarking di server e protocolli DNS sicuri

Reti Geografiche: Struttura, analisi e prestazioni

A.A. 2023/2024

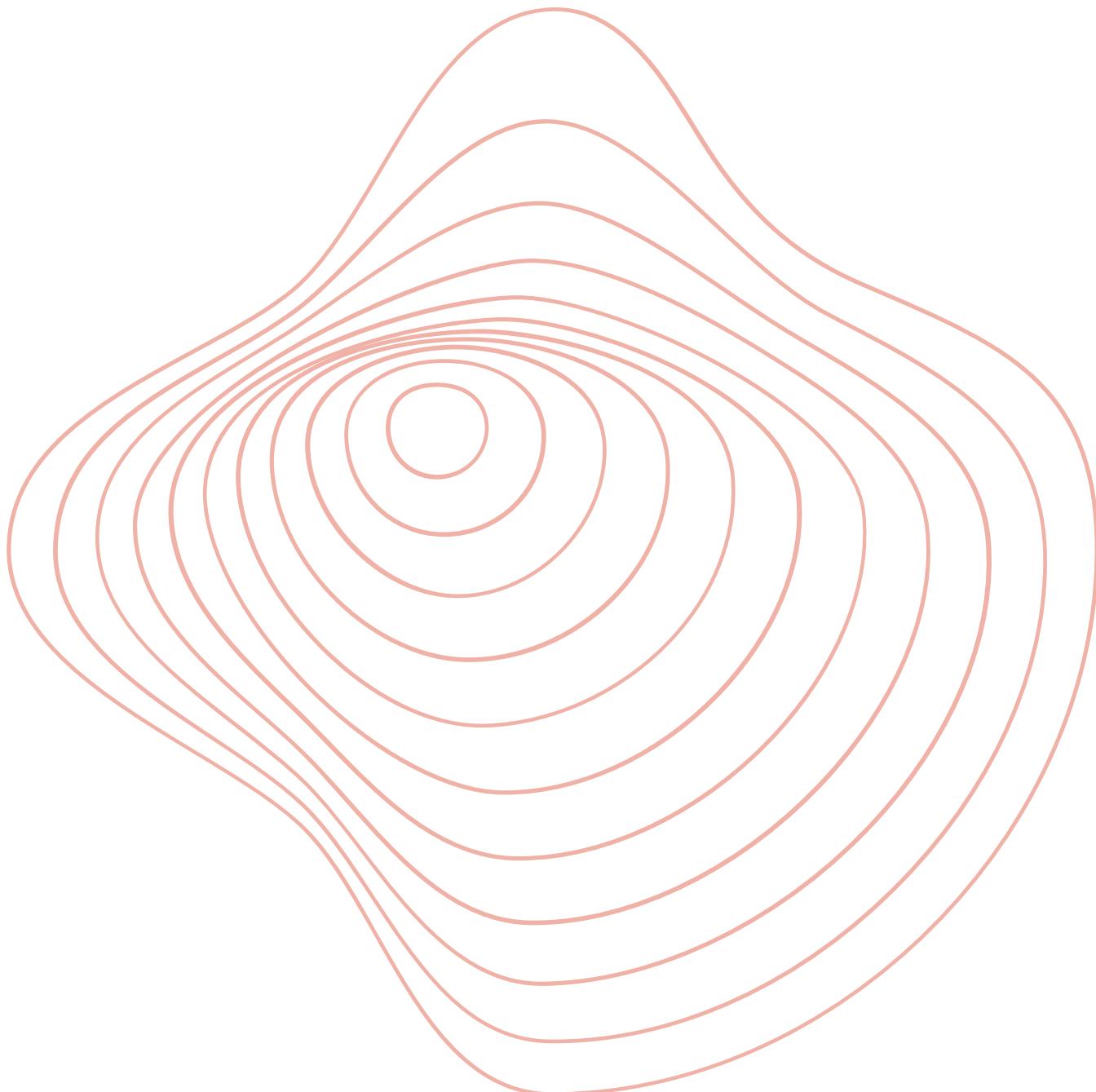
Team:

Nicolapio Gagliarde - 05225 01488
Alessandro Macaro - 05225 01459
Alberto Montefusco - 05225 01498

Introduzione

Panoramica dei contenuti

- *Background*
- *Stato dell'arte*
- *Dataset*
- *Virtual Machine*
- *Tools utilizzati*
- *BIND9, PowerDNS e Technitium*
- *Benchmarking - Un protocollo su tutti i server*
- *Benchmarking - Un server con tutti i protocolli*
- *Conclusioni*

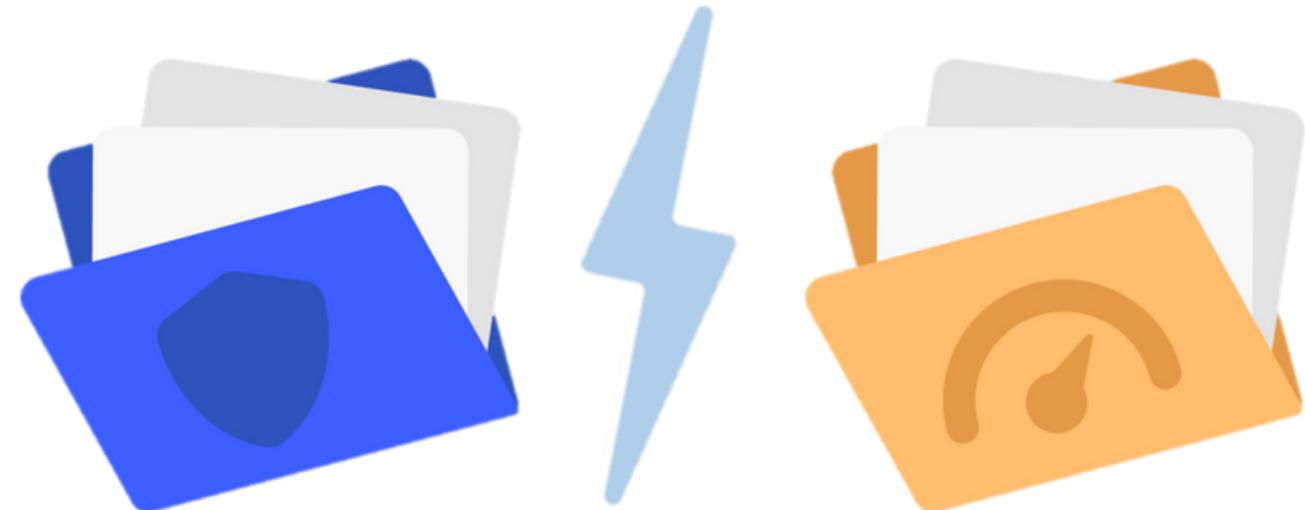


Background

Un server DNS è principalmente un registro di domini che quando viene interrogato da un client risolve il dominio richiesto inviando l'IP corrispondente. Tuttavia, la sua importanza non si limita a questo ruolo fondamentale; assume anche responsabilità cruciali, quali la gestione di liste anti-spam, la risoluzione dei servizi di posta elettronica e supporta sia IPv4 che IPv6.

Progettato inizialmente su

- **UDP**: connection-less, offre alte performance, ma non offre affidabilità
- **TCP**: offre affidabilità, ma causa un overhead maggiore dovuto all'handshake della connessione

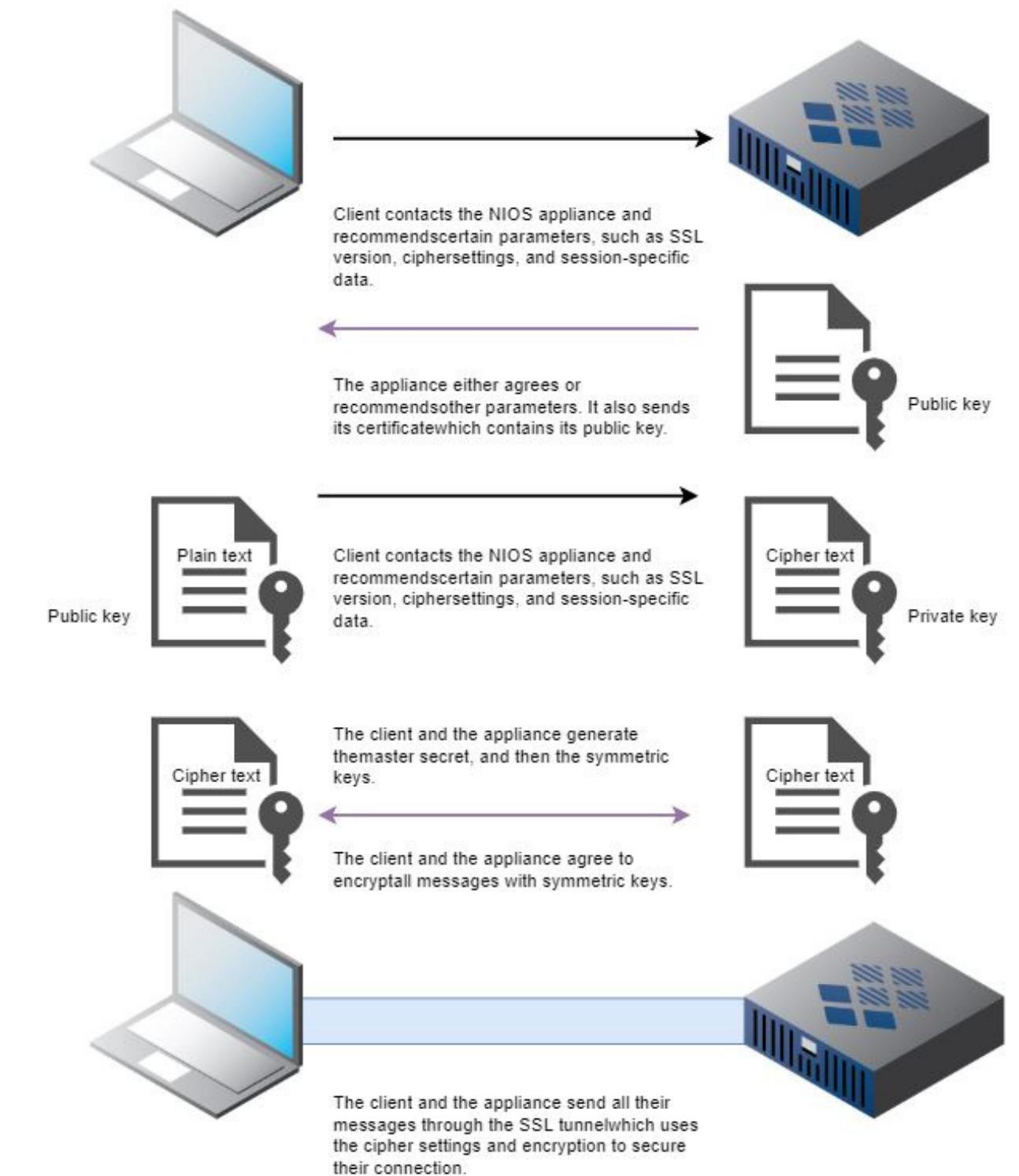


Per risolvere i problemi di sicurezza di DNS sono stati creati i seguenti protocolli:

- **DNS-over-TLS**

Viene utilizzata una connessione TLS, e quindi TCP, per garantire integrità e confidenzialità. Inizialmente vengono scambiati due messaggi per derivare dalle chiavi asimmetriche una **chiave simmetrica**, essa verrà utilizzata per cifrare le richieste e le risposte DNS.

Durante il processo il client verifica l'identità del server utilizzando i **certificati digitali**.

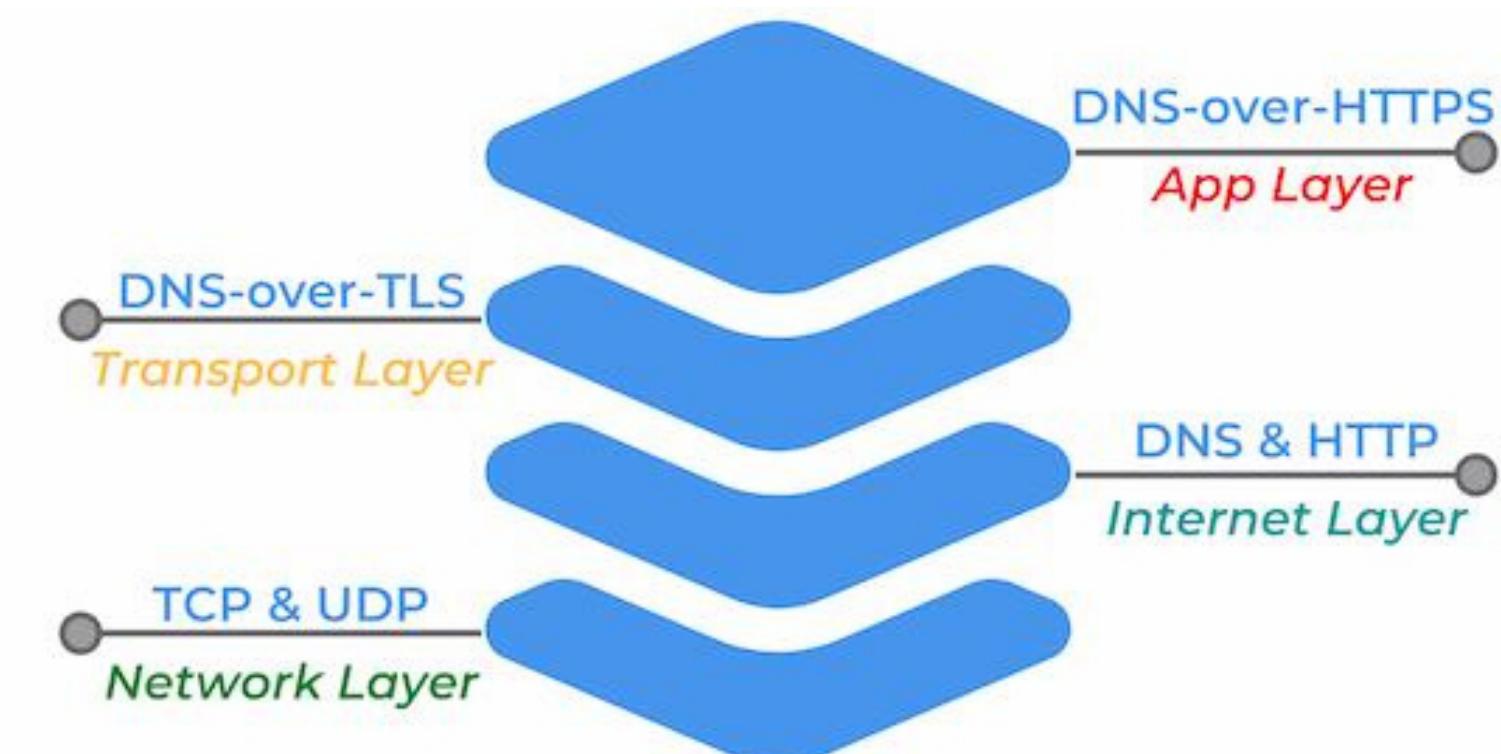


- **DNS-over-HTTPS**

Prevede un **layer addizionale** sopra TLS e una volta che la connessione TLS viene stabilita vengono creati streams multipli del protocollo HTTP su cui vengono scambiate richieste e risposte DNS

- **DNSSEC**

Vengono utilizzati **certificati** e **firme digitali** per fornire autenticazione dei dati, autenticazione di denial of existence ed integrità



Stato dell'arte

Comparing the effects of DNS, DoT, and DoH on web performance

Obiettivo: Analizzare le performance dei protocolli DNS, DoT e DoH utilizzando i resolver di Google, Cloudflare e Quad9 con una rete in condizioni non ottimali

Tool: Per salvare il tempo di caricamento della pagina è Selenium, invece per i tempi di risposta delle query DNS sono state utilizzate le due librerie C: getdns e libcurl

Risultati: Per le query più lente DoH ha tempo di risposta medio e deviazione standard migliori di DNS e con una rete che perde pacchetti il tempo di caricamento della pagina è più veloce usando DoT e DoH rispetto DNS

Benchmarking Authoritative DNS Servers

Obiettivo: Esaminare le performance dei server BIND, NSD, Knot DNS e YADIFA utilizzati con il protocollo DNS64

Tool: Il tool di benchmarking utilizzato è dns64perf++, per quanto riguarda la metodologia gli autori seguono l'RFC 8219

Risultati: Dai risultati risulta che all'aumentare dei core aumentano le prestazioni dei server tranne di YADIFA, dai test in cui si raddoppia la taglia del file di zone si evince una degradazione delle performance solo con BIND, infine risulta che NSD e KnotDNS offrono performance migliori di BIND e YADIFA

Dataset

Il dataset utilizzato in questo lavoro è stato creato a partire dalla lista di URL "italy" presente in un Dataset aggiornato nel 2021.

Ogni URL è stato sottoposto a un processo di pre-processing per rimuovere caratteri non ammessi dallo standard URL e poi utilizzato per creare un record di tipo A nel file di zona presente nei server DNS, per un totale di **2 milioni di record**.

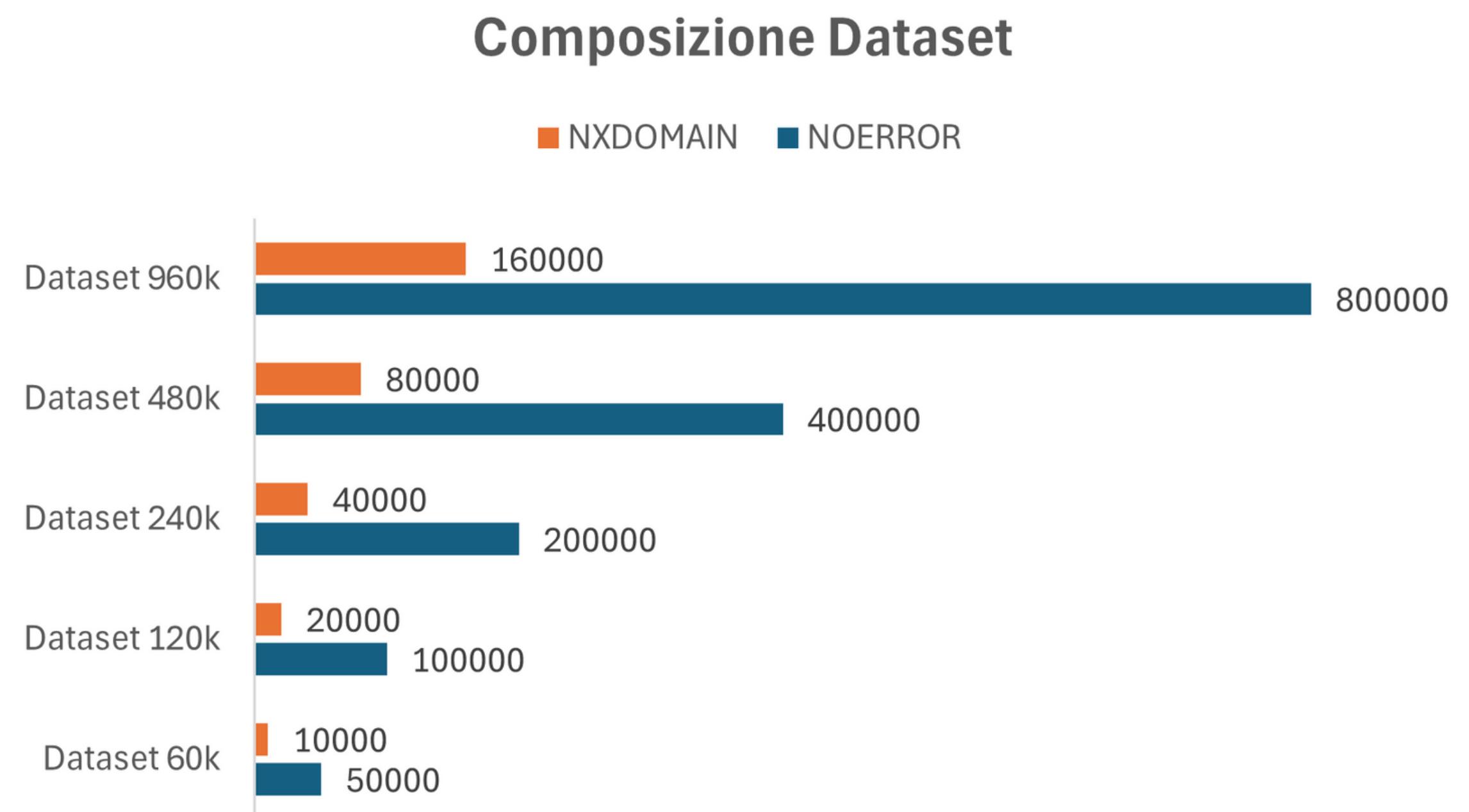
Il formato del record è il seguente

url IN A indirizzoIP

Ogni dataset ha un insieme di records inseriti precedentemente nei server DNS e un insieme di records NON inseriti nei server che quindi causano risposte NXDOMAIN.



Sono stati creati i seguenti dataset:



Virtual Machine

Per effettuare il benchmarking si è deciso di utilizzare le Virtual Machine, una decisione motivata da diversi test:

- Inizialmente, è stato condotto un test utilizzando due PC differenti (uno per il lato client e uno per il lato server), ma si sono manifestati diversi problemi nella comunicazione tra le due macchine e nelle schede di rete
- Successivamente si è optato per un approccio diverso, in cui il test veniva eseguito su un singolo PC, ma con due Virtual Machine differenti (una configurata come client e l'altra come server)

Infine, si è giunti alla soluzione definitiva di utilizzare una singola Virtual Machine con funzionalità sia server che client per effettuare i test



Tools utilizzati

Per testare il corretto funzionamento e configurazione dei server sono stati utilizzati diversi tool:

- **dig**, che permette di effettuare anche controlli relativi ai protocolli crittografici utilizzati da DNS-over-TLS, DNS-over-HTTPS e DNSSEC
- **dnsperf**, che permette di effettuare il benchmarking dei protocolli DNS-over-UDP, DNS-over-TCP e DNS-over-TLS

Purtroppo dnsperf non permette di eseguire richieste DNSSEC e DNS-over-HTTPS, quindi si è deciso di utilizzare **kdig** all'interno di uno script realizzato ad hoc per effettuare richieste multiple e tenere traccia dei nanosecondi necessari per risolvere la richiesta



Panoramica dei Server DNS

BIND



Anno di uscita: 1988

BIND è una suite di software mantenuta dalla Internet Systems Consortium per implementare sistemi DNS. Nella suite è presente il componente named che funge sia da server DNS autoritativo per le zone DNS che da resolver ricorsivo.



PowerDNS



Anno di uscita: 2002

PowerDNS offre un'alta scalabilità ed è in grado di funzionare con vari backend. In questo lavoro è stato scelto gsqlite3 siccome è quello più utilizzato e inoltre è stato installato DNSdist per attivare l'uso di DNS-over-HTTPS e DNS-over-TLS.

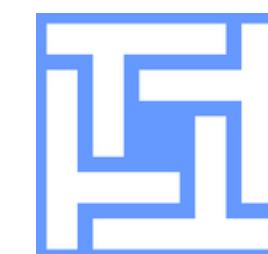


Technitium



Anno di uscita: 2017

Technitium è un server DNS autoritativo e open source, inoltre può essere usato come resolver ricorsivo. E' possibile installarlo con una configurazione minima ed offre un interfaccia web avanzata.



BIND9

Con questo server sono stati configurati i seguenti protocolli:

DNS-OVER-UDP & DNS-OVER-TCP

Dopo aver installato BIND è stato creato il file di zona contenente i records, il quale è stato aggiunto al file **named.conf.local**.

Inoltre è stato modificato il file **named.conf.option** per configurare l'interfaccia di loopback e l'IP su cui ricevere le richieste DNS.

DNSSEC

Innanzitutto è stata generata la zone-signing key (**ZSK**) e la key-signing key (**KSK**). Queste chiavi sono state utilizzate per firmare la zona e successivamente aggiunta al file named.conf.local

DNS-OVER-TLS

Nel file named.conf.options è stata aperta la porta **853** e abilitato tls ephemeral sull'ip di loopback

DNS-OVER-HTTPS

Dopo aver installato BIND è stato creato il file di zona contenente i records, il quale è stato aggiunto al file **named.conf.local**.

Inoltre è stato modificato il file **named.conf.option** per configurare l'interfaccia di loopback e l'IP su cui ricevere le richieste DNS.

PowerDNS

Con questo server sono stati configurati i seguenti protocolli:

DNS-OVER-UDP

È stato installato PowerDNS e aggiunto il file di zona nel file **named.conf**

DNSSEC

Viene modificato il file **pdns.conf** aggiungendo le istruzioni:

- launch=gsqlite3
- gsqlite3-database=/var/lib/powerdns/pdns.sqlite3
- gsqlite3-dnssec=yes

DNS-OVER-TLS

Vengono creati i certificati e la chiave mediante openssl. Successivamente viene creato il file **dnsdist.conf** in cui è stata aggiunta la riga “**addTLSLocal('127.0.0.1', '/path/certificate', '/path/key')**”

DNS-OVER-HTTPS

Vengono creati i certificati e la chiave mediante openssl. Successivamente viene creato il file **dnsdist.conf** in cui è stata aggiunta la riga “**addDOHLocal('127.0.0.1', '/path/certificate', '/path/key')**”

Technitium

Con questo server sono stati configurati i seguenti protocolli:

DNS-OVER-UDP & DNS-OVER-TCP

Dopo aver installato Technitium sono stati caricati 1,4 milioni di record utilizzando l'interfaccia web del server DNS e il tool **xclip**.

DNSSEC

Inizialmente viene creata una zona vuota, dall'interfaccia web è stata poi firmata impostando **ECDSA**, **P256** e **SHA256**. Successivamente sono stati importati i record.

DNS-OVER-TLS

Innanzitutto vengono creati i certificati usando openssl, poi attraverso l'interfaccia web sono stati configurati nel sistema, sono state impostate le porte e nella sezione forwarder è stato aggiunto "**tls-certificate-domain:853**"

DNS-OVER-HTTPS

La configurazione di questo protocollo è identica a quella di DNS-over-TLS con la differenza che in forwarders va inserita la riga "**https://tls-certificate-domain/dns-query**"

Benchmarking

In questa prima sezione vengono riportati i dati ottenuti dal benchmarking effettuato su **tutti i server dato uno specifico protocollo**, quindi per ogni protocollo vengono riportati i risultati ottenuti da ogni server.

NB: Tra ogni sessione di benchmarking è stato eseguito uno spegnimento del server seguito dal riavvio della macchina virtuale, al fine di eliminare eventuali residui di buffer, cache e file temporanei, garantendo così una valutazione più accurata delle prestazioni.



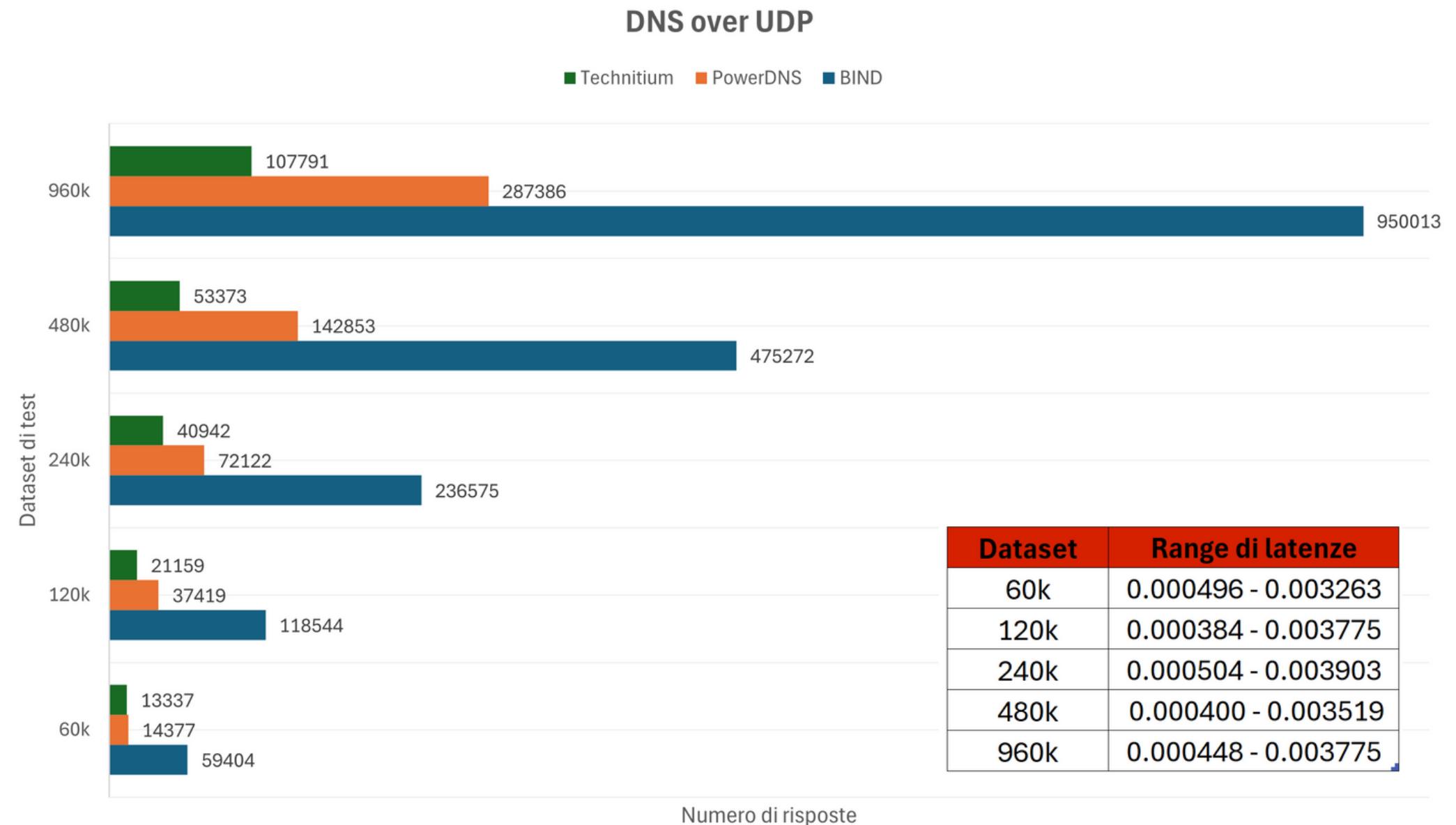
DNS over UDP

SERVER VINCENTE: BIND

BIND si è dimostrato il server più efficiente, risolvendo il 95% delle richieste in un intervallo di latenze inferiore rispetto a PowerDNS e Technitium.

PRESTAZIONI E NUMERO DI RISPOSTE

BIND supera significativamente gli altri due server in termini di numero di richieste risolte. Nel caso del protocollo UDP il peggiore si rivela essere Technitium.



NB: Il range di latenze utilizzato viene selezionato in base al server che presenta il range di latenze più basso e che riesce a gestire il 95% delle richieste

GRAFICO DELLE LATENZE

BIND si è dimostrato il server più efficiente, risolvendo il 95% delle richieste in un intervallo di latenze inferiore rispetto a PowerDNS e Technitium.

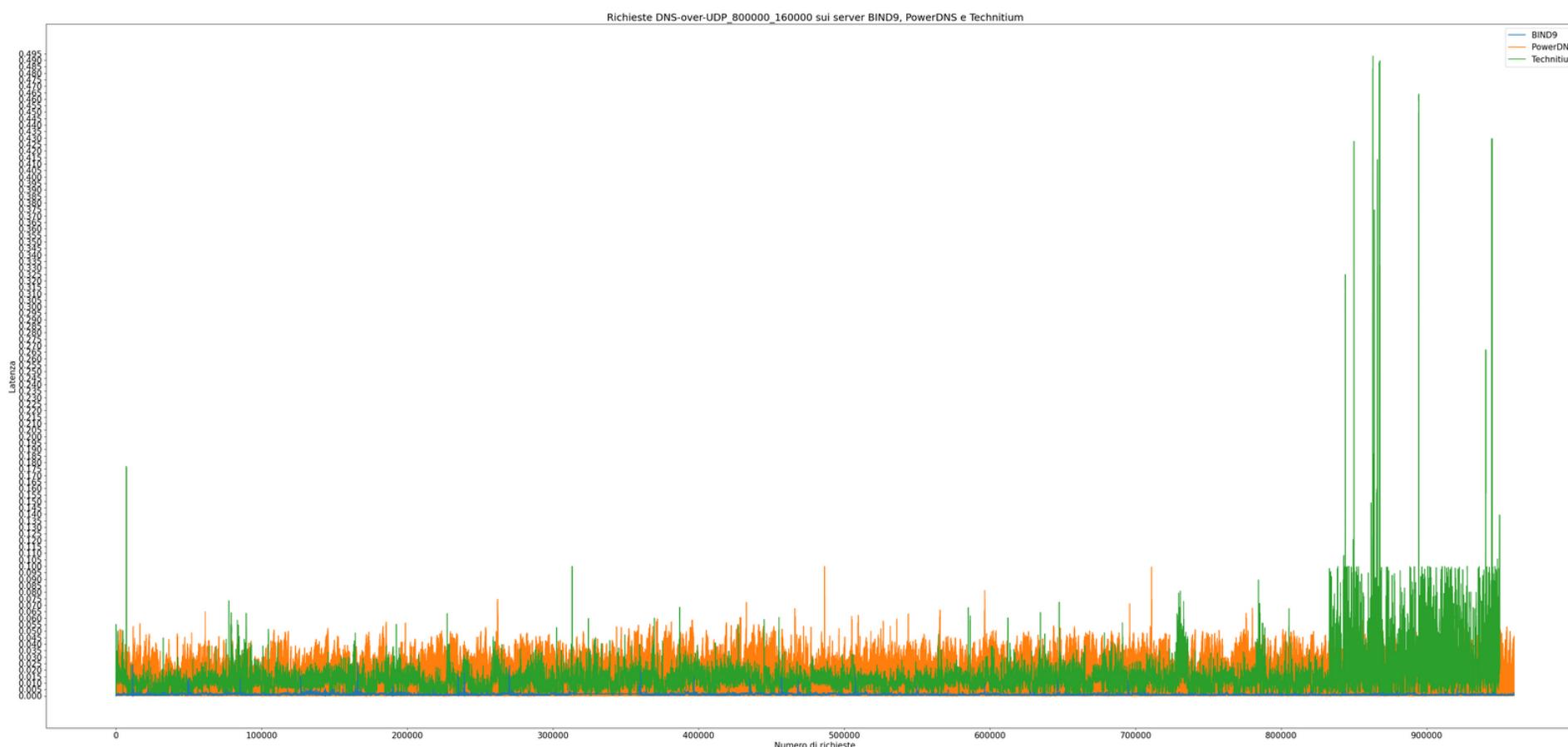
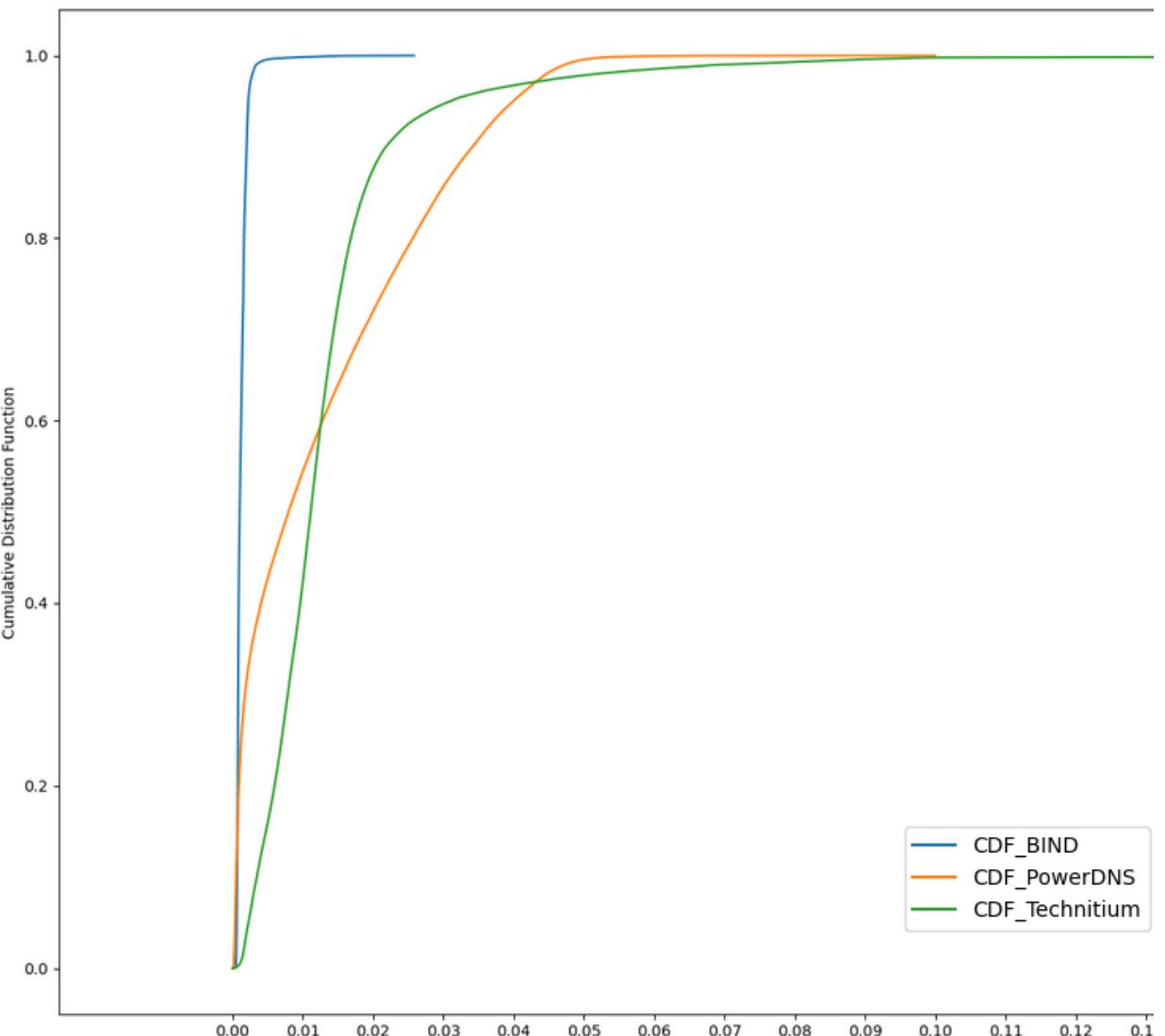


GRAFICO DELLE CDF

BIND converge molto rapidamente a 1, mentre gli altri due server convergono ad uno più lentamente. In particolare Technitium risulta essere il più lento.



DNS over TCP

SERVER VINCENTE: BIND

il server in grado di risolvere il 95% delle richieste in un range di latenze più basso rispetto agli altri server si riconferma essere BIND.

PRESTAZIONI E NUMERO DI RISPOSTE

BIND supera significativamente gli altri due server in termini di numero di richieste risolte. Nel caso del protocollo TCP il peggiore si rivela essere Technitium.

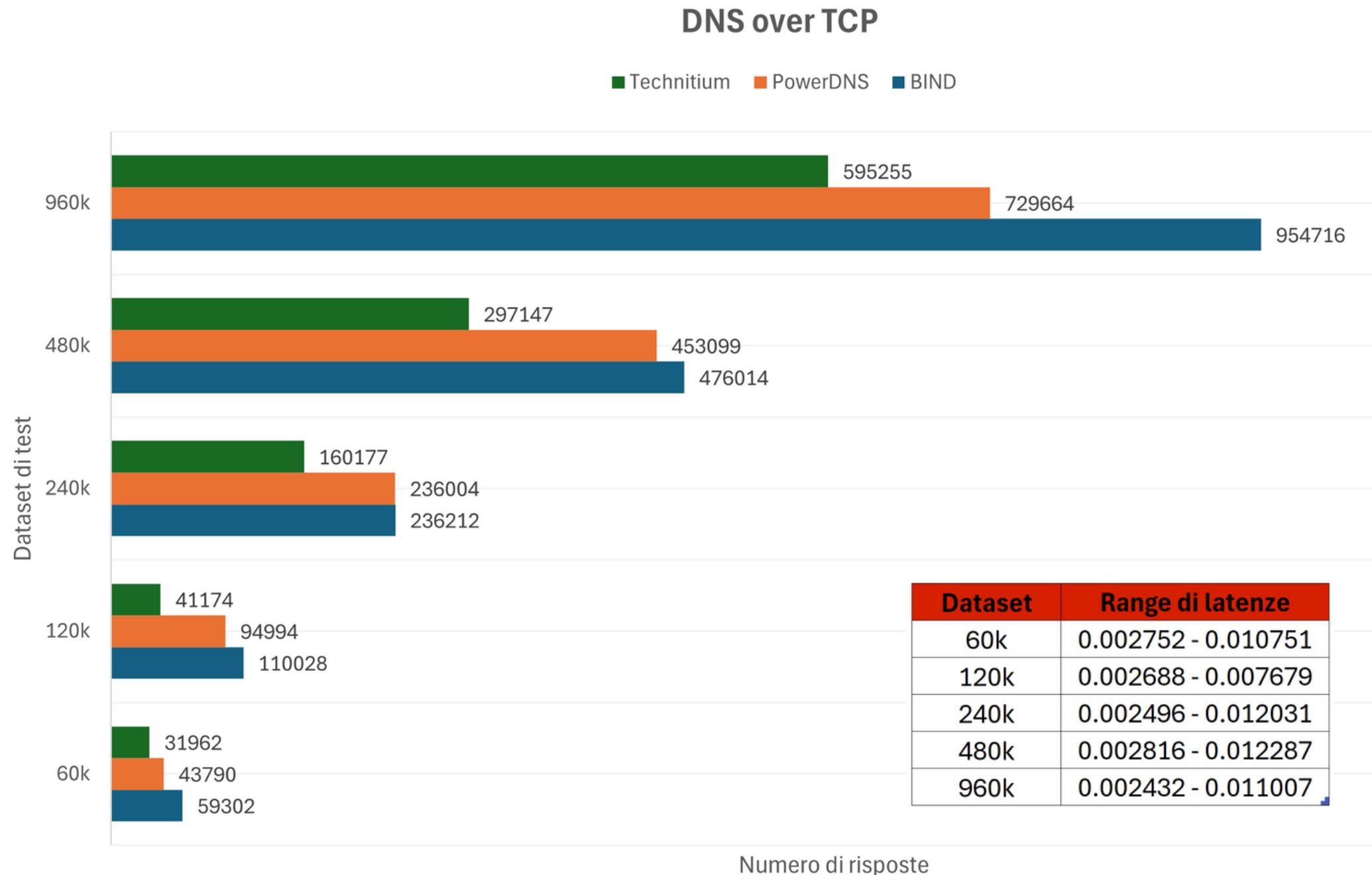


GRAFICO DELLE LATENZE

In questo caso il grafico delle latenze non si discosta molto da quello di UDP a parte il fatto di avere latenze più alte giustificate dal protocollo sottostante. Si rende solo più evidente che Technitium presenta picchi più alti e più numerosi rispetto a PowerDNS.

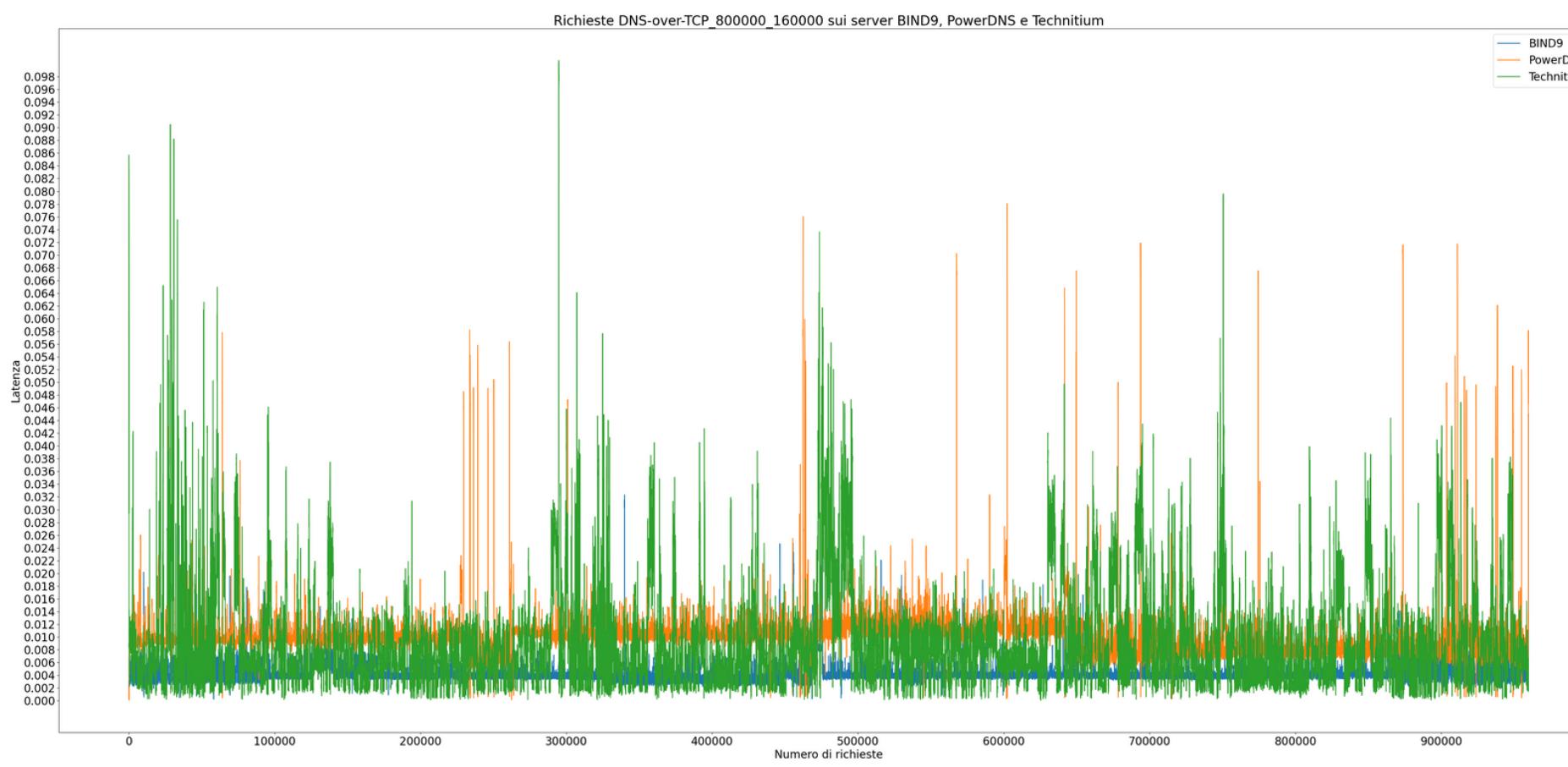
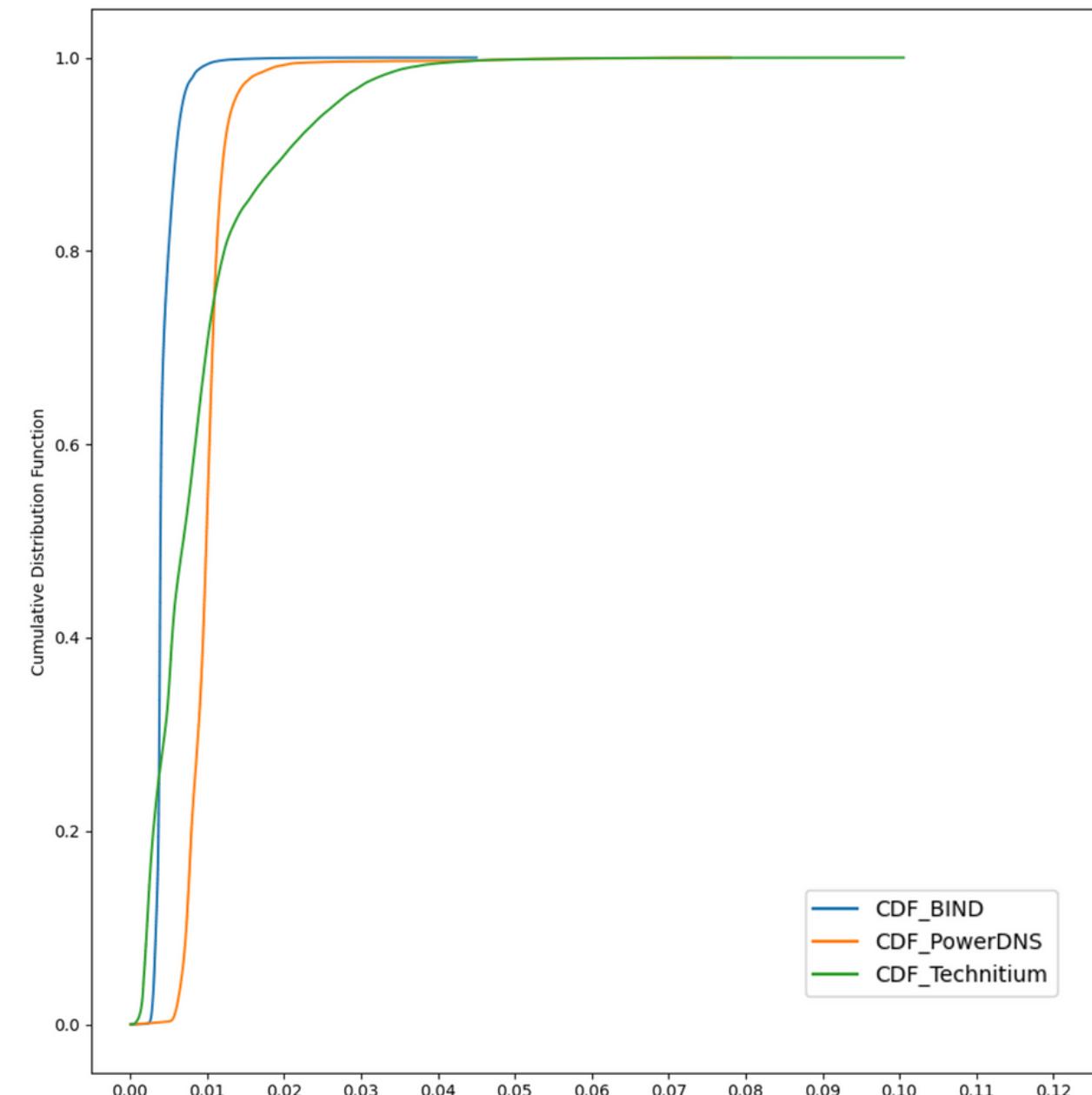


GRAFICO DELLE CDF

BIND converge molto rapidamente a 1, mentre gli altri due server convergono ad uno più lentamente. In particolare Technitium risulta essere il più lento.



DNSSEC

SERVER VINCENTE: BIND

BIND si è dimostrato il server più efficiente, risolvendo il 95% delle richieste in un intervallo di latenze inferiore rispetto a PowerDNS e Technitium.

PRESTAZIONI E NUMERO DI RISPOSTE

BIND supera significativamente gli altri due server in termini di numero di richieste risolte. Nel caso del protocollo DNSSEC il peggiore si rivela essere PowerDNS.

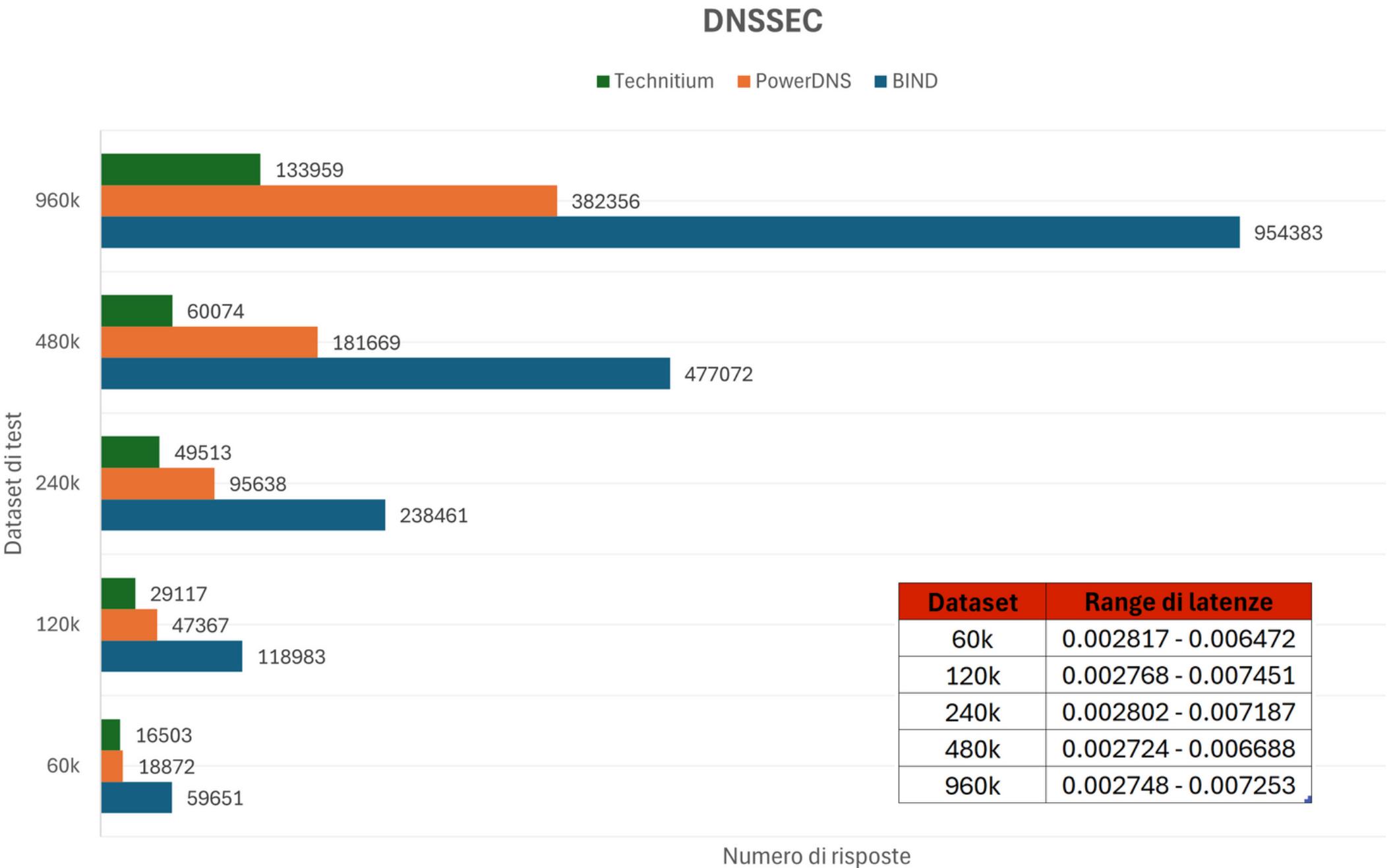


GRAFICO DELLE LATENZE

Ciò che si evince da questo grafico è che il peggiore risulta essere PowerDNS e che Technitium nelle ultime 100000 richieste raggiunge latenze di gran lunga più alte, ma si ipotizza che ciò sia dovuto al tool dnsperf.

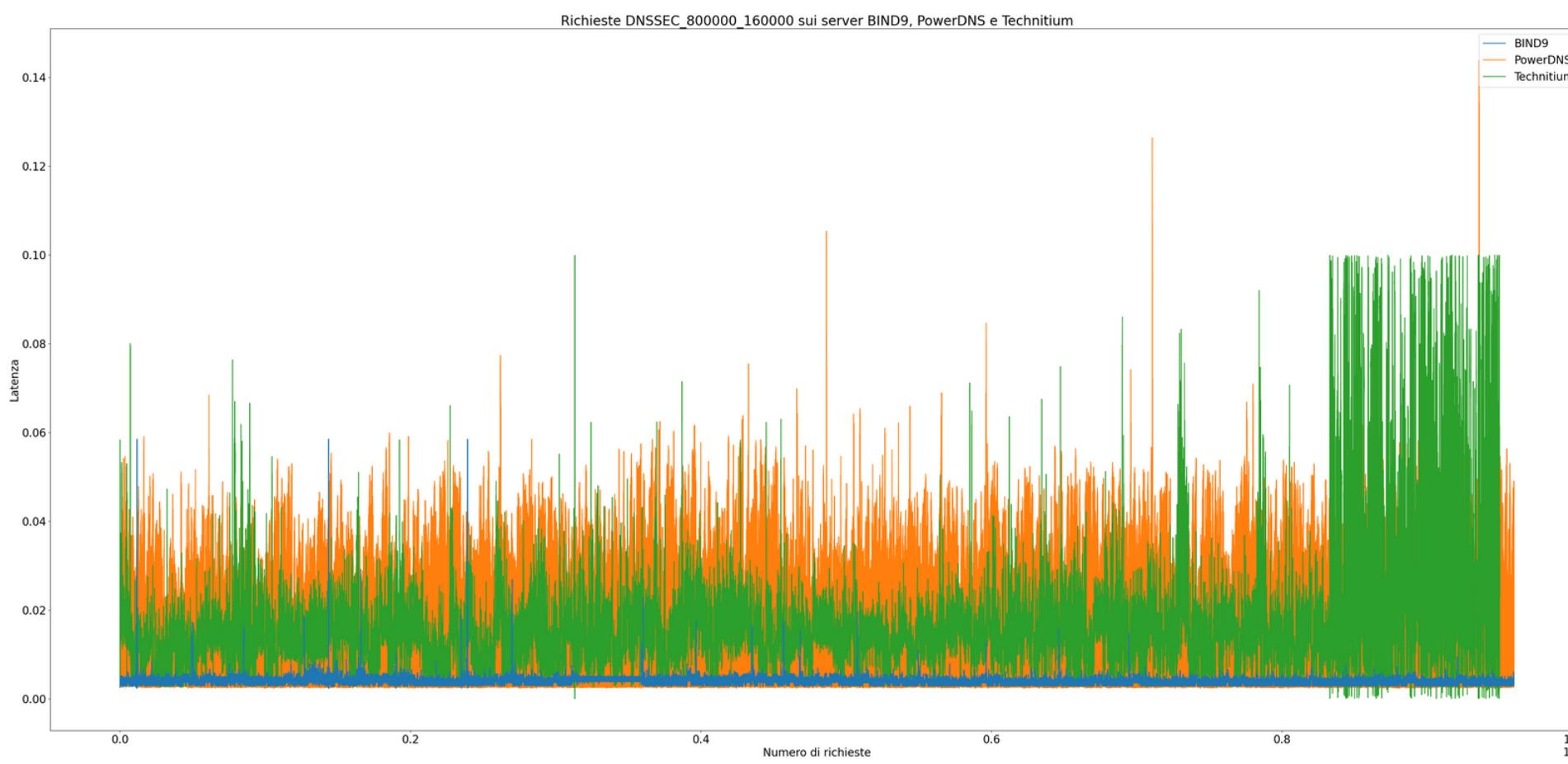
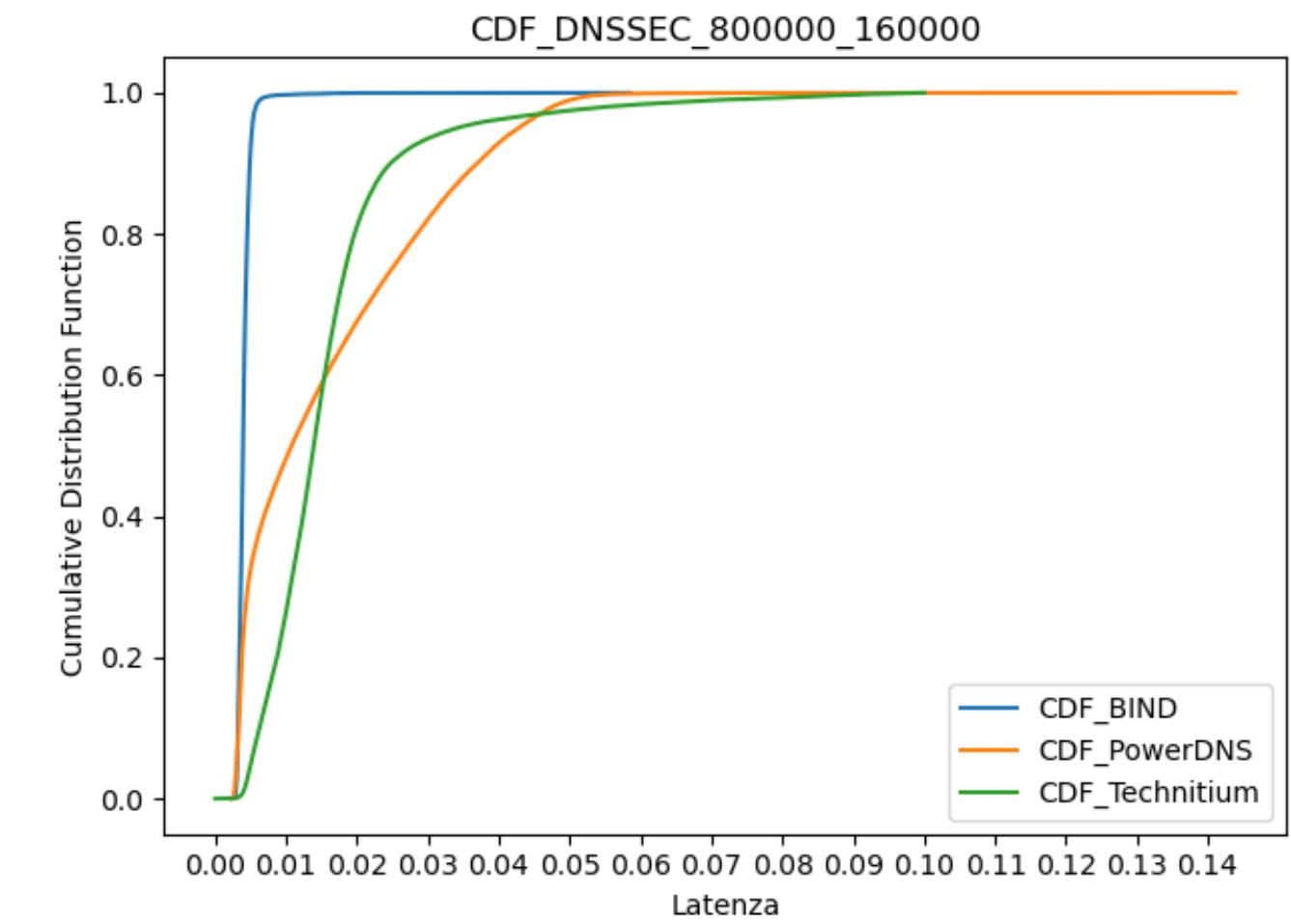


GRAFICO DELLE CDF

BIND converge rapidamente a 1, mentre gli altri server impiegano più tempo. Inizialmente, PowerDNS ha una latenza inferiore o uguale a 0.02 con una probabilità maggiore, ma successivamente Technitium supera tale andamento.



DNS over TLS

SERVER VINCENTE: BIND

BIND si è dimostrato il server più efficiente, risolvendo il 95% delle richieste in un intervallo di latenze inferiore rispetto a PowerDNS e Technitium.

PRESTAZIONI E NUMERO DI RISPOSTE

BIND supera significativamente gli altri due server in termini di numero di richieste risolte. Nel caso del protocollo TLS il peggiore si rivela essere PowerDNS.

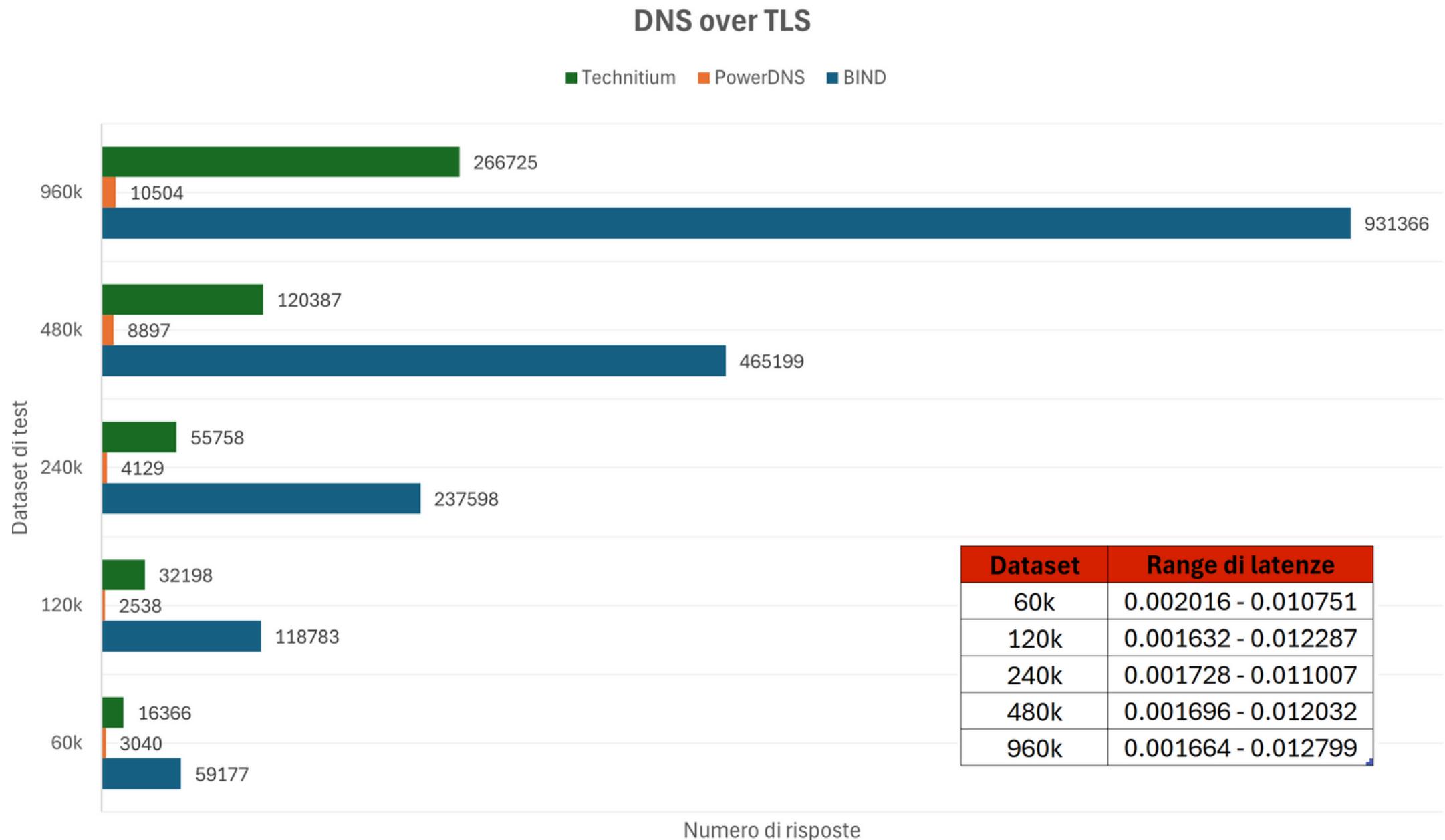


GRAFICO DELLE LATENZE

BIND si è dimostrato il server più efficiente, risolvendo il 95% delle richieste in un intervallo di latenze inferiore rispetto a PowerDNS e Technitium.

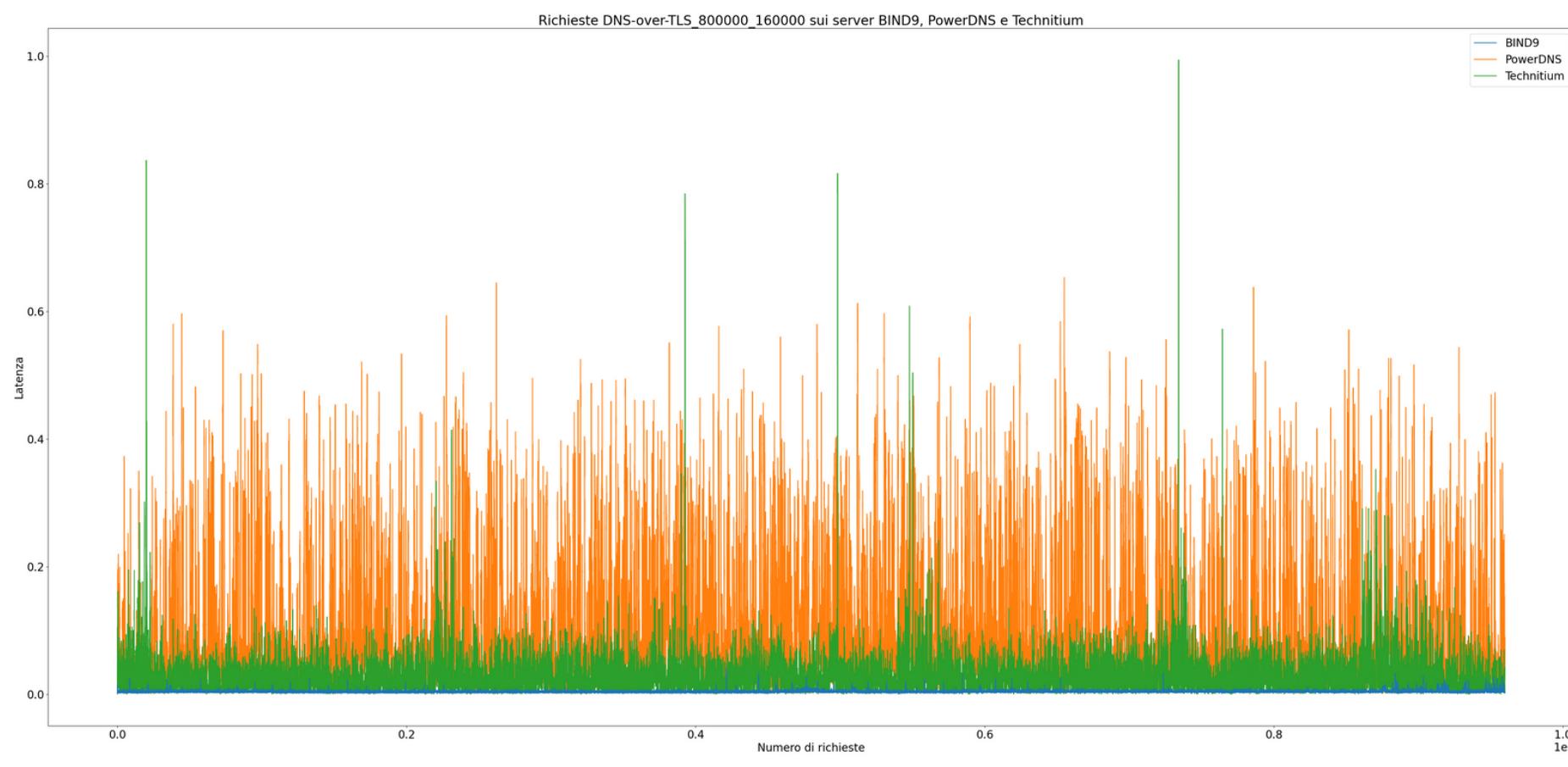
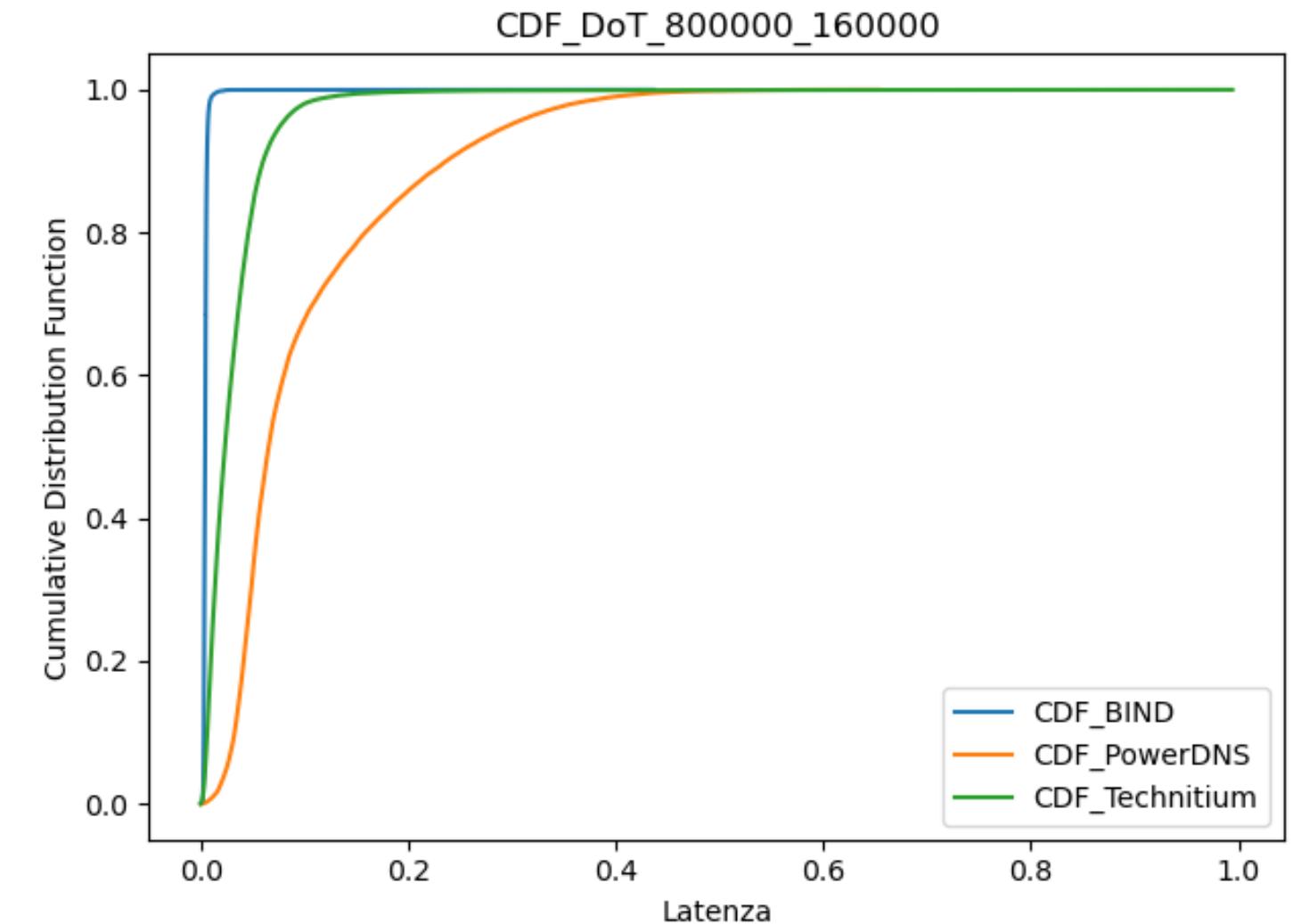


GRAFICO DELLE CDF

BIND converge molto rapidamente a 1, Technitium si discosta di poco e PowerDNS converge molto lentamente a 1.



DNS over HTTPS

SERVER VINCENTE: BIND

BIND si è dimostrato il server più efficiente, risolvendo il 95% delle richieste in un intervallo di latenze inferiore rispetto a PowerDNS e Technitium.

PRESTAZIONI E NUMERO DI RISPOSTE

BIND supera significativamente gli altri due server in termini di numero di richieste risolte. Nel caso del protocollo HTTPS il peggiore si rivela essere PowerDNS.

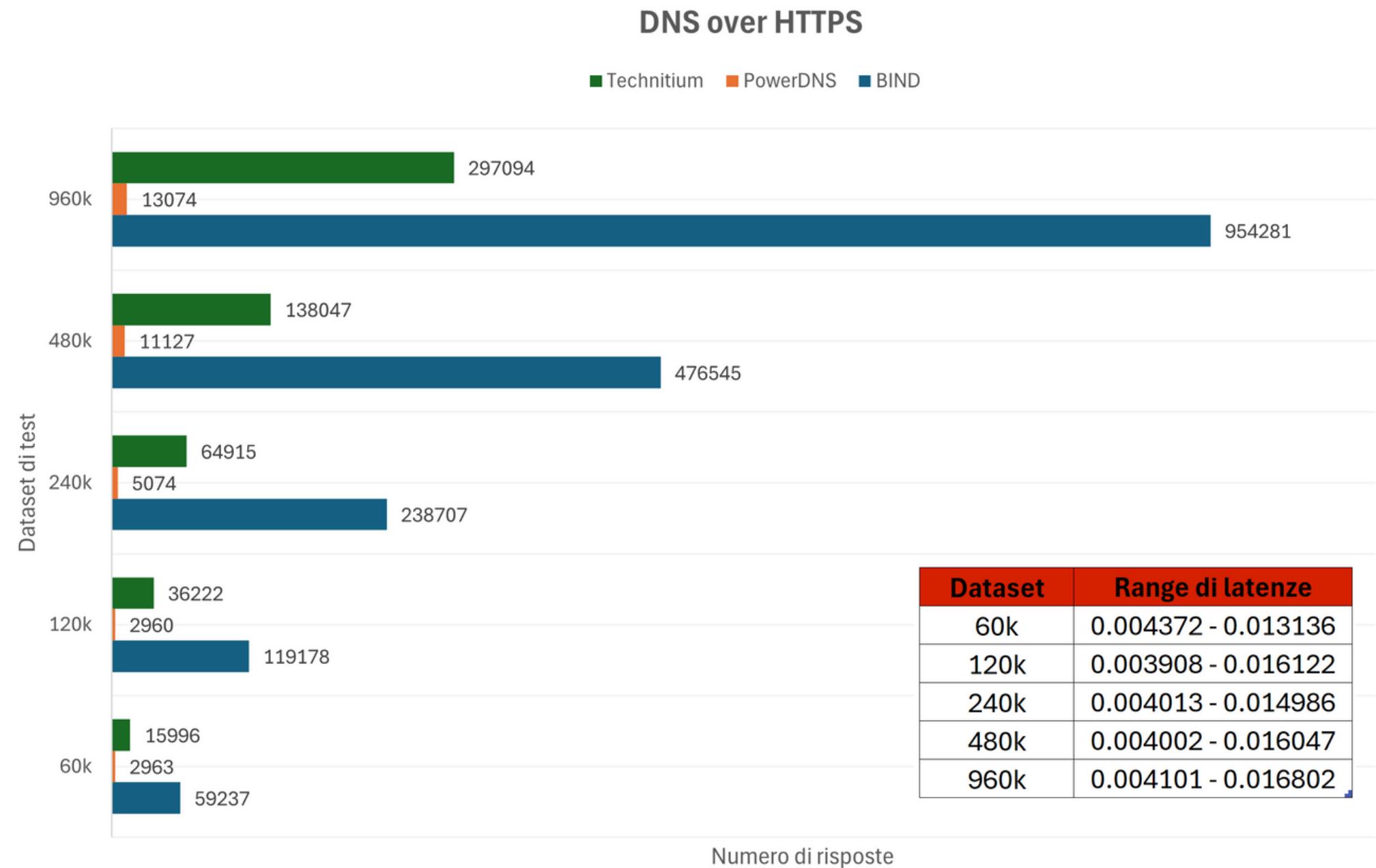


GRAFICO DELLE LATENZE

BIND si è dimostrato il server più efficiente, risolvendo il 95% delle richieste in un intervallo di latenze inferiore rispetto a PowerDNS e Technitium.

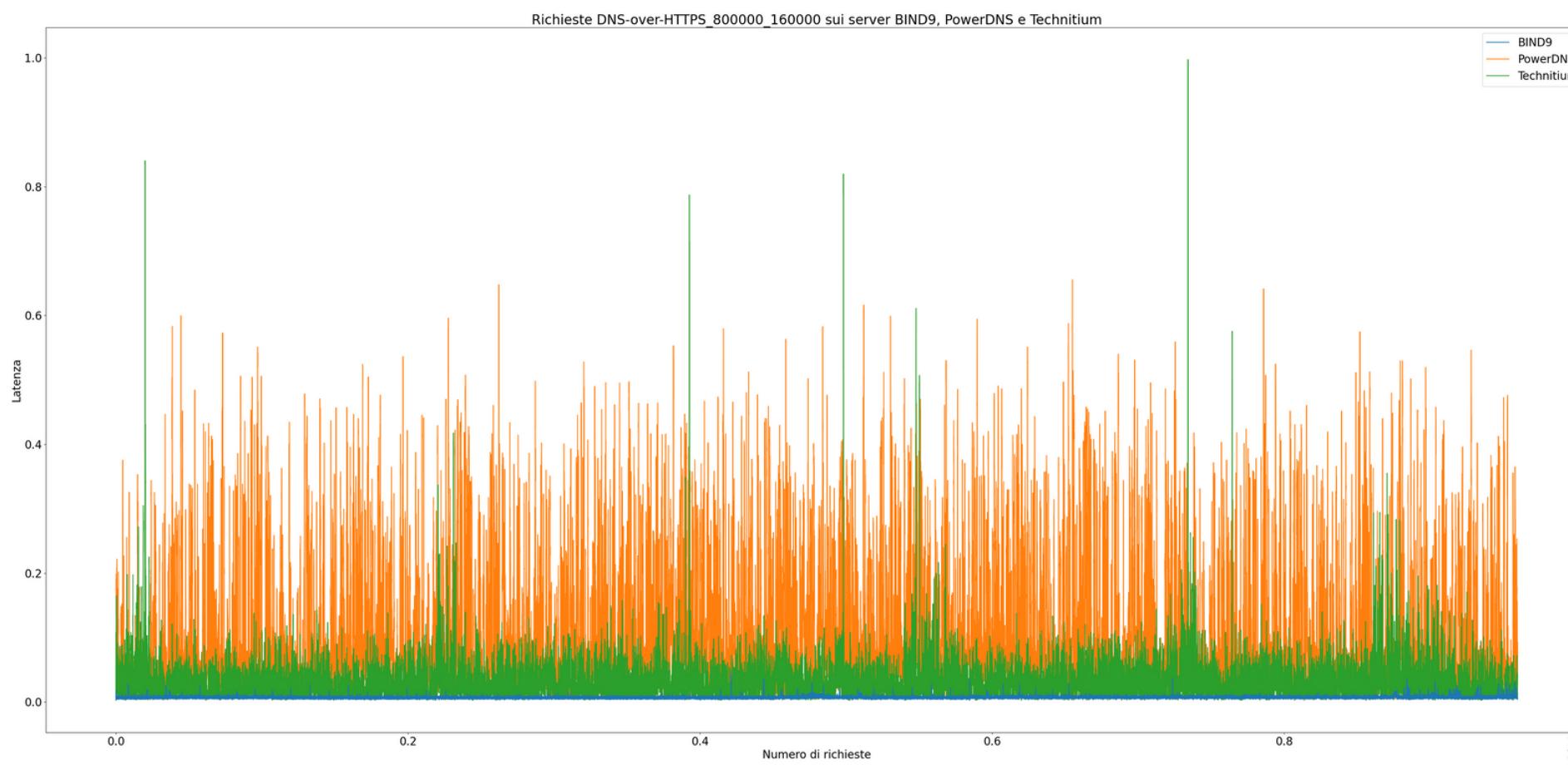
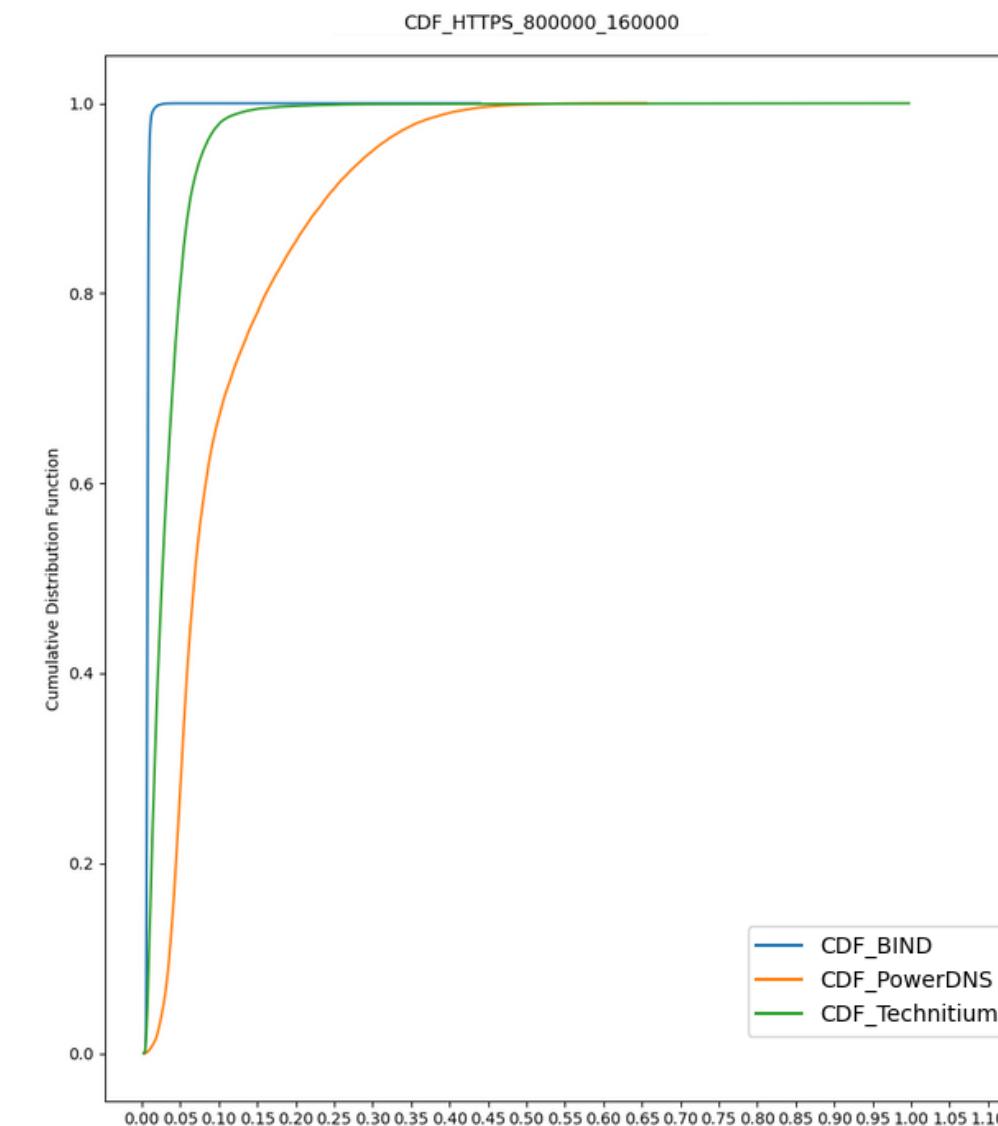


GRAFICO DELLE CDF

BIND converge molto rapidamente a 1, Technitium converge in maniera simile alla curva di BIND e PowerDNS converge molto lentamente a 1.



Benchmarking

In questa seconda sezione sono riportati in dettaglio i dati ottenuti dal benchmarking di **ciascun protocollo eseguito sullo stesso server**.

NB: Tra ogni sessione di benchmarking è stato eseguito uno spegnimento del server seguito dal riavvio della macchina virtuale, al fine di eliminare eventuali residui di buffer, cache e file temporanei, garantendo così una valutazione più accurata delle prestazioni.



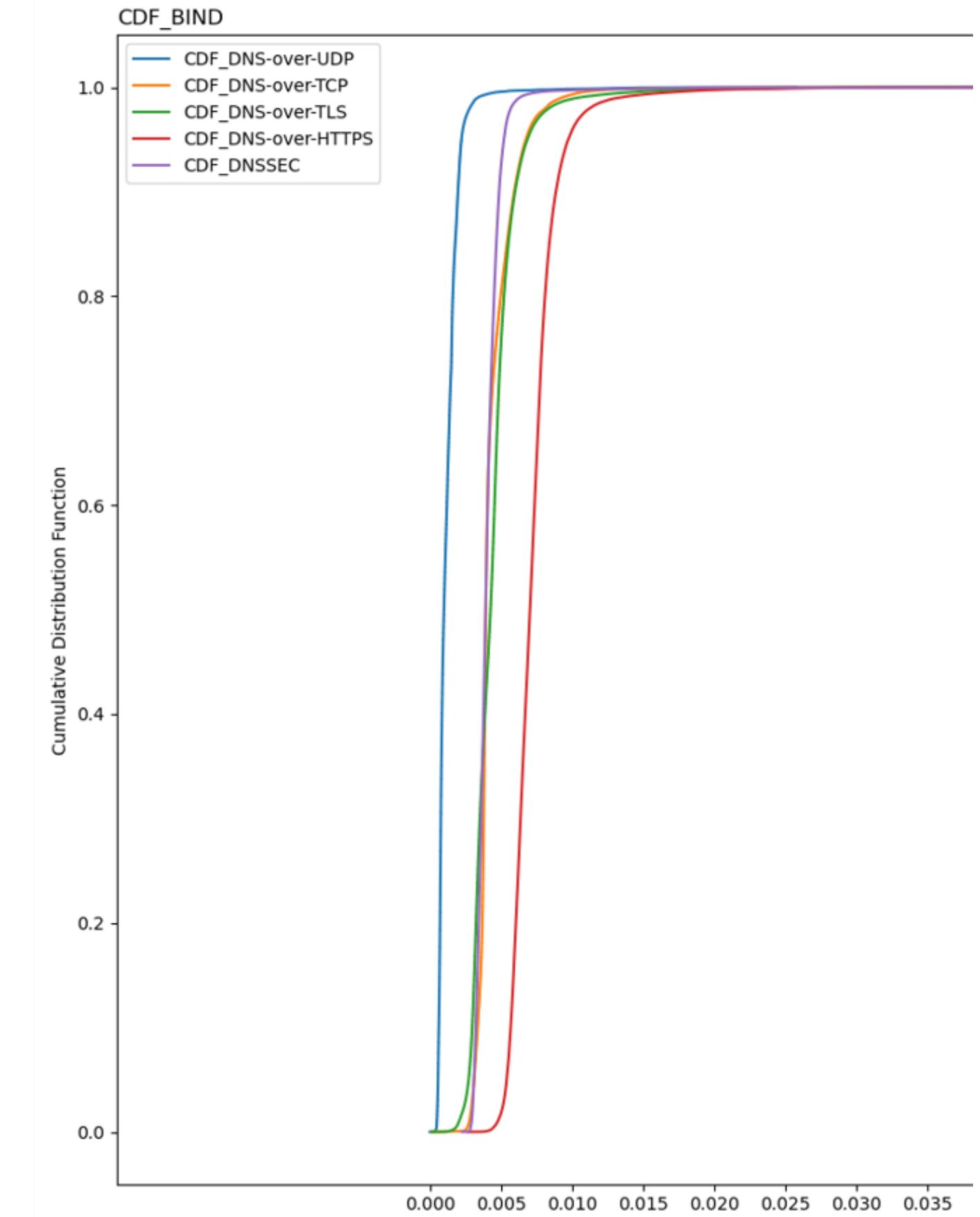
BIND

LATENZE TRA I PROTOCOLLI

- Le latenze di **DNS-over-TCP** sono superiori di circa 0.004 secondi rispetto alle latenze di **DNS-over-UDP**
- Stessa differenza di latenze si ha tra DNS-over-UDP e **DNSSEC**, probabilmente dovuto ai protocolli crittografici
- **DNS-over-HTTPS** presenta delle latenze superiori del 45% circa rispetto **DNS-over-TLS**, dovuto al fatto che HTTPS utilizza TLS e quindi HTTPS aggiunge overhead protocollare a TLS

LATENZA MEDIA E RECORDS

La latenza media è correlata al numero di records. Dai risultati ottenuti si evince che l'aumento del numero di records comporta un incremento molto lento della latenza media, anche con un protocollo ad alto overhead come HTTPS.



PowerDNS

SICUREZZA

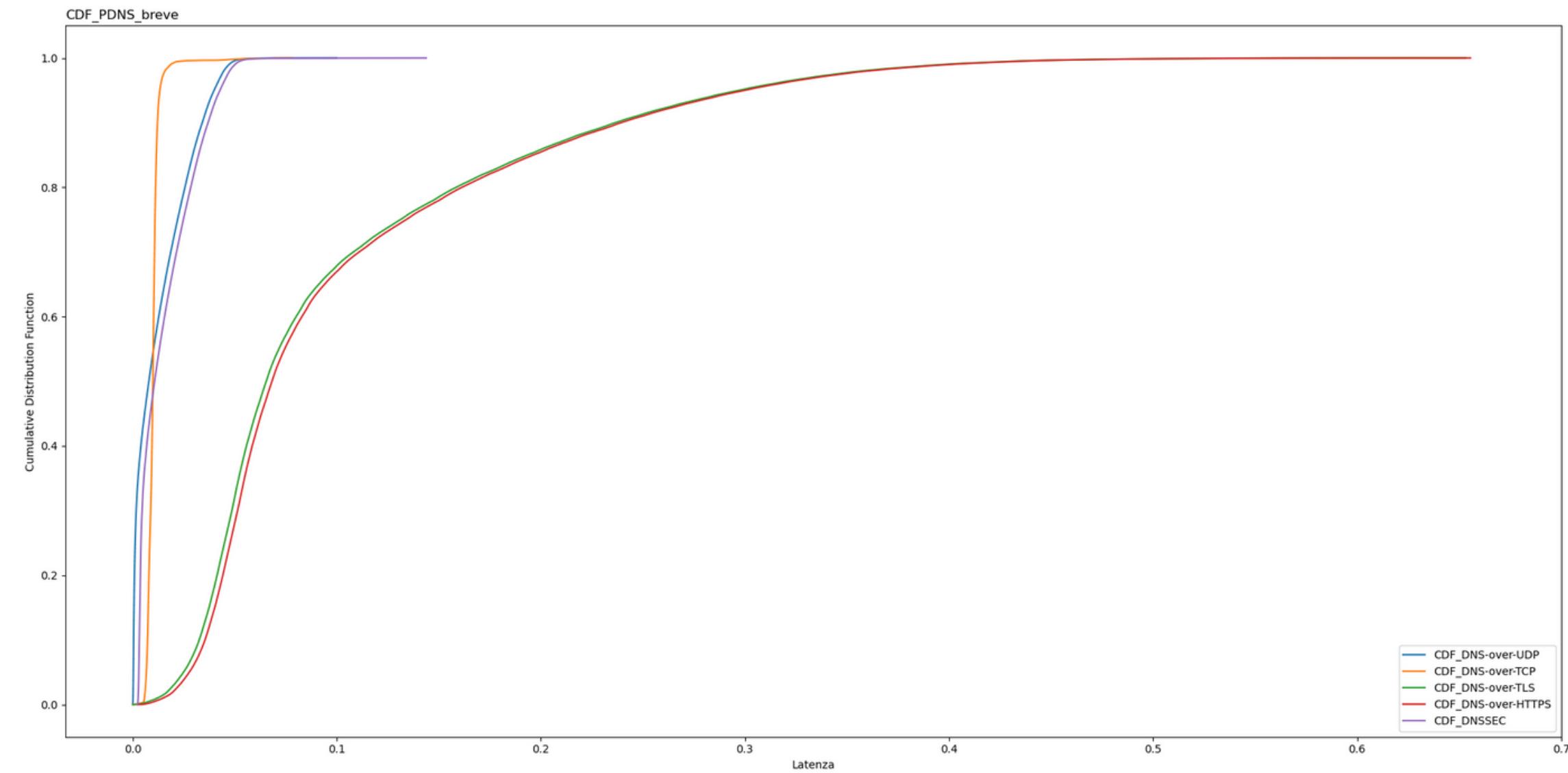
Si nota che i due protocolli DNS sicuri, rispetto agli altri, hanno una media e una deviazione standard ben maggiore e questo risultato viene ben rappresentato dall'andamento delle CDF.

LATENZA MEDIA E RECORDS

Anche in questo caso l'aumento del numero di records nel dataset è correlato con la latenza media.

RISULTATO INATTESO

Analizzando i dati del benchmarking dei protocolli DNS risulta che DNS-over-TCP ha una latenza media inferiore di DNS-over-UDP, in particolare con i dataset 120k, 240k e 480k la latenza media di DNS-over-TCP è inferiore di un ordine di grandezza rispetto DNS-over-UDP sugli stessi dataset.



Technitium

DNS-OVER-TCP

Si nota che DNS-over-TCP presenta una latenza media inferiore a DNS-over-UDP, in particolare con i dataset più grandi (480k e 960k). Inoltre all'aumentare delle richieste diminuisce la latenza media.

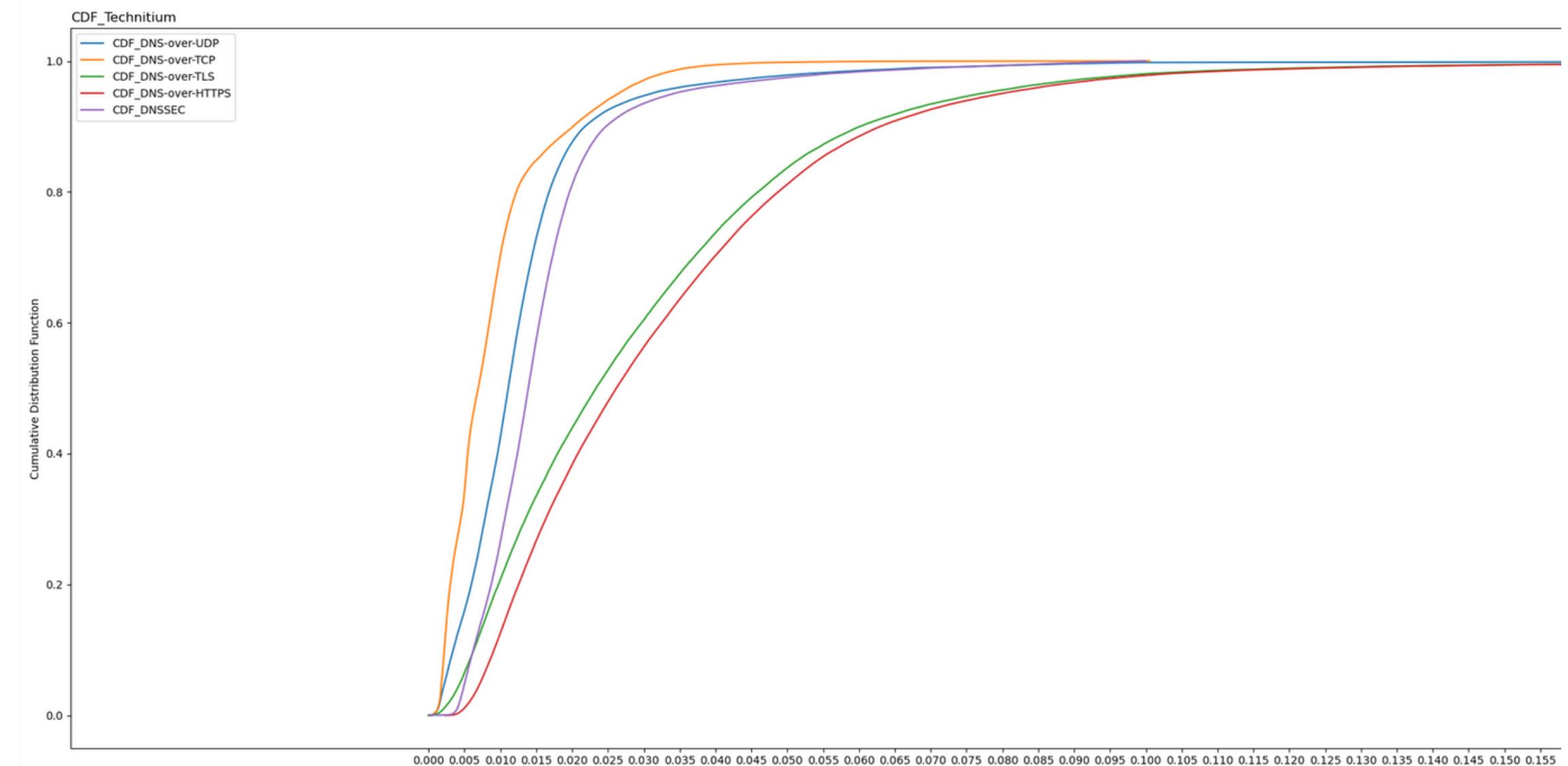
DNSSEC

Un risultato molto simile è dato da DNSSEC:

- Nei primi tre dataset la latenza media rispetto a UDP è inferiore di **0.0050** secondi
- Nei dataset da 480k e 960k DNSSEC ha latenze inferiori di **0.017** secondi

LATENZA MEDIA E RECORDS

Anche con Technitium si ha una forte correlazione tra la taglia del dataset e la latenza media tuttavia la latenza non subisce forti aumenti.



Sviluppi futuri

NUMERO DI CLIENT

Si potrebbero utilizzare diverse macchine client e macchine server con file di zona di taglie reali.

DNS-OVER-QUIC

Questo nuovo protocollo di trasporto include le funzionalità di TCP aggiungendo la sicurezza di TLS, con una latenza inferiore a TCP. In questo lavoro non è stato preso in considerazione perchè non è stato ancora implementato in BIND e Technitium.



Conclusioni

BIND è il server che presenta le performance migliori in tutti i casi, poi c'è PowerDNS e infine Technitium. Anche se le prestazioni di questi ultimi due server sono nettamente inferiori rispetto a BIND, bisogna spendere qualche parola in loro difesa

BIND

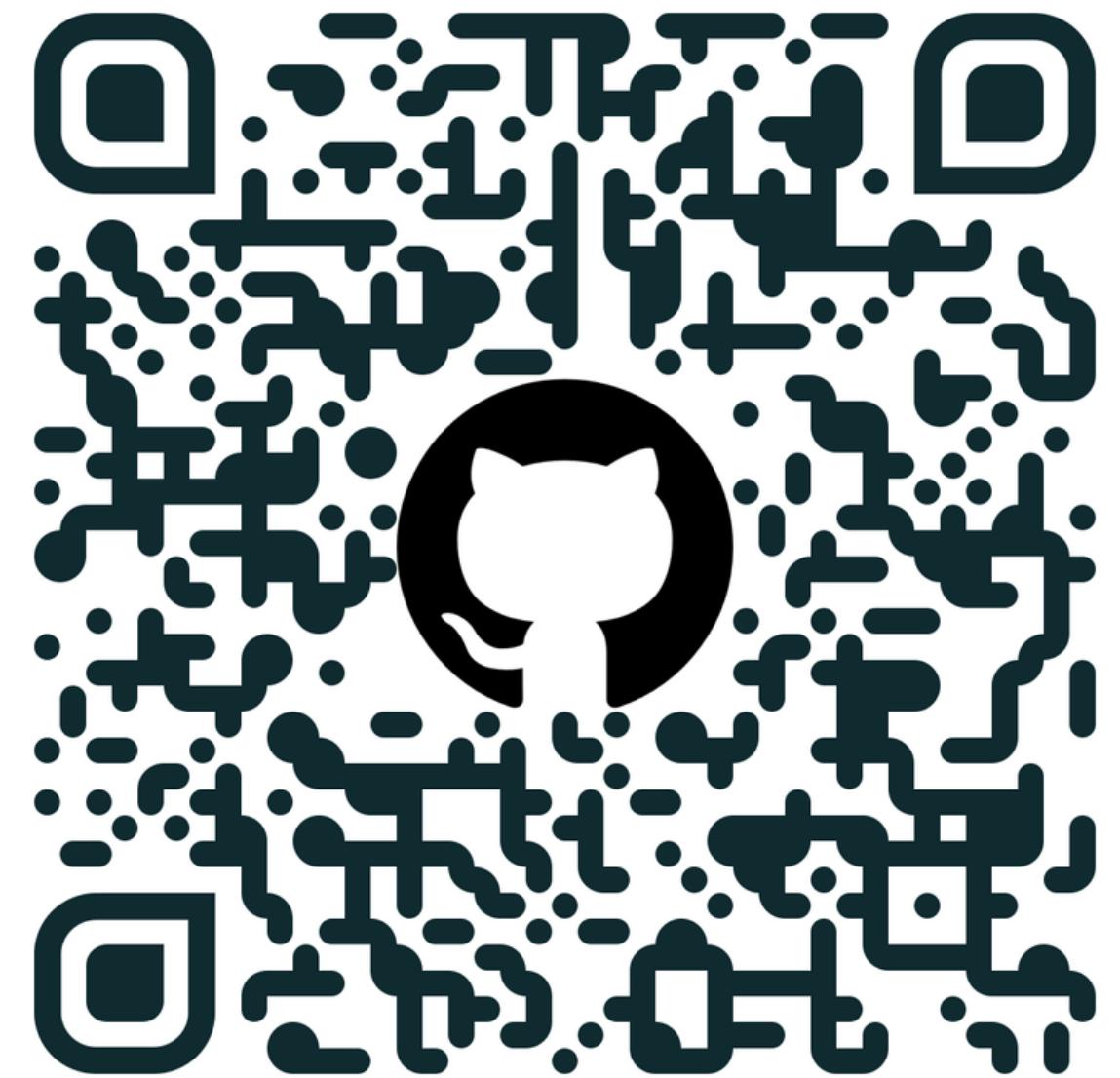
- Molti problemi durante la configurazione
- Non offre un'interfaccia grafica
- La documentazione risulta enorme e difficile da studiare per chi è alle prime armi con i sistemi DNS
- Il materiale online per la configurazione di DNSSEC,
- DNS-over-TLS e DNS-over-HTTPS risulta essere superficiale o addirittura errato

TECHNITIUM

- Installazione molto semplice
- Offre un interfaccia grafica web molto user friendly e utile
- Documentazione chiara con tutorial molto esplicativi

POWERDNS

- Buona documentazione
- Risulta complicato configurare i vari protocolli
- Per i protocolli DNS sicuri bisogna utilizzare l'estensione dnsdist



Scan per la repository completa
con tutti i risultati ottenuti

Thank you
for your
attention!