allot

When the Internet Went Dark: How Allot Brings Observability Light Back to Encrypted Traffic

January 2026

Executive summary - for non-technical leadership

The Shift to Encrypted Internet

Until a decade ago, most Internet traffic was sent in plain view. Anyone with physical access could see what users were doing online. But over the past decade, that changed dramatically. Today, about 90–95% of all Internet traffic is encrypted.

Two current trends that are driving the next phase in Internet encryption:

1. Stronger encryption — new algorithms designed to withstand even quantum computers that may appear.
2. More complete encryption — protecting parts of online communication that currently remain exposed, such as the security configuration data exchanged when you connect to a website.

For Communication Service Providers (Telcos), this transformation presents both opportunity and challenge. Encryption improves user privacy, but it also limits the visibility providers need to manage traffic, ensure quality of service, and protect users from cyber threats. Allot is investing in and developing solutions to provide such solutions and works closely with Telcos to bridge this gap — keeping networks efficient, secure, and intelligent even as encryption becomes stronger and more complete.

Post-Quantum Encryption: Preparing for the Future

Today's encryption methods, such as RSA and ECC, are safe against current computers. But quantum computing could change that. A powerful enough quantum computer might one day break conventional key exchange in minutes. Moreover, harvest-now-decrypt-later attacks would allow storing today's emails, IM chats, and banking transactions and reading them in the future when quantum computers become a reality.

That's why the world is shifting toward Post-Quantum Cryptography (PQC) algorithms designed to resist even quantum attacks. In 2022–2024, the U.S. standards body NIST approved several PQC algorithms for encrypting data and digital signatures. Modern web browsers like Chrome have already deployed hybrid algorithms that combine traditional and quantum-safe encryption. This ensures security today while preparing for tomorrow.

However, PQC introduces a new side effect: larger security set-up messages. When your browser connects to a website, it begins with a “Client Hello” message. With PQC, that message becomes too large for a single network packet, often spanning two or more packets. Allot refers to this as “Long TLS.”

Long TLS increases the processing effort needed to identify and classify traffic — but Allot anticipated this. Our systems now automatically reassemble and process multi-packet handshakes, so Telcos retain complete traffic visibility and control.

Encrypted Client Hello (ECH): Hiding the Last Visible Clues

Even with strong encryption, certain parts of Internet traffic are still visible — especially the Server Name Indication (SNI) in the Client Hello message, which reveals which website a user is visiting. Security tools and service providers often rely on this data for traffic management and cybersecurity.

The new Encrypted Client Hello (ECH) TLS extension closes this gap by encrypting the entire security setup, hiding the SNI and other fields. ECH is still in its initial phase. While browsers primarily support it, the only hosting service currently offering it is Cloudflare, and full adoption is expected to take years. Only about 1% of traffic uses ECH today, but this is expected to grow significantly once the RFC is officially released.

This is a significant milestone for user privacy — but it also makes application classification and threat prevention more complex. Once again, Allot is ready for this shift.

How Allot Keeps Visibility in an Encrypted World

As encryption proliferates, Allot has developed a multi-layered strategy to ensure service providers can continue to understand and manage their traffic effectively.

3. Handling Post-Quantum Encryption:
    - Allot’s Deep Network Intelligence has been upgraded to handle multi-packet handshake messages correctly.
    - For both TCP and QUIC traffic, the system reconstructs and analyzes all relevant handshake data — maintaining accuracy even when encryption becomes stronger.

4. Managing Encrypted Client Hello (ECH):
    - Regulatory compliance tools: In markets where regulators require, encourage, or allow it, Telcos can block ECH using a variety of methods provided by Allot.
    - IP-based identification: Over half of all connections can be uniquely identified by server IP addresses. Allot correlates these with known services to obtain accurate classification.
    - Real-Time AI inference Engine: For cases where server IP addresses are not unique to a single application, Allot's **TraffiCognition**, a new real-time AI/ML inference engine within DART, analyzes traffic patterns to identify applications with over 95% accuracy.
    - Behavioral analytics: Allot can distinguish between different traffic types — video, voice, file transfer, etc. - even inside encrypted tunnels like VPNs.

Together, these layers allow Allot to see what matters without breaking encryption, keeping networks efficient and secure.

What This Means for Telcos

Encryption is essential for privacy, but it shouldn't come at the cost of performance, visibility, or safety. Allot's futureproof solutions ensure that Telcos can continue to:

- Understand traffic patterns across their networks
- Optimize performance and QoE for subscribers
- Enforce regulatory requirements
- Detect and mitigate threats, even inside encrypted flows

The Internet is entering a new era of encryption — and Allot is already there, helping service providers stay ahead with Deep Network Intelligence that adapts as fast as the technology itself.

Part I – Current Trends in Internet Traffic Encryption

A Brief History

It is widely accepted that the birth of Internet traffic encryption took place well before most of the public was even aware that the Internet even existed. The second half of the 1970's saw quite a few dramatic discoveries and inventions in the field of cryptography (Diffie-Hellman key exchange method, RSA public key cryptography) that laid the foundation for public key encryption. But it took several decades for network encryption to mature. Even as late as 2015, the majority of Internet traffic was still not encrypted. Still, the past few years have witnessed an escalation in the deployment pace of encryption throughout the web. Today approximately 90-95% of the Internet (depending on the geography) is at least somewhat encrypted and we are now standing on the verge of a new age in the evolution of the Internet – the age of network traffic encryption. This age is being ushered in by two main development factors: first – stronger encryption algorithms, notably including ones designed to withstand cryptographically relevant quantum computers; and second – encrypting whatever parts of the Internet traffic that are still inherently carried in the clear.

In parallel, Communication Services Providers are feeling an increasing need for data traffic management, visibility and security. They need robust solutions to be able to absorb data volume peaks while maintaining high quality of experience for their subscribers; they are required to apply regulatory and governmental enforcement rules to block some websites or services that potentially pose a threat to national security or specific laws; and they are expected to protect their subscribers against cyber-threats and attacks. Allot is committed to providing such solutions to Communication Service Providers and therefore closely follows the evolution of Internet technology.

This document highlights how Allot is addressing the challenges of the age of network traffic encryption to continue serving Communication Service Providers with efficient network management solutions.

Post Quantum Cryptography – (Truly) Unbreakable Encryption

Conventional public-key cryptosystems, such as RSA or ECC, are practically unbreakable using conventional digital computers, but in 1994, Peter Shor discovered an algorithm that breaks them, assuming the existence of a suitably capable quantum computer. While current quantum computers are still woefully inadequate for such an undertaking, the harvest-now decrypt-later (HNDL) strategy would enable an eavesdropper to record encrypted traffic today and decipher it at some later date when a suitably powerful quantum computer becomes available. Since the discovery of Shor's algorithm, several post-quantum cryptography (PQC, AKA quantum-safe) public-key encryption algorithms have been developed. These algorithms are not known to be broken by Shor's algorithm, or any other known quantum algorithm, and are thus deemed preferable to conventional public-key algorithms.

In July 2022 US National Institute of Standards and Technology (NIST) selected[1] for standardization four PQC algorithms: CRYSTALS-Kyber for general encryption including key exchange, and CRYSTALS-Dilithium, FALCON, and SPHINCS for digital signatures. In 2024 it released three of these as FIPS standards: FIPS 203 ML-KEM (Kyber for key exchange), FIPS 204 ML-DSA (Dilithium for signature), and FIPS 205 SLH-DSA (SPHINCS+ for signatures). In March, NIST selected an additional key exchange algorithm – Hamming Quasi-Cyclic (HQC) – based on a completely different mathematical framework from Kyber. Thus, there are now preferred key exchange and digital signature algorithms (ML-KEM and ML-DSA) with each having a backup one in case they are compromised. Various standardization organizations, including the Internet Engineering Task Force (IETF), have been adopting the NIST choices for use in secure telecommunications protocols, such as TLS.

TLS (Transport Layer Security[2]) is the cryptographic protocol currently used for securing many Internet applications, including web browsing, email, and some types of VoIP. When TLS is utilized to protect web traffic, which uses the HTTP protocol, the result is called HTTPS. HTTPS establishes a secure channel by first exchanging secret key information in a handshake between the web client and the server and then encrypting all subsequent messages using cryptography that is bootstrapped from this key information. The handshake commences with the client sending a "Client Hello" (CH) message to the server, followed by the server replying with a "Server Hello". The Client and Server Hello messages are unencrypted (unless Encrypted Client Hello, or ECH, is employed, as will be discussed later) but subsequent messages are fully encrypted.

The Client Hello message contains a plethora of information elements. For example, the CH message is used to inform the server of all the lists of symmetric encryption, public-key encryption, and digital signature algorithms it supports (in order of descending preference), from which the server will select the algorithms to be used. Before PQC, a TLS version 1.3 Client Hello would probably offer at least AES_256_GCM_SHA384 and CHACHA20-Poly1305 for the symmetric cipher, X25519 and P-256 elliptical curve public key alternatives and some version of RSA or ECDSA for the signature algorithm. Incidentally, the X25519 cryptosystem gets its unusual name from the prime number 2^255-19 upon which it is based.

The CH message usually contains two extensions that are of interest. One is the SNI (Server Name Indication), which contains the domain name (e.g. www.example.com) of the desired server. This is needed when multiple (virtual) servers are hosted behind a single IP address. Without the SNI the CH would arrive at a physical server responding to the IP address, but that physical server would not know which identity certificate to return, nor to which service to forward the client's request. In practice, SNI is also exploited for entirely different reasons; for instance, many DPI signatures rely on the SNI in the unencrypted CH message, in combination with information from other CH fields, to identify a service despite the rest of the interchange being encrypted.

Another TLS extension is the list of key shares. This list contains the cryptographic parameters that are needed for the public-key algorithms the client supports, one entry for each public-key alternative. For example, for the X25519 ECDH cryptosystem the key share consists of the client's 32-byte public key, without which the server would be unable to encrypt its Server Hello message. This extension is used to speed up the handshake; without it, the client would not be able to send its public key for the selected algorithm until the server informs it of the public-key algorithm it selected from the list of alternatives, necessitating delaying session establishment by an additional round-trip time.

Returning to PQ cryptosystems, the leading candidate has the somewhat awkward name X25519MLKEM768[3] (which replaced an earlier version with the only slightly more pronounceable moniker X25519**Kyber**768). This is a hybrid key exchange scheme[4], employing both the NIST post quantum standard ML-KEM (ML-KEM is available in 512, 768 and 1024 flavors and this proposal employs the intermediate-strength variant) and the conventional X25519 ECDHE scheme. The motivation for such hybrid schemes is that the PQ cryptosystems are still new and untested, and attacks on them may yet be discovered. By using MLKEM768 alongside the tried-and-true X25519, one maintains at least the strength of X25519 against conventional attacks and, moreover, achieves state-of-the-art post-quantum safety measures.

Adoption of PQC for hybrid key exchange has been rapid. Chrome and other major browsers support X25519MLKEM768, and observations of live networks demonstrate that about 95% of clients now support it (followed by about 5% supporting the obsolete X25519Kyber768 variant, but only under 1% supporting nonhybrid MLKEM). Active probing reveals that many services already accept X25519MLKEM768 offers, including Google, YouTube, Gmail, ChatGPT, Claude, Facebook, Instagram, X (Twitter), LinkedIn, and services hosted on AWS, Cloudflare, Akamai, and Fastly servers.

DSA	Security Level	Public Key Size	Signature Size	Remarks	
ECDSA P-256	128-bit	~65 B (uncompressed)	~72 B (DER-encoded)	Widely used in TLS certificates	Basic security
Ed25519	128-bit	32 B	64 B	EdDSA using Curve25519	
ML-DSA-44	128-bit	1,312 B	2,420 B	Dilithium "lightweight"	
SLH-DSA-128s	128-bit	32 B	7,856 B	128-bit small SPHINCS+	
SLH-DSA-128f	128-bit	32 B	17,088 B	128-bit fast SPHINCS+	
ECDSA P-384	192-bit	~97 B	~104 B	Higher assurance certificates	Medium security
ML-DSA-65	192-bit	1,952 B	3,309 B	Medium security Dilithium	
SLH-DSA-192s	192-bit	48 B	16,224 B	192-bit small SPHINCS+	
SLH-DSA-192f	192-bit	48 B	35,664 B	192-bit fast SPHINCS+	
ECDSA P-521	256-bit	~133 B	~141 B	Largest NIST standard curve	High security
Ed448	256-bit	57 B	114 B	EdDSA using Curve448	
ML-DSA-87	256-bit	2,592 B	4,627 B	Strongest Dilithium	
SLH-DSA-256s	256-bit	64 B	29,792 B	256-bit small SPHINCS+	
SLH-DSA-256f	256-bit	64 B	49,856 B	256-bit fast SPHINCS+	

It is worthwhile noting that the initial release of PQC KEMs did not go as smoothly as one might have hoped, with multiple reports regarding apps, servers and middleboxes not being ready for this change with various implications[5,6,7,8]. This was due to subtle changes to the TLS handshake. For conventional X25519 public key encryption the key share data occupies 32 bytes, and the entire CH message rarely exceeds 600 bytes, comfortably fitting into a single packet. On the other hand, the key-share for the new proposal is the concatenation of X25519's 32 bytes with the 1,184- byte ML-KEM768 key share, for a total of 1,216 bytes. This means that the CH message no longer fits into a single 1500-byte packet. Two packets generally suffice for now, but it may take three packets or even four in other cases. Allot dubbed this phenomenon of more than a single CH packet, **Long TLS**.

We will discuss the effects of LongTLS on the traffic observed and managed by Allot's platforms and how Allot successfully addressed these effects in the second part of this document. Still, it is worthwhile noting at this stage that unlike the examples from other vendors referenced above, Allot has prepared for this change and has embedded a complete solution for this within its software to continue and provide traffic visibility, management and security to its customers **on time**.

While the harvest-now decrypt-later strategy is irrelevant for digital signatures, the use of ML-DSA in certificates is being standardized as well[9]. But these too are somewhat problematic in that they turn out to be much longer than their conventional counterparts. In the table below we compare the footprint of legacy and the PQC signature schemes:

As can be seen, the new proposals incur considerably more overhead than conventional signature schemes, and for certificates with long chains of trust may be impractical. As an example, a certificate with 3 SLH-DSA-256f signatures would occupy a hundred 1500-byte packets, even were the data message to be a few bytes in length!

Encrypted Client Hello – Eliminating all Traffic Still in the Clear

While the PQC vector of enhancing encryption on the Internet focuses on making the actual encrypted traffic impervious to future decryption, another direction in which network traffic encryption is evolving, is encrypting parts of the traffic that are still unencrypted. We have already mentioned above that the CH message includes many information elements which are used by Allot (and other vendors of internet equipment and software) to identify and classify the traffic associated with each particular CH message. The most important of these is, as mentioned, the SNI, and in 2018, Encrypted Server Name Indication (ESNI) was proposed in order to prevent access to SNI information by devices performing pervasive monitoring. It was deployed as an opt-in by Cloudflare and supported by Mozilla Firefox and was floated in parallel as a draft RFC to the IETF. ESNI aimed to encrypt just the SNI part of the CH and failed to gain much traction. In 2020 the IETF draft was expanded to include the entire CH message and was transformed into the now-almost final draft RFC[10] of Encrypted Client Hello (originally named ECHO, then renamed ECH). Unfortunately, hiding the SNI and other CH fields makes it harder to classify applications and almost impossible for the network to prevent access to malicious websites.

Using ECH requires the client to somehow acquire the server's public ECH key, which is usually accomplished using DNS. A new DNS extension field for HTTPS-RR responses has been defined precisely for this purpose. Of course, DNS A/AAAA messaging may itself reveal the domain name to IP address mapping, and so there is little advantage to employing ECH without encrypted DNS as well.

The ECH draft has passed all approval stages and is currently awaiting publication (but publication as an RFC cannot occur before publication of the draft detailing the use of DNS to distribute ECH public keys that it normatively references). We estimate that the process will be completed in the near future and ECH will become an official IETF standard within the next few months. Once the RFC is released, we expect to begin seeing more implementations in the field.

In this context it is worthwhile mentioning that at the end of 2023, long before the process of ECH standardization was completed, Cloudflare – one of the forces strongly promoting ECH (and before it, ESNI) – tried launching ECH for some websites they host. This trial launch was apparently premature and caused considerable technical problems, necessitating a rollback just a day after launch. After fixes, they deployed ECH on all free web hosting plans with no issues, and it is now available (but not mandatory) for paying customers as well.

All major browsers now support ECH, and if they receive a server key, they will use it. Moreover, most browsers employ GREASE whereby they masquerade as ECH for servers that don't support it. A recent study[11] claimed that 10% of the top million sites support ECH, but that is not what Allot and others are observing. Most Cloudflare sites are now using ECH, and Cloudflare is the single most popular hosting provider (about 20% of the hosting market, and about 4% of all websites), but only accounts for < 1% of all web traffic. Another recent study[12] discovered many ECH-ready sites that are yet actively publicizing their ECH support, most of which belong to Meta (probably still just testing, but ready to go live at any time). So, we estimate that about 75% of connections utilize fake ECH (GREASE), 1% true ECH, but with the possibility of a rapid jump to over 15%.

How quickly will ECH ramp up? As mentioned above, Google's launch of X25519Kyber768 in Chrome did not go entirely smoothly due to internal delays and unexpected implications on various vendors, apps and content providers. Similarly, when HTTPS was first deployed at scale circa 2005, and it took approximately a decade for HTTPS traffic to reach about 30 percent of total web traffic, and another decade for it to reach the current level of 90-95 percent penetration. IPv6 has been around for over 20 years and still accounts for only about half of the Internet. Likewise, we do not expect all Internet traffic to switch to ECH immediately. This will be a lengthy process not only because it will take the market a lot of time to adapt and adopt the new extension but also because of both technical and regulatory reasons. For example, Firefox's attempt to rollout ESNI in the UK during 2019-2020[13] met with fierce resistance from the UK regulator, Ofcom, first leading to delays[14], then public consultation[15] and ultimately canceling the planned rollout altogether. ECH is more advanced, and we believe it will eventually be successfully launched and deployed worldwide, but it is quite possible that objections presented by regulators will slow down the process as well, or even impose a ban in some countries.

Part II – Allot Solutions for the Encryption Challenge

Another Brief History

The past years have seen many challenges posed to Allot's ability to continue and provide its customers with the ability to "see, control and secure" their networks. QUIC obfuscation and chaosification made straightforward extraction of information from CH far more difficult than before; the rise of consumer VPNs and other anonymity applications made service identification and management more challenging than ever; and encrypted DNS services eliminated lead information once extracted from DNS queries and responses. Still, we have managed to overcome these changes by enhancing our identification capabilities with Machine Learning and sophisticated heuristics, and by extracting whatever information remains in the clear to stay ahead of the changing Internet landscape. As detailed in the following pages, this approach also applies to the current challenges in traffic encryption. Allot has already invested significant resources in adapting to these changes and will continue to do so.

Handling PQC Impacts on Internet Traffic

How does Long TLS and the use of a new public-key encryption algorithm affect Allot's DPI, which does not even open the encryption in any case? As mentioned above, many DPI signatures require observing the SNI, which was assumed to be in the first packet. With X25519MLKEM768 (and other PQC key exchange mechanisms), the SNI may now be in any of the packets comprising the CH message, depending on the order and size of the TLS extensions. The search for SNI and other fields of interest to the DPI engine becomes more expensive in terms of CPU. The situation is even slightly more complicated when it comes to QUIC[16] connections. The QUIC CH message is not sent in the clear but is not truly confidential either. Instead, the QUIC CH message is obfuscated and may be chaosified. Obfuscation entails encrypting the message with AES but with a per-version known key. While this does not prevent an eavesdropper or a DPI system from observing the CH information, this observation comes at a computational price. Chaosification refers to deliberately scrambling the continuity and order of the various QUIC frames, so that the deobfuscated content must be pieced back together —once again, not an actual impediment but merely a scare tactic aimed at the faint-hearted eavesdropper.

Traditional QUIC CH messages fit into a single packet (although always a maximal length one), which must be deobfuscated and perhaps dechaosified. A QUIC PQC CH message now occupies multiple packets, each of which must be deobfuscated, and the concatenation of which must be dechaosified before searching for the SNI and other fields of interest.

Allot has addressed the aforementioned PQC challenges by modifying the processing of CH messages, whether in TCP or QUIC. Starting with Allot's Smart Deep Network Intelligence R18.3.50 GA, Allot's DART (Dynamic Application Recognition Technology) extracts and concatenates the contents of all TCP CH packets, creating a single large *message body*. For QUIC, it also deobfuscates all CH packets, concatenates and dechaosifies them, and once again creates a single large message body. This message body is now parsed by the various DPI engines working within the Allot platform, searching for SNI and other fields of interest. This processing method exposes all unencrypted Client Hello information, regardless of the number of packets the CH spans. More importantly, the implementation is agnostic to the number of packets included in the CH message, making the mechanism resistant to the deployment of additional hybrids that would lead (or are already leading) to CH messages extending to three, four, or even five packets.

To sum up: deployment of PQ cryptosystems in general – and X25519MLKEM768 in particular – results in multipacket CH messages, and requires additional resources to locate the relevant parts of the message and prepare them for use by the Allot platform. Allot has prepared for this change and has already implemented a CH message reassembly mechanism that allows all components of the Allot platform to continue functioning as before. PQC is therefore handled by the current Allot solution and traffic management, insights collection, and security solutions remain perfectly intact.

Handling ECH

The solution for ECH involves multiple mechanisms and components. Since ECH usage is still in the low single digits, it is too early to evaluate the contribution of each element to the complete solution. However, at a high level, the following elements have been implemented and released (and are continuing to evolve and develop) to mitigate the expected impact of the launch and proliferation of ECH deployments on Allot's ability to identify and manage traffic correctly:

1. In some geographies where regulators take a stricter approach towards uncoordinated deployment of encryption (as the UK regulator did a few years back), Allot offers customers the capability to block ECH. Blocking may be achieved gracefully by removing the server's public ECH key from unencrypted HTTPS-RR DNS responses. With ECH blocked, clients will establish their TLS connections with unencrypted CH messages, enabling management and securing data traffic just as done today.
2. IP-based identification – for most traffic, server IP addresses will continue to be exposed. Our research and field results have shown that a significant percentage – over 50% – of connections can be uniquely associated with a single application or service based on the server IP address. We obtain the correlation through various sources and integrate this data into our identification and classification engines.
3. Where IP based identification is not unique, we have integrated the Allot **TraffiCognition**, a real-time inference engine, into our DART (Dynamic Application Recognition Technology) engine to allow classification of services. The research results show that for this part of the traffic (under 10%, as mentioned above) very high accuracy (over 95%) can be achieved using AI/ML algorithms.
4. Another component that can allow fine-tuning identification is Behavioral Traffic Analysis. Additional traffic metrics that are not used today can be used in order to differentiate between traffic types and different services, similarly to the way **Allot In-VPN Visibility** identified traffic types within VPN tunnels – breaking OpenVPN and WireGuard-based traffic into various traffic types (VoIP, Video Streaming, File Transfer, etc.), but in a far more enhanced way.

Conclusion

Encryption is essential for privacy, but it shouldn't come at the cost of performance, visibility, or safety. Allot's futureproof solutions ensure that Telcos can continue to:

- Understand traffic patterns across their networks
- Optimize performance and QoE for subscribers
- Enforce regulatory requirements
- Detect and mitigate threats, even inside encrypted flows

The Internet is entering a new era of encryption — and Allot is already there, helping service providers stay ahead with Deep Network Intelligence that adapts as fast as the technology itself.

For further information, contact us at info@allot.com

[1] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[2] https://www.internetsociety.org/deploy360/tls/
[3] https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/
[4] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
[5] https://www.bleepingcomputer.com/news/security/google-chromes-new-post-quantum-cryptography-may-break-tls-connections/#google_vignette
[6] https://tldr.fail/
[7] https://www.reddit.com/r/sysadmin/comments/1carvpd/chrome_124_breaks_tls_handshake/?rdt=62216
[8] https://issues.chromium.org/issues/336007383
[9] https://datatracker.ietf.org/doc/draft-ietf-tls-mldsa/
[10] https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
[11] https://itbrief.com.au/story/report-finds-low-ech-use-but-risks-from-malicious-actors-grow
[12] https://dl.acm.org/doi/pdf/10.1145/3744969.3748401
[13] https://www.ispreview.co.uk/index.php/2019/09/headache-for-uk-isps-as-firefox-adopt-dns-over-https-by-default.html
[14] https://www.theregister.com/2019/09/24/mozilla_backtracks_doh_for_uk_users/
[15] https://www.itpro.com/network-internet/domain-name-system-dns/357820/mozilla-dns-https-public-consultation
[16] https://datatracker.ietf.org/doc/rfc9000/