



It's DNS Jim,
but not as we know it!

Sara Dickinson sara@sinodun.com

What this talk will cover

Overview: Summarise the most recent evolutions in how end-device DNS resolution is being done (~past 5 years)

- **New IETF standards:** Encrypted transports for DNS (TLS & HTTPS)
- **Deployment Status:** Clients and resolver services for encrypted DNS
- **DNS resolution directly from applications:** Browsers
 - **DNS resolution to third party providers:** Implications for operators

My Background

- Co-founder of Sinodun IT - small UK based consultancy
 - Focussed on DNS, DNSSEC and DNS Privacy
 - R&D, Open source dev, Standards dev
- **DNS-over-TLS:** involved in standards dev, implementation and deployment (we contribute to dnsprivacy.org).
- **DNS-over-HTTPS:** Not directly involved, no links to browser vendors

My Background

- Co-founder of Sinodun IT - small UK based consultancy
 - Focussed on DNS, DNSSEC and DNS Privacy
 - R&D, Open source dev, Standards dev
- **DNS-over-TLS:** involved in standards dev, implementation and deployment (we contribute to dnsprivacy.org).
- **DNS-over-HTTPS:** Not directly involved, no links to browser vendors

Goal today is to bring awareness to this audience of fast moving changes: **The good, the bad and the ugly....**

The DNS is showing its age

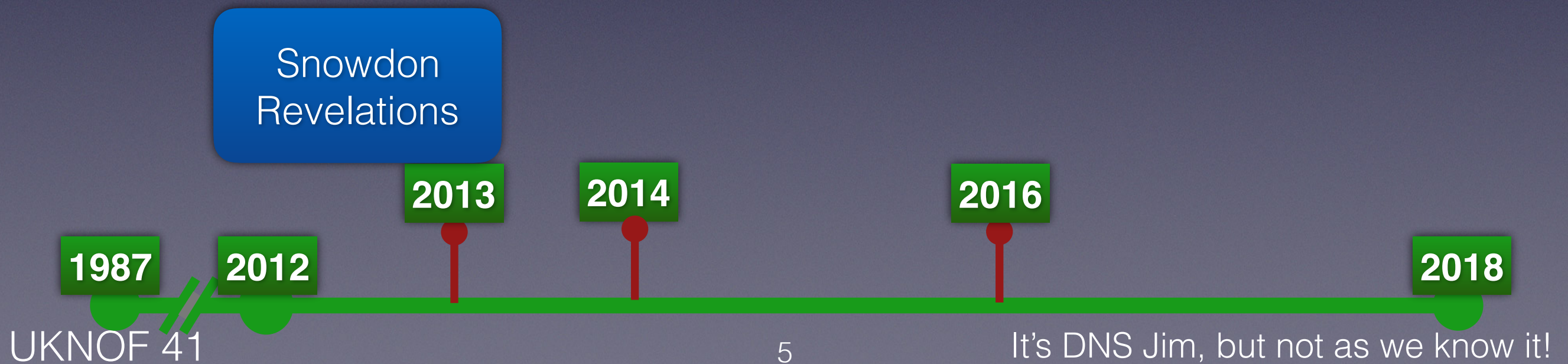
- **Nov 1987** - RFC1034 and RFC1035 published!

No Security or Privacy in the original design!

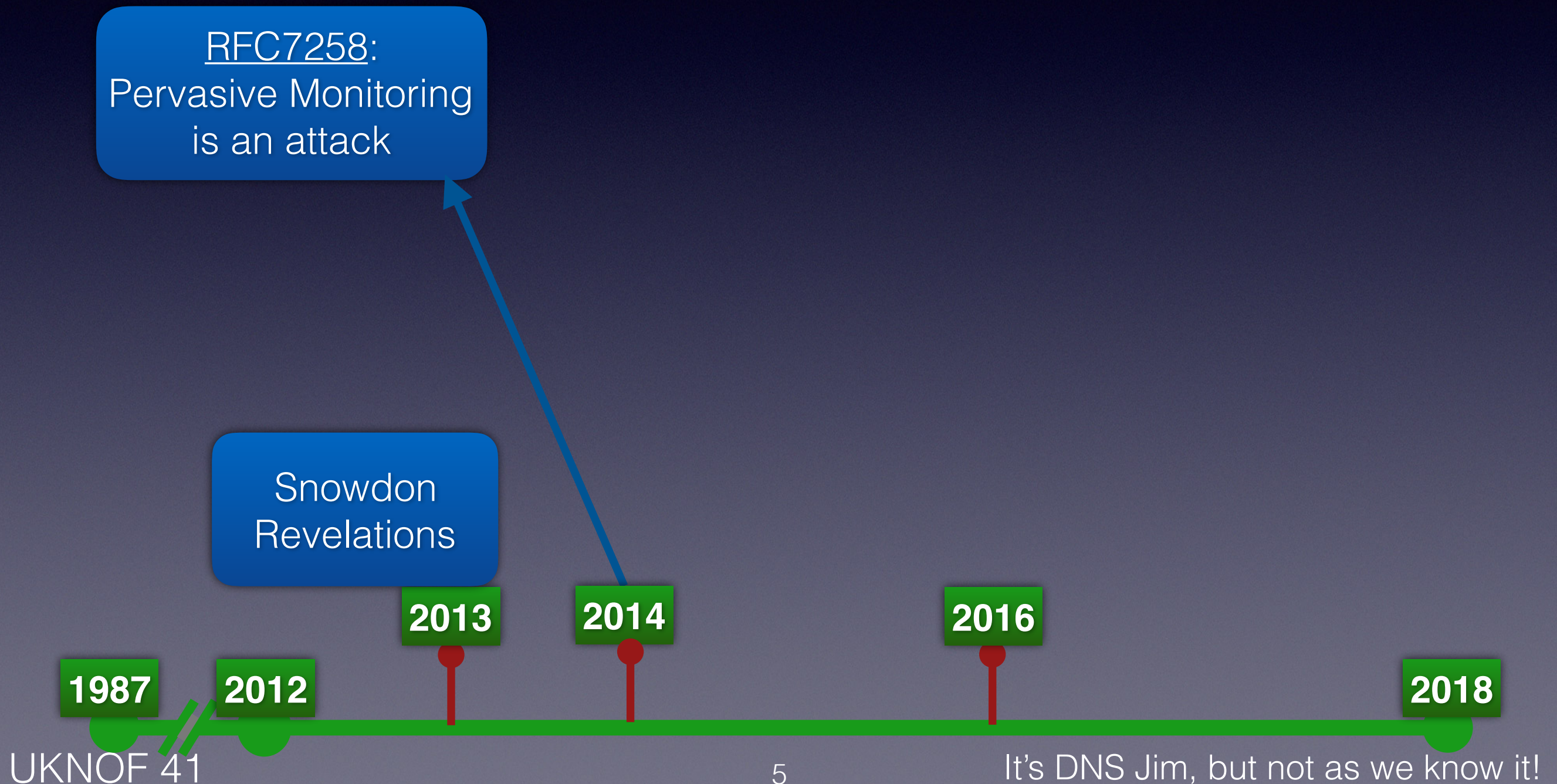
1987

2018

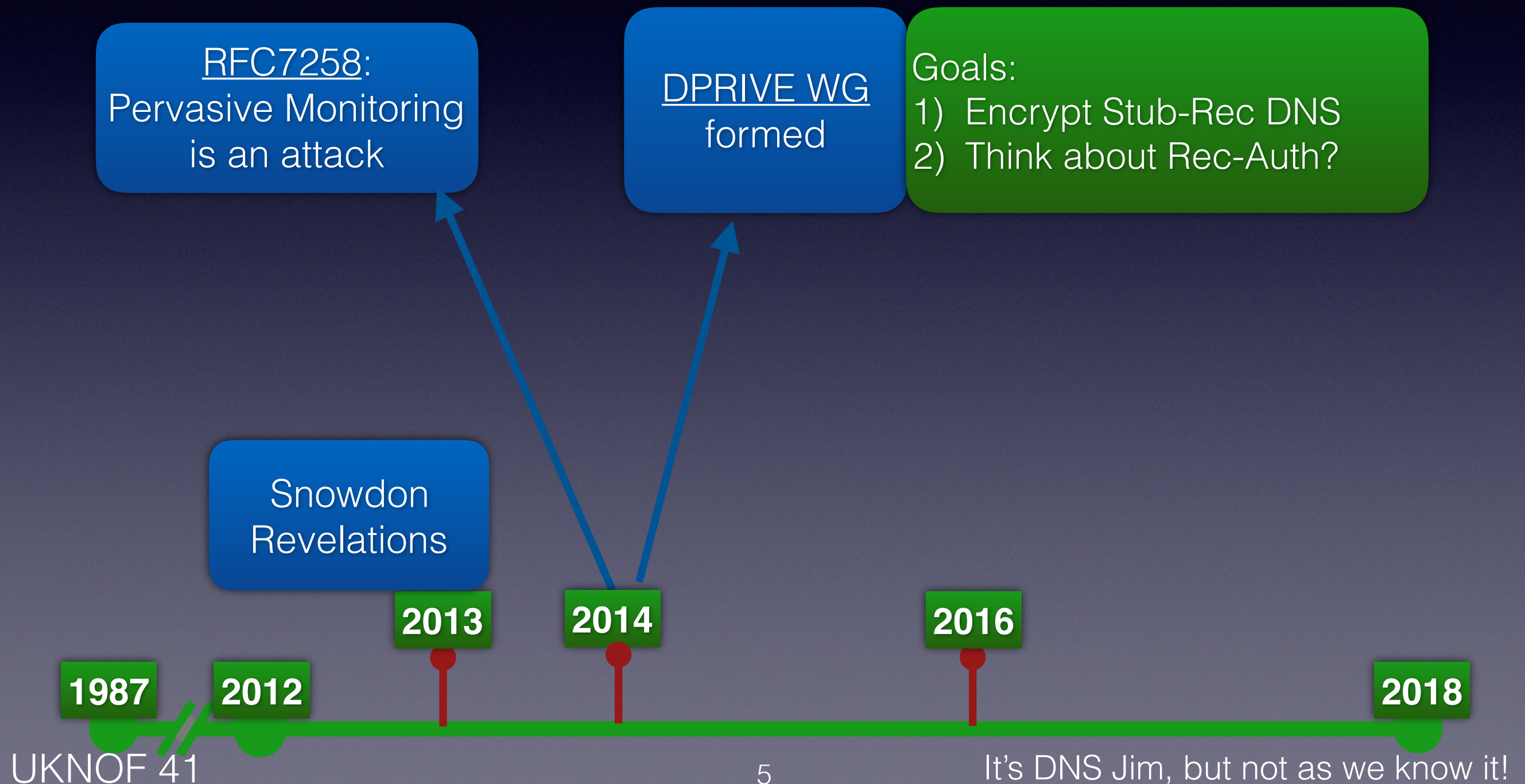
DNS-over-TLS (DoT)



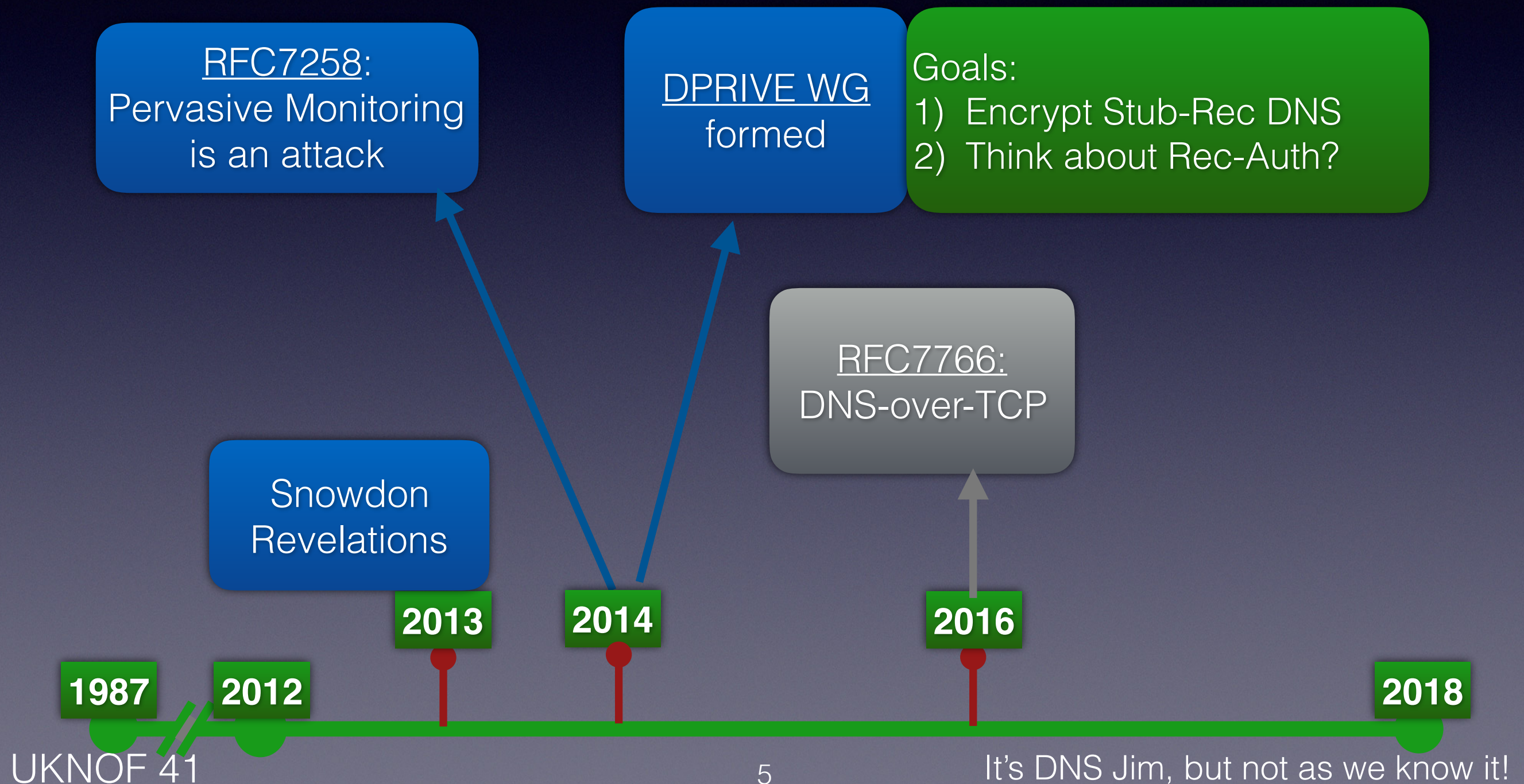
DNS-over-TLS (DoT)



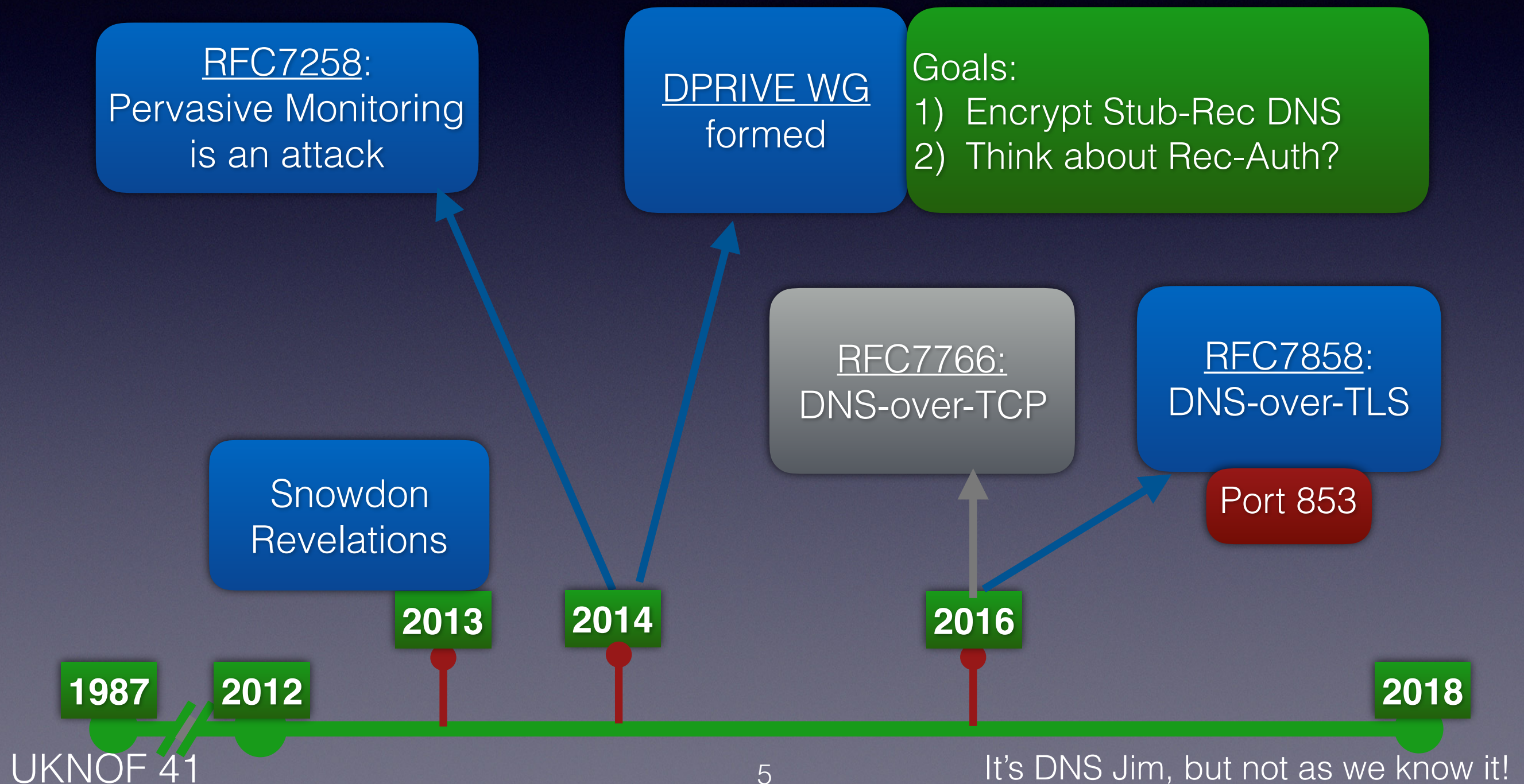
DNS-over-TLS (DoT)



DNS-over-TLS (DoT)



DNS-over-TLS (DoT)



DNS-over-TLS (DoT) Status

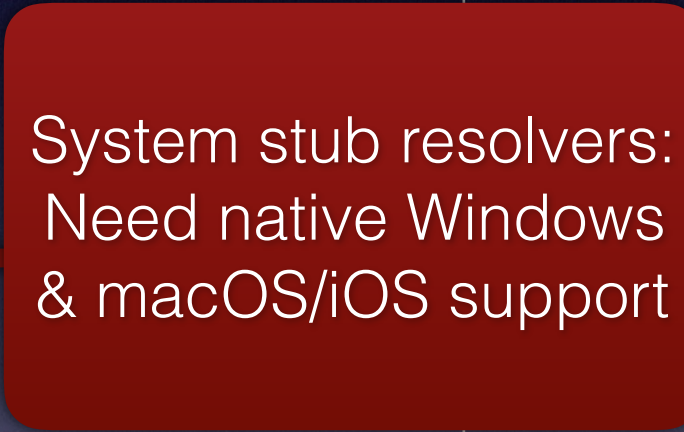
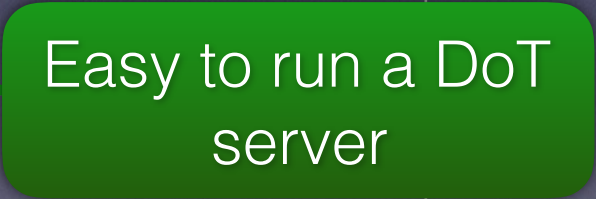
Date	Event
2015 - 2018	Implementations: <u>Clients</u> : Android Pie, systemd, Stubby <u>Servers</u> : Unbound, Knot resolver, dnsmdist, (BIND)
2015 - now	<u>Set of 20 test DoT servers</u>
Nov 2017	Quad9 (9.9.9.9) offer DoT
Mar 2018	Cloudflare launch 1.1.1.1 with DoT

DNS-over-TLS (DoT) Status

Date	Event
2015 - 2018	Implementations: <u>Clients</u> : Android Pie, systemd, Stubby <u>Servers</u> : Unbound, Knot resolver, dnsmdist,
2015 - now	<u>Set of 20 test DoT servers</u>
Nov 2017	Quad9 (9.9.9.9) offer DoT
Mar 2018	Cloudflare launch 1.1.1.1 with DoT

System stub resolvers:
Need native Windows
& macOS/iOS support

DNS-over-TLS (DoT) Status

Date	Event
2015 - 2018	Implementations: <u>Clients</u> : Android Pie, systemd, Stubby <u>Servers</u> : Unbound, Knot resolver, dnsmdist, 
2015 - now	<u>Set of 20 test DoT servers</u> 
Nov 2017	Quad9 (9.9.9.9) offer DoT
Mar 2018	Cloudflare launch 1.1.1.1 with DoT

Encrypted DNS: the good... ✓



- Defeats **passive surveillance**
- Server **authentication** if a name is **manually configured** (PKIX or DANE - [RFC8310](#))
 - Prevents redirects, can't intercept DNS queries
 - Increases 'trust' in service (DNSSEC, filtering...)
- **Data integrity of transport** - can't inject spoofed responses

Encrypted DNS: the good... ✓



- Defeats **passive surveillance**
- Server **authentication** if a name is **manually configured** (PKIX or DANE - [RFC8310](#))
 - Prevents redirects, can't intercept DNS queries
 - Increases 'trust' in service (DNSSEC, filtering...)
- **Data integrity of transport** - can't inject spoofed responses

Opportunistic DoT:
just need IP address
(Android Pie default)

Encrypted DNS: the good... ✓



- Defeats **passive surveillance**
- Server **authentication** if a name is **manually configured** (PKIX or DANE - [RFC8310](#))
 - Prevents redirects, can't intercept DNS queries
 - Increases 'trust' in service (DNSSEC, filtering...)
- **Data integrity of transport** - can't inject spoofed responses

Opportunistic DoT:
just need IP address
(Android Pie default)

Strict DoT: need
a name too

Encrypted DNS: the bad & ugly...



- **SNI still leaks** (but not for long! [draft-rescorla-tls-esni](#))
- A dedicated port (853) can be **blocked** (443 fallback)
- **Resolver** still sees all the traffic (who do you 'trust'?)
- If using a resolver NOT on the local network (not available)
 - Breaks Split horizon DNS (fallback possible), leaks internal names. Similar to e.g. using 8.8.8.8 but....

Encrypted DNS: the bad & ugly...



- **SNI still leaks** (but not for long! [draft-rescorla-tls-esni](#))
- A dedicated port (853) can be **blocked** (443 fallback)
- **Resolver** still sees all the traffic (who do you 'trust'?)
- If using a resolver NOT on the local network (not available)
 - Breaks Split horizon DNS (fallback possible), leaks internal names. Similar to e.g. using 8.8.8.8 but....

**Encrypted traffic bypasses local
monitoring & security policies**

Encrypted DNS: the bad & ugly...



- **SNI still leaks** (but not for long! [draft-rescorla-tls-esni](#))
- A dedicated port (853) can be **blocked** (443 fallback)
- **Resolver** still sees all the traffic (who do you 'trust'?)
- If using a resolver NOT on the local network (not available)
 - Breaks Split horizon DNS (fallback possible), leaks internal names. Similar to e.g. using 8.8.8.8 but....

Encrypted traffic bypasses local monitoring & security policies

For DoT, seen as short term or rare...



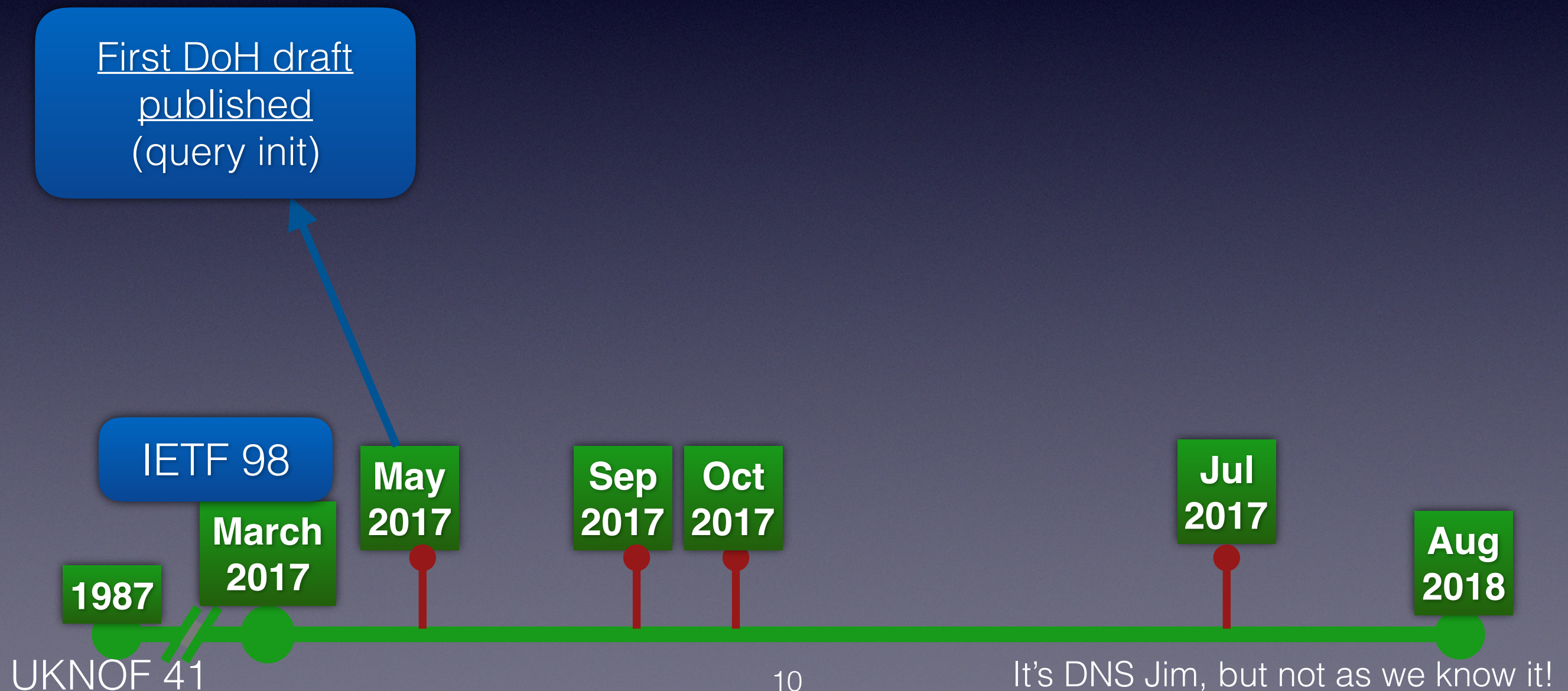


.....to their own chosen cloud resolver service!

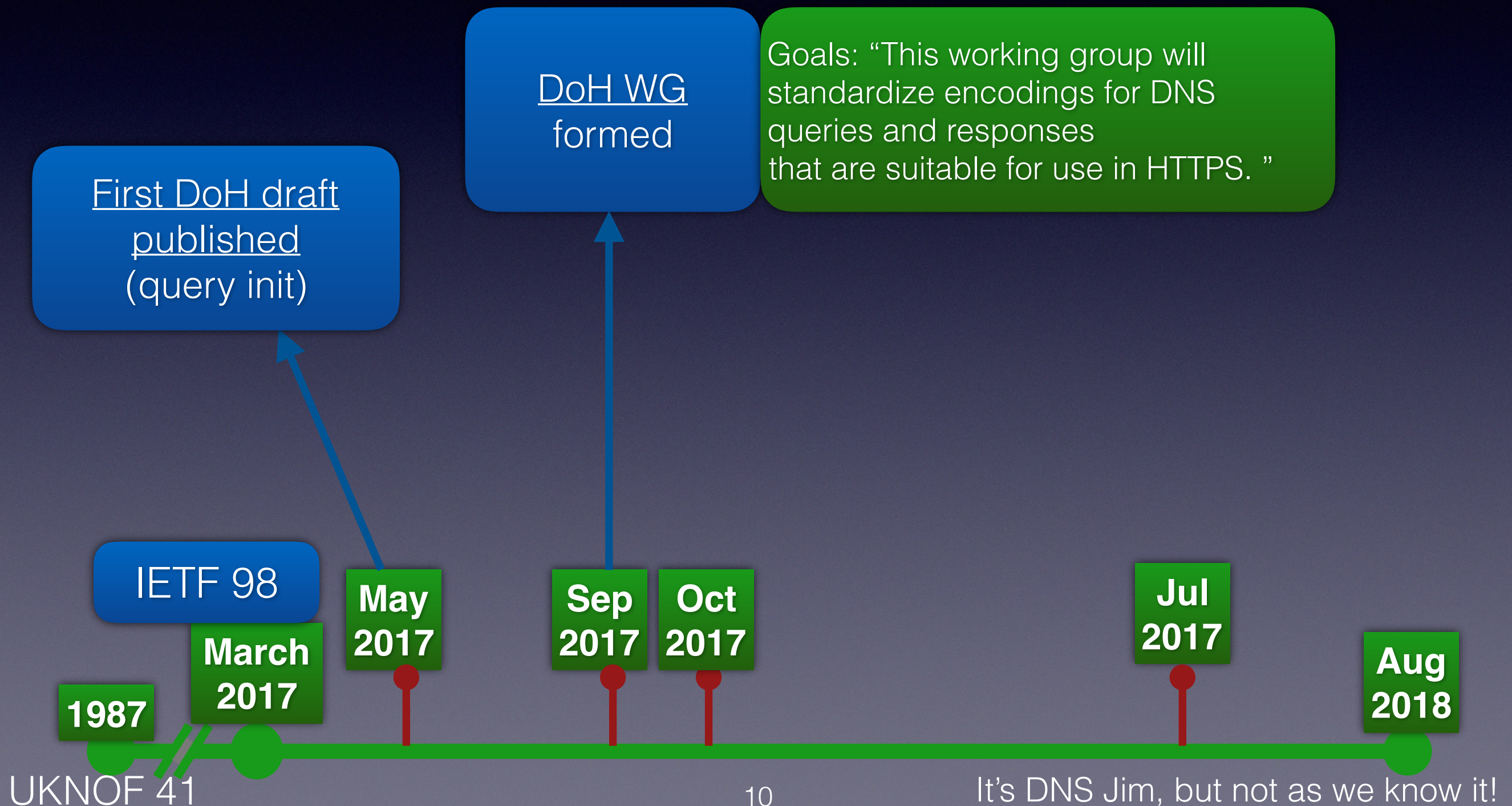
DNS-over-HTTPS (DoH)



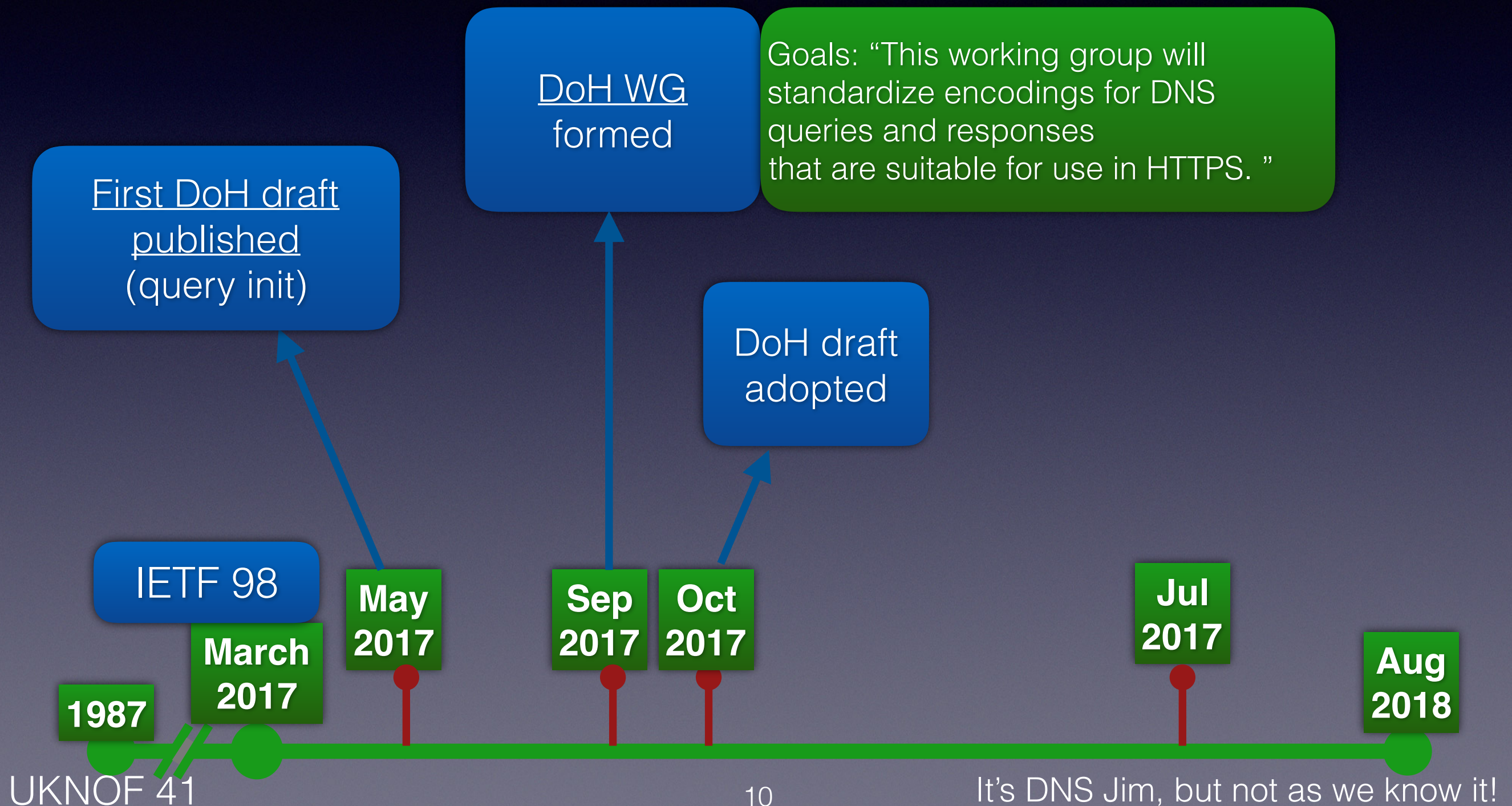
DNS-over-HTTPS (DoH)



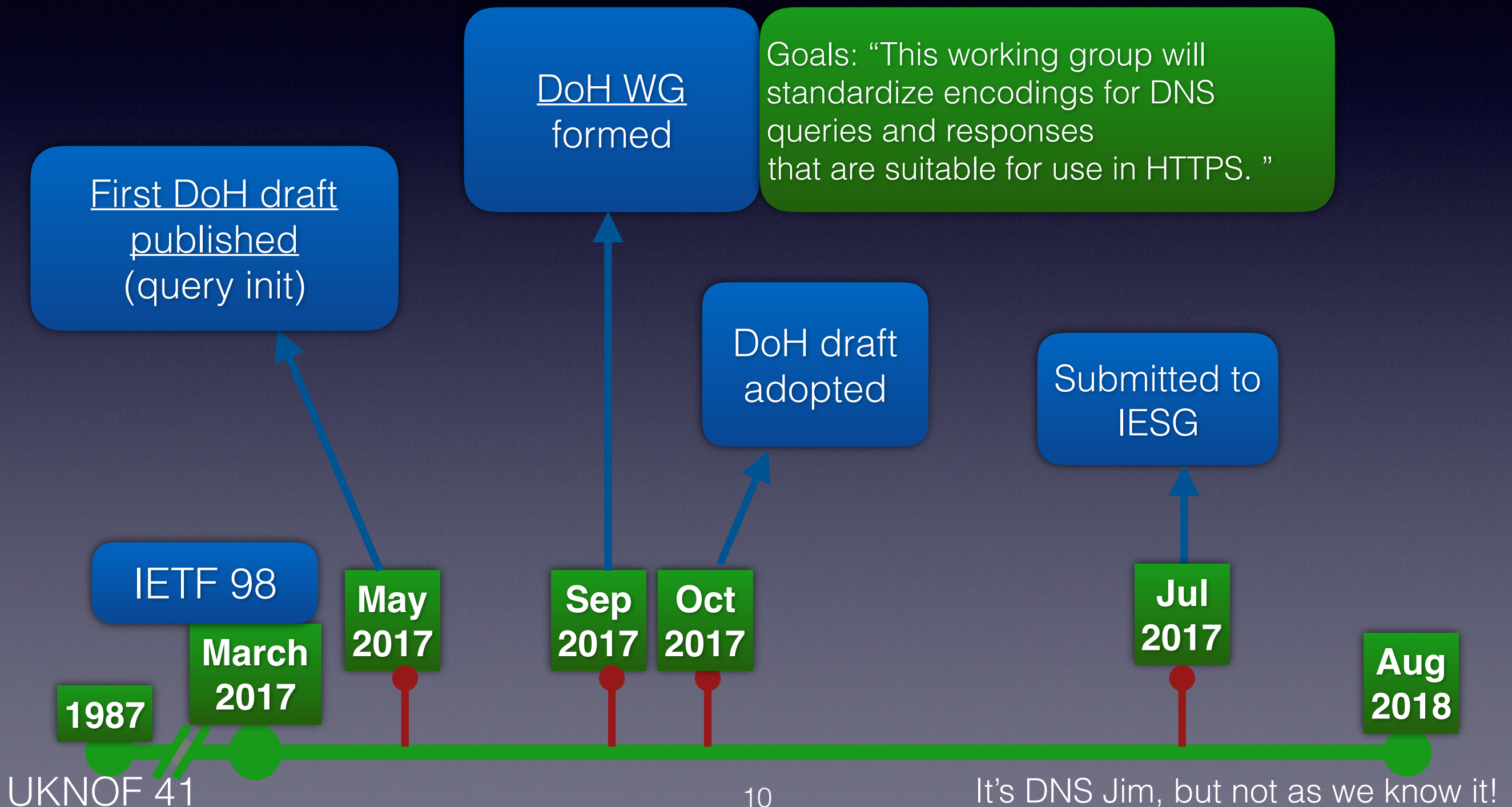
DNS-over-HTTPS (DoH)



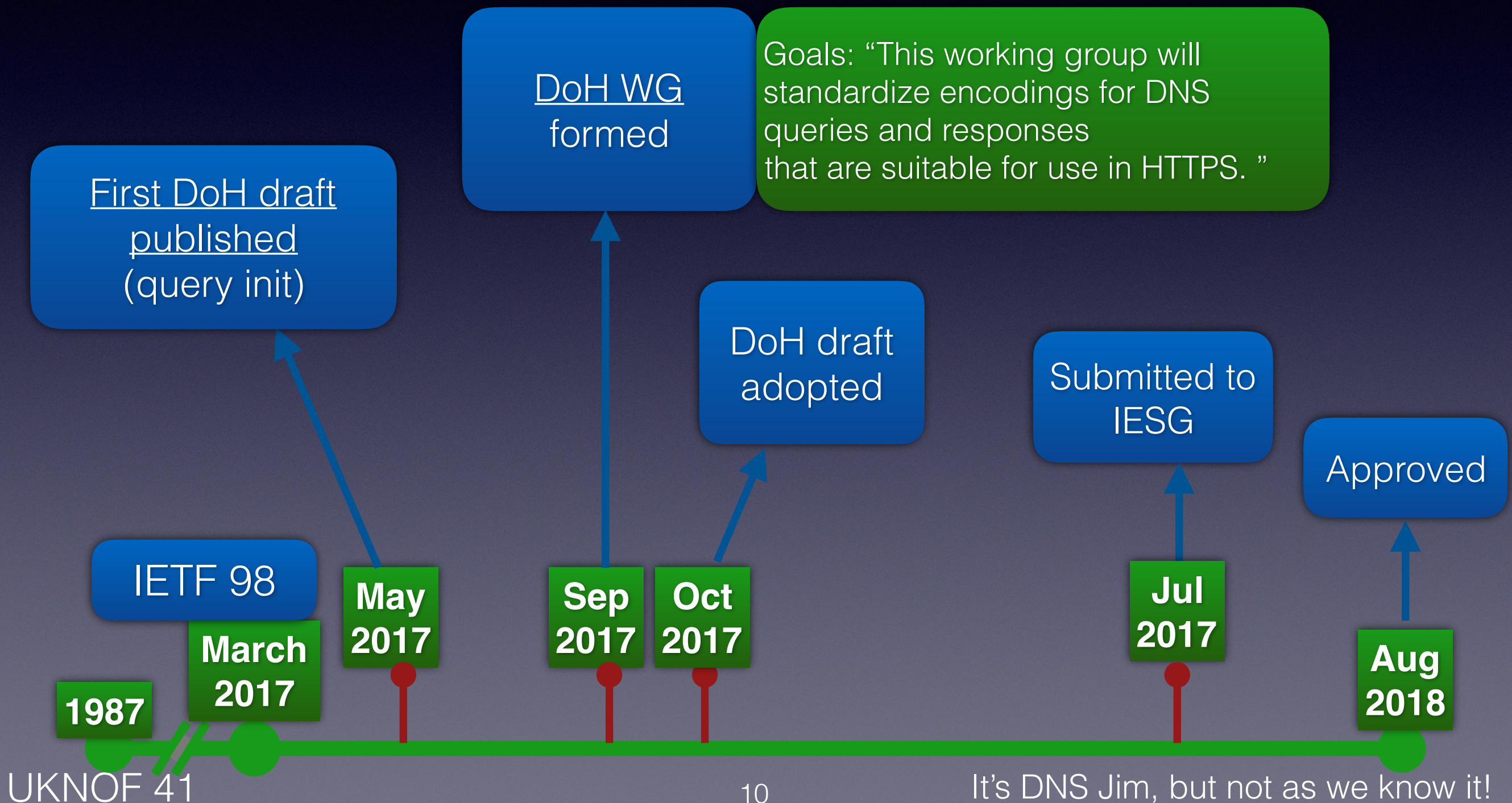
DNS-over-HTTPS (DoH)



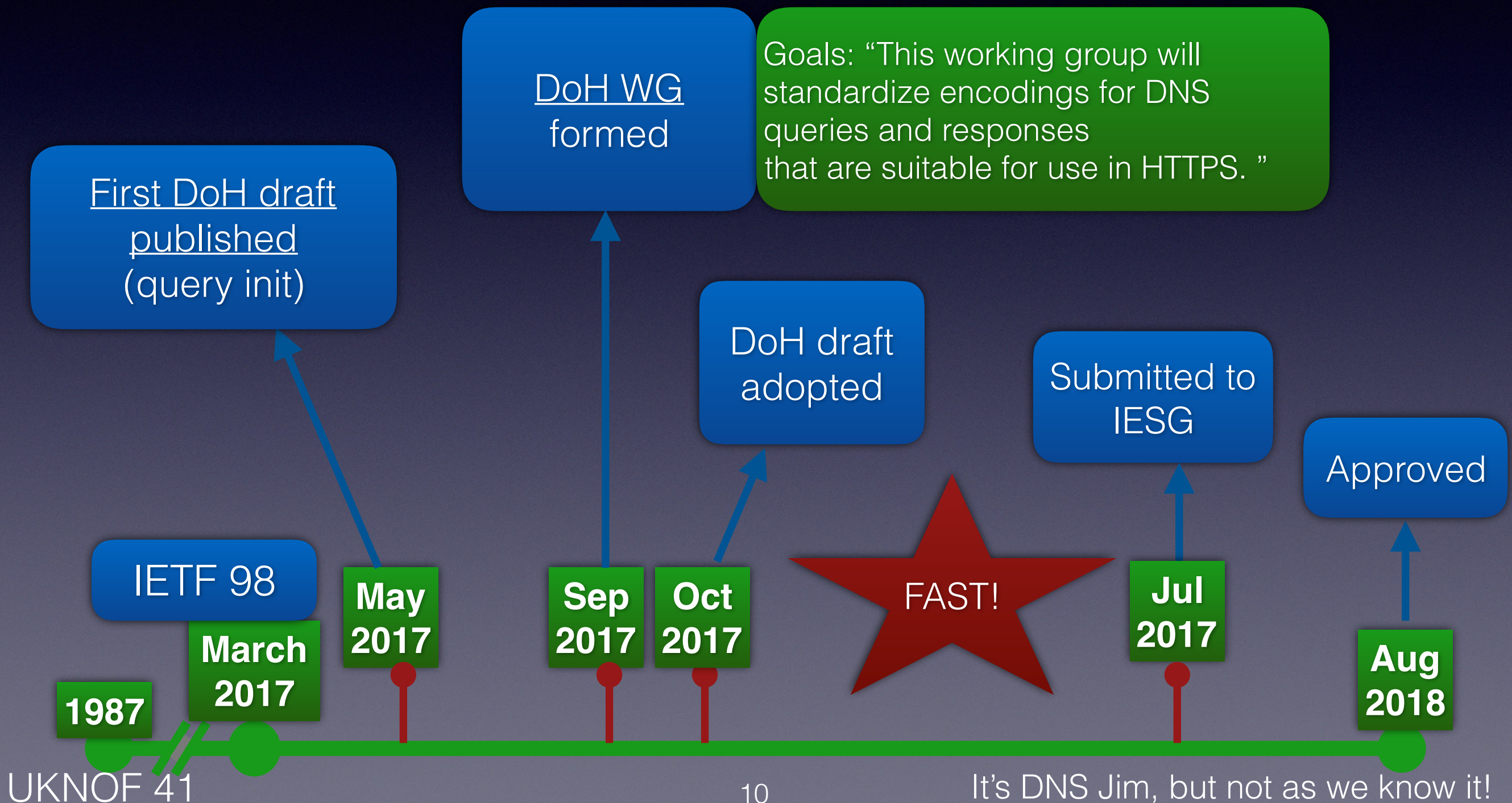
DNS-over-HTTPS (DoH)



DNS-over-HTTPS (DoH)



DNS-over-HTTPS (DoH)



How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”
- **Discovery - MUST use a URI template (not IP address)**
- **Two models:**
 - **Dedicated** connections (only DoH traffic) - hard to block
 - **Mixed** connections (send DoH on existing HTTPS connections)
 - Better privacy? Not leaking queries
- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”
- **Discovery - MUST use a URI template (not IP address)**
- **Two models:**
 - **Dedicated** connections (only DoH traffic) - hard to block
 - **Mixed** connections (send DoH on existing HTTPS connections)
 - Better privacy? Not leaking queries
- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

No
‘Opportunistic’

How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”
- **Discovery - MUST use a URI template (not IP address)**
- **Two models:**
 - **Dedicated** connections (only DoH traffic) - hard to block
 - **Mixed** connections (send DoH on existing HTTPS connections)
 - Better privacy? Not leaking queries
- **Increased tracking:** HTTP headers allow tracking of query via e.g. ‘User-agent’ (application), language, etc.

No
‘Opportunistic’**Impossible to block JUST DNS traffic**

How is DoH different to DoT?

- **A Use case (of many):** “allowing web applications to access DNS information via existing browser APIs”

- **Discovery - MUST use a URI template (not IP address)**

No
'Opportunistic'

- **Two models:**

- **Dedicated** connections (only DoH traffic) - hard to block
- **Mixed** connections (send DoH on existing HTTPS connections)
 - Better privacy? Not leaking queries

Impossible to block JUST DNS traffic

- **Increased tracking:** HTTP headers allow tracking of query via 'User-agent' (application), language, etc.

New privacy
concerns

DoH Status

	Standalone	Large Scale
Servers	<ul style="list-style-type: none">• Google https://dns.google.com/experimental• <u>Few other test servers</u>	<ul style="list-style-type: none">• <u>Cloudflare</u><ul style="list-style-type: none">• https://cloudflare-dns.com/dns-query• https://mozilla.cloudflare-dns.com/dns-query

DoH Status

	Standalone	Large Scale
Servers	<ul style="list-style-type: none">Google https://dns.google.com/experimental<u>Few other test servers</u>	<ul style="list-style-type: none"><u>Cloudflare</u><ul style="list-style-type: none">https://cloudflare-dns.com/dns-queryhttps://mozilla.cloudflare-dns.com/dns-query

	Client	Servers
Implementations	<ul style="list-style-type: none">Firefox Nightly config optionChrome (Bromite)Android 'Intra' AppCloudflaredStubby (next release)<u>Various experimental</u>	<ul style="list-style-type: none">dnsmdist (WIP)Knot resolver (patches)<u>Various experimental</u>

DoH Status

	Standalone	Large Scale
Servers	<ul style="list-style-type: none"> Google https://dns.google.com/experimental <u>Few other</u> 	<ul style="list-style-type: none"> <u>Cloudflare</u> <ul style="list-style-type: none"> https://cloudflare-dns.com/dns-query https://mozilla.cloudflare-dns.com/dns-query
Implementations	<ul style="list-style-type: none"> <u>Firefox Nightly</u> config option Chrome (Bromite) Android 'Intra' App Cloudflared Stubby (next release) <u>Various experimental</u> 	<ul style="list-style-type: none"> dnsmdist (WIP) Knot resolver (patches) <u>Various experimental</u>

“Moziflare”

DNS in Browsers

- Some already have their own DNS stub (e.g. Chrome)
- Some already use encrypted DNS ([Yandex](#), [Tenta](#))
- **Firefox 62 already has DoH, not enabled by default**
- **Firefox Nightly DoH experiment completed....**
- Chrome has a DoH implementation (not exposed, not advertised)
 - Used in the Chrome fork “[Bromite](#)”
 - And Google has a handy recursive resolver service in 8.8.8.8...



Dedicated DoH
connections

DNS in Browsers

- Some already have their own DNS stub (e.g. Chrome)
- Some already use encrypted DNS ([Yandex](#), [Tenta](#))
- **Firefox 62 already has DoH, not enabled by default**
- **Firefox Nightly DoH experiment completed....**
- Chrome has a DoH implementation (not exposed, not advertised)
 - Used in the Chrome fork “[Bromite](#)”
 - And Google has a handy recursive resolver service in 8.8.8.8...



Dedicated DoH connections

Browser vendors control the client and update frequently.

DoH in Browsers

- Why encrypt directly from the browser? Browser folks say:
- Why DoH, not DoT? Mozilla's answer:

DoH in Browsers

- Why encrypt directly from the browser? Browser folks say:

OS's are slow to offer new DNS features (DoT/DoH)

Selling point: “we care about the privacy of our users”

Performance: “reduce latency within browser”

- Why DoH, not DoT? Mozilla's answer:

DoH in Browsers

- Why encrypt directly from the browser? Browser folks say:

OS's are slow to offer new DNS features (DoT/DoH)

Selling point: “we care about the privacy of our users”

Performance: “reduce latency within browser”

- Why DoH, not DoT? Mozilla's answer:

Integration: “leverage the HTTPS ecosystem”

HTTPS everywhere: “it works... just use port 443, mix traffic”

Cool stuff: “JSON, Server Push, ‘Resolverless DNS’....”

DoH in Browsers

- Why encrypt directly from the browser? Browser folks say:

OS's are slow to offer new DNS features (DoT/DoH)

Selling point: “we care about the privacy of our users”

Performance: “reduce latency within browser”

- Why DoH, not DoT? Mozilla's answer:

Integration: “leverage the HTTPS ecosystem”

HTTPS everywhere: “it works... just use port 443, mix traffic”

Cool stuff: “JSON, Server Push, ‘Resolverless DNS’....”

DNS 2.0?

DoH in Firefox

- Mozilla blogs:
 - [Experiment & Future plans](#) (May 2018):

DoH in Firefox

- Mozilla blogs:
 - [Experiment & Future plans](#) (May 2018):

- **“We’d like to turn this [DoH] on as the default for all of our users”**
- **“Cloudflare is our ‘Trusted Recursive Resolver’ (TRR)”**

DoH in Firefox

- Mozilla blogs:
 - [Experiment & Future plans](#) (May 2018):

- “We’d like to turn this [DoH] on as the default for all of our users”
- “Cloudflare is our ‘Trusted Recursive Resolver’ (TRR)”

“With this [agreement], we have a resolver that we can trust to protect users’ privacy. This means **Firefox can ignore the resolver that the network provides** and just go straight to Cloudflare.”

DoH in Firefox



- Mozilla blogs:
 - [Firefox Nightly 'Experiment'](#) (June) & [Experiment results](#) (Aug)
 - Half of users opted-in: Send all DNS queries to system resolver **AND to Cloudflare**, compare the results.
 - “Initial experiment focused on validating:

DoH in Firefox



- Mozilla blogs:
 - [Firefox Nightly 'Experiment'](#) (June) & [Experiment results](#) (Aug)
 - Half of users opted-in: Send all DNS queries to system resolver **AND to Cloudflare**, compare the results.
 - “Initial experiment focused on validating:

1. Does the use of a **cloud DNS service** perform well enough to replace traditional DNS?”

DoH in Firefox



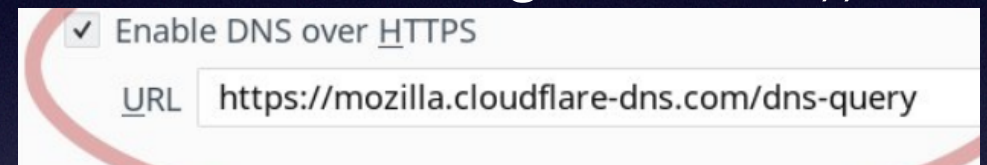
- Mozilla blogs:
 - [Firefox Nightly 'Experiment'](#) (June) & [Experiment results](#) (Aug)
 - Half of users opted-in: Send all DNS queries to system resolver **AND to Cloudflare**, compare the results.
 - “Initial experiment focused on validating:

1. Does the use of a **cloud DNS service** perform well enough to replace traditional DNS?”

RESULTS: 6ms performance overhead is acceptable
“**We’re committed long term to building a larger ecosystem of trusted DoH providers that live up to a high standard of data handling.**”

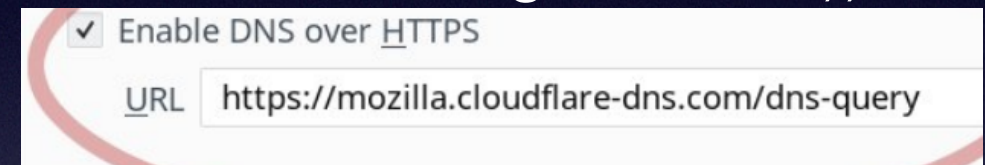
“Trusted recursive resolver”

- Tweet from Patrick McManus: “We haven't announced what that config will be or when it will be deployed (because we're still working on on it :)).”
- New UI to make config more obvious



“Trusted recursive resolver”

- Tweet from Patrick McManus: “We haven't announced what that config will be or when it will be deployed (because we're still working on on it :)).”
- New UI to make config more obvious

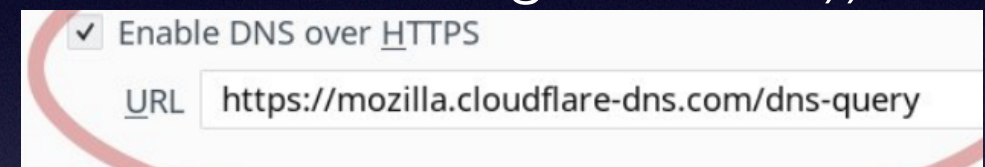


Impact of TRRs? Applications using default TRRs fundamentally change the existing **implicit** consent model for DNS:

- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C's (including DNS?)

“Trusted recursive resolver”

- Tweet from Patrick McManus: “We haven't announced what that config will be or when it will be deployed (because we're still working on on it :)).”
- New UI to make config more obvious



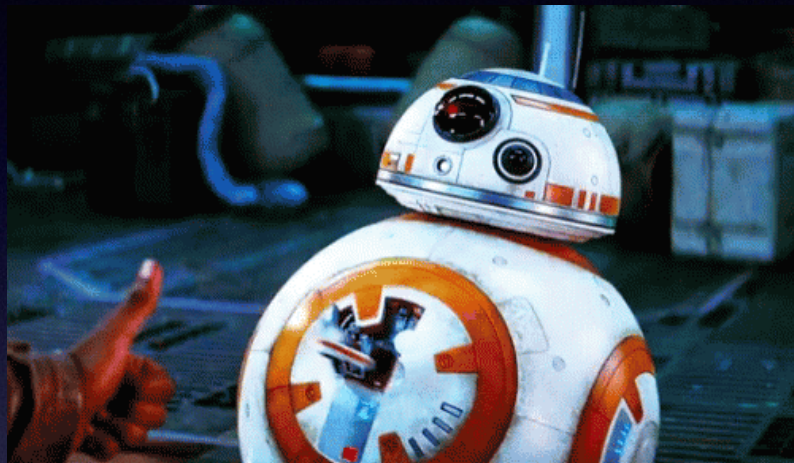
Impact of TRRs? Applications using default TRRs fundamentally change the existing **implicit** consent model for DNS:

- (Current) Log onto a network and use the DHCP provided resolver
- (New?) Use an app and agree to app T&C's (including DNS?)

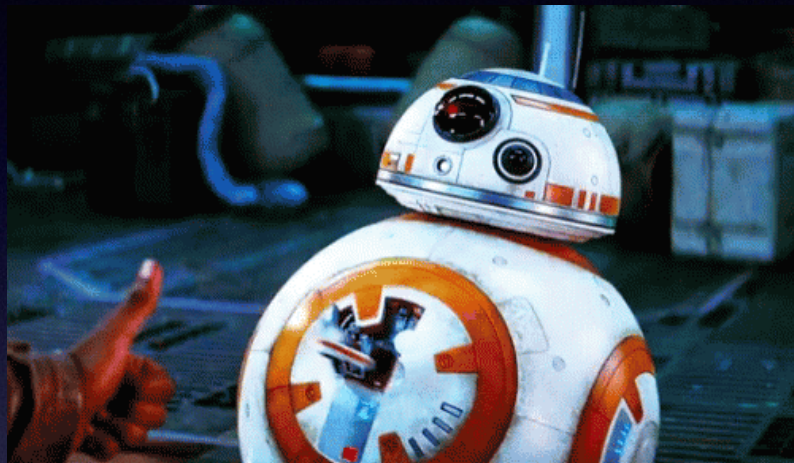
Potential **centralisation** of DNS resolution to a few providers?

Reactions are mixed...

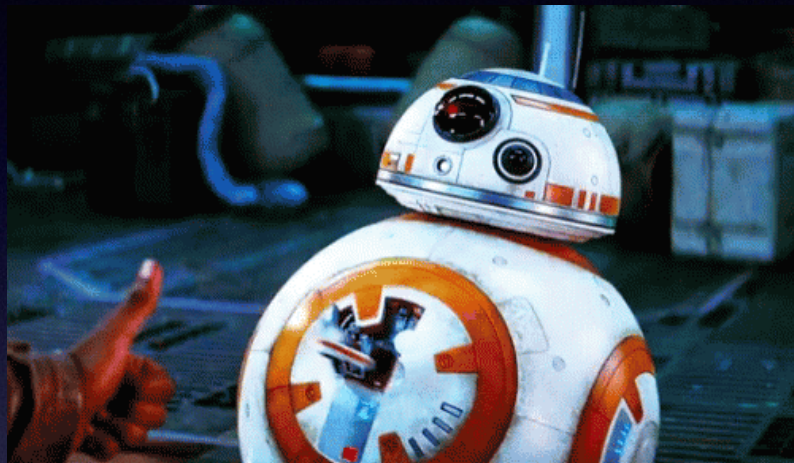
Reactions are mixed...



Reactions are mixed...



Reactions are mixed....



Soon, DoH+TRR in this browser will be fully operational!



Reactions?

- Ban/Block/Intercept Moziflare - ‘My network, my rules’
 - Operators need visibility (TLS 1.3 deja vu)
 - Is it even legal?
- Threat model analysis needed:
 - TRR useful but only in untrusted networks?
 - Users need choice (US lack of net neutrality vs EU GDPR)
 - Government regulation of TRRs, monetary incentives for apps?
- Analysis of third party DNS by PowerDNS
 - Neutrality of DNS operators (CDN’s?)
 - Legislation for blocking/filtering/interception?

[EPIC thread on
DNSOP](#)

Reactions?

- Ban/Block/Intercept Moziflare - 'My network, my rules'
 - Operators need visibility (TLS 1.3 deja vu)
 - Is it even legal?
- Threat model analysis needed:
 - TRR useful but only in untrusted networks?
 - Users need choice (US lack of net neutrality vs EU GDPR)
 - Government regulation of TRRs, monetary incentives for apps?
- Analysis of third party DNS by PowerDNS
 - Neutrality of DNS operators (CDN's?)
 - Legislation for blocking/filtering/interception?

[EPIC thread on
DNSOP](#)

Lots of
questions...

Managing many devices in enterprises

- What are **Chrome**, Safari, IE/Edge plans?
- What if **other apps** also do their own DoH/DoT?
- **Loss of central point of config on an end device?**
 - Loss of network settings as the default
 - DNS no longer part of the device infrastructure?

What to do?

- Think about running a **DoT server** in your network: for system level resolvers e.g. *Android*, *Stubby*, *systemd* it is the right thing!
- Think about running a **DoH server** in your network: gives users the option to use that, centralisation of DNS to a few players is a bad thing!
- **Watch this space and spread the word!** Work in progress:
 - Draft on an ‘opportunistic’ DoH discovery mechanism
 - Work in progress on Best Current Practices for Operators...
 - dnsprivacy.org website & twitter

What to do?

- Think about running a **DoT server** in your network: for system level resolvers e.g. *Android*, *Stubby*, *systemd* it is the right thing!
- Think about running a **DoH server** in your network: gives users the option to use that, centralisation of DNS to a few players is a bad thing!
- **Watch this space and spread the word!** Work in progress:
 - Draft on an ‘opportunistic’ DoH discovery mechanism
 - Work in progress on Best Current Practices for Operators...
 - dnsprivacy.org website & twitter

Stay tuned....

And now for something
completely different...!

A (EDNS) change is coming



- **When?** 1st Feb 2019
- **What?** Removal of workarounds for EDNS issues (failures, timeouts, incorrect responses due to middleboxes, firewalls, old nameserver s/w)
- **Who?** 'Big 4' open source DNS implementors
- **Your problem?** Only if your zone is not compliant!



- **To check:** <https://dnsflagday.net/>

Thank you!