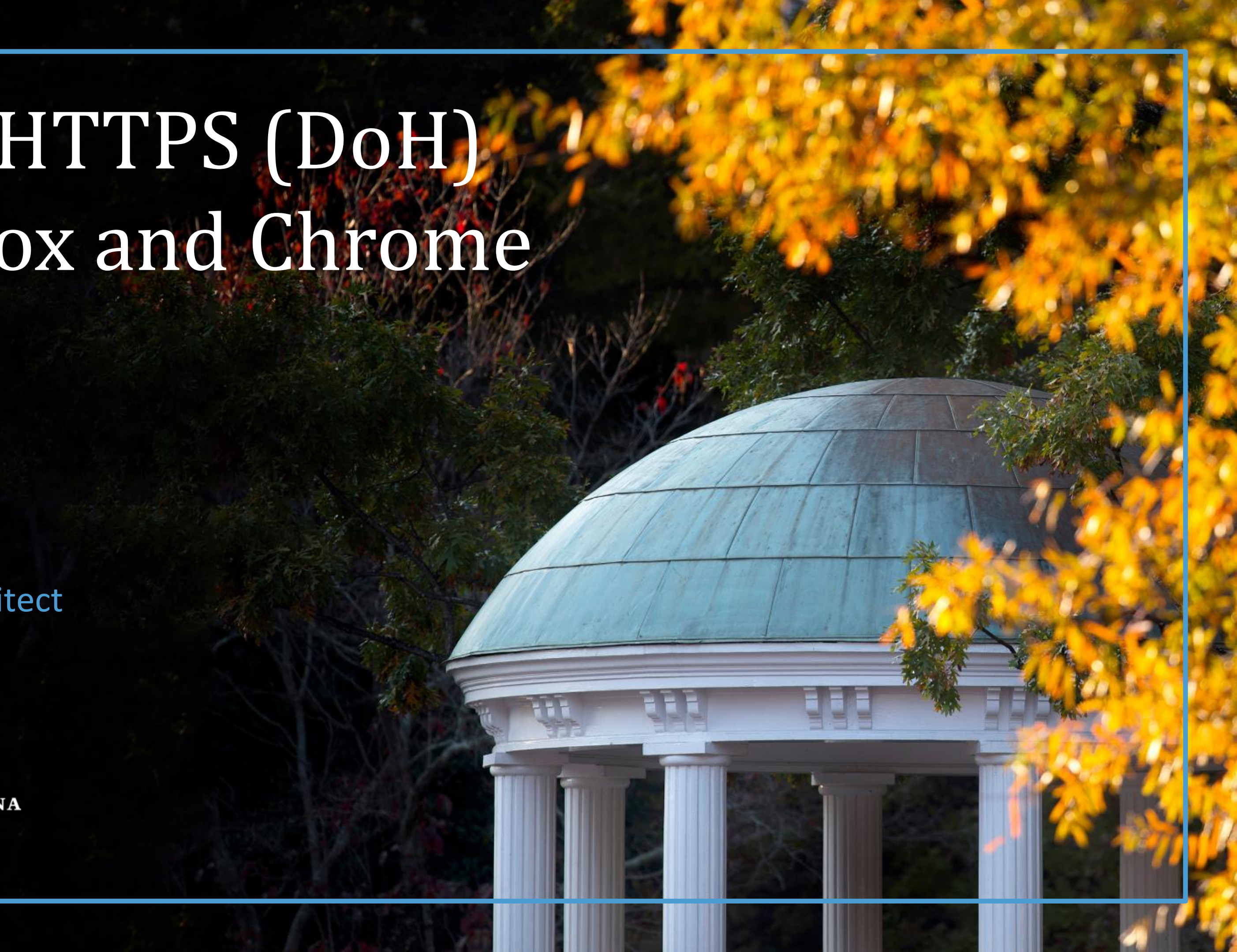
DNS over HTTPS (DoH) with Firefox and Chrome



Will Whitaker, DDI Architect

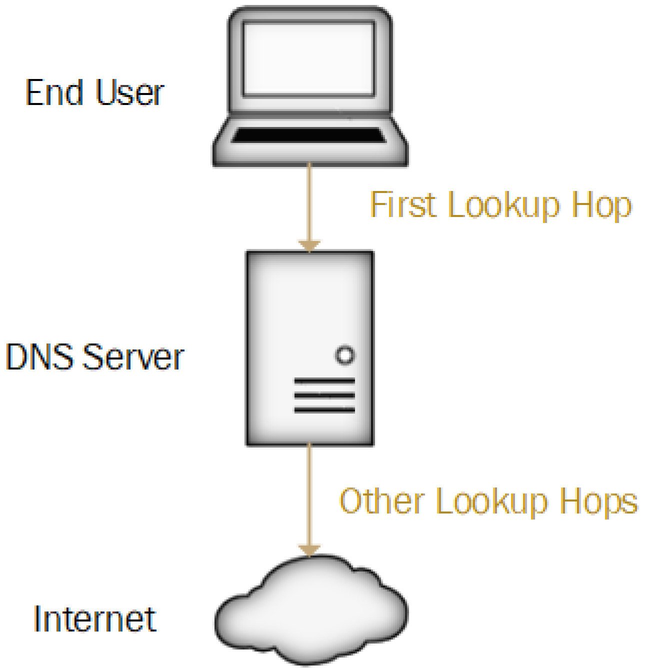
THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Technical Overview

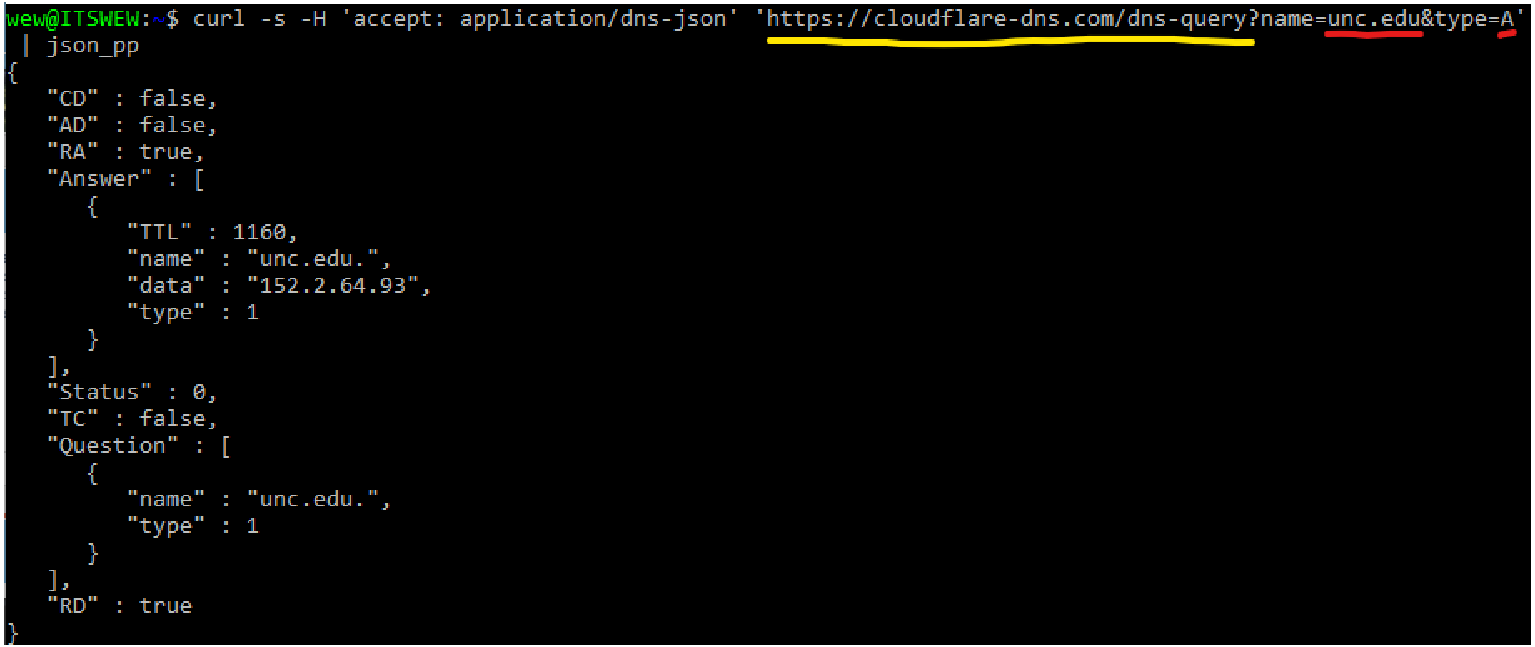
What is DoH all about?

The Goal: Increase User Privacy and Security

- First lookup hop can expose:
  - Client IP (i.e. user's address)
  - Query Name (i.e. website's name)
  - Query Answer (i.e. website's address)
- DNS Server can:
  - Selectively manipulate query answers
  - Log query traffic and share with others
- Other Lookup Hops:
  - Obscure Client IP by DNS server's IP



Query with Curl Example



```
wew@ITSWEW:~$ curl -s -H 'accept: application/dns-json' 'https://cloudflare-dns.com/dns-query?name=unc.edu&type=A'
 | json_pp
{
   "CD" : false,
   "AD" : false,
   "RA" : true,
   "Answer" : [
      {
         "TTL" : 1160,
         "name" : "unc.edu.",
         "data" : "152.2.64.93",
         "type" : 1
      }
   ],
   "Status" : 0,
   "TC" : false,
   "Question" : [
      {
         "name" : "unc.edu.",
         "type" : 1
      }
   ],
   "RD" : true
}
```

Enterprise Challenges

What could be impacted?

Firefox and Chrome DoH Adoption

Firefox

- Late September 2019
- New default: DoH to Cloudflare

Chrome

- Version 78 expected October 22, 2019
- Switch to DoH providers in some situations

The Negatives

DNS Firewalls

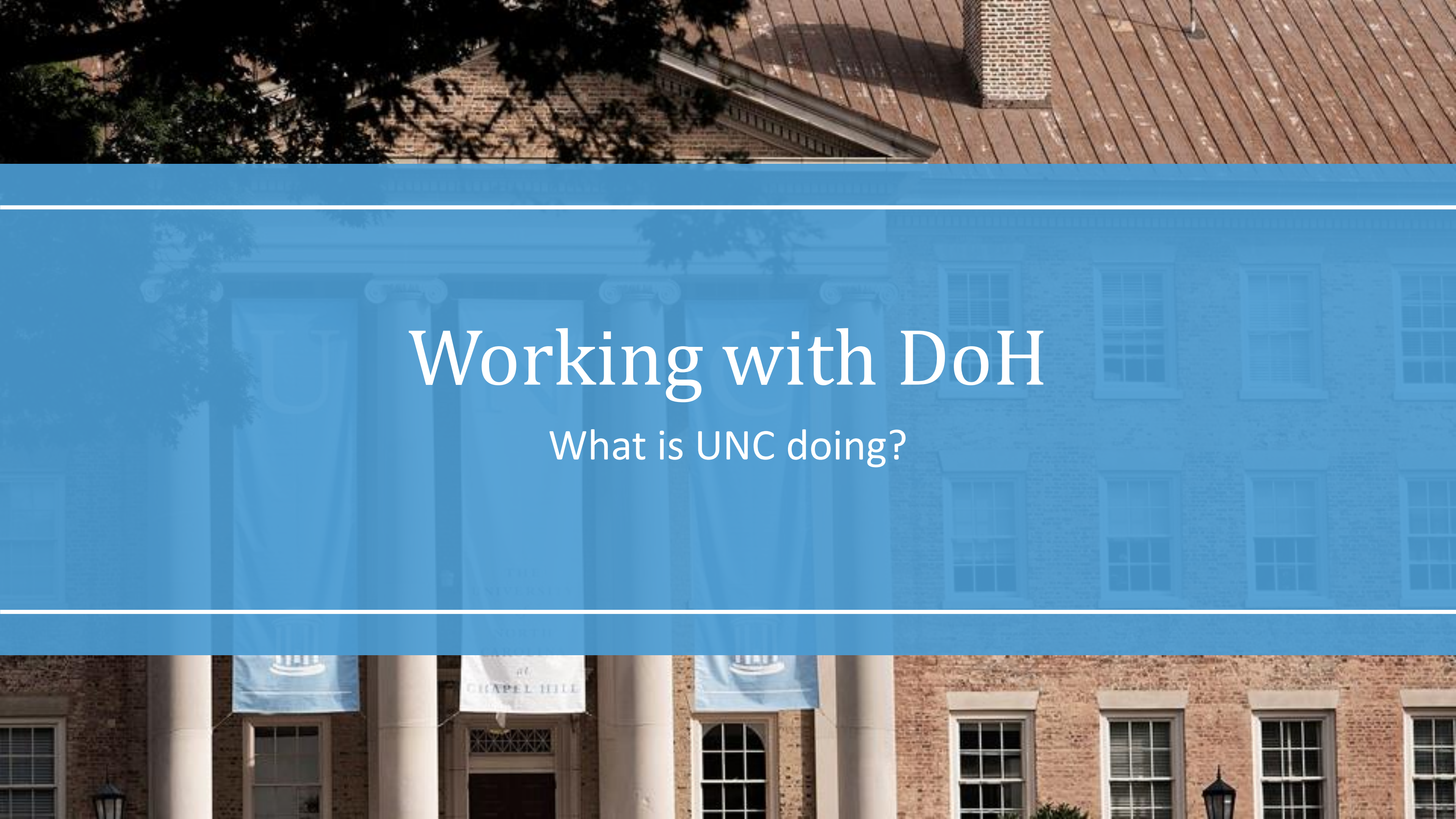
- Users lose protections provided by default
- Harder to identify compromised systems

Split-View DNS

- On-campus users see the “External” view
- Internal-only names leak to DoH provider

Support Issues

- Troubleshooting complexities
- Service level agreements and performance



Working with DoH

What is UNC doing?

Enterprise Management Response

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Manage Defaults (for non-technical users)

- Implement canary domain “use-application-dns.net” for Firefox

User Education (for technical users)

- Explain query log retention and content blocking policies.
- Communicate the value of DNS Firewall protections (i.e. malware, phishing, botnet)

Technical Controls (for all users)

- Allow users to opt in for DoH usage on most networks
- Restrict DoH where appropriate with sensitive networks

Prominent DNS Security and Privacy Efforts

Protocol	IETF	Features	Port
DNSSEC	RFC 4033 (2005)	Authenticated responses, not applicable to first hop	53
DNSCrypt	No RFC, Circa 2008	Crypto wrapper on raw DNS query/response packets	443
DNS over TLS (DoT)	RFC 7858 (2016)	TLS wrapper	853
DNS over HTTPS (DoH)	RFC 8484 (2018)	HTTP/2 wrapper	443

* DoH is not the first in this space

References

- Mozilla, Configuring Networks to Disable DNS over HTTPS https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https
- Infoblox DoT, DoH and the DNS “Last Mile” Security Problem https://community.infoblox.com/t5/Company-Blog/DoT-DoH-and-the-DNS-Last-Mile-Security-Problem/ba-p/15468
- REN-ISAC DoH Advisory https://www.ren-isac.net/public-resources/alerts/REN-ISAC_DoH_Advisory_20190920.pdf

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL