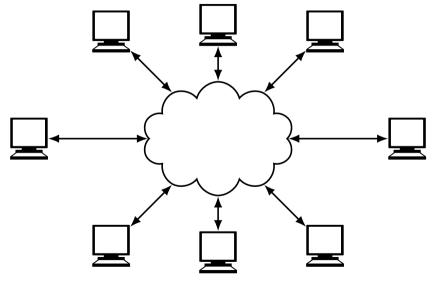
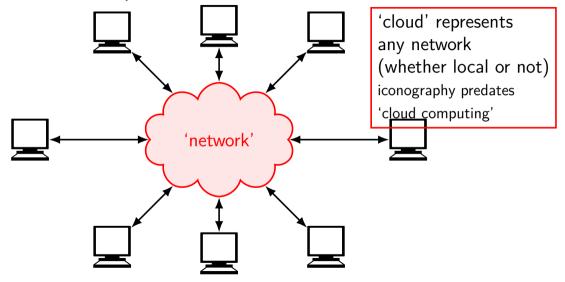
networks / hosts aka end systems

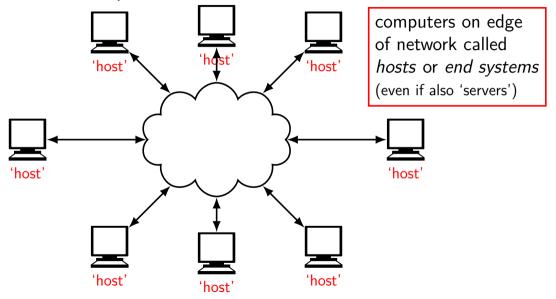


networks / hosts aka end systems *networks* connect computers 'network'

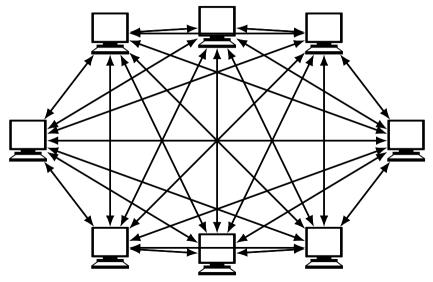
networks / hosts aka end systems



networks / hosts aka end systems



direct connections?



shared medium: radio?

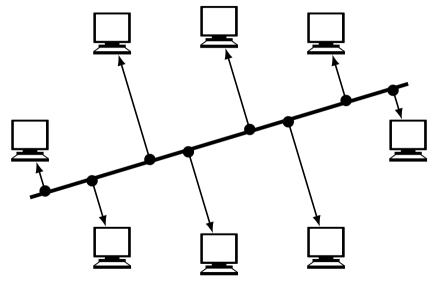




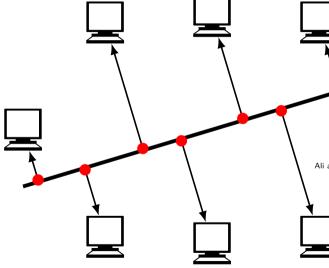


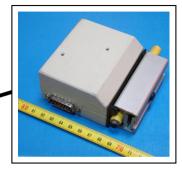


shared medium: wires



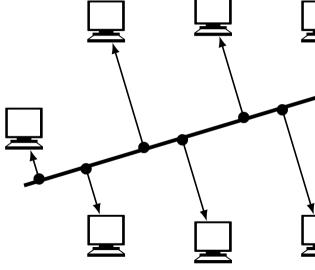
shared medium: wires





Ali at gwc.org.uk / Alistair1978 via Wikimedia commons / CC-BY-SA 2.5

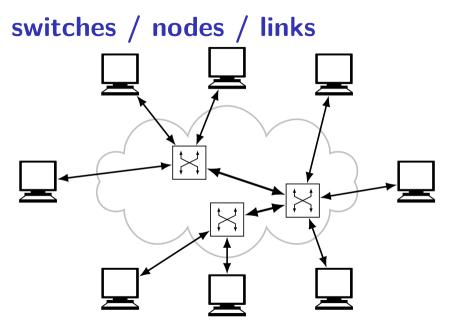
shared medium: wires

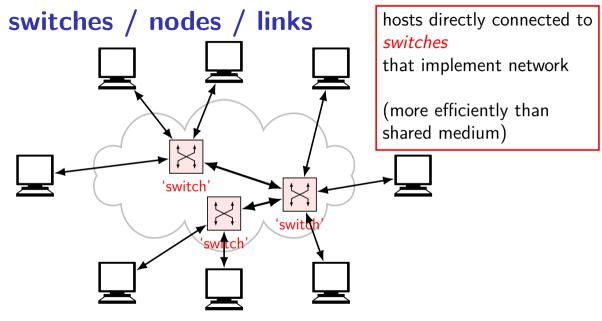


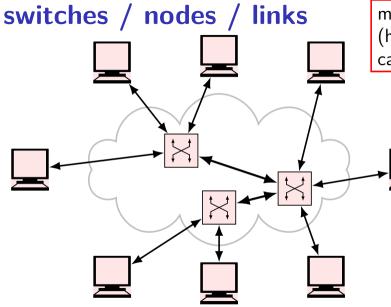


Ali at gwc.org.uk / Alistair 1978 via Wikimedia commons / CC-BY-SA 2.5

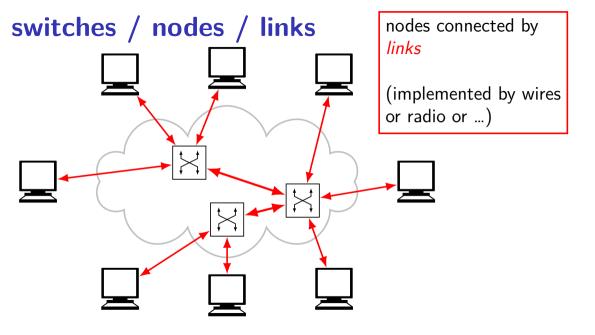




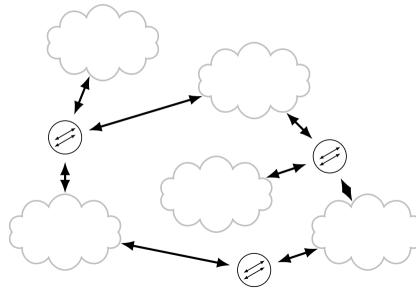




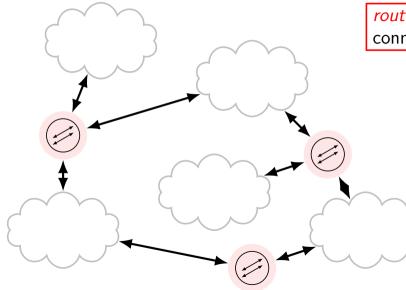
machines on network (hosts, switches, ...) called *nodes*



routers / internetwork

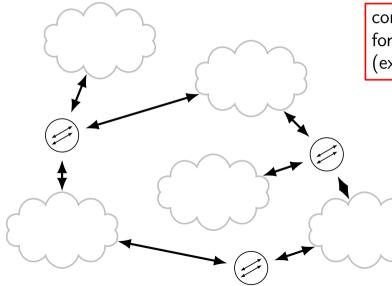


routers / internetwork



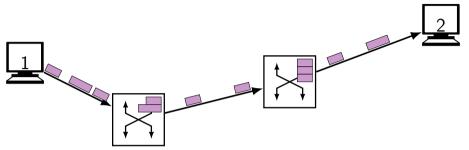
routers or *gateways* connect networks

routers / internetwork



connected networks form *internetwork* (example: the Internet)

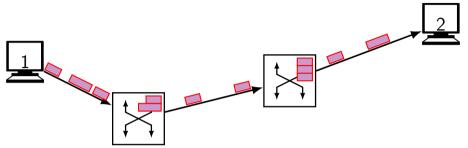
flows / packets



flow of data between two machines

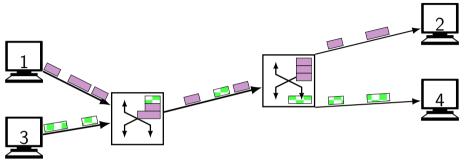
flow is very general term will depend on context how it relates to connections, sockets, etc.

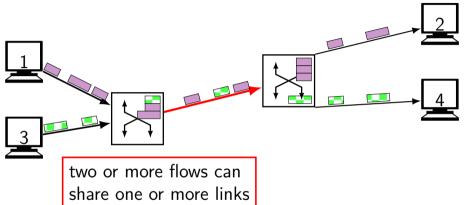
flows / packets

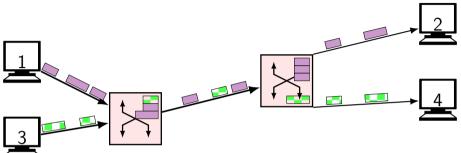


flow of data between two machines

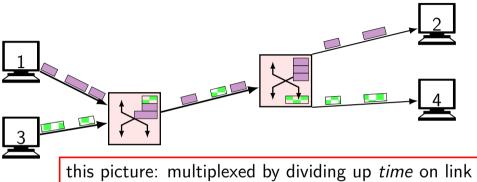
possibly divided up into pieces, called *packets*, *frames*, *segments* (which name is best depends on context)

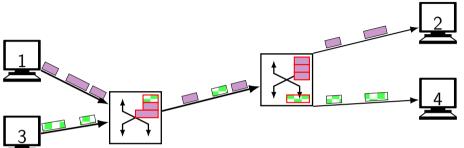






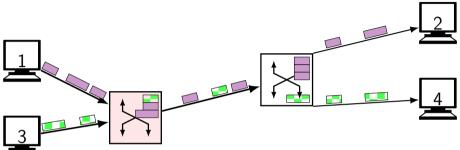
left switch *multiplexes* the two flows onto one link right switch *demultiplexes* them to separate them





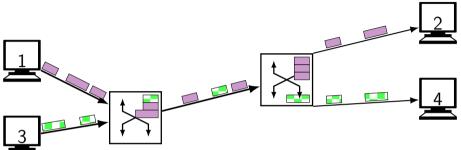
switches usually have *buffers* (also called *queues*) hold waiting packets

absorbs temporary "bursts" where packets come faster than outgoing link can handle



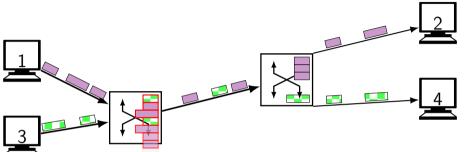
incomplete list of causes of 'bursts':

multiple unsynchronized flows fast links produce packets faster for slow can send



incomplete list of causes of 'bursts':

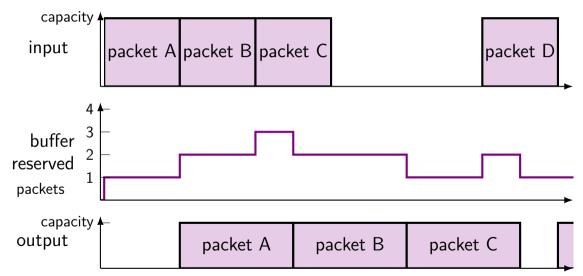
multiple unsynchronized flows fast links produce packets faster for slow can send



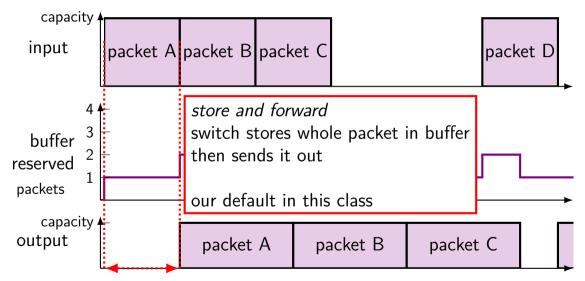
if buffer full, switch must *drop* packets will happen eventually if overall rate faster than outgoing link

scenario is called *congestion*

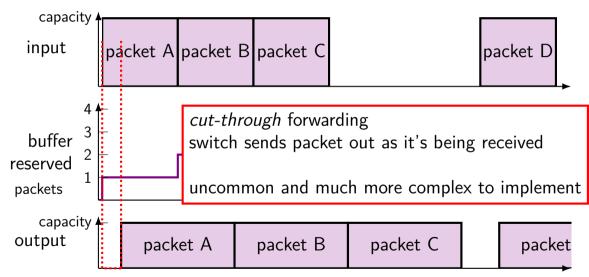
buffer usage: fast to slow, store + forward



buffer usage: fast to slow, store + forward



buffer usage: fast to slow, cut-through



channel abstractions

want to avoid custom network for each application

but applications have different needs

 \rightarrow multiple application interfaces to networks common implementation of common patterns

some abstractions

stream

continuous stream of bytes from one program to another 'connection' from one program to another

datagrams

send small messages (*datagrams*) each datagram's destination independently set

remote procedure calls make function calls that run on remote machine

remote memory access read/write bytes of data in remote memory

some abstractions

stream

continuous stream of bytes from one program to another 'connection' from one program to another

datagrams

send small messages (*datagrams*) each datagram's destination independently set

remote procedure calls make function calls that run on remote machine

remote memory access read/write bytes of data in remote memory

focus on streams

this class: focus on implementing streams of bytes

why?

most commonly used by applications on the Internet many common tasks with other abstractions

stream abstraction and sockets

BSD sockets are most used abstract for using streams

```
server (passive end)
    create socket (socket())
    select address (bind())
    wait for+get connection (listen()+accept())
    read+write on
    connection(read()+recv*()+write()+send*())
```

```
client (active end)
    create socket (socket())
    connect to address (connect()
    read+write on
    connection(read()+recv*()+write()+send*())
```

sockets and other options

sockets can also provide *datagram* abstraction difference: mode where read/write keeps messages together

socket details later

we're doing mostly bottom-up approach

will actually talk in detail about socket interface later in semester

client/server

server = entity that waits for + responds to *clients*

server:

always-on well-known how to contact

client

sometimes on only contacted by server responding to it

not client/server?

not everything fits into client/server neatly

sometimes something is both client and server

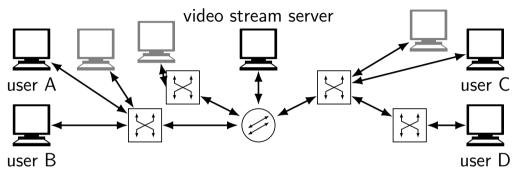
sometimes no distinguished entities ("peer-to-peer")

client/server and channels

can have channels without client/server model

but the interface sockets provide assume client/server (so you have to make something server-like to do peer-to-peer with sockets)

exercise



if each of users A–D are receiving (potentially different) video and audio from the video streaming server, then...

how many flows? how many nodes are involved? how many switches/routers?

IETF

IETF = Internet Engineering Task Force part of non-profit called *Internet Society*

most common internet protocols standardized by IETF

most IETF documents called RFCs requests for comment have unique number

https://rfc-editor.org

other standard orgs

Bluetooth Special Interest Group

IEEE (Institute of Electrical and Electronics Engineers) Wifi, Ethernet, ...

3GPP (3rd Generation Partnership Project) cellular phone networks

SCTE (Society of Cable Televsion Engineers)

ITU (International Telecommunication Union)

ISO (International Organization for Standardization)

separating data into pieces network can handle

putting pieces back together

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

separating data into pieces network can handle

putting pieces back together

getting network to send piece to correct remote network

getting ne lots of work! don't want to implement all at once!

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

separating data into pieces network can handle

puttin some parts need to be different for different local networks

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

separa some parts should not concern local network implementors

putting pieces back together

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

separating some parts should be same for different abstraction

putting pieces back together

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

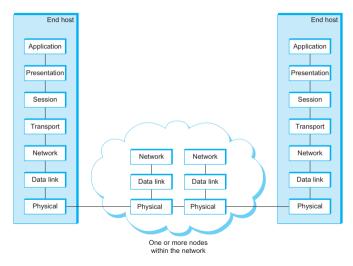
layered model

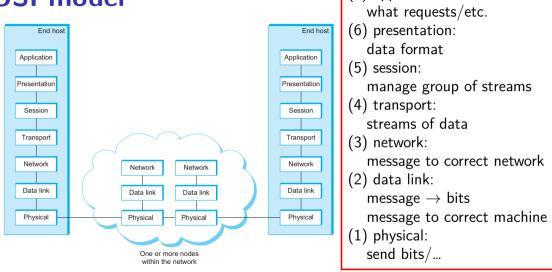
networking implemented in 'layers'

upper layers implemented by making calls to lower layers

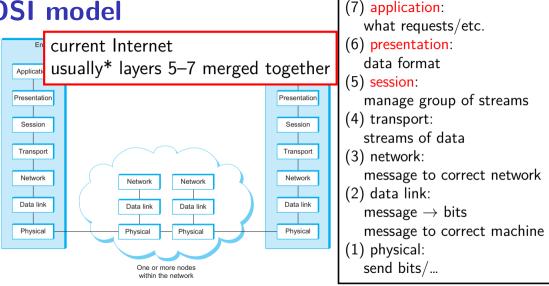
example: network implements 'send data to (remote) machine' function ("network layer")

stream implementation calls this to implement 'send stream to remote application'





(7) application:



standardized by ISO (International Standards Organization) and ITU (International Telecommunications Union)

full set of protocols...

file transfer, message sending, directory lookups ...

that were often implemented and sometimes used...

but mostly lost out to IETF-standardized Internet protocols Internet Engineering Task Force

OSI influence (1)

term 'layer 7', 'layer 4', 'layer 3', etc. almost always refer to OSI model

...even though most of Internet does not follow it early Internet protocols predate OSI

OSI influence (2)

...

are a lot of Internet protocols influenced by OSI protocols

OSI's DAP (directory access protocol) adapted into IETF's LDAP (lightweight directory access protocol)

OSI presentation layer ASN.1 used in... telephony (between telephone companies) inter-bank messaging lots of cryptography-related protocols

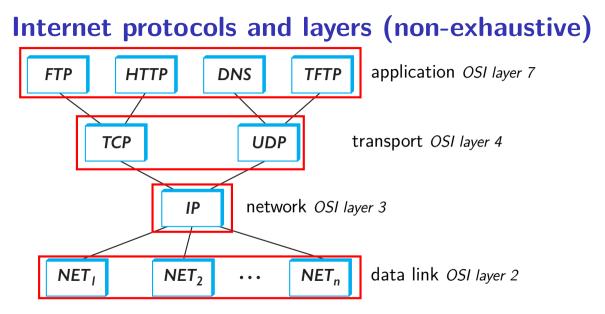
OSI's routing protocol IS-IS still common in large Internet-connected networks (adapted to work alongside IETF protocols)

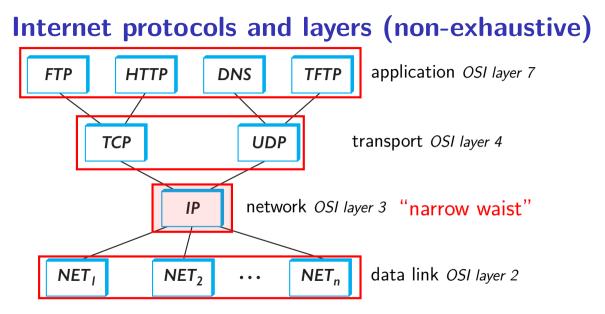
Internet layers

OSI layer	name	examples	purpose
7	application	HTTP, SSH,	application-defined meanings
		SMTP, DNS,	
4	transport	TCP, UDP,	reach correct program,
			reliablity/streams
3	network	IPv4, IPv6,	reach correct machine
			(across networks)
2	link	Ethernet, Wi-Fi,	coordinate shared wire/radio
1	physical		encode bits for wire/radio

Internet layers

OSI layer	name	examples	purpose
7	application	HTTP, SSH,	application-defined meanings
		SMTP, DNS,	
4	transport	TCP, UDP,	reach correct program,
			reliablity/streams
3	network	IPv4, IPv6,	reach correct machine
			(across networks)
2	link	Ethernet, Wi-Fi,	coordinate shared wire/radio
1	physical		encode bits for wire/radio





fuzzy layers (1)

ICMP (Internet Control Message Protocol)...

implemented using a network layer...
so seems like a transport layer protocol?

fuzzy layers (1)

ICMP (Internet Control Message Protocol)...

implemented using a network layer... so seems like a transport layer protocol?

used to send errors/control messages about routing... routing is the network layer's job so ICMP is part of network layer?

fuzzy layers (1)

ICMP (Internet Control Message Protocol)...

implemented using a network layer... so seems like a transport layer protocol?

used to send errors/control messages about routing... routing is the network layer's job so ICMP is part of network layer?

I think saying network layer is probably better...

but we're not going to be picky about it

fuzzy layers (2)

TLS (Transport Control Protocol)...

implemented on top of TCP...

so seems like a application layer protocol?

fuzzy layers (2)

TLS (Transport Control Protocol)...

implemented on top of TCP... so seems like a application layer protocol?

used to send other application layer protocols so maybe a transport layer? or presentation layer?

I'll call it an application layer...

'extra' layers

layer terminology doesn't always work cleanly often "extra" layers in practice

- e.g. HTTPS: HTTP (app layer) on TLS (another app layer) on TCP (network) on ...
- e.g. DNS over HTTPS: DNS (app layer) on HTTP on on TLS on TCP on ...
- e.g. SFTP:

SFTP (app layer??) on SSH (another app layer) on TCP on ...

e.g. HTTP over OpenVPN: HTTP on TCP on IP on OpenVPN on UDP on different IP on ...

'extra' layers

layer terminology doesn't always work cleanly often "extra" layers in practice

e.g. HTTPS:

HTTP (app layer) on TLS (another app layer) on TCP (network) on ...

e.g. DNS over HTTPS:

DNS (app layer) on HTTP on on TLS on TCP on ...

e.g. SFTP:

SFTP (app layer??) on SSH (another app layer) on TCP on ...

e.g. HTTP over OpenVPN: HTTP on TCP on IP on OpenVPN on UDP on different IP on ...

protocols usually over HTTP

SOAP (Simple Object Access Protocol) — messaging/remote procedure calls

gRPC (originally form Google) — remote procedure calls

HLS (HTTP Live Streaming) — video streaming

DASH (Dynamic Adaptive Streaming over HTTP) — video streaming

packet capture tools

packet capture = log of everything sent/received on some link(s)

wireshark is popular tool for making, analyzing packet captures

will be showing screenshots from that

you can download these packet captures, follow along in wireshark

◢ ■ ∅ ◎ 🚞 🖹 🖄 🙆 ۹ 🗢 🔶 警 🖉 曼 📃 🔍 ۹ ۹ ୩

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol L	Length Info
16	20 18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
16	21 18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
16	22 18.605415235	162.159.61.4	10.0.2.15	iresha	rk window ponse 0x0000 HTTPS www.cs.virginia.edu SOA co
				ii Cona	
	24 18.606080777	10.0.2.15	162.159.61.4	DOH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
	25 18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
	26 18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
	27 18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query
	28 18.606287808		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
	29 18.606305512	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT
	30 18.606380752	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
16	31 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK
1					
			its), 213 bytes captu		
			dc (08:00:27:cc:86:dc		
			0.2.15, Dst: 162.159.	61.4	0020 3d 04 ec 5e 01 bb 58 2f 90 0d 0a 60 df eb 50 18 =··^·X/···
	0100 = Versi		(-)		0030 f9 0c ec 6b 00 00 17 03 03 00 9a 16 c6 b5 b2 4e ···k····
		er Length: 20 bytes			0040 b3 68 7c 03 5e af 57 1f 88 6a 55 92 ae f5 0f 2c h h h w ju
			0 (DSCP: CS0, ECN: No	t-ECT)	0050 ab af 6a a3 6a 13 97 1f 72 94 49 37 10 f5 e2 0fj.jr.I
	otal Length: 199 Identification: 0				0060 db 3d da 88 ab 3f 98 91 1c 8c 53 eb 6d 79 40 b0 =
		:: 0x2, Don't fragm	pont		0080 1b d4 18 f1 f4 b3 f5 25 95 0c a2 21 15 93 21 13%
		000 = Fragment Offs			0090 d6 9e ec 48 5b d1 cc 83 03 b6 c4 8b ab 0b c0 ee
	Time to Live: 64	100 - Fragment Oris	set. 0		00a0 35 f7 d5 e2 ad 6e 7d 5b d1 a2 50 2b 44 31 ab 36 5
	Protocol: TCP (6)				00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64
		0x7e03 [validation	disabled]		00c0 be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8 +NZI B· MO·
		status: Unverified			00d0 d6 04 d0 14 7b
	Source Address: 1		•1		
		ss: 162.159.61.4			
			rt: 60510, Dst Port:	443, Seq: 172	
	nsport Layer Secu				
Нуре	erText Transfer I	Protocol 2			
(•	Frame (213 bytes) Decrypted TLS (137 bytes)

- +

◢ ■ ∅ ◎ 🖿 🗅 🗴 🙆 ۹ 👄 🔶 警 🖉 📃 📃 ۹. ۹ ۹ 🏢

Destination

10.0.2.15

Apply a display filter ... <Ctrl-/>

Time

No

Source

1620 18,594474318 162,159,61,4

										• +		
ngth	Info										-	
60	443	-+	60510	[ACK]	Seq=40361	Ack=16799	Win=65535	Len=0		_		
60	443	-+	60510	[ACK]	Seq=40361	Ack=16958	Win=65535	Len=0		_	-	
0.04	04	a set a	and the second			DOO UTTOO	and a second second second	and and an an also	004			

	1020 10.0044/4010	102.109.01.4	10.0.2.10	TOP	00 445 → 00510 [ACK] SEQ-40501 ACK-10755 WII-05555 LEI-0	
	1621 18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0 🗕	_
	1622 18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co	
	1623 18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query	
	1624 18.606080777	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT	
	1625 18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0	
	1626 18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0	
	1627 18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query	_
	1628 18.606287808	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seg=40938 Ack=17229 Win=65535 Len=0	
	1629 18.606305512	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT	
	1630 18.606380752	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0	
	1631 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK	-
4						
•	Frame 1629: 213 byt	es on wire (1704 b	its), 213 bytes captu	red (1704 bit	0000 52 54 00 12 35 02 08 00 27 cc 86 dc 08 00 45 00 RT 5 ···· ···	• • • • F
	Ethernet II, Src: P	CSSystemtec cc:86:	dc (08:00:27:cc:86:dc), Dst: 52:54	0010 00 c7 d0 7b 40 00 40 06 7e 03 0a 00 02 0f a2 9f {@.@. ~.	
-	Internet Protocol V	ersion 4, Src: 10.	0.2.15, Dst: 162.159.	61.4	0020 3d 04 ec 5e 01 bb 58 2f 90 0d 0a 60 df eb 50 18 = · · · · X/ · ·	• * • • P
	0100 = Vers	ion: 4			0030 f9 0c ec 6b 00 00 17 03 03 00 9a 16 c6 b5 b2 4ek	
	0101 = Head	er Length: 20 byte	s (5)		0040 b3 68 7c 03 5e af 57 1f 88 6a 55 92 ae f5 0f 2ch -^-Wjt	U · · · ·
	Differentiated Second Secon	ervices Field: 0x0	0 (DSCP: CS0, ECN: Not	-ECT)	0050 ab af 6a a3 6a 13 97 1f 72 94 49 37 10 f5 e2 0f jj. r	17
	Total Length: 19	9			0060 db 3d da 88 ab 3f 98 91 1c 8c 53 eb 6d 79 40 b0 =?	S · my@
	Identification:	0xd07b (53371)			0070 db 44 14 fb 9c fc 4d 34 05 7f ad ab f4 ce 36 7c D M4	6
	▶ 010 = Flag:	s: 0x2, Don't frag	ment		0080 1b d4 18 f1 f4 b3 f5 25 95 0c a2 21 15 93 21 13%	1111
	0 0000 0000 0	000 = Fragment Off	set: 0		0090 d6 9e ec 48 5b d1 cc 83 03 b6 c4 8b ab 0b c0 eeH[
	Time to Live: 64	-			00a0 35 f7 d5 e2 ad 6e 7d 5b d1 a2 50 2b 44 31 ab 36 5 n}[P+D1
	Protocol: TCP (6)			00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64 p:	i :
	Header Checksum:	0x7e03 [validatio	n disabled]		00c0 be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8 +NZI B MQ	• q • • •
	[Header checksum	status: Unverifie	d]		00d0 d6 04 d0 14 7b	
	Source Address: :	10.0.2.15				
	Destination Addr	ess: 162.159.61.4				
			ort: 60510, Dst Port: -	443, Seq: 172		
	Transport Layer Sec				4	•
•	HyperText Transfer	Protocol 2				
4				•	Frame (213 bytes) Decrypted TLS (137 bytes)	
(🔰 🍸 Source Address (i	p.src), 4 bytes			Packets: 1765 · Displayed: 1765 (100.0%) Profile: Defaul	lt -

Protocol Length Info

TCP

◢ ■ ∅ ◎ 🚍 🖹 🛛 🗳 ۹ 👄 🛎 春 🖢 📃 🗐 ۹ ۹ ۹ ୩ 🏦

Apply a display filter ... <Ctrl-/>

- +

	Apply a display filter >	curv-			
No.	Time	Source	Destination	Protocol Le	Length Info
	1620 18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
	1621 18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
	1622 18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
	1623 18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query
	1624 18.606080777	10.0.2.15	162.159.61.4	DoH	213 Candard query 0x0000 AAAA www.cs.virginia.edu OPT
	1625 18.606168058	162.159.61.4	10.0.2.15	nacke	et list 9510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0 9510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
	1626 18.606168109		10.0.2.15	pache	
	1627 18.606221426	10.0.2.15	162.159.61.4		110 HEADERS[149]: POST /dns-query
	1628 18.606287808		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
-	1629 18.606305512		162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT
	1630 18.606380752		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
	1631 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK
•	Internet Protocol V 0400 Vers 0101 = Head b Differentiated S Total Length: 30 Identification: 0400 = Fla 04000 e0000 Time to Live: 6 Protocol: TCP (Header Checksum: [Header Checksum: Source Address: Destination Address: Destination Contro	ersion 4, Src: 10.6 ion: 4 er Length: 20 bytes ervices Field: 0x06 9 0x007b (53371) Dacket d 0x7e03 [validation status: Unverifice ess: 162.159.61.4 L Protocol, Src Per) (dścp: cs0, ecn: No etails) disabled]	.61.4 ot-ECT)	$\begin{array}{llllllllllllllllllllllllllllllllllll$
	Transport Layer Sec				4
	HyperText Transfer	Protocol 2			Energy (MAR Lands) Descripted TIC (407 hadres)
				•	Frame (213 bytes) Decrypted TLS (137 bytes)
0	Source Address (i	p.src), 4 bytes			Packets: 1765 · Displayed: 1765 (100.0%) Profile: Default

📕 🖩 🖉 💿 💼 🖹 🛛 🖸 🤇 🖛 🔶 警 🖉 曼 📃 🔍 Q. Q. 🏦

Apply a display filter ... <Ctrl-/>

- +

Time Source Destination Protocol Length Info 1620 18.594474318 162.159.61.4 10.0.2.15 TCP 60 443 - 60510 [ACK] Seq=40361 Ack=16799 Win=65535 I 1621 18.694474390 162.159.61.4 10.0.2.15 TCP 60 443 - 60510 [ACK] Seq=40361 Ack=16958 Win=65535 1622 18.605415235 162.159.61.4 10.0.2.15 DOH 631 Standard query response 6X0000 HTTPS www.cs.virg	Len=0
1621 18.594474390 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 H	Len=0
1622 18.605415235 162.159.61.4 10.0.2.15 DoH 631 Standard query response 0x0000 HTTPS www.cs.virg	inia.edu SOA co
1623 18.606050489 10.0.2.15 162.159.61.4 HTTP2 110 HEADERS[147]: POST /dns-query	
1624 18.606080777 10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 AAAA www.cs.virginia.edu 04	
1625 18.606168058 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 H	
1626 18.606168109 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 I	_en=0
1627 18.606221426 10.0.2.15 162.159.61.4 HTTP2 110 HEADERS[149]: POST /dns-query	
1628 18.606287808 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 H	_en=0
- 1629 18.606305512 10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 A www.cs.virginia.edu OPT	
$1630 \ 18.606380752 \ 162.159.61.4 \\ 10.0.2.15 \\ \text{TCP} \ 60 \ 443 \rightarrow 60510 \ [ACK] \ Seq=40938 \ Ack=17388 \ Win=65535 \ Hermitian (ACK) \ Seq=40938 \ Ack=17388 \ Win=65535 \ Hermitian (ACK) \ Seq=40938 \ Ack=17388 \ Win=65535 \ Hermitian (ACK) \ Win=65535 \ Win=65535 \ Hermitian (ACK) \ Win$	_en=0
1631 18.616270366 162.159.61.4 10.0.2.15 HTTP2 109 HEADERS[147]: 200 OK	
Frame 1629: 213 bytes on wire (1764 bits), 213 bytes contured (1764 bit 6000 52 54 66 12 35 62 68 60 27 cc 86 dc 88 60 45 6	•
$\begin{array}{c} \dots & 0101 = Header Length: : : : : : : : : : : : : : : : : : : $	b0 =
Destination Address: 162.159.61.4 Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 17: $2 = 0 \times 02$	
Transport Layer Security HyperText Transfer Protocol 2	
Frame (213 bytes) Decrypted TLS (137 bytes)	
Source Address (ip.src), 4 bytes Packets: 1765 · Displayed: 1765 (100.0%)	Profile: Default

◢ ■ ∅ ◎ 🚍 🖹 🖄 🗳 ۹ 👄 🛸 🐐 🚽 📃 🗐 ۹. ۹ ۹ 🏦

Apply a display filter ... <Ctrl-/>

1 620 18.99474308 162.159.61.4 10.0.2.15 TCP 1 621 18.99474308 162.159.61.4 10.0.2.15 TCP 1 622 18.695415235 162.159.61.4 10.0.2.15 TCP 1 622 18.6954168958 10.0.2.15 162.159.61.4 10.0.2.15 1 622 18.69512 [ACK] Seq=40361 ACK1 Seq=40361 ACK1 Seq=40363 Ack=17034 Acks.Virginia.edu OPT 60 443 - 60510 [ACK] Seq=40383 Ack=17034 Acks.Virginia.edu OPT 1 623 18.696287808 162.159.61.4 10.0.2.15 TCP 1 623 18.696287808 162.159.61.4 10.0.2.15 TCP 1 633 18.696287808 162.159.61.4 10.0.2.15 TCP 1 1633 18.696287808 162.159.61.4	(11)									
1621 18.99474300 162.159.61.4 10.0.2.15 TCP 60 443 - 66510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0 1622 18.666108564 162.159.61.4 10.0.2.15 DCH 631 81andard query Preponse Wowl.cs.virginia.edu OPT 1622 18.666108564 162.159.61.4 10.0.2.15 TCP DCH Frame 16291 [ACK] Seq=40381 Ack=16958 Win=65535 Len=0 1627 18.666108564 162.159.61.4 10.0.2.15 TCP DCH DCH DCH 1628 18.666221420 16.0.2.15 162.159.61.4 10.0.2.15 TCP 1627 18.666221420 16.0.2.15 162.159.61.4 10.0.2.15 TCP 1628 18.666227808 120.0.2.55 162.159.61.4 10.0.2.15 TCP 1630 18.666238051 162.159.61.4 10.0.2.15 TCP 1631 18.618270366 162.159.61.4 10.0.2.15 TCP 1630 18.606234250 10.0.2.15 TCP TCP 1631 18.618270366 162.159.61.4 10.0.2.15 TCP TCP 1630 18.60	No.	Time	Source	Destination	Protocol	Length Info				-
1622 18.666364899 16.0.2.15 10.0.2.	1620	18.594474318								
1623 18.0606980499 10.0.2.15 162.159.61.4 HTTP2 1624 18.060698077 10.0.2.15 162.159.61.4 10.0.2.15 TCP 1625 18.060168058 162.159.61.4 10.0.2.15 TCP 1627 18.060221420 10.0.2.15 162.159.61.4 10.0.2.15 TCP 1628 18.060221420 10.0.2.15 162.159.61.4 10.0.2.15 TCP 1628 18.060221420 10.0.2.15 162.159.61.4 10.0.2.15 TCP 1628 18.060221420 10.0.2.15 162.159.61.4 10.0.2.15 TCP 1633 18.0602207808 162.159.61.4 10.0.2.15 TCP 1633 18.060230752 162.159.61.4 10.0.2.15 TCP 1633 18.060230752 162.159.61.4 10.0.2.15 TCP 1633 18.060230752 162.159.61.4 10.0.2.15 TCP 1631 18.01270366 162.159.61.4 10.0.2.15 TCP 1631 18.01270366 162.159.61.4 10.0.2.15 TCP 1631 18.01270366 162.159.61.4 10.0.2.15 TCP 1600 18.060030752 162.159.61.4 10.0.2.15 TCP 1600 18.06000000 CF CPS CSS ystemtec.cc.86:dC), DSC YSC YS (SOP CSC SSO, ECN: NOt-ECT) TOTAL Length: 197 TCP 1040 11:190 1040 18 17 4 bi 57 25 95 6.42 21 15 93	1621	18.594474390	162.159.61.4	10.0.2.15	TCP					
1624 18.66688977 10.0.2.15 162.159.61.4 DoH 213 standard query 0x0000 AAA www.cs.vtrginia.edu OPT 1625 18.666180169 162.159.61.4 10.0.2.15 TCP 1626 18.666180109 162.159.61.4 10.0.2.15 TCP 1626 18.666180109 162.159.61.4 10.0.2.15 TCP 1628 18.666287026 162.159.61.4 10.0.2.15 TCP 1630 18.666830752 162.159.61.4 10.0.2.15 TCP 1631 18.616270366 162.159.61.4 10.0.2.15 TCP 1641 Therme TProtocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4 00H 00F 76 0F 05 26 0F 02 0F 05 0F 26 0F 26 0F 04 00 02 0F 03 0F 07 0F 74 06 04 06 07 0F 03 00 02 0F 03 0F 08 0F 76 05 0F 06 0F 05 0F 02 0F 05									www.cs.virginia	a.edu SOA co
1625 18.606168095 162.159.61.4 10.0.2.15 TCP 1626 18.606168095 162.159.61.4 100.2.15 TCP 1627 18.606221426 10.0.2.15 162.159.61.4 100.2.15 1628 18.606287086 162.159.61.4 100.2.15 TCP 1630 18.606287086 162.159.61.4 100.2.15 TCP 1631 18.606287086 162.159.61.4 10.0.2.15 TCP 1631 18.606380751 262.159.61.4 10.0.2.15 TCP 1631 18.606380752 162.159.61.4 10.0.2.15 TCP Threme 1529: 213 bytes on wire (1704 bits), 213 bytes captured (1704, bits) 213 bytes captured (1704 bits) 213 bytes captured (1704 bits) 0100 = Version: 4 10.0.2.15, DSI: 162.159.61.4 10.0.2.15, DSI: 162.159.61.4 10.0.2.15 0100 = Version: 4 10.0.2.15, DSI: 162.159.61.4 10.0.2.15, DSI: 162.159.61.4 10.0.2.15 0100 = Version: 4 10.0.2.15, DSI: 162.159.61.4 10.0.2.15, DSI: 162.159.61.4 10.0.2.15 0101 Header Lengthi 120 bytes (5) 0116 renetiated Services Field: 8x00 (DSCP: CS9, ECN: Not-ECT) 0060 for 6 50 80 40 17 63 80 40 92 20 21 59 32 at 55 67 7 11.0.2.15 95 62.2 21 15 93 21 15 95 7.2. 15 95 60 62 21 15 93 21 15 95 7.2. 15 95 60 62 21 15 93 21 15 95 61 -4 10 10 -5 -7 .5 Smytes 00000 0000 0000 0000 Fragment 0ffset: 0										
1620 18.0001080109 162.159.61.4 10.0.2.15 TCP 1627 18.0002126 10.0.2.15 102.159.61.4 10.0.2.15 1628 18.00020512 10.0.2.215 102.215.0.1.4 10.0.2.15 1630 18.00020512 10.0.2.215 102.215.0.1.4 10.0.2.15 1631 18.010270366 122.159.61.4 10.0.2.15 TCP 1627 18.00020512 10.0.2.715 10.0.2.15 TCP 1631 18.010270366 122.159.61.4 10.0.2.15 TCP 1627 18.00020612 10.0.2.715 10.0.2.15 TCP 1631 18.010270366 122.159.61.4 10.0.2.15 TCP 1627 18.00020612 10.0.2.715 TCP TCP 1628 18.00020612 10.0.2.715 TCP TCP 1629 18.00020612 10.0.2.715 TCP TCP 1620 18.00020612 10.0.2.715 TCP TCP 1620 18.00020612 10.0.2.715 TCP TCP 1610 18.00020612 10.0.2.715 TCP TCP 1610 18.00020612 10.0.2.715 TCP TCP										
1627 18.606227426 10.0.2.15 162.159.61.4 100.2.15 17000000000000000000000000000000000000						60 443 → 60510 [
Frame 1629 18.6063807512 18.6.9.2.15 162.159.61.4 10.6.2.15 THTP2 1631 18.616270366 162.159.61.4 10.6.2.15 THTP2 164 bits, 060580752 162.159.61.4 10.6.2.15 THTP2 164 bits, 061680752 162.159.61.4 162.159.6						$60 \ 443 \rightarrow 60510$ [Seq=4093		3 Win=65535 Len:	=0
Frame 1629 18.6063807512 18.6.9.2.15 162.159.61.4 10.6.2.15 THTP2 1631 18.616270366 162.159.61.4 10.6.2.15 THTP2 164 bits, 060580752 162.159.61.4 10.6.2.15 THTP2 164 bits, 061680752 162.159.61.4 162.159.6						protoco	POST /dns-qu			
1630 18.060380752 162.159.61.4 10.0.2.15 TCP HTTP2 HTTP2 Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) Prame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) Prame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits), 200 cr do 70 bits, 200 cr do 70 bit						prococo				=0
1 1031 18.616270366 162.159.61.4 10.0.2.15 HTTP2 Frame 1629: 213 bytes on wire (1764 bits), 213 bytes captured (1764 bit, Ethernet II, Src: PCSSystemete.cc:86:dc (08:08:27:cc:86:dc), Dst: 52:57 bit for entiated Services Field: 80:08:27:cc:86:dc), Dst: 52:57 bit of a data discrete the services field: 80:08:27:cc:86:dc), Dst: 52:57 bit of a data discrete the services field: 80:08:27:cc:86:dc), Dst: 52:57 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 80:08:27:10: CS9, ECN: Not-ECT) Total Length: 199 Identification: 8xd07b (53371) > 0100 = Flags: 6x2, Don't fragment 0 00000 0000 0000 = Fragment Offset: 0 Time to Live: 64 Protocol: TCP (6) Header checksum status: Unverified] Destination Address: 162.159.61.4 Transport Layer Security HyperFext Transfer Protocol 2 Security HyperFext Transfer Protocol 2 Decrypted TL5(137 bytes)						213 Standard quer	ry 0x0000 A ₩₩	w.cs.virgi	nia.edu OPT	
Frame 1629: 213 bytes on wire (1764 bits), 213 bytes captured (1764 bit), Ethernet II, Src: PCSSystemete.cc:68:dc (08:08:27:cc:88:dc), Dst: 52:54 Differentiat II, Src: PCSSystemete.cc:68:dc (08:08:27:cc:88:dc), Dst: 52:54 0100 00 c7 d0 7b 40 00 40 66 7e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 60 00 90 91 03 03 00 9a 16 c6 b5 b2 4e (8 00 00 52 c7 c7 a1 0.2.2.15 0, 01 17 72 94 49 37 10 f5 c2 6f 						$60 \ 443 \rightarrow 60510$	[ACK] Seq=4093	38 Ack=1738	8 Win=65535 Len:	
Frame 1629: 213 bytes on wire (1764 bits), 213 bytes captured (1764 bit), Ethernet II, Src: PCSSystemete.cc:68:dc (08:08:27:cc:88:dc), Dst: 52:54 Differentiat II, Src: PCSSystemete.cc:68:dc (08:08:27:cc:88:dc), Dst: 52:54 0100 00 c7 d0 7b 40 00 40 66 7e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 c7 d0 7b 40 00 40 66 07e 03 0n 00 02 01 a2 9f 0100 00 60 00 90 91 03 03 00 9a 16 c6 b5 b2 4e (8 00 00 52 c7 c7 a1 0.2.2.15 0, 01 17 72 94 49 37 10 f5 c2 6f 	1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	the highes	st-laver	protoc	ol decod	ed
<pre>> Ethernet II, Src: PCSSystemete_cc:08:dc (08:00:22:cc:08:dc), Dst: 52:54 > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS9, ECN: Not-ECT) Total Length: 199 Identification: 0xd07b (53371) > 010 = Prame(CS3, Don't fragment 0000 0000 00000 = Fragment Offset: 0 Time to Live: 64 Protocol: TCP (6) Header Checksum: 0xr081 (validation disabled] (Header Checksum: 0xr081 (validation disabled] (Header Checksum: 0xr081 (validation disabled] (Header Checksum: 0xr081 (validation disabled] Header Checksum: 0xr081 (validation disabled) Header Checksum: 0xr081 (validation disabled) Head</pre>	4					the monor	ou layor	p. 0 0 0 0		
<pre>> Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172 > Transport Layer Security + HyperText Transfer Protocol 2 </pre>	✓ Intern 010 > Dif Tot Idd > 010 Tir Pro Hea [H4]	het Protocol V 10 = Vers: . 0101 = Head ferentiated Se cal Length: 199 0 0000 0000 0000 00 10 to Live: 64 tocol: TCP (6 der Checksum: cader checksum irce Address:	ersion 4, Src: 10.0. ion: 4 er Length: 20 bytes ervices Field: 0x00 0 0x007b (53371) s: 0X2, Don't fragment 000 = Fragment Offset 0 0x7e03 [validation of status: Unverified] 10.0.2.15	2.15, Dst: 162.159.61. (5) (DSCP: CS0, ECN: Not-Er nt t: 0	4	0020 3d 04 ec 5d 0030 f9 0c ec 6l 0040 b3 68 7c 0c 0050 ab af 6a at 0060 db 3d da 4f 6a 0070 db 44 14 ff 0080 1b d4 18 ff 0090 d6 9e ec 4d 0080 35 f7 d5 ef 0080 cf 9e 2c db de 0080 cf f6 92 2d db de 0080 bf 9e 2c db de de db db	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	90 0d 0a 03 00 9a 88 6a 55 72 94 49 1c 8c 53 05 7f ad 95 0c a2 03 b6 c4 d1 a2 50 70 d8 69	60 df eb 50 18 16 c6 b5 b2 4e 92 ae f5 of2 de 92 ae f5 of2 off ab f4 ce 36 fc ab f4 ce 36 rc 21 15 93 21 13 8b ab bc ce ee 2b 44 31 ab 66 f0 1e f6 3a 64	=
HyperText Transfer Protocol 2 Frame (213 bytes)				: 60510 Det Port: 443	Seg: 17	re				
HyperText Transfer Protocol 2 Frame (213 bytes) Decrypted TLS (137 bytes)				. 00510, D3t F01t. 443	, 504. 1/					
Frame (213 bytes)						4				
Source Address (ip.src), 4 bytes Packets: 1765 · Displayed: 1765 (100.0%) Profile: Default	4				•	Frame (213 bytes)	Decrypted TLS	(137 bytes)		
	0 7	Source Address (i	p.src), 4 bytes				Packets: 1765	· Displayed: 17	765 (100.0%)	Profile: Default

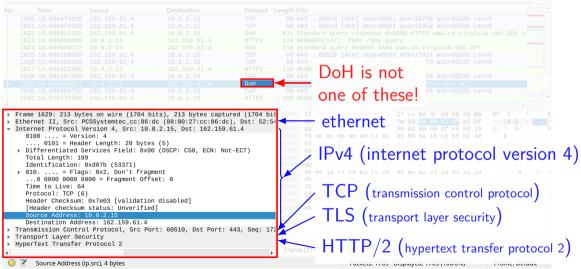
_ ■ 2 ◎ = 1 ≥ 0 < ← ⇒ ≌ 7 ± , = 0 < < 1

					Length Info 60 443 - 60510 [ACK] Sec=40361 Ack=16799 Win=65535 Len=0	
				DoH		
						~
 Intern 010 Dii Toi Ide 010 Toi Toi Toi Hea 	net Protocol V 00 = Vers . 0101 = Head fferentiated S cal Length: 19 entification: 0 = Flag 0. 0000 0000 0 ne to Live: 64 otocol: TCP (6 ader Checksum:	ersion 4, Src: 10 ion: 4 er Length: 20 byt ervices Field: 0x 0xd07b (53371) s: 0x2, Don't fra 000 = Fragment Of) 0x7e03 [validati	00 (DSCP: CSO, ECN: No gment fset: 0 on disabled]	.61.4	ab IPv4 (internet protocol vers	sion
		status: Unverifi	.ed]			
	urce Address:				TLS (transport layer security)	
		ess: 162.159.61.4		440 0000 47		
			Port: 60510, Dst Port:	443, Seq: 17		
	port Layer Sec					
▶ нуper	Text Transfer	PIOLOCOL Z			Frame (21: HTTP/2 (hypertext transfer prot	locol
4				•		.0001
0 7	Source Address (i	p.src), 4 bytes			Packets: 1765 - Displayed: 1765 (100.0%) Profile: Defa	uit

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

◢ ■ ◢ ◎ ⊨ 🗎 🛛 🏹 । ९ 🗢 🛸 🖀 🖌 📃 📃 €, ९ ९ 🏦

Apply a display filter ... <Ctrl-/>



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

_ ■ ⊿ ◎ 🖿 🖹 🛛 | ♀ ᆃ ≱ 🗍 🖳 🔍 ♀ ♀ 🏦

Apply a display filter ... <Ctrl-/>

1630 18.60638 1631 18.61627 Frame 1629: 21 Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT/ > Domain Name	74300 162,159,61,4 1525 162,159,61,4 50480 10,0,2,15 6077 10,0,2,15 60680 162,159,61,4 6109 162,159,61,4 74680 162,159,61,4 10752 162,159,61,4 10752 162,159,61,4 13 bytes on wire (1704 Src: PCSSystemtec_cc:08 0col Version 4, Src: 1 Control Protocol, Src Fer Security	6:dc (08:00:27:cc:86:d 0.0.2.15, Dst: 162.159	dc), Dst: 52: 9.61.4	$\begin{array}{c} \begin{array}{c} \begin{array}{c} 0e \\ 443 \\ - \ 0e518 \\ - $
1622 18 60541 1623 18 6065 1624 18 6060 1625 18 60616 1626 18 60616 1627 18 6062 1628 18 60626 1629 18 60628 1639 18 60628 1649	15235 162.159.61.4 58409 1.0.2.15 8077 10.0.2.15 80161 162.159.61.4 80109 162.159.61.4 80109 162.159.61.4 80109 162.159.61.4 91010 162.159.61.4 91010 162.159.61.4 91010 162.159.61.4 91010 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91052 162.159.61.4 91050 162.159.61.4 91050 162.159.61.4 91050 162.159.61.4 91050 162.159.61.4 91050	10.0.2.15 102.159.61.4 102.159.61.4 10.0.2.15 102.2.15 102.159.61.4 102.2.15 102.159.61.4 102.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (00:00:27:cc:86:d) 0.0.2.15	DoH HTTP2 DOH TCP TCP HTTP2 DOH TCP HTTP2 tured (1704 t dc), Dst: 52: 9.61.4	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu S0A ct 110 HACMERS[147]: POST /dns.query 213 Standard query 0x0000 AAA www.cs.virginia.edu OPT 60 443 0 0516 00 443 00 443 00 00 00 443 00 00 00 443 00 00 00 443 00 00 00 443 00 00 00 443 00 00 00 443 00 443 00 00 00 443 00 00 00 443 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1021 18.00005 1024 18.0000 1025 18.0011 1026 18.0011 1027 18.0022 1028 18.0022 1029 18.0022 1039 18.0023 1031 18.0027 Frame 1629: 21 Ethernet JI, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT > Domain Name	86480 10.0.2.15 8677 10.0.2.15 8678 162.159.61.4 86100 162.159.61.4 8768 162.159.61.4 90752 162.159.61.4 90752 162.159.61.4 90752 162.159.61.4 90656 152.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90560 162.159.61.4 90570 162.159.61.4 9050 162.159.61.4 9050 162.159.61.4 9050 162.159.61.4 9050 <	162.150.61.4 162.150.61.4 16.0.2.15 162.150.61.4 10.0.2.15 10.0.2.15 10.0.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d) 0.0.2.15	HTTP2 DOH TCP TCP TCP DOH TCP HTTP2 TCP HTTP2 tured (1704 <u></u> dc), Dst: 52: 9.61.4	110 HEADERS[147]: POST //dns-query 213 Standard query 9K9889 AAA www.cs.virginia.edu OPT 60 443 - 60518 [ACK] Seq=46938 Ack=17014 Win=65535 Len=0 60 443 - 60518 [ACK] Seq=46938 Ack=17173 Win=65535 Len=0 110 HEADERS[140]: BOST //dns query 60 443 - 60518 [ACK] Seq=46938 Ack=17173 Win=65535 Len=0 100 HEADERS[140]: BOST //dns query 60 443 - 0064 [BOST //dns query 60 443 [BOST //dns quer
1624 18. 6668 1625 18. 6661 1626 18. 6661 1627 18. 6662 1628 18. 6662 1628 18. 6662 1629 18. 6662 1639 18. 6662 1639 18. 6662 1639 18. 6662 Frame 1629: 21 Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT > Domain Name	80777 10.0.2.15 80698 162.159.61.4 81109 162.159.61.4 81426 10.0.2.15 87086 162.159.61.4 80587 10.0.2.15 80758 162.159.61.4 80858 10.0.2.15 80752 162.159.61.4 13 bytes on wire (1704 Src: PCSSystemtec_cc:86 Scol Version 4, Src: IC Cool Version 4, Src: Fer For Security	162.150.61.4 10.0.2.15 102.159.61.4 102.159.61.4 102.155 102.155 10.2.15 10.0.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d) 0.0.2.15, bt: 162.159	DoH TCP TCP HTTP2 TCP DOH TCP HTTP2 tured (1704 1 dc), Dst: 52: 9.61.4	213 Standard query 0x0000 AAA www.cs.virginia.edu 0PT 60 443 - 06516 [Ack] Seq=40938 Ack=17173 Win=65535 Len=0 60 443 - 06516 [Ack] Seq=40938 Ack=17173 Win=65535 Len=0 10 HEADEWEI1410 DOH = DNS over HTTPS 00 HTTPS 10 HEADEWEI1411 200 0K - 00 00 00 00 00 10 HEADEWEI1411 200 0K - 00 00 00 00 00 00
1625 18.00016 1626 18.00016 1627 18.00020 1628 18.00020 1630 18.00020 1630 18.00020 1630 18.00020 Frame 1629: 21 Ethernet II, S Internet Proto Transport Laye HyperText Tran > Stream: DAT > Dream Name	B0658 162,159,61,4 B0109 162,159,61,4 21426 10,9,2,15 B0762 162,159,61,4 B0752 162,159,61,4 B0764 162,159,61,4 Strip PCSSystemtec_cc:86 Coll Version 4, Src: PCSSystemtec, Ac: 86 Coll Version 4, Src: PCSSystemtec, BC: 86 Coll Version 4, Src: PCSSystemtec, BC: 86 Coll Version 4, Src: PCSSystemtec, BC: 86 Coll Version 4, Src: PCS	10.0.2.15 10.2.2.15 102.159.61.4 10.0.2.15 10.0.2.15 10.0.2.15 10.0.2.15 10.0.2.15 5:dc (08:00:27:cc:86:d) 0.0.2.15 t: 102.15	TCP TCP TCP DOH TCP HTTP2 tured (1704 t dc), Dst: 52: 9.61.4	69 443 - 69518 [ACK] Seq=40938 Ack=17014 kin=65535 Len=0 19 HEADERS(1401) 0057 4ins murry 60 443 DoH = DNS over HTTPS 10 HEADERS(141) 1 200 0K 10 HEADERS(147) 200 0K 10
1626 18.0616 1627 18.0622 1628 18.0628 1629 19.0628 1639 19.0628 1631 18.0628 1631 18.0627 Frame 1629: 21 Ethernet II, S Internet Proto Transport Laye HyperText Tran > Stream: DAT > Dream Name	68100 162.159.61.4 21426 68.0.2.15 7088 162.159.61.4 15552 10.0.2.15 160752 162.159.61.4 70366 162.159.61.4 13 bytes on wire (1704 Scol Version 4, Src: 16 col Version 4, Src: 16 col Version 4, Src: 17 col Version 4, Src: 18 bytes on wire (1704	10.0.2.15 162.159.61.4 10.0.2.15 102.159.63.4 10.0.2.15 10.0.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d 0.0.2.15, Dst: 162.159	TCP HTTP2 TCP DoH TCP HTTP2 tured (1704 t dc), Dst: 52: 9.61.4	60 443 _ 06510 [Ack] 56940938 Acket27173 Wine65535 Len=0 110 HEADENETATOL 000 / 00
1627 18.60622 1628 18.60620 1639 18.60620 1639 18.60620 Frame 1629: 21 Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT/ > Domain Name	21426 10.0.2.15 8708 102.159.61.4 8708 102.159.61.4 87072 102.159.61.4 13 bytes on wire (1704 87c: PCSSystemtec_cc:08 0col Version 4, Src: 18 Control Protocol, Src Fer Security	162.159.61.4 10.0.2.15 102.159.63.4 10.0.2.15 10.0.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d 0.0.2.15, Dst: 162.159	HTTP2 TCP DoH TCP HTTP2 tured (1704 t dc), Dst: 52: 9.61.4	
1628 18.66628 1029 18.66638 1639 18.66638 1631 18.61627 Frame 1629: 21 Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT/ > Domain Name	87808 162.159.61.4 9551 10.052.15 80752 162.159.61.4 78366 162.159.61.4 13 bytes on wire (1704 5rc: PCSSystemtec_cc:86 pcol Version 4, Src: 16 Control Protocol, Src F er Security	10.0.2.15 162.159.61.4 10.0.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d 9.0.2.15, Dst: 162.159	TCP DoH TCP HTTP2 tured (1704 & dc), Dst: 52: 9.61.4	
1630 18.0058 1631 18.01627 Frame 1629: 21 Ethernet II, S Internet Proto Transport Laye HyperText Tran > Stream: DAT/ > Domain Name	1512 10.0.2.15 80752 162.159.61.4 70366 162.159.61.4 13 bytes on wire (1704 Src: PCSSystemtec_cc:86 pool Version 4, Src: 16 Control Protocol, Src F er Security	162.159.61.4 10.0.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d 0.0.2.15, Dst: 162.159	DOH TCP HTTP2 tured (1704 t dc), Dst: 52: 9.61.4	
1630 18.60638 1631 18.61627 Frame 1629: 21 Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT/ > Domain Name	80752 162.159.61.4 70366 162.159.61.4 13 bytes on wire (1704 Src: PCSSystemtec_cc:86 ocol Version 4, Src: 16 Control Protocol, Src F er Security	10.0.2.15 10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d 0.0.2.15, Dst: 162.159	TCP HTTP2 tured (1704 ≹_ dc), Dst: 52: 9.61.4	
Frame 1629: 21 Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT/ > Domain Name	70366 162.159.61.4 13 bytes on wire (1704 Src: PCSSystemtec_cc:86 ocol Version 4, Src: 16 Control Protocol, Src F er Security	10.0.2.15 bits), 213 bytes capt 5:dc (08:00:27:cc:86:d 5.0.2.15, Dst: 162.159	HTTP2 tured (1704 t dc), Dst: 52: 9.61.4	
Frame 1629: 21 Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DAT/ > Domain Name	13 bytes on wire (1704 Src: PCSSystemtec_cc:86 ocol Version 4, Src: 16 Control Protocol, Src F er Security	bits), 213 bytes capt 5:dc (08:00:27:cc:86:d 9.0.2.15, Dst: 162.159	dc), Dst: 52: 9.61.4	
Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DATJ > Domain Name	Src: PCSSystemtec_cc:86 ocol Version 4, Src: 10 Control Protocol, Src F er Security	6:dc (08:00:27:cc:86:d 0.0.2.15, Dst: 162.159	dc), Dst: 52: 9.61.4	010 00 01 00 01 01 01 01 01 01 01 01 02 03 73 08 76 09 72 01 01 0W WICS VI
Ethernet II, S Internet Proto Transmission C Transport Laye HyperText Tran > Stream: DATJ > Domain Name	Src: PCSSystemtec_cc:86 ocol Version 4, Src: 10 Control Protocol, Src F er Security	6:dc (08:00:27:cc:86:d 0.0.2.15, Dst: 162.159	dc), Dst: 52: 9.61.4	010 00 01 00 01 01 01 01 01 01 01 01 02 03 73 08 76 09 72 01 01 0W WICS VI
 Flags: 0> Questions Answer RF Authority Additions 	FA, Stream ID: 149, Len e System (query) ion ID: 0x0000 0x0100 Standard query IS: 1 RRS: 0	gth 128		TCP (transmission control protocol) TLS (transport layer security) HTTP/2 (hypertext transfer protocol 2)
	s.virginia.edu: type A me: www.cs.virginia.edu			DNS (domain name system)

Apply a display filter ... <Ctrl-/>

o.	Time	Source	Destination	Protocol	Length Info			
1620	18.594474318	162.159.61.4	10.0.2.15	TCP		CK] Seq=40361 Ack=167		
	. 18.594474390	162.159.61.4	10.0.2.15	TCP		CK] Seq=40361 Ack=169		
	18.605415235		10.0.2.15	DoH		response 0x0000 HTTP	S www.cs.virginia	a.edu SOA co
	18.606050489		162.159.61.4	HTTP2	110 HEADERS[147]:			
	18.606080777	10.0.2.15	162.159.61.4	DoH		0x0000 AAAA www.cs.v		
	18.606168058		10.0.2.15	TCP		CK] Seq=40938 Ack=170		
	5 18.606168109		10.0.2.15	TCP		CK] Seq=40938 Ack=171	73 Win=65535 Len	=0
	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]:			
	18.606287808		10.0.2.15	TCP		CK] Seq=40938 Ack=172		=0
	18.606305512		162.159.61.4	DoH		0x0000 A www.cs.virg		
	18.606380752		10.0.2.15	TCP		CK] Seq=40938 Ack=173	88 Win=65535 Len	=0
1631	. 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]:	200 OK		
								•
Eramo	1620 - 213 byt	es on wire (1704 bi	ite), 213 bytes captur	ed (1704 bit		35 02 08 00 27 cc 86		RT++5+++ '+++
Ether	net II, Src: P	CSSystemtec_cc:86:c	dc (08:00:27:cc:86:dc)	, Dst: 52:54	0010 00 c7 d0 7b	40 00 40 06 7e 03 0a	00 02 Of a2 9f	···{@·@· ~···
			0.2.15, Dst: 162.159.6		0020 3d 04 ec 5e		60 df eb 50 18	=··^·×X/ ···`
Trans	mission Contro	l Protocol, Src Por	rt: 60510, Dst Port: 4	43, Seq: 172	0030 f9 0c ec 6b	00 00 17 03 03 00 9a	16 c6 b5 b2 4e	· · · k · · · · · · · · · ·
	port Layer Sec				0040 b3 68 7c 03		92 ae f5 0f 2c	·h ·^·W· ·jU··
Hyper	Text Transfer	Protocol 2			0050 ab af 6a a3		37 10 f5 e2 Of	··j·j··· r·I7·
							eb 6d 79 40 b0	·=··?··S·r
					0070 db 44 14 fb		ab f4 ce 36 7c	· D · · · · M4 · · · · ·
					0080 1b d4 18 f1		21 15 93 21 13	· · · · · % · · · !
						5b d1 cc 83 03 b6 c4		···H[···
						ad 6e 7d 5b d1 a2 50		5 · · · n}[· · P+[
						95 ca a2 a0 70 d8 69		••••• p·i··
					00c0 be 2b 4e 5a		71 f6 10 a4 f8	·+NZI·B· MQ·q
					00d0 d6 04 d0 14	7b		· · · · {
					4			
					Frame (213 bytes)	Decrypted TLS (137 bytes)		
				Þ		,		
) 🍸	Ethernet (eth), 14	bytes				Packets: 1765 · Displayed:	765 (100.0%)	Profile: Default

Apply a display filter ... <Ctrl-/>

o. 🕺	Time	Source	Destination	Protocol	Length Info			
	18.594474318	162.159.61.4	10.0.2.15	TCP		ACK] Seq=40361 Ack=167		
	18.594474390	162.159.61.4	10.0.2.15	TCP		ACK] Seq=40361 Ack=169		
	18.605415235	162.159.61.4	10.0.2.15	DoH		/ response 0x0000 HTTP	S www.cs.virginia	.edu SOA co
	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]:			
	18.606080777	10.0.2.15	162.159.61.4	DoH		/ 0x0000 AAAA www.cs.v		
	18.606168058	162.159.61.4	10.0.2.15	TCP		ACK] Seq=40938 Ack=170		
	18.606168109	162.159.61.4	10.0.2.15	TCP		ACK] Seq=40938 Ack=171	73 Win=65535 Len=	0
	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]:			
	18.606287808		10.0.2.15	TCP		ACK] Seq=40938 Ack=172		:0
	18.606305512		162.159.61.4	DoH		/ 0x0000 A www.cs.virg		
	18.606380752		10.0.2.15	TCP		ACK] Seq=40938 Ack=173	88 Win=65535 Len=	0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]:	200 OK		
								•
Frame	1629: 213 byt	es on wire (1704 bit	s), 213 bytes capture	d (1704 bi	t 0000 52 54 00 12	35 02 08 00 27 cc 86	dc 08 00 45 00	RT++5+++ '+++
			(08:00:27:cc:86:dc),			40 00 40 06 7e 03 0a	00 02 0f a2 9f	····{0·0· ~···
Intern	et Protocol V	ersion 4, Src: 10.0.	2.15, Dst: 162.159.61	.4	0020 3d 04 ec 5e	01 bb 58 2f 90 0d 0a	60 df eb 50 18	= · · ^ · · X/ · · · ` ·
Transm	ission Contro	l Protocol, Src Port	: 60510, Dst Port: 44	3, Seq: 17	2 0030 f9 0c ec 6b	00 00 17 03 03 00 9a	16 c6 b5 b2 4e	· · · k · · · · · · · · ·
Transp	ort Layer Sec	urity			0040 b3 68 7c 03	5e af 57 1f 88 6a 55	92 ae f5 0f 2c	·h ·^·W· ·iU··
HyperT	ext Transfer	Protocol 2			0050 ab af 6a a3	6a 13 97 1f 72 94 49	37 10 f5 e2 Of	· · · j · j · · · · r · I7
					0060 db 3d da 88	ab 3f 98 91 1c 8c 53	eb 6d 79 40 b0	-=··?···S·r
					0070 db 44 14 fb	9c fc 4d 34 05 7f ad	ab f4 ce 36 7c	·D····M4 ····
					0080 1b d4 18 f1	f4 b3 f5 25 95 0c a2	21 15 93 21 13	% ! .
					0090 d6 9e ec 48	5b d1 cc 83 03 b6 c4	8b ab 0b c0 ee	H[
					00a0 35 f7 d5 e2	ad 6e 7d 5b d1 a2 50	2b 44 31 ab 36	5 · · · · n}[· · · P+D
					00b0 cf f0 93 2d	95 ca a2 a0 70 d8 69	f0 1e f0 3a 64	p.i.
						49 9c 42 f3 4d 51 f9		+NZI·B· MO·a
					00d0 d6 04 d0 14			
					•			
				Þ	Frame (213 bytes)	Decrypted TLS (137 bytes)		

◢ ■ ∅ ◎ 🚍 🖹 🛛 🗳 ۹ 👄 🛎 春 🖢 🚍 🖲 ۹ ۹ ۹ 🏦

Apply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol L	ength Info	
	0 18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0	
162	1 18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0 🛛 🗕	_
	2 18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c	
	3 18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query	
	4 18.606080777	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT	
	5 18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0	
	6 18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0	
	7 18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query	
	8 18.606287808	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0	
	9 18.606305512		162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT	
	0 18.606380752	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0	
163	1 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK	
Fram	e 1629: 213 byt	es on wire (1704 bit:	s), 213 bytes capture	ed (1704 bit	0000 52 54 00 12 35 02 08 00 27 cc 86 dc 08 00 45 00 RT . 5	
Ethe	rnet TT_Src: P	CSSystemter cc:86.dc	(08.00.27.cc.86.dc)	Dst : 52:54	0010 00 c7 d0 7b 40 00 40 06 7e 03 0a 00 02 0f a2 9f ····{@·@· ~·	
Inte	rnet Protocol V	ersion 4. Src: 10.0.	2.15. Dst: 162.159.61	1.4	0020 3d 04 ec 5e 01 bb 58 2f 90 0d 0a 60 df eb 50 18 = 1 ^ · · · X/ · ·	1 A Y
			2.15. Dst: 162.159.61 : 60510, Dst Port: 44		0020 3d 04 ec 5e 01 bb 58 2f 90 0d 0a 60 df eb 50 18 =: ·^X/ ·· 0030 f9 0c ec 6b 00 00 17 03 03 00 9a 16 c6 b5 b2 4e ···· k········	
Tran		l Protocol, Src Port			0030 f9 0c ec 6b 00 00 17 03 03 00 9a 16 c6 b5 b2 4ek 0040 b3 68 7c 03 5e af 57 1f 88 6a 55 92 ae f5 0f 2ch .^.w	jU∘
Tran Tran	smission Contro	l Protocol, Src Port urity			0030 19 0C cc b5 00 01 70 03 00 9a 16 c6 b5 b2 ce k.	jU .I7
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			0030 19 0c 0c 0c 00 00 17 03 03 00 9a 16 c6 b5 b2 4e ········· 0040 b3 68 7c 08 6a 55 92 ae f5 67 c h ····W····· j j j j j j j j j j r j j r j j r j j r j j r r j j r r j j r r j j r r j j r r j j r r j r r j r r j r r i j r r i j i r i j i i j i j i j i j i	jU I7 S
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			0030 150 Gc 0c 6b 09 00 00 3 00 90 10 c cb b2 4	jU I7 S I
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			0030 F9 0C 0C 60 00 01 70 30 90 9a 16 c6 b5 b2 4e ··········· ····· </td <td>jU I7 S I</td>	jU I7 S I
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			0030 150 Cc cc bb 090 01 cc cb bb cb cb <th< td=""><td>jU I7 S r</td></th<>	jU I7 S r
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			0030 F9 0C 0C 60 00 01 70 30 90 9a 16 c6 b5 b2 4e ··········· ····· </td <td>jU I7 S I</td>	jU I7 S I
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			0030 150 Cc cc bb 090 01 cc cb bb cb cb <th< td=""><td>jU I7 S </td></th<>	jU I7 S
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	jU I7 S !
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	jU I7 S
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	jU I7 S !
Tran Tran	smission Contro sport Layer Sec	l Protocol, Src Port urity			0030 150 6C 0c 6b 00 00 17 03 03 00 9a 16 C6 b5 b2 4e	jU I7 S !

Apply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol Le	ength Info	
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0	_
	l 18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0 🗕	_
	2 18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co	
	3 18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query	_
	18.606080777	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT	
	5 18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0	
	3 18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0	
	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query	
	3 18.606287808		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0	
	9 18.606305512		162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT	
	18.606380752	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0	
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK	
Ether Inter Trans Trans	net II, Src: P net Protocol V		(08:00:27:cc:86:dc), .15, Dst: 162.159.61.	Dst: 52:54 4	0010 00 7 00 70 70 0	U - 17
					0060 db 3d da 88 ab 3f 98 91 1c 8c 53 eb 6d 79 40 b0	
					0080 1b d4 18 f1 f4 b3 f5 25 95 0c a2 21 15 93 21 13%	11
					0090 d6 9e ec 48 5b d1 cc 83 03 b6 c4 8b ab 0b c0 ee	
					00a0 35 f7 d5 e2 ad 6e 7d 5b d1 a2 50 2b 44 31 ab 36 5n}[]	
					00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64 p.:	i.
					00c0 be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8 +NZI B MO) · a
					00d0 d6 04 d0 14 7b	
					4 Frame (213 bytes) Decrypted TLS (137 bytes)	
					Frame (213 bytes) Decrypted TLS (137 bytes)	
				•		

Apply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol L	ength Info
1620	9 18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
	1 18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
	2 18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
	3 18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query
	4 18.606080777	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
	5 18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
	6 18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
	7 18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query
	8 18.606287808	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
	9 18.606305512		162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT
	9 18.606380752	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
163:	1 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK
			its), 213 bytes captu		
			dc (08:00:27:cc:86:dc		
			0.2.15, Dst: 162.159.		0020 3d 04 ec 5e 01 bb 58 2f 90 0d 0a 60 df eb 50 18 = ·^··X/ ···
			ort: 60510, Dst Port:	443, Sea: 172	
	sport Layer Sec				0040 b3 68 7c 03 5e af 57 1f 88 6a 55 92 ae f5 0f 2c h A.W. jU
нурег	Text Transfer	Protocol 2			0050 ab af 6a a3 6a 13 97 1f 72 94 49 37 10 f5 e2 0f ··j·j·· r·I
					0060 db 3d da 88 ab 3f 98 91 1c 8c 53 eb 6d 79 40 b0 -=?S
					0070 db 44 14 fb 9c fc 4d 34 05 7f ad ab f4 ce 36 7c D M4 0080 1b d4 18 f1 f4 b3 f5 25 95 0c a2 21 15 93 21 13%
					0090 d6 9e ec 48 5b d1 cc 83 03 b6 c4 8b ab 0b c0 ee
					00a0 35 f7 d5 e2 ad 6e 7d 5b d1 a2 50 2b 44 31 ab 36 5 · · · n}[· P
					00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64
					00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64 ······ p i 00c0 be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8 ···NZI·B· MQ·
					00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64
					00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64 ······ p i 00c0 be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8 ···NZI·B· MQ·
					00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64 ······ p i 00c0 be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8 ···NZI·B· MQ·
					00b0 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64 ······ p i 00c0 be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8 ···NZI·B· MQ·
					06b9 cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64

Apply a display filter ... <Ctrl-/>

lo.	Time	Source	Destination	Protocol L	ength Info			
	0 18.594474318	162.159.61.4	10.0.2.15	TCP		[ACK] Seq=40361 Ack=16		
	1 18.594474390	162.159.61.4	10.0.2.15	TCP		ACK] Seq=40361 Ack=169		
	2 18.605415235	162.159.61.4	10.0.2.15	DoH		y response 0x0000 HTTP	PS www.cs.virginia	a.edu SOA co
	3 18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]:			
	4 18.606080777	10.0.2.15	162.159.61.4	DoH		y 0x0000 AAAA www.cs.v		
	5 18.606168058	162.159.61.4	10.0.2.15	TCP		ACK] Seq=40938 Ack=170		
	6 18.606168109		10.0.2.15	TCP		ACK] Seq=40938 Ack=17:	173 Win=65535 Len=	=0
	7 18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]:			
	8 18.606287808		10.0.2.15	TCP		ACK] Seq=40938 Ack=172		=0
	9 18.606305512		162.159.61.4	DoH		y 0x0000 A www.cs.vir		0
	0 18.606380752		10.0.2.15	TCP		[ACK] Seq=40938 Ack=173	388 Win=65535 Len=	=0
163	1 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]:	200 OK		Þ
Inte Tran Tran	net Protocol V	ersion 4, Src: 10.0 l Protocol, Src Por urity	ic (08:00:27:cc:86:dc .2.15, Dst: 162.159.0 t: 60510, Dst Port: -	61.4	0020 3d 04 ec 5d 0030 F9 0c ec 6l 0040 b3 68 7c 0c 0050 ab af 6a ac 0070 db 44 14 f1 0080 1b d4 18 f2 0080 d6 9c ec 44 0080 1b d4 18 f2 0090 d6 9e ec 44 0040 35 f7 d5 ec 0040 57 76 93 ec 44	3 6a 13 97 1f 72 94 43 3 ab 3f 98 91 1c 8c 55 9 9c fc 4d 34 05 7f at 1 f4 b3 f5 25 95 0c at 3 5b d1 cc 83 03 b6 c. 2 ad 6e 7d 5b d1 a2 5f 4 95 ca a2 a0 76 d8 6f 4 95 ca a2 a0 76 d8 6f 4 95 ca a2 a0 76 d8 6f	a 60 df eb 50 18 a 16 c6 b5 b2 4e 5 b7 5 92 a f5 of f7 f0 f5 e2 of 3 10 f5 e2 of a b6 d7 y4 b0 a b6 d7 y4 b0 d b4 c6 a f2 c1 13 b4 b4 a6 a f2 c1 13 b4 b4 b4 b5 a6 a b4 a a a6 b5 b2 b4 31 ab b5 a6 b7 a6 b4 b7 a6 b4 b7 a6 b7 b7 a6 b7 b7 a6 b7 b	
					4			
				Þ	Frame (213 bytes)	Decrypted TLS (137 bytes)		

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol L	Length Info
	1620 18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
	1621 18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
	1622 18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co
	1623 18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query
	1624 18.606080777	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
	1625 18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
	1626 18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
	1627 18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query
	1628 18.606287808	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
•	1629 18.606305512	10.0.2.15	162.159.61.4	DOH TCP	213 Standard query 0x0000 A www.cs.virginia.edu OPT
	1630 18.606380752		10.0.2.15		60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
	1631 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK
r T		l Protocol, Src Por urity	0.2.15, Dst: 162.159.		0020 3d 04 ec 56 01 bb 56 2f 90 of 0a 66 df eb 56 18 = kV · V 0030 69 0c ec 56 09 00 [7 03 30 09 0a 16 cb 5b 24 ac = kV · V kV 0040 D3 05 /c 02 56 at 57 1f 88 6a 55 92 ac f5 6f 2c kV · V 0050 ab af 6a a3 6a 13 97 1f 72 94 49 37 16 f5 e2 0f kV · V kV 0066 b3 dd a 8a ab 3f 98 91 1c 8c 53 eb 6d 79 46 bb kV · SV kV · V 0070 db 44 18 f1 f4 b9 cf c 4d 34 05 7f ad ab f4 cc 36 7c kV · V kV · V 0080 b6 9e ec 48 5b d1 cc 83 03 b6 cd 4b ab 0b c6 ee V
				Þ	Frame (213 bytes) Decrypted TLS (137 bytes)

Apply a display filter ... <Ctrl-/>

NO.	Time	Source	Destination	Protocol	Length Info			
1620	18.594474318	162.159.61.4	10.0.2.15	TCP		[ACK] Seq=40361 Ack=167		
	. 18.594474390	162.159.61.4	10.0.2.15	TCP		[ACK] Seq=40361 Ack=169		
	18.605415235	162.159.61.4	10.0.2.15	DOH		ry response 0x0000 HTTP	'S www.cs.virginia	a.edu SOA co
	18.606050489	10.0.2.15	162.159.61.4	HTTP2		: POST /dns-query		
	18.606080777	10.0.2.15	162.159.61.4	DoH		ry 0x0000 AAAA www.cs.v		
	18.606168058	162.159.61.4	10.0.2.15	TCP		[ACK] Seq=40938 Ack=170		
	5 18.606168109	162.159.61.4	10.0.2.15	TCP		[ACK] Seq=40938 Ack=171	.73 Win=65535 Len=	=0
	18.606221426	10.0.2.15	162.159.61.4	HTTP2		: POST /dns-query		
	18.606287808	162.159.61.4	10.0.2.15	TCP		[ACK] Seq=40938 Ack=172		=0
	18.606305512		162.159.61.4	DoH		ry 0x0000 A www.cs.virg		
	18.606380752		10.0.2.15	TCP		[ACK] Seq=40938 Ack=173	88 Win=65535 Len=	=0
1631	. 18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]	: 200 OK		
								•
			s), 213 bytes captur			2 35 02 08 00 27 cc 86		RT - 5 '
Ether	net II, Src: P	CSSystemtec_cc:86:dc	(08:00:27:cc:86:dc)	, Dst: 52:5	4 0010 00 c7 d0 7	b 40 00 40 06 7e 03 0a	1 00 02 0f a2 9f	···{@·@· ~···
			2.15, Dst: 162.159.6			e 01 bb 58 2f 90 0d 0a		=··^·X/ ···`
Trans	mission Contro	l Protocol, Src Port	: 60510, Dst Port: 4	43, Seq: 17	2 0030 f9 0c ec 6	b 00 00 17 03 03 00 9a	16 c6 b5 b2 4e	· · · <mark>k</mark> · · · · · · · · ·
	port Layer Sec					3 5e af 57 1f 88 6a 55		·h ·^·W· ·jU··
Hyper	Text Transfer	Protocol 2				3 6a 13 97 1f 72 94 49		••j•j••• r•I7•
							8 eb 6d 79 40 b0	$\cdot = \cdot \cdot \cdot ? \cdot \cdot \cdot \cdot S \cdot m$
							l ab f4 ce 36 7c	• D • • • • M4 • • • • •
								•••••
								····H[····
						2 ad 6e 7d 5b d1 a2 50		5 · · · · n}[· · · P+D
								••••• p·i·•
						a 49 <u>9c 42 f3 4d 51 f</u> 9) 71 f6 10 a4 f8	·+NZI <u>·B</u> · MQ·q·
					00d0 d6 04 d0 1	4 7b		$\cdots \{$
					4			
				•	Frame (213 bytes)	Decrypted TLS (137 bytes)		

▲ ■ ∅ ◎ = 🖹 🛛 🖉 ۹ ← → 🛎 🖌 🖢 📰 ۹ ۹ ۹ ۹ 🏦

Apply a display filter ... <Ctrl-/>

).	Time	Source	Destination	Protocol	Length Info
	18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
	l 18.594474390		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
	2 18.605415235		10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co
		10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query
	18.606080777		162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
		162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
	5 18.606168109		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
	18.606221426		162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query
	3 18.606287808		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
	18.606305512		162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT
	18.606380752		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK
					P
Trans Hyper ▶ St ▼ Do	port Layer Sec Text Transfer ream: DATA, St main Name Syste Transaction II	urity Protocol 2 ream ID: 149, Length em (query)	: 60510, Dst Port: 443		0030 29 10 00 <
	Authority RRs:			cot.	up step: got Firefox to output
				Seri	
		· 1			
	Additional RRs	s: 1			
¥	Additional RRs Queries		ass TN		
•	Additional RRs Queries	jinia.edu: type A, cl	ass IN		
*	Additional RRs Queries • www.cs.virg Name: ww	jinia.edu: type A, cl w.cs.virginia.edu	ass IN		
Ŧ	Additional RRs Queries • www.cs.virg Name: ww [Name Le	jinia.edu: type A, cl w.cs.virginia.edu ngth: 19]	ass IN		otographic keys (using SSLKEYLOGFILE)
Ŧ	Additional RRs Queries • www.cs.virg Name: ww [Name Le	jinia.edu: type A, cl w.cs.virginia.edu	ass IN		ptographic keys (using SSLKEYLOGFILE)

Apply a display filter ... <Ctrl-/>

lo.	Time	Source	Destination	Protocol	Length Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
	18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
	18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query
	18.606080777	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
	18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
	18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query
	18.606287808		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
	18.606305512		162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT
	18.606380752		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK
			its), 213 bytes captu		
			dc (08:00:27:cc:86:dc		0010 00 00 00 00 01 03 77 77 77 02 63 73 08 76 69 72 ·····www.w.c
			0.2.15, Dst: 162.159.		0020 67 69 6e 69 61 03 65 64 75 00 00 01 00 01 00 00 ginia.ed u
			rt: 60510, Dst Port:	443, Seq: 1	0030 29 10 00 00 00 00 00 50 00 08 00 04 00 01 00)······ P··
	ort Layer Sec				0040 00 00 0c 00 44 00 00 00 00 00 00 00 00 00 00 00
	ext Transfer				0050 00 00 00 00 00 00 00 00 00 00 00 00
		eam ID: 149, Leng	th 128		0060 00 00 00 00 00 00 00 00 00 00 00 00
	ain Name Syst				0070 00 00 00 00 00 00 00 00 00 00 00 00
	Transaction II				0080 00 00 00 00 00 00 00 00 00 00
		Standard query			
	Questions: 1				
	Answer RRs: 0				
	Authority RRs				
	Additional RRs	: 1			
	Queries	1.1	-1		
– (
– (www.cs.virg		otuss in		
– (www.cs.virg Name: www 	w.cs.virginia.edu	01035 11		
– (www.cs.virg Name: ww [Name Le 	w.cs.virginia.edu ngth: 19]	01035 11		4
• (www.cs.virg Name: www 	w.cs.virginia.edu ngth: 19]			Frame (213 bytes) Decrypted TLS (137 bytes)

Apply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol	Length Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
	18.594474390	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
	18.605415235	162.159.61.4	10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co
	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query
	18.606080777	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
	18.606168058	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
	18.606168109	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110 HEADERS[149]: POST /dns-query
		162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
	18.606305512		162.159.61.4	DoH	213 Standard query 0x0000 A www.cs.virginia.edu OPT
	18.606380752		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1031	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK
Ethern	net II, Src: P	CSSystemtec_cc:86:	bits), 213 bytes captu dc (08:00:27:cc:86:dc), Dst: 52:	0010 00 00 00 00 01 03 77 77 77 02 63 73 08 76 69 72 ·····ww w·cs
			0.2.15, Dst: 162.159. ort: 60510, Dst Port:		0020 67 69 6e 69 61 03 65 64 75 00 00 01 00 01 00 00 ginia.ed u 0030 29 10 00 00 00 00 00 50 00 88 00 04 00 01 00) P
	port Layer Sec		ort: 60510, DSt Port:	443, Sey: J	0040 00 00 0c 00 44 00 00 00 00 00 00 00 00 00 00 00
	Text Transfer				
		ream ID: 149, Leng	th 128		
	nain Name Syst				0070 00 00 00 00 00 00 00 00 00 00 00 00
	Transaction II				0080 00 00 00 00 00 00 00 00 00 00 00 00
•	Flags: 0x0100	Standard guery			
	Questions: 1				
	Answer RRs: 0				
	Authority RRs:	· •			
	Authority RRs:			_	
Ŧ	Authority RRs Additional RRs Queries • www.cs.virg	s: 1 jinia.edu: type A,	class IN	_	
Ŧ	Authority RRs: Additional RRs Queries • www.cs.virg Name: ww	s: 1 jinia.edu: type A, w.cs.virginia.edu	class IN	_	
Ŧ	Authority RRS: Additional RRS Queries • www.cs.virg Name: ww [Name Le	s: 1 Jinia.edu: type A, w.cs.virginia.edu ngth: 19]	class IN	_	4
Ŧ	Authority RRS: Additional RRS Queries • www.cs.virg Name: ww [Name Le	s: 1 jinia.edu: type A, w.cs.virginia.edu	class IN		Frame (213 bytes) Decrypted TLS (137 bytes)

🔳 🖉 💿 💼 🖹 🗙 🙆 🍳 👄 🧼 🖄 🏹 📃 🔍 Q, Q, 🎹

Apply a display filter ... < Ctrl-/>

Source 1620 18.594474318 162.159.61.4 1621 18 504474300 162 150 61 4 1622 18,605415235 162,159,61,4 1623 18.606050489 10.0.2.15 1624 18 606080777 10 0 2 15 1625 18,606168058 162,159,61,4 1626 18,606168109 162,159,61,4 1627 18,606221426 10.0.2.15 1628 18,606287808 162,159,61,4 1629 18 606305512 10 0 2 15 1630 18,606380752 162,159,61,4 1631 18,616270366 162,159,61,4 Frame 1629: 213 bytes on wire (17) Ethernet II, Src: PCSSystemtec cc Internet Protocol Version 4, Src: Transmission Control Protocol, Sr Transport Laver Security HyperText Transfer Protocol 2 ▶ Stream: DATA, Stream ID: 149, Domain Name System (duery) Transaction ID: 0X0000

No

pply a display filter	<ctrl-></ctrl->				
Time	Source	Destination	Protocol	Length Info	P
1620 18.594474318		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0	1
1621 18.594474390		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0	-
1622 18.605415235		10.0.2.15	DoH	631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co	
1623 18.606050489		162.159.61.4	HTTP2	110 HEADERS[147]: POST /dns-query	
1624 18.606080777		162.159.61.4	DoH	213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT	
1625 18.606168058		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0	
$1626 \ 18.606168109$ $1627 \ 18.606221426$		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0	
1628 18.606287808		10.0.2.15	HTTP2 TCP	110 HEADERS[149]: POST /dns-query 60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0	
1628 18.606287802		162.159.61.4	DoH	213 Standard guery 0x0000 A www.cs.virginia.edu OPT	
1630 18.606380752		10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0	4
		10.0.2.15	HTTP2	109 HEADERS[147]: 200 OK	۰.
1001 10.0102/0000	102.100.01.4	10.0.2.110			
amo 1620, 212 h	tes on wire (1704 bits) 212 bytes contured	(1704 k	▲ 0000 <u>00 00 80 00 01 00 00 00 95 00 00 01 00 00 01 00</u> ······	
	PCSSystemtec_cc:86:dc				
	Version 4, Src: 10.0.2			0020 67 69 6e 69 61 03 65 64 75 00 00 01 00 01 00 00 ginia·ed u····	
	ol Protocol, Src Port:			0030 29 10 00 00 00 00 00 00 50 00 08 00 04 00 01 00 00) P	
ansport Layer Se		00010, 030 1010. 440	, beq. 1	0040 00 00 00 00 44 00 00 00 00 00 00 00	
perText Transfer					
	tream ID: 149, Length	128		0060 00 00 00 00 00 00 00 00 00 00 00 00	
Domain Name Sys				0070 00 00 00 00 00 00 00 00 00 00 00 00	
Transaction			_	0080 00 00 00 00 00 00 00 00	
Flags: 0x010	9 Standard query				
Questions: 1					
Answer RRs:	9				

Decrypted TLS (137 bytes)

Packets: 1765 · Displayed: 1765 (100.0%)



h

Profile: Default

.

📕 🖩 🖉 🕲 🚞 🖹 🔽 🗳 🗢 👄 🛸 🏝 🖉 📃 📃 🔍 Q. Q. 🏦

Apply a display filter ... <Ctrl-/>

1 1620 18.594474310 162.159.61.4 10.0.2.15 TCP 60 443 - 66510 ACK1 Seq=40361 Ack=16790 Win=65535 Len 1 1621 18.594474300 162.159.61.4 10.0.2.15 TCP 60 443 - 66510 ACK1 Seq=40361 Ack=16790 Win=65535 Len 1 1621 18.594474300 10.0.2.15 162.159.61.4 10.0.2.15 DDH 631 Standard query response 0x0000 HTTPS www.cs.virginia.edu OTT 1 162 18.606168100 100.2.15 162.159.61.4 DOH 213 Standard query 0x0000 AAAA www.cs.virginia.edu OTT 1 162 18.606168100 162.159.61.4 10.0.2.15 TCP 60 443 - 66510 ACK1 Seq=40938 Ack=17014 Win=6553 Len 1 162 18.60618100 162.159.61.4 10.0.2.15 TCP 60 443 - 66510 ACK1 Seq=40938 Ack=17014 Win=65535 Len 1 162 18.60618100 162.159.61.4 10.0.2.15 TCP 60 443 - 66510 ACK1 Seq=40938 Ack=17014 Win=65535 Len 1 162 18.606287080 162.159.61.4 10.0.2.15 TCP 60 443 - 66510 AcK1	o.	Time	Source	Destination	Protocol	Length Info
1628 18.666287808 162.159.61.4 10.0.2.15 TCP 60 443 -= 66510 [ACK] Seq-40938 Ack=17220 Win=65535 Lem 1630 18.666369512 10.0.2.15 100.0.2.15 TCP 60 443 -= 66510 [ACK] Seq-40938 Ack=17220 Win=65535 Lem 1631 18.666369512 10.0.2.15 100.0.2.15 TCP 60 443 -= 66510 [ACK] Seq-40938 Ack=17388 Win=65535 Lem 1631 18.616270366 162.159.61.4 10.0.2.15 TCP 60 443 -= 66510 [ACK] Seq-40938 Ack=17388 Win=65535 Lem 1631 18.616270366 162.159.61.4 10.0.2.15 HTTP2 109 HEADERS[147]: 200 0K Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 k * 6000 0 60 60 60 10 37 77 77 70 2 63 73 08 76 69 72 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4 6010 0 0 60 0 60 0 0 0 0 0 0 0 0 0 0 0 0	162 162 162 162 162 162	20 18.594474318 21 18.594474390 22 18.605415235 23 18.606050489 24 18.606080777 25 18.606168058 26 18.606168058	162.159.61.4 162.159.61.4 162.159.61.4 10.0.2.15 10.0.2.15 162.159.61.4 162.159.61.4	10.0.2.15 10.0.2.15 162.159.61.4 162.159.61.4 10.0.2.15 10.0.2.15	TCP TCP DoH HTTP2 DoH TCP TCP	66 443 - 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0 60 443 - 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0 631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA cc 110 HEADERS[147]: POST /dns-query Vas0000 AAA www.cs.virginia.edu OPT 213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT 0443 - 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0 06 443 - 60510 [ACK] Seq=40938 Ack=17014 Win=65555 Len=0 06 443 - 60510 [ACK] Seq=40938 Ack=17014 Win=65555 Len=0 0
<pre>> Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: S2: Internet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: S2: Internet Protocol Version 4, Src: 10.0.2.15, Dst: 102.159.61.4 > Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 1 > Transport Layer Security + HyperFext Transfer Protocol 2 > Stream: DATA, Stream ID: 149, Length 128 > Domain Name System (query) Questions: 1 Answer RRs: 0 Authority RRs: 0 Authority RRs: 0 Authority RRs: 0 Authority RRs: 0 Additional RRs: 1 * Www.cs.virginia.edu: type A, class IN Name: www.cs.virginia.edu</pre>	162 - 162 163	2818.6062878082918.6063055123018.606380752	162.159.61.4 10.0.2.15 162.159.61.4	10.0.2.15 162.159.61.4 10.0.2.15	TCP DoH TCP	60 443 → 66510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0 213 Standard query 0x0000 A www.cs.virginia.edu 0PT 66 443 → 66510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
[Label Count: 4]	 Ethe Inte Tran Tran Hype S D 	rnet II, Srci'P rnet Protocol V ismission Contro isport Layer Sec rText Transfer tream: DATA, St omain Name Syst Transaction II Flags: 0x0400 Questions: 1 Answer RRs: 0 Authority RRs Additional RR: - Queries - Www.cs.virg Name: ww [Name Le	CSSystemtec_cc:86 ersion 4, Src: 10 l Protocol, Src Po urity Protocol 2 ream ID: 149, Leng (QUGTy) 2: 0x0000 Standard query : 0 : 1 jinia.edu: type A, w.cs.virginia.edu ngth: 19]	dc (08:00:27:cc:86:dd 0.2.15, Dost: 162.159 prt: 60510, Dst Port: hth 128 class IN	c), Dst: 52: .61.4	0010 00 00 00 00 01 03 77 77 77 77 02 03 73 08 76 00 72

◢ ■ ∅ ◎ 💼 🖹 🛛 🖓 🗢 ⇒ 🛎 🖉 🚽 📃 🖲 ९, ९, ୩

Apply a display filter ... <Ctrl-/>

о.	Time	Source	Destination	Protocol L	ength Info							
	21 18.594474390	162.159.61.4	10.0.2.15	TCP] Seq=40361 Ack=16958 W				
	22 18.605415235	162.159.61.4	10.0.2.15	DoH				esponse 0x0000 HTTPS ww	ww.cs.vir@	yinia	.edu SOA d	26
	23 18.606050489 24 18.606080777	10.0.2.15 10.0.2.15	162.159.61.4					ST /dns-query x0000 AAAA www.cs.virgi		DT		
	224 18.606080777	162,159,61,4	10.0.2.15	TCP				Seg=40938 Ack=17014 V			0	_
		162.159.61.4	10.0.2.15	TCP] Seq=40938 Ack=17014 V				
	27 18.606221426		162.159.61	IUTTDO	440 11540	- 00010		ST /dns-query	win=055555	Len-	.0	
		162,159,61,4	10.0.2.1	Mark/Unmark Packet		Ctrl+M	K	Seg=40938 Ack=17229 V	lin=65535	Len=	:0	_
16	29 18.606305512	10.0.2.15	162.159.0	-				x0000 A www.cs.virginia				
16	30 18.606380752	162.159.61.4	10.0.2.1	Ignore/Unignore Pack	et	Ctrl+D		BPv7	in=65535	Len=	:0	
		162.159.61.4	10.0.2.1	Set/Unset Time Refere	ance	Ctrl+T		DFV/				
16	32 18.616270417	162.159.61.4	10.0.2.1	Sed onset nine kerere		curri		DCCP	.cs.virgi	inia.	edu SOA co	
				Time Shift		Ctrl+Shift+	Т					•
		es on wire (880 bits)		Dealers Comments				CIP Connection	98 00 45		$RT \cdot \cdot 5 \cdot \cdot \cdot$	
		CSSystemtec_cc:86:dc		27: Facket comments				Ethernet	92 Of a2		·`·z@·@·	
		ersion 4, Src: 10.0.2		Edit Resolved Name					df eb 50		=··^·X/	
		l Protocol, Src Port:	: 60510, D≶	Eult Resolved Name			_	F5 TCP	ab 13 1e			
	nsport Layer Sec erText Transfer I			Apply as Filter			•	F5 UDP	08 1e 8e 2b 50 4c		··g·{·^· w··v	
нур	erlext Iranster I	Protocol 2						F5 UDP	20 50 4C a0 3b	32	:·\i·E·L	
				Prepare as Filter				F5 IP	a0 30		1. (T.E.F	552
				Conversation Filter			•	IEEE 802.15.4				
								IEEE 802.15.4				
				Colorize Conversation			1	IPv4				
				SCTP			•	IPv6				
				Follow			•	LTP				
				Сору			•	ТСР				
				Protocol Preferences			•	UDP				
				Decode As				ZigBee Network Laver	ompresse	d Hea	der (313 byte	es)
2	Cthornot (oth) 14	huter						5	100.0%		Drafile: Da	fault
<u> </u>	Ethernet (eth), 14	bytes		Show Packet in New W	lindow			PN-IO AR	(100.0%)		Profile: De	nault

1		= 🔝 🔀 🎑 I 🤇	रे 🗢 🔶 警 🍝		
(ij	p.addr eq 10.0.2.15 an	d ip.addr eq 162.159.61.	4) and (tcp.port eq 60510 a	nd tcp.port eq 4	443)
	Time 116 0.155053894 118 0.160484358 119 0.160500515	Source 10.0.2.15 162.159.61.4 10.0.2.15	Destir 162.1 10.0	expre	SSION - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSVal 60510 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
	124 125 based o	n address (\sim	machine) and	d nort n	umber (~ program/socket) fields 💩
	127 USUALLY	means all pa	rt of one sock	et conne	CCTION ic, settings[0], WINDOW_UPDATE[0]
	128 0.161189517	162.159.61.4	10.0.2.15	TCP	60 443 - 60510 [ACK] Seq=1 Ack=1176 Win=65535 Len=0
	129 0.161189548	162.159.61.4	10.0.2.15	TCP HTTP2	60 443 → 60510 [ACK] Seq=1 Ack=1268 Win=65535 Len=0
	134 0.170787727 135 0.170791720	10.0.2.15	10.0.2.15		882 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
		10.0.2.15	162.159.61.4 162.159.61.4	TCP TLSv1.3	54 60510 → 443 [ACK] Seq=1268 Ack=829 Win=63756 Len=0
	136 0.171049539 137 0.171103419	162,159,61,4	10.0.2.15	TCP	138 End of Early Data, Finished 60 443 → 60510 [ACK] Seg=829 Ack=1352 Win=65535 Len=0
		10.0.2.15	162,159,61,4	HTTP2	60 443 → 60510 [ACK] SEQ=829 ACK=1352 WIN=65535 LEN=0 85 SETTINGS[0]
	138 0.171278790	162.159.61.4		TCP	
	139 0.171322666 140 0.171340513		10.0.2.15	HTTP2	60 443 → 60510 [ACK] Seq=829 Ack=1383 Win=65535 Len=0
	140 0.171340513	10.0.2.15 10.0.2.15	162.159.61.4 162.159.61.4	DoH	205 HEADERS[3]: POST /dns-query 213 Standard guery 0x0000 NS example.com OPT
		10.0.2.15		HTTP2	
	142 0.171388167 143 0.171394454		162.159.61.4	TCP	325 Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA
	143 0.171394454 144 0.171394495	162.159.61.4 162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=1534 Win=65535 Len=0 60 443 → 60510 [ACK] Seq=829 Ack=1693 Win=65535 Len=0
		10.0.2.15	162,159,61,4	HTTP2	
	145 0.171407305	162,159,61,4	102.159.61.4	TCP	269 Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER 60 443 → 60510 [ACK] Seg=829 Ack=1964 Win=65535 Len=0
	146 0.171466560				
	147 0.171466601	162.159.61.4	10.0.2.15	TCP DoH	60 443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0
	148 0.171468885				858 Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St
	149 0.171512699 150 0.180410746	162.159.61.4	10.0.2.15	TCP HTTP2	60 443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0 171 HEADERS[3]: 200 0K
	150 0.180410746	162.159.61.4	10.0.2.15	DOH	553 Standard query response 0x0000 NS example.com NS a.iana-servers.
	152 0.180440215	10.0.2.15	162,159,61,4	TCP	553 Standard query response 6x0000 NS example.com NS a.1ana-servers. 54 60510 \rightarrow 443 [ACK] Seg=2983 Ack=946 Win=63756 Len=0
	152 0.180440215	10.0.2.15	162.159.61.4	TCP	54 60510 → 443 [ACK] Seq=2983 Ack=946 Win=63756 Len=0
	153 0.180475992	162,159,61,4	10.0.2.15	HTTP2	
	134 0.100/1141/	102.109.01.4	10.0.2.15	ni IP2	¹⁰⁸ HEADE 499 packets in "conversatio
_				F	Frame (20 5 bytes) Decrypted ILS (129 bytes) Decompressed Header (313 bytes)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

📕 🖩 🖉 🕲 💼 🖹 🕱 🗳 🔍 👄 🔶 警 🖉 💆 🔜 🔍 Q. Q. 🏦

(ip.addr eq 10.0.2.15 and ip.addr eq 162.159.61.4) and (tcp.port eq 60510 and tcp.port eq 443)

No.	Time	Source	Destination	Protocol	Length Info	•
_	116 0.155053894	10.0.2.15	162,159,61,4	TCP	74 60510 → 443 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval	
	118 0.160484358	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [SYN, ACK] Seg=0 Ack=1 Win=65535 Len=0 MSS=1460	
	119 0.160500515	10.0.2.15	162.159.61.4	TCP	54 60510 → 443 [ACK] Seg=1 Ack=1 Win=64240 Len=0	
	124 0.161038813	10.0.2.15	162.159.61.4	TLSv1.3	1223 Client Hello (SNI=mozilla.cloudflare-dns.com)	
	125 0.161095683	162,159 61,4	10.0.2.5	CCP	[1] 3 60510 [ACK] Seg=1 Ack=1170 Win=65535 Len=0	
	126 Some	DACKETS	not shown	trom	TITE ipher Spec	
	127 0.161131275	10.0.2.15	162.159.61.4	HTTP2	146 Magic, SETTINGS[0], WINDOW_UPDATE[0]	
	128 0.101109517	162.159.61.4	10.0.2.15	TCP	00 443 → 00510 [ACK] Seg=1 Ack=1176 Win=65535 Len=0	
	129 0.161189548	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seg=1 Ack=1268 Win=65535 Len=0	
	134 0.170787727	162.159.61.4	10.0.2.15	HTTP2	882 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]	
	135 0.170791720	10.0.2.15	162.159.61.4	TCP	54 60510 → 443 [ACK] Seg=1268 Ack=829 Win=63756 Len=0	
	136 0.171049539	10.0.2.15	162.159.61.4	TLSv1.3	138 End of Early Data, Finished	
	137 0.171103419	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=1352 Win=65535 Len=0	
	138 0.171278790	10.0.2.15	162.159.61.4	HTTP2	85 SETTINGS[0]	
	139 0.171322666	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=1383 Win=65535 Len=0	
	140 0.171340513	10.0.2.15	162.159.61.4	HTTP2	205 HEADERS[3]: POST /dns-query	
	141 0.171349002	10.0.2.15	162.159.61.4	DoH	213 Standard query 0x0000 NS example.com OPT	
	142 0.171388167	10.0.2.15	162.159.61.4	HTTP2	325 Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA	
	143 0.171394454	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=1534 Win=65535 Len=0	
	144 0.171394495	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=1693 Win=65535 Len=0	
	145 0.171407305	10.0.2.15	162.159.61.4	HTTP2	269 Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER	
	146 0.171466560	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=1964 Win=65535 Len=0	
	147 0.171466601	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0	
	148 0.171468885	10.0.2.15	162.159.61.4	DoH	858 Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St	
	149 0.171512699	162.159.61.4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0	
	150 0.180410746	162.159.61.4	10.0.2.15	HTTP2	171 HEADERS[3]: 200 OK	
	151 0.180411361	162.159.61.4	10.0.2.15	DoH	553 Standard query response 0x0000 NS example.com NS a.iana-servers.	
	152 0.180440215	10.0.2.15	162.159.61.4	TCP	54 60510 → 443 [ACK] Seq=2983 Ack=946 Win=63756 Len=0	
	153 0.180475992	10.0.2.15	162.159.61.4	TCP	54 60510 → 443 [ACK] Seq=2983 Ack=1445 Win=63756 Len=0	
	154 0.180711417	162.159.61.4	10.0.2.15	HTTP2	108 HEADERS[5]: 200 OK	-
4					۱. Example 2. Example	
4				Þ	Frame (205 bytes) Decrypted ILS (129 bytes) Decompressed Header (313 bytes)
0	Ethernet (eth), 14	l bytes			Packets: 1765 · Displayed: 499 (28.3%) Profile: Defa	ult

41

X -> - +

<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>

◢ ■ ∅ ◎ 🖿 🖹 🛛 🗳 ۹ 👄 🔶 警 🖌 🖳 🗐 ۹. ۹. ۹. 🟦

(ip.addr eq 10.0.2.15 and ip.addr eq 162.159.61.4) and (tcp.port eq 60510 and tcp.port eq 443)

No.	Time	Source	Destination		Length Info
	116 0.155053894	10.0.2.15	162 159 61 4	TCP	74 60510 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
	118 0.160484358	102.159.01.4	10.0.2.15	TCP	60 443 → 60510 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
	119 0.160500515	nignest	layer used	TCP TLSv1.3	54 60510 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
	124 0.161038813 125 0.161095683	162 150 61 4	10 0 2 15	TLSV1.3	1223 Client Hello (SNI=mozilla.cloudflare-dns.com) 60 443 → 60510 [ACK] Seg=1 Ack=1170 Win=65535 Len=0
	126 0.161121701	10 proces	nackat	TLSv1.3	
	127 0.161131275	in each	packet	HTTP2	146 Magic, SETTINGS[0], WINDOW_UPDATE[0]
	128 0.161189517	162,159,61,4	10.0.2.15	TCP	60 443 → 60510 [ACK] Seg=1 Ack=1176 Win=65535 Len=0
	129 0.161189548			TCP	60 443 → 60510 [ACK] Seq=1 Ack=1268 Win=65535 Len=0
	1 connoc	tion only	'for'	HTTP2	882 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
	1 COITIEC	tion only	1 O 5 9 . 61 . 4	TCP	54 60510 → 443 [ACK] Seq=1268 Ack=829 Win=63756 Len=0
	136 0.171049539	10.0.2.15		TLSv1.3	
	1 DNIS	VOR HTTI	PS (DoH)	TCP	60 443 → 60510 [ACK] Seq=829 Ack=1352 Win=65535 Len=0
		VELILIII	J (DOIT)	HTTP2	85 SETTINGS[0]
	139 0.171322666		10.0.1.15	TCP HTTP2	60 443 → 60510 [ACK] Seq=829 Ack=1383 Win=65535 Len=0 205 HEADERS[3]: POST /dns-query
	hut ma	any packe	tc., 159 61 4	DOH	205 HEADERS[3]: POST 70hS-query 213 Standard guery 0x0000 NS example.com OPT
	j Dut ma	iny packe	162.159.61.4	HTTP2	325 Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA
	143 0.171394454	162.159.61.4		TCP	60 443 → 60510 [ACK] Seg=829 Ack=1534 Win=65535 Len=0
	1 only ne	eded for		TCP	60 443 - 60510 [ACK] Seg=829 Ack=1693 Win=65535 Len=0
	1 Only ne	cucu ioi		HTTP2	269 Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER
	146.0.171466560	162.159.61.4 📕		TCP	60 443 → 60510 [ACK] Seq=829 Ack=1964 Win=65535 Len=0
	1 bookke	eping for		TCP	60 443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0
		child ioi		DoH	858 Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St
	149 0.171512699	162.159.61.4		TCP	60 443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0
-	the low	wer' layer	S 10.0.2.15	HTTP2 DoH	171 HEADERS[3]: 200 OK 553 Standard guery response 0x0000 NS example.com NS a.iana-servers.
	152 0 180440215	in cristica y cris	162 159 61 4	TCP	53 Standard query response 6x6666 NS exampte.com NS a.tana-servers. 54 60510 → 443 [ACK] Seg=2983 Ack=946 Win=63756 Len=0
	153 0.180475992	10.0.2.15	162.159.61.4	TCP	54 60510 → 443 [ACK] Seq=2983 Ack=1445 Win=63756 Len=0
	154 0.180711417	162,159,61,4	10.0.2.15	HTTP2	108 HEADERS[5]: 200 OK
4					•
4				Þ	Frame (205 bytes) Decrypted LS (129 bytes) Decompressed Header (313 bytes)
0	Z Ethernet (eth), 14	bytes			Packets: 1765 · Displayed: 499 (28.3%) Profile: Default

<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>

🚄 🔳 🖉 🕲 🚞 🖺 🔀 🖸 🔍 🖛 🌩 錾 🚡 🖢 📃 📃 🍭 Q. Q. 🏦

(ip.addr eq 10.0.2.15 and ip.addr eq 162.159.61.4) and (tcp.port eq 60510 and tcp.port eq 443)

N	o. Time	Source	Destination	Protocol Length Info
-	116 0.155053894	10.0.2.15	162.159.61.4	TCP 74 60510 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
	118 0.160484358	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
Т	119 0.160500515	10.0.2.15	162.159.61.4	TCP 54 60510 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
	124 0.161038813	10.0.2.15	162.159.61.4	TLSv1.3 1223 Client Hello (SNI=mozilla.cloudflare-dns.com)
	125 0.161095683	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seg=1 Ack=1170 Win=65535 Len=0
	126 0.161121701	10.0.2.15	162.159.61.4	TLSv1.3 60 Change Cipher Spec
	127 0.161131275	10.0.2.15	162.159.61.4	HTTP2 146 Magic, SETTINGS[0], WINDOW_UPDATE[0]
	128 0.161189517	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seq=1 Ack=1176 Win=65535 Len=0
	129 0.161189548	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seq=1 Ack=1268 Win=65535 Len=0
	134 0.170787727	162.159.61.4	10.0.2.15	HTTP2 882 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
	135 0.170791720	10.0.2.15	162.159.61.4	TCP 54 60510 - 443 [ACK] Seq=1268 Ack=829 Win=63756 Len=0
	136 0.171049539	10.0.2.15	162.159.61.4	bookkeeping packets sent
	137 0.171103419	162.159.61.4	10.0.2.15	DOORKEEping packets sent 5 Len=0
	138 0.171278790	10.0.2.15	162.159.61.4	HTTP2 85 SETTINGS[0]
	139 0.171322666	162.159.61.4	10.0.2.15	in both directions Active Managers Leneo
÷	 140 0.171340513 	10.0.2.15	162.159.61.4	
	141 0.171349002	10.0.2.15	162.159.61.4	DoH 213 Standard query 0x0000 NS example.com OPT
	142 0.171388167	10.0.2.15	162.159.61.4	HTTP2 325 Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA
	143 0.171394454	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seq=829 Ack=1534 Win=65535 Len=0
	144 0.171394495	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seq=829 Ack=1693 Win=65535 Len=0
	145 0.171407305	10.0.2.15	162.159.61.4	HTTP2 269 Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER
	146 0.171466560	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seq=829 Ack=1964 Win=65535 Len=0
	147 0.171466601	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0
	148 0.171468885	10.0.2.15	162.159.61.4	DoH 858 Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St
	149 0.171512699	162.159.61.4	10.0.2.15	TCP 60 443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0
-	150 0.180410746	162.159.61.4	10.0.2.15	HTTP2 171 HEADERS[3]: 200 0K
	151 0.180411361	162.159.61.4	10.0.2.15	DoH 553 Standard query response 0x0000 NS example.com NS a.iana-servers.
	152 0.180440215	10.0.2.15	162.159.61.4	TCP 54 60510 → 443 [ACK] Seq=2983 Ack=946 Win=63756 Len=0
	153 0.180475992	10.0.2.15	162.159.61.4	TCP 54 60510 → 443 [ACK] Seq=2983 Ack=1445 Win=63756 Len=0
	154 0.180711417	162.159.61.4	10.0.2.15	HTTP2 108 HEADERS[5]: 200 OK
4				
4				Frame (205 bytes) Decrypted ILS (129 bytes) Decompressed Header (313 bytes)
(🔵 🌋 🛛 Ethernet (eth), 14	l bytes		Packets: 1765 · Displayed: 499 (28.3%) Profile: Default

X ⇒ ▼ +

end-to-end argument

Saltzer, Reed, Clark, "End-to-End Arguments in System Design"

"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

end-to-end argument

Saltzer, Reed, Clark, "End-to-End Arguments in System Design"

"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

example: reliable file transfer

want to make sure correct data transferred

want to protect against:

error in hardware/software on sending machine reading file bits being flipped in memory on forwarding machine communication system flipping bits in data hosts crashing during communication

example: reliable file transfer

want to make sure correct data transferred

want to protect against:

error in hardware/software on sending machine reading file bits being flipped in memory on forwarding machine communication system flipping bits in data hosts crashing during communication

communication system can't help a lot of these things

example: reliable file transfer

want to make sure correct data transferred

want to protect against:

error in hardware/software on sending machine reading file bits being flipped in memory on forwarding machine communication system flipping bits in data hosts crashing during communication

communication system can't help a lot of these things

authors experienced router with bad memory/processor

solution: end-to-end checks

want reliable transfer: compare final files (with hash or similar)

"end-to-end" — doesn't care what middle systems do

end-to-end argument

Saltzer, Reed, Clark, "End-to-End Arguments in System Design"

"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

end-to-end in practice

"narrow waist" of IP doesn't provide many gaurnetees no gaurentees about reliable transmission, duplicate suppression, message order, ...

but try to provide good service ("best effort")

in design: typically middle systems won't know/care about what's forwarded

but many exceptions

backup slides