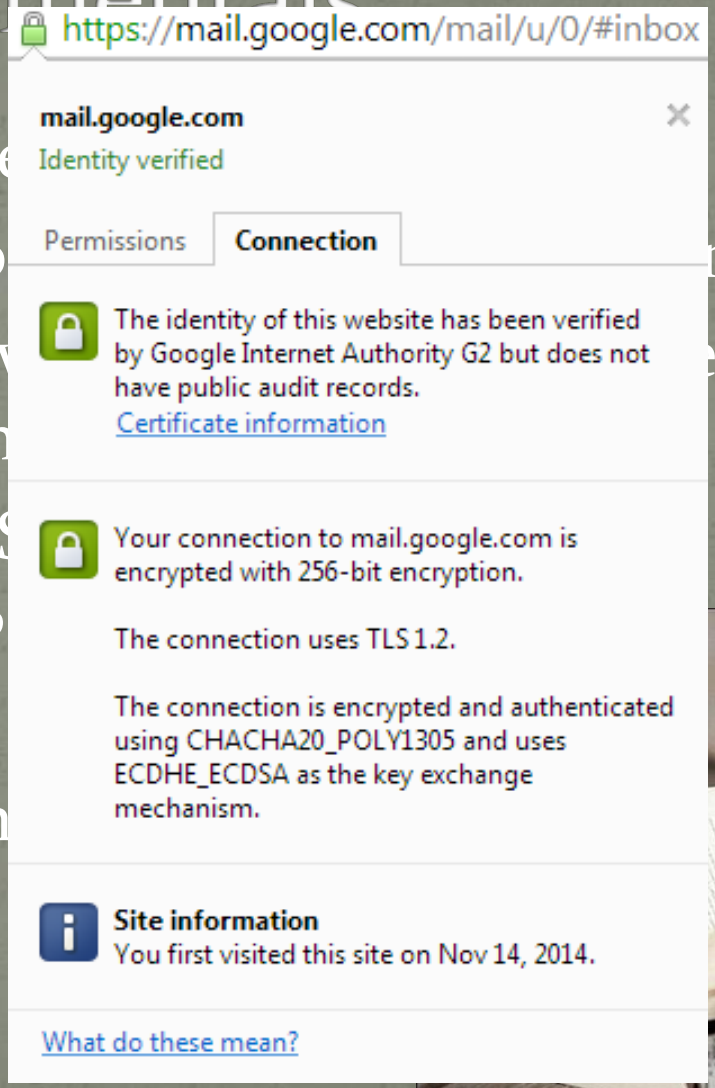
TLS and HTTPS

CSE 461 Section

A joke about bad weather

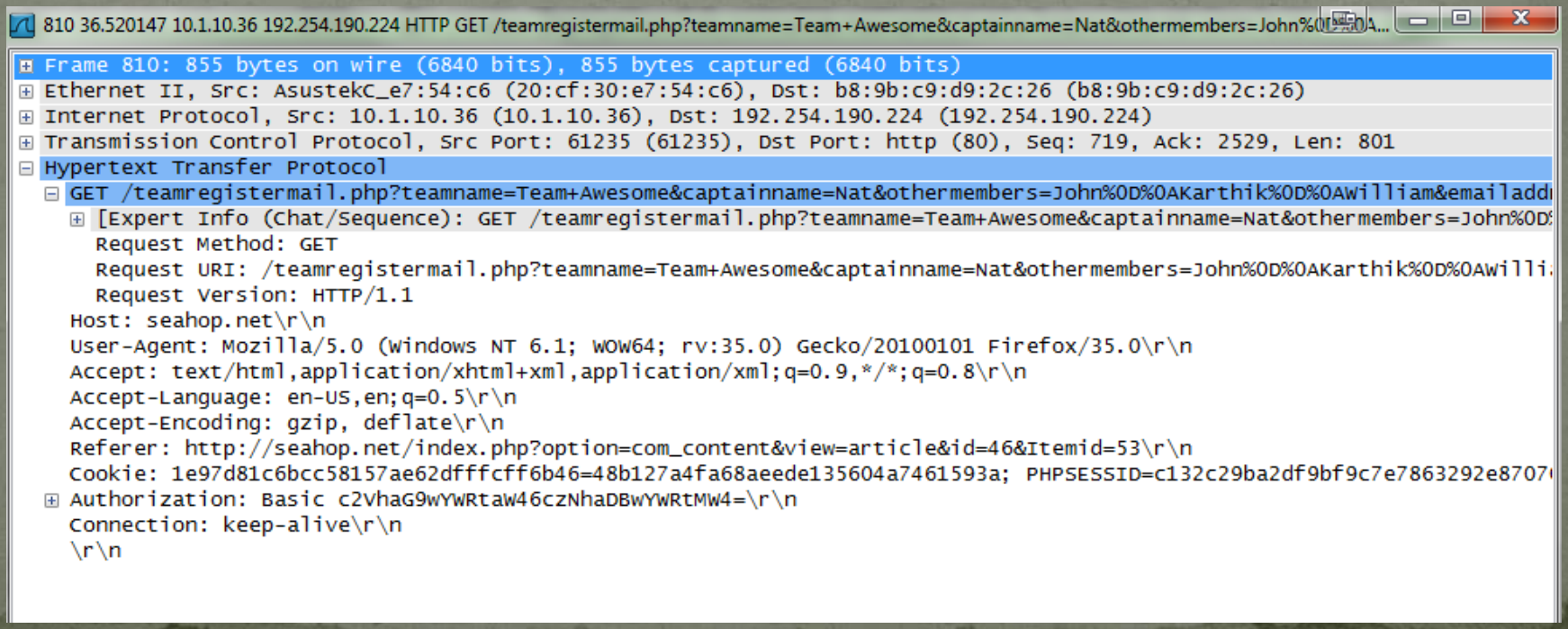
TLS Fundamentals

- "Transport Laye
- Standard proto net traffic
- Previously knov ets Layer), which has been
- TLS replaced S
- Used for HTTP Secure) traffic
- Supported by n web browser



Purposes for TLS (1)

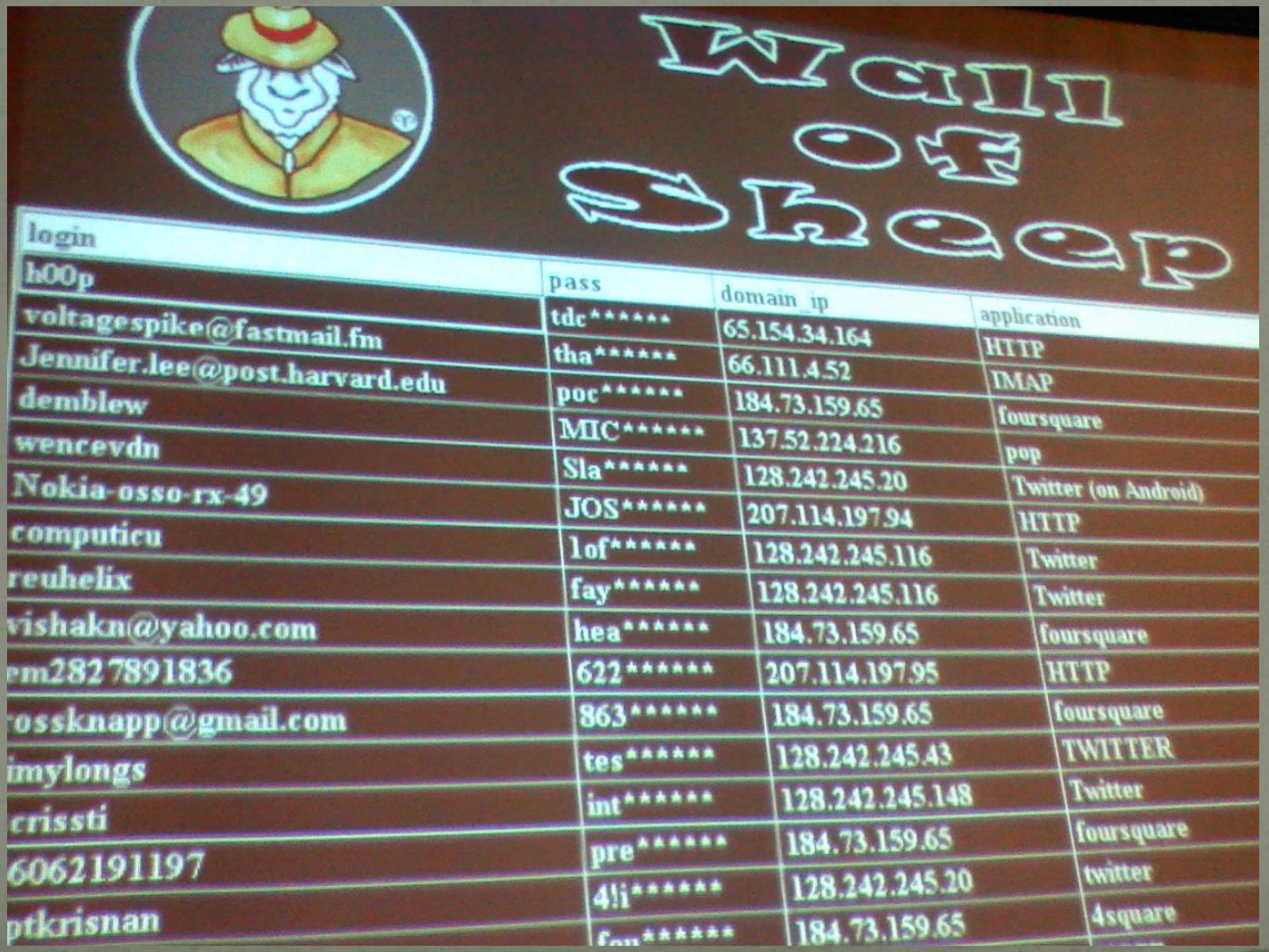
- When we don't use TLS, web traffic goes over unencrypted
- This includes HTTP payloads, but also HTTP headers
- Why are headers a problem too?



Purposes for TLS (2)

- Data integrity
- Server (and client) authentication

Defcon Wall of Sheep



login	pass	domain ip	application
h00p	tdc******	65.154.34.164	HTTP
voltagespike@fastmail.fm	tha******	66.111.4.52	IMAP
Jennifer.lee@post.harvard.edu	poc******	184.73.159.65	foursquare
demblew	MIC******	137.52.224.216	pop
wencevdn	Sla******	128.242.245.20	Twitter (on Android)
Nokia-osso-rx-49	JOS******	207.114.197.94	HTTP
computicu	1of******	128.242.245.116	Twitter
reuhelix	fay******	128.242.245.116	Twitter
vishakn@yahoo.com	hea******	184.73.159.65	foursquare
em2827891836	622******	207.114.197.95	HTTP
rossknapp@gmail.com	863******	184.73.159.65	foursquare
imylongs	tes******	128.242.245.43	TWITTER
crissti	int******	128.242.245.148	Twitter
6062191197	pre******	184.73.159.65	foursquare
ptkrisnan	4!i******	128.242.245.20	twitter
	fou******	184.73.159.65	4square

TLS and CONNECT

- HTTP CONNECT is used to establish a two-way connection “tunnel” between two parties
- After this, a “triple handshake” is performed over the tunnel
- After the handshake, the two parties can communicate securely
- We’ll take a closer look at this handshake

TLS Handshake Protocol (Concept)

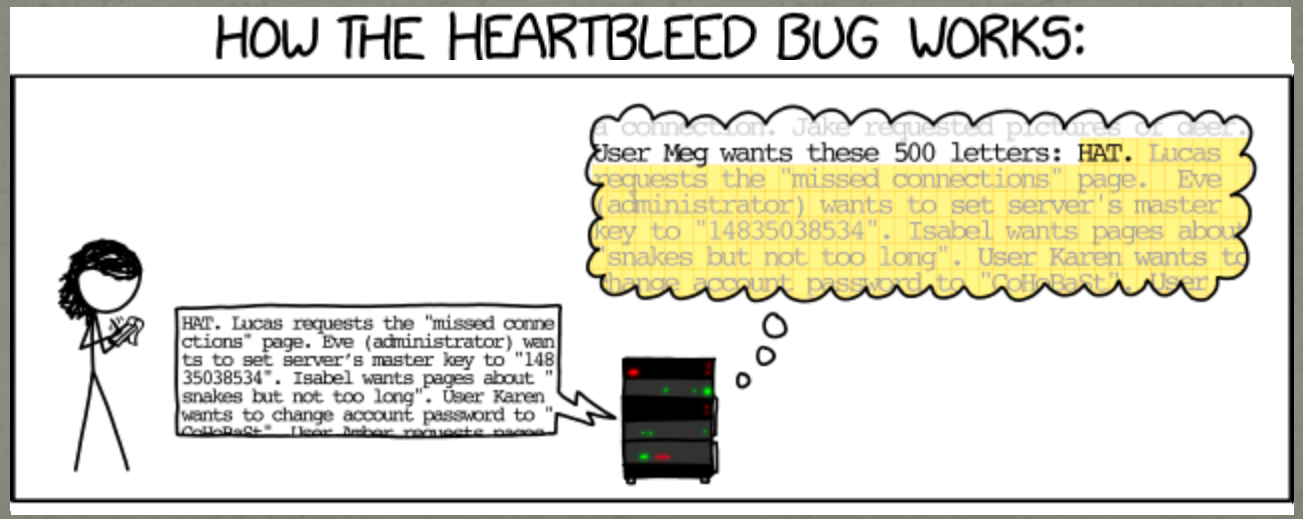
- What do we need to do to communicate securely?
  - Make sure we're speaking the same language
  - Prove who we are
  - Establish a secret code

TLS Handshake Protocol (Rough Details)

- Client tells the server its protocol version and what cryptographic algorithms it can use
- Server responds with a protocol version and cryptographic algorithm to use
- Server sends its certificate to verify its identity
- Client verifies certificate and sends Pre-Master Secret, encrypted so only the server can read it
- Client and server both use that PMS to generate a Master Secret, which is used to generate encryption keys
- Communication commences

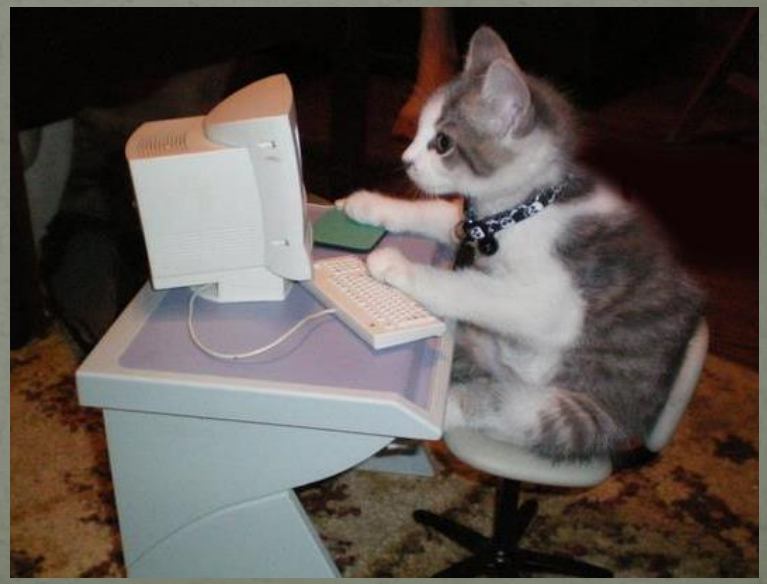
Heartbleed bug

- 2014 Bug in OpenSSL implementation of TLS
- Clients ask for a “heartbeat” message to test and keep alive communication links
- In OpenSSL, length checking wasn’t properly performed on the heartbeat data



TLS Exploits

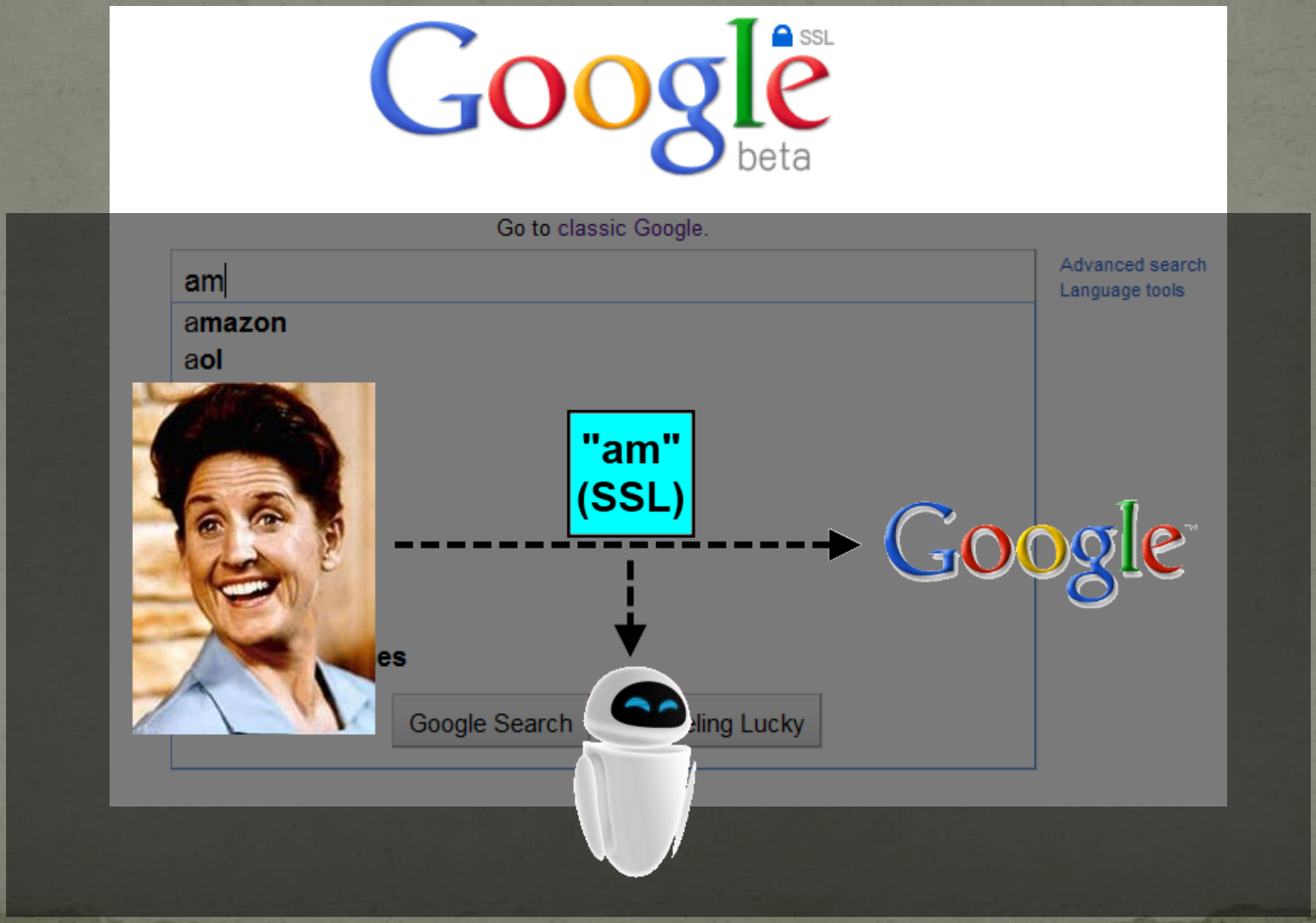
- How might data be intercepted by a MITM, even when encrypted over TLS?
  - Implementation bugs (e.g., Heartbleed, 3Shake)
  - Server/browser attacks (e.g., truncation attack)
    - "Truncate" logout packet from user
    - User's browser tells them they've logged out
    - They haven't
  - Side-channel attacks



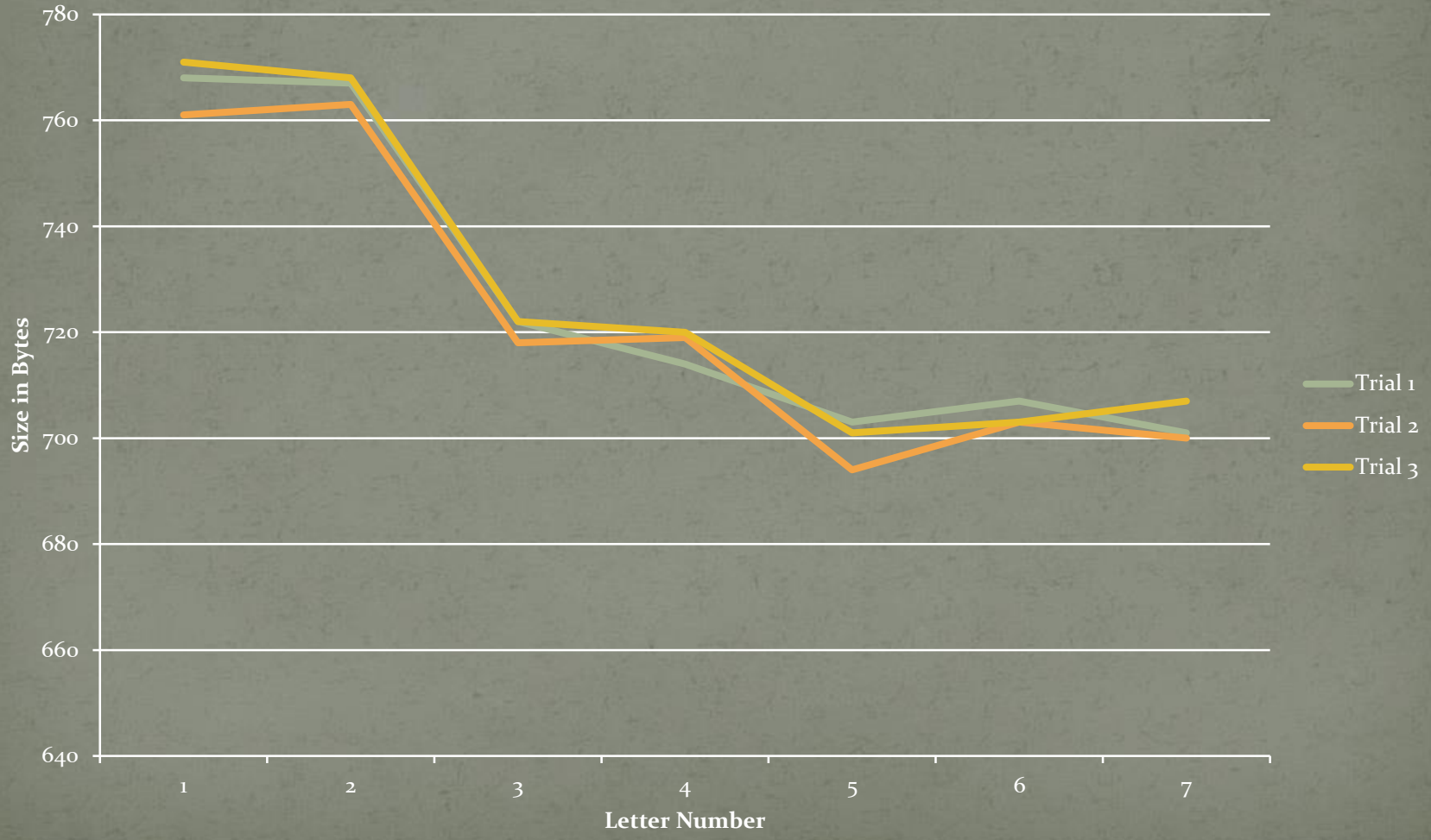
Side-channel TLS Attacks (1)

- Some data is leaked even with encryption
  - Packet send timing
  - Payload size
  - AJAX interfaces that load content dynamically provide insight into what the user is typing

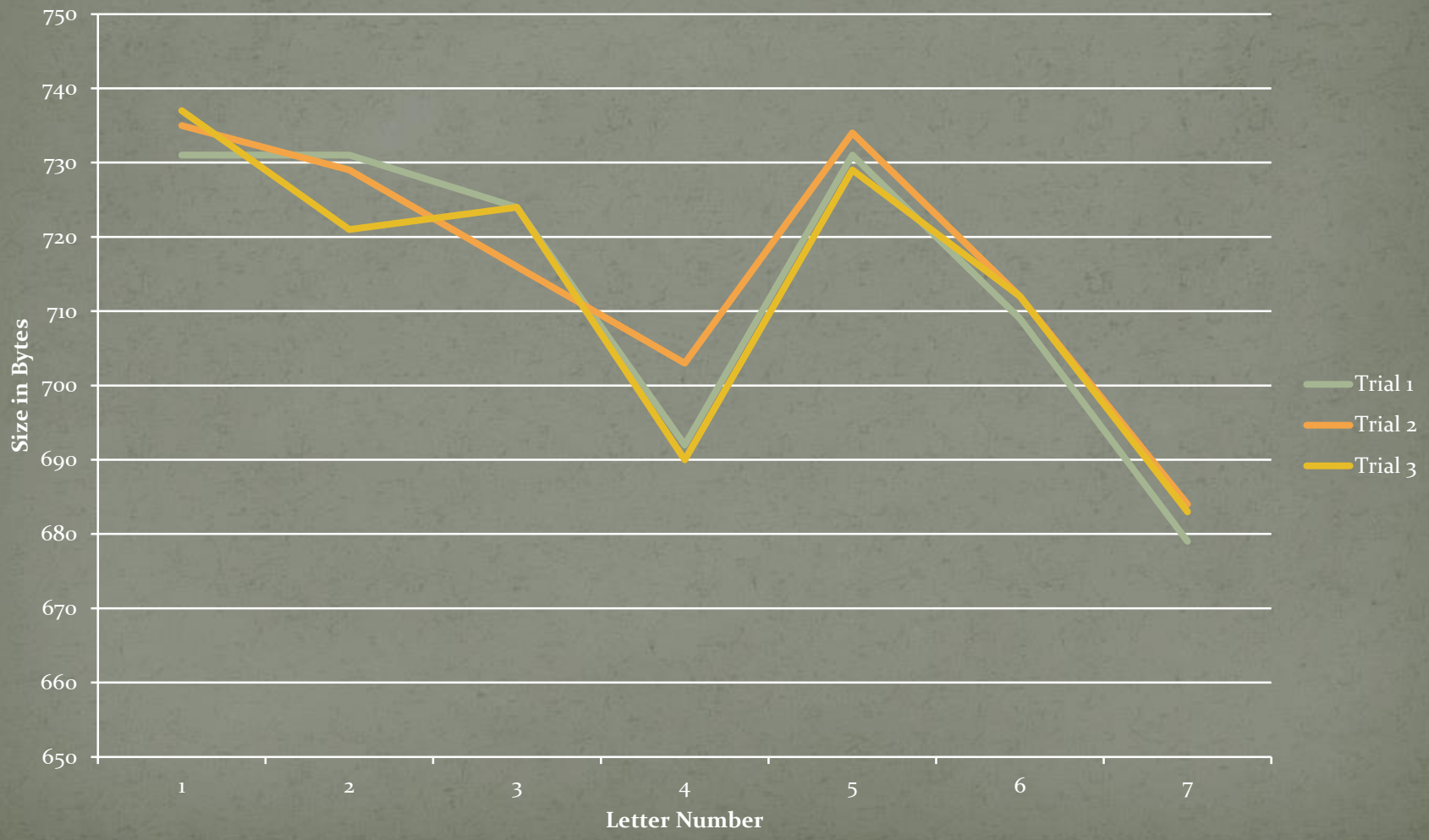
Side-channel TLS Attacks (2)



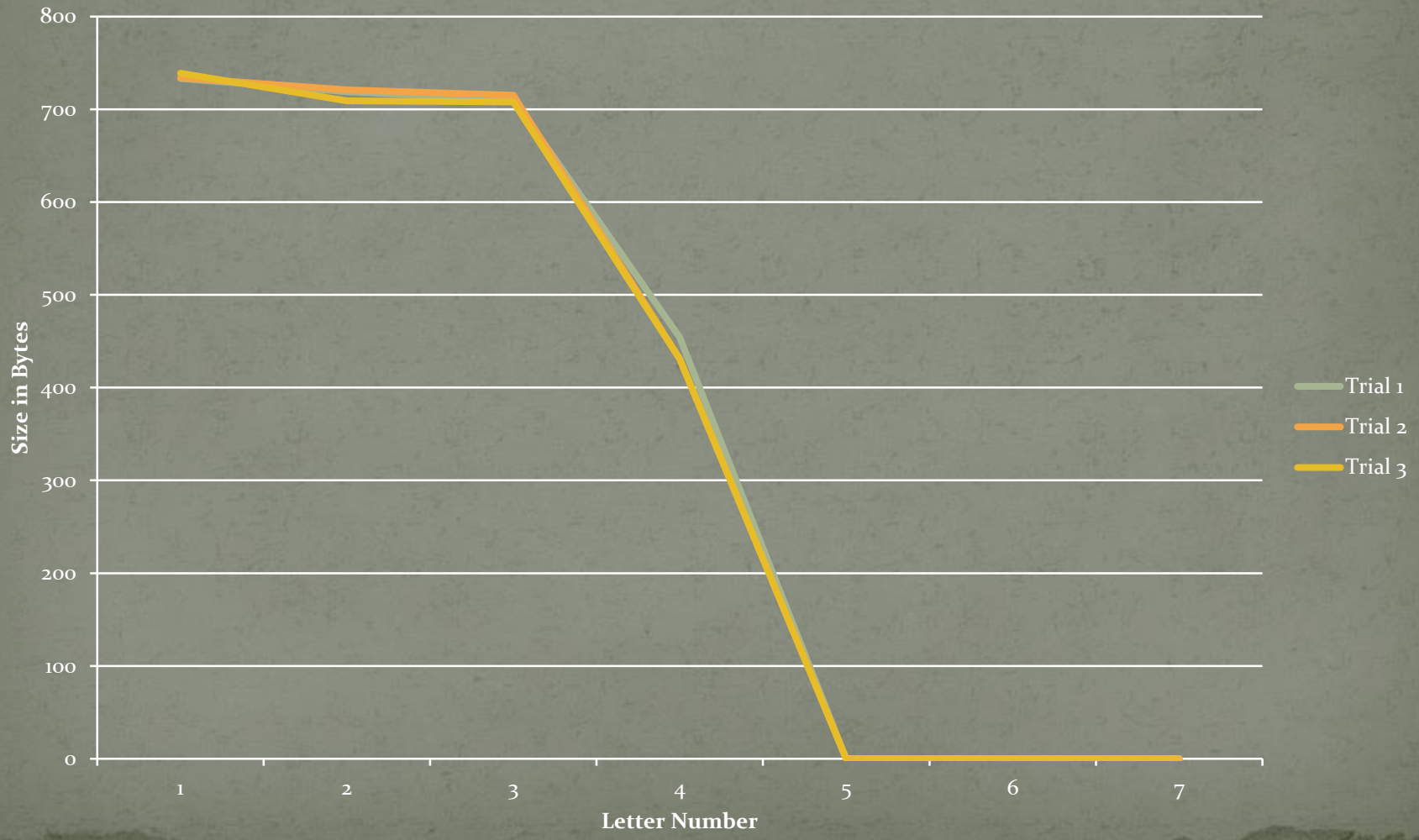
Autocomplete Packet Sizes for "hackers"



Autocomplete Packet Sizes for "benaloh"



Autocomplete Packet Sizes for "xvwqxzx"



Questions?