**Cryptography and Computer Forensics**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**SLP 04**

INTRODUCTION

BODY

Protocol stuff

SECURE ELECTRONIC TRANSACTIONS

In February, 1996, Visa and Mastercard published the Secure Electronic Transactions (SET) protocols to broaden their business for electronic commerce. SET is an open standard that was designed to protect the privacy and ensure the authenticity of electronic transactions (“Secure Electronic”, n.d.).

SET is efficient, easy to implement and minimally impacts the, merchant, acquirer, and payment system infrastructure. The participants of the SET protocol are the, cardholder, issuer, merchant, aquirer, acquirer’s payment gateway, brand, and the certification authority.

Figure 1 shows all the different participants of the SET specification.

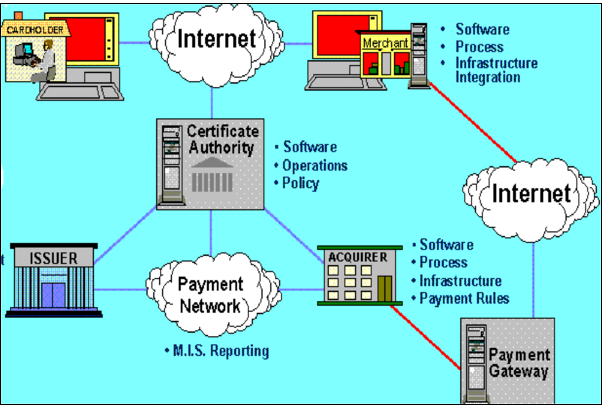


Figure 1: Secure Electronic Transaction (SET) - Korhonen, M. (n.d.). Secure Electronic Transaction (SET). Retrieved January 4, 2016, from http://www.tml.tkk.fi/Opinnot/Tik-110.501/1996/seminars/works/set/SET.html

SECURE SOCKET LAYER

In 1994, Netscape created and adopted the use of the Secure Sockets Layer Protocol (SSL) in order to encrypt the data path from the client to a server. “SSL creates and encrypted connection between your web server and your visitor’s web browser” with public and private key pairs (“What is SSL”, 2015). This encrypted communication path enables a user to confidently transmit private data without, eavesdropping, data tampering, or message forgery (“History of SSL”, 2015).

To enable SSL on a given web server a SSL Certificate must be obtained. The SSL Certificate identifies the owner and must be installed on the server. Either a padlock icon or a green address bar in the web browser indicates that there is an SSL Certificate in use. This visual indicator allows the user to be confident while sending secure data that their information is protected and only seen by the organization that owns the website (“What is SSL”, 2015).

TRANSPORT LAYER SECURITY

Transport Layer Security (TLS), established in 1996, like SSL ensures communications are encrypted via users and web sites, but it also employs the use of cryptography. TLS is composed of two layers, the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol can be encrypted or not and as such is able to utilize encryption methods like the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES). The TLS Handshake Protocol enables the server and client to authenticate each other prior to sending, receiving data. This is done by negotiating algorithms and cryptographic keys (“What is Transport”, 2015).

HYPER TEXT TRANSFER PROTOCOL

Hypertext Transfer Protocol (HTTP) is a set of rules that has been established in order to transmit files across the internet. These files can be any form of multimedia such as, text, graphic images, sound, and video, files. Furthermore, these files may contain references to other files that, with selection, elicit additional transfer requests; thereby, defining the implications of the hypertext portion of HTTP (“What is HTTP”, 2015).

Users’ browsers act as an HTTP client which send requests to server machines. As soon as the user opens a browser, she inadvertently makes use of HTTP which is an application protocol that runs on top of the TCP/IP suite of protocols. Any web server must not only have the web page files it can serve, but also a HTTP daemon. The HTTP daemon is a program that waits for HTTP requests and handles them, when they arrive (“What is HTTP”, 2015).

HYPER TEXT TRANSFER PROTOCOL SECURE

Hypertext transfer protocol secure (HTTPS) also known as, HTTP over SSL, HTTP over TSL, and HTTP Secure, is a protocol for secure communication over the internet and is the secure version of HTTP. HTTPS utilizes asymmetric Public Key Infrastructure (PKI) with either SSL or TSL during implementation.

Upon requesting an HTTPS connection to a webpage, the server responds with its SSL Certificate. Within the certificate lies the public key which is needed to begin the secure session. Next, the browser and the server initiate the ‘SSL handshake’. This is done through the encryption process of either SSL or TSL. Once the trusted SSL or TSL Digital Certificate is used, users, depending on the web browser being used, will see a padlock or a green address bar. The green address bar specifically indicates when an Extended Validation Certificate is being utilized (“What is HTTPS”, 2015).

Websites specifics protocols

AMAZON

Upon navigating to Amazon’s shopping cart web page from the signed-in user portion of their site, the session becomes secure. The Uniform Resource Locator (URL) switches from the standard [www.amazon.com](http://www.amazon.com) address to the secure HTTPS utilizing TLS. Additional visual indicators are given with a green padlock and the ‘https:’ prefix in the URL.

Figure 2 is a snap shot of Amazon’s shopping cart page.

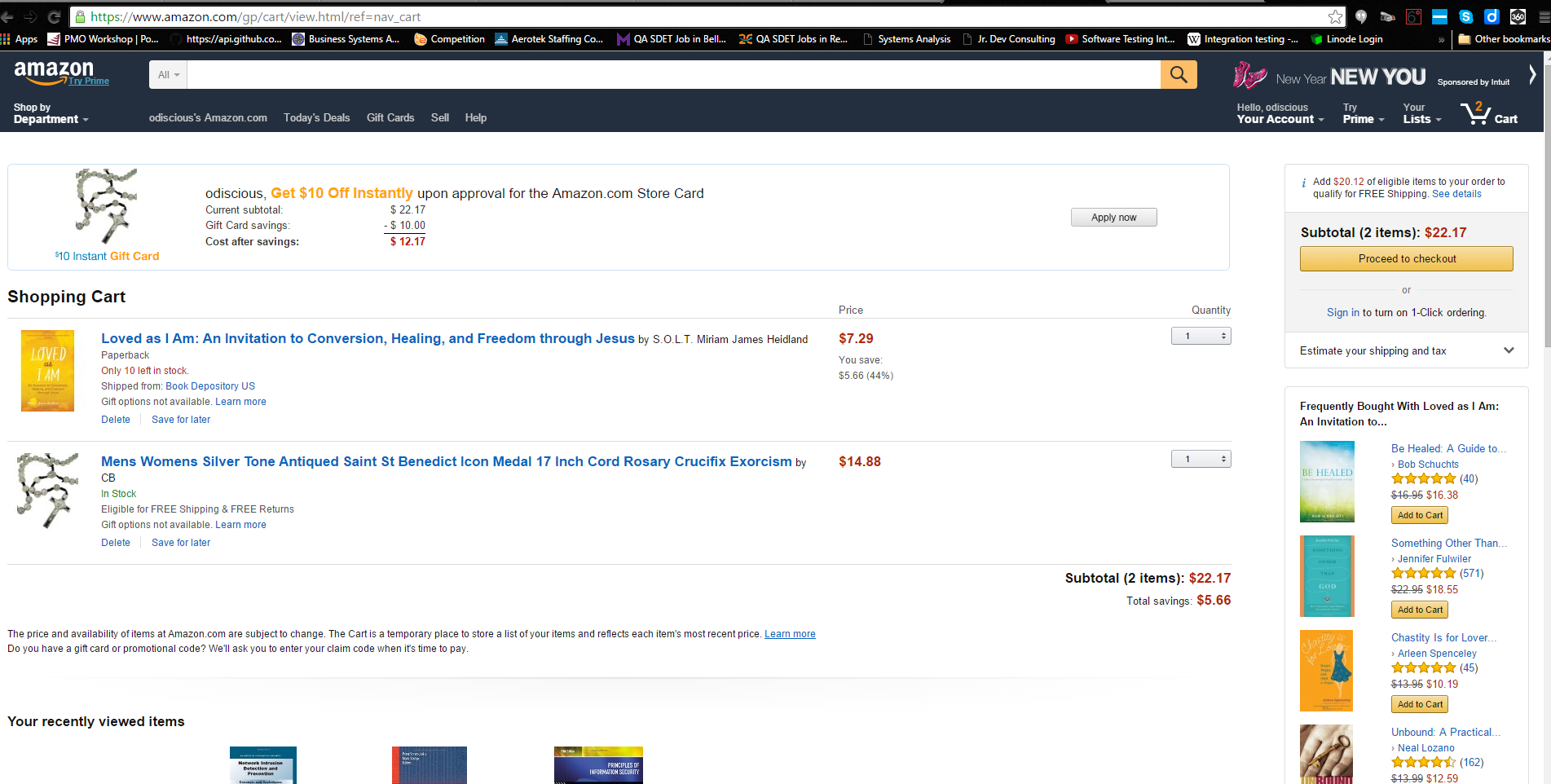


Figure 2: Amazon Shopping Cart Page - Your Shopping Cart is empty. (2016). Retrieved January 5, 2016, from https://www.amazon.com/gp/cart/view.html/ref=nav\_cart

EBAY

Upon navigating to Ebay’s shopping cart web page from the signed-in user portion of their site, the session remains unsecure. On the next page, however, the user is asked to choose a payment option and it’s secure. The URL switches from the standard, http://cart.payments.ebay.com/sc/add?ssPageName=CART:ATC&item=iid:131660742904,qty:1, address to the secure HTTPS utilizing TLS. Additional visual indicators are given with a green padlock and the ‘https:’ prefix in the URL.

Figure 3 is a snap shot of Ebay’s checkout page.

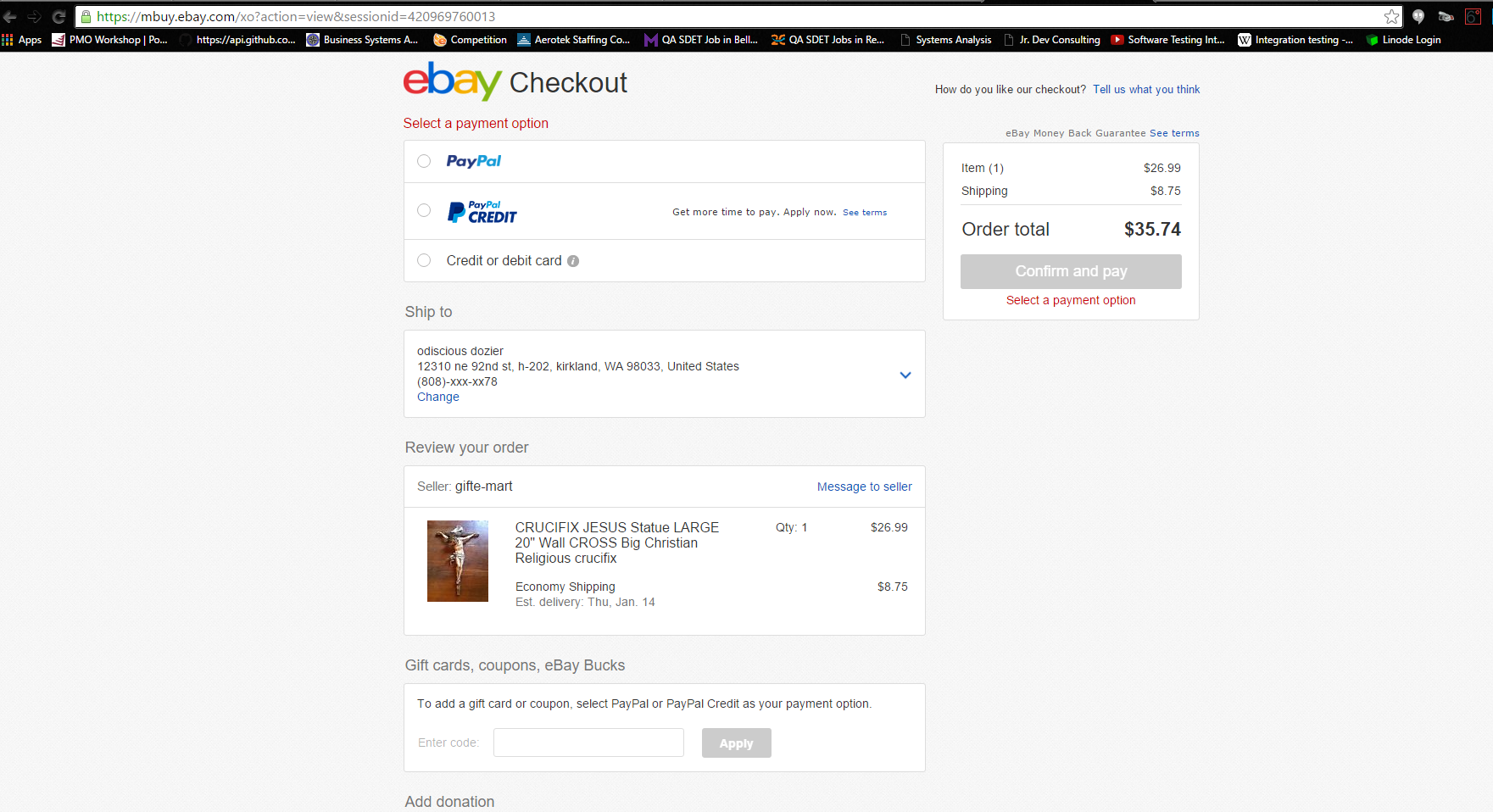


Figure 3: Ebay's Checkout Page - Welcome to eBay. (2016). Retrieved January 5, 2016, from https://mbuy.ebay.com/xo?action=view&sessionid=420969760013

MACY\*S

Upon navigating to Macy’s shopping bag web page from the signed-in user portion of their site, the session remains unsecure. On the next page, however, the user is asked to choose a payment option and it’s secure. The URL switches from the standard, http://www1.macys.com/bag/index.ognc?&cm\_sp=add\_to\_bag-\_-checkout-\_-men-men%27s+clothing-blazers+%26+sport+coats, address to the secure HTTPS utilizing TLS. Additional visual indicators are given with a green padlock and the ‘https:’ prefix in the URL.

Figure 4 is a snap shot of Macy’s Shipping and Payment page.

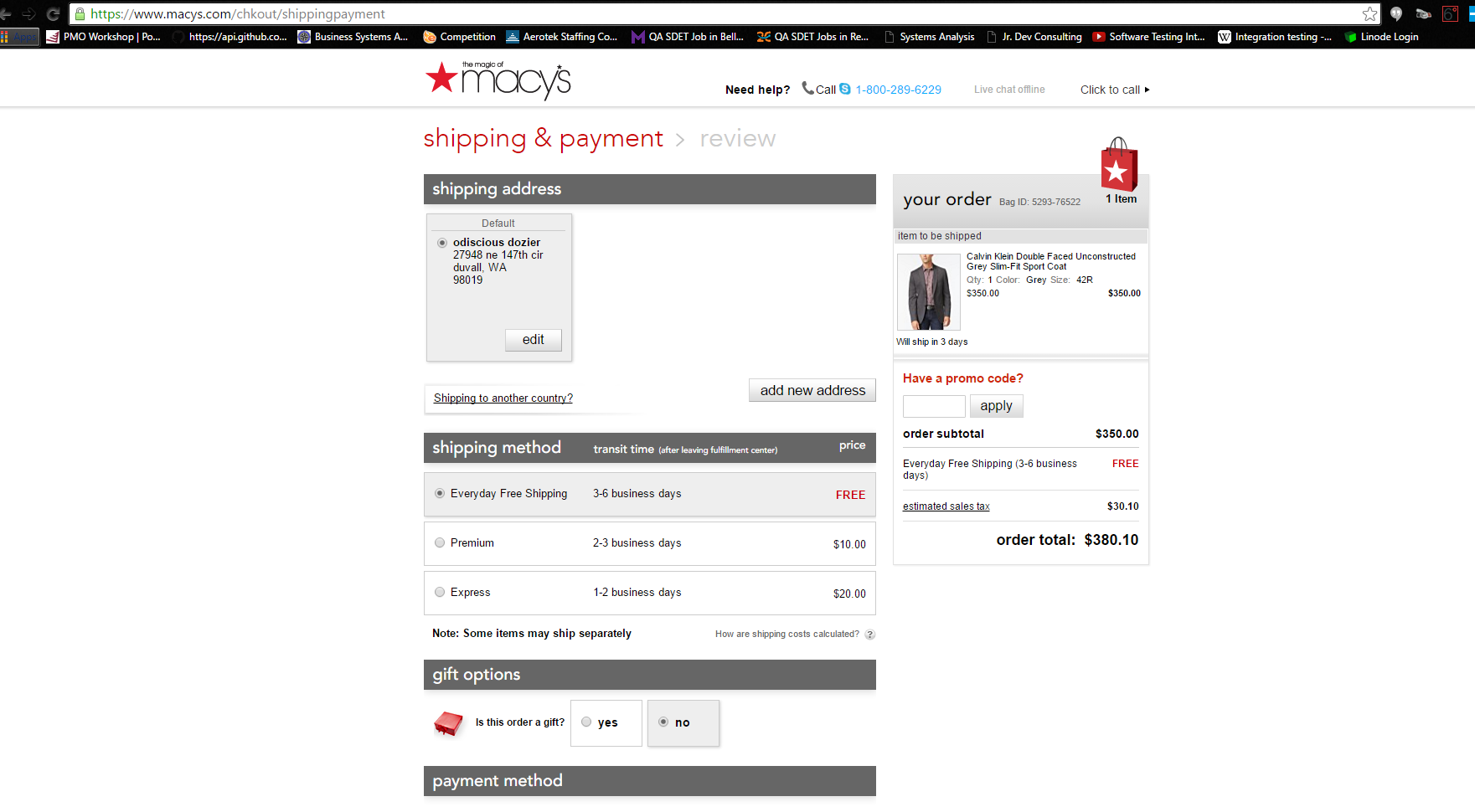


Figure 4: Macy\*s Shipping and Payment Web Page - Shipping and Payment. (2016). Retrieved January 5, 2016, from https://www.macys.com/chkout/shippingpayment

Part II

Computer forensic story I

* Point 100wds
* Point 100wds
* Point 100wds

Computer forensic story II

* Point 100wds
* Point 100wds
* Point 100wds

Computer forensic story III ?

* Point 100wds
* Point 100wds
* Point 100wds

CONCLUSION

REFERENCE

History of SSL Certificate. (2015). Retrieved December 30, 2015, from <https://www.evsslcertificate.com/ssl/ssl-history.html>

The history of SSL. (2015). Retrieved December 30, 2015, from <http://www.gemalto.com/identity/inspired/secure-ecommerce/ssl>

Korhonen, M. (n.d.). Secure Electronic Transaction (SET). Retrieved January 4, 2016, from <http://www.tml.tkk.fi/Opinnot/Tik-110.501/1996/seminars/works/set/SET.html>

Secure Electronic Transactions. (n.d.). Retrieved January 5, 2016, from <http://www.davidreilly.com/topics/electronic_commerce/essays/secure_electronic_transaction> s.html

Shipping and Payment. (2016). Retrieved January 5, 2016, from https://www.macys.com/chkout/shippingpayment

Welcome to eBay. (2016). Retrieved January 5, 2016, from https://mbuy.ebay.com/xo?action=view&sessionid=420969760013

What is HTTP (Hypertext Transfer Protocol)? - Definition from WhatIs.com. (2015). Retrieved January 4, 2016, from <http://searchwindevelopment.techtarget.com/definition/HTTP>

What is HTTPS? (2015). Retrieved December 30, 2015, from [https://www.instantssl.com/ssl-certificate- products/https.html](https://www.instantssl.com/ssl-certificate-%09products/https.html)

What is SSL? SSL Certificate Basics. (2015). Retrieved December 30, 2015, from <https://www.sslshopper.com/what-is-ssl.html>

What is Transport Layer Security (TLS)? - Definition from WhatIs.com. (2015). Retrieved December 30, 2015, from <http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS>

Your Shopping Cart is empty. (2016). Retrieved January 5, 2016, from <https://www.amazon.com/gp/cart/view.html/ref=nav_cart>