**Cryptography and Computer Forensics**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**SLP 04**

INTRODUCTION

As the amount of data in the world increases, various efforts have been made to embrace technology for enhanced consumer experiences while shopping. With these positive works, there has been a rise in criminal activity. This discussion includes some of the technological protocols and steps in providing consumer protection and moves to a discussion about the empowerment of law enforcement with the use of computer forensics.

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.

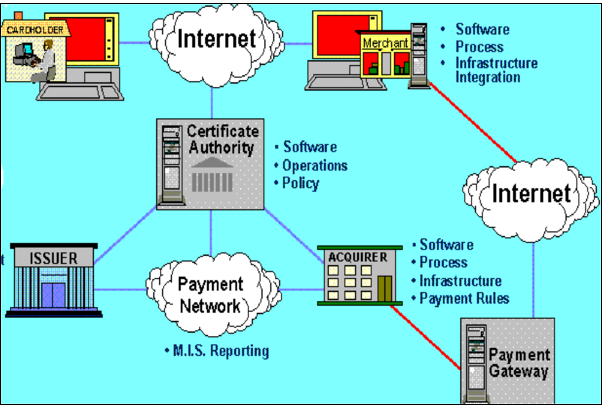


Figure 1: Secure Electronic Transaction (SET) - Korhonen, M. (n.d.). Secure Electronic Transaction (SET). Retrieved January 4, 2016, from http://www.tml.tkk.fi/Opinnot/Tik-110.501/1996/seminars/works/set/SET.html

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).

COMMON WEBSITE SHOPPING

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.

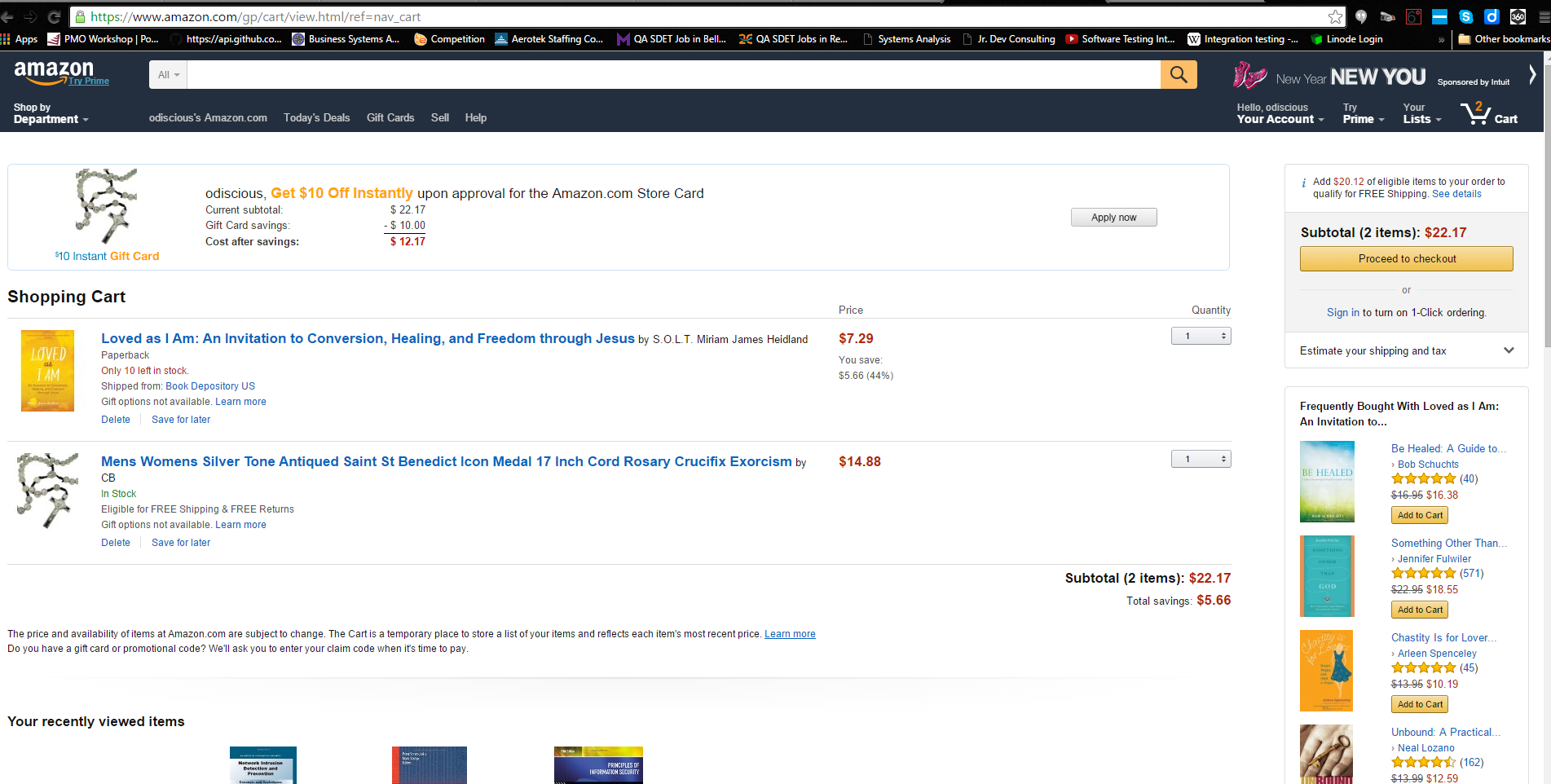


Figure 2: Amazon Shopping Cart Page - Your Shopping Cart is empty. (2016). Retrieved January 5, 2016, from https://www.amazon.com/gp/cart/view.html/ref=nav\_cart

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.

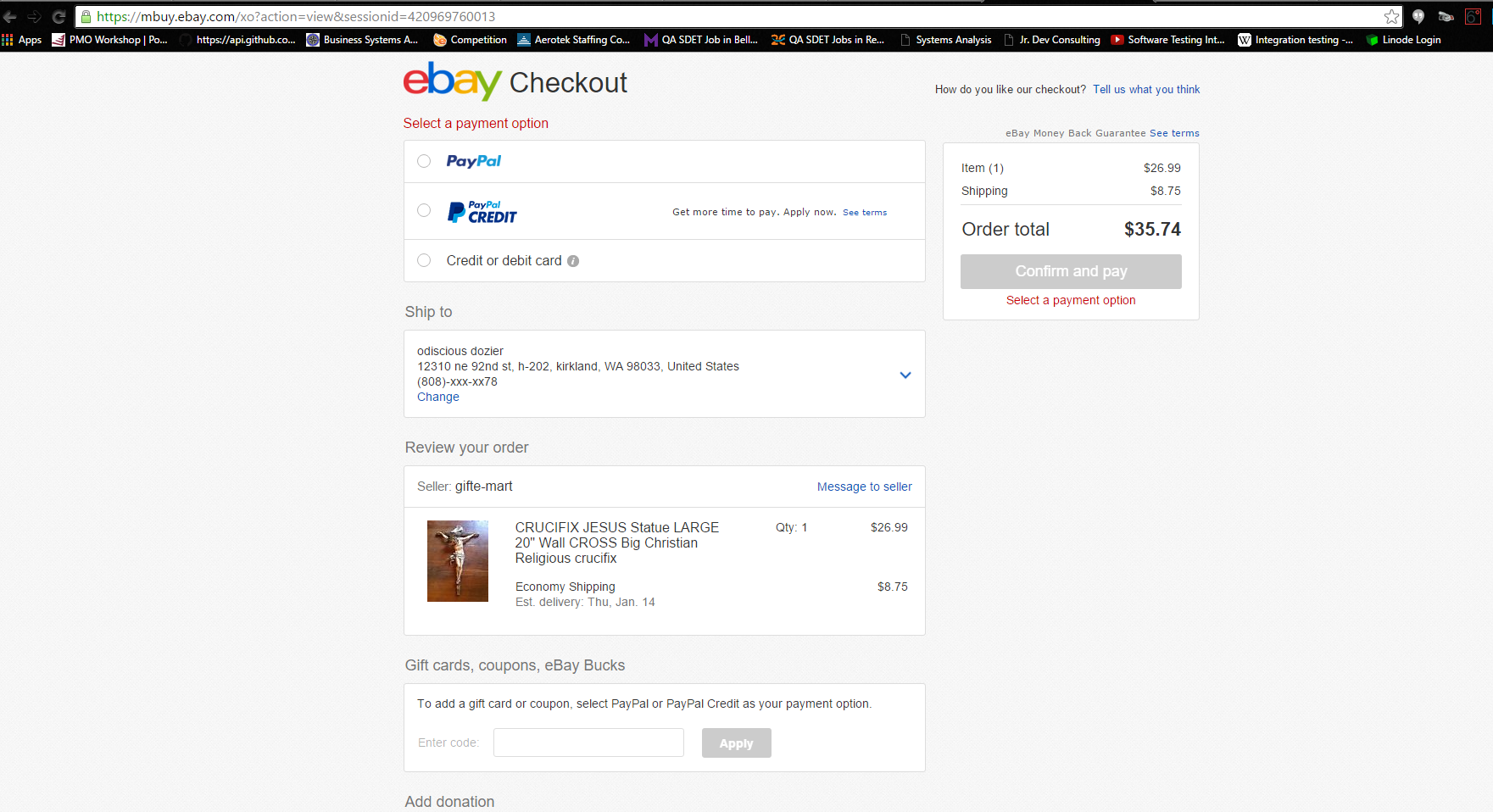


Figure 3: Ebay's Checkout Page - Welcome to eBay. (2016). Retrieved January 5, 2016, from https://mbuy.ebay.com/xo?action=view&sessionid=420969760013

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.

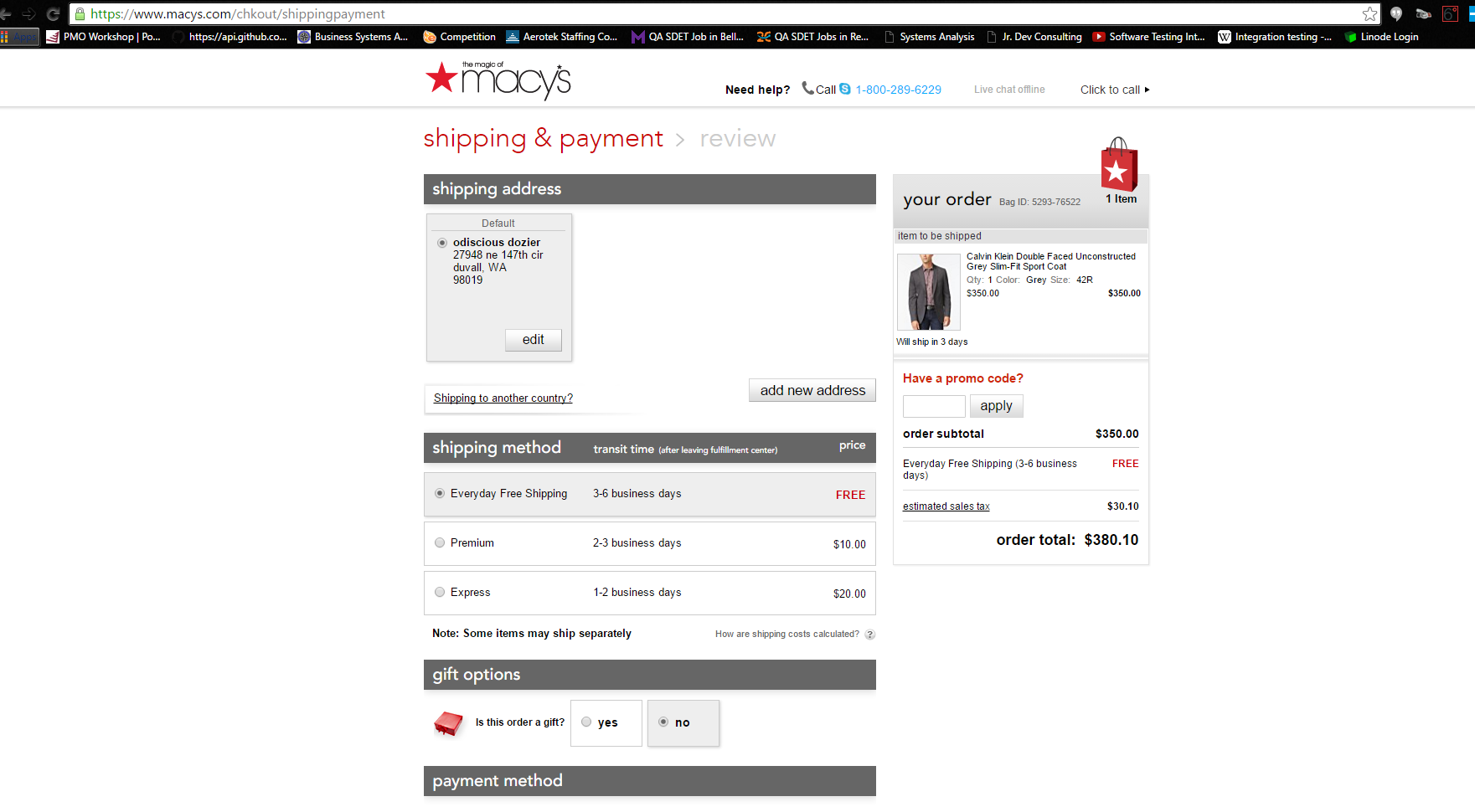


Figure 4: Macy\*s Shipping and Payment Web Page - Shipping and Payment. (2016). Retrieved January 5, 2016, from https://www.macys.com/chkout/shippingpayment

COMPUTER FORENSICS IN ACTION

This section discusses the use of computer forensics to solve cyber-crimes.

CRAIGSLIST ROBBERIES

On May 5th and May 17th, 2009, three men were, charged, plead guilty, and convicted, of robbery charges, involving the online classifieds site Craigslist, in Durham County, North Carolina. Edwin Langolis, 21, Jahid Diggs, 17, and Ashton Darielle Byrd, 17, were the convicted individuals associated with these crimes. Edwin Langolis was the suspected ring leader. There were two victims associated with these crimes (Carlson, 2009).

The first victim was a 36-year old man from Virginia. He stated that he was approached by several armed men and that they robbed him of a, ring, cell phone, and $4,000.00 in cash. There was no instance of physical harm reported.

The second victim was a 34-year old man from Greensboro, North Carolina. He stated that he was able to get away from his attacker. He went on to say that a teenager pointed a gun at him and threatened to shoot him.

The crimes, as stated by Durham County Assistant District Attorney Stormy Ellis, were traced to the home of one of the suspects. The email address that was associated with the Craigslist posting was traced to the suspect’s modem. With the help of Time Warner Cable, the trace was brought to the suspect’s home address.

According to Ryan Johnson, a consultant with Forward Discovery, a company contracted/hired to track down the suspects electronically, suggested that the evidence was overwhelming. His team was able to find a tremendous amount of Craigslist ads that were placed using the suspect’s computer. His team was also able to find emails to and from not only the victims who were robbed, but also potential victims. It was further deduced that the computer evidence proved to be very damning.

U.S. v. DIAZ – MARIJUANA POSSESSION – NEW MEXICO

On March 19th, 2007, Jesus Manuel Diaz was arrested for the possession of more than 3,300 pounds of marijuana in New Mexico. This case required the use of computer forensics to discern that a false bill of lading was created and used by the defendant, a truck driver (“U.S. v. Diaz”, 2009).

Jesus Manuel Diaz was the owner-operator of a company known as JD Easyline, a one rig trucking company. At approximately 9:40am, he drove his tractor-trailer eastbound through the Port of Entry in Gallop, New Mexico. Upon entering the lobby, to obtain permits to drive the rig across New Mexico, he met Motor Transportation Division officer James Smid.

Due to irregularities in weight and abnormal driver decision making, officer Smid was quickly able to deduce suspicious activity. At 9:45am, officer Smid informed Diaz that he was going to perform a Level Two Regulatory Inspection of his tractor-trailer. The search revealed irregularities in Diaz’s, log book, demeanor, cell phone quantity and usage, CB radio equipment, and trailer cargo. By 10:17am, officer Smid was confident that Diaz’s trailer contained contraband. In searching further, and with the help of a K-9 unit, a plywood tunnel that was built into the trailer was discovered. Its contents produced 230 bundles of marijuana that grossed over 3,300 pounds in weight. Diaz was placed under arrest at 12:45pm.

During the trial, a computer forensics expert was called upon to testify to the evidence procured from various electronics found during the search and seizure process. The expert testified that Diaz owned a computer that had a bill of lading program deleted from the computer a day before Diaz’s arrest. Diaz was also found to possess a bill of lading for a return trip from Georgia that was identical to the one presented to officer Smid, only the cargo was listed in a different sequence or order.

THE FLOPPY DID ME IN

Dennis Rader, born March 9th, 1945, is a 70 year old convicted serial killer living out 10 consecutive life sentences in a Kansas State prison (Hansen, 2006).

Dennis Rader was the first of four sons born to William and Dorothea Rader and he was baptized at Zion Lutheran Church in Pittsburg, Kansas. As a young boy, Dennis joined the Boy Scouts and participated in church youth group activities. It wasn’t until he was in grade school that he started having fantasies about, tying people up, controlling them, and torturing them. As he became sexual, his fantasies moved toward tying girls up and having his way with them (“Dennis Rader”, n.d.).

In 1965, Rader entered Kansas Wesleyan College in Salina, Kansas. He wasn’t earning very good grades and worked a couple of jobs to make ends meet. It was here that he first started ‘trolling’ for victims, as he puts it (Magnus, 2005).

In 1966, Rader joined the United States Air Force. Here he earned ranks up to and including sergeant. During this period, he started having sexual relations using prostitutes. Eventually, he attempted to engage in bondage activities with these prostitutes which was rejected. In his personal journal, there was no mention of any activities other than stalking and no victims, at this point, were mentioned.

Amongst other jobs and completing his Associates degree in Electronics, Rader worked for Cessna, a small aircraft manufacturer. In 1973, he was let go by Cessna due to the oil embargo crisis which caused sales to plummet. This caused him to slip into a state of unhappiness falling deeper into his childhood fantasies.

On January 15th 1974, Rader broke into the home of his first victims – the Oteros family. For just about 30 years, Rader evaded and taunted the authorities. Finally, on February 25, 2005, Rader was taken into custody. In an attempt to communicate with authorities, Rader was misled and ended up sending in a disk to the police. The computer forensics team’s investigation revealed a file that had been saved by someone known as, Dennis. “They also found that the disk had been used at the Christ Lutheran Church and the Park City library” (Hansen, 2006).

CONCLUSION

This discussion included some of the technological protocols and steps in providing consumer protection and moves to a discussion about the empowerment of law enforcement with the use of computer forensics. With the help of secure purchasing, consumers and vendors alike can now make online purchases with confidence. With the aid of computer forensics, cases that might have been considered unsolvable can now reach resolution with minimal costs on manpower and resources.

REFERENCE

Carlson, K. (2009, January 13). Computer forensics helped solve Craigslist robberies :: WRAL.com. Retrieved January 5, 2016, from <http://www.wral.com/news/local/story/4305416/>

Dennis Rader - BTK Killer - a Biography. (n.d.). Retrieved January 6, 2016, from <http://dennisraderbtk.blogspot.com/>

Hansen, M. (2006, April 21). How the Cops Caught BTK. Retrieved January 6, 2016, from <http://www.abajournal.com/magazine/article/how_the_cops_caught_btk/>

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

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>

Magnus, E. (2005, August 24). 31 years of the BTK killer. Retrieved January 6, 2016, from http://www.nbcnews.com/id/8916264/#.VoyRlxUrKUk

Secure Electronic Transactions. (n.d.). Retrieved January 5, 2016, from [http://www.davidreilly.com/topics/electronic\_commerce/essays/secure\_electronic\_transa ction](http://www.davidreilly.com/topics/electronic_commerce/essays/secure_electronic_transa%09ction)s.html

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

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

U.S. v. Diaz - Marijuana possession - New Mexico. (2011, November 29). Retrieved January 5, 2016, from http://infosecusa.com/us-v-diaz-marijuana-possession-new-mexico

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>