

## Unlawful Redemption and How to Fight Back using Automated Inspection of X-Ray Cargo Images using ZAP OWASP, Image Stenography, Mobile Device Forensics, Port Authority Mobile Application, Machine Learning, Cassandra, MongoDB NoSQL Databases

**Wilbert A McClay\***

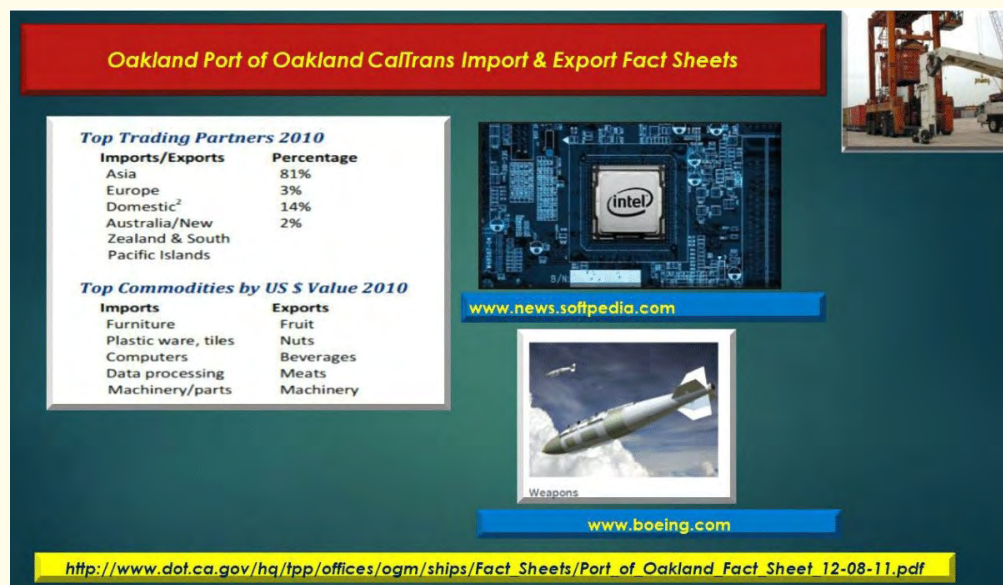
Northeastern University, USA

**\*Corresponding Author:** Wilbert A McClay, Northeastern University, USA.

**Received:** July 19, 2017; **Published:** July 26, 2017

### Case Study

The Port of Oakland randomly screens millions of cargo containers every day using the SAIC VACIS (Vehicle and Cargo Imaging System) for random threats from weapons and ammunitions, human trafficking, counterfeit items, and drugs. The SAIC VACIS X-Ray Systems scans cargo containers randomly for threats utilizing statistical analysis to find threats. Furthermore, “the Port of Oakland loads and discharges more than 99% of the containerized goods moving through Northern California, the nation’s fourth largest metropolitan area. Oakland’s cargo volume makes it the fifth busiest container port in the United States, and ranks San Francisco Bay among the three principal Pacific Coast gateways for U.S. containerized cargoes, along with San Pedro Bay in southern California and Puget Sound in the Pacific Northwest. About 75.82% of Oakland’s trade is with Asia. Europe accounts for 13.52%, Australia/New Zealand and Oceania about 5.25% and other foreign economies about 5.38%. About 0.2% of Oakland’s trade is domestic (Hawaii and Guam) and military cargo. California’s three major container ports carry approximately 50% on the nation’s total container cargo volume [1-3]”.



**Illustration A:** Port of Oakland Import and Export Fact Sheet and military cargo.

An organized criminal syndicate corporation are working together using the internet and cargo containers for smuggling of random threats typically for financial gain. Moreover, they have hired a former Top-Secret government employee to work as a contractor for their international corporation. The Top-Secret government contractor employee is oblivious to the nature of the international criminal syn-

dicating corporation business practices and framework, and is extorted into a dangerous liaison as an indentured servant committed to destroy his career and life. The final impediment which almost cost the Top-Secret government contractor, his life was the theft of his belongings, vehicle, and finances, which warranted retribution at all costs to save his life. The Top-Secret government contractor contacted his father a disabled former U.S. Army Captain and Medical Doctor for assistance in Louisiana. The Top-Secret government contractor and his father utilize their resources of contacting former government allies, friends, teachers, private investigators, and associates to strategically combat the international organized criminal syndicate corporation. The Top-Secret government contractor with his aunt a retired teacher and cousins whom are instructors at "America's Promise" funded by General Colin Powell design a corporation called, "Just Us Youth" to assist impoverished communities and at-risk youths with poor parental controls and deleterious health conditions, such as obesity, asthma, allergies, and cancer. In addition, the Top-Secret government contractor and his father develop a non-profit organization called, "Wolfsmilch Drones", to perform Big Data Analytics and data acquisition with the usage of Aerial drones over impoverished communities and surveillance of communities with high criminal activity to alert law enforcement and federal agencies, to assist in thwarting the malicious efforts of the organized criminal syndicate corporation.

This article involves a real-life scenario which is highly relevant during this new millennium. Moreover, the innovative aspect of utilizing Big data, NoSQL databases with computer forensics demonstrates the next generation technology for criminal investigations and procedures.

It is necessary to sort through diverse categories and evidence which is considered structured and unstructured, using network forensics tools (e.g. ZAP, and machine learning algorithms for detection and classification of cargo container threats. The computational rigor to sort through diverse categories and terabytes of information using advanced forensic tools, machine learning, and NoSQL databases to detect malicious behavior and trends will be discussed in this manuscript.

## Setup

Acrylic WIFI Analyzer

OWASP ZAP Version 2.6.0

Linux Stenography Tool, Steghide

www.tinypics.com (image hosting account)

MongoDB NoSQL database running on Windows Operating System

Emacs editor, Linux C/C++ compiler and graphical image libraries (i.e. libtiff) for image analysis.

Google Chrome Internet Browser

Windows BING Internet Browser

Google Play Applications Store: Port Authority Mobile Application

## System Requirements

"As we will be using virtual machine images to create a cluster, you will need a computer that is relatively high specifications, to do the hands-on exercises. Specifically, the computer needs to have the following:

64-bit operating system (Mac, Windows, or Linux)

8GB (or more) of RAM

30GB (or more) of free hard drive space

Linux version Cassandra NoSQL database for Linux Operating System

Latest version of VMware Player installed and working [25]".

### Case Study

In this scenario, we demonstrate how a competent and resourceful Fortune 500 ChipMaker Pinkerton Security network administrator alerts the Federal Bureau of Investigations (FBI) to catch the individuals involved in the international criminal syndicate organization by sending them inside information. The international criminal syndicate corporation recently stole the highly lucrative Fortune 500 ChipMaker microchips from the Fortune 500 Defense Contractor military contractors advanced Weaponry Program, which are worth millions, illustrated in Figure B.



**Illustration B:** Oakland Port Authority Export of military products for Fortune 500 Defense Contractor military Defense Contractor.

As a decoy, the international criminal syndicate corporation has placed 2 disc-shaped threat containers inside of 2 different Fortune 500 Defense Contractor military weaponry SUVs’ for the Directed Energy program. The criminal syndicate are aware that the Fortune 500 Defense Contractor military SUVs’ will be searched onsite at the Oakland Port Authority, thus to camouflage the threat container on 1 of the Fortune 500 Defense Contractor SUVs’, the threat container containing an explosive detonator device, which is placed on the outside of the vehicle and draped with a wire connected to an explosive located near the gas tank. The other non-threat container is placed inside the vehicle and when initially searched by Oakland Port Authority Security guards it displays as a container with benign microchips which appears oblivious to the Oakland Port Authority Security.

The Fortune 500 ChipMaker Pinkerton Security organization has been informed by Fortune 500 ChipMaker high level management to keep the confiscated microchips highly confidential due to the financial risk assessment for loss of public trust and stock market equity for stakeholders. Thus, in hopes to ameliorate and thwart the malicious syndicate activity the Fortune 500 ChipMaker Pinkerton Security organization has secretly contacted the FBI and CIA to capture or terminate the organized criminal syndicate corporation individuals by any means necessary, and to recover the highly lucrative Fortune 500 ChipMaker micro-chips in the immediate future.



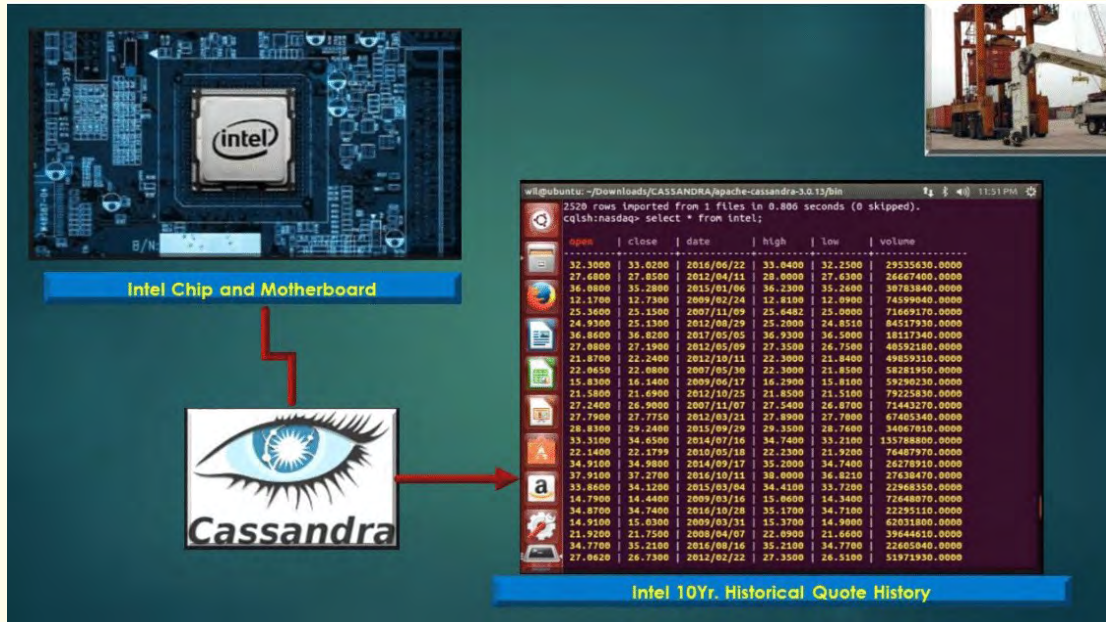


Illustration C: Fortune 500 ChipMaker Microchip and 10yr. Fortune 500 ChipMaker Historical Stoke Market Quotes

The FBI and Central Intelligence Agency (CIA) have been monitoring the criminal syndicate under investigation for a vast amount of time, since both containers will be shipped overseas.

The FBI SWAT team has been utilized since the FBI is a domestic law enforcement agency and to terminate the criminal syndicate before the explosive threat container explodes at the Oakland Port Authority after the non-threat SUV is shipped in a cargo container overseas, and presents a harder task for the CIA to apprehend the stolen Fortune 500 ChipMaker microchips abroad. The FBI SWAT utilizes ZAP OWASP to find vulnerabilities in the organized criminal syndicate corporation's network by placing an undercover FBI agent as a benign data scientist for the organized international criminal syndicate corporation. The undercover FBI agent (Agent 7) is utilizing a Linux Virtual machine and a series of tools (i.e. machine learning algorithms, stenography tools for instance Linux Steghide, Acrylic with other mobile forensics and vulnerability tools, and MongoDB, and Cassandra NoSQL databases for uncovering the information and high stakes espionage of criminal activity and passing the information to the FBI Cloud Security SWAT team with the undercover FBI agents out-sourced private cloud security network utilizing virtual machines and network information to hidden instructions and information, for the termination of the organized international criminal syndicate individuals.

### Background on Investigative Data Mining to Fight Terrorism

During 2003, Federal Computer Week (FCW) wrote an article: "Investigative Data Mining Part of Broad Initiative to Fight Terrorism [10,11]". The FCW article states, "investigative data mining and analytical software comb vast amounts of digital information to discover patterns and relationships that indicate criminal activity". This form of analysis to discover patterns in criminal activity is considered forensic data analysis.

Computer Forensics Data Analysis (CFDA) is considered one of the most data-intensive areas of information security [12-24]. The use of machine learning in computer forensics data analysis is a form of Artificial Intelligence (AI) that instructs a computer to learn without

having to be explicitly programmed to find patterns in criminal activity. The significant benefits from applying machine learning algorithms to CFDA are: to evaluate data of forensic images, novel automation and training tools for forensic software analysis, and investigating system logs or logged network traffic after a security incident or predict a future vulnerability.

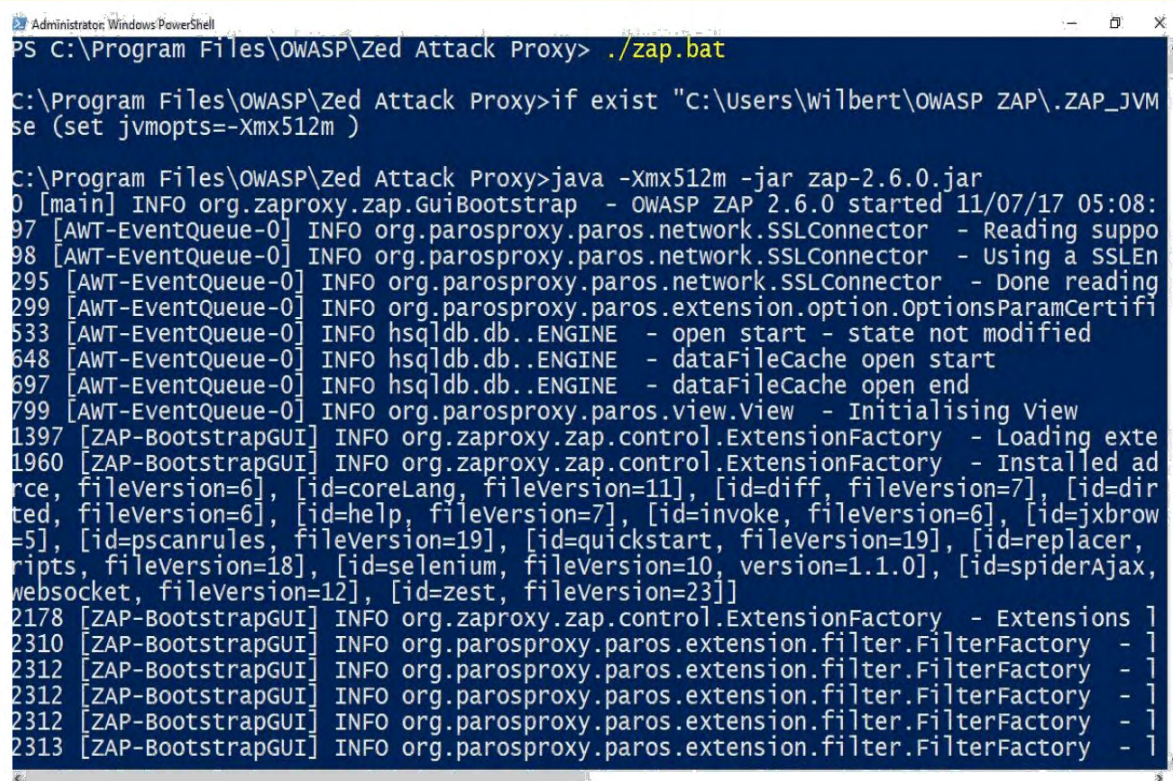
The primary objective of utilizing machine learning algorithms and NoSQL databases is to focus attention on the most relevant and important information related to solving an investigation. Secondly, the cybersecurity researcher would predict future vulnerabilities and automate the inspection of extremely large volumes of forensic data.

Thus, the need for penetration testing to exploit vulnerabilities for inspection and analysis is crucial to track malicious, criminal activities in penetration-testing forensics. In this study, we utilize ZAP OWASP, Linux Stenography Tools, Mobile Forensics for Android Devices, Machine learning, Image Processing, Apache Spark, MongoDB, and Cassandra NoSQL databases; for penetration testing to investigate this highly important are of computerized forensics data analysis.

### OWASP ZAP Version 2.6.0

“OWASP ZAP version 2.6.0 is a fork of the opensource Paros Proxy product originally developed by Chinotec Technologies Company. The OWASP ZAP product includes software’s developed by the Apache Software Foundation at <http://www.apache.org> licensed under Apache License 2.0 HSQLDB under BSD license, and JDIC is licensed by Sun Microsystems, Inc [8]”. OWASP ZAP additionally contains BeanShell under the LGPL license.

The ZAP penetration tool is utilized to detect vulnerabilities in web based applications, and its primary utilization is for individuals with a diverse domain of security expertise, and is quintessential for vulnerability and penetration testing for security researchers and developers. Additional enhancements of ZAP are provisioned with automated scanners and a compilation of tools, which the security researcher would utilize to detect and classify security vulnerabilities manually. However, from the command line Windows Power shell executed in Illustration D, below displaying the process which can be invoked automatically with the “./zap.bat” script on Windows PowerShell. In addition, using the Linux command line in a Linux Ubuntu Virtual machine by “./zap.sh” which can also run other processes and commands inside a Linux based bash shell script for instance with the usage of sed commands for data cleansing (e.g. spurious characters (misplaced quotes or semicolons)).



```
Administrator: Windows PowerShell
PS C:\Program Files\OWASP\Zed Attack Proxy> ./zap.bat

C:\Program Files\OWASP\Zed Attack Proxy>if exist "C:\Users\wilbert\OWASP ZAP\ZAP_JVM
se (set jvmopts=-Xmx512m )

C:\Program Files\OWASP\Zed Attack Proxy>java -Xmx512m -jar zap-2.6.0.jar
0 [main] INFO org.zaproxy.zap.GuiBootstrap - OWASP ZAP 2.6.0 started 11/07/17 05:08:
97 [AWT-EventQueue-0] INFO org.parosproxy.paros.network.SSLConnector - Reading suppo
98 [AWT-EventQueue-0] INFO org.parosproxy.paros.network.SSLConnector - Using a SSLEn
295 [AWT-EventQueue-0] INFO org.parosproxy.paros.network.SSLConnector - Done reading
299 [AWT-EventQueue-0] INFO org.parosproxy.paros.extension.option.OptionsParamCertifi
533 [AWT-EventQueue-0] INFO hsqldb.db..ENGINE - open start - state not modified
648 [AWT-EventQueue-0] INFO hsqldb.db..ENGINE - dataFileCache open start
697 [AWT-EventQueue-0] INFO hsqldb.db..ENGINE - dataFileCache open end
799 [AWT-EventQueue-0] INFO org.parosproxy.paros.view.view - Initialising View
1397 [ZAP-BootstrapGUI] INFO org.zaproxy.zap.control.ExtensionFactory - Loading exte
1960 [ZAP-BootstrapGUI] INFO org.zaproxy.zap.control.ExtensionFactory - Installed ad
rce, fileVersion=6], [id=coreLang, fileVersion=11], [id=diff, fileVersion=7], [id=dir
ted, fileVersion=6], [id=help, fileVersion=7], [id=invoke, fileVersion=6], [id=jxbrow
=5], [id=pscanrules, fileVersion=19], [id=quickstart, fileVersion=19], [id=replacer,
cripts, fileVersion=18], [id=selenium, fileVersion=10, version=1.1.0], [id=spiderAjax,
websocket, fileVersion=12], [id=zest, fileVersion=23]]
2178 [ZAP-BootstrapGUI] INFO org.zaproxy.zap.control.ExtensionFactory - Extensions 1
2310 [ZAP-BootstrapGUI] INFO org.parosproxy.paros.extension.filter.FilterFactory - 1
2312 [ZAP-BootstrapGUI] INFO org.parosproxy.paros.extension.filter.FilterFactory - 1
2312 [ZAP-BootstrapGUI] INFO org.parosproxy.paros.extension.filter.FilterFactory - 1
2312 [ZAP-BootstrapGUI] INFO org.parosproxy.paros.extension.filter.FilterFactory - 1
2313 [ZAP-BootstrapGUI] INFO org.parosproxy.paros.extension.filter.FilterFactory - 1
```

Illustration D: Running ZAP by Windows PowerShell command line using “./zap.bat” script.

Next, we evaluate the default gateway ATT264 network in the Windows PowerShell to view MAC Addresses and IP information at 192.168.1.254, utilizing Window ipconfig network command, denoted in Illustration E, below.



```

Administrator: Windows PowerShell
Temporary IPv6 Address . . . . . : 2602:306:cc3c:7130:b03a:ec32:917a:f9f0
Temporary IPv6 Address . . . . . : 2602:306:cc3c:7130:bcd9:b862:4997:1749
Link-local IPv6 Address . . . . . : fe80::896b:60ee:f4bf:f0f3%8
IPv4 Address . . . . . : 192.168.1.172
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::3a6b:bbff:fec1:62d0%8
                          192.168.1.254

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . . : 
Link-local IPv6 Address . . . . . : fe80::75b4:c077:db66:8874%5
IPv4 Address . . . . . : 192.168.79.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . . : 
Link-local IPv6 Address . . . . . : fe80::31c8:39a0:6cc:af36%18
IPv4 Address . . . . . : 192.168.60.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : 
    
```

**Illustration E:** Demonstrates dubious and hidden VMware virtual machines VMnet1 and VMnet8.

In Illustration E (above), we notice 2 possible unknown Virtual machines running and proceed with a OWASP ZAP vulnerability and penetration-testing scan report on default gateway, <http://192.168.1.254/cgi-bin/home.ha>.

However, in Illustration F (below), emanating a ZAP OWASP vulnerability and penetration test on the default gateway, <http://192.168.1.254/cgi-bin/home.ha>, we notice a major alert of click-jacking alerts. A Click-Jacking indicates a security risk where malware installation through phishing include XFS exploits with click-jacking attacks. The click-jacking attack proceeds as follows the victim is malicious mislead and perjured by performing undesired actions with malware. An example from a malicious hacker mobile engineering perspective is to click on a malicious link in emails and messages that consist of “malware payloads” [25].

**ZAP Scanning Report**

**Summary of Alerts**

Risk (Level)	Number of Alerts
High	0
Medium	7
Low	7
Informational	0

**Alert Detail**

**Medium (Medium)** **ClickJacking**

**Description:** X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

**URL:** https://192.168.1.254/cgi-bin/home.ha

**Method:** GET

**Parameter:** X-Frame-Options

**URL:** https://192.168.1.254/cgi-bin/home.ha

**Method:** GET

**Parameter:** X-Frame-Options

**Instances:** 2

**Solution:** Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed) by pages on your server (a.g. as part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM is only for specific websites to frame the web page. In supported web browsers.

**Reference:** <http://blog.troyhunt.com/2010/03/30/combating-clickjacking-with-x-headers/>

**CWE id:** 116

**WASC id:** 15

**Source id:** 3

**Low (Medium)** **Web Browser XSS Protection Not Enabled**

**Description:** Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server.

**URL:** http://192.168.1.254/cgi-bin/home.ha

**Method:** GET

**Parameter:** X-XSS-Protection

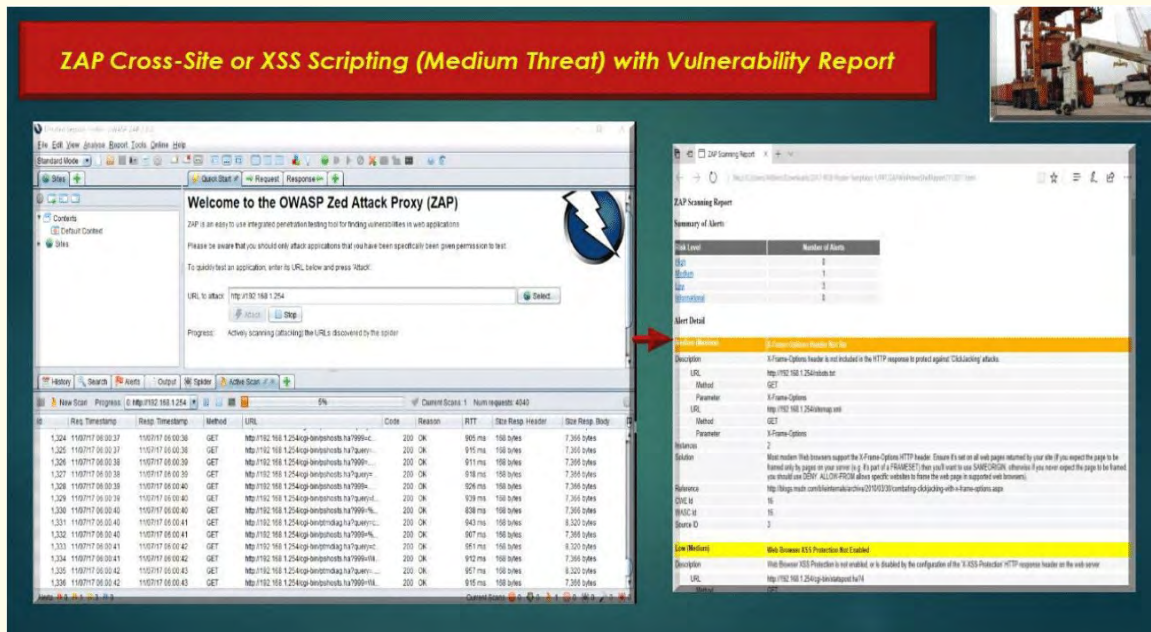
**URL:** http://192.168.1.254/cgi-bin/home.ha

**Method:** GET

**Parameter:** X-XSS-Protection

**"ClickJacking Attacks Alerts" on June 18, 2017**

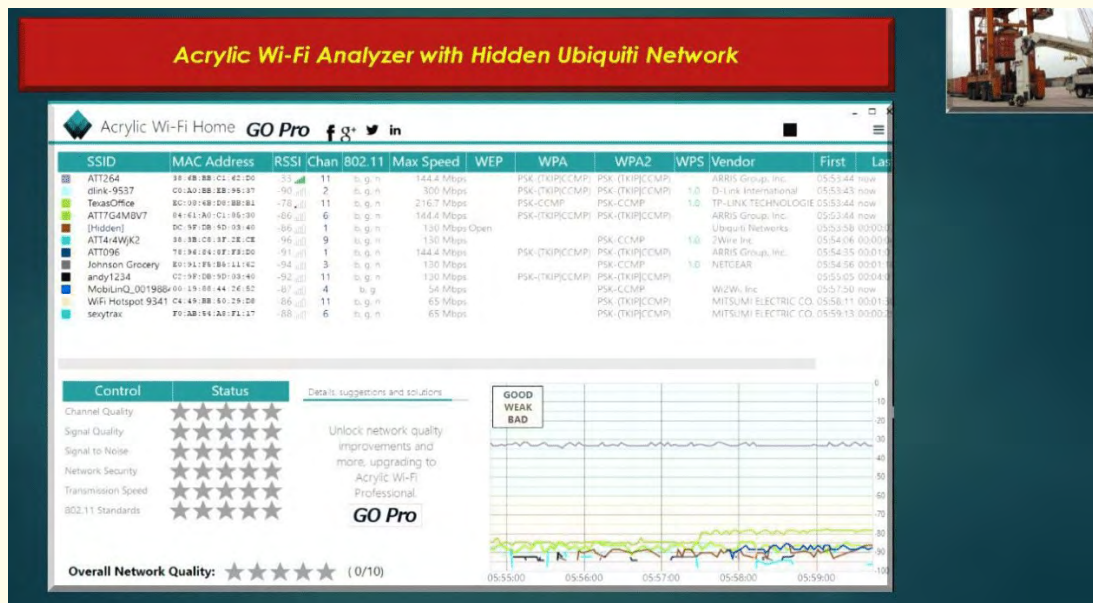
**Illustration F:** “Click-Jacking Attack”, on June 18, 2017 demonstrated in OWASP ZAP vulnerability scan.



**Illustration G:** Scan report from ZAP using Port Authority Mobile Application of Common Gateway Interface (CGI) <https://192.168.1.254/cgi-bin/home.html>. The OWASP ZAP Scan.

Report illustrates a Medium Threat of a Cross-Site Scripting attack, which indicates a browser setting needs to be enabled to thwart this issue in Microsoft Windows BING.

Acrylic Wi-Fi Analyzer to discover other networks and displaying a Hidden Ubiquiti Network on July 11, 2017.



**Illustration H:** Acrylic WIFI Analyzer displaying Hidden Network, Ubiquiti Networks.

Acrylic WIFI Professional is a Tarlogic Security: cybersecurity start-up. The main impetus of Tarlogic is the goal of providing innovative quality to protect corporations from malicious cyber-attacks and industrial espionage. Moreover, Acrylic WIFI Profession is the quintes-



sentinal WIFI analyzer software to detect and identify access points and WIFI channels to ameliorate any incidences on wireless networks on 802.11 a/b/g/n in real-time. Acrylic WIFI is a logical tool for tenured WIFI security analysts to control and detect wireless network performance and classify access points and transmission speeds [26]. The hidden Ubiquiti Network has a transmission speed of 130Mbps with a MAC Address of DC:9F:DB:9D: 03:40 on channel 1 with hidden WPA and WPA2 encryption.

### Cargo Container VBFA Machine Learning and Sobel Gradient Feature Attraction for Image Processing

Machine learning and image processing algorithms are used to extract features from graphical images within the payload. These extracted features are generated using Sobel Edge operators and other measurements based on the local and global statistical characteristics of the graphical images [4-7], such as the opacity of the image. It calculates the gradient (smooth blending shades) outlines extracted features of a vehicle within an image based on its intensity. Figure 1, 2, 3, and 4, respectively, demonstrated below illustrates the VACIS X-RAY Cargo System shown in Figure 1, X-ray Cargo container ID and registration shown on Figure 2. Figure(s) 3 and 4, illustrates the use of a Sobel Edge Operator and local and global statistics (e.g. average intensity, opacity, and transparency) on X-ray cargo scans of vehicles.



Figure 1: VACIS X-RAY Cargo System.





Figure 2: Port of Oakland Cargo Container Registration and ID.

Inbound	date	Outbound	Total
62546	Sep-04	65037	127583
42573	Feb-03	63742	106315
38203	Feb-04	58755	96958
41595	Mar-01	67247	108842
38128	Nov-01	60099	98227
49162	Mar-04	72452	121614
50942	Oct-03	74549	125491
59700	Jul-04	68049	127749
34944	Feb-02	55405	90349
66760	Aug-04	70321	137081
41296	Apr-02	62250	103546
53072	Jul-03	70933	124005
38829	Jan-01	64052	102881
53433	Apr-04	66405	119838
43327	Oct-01	71441	114768
67896	Dec-04	74196	142092
44286	Jul-01	63465	107751
39498	Jun-01	60197	99695
Inbound	Date	Outbound	Total
52345	Apr-03	62737	115082
50385	Nov-03	67724	118109
52747	Oct-02	50808	103555

CASSANDRA CARGO\_STATS DATABASE in KEYSPACE CARGO\_HOMELAND\_SECURITY  
<http://www.portofoakland.com/>

Figure 2a: Port of Oakland Cargo Container Registration and ID and CASSANDRA Database Cargo Statistics.

In Figures 1, 2, 2a (above) we demonstrate the SAIC VACIS System scanning a cargo container where each respective cargo container has a registration and ID the cargo container statistics for inbound and outbound cargo container traffic with the date; is ingested into the NoSQL Cassandra column oriented database where the rows and columns in the database do not need to be uniform as in a relational database. In addition, if a SAIC VACIS sensor fails scanning a cargo container for instance, opacity the Cassandra database will not crash due to NULL values in the rows for large queries. In addition, Cassandra NoSQL database was utilized for speed and fault tolerance in distributed computing and works well on Linux Virtual Machines particularly for a Cloud provider environment.

### Image Processing with Cargo Bfa generator with Threat Analysis



Figure 3: VACIS x-ray cargo vehicle SUV image with threat.

### VACIS X-RAY CARGO VEHICLE SUV IMAGE WITHOUT THREAT USING CARGOVBFGENERATOR (TRAINING MATRICES)

The figure displays a terminal window and an image processing result. The terminal window shows the command: `./cargoVBFgenerator 50 35 45 0 ROI_44_23Cargo 2003.09.22 13.44.23.tif` and the output: `Total compute time = 25.79 seconds` followed by a list of files written. The image processing result shows a grayscale X-ray scan of a vehicle without a threat, with a blue title bar that reads "VACIS X-RAY CARGO VEHICLE SUV IMAGE WITHOUT THREAT". A red arrow points from the terminal command to the image processing result. A blue arrow points from the image processing result to the terminal output. A small inset image in the top right corner shows a forklift in a warehouse setting.

Figure 4: VACIS x-ray cargo vehicle SUV without threat image and cargo Bfa generator (training matrices) with Computational time = 25.79 seconds.



The VACIS x-ray cargo image without any non-threat explosive or threat explosive discs in the x-ray cargo scanned SUV image is illustrated in figure 3 (above), with an intensity gradient of 50 and utilizes the Cargo Bfa generator with 35 iterations, 45 hidden factors, threat value of 0 with the base name of the cargo output image with generated training matrices and a given input image.

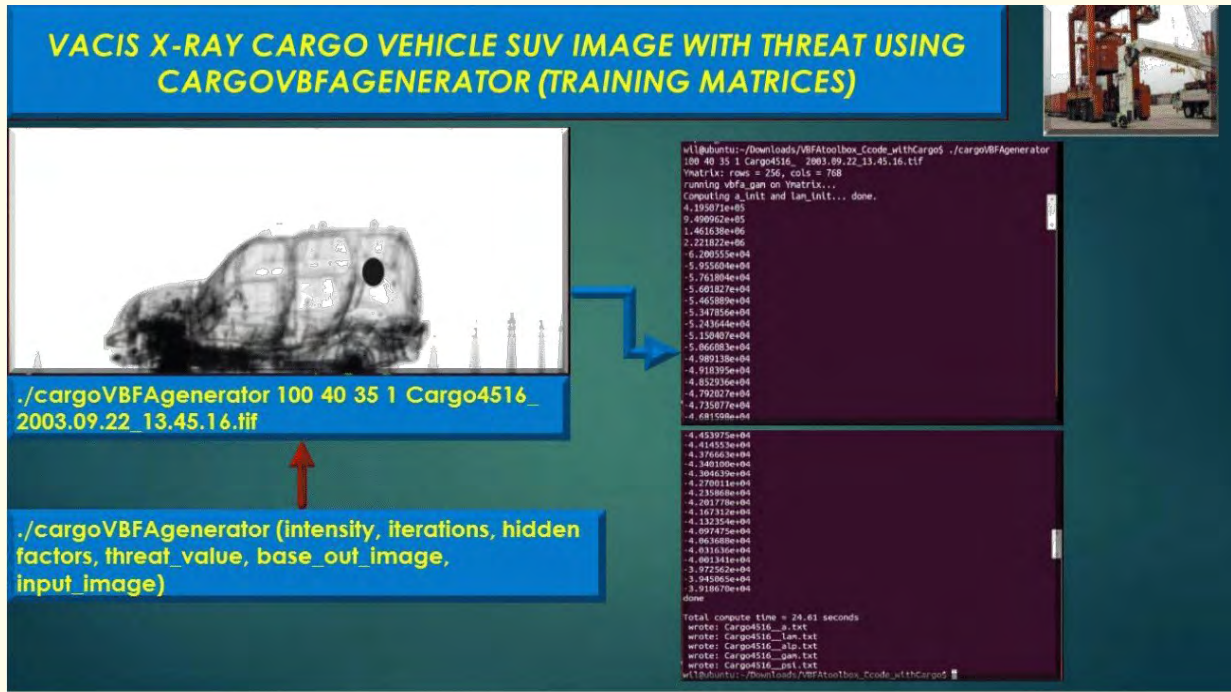


Figure 5: VACIS x-ray cargo vehicle SUV with threat image and cargo Bfa generator (training matrices) with Computational Time= 24.61 seconds.

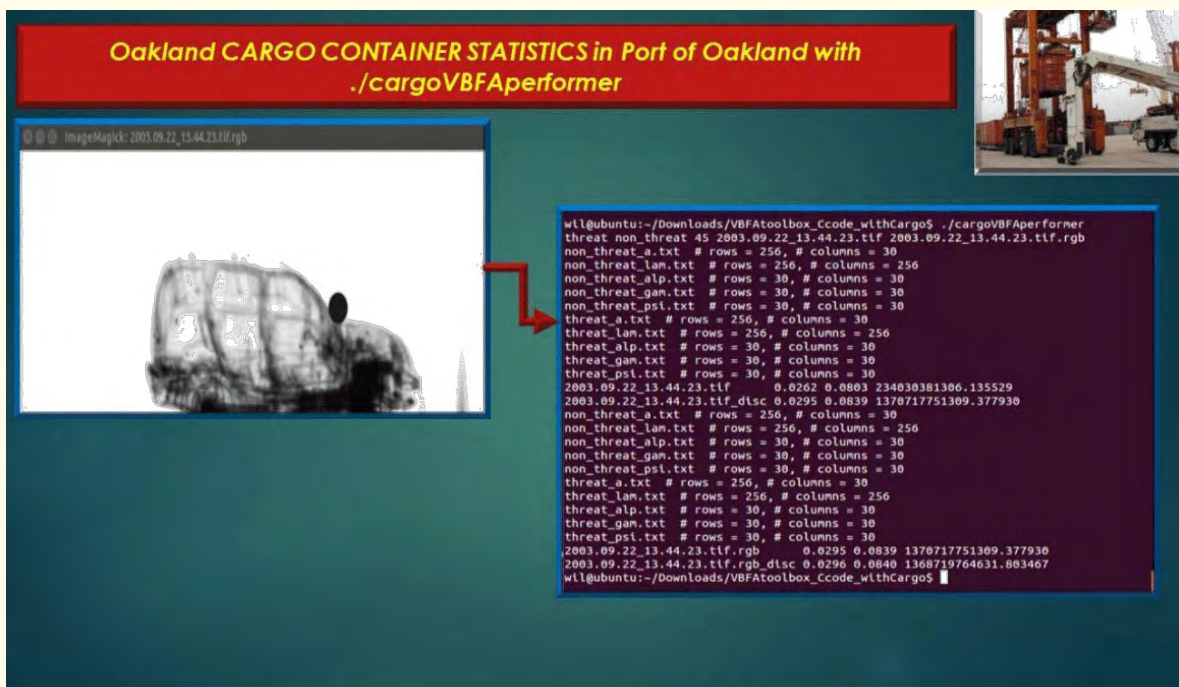


Figure 6: VACIS x-ray cargo vehicle SUV with threat placed in a different location image using cargo Bfa performer displaying the opacity with threat disc referenced on 2003.09.22\_13.44.23.tif.rgb\_disc.

The extracted gradient features from the Sobel feature extraction are to characterize the separability and variability within the images. The Cargo VBFA Performer utilized by Agent 7 involves using the variational Bayesian Factor Analysis (VBFA) classifier to automatically detect and classify the threat image, illustrated in Figure 6, above.



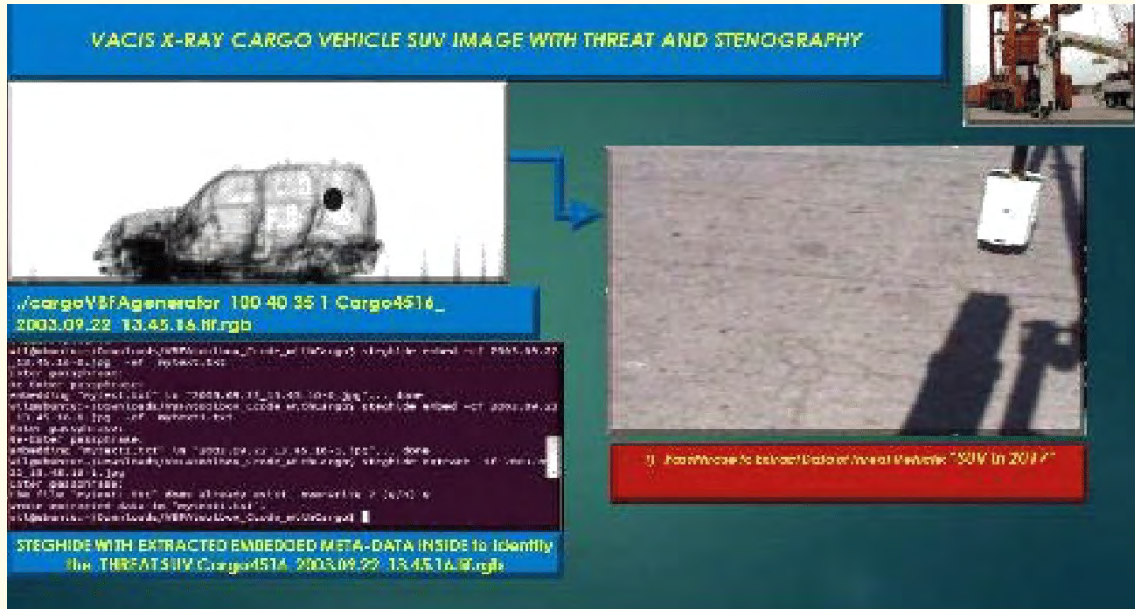


Figure 7: VACIS x-ray cargo vehicle SUV with threat image and hidden meta-data within steghide.

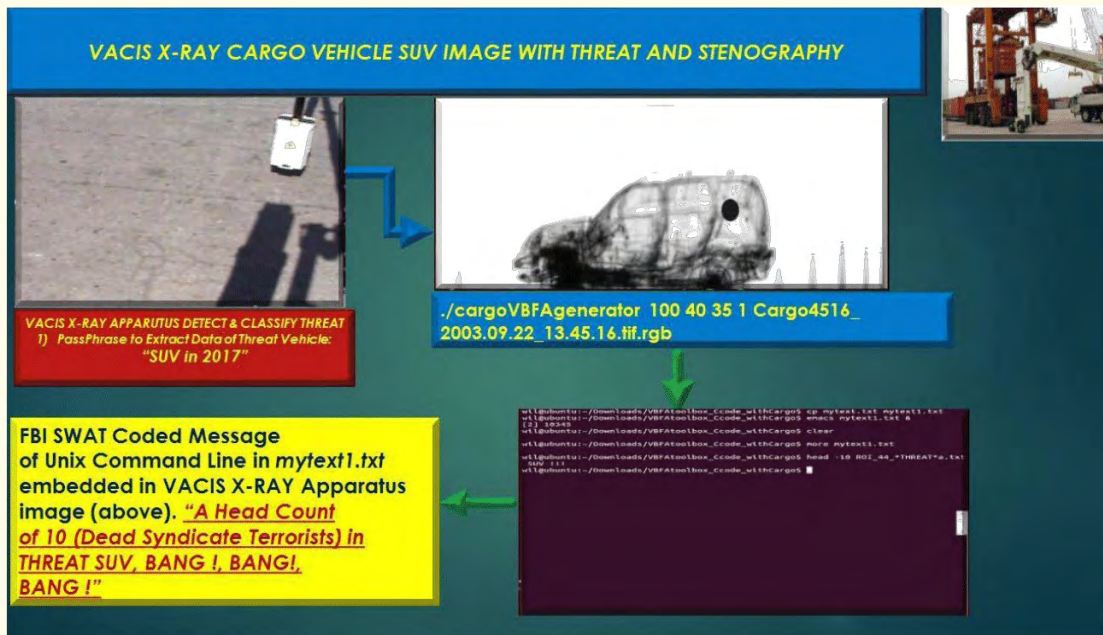


Figure 8: VACIS x-ray cargo vehicle SUV with threat image and hidden meta-data within steghide.

### TINYPIC.COM Account for Information Transfer to Syndicate and Zap Owasp



**Figure 9:** VACIS scanner placed in [www.tinypics](http://www.tinypics.com) URL on specific dates with tagged messages “NEED NOT WORRY, PETRO”, to the organized criminal syndicate and undercover FBI outsourced-cloud security network and analyzing vulnerabilities with ZAP OWASP.

An attempt to communicate the comprehensive procedures to the organized criminal syndicate and undercover FBI outsourced-cloud security provider. A [www.tinypics](http://www.tinypics.com) account was registered by Agent 7 with a hidden message inside utilized with the Linux based Stegography tool known as StegHide. StegHide is very versatile a root user only needs to type `sudo apt-get install steghide` on the Linux command line terminal. Once Steghide is installed a user can begin to embed a file into a jpeg image, illustrated in Figures 7, and 8 above.

#### Phase I. Agent 7 types `steghide embed -cf input-image.jpg -ef textfile.txt`

Enter a passphrase:  
Re-Enter passphrase:  
Linux Steghide displays embedding “textfile.txt” in “input.jpg” ...done.

#### Phase II. Agent 7, extracts the embedded file with the following command

```
$ steghide extract -sf input image.jpg
```

Enter passphrase:  
Linux Steghide displays wrote extracted data to “textfile.txt”.  
Agent 7 issues the following kill command in Linux/Unix commands: `head -10 ROI*THREAT*.txt SUV !!!`, which means a “A Head count of (10 Dead Syndicate Terrorists) in THREAT SUV, BANG! BANG! , BANG!”.

The X-RAY Cargo Apparatus Image with Linux Kill Instructions embedded are uploaded to www.tinypic.com account with Tag line "NEED NOT WORRY, PETRO", illustrated in Figures 10 and 11 (below) and monitored on different days with ZAP OWASP vulnerability Scan reports.



Figure 10: VACIS scanner placed in www.tinypics URL on specific dates with tagged messages "NEED NOT WORRY, PETRO", to the organized criminal syndicate and undercover FBI outsourced-cloud security network and analyzing vulnerabilities with ZAP OWASP.

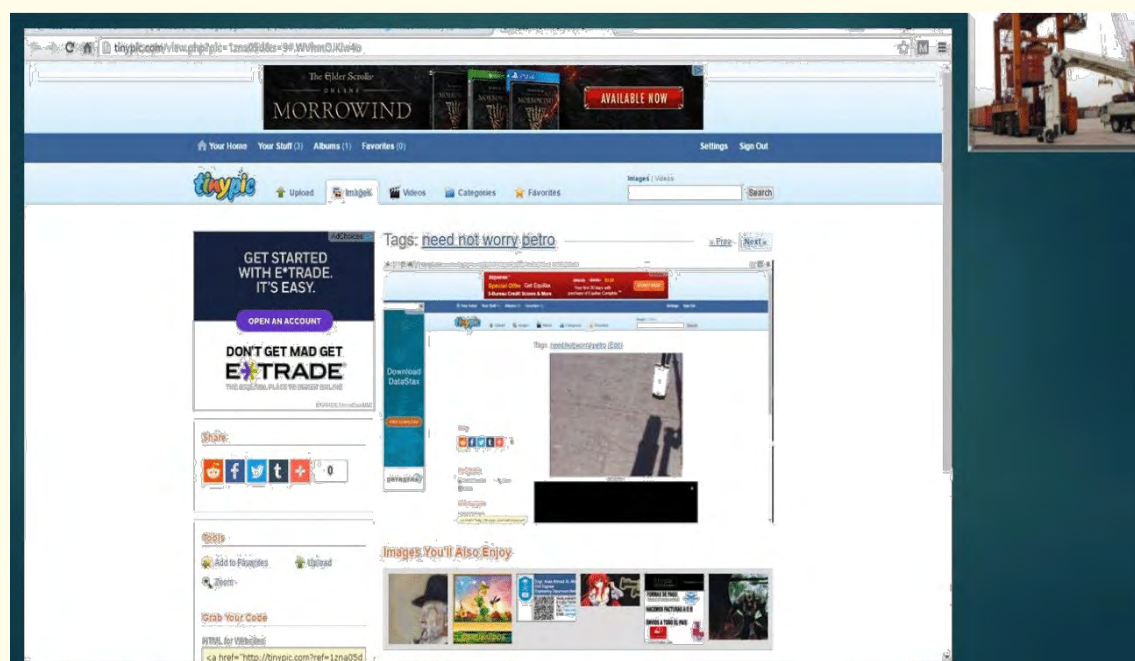


Figure 11: VACIS scanner placed in www.tinypics URL on specific dates with tagged messages "NEED NOT WORRY, PETRO", to the organized criminal syndicate and undercover FBI outsourced-cloud security network and analyzing vulnerabilities with ZAP OWASP.



Cassandra NoSQL Database Acquisition of X-Ray Cargo Statistics and X-Ray Cargo Image Acquisition

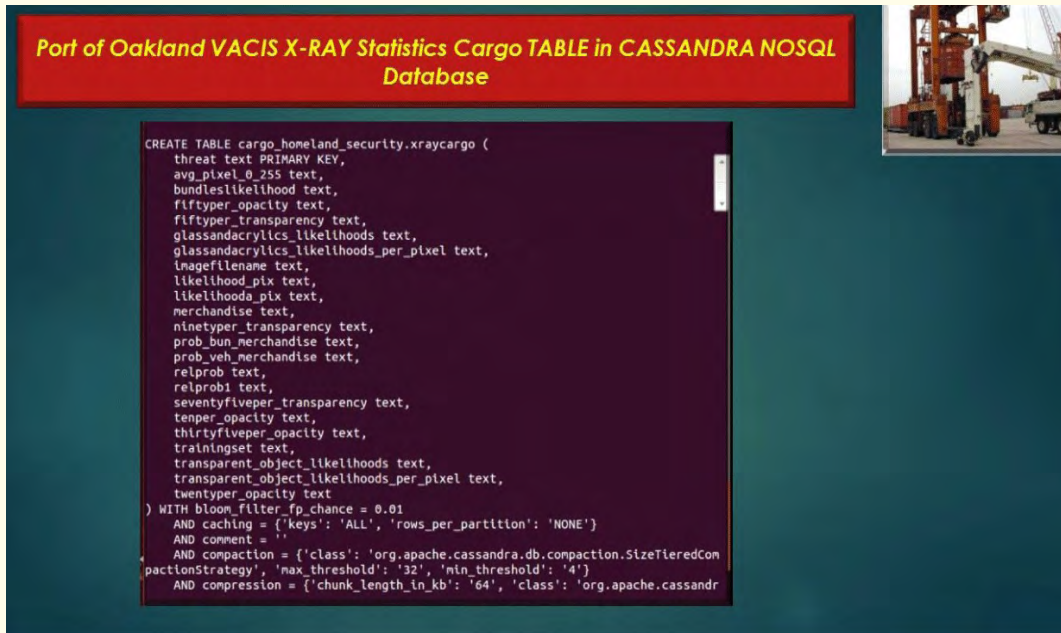


Figure 12: CASSANDRA Port of Oakland VACIS X-Ray Statistics Cargo KeySpace: cargo\_homeland\_security and Table: x-ray cargo.

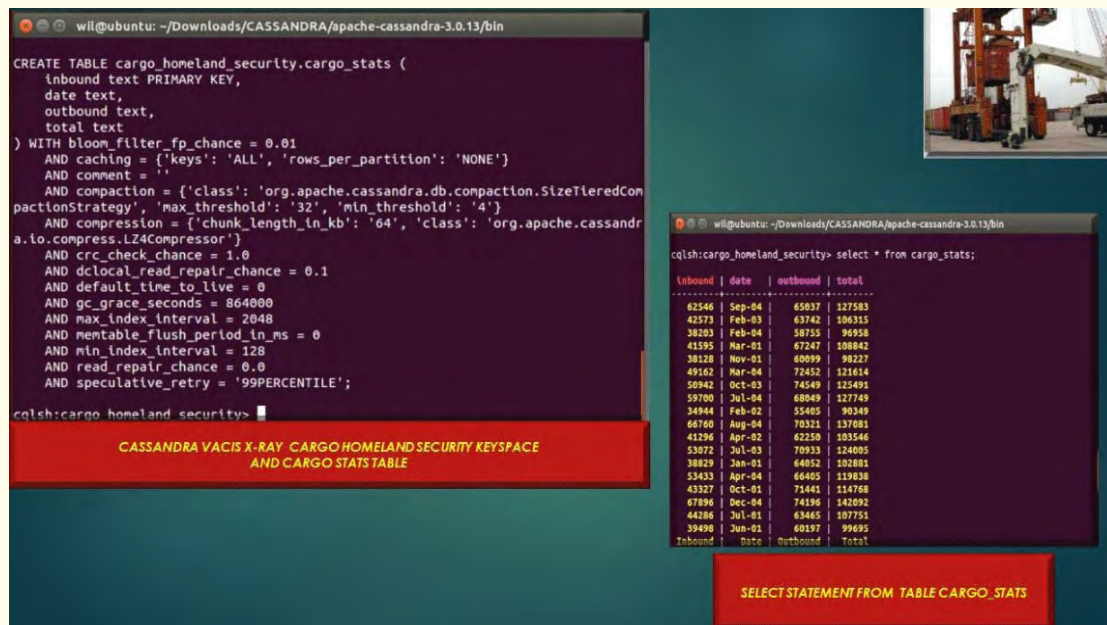


Figure 13: CASSANDRA Port of Oakland VACIS X-Ray Statistics Cargo KeySpace: cargo\_homeland\_security and Table: cargo\_stats.

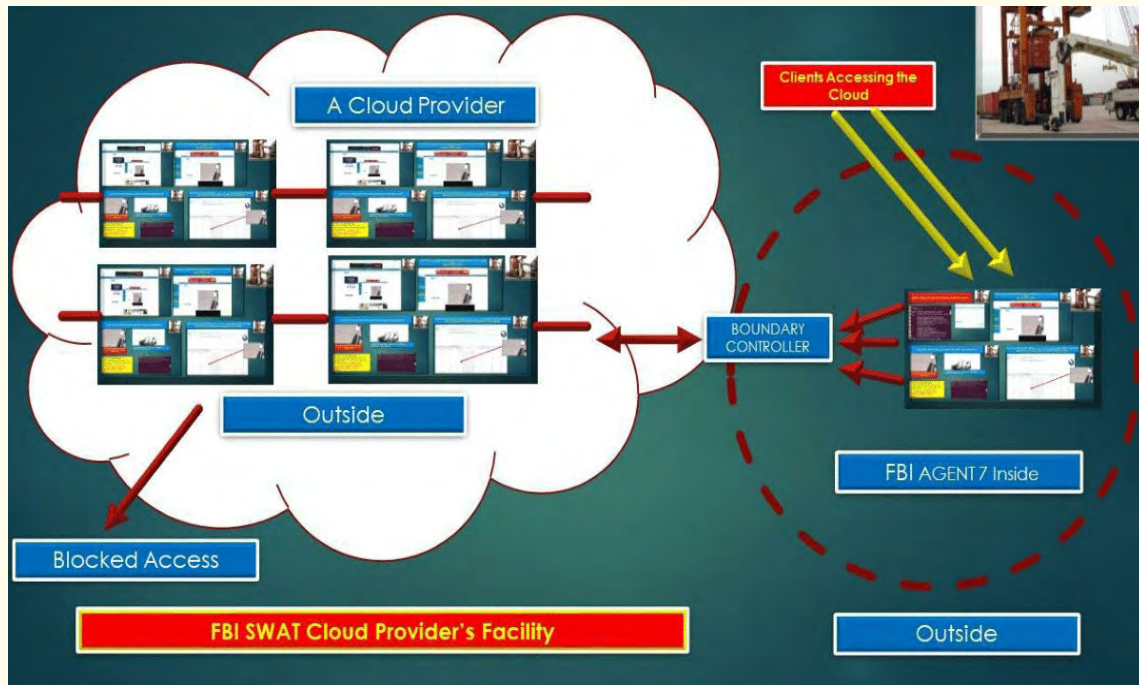


Figure 14: FBI SWAT Out-Sourced Cloud Provider Security and Acrylic Mobile WIFI Analyzer and Agent 7 if config ATT264 Linux Virtual Machine.

The primary aspect of utilizing an FBI out-sourced private cloud scenario from a multi-tenant perspective are that the workload locations are hidden and elasticity of the network may be enhanced or ameliorated dependent on the extent of the criminal investigation. Moreover, for the outsourced-private deployment model in Figure 8 (above), cloud computing can provide elasticity, where Fortune 500 ChipMaker Pinkerton consumer (clients) can rapidly execute requests, receive, and later release multitudes of resources as necessary to the FBI out-sourced private security provider.

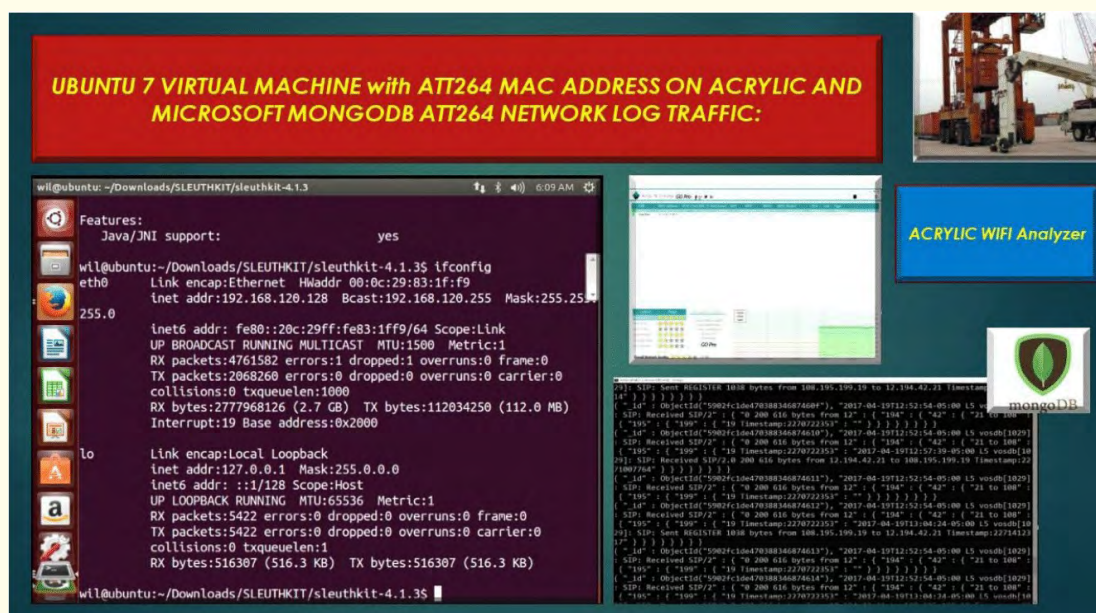
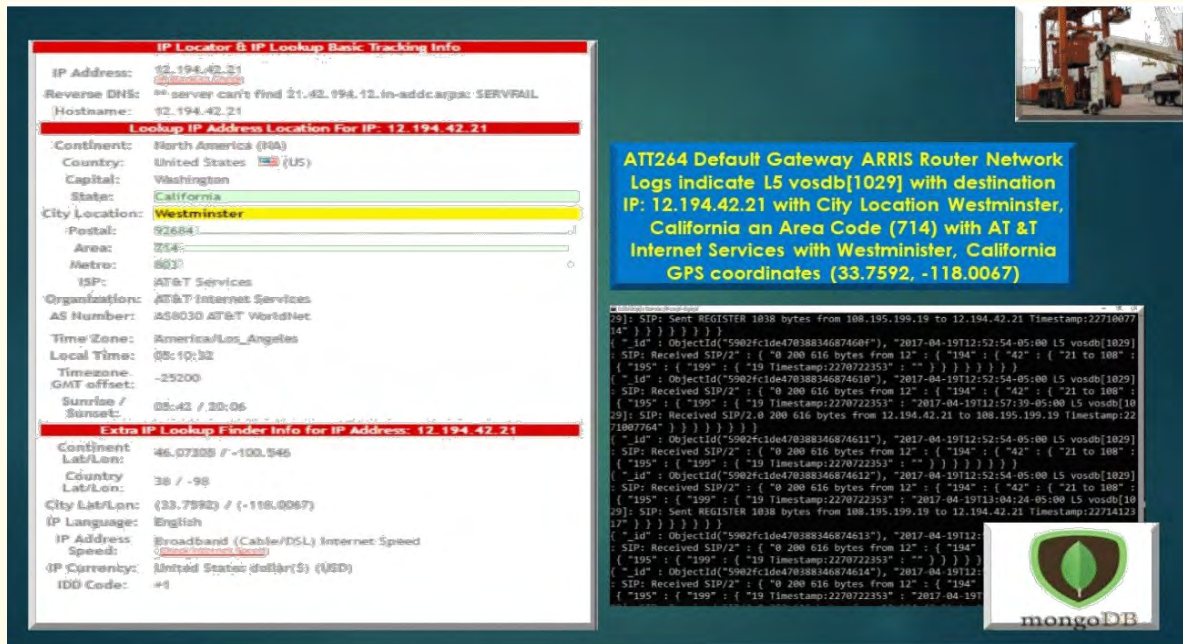


Figure 15: Acrylic WIFI Analyzer and VMware Virtual Machine for Agent 7 and MongoDB.

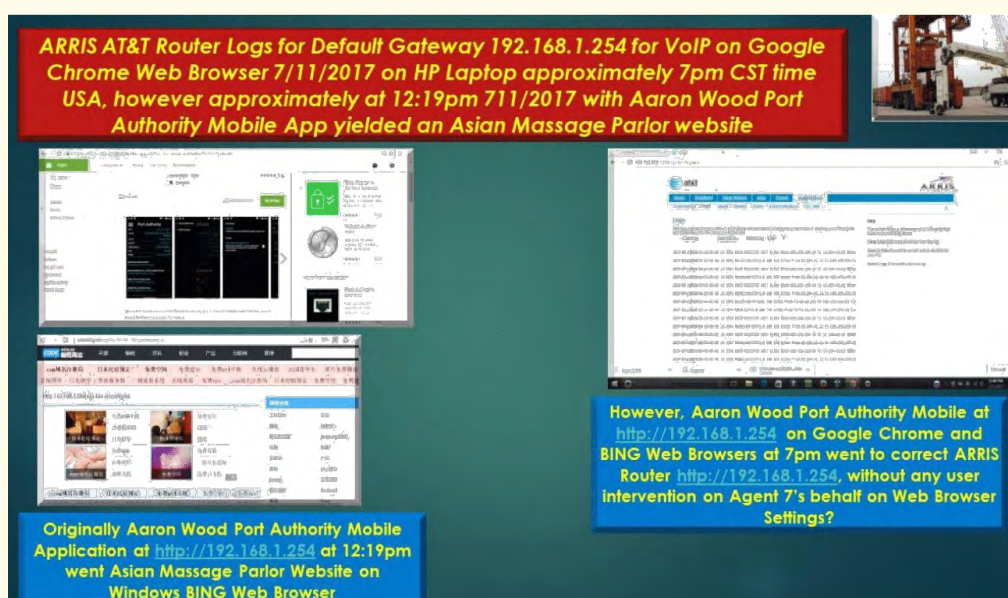




**Figure 16:** Plausible Malicious Intruder from ATT264 Fortune 500 Telecommunication Router Network Logs stored in MongoDB from L5 vosdb [1029] with destination IP Address:12.194.42.21 with city location, Westminster, California and GPS coordinates (33.7592, -118.0067) and phone Area Code (714).

Next, I utilized the Port Authority Mobile Application developed by Aaron Wood. The security tool is a versatile mobile and desktop application to promptly ascertain hosts on your network and facilitate vast network information regarding the user’s mobile device and other network hosts [9]. Moreover, Port Authority is the quintessential port scanner with performance intervals under 5 seconds and with the ability to scan 65.5k ports within less than ½ a minute [9], illustrated in Figure 17 (below).

Agent 7 recognizes utilizing the Port Authority Mobile device on default gateway on <http://192.168.1.254/cgi-bin/home.ha>; on Windows BING web browser originally points to an Asian Massage Parlor website at approximately 12:19 pm Central Standard Time, USA. However, on Google Chrome it proceeds to the correct setting of the ATT264 Fortune 500 Telecommunication Router to capture network logs for System, Firewall, and VoIP at 12:19 pm CST, USA. Agent 7 finds the behavior very questionable regarding originally possible malware on the Port Authority Application, where a malware attacker may have bypassed a malware testing technique, such as



**Figure 17:** Port Authority Mobile Application originally displaying spurious behavior at 2 different time intervals on 7/11/2017, with Agent 7 intervention on mobile web browser settings?



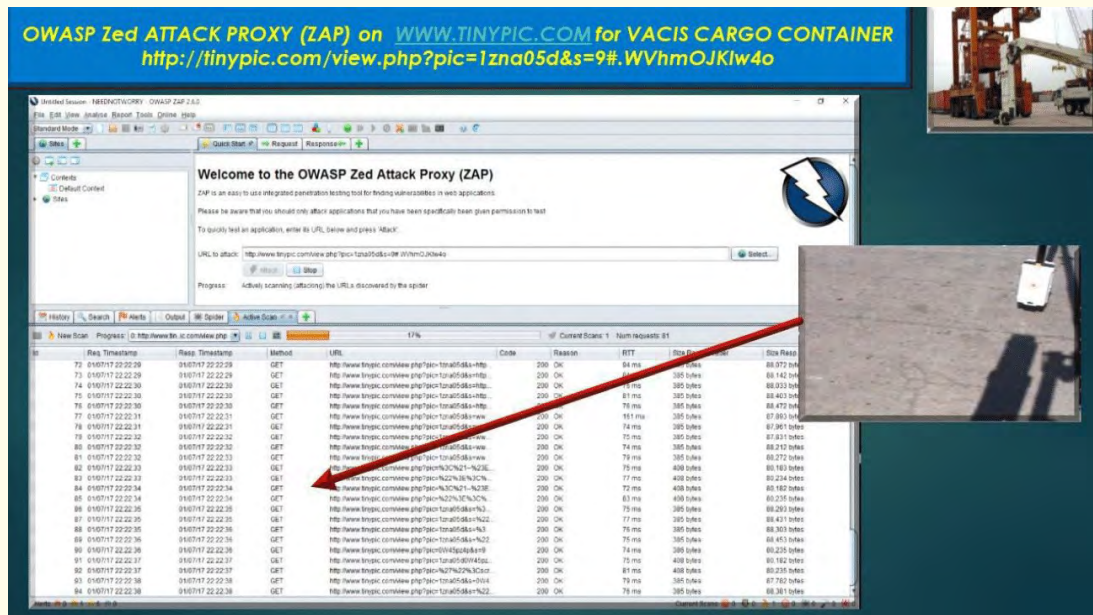


Figure 18: ZAP OWASP indicating a series of HTTP responses from vulnerability scanning.

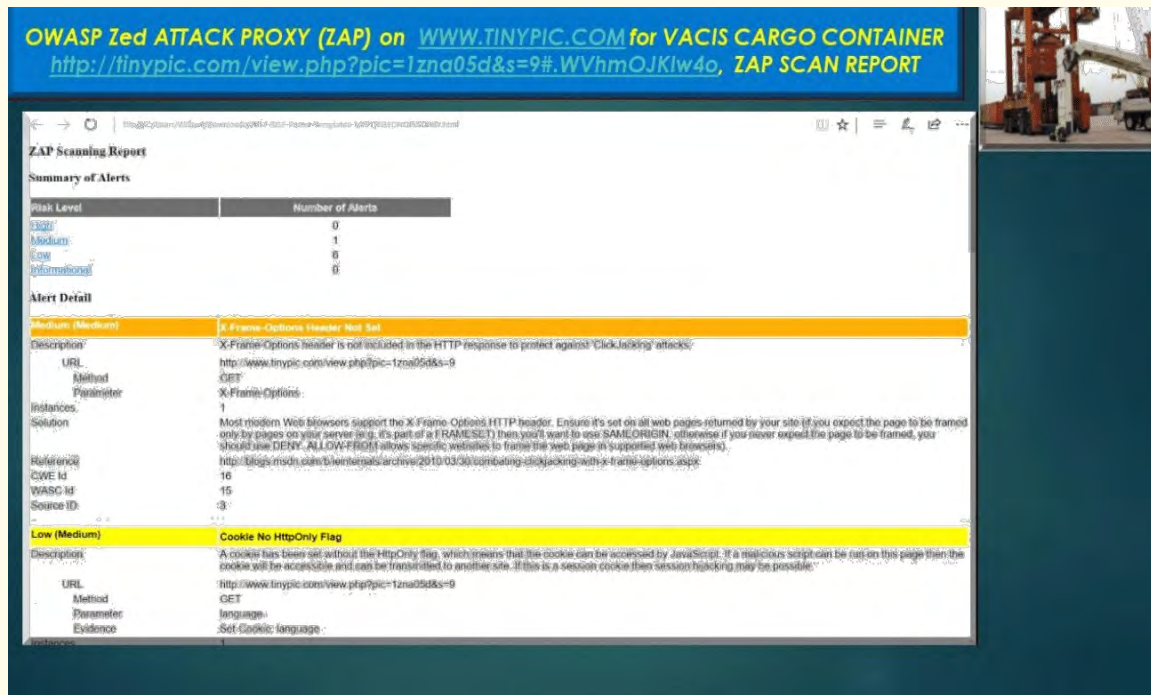


Figure 19: Illustrates a X-Frame-Options Header Not Set as a medium vulnerability of an another click-jacking attack, as previously in illustration F, on June 18, 2017.

## Conclusion

The repeated click-jacking attacks on the organized international criminal syndicate corporation, illustrates that a malicious attacker is installing malware through phishing attempts and plausible intellectual property theft warranting a thorough investigation of the organized international criminal syndicate corporation ARRIS ATT264 network. Thus, in turn the Fortune 500 Telecommunication Router POC policy abuse may already be compromised by other networks demonstrated by the Acrylic WIFI Analyzer constituting industrial espionage and total loss of intellectual property to "Just Us Youth and Wolfsmilch Drones Corporation", and devastating the lives of impoverished communities and at-risk youths domestically, thus the Linux kill command to the organized syndicate terrorists cannot be executed now.

Furthermore, the malicious malware attackers may have already installed other forms of malware such as trojan horses and worms which could be invoked in the future and totally compromise the entire ARRIS ATT264 network, which the AT and T Corporation is evidently already privy to this information.

## **Bibliography**

1. W McClay and A Nayak. "Automated Inspection of X-Ray Cargo Images using Wireshark, Image Stenography, Machine Learning". eForensics Magazine (2014).
2. <http://www.oaklandseaport.com/performance/facts-figures/>
3. Lee Badger, *et al.* "Cloud Computing and Synopsis and Recommendations". National Institute of Standards and Technology (NIST), Special Publication 800-146 (2012).
4. Ramesh Naggapan. "Cloud Security". Harvard Extension School and Brandeis University GPS Program, Spring (2017).
5. Kyle Banker. "MongoDB in Action Chapter 8 Replication". O'Reilly (2017).
6. "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0". Cloud Security Alliance (2011).
7. Wilbert A McClay, *et al.* "A Real-Time Magnetoencephalography Brain Computer Interface Using Interactive 3D Visualization and the Hadoop Ecosystem". *Journal of Brain Sciences* 5.4 (2015): 419-440.
8. OWASP ZAP Version 2.6.0.
9. Aaron Wood. "Google Play Application Store Port Authority Mobile Application".
10. Mena Jesus. "Investigative Data Mining for Security and Criminal Detection". Elsevier Science (2003).
11. Wilbert A McClay, *et al.* "Image Analysis of Radiographic Scans for Detection of Threats in Cargo Containers". Lawrence Livermore, National Laboratory CASIS Signal Processing Workshop (2007).
12. Anthony Joseph, *et al.* "Machine Learning Methods for Computer Security". Manifesto from Dagstuhl Perspectives Workshop 12371, (2012).
13. Hagai Thomas Attias. "A Variational Bayesian framework for graphical models". *Advances in Neural Information Processing Systems* 12 (2000): 209-215.
14. AP Dempster, *et al.* "Maximum Likelihood from incomplete data via the EM algorithm (with discussion)". *Journal of Royal Statistical Society, Series B* 39.1 (1977): 1-38.
15. Marco Barreno, *et al.* "The security of machine learning". *Machine Learning* 81.2 (2010): 121-148.
16. Michael Bailey, *et al.* "Automated classification and analysis of internet malware". In *Recent Advances in Intrusion Detection (RAID)* (2007): 178-197.
17. Dana Angluin and Philip Laird. "Learning from noisy examples". *Machine Learning* 2.4 (1988): 434-470.
18. Arthur Asuncion and David J Newman. "UCI machine learning repository" (2007).
19. AV-TEST. Malware Statistics.
20. Hagai Thomas Attias. "Planning by probabilistic Inference". *Proceedings of the 9<sup>th</sup> International Conference on Artificial Intelligence and Statistics* (2003).
21. Hagai Thomas Attias. "ICA, graphical models, and variational methods". In *Independent Component Analysis: Principles and Practice* (eds: S Roberts, R Everson), Cambridge UP (2001): 95-112.
22. D Puttavidhya, *et al.* "Topic-Regression Multi-modal Latent Dirichlet Allocation for Image and Video Annotation". *Proceedings of the 23<sup>rd</sup> IEEE Conference on Computer Vision and Pattern Recognition* (2010).
23. Barry J Grundy. "The Law Enforcement and Forensic Examiner's Introduction to Linux". Ver 3.78 (2008).
24. Ruth Stryker

25. CISCO AppSec Guide: Criteria for Managing Application Security Risks (2013).
26. Acrylic WIFI, Tarlogic Security: cybersecurity start-up.

**Volume 4 Issue 4 July 2017**

**©All rights reserved by Wilbert A McClay.**