Examiner – Alexander Smetana
Case Investigation #3
11/17/2022

DIGITAL FORENSIC REPORT

Investigation #3

EVIDENCE ITEM

Lab 7.E01_1Host

11/14/2022

PREPARED BY: ALEXANDER SMETANA

REVISION SUMMARY

DATE	*REVISION HISTORY*	*COMMENTS*
11/14/2022	1.0	Creation of the document
11/16/2022	1.1	Finalization of document

INVENTORY

Hardware	Details	
Lab 7.E01	Hostname	Lab7.E01
	Timezone	America/Chicago
	HDD/SSD	64.42 GB (64424509440 bytes)
	OS	Windows 8
	Version	Windows 8.1 Pro
	Device ID	3dfeddca-d6ea-4fdb-bdcc-a07440bbfad3
GIMP	Version	GIMP v.2.8.10
Google Chrome	Version	Google Chrome v.31.0.1650.63
WinRAR	Version	WinRAR 5.01 (64-bit) v.5.01.0
Accounts	Details	
Local Account	Craig Tucker	/Users/Craig
Outlook Account	Craig Tucker	Coupon-king@outlook.com
Outlook Account	Stan Marsh	stan.marsh27@yahoo.com

Hardware	Details	
Kingston Data Traveler	Make	Toshiba Corp.
	Model	Kingston DataTraveler 102/2.0 / HEMA Flash Drive 2 GB / PNY Attache 4GB Stick
	Device ID	000FEAFB938CECC027E200F6
	Source File Path	/img_Lab 7.E01/vol_vol2/Windows/System32/config/SYSTEM

SOFTWARE USED FOR ANALYSIS

Recent Activity	4.19.3
File Type Identification	4.19.3
Extension Mismatch Detector	4.19.3
Embedded File Extractor	4.19.3
Picture Analyzer	4.19.3
Keyword Search	4.19.3
Email Parser	4.19.3
Encryption Detection	4.19.3
Interesting Files Identifier	4.19.3
PhotoRec Carver	7.0
Virtual Machine Extractor	4.19.3
Plaso	4.19.3

EXECUTIVE SUMMARY

As part of a normal business practice, Walmart security receives Counterfeit Coupon Alerts from the Coupon Information Corporation. Within the past month, Walmart security has received specific information regarding fraudulent coupons being passed at their store. Using the information they received, they conducted an internal investigation using video surveillance footage to identify the customers who are engaged in this activity.

One of the suspects was an unknown white, male adult, approximately 28 years old, brown hair, 5’ 9”, 200 pounds, no facial hair, and no visible tattoos. A photograph of this suspect was circulated to the employees in the store. On December 22, 2013, Craig Tucker was detained by Walmart security as he matched the description and he had just passed 2 fraudulent coupons for Monster energy drink and Arizona Iced Tea beverages while paying for other items.

Walmart security contacted the Santa Monica Police Department to arrest and prosecute Tucker for theft. Santa Monica PD Officer Smith interviewed Tucker and he denied knowing the coupons were fraudulent. He claimed to have received the coupons after completing an online survey for students at Santa Monica Community College. Although Tucker gave consent to the search of his personal computer, a search warrant was obtained to search his computer for evidence as it may be an instrument to committing a crime.

OBJECTIVES

It is determined beyond a reasonable doubt that fraudulent coupons were used by Craig Tucker. The objective is not to determine if the individual used the coupons, rather the origin of the source. Was foul play involved? Or did Craig Tucker not knowingly use fake coupons?

Main objectives:

- Find enough evidence to determine as to how the origin of the fraudulent coupons.
- Determine if there is enough evidence to prove whether malicious intent was conducted.
- Determine the information or communication accounts wit the creation, downloading, distribution, and possession of the fraudulent coupons.
- Execute the steps by following procedure to hold the perpetrators accountable based off the evidence conducted.

It must be determined beyond a reasonable doubt that Craig Tucker knowingly used fraudulent coupons. Evidence of past crimes might be uncovered. However, it might lead to a much bigger operation so we must leave no stone unturned.

EVIDENCE

Images	Details	
Lab7.E01	Start	2022/11/16 13:58:52
	End	2022/11/16 20:20:52
	MD5	4e1832956d635ec4e4feba8775a83661
	SHA1	12db0624b2c740f3b5195761ab86a85730550a45

EXAMINATION OF EVIDENCE

Item #1 – Can be described a image taken from Craig Tuckers computer.

HASH OF ORIGINAL EVIDENCE

The hash values obtained from the original evidence were as follows:

MD5	4e1832956d635ec4e4feba8775a83661
SHA1	12db0624b2c740f3b5195761ab86a85730550a45

DRIVE GEOMETRY

64.42 = (64424509440/512 BYTES/SECTOR)

VIRUS SCAN RESULTS

N/A

EXAMINATION OF FILES

21,620 Documents
7,371 Other
8,390 Images
76 Videos

28,764 Executables
7,371 Unknown
162 Audio
455 Not Analyzed

ANALYSIS

The image was analyzed. Crucial email evidence was found, with relevant attachments including fraudulent coupons and coupons making guides. Hundreds of fraudulent coupons were found on Craig Tuckers PC. Two files made use of encryption, which most likely have fraudulent coupons stored on them. Multiple instances of child pornography were found on the computer in both JPEG and WMV files.

FILE ANALYSIS

MyCoupons.zip

A zip file found on the desktop. Makes use of encryption and is locked with a password. The coupons believed to be created by Craig Tucker.

Metadata

Name:	/img_Lab 7.E01/vol_vol2/Users/Craig/Desktop/MyCoupons.zip
Type:	File System
MIME Type:	application/zip
Size:	8057474
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2013-12-21 13:08:18 CST
Accessed:	2013-12-21 13:08:17 CST
Created:	2013-12-21 13:08:17 CST
Changed:	2013-12-21 13:08:26 CST
MD5:	341a22590c8bec1f227549ba7c994135
SHA-256:	de001d18ee5224ada40ada51ce889256143647bf00c61676b1e775d5d2d35cff
Hash Lookup Results:	UNKNOWN
Internal ID:	10916

COUPONS.zip

A zip file containing 128 coupons. Illegal coupons that were downloaded by Craig Tucker.

Metadata

Name:	/img_Lab 7.E01/vol_vol2/Users/Craig/Downloads/Coupons.zip
Type:	File System
MIME Type:	application/zip
Size:	145954735
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2013-12-21 13:01:13 CST
Accessed:	2013-12-21 13:01:10 CST
Created:	2013-12-17 21:02:50 CST
Changed:	2013-12-21 13:01:11 CST
MD5:	cd79de0a0fc5658cbb69de71bbbe7c68
SHA-256:	a778fa113ba3dcc97d0f67a2e3bd5ac39bfc742cfd5c604c45e939d91f97897f
Hash Lookup Results:	UNKNOWN
Internal ID:	11056

AWESOME COUPONS.DOCX

Can be identified as a document found on Craig Tuckers computer. Makes use of encryption.

Metadata	
Name:	/img_Lab 7.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps_8wekyb3d8bbwe/LocalState/LiveComm/ba871ed4e8a350e0/120712-0049/Att/20000275/AWESOME COUPONS.docx
Type:	File System
MIME Type:	application/x-ooxml-protected
Size:	632320
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2013-12-29 21:58:17 CST
Accessed:	2013-12-29 21:58:17 CST
Created:	2013-12-29 21:58:17 CST
Changed:	2013-12-29 21:58:17 CST
MD5:	6c9d3ff0af82e9b24e842e6c4bcee39d
SHA-256:	7908952346ee1009485d67473d702c3939ca6ce4e3a559fd98b0e3ec863d96ad
Hash Lookup Results:	UNKNOWN
Internal ID:	5320

6CommandmentsofCouponMaking.docx

A document detailing the process on how to make coupons. Attachment from the email stan.marsh27@yahoo.com.

MetaData	
Name:	/img_Lab 7.E01/vol_vol2/Users/Craig/Documents/Guides/6CommandmentsofCouponMaking.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	371041
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2013-12-20 15:27:33 CST
Accessed:	2013-12-20 15:27:33 CST
Created:	2013-12-20 15:27:33 CST
Changed:	2013-12-20 15:27:42 CST
MD5:	ff47d22743ca6b48034263b24a9a6baf
SHA-256:	6c986e314115eeb2892eea30f775cab1f6fce003729ab3e0437313db6182969d
Hash Lookup Results:	UNKNOWN
Internal ID:	10927

$R8MHF6S.jpg

Can be identified as a jpg of child pornography that was found in the recycling bin.

Metadata	
Name:	/img_Lab 7.E01/vol_vol2/$Recycle.Bin/S-1-5-21-1049150138-4017234595-3791460656-1001/$R8MHF6S.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	562101

File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2013-12-20 23:50:16 CST
Accessed:	2013-12-21 13:32:57 CST
Created:	2013-12-21 13:32:57 CST
Changed:	2013-12-27 01:27:06 CST
MD5:	fb248599cee84f77e409b2b65407fe10
SHA-256:	d5948f2c4e0a101abc73f0706b42c0341a8cdac6c7cf5b397291739c2c3f9284
Hash Lookup Results:	UNKNOWN
Internal ID:	11583

$RGQWXSI.jpg

Can be identified as a jpg of child pornography that was found in the recycling bin.

Metadata

Name:	/img_Lab 7.E01/vol_vol2/$Recycle.Bin/S-1-5-21-1049150138-4017234595-3791460656-1001/$RGQWXSI.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	626337
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2013-12-20 23:56:30 CST
Accessed:	2013-12-21 13:32:57 CST
Created:	2013-12-21 13:32:57 CST
Changed:	2013-12-27 01:27:09 CST
MD5:	9050b5cb16c4e554c18e37a7be64bc84
SHA-256:	4e235025729c1254183fd87b7ce884eab1e7fe3033d5a2244450fa031aae60d2
Hash Lookup Results:	UNKNOWN
Internal ID:	11585

underage daughter R2ygold.wmv

File of child pornography found underneath Craig/Videos

Metadata

Name:	/img_Lab 7.E01/vol_vol2/Users/Craig/Videos/underage daughter R@ygold.wmv
Type:	File System
MIME Type:	video/x-ms-wmv
Size:	8076724
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2013-12-27 02:45:34 CST
Accessed:	2013-12-21 13:43:02 CST
Created:	2013-12-21 13:43:02 CST
Changed:	2013-12-27 02:45:34 CST
MD5:	Not calculated

SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	224202

Underage_lolita_r@ygold_001.jpg

Deleted child pornography jpg found on computer

Metadata

Name:	/img_Lab 7.E01/vol_vol2/Users/Craig/Pictures/Underage_lolita_r@ygold_001.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	562101
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2013-12-27 01:27:06 CST
Accessed:	2013-12-21 13:32:57 CST
Created:	2013-12-21 13:32:57 CST
Changed:	2013-12-27 01:27:06 CST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	224198

Underage_lolita_r@ygold_002.jpg

Deleted child pornography jpg found on computer

Metadata

Name:	/img_Lab 7.E01/vol_vol2/Users/Craig/Pictures/Underage_lolita_r@ygold_002.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	626337
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2013-12-27 01:27:09 CST
Accessed:	2013-12-21 13:32:57 CST
Created:	2013-12-21 13:32:57 CST
Changed:	2013-12-27 01:27:09 CST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN

TIMELINE

Table 4-1 Timeline

Timestamp (UTC 24hr)	Event	Evidence Source
2013-12-17 17:34:26 CST	To: coupon-king@outlook.com; From: member_services@outlook.com; Subject: Please sign in to your Outlook.com account Hello Craig Tucker, To continue sending messages, please sign in and validate your Outlook.com account **Conclusion:** • Email sent member services@outlook.com to coupon-king@outlook.com. This email confirms that email address of coupon-king@outlook.com does belong to Craig Tucker.	Lab 7.E01
2013-12-17 17:43:42 CST	To: stan.marsh27@yahoo.com; From: coupon-king@outlook.com; Subject: Re: Free Coupons I got them at 4chan. Go 2 the random channel and get sum 2 share w/ me! On Tuesday, December 17, 2013 3:33 PM, Craig Tucker <coupon-king@outlook.com> wrote: Cool thx! ������ Where did u get these? Sent from Windows Mail **From:** Stan Marsh **Sent:** Tuesday, December 17, 2013 12:37 AM **To:** Craig Tucker Hey, I got sum more free stuff at wallmart 2day! U gotta start using coupons dude. Here's sum 4 u 2 get started. **Conclusion:** • Email sent from Craig Tucker to Stan Marsh. Attachments were sent with fraudulent coupons. It identifies the origin of the fraudulent coupons. It is also evidence of Stan Marsh distributing them.	Lab 7.E01
2013-12-17 17:45:21 CST	Craig Tucker searches "**4chan**" using google chrome. Based on the prior emails, we can assume that this search history demonstrates intent is to search for fraudulent coupons.	Lab 7.E01
2013/12/18 14:05:57 CST	Craig Tucker downloads the file "**ALL COUPONS.rar**" from the domain "mediafire.com" Filepath: C:\Users\Craig\Downloads\ALL COUPONS.rar	Lab 7.E01

2013-12-18 14:06:19 CST	Craig Tucker searches “**Winrar**” using google chrome	Lab 7.E01
2013-12-20 15:11:00 CST	Craig Tucker searches “**how to make coupons**” using google chrome	Lab 7.E01
2013-12-20 15:25:40 CST	Email History To: stan.marsh27@yahoo.com; From: coupon-king@outlook.com; Subject: Re: Coupon Making Here r sum guides but just warning u that u r getting in 2 a whole new deal by making them urself. u get caught using them, not so bad and u can make up an excuse...u get caught making them, u r doomed. So dont be a newb and get caught. BTW u need GIMP 2 make ur own, so go download it. On Friday, December 20, 2013 1:13 PM, Craig Tucker <coupon-king@outlook.com> wrote: Hey Stan, I was trying 2 find stuff on making my own coupons. U got any good guides 4 that? Sent from Windows Mail **Conclusion:** Stan Marsh gave Craig Tucker the tools to start making fraudulent coupons	Lab 7.E01
2013-12-20 15:27:33 CST	Craig Tucker opens the file “**6CommandmentsOfCouponMaking**”. Demonstrates intent to start making coupons.	Lab 7.E01
2013-12-20 15:28:59 CST	Craig Tucker searches “**gimp**” using google chrome. This demonstrates that Craig Tucker had the tools to make the tools.	Lab 7.E01
2013-12-20 15:43:25 CST	**AWESOME COUPONS.docx** was created. Encryption was added as a level of security.	Lab 7.E01
2013-12-21 13:08:17 CST - 2013-12-21 13:08:26 CST	**MyCoupons.ZIP** was created and changed. Encryption was added Accessed: 2013-12-21 13:08:17 CST Created: 2013-12-21 13:08:17 CST Changed: 2013-12-21 13:08:26 CST	Lab 7.E01
2013-12-21 15:23:14 CST	A USB Kingstone Device is attached to the computer. Toshiba Corp. Kingston DataTraveler 102/2.0 / HEMA Flash Drive 2 GB / PNY Attache 4GB Stick Device ID: 000FEAFB938CECC027E200F6	Lab 7.E01
2013/12/21 13:32:38	File **Underage_lolita_r@ygold_001.jpg** of child pornography is accessed	Lab 7.E01

	File Path: C:\Users\Craig\Pictures\Underage_lolita_r@ygold_001.jpg	
2013/12/21 13:32:45	File **Underage_lolita_r@ygold_002.jpg of** child pornography is accessed File Path: C:\Users\Craig\Pictures\Underage_lolita_r@ygold_002.jpg	Lab 7.E01
2013-12-21 13:32:57 CST	***R8MHF6S.jpg*** and ***$RGQWXSI.jpg*** File of child pornography found in the recycling bin is accessed.	Lab 7.E01
2013/12/21 13:42:16	**E:\Russian Videos** file is accessed. Presumably on the Kingstone device.	Lab 7.E01
2013/12/21 13:43:02	Underage child pornography is accessed by the file name "**underage daughter R@ygold.**wmv"	Lab 7.E01
2013/12/22	Craig Tucker is detained by Walmart security and arrested.	Lab 7.E01
2013-12-27 01:53:35 CST	Email History An email sent between Stan Marsh and Craig Tucker. Its evidence of the distribution of child pornography and an attempted cover up. The attachments are found in the recycling bin on Craig Tuckers computer. To: coupon-king@outlook.com; From: stan.marsh27@yahoo.com; Subject: Re:More Hot Pics Thx bro! I hid them and deleted your msg Sent from Windows Mail	Lab 7.E01

RELEVANT FINDINGS

Based on email history, we can confirm that the email address coupon-king@outlook.com belongs to Craig Tucker. Craig Tucker actively communicating with the email address stan.marsh27@yahoo.com belonging to Stan Mash.

Email logs were found on Craig Tuckers computer, containing fraudulent coupons sent by Stan Marsh to Craig Tucker by via email attachments. Craig Tucker would download these files and store them on his computer. Craig Tucker would go onto download fraudulent coupons from the domain “mediafire.com.” A coupon zip file “COUPONS.zip” was found on Craig Tuckers pc, containing 128 coupons.

Stan Marsh would provide Craig Tucker the means to make coupons. Email logs detail Stan Marsh educating Craig Tucker on how to make fraudulent coupons by himself. Stan Marsh would attach coupon making guides by email with these files stored on Craig Tuckers desktop. One notable coupon guide was the “6Commandmentsofcouponmaking” which was opened by Craig Tucker.

Craig Tucker would download the tools to make fraudulent coupons such as GIMP an WINRAR. Craig Tucker would run these programs. The fraudulent coupons that Craig Tucker made are coupons are store in the zip file “MyCoupons.zip”. and “AWESOME COUPONS.docx” Craig Tucker made use of encryption to hide his coupons an attempt to cover up.

Finally, child pornography was found on the computer. 3 Files were found in the recycling bin detailing child pornography, “*R8MHF6S.jpg”, “$RGQWXSI.jpg”, “*underage daughter R@ygold.wmv”. A deleted email contains details that Stan Marsh sent child pornography to Craig Tucker. The child pornography was discovered on Craig Tuckers under the path E:/ Russian videos. The files include, “Underage_lolita_r@ygold_001.jpg” and “Underage_lolita_r@ygold_002.jpg.”

SUPPORTING DETAILS

It is believed that Craig Tucker and Stand Marsh are close friends due to the content and number of emails. Stan Marsh potentially could be involved in the coupon making scandal due his distribution of coupons in the attachments. We can infer that Craig Tucker had the intent to not only use illegal coupons but create his own and potentially distribute them. Craig Tucker had illegal coupons downloaded and had the tools installed on his PC to do so.

There is an enormous correlation between the time GIMP was download (2013-12-20 15:28:59 CST) with the creation of AWESOME COUPONS.docx (2013-12-20 15:43:25 CST). Based off this correlation, it is likely that incriminating evidence of Craig Tuckers fraudulent coupons are hidden in the document.

The child pornography location of the recycling bin and the deletion of Stan Marsh’s email, we can infer that Stan Marsh was aware of his wrongdoing and appears to be an attempt of a cover up. It is also believed that there is a connection between a Kingstone USB device and the path to child pornography.

INVESTIGATIVE LEADS

Action must be taken against Craig Tucker. There is enough evidence to prove that beyond a reasonable doubt that Craig Tucker aware of the fraudulent coupons. Craig Tucker took part creating and distributing fraudulent coupons.

There must be an investigation into the encrypted files. It is most likely that it contains crucial evidence into the fraudulent coupons. There are two files “AWESOME COUPONS.DOCX” and “MyCoupons.zip” should be cracked using password cracking software. If coupons are found within the files, it must be determined when, where, and how the coupons were made. It must be determined if Craig Tucker did in fact make the images by analyzing them.

An investigation must occur into the Kingstone device located on the computer. He should be questioned into the Kingstone device that was connected to his PC. Action must child pornography was found on Craig Tuckers PC and based on the timing of the Kingston; it is most likely that it contains child pornography on the drive. Authorities must look for any leads leading to “E:/Russian Videos” on the device. It is also possible that the Kingstone device contains evidence of more fraudulent coupons.

Authorities must be contacted due to the illegal contact that occurred between Stan Marsh and Craig Tucker. Stan Marsh should be called into questioning into the illegal coupon business and the distribution of child pornography. A search warrant should be obtained, and an investigation should occur into Craig Tuckers Kingstone device and Stan Marsh’s PC.