DIGITAL FORENSIC EXAMINATION REPORT

Case Number: 04152026

Report Date: April 25, 2026

Examiner Name: Ulysses Ochoa

Organization: Digital Forensics Unit

Classification: Law Enforcement Sensitive

---

1. Executive Summary

A forensic examination was conducted on a bit-for-bit forensic image (2020JimmyWilson.E01) of a hard drive attributed to Jimmy Wilson. The examination revealed substantial digital evidence consistent with an organized criminal operation involving (1) the production and sale of fraudulent identity documents — including counterfeit driver's licenses, identification cards, credit cards, green cards, and insurance certificates — and (2) the acquisition, distribution, and likely sale of credit card skimming devices.

Key findings include: an unencrypted price list recovered from the Recycle Bin establishing the specific goods and prices offered by Wilson; a series of encrypted email communications between Wilson and two identified clients (Jose Badguy and Robert Ripoff) in which orders were negotiated and placed using the BCTextEncoder encryption utility; a hidden virtual hard drive (SYSTEM.vhd) containing images, schematics, and saved webpages directly related to ATM credit card skimmers; browser and web cache history reflecting searches for identity theft methods, card printer procurement, and financial concealment; and a TrueCrypt-encrypted container named "moneymaker" whose contents remain undetermined pending decryption. Wilson also created a document explicitly refusing consent to a search of his computer, which was recovered from his Documents folder.

The evidence collectively indicates that Jimmy Wilson operated a clandestine commercial enterprise in which he manufactured and sold counterfeit identity and financial documents and was actively involved in the acquisition of credit card skimming hardware and methodology.

---

2. Case Information

Field	Details
Case Number	04152026
Case Name / Title	2020JimmyWilson

Requesting Party	Digital Forensics Unit
Date of Request	April 15, 2026
Date Examination Began	April 15, 2026
Date Examination Completed	April 25, 2026
Examiner Name	Ulysses Ochoa
Examiner Title / Role	Digital Forensic Examiner

Subject of Investigation: Jimmy Wilson

Subject Email Address: wilsonjimmy807@gmail.com

Subject Computer Hostname: IACISHDD2014

---

3. Scope and Methodology

3.1 Scope of Examination

The examination was limited to the forensic image file `2020JimmyWilson.E01`, a complete bit-for-bit image of a physical hard drive. The image was verified against its MD5 hash prior to examination to confirm integrity. All analysis was performed on the working copy of the forensic image; the evidence original was not altered. The examination encompassed all allocated and unallocated space within the image, including deleted files, the Recycle Bin, file system metadata, email archives, browser artifacts, registry data, and a hidden virtual hard drive partition.

The following were not in scope for this examination: live analysis of any network environment; cloud storage accounts; mobile devices; or external media not contained within the forensic image.

3.2 Tools and Software Used

Tool / Software	Version	Purpose
Autopsy	(current)	Primary forensic analysis platform; file recovery, artifact extraction, email parsing, keyword search
Microsoft Windows Live Mail	16.4.3508.205	Email client identified on subject device; email archive parsing
ExifTool	(current)	Image and file metadata extraction
BCTextEncoder	v. 1.01.1	Identified on subject device; encryption utility used in subject's communications
Regripper	(current)	Windows registry extraction and

		analysis
HashCalc / MD5 verification	—	Evidence image integrity verification

---

4. Chain of Custody

Item #	Item Description	Received From	Date / Time Received	MD5 Hash Verified	Notes
1	2020JimmyWilson.E01 — Forensic disk image	Evidence custodian	April 15, 2026	Yes — 4193cc3bc7111ddf8be7a00677f2a2f4	Working copy used for examination; original retained

> ***Chain of Custody documentation*** *(signed transfer records) is maintained separately in the physical case file and in the attached chain-of-custody form (`2020JimmyWilson-Chain-of-Custody.docx`).*

---

5. Evidence Inventory

Full evidence inventory is attached as **Exhibit A** (Autopsy Excel export: `Excel.xlsx`). Notable items tagged during the examination are summarized below.

Exhibit	File Name	Type	File System Date (Modified)	MD5 Hash
EX-01	New Price List.txt	Text file	2015-05-26 06:46:44 PDT	b904a9c79b81406371411751d203a0f8
EX-02	New Price List Encoded.TXT	Encoded text (BCTextEncoder)	N/A	c6dc3deffb0f1735d4edd964c0027ad2
EX-03	Jose 42 encoded.TXT	Encoded text (BCTextEncoder)	N/A	cab28084bdeb55bbf43bf92a533fbe83
EX-04	Robert 17 Encoded.TXT	Encoded text	N/A	b9a6497f0c4dece6022199c05b45452

		(BCTextEncoder)		1
EX-05	59106BB8-00000005.eml	Email	2015-05-26 05:46:04 PDT	eb88bb810c945d945ef3351cca1703e7
EX-06	72AE6952-00000009.eml	Email	2015-05-26 05:46:16 PDT	c9cf76d9cab07a0fbecd0860a4bf99f1
EX-07	447018D5-00000006.eml	Email	2015-05-26 05:45:58 PDT	f3cb26bcfb83439df01861c18959110c
EX-08	3D6C2CD6-00000008.eml	Email	2015-05-26 05:46:16 PDT	a01b0ed35af07d8191102075adebaa61
EX-09	5F901649-0000000A.eml	Email	2015-05-26 05:46:16 PDT	ab781ace421cfa2813e59c29a118f0b9
EX-10	6DF15AF1-0000000B.eml	Email	2015-05-26 05:46:16 PDT	fd4ac19e13733fa848640e3d08398ae6
EX-11	15611658-0000000C.eml	Email	2015-05-26 05:46:16 PDT	ed11dbb0ee326fba6d8ee26958857890
EX-12	0C191CD4-0000000D.eml	Email	2015-05-26 05:46:16 PDT	b35d8e801cbcc2f86925209d2b455675
EX-13	196A62A1-00000008.eml	Email	2015-05-26 05:46:16 PDT	87491ec1f9120f479caeaaa7d0782352
EX-14	TrueCrypt	Application	2014-01-29 09:37:27 PST	N/A
EX-15	moneymaker	TrueCrypt encrypted container	2014-02-11 06:02:34 PST	b9a3a085d259c036d31b5a7839c64785
EX-16	ATM-Skimmer-Overlay-2.jpg	Image	2014-01-30	f9253444b964aaf2e9e47243dadfe7a9

			08:04:42 PST	
EX-17	ATM-Skimmer-Overlay-3.jpg	Image	2014-01-30 08:04:42 PST	bf3bf6a08c1de67ff23840c45ad8301e
EX-18	atm-skimmer-and-keypad.jpg	Image	2014-01-30 08:04:42 PST	b422e8b1547b7170e875e5841f573fb4
EX-19	AISB08.pdf	PDF / schematic	2014-01-30 07:58:26 PST	86ffa112c11f0b9ea0f2ef44745ad09c
EX-20	Credit Card Skimmers and ATM Card Skimmers pictures and images.htm	HTML saved page	2014-01-30 08:04:50 PST	15403804c9bbd9d7551213c1e24cf5e2
EX-21	Driver License Card Printer...Alibaba_com.htm	HTML saved page	2014-01-30 08:01:26 PST	e0de19f8d449ac7c39fdb8cf573dc169
EX-22	Card Printers.htm	HTML saved page	2014-01-30 08:02:44 PST	53fb37fea92358c17e9c4bb2d7a0d8fc
EX-23	All About Skimmers — Krebs on Security_files	HTML saved folder	2014-01-30 08:04:16 PST	N/A
EX-24	pdf.pdf	Disguised folder / steganographic container	2014-01-30 07:57:58 PST	8bd6509aba6eafe623392995b08c7047
EX-25	image21.jpg	Image (embedded in IDtheftrev.pdf)	N/A	eaf4511fc762cbf3bc19c03e02898d9f
EX-26	image31.jpg	Image (embedded in IDtheftrev.pdf)	N/A	009ceae569c4cc1e8ba60e80ef4344f2
EX-27	image35.jpg	Image (embedded in IDtheftrev.pdf)	N/A	c1ce87b39e17562aa21ff8e2bf1333de
EX-28	places.sqlite	Firefox browser history database	2015-05-26 05:46:09 PDT	86bd9af8f5535338b69fcc9edf335b99
EX-29	WebCacheV01.dat	Internet	2015-05-	63d516b8bfea9dbf6e0fa102ab4f318f

		Explorer / Edge web cache	26 05:46:18 PDT	
EX-30	How to Hide Money From The Government — Libertarian Money.url	Internet shortcut (bookmark)	2015-05-26 05:46:02 PDT	e792b89742e8e2d7c26110e7b58467bd
EX-31	SYSTEM.vhd	Virtual Hard Drive (hidden partition)	—	—
EX-32	To Whom it may concern.doc	Word document	2015-05-26 05:46:12 PDT	5c02e0f5f7f527de8a99d65d2e50a159
EX-33	$R8OPSCS.JPG	Image (Recycle Bin, deleted)	2015-05-26 06:46:44 PDT	29dd9fb25146f68d0517d525103810c1
EX-34	AgGlFaultHistory.db	Database (suspected encrypted)	2015-05-26 05:47:22 PDT	da132450ab567fab9fe171d38c787333
EX-35	AgGlFgAppHistory.db	Database (suspected encrypted)	2015-05-26 05:47:22 PDT	b0aac6ba401417484ba64dfe9fd00874
EX-36	AgGlGlobalHistory.db	Database (suspected encrypted)	2015-05-26 05:47:22 PDT	99a9531bb4466614740656cf083219c2

---

6. Findings

6.1 Fraudulent Document Price List (EX-01)

Evidence Item	Details
Exhibit #	EX-01
File Name	New Price List.txt
Description	Plain-text price list for fraudulent identity documents
File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/$RECYCLE.BIN/S-1-5-21-1171287513-3642516788-2358256967-1004/$R3TS6GA/New Price List.txt`
File Type	Plain text (.txt)
File Size	175 bytes

Date Created	2015-05-26 06:45:22 PDT
Date Modified	2015-05-26 06:46:44 PDT
Date Accessed	2015-05-26 06:45:22 PDT
MD5 Hash	b904a9c79b81406371411751d203a0f8
Tool Used	Autopsy
Analysis / Notes	The file was recovered from the Recycle Bin of the subject's user profile, indicating it was deleted but not permanently removed at the time of imaging. The file contains an itemized price list dated February 1, 2014, listing the following fraudulent items and prices: Credit Cards ($350.00), Drivers License ($250.00), ID Cards ($250.00), Green Cards ($300.00), and Insurance Certificates ($100.00). This file is the decrypted counterpart of EX-02 and corresponds directly to the encoded attachments distributed to clients via email (EX-09, EX-10, EX-11). The deletion of this file from the main file system but its presence in the Recycle Bin indicates an attempt to conceal the document.
Linked Exhibits	EX-02, EX-09, EX-10, EX-11

Extracted Content:

```
New Price List as of 01 FEBRUARY 2014

Credit Cards: $350.00
Drivers License: $250.00
ID Cards: $250.00
Green Cards: $300.00
Insurance Certificates: $100.00
```

6.2 Encoded Price List Attachment (EX-02)

Evidence Item	Details
Exhibit #	EX-02
File Name	New Price List Encoded.TXT
Description	BCTextEncoder-encrypted version of the fraudulent document price list; recovered as email attachment
File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows Live Mail/Gmail (wils 48a/[Gmail]/All Mail/15611658-0000000C.eml/New Price List Encoded.TXT`
File Type	Encoded text (.TXT)
File Size	862 bytes
MD5 Hash	c6dc3deffb0f1735d4edd964c0027ad2
Tool Used	Autopsy
Analysis / Notes	This file is the encrypted version of EX-01. It was attached to email messages sent by Wilson to clients Robert Ripoff (EX-10, EX-11)

	and Jose Badguy (EX-09) on February 16, 2014. The file uses BCTextEncoder Utility v. 1.01.1, the same encryption application found to be in use across all client order communications. The identical BCTextEncoder ciphertext block appears in multiple emails (EX-09, EX-10, EX-11), confirming it is the same file distributed to multiple clients. The decrypted contents are reflected in EX-01.
Linked Exhibits	EX-01, EX-09, EX-10, EX-11

6.3 Encrypted Order — Client Jose Badguy (EX-03)

Evidence Item	Details
Exhibit #	EX-03
File Name	Jose 42 encoded.TXT
Description	BCTextEncoder-encrypted order/message from client Jose Badguy to Jimmy Wilson
File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows Live Mail/Gmail (wils 48a/Inbox/5ECE797A-00000007.eml/Jose 42 encoded.TXT`
File Type	Encoded text (.TXT)
File Size	1,690 bytes
MD5 Hash	cab28084bdeb55bbf43bf92a533fbe83
Tool Used	Autopsy
Analysis / Notes	This file is an attachment to an email from Jose Badguy to Jimmy Wilson and represents an order submission encrypted using BCTextEncoder. The file could not be decrypted without the agreed-upon password referenced in email EX-06 and EX-08. The file is associated with the email chain in EX-12, in which Jose confirms acceptance of Wilson's price list and indicates the attachment contains his order. The use of encryption to transmit the specific items ordered is consistent with an intent to conceal the nature of the transaction from interception.
Linked Exhibits	EX-12, EX-06

6.4 Encrypted Order — Client Robert Ripoff (EX-04)

Evidence Item	Details
Exhibit #	EX-04
File Name	Robert 17 Encoded.TXT
Description	BCTextEncoder-encrypted order/message from client Robert

	Ripoff to Jimmy Wilson
File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows Live Mail/Gmail (wils 48a/Inbox/196A62A1-00000008.eml/Robert 17 Encoded.TXT`
File Type	Encoded text (.TXT)
File Size	1,862 bytes
MD5 Hash	b9a6497f0c4dece6022199c05b454521
Tool Used	Autopsy
Analysis / Notes	This file is an attachment to an email from Robert Ripoff to Jimmy Wilson (EX-13) and represents an encrypted order submission. Robert's accompanying email states: "I'm ok with the new prices, I attached what I need to this email." The file could not be decrypted without the pre-arranged password. The BCTextEncoder application and version are identical to those used in EX-02 and EX-03, indicating a consistent, pre-arranged encryption protocol among all parties.
Linked Exhibits	EX-13, EX-08

6.5 TrueCrypt Application (EX-14)

Evidence Item	Details
Exhibit #	EX-14
File Name	TrueCrypt
Description	TrueCrypt encryption application present on hidden virtual hard drive
File Path / Location	`/img_SYSTEM.vhd/vol_vol7/TrueCrypt`
File Type	Application / directory
File Size	56 bytes
Date Created	2014-01-29 09:37:21 PST
Date Modified	2014-01-29 09:37:27 PST
Date Accessed	2014-01-29 09:37:27 PST
Tool Used	Autopsy
Analysis / Notes	TrueCrypt is a discontinued open-source encryption utility capable of creating encrypted virtual disk containers within files. Its presence on the hidden virtual hard drive is significant in combination with the encrypted container identified as EX-15. The installation date of January 29, 2014, precedes the email communications of February 16, 2014, indicating the subject established encrypted storage prior to the documented order transactions.

Linked Exhibits	EX-15, EX-31

6.6 TrueCrypt Encrypted Container — "moneymaker" (EX-15)

Evidence Item	Details
Exhibit #	EX-15
File Name	moneymaker
Description	TrueCrypt-encrypted container; contents unknown pending decryption
File Path / Location	`/img_SYSTEM.vhd/vol_vol7/TrueCrypt/moneymaker`
File Type	TrueCrypt encrypted volume
File Size	10,485,760 bytes (~10 MB)
Date Created	2014-01-29 09:37:21 PST
Date Modified	2014-02-11 06:02:34 PST
Date Accessed	2014-01-29 09:37:21 PST
MD5 Hash	b9a3a085d259c036d31b5a7839c64785
Tool Used	Autopsy
Analysis / Notes	This file is a TrueCrypt-encrypted virtual disk container. The file name "moneymaker" is contextually significant given the nature of the investigation. The modified date of February 11, 2014, places the last modification within days of the confirmed email order transactions of February 16, 2014, suggesting active use during the period of criminal activity. The container size of approximately 10 MB is sufficient to store a significant quantity of files including customer records, financial records, identification templates, or skimmer designs. Decryption of this container would require the password or the application of cryptographic analysis tools. This exhibit is flagged for follow-up decryption efforts.
Linked Exhibits	EX-14, EX-31

6.7 Hidden Virtual Hard Drive Partition (EX-31)

Evidence Item	Details
Exhibit #	EX-31
File Name	SYSTEM.vhd
Description	Hidden virtual hard drive containing covert file storage across multiple volumes (vol_vol7, vol_vol8)

File Path / Location	`/img_SYSTEM.vhd` (extracted by Autopsy Virtual Machine Extractor module)
File Type	Virtual Hard Drive (.vhd)
Tool Used	Autopsy (Virtual Machine Extractor module)
Analysis / Notes	Autopsy identified a virtual hard drive file (SYSTEM.vhd) within the forensic image. Upon mounting, the VHD contained at least two volumes: vol_vol7 (housing TrueCrypt and the moneymaker encrypted container) and vol_vol8 (housing ATM skimmer images, skimmer schematics, saved research webpages, and a steganographic PDF). The use of a hidden VHD within the primary drive represents a deliberate effort to conceal criminal activity from casual inspection. All exhibits from EX-14 through EX-24 were recovered from within this hidden virtual hard drive.
Linked Exhibits	EX-14 through EX-24

6.8 ATM Skimmer Overlay Images (EX-16, EX-17)

Evidence Item	Details
Exhibit #	EX-16 / EX-17
File Names	ATM-Skimmer-Overlay-2.jpg / ATM-Skimmer-Overlay-3.jpg
Description	Photographic images of ATM card skimmer overlay devices
File Path / Location	`/img_SYSTEM.vhd/vol_vol8/Credit Card Skimmers and ATM Card Skimmers pictures and images_files/`
File Type	JPEG image
File Sizes	55,283 bytes / 31,382 bytes
Date Created	2014-01-30 08:04:48 PST (both)
Date Modified	2014-01-30 08:04:42 PST (both)
MD5 Hashes	f9253444b964aaf2e9e47243dadfe7a9 / bf3bf6a08c1de67ff23840c45ad8301e
Tool Used	Autopsy, ExifTool
Analysis / Notes	Both images depict ATM card skimmer overlay devices — physical hardware designed to be placed over legitimate ATM card readers to covertly capture card data. These images were found within a directory associated with a saved ATM skimmer reference website (EX-20), stored

	on the hidden virtual hard drive. The colocation of these images with skimmer schematics (EX-19) and a sales/ordering page (EX-20) indicates these images were retained as product references, consistent with someone selling or manufacturing skimming devices.
Linked Exhibits	EX-18, EX-19, EX-20, EX-31

6.9 ATM Skimmer with Wiring Diagram (EX-18)

Evidence Item	Details
Exhibit #	EX-18
File Name	atm-skimmer-and-keypad.jpg
Description	Image of reverse side of an ATM skimmer with visible wiring schematics
File Path / Location	`/img_SYSTEM.vhd/vol_vol8/Credit Card Skimmers and ATM Card Skimmers pictures and images_files/atm-skimmer-and-keypad.jpg`
File Type	JPEG image
File Size	49,809 bytes
Date Created	2014-01-30 08:04:48 PST
Date Modified	2014-01-30 08:04:42 PST
MD5 Hash	b422e8b1547b7170e875e5841f573fb4
Tool Used	Autopsy, ExifTool
Analysis / Notes	This image depicts the reverse side of an ATM skimmer device placed on paper that appears to contain annotated wiring schematics for the device. This image goes beyond reference material and is consistent with technical documentation that would be used in the manufacture or assembly of skimming hardware. Its storage on the hidden partition alongside EX-19 (technical schematics PDF) reinforces this assessment.
Linked Exhibits	EX-16, EX-17, EX-19

6.10 Credit Card Skimmer Schematics PDF (EX-19)

Evidence Item	Details

Exhibit #	EX-19
File Name	AISB08.pdf
Description	PDF file containing credit card skimmer circuit schematics; also contained a hidden subfolder with document engraving templates
File Path / Location	`/img_SYSTEM.vhd/vol_vol8/AISB08.pdf`
File Type	PDF
File Size	79,262 bytes
Date Created	2014-01-30 07:58:25 PST
Date Modified	2014-01-30 07:58:26 PST
MD5 Hash	86ffa112c11f0b9ea0f2ef44745ad09c
Tool Used	Autopsy
Analysis / Notes	This file presents as an ordinary PDF but upon examination was found to contain a hidden subfolder holding TIFF image files and engraving templates consistent with those used in the production of identity documents and cards. The main PDF document contains pages that are largely blank with at least one page bearing visible circuit schematics for credit card skimmer hardware. This file represents a dual-purpose concealment document: it contains both identity document production materials and credit card skimmer construction data. This is consistent with a subject engaged in both fraudulent document production and credit card skimmer manufacturing or sales.
Linked Exhibits	EX-15, EX-16, EX-17, EX-18, EX-24

6.11 Credit Card Skimmer Sales/Reference Website (EX-20)

Evidence Item	Details
Exhibit #	EX-20
File Name	Credit Card Skimmers and ATM Card Skimmers pictures and images.htm
Description	Saved HTML webpage relating to credit card skimmer devices; file presents as an informational page while functioning as an order-placement interface
File Path / Location	`/img_SYSTEM.vhd/vol_vol8/Credit Card Skimmers and ATM Card Skimmers pictures and images.htm`
File Type	HTML saved page
File Size	34,936 bytes

Date Created	2014-01-30 08:04:48 PST
Date Modified	2014-01-30 08:04:50 PST
MD5 Hash	15403804c9bbd9d7551213c1e24cf5e2
Tool Used	Autopsy
Analysis / Notes	This saved HTML page is disguised as an informational resource on card skimming, but examination reveals it to be a platform through which skimmer orders could be placed. The file was found on the hidden virtual hard drive, consistent with intentional concealment. The colocation of this file with skimmer overlay images (EX-16, EX-17, EX-18), schematics (EX-19), and card printer research (EX-21, EX-22) supports the interpretation that this is operational material, not incidental browsing.
Linked Exhibits	EX-16, EX-17, EX-18, EX-19

6.12 Driver's License Card Printer Research (EX-21)

Evidence Item	Details
Exhibit #	EX-21
File Name	Driver License Card Printer, Driver License Card Printer Suppliers and Manufacturers at Alibaba_com.htm
Description	Saved Alibaba.com product listing page for industrial driver's license card printers
File Path / Location	`/img_SYSTEM.vhd/vol_vol8/Driver License Card Printer, Driver License Card Printer Suppliers and Manufacturers at Alibaba_com.htm`
File Type	HTML saved page
File Size	266,508 bytes
Date Created	2014-01-30 08:01:25 PST
Date Modified	2014-01-30 08:01:26 PST
MD5 Hash	e0de19f8d449ac7c39fdb8cf573dc169
Tool Used	Autopsy
Analysis / Notes	This saved page from Alibaba.com lists industrial-grade printer equipment marketed specifically for driver's license and identification card production. This is directly consistent with the fraudulent document price list (EX-01), which includes driver's licenses and ID cards as items offered for sale. The presence of this procurement research

	on the hidden partition indicates the subject was exploring sourcing channels for equipment used in document forgery.
Linked Exhibits	EX-01, EX-22

6.13 Card Printer Research — Zebra Technologies (EX-22)

Evidence Item	Details
Exhibit #	EX-22
File Name	Card Printers.htm
Description	Saved Zebra Technologies product page for commercial-grade card printers
File Path / Location	`/img_SYSTEM.vhd/vol_vol8/Card Printers.htm`
File Type	HTML saved page
File Size	44,276 bytes
Date Created	2014-01-30 08:02:43 PST
Date Modified	2014-01-30 08:02:44 PST
MD5 Hash	53fb37fea92358c17e9c4bb2d7a0d8fc
Tool Used	Autopsy
Analysis / Notes	This file is a saved product page from Zebra Technologies, a manufacturer of commercial-grade ID and card printing equipment. In conjunction with EX-21, this demonstrates that Wilson was actively researching multiple vendors for card printing hardware consistent with the production of the fraudulent identity documents listed in EX-01.
Linked Exhibits	EX-01, EX-21

6.14 Steganographic / Disguised PDF Container (EX-24)

Evidence Item	Details
Exhibit #	EX-24
File Name	pdf.pdf
Description	File presenting as a PDF but functioning as a disguised folder containing hidden image files
File Path / Location	`/img_SYSTEM.vhd/vol_vol8/pdf.pdf`
File Type	Disguised container / steganographic file

File Size	433,994 bytes
Date Created	2014-01-30 07:57:57 PST
Date Modified	2014-01-30 07:57:58 PST
MD5 Hash	8bd6509aba6eafe623392995b08c7047
Tool Used	Autopsy
Analysis / Notes	This file presents as a standard PDF document but upon forensic examination was determined to contain a hidden folder structure housing multiple image files, including colorful graphics consistent with identity document templates or design elements. This technique of disguising a file container as a different file type is a form of steganography and demonstrates technical knowledge of file concealment methods. This file was located on the hidden virtual hard drive, adding an additional layer of concealment.
Linked Exhibits	EX-19, EX-31

6.15 Browser History — Firefox (EX-28)

Evidence Item	Details
Exhibit #	EX-28
File Name	places.sqlite
Description	Mozilla Firefox browser history database
File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/AppData/Roaming/Mozilla/Firefox/Profiles/8pp14cbi.default/places.sqlite`
File Type	SQLite database
File Size	104,857 bytes
Date Modified	2015-05-26 05:46:09 PDT
MD5 Hash	86bd9af8f5535338b69fcc9edf335b99
Tool Used	Autopsy (Firefox Analyzer module)
Analysis / Notes	The Firefox browser history database for the Jimmy Wilson user profile contains the following notable search queries: "handguns," "how to steal identities," and "identity theft jail time." The search for "identity theft jail time" is particularly noteworthy as it suggests the subject had awareness of the criminal nature of the activity and was researching the potential legal consequences. Full browser history details are documented in Exhibit A (Excel export).

Linked Exhibits	EX-29, EX-30

6.16 Internet Explorer / Edge Web Cache (EX-29)

Evidence Item	Details
Exhibit #	EX-29
File Name	WebCacheV01.dat
Description	Microsoft Internet Explorer / Edge browsing cache and search query log
File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat`
File Type	Database (JET Blue / ESE)
File Size	33,619,968 bytes
Date Modified	2015-05-26 05:46:18 PDT
MD5 Hash	63d516b8bfea9dbf6e0fa102ab4f318f
Tool Used	Autopsy (Microsoft Edge Analyzer module)
Analysis / Notes	The web cache database contains the following notable search queries: "ID Theft" (Yahoo.com, 2014-02-10 15:07:57 PST), "ID Theft" (Yahoo.com, 2014-02-10 15:18:21 PST), "fast getaway cars" (Bing.com, 2014-02-10 15:12:27 PST), and "how to disappear without a trace" (Bing.com, 2014-02-10 15:18:35 PST). The date of these searches — February 10, 2014 — is six days prior to the documented email order communications of February 16, 2014, suggesting the subject was conducting operational research in the days leading up to those transactions. The searches for "fast getaway cars" and "how to disappear without a trace" indicate awareness of law enforcement risk and potential planning for flight. Full web cache records are documented in Exhibit A (Excel export).
Linked Exhibits	EX-28, EX-30

6.17 Financial Concealment Bookmark (EX-30)

Evidence Item	Details
Exhibit #	EX-30
File Name	How to Hide Money From The Government — Libertarian Money.url
Description	Internet shortcut bookmarked by the subject to a webpage about concealing money from government authorities

File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/Favorites/How to Hide Money From The Government  Libertarian Money.url`
File Type	Internet shortcut (.url)
File Size	244 bytes
Date Created	2015-05-26 05:46:02 PDT
MD5 Hash	e792b89742e8e2d7c26110e7b58467bd
Tool Used	Autopsy
Analysis / Notes	This file represents a saved browser bookmark by the subject to an article titled "How to Hide Money From The Government." The preservation of this resource as a bookmark indicates sustained interest in financial concealment. Taken together with the web cache entries in EX-29, this is consistent with a subject engaged in cash-based criminal activity seeking to avoid financial detection or seizure.
Linked Exhibits	EX-28, EX-29

6.18 Refusal to Consent to Search (EX-32)

Evidence Item	Details
Exhibit #	EX-32
File Name	To Whom it may concern.doc
Description	Word document authored by Jimmy Wilson formally declining to consent to a search of his computer
File Path / Location	`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/Documents/To Whom it may concern.doc`
File Type	Microsoft Word document (.doc)
File Size	10,752 bytes
Date Created	2015-05-26 05:46:12 PDT
Date Modified	2015-05-26 05:46:12 PDT
MD5 Hash	5c02e0f5f7f527de8a99d65d2e50a159
Tool Used	Autopsy
Analysis / Notes	This document was authored by the subject and states that he declines and does not consent to a search of his computer. This document does not affect the admissibility of evidence obtained pursuant to lawful legal authority but is noted as it demonstrates the subject's awareness of law enforcement interest in his device and a deliberate effort to obstruct examination.
Linked Exhibits	None

---

7. Email Evidence Analysis

All email messages were recovered from the Windows Live Mail archive located at:

`/img_2020JimmyWilson.E01/vol_vol6/USERS/Jimmy Wilson/AppData/Local/Microsoft/Windows Live Mail/Gmail (wils 48a/`

All emails involving criminal activity were transmitted from the hostname **IACISHDD2014** via IP address **166.149.54.198** (resolved to `sub-166-149-54.myvzw.com` — Verizon Wireless mobile network), using Microsoft Windows Live Mail version 16.4.3508.205.

Raw email headers for all exhibits are preserved in the `reports/email-headers/` directory and constitute **Exhibit D** of this report.

7.1 EX-05 — Jose Badguy Inquires About Services

Email Item	Value
Exhibit #	EX-05
From (Display Name)	jose.badguy@hushmail.com
From (Actual Address)	jose.badguy@hushmail.com
To	wilsonjimmy807@gmail.com
Subject	R U Still in business
Date Sent (Header)	2014-02-16T18:01:25Z (10:01:26 AM PST)
Date Received	2014-02-16 10:01:26 PST
Message-ID	`<20140216180125.349412035E@smtp.hushmail.com>`
Originating IP	65.39.178.239 (Hushmail SMTP server)
Mail Server / Received Chain	smtp.hushmail.com → mx.google.com → Gmail inbox (wilsonjimmy807@gmail.com)
Attachments	None
Key Findings	Jose Badguy contacts Wilson via privacy-oriented Hushmail service, asking whether Wilson is still offering his illicit "items made" service. The use of Hushmail — a privacy-focused, encrypted email provider — rather than a conventional email service is consistent with an intent to conceal the nature of communications. The phrase "I need some items made" directly parallels the language used in other emails placing orders for fraudulent documents.

7.2 EX-06 — Wilson Confirms Active Business and Establishes Encryption Protocol

Email Item	Value
Exhibit #	EX-06
From (Display Name)	wilsonjimmy807@gmail.com

From (Actual Address)	wilsonjimmy807@gmail.com
To	jose.badguy@hushmail.com
Subject	Re: R U Still in business
Date Sent (Header)	2014-02-16T19:35:28Z (11:35:29 AM PST)
Date Received	—
Message-ID	<5EB608B40DF74C1A907D22E4FB81FFB8@IACISHDD2014>
Originating IP	166.149.54.198 (sub-166-149-54.myvzw.com — Verizon Wireless)
Mail Server / Received Chain	IACISHDD2014 → mx.google.com (TLSv1 / ECDHE-RSA-AES128-SHA) → Hushmail
Attachments	None
Key Findings	Wilson confirms he is still providing services, references a prior computer crash requiring a new setup, and explicitly instructs Jose: "when you request items make sure you send it in a best crypt encode text file with the password we were using before." This instruction establishes a pre-arranged communication security protocol between Wilson and the client — consistent with an organized criminal enterprise deliberately shielding its transactions from detection. Wilson also states he will send a new price list, acknowledging ongoing commercial activity.

7.3 EX-07 — Robert Ripoff Introduces New Email Address

Email Item	Value
Exhibit #	EX-07
From (Display Name)	Robert Ripoff
From (Actual Address)	robert.ripoff@gmx.com
To	wilsonjimmy807@gmail.com
Subject	New email address
Date Sent (Header)	2014-02-16T17:55:09Z (09:55:13 AM PST)
Message-ID	<20140216175509.190490@gmx.com>
Originating IP	74.208.4.200 (GMX mail server)
Mail Server / Received Chain	GMX.com Web Mailer → mx.google.com → Gmail
Attachments	None
Key Findings	Robert Ripoff notifies Wilson of his new GMX email address, stating he lost the previous one, and that he will forward information for "items that I need you to make for me." The phrase mirrors Jose Badguy's language in EX-05 and confirms a second client actively using Wilson's forgery service. SPF authentication passed for the GMX sending domain, confirming the email's

	origin.

7.4 EX-08 — Wilson Instructs Robert on Encryption Protocol

Email Item	Value
Exhibit #	EX-08
From (Display Name)	wilsonjimmy807@gmail.com
From (Actual Address)	wilsonjimmy807@gmail.com
To	Robert Ripoff (robert.ripoff@gmx.com)
Subject	Re: New email address
Date Sent (Header)	2014-02-16T19:32:15Z (11:32:18 AM PST)
Message-ID	<C84F729D6AD34D84A4BC16295569FA41@IACISHDD2014>
Originating IP	166.149.54.198 (Verizon Wireless)
Mail Server / Received Chain	IACISHDD2014 (TLSv1) → mx.google.com → robert.ripoff@gmx.com
Attachments	None
Key Findings	Wilson instructs Robert to "send it in a best crypt encode test file with the password we discussed earlier." The phrase "best crypt encode" is a reference to BCTextEncoder, the same encryption application used in all subsequent order attachments. This email confirms that Wilson imposed a standard, pre-arranged encryption protocol on all client order communications, consistent with deliberate operational security practices to protect criminal transactions.

7.5 EX-09 — Wilson Sends Encoded Price List to Jose Badguy

Email Item	Value
Exhibit #	EX-09
From (Display Name)	wilsonjimmy807@gmail.com
From (Actual Address)	wilsonjimmy807@gmail.com
To	jose.badguy@hushmail.com
Subject	New Price List
Date Sent (Header)	2014-02-16T20:48:48Z (12:48:49 PM PST)
Message-ID	<9C87FF45FFB741899C3EB29F22FAA73A@IACISHDD2014>
Originating IP	166.149.54.198 (Verizon Wireless)
Attachments	New Price List Encoded.TXT (EX-02)
Key Findings	Wilson sends the encrypted price list (EX-02) to Jose Badguy. The email body states: "Jose, the new price list is attached." The attached

	encoded text matches the BCTextEncoder ciphertext also found in EX-10 and EX-11, confirming the same price list was distributed to both clients simultaneously.

7.6 EX-10 / EX-11 — Wilson Sends Encoded Price List to Robert Ripoff

Email Item	Value
Exhibits #	EX-10 (6DF15AF1), EX-11 (15611658)
From	wilsonjimmy807@gmail.com
To	robert.ripoff@gmx.com
Subject	New Price List / new price list
Dates Sent	2014-02-16T20:50:41Z and 2014-02-16T20:53:57Z
Message-IDs	<FA89914B5C604B3BACC50A3A6CB9EB57@IACISHDD2014> and <11313DF999AD4157A7510AD6EC23231F@IACISHDD2014>
Originating IP	166.149.54.198 (Verizon Wireless)
Attachments	New Price List Encoded.TXT (EX-02)
Key Findings	Wilson sent the encrypted price list to Robert Ripoff twice within a four-minute window (12:50 PM and 12:54 PM). Both emails originate from the same host and IP as all other Wilson-authored emails in this case. The duplication suggests a possible resend or confirmation. The attached BCTextEncoder ciphertext in both emails is identical to the attachment sent to Jose Badguy (EX-09), confirming this is the same price list transmitted to both clients.

7.7 EX-12 — Jose Badguy Accepts Price List and Submits Encrypted Order

Email Item	Value
Exhibit #	EX-12
From	jose.badguy@hushmail.com
To	wilsonjimmy807@gmail.com
Subject	Re: New Price List
Date Sent (Header)	2014-02-16T21:02:29Z (1:02:29 PM PST)
Message-ID	<20140216210229.EAB962035E@smtp.hushmail.com>
Originating IP	65.39.178.239 (Hushmail SMTP)
Attachments	Jose 42 encoded.TXT (EX-03); additional image attachments (animals)
Key Findings	Jose Badguy replies: "Jimmy, The new price list is ok, here is what I need." The encoded attachment (EX-03) constitutes the

	encrypted order for fraudulent items. The animal images served as decoy attachments to obscure the significance of the encoded text file to casual inspection.

7.8 EX-13 — Robert Ripoff Accepts Price List and Submits Encrypted Order

Email Item	Value
Exhibit #	EX-13
From	Robert Ripoff (robert.ripoff@gmx.com)
To	wilsonjimmy807@gmail.com
Subject	Re: new price list
Date Sent (Header)	2014-02-16T22:26:52Z (2:26:52 PM PST)
Message-ID	`<20140216222652.231940@gmx.com>`
Originating IP	74.208.4.200 (GMX mail server)
Attachments	Robert 17 Encoded.TXT (EX-04); additional image attachments (animals)
Key Findings	Robert Ripoff replies: "Jimmy, I'm ok with the new prices, I attached what I need to this email. Let me know when you finish the task." The phrase "when you finish the task" confirms that Wilson is the manufacturer/producer of the ordered items. As with EX-12, the accompanying animal images are assessed as decoy attachments. The encoded file (EX-04) constitutes the encrypted order submission.

---

8. Image Evidence Analysis

All images listed below were extracted from the forensic image using Autopsy. Metadata was examined using ExifTool. Original image files are preserved in `reports/image-evidence/originals/`. Reference screenshots are located in `reports/image-evidence/screenshots/`.

8.1 EX-25 — Identity Theft Method Reference Image (image21.jpg)

Image Item	Value
Exhibit #	EX-25
File Name	image21.jpg

File Path	`/img_2020JimmyWilson.E01/vol_vol6/USERS/JimmyWilson/Documents/IDtheftrev.pdf/image21.jpg`
File System Created	N/A (embedded in document)
File Size	101,080 bytes
MD5 Hash	eaf4511fc762cbf3bc19c03e02898d9f
Key Findings	This image depicts a transaction at a retail clothing store in which a customer is paying by credit card. A third party, partially visible at the edge of the frame, is covertly photographing the customer's credit card with a mobile device. The image was embedded within a document titled "IDtheftrev.pdf" (Identity Theft Review), stored in the subject's Documents folder. This image is consistent with documentation of a credit card skimming/theft technique using mobile device photography — a method for capturing card data without physical contact.

8.2 EX-26 — Mail Surveillance Reference Image (image31.jpg)

Image Item	Value
Exhibit #	EX-26
File Name	image31.jpg
File Path	`/img_2020JimmyWilson.E01/vol_vol6/USERS/JimmyWilson/Documents/IDtheftrev.pdf/image31.jpg`
File Size	85,634 bytes
MD5 Hash	009ceae569c4cc1e8ba60e80ef4344f2
Key Findings	This image is a close-up photograph focused on envelopes being deposited into a mailbox by a mail carrier. The framing of the image — with the letter carrier not centered but the mail pieces prominent — indicates the photographic subject of interest is the mail itself rather than the carrier. This image is consistent with documentation of mail theft methodology, wherein the target is capturing personally identifiable information from intercepted correspondence.

8.3 EX-16 / EX-17 / EX-18 — ATM Skimmer Overlay Images

(Full analysis provided in Section 6.8 and 6.9 above.)

These images were recovered from the hidden virtual hard drive (EX-31) and depict physical ATM card skimmer overlay devices. EX-18 specifically depicts the internal wiring configuration of a skimmer. These images, combined with the technical schematics in EX-19, constitute a collection of materials consistent with ATM skimmer manufacture and distribution.

9. Conclusions

The forensic examination of the disk image `2020JimmyWilson.E01` revealed a substantial and consistent body of digital evidence supporting the conclusion that **Jimmy Wilson** (wilsonjimmy807@gmail.com) operated an organized criminal enterprise engaged in **the production and sale of fraudulent identity documents and credit/financial cards** and was involved in **the acquisition, research, and likely distribution of credit card skimming devices**.

The following specific findings support these conclusions:

1. Fraudulent Document Production and Sales Operation

A decrypted price list (EX-01) recovered from the subject's Recycle Bin, dated February 1, 2014, establishes that Wilson offered for commercial sale: counterfeit credit cards ($350), driver's licenses ($250), identification cards ($250), green cards ($300), and insurance certificates ($100). This file was transmitted in encrypted form (EX-02) to at least two identified clients — Jose Badguy (jose.badguy@hushmail.com) and Robert Ripoff (robert.ripoff@gmx.com) — via email on February 16, 2014 (EX-09, EX-10, EX-11). Both clients confirmed acceptance of the pricing and submitted encrypted orders (EX-03, EX-04) via the pre-arranged BCTextEncoder protocol. Robert Ripoff's response explicitly states: "Let me know when you finish the task" — language directly establishing Wilson as the manufacturer. Research into industrial card printing equipment was found preserved on the hidden virtual hard drive, including a saved Alibaba.com listing for driver's license card printers (EX-21) and a Zebra Technologies commercial card printer catalog (EX-22), consistent with sourcing equipment for document production.

2. Deliberate Use of Encryption and Operational Security

All order transactions between Wilson and his clients were conducted using BCTextEncoder v. 1.01.1, an encryption utility identified on the subject's system. Wilson instructed both clients in writing to use the encryption tool with a pre-agreed password for all order submissions (EX-06, EX-08). Client Jose Badguy used Hushmail — a privacy-focused encrypted email provider — as an additional layer of communication concealment. Wilson employed a hidden virtual hard drive (SYSTEM.vhd, EX-31) to conceal criminal materials from casual inspection. A TrueCrypt-encrypted container named "moneymaker" (EX-15) was found within the hidden partition and remains undecrypted; its name and the recency of its modification date (February 11, 2014) place it within the active period of the criminal operation. Decoy animal image attachments were used in client emails to obscure the significance of the encrypted order files. The subject also created a document formally refusing consent to a computer search (EX-32), indicating consciousness of guilt.

3. Credit Card Skimmer Involvement

Stored within the hidden virtual hard drive, examiners recovered: photographic images of ATM card skimmer overlay devices (EX-16, EX-17); a detailed image of a skimmer's internal wiring configuration (EX-18); a PDF document (EX-19) containing credit card skimmer circuit schematics

alongside hidden document engraving templates; a saved webpage (EX-20) assessed as an operational reference or ordering platform for skimming devices; and comprehensive background research materials (EX-23) from the security journalism site Krebs on Security, specifically their coverage of card skimming operations. The co-location of skimmer schematics and identity document production materials within a single hidden partition, combined with the fraudulent price list's inclusion of credit cards as a product offering, is consistent with a vertically integrated operation manufacturing both fraudulent payment cards and the hardware to capture the underlying card data.

4. Identity Theft Methodology Research

The subject's browser history (EX-28) reflects searches for "handguns," "how to steal identities," and notably "identity theft jail time" — indicating awareness of the criminal nature of the activity and research into its legal consequences. Web cache records (EX-29) show additional searches for "ID Theft," "fast getaway cars," and "how to disappear without a trace" on February 10, 2014 — six days prior to the documented order transactions. Images consistent with credit card skimming and mail theft techniques were preserved in a document titled "IDtheftrev.pdf" within the subject's Documents folder (EX-25, EX-26). A bookmarked webpage titled "How to Hide Money From The Government" (EX-30) is consistent with the subject seeking to conceal proceeds from criminal activity.

5. Limitations of the Examination

The following items require additional analysis and may yield further evidence upon successful completion:

- The TrueCrypt-encrypted container "moneymaker" (EX-15) could not be decrypted without the password. Its contents are unknown.
- Three database files (EX-34, EX-35, EX-36) flagged by Autopsy for suspected encryption were not decrypted due to time constraints and may contain additional probative information.
- The specific contents of the encoded order files submitted by Jose Badguy (EX-03) and Robert Ripoff (EX-04) could not be determined without the pre-arranged BCTextEncoder password.
- The deleted image $R8OPSCS.JPG (EX-33), recovered from the Recycle Bin, warrants further analysis to determine its relevance to the case.

---

10. Examiner Certification

I certify that the information contained in this report is true and accurate to the best of my knowledge, and that the examination was conducted in accordance with accepted digital forensic principles and practices. The forensic image was examined in a read-only forensic environment; the original evidence was not altered or modified at any point during the examination process.

Field	Details

Examiner Name	Ulysses Ochoa
Title / Role	Digital Forensic Examiner
Date of Report	April 25, 2026
Signature	_____

Appendices

Exhibit	Description
Exhibit A	Autopsy Evidence Export (Excel) — `reports/evidence-inventory/Excel.xlsx`
Exhibit B	Evidence Item Notes (per tagged item) — `reports/evidence-notes/`
Exhibit C	ExifTool Metadata Exports (per image)
Exhibit D	Raw Email Headers — `reports/email-headers/`
Exhibit E	Reference Screenshots — `reports/image-evidence/screenshots/`
Exhibit F	Chain of Custody Form — `reports/chain-of-custody/2020JimmyWilson-Chain-of-Custody.docx`
Exhibit G	Original Image Files — `reports/image-evidence/originals/`