SWGDE Best Practices for Examining Magnetic Card Readers

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Best Practices for Examining Magnetic Card Readers

Table of Contents

Table of Figures

1. Purpose

The purpose of this document is to describe best practices for seizing, acquiring, and analyzing the data contained within magnetic card readers. As a skimming device is not typically deemed contraband, it is the responsibility of the investigator/examiner to determine if the device was used illegally.

2. Scope

Magnetic card readers, when used for illegal purposes, are commonly referred to as skimmers. This document provides information on seizing, acquiring, and analyzing skimming devices capable of acquiring and storing personally identifiable information (PII) in an unauthorized manner.

3. Limitations

Skimmers present unique examination challenges due to:

- rapid changes in technology;
- difficulty of device disassembly;
- lack of standards in use of the technology;
- use of alternate/repurposed components;
- use of encryption and/or countermeasures;
- multiple data encoding/modulation formats;
- prevention of chip identification by obfuscation of the device;
- availability of training and documentation;
- lack of chip information/ documentation;
- lack of adapters available for chip reading;
- lack of software's ability to support reading chip data;
- lack of commercially available software to analyze data extracted from skimmers.

4. Technical Background

As skimmers are often unique in design and implementation, examination processes vary depending upon the category and/or type of device.

In general, skimmers can be broken down into the following three categories:

1. Hand-held
2. Altered hand-held
3. Custom

The processes used in examinations vary greatly depending on the device itself and the manner in which the stored information is encoded.

4.1 Hand-Held

Data extraction of hand-held skimmers (see ***Figure 1***) is accomplished by connecting the skimmer to the examiner's computer via a data cable. Once connected, a program is executed that extracts all of the stored track data from the device.

Figure 1. Example of a hand-held skimmer

4.2 Altered Hand-Held

It is common for commercial skimmer devices to be dismantled and used for parts (cannibalized). These devices are commonly seized from automated teller machines (ATMs), bank point of sale terminals, and gas pumps. Examination of these devices is frequently performed in a manner similar to hand-held devices. Wireless enabled skimmers are often considered to be an alteration of commercial skimmers (see ***Figure 2*** and ***Figure 3***).

Figure 2. Example of an altered hand-held skimmer

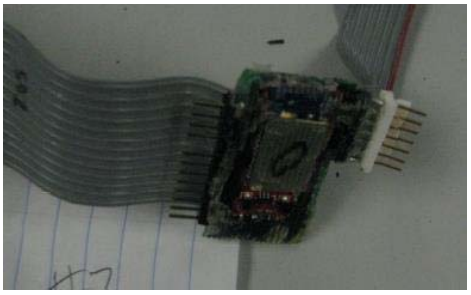

Figure 3. Example of an altered hand-held skimmer with Bluetooth™

4.3 Custom

By far, the most complicated and difficult-to-examine skimmers are custom manufactured devices (see ***Figure 4***). These devices use many different circuit designs and proprietary data encoding, modulation, and encryption schemes. These skimmers can be combined with a pinhole camera or a keypad overlay to capture the personal identification number (PIN) of the account holder.

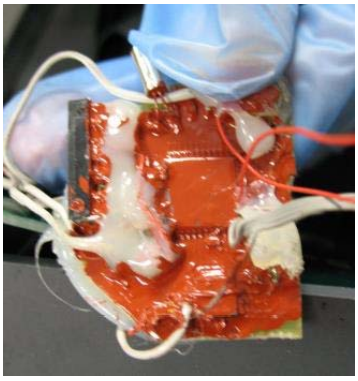

Figure 4. Example of a custom skimmer

As it is common in some larger metropolitan area ATMs to require a customer to use their account card for entry to a vestibule, subjects can implant foreign circuitry into the door reader (see ***Figure 5***).

Figure 5. Example of a custom skimmer (door)

Some skimming devices have the capability to output captured data via wireless communication methods (see ***Figure 6***). These devices transmit their data in real-time or batch mode. The transmitting ability of these devices and the choice of transmission protocols used make detection of these receivers difficult.

Figure 6. Example of a cellular enabled skimmer

4.4 Card Data/Structure

4.4.1 Fundamentals of Track Data

The International Standards Organization (ISO) created ISO/IEC 7812, which specifies, "a numbering system for the identification of issuers of cards that require an issuer identification number (IIN) to operate in international, inter-industry and/or intra-industry interchange."

The primary account numbers are generally 15 or 16 digits in length but can be as short as 12 (Maestro) or as long as 19 (China UnionPay). The credit card companies have reserved prefixes, for example, American Express cards begin with 34 or 37. Credit card processors use the Luhn algorithm, see ISO/IEC 7812, to ensure the integrity of the primary account number (PAN).

Applications such as access control, identification, and driver licenses have developed their own custom formats for each track. This capability to reformat the content of each track has allowed magnetic stripe card technology to expand into many industries. As defined for financial industry applications, the magnetic stripes carry three tracks of data.

4.4.1.1 Track 1

Track 1 contains alphanumeric information for the automation of airline ticketing or other transactions in which a reservation database is accessed. In addition to the account number and expiration date, this track contains the account holder's name. Typically, Track 1 is only read by hand-held and altered hand-held skimmers.

4.4.1.2 Track 2

Track 2 contains numeric information for the automation of financial transactions. While this track does not contain the account holder name, it does contain the electronic card verification value (CVV). This track is read by systems that require a PIN (e.g., ATMs). Typically, custom skimmers capture only Track 2 information.

4.4.1.3 Track 3

Track 3 contains information that is intended to be updated (re-recorded) with each transaction (e.g., cash dispensers that operate off-line). This track is rarely used and is not of forensic value in most financial fraud investigations.

4.4.2 Card Verification Value 2 (CVV2)

This code is a three to four digit number printed on the back of a card (hard to steal electronically) (see ***Figure 7***). It was designed to help curb fraud in "card not present" transactions, such as Internet purchases.

Figure 7. Example of CVV2

4.4.3 Debit Cards

When skimmed, debit cards and credit cards convey similar data. However, debit cards are different from credit cards as the account is directly linked to fund availability in a bank (or otherwise stored) account. Debit cards present a much more attractive target for skimming as compromised accounts can be converted directly into cash as opposed to goods and services.

5. Evidence Collection

5.1 Seizing Evidence

Devices should be collected and protected in the same manner as flash memory devices (refer to *ASTM E2763 Standard Practice for Computer Forensics* and *SWGDE Best Practices for Computer Forensics*). Associated cables, documentation, and software should also be collected.

Identifying parasitical devices can be challenging, as they are, by their nature, designed to be hidden. These include recording devices hidden under keypads and those placed in-line with a legitimate card reader (see ***Figure 8*** and ***Figure 9***). Removal of these devices can be destructive in nature and should be done cautiously.

Figure 8. Example of keypad overlay

Figure 9. Example of an inline skimmer

5.2 Handling Evidence

Evidence should be handled according to laboratory policy while maintaining a chain of custody and by using best practices (refer to *ASTM E2763 Standard Practice for Computer Forensics* and *SWGDE Best Practices for Computer Forensics*).

5.3 Equipment

Equipment in this section refers to the non-evidentiary hardware and software the examiner uses to conduct data extraction and analysis of the evidence. Equipment and software applications should be verified[1] to ensure proper performance.

[1] The validation process is discussed in *SWGDE Recommended Guidelines for Validation Testing*.

6. Data Extraction

6.1 Hand-Held/Altered Skimming Devices

As commercially available skimmers are not useful unless one can extract the swiped card information, the manufacturers of these devices provide software to facilitate the exportation of the stored data. The software typically has the added functionality to decode stored user passwords from the device. The Windows-based software only provides for logical extraction (that is, no deleted information) into a text format. The examiner requires the device, appropriate software, and the appropriate data cable to conduct a successful data extraction. The cable used performs the extraction via serial over Universal Serial Bus (USB) connectivity. The proper driver loaded on the examination computer and a low COM port setting should be selected so the device has sufficient priority on the system.

6.2 Custom Skimming Devices

All skimming devices must first read the magnetically stored data on a card. This process is accomplished by means of an electromagnetic head, similar to that found in an audiocassette tape player. As the card is manually swiped through the device, the head converts the magnetic information on the card into an electrical signal of time-varying voltage, which is passed to other signal processing components for digital conversion. Devices that store that waveform without further processing are referred to as "analog" devices. "Digital" devices further process the waveform to recover the encoded digital data and only store the decoded information.

6.2.1 Analog Skimming Devices

"Analog" skimming devices pass the captured analog swipe waveform to an analog-to-digital converter (ADC), to produce a digital waveform, which is stored, undecoded, in flash memory. The resulting data file extracted from a device is similar to an audio file and significantly larger than a decoded bit string of account data.

6.2.1.1 Identification

Recognizing an analog skimmer is important, as the method of extraction differs from that of a custom, digital skimmer. While the examiner may or may not notice the lack of an analog-to-digital encoder chip, identification of an analog skimmer is typically made by recognizing the unusually large storage capacity of the device's flash memory chip and are typically indicative of an audio-based skimming device (see ***Figure 10***). Digital skimmers can lack an analog-to-digital encoder chip, with the processing being computed by a microcontroller. While a typical custom skimmer uses a flash chip with two megabytes of storage, an analog skimmer typically contains a flash storage chip in the two-gigabyte range.

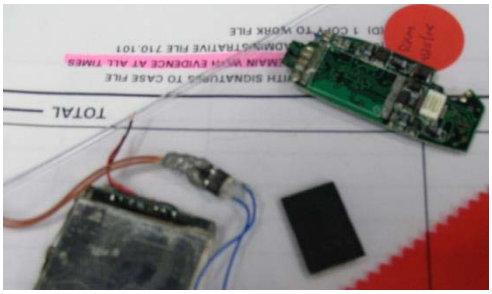

Figure 10. Example of an analog based skimming device

6.2.1.2 Extraction

Many analog skimmers originated as other devices (e.g., MP3 sunglasses). Therefore, an examiner may extract data from the device using its built-in USB mass storage mode. As it is common for a person constructing the skimmer to remove the USB header, the examiner must recognize this architecture and solder a header on the device to facilitate communication. Once the header is attached, the examiner can create an image using traditional computer forensics imaging techniques and software.

6.2.2 Digital Skimmer Devices

Digital skimming devices pass the analog swipe waveform to an analog-to-digital converter (ADC), to produce a digital waveform, which is stored and coded in flash memory. Digital skimmer devices accept input via a magnetic stripe reader like analog skimmers; however, once the skimmer's processor receives the waveform, the signal is decoded with logic before being stored in flash memory. Data is stored in a digital format, which might or might not be encoded, encrypted or both. Extraction of information from a digital skimmer is most commonly done by removing the flash chip and reading the information through the use of a chip programmer.

6.2.2.1 Extraction

As custom (and some altered) skimming devices typically do not have a universal method to connect to and download the skimmed account information (other than USB used by analog devices), an examiner should consider removing the data storage chip and then read the information stored therein. The microcontroller might also need to be removed and read to understand the encoding or encryption methods used by the device. Code protection can prevent the extraction of data from the device's microcontroller.

6.2.2.2 Chip Identification

As previously referenced, custom skimming devices can be quite complicated in nature. Their design can be developed using both new and cannibalized circuits/chips. One of the first steps in examining such a device is to identify how the skimmer is extracting and storing account information. The identification of the components that make up a skimmer is crucial to understanding how to extract stored data successfully. The main components of chip identification are their manufacturer and chip number. Examiners should be able to identify successfully both the microcontroller and the flash storage chips. It is important to document/photograph them before removal as extreme temperatures can remove identification markings. In cases where the identification number is worn or difficult to read, a microscope might be required. Additionally, applying a non-reactive and easily removed solution, such as isopropyl alcohol, can make identification numbers easier to read.

6.2.2.3 Chip Removal

Once the chips of forensic significance are identified, they should be properly removed from the circuit board in a manner that ensures they are not damaged. Removal should only be performed by properly trained and experienced personnel. The two most predominantly used methods of extraction for Ball Grid Array (BGA) chips include hot air and infrared. Methods that heat the entire chip being removed at once are preferred as they reduce the chance of physical damage induced by prying and bending the pins.

6.2.2.4 Chip Connectivity and Reading

There are several chip readers commercially available, with each reader possibly supporting a different subset of chips. Most readers require a socket adapter, which is dependent on the chip package. However, on certain smaller chips (e.g., 8-pin flash) connectivity between the chip and the socket adapter can be established through a series of wires soldered to the chip pins and inserted into the reader, typically via a Zero Insertion Force (ZIF) socket. Once properly connected, it can then be read using the vendor provided software. The extracted data should be saved, write protected, and hashed prior to analysis. Analysis should then be performed on a working copy.

As was mentioned in **Section 4.3**, custom skimming devices may use a wireless technology (i.e., Bluetooth™ and/or ZigBee™) to broadcast card information. It might be possible, and preferred, to extract data from these devices through a wireless connection if certain pairing data is known to the examiner, i.e., the specific channel on which a ZigBee™ radio skimmer is broadcasting or the pairing code for a Bluetooth™ enabled skimmer.

7. Data Analysis

7.1 Data Format Types

Relative to skimmer data analysis, there are two types of recordings, analog and digital. Digital skimmer data recordings consist of several different sub-types that will be discussed later. The ISO/IEC 7812 and 7813 track data formatting assists the examiner in analyzing the extracted data, as it provides a set of rules to which the decoded information should conform. As most card readers are bidirectional, care must be taken during the analysis phase to account for numbers sequenced forward and backward while also ensuring duplicate account numbers are not repeated in the final report.

7.1.1 Analog Skimmer Data

The file(s) present on an analog skimming device are not immediately perceived as potential stolen account information to the examiner (or automated credit card finder scripts). Most commonly, the file(s) can be in the form of a WAV audio file. An examiner begins analysis by carving the physical image identifying all file segments with audio file headers. This can be done using traditional data carving tools. Once the files are carved, they need to be converted to a format that is agreeable to scripting. This can be done using a variety of audio-based software tools. This part of the process can be accomplished by converting the file into a new format (e.g., 16-PCM, ADPCM). With the data in this new format, a clock-recovery algorithm with noise threshold activation is scripted to drive an adaptive BFSK algorithm to generate the bit stream (see top of ***Figure 11***). From the track's bit stream, scripting is further used to decode the Aiken bi-phase encoding to the actual account numbers.

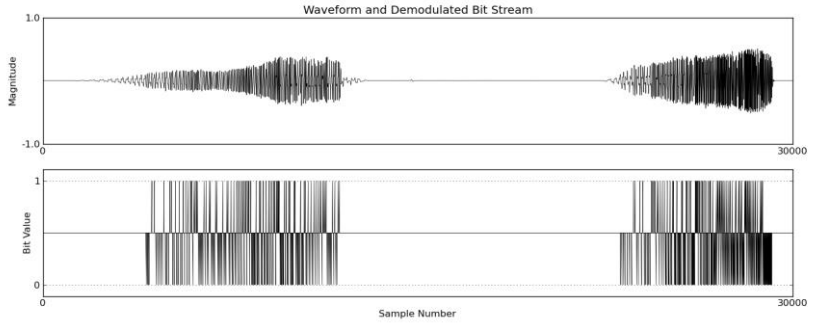

Figure 11. Example of a 5-bit graph

While scripting utilities can assist the examiner in converting the 1's and 0's into possible account numbers, the examiner should validate the results of the script by completing at least one transcription by hand. Analog skimmers typically capture the second track on a magnetic card. Track 2 is encoded using 5-bit ASCII (4-bit odd parity per *ANSI X4.16 American National Standard for financial services, financial transaction cards, magnetic stripe encoding*) and the account information follows a start sentinel of 11010. Using a fictitious example of a credit card that begins with a Bank Identification Number (BIN) number or IIN, of "4271", and taking into account the possibility that swipes can be recorded forward or reverse, the examiner would then examine the bottom part of the graph in ***Figure 11*** (representing the bits decoded from the

waveform) and attempt to locate the start sentinel (11010). Once it is located, using 5-bit ASCII encoding the examiner decodes the 1's and 0's (graphed by the highs and lows) to determine if the results were accurate. Continuing to use "4271" as an example, the examiner would expect to find the string: 11010001000100011100100000.

As the data was originally recorded in an analog manner, the files being analyzed can contain noise. As such, the threshold for any analysis must be tuned so that an examiner does not miss account numbers. This threshold analysis begins by looking at the extracted track data in a spectrum analyzer (see ***Figure 12***). The analyzer gives a visual representation of the number of potential account numbers recorded by the skimmer. An examiner must compare the number of account numbers visually seen versus those decoded in the spectrum analyzer. If there are more seen than decoded, then the threshold of the process to decode the information into account numbers should be reconfigured.

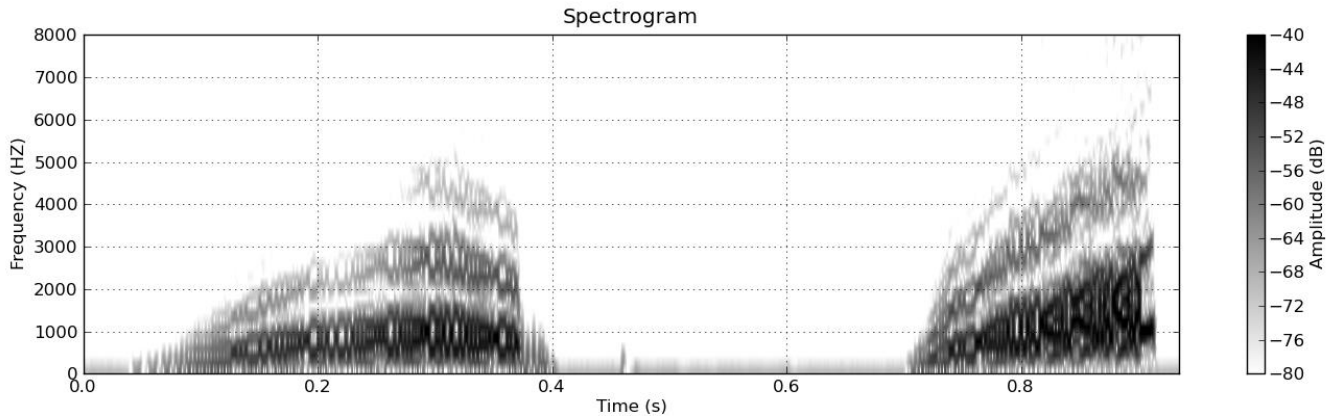

Figure 12. Example of swipes shown in a spectrum analyzer

7.1.2 Digital Data

Data can be recorded digitally and encoded or encrypted in a wide variety of formats. Common encoding formats include 8-bit ASCII, 5-bit ASCII, and Little Endian Binary-Coded Decimal. Common encryption practices vary in their confusion/diffusion implementation. In some cases, single byte XOR keys are used, others implement cryptographically sound algorithms, such as Advanced Encryption Standard (AES). The use of statistical analysis on the extracted data is an important first step in determining if information read is encoded or encrypted. Data that is encrypted typically exhibits higher levels of diffusion than encoded data, resulting in byte values being more evenly distributed (see ***Figure 13*** and ***Figure 14***).

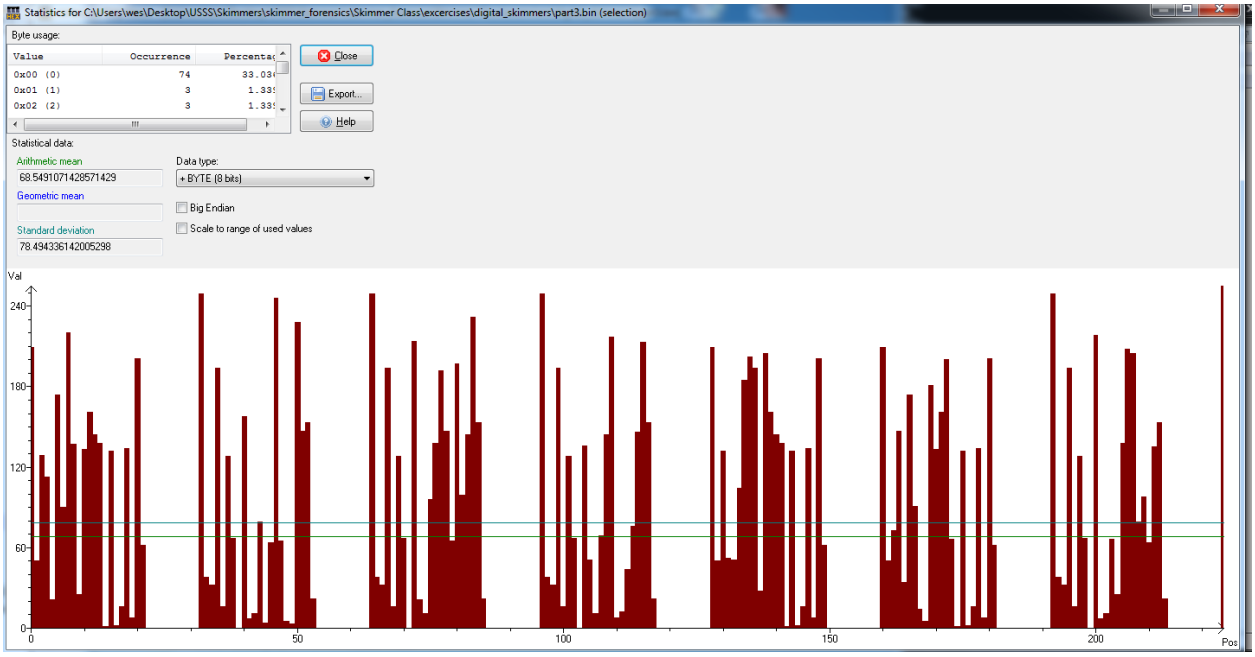

Figure 13. Example of unencrypted data

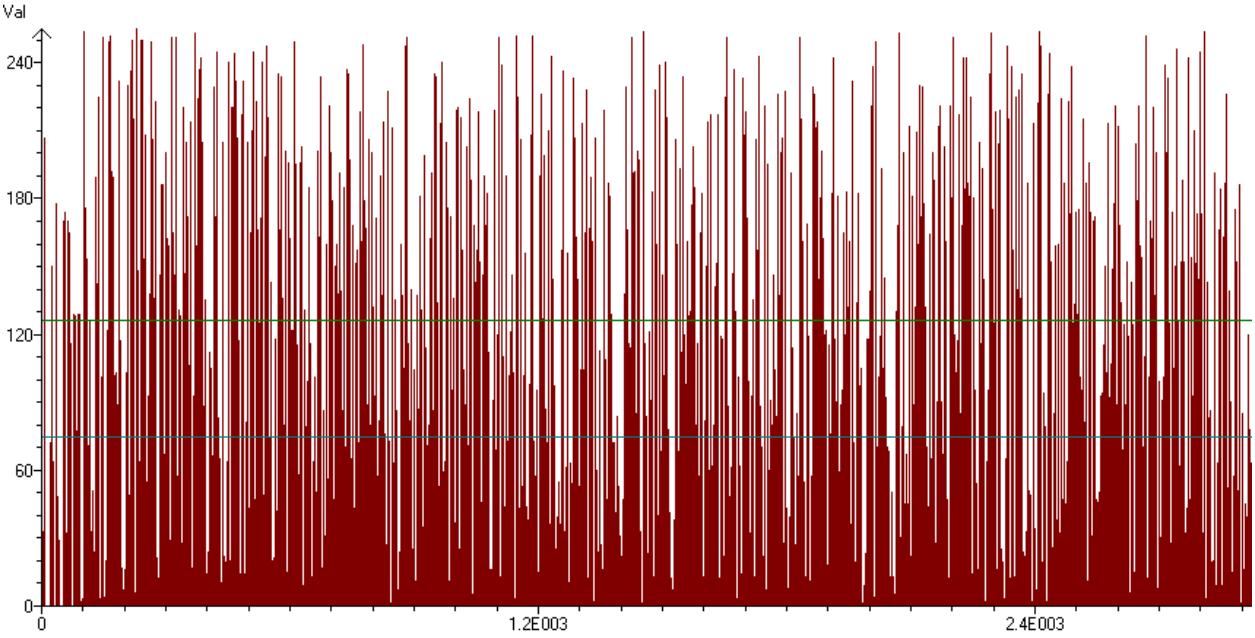

Figure 14. Example of encrypted data

7.1.2.1 8-bit ASCII

The majority of hex viewers have the ability to display data in both hexadecimal and ASCII formats. ASCII makes data identification easy as information is displayed in a human readable format (e.g., 1238585934020). The examiner may also yield additional results by running a strings command against the extracted data to easily identify ASCII word groupings.

7.1.2.2 5-bit ASCII

This type of encoding is best recognized using a tool that displays data in Base2 (Binary). Once viewed as binary, the examiner can then search for a 5-bit account number start sentinel (11010, or 01011 if a reverse swipe). Once the start sentinel is located, the examiner can decode the binary characters following (or proceeding, if it was a backwards swipe) and check to see if any possible account numbers conform to the Luhn algorithm. The range of binary characters varies according to the potential account number, e.g., 80 bits (16 digit account numbers multiplied by 5 bits) for a Visa or MasterCard account number. If the examiner is able to recover a valid (per Luhn) account number, then the rest of the data can be decoded using an automated process.

7.1.2.3 Unpacked Binary-Encoded Decimal (BCD)

This encoding scheme is discernable using traditional hex viewing software. If the data is stored with unpacked BCD encoding, the account number will be displayed in hexadecimal with a header value of 0x21. The account number data following the header will be 12 to 19 bytes in length followed by an indeterminate number of 0x00 values (padding). The next account number will begin with a 0x21 header followed by the second account number, etc. See ***Figure 15*** for an example showing two fictitious account numbers (Red = Header; Green = Account Number; Orange = Padding). The sample below depicts unpacked BCD data for the following account numbers: 4344562104567443 and 34563210876543011.

Once successfully identified, the examiner can then check the validity of the account numbers using the Luhn algorithm.

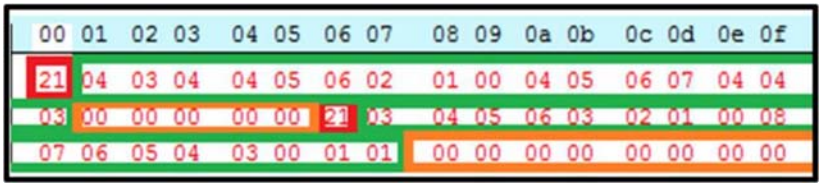

Figure 15. Example of unpacked BCD data

7.1.2.4 Encrypted Data

As opposed to the use of encryption on an entire hard drive, the analysis of an encrypted skimmer is assisted by the fact that there is a predefined structure of the plain text of the extracted information (ISO/IEC 7812 and 7813) unless the format was changed prior to encryption. However, the decoding of the information is still limited to the complexity of the encryption used. For instance, data that is encrypted with a 2-byte XOR cipher is manageable, while data encrypted with AES represents a much harder problem.

In the situation where the stored data is obscured with an XOR cipher (or equivalent level of encryption), using the known structures (ISO/IEC 7812 and 7813), an examiner can construct a cryptanalysis system based on mathematical equations, i.e., algebraic cryptanalysis. An example of such is the creation of Boolean polynomials that describe aspects of unencrypted, true account numbers. For a polynomial to be true, it must equal zero. As such, if one were to write a polynomial for an account number structure, such as every Track 2 character has an odd parity bit as its fifth bit, the equation would look like the following: $p_i + p_{i1} + p_{i2} + p_{i3} + p_{i4} + 1 = 0$ where i is the first bit of the character is always true. Another polynomial specific to XOR is in regard to the basic XOR equation itself, $p_i \oplus k_j = c_j$ where p_i = plain text, k_j = the key, and c_j = the cipher text. As every Boolean polynomial defined must equal zero, both sides of the equation are XOR'd by c_j resulting in $p_i + k_j + c_j = 0$. Additional equations could include the following: key restriction to printable ASCII; decimal and other value-restricted fields (e.g., a month field cannot contain a 13); and the Luhn algorithm. When combined, values that are true across all of these equations will be the unencrypted, plain text account numbers. Again, this process is not a viable solution for higher levels of encryption such as AES.

7.1.2.4.1 Microcontrollers

Microcontrollers can also be examined as they frequently contain information required to decrypt or decode the data stored in flash memory. Analyzing code from microcontrollers can reveal passwords and encryption keys as well as providing insight to the encryption or encoding scheme, or perhaps both. While using a program, such as Strings, against the data might prove helpful, de-compilation tools and reverse engineering skills may be required to obtain pertinent information. Side channel attacks can prove beneficial to deal with code protection used in microcontrollers, where data is stored at a high level of encryption. Research is ongoing for this method. The microcontroller can contain both captured account information as well as microcode.

8. Reference Sites and Publications

The resources listed below are referenced in this document and/or provide information that may prove helpful to the examiner:

[1] *Identification cards -- Identification of issuers -- Part 1: Numbering system*, ISO/IEC 7812-1:2015.

[2] *Identification cards -- Identification of issuers -- Part 2: Application and registration procedures*, ISO/IEC 7812-2:2015.

[3] *Information technology -- Identification cards -- Financial transaction cards*, ISO/IEC 7813:2006.

[4] *ANSI X4.16 American National Standard for financial services, financial transaction cards, magnetic stripe encoding*, 1983.

[5] *Standard Practice for Computer Forensics*, ASTM Standard E2763 - 10.

[6] *Standard Terminology for Digital and Multimedia Evidence Examination*, ASTM Standard E2916 - 13.

[7] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Computer Forensics". [Online]. HYPERLINK "https://www.swgde.org/documents/Current%20Documents" https://www.swgde.org/documents/Current%20Documents

[8] Scientific Working Group on Digital Evidence, "SWGDE Recommendations for Validation Testing". [Online]. HYPERLINK "https://www.swgde.org/documents/Current%20Documents" https://www.swgde.org/documents/Current%20Documents

[9] Brian Krebs. Krebs on Security - All About Skimmers. [Online]. HYPERLINK "http://krebsonsecurity.com/all-about-skimmers/" http://krebsonsecurity.com/all-about-skimmers/

SWGDE Best Practices for Examining Magnetic Card Readers

History

Revision	Issue Date	Section	History
Draft	01/16/2014	All	Initial draft for public comment.
1.0	02/06/2014	All	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0	06/11/2014	All	Formatted for release as an Approved document.
1.0	--	--	Updated document per current SWGDE Policy with: new disclaimer, removed Definitions section, and corrected SWGDE hyperlinks. No changes to content and no version/publication date change. (9/27/2014)
2.0	06/03/2015	All	Updated per changes made during ASTM process. Minor changes/additions to content in Sections 1 through 5. Significant content changes/additions made to Section 6, regarding extraction and identification for each device type; Section 6.3 and sub-paragraphs were removed. Significant content additions to Section 7, providing detailed information on data analysis. Section 8 updated. Voted to release as a Draft for Public Comment.
2.0	06/20/2015	All	Formatted and technical edit performed for release as a Draft for Public Comment.
2.0	09/17/2015	7.1.1	Minor grammatical change. Voted by SWGDE for release as an Approved document.
2.0	09/29/2015	All	Formatting and technical edit performed for release as an Approved document.