Designation: E3017 – 15

Standard Practice for Examining Magnetic Card Readers[1]

This standard is issued under the fixed designation E3017; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

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

1.2 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *ASTM Standards:*[2]

E2763 Practice for Computer Forensics

E2916 Terminology for Digital and Multimedia Evidence Examination

2.2 *ISO Standards:*[3]

ISO/IEC 7812 Identification Cards—Identification of Issuers

ISO/IEC 7813 Information Technology—Identification Cards—Financial Transaction Cards

2.3 *SWGDE Standards:*[4]

SWGDE Best Practices for Computer Forensics

SWGDE Recommendations for Validation Testing

3. Terminology

3.1 *Definitions of Terms Specific to This Standard:*

3.1.1 *parasitic skimmer, n*—a type of device manufactured for the capture of account data from magnetically encoded cards that operates in-line with the original ATM, gas pump, or other card reading device.

3.1.2 *start sentinel, n*—a 5-bit binary sequence, or equivalent ASCII character, used to signify the beginning of track data. (See ISO/IEC 7813).

3.1.3 *skimmer, n*—a magnetic card reader, specifically when used for an illegal purpose.

3.1.4 *skimming, n*—using a skimmer to acquire PII in an unauthorized manner.

3.1.5 *swipe, v*—to manually pass a magnetically encoded card through a card reader device to transfer information from the card.

3.2 *Acronyms:*

3.2.1 *ADPCM, n*—adaptive pulse code modulation

3.2.2 *AES, n*—advanced encryption standard

3.2.3 *ASCII, n*—American standard code for information interchange

3.2.4 *BFSK, n*—binary frequency-shift keying

3.2.5 *CVV, n*—card verification value

3.2.6 *CVV2, n*—card verification value 2

3.2.7 *EEPROM, n*—electrically erasable programmable read only memory

3.2.8 *IIN, n*—issuer identification number

3.2.9 *PAN, n*—primary account number

3.2.10 *PCM, n*—pulse code modulation

3.2.11 *PII, n*—personally identifiable information

3.2.12 *PIN, n*—personal identification number

3.2.13 *USB, n*—universal serial bus

3.2.14 *XOR, n*—exclusive or

3.2.15 *ZIF, adj*—zero insertion force

3.2.16 *BIN, n*—bank identification number

4. Significance and Use

4.1 As a skimming device is not typically deemed contraband in of itself, it is the responsibility of the examiner to determine if the device contains unauthorized account information. The purpose of this practice is to describe best practices for seizing, acquiring, and analyzing the data contained within magnetic card readers.

4.2 *Limitations*—Skimmers present unique examination challenges due to:

[1] This practice is under the jurisdiction of ASTM Committee E30 on Forensic Sciences and is the direct responsibility of Subcommittee E30.12 on Digital and Multimedia Evidence.

Current edition approved May 1, 2015. Published June 2015. DOI: 10.1520/E3017-15.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

[4] Available from the Scientific Working Group on Digital Evidence (SWDGE), https://www.swgde.org.

FIG. 1 Example of a Hand-Held Skimmer

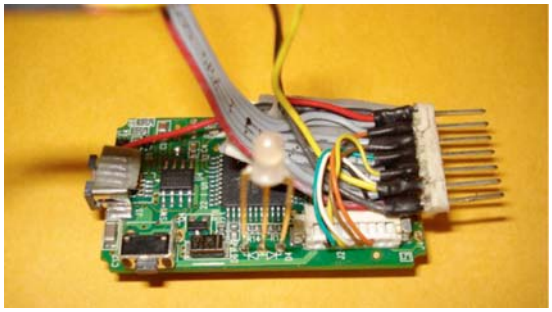

FIG. 2 Example of an Altered Hand-Held Skimmer

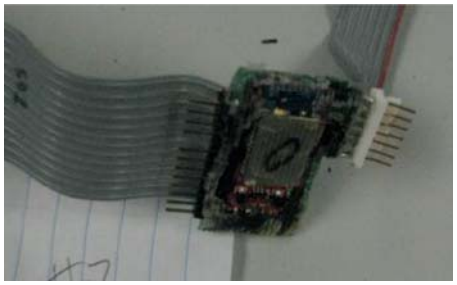

FIG. 3 Example of an Altered Hand-Held Skimmer with Bluetooth[5]

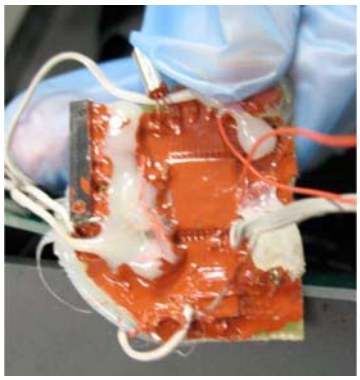

FIG. 4 Example of a Custom Skimmer

4.2.1 Rapid changes in technology,
4.2.2 Difficulty of device disassembly,
4.2.3 Lack of standards in use of the technology,
4.2.4 Use of alternate/repurposed components,
4.2.5 Use of encryption,
4.2.6 Multiple data encoding/modulation formats,
4.2.7 Prevention of chip identification by obfuscation of the device,
4.2.8 Availability of training and documentation,
4.2.9 Lack of chip information/documentation,
4.2.10 Lack of adapters available for chip reading,
4.2.11 Lack of software's ability to support reading chip data, and
4.2.12 Lack of commercial software available to analyze encrypted data extracted from skimmers.

5. Technical Background

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

5.2 In general, skimmers may be broken down into the following three categories:
5.2.1 Hand-held,
5.2.2 Altered hand-held, and
5.2.3 Custom.

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

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

5.5 *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 seen as an alteration of commercial skimmers (Figs. 2 and 3[5]).

5.6 *Custom:*
5.6.1 By far, the most complicated and difficult-to-examine skimmers are custom-manufactured devices (Fig. 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.
5.6.2 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 (Fig. 5).
5.6.3 Some skimming devices may have the capability to output captured data by means of wireless communication methods (Fig. 6). These devices may 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 receivers difficult.

5.7 *Card Data/Structure:*

[5] A trademark of Bluetooth SIG, Inc., Kirkland, WA.

FIG. 5 Example of a Custom Skimmer (Door)

FIG. 6 Example of a Cellular Enabled Skimmer

FIG. 7 Example of CVV2

5.7.1 *Fundamentals of Track Data:*

5.7.1.1 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."

5.7.1.2 The primary account numbers are generally 15 or 16 digits in length but may be as short as 12 (Maestro) or as long as 19 (China UnionPay). The credit card companies have reserved prefixes, for example, American Express credit 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).

5.7.1.3 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.

(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 will contain the account holder's name. Typically, Track 1 is only read by hand-held and altered hand-held skimmers.

(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 (for example, ATMs). Typically, custom skimmers will capture only Track 2 information. Track 2 is encoded using 5-bit ASCII (4-bit odd parity). The account information follows a start sentinel of 11010.

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

5.7.2 *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) (Fig. 7). It was designed to help curb fraud in "card not present" transactions, such as Internet purchases.

5.7.3 *Debit Cards*—When skimmed, debit cards and credit cards contain 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.

6. Evidence Collection

6.1 *Seizing Evidence:*

6.1.1 Devices should be collected and protected in the same manner as flash memory devices (refer to Practice E2763). Associated cables, documentation, and software should also be collected.

6.1.2 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 (Figs. 8 and 9). Removal of these devices may be destructive in nature and should be done cautiously.

6.2 *Handling Evidence*—Evidence should be handled according to laboratory policy while maintaining a chain of custody and by using best practices (refer to Practice E2763).

6.3 *Equipment*—Equipment in this section refers to the non-evidentiary hardware and software the examiner uses to

FIG. 8 Example of Keypad Overlay

FIG. 9 Example of an In-Line Skimmer

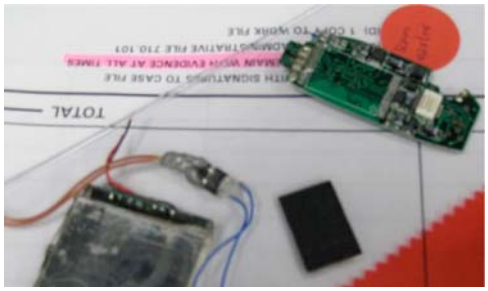

FIG. 10 Example of an Analog-Based Skimming Device

conduct data extraction and analysis of the evidence. Equipment and software applications should be verified[6] to ensure proper performance.

7. Data Extraction

7.1 *Hand-Held/Altered Hand-Held Skimming Devices*—As 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 software only provides for logical extraction (that is, no deleted information) into a text format. The examiner will need the device, appropriate software, and the appropriate data cable to conduct a successful data extraction. Of particular note, the cable used performs the extraction by means of 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.

7.2 *Custom Skimming Devices*—All skimming devices must first read the magnetic signal stored on a card. This process is accomplished by means of an electromagnetic head, similar to that found in an audio cassette tape player. As the card is manually swiped through the device, the head converts the magnetic signals 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.

7.2.1 *Analog Skimming Devices*—"Analog" skimming devices pass the 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 will be significantly larger than a decoded bit string of account data.

7.2.1.1 *Identification*—Recognizing an analog skimmer is important as the method of extraction is different than that of a custom, digital skimmer. While the examiner may notice the lack of an analog to digital encoder chip (although a digital skimmer may lack this chip as well with the processing being completed by the microcontroller), the identification of an analogue 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 (Fig. 10). While a typical custom skimmer may use a flash chip with two megabytes of storage, an analogue skimmer will typically contain a flash storage chip in the two gigabyte range.

7.2.1.2 *Extraction*—As analog skimmers likely originated as other devices, that is, MP3 sunglasses, an examiner may extract the information from the device over USB mass storage device mode. As it is common for a person constructing the skimmer to remove the USB header, the examiner must recognize the architecture and solder a new header on the device to facilitate communication. Once the header is attached, a write blocker shall be used between the device and an examiner's computer, and an image (Terminology E2916) of the device can be extracted using traditional computer forensics imaging software.

7.2.2 *Digital Skimmer Devices*—Digital skimmer devices accept input via a magnetic stripe reader just 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 may or may not be encoded or 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.

7.2.2.1 *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 may also need to be removed and read to understand the encoding or encryption methods used by the device. Code protection may prevent the extraction of code from the device's microcontroller.

7.2.2.2 *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

[6] The validation process is discussed in SWGDE Recommendations for Validation Testing.

stored data successfully. The main components of chip identification are their manufacturer and chip number. The primary chips the examiner should be able to successfully identify are the microcontroller and the flash storage chips. It is important to document/photograph them before removal as extreme temperatures may remove the markings on the chip. In cases where the chip identification number is worn or difficult to read, a microscope may be required. Additionally, applying a non-reactive and easily removed solution such as isopropyl alcohol can make chip numbers easier to read.

7.2.2.3 *Chip Removal*—Once the chips of forensic significance are identified, they should be properly removed from the circuit board in a manner that ensures the chips are not damaged. Chip removal should only be performed by properly trained and experienced personnel. The two most prominently used methods of extraction 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 to the chip induced by prying and bending the pins.

7.2.2.4 *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 (that is, 8-pin flash chips) connectivity between the chip and the socket adapter may be established through a series of wires soldered to the chip pins and inserted into the reader, typically by means of a ZIF (zero insertion force) socket. Once properly connected, the chip can then be read using the vendor-provided software, which should be saved and handled as original evidence.

7.2.2.5 As was mentioned in 5.6.3, some skimming devices use a wireless technology to broadcast the stolen card information, that is, Bluetooth,[5] ZigBee,[7] etc. It may be possible, and preferred, to extract data from these through a wireless connection (as the creator intended) if certain pairing data is known to the examiner, for example, the correct channel on which a ZigBee radio skimmer is broadcasting, the pairing code for a Bluetooth enabled skimmer.

8. Data Analysis

8.1 *Data Format Types*—Relative to skimmer data analysis, there are two kinds of recordings, analog and digital; there are several sub-types within digital. The ISO/IEC 7812 and ISO/IEC 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 both contend with account numbers sequenced both forward and backward while ensuring duplicate account numbers are not reported in a way that over-inflates the number of accounts recovered from the device. The goal of the examiner is to analyze the data by preparing the information into an easily human readable format.

8.1.1 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) will be in the form of an audio file such as WAV. An examiner will begin his/her analysis by carving from the physical image all file segments with audio file headers. This can be done using traditional data carving tools. Once the audio file(s) are carved, in order for automated processes to be run against the file(s), 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 is as simple as opening the file in the software and exporting it into the new format (16-PCM, ADPCM, etc.). With the data in the new format, a clock-recovery algorithm with noise threshold activation is scripted to drive an adaptive BFSK algorithm to generate the bit stream (top of Fig. 11). From the track's bit stream, scripting is further used to decode the Aiken bi-phase encoding to the actual account numbers.

8.1.1.1 While scripting utilities will assist the examiner in converting the 1's and 0's into possible account numbers, the standard practice is to validate the results of the script by

[7] A trademark of ZigBee Alliance, San Ramon, CA.

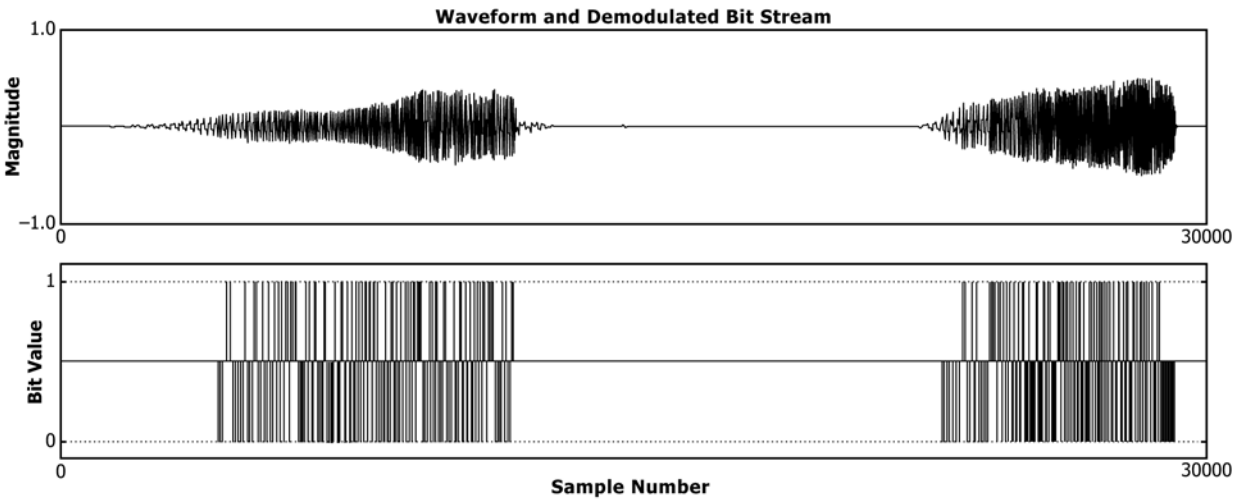

FIG. 11 Example of a 5-Bit Graph

completing at least one transcription by hand. Using a fictitious example of a credit card that begins with a BIN number of "4271" (for example), and taking into account the possibility that swipes can be recorded forward or reverse, the examiner would examine the bottom part of the graph in Fig. 11 (representing the bits decoded from the waveform) and attempt to locate a start sentinel (11010, mentioned in 5.7.1.3 (*2*)). Once the start sentinel 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 of his or her final automated process were accurate. Continuing to use "4271" as an example, the examiner would expect to find the string (again, using our example which is just a partial of a possible true account number): 11010001000100011100010000.

8.1.1.2 As the data was originally recorded in an analog manner, the files being analyzed may 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 (Fig. 12). The analyzer gives a good visual representation of the number of potential account numbers recorded by the skimmer. An examiner must compare the number of account numbers decoded versus what is visually seen in the spectrum analyzer. If there are more seen then decoded, then the threshold of the process to decode the information into account numbers should be reconfigured.

8.1.2 *Digital Data*—Data may 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 will implement cryptographically sound algorithms such as AES. The use of statistical analysis on the file extracted from the skimmer is an important first step in determining if information read from a FLASH chip 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 (Figs. 13 and 14).

8.1.2.1 *8-bit ASCII*—As most hex viewers have a default view of Base 16 Hex on the left and 8-bit ASCII on the right, 8-bit ASCII is the most simple of the common encoding formats for an examiner to analyze. In this situation, the examiner copies the readily identifiable possible account numbers from the hex viewer or simply runs a common program such as Strings against the extracted file(s).

8.1.2.2 *5-bit ASCII*—This type of encoding is best recognized by using a hex viewer that allows the examiner to interact with the data as binary text. Once viewed as binary, the examiner will search the data for the 5-bit account number start sentinel (11010, or 01011 if a reverse swipe). If a start sentinel is found, the examiner will 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 will vary according to the potential account number, for example, 80 characters (16 account numbers multiplied by 5 binary characters) for a VISA or MasterCard account number. If the examiner is able to recover a valid (in accordance with Luhn) account number, then he or she may then automate the decoding of the rest of the 5-bit data using an automated process such as scripting.

8.1.2.3 *Little Endian Binary Encoded Decimal*—This encoding scheme is able to be discerned by an examiner using traditional Base 16 hex/8-bit ASCII hex viewer software. In the hex viewer, the account number will follow a header. Typically in Base 16, the header value is 0 × 21 and in 8-bit ASCII the value is "!". The account number will appear in the hex view as the second digit, or nibble. For example, a value of 0 × 04 immediately following the 0 × 21 header equals the first number of the account, 4. Once the account number is complete, there will be padding values of 0 × 00 until the next header occurrence. Again, once recognized, the examiner carves the information from the file(s) and checks his or her interpretation of the decoding by using the Luhn algorithm against at least one extracted account number.

8.1.2.4 *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 ISO/IEC 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 two byte XOR cipher is manageable, while data encrypted with AES represents a much harder problem.

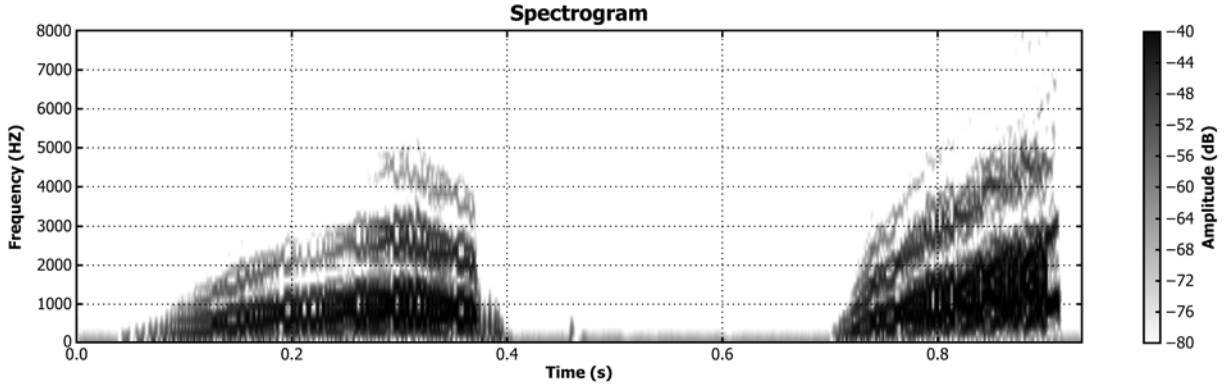

FIG. 12 Example of Swipes Shown in a Spectrum Analyzer

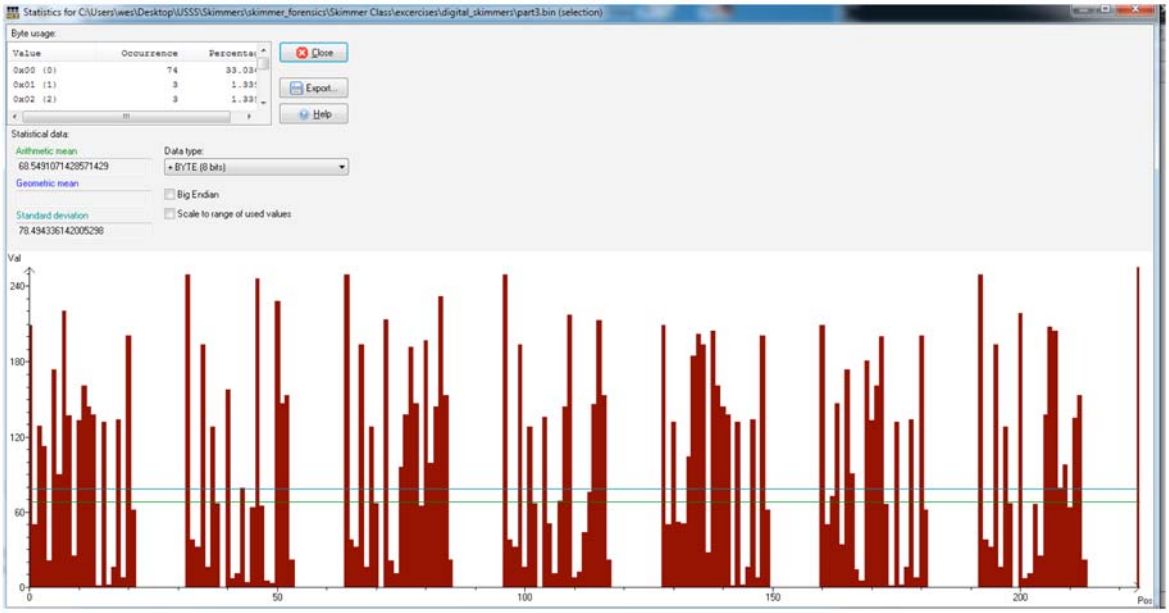

FIG. 13 Example of Unencrypted Data

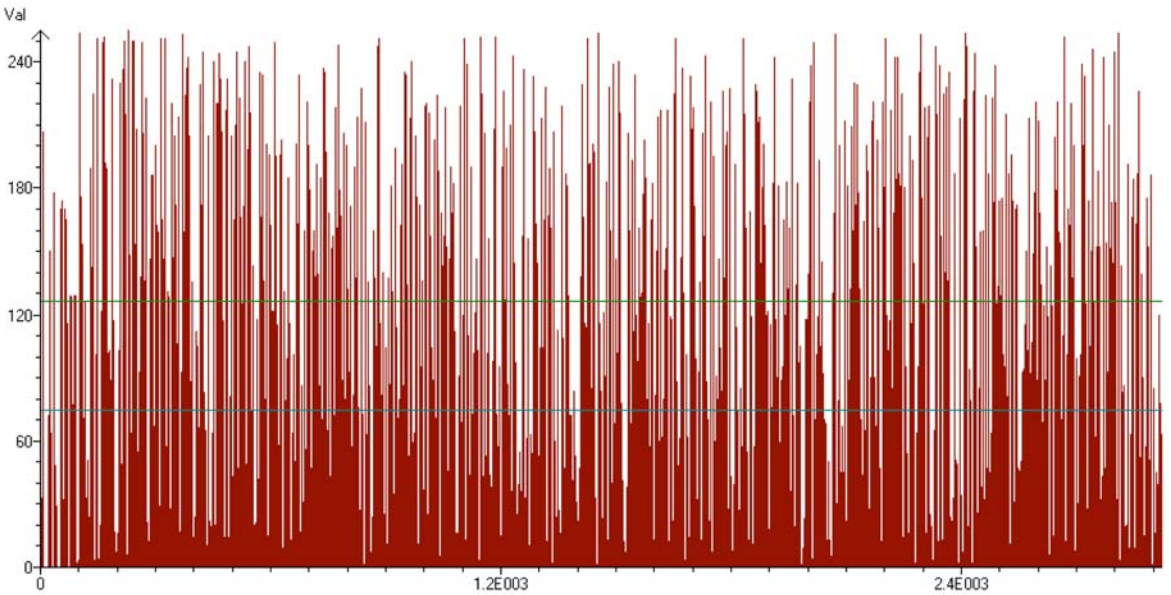

FIG. 14 Example of Encrypted Data

8.1.2.5 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 ISO/IEC 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 deals with the basic 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 (for example, a month field cannot contain a 13); and the Luhn algorithm. When combined, values that are true for 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.

8.1.3 *Microcontrollers*—Microcontrollers may also need to be examined as they frequently contain information required to decrypt or decode the data stored in flash memory. Analyzing code from microcontrollers may reveal passwords and encryption keys as well as providing insight to the encryption or

encoding scheme or both. While using a program such as Strings against the data may prove helpful, de-compilation tools and reverse engineering skills may be required to obtain pertinent information. Also, the use of side channel attacks may prove beneficial to deal with the code protection possibly used in microcontrollers where data is stored at a high level of encryption. Research is on-going in this method. Additionally, in addition to the device's logic, microcontrollers may serve as the data storage area used for captured account information (as opposed to using a separate FLASH storage chip).

9. Keywords

9.1 magnetic card reader; personally identifiable information; skimmer