Designation: E3017 – 19

An American National Standard

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 cannot replace knowledge, skills, or abilities acquired through education, training, and experience and is to be used in conjunction with professional judgment by individuals with such discipline-specific knowledge, skills, and abilities.*

1.3 *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, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.4 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *ASTM Standards:*[2]

E2763 Practice for Computer Forensics (Withdrawn 2019)[3]

E2916 Terminology for Digital and Multimedia Evidence Examination

2.2 *ISO Standards:*[4]

ISO/IEC 7811 Identification Cards—Recording Technique

ISO/IEC 7812-1:2017 Identification Cards—Identification of Issuers—Part 1: Numbering SSystem

ISO/IEC 7813:2006 Information Technology—Identification Cards—Financial Transaction Cards

2.3 *SWGDE Standards:*[5]

SWGDE Best Practices for Chip-Off

SWGDE Best Practices for Computer Forensics

SWGDE Recommendations for Validation Testing

SWGDE Tech Notes Regarding Chip-Off via Material Removal Using a Lap and Polish Process

2.4 *ANSI Standards:*[6]

ANSI X4.16 Financial Services—Financial Transaction Cards—Magnetic Stripe Encoding

3. Terminology

3.1 *Definitions:*

3.1.1 For definitions of terms used in this practice, refer to Terminology E2916.

3.2 *Definitions of Terms Specific to This Standard:*

3.2.1 *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.

3.2.2 *start sentinel, n*—a 5-bit binary sequence, or equivalent ASCII character, used to signify the beginning of track data. (See ISO/IEC 7813:2006.)

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

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

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

3.3 *Acronyms:*

3.3.1 *ADPCM, n*—adaptive pulse code modulation

3.3.2 *AES, n*—advanced encryption standard

[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 June 1, 2019. Published June 2019. Originally approved in 2015. Last previous edition approved as E3017 – 15. DOI: 10.1520/E3017-19.

[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] The last approved version of this historical standard is referenced on www.astm.org.

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

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

[6] Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036, http://www.ansi.org.

FIG. 1 Example of a Hand-Held Skimmer

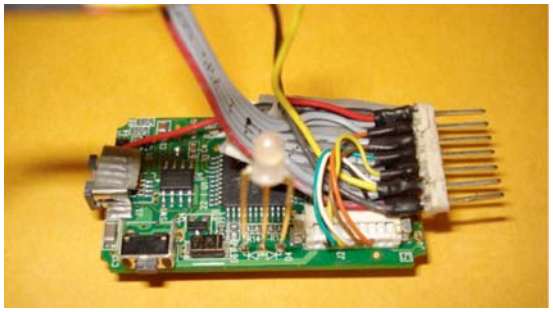

FIG. 2 Example of an Altered Hand-Held Skimmer

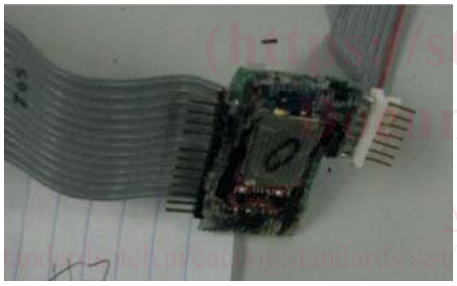

FIG. 3 Example of an Altered Hand-Held Skimmer with Bluetooth[7]

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

3.3.4 *BIN, n*—bank identification number

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

3.3.6 *CVV, n*—card verification value

3.3.7 *CVV2, n*—card verification value 2

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

3.3.9 *IIN, n*—issuer identification number

3.3.10 *PAN, n*—primary account number

3.3.11 *PCM, n*—pulse code modulation

3.3.12 *PII, n*—personally identifiable information

3.3.13 *PIN, n*—personal identification number

3.3.14 *USB, n*—universal serial bus

3.3.15 *XOR, n*—exclusive or

3.3.16 *ZIF, adj*—zero insertion force

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:

4.2.1 Rapid changes in technology;

4.2.2 Difficulty of device disassembly;

4.2.3 Use of alternate/repurposed components;

4.2.4 Use of encryption or examination countermeasures, or both;

4.2.5 Multiple data encoding/modulation formats;

4.2.6 Prevention of chip identification by obfuscation of the device;

4.2.7 Availability of training and documentation;

4.2.8 Lack of chip information/documentation;

4.2.9 Lack of adapters available for chip reading;

4.2.10 Expense of available equipment used in chip removal and 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 *Skimmer Examples:*

5.4.1 *Hand-Held*—Manufactured primarily for legitimate uses, for example, registering attendance at a conference, handheld skimmers can also be used for illegitimate purposes, for example, a collusive waiter that will skim customers' credit cards (see Fig. 1).

5.4.2 *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 (see Fig. 2). Commercial skimmers can be altered by adding wireless functionality, for example, the addition of a Bluetooth[7] module (see Fig. 3) used to remotely download stolen track data.

5.4.3 *Custom*—Custom manufactured devices use many different circuit designs (see Fig. 4) and typically employ

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

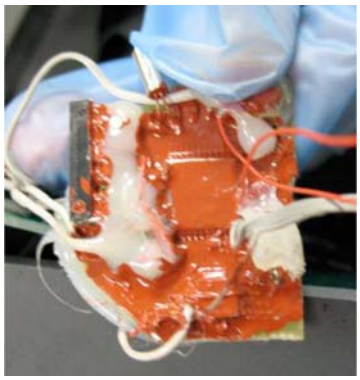

FIG. 4 Example of a Custom Skimmer

FIG. 5 Example of a Custom Skimmer (Door)

FIG. 6 Example of a Cellular Enabled Skimmer

FIG. 7 A Bluetooth Custom Skimmer

varied 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.

5.4.3.1 As it is common in some larger metropolitan areas for 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 Fig. 5).

5.4.3.2 As previously noted, skimming devices may have the capability to output captured data by means of wireless communication methods (see Fig. 6). These devices transmit their data in real-time or batch mode. Transmission protocols of these devices vary.

5.4.3.3 Similar to the altered handheld devices, custom skimmers can use Bluetooth transmission technology (see Fig. 7 and Fig. 8).

5.4.3.4 In addition to Bluetooth and Global System for Mobile Communications (GSM) modules, skimmers can be remotely accessed through other transmission technologies, to include ZigBee[8] radio (see Fig. 9).

5.4.3.5 Skimmers used on ATMs typically will capture both the data on the card and a user's PIN number. As noted above, the method to capture the user's PIN could be a completely different device, but even if that is true, the PIN information could be sent to storage on the same skimming device that is capturing the track data (see Fig. 10). That information can be saved on flash chip(s) or a secure digital (SD) card, as seen in Fig. 11.

5.4.3.6 Some ATM skimmers may be affixed to the front of an ATM, others are secreted inside the card slot (see Fig. 12). Many of these types of skimmers will read data from a chip-enabled card.

NOTE 1—Just because data is skimmed from a chip, does not mean that the subject can use that data to create future, fraudulent transactions.

5.5 *Card Data/Structure*—Understanding the manner in which credit and debit cards store their data is important. The ability to decode skimmer-stored information relates to how data is stored on the magnetic stripe of a card.

5.5.1 *Fundamentals of Track Data:*

5.5.1.1 The International Standards Organization (ISO) created ISO/IEC 7812-1:2017, 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."

5.5.1.2 The primary account numbers are generally 15 or 16 digits in length but may be as short as 12 (Maestro[9]) or as long as 19 (China UnionPay[10]). The credit card companies have reserved prefixes, for example, American Express[11] credit cards begin with 34 or 37. Credit card processors use the Luhn algorithm (see ISO/IEC 7812-1:2017) to ensure the integrity of the primary account number (PAN).

5.5.1.3 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.

[8] A trademark of ZigBee Alliance in San Ramon, CA.
[9] A trademark of MasterCard International Incorporated in Purchase, NY.
[10] A trademark of China UnionPay Co., Ltd., in Shanghai, China.
[11] A trademark of American Express Marketing and Development Corp. in New York, NY.

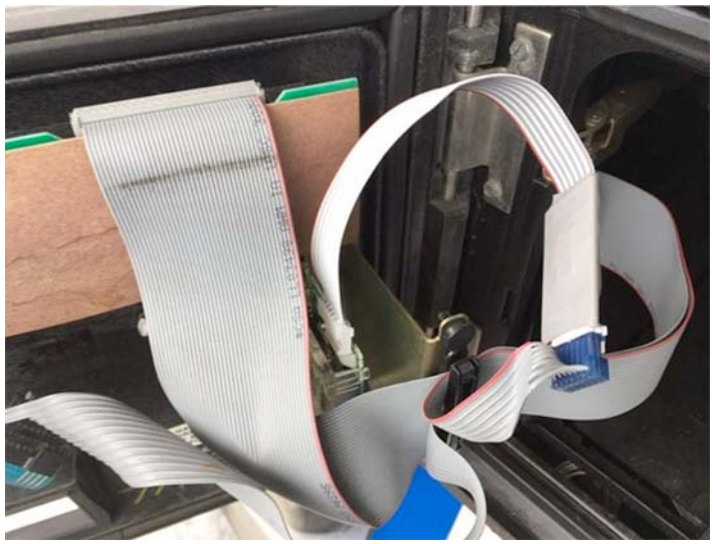

FIG. 8 A Bluetooth Custom Skimmer Secreted Inside a Gas Pump

FIG. 9 A ZigBee Radio Recovered from the Interior of a Gas Pump

FIG. 11 Rear View of a Skimmer Using Separate Boards for Capturing Track Data and PINs

FIG. 10 Front View of a Skimmer Using Separate Boards for Capturing Track Tata and PINs

5.5.1.4 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 contains the account holder's name.

(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.

(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.

5.5.2 *Card Verification Value (CVV)*—This code is recorded on the second track of a card and used to verify the card is present during a transaction.

5.5.3 *Card Verification Value 2 (CVV2)*—This code is a three- to four-digit number printed on the back of a card (see Fig. 13). It was designed to help curb fraud in "card not present" transactions, such as Internet purchases.

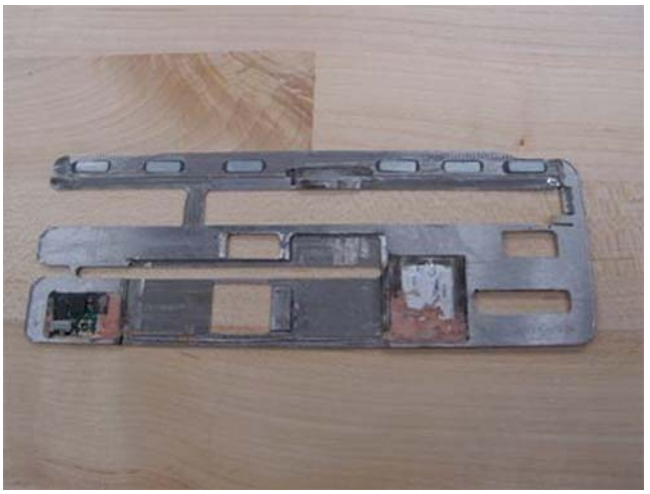

FIG. 12 A Skimmer That is Inserted Into an ATM Card Slot

FIG. 13 Example of CVV2

5.5.4 *Debit Cards:*

5.5.4.1 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 an attractive target for skimming, as compromised accounts can be converted directly into cash as opposed to goods and services.

6. Collection

6.1 *Seizure:*

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

6.1.2 *Specific Skimmer Considerations Related to Seizure:*

6.1.2.1 There is a possibility of two devices being used to make up the skimmer, one device capturing card track data and a separate device capturing PINs, for example, video and keypad overlay.

6.1.2.2 If a device is wired into something like a gas pump, it is most likely using power from the pump. Removing the device from that type of power connection will not affect the examination. If a battery is observed on a skimmer, leave the battery in place, unless there will be a significant delay before examination, that is, more than a month.

6.1.2.3 If the skimmer is using a universal integrated circuit card (UICC) or SD card, it should be removed at the time of seizure.

FIG. 14 Example of Keypad Overlay

6.1.2.4 If a device uses video or audio recording, or both, to capture information, that recording may continue after the device is seized.

6.1.2.5 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 Fig. 14 and Fig. 15). Removal of these devices can be destructive in nature and should be done cautiously.

6.2 *Handling Evidence:*

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

7. 7. Acquisition – Account Data

7.1 *Background:*

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

7.1.2 When considering retrieving stored account information, due to differences in acquisition and analysis, skimmers can be broken down into two general categories, analog or digital.

7.1.3 The processes used in examinations vary depending on the device itself and the manner in which the stored information is encoded. While many skimmers will be manufactured with the capability of remotely downloading skimmed account data by the subject, that functionality does not typically change the way skimmed account information is stored on the skimmer or acquired by the examiner. Acquiring and analyzing Bluetooth module artifacts is completed separately from processing the skimmer for stolen account data (see Section 10, Bluetooth Modules).

7.1.4 All skimming devices read 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 may be passed to other signal processing components. Devices that store that

FIG. 15 Example of an In-Line Skimmer

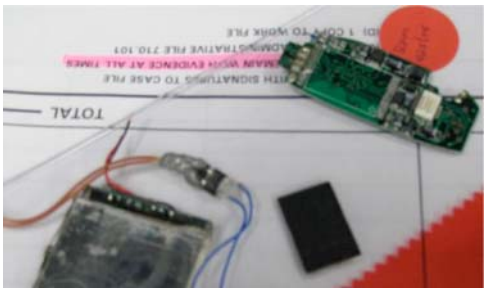

FIG. 16 Example of an Analog-Based Skimming Device

waveform without further processing are referred to as "analog" devices. "Digital" devices further process the waveform.

7.2 *Analog Skimming Devices:*

7.2.1 Analog skimming devices capture the magnetic signal on the card stripe to a digital waveform in flash memory. This signal is encoded according to the ISO/IEC 7811 suite of standards, but is otherwise similar to an audio waveform. The resulting file extracted from a device is similar to an audio file and significantly larger than a decoded bit-string of account data. Recovery of the encoded data requires further processing.

7.2.2 *Identification:*

7.2.2.1 Recognizing an analog skimmer is important, as the method of extraction differs from that of a custom, digital skimmer. Identification of an analog skimmer can be made by either recognizing the cannibalization of an MPEG-2 Audio Layer III (MP3) device or by recognizing the unusually large storage capacity of the device's flash memory chip, or both (see Fig. 16). As an example, a typical digital skimmer uses a flash chip in the area of two megabytes of storage, an analog skimmer typically contains a flash storage chip in the two gigabytes or more range.

7.2.3 *Extraction:*

7.2.3.1 Many analog skimmers originated as other devices, for example, MP3 sunglasses. Therefore, an examiner may extract data from the device using its built-in universal serial bus (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 or leads on the device to facilitate communication. Once the header is attached, the examiner creates an image using traditional computer forensics imaging techniques and software (refer to Practice E2763 and SWGDE Best Practices for Computer Forensics).

7.3 *Digital Skimming Devices:*

7.3.1 Digital skimming devices pass the analog swipe waveform to an ADC to produce a digital waveform, which is stored and coded in flash memory. Digital skimmer devices accept input by means of 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 can be stored in a variety of formats, which might or might not be ciphered or encrypted.

7.3.2 *Chip Identification:*

7.3.2.1 Custom skimming devices can be complicated in nature. Their design can be developed using new or cannibalized circuits/chips, or both. The main components of chip identification are the manufacturer and chip model numbers of both the microcontroller and flash 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.

7.3.3 *Chip Removal:*

7.3.3.1 As skimming devices typically do not have a universal and dependable method to connect to and download skimmed account information (other than USB used by analog devices), an examiner should remove 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. Unfortunately, code protection may prevent the extraction of data from a device's microcontroller.

7.3.3.2 The chips 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. Methods of extraction include hot air, infrared, and chip polishing/lapping/milling. Methods that require the entire chip being removed at once are preferred, as they reduce the chance of physical damage induced by prying and bending pins or destroying connection pads, or both (refer to SWGDE Best Practices for Chip-Off and SWGDE Tech Notes regarding Chip-Off via Material Removal Using a Lap and Polish Process).

7.3.4 *Chip Connectivity and Reading:*

7.3.4.1 There are several chip readers commercially available, with each reader possibly supporting a wide array of chips. Most of the time, the examiner will need to use a chip socket adapter that matches the chip package. However, on certain smaller chips, for example, 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 by means of a Zero Insertion Force (ZIF) socket (see Fig. 17 and Fig. 18).

7.3.4.2 Once properly connected, a chip can be read using vendor provided software. The extracted data should be saved, write protected, and hashed prior to analysis. Analysis should