



Standard Practice for Examining Magnetic Card Readers¹

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 (SWGDE), <http://www.swgde.org>.



FIG. 1 Example of a Hand-Held Skimmer



FIG. 2 Example of an Altered Hand-Held Skimmer

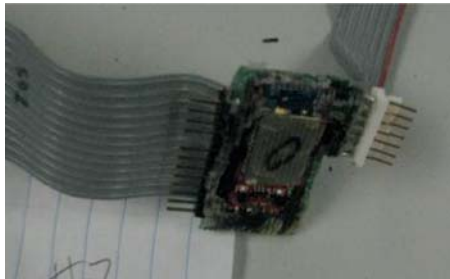


FIG. 3 Example of an Altered Hand-Held Skimmer with Bluetooth⁵

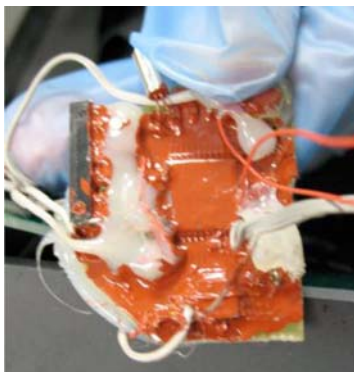


FIG. 4 Example of a Custom Skimmer

- 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 3⁵).

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