available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Forensic data recovery and examination of magnetic swipe card cloning devices

*Gerry Masters, Philip Turner**

QinetiQ, Digital Investigation Services, Trusted Information Management Department, Malvern Technology Centre, St. Andrews Road, Malvern, Worcestershire WR14 3PS, UK

Keywords:
Digital Forensics
Magnetic swipe cards
Skimmers
Digital Evidence Bags
Data recovery

ABSTRACT

Magnetic swipe card technology is used for many purposes including credit, debit, store loyalty, mobile phone top-up and security identification cards. These types of cards and the details contained on them are often relied upon as a form of identification and personal authentication. As such reliance is placed upon them it is surprising that they do not incorporate more stringent security features, and because of this lack of features it is not surprising that they attract the attention of people who wish to exploit them for illegal gain. The paper introduces the type of technology, and range of devices available for manipulating magnetic swipe card data. It proposes the use of Digital Evidence Bags as a suitable format for the evidential storage of information obtained from them, thus further illustrating the flexibility of the format and demonstrating the diverse range of devices that have to be handled within the digital investigation and law enforcement community.

1. Introduction

The use of credit and debit cards to purchase goods and services has changed the way society and financial organisations process and handle monetary and financial transactions. This cash-less mode of working means more reliance is placed on the small pieces of plastic and the few numbers that are embossed or printed on the surface and stored on the magnetic stripe. It is common for card details to be used for internet based purchases thereby anonymizing the purchase process. Furthermore, the value and security reliance that is placed on those details should not be underestimated or treated trivially. The aim of this paper is to demonstrate the ease by which magnetic swipe cards are often fraudulently cloned and demonstrate how such devices can be processed in a forensically sound manner. The extraction of information from these devices is ad hoc at best, so a solution to this problem is proposed using Digital Evidence Bags as the secure storage container.

2. Magnetic stripe card details

A magnetic stripe card (swipe card) is a type of card capable of storing digital data by recording a magnetic pattern within a stripe on the reverse of the card. Swipe cards are commonly used for applications including credit cards, department store (loyalty) cards and mobile (or cell) telephone 'top-up' cards. There are three data tracks within a magnetic stripe. A credit card typically uses only Tracks 1 and 2.

Track 1 typically stores the primary account number, cardholder's name and card expiration date. This track can also be used to contain 'discretionary' data maintained by the card issuer. Depending on the issuing authority, this discretionary

* *Corresponding author*. Tel.: +44 1684 895777; fax: +44 1684 894365.
E-mail addresses: grmasters@qinetiq.com (G. Masters), pbturner@qinetiq.com (P. Turner).
1742-2876/$ – see front matter © 2007 DFRWS. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2007.06.018

data may, but not necessarily, be used for PIN or card verification and transaction counting purposes.

Track 2, developed by the banking industry, typically stores a copy of Track 1, but without the cardholder's name, and a 'service code' entry related to card security functions, such as the type of transaction permitted (cash only, goods and services only or ATM (Automatic Teller Machine – 'hole-in-the-wall') with PIN verification).

A mobile telephone top-up card is a form of magnetic swipe card. It is normal for a mobile telephone top-up card to store in both Tracks 1 and 2 the account number that has been embossed or printed onto the card. In addition, the card issuer's name would also be stored in Track 1.

A top-up card is a convenient vehicle for cloning 'dumb' credit cards (i.e. not the new 'chip and PIN' enabled cards). It appears to be sufficient only to overwrite Track 2 with a valid account number.

2.1. *Associated standards – card standards, bank ID numbers*

A number of standards define both the physical layout and construction details of a magnetic swipe card and the data format of the tracks:

- ISO 7810 – physical characteristics of credit cards (ISO/IEC 7810, 2003).
- ISO 7811 (1–6) – embossing, track location, Lo/Hi coercivity (ISO/IEC 7811).
- ISO 7813 – financial transaction cards (ISO 7813).
- ISO 4909 – card data format – Track 3 (ISO 4909, 2000).

The ISO 7811 standard uses 210 BPI (Bits Per Inch) encoding for Track 1 in the International Air Transport Association (IATA) format of 79 alphanumeric characters at 7 bits per character.

Track 2 uses 75 BPI encoding to store 40 numeric characters at 5 bits per character in the American Banking Association (ABA) format, and Track 3 uses 210 BPI encoding of 107 numeric characters at 5 bits per character in THRIFT format.

These formats have evolved from the historical 'owners' requirements for these tracks, but even in the ISO 7811 format, the tracks can be used to store any compatible data the issuer requires, such as basic personal or biometric information.

2.2. *Financial track information*

- Track 1 – 76 alphanumeric characters
  - Start sentinel = %
  - Format code, B = bank/financial format
  - Primary Account Number (PAN), up to 19 digits
  - Name, 2–26 characters
  - Expiry date

Example
%B0123456789123456^MR A SMITH^0612…?

- Track 2 – 37 numeric characters
  - Start sentinel = ;
  - Primary Account Number (PAN), up to 19 digits
  - Expiry date – four characters
  - Service code – three characters (sss)
  - Discretionary data (DD) – PIN/card verification

Example
;0123456789123456=0612sssDD…?

Track 3
- Not usually used for financial transaction cards
- Track 3 – 104 numeric data characters
  - Start sentinel = +
  - Field code (FC)
  - Primary Account Number (PAN), up to 19 digits

Example
+FC0123456789123456=…?

3. Magnetic stripe devices

A range of different devices is commonly used to read magnetic swipe cards (Escan Technologies Corp.). These vary from standalone pocket devices to devices that are incorporated into keyboards. A range of these devices is now presented and a summary of their individual capabilities is highlighted. Some of the devices listed here are often used for more extravagant fraudulent activities; an example is presented in this paper together with some of the associated equipment that is used in these scams.

3.1. *Basic skimmers – types and capabilities*

There are many magnetic stripe card readers or skimmers, as they are commonly known, produced by a small number of manufacturers. These devices are marketed for use by legitimate commercial retail purposes. They also have become increasingly used for illegal fraudulent activities. An example of a portable magnetic stripe device is shown in Fig. 1 with a brief synopsis of its features:

- Standalone, battery powered – CR2032 button cell.
- Size – *L*50 mm × *W*30 mm × *H*38 mm.
- Reads three tracks.
- 512 K bytes memory – up to 2048 records.
- RS232/USB interface connections.
- PIN protected – four digit.
- Software deletes records/wipes information from device when saved.

Fig. 1 – MSR-500M (Mini-123) magnetic swipe card reader.

Fig. 2 – MSR206 magnetic swipe encoder.

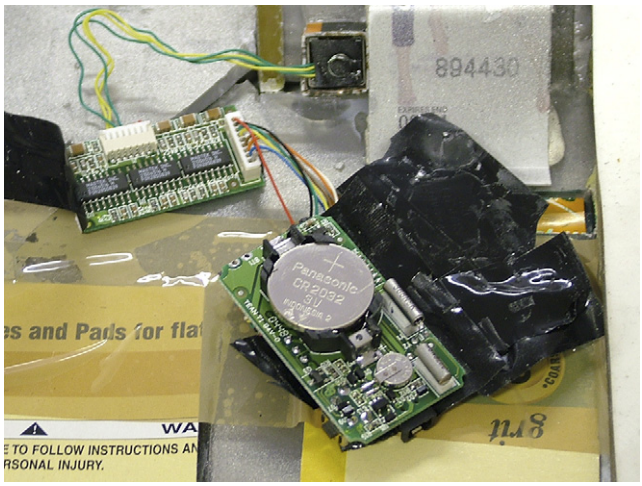


Fig. 4 – Components from a Mini-123 used in an imitation ATM facia.

3.2. *Magnetic swipe card encoders*

The magnetic swipe card readers shown above are only part of the equipment that is usually used to create clone cards, as they only have the ability to read a cards details. In order to create the clone an encoder (Fig. 2) is also used to be able to write to a blank card. Again, many variants are available, the following is a summary of the MSR206 features:

- Ability to read and write magnetic track data.
- Track reading/writing options 1, 2&3, 1&2, 2.
- Hi/Lo coercivity.
- Serial/USB/PS/2 connection types.
- Can be used to clone magnetic stripe cards.

4. Repackaged skimmers – ATM fronts, and slot adaptors and associated equipment

The skimmers shown above, although they can be used for legitimate purposes are commonly used for fraudulent activities. Typically they are removed from their standard packages and incorporated into false ATM fascias and ATM slot adaptors. An unsuspecting person would then use one of these machines and unknowingly have their card details stolen. The quality of the fake fascias (Fig. 3), particularly on the user interface side, is exceedingly accurate in appearance. It is only the reverse side that shows the haphazard build quality.

Fig. 4 shows the extracted components of a Mini-123 card reader removed from its manufactured packaging and re-packaged for use in a fake ATM fascia.

Fig. 5 shows further examples of a Mini-123 magnetic swipe card reader. On this occasion they are re-packaged in a slot adaptor.

4.1. *Associated equipment – cameras*

It is quite common for other equipment to be used in association with the skimmers; these are used to obtain PIN number

Fig. 3 – Imitation ATM facia – front and rear view.

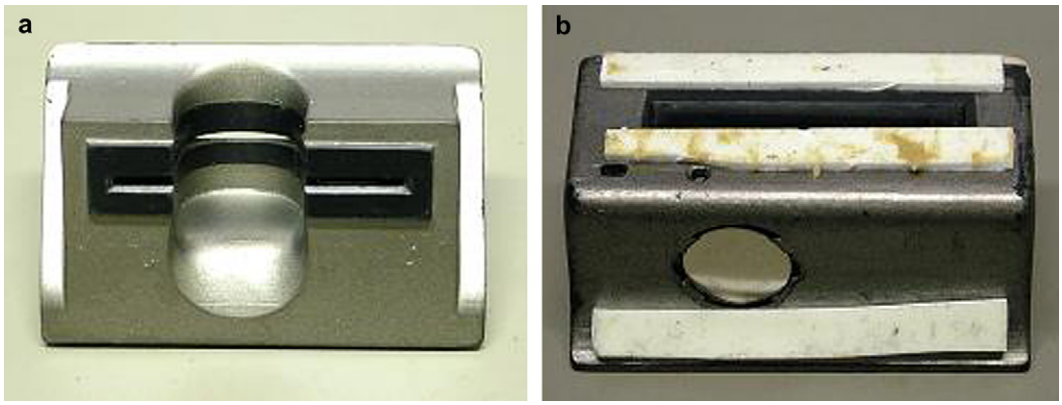


Fig. 5 – Repackaged Mini-123 card reader as an ATM slot adaptor: (a) slot adaptor – front view and (b) slot adaptor – rear view.

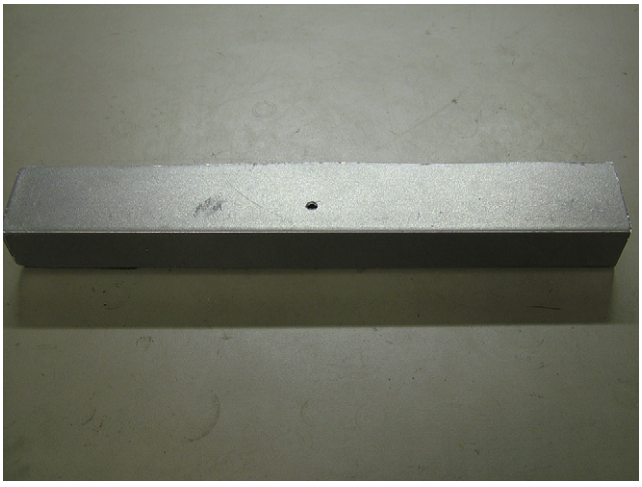


Fig. 6 – Front face of plastic strip containing a small pinhole for the camera lens.

Fig. 7 – Rear view of plastic strip showing the components of a small digital camera.

details. Typically a camera would be used and positioned above the keypad area on the ATM machine to record the PIN number. A number of types of this device are commonly used.

Figs. 6 and 7 show a plastic strip that contains a small compact digital camera. This is typically installed with a suitable memory card and setup in a 'movie' mode of operation. The strip would be affixed to the ATM machine and left operating for an hour or so. During that time the camera would record all users of the machine entering their PIN. This information can then be easily correlated with that obtained from the skimmers by synchronising the clocks.

Other variants are commonly used that utilise small wireless cameras. Again this would be affixed in a small plastic strip and the perpetrator would then record the transmitted picture from a short distance away.

Fig. 7 shows the dismantled components of a Sony DSC-50 camera (main circuit board, control panel and batteries) affixed to the plastic strip minus the viewfinder.

5. Forensic data recovery/extraction

The applications that are packaged with these types of devices are, as with most digital systems, provided with user functionality and the requirements tailored toward that of the particular device. There is no thought given in the packaged applications to any form of evidential data collection; why should it be? Because of the limited processing capability that these devices possess, they also have a fairly simple interface to connect them to a computer for data extraction. The majority of devices use a USB or serial interface connection and a basic handshake protocol exchange to request data from the device. The data stored in these devices are limited to basic device identification, firmware revision and timestamp information. The magnetic stripe information is ASCII based and contains all the encoded track information.

5.1. *Communication protocol*

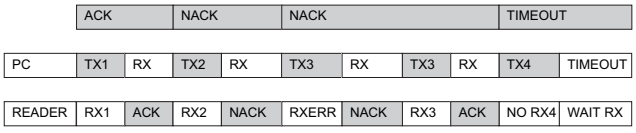
As an example, the Mini-123 illustrated earlier uses a simple serial communication protocol (GNET Library) when

connected to a computer. GNET is a simple networking library. It is written in 'C' and built using GLIB as a basis. It is intended to be easy to use and portable. Documentation and examples are provided and it is licensed under the GNU Library General Public License.

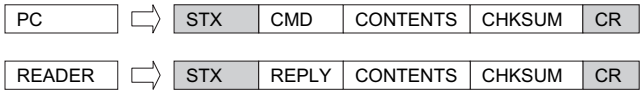
GNET features

- Supports TTY operation (use teletype to send commands).
- Simple handshaking – one enquiry/one answer.
- Multi-link capability.
- Expandability – GNET provides four major functions:
  - Polling.
  - Login/logout.
  - Database.
  - Information.
- Simple format – uses ASCII value for each field, separator between fields.

5.1.1. *GNET handshaking*



5.1.2. *GNET packet*



Item	Dec	Hex	Control key	Function
STX	2	02	^B	Start of text
CMD	ASCII	ASCII	ASCII	Command code
CONTENTS	ASCII	ASCII	ASCII	Contents data
CHKSUM	ASCII	ASCII	ASCII	Check sum
CR	13	0D	^M	Carriage return
REPLY	78(65)	4E(41)	(N)A	(Negative) Ack

5.1.3. *GNET command table – typical command set supported by the Mini-123*

Topic	Command	Contents	Description
Setting	F	–	Get product version
	S	Date, time, week	Set data, time, week
	T	–	Get date and time
	C	Number + param + chksum	Set register by number
	B	Number	Get register by number
Database	N	–	Get number of record
	G	Number	Read record by number
	E	–	Erase all records!!

5.2. *Skimmer extracted data*

The following shows a sample of the data that would be extracted from a Mini-123 reader. The card details being contained in records containing concatenated track information:

Unit login ID: 0000
Actual date and time: 13/10/06 and 12:12:30
Unit date and time: 200703142328394
Product version: 1.0R16
Number of records: 0001
000,;8944129990123456789=99121010000000000?2006/11/09 09:35:39 53F

This track information requires interpretation in order to extract more human readable information. The decoded track information from the Mini-123 is shown below:

Record: 000
Timestamp 09:35:39, 09/11/2006
No Track 1 data
No Track 3 data
Track 2
Account code: 8944129990123456789
Valid from: 12/99

Some of the packaged applications are almost anti-forensic in nature as they actually delete the information contained in the skimmer once downloaded to the PC. Furthermore, they may even require a basic password in order to access the stored data. Fig. 8 shows such a packaged application supplied with the Mini-123 reader in action, with several uploaded card records visible.

To overcome some of these problems, bespoke applications are required by the forensic investigator to connect to the device and extract the information in a forensically sound manner. A suggested container for encapsulating the extracted information is the Digital Evidence Bag (DEB). The DEB concept has been described in previous papers (Turner, 2005, 2006, 2007). The DEB was chosen to further illustrate how the DEB framework can be used with disparate digital devices.

Digital Evidence Bags are ideally suited as they are capable of storing typical device metadata such as make, model, serial number, access password and device timestamp.

Fig. 9 shows how the data contained within a Mini-123 magnetic stripe card reader can be stored in a DEB. It can be seen that integrity check information can be readily associated with the record information extracted from the device.

The DEB tag file is a plain text file containing the following information:

- DEB reference identifier/exhibit number;
- details of the evidence contained in the DEB (e.g. Mini-123 magnetic card reader data);
- the name and organisation of the person capturing the information;
- the date and time the capture process started;
- a list of Evidence Units (EUs) contained in the DEB. An EU is the name given to an .indexnn file and its corresponding .bagnn file. Fig. 9 illustrates one EU;

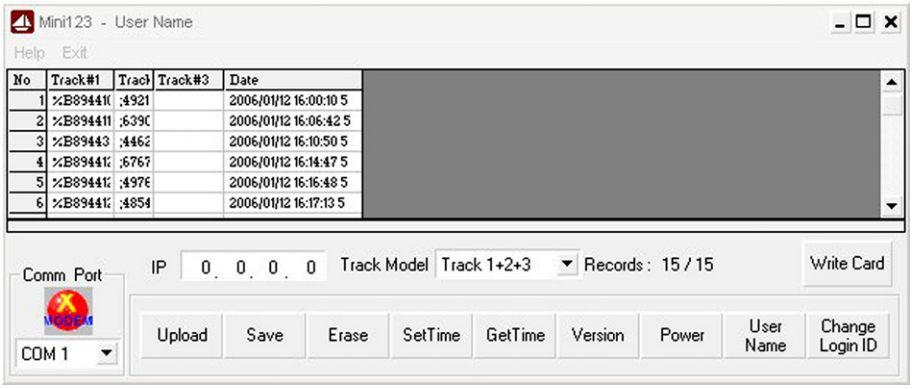


Fig. 8 – Mini-123 packaged application.

- a hash of each .indexnn file and .bagnn file contained in the DEB;
- tag seal number expressed as the hash of the tag file to date, this is equivalent to the traditional seal number;
- the format definition of information stored in the .index file.

The Evidence Unit composed of two files: an index file and a bag file. The index file is a text-based tab-delimited file detailing the contents of the corresponding bagnn file. The index file in this scenario uses a basic index reference structure (Record Number {Rnum} and Record Length {Rlen}) and associated integrity check information (MD5 hash {hmd5}) associated with the actual magnetic swipe card data extracted from the Mini-123 device that is contained in the bag file.

6. Conclusion

The paper has highlighted some of the common equipment associated with magnetic stripe card fraud and associated equipment used for fraudulent activity. It has also shown that many of the applications used to extract information from these devices do not permit the information to be extracted in a forensically sound manner and has demonstrated the Digital Evidence Bag as a suitable format to store and associate integrity assurance information with that obtained from such devices.

It should also be noted that other technologies are being introduced to accompany magnetic strip card technology (Chip and PIN), to help defeat the identified skimming techniques described in this paper. This includes the addition of a 'smart'

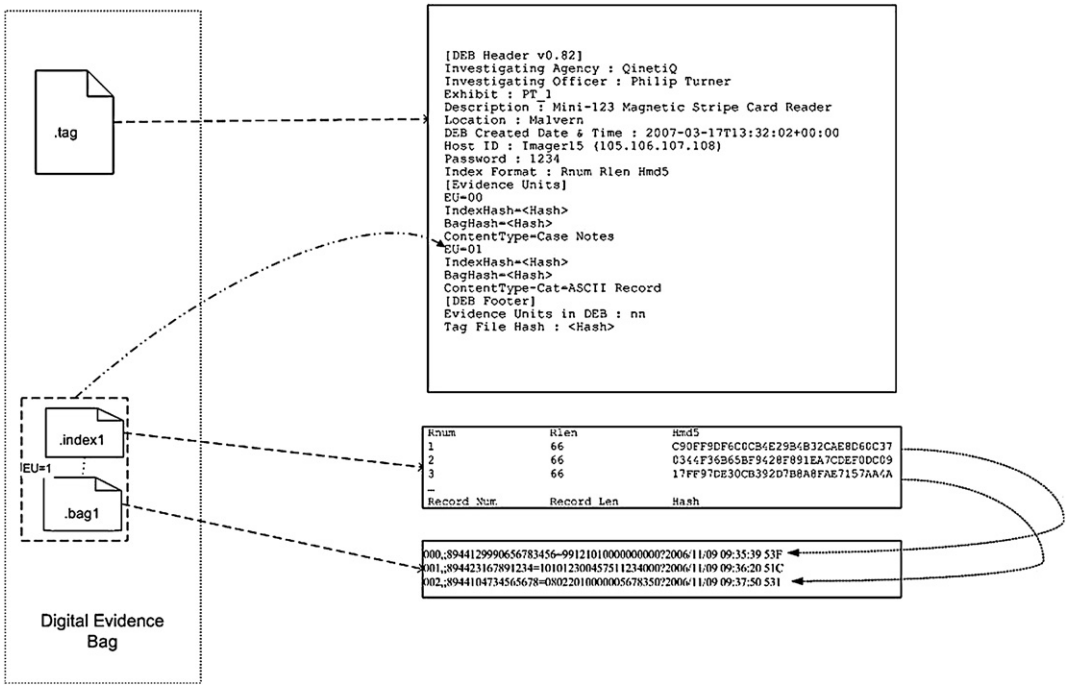


Fig. 9 – Digital Evidence Bag schematic.

chip incorporated on the card. This provides a more secure method of storing data than magnetic stripes. Contact smart cards contain an array of gold metallic contacts connected to a silicon chip embedded inside the card. The chip usually includes a control microprocessor an encryption/decryption engine, a Read Only Memory containing the operating program, and up to small amount of reusable memory.

Contact-less smart card technology (RFID) is becoming widely used in applications that traditional magnetic swipe cards were used. This is primarily used for security access control systems in the form of RFID technology. It should be noted, however, that this type of technology may also susceptible to skimming opportunities and there are already some devices that are being marketed to thwart such attacks (Skim Block).

REFERENCES

Chip and PIN, <www.chipandpin.co.uk>, <www.apacs.org.uk>.
Escan Technologies Corp., <www.e-scan.com>, <www.exeba.com>.
Gnet Network Library, <www.gnetlibrary.org>.
ISO/IEC 7810. Identification cards – physical characteristics. International Organisation for Standardisation; 2003.
ISO/IEC 7811. Identification cards – track information. International Organisation for Standardisation.
ISO 7813. Financial transaction cards. International Organisation for Standardisation.
ISO 4909. Bank cards – magnetic stripe data content for track 3. International Organisation for Standardisation; 2000.
RFID, <www.rfidc.com>, <www.rfidjournal.com>.
Skim Block, <www.orient-computer.co.jp/english2/products/en_skim.htm>.
Turner Philip. Unification of digital evidence from disparate sources (digital evidence bags). In: Proceedings of the 5th annual digital forensic research workshop (DFRWS), August 2005.
Turner Philip. Selective and intelligent imaging using digital evidence bags. In: Proceedings of the 6th annual digital forensic research workshop (DFRWS), August 2006.
Turner Philip. Applying a forensic approach to incident response, network investigation and system administration using digital evidence bags. Digit Investig 2007;4(1).