Forensic Data Recovery and Examination of Magnetic Swipe Card Cloning Devices

By

Gerry Masters and Philip Turner

Presented At

The Digital Forensic Research Conference

DFRWS 2007 USA Pittsburgh, PA (Aug 13th - 15th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org


QinetiQ

Forensic Data Recovery and Examination of Magnetic Swipe Card Cloning Devices

Philip Turner
Digital Investigation Services

Magnetic Swipe Cards

- Capable of storing digital data by recording a magnetic pattern within a stripe on the reverse of the card
- Cards used as a form of identification and personal authentication
- Typical uses:
  - Credit cards
  - Debit cards
  - Store loyalty cards
  - Mobile phone ‘top-up’ cards
  - Security ID cards

Magnetic Stripe Card Standards

- ISO 7810 – Physical characteristics of credit cards
- ISO 7811 (1-6) – Embossing, Track location, Lo / Ho coercivity
- ISO 7813 – Financial Transaction Cards
- ISO 4909 – Card Data Format – Track 3

Track 1 Information

- Track 1 – 76 alphanumeric characters
  - Start Sentinel = %
  - Format Code, B = Bank/financial format
  - Primary Account Number (PAN), upto 19 digits
  - Name, 2-26 characters
  - Expiry Date

  Example

  %B0123456789123456^MR A SMITH^0612…?

Track 2 Information

- Track 2 – 37 numeric characters
  - Start Sentinel = ;
  - Primary Account Number (PAN), upto 19 digits
  - Expiry Date – 4 characters
  - Service Code – 3 characters (sss)
  - Discretionary Data (DD) - PIN / Card Verification Value

  Example

  ; 0123456789123456=0612sssDD…?

Track 3 Information

- Not usually used for financial transaction cards
- Track 3- 104 numeric data characters
  - Start Sentinel = +
  - Field Code (FC)
  - Primary Account Number (PAN), upto 19 digits

  Example

  + FC0123456789123456=…?

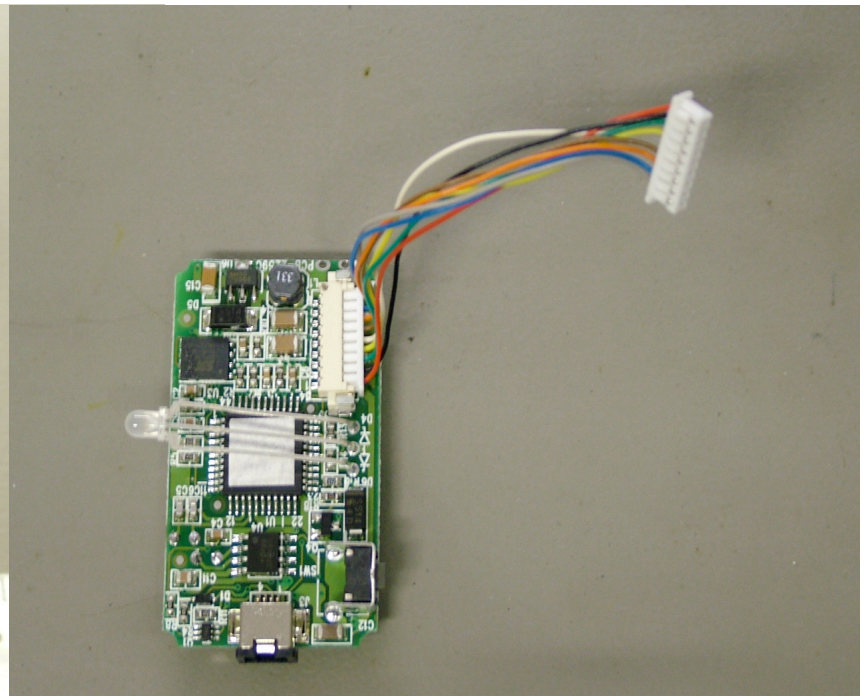
Magnetic Stripe Encoders

- 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

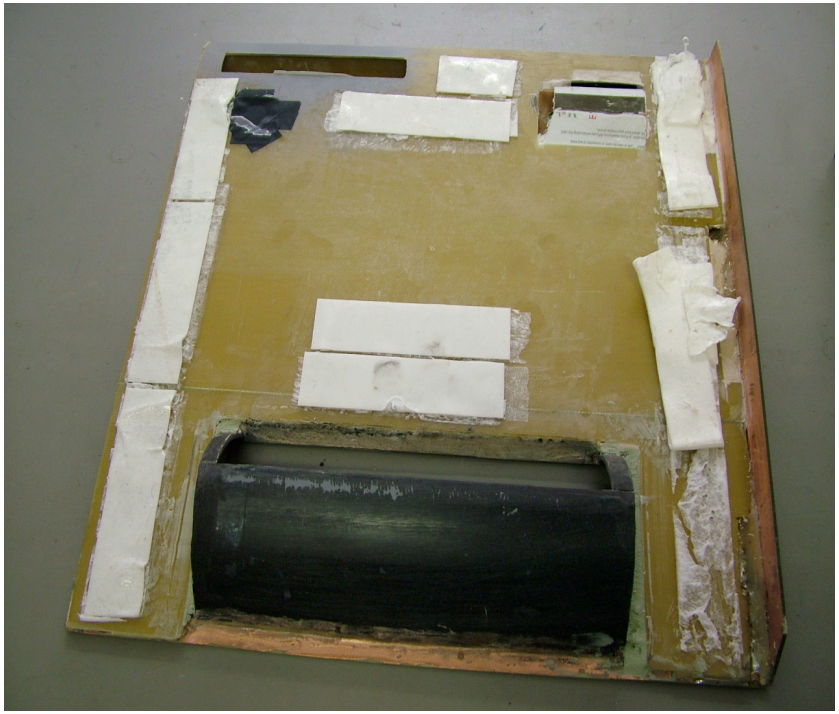
Magnetic Stripe Readers – Mini 123 (1)

- Standalone, battery powered – CR2032 button cell
- Size - L50 x W30 x H38 mm
- 3 Track
- 512K bytes memory – up to 2048 records
- RS232 / USB interface – simple communication protocol
- PIN protected – 4 digit
- Software deletes records/wipes information from device when saved

Magnetic Stripe Readers – Mini 123 (2)



Magnetic Stripe Readers – Mini 123 (3)

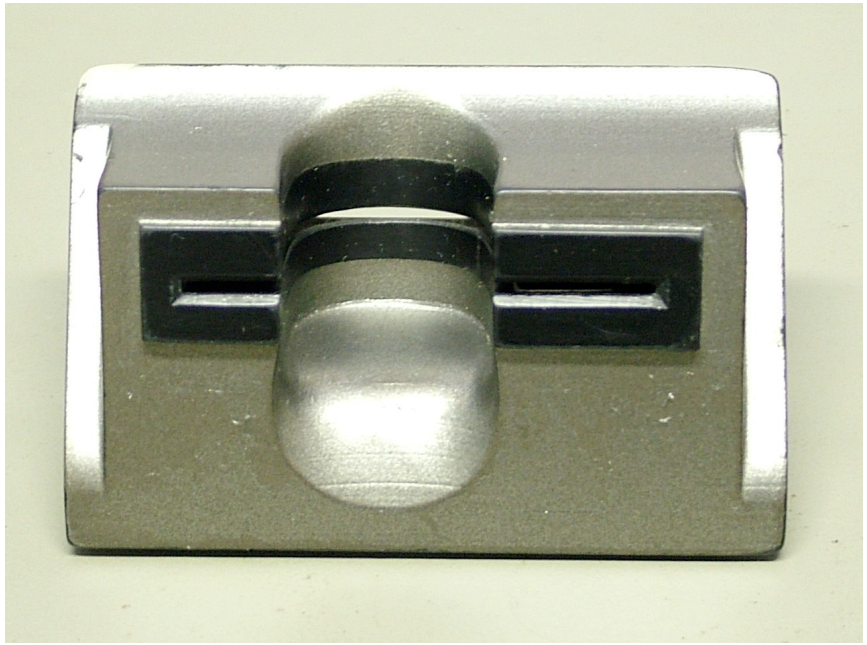


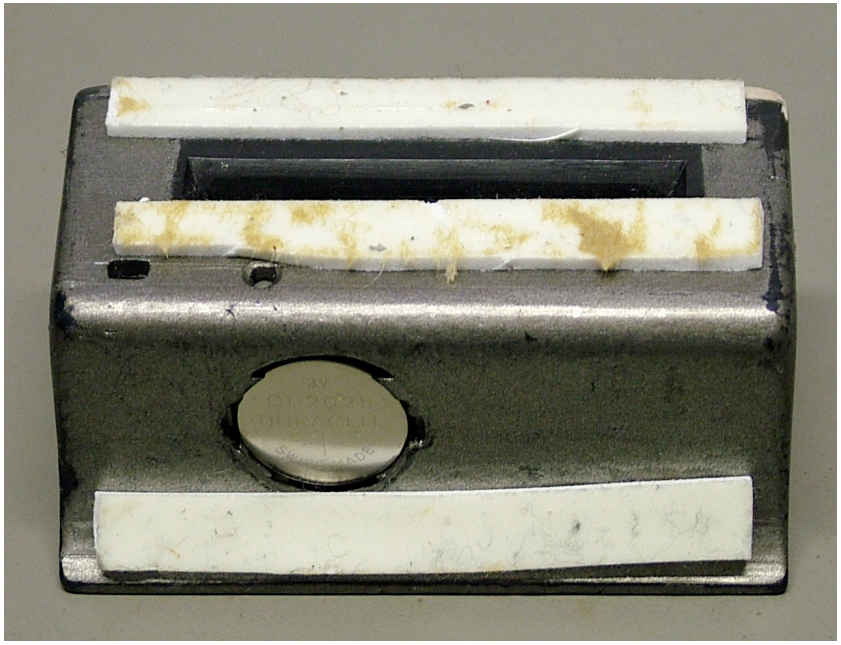
Magnetic Stripe Readers – Mini 123 (4)

- Amazing what you can do with a bit of sticky tape !

Magnetic Stripe Readers – Mini 123 (5)

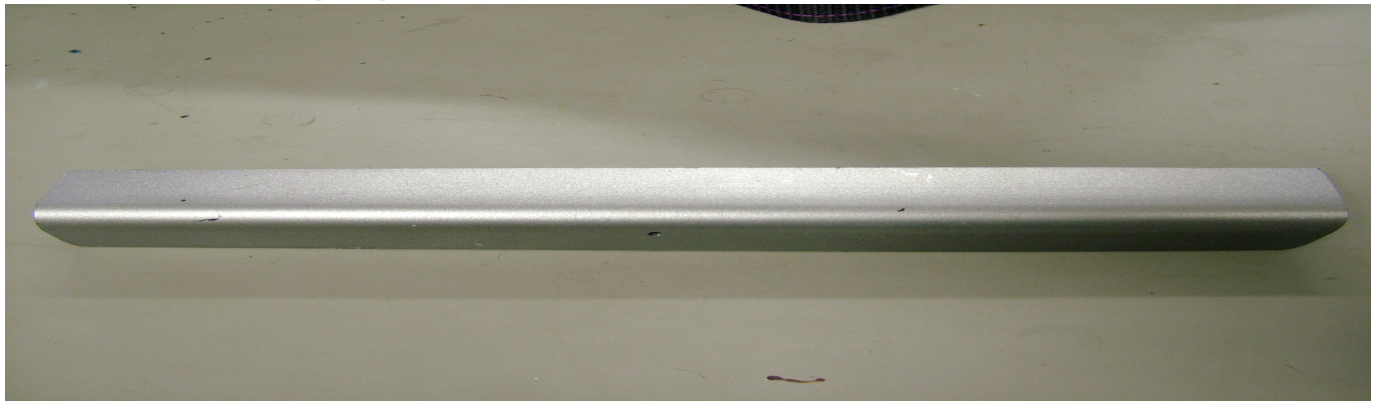
- Other forms…

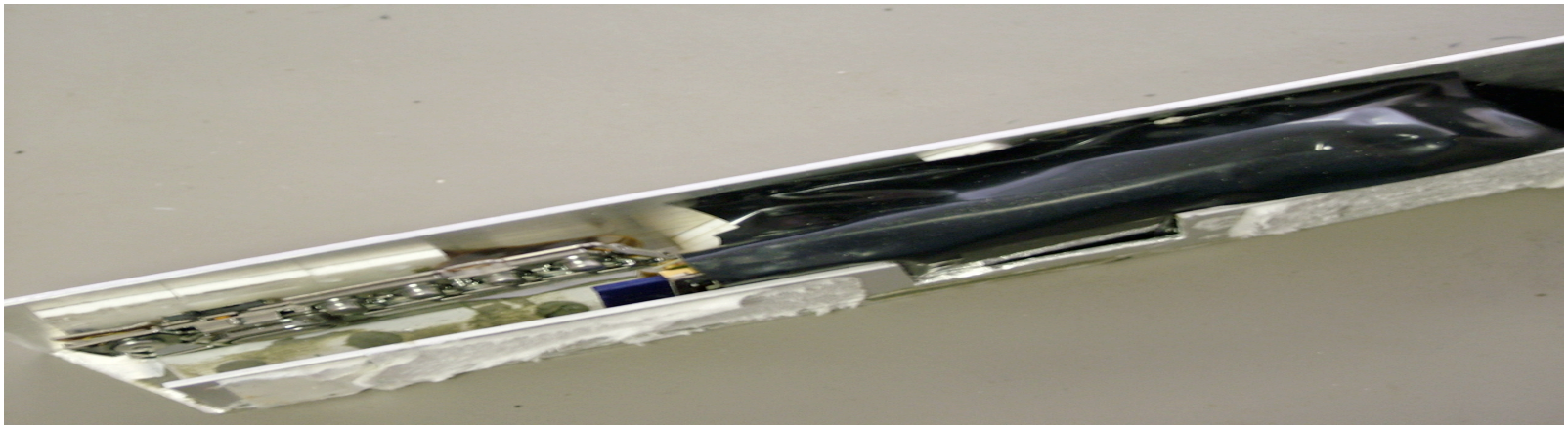




Magnetic Stripe Readers – Cameras

- Associated equipment !





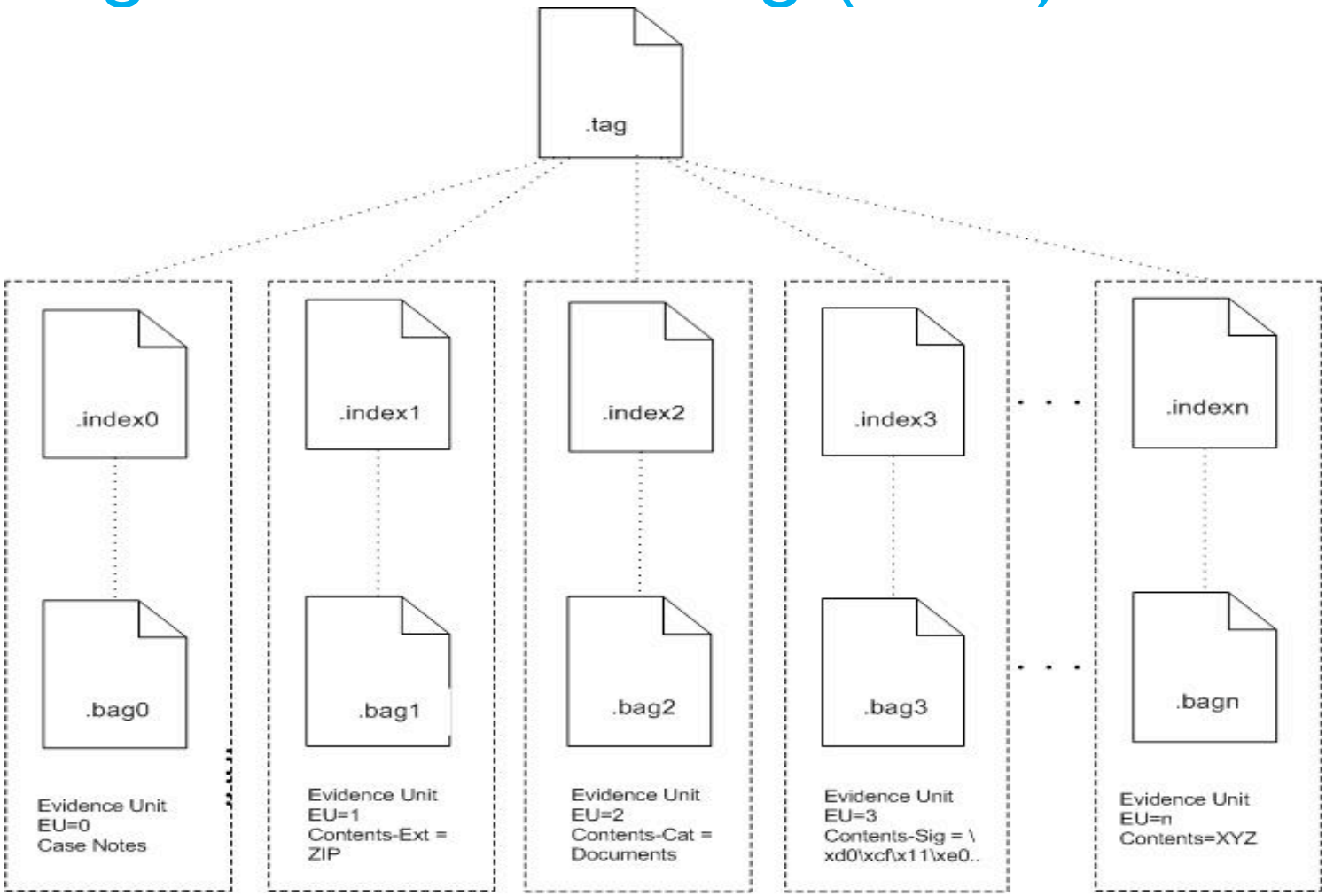
Mini 123 –Forensic Data Extraction

- Simple text data strings in a record format, e.g:

  000,;89441299901234567 89=99121010000000000?2006/11/09 09:35:39 53F

- Other information– product version, unit date & time,number of records,
- The problem:
  - No forensic provenance or continuity of extracted information
  - No integrity assurance information
  - No facility to record associated device metadata e.g. PIN used to access device

Digital Evidence Bag (DEB) structure

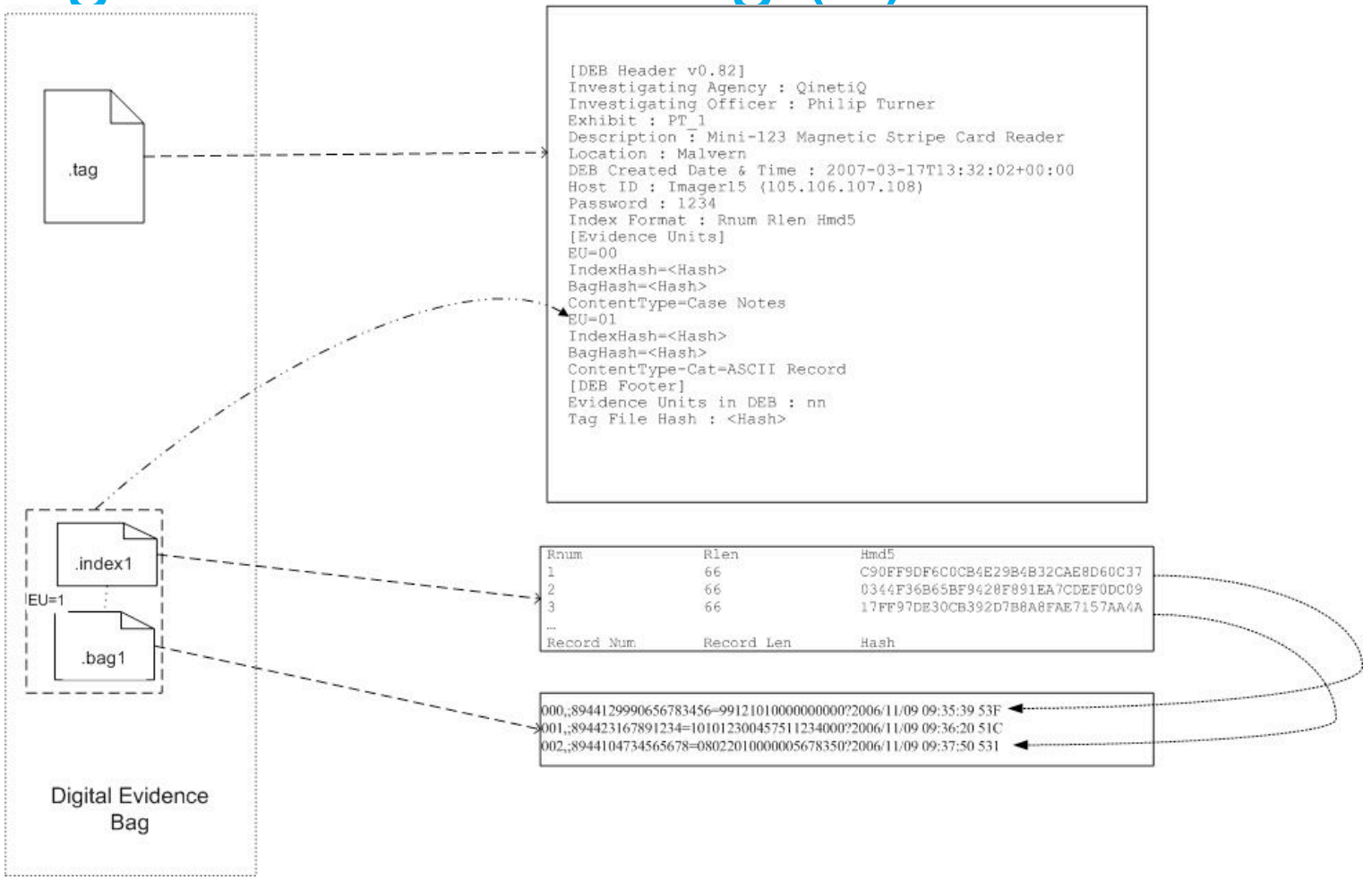


Digital Evidence Bag (DEB)

Mini 123 –Forensic Data Extraction into a Digital Evidence Bag (1)

- Benefits of using a DEB:
  - record provenance
  - track continuity
  - integrity assurance information
  - additional device specific metadata e.g. device login PIN, photographs

Mini 123 –Forensic Data Extraction into a Digital Evidence Bag (2)



Summary

- Overview of Magnetic swipe card standards and types of devices used to read and write magnet swipe data
- These devices are forensically unfriendly
- Proposed solution – the use of Digital Evidence Bags to store extracted information in a forensically sound manner

Questions???