NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

Crowbar Data Recovery Tool
Model: CSHEL-CB-1.0

EVALUATION REPORT

February 2011

NIJ Criminal Justice Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary
Russell Yawn
Laurie Ann O'Leary
Michael Terminelli
Donald Stewart
Randy Becker
Mark Davis, Ph.D.
Kall Loper, Ph.D.
Victor Fay-Wolfe, Ph.D.
Chester Hosmer

Table of Contents

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ research, development, testing and evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. This rigorous process has five phases:

- **Phase I. Determine technology needs, principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www.justnet.org/.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multi-year research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions.** Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides. After adoption, the solution's impact on practice is evaluated.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

NIJ's High-Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making

These NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high-priority needs for criminal justice technology.

[1] National Institute of Justice High-Priority Criminal Justice Technology Needs, March 2009, NCJ 225375.

Overview

The capability to password protect the data on secure digital (SD) cards will become a more common function of cell phones and third-party applications as technology develops to meet the increase in user demand for this functionality. Many cell phones based on the Symbian operating system already feature an option to lock SD cards. This protection can also be enabled on devices using the Linux Operating System. SD cards support personal identification number (PIN) locking through password protection. It is anticipated that the practice of securing data on SD cards will become more common as cell phone users become aware of this function and the ease at which it can be employed. If password-protected SD cards are reported as corrupt or are not detected by existing digital evidence forensic solutions, information of investigative value may be inaccessible or overlooked by examiners not familiar with this technology. Successfully defeating passwords is a technically complicated process that is more effectively and efficiently performed through the use of automated tools and utilities such as the Crowbar, combined with character sets comprised of investigation relevant information.

Crowbar Evaluation

The following press release comes from the ManTech Cyber Solutions website:

ManTech CSI's Crowbar™ Helps Law Enforcement and Military Unlock PIN Protected Data: Unique forensic solution allows government authorities to recover data from memory cards used in cell phones, PDAs and other devices

VIENNA, Virginia, July 09, 2009 – ManTech Cyber Solutions International, Inc. (ManTech CSI), a wholly owned subsidiary of ManTech International Corporation (Nasdaq:MANT), announces its most recent product, Crowbar. This unique digital forensic tool was designed to perform critical functions needed by the law enforcement and military digital forensics community. Crowbar deciphers personal identification numbers (PINs) on multi-media flash memory cards typically used in mobile phones, personal digital assistants, digital cameras, and other devices. ManTech CSI is proud to partner with Teel Technologies (www.TeelTech.com) as a value-added reseller.

"We developed Crowbar as a solution to a dilemma faced by many of our customers – how to recover PIN-protected data from electronic devices taken into evidence," said Alex Nieves, President of ManTech CSI. "Crowbar is currently being used successfully by our customers and we are excited about the growing demand for this product."

Crowbar is available for sale to federal, state and local government agencies.

Crowbar addresses several forensics challenges. For example, many traditional forensics tools will identify a PIN locked flash memory card as 'corrupt' without indicating that the card may be PIN-locked. Crowbar is able to determine if a memory card is PIN-locked, corrupt, or damaged.

Before Crowbar, the only way a military, law enforcement or civilian government investigator could unlock these storage devices was to obtain the PIN from the owner, or manually guess at the PIN. Crowbar gives investigators access to data stored on PIN-locked secure digital or multi-media card flash memory cards by rapidly attempting to determine the PIN.

Crowbar is a user-friendly, portable, handheld device that is designed for tactical field operations. Crowbar delivers results by

- Saving precious field-investigation time by attempting to crack PINS faster and more efficiently than could be done manually
- Creating forensically sound images of unlocked cards for further examination back at the lab
- Serving as a write-blocked card reader for unlocked cards.[2]

Product Information

Traditional forensics tools will identify a PIN-locked flash memory card as *corrupt* without ever indicating that the card may be PIN-locked. Recognizing that the mass of corrupt SD and MultiMediaCard (MMC) media being received from captured terrorists and insurgents was highly anomalous, ManTech CSI's research and development arm attacked the problem and discovered the PIN-locking phenomenon was throwing off forensics tools and letting highly valuable intelligence go undiscovered.

[2] http://cybersolutions.mantech.com/library/ManTech%20CSI%20PR002.pdf

Product Description

The Crowbar is a custom-designed and -built multi-media flash memory card PIN cracking and forensic imaging device. It is a unique hardware-based solution to the forensic problems associated with PIN locked multimedia cards used in mobile phones, PDAs, digital cameras and a wide range of other devices.

Special Features

- Designed for rugged use in the field. It has one joystick-like control mechanism for ease of use and has no internal light source for situations where a covert posture is essential.
- Easy-to-use handheld portability.
- Saves field investigation time by attempting to crack PINs much faster than could be done manually.
- Creates a forensically sound image of an unlocked card for further examination in a lab.
- Serves as a write-blocked card reader for unlocked memory cards.

Target Customers

- U.S. federal, state and local agencies, as well as commercial enterprises.

Law Enforcement Applications for Crowbar

- At border entry points, agents can quickly image (and unlock if necessary) the memory cards being carried by visitors to the United States who are selected for supplementary screening.
- Officers working gang-related issues can use the Crowbar to obtain information about which members are calling or texting, providing information about the scope and scale of gang activity and communications that might not otherwise have been known.
- The Crowbar is able to support special activities units that may have a need to obtain information from a memory card in confidence without the owner of the original card's knowing that his information has been copied.

Evaluation and Testing Details

Bill Teel of Teel Technologies, the U.S. distributor for the Crowbar, sent the following items to the NIJ ECTCoE for the Crowbar testing and evaluation:

- Hand-held Crowbar device (no serial number, model number or other unique identifiers).
- A 19-page manual on hardware and software installation and Crowbar use.
- Two AA batteries.
- One two-gigabyte (GB) SD memory host card.
- USB data cable.
- Crowbar software installation CD.
- Nokia® E65 type RM-208, model E65-1 IMEI-353263010901905 cell phone with power supply.

The Crowbar unit itself is a handheld device with a protective rubber sleeve. The LCD display screen is 1.125-inch wide by .75-inch high. The LCD display characters measure .0625-inch high and the display is not lighted. There is a control stick below the LCD screen to navigate through the Crowbar menu options displayed on the LCD screen. The Crowbar emits no audio. It is equipped with two MMC/SD card slots on the top of the unit labeled *Host* and *Subject*. The Subject slot is outlined in red and is "read only" to prevent modification of data on the Subject card.

Flash memory or SD cards are used as data storage devices in cell phones, cameras and other mobile devices. Whereas SD cards can be password protected using a PIN, few devices provide this functionality. Cell phones with the Symbian Operating System are capable of enabling PIN codes to password protect the data on SD cards. The Symbian OS is primarily used in Global System for Mobile Communications (GSM)

cell phones in the European/Asian markets. Currently, Symbian-based phones are in limited use in the United States.

Test Phone Description

The test phone for this project was a Nokia E65 released in the European market in February 2007. This is a dual mode phone that operates on both the GSM and the Code Division Multiple Access (CDMA) service. The Nokia E65 memory card slot accommodates a Micro SD card for additional data storage. The operating system on the device is Symbian OS 9.1, Series 60 UI.

Note: Micro SD cards are a common form factor used in mobile phones due to the compact size and data storage capacity. The Crowbar does not accommodate Micro SD cards in their native form factor. A Micro SD to SD card adaptor is required to insert the Micro SD into the Crowbar Subject SD card slot.

A two-GB Micro SD card and a one-GB Micro SD card were used for these tests. Additionally, a four-GB card was tested to determine if the Crowbar unit would read the Secure Digital High Capacity (SDHC) card. No information in the Crowbar user manual indicates a size limitation of the Host slot and the Subject slot of the unit.

Crowbar Overview

Crowbar as shipped includes a CD-ROM containing the files needed to configure the Crowbar, a USB cable to connect the Crowbar directly to a forensic examination computer and a two-GB SD card used as the Host card to store the Crowbar configuration files. The SD card is a non-volatile memory card format measuring 24 mm by 32 mm by 2.1mm. It was developed for use in electronic devices including mobile phones, digital cameras and computers. Standard SD cards have a maximum capacity of two-GB according to the SD Association website (http://www.SDCard.org).

The Nokia E65 cell phone provided by Teel Technologies was used to prepare the SD cards to test and evaluate Crowbar functionality. Although the primary market for this cell phone is Europe, it is an example of a phone that may become evidence in an investigation conducted by U.S. law enforcement. This particular phone is capable of locking the micro SD memory card with a PIN. Micro SD cards are a smaller form factor of the SD card. At approximately one-fourth the size of a standard SD card, Micro SD cards measure 15 mm by 11 mm by 1 mm. These cards require an adapter to convert them from the Micro SD card form factor to the larger SD card form factor and make them compatible with the Crowbar Subject SD card slot.

The Crowbar manual is also included on the CD-ROM in PDF format for reference. The manual clearly details the initial setup of the Crowbar and includes a glossary of terms used to describe the operation of the device.

The manual is well written. The section on creating character sets is easy to follow. A fundamental knowledge of password-cracking techniques is advantageous since the Crowbar relies on investigator-created character sets used in brute force attacks to identify the PIN protecting the SD cards. The more the investigator knows about the user, the phone used to PIN lock the SD cards and the details of the investigation, the higher the likelihood that the character sets created will successfully identify the PIN lock passwords.

Pin Recovery Tests Initial Setup

The following steps identify and assess the functionality of the cell phone memory card locking options, the SD card and the ability to access data stored on password-protected SD cards. The Nokia E65 cell phone, a two-GB Micro SD card identified as SD #1 and the Crowbar were used to conduct this evaluation.

1. The Nokia RM-208 cell phone was visually examined and no visual anomalies were identified.
2. Proper insertion of the two-GB Micro SD #1 subject card into the Nokia phone was confirmed.
3. The phone was powered on.

4. Using the phone menu screens, the memory card setup option was selected from the Tools Menu.
5. The Set Password option was selected to enter a PIN code and lock the SD card.
6. A PIN code was entered and SD card #1 was password protected.
7. The phone was powered off and back on.
8. Four photos were taken using the phone's camera feature.
9. Using the cell phone memory card options, the SD card was formatted.
10. On completion of the SD Memory card formatting process, the Tool Menu options included Change Password and Remove Password, but not Set Password, indicating that the password previously set was still enabled.
11. Using the Remove Password option, the PIN previously set was removed.
12. The cell phone gallery option was selected to view photos on the memory card.
13. No photos were displayed.
14. The two-GB Micro SD card #1 was removed from the Nokia cell phone and inserted into a SD card reader connected to a forensic examination computer.
15. AccessData's FTK Imager® v2.9.0.1385 was used to examine the two-GB Micro SD card #1. No image files were found.
16. GetData's Recover My Files® and Smart Media Data Recovery® were used to access and examine the two-GB Micro SD card #1. No image files were recovered.
17. WinHex® v15.6 was used to examine the data on the two-GB Micro SD card #1.
18. WinHex revealed that Sector 0, the first sector of the two-GB Micro SD card #1, contained the Hexadecimal characters 55 AA in offsets 510 and 511 respectively. These are the last two offsets in the 512 byte sector 0 of the two-GB Micro SD card #1.
19. This information reveals that that Sector 0 of the two-GB Micro SD card #1 was properly formatted as a valid File Allocation Table (FAT)16-bit Master Boot Record in the Logical Block Addressing scheme of Data Storage Devices. FAT16 is the common file system for memory cards and is supported by nearly all operating systems.
20. It was determined that when the Nokia cell phone is used to enable password protection on an SD card, the Nokia phone will subsequently access the SD card on powering on the phone without requiring the user to enter the SD card PIN.
21. The phone camera functions are enabled and the SD card can be formatted without entering the password. The Nokia phone Format Card function overwrites the data on the SD card.
22. No data was found on SD card #1 and no data stored on the SD card prior to formatting was unrecoverable.
23. The SD card password protection makes the card inaccessible to other devices including forensic examination computers.
24. Removal of the SD card password protection is accomplished through the Nokia cell phone Memory Card options.
25. When the password is unknown, it must be identified in order to access the data on the SD card.

The following tests were used to evaluate the Crowbar's ability to identify passwords used to lock SD cards.

1. A one-GB Micro SD card identified as Micro SD card #2 was prepared for use in evaluating the performance of the Crowbar.
2. Micro SD card #2 was inserted into a SD card reader attached to a forensic examination computer.

3. Micro SD card #2 was formatted with a FAT16 file system architecture using the forensic examination computer.
4. Cryptomax CleanUSB® v1.0 was then used to clean the SD card by overwriting the data on the SD card.
5. FTK Imager v2.9.0.5 was used to examine Micro SD card #2 and it was found to contain no readable data.
6. Micro SD card #2 was subsequently inserted into the Nokia E65 cell phone and formatted using the Format Card option in the memory card menu.
7. Four photographs were taken using the cell phone camera function and stored on the one-GB Micro SD card #2.
8. The Micro SD card was removed from the Nokia cell phone and inserted into an SD card adapter, making the Micro SD card compatible with the SD card form factor required by the Crowbar Subject card slot.
9. The one-GB Micro SD card #2 in the SD card adapter was inserted into the Crowbar Subject card slot.
10. The Crowbar Subject card menu reported this Micro SD card #2 was unlocked.
11. Micro SD card #2 was removed from the Crowbar and inserted into a SD card reader connected to the forensic examination computer.
12. The four photos taken with the Nokia cell phone camera were viewable on the forensic examination computer.
13. The one-GB Micro SD card #2 was removed from the Crowbar and inserted into the Nokia cell phone.
14. A PIN lock code was enabled on the one-GB Micro SD card #2 using the Nokia cell phone Memory card menu option.
15. The PIN code used in this test was “don55”.
16. The one-GB Micro SD card #2 was removed from the Nokia cell phone and inserted into the Micro SD card reader attached to the forensic examination computer.
17. The forensic examination computer did not detect the one-GB Micro SD card as an available data storage device.
18. A check of the device properties revealed that the forensic examination computer operating system reported it was unable to start the device.
19. FTK Imager installed on the forensic examination computer was used to access the one-GB Micro SD card #2.
20. FTK Imager v2.9.0.1385 detected the card but reported it as an unrecognized file system and could not read information on the card.
21. This corroborates the information provided by the Crowbar developer and reported in the Crowbar information sheet.

PIN Recovery Test 1

The test was to determine if the Crowbar unit would detect the four-GB Micro SDHC card.

1. The four-GB Micro SDHC memory card was inserted into a SanDisk card adapter that would make it compatible to fit into the Crowbar unit.
2. After inserting the four-GB Micro SDHC card and adapter into the Subject slot of the unit, the Subject card was accessed by navigating through the Options menu.
3. The Crowbar displayed that the Subject card was “locked.”
4. The Details icon was selected using the control stick.
5. The Crowbar unit displayed an error in the LCD window that read “problem with retrieving info.”

6. The four-GB Micro SDHC card was removed from the Crowbar Subject slot and inserted into a USB card reader to determine if the card was locked.
7. The four-GB Micro SDHC card was then inserted into a SD card reader connected to a forensic examination computer.
8. The four-GB Micro SDHC card was detected and the data on the card was accessible via the forensic examination computer, revealing that the four-GB Micro SDHC card was not locked.
9. The four-GB Micro SDHC card was removed from the card reader and placed into the Crowbar Host slot to determine if the Crowbar unit could read the four-GB card.
10. After placing the four-GB Micro SDHC card into the Host slot, the Crowbar reported the Host card was locked.

Results. It was determined that the Crowbar cannot accurately read SDHC cards that exceed two GB of storage capacity.

PIN Recovery Test 2

This is a test to determine the capability of the Crowbar to defeat password PIN protection on a two GB Micro SD card.

1. The software from the Crowbar CD was copied to a folder named CROWBAR on the forensic examination computer as per the instructions in the Crowbar manual (page 12). The Crowbar instruction manual describes creation of *character set files* and *configuration files* to improve the performance of the Crowbar in identifying the password used to lock the SD card. Character set files consist of user-selected characters, configuration files consist of user-selected character set files. The user must generate the character set files and configuration files using the Character Set Generator within the Crowbar User Interface. This process is well detailed in the Crowbar user's manual.
2. Two character sets were generated to crack the password "mike".
3. The first character set contained lowercase letters of the alphabet only and was saved with the name "lowercase.chr" in the Crowbar folder previously created.
4. A second character set was generated containing only the numbers 0 through 9, which was saved to the Crowbar folder under file name "numbers.chr".
5. These character sets were selected to create the configuration file "alpha-numeric.cfg" used in this test. The first test was designed to determine the speed and success that the Crowbar had in identifying the SD card password "mike".
6. Two AA batteries were inserted into the Crowbar unit.
7. The two-GB Host card that came with the package was inserted into the Crowbar Host slot.
8. The USB data cable was connected to the Crowbar unit and to the forensic examination computer.
9. On connection of the USB cable to the Crowbar and the forensic examination computer, the Crowbar LCD screen indicated it was operational and the option to connect to the forensic examination computer was enabled. According to the Crowbar user's manual, while the Crowbar is connected to a computer via USB cable, the Crowbar batteries are not used as the Crowbar uses power from the computer supplied through the USB cable.
10. The Crowbar configuration files and character sets on the forensic examination computer were loaded onto the Host card inserted into the Crowbar Host card slot. The file transfer was accomplished quickly, and on completion, the available configuration files were listed on the Crowbar LCD when the Unlock Feature was selected.
11. The two GB Micro card SD #1 was prepared for this test as follows:

12. The two-GB Micro card #1 was inserted into the SD card reader connected to the forensic examination computer and formatted with a FAT16 file system.
13. The formatted two-GB Micro SD card was then inserted into the Nokia E65 cell phone.
14. The Nokia cell phone was then powered on and the camera function was accessed.
15. Four photos were taken with the Nokia phone camera and the images were saved to the two-GB Micro SD card #1.
16. The two-GB Micro SD card #1 was removed from the Nokia cell phone and inserted into a SD card reader connected to a forensic examination computer and viewed.
17. It was confirmed that the four photos were stored on the two-GB Micro SD card #1.
18. The two-GB Micro SD card #1 was removed from the SD card reader and inserted into the Nokia cell phone.
19. The Nokia cell phone Memory Card menu was accessed and the option to Set Password was selected to PIN protect the memory card.
20. The Nokia cell phone confirmed that the password was set.
21. The locked two-GB Micro SD card #1 was removed from the Nokia cell phone and placed into a SD card adapter to make it compatible with the Crowbar Subject card slot and inserted into the Subject slot in the Crowbar unit.
22. The LCD screen on the Crowbar unit indicated the Host card and the Subject card were detected.
23. Using the control stick, the Subject card was selected by depressing the control stick.
24. On selection of the Subject card, the Crowbar indicated that the Subject card was locked.
25. The “Unlock” option was then selected and a prompt appeared to select the configuration file from a list of files previously loaded onto the Host card.
26. The configuration file saved as “alpha-numeric.cfg” was selected.
27. The Crowbar began to test permutations of the characters within the configuration file “lowercase” to identify the password use to PIN lock the 2 GB Micro SD card #1.
28. The LCD screen displays the time in 24-hour format, the number of passwords tested per second, the name of the configuration file in use and the password currently being tested in Unicode Hexadecimal.

Results. After nine minutes and 56 seconds, the Crowbar successfully identified the password “mike”. The LCD screen then displayed that the card in now unlocked and displayed the password in Unicode Hexadecimal format 006d0069006b0065, (“mike”). A log file is generated and preserved as a text document in the same folder where the Crowbar software was located. The log file contains the detail of the attack as well as the number of passwords applied to the PIN locked SD card per second. It also reports that the password was identified. The password is displayed in hexadecimal format and must be converted to ASCII text to identify the characters that were entered into the cell phone keypad to lock the SD card.

After the completion of the first test, the Crowbar was then disconnected from the forensic examination computer and the Subject card was ejected in preparation for the next test.

PIN Recovery Test 3

This test was conducted to determine the timeframe required for the Crowbar to identify a six-character alpha-numeric SD card password using 26 lowercase alpha characters and 10 numeric characters.

1. The two-GB Micro SD card #1 was inserted into the Nokia E65 cell phone.
2. The two-GB Micro SD card #1 was locked with the password "mike17" using the Nokia cell phone memory card Set Password option.
3. After confirming the two-GB Micro SD card #1 was password protected, it was inserted back into the SD card adapter and into the Crowbar Subject card slot.
4. The Host card was not changed from the previous test and the configuration file and character sets previously loaded onto the Host card were used for this test.
5. After confirming that the Subject card was locked on the Crowbar, the USB cable was detached from the laptop.
6. The unlocking procedure was then initiated as detailed above.

Results. The batteries in the Crowbar unit expired before the password could be retrieved. This test was repeated using the USB power supply. On the third day of processing, the Crowbar unit identified the password used to lock the two-GB Micro SD card. The total time to identify the six-character alpha-numeric password was approximately 52 hours.

PIN Recovery Test 4

This test was conducted to determine the timeframe required for the Crowbar to identify a five-character alpha-numeric SD card password using only the alpha and numeric characters used to create the password.

1. A new configuration file was created. This configuration file contained only special characters, the number 5, and lower case alpha characters d, o and n.
2. The configuration file was saved as filename "don.cfg" and transferred to the SD card inserted into the Crowbar Host card slot using the same procedure previously detailed.
3. The one-GB Micro SD card #2 password protected using the Nokia cell phone with password "don55" was inserted into SD card adapter and into the Crowbar Subject card slot. On insertion, the Crowbar powered on and reported that one-GB Micro SD card #2 was locked.
4. Using the Unlock Menu, the Crowbar prompt required selection of the configuration file to be used. The configuration file "don.cfg" was selected for this test.
5. This test commenced at 1840 hours or 6:40 p.m. and finished at 1943 or 7:43 p.m., one hour and three minutes later.

Results. The Crowbar reported a Found Password. The Crowbar creates a file named Runlog.txt during the operation. This file contains the details of the unlock test and the results. The SD Host card containing the configuration files and Runlog.txt file were removed from the Crowbar and inserted into a SD card reader connected to the examination computer. The Runlog.txt text file was opened as a text file. The last entry in the text file was Password Found: 0064006f006e00350035. The user must recognize the results are reported in hexadecimal format and must be able to convert the results reports to text format to identify the actual PIN used to lock the SD card. On converting the hexadecimal results to text, it was revealed the password found was "don55".

Crowbar SD Card Image Tests

The Crowbar can also be used to create an image file of a Subject SD card for later forensic examination or to preserve as evidence. The following tests were conducted to evaluate the Crowbar imaging capabilities and the image file type created by the Crowbar.

SD Card Image Test 1

This tested involved imaging a Subject SD card to a larger capacity Host SD card using the Crowbar.

1. For image test 1, a two-GB SD card identified as two-GB SD card #3 was used as the Host card.

2. The two-GB SD card #3 was prepared as a new Host card to save the image created by the Crowbar.

3. The two-GB SD card #3 was inserted into the SD card reader connected to forensic examination computer. The forensic examination computer was used to format the two-GB SD card #3. While connected to the forensic examination computer, Cryptomax CleanUSB v 1.0 was used to overwrite any data on the SD card. FTK imager was used to examine the two-GB SD card #3 to determine if contained any data. This examination revealed that the two-GB SD card #3 was free of data.

4. The one-GB Micro SD card #2 was inserted into the Nokia E65 cell phone.

5. Using the Memory card option on the Nokia cell phone, the password enabled on the one-GB Micro SD card #2, previously identified by the Crowbar as don55, was removed.

6. On removal of the one-GB Micro SD card #2 from the Nokia cell phone, it was inserted into the Crowbar using the SD card adapter. Using the Subject Menu, the Crowbar reported the one-GB Micro SD card #2 was unlocked.

7. The Crowbar Subject Menu options include the capability to image a Subject SD card. The Image option was selected, and the Crowbar began imaging the one-GB Micro SD card #2 inserted in the Subject card slot to the two-GB SD card #3 inserted in the Host card slot.

8. Crowbar reported the imaging process would take 420 minutes or seven hours to image the one-GB Micro SD card #2 in the Subject card slot to the 2 GB SD card #3 in the Host card slot. This estimate calculates out to an imaging rate of 2.438 MB (megabytes) per minute.

9. On completion of the imaging process, the two-GB SD card #3 was removed from the Crowbar Host card slot and inserted into the SD card reader connected to a forensic examination computer.

Results. Examination of the two-GB SD card #3 was conducted using FTK Imager. The two-GB SD card #3 was found to contain one file bearing the filename “Image.img”. The “Image.img” file on the two-GB SD card #3 was accessed revealing both deleted and non-deleted files contained within the image file of the one-GB Micro SD card #2. The Crowbar successfully imaged the one-GB Micro SD card #2.

SD Card Image Test 2

This test used the Crowbar as a SD card reader to conduct imaging with a forensic examination computer.

1. The user manual indicates that the Crowbar can also be connected to the forensic examination computer using the USB cable supplied and an image of an SD card inserted into the Crowbar Subject card slot can be acquired using forensic imaging software on the forensic examination computer.

2. The one-GB Micro SD card #2 was placed into the Crowbar Subject card slot using the SD card adapter and the unit powered on. The Crowbar was connected to the forensic examination computer with the USB cable supplied.

3. Using FTK Imager, the one-GB Micro SD card #2 inserted in the Crowbar Subject card slot was imaged to a directory on the forensic examination computer.

4. The RAW image file type option was selected to create a duplicate disk (DD) image.

5. The location to save the image file was the folder previously created on the forensic examination computer.

6. FTK Imager reported this imaging process would take one hour to complete the imaging process of the one-GB Micro SD card #2. This calculates to an imaging rate of 17.066 megabytes per minute.

Results. On completion of the imaging process, FTK Imager was used to open the image file acquired from

the one-GB Micro SD card. The image file contained both the deleted and active files contained on the one-GB Micro SD card. These files were accessible for forensic examination. The Crowbar can be successfully used as a SD card reader to image a SD card with a forensic examination computer and acquisition software.

SD Card Image Test 3

This test evaluated imaging a Subject SD card to a Host SD card of the same size using the Crowbar.

1. The two-GB SD Host card was inserted into a SD card reader connected to the forensic examination computer.
2. All files were deleted from the two-GB SD Host card and it was formatted to create sufficient space for the Subject SD card image.
3. The two-GB SD Host card was returned to the Host slot on the Crowbar.
4. The two-GB Micro SD card #1 was inserted into the Crowbar Subject card slot to be imaged to the two-GB SD card inserted into the Crowbar Host card slot.
5. The Subject option was selected using the control switch.
6. The Image option was selected using the control switch.
7. The Crowbar screen then displayed that the destination card for the image was not of sufficient size.

Results. The Crowbar will detect insufficient capacity for the image destination prior to initiating the imaging process.

Evaluation and Testing Summary

Crowbar Manual and Documentation

1. The manual is clearly written and well documented with photos and instructions to create character sets and configuration files. The Crowbar User Manual and Quick Facts Sheet are attached to this report.
2. The manual referred to features or options that could not be found on the Crowbar function menu or the software used to create the character set files including:
3. A reset icon in the System Menu is indicated in the user manual but is not a System Menu option.
4. A field named dictionary field in the configuration software is referenced in the user manual but is not found in the configuration options.
5. The manual indicated a “foundpwd.txt” file would be written to the Host card when a password was found. The recovered password was found in a “Runlog.txt” created by the Crowbar software.

Crowbar Device

1. The Crowbar is a solid and well-built unit. The unit is very well marked and the Host cards and the Subject cards insertion methods are unique to prevent insertion of the SD cards into the slots incorrectly. The Crowbar Host and Subject card slots accommodate SD cards. Cell phones and small scale mobile devices such as the Nokia E65 cell phone supplied and used in these evaluations accommodate Micro SD cards. An adapter is required to change the form factor of Micro SD cards to SD card size to use the Crowbar with Micro SD cards.
2. The small LCD screen is very hard to read, the small screen size and the small font makes reading the screen in low light conditions difficult if not unreadable. In most conditions a light would be needed to read the screen because of the small display and font size.
3. The “joystick-like control mechanism” is small and difficult to use resulting in inadvertent selection of incorrect menu options.
4. The length of time required to identify a password can be excessive to make this a suitable field tool for criminal justice. When a character set and configuration file was created consisting of characters comprising the known password the Crowbar required between 10 minutes and 52 hours.
5. When the Crowbar did identify the password it was reported in Hexadecimal format. The user is required to convert the results from hexadecimal to text in order to enter the password as the PIN on the cell phone keypad to remove the SD card password protection.
6. The Crowbar imaging function required 420 minutes or seven hours at a rate of 2.438 MB per minute to image the one-GB micro SD subject card using a Host card as the storage device. Acquisition of a SD card inserted into the Crowbar by a forensic examination computer connected to the Crowbar by a USB cable is faster at approxi-

mately 17.066 MB per minute requiring about one hour to complete. The time required to image a one-GB SD card connected directly to a forensic examination computer was approximately 1:31.

7. Determinations of imaging time and acquisition rates vary depending on hardware configuration.

8. The Crowbar unit will only read up to a two-GB SD or Micro SD card. Many Micro SD cards in use in cell phones are SDHC (Secure Digital High Capacity), which are greater than four GB.

9. The Crowbar unit will only read up to a two-GB SD or Micro SD card. Many Micro SD cards in use in cell phones are SDHC (Secure Digital High Capacity), which are greater than four GB.

Conclusion

The Crowbar is a good initial approach to address this potential forensic examination challenge. However, the Crowbar and the criminal justice community would benefit from improvements to the Crowbar functionality and performance, including, but not limited to:

- Enable compatibility with SD cards with storage capacity over two GB.
- Larger LCD screen and display fonts.
- Automatic conversion of displayed password from hexadecimal to test.
- Backlight to view results in low light conditions.
- Interface to view Crowbar operations on forensic examination computer or laptop and export results to computer to incorporate into reports.
- AC and DC power supply options.

Also, clarifications to the Crowbar documentation would make it easier to understand the environments in which the Crowbar can be expected to work properly. The Crowbar Quick Facts product description from the developer states the Crowbar is designed for rugged use in the field and under harsh conditions. However, the Crowbar Users' Manual states:

> "Crowbar™ is designed to withstand normal daily usage. It is not intended for use in dirty or wet environments. Exposure of the unit to excessive dirt or moisture may compromise the functionality of the product and will void any warranty. The screen of the product is a liquid crystal display. Subjecting the display screen to excessive temperatures, pressure or sharp objects may distort or destroy the display screen. This type of damage to the display screen will NOT be covered by any warranty."

These statements appear to be contradictory and make it unclear whether the Crowbar is appropriate for use in the field.

At a purchase price of approximately $2,300 per unit, the Crowbar may be cost prohibitive for many agencies. Current demand for this technology is limited; however, developments in SD card locking technologies and increased use of that capability will result in an increased demand for technologies to defeat locked SD cards. This is a technology that would benefit from further development based on recommendations from the criminal justice community.

Appendix A - Hexadecimal to Text Conversion Chart

Hexadecimal Unicode = Hexadecimal = Text
00 64 00 6f 00 6e 00 35 00 35 = 64 6f 6e 35 35 = don55
Hexadecimal to text conversion chart:

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Note: The Crowbar reports the PIN Lock Code in Hexadecimal Unicode.

Appendix B - Crowbar Quick Facts

ManTech CYBER SOLUTIONS INTERNATIONAL, INC.

ManTech Cyber Solutions International, Inc., is a wholly-owned subsidiary of ManTech International Corporation

For more information please contact:

ManTech CSI *- 1951 Kidwell Drive, Suite 500, Vienna, VA 22182*
Telephone: 1-877-416-2195 • Email: Crowbar@CyberSolutions.ManTech.com

Teel Technologies *- 16 Knight Street, Norwalk, CT 06851*
Telephone: 1-203-855-5387 • Email: info@TeelTech.com

TEELtechnologies
Value Added Reseller

Teel Technologies provides advanced analysis and solutions to federal, state and local law enforcement, digital investigators, network operators and security professionals.

Quick Facts:
Crowbar™

Questions & Answers

Q: *How does Crowbar address current challenges in the forensic field?*

A: *Crowbar addresses the problem that PIN-locked SD and MMC media is presented by traditional forensic hardware and software, and common operating systems as "corrupt" without indication that the device is locked. By creating a proprietary combination of hardware and software, the Crowbar is not subject to this limitation, enabling it to attempt unlocking the media at a far greater rate than a human would be capable of performing.*

Q: *What are some other benefits of using Crowbar?*

A: *Crowbar is an easy-to-use, handheld portable tool designed for use in the field. It saves field investigation time by attempting to crack PINs much faster than could be done manually. Crowbar also creates a forensically sound image of an unlocked card for further examination in a lab and serves as a write-blocked card reader for unlocked memory cards.*

Q: *Who can buy Crowbar?*

A: *Crowbar is available for sale to federal agencies as well as state and local law enforcement organizations. "Crowbar as a service" is also available to commercial customers, who can send their multi-media cards to ManTech CSI for processing.*

Q: *Does ManTech CSI offer a demo of Crowbar?*

A: *Yes. ManTech CSI has time-limited demo units available for potential customers to test under real-world conditions.*

Q: *How can I learn more about the purchasing process and speak to a Crowbar expert?*

A: *Law enforcement agencies who would like additional information about Crowbar, who would like to arrange for free delivery of a time-limited demonstration model, or for more information about other ManTech CSI digital forensics products and services call 1-877-416-2195, e-mail Crowbar@Cybersolutions.ManTech.com for general inquiries.*

To learn more go to: http://CyberSolutions.ManTech.com

The Challenge:

Traditional forensics tools will identify a PIN-locked flash memory card as "corrupt" without ever indicating that the card may be PIN-locked. Recognizing that the mass of "corrupt" secure digital (SD) and multi-media card (MMC) media they were receiving from captured terrorists and insurgents was highly anomalous, ManTech CSI's research and development arm attacked the problem and discovered the PIN locking phenomenon that was throwing off forensics tools and letting highly valuable intelligence go undiscovered.

The Solution:

By building a unique hardware-based approach to the problem, ManTech CSI engineers were able to build Crowbar which is able to determine if a memory card is PIN locked, actually corrupt, or damaged. If it is PIN locked, Crowbar is designed to launch a brute-force attack against the PIN. Simple alpha-numeric PINs can be cracked in as little as a few seconds. Crowbar is Unicode compliant, so PINs that may be based on foreign languages are no obstacle.

Product Description: Crowbar is a custom-designed and built multi-media flash memory card PIN cracking and forensic imaging device. It is a unique hardware-based solution to the forensic problems associated with PIN locked multi-media cards that are used in mobile phones, PDAs, digital cameras and a wide range of other devices.

Special Features:

- Crowbar was designed for rugged use in the field and under harsh conditions. It has only one joystick-like control mechanism for ease of use and has no internal light source for situations where a covert posture is essential (a model with a backlit screen will also be available)
- Easy-to-use handheld portability designed for use in the field
- Saves field investigation time by attempting to crack PINs much faster than could be done manually
- Creates a forensically sound image of an unlocked card for further examination in a lab
- Serves as a write-blocked card reader for unlocked memory cards.
- Will distinguish between locked and corrupt cards and is able to read all corrupt cards.

Target Customers: U.S. federal, state and local agencies, as well as commercial enterprises.

Law Enforcement Applications for Crowbar:

- At border entry points agents can quickly image (and unlock if necessary) the memory cards being carried by visitors to the US who are selected for supplementary screening.
- Officers working gang-related issues can use a Crowbar to obtain information about who members are calling or texting, providing information about the scope and scale of gang activity and communications that might not otherwise have been known.
- Crowbar is able to support special activities units that may have a need to obtain information from a memory card in confidence without the owner of the original card knowing that his information has been copied.

Appendix C - Users' Manual

Crowbar™

User's Manual

Model: CSHEL-CB-1.0

ManTech CyberCorps International, Inc.
7799 Leesburg Pike, Suite 700 S
Falls Church, VA 22043

1-877-416-2195 crowbar@mantech.com

TABLE OF CONTENTS

CONTACTING MANTECH

Technical Support

Please contact technical support for all concerns regarding operation of the licensed hardware and/or software. Technical support may be reached via e-mail at crowbar @mantech.com, or via mail at the following address:

ManTech CyberCorps International, Inc.
Attn: Crowbar™ Support Team
7799 Leesburg Pike, Suite 700 S
Falls Church, Virginia 22043

Sales

For all licensing related inquires, please contact us via e-mail at crowbar@mantech.com

NOTICES

Information in this document is subject to change without notice.

The trademark used in this text; Crowbar™ is a trademark of ManTech CyberCorps International, Inc.. ManTech CyberCorps International, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

WARNING

Exposure to Certain Environmental Hardships

Crowbar™ is designed to withstand normal daily usage. It is not intended for use in dirty or wet environments. Exposure of the unit to excessive dirt or moisture may compromise the functionality of the product and will void any warranty. The screen of the product is a liquid crystal display. Subjecting the display screen to excessive temperatures, pressure or sharp objects may distort or destroy the display screen. This type of damage to the display screen will NOT be covered by any warranty.

Electrical

Crowbar™ uses two (2) AA batteries. Batteries should not be stored in the unit for extended periods of non-use. When installing batteries, always install two (2) fresh batteries of the same type. Ensure that the new batteries are oriented correctly and in accordance with the label located on the interior of the battery compartment. Damage attributable to use of incorrect batteries or improper installation of batteries will NOT be covered by this warranty.

Crowbar™ uses two (2) types of connection sockets. Always ensure that memory cards and cables are oriented correctly before inserting them into the product. No connector or memory card should ever be force fit into the product. Force fitting or fitting of improper connectors or cards will damage the connection sockets of the product and the resulting damage will NOT be covered by any warranty.

PARTS LIST

The following items are included in the Crowbar™ product set:

(1) Crowbar™ unit

(1) USB Cable

(2) AA batteries

(1) Software Installation CD

(1) MMC Memory Card

(1) User's Manual

Figure 1 illustrates the contents of the Crowbar™ product set. These photos in Figure 1 are used for general identification purposes and the actual contents of the Crowbar™ product set may differ in appearance.

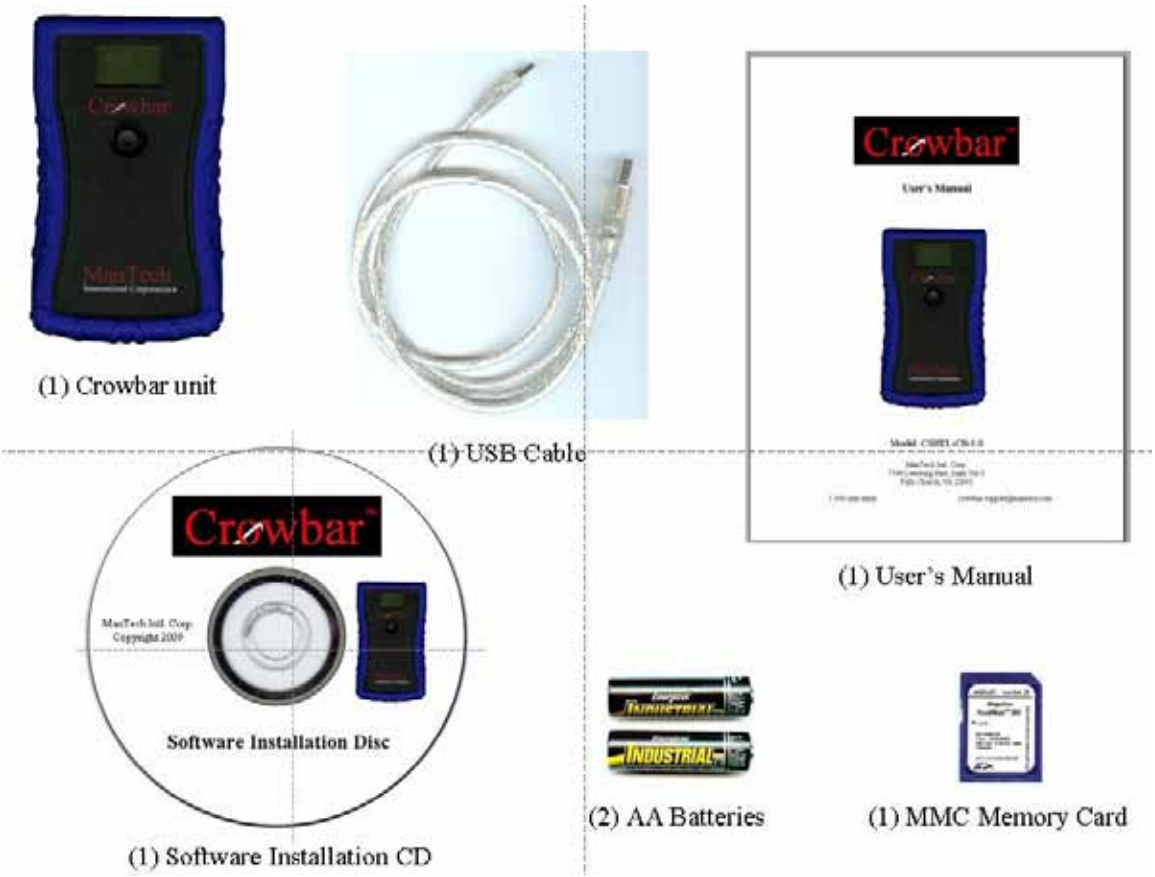


Figure 1

INTRODUCTION

Thank you for licensing Crowbar™ from ManTech CyberCorps International, Inc.

This quality product was developed by ManTech's engineers to improve the user's ability to efficiently access corrupt and PIN locked MMC/SD cards. Crowbar™ is a data recovery tool. When a locked or corrupted card is connected to Crowbar™, the user will be provided with the current status of the card, card meta data, and to the opportunity to unlock and image the MMC/SD card.

Crowbar™ is designed to comply with all standard forensic protocols. As a compact and portable device, Crowbar™ is readily deployable for field operations to help the user meet mission objectives. Crowbar™ always maintains a permanent hardware write block on the subject card. When Crowbar™ unlocks a card, the PIN assigned to the card remains intact while allowing the user to image the card. When an unlocked card is removed from Crowbar™, the PIN lock is automatically reinstated by the card. Crowbar™ identifies the PIN for the user to enable the use of the password on other subject media/files (as users tend to reuse passwords). Crowbar™ automatically stores the PIN in a dictionary file for quick access and unlocking of the same card in the future.

While Crowbar™ is a sensitive electronic device that should be handled with care, use of the protective rubber sleeve provided with Crowbar™ will help this product withstand the rigors of conventional field operations. With a set of fresh batteries, Crowbar™ product should perform unlocking and imaging operations for up to twelve (12) hours. When the included USB cable is plugged into Crowbar™ and a powered USB port, Crowbar™ will automatically discontinue battery power in favor of the USB power source. Crowbar™ has been designed to be a no light/low noise emitting device, enabling use in sensitive areas without detection. Crowbar™ allows the user to store data from subject MMC/SD cards to internal storage, or directly to a PC using the included USB cable. If mission requirements dictate use of a specific imaging utility, Crowbar™ allows access to unlocked media by way of a transparent (although still write blocked) interface. The imaging tools will detect and recognize the media as if it were connected directly to the PC.

TERMS

The following list identifies unique terms used in this manual as they apply to Crowbar™ and its operation.

Host Card: Any MMC/SD card, such as the one provided with Crowbar™ that is used to contain the configuration files and dictionaries required for Crowbar™ to operate. This card is always placed in the card slot marked HOST on Crowbar™. This card is able to be read or written to and when installed, will fit further into the Crowbar™ case than a card in the SUBJECT slot.

Subject Card: Any MMC/SD card that you wish to access using Crowbar™. These cards may be PIN locked or corrupted, and are always placed in the card slot marked SUBJECT. This slot has a red border around it on the Crowbar™ case. This card is write protected, and Crowbar™ can only read from any card in this slot.

SYSTEM ICONS/COMMANDS:

HOST: Enters the Host Card submenu system. Available from the main menu.

SUBJECT: Enters the Subject Card submenu system. Available from the main menu.

SYSTEM: Enters the Crowbar™ system submenu. Available from the main menu.

EXIT: Returns to the previous menu. Available from all submenus.

INFO: Provides information about the Crowbar™ unit including the version number on the installed firmware and the date/time of the firmware build. When contacting ManTech about Crowbar™, be sure to include this information. Available from the system submenu.

BATTERY: Displays the remaining charge in each of the Crowbar™'s battery systems. The primary (AA) batteries, used for operations, will only have the status displayed if they are installed. The system clock battery is used to maintain the internal clock, and should provide years of use. Available from the system submenu.

RESET: Used to perform a soft reset of Crowbar™. Available from the system submenu.

IMAGE: Command to create an image file of the Subject Card on the Host Card. Sufficient space must be available on the Host Card for this feature to operate. Available from the subject submenu.

TIME: Displays and allows editing of the internal date/time settings. Holding the control stick up and down will scroll the selected number. Click the control stick to save your settings and return to the main menu. Available from the system submenu.

CONNECT: Available from both the subject and host submenus, this command sets Crowbar™ into remote access mode. Allows a PC connected via a USB cable to directly access the MMC/SD card indicated by the submenu from which the command was entered. Host Cards will always be presented in read/write mode. Subject Cards will always be presented in read only mode. This allows updating the host card from the PC as well as coping card images from the Host Card to the PC. When used from the subject submenu, it allows the PC to read files from or image the Subject Card.

DETAIL: Available from both the subject and host submenus, this command displays the following information from/about the MMC/SD card indicated by the submenu from which the command was entered; Manufacturer/OEM Codes, Product Name/Revision, Card Serial Number, Card Production Date, and Card Capacity. It should be noted that all information shown by Crowbar™ is the data being reported by the card. It has been shown that some manufacturers do not follow the standards regarding the format of these values, nor always enter values for all fields.

UNLOCK: Initiates the password cracking process on a Subject Card. Available from the subject submenu.

SETUP

Inserting the Primary AA Batteries

Step 1: Remove the rubber protective sleeve from the unit by carefully stretching one corner off at a time.

Step 2: Using light downward pressure on the cast in arrow, gently slide the cover in the direction shown.

Step 3: Insert batteries into the open compartment using the polarity indicators inside the case to correctly orient each battery.

Properly installed batteries should look like this:

Step 4: Reverse the opening procedure to close the unit.

Installing the Host Card

Step 1: Insert the provided SD card into the slot marked "HOST" on the top of the Crowbar™ unit. The end of the card with the exposed contacts should be inserted first, with the contacts facing the back of the Crowbar™ unit.

Step 2: Carefully press the card into the connector until a clicking noise is heard. When releasing pressure on the card, it will move out slightly. This is the normal position for the card. If you need to remove the card for any reason, pressing in on the card, will cause another click, and the card will be ejected. Never remove a card by simply pulling on it; damage to the connector will result.

Crowbar™ is now ready for use!

NOTE: Although Crowbar™ will be operational at this point, it is imperative that users understand that the key to efficient use of Crowbar™ comes from creating effective and relevant character sets and configuration files. It is incumbent upon each user of Crowbar™ to create and use the most efficient configurations for their individual requirements. To create an efficient configuration, the user should whenever possible, review the system that was used to lock the card. This review should attempt to discover the languages and character sets available on the system, as well as the default method used to generate PINs. By fine tuning the Crowbar™ configuration file to only include languages/character sets that were available on the locking system, a great reduction is made in the key space that is required to be searched. Further reductions can be had by studying the locking mechanism. For example, if the media was locked using a mobile phone, what characters are the default characters when entering data? Uppercase? Lowercase? Numbers? If the user can determine that the first character generated when pressing any key on the keypad is a lower case alphabetic character where applicable, else the primary key function, the key space can be further reduced. Using this picture of a cell phone keypad as an example, our sample character set would be: 1, a, d, g, j, m, p, t, w, *, 0, #. Running this 12 character sample set against a locked piece of media is much faster then running the entire alphabet, and more likely to succeed, as many users only use the first key press when creating their PIN, and the standard alphabet search would not take into account the special characters * and # nor the numbers 0 and 1. Instructions on how to create these configuration files can be found in the 'Using Crowbar™' section of this manual.

SOFTWARE INSTALLATION

Microsoft Windows

No software installation is required. The file "Crowbar.exe" is a standalone executable, and may be copied from the provided CD-ROM to a directory of your choice.

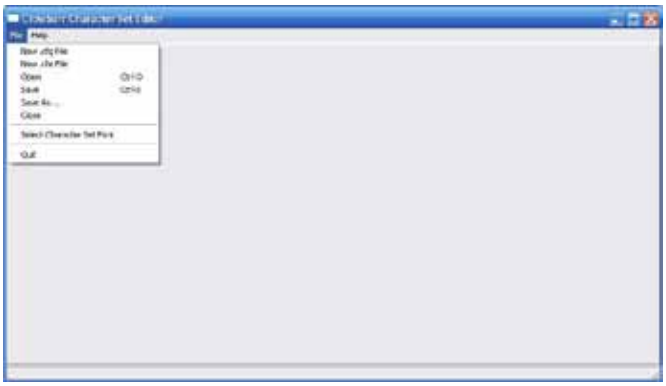
Linux

Although no software installation procedure is required, the four files that make up the software package need to remain in the same directory. Copy all of the files with the "py" extension from the CD-ROM to a directory of your choice. The main executable of this package is "Crowbar.py". The remaining support files, "tabbase.py", "chrtab.py", and "cfgtab.py" are all referenced by the main file and should not be run separately.

USING CROWBAR□

Character Set Generator

To create a new character set, open the provided software package and select 'New .chr File' from the 'File' menu dropdown.



The scroll bar on the right side of the application can be used to scroll through the entire character set to find the characters you wish to select. If you know the language or values for the characters you are interested in, one of the jump fields along the bottom of the application can be used to go directly to that location in the character set. When the desired character is displayed, left click to select that

character. Each selected character will be highlighted in red in the character set grid, and displayed in the selected characters field. Selections can be made individually, or by holding the left mouse button down and dragging a selection box across all the characters you wish to select. Selection of an entire column or row is also possible by left clicking the header for that row/column. Remove unwanted characters from your selection by holding down the Ctrl button on the keyboard and use any of the

selection methods listed above. When done selecting characters for your new character set file, use the 'File' drop down menu option 'Save As...'. Ensure that you choose a filename of 8 characters or less to allow use with Crowbar™.

Additionally, if you wish to edit an existing character set file, use the open command from the 'File" menu drop down. Select the character set you wish to edit, and the software will open that file, and display it using the same interface. You may make any edits you wish, and either resave the character set to the same file, or use the "Save As' feature to create a new file.

The 'Select Character Set Font' command is also available from the 'File' menu drop down. This command allows the selection and use of another font that is installed in your computer. Although the default font was selected for its ability to have as much foreign language compatibility as possible, the Select Character Set Font feature allows users to select others as needed to obtain access to unusual characters only available in other foreign language fonts.

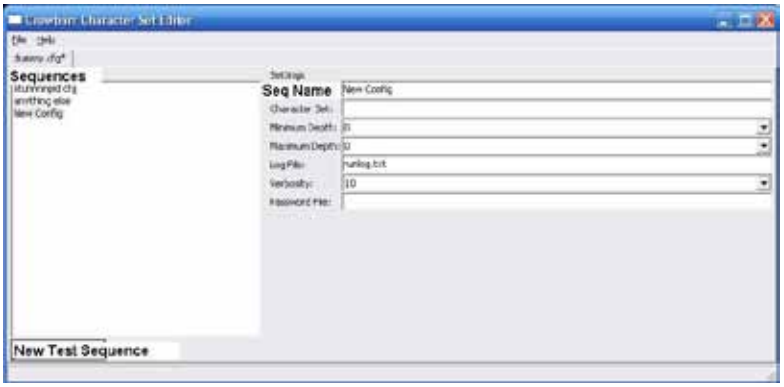
Configurator

To create a new password cracking configuration file, open the provided software package and select 'New .cfg File' from the 'File' menu dropdown. Each configuration file is made up of one or more test sequences. Each sequence uses a unique set of values in an attempt to crack the password. Each sequence runs in the order in which it is saved in the configuration file. Any and all of the sequence configuration values may chance from one sequence to the next. Obviously, no overlap should exist between the sequences, as this simply wastes time repeating previous attempts. A sample set of sequences might consist of:

1) Search all PINs of 0-6 characters in length using the first digits pressed on a cell phone
2) Search all English lowercase alpha-numeric combinations between 0 and 4 characters in length
3) Search all PINs of 7 characters in length using the first digits pressed on a cell phone
4) Search a dictionary file of English words
5) Search all PINs of 8 characters in length using the first digits pressed on a cell phone
6) Search all English upper and lower case alpha numeric combinations between 0 and 8 characters in length.

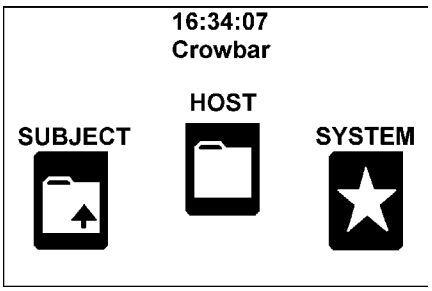
To ensure maximum efficiency in using Crowbar™, you should ensure that each sequence is aligned using a combination of most likely to least likely and quickest to slowest. In the example above, you can see where we split the searching of the "first digits" into multiple pieces to allow other quicker (and still somewhat likely) sequences to be performed, before resuming the first digit search. Our slowest search (the entire English alphabet and numbers) was reserved until the end, as it is much slower than any other search, even though we believe (remember, we didn't search for foreign characters or special characters there) it will ultimately find the password.

To begin creating sequences, on the lower left hand side of the program, click 'New Test Sequence'. Rename this sequence by deleting "New Config" from the 'Name' field and typing in a new name. Set the minimum and maximum search lengths by clicking on the 'Minimum Depth' and 'Maximum Depth' and selecting the desired settings. The minimum and maximum depth values represent how many characters are in the search space. If we set our minimum depth to 0 and our maximum depth to 5, our search will attempt to crack passwords that are 5 characters long or less (the zero length password must be examined (although only once) as a null password is not the same as no password). In the 'Character Set' field, type in the filename for the .chr file you wish to use with this sequence. The default name of the 'Log File' is "runlog.txt". This value may be changed if you wish to single out this sequence for later log review (helpful for enhancing your sequence efficiency.) 'Verbosity' is normally set to the maximum value of 10 to provide the most on screen info to the user during password cracking attempts. The dictionary file field by default contains the file name "foundpwd.txt", the default storage location for all passwords that your Crowbar™ has found previously. If both a dictionary name and brute force settings are listed in a single sequence block, the dictionary attack will always run first, as it is typically much faster. To set up a brute force attack only sequence, simply leave the dictionary field blank. To set up a dictionary attack only sequence, leave the character set field blank and the min/max depth values at 0.



This process may be repeated until you have created all of the desired test sequences. Each test sequence can be reordered by simply dragging the name of the sequence in the 'sequences' field to its new position within the list. When complete, click 'File' and 'Save As..' to save the configuration file. Choose a filename of 8 characters or less.

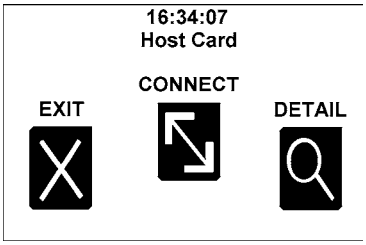
Loading custom configuration files into Crowbar



In order for Crowbar™ to use the files you have just created, they must be stored in the root directory of the Crowbar™ host card. These files can be added directly to the card through an existing card interface you may have, or they can be loaded through the Crowbar™ USB interface.

To load using the Crowbar™ USB interface, simply plug the USB cable into both the Crowbar™ unit and the computer on which the files were created. When Crowbar™ detects power on the USB cable, it will automatically turn itself on. After the boot

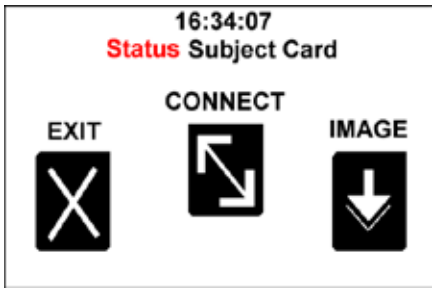
sequence, you should see the main menu depicted here. Using a side to side motion of the Crowbar™ control stick, rotate the icons until the HOST icon is in the center of the screen if it is not already. Depress the control stick, selecting the HOST card, and Crowbar™ will open the Host Card submenu, allowing you to obtain information about the host card "detail", connect to a PC using the USB connection "connect", or return to the main menu "exit". Selecting connect from this menu by again depressing the control stick will instruct Crowbar™ to present the Host Card to the PC as if Crowbar™ were a simple card reader. The PC sees only the card, allowing read/write access through normal file transfer procedures for your system. At this point, use your PC to transfer the files to the Host Card and "disconnect" the media via software from the PC side before unplugging the USB cable.



Card Assessment

The slot for the Subject Card has a red outline for easy identification. **Whereas the Host Card is inserted with the contacts facing down, Subject Cards must be inserted with the contacts facing up.** NOTE: The Subject Card should be inserted until a faint clicking noise is heard. When pressure is released, the card will move slightly out and lock into position. When removing the card later, push the card into the slot until another click is heard, and the card will spring out of the slot. Never pull a card out of any Crowbar™ slot by force. When properly inserted, the Subject Card will extend further out than the Host Card. This feature makes it easier to swap Subject Cards without removing the Host, and aids in quick and easy identification of the card.

The first part of the data recovery process involves inspection the condition of the Subject Card. If Crowbar™ is currently plugged into a PC, the unit should already be turned on. If the unit is not, the insertion of the Subject Card into the Crowbar™ unit will have automatically powered the unit on. After the card is inserted, and Crowbar™ is at the main menu, using a side to side motion of the Crowbar™ control stick, rotate the icons until the SUBJECT icon is in the center of the screen if it is not already. Depress the control stick, selecting the SUBJECT card, and Crowbar™ will open the Subject Card submenu, automatically providing you information regarding the status of the card. The menu should show either "Unlocked" or "Locked" in the status portion of the screen as shown here.

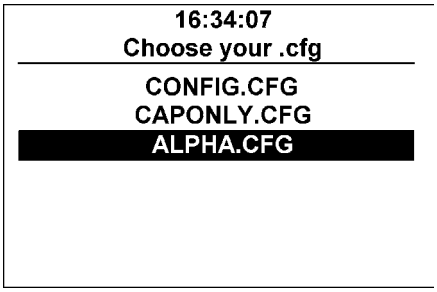


If the status shows that the card is unlocked, then you may proceed immediately to imaging the media using either the image command to create an image file of this media on the host card, or the connect command to allow imaging via a USB connected PC. If the status field shows that the card is currently locked, then you will need to begin cracking the password. If a card is inaccessible via standard card readers, but shows as unlocked in Crowbar™, it is likely that the file system of the card has become corrupt. Crowbar™ will allow imaging of these cards, however there is no "repair" for the corruption. Any resulting image file from a corrupt card will contain the same file system errors as the original card. Manual forensics review of these images frequently results in large portions of the data being recovered. If a Subject Card is correctly inserted however Crowbar™ returns the message "SUBJECT CARD MISSING!", that would indicate that the MMC/SD card has suffered catastrophic internal

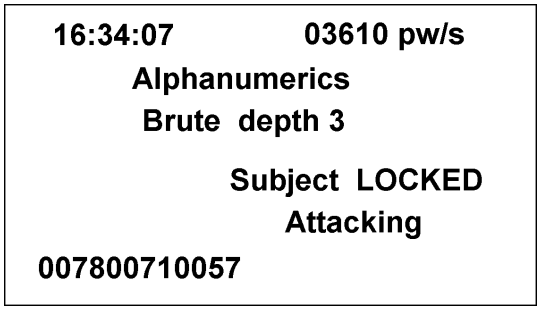
failure, and will not operate.

Password Cracking

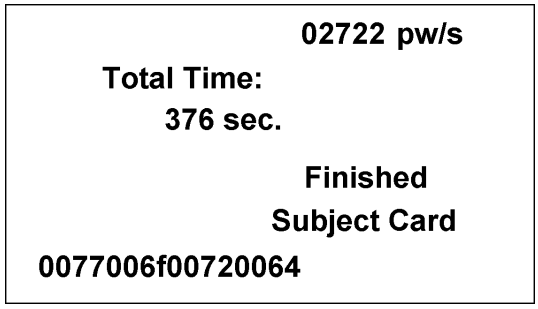
When the status line of the subject card submenu indicates that the card is locked, simply use to the control stick to select the unlock icon. The screen will then display the configuration files that have been loaded into the host card of the unit. Again using the control stick, select the configuration file you wish to use by clicking and moving the highlighted bar to the configuration file name you wish to use and click the control stick to initiate processing of the card. The selected .CFG file will determine what subset of UNICODE characters are to be used in the password cracking attempt. For this example alpha.cfg is selected.



While processing a password cracking attempt, Crowbar™ will display a status screen, as shown below. The status screen displays the current time and the approximate number of password attempts per second on the first line. NOTE: Crowbar™ will operate at the maximum speed of the Subject Card. Altering configuration settings will not change the speed of processing, only the length of time that a process will take. Speeds have been noted in excess of 10,000 passwords per second on newer samples of media. The second line of the screen displays which specific test sequence within the configuration file is currently being executed, and the third shows the type of attempt (brute force guessing, or dictionary based as well as the number of characters in the current attempt. The following two lines simply indicate that the Subject Card is still locked, and that Crowbar™ is still attempting to unlock the card. The bottom line shows the UNICODE values of the current attempt. UNICODE was used throughout the Crowbar™ PIN unlocking process as it provides a universal method for accessing multiple language character sets. In the example below, the password being tried is "xqW" where x0078 = "x", x0071 = "q", and x0057 = "W". The frequency with which this screen is updated is controlled by the verbosity value in your configuration file. The lower the verbosity setting, the less frequent the updates, which will result in a small speed increase in processing.



When Crowbar™ has correctly determined the password, the screen below will appear. In this example, Crowbar™ attempted 2,722 passwords per second, finished in 376 seconds and displayed in hex format the Subject Card's password as 0077006f00720064 which corresponds to "word". The successful password is stored on the host card in the "foundpwd.txt" file by default. Press down on the six-directional button to exit this screen and return to the subject submenu, which will indicate that the card is now unlocked in the status field.

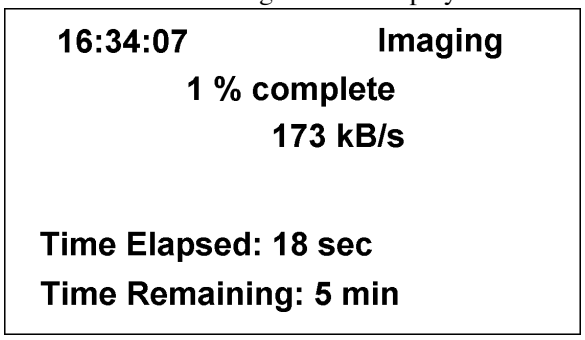


Imaging a Subject Card via USB

Ensure that Crowbar is properly connected via USB to a PC. From the subject card submenu, select the CONNECT option to initiate a connection to the computer. When successfully connected, Crowbar™ will display the message "SUBJECT CARD USB CONNECTED". Crowbar™ has now created a transparent read only link from the Subject Card to the PC. Data on the Subject Card is now available to the PC in a read only format. You may use your PC to browse the files, or use standard media imaging software to image the device as if it were plugged directly into the PC. Once Crowbar™ is connected to the computer, click on "My Computer", then double click on the newest edition to "Devices with Removable Storage". Browse data files at your convenience.

Imaging the Subject Card to the Host Card

From the subject card submenu, select the IMAGE option to initiate the process. If the Host Card has insufficient room to store the image file of the Subject card the error message will be displayed: "Failed Imaging Host too small…". All images made to the Host Card will be named using the convention "xxxx". The screen shown here will appear as the Subject Card image is copied to the Host Card. Once the copying process is complete, something happens. The image file can be copied off of the Host Card at a later time by connecting the Host Card to a PC through Crowbar™, or the card may be removed and used in another card reader.



Maintenance

Installing a firmware update

ManTech may periodically issue new firmware for use in Crowbar™. This firmware may include new and/or improved features to improve MMC/SD processing. To install the firmware, simply copy the file, "crowbar.fwr" to the Host Card. The next time Crowbar™ is turned on or reset, the firmware will automatically install as part of the boot process.

Replacing the Clock Battery

The CR1220 battery installed in Crowbar™ by the manufacturer should provide years of service. Should it fail, it should be replaced with care by someone with experience working with embedded electronics. Opening the Crowbar™ case to replace the battery may cause damage to interior components if done improperly. Please contact ManTech should you require assistance.