

MacLockPick

Ideal for conducting on-scene triage and clandestine or covert operations.

MacLockPick™ is an indispensable tool designed for first responders and law enforcement professionals performing live forensic triage on Mac OS X systems. The solution is based on a USB Flash drive that can be inserted into a suspect's Mac OS X computer that is running (or sleeping).

The following is a list of file items that can be extracted using MacLockPick:

- Enumerates Apple Keychain passwords, such as the user password, and validates it to ensure it is correct.
- Extracts Internet login password, WiFi, AppleShare, and more.
- File and Folder details such as creation, modification, and the most recently accessed dates, recently accessed disk images, pictures, movies, applications and documents.



- Instant Messaging details such as password for iChat and complete buddy list - including buddies who have since been deleted.
- Email account details such as login names and server addresses used, address book, and the date and time of opened attachments.
- Web History and Preferences such as current and cached bookmarks, recently searched strings, cookies, and browsing history.
- Hardware Preferences such as serial numbers of connected iPods, hardware address of recently connected bluetooth devices, listings for WiFi base stations, and MAC address for each integrated network interface on the machine.

MacLockPick takes advantage of the fact that the default state of the Apple Keychain is open, even if the system has been put to sleep. It also makes use of the openly readable settings files used to keep track of your suspect's contacts, activities and history. These data sources even include items that your suspect may have previously deleted or has migrated from previous Mac OS X computers.

A database of the suspect's information is compiled on the Flash Drive to allow for easy transportation away from the suspect's system. This database can be read by the included log readers on Microsoft Windows, Linux, or Apple Mac OS X computers back at base.

Written specifically for Mac OS X, MacLockPick also includes log reader tools that can be used to access your suspect's data even if you do not have a Mac. MacLockPick functions in a forensically safe manner and will never write to the disk or device being investigated. Instead MacLockPick simply extracts and saves the data to its own flash drive.

MacLockPick can recover files from sleeping computers. Once awakened a Mac will return its keychain access levels to the default state found when it was initially put to sleep. Suspects often (and usually) transport portable systems in this sleeping state.

System Requirements:

The suspect's computer must be running:
Mac OS X 10.3.9 or higher
Macintosh CPU with G3, G4, G5, or Intel processor

The investigator's computer can be running:
Mac OS X 10.3.9 or higher
Microsoft Windows 2000 or higher
x86-based Linux distributions with GTK+ 2.0 (or higher)

Data
Duplication Ltd

4 Station Approach, Wendover, Bucks HP22 6BN
Tel: 01296 621121 Fax: 01296 621125
e-mail: info@dataduplication.co.uk
www.dataduplication.co.uk

Forensic Software Products

AccessData Forensic Toolkit™ 2.0

The Ideal Toolkit for the Forensics Specialist

Includes Forensic Toolkit, Password Recovery Toolkit, Registry Viewer and 50 Client DNA License. Includes the Oracle database.

AccessData Password Recovery Toolkit™ (PRTK)

Recover Passwords Quickly & Easily

The Password Recovery Toolkit gives you the ability to recover passwords from well-known applications and gain access to encrypted files and drives, including the encrypted file system (EFS) from Microsoft.

AccessData Distributed Network Attack

Putting Idle Time To Work

In the past, recoveries have been limited to the processing power of one machine. DNA uses the power of machines across the network or across the world to decrypt passwords.

Infinadyne CD/DVD Inspector software

Professional software for intensive analysis and extraction of data from CD-R, CD-RW and DVD media. Tailored for professionals in data recovery, forensics, and law enforcement.

Spector

Automatically Record Everything Someone Does on Their PC

Spector AUTOMATICALLY takes hundreds of screen snapshots every hour, very much like a surveillance camera. With Spector, you will be able to see EVERY instant message, e-mail, web-site visited and keystroke typed.

WetStone - Gargoyle Investigator™

Malware Detection Software

Forensic Pro Edition includes WetStones most advanced malware detection software package and malware datasets for rapid, in-depth forensic investigations. It is designed for forensic analysts, forensic laboratories, law enforcement personnel, corporate investigation teams, and advanced private investigators

WetStone - Stego Suite™

Recover Hidden Information

Provides investigators with advanced steganography investigation capabilities. This suite includes four software tools; Stego Hunter, StegoWatch, StegoAnalyst and StegoBreak, allowing investigators to detect, analyse and in certain circumstances recover hidden information.

Other Products:-

- Forensic Tools
- Hard Disk Duplicators
- Floppy Disk Copiers
- CD/DVD Duplicators
- CD/DVD Printers

Media Duplication Services For:-

- Floppy Disk
- CD
- DVD
- Tape
- Blank Media Supply
- Standard or Customised Packaging
- Fulfilment Service

Data
Duplication Ltd

4 Station Approach, Wendover, Bucks HP22 6BN
Tel: 01296 621121 Fax: 01296 621125
E-Mail: info@dataduplication.co.uk
Website: www.dataduplication.co.uk