



Forensic Analysis of Laptop Data Protection Software

Kris Herrin, CISSP

CSO, Intervice Inc.

Adjunct Professor, Univ. of Dallas

kherrin@gsm.udallas.edu



Forensics ... Lots of Interest

- ◆ Hey, digital forensics is important too!!
 - eDiscovery and digital forensics are now mainstays of security programs
 - Generally required as part of incident response (think PCI, HIPAA, GLBA, et. al.)
 - US market for digital forensics is expected to be \$630m by 2009



The Enterprise Dilemma

- ◆ Compliance with encryption regulations means making data less available ...ensuring privacy
- ◆ Forensics needs data and metadata to be completely available ... enabling visibility



So What's The Problem?

- ◆ When it comes to systems, digital forensics has some unique requirements:
 - Low level access to disks
 - Preservation of file / date stamps
 - Access to system locked areas
 - Access to deleted files that may still reside on the system
- ◆ Forensics requires this in a timely manner with verifiable certainty, not guesswork



Different Problems

- ◆ Intelligent or File encryption generally seeks to encrypt only user data while leaving OS and applications files alone
- ◆ *Forensics vs. Intelligent or File encryption*
 - The general advantage is speed
 - How are files modified? Are timestamps preserved?
 - Can deleted files be recovered?
 - Can we still get access to the pagefile and other system files?



Different Problems

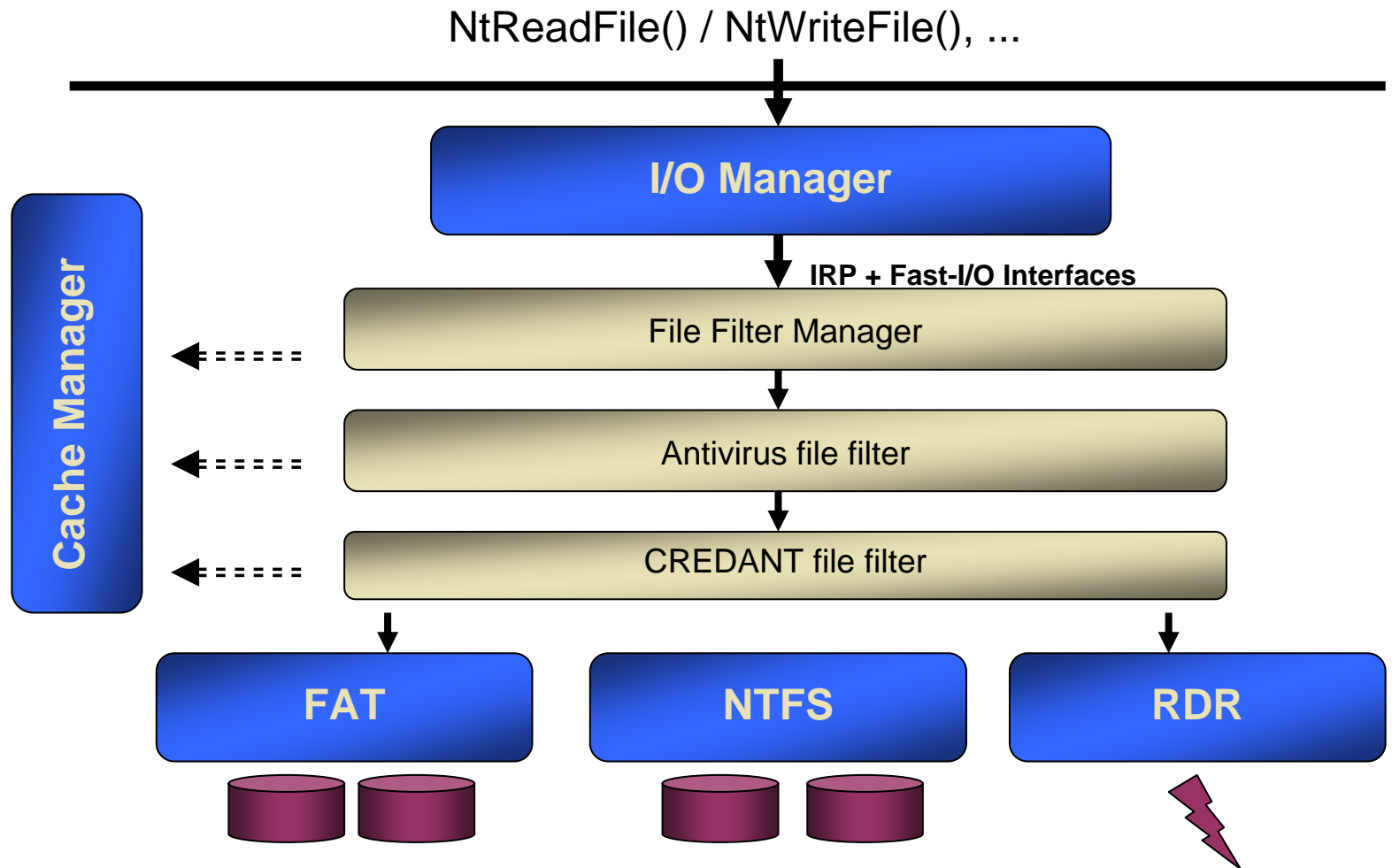
- ◆ Full Disk Encryption (FDE), as the name implies, encrypts the entire disk and everything on it
- ◆ *Forensics vs. Full Disk Encryption*
 - General advantage is preservation of file system, OS, and application evidence
 - How do you decrypt the entire disk before acquiring it?
 - What vendor recovery tools exist?
 - How long will it take? Are there additional hardware requirements?



Forensic Analysis of CREDANT

- ◆ **CREDANT Mobile Guardian (CMG)**
 - “The only centrally managed solution that addresses the complete mobile data security life cycle, across the broadest number of platforms, with the industry’s most comprehensive compliance reporting”
- ◆ CMG is an “Intelligent Encryption” solution, protecting user data only
- ◆ CREDANT is well known for hand-held device

File Filters 101





Forensic Analysis Objectives

- ◆ The decryption of a file must result in an unaltered, original file
- ◆ File date / time stamps must be preserved, both on initial encryption and final decryption
- ◆ The deletion of encrypted files by the underlying file system should be recoverable when possible using standard forensic techniques
- ◆ System files (pagefile, hiberfil.sys, \$LogFile) should remain intact

Analysis – File Integrity

| Name | Evidence File | Hash Value | File Created | Last Written | Last Accessed | Entry Modified |
|-------------------|----------------------|----------------------------------|---------------------|---------------------|---------------|----------------|
| 01072128.POT | FAT-base-data | 035aa796350f7d010dcc52c69d21e4e7 | 11/16/06 03:29:44PM | 10/28/03 05:58:04AM | 11/16/06 | |
| 01072128.POT | FAT-decrypt | 035aa796350f7d010dcc52c69d21e4e7 | 11/16/06 03:29:44PM | 10/28/03 05:58:04AM | 11/16/06 | |
| 01072128.POT | FAT-encrypt-nochange | 01b72c183d110b08b9ad7a46a46d0970 | 11/16/06 03:29:44PM | 10/28/03 05:58:04AM | 11/16/06 | |
| Policy Intro.html | FAT-encrypt-nochange | 05b8dcd7a2eebb9dcdcc5ec90460c84d | 11/16/06 03:29:32PM | 11/22/05 02:50:16PM | 11/16/06 | |
| Policy Intro.html | FAT-decrypt | 837f992d5a60c5e085c9f5bd95bddc6e | 11/16/06 03:29:32PM | 11/22/05 02:50:16PM | 11/16/06 | |
| Policy Intro.html | FAT-base-data | 837f992d5a60c5e085c9f5bd95bddc6e | 11/16/06 03:29:32PM | 11/22/05 02:50:16PM | 11/16/06 | |

Figure 1. MD5 hash values show unaltered FAT files after decryption

| Name | Evidence File | Hash Value | File Created | Last Written | Last Accessed | Entry Modified |
|-------------------|---------------|----------------------------------|---------------------|---------------------|---------------------|---------------------|
| access file 1.mdb | Encrypted-1 | 8dc44403d581af47a7909c14dfc27f18 | 11/16/06 01:45:35PM | 11/16/06 01:45:35PM | 11/16/06 01:45:41PM | 11/16/06 02:13:02PM |
| access file 1.mdb | Decrypt-1 | cef56ba29522524fee11244dcdbbd432 | 11/16/06 01:45:35PM | 11/16/06 01:45:35PM | 11/16/06 01:45:41PM | 11/16/06 02:54:28PM |
| access file 1.mdb | F | cef56ba29522524fee11244dcdbbd432 | 11/16/06 01:45:35PM | 11/16/06 01:45:35PM | 11/16/06 01:45:41PM | 11/16/06 01:45:41PM |
| Unit-G-1.rm | Decrypt-1 | 62ae3df5340b904af294b4ecf15bf0cf | 11/16/06 01:45:25PM | 09/18/05 11:55:34PM | 11/16/06 01:45:25PM | 11/16/06 02:55:14PM |
| Unit-G-1.rm | Encrypted-1 | 3251e15f9d82dcff3c8300245fc6ca24 | 11/16/06 01:45:25PM | 09/18/05 11:55:34PM | 11/16/06 01:45:25PM | 11/16/06 02:13:48PM |
| Unit-G-1.rm | F | 62ae3df5340b904af294b4ecf15bf0cf | 11/16/06 01:45:25PM | 09/18/05 11:55:34PM | 11/16/06 01:45:25PM | 10/13/05 04:04:56PM |

Figure 2. MD5 hash value show unaltered NTFS files after decryption

- ◆ As expected, the FIP 140-2 certified AES works



Analysis – Timestamps

- ◆ Initial Encryption / Final Decryption:
 - FAT: All timestamps were correctly preserved
 - NTFS: MAC timestamps are correctly preserved but Entry Modified was changed as expected
- ◆ Ongoing encryption / decryption:
 - File system functions remain the same and are not changed by the file system filter



Analysis – File Deletion

- ◆ File deletions are handled by the file system per normal deletion procedures
- ◆ System deletion calls (System::IO or NTDeleteFile) are not intercepted by the file filter, therefore file remains encrypted
- ◆ Subsequent encryption policy changes do not impact deleted files

Analysis – File Deletion

- ◆ To recover a deleted file, you need the following:
 - File contents
 - Some registry entries
 - A per-folder config file
 - Access to CMG server
- ◆ If you're missing the config file, some files may be impacted

| Ext | Files Tested | # No Prob. | # Prob. | % Files Affected |
|------|--------------|------------|---------|------------------|
| .ppt | 2552 | 2524 | 28 | 1.10% |
| .xls | 1466 | 1433 | 33 | 2.25% |
| .doc | 8336 | 7649 | 687 | 8.24% |
| .avi | 215 | 197 | 18 | 8.37% |
| .zip | 1500 | 303 | 1197 | 79.80% |
| .mpg | 80 | 11 | 69 | 86.25% |
| .mp3 | 3475 | 356 | 3119 | 89.76% |
| .pdf | 3179 | 130 | 3049 | 95.91% |
| .htm | 5850 | 221 | 5629 | 96.22% |
| .txt | 2542 | 94 | 2448 | 96.30% |
| .png | 3949 | 140 | 3809 | 96.45% |
| .gif | 9914 | 308 | 9606 | 96.89% |
| .jpg | 16194 | 495 | 15699 | 96.94% |



Analysis – System Files

- ◆ By default CMG Shield does not touch the following:
 - %SYSTEMROOT%\Program Files
 - %SYSTEMROOT%\Documents and Settings
 - %SYSTEMROOT%\hiberfil.sys
- ◆ These could be turned on in the particular deployment, so be sure to double-check the central config
- ◆ Pagefile.sys will be a problem because CMG Shield uses a temporary key
- ◆ NTFS \$LogFile will contain encrypted data

Investigative Options

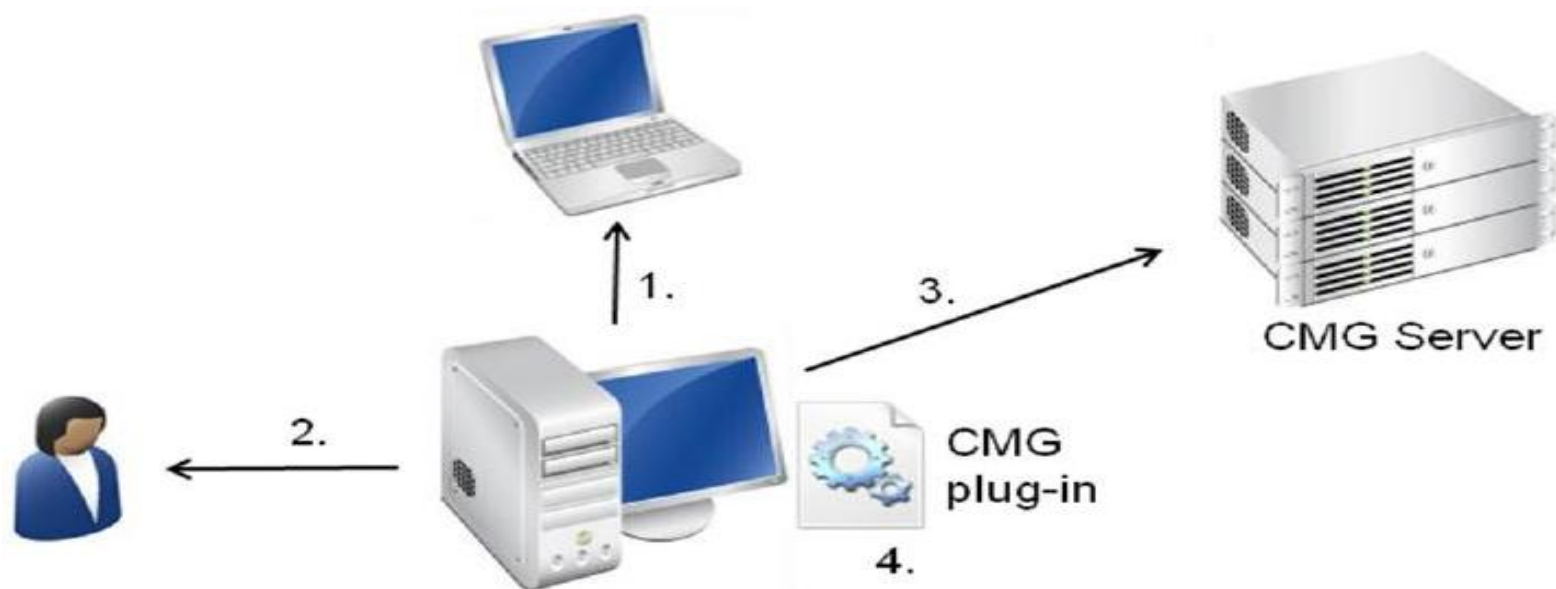
| Technique | Advantages | Disadvantages |
|---|---|---|
| Do nothing – decryption is not necessary | <ul style="list-style-type: none">• Requires no changes in existing processes• Requires no new tools or knowledge | <ul style="list-style-type: none">• Only works for system data not encrypted by CMG Shield |
| Post-acquisition decryption with tool | <ul style="list-style-type: none">• Preserves existing acquisition procedures with minimal impact to the target machine• Allows for decryption of deleted files• Future integration with forensic software allows for seamless decryption | <ul style="list-style-type: none">• Tools not readily available• An external, non-integrated tool requires export and re-import of files |
| Post-acquisition decryption with VMware | <ul style="list-style-type: none">• Tools readily available• Preserves existing acquisition procedures with minimal impact to the target machine• Allows for decryption of deleted files | <ul style="list-style-type: none">• Complicated process to duplicate the target computer• Requires export and re-import of files |
| Pre-acquisition decryption using direct login | <ul style="list-style-type: none">• Simple methodology• Allows for targeted decryption of existing files | <ul style="list-style-type: none">• Requires logging into live machine possibly against forensic best practices• Does not natively recover deleted files |



Future Trends - Integration

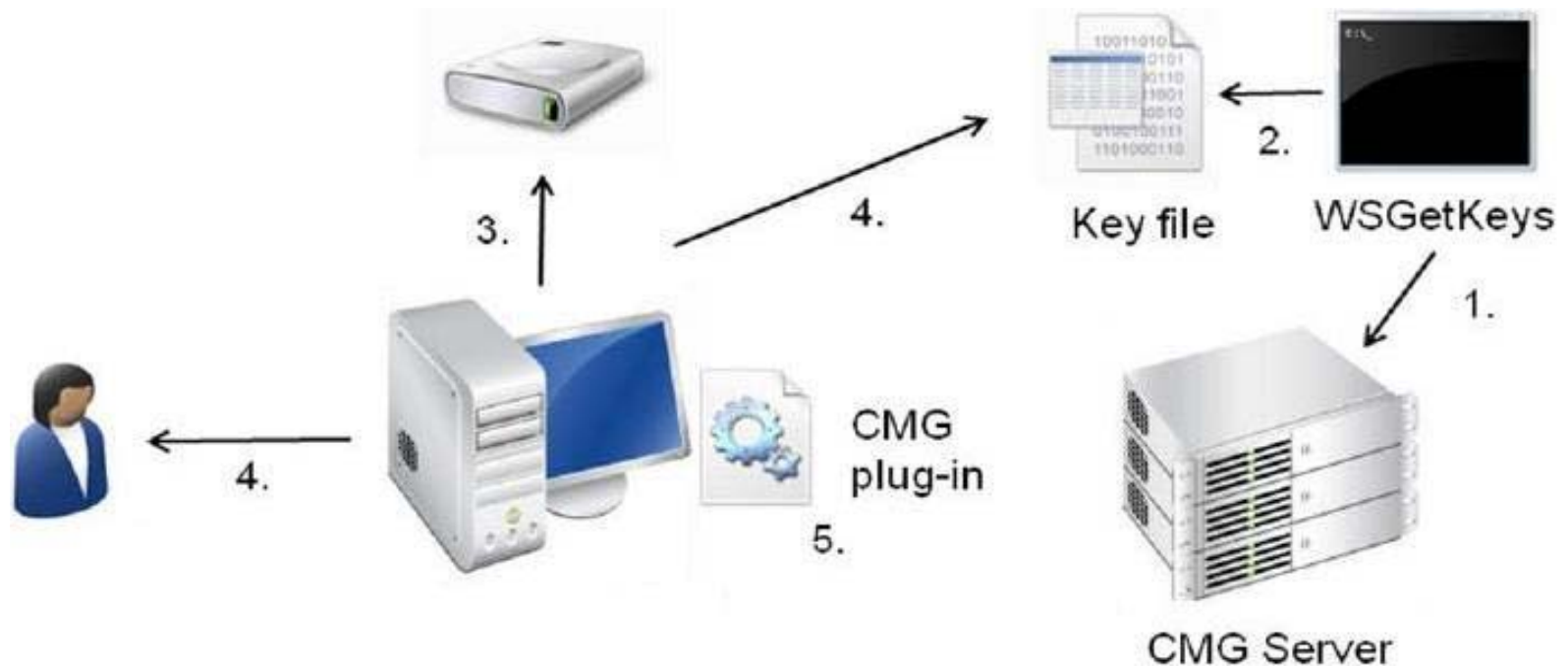
- ◆ None of the previous options are great for forensic examiners
- ◆ As such, the future trend is to tightly integrate enterprise encryption into forensic examination products
- ◆ This can work well if done right, but it is not problem free:
 - How is offline key recovery done?
 - Does this work with “live acquisitions”?
 - What is the performance impact?

Integration Goal: Online



1. Detect CMG-encrypted data is present on remote hardware
2. Prompts investigator for CMG Server credentials
3. Requests encryption keys from the CMG Server
4. Decryption plug-in decrypts data on-the-fly

Integration Goal: Offline



1. Command-line key tool used to export keys from the CMG Server
2. Keys are saved in a password-protected file
3. Detect CMG-encrypted data is present on target drive
4. Tool prompts investigator for the key file and password
5. CMG decryption plug-in decrypts data on-the-fly



Take-Aways

- ◆ The coexistence of encryption and forensics has become the norm
- ◆ As we've seen, most forensic techniques still work but some techniques may require modification
- ◆ Know, test, and validate your enterprise encryption solution before the big case



Thanks!

Kris Herrin, CISSP

CSO, Intervice Inc.

Adjunct Professor, Univ. of Dallas

kherrin@gsm.udallas.edu