Project Report
22 February 2009
4055.841.39/90 – Advanced Computer Forensics
Professor Yin Pan

Table of Contents

Executive Summary

This report provides an overview of how to conduct a forensic investigation of an Apple iPod. The report provides an explanation of the unique features of the iPod which are important for forensic analysis. In addition, the key files which will be of primary interest to the forensic investigator will be detailed and evidence acquisition will be demonstrated. The report includes references to previous research and contributes some new discoveries not previously considered in the forensic analysis of iPods.

Caveats in the Research Process

Due to time constraints and available resources we were not able to examine how the iPod file system works under various conditions. For example, we did not have access to an iPod that was formatted for Mac; as a result we were not able to observe differences between the various formatting options. It is noteworthy to mention, that in our situation, the dd image engulfs only the data partition of the iPod, rather than an entire disk. Certain data which is known to be useful in a forensic investigation was not created or available in our test images. As a result, our techniques and results are limited to the test images and data which were available during this time. In the future, it would be necessary to have a more advanced laboratory with various host computers and iPod variations in order to build out more complex procedures and scripts.

The iPod can contain data on past calendar entries as well as upcoming ones. Though they did not exist on the provided iPod images, they would prove useful in an iPod's forensic analysis.

DeviceInfo

This file was once useful at one time for acquiring useful user-related data; however, it is not created on modern iPods or on modern version of iTunes or other software. Therefore we were unable to examine and put this file to use.

Process Overview

In order to conduct the forensic analysis, we used multiple tools to demonstrate evidence acquisition. In addition, we developed a BASH script which employs command line Sleuthkit tools in order to automate some common forensics tasks. In order to conduct the experiments we acquired images of the iPod file system using command line dd after mounting the iPod as read only in Linux (note, the device can be accessed directly as a block device, therefore there is no need to actually mount the device). The raw image in the dd format was chosen since it could easily be imported into all of the tools selected for demoing the forensics process. In this report, we selected the following tools to perform a forensics analysis: EnCase, FTK, Autopsy, and Sleuthkit for scripting.

Problem Statement

At first glance, the iPod may seem like an innocuous portable audio player. However, the common acceptance of the iPod makes it a clever storage medium for illegal activity. For example, an employee could employ his iPod as an external hard drive and use it to copy company data for illegitimate purposes; since the iPod is not primarily understood to be used for this purpose, it is less likely to draw attention. In another case, a criminal may store his records or other data on his iPod. Current law enforcement may not be knowledgeable about the potential to hide electronic data on the iPod and it may not be included in a warrant or seized during a search of the criminal's property. A craftier criminal may even use the interactive features of the iPod to access and modify data without connecting to a host computer. For example, a loan shark could secretly store and modify payment records on his iPod. Again, because most people believe that the iPod is simply a music player, they may never seize the device for forensics analysis.

As one can see, the iPod can easily be converted from is innocent design to a tool for illegal activity. As a result, it becomes important to understand how the internal workings of the iPod function. iPods can natively store calendar, contact, and image data in addition to audio files. It is also possible to directly access the file system of the iPod allowing a criminal to store data in unusual places or using steganography techniques. Therefore, we are conducting this research in order to facilitate real world investigations of seized iPods. We hope that our research will streamline the process for forensic investigators and help them better understand the challenges they face in their investigations.

While not covered explicitly within this report, the forensic investigation of an iPod can also provide some interesting secondary evidence. Under some operating situations, when an iPod is synced to a host system artifacts of the connection are left on both the iPod and on the host computer. These artifacts can later be discovered and used in a comprehensive forensic investigation. As a result, secondary evidence may be available such as when they information was copied or moved or what other machines or devices may have also been used in perpetrating the crime. This information may also be useful to prove ownership of the device so that a criminal cannot claim planted evidence.

Forensic Investigation Tasks

In this section we will address some key processes and techniques used in the analysis of an iPod. For each task, we will demonstrate how to perform the task with each tool.

EnCase Forensics v. 6.10

As technology of mobile devices becomes more advanced, and mechanisms becoming more and more popular, investigators must be prepared for analyzing them for interesting and valuable data. For instance, iPod's are capable of storing vast amounts of data for their size. These devices have grown in functionality. They play music, store photos, contacts, and files and even play full-length movies. Apple's iPod has taken mobile entertainment to the next level by incorporating all of this into a single device. However, with increased popularity, criminals have found ways to exploit an otherwise altruistic device. It is important that the potential evidence contained on an iPod not be ignored by investigators because more and more criminals rely on these devices to obscure their data. For instance, child pornography to stolen information, the iPod is no longer a simple music device.

The challenge that now lies before law enforcement is identifying the evidence an iPod may contain. Thus, there are a number of tools that can be used to analyze the information on an iPod. In order to truly understand the underlying technologies of the device, the forensic tool EnCase will be focused upon for data recovery, analysis, device and system information, and more. Therefore, using EnCase, it is now possible to analyze the files within the device such as calendar entries, contact information, deleted images, and documents through using string searches and file carving.

The system information highlights the information that is significant to the device such as the last accessed date, file creation date and time, and last written date and time.

Relevant information because:

The last accessed date displays the date of the last activity of the file, but not necessarily when it was altered – only accessed. Activity such as viewing, dragging, or even right-clicking will indicate to the investigator that there has been a change in the last accessed date.

The file creation data and time is a record of when a particular file was created. If the file was edited, changed, copied, or acquired then the creation date is after it was written to or accessed.

The last written date is important to forensic examiners because it tells them when the file was opened, edited, and saved last. This is illustrated in A.5.

Technique

The device in question must be imaged, sector by sector including all allocated and unallocated clusters, and then further analyzed for the presence of data that would indicate sensitive information in an actual scenario. The reason behind the image is a lot of files may no longer have an entry in the FAT or directory and need to be carved out of unallocated clusters.

Task 1: Finding Deleted Files

The procedure used to determine if a file was deleted is seeing if there is a dot in the "Is Deleted" box; the file is noted as deleted if this box is occupied. This also appears if an entity in an Info2 file on an NTFS volume has a deleted file as well. "Is Deleted" displays TRUE if the file is deleted but not emptied from the Recycle Bin. In addition, "File Deleted" shows the deletion date and time as well. This attribute can be beneficial for investigators to compare from when and where something was to when it was deleted. Appendix Figure A.1 provides a visual, depicting the situation at hand.

When looking at the deleted file, it is possible to note the first character in Hex of the filename as well (Appendix Figure A.2).

Task 2: Finding Suspicious Files

EnCase is efficient in searching all of the files in an entry for keywords. In order to search for a specific word, a forensic examiner must select the files to be searched, create the keywords to use in the search and then select the keyword they want to use in the search. However, in EnCase, there is a difference in searches – global keywords and local keywords. Global keywords can be used in any case, or they can be made case-specific and used only within the existing case. On the other hand, local keywords are associated with a unique case, and can be searched for only when the case is open. In this specific case, I searched for the word "secret," and received a few different search hits (Appendix Figures A.6 and A.7). The word "secret" was also found in a couple music files, which is unlikely, because they're files named, "secret hideout," and "secret information" (Appendix Figures A.8 and A.9).

EnCase also allows for the search of known corrupted or attack-based files on machines using keywords, hash values, and hex strings from headers and partial headers.

Task 3: Key File Acquisition

Device information highlights the file system of the mechanism, which in this case is FAT32. It also tells how many bytes per sector EnCase uses with disk images. This is significant for data carving and for looking for the beginning of the next file. Figure sA.3 and A.4 provide screenshots of what an investigator would see in EnCase, for an iPod file system formatted with FAT32.

SysInfo

This file stores device related information, and other non-user identifiable information. The acquisition process in EnCase follows similar steps as in the other applications used through this investigation, so it would be only redundant to give specific details of the acquisition.

NOTE: If the file did not exist, it is a good indication that the iPod was formatted at one point or tampered with.

Task 4: Additional Forensic Tasks – Owner Identification

Unfortunately, the iPod does not store user ownership information regarding the files stored on the iPod. Due to the FAT32 file system in operation on the Windows format iPod, the file system has no means to store any ownership information. Although, the Macintosh formatted iPod utilizes the HFS+ file system, which has the potential to store user information in individual file streams, it would not exist on an acquired iPod image either. But, investigation on such an acquired iPod image would need to take place to prove this.

Forensic Toolkit (FTK):

People think of more ways to hide data and it becomes very difficult on investigators' part to think more like the hackers. FTK, Forensic Toolkit by Access Data is a very powerful forensics tool. It can parse FAT12, FAT16, FAT 32, NTFS, NTFS compressed, Ext2 and Ext3 file systems. It can also use images created by EnCase, SMART, Snapback, Safeback and dd. It is a very powerful tool with a very easy to use interface and has rich functionality. Appendix Figure B.1 shows a mounted iPod image in FTK.

Task 1: Finding Deleted Files

There were quite a few deleted files in the iPod Image. Clicking on the deleted files in the overview tab shows a list of the deleted files (illustrated in Figures B.2 and B.3).

Task 2: Key File Acquisition

SysInfo

Figure B.4 of the appendix captures the information read from the SysInfo file, which contains information about the hardware device. The SysInfo file contains the BoadrdHwName, the serialnumber, firmware Guid and all hardware related information. The device folder also has information on the iPodFamily.

Task 3: Identifying Formatting and Host Computer Information

Task 4: Additional Forensic Tasks – Owner Identification

Figure B.5 shows an acquired Microsoft Word document, with the authoring name clearly visible in the file header.

Unfortunately, this iPod image does not have user information to directly link it to an owner.

Important Screenshots:

Appendix Figures B.6 – B.10 show important file acquisition information. This helps identify key elements of the investigation process that could potentially convict a criminal in an investigation. At the very least, it helps paint a better picture of the situation.

FTK provides the ability for granular searching, and through this technique, key evidence could be found. Simply searching for keywords 'secret' or 'kill' revealed information that was useful in the investigation process. Per the screen shots in Appendix section B, one can see the information discovered when doing such searches.

Autopsy & Helix LiveCD

Mounting the DD image of the iPod in Autopsy is effortless, and provides some useful information immediately. The basic information that one will realize immediately is the file system of the iPod partition (FAT32). Though perhaps not entirely useful to the Forensic analysis, bear in mind the 4GB file size limitation imposed by FAT32.

The other tools used, to fill in the shortcomings of Autopsy, are extremely easy to use, and command references are listed in the Appendix (referenced for each situation).

Task 1: Finding Deleted Files

Autopsy was useful for finding the deleted files on the iPod partition, but lacked in its ability to restore said files. A more in-depth analysis would be required on these files with an application that has more capabilities in terms of deleted file recovery. With this in mind, it was necessary to employ the use of a data carving utility that may provide more information on contents of the deleted file.

Using the utility Scalpel, the deleted files noted in the previous example could be 'carved' based on file header information and exported to a working file. Commands issued and configuration file changes made can be viewed in Appendix C.1 and C.2, respectively. When performing this procedure on the two iPod images obtained, various pictures and word documents were discovered. Appendix C.3 shows how Scalpel organizes the exported and deleted files, based on file type. As you will see in Appendix C.4 and Appendix C.5, both files appear to be the same except for one line of text. Autopsy helped identify that the files were still on the FAT32 volume, but could not show the contents. Scalpel helped reveal that a previous version of a Microsoft Word documented existed at one time, with information that would be extremely useful for an investigator.

Furthermore, it was necessary to check the image files gathered from Scalpel for traces of steganography. This was achieved by using the Stegdetect command (see Appendix C.6 for command reference). If Stegdetect exits with asterisks when running the command on a specific file it is an indication that steganography may exist in the file. In one situation (Appendix C.7), Stegdetect found a file likely to have steganography, but Stegbreak was unable to bruteforce the hidden information. This indicates that Stegdetect encountered a false positive, or the file was modified with a more enhanced steganography tool such as Steghide.

Task 2: Finding Suspicious Files

In the particular setup of the iPod that we used, music is housed within the root of the volume in the iPod_Control/Music directory. Audio files are placed arbitrarily into folders with the naming convention FXX, where X represents an integer. The folders increment from F00 to F50, giving a possible total of 51 folders. The individual audio files within the folders use a four character alphabet-only prefix as a naming convention. This would mark a good starting point for finding files out of the norm.

Starting with the iPod_Control/Music folder directly, searching for the string 'mp3' in the search feature of Autopsy will yield a list of files (deleted or intact). Further useful analysis can be provided by using the hexadecimal 'report' view of each file. As stated previously, deleted files did not prove much information in Autopsy. However, files in tact did yield useful information. File signature information is available in the hexadecimal header of the file. To the untrained eye, a renamed MP3 file will go unnoticed. However, if analyzing the header of the file, one can determine if this truly is a MP3 or an audio file at all. This is extremely important for an investigator to pay attention to, as the iPod will completely disregard any file without the correct file signature (including the portion in the file structure that holds the ID3 tag information). This could be an extremely useful place to hide files, due the lack of impact on the iPod's functionality and the low likelihood of an iPod being chosen for a Forensic investigation. In fact, placing files on an iPod truly isn't much different than saving files to a USB flash drive; they typically even share a common file system (FAT32).

Task 3: Key File Acquisition

SysInfo

The SysInfo file provides useful information, such as the serial number and model generation of the iPod. As previously stated, this can be useful under certain situations. The BASH script to follow will highlight some of the importance of this file.

iSync.vcf

An iPod user may wish to store contact information on their iPod for quick reference. In one of the acquired iPod images, iSync.vcf did exist, and provided user information that could be helpful in an investigation. Appendix Figure C.8 shows the HEX display of the file, and the contact information can be parsed from here. This is the primary virtual contact file, containing all information for the specified address book that is being synchronized to the iPod.

Task 4: Identifying Formatting and Host Computer Information

With information provided in the acquired iPod images, it is likely that the Host OS we are dealing with is Windows XP or earlier.

This is based upon the files gathered and the certain known information. The contacts taken from the iPod were formatted in a fashion that would suggest Outlook Express was used. This indicates that the OS cannot be newer than Windows XP if at all a Microsoft OS. This is based upon the fact that Vista does not have Outlook Express built in.

However, with applications such as WINE that act as a Windows emulated environment in *NIX operating systems, it would be unjust to base our conclusions solely on these facts.

Task 5: Additional Forensic Tasks – Owner Identification

Due to the nature of this investigation, the tools utilized could not exactly identify the owner of the iPod, but instead leaves it up to the investigator to make an educated guess.

The word documents on the iPod contain information on the computer to which the Word documents were generated. This does not necessarily identify the user (in fact, this information is often bogus), but it is a good starting point. Appendix C.9 shows the name associated with a particular seized Word file in the file's header (screenshot taken within Autopsy).

Forensic Script

In addition to the manual investigation, we attempted to create a script that would be useful in quickly obtaining some key information. The script is based upon some of the manual analysis techniques, but streamlines the process. This can be used to quickly create an inventory record and overview of the iPod to be used in a comprehensive investigation. The script is currently limited to the available test images. Other useful information can be added to the script; however, this would first require an analysis of a more comprehensive set of images. This is because there are various way of interacting with an iPod, including third party syncing tools and alternate operating systems. As each of these individual cases is analyzed, the script can be enhanced to automatically perform the necessary analysis.

For the current version of the script, two forensics images were used. The first image was made on a freshly formatted iPod that was only connected to a Linux operating system in hard drive mode. The second test image was of a different iPod that was managed over time using GTKPod (http://www.gtkpod.org/about.html) on a Linux operating system. This second image presented some different modifications and artifacts on the iPod's operating system, which were not documented in previous forensics research.

The script is designed to run in a BASH shell on a Linux operating system. Various command line system utilities are used in the process. In addition, the script uses Sleuthkit (Version 3.0.1) on the command line in order to pull information out of the image file without mounting it locally. The script could be ported to other operating environments as long as all the command line tools and Sleuthkit is available. Other versions of Sleuthkit were not tested.

The script currently checks for Deleted Files and Trash files on the iPod image and will extract the contents of Key data files. The script itself is presented below in addition to sample outputs:

Script

```
#!/bin/bash

##########Notes#########################################
#Script does not run in interactive mode, simply pass an image of an iPod to the program and it
will attempt to find some useful information for cataloging and the primary investigation.  This
program is not designed to replace a full human audit as it is limited to previously known and
researched scenarios
#This is version: 0.9.5 (2009-19-Feb)
#Written by Eric Goldman
########################################################

###########Preliminary Checks Before running###########
if [ $#  != 1 ]
then
        echo "Usage: bash iPod-inventory name-of-dd.img";
        exit;
fi
if [ ! -f $1 ]
then
        echo "You did not provide a valid file.";
        exit;
fi
########################################################

####Global Variables###################################
LINE="-----------------------------------------------";
SPACER=$'\n';
```

```
#iPodImage=$1  #list as absolute path instead
D=`dirname "$1"`; B=`basename "$1"`;
iPodImage="`cd \"$D\" 2>/dev/null && pwd || echo \"$D\"`/$B";

#####################################################

#####Basic Forensic Data##############################
echo "$SPACER$LINE";
echo "Basic Image Cataloging Information $SPACER";
echo "iPod Image Being Cataloging: $iPodImage";
echo "MD5 Hash: ` md5sum $iPodImage | cut -d " " -f 1`";
echo "SHA1 Hash: ` sha1sum $iPodImage | cut -d " " -f 1`";
echo "";
echo "File System Type: ` fsstat -t $iPodImage `";
echo "--Likely host PC type(s)--"
#Windows and Mac test are not yet developd because we only had linux-created test iPods
##According to some documents, it seem a file 'iPod_Control/iTunes/winPrefs' is created during
some iTunes process on windows, but we could not verify this with our test machines, the test
would be similar to below with ifind check
#Linux Test - Looking for GTKPod Preference file on iPod
onLinux=`ifind $iPodImage -n "iPod_Control/iTunes/gtkpod.prefs"`;
echo "Linux: `if [[ "$onLinux" =~ [0-9][0-9]* ]]; then echo "Yes"; else echo "No"; fi;`";
#Further research on the time stamp would be good, but no further with our current test cases:
http://www.iPodlinux.org/wiki/ITunesDB/Misc._Files#Preferences

#####################################################

#####Key Forensic Files##############################
echo "$SPACER$SPACER$LINE";
echo "Key Files $SPACER";
echo "-----SysInfo------";
SysInfoInode=`ifind $iPodImage -n "/iPod_Control/Device/SysInfo"`;
if [[ $SysInfoInode  =~ [0-9][0-9]* ]]; then icat $iPodImage $SysInfoInode; else echo "The
SysInfo File was not present"; fi;
echo "$SPACER-----DeviceInfo----";
deviceInfoInode=`ifind $iPodImage -n "/iPod_Control/iTunes/DeviceInfo"`
if [[ $deviceInfoInode =~ [0-9][0-9]* ]]; then icat $iPodImage $deviceInfoInode; else echo "The
DeviceInfo File was not present"; fi;
#Add other important common files here

#####################################################

#####Deleted Files###################################
echo "$SPACER$SPACER$LINE";
echo "---Deleted Files----$SPACER";
fls -rd $iPodImage;
echo " ";
echo "*Note: You may want to manually look at the following directories if present and do further
analysis: \$OrphanFiles, .Trash*, .*";

##Incase you want to see a more complicated way, we can select the known Trash folders and other
"deleted" folders which are still visible and pop these out as well with the following code:
#$TrashFolders=`fls $iPodImage -p | grep Trash | grep ^d/d | sed 's/\(d\/d\s\)\(.[0-
9]\)\(.*\)/\2/'`
#for inode in $TrashFolders; do echo $'\n\n'"-----------------------"; istat $iPodImage $inode;
echo $'\n\n'"Files in this Trash Directory:"; fls -p $iPodImage $inode; done;
#should also obviously be checked with ils when doing full audit

#####################################################

#####Contact/Calendar Files Report###################
echo "$SPACER$SPACER$LINE";
echo "PIM Files Found$SPACER";
echo "-----Contacts------";
contactsInode=`ifind $iPodImage -n "/Contacts"`;
if [[ $contactsInode  =~ [0-9][0-9]* ]]; then fls $iPodImage $contactsInode | grep ".vcf"; else
echo "The Standard Contacts Folder was not present"; fi;
echo " ";
#Calendar Data not available for testing
echo "----Calendar-----"
calendarInode=`ifind $iPodImage -n "/Calendars"`;
```

```
if [[ $calendarInode  =~ [0-9][0-9]* ]]; then fls $iPodImage $calendarInode | grep ".ical"; else
echo "The Standard Calendar Folder was not present"; fi;
echo " ";
echo "*Note: You should run further tests to see if these are valid PIM files.  There may also be
non PIM files hidden here.";

##################################################
```

Example Output 1

```
-------------------------------------------------
Basic Image Cataloging Information

iPod Image Being Cataloging: /forensics/images/iPod_A.img
MD5 Hash: df0729bd417bbaac5cf32bb890a77ad3
SHA1 Hash: bd6a464a50d314bb7bad862d1621080cf493e8aa

File System Type: fat32
--Likely host PC type(s)--
Linux: No


-------------------------------------------------
Key Files

-----SysInfo------
BoardHwName: iPod Q21
pszSerialNumber: JQ4465XJPS9
ModelNumStr: M9282
FirewireGuid: 0x000A270002B8418B
HddFirmwareRev: BM111A
RegionCode: LL(0x0001)
PolicyFlags: 0x00000000
buildID: 0x03118000 (3.1.1)
visibleBuildID: 0x03118000 (3.1.1)
boardHwRev: 0x00000000 (0.0 0)
boardHwSwInterfaceRev: 0x00050013 (0.0.5 19)
bootLoaderImageRev: 0x00000000 (0.0 0)
diskModeImageRev: 0x00000000 (0.0 0)
diagImageRev: 0x00000000 (0.0 0)
osImageRev: 0x00000000 (0.0 0)
iPodFamily: 0x00000004
updaterFamily: 0x00000004




-----DeviceInfo----
The DeviceInfo File was not present


-------------------------------------------------
---Deleted Files----

r/r * 278:     iPod_Control/iTunes/iTunesLock
r/r * 287:     iPod_Control/iTunes/Temp File.tmp
r/r * 290:     iPod_Control/iTunes/_EMPFI~1.TMP
r/r * 310:     iPod_Control/Music/F00/04 Honor.mp3
r/r * 314:     iPod_Control/Music/F00/01 Black Thunder.mp3
r/r * 327:     iPod_Control/Music/F01/01 Track 01.mp3
r/r * 331:     iPod_Control/Music/F01/06 No Heroes.mp3
r/r * 332:     iPod_Control/Music/F01/_AXB.mp3
r/r * 343:     iPod_Control/Music/F02/09 How Qui.mp3
r/r * 186:     iPod_Control/Music/F05/ASDF.doc
r/r * 188:     iPod_Control/Music/F05/ASDX.doc
d/d * 297:     iPod_Control/Music/_EWFOL~1
r/r * 8631:    iPod_Control/Music/F03/secret_hideout.mp3
d/d * 300:     iPod_Control/Music/New Folder
r/r * 1048631: iPod_Control/Music/F04/secret_information.mp3
d/d * 304:     iPod_Control/Music/untitled folder
r/r * 79:      Contacts/Temp File.tmp
```

```
r/r * 81:      Contacts/Temp File.tmp

*Note: You may want to manually look at the following directories if present and do further
analysis: $OrphanFiles, .Trash*, .*


-------------------------------------------------
PIM Files Found

-----Contacts------
r/r 72: iPod_created_instructions.vcf
r/r 75: iPod_created_sample.vcf
r/r 77: iSync.vcf

----Calendar-----

*Note: You should run further tests to see if these are valid PIM files.  There may also be non
PIM files hidden here.
```

Example Output 2

```
-------------------------------------------------
Basic Image Cataloging Information

iPod Image Being Cataloging: /forensics/images/iPod_B.img
MD5 Hash: 2d58d084af0f19038138ef84cb0519a3
SHA1 Hash: f2b5c32a8c941e6ae330623627821050f9193b73

File System Type: fat32
--Likely host PC type(s)--
Linux: Yes


-------------------------------------------------
Key Files

-----SysInfo------
ModelNumStr: xA107

-----DeviceInfo----
The DeviceInfo File was not present


-------------------------------------------------
---Deleted Files----

r/r * 1686:    iPod_Control/iTunes/_TGPLA~1
r/r * 1694:    iPod_Control/iTunes/Temp File.tmp
r/r * 1695:    iPod_Control/iTunes/_TUNES~4
r/r * 1697:    iPod_Control/iTunes/Temp File
r/r * 1699:    iPod_Control/iTunes/iTunesPrefs
r/r * 1701:    iPod_Control/iTunes/Temp File
r/r * 1703:    iPod_Control/iTunes/iTunesPrefs
r/r * 1705:    iPod_Control/iTunes/iTunesLock
r/r * 1707:    iPod_Control/iTunes/iTunesPrefs
r/r * 1710:    iPod_Control/iTunes/iTunesPlaylists
r/r * 1712:    iPod_Control/iTunes/Temp File
r/r * 83886124:       iPod_Control/Music/F00/gtkpod610293.mp3
r/r * 839278:  iPod_Control/Artwork/Temp File
r/r * 3402384: .Trash-jeff/PIHS.mp3
r/r * 3402386: .Trash-jeff/NLQZ.mp3
d/d * 658054:  .Trashes/1378807646
r/r * 658056:  .Trashes/._1378807646
d/d * 21:      .fseventsd
r/r * 802823:  .fseventsd/fseventsd-uuid
r/r * 802826:  .fseventsd/0000000000001e6ee

*Note: You may want to manually look at the following directories if present and do further
analysis: $OrphanFiles, .Trash*, .*
```

```
-----------------------------------------------
PIM Files Found

-----Contacts------
r/r 520:       iPod_created_instructions.vcf
r/r 523:       iPod_created_sample.vcf

----Calendar-----

*Note: You should run further tests to see if these are valid PIM files.  There may also be non
PIM files hidden here.
```

Conclusions

The forensic investigation of an iPod can present a very difficult challenge for computer forensic investigators. Criminals who are clever enough to use the iPod to store information about their crimes will also likely know how to obfuscate their data or use steganography. Compared to a complete PC host, there are less common files and the file and directory structure is not as complicated. However, various programs interact with the iPod in different ways, leaving different artifacts on the iPod itself and on host machines. In addition, iPod-PC interactions can be very different depending on what application was used to sync data between the two. As a result, the forensic investigator must be prepared for a wide variety of situations. In the future, iPods and other "non-computer" digital devices will become more important to criminal investigations as criminals look for more deceptive and creative ways to hide their illegal activities.

References

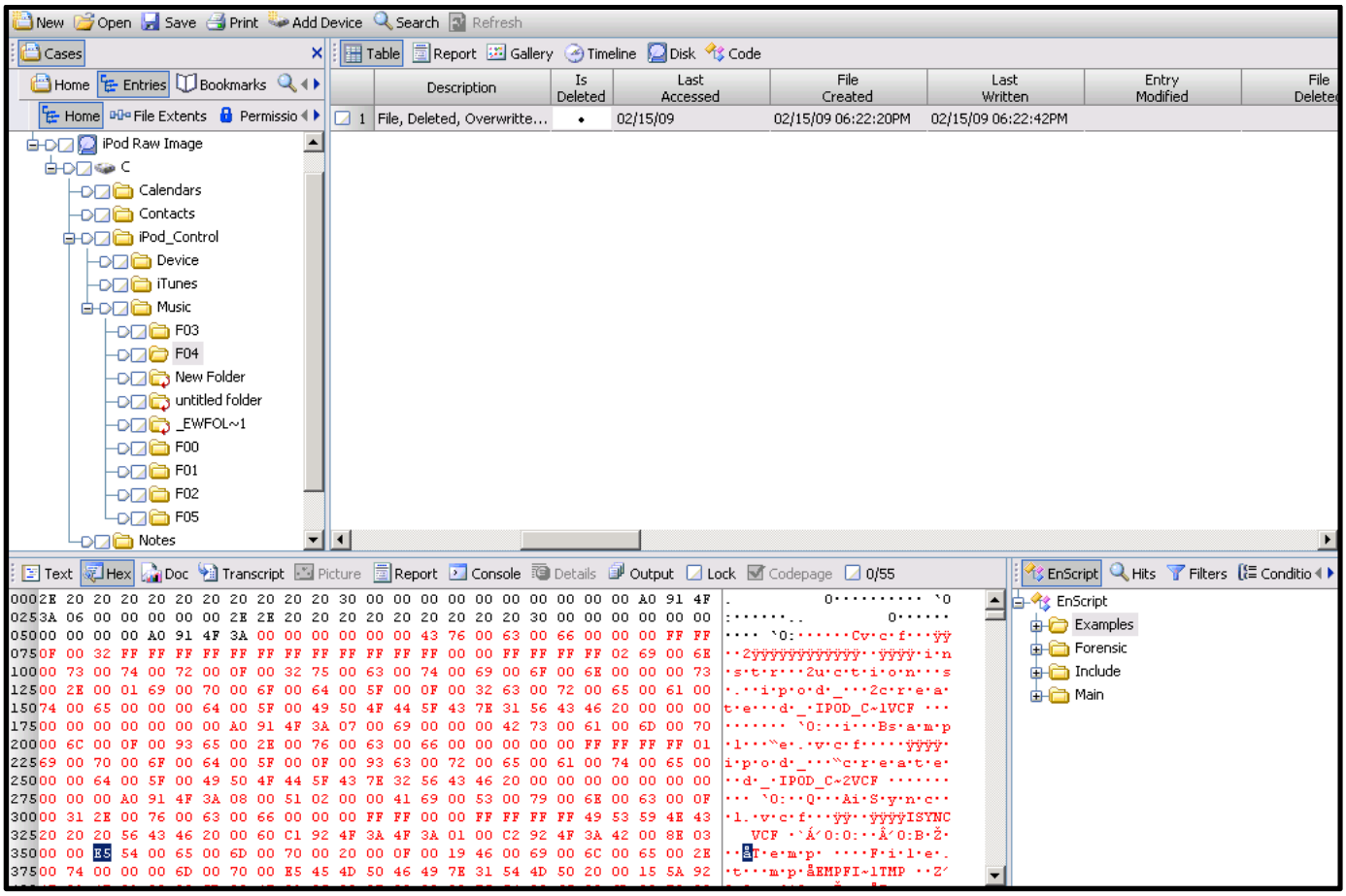
1. *iPod Forensics: Forensically Sound Examination of an Apple iPod.* **Slay, Dr. Jill and Przibilla, Andrew.** s.l. : IEEE, 2007. Proceedings of the 40th Hawaii International Conference on System Sciences. 0-7695-2755-8/07.

2. **Stern, Hadley.** Hacking iPod and iTunes. *O'Reilly.* [Online] O'Reilly Media, Inc., October 28, 2004. [Cited: February 10, 2009.] http://digitalmedia.oreilly.com/pub/a/oreilly/digitalmedia/2004/10/28/iPoditunes_hcks.html?page=3.

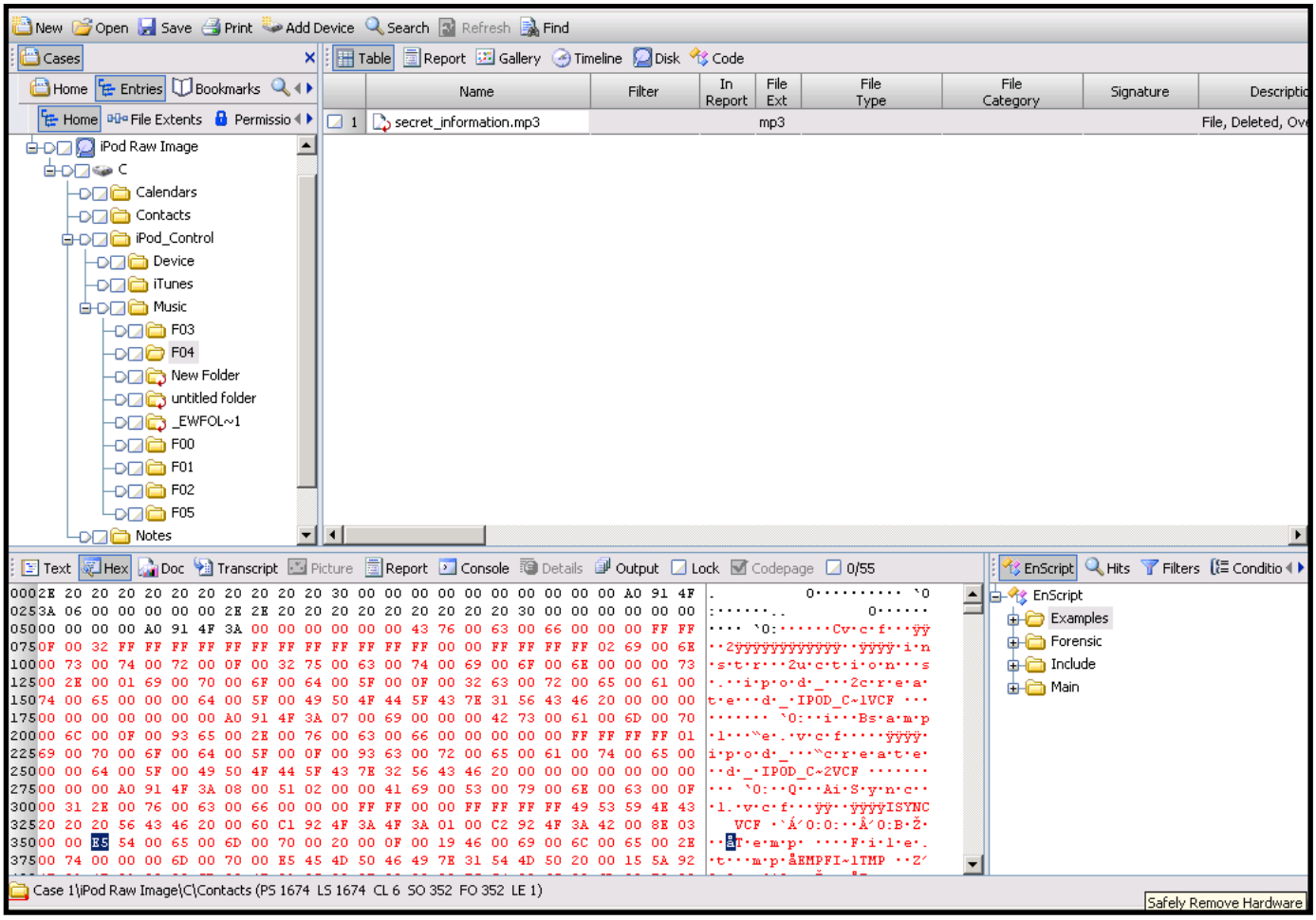
3. *iPod Forensics.* **Marisco, Christopher V. and Rogers, Marcus K.** 2, Fall 2005, International Journal of Digital Evidence, Vol. 4.

Appendix

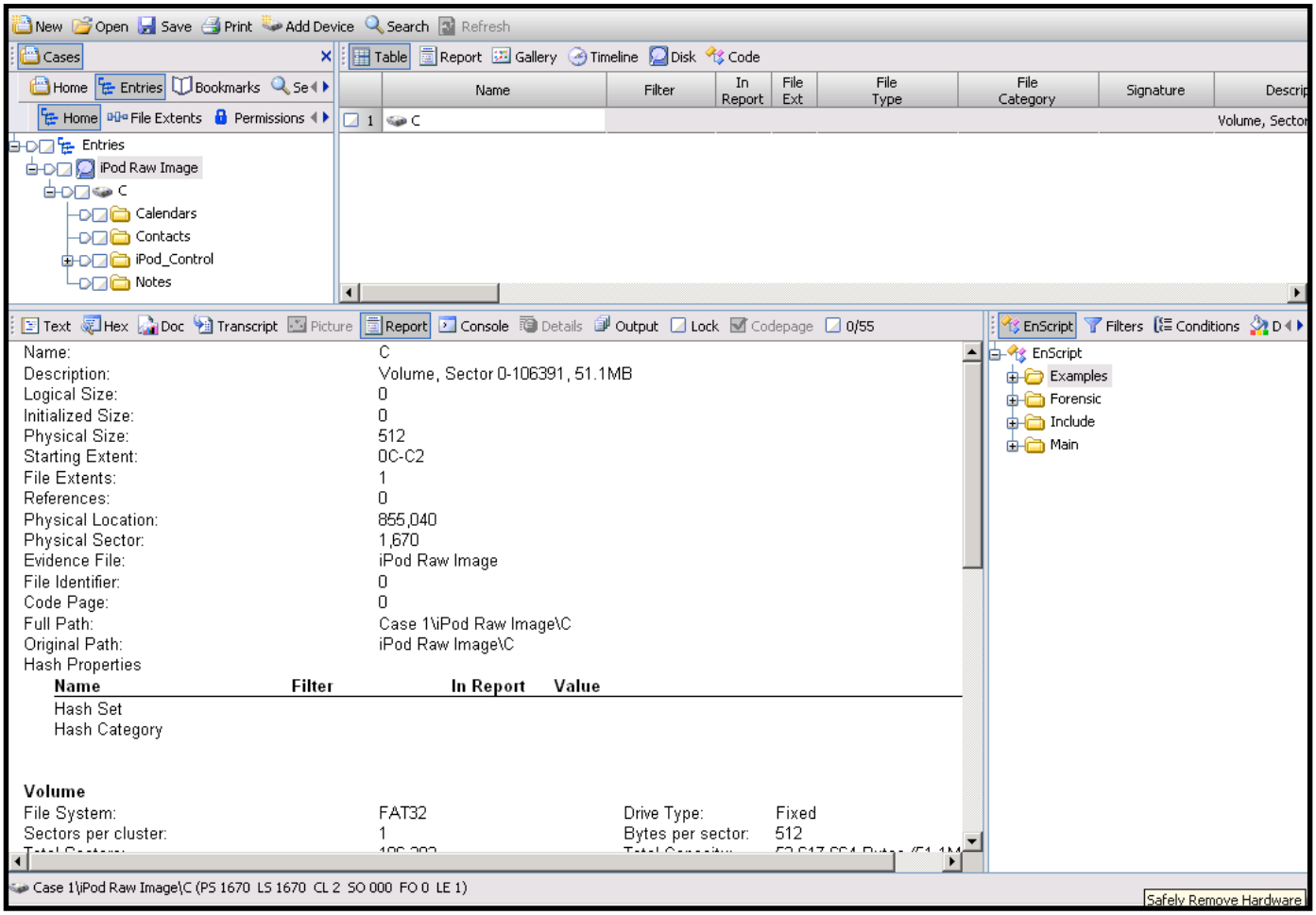
A.1


New
Open
Save
Print
Add Device
Search
Refresh
Cases
Table
Report
Gallery
Timeline
Disk
Code
Home
Entries
Bookmarks
File Extents
Permissio
Description
Is Deleted
Last Accessed
File Created
Last Written
Entry Modified
File Deleted
1
File, Deleted, Overwritte...
02/15/09
02/15/09 06:22:20PM
02/15/09 06:22:42PM
iPod Raw Image
C
Calendars
Contacts
iPod_Control
Device
iTunes
Music
F03
F04
New Folder
untitled folder
_EWFOL~1
F00
F01
F02
F05
Notes
Text
Hex
Doc
Transcript
Picture
Report
Console
Details
Output
Lock
Codepage
0/55
EnScript
Hits
Filters
Conditio
EnScript
Examples
Forensic
Include
Main

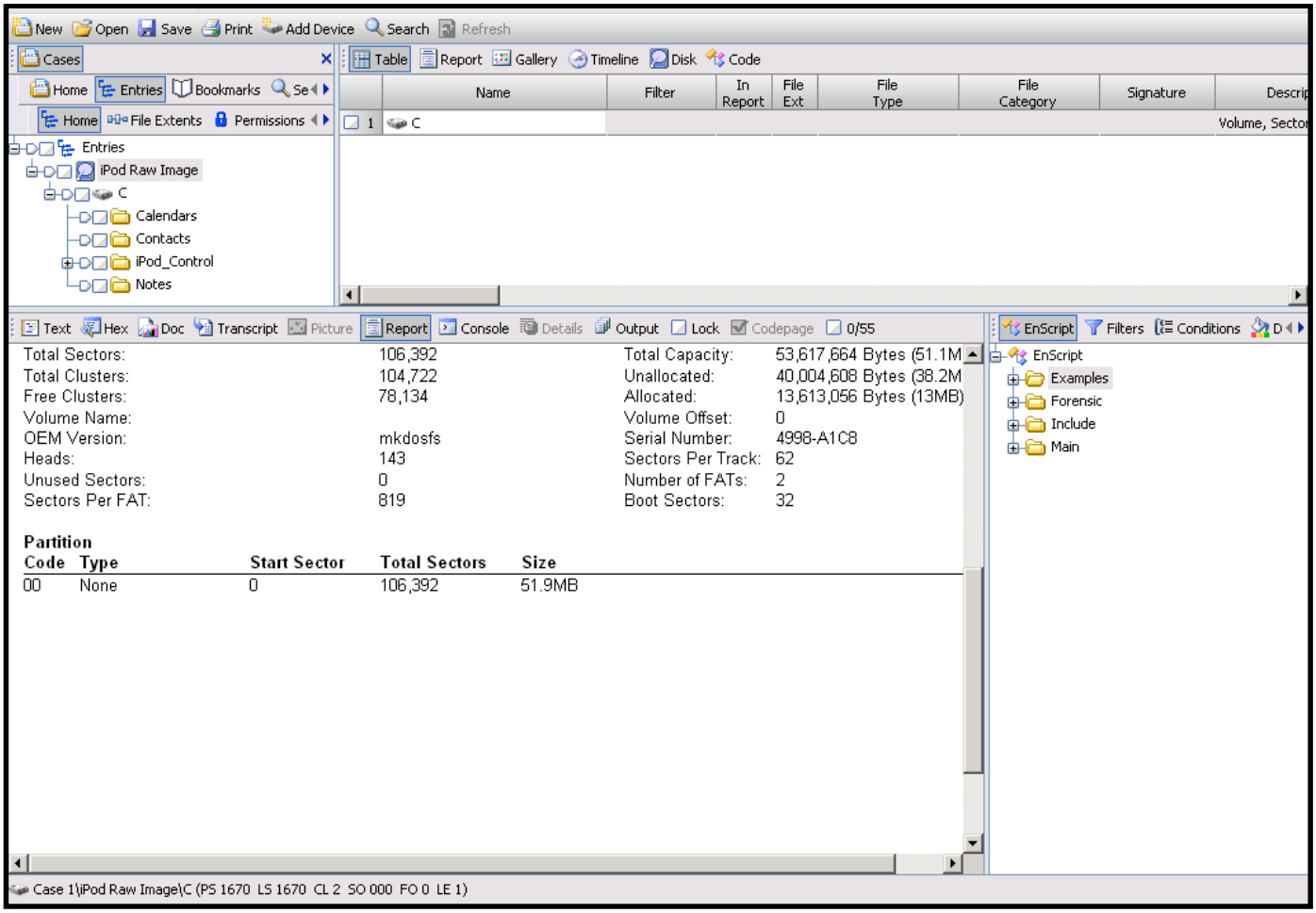
A.2


New Open Save Print Add Device Search Refresh Find
Cases
Home Entries Bookmarks
Home File Extents Permissio
iPod Raw Image
C
Calendars
Contacts
iPod_Control
Device
iTunes
Music
F03
F04
New Folder
untitled folder
_EWFOL~1
F00
F01
F02
F05
Notes
Table Report Gallery Timeline Disk Code
Name Filter In Report File Ext File Type File Category Signature Descriptio
1 secret_information.mp3 mp3 File, Deleted, Ov
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/55
EnScript Hits Filters Conditio
EnScript
Examples
Forensic
Include
Main
Case 1\iPod Raw Image\C\Contacts (PS 1674 LS 1674 CL 6 SO 352 FO 352 LE 1)
Safely Remove Hardware

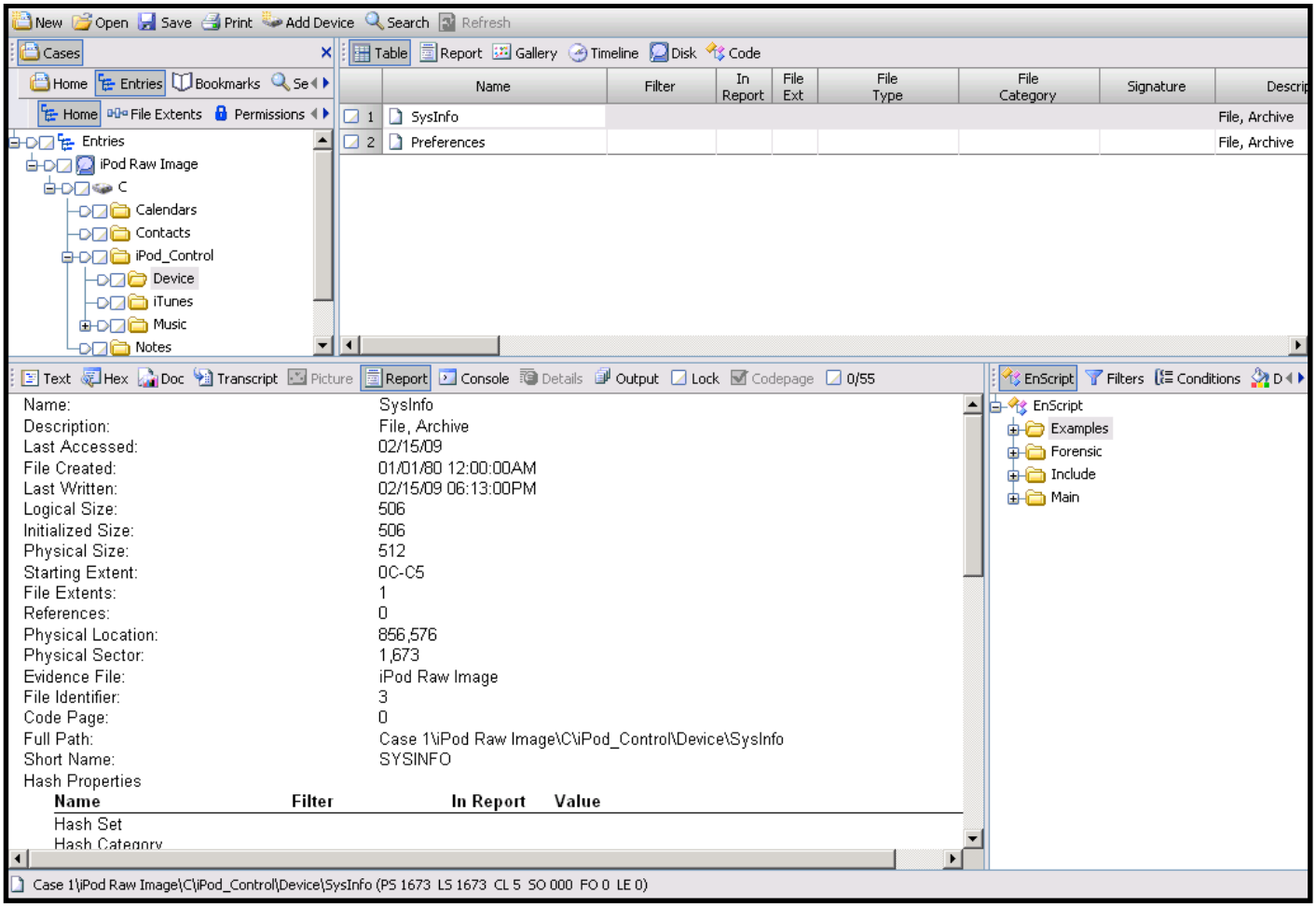
A.3


New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Se
Home File Extents Permissions
Entries
iPod Raw Image
C
Calendars
Contacts
iPod_Control
Notes
Table Report Gallery Timeline Disk Code
Name Filter In Report File Ext File Type File Category Signature Descrip
1 C
Volume, Sector
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/55
Name: C
Description: Volume, Sector 0-106391, 51.1MB
Logical Size: 0
Initialized Size: 0
Physical Size: 512
Starting Extent: 0C-C2
File Extents: 1
References: 0
Physical Location: 855,040
Physical Sector: 1,670
Evidence File: iPod Raw Image
File Identifier: 0
Code Page: 0
Full Path: Case 1\iPod Raw Image\C
Original Path: iPod Raw Image\C
Hash Properties
Name Filter In Report Value
Hash Set
Hash Category
Volume
File System: FAT32
Drive Type: Fixed
Sectors per cluster: 1
Bytes per sector: 512
EnScript Filters Conditions D
EnScript
Examples
Forensic
Include
Main
Case 1\iPod Raw Image\C (PS 1670 LS 1670 CL 2 SO 000 FO 0 LE 1)
Safely Remove Hardware

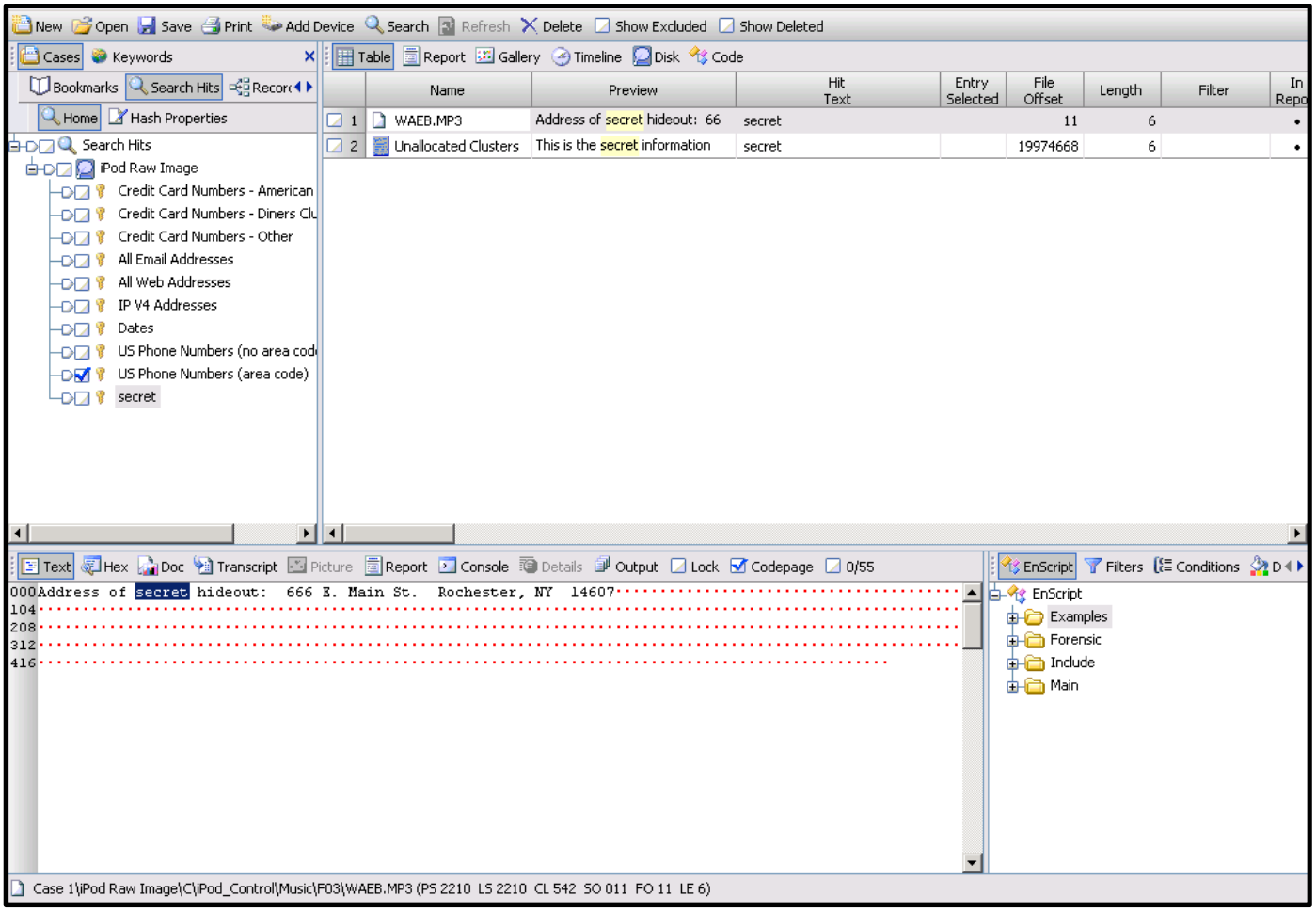
A.4


New Open Save Print Add Device Search Refresh
Cases
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks
Home File Extents Permissions
Entries
iPod Raw Image
C
Calendars
Contacts
iPod_Control
Notes
Name Filter In Report File Ext File Type File Category Signature
1 C
Volume, Sector
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/55
Total Sectors: 106,392
Total Clusters: 104,722
Free Clusters: 78,134
Volume Name:
OEM Version: mkdosfs
Heads: 143
Unused Sectors: 0
Sectors Per FAT: 819
Total Capacity: 53,617,664 Bytes (51.1M
Unallocated: 40,004,608 Bytes (38.2M
Allocated: 13,613,056 Bytes (13MB)
Volume Offset: 0
Serial Number: 4998-A1C8
Sectors Per Track: 62
Number of FATs: 2
Boot Sectors: 32
Partition
Code Type Start Sector Total Sectors Size
00 None 0 106,392 51.9MB
EnScript Filters Conditions
EnScript
Examples
Forensic
Include
Main
Case 1\iPod Raw Image\C (PS 1670 LS 1670 CL 2 SO 000 FO 0 LE 1)

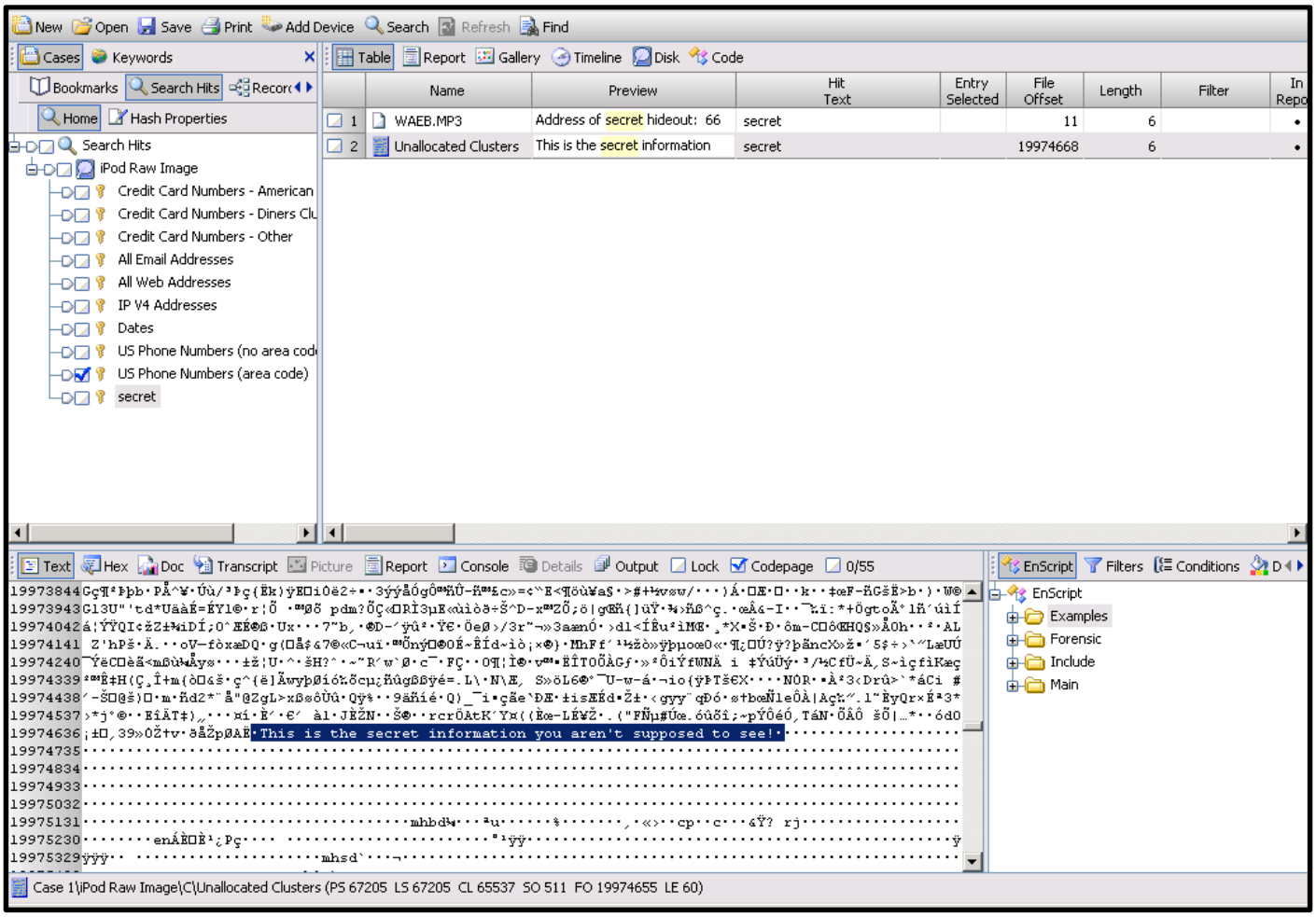
A.5


New Open Save Print Add Device Search Refresh
Cases
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks Se
Home File Extents Permissions
Entries
iPod Raw Image
C
Calendars
Contacts
iPod_Control
Device
iTunes
Music
Notes
Name Filter In Report File Ext File Type File Category Signature Descrip
1 SysInfo File, Archive
2 Preferences File, Archive
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/55
EnScript Filters Conditions D
EnScript
Examples
Forensic
Include
Main
Name: SysInfo
Description: File, Archive
Last Accessed: 02/15/09
File Created: 01/01/80 12:00:00AM
Last Written: 02/15/09 06:13:00PM
Logical Size: 506
Initialized Size: 506
Physical Size: 512
Starting Extent: 0C-C5
File Extents: 1
References: 0
Physical Location: 856,576
Physical Sector: 1,673
Evidence File: iPod Raw Image
File Identifier: 3
Code Page: 0
Full Path: Case 1\iPod Raw Image\C\iPod_Control\Device\SysInfo
Short Name: SYSINFO
Hash Properties
Name Filter In Report Value
Hash Set
Hash Category
Case 1\iPod Raw Image\C\iPod_Control\Device\SysInfo (PS 1673 LS 1673 CL 5 SO 000 FO 0 LE 0)

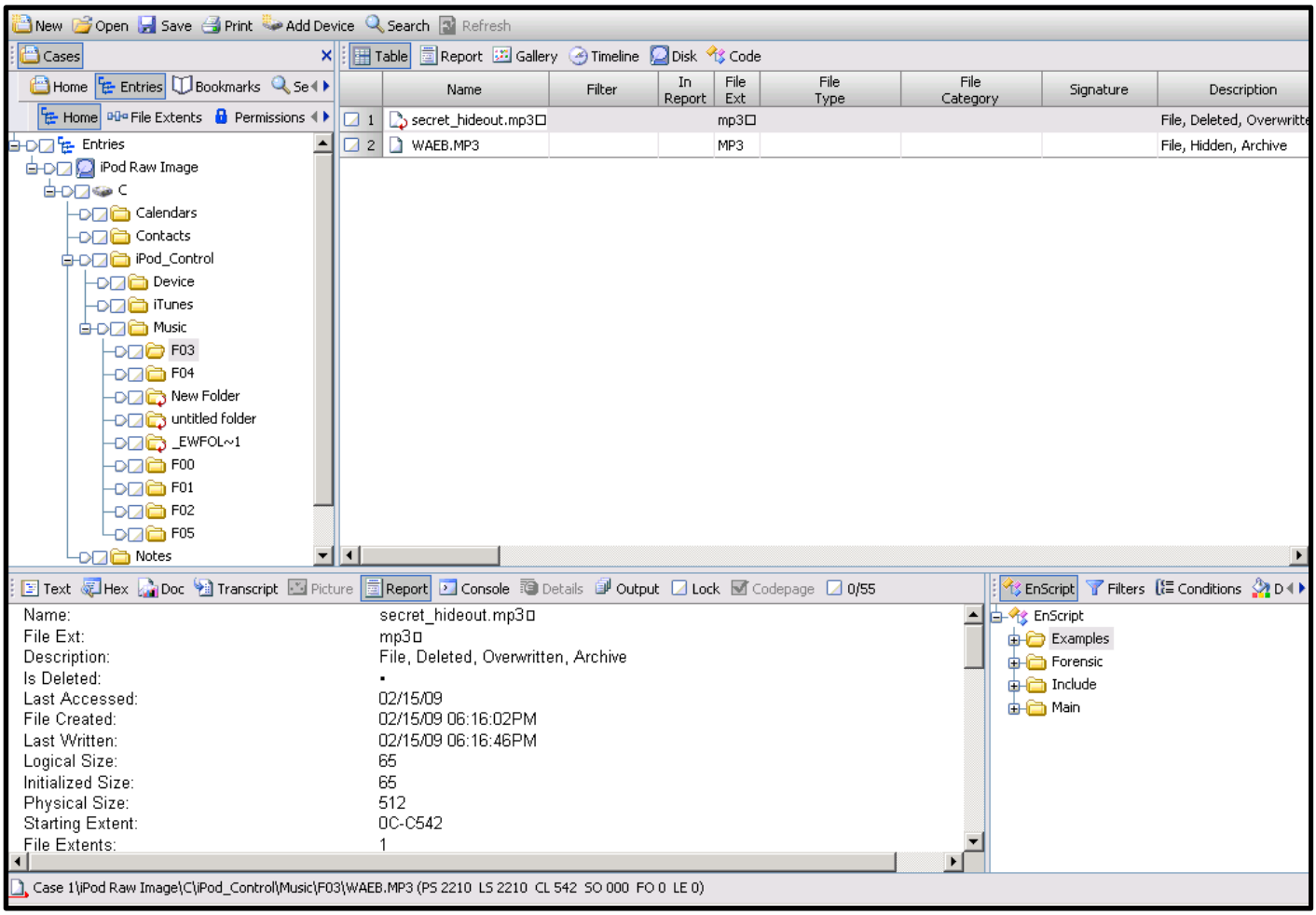
A.6


New Open Save Print Add Device Search Refresh Delete Show Excluded Show Deleted
Cases Keywords
Bookmarks Search Hits Recor
Home Hash Properties
Search Hits
iPod Raw Image
Credit Card Numbers - American
Credit Card Numbers - Diners Clu
Credit Card Numbers - Other
All Email Addresses
All Web Addresses
IP V4 Addresses
Dates
US Phone Numbers (no area cod
US Phone Numbers (area code)
secret
Table Report Gallery Timeline Disk Code
Name Preview Hit Text Entry Selected File Offset Length Filter In Repo
1 WAEB.MP3 Address of secret hideout: 66 secret 11 6
2 Unallocated Clusters This is the secret information secret 19974668 6
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/55
000 Address of secret hideout: 666 E. Main St. Rochester, NY 14607
104
208
312
416
EnScript Filters Conditions
EnScript
Examples
Forensic
Include
Main
Case 1\iPod Raw Image\C\iPod_Control\Music\F03\WAEB.MP3 (PS 2210 LS 2210 CL 542 SO 011 FO 11 LE 6)

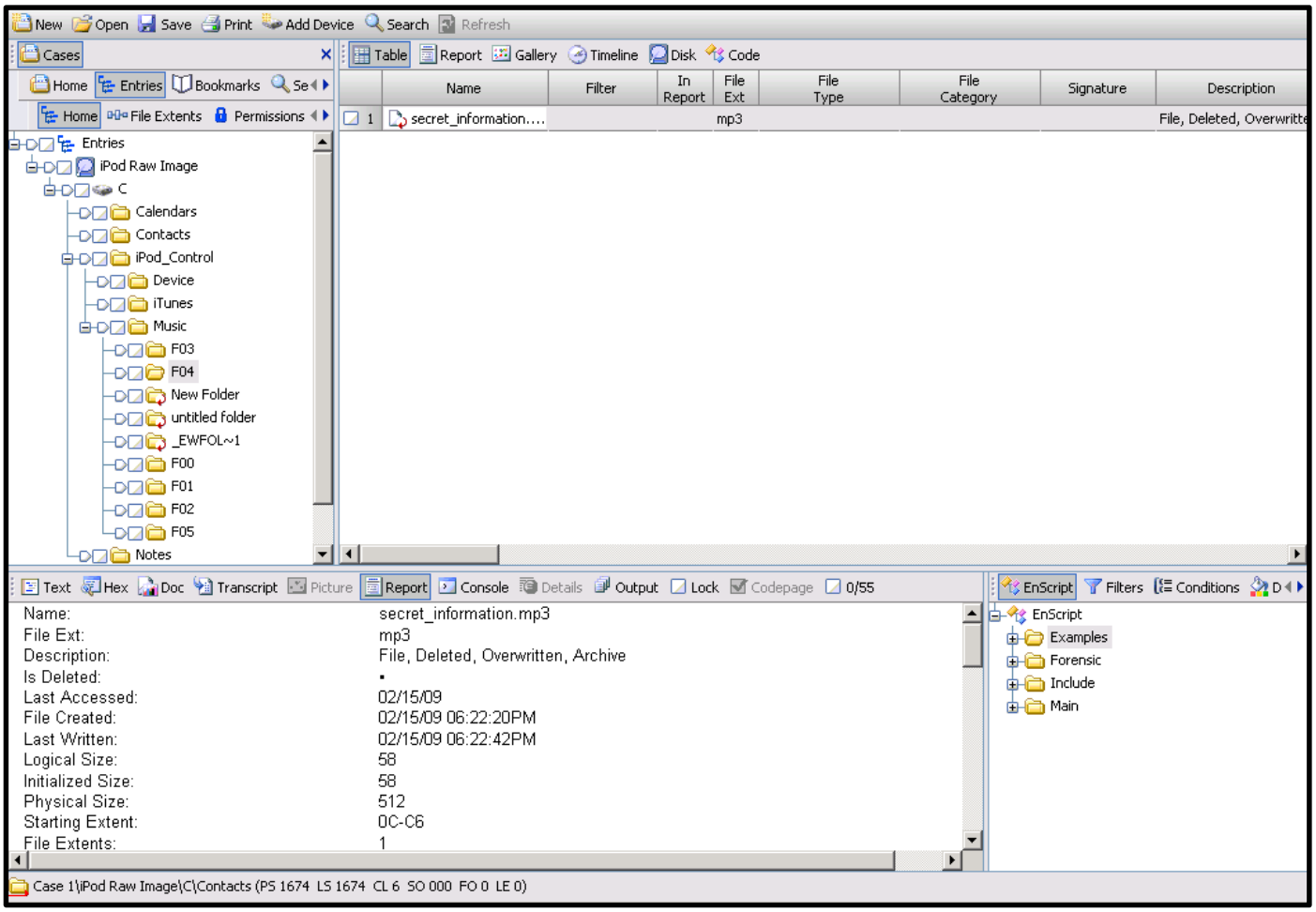
A.7


New Open Save Print Add Device Search Refresh Find
Cases Keywords
Bookmarks Search Hits Recor
Home Hash Properties
Search Hits
iPod Raw Image
Credit Card Numbers - American
Credit Card Numbers - Diners Cl
Credit Card Numbers - Other
All Email Addresses
All Web Addresses
IP V4 Addresses
Dates
US Phone Numbers (no area cod
US Phone Numbers (area code)
secret
Table Report Gallery Timeline Disk Code
Name Preview Hit Text Entry Selected File Offset Length Filter In Repo
1 WAEB.MP3 Address of secret hideout: 66 secret 11 6
2 Unallocated Clusters This is the secret information secret 19974668 6
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/55
This is the secret information you aren't supposed to see!
EnScript Filters Conditions
EnScript
Examples
Forensic
Include
Main
Case 1\iPod Raw Image\C\Unallocated Clusters (PS 67205 LS 67205 CL 65537 SO 511 FO 19974655 LE 60)

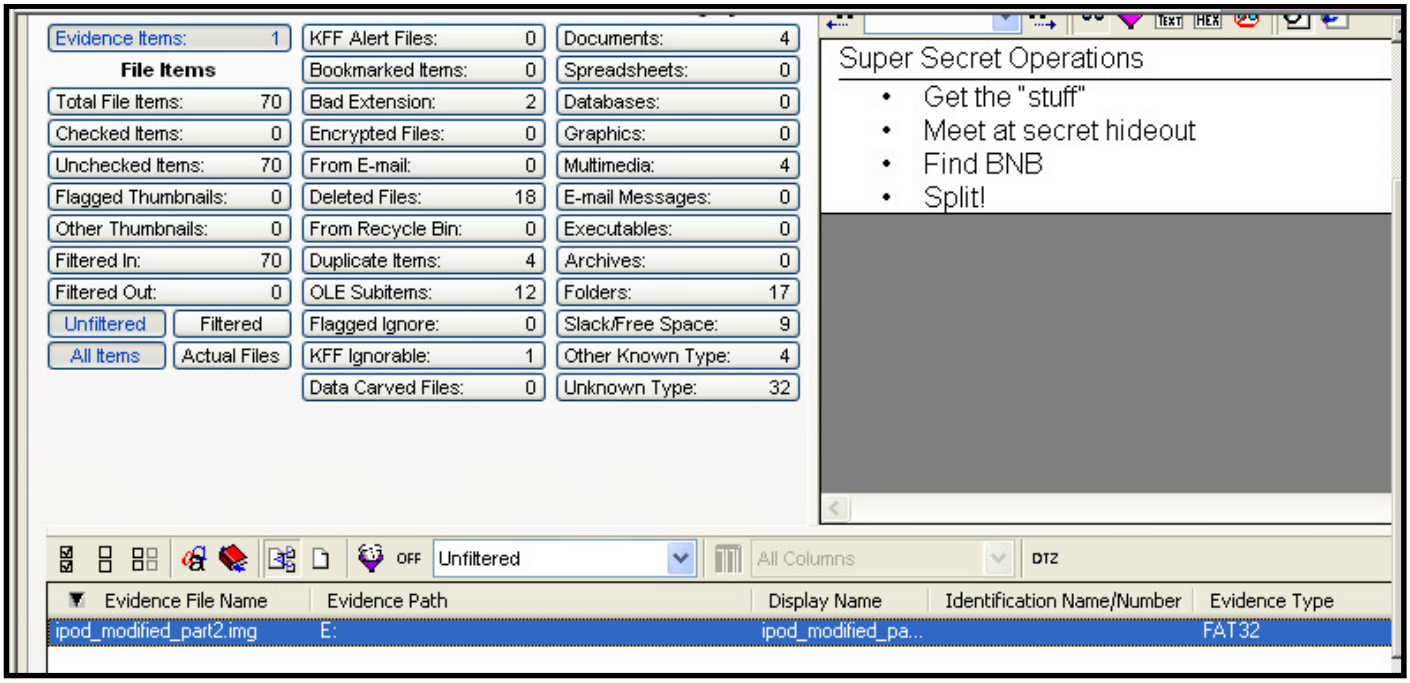
A.8


New Open Save Print Add Device Search Refresh
Cases
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks Se
Home File Extents Permissions
Entries
iPod Raw Image
C
Calendars
Contacts
iPod_Control
Device
iTunes
Music
F03
F04
New Folder
untitled folder
_EWFOL~1
F00
F01
F02
F05
Notes
Name Filter In Report File Ext File Type File Category Signature Description
1 secret_hideout.mp3 mp3 File, Deleted, Overwritte
2 WAEB.MP3 MP3 File, Hidden, Archive
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/55
EnScript Filters Conditions
EnScript
Examples
Forensic
Include
Main
Name: secret_hideout.mp3
File Ext: mp3
Description: File, Deleted, Overwritten, Archive
Is Deleted:
Last Accessed: 02/15/09
File Created: 02/15/09 06:16:02PM
Last Written: 02/15/09 06:16:46PM
Logical Size: 65
Initialized Size: 65
Physical Size: 512
Starting Extent: 0C-C542
File Extents: 1
Case 1\iPod Raw Image\C\iPod_Control\Music\F03\WAEB.MP3 (PS 2210 LS 2210 CL 542 SO 000 FO 0 LE 0)

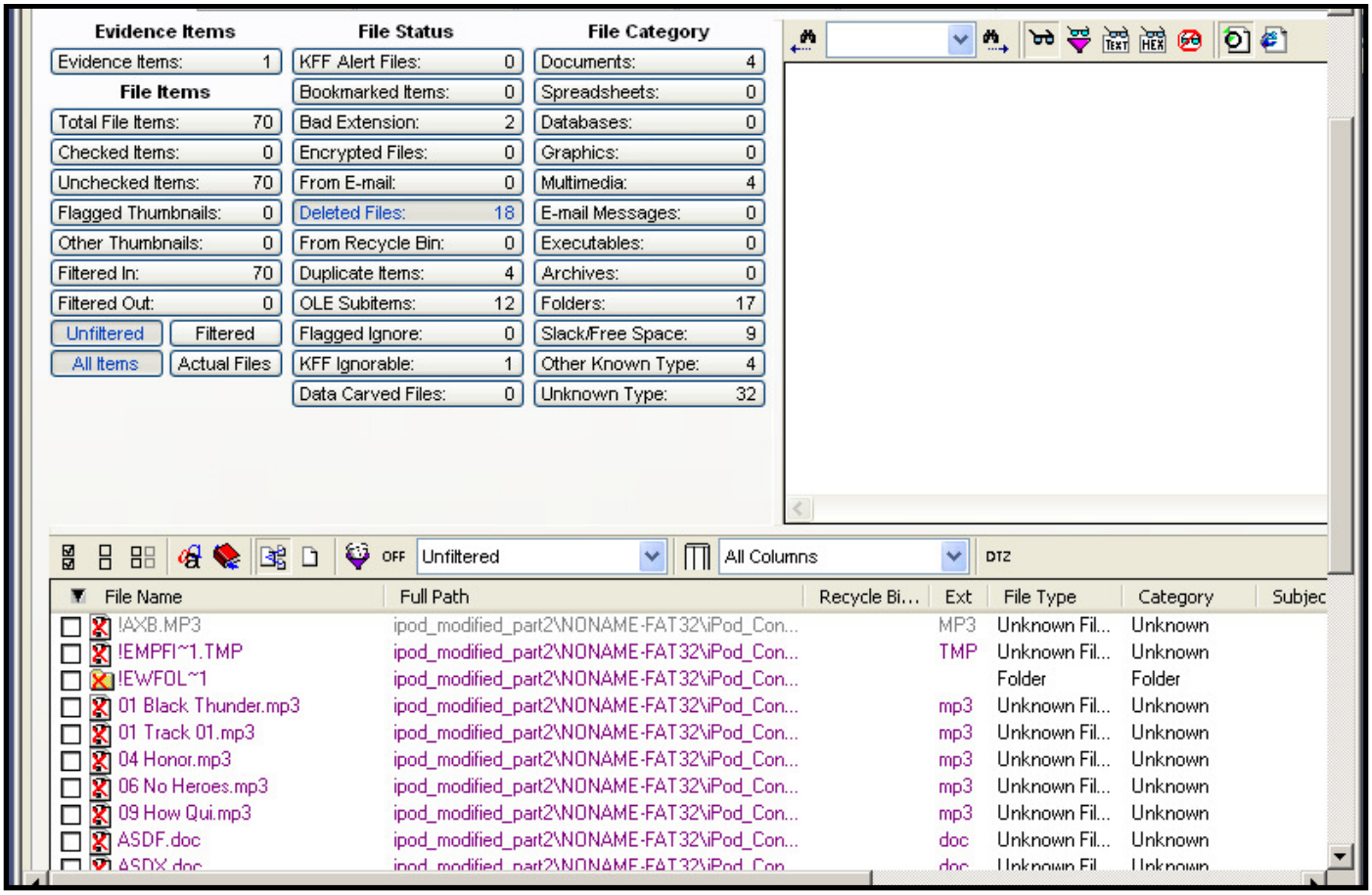
A.9


New
Open
Save
Print
Add Device
Search
Refresh
Cases
Table
Report
Gallery
Timeline
Disk
Code
Home
Entries
Bookmarks
Home
File Extents
Permissions
Name
Filter
In Report
File Ext
File Type
File Category
Signature
Description
1
secret_information....
mp3
File, Deleted, Overwritte
Entries
iPod Raw Image
C
Calendars
Contacts
iPod_Control
Device
iTunes
Music
F03
F04
New Folder
untitled folder
_EWFOL~1
F00
F01
F02
F05
Notes
Text
Hex
Doc
Transcript
Picture
Report
Console
Details
Output
Lock
Codepage
0/55
EnScript
Filters
Conditions
Name: secret_information.mp3
File Ext: mp3
Description: File, Deleted, Overwritten, Archive
Is Deleted:
Last Accessed: 02/15/09
File Created: 02/15/09 06:22:20PM
Last Written: 02/15/09 06:22:42PM
Logical Size: 58
Initialized Size: 58
Physical Size: 512
Starting Extent: 0C-C6
File Extents: 1
EnScript
Examples
Forensic
Include
Main
Case 1\iPod Raw Image\C\Contacts (PS 1674 LS 1674 CL 6 SO 000 FO 0 LE 0)

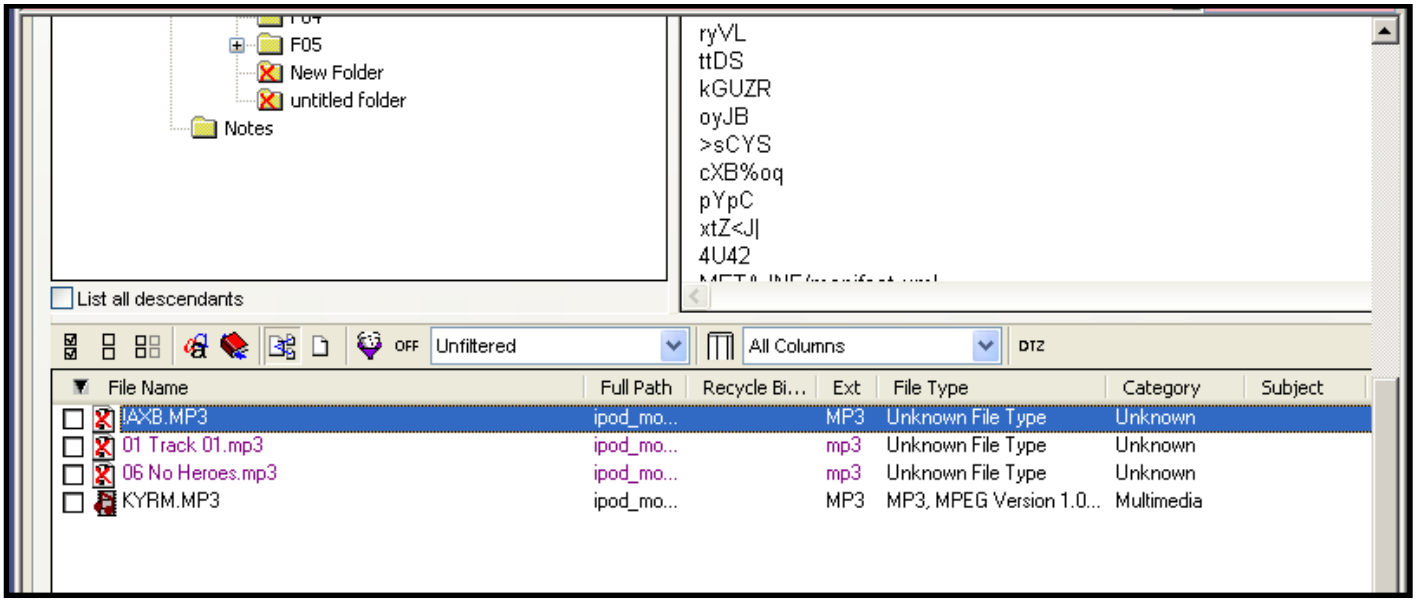
B.1


Evidence Items: 1
File Items
Total File Items: 70
Checked Items: 0
Unchecked Items: 70
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 70
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 2
Encrypted Files: 0
From E-mail: 0
Deleted Files: 18
From Recycle Bin: 0
Duplicate Items: 4
OLE Subitems: 12
Flagged Ignore: 0
KFF Ignorable: 1
Data Carved Files: 0
Documents: 4
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 4
E-mail Messages: 0
Executables: 0
Archives: 0
Folders: 17
Slack/Free Space: 9
Other Known Type: 4
Unknown Type: 32
Super Secret Operations
Get the "stuff"
Meet at secret hideout
Find BNB
Split!
OFF
Unfiltered
All Columns
DTZ
Evidence File Name
Evidence Path
Display Name
Identification Name/Number
Evidence Type
ipod_modified_part2.img
E:
ipod_modified_pa...
FAT32

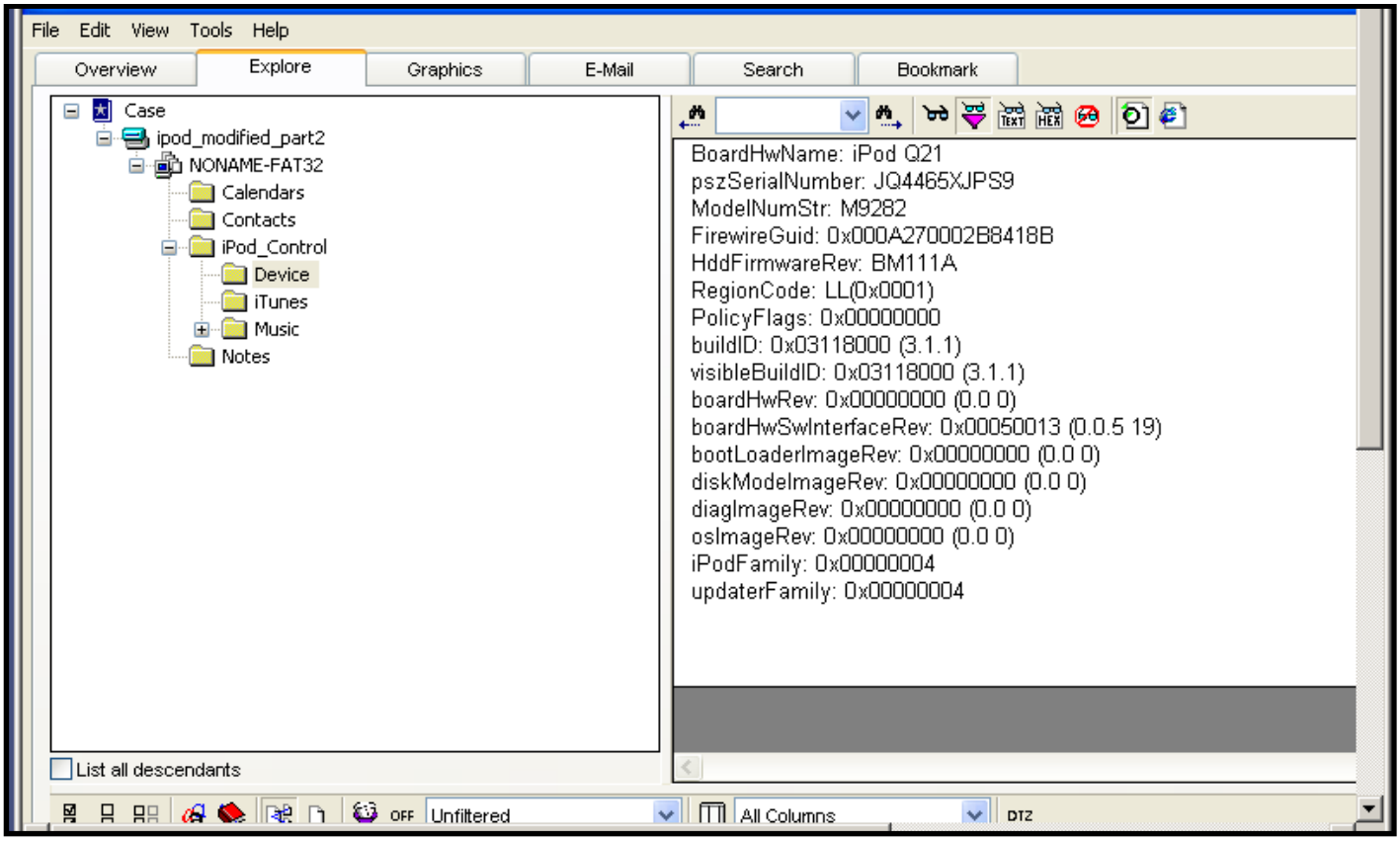
B.2


Evidence Items
Evidence Items: 1
File Items
Total File Items: 70
Checked Items: 0
Unchecked Items: 70
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 70
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 2
Encrypted Files: 0
From E-mail: 0
Deleted Files: 18
From Recycle Bin: 0
Duplicate Items: 4
OLE Subitems: 12
Flagged Ignore: 0
KFF Ignorable: 1
Data Carved Files: 0
File Category
Documents: 4
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 4
E-mail Messages: 0
Executables: 0
Archives: 0
Folders: 17
Slack/Free Space: 9
Other Known Type: 4
Unknown Type: 32
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subjec
!AXB.MP3 ipod_modified_part2\NONAME-FAT32\iPod_Con... MP3 Unknown Fil... Unknown
!EMPFI~1.TMP ipod_modified_part2\NONAME-FAT32\iPod_Con... TMP Unknown Fil... Unknown
!EWFOL~1 ipod_modified_part2\NONAME-FAT32\iPod_Con... Folder Folder
01 Black Thunder.mp3 ipod_modified_part2\NONAME-FAT32\iPod_Con... mp3 Unknown Fil... Unknown
01 Track 01.mp3 ipod_modified_part2\NONAME-FAT32\iPod_Con... mp3 Unknown Fil... Unknown
04 Honor.mp3 ipod_modified_part2\NONAME-FAT32\iPod_Con... mp3 Unknown Fil... Unknown
06 No Heroes.mp3 ipod_modified_part2\NONAME-FAT32\iPod_Con... mp3 Unknown Fil... Unknown
09 How Qui.mp3 ipod_modified_part2\NONAME-FAT32\iPod_Con... mp3 Unknown Fil... Unknown
ASDF.doc ipod_modified_part2\NONAME-FAT32\iPod_Con... doc Unknown Fil... Unknown

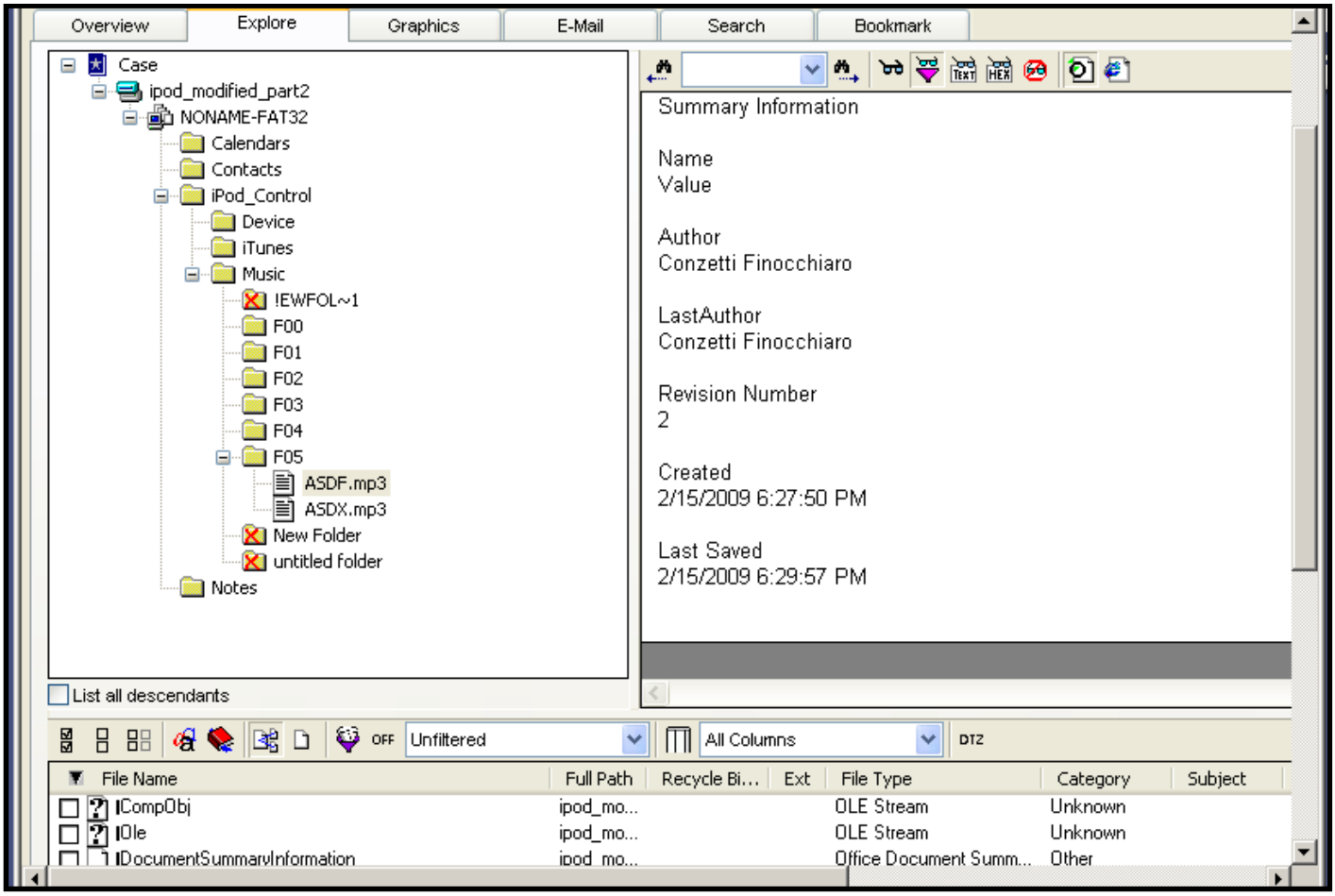
B.3


F05
New Folder
untitled folder
Notes
ryVL
ttDS
kGUZR
oyJB
>sCYS
cXB%oq
pYpC
xtZ<J|
4U42
List all descendants
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
!AXB.MP3 ipod_mo... MP3 Unknown File Type Unknown
01 Track 01.mp3 ipod_mo... mp3 Unknown File Type Unknown
06 No Heroes.mp3 ipod_mo... mp3 Unknown File Type Unknown
KYRM.MP3 ipod_mo... MP3 MP3, MPEG Version 1.0... Multimedia

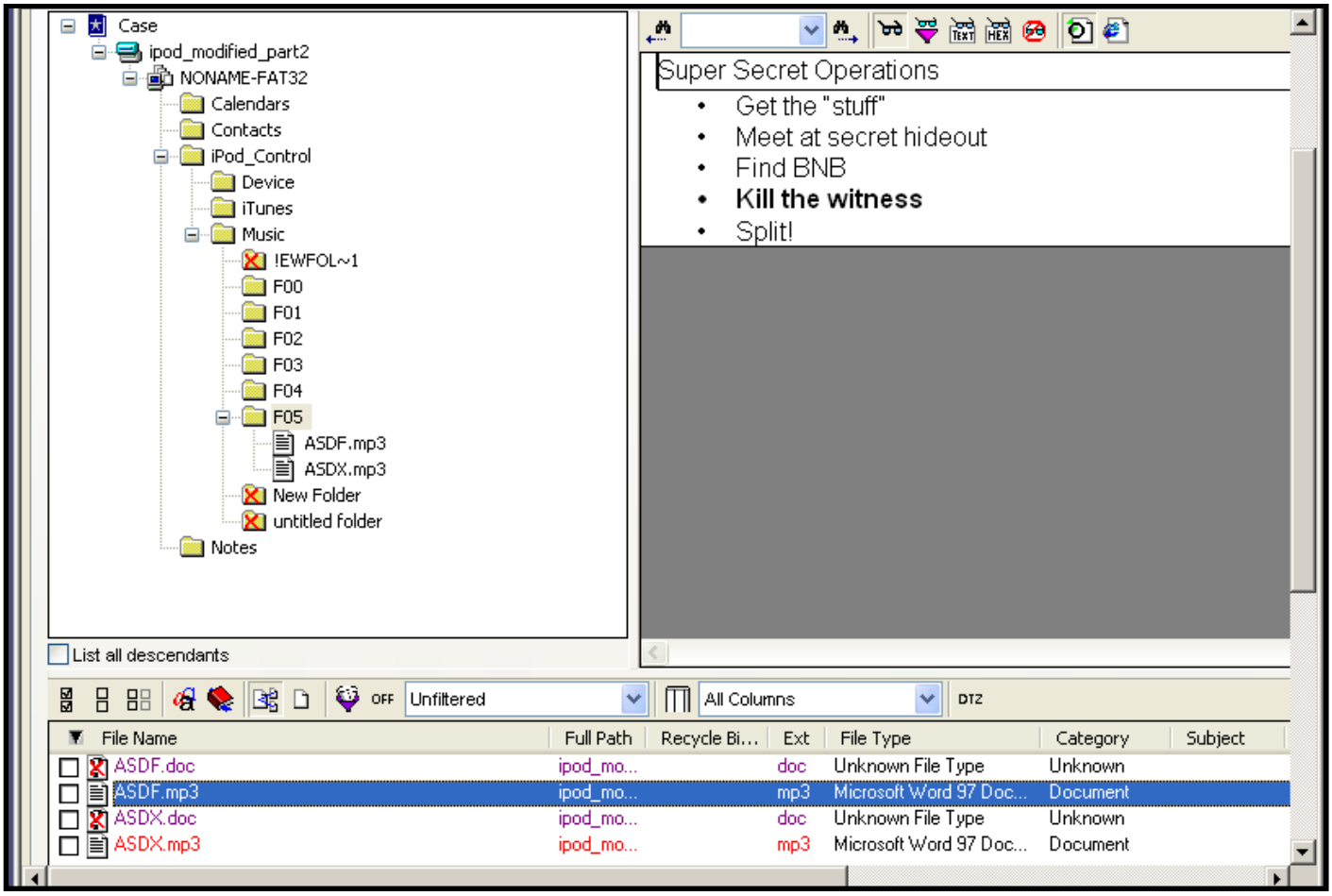
B.4


File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Case
ipod_modified_part2
NONAME-FAT32
Calendars
Contacts
iPod_Control
Device
iTunes
Music
Notes
List all descendants
BoardHwName: iPod Q21
pszSerialNumber: JQ4465XJPS9
ModelNumStr: M9282
FirewireGuid: 0x000A270002B8418B
HddFirmwareRev: BM111A
RegionCode: LL(0x0001)
PolicyFlags: 0x00000000
buildID: 0x03118000 (3.1.1)
visibleBuildID: 0x03118000 (3.1.1)
boardHwRev: 0x00000000 (0.0 0)
boardHwSwInterfaceRev: 0x00050013 (0.0.5 19)
bootLoaderImageRev: 0x00000000 (0.0 0)
diskModeImageRev: 0x00000000 (0.0 0)
diagImageRev: 0x00000000 (0.0 0)
osImageRev: 0x00000000 (0.0 0)
iPodFamily: 0x00000004
updaterFamily: 0x00000004
OFF
Unfiltered
All Columns
DTZ

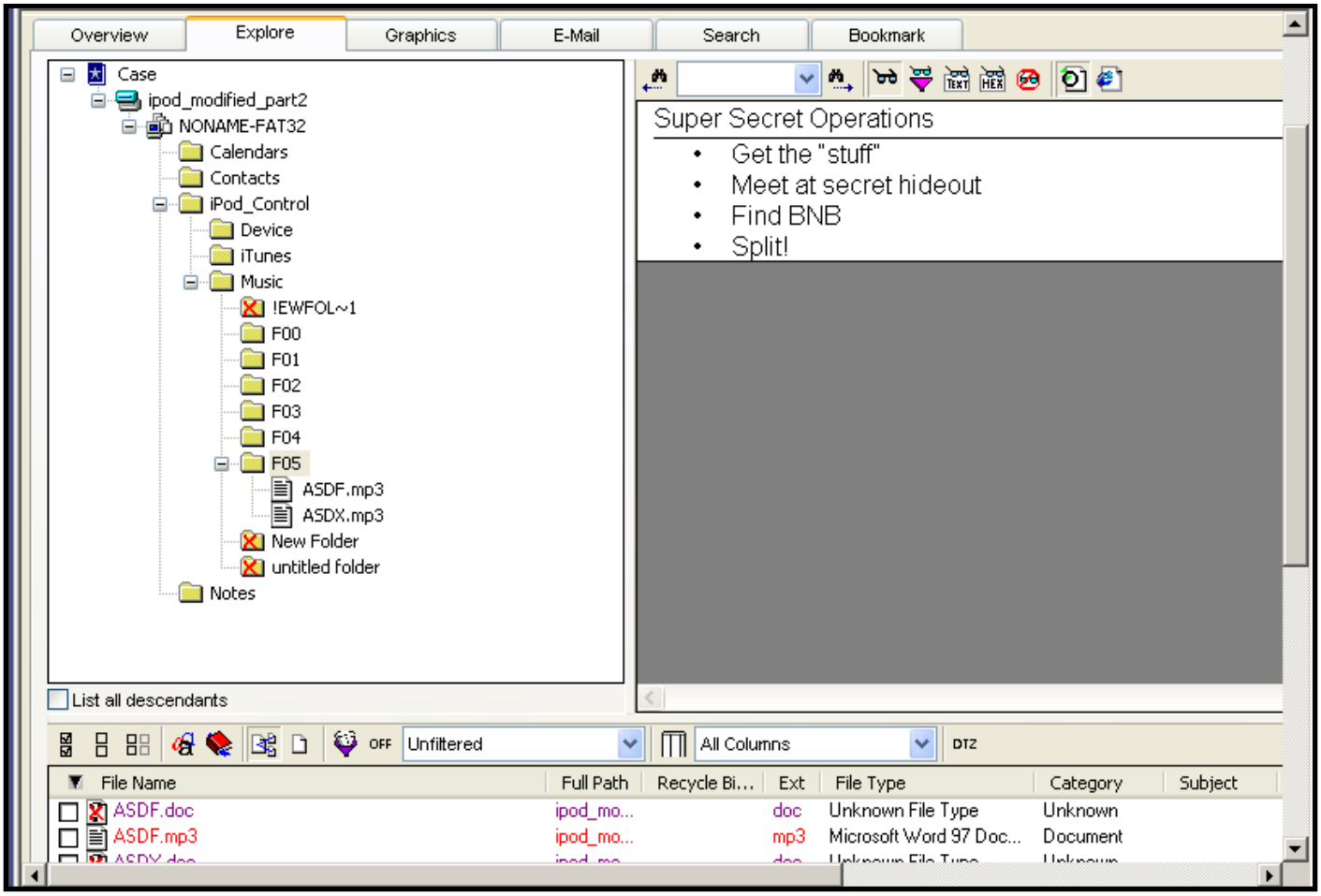
B.5


Overview
Explore
Graphics
E-Mail
Search
Bookmark
Case
ipod_modified_part2
NONAME-FAT32
Calendars
Contacts
iPod_Control
Device
iTunes
Music
!EWFOL~1
F00
F01
F02
F03
F04
F05
ASDF.mp3
ASDX.mp3
New Folder
untitled folder
Notes
List all descendants
Summary Information
Name
Value
Author
Conzetti Finocchiaro
LastAuthor
Conzetti Finocchiaro
Revision Number
2
Created
2/15/2009 6:27:50 PM
Last Saved
2/15/2009 6:29:57 PM
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
CompObj
ipod_mo...
OLE Stream
Unknown
Ole
ipod_mo...
OLE Stream
Unknown
DocumentSummaryInformation
ipod_mo...
Office Document Summ...
Other

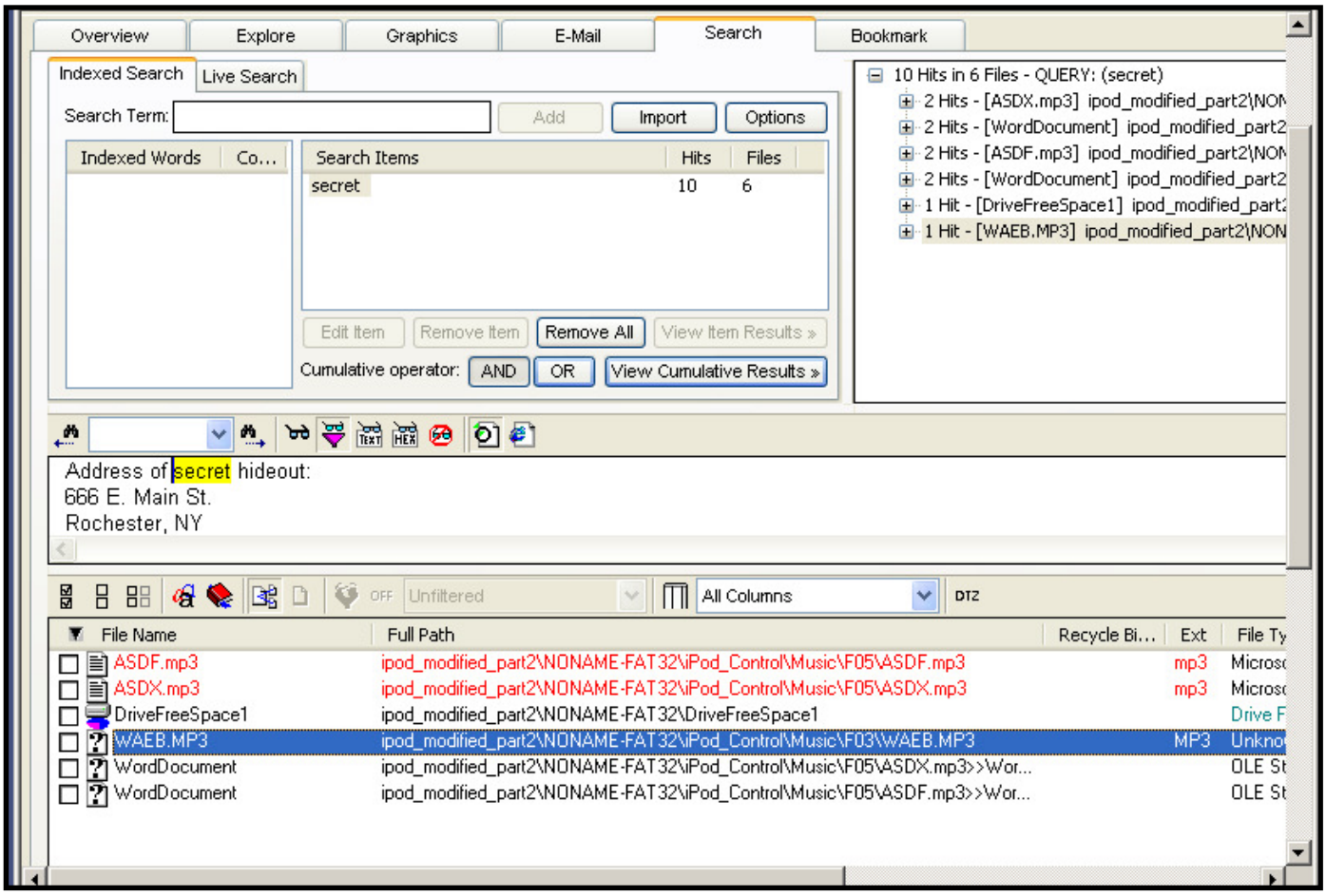
B.6


Case
ipod_modified_part2
NONAME-FAT32
Calendars
Contacts
iPod_Control
Device
iTunes
Music
!EWFOL~1
F00
F01
F02
F03
F04
F05
ASDF.mp3
ASDX.mp3
New Folder
untitled folder
Notes
List all descendants
Super Secret Operations
Get the "stuff"
Meet at secret hideout
Find BNB
Kill the witness
Split!
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
ASDF.doc ipod_mo... doc Unknown File Type Unknown
ASDF.mp3 ipod_mo... mp3 Microsoft Word 97 Doc... Document
ASDX.doc ipod_mo... doc Unknown File Type Unknown
ASDX.mp3 ipod_mo... mp3 Microsoft Word 97 Doc... Document

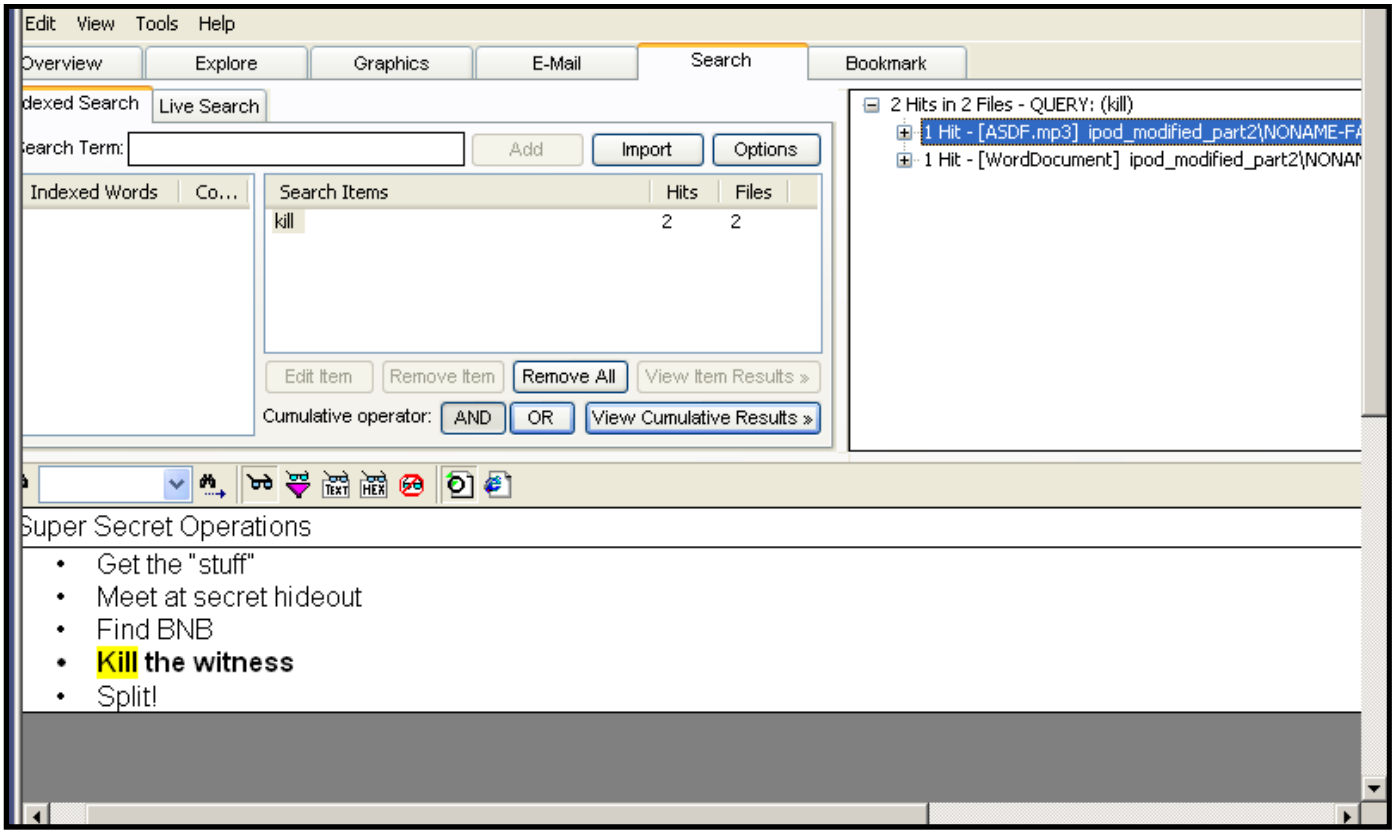
B.7


Overview
Explore
Graphics
E-Mail
Search
Bookmark
Case
ipod_modified_part2
NONAME-FAT32
Calendars
Contacts
iPod_Control
Device
iTunes
Music
!EWFOL~1
F00
F01
F02
F03
F04
F05
ASDF.mp3
ASDX.mp3
New Folder
untitled folder
Notes
List all descendants
Super Secret Operations
Get the "stuff"
Meet at secret hideout
Find BNB
Split!
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
ASDF.doc
ipod_mo...
doc
Unknown File Type
Unknown
ASDF.mp3
ipod_mo...
mp3
Microsoft Word 97 Doc...
Document

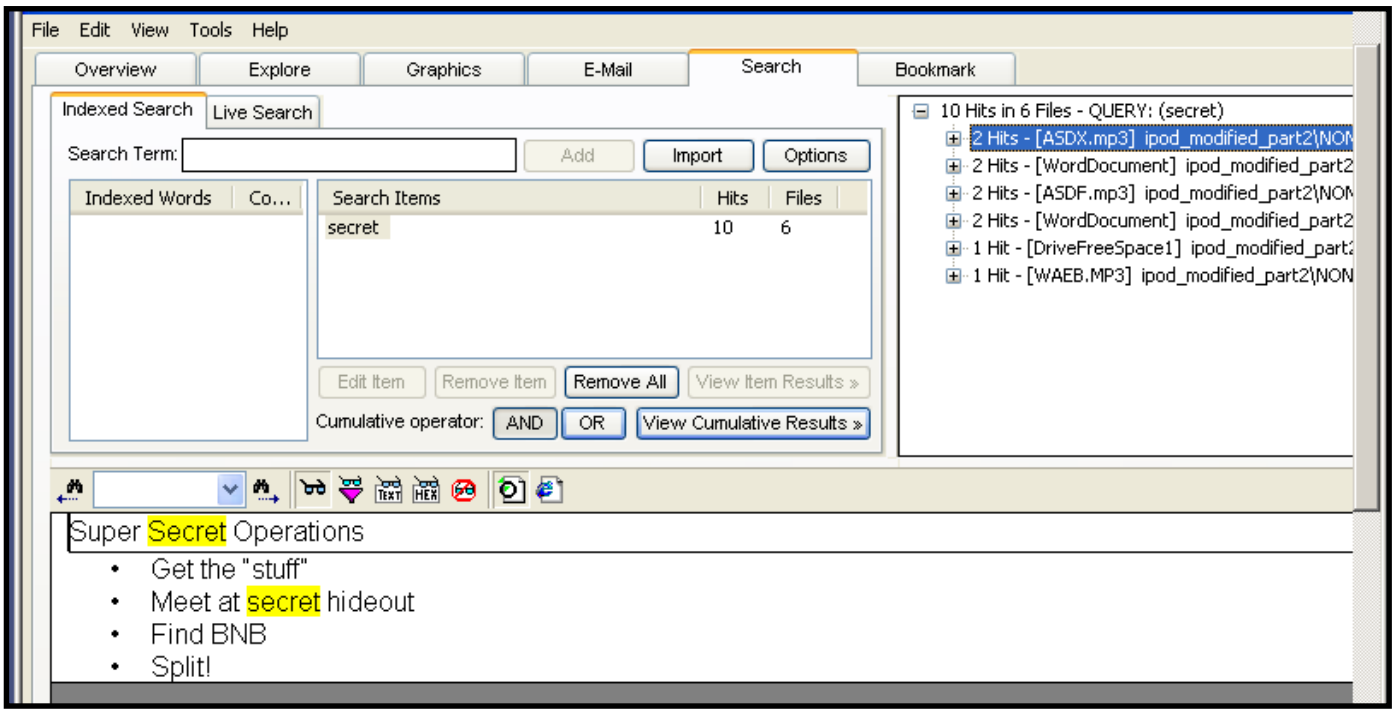
B.8


Overview
Explore
Graphics
E-Mail
Search
Bookmark
Indexed Search
Live Search
Search Term:
Add
Import
Options
Indexed Words
Co...
Search Items
Hits
Files
secret
10
6
Edit Item
Remove Item
Remove All
View Item Results »
Cumulative operator:
AND
OR
View Cumulative Results »
10 Hits in 6 Files - QUERY: (secret)
2 Hits - [ASDX.mp3] ipod_modified_part2\NON
2 Hits - [WordDocument] ipod_modified_part2
2 Hits - [ASDF.mp3] ipod_modified_part2\NON
2 Hits - [WordDocument] ipod_modified_part2
1 Hit - [DriveFreeSpace1] ipod_modified_part2
1 Hit - [WAEB.MP3] ipod_modified_part2\NON
Address of secret hideout:
666 E. Main St.
Rochester, NY
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Ty
ASDF.mp3
ipod_modified_part2\NONAME-FAT32\iPod_Control\Music\F05\ASDF.mp3
mp3
ASDX.mp3
ipod_modified_part2\NONAME-FAT32\iPod_Control\Music\F05\ASDX.mp3
mp3
DriveFreeSpace1
ipod_modified_part2\NONAME-FAT32\DriveFreeSpace1
Drive F
WAEB.MP3
ipod_modified_part2\NONAME-FAT32\iPod_Control\Music\F03\WAEB.MP3
MP3
WordDocument
ipod_modified_part2\NONAME-FAT32\iPod_Control\Music\F05\ASDX.mp3>>Wor...
OLE St
WordDocument
ipod_modified_part2\NONAME-FAT32\iPod_Control\Music\F05\ASDF.mp3>>Wor...
OLE St

B.9


Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
dexed Search Live Search
earch Term:
Add Import Options
Indexed Words Co...
Search Items Hits Files
kill 2 2
Edit Item Remove Item Remove All View Item Results »
Cumulative operator: AND OR View Cumulative Results »
2 Hits in 2 Files - QUERY: (kill)
1 Hit - [ASDF.mp3] ipod_modified_part2\NONAME-FA
1 Hit - [WordDocument] ipod_modified_part2\NONAM
Super Secret Operations
Get the "stuff"
Meet at secret hideout
Find BNB
Kill the witness
Split!

B.10


File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Indexed Search Live Search
Search Term:
Add Import Options
Indexed Words Co...
Search Items Hits Files
secret 10 6
Edit Item Remove Item Remove All View Item Results »
Cumulative operator: AND OR View Cumulative Results »
10 Hits in 6 Files - QUERY: (secret)
2 Hits - [ASDX.mp3] ipod_modified_part2\NON
2 Hits - [WordDocument] ipod_modified_part2
2 Hits - [ASDF.mp3] ipod_modified_part2\NON
2 Hits - [WordDocument] ipod_modified_part2
1 Hit - [DriveFreeSpace1] ipod_modified_part2
1 Hit - [WAEB.MP3] ipod_modified_part2\NON
Super Secret Operations
Get the "stuff"
Meet at secret hideout
Find BNB
Split!

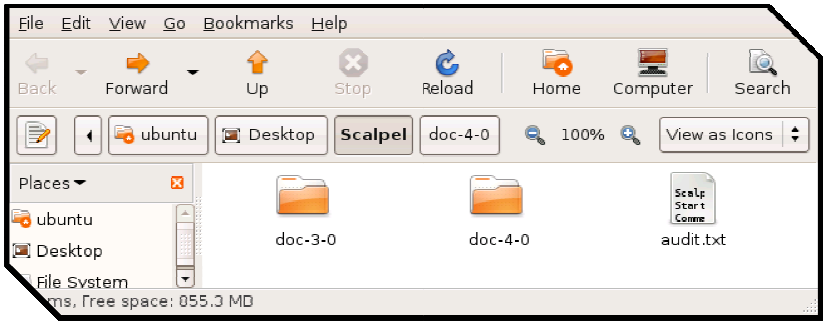
C.1

```
scalpel -b -o -v Scalpel iPod_modified_part2.img
```

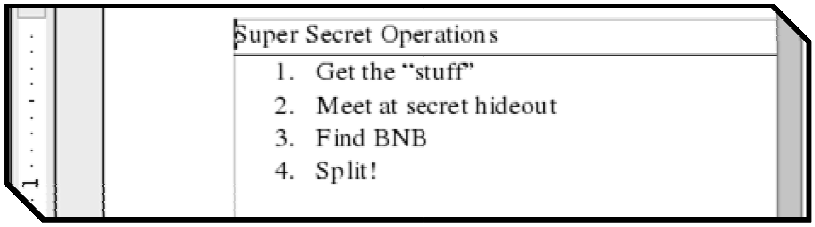
C.2

```
gif    y     5000000       \x47\x49\x46\x38\x37\x61          \x00\x3b
gif    y     5000000       \x47\x49\x46\x38\x39\x61          \x00\x3b
jpg    y     200000000     \xff\xd8\xff\xe0\x00\x10          \xff\xd9
doc    y     10000000      \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00
NEXT
doc    y     10000000   \xd0\xcf\x11\xe0\xa1\xb1
```

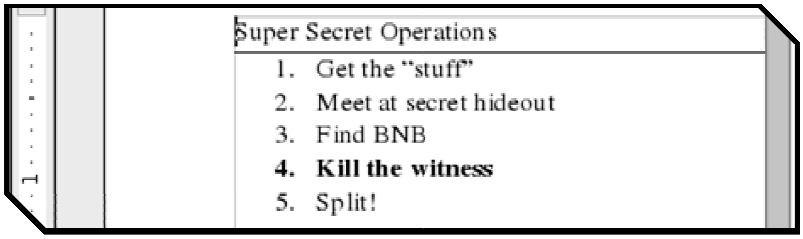
C.3



C.4



C.5



C.6

```
stegdetect -t p 00000000.jpg
```

C.7

```
00000000.jpg : jphide(***)
```

C.8

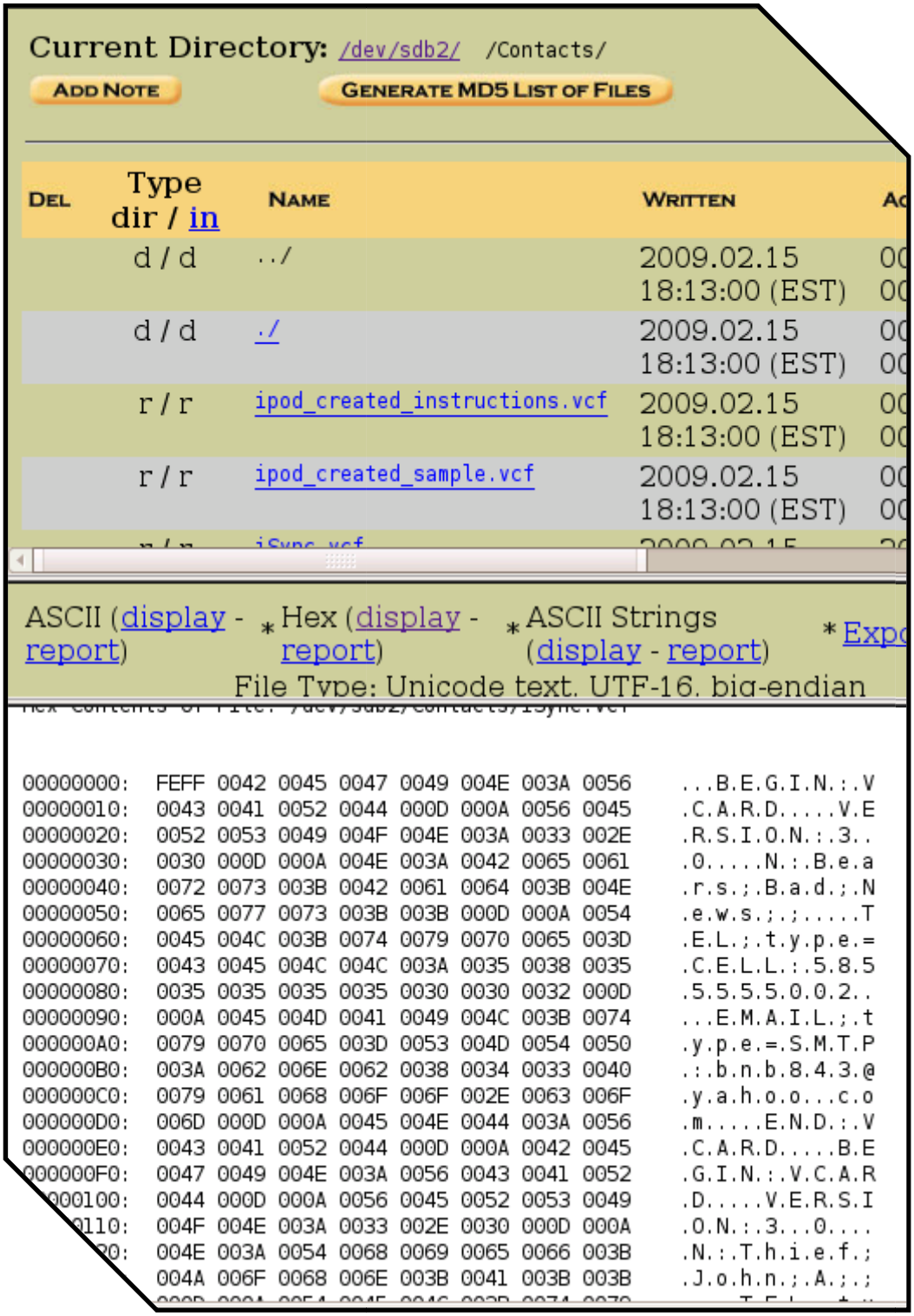
Current Directory: /dev/sdb2/ /iPod_Control/ /Music/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESS
	d / d	../	2009.02.15 18:26:48 (EST)	2009.(
	d / d	./	2009.02.15 18:26:48 (EST)	2009.(
✔	r / r	ASDF.doc	2009.02.15 18:31:08 (EST)	2009.(
	r / r	ASDF.mp3	2009.02.15 18:31:08 (EST)	2009.(
✔	r / r	ASDX.doc	2009.02.15 18:31:30 (EST)	2009.(
	r / r	ASDX.mp3	2009.02.15 18:31:30 (EST)	2009.(

```
00001390:  0000 0000 0000 0000 0000 0000 0000 0000  ................
000013A0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
000013B0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
000013C0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
000013D0:  0000 0000 0080 0000 0000 0000 0000 0000  ................
000013E0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
000013F0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
00001400:  FEFF 0000 0100 0200 0000 0000 0000 0000  ................
00001410:  0000 0000 0000 0000 0100 0000 E085 9FF2  ................
00001420:  F94F 6810 AB91 0800 2B27 B3D9 3000 0000  .Oh.....+'..0...
00001430:  F474 0100 0900 0000 0100 0000 5000 0000  .t..........P...
00001440:  0400 0000 5800 0000 0800 0000 7800 0000  ....X.......x...
00001450:  0900 0000 9800 0000 0A00 0000 A400 0000  ................
00001460:  0B00 0000 B000 0000 0C00 0000 BC00 0000  ................
00001470:  0D00 0000 C800 0000 1100 0000 D400 0000  ................
00001480:  0200 0000 E9FD 0000 1E00 0000 1500 0000  ................
00001490:  436F 6E7A 6574 7469 2046 696E 6F63 6368  Conzetti Finocch
000014A0:  6961 726F 0000 0000 1E00 0000 1500 0000  iaro............
000014B0:  436F 6E7A 6574 7469 2046 696E 6F63 6368  Conzetti Finocch
000014C0:  6961 726F 0000 0000 1E00 0000 0200 0000  iaro............
000014D0:  3200 0000 4000 0000 0000 0000 0000 0000  2...@...........
000014E0:  4000 0000 0000 0000 0000 0000 4000 0000  @...........@...
000014F0:  001F 4904 C58F C901 4000 0000 80C8 FB4F  ..I.....@......O
01500:  C58F C901 4700 0000 1874 0100 FFFF FFFF  ....G....t......
5110:  0800 0000 2800 0000 7C00 0000 A000 0000  ....(...|.......
0:  0100 1800 0000 0000 80E8 0000 0000 0000  ................
    0000 0000 0000 0000 0000 0000 FFFF FFFF  ................
```

C.9


Current Directory: /dev/sdb2/ /Contacts/
ADD NOTE
GENERATE MD5 LIST OF FILES
DEL
Type dir / in
NAME
WRITTEN
d / d ../ 2009.02.15 18:13:00 (EST)
d / d ./ 2009.02.15 18:13:00 (EST)
r / r ipod_created_instructions.vcf 2009.02.15 18:13:00 (EST)
r / r ipod_created_sample.vcf 2009.02.15 18:13:00 (EST)
ASCII (display - report)
Hex (display - report)
ASCII Strings (display - report)
File Type: Unicode text, UTF-16, big-endian
00000000: FEFF 0042 0045 0047 0049 004E 003A 0056 ...B.E.G.I.N.:.V
00000010: 0043 0041 0052 0044 000D 000A 0056 0045 .C.A.R.D.....V.E
00000020: 0052 0053 0049 004F 004E 003A 0033 002E .R.S.I.O.N.:.3..
00000030: 0030 000D 000A 004E 003A 0042 0065 0061 .0.....N.:.B.e.a
00000040: 0072 0073 003B 0042 0061 0064 003B 004E .r.s.;.B.a.d.;.N
00000050: 0065 0077 0073 003B 003B 000D 000A 0054 .e.w.s.;.;.....T
00000060: 0045 004C 003B 0074 0079 0070 0065 003D .E.L.;.t.y.p.e.=
00000070: 0043 0045 004C 004C 003A 0035 0038 0035 .C.E.L.L.:.5.8.5
00000080: 0035 0035 0035 0035 0030 0030 0032 000D .5.5.5.5.0.0.2..
00000090: 000A 0045 004D 0041 0049 004C 003B 0074 ...E.M.A.I.L.;.t
000000A0: 0079 0070 0065 003D 0053 004D 0054 0050 .y.p.e.=.S.M.T.P
000000B0: 003A 0062 006E 0062 0038 0034 0033 0040 .:.b.n.b.8.4.3.@
000000C0: 0079 0061 0068 006F 006F 002E 0063 006F .y.a.h.o.o...c.o
000000D0: 006D 000D 000A 0045 004E 0044 003A 0056 .m.....E.N.D.:.V
000000E0: 0043 0041 0052 0044 000D 000A 0042 0045 .C.A.R.D.....B.E
000000F0: 0047 0049 004E 003A 0056 0043 0041 0052 .G.I.N.:.V.C.A.R
00000100: 0044 000D 000A 0056 0045 0052 0053 0049 .D.....V.E.R.S.I
00000110: 004F 004E 003A 0033 002E 0030 000D 000A .O.N.:.3...0....
00000120: 004E 003A 0054 0068 0069 0065 0066 003B .N.:.T.h.i.e.f.;
004A 006F 0068 006E 003B 0041 003B 003B .J.o.h.n.;.A.;.;