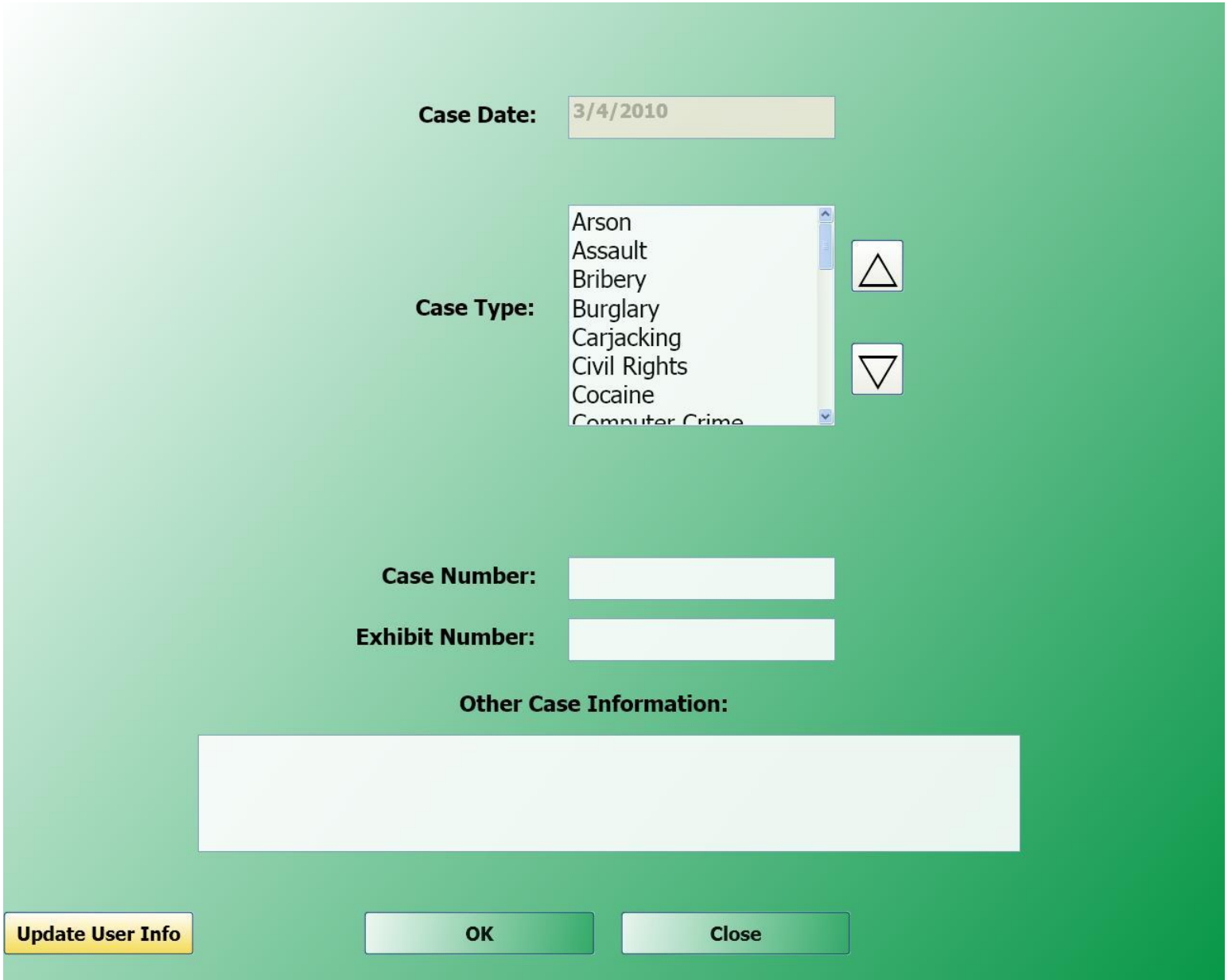
Loose Media Kiosk Quick Reference Guide

Table of Contents

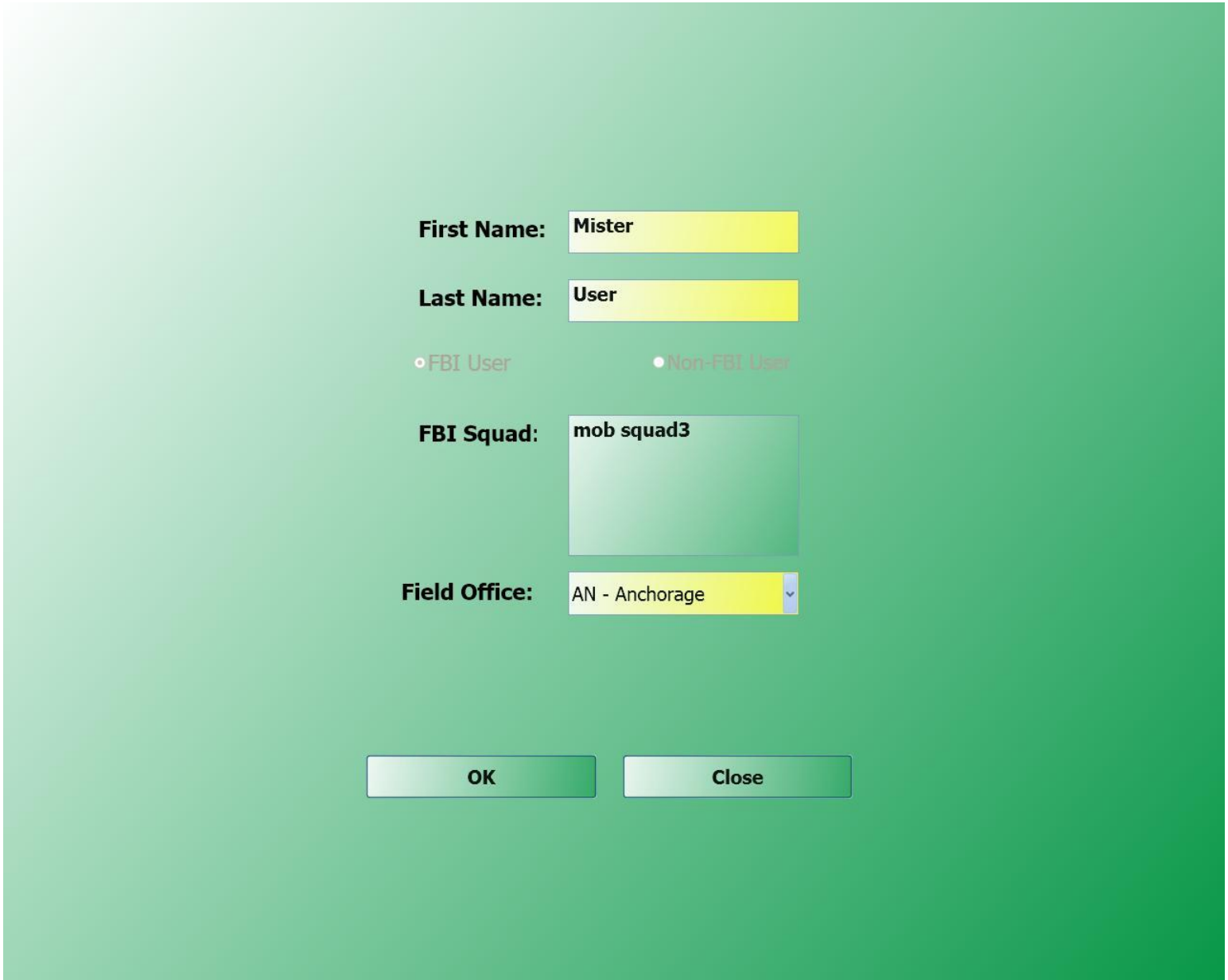
User Sign On	Slide 3
Case Information	Slide 4
Update User Information	Slide 5
Examining Media	Slide 6
Recover Deleted Data	Slide 11
Progress Bar	Slide 15
Selecting New Input	Slide 16
Selecting Output Report Format	Slide 20
Output File Format	Slide 22

User Sign On Screen

Type in Case Information



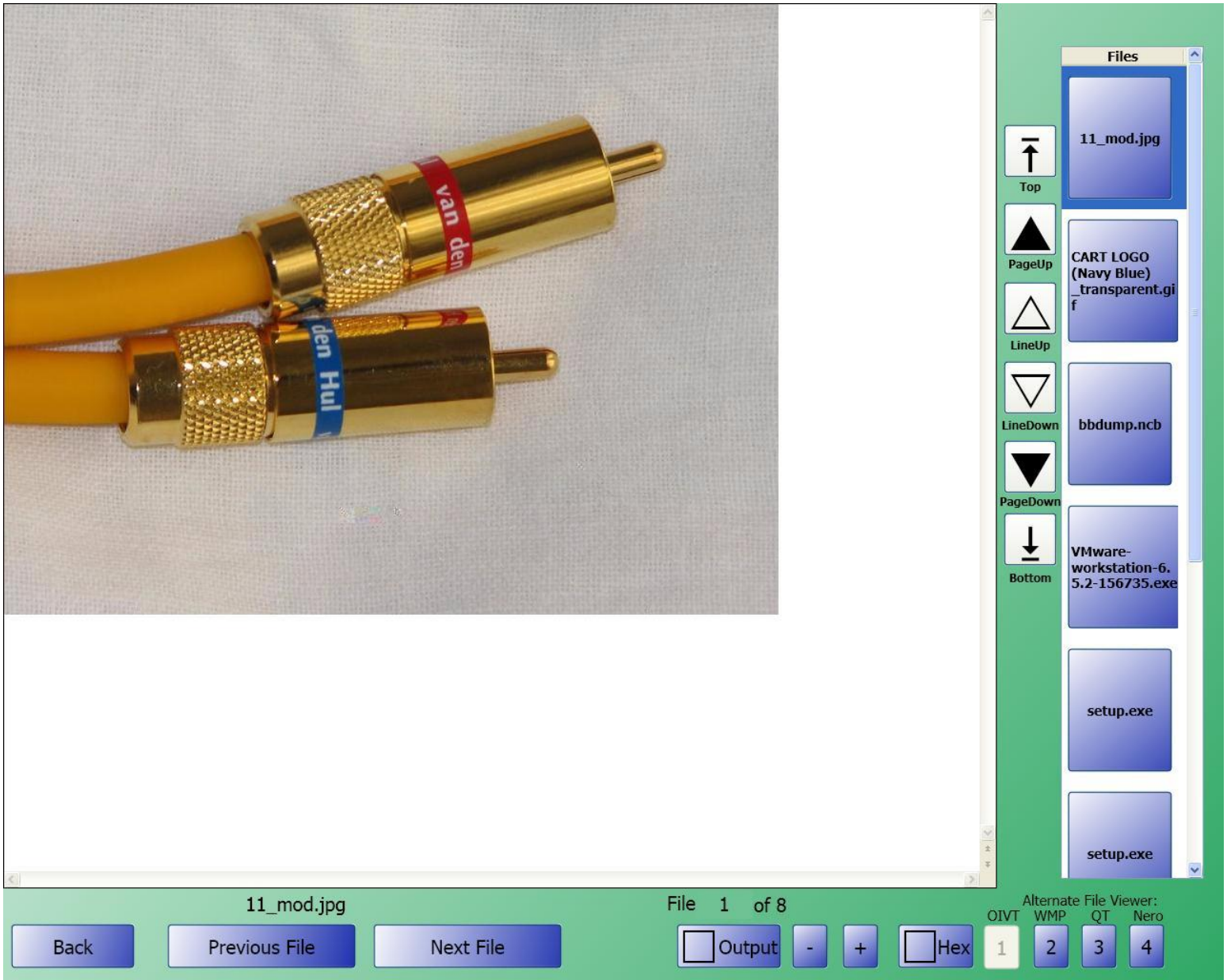
Update User Information



When prompted by this screen, insert the evidentiary digital media that is to be previewed.

Select the category of file that is to be previewed

File preview screen



File preview screen for video

WINDOWS EXECUTABLE
32bit for Windows 95 and Windows NT

Technical File Information:

Image File Header

Signature:	00004550
Machine:	Intel 386
Number of Sections:	0004
Time Date Stamp:	4a300389
Symbols Pointer:	00000000
Number of Symbols:	00000000
Size of Optional Header	00e0
Characteristics:	Relocation info stripped from file. File is executable (i.e. no unresolved external references). Line numbers stripped from file. Local symbols stripped from file. 32 bit word machine.

Image Optional Header

Magic:	010b
Linker Version:	6.00
Size of Code:	0008a000
Size of Initialized Data:	00070600
Size of Uninitialized Data:	00000000
Address of Entry Point:	0006a832
Base of Code:	00001000
Base of Data:	0008b000
Image Base:	00400000
Section Alignment:	00001000
File Alignment:	00000200
Operating System Version:	4.00
Image Version:	0.00
Subsystem Version:	5.00
Reserved1:	00000000
Size of Image:	00101000
Size of Headers:	00000400
Checksum:	00000000
Subsystem:	Image runs in the Windows GUI subsystem.
DLL Characteristics:	32768
Size of Stack Reserve:	00100000
Size of Stack Commit:	00001000
Size of Heap Reserve:	00100000
Size of Heap Commit:	00001000
Loader Flags:	00000000
Size of Data Directory:	00000010
Import Directory Virtual Address:	0009f290
Import Directory Size:	000000dc
Resource Directory Virtual Address:	000b3000
Resource Directory Size:	0004dcf0

Top
PageUp
LineUp
LineDown
PageDown
Bottom

Files

- 11_mod.jpg
- CART LOGO (Navy Blue)_transparent.gif
- bbdump.ncb
- VMware-workstation-6.5.2-156735.exe
- setup.exe
- setup.exe

setup.exe

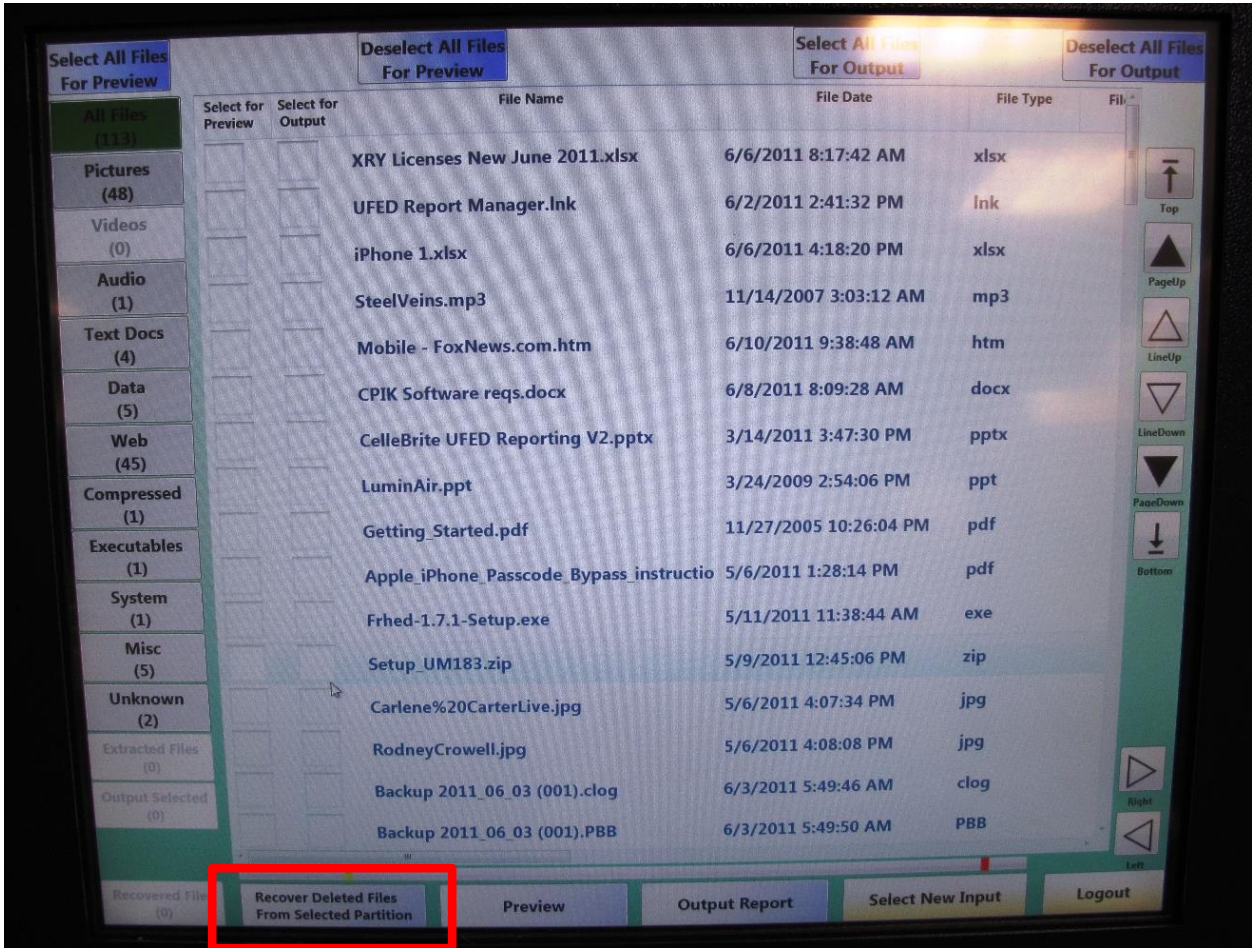
File 5 of 8

Alternate File Viewer:
OIVT WMP QT Nero

Back | Previous File | Next File | Output | Hex | 1 | 2 | 3 | 4

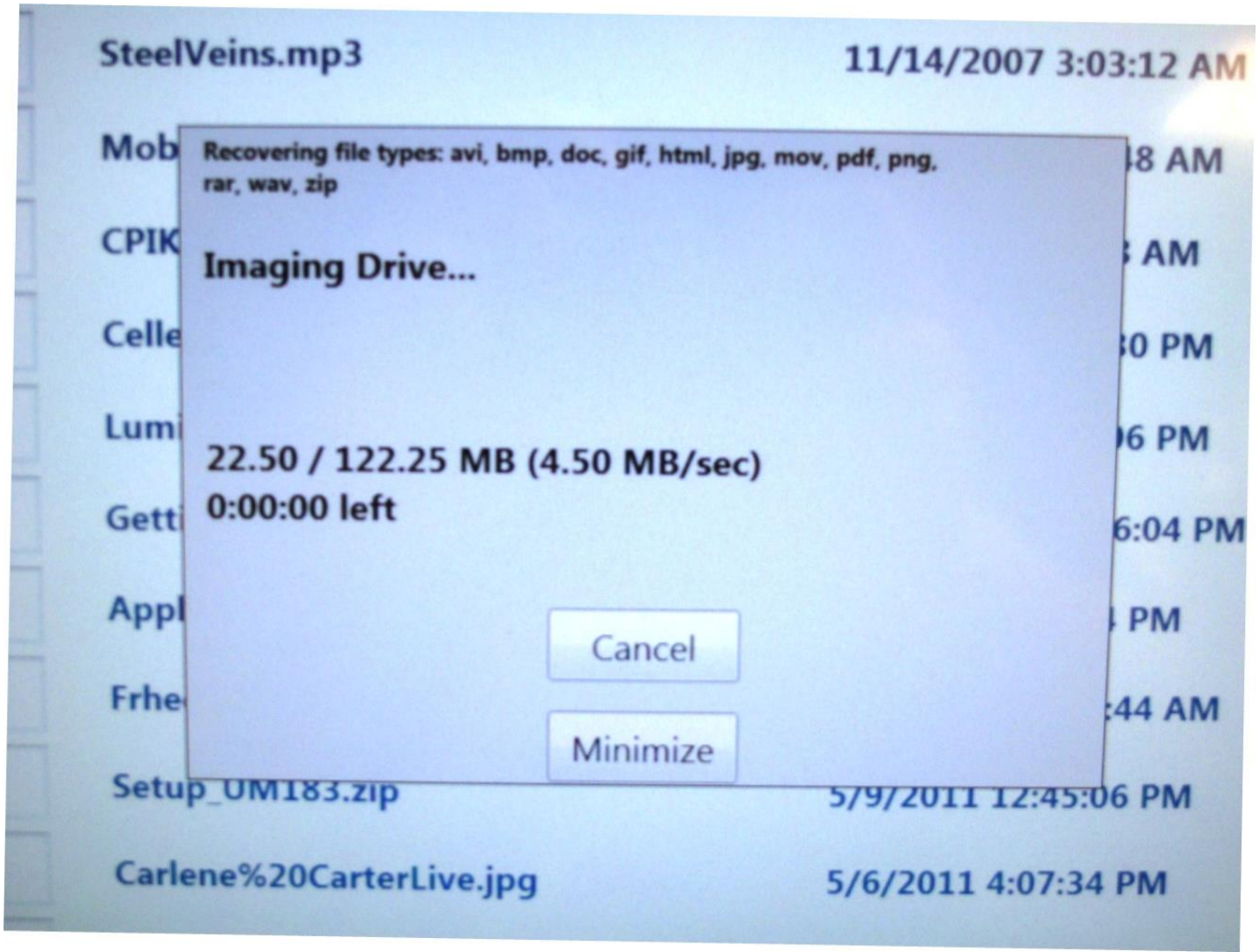
Recovering Deleted Data

- The LMK allows users to recover many deleted file types
- To recover deleted data, select the Recover Deleted Data button from the bottom of the screen :



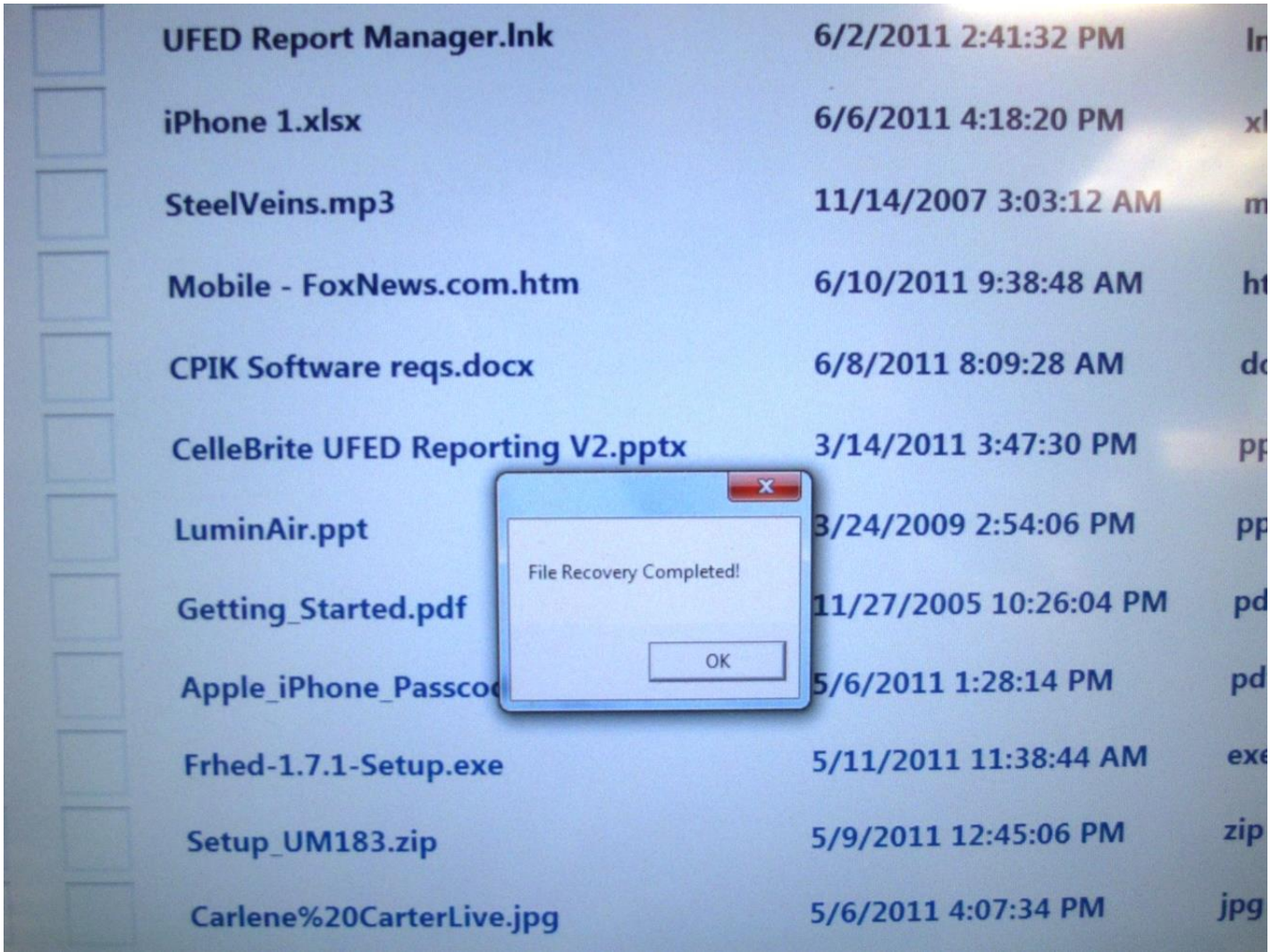
Recovering Deleted Data

- The following box will be displayed showing the recovery progress
  (Note: The time is displayed as (Days:Hours:Minutes)



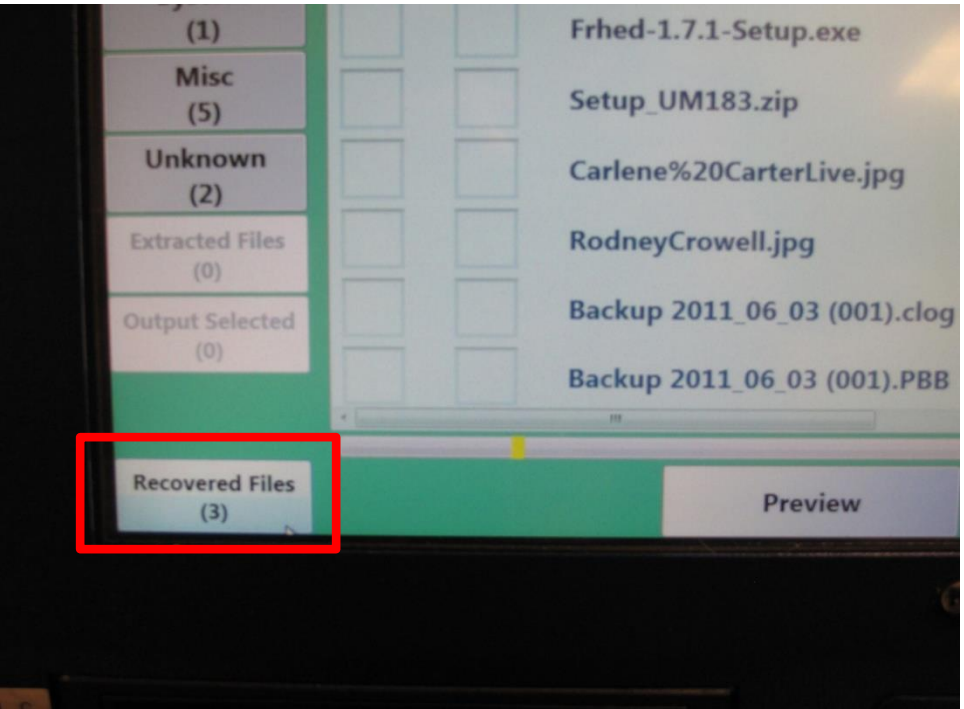
Recovering Deleted Data

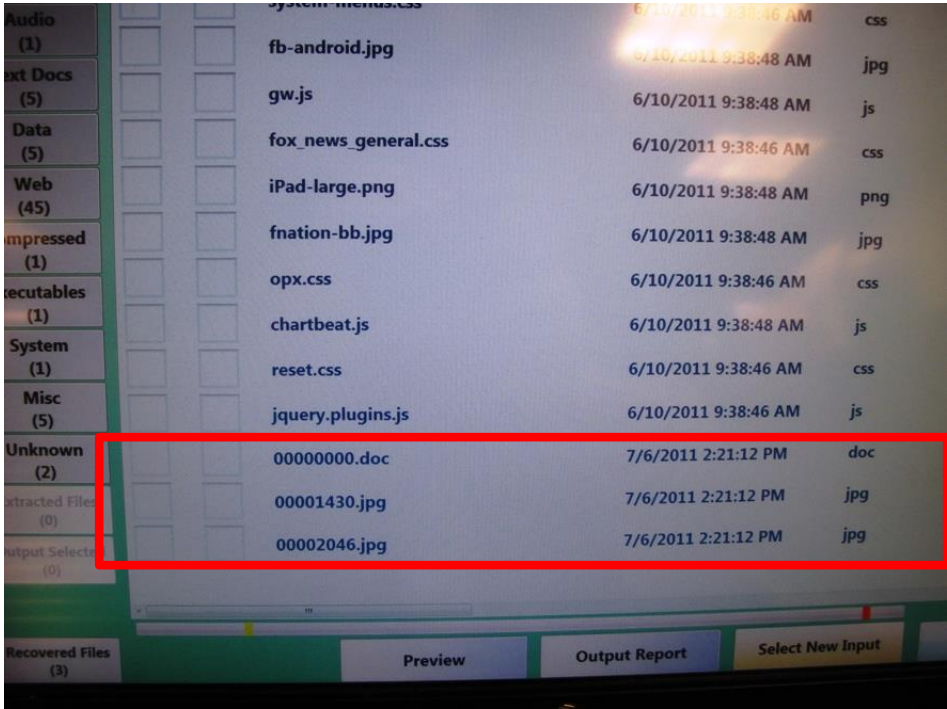
- Upon completion, the following box will be displayed.



Recovering Deleted Data

- Recovered data can be found by selecting the Recovered tab on the left or at the bottom of the file list screen
- Currently file names can **not** be recovered

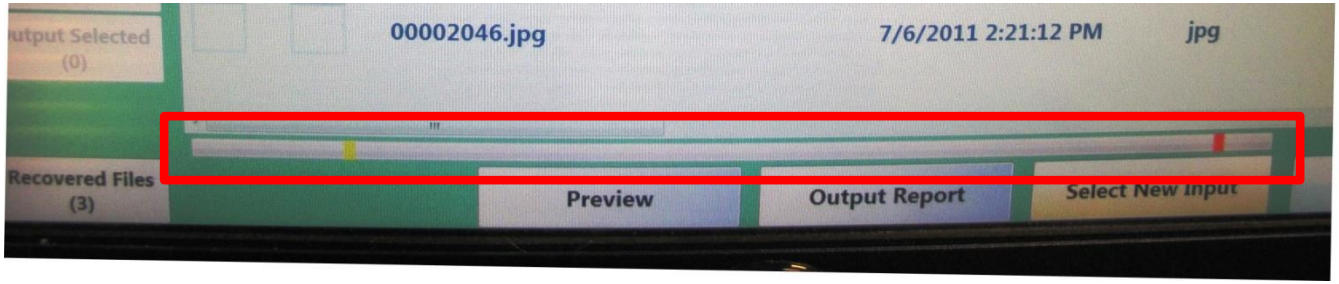




Progress Bar

- A progress bar is displayed at the bottom of the File List screen

  - A yellow line to show the size of the files selected for output
  - A red line to show the size of the output media

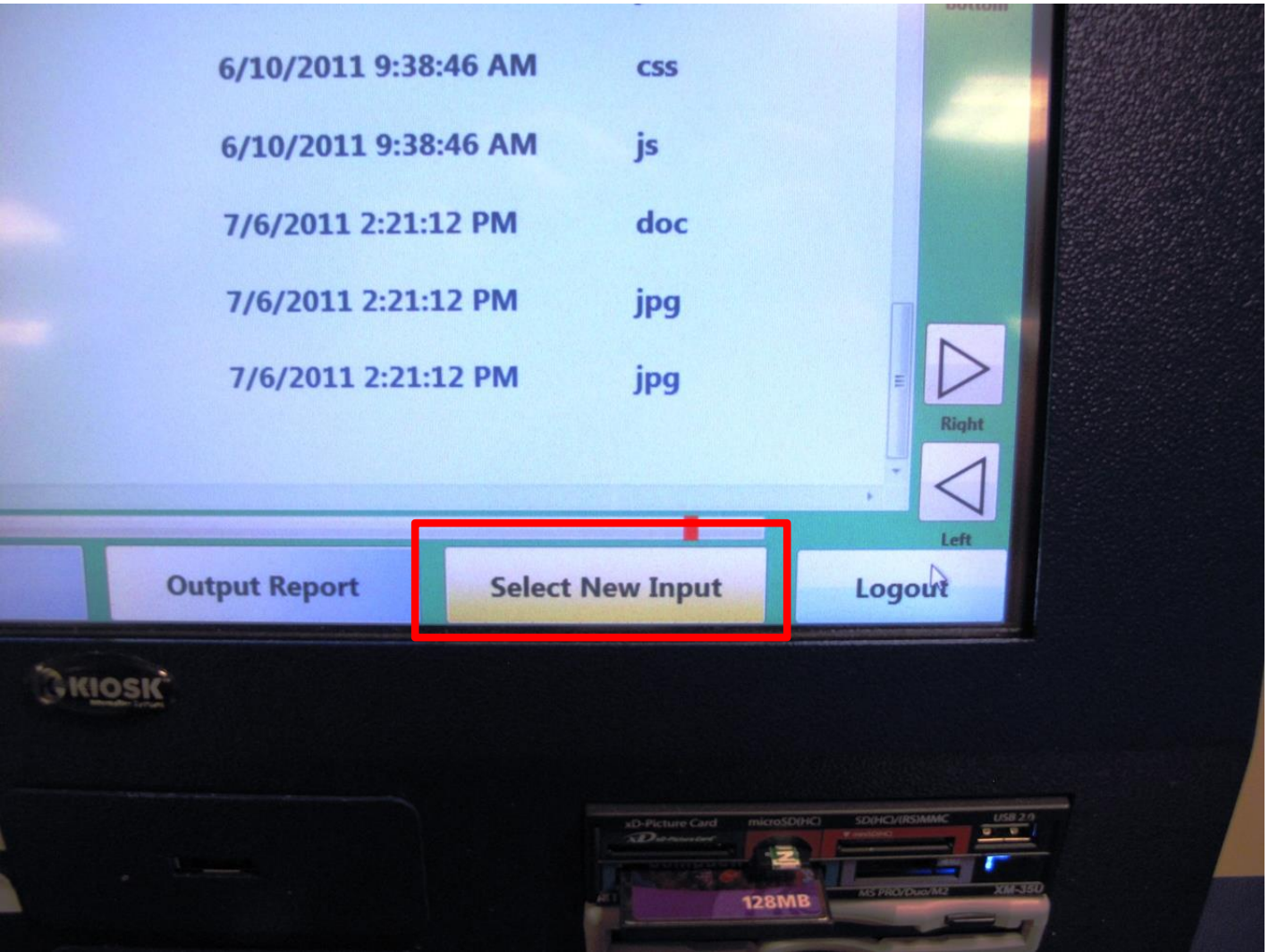


Selecting a New Input

There are two places in which to choose to view a different evidentiary input without having to reboot the kiosk

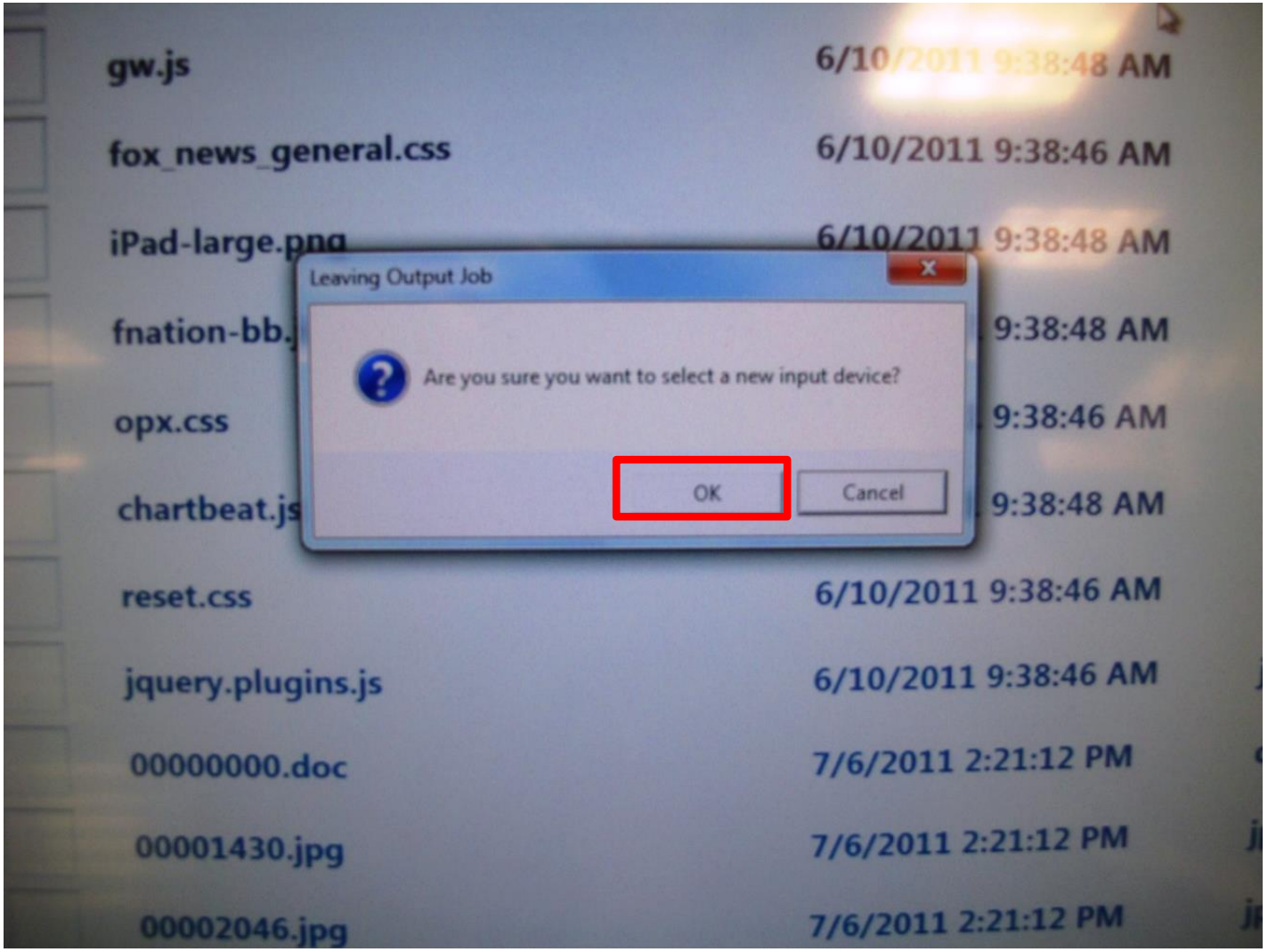
Selecting a New Input

The lower right corner of the File List screen



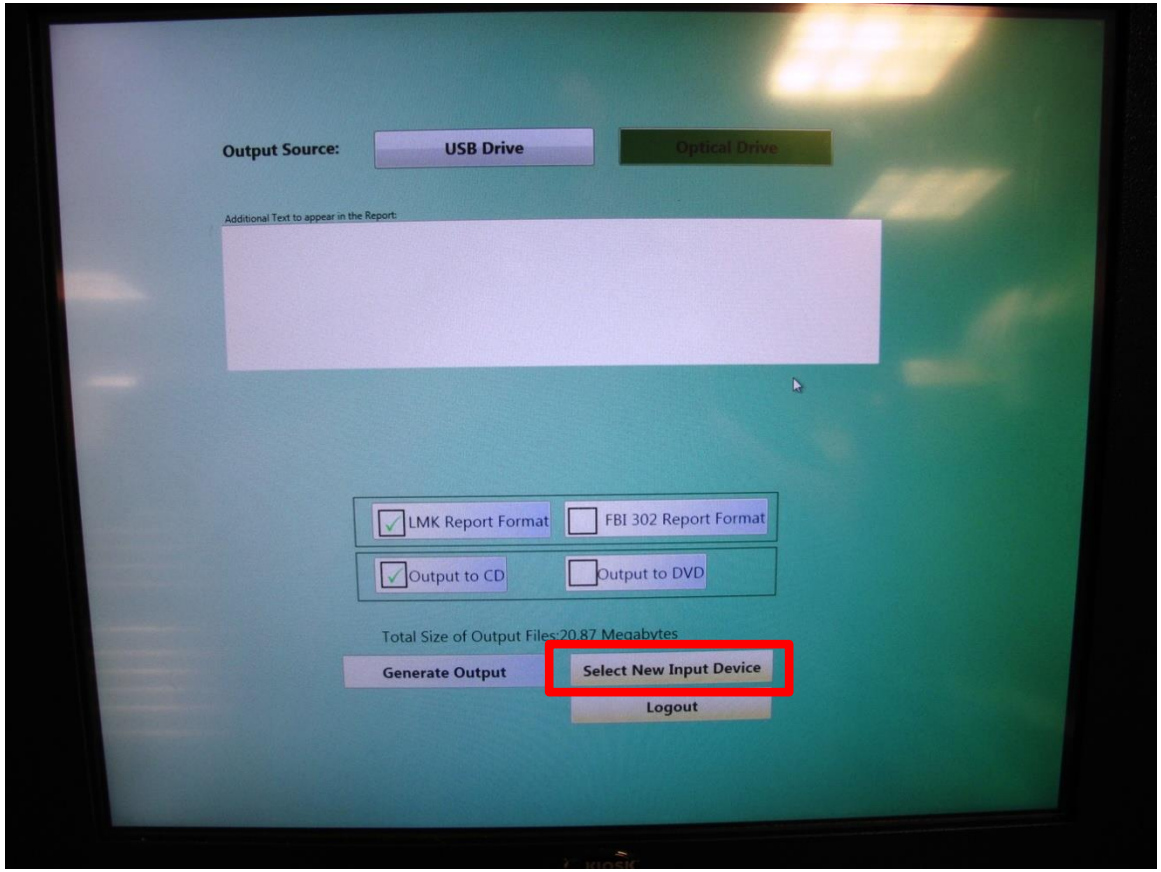
Selecting a New Input

After selecting the new input, select the OK button when prompted



Selecting a New Input

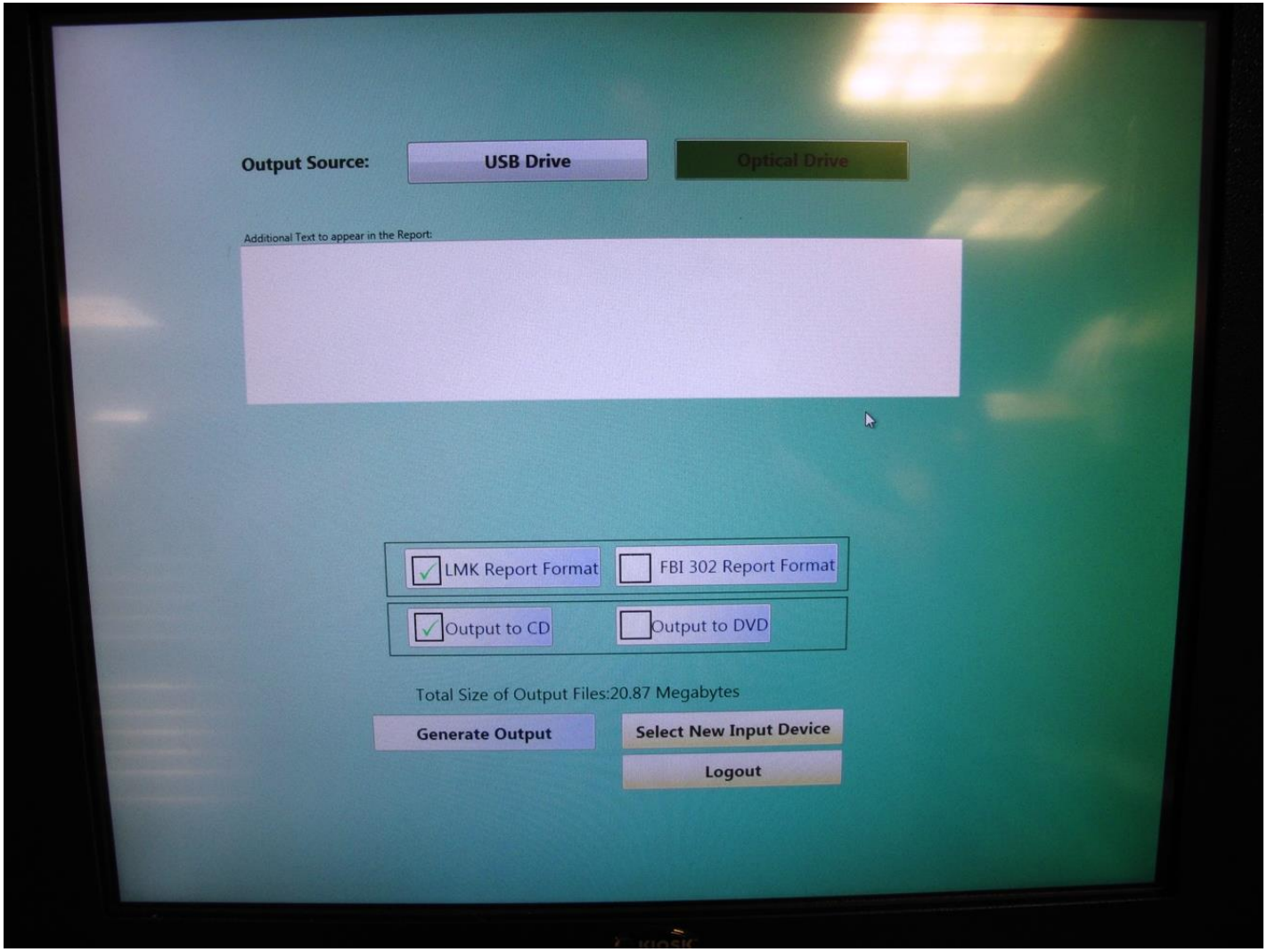
A new input can be chosen from the File Output screen as well

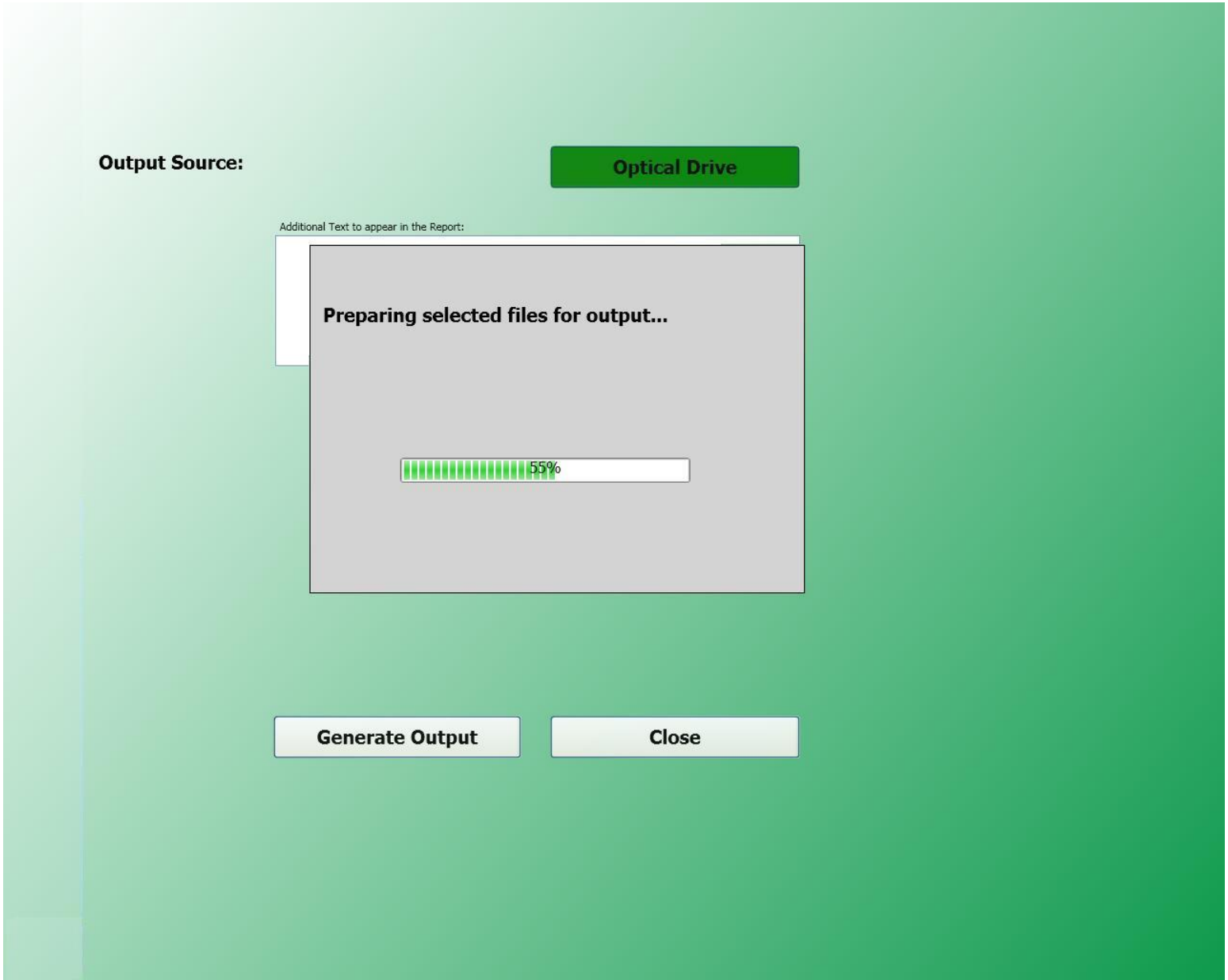


NOTE: Each piece of media examined requires a separate report

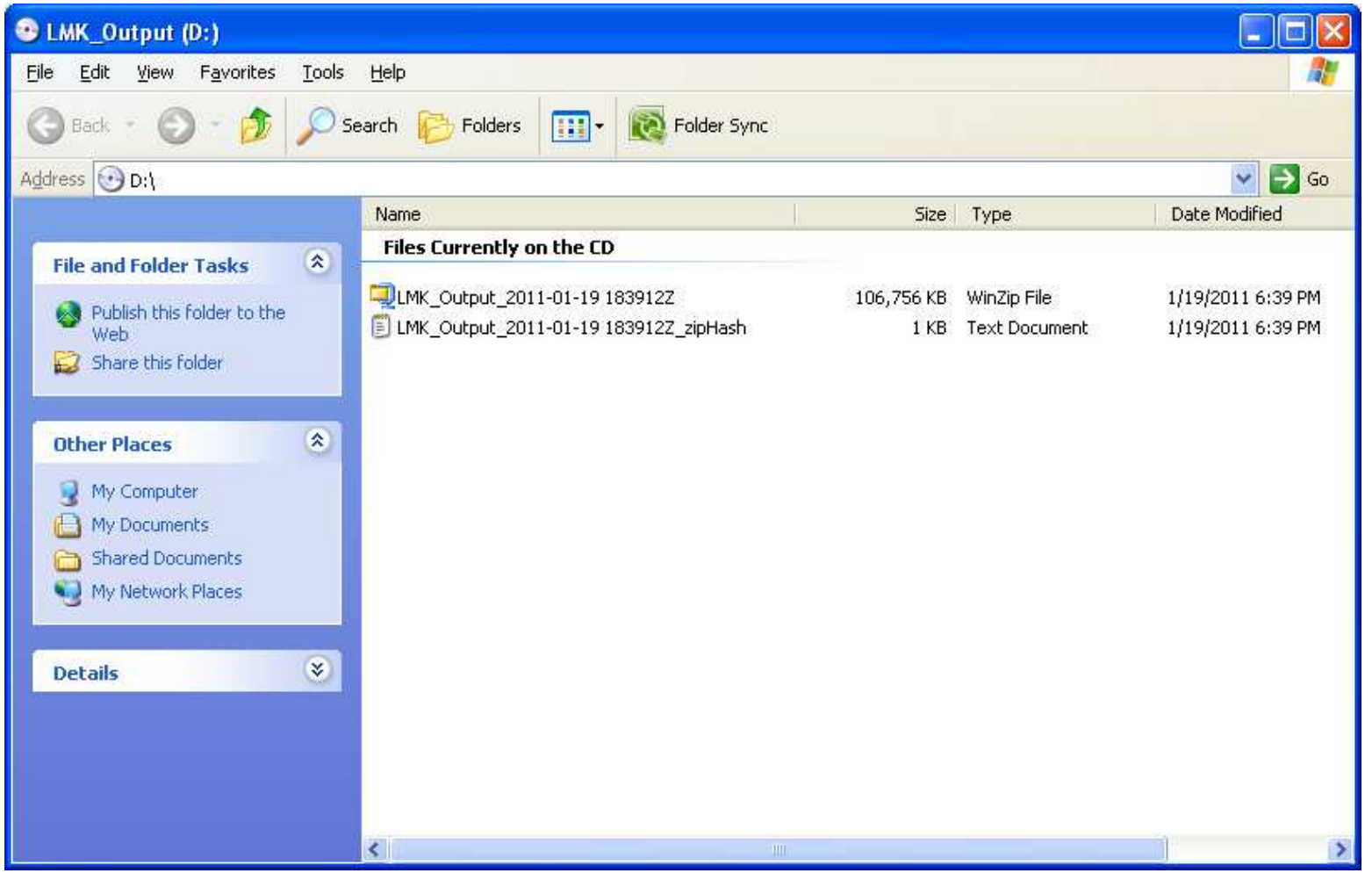
If a piece of media is examined and a report is needed, ensure that a report is output before examining a new piece of media

Select report format and CD or DVD output

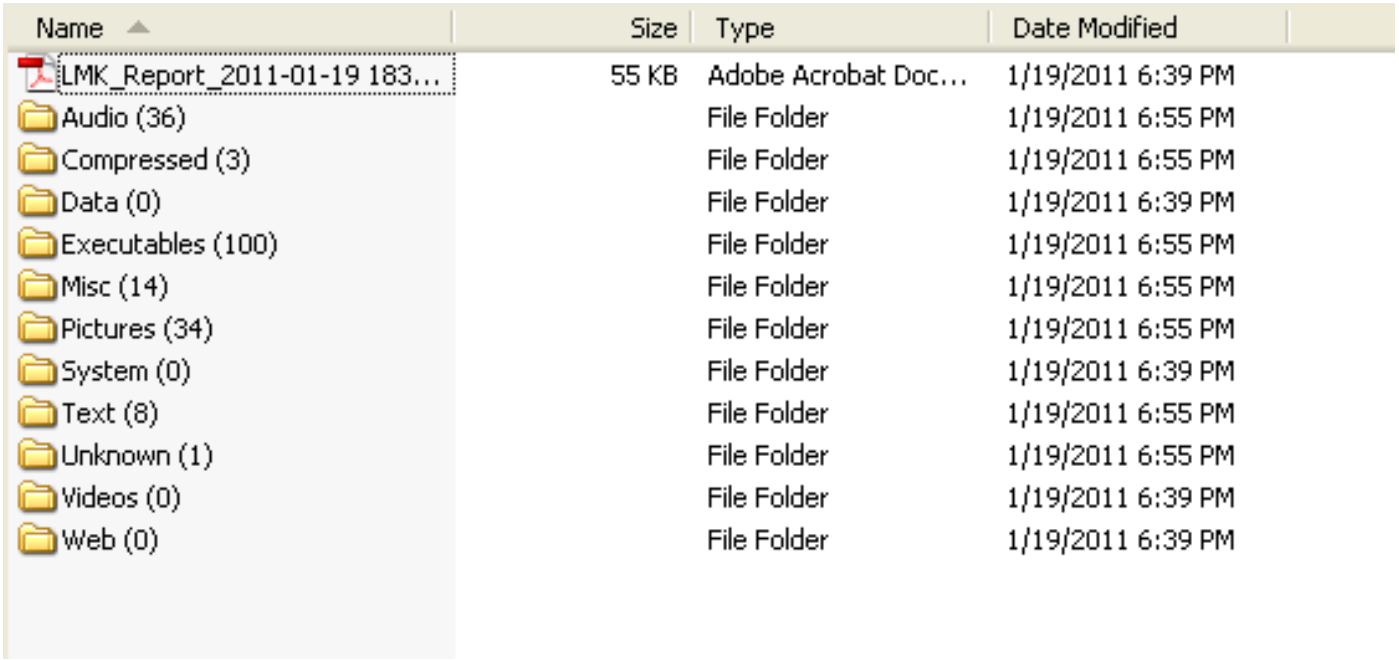



Output Source:
Optical Drive
Additional Text to appear in the Report:
Preparing selected files for output...
55%
Generate Output
Close

Selected output files will be contained in a single uncompressed Zip file



File format contained within the zip file



Name	Size	Type	Date Modified
LMK_Report_2011-01-19 183...	55 KB	Adobe Acrobat Doc...	1/19/2011 6:39 PM
Audio (36)		File Folder	1/19/2011 6:55 PM
Compressed (3)		File Folder	1/19/2011 6:55 PM
Data (0)		File Folder	1/19/2011 6:39 PM
Executables (100)		File Folder	1/19/2011 6:55 PM
Misc (14)		File Folder	1/19/2011 6:55 PM
Pictures (34)		File Folder	1/19/2011 6:55 PM
System (0)		File Folder	1/19/2011 6:39 PM
Text (8)		File Folder	1/19/2011 6:55 PM
Unknown (1)		File Folder	1/19/2011 6:55 PM
Videos (0)		File Folder	1/19/2011 6:39 PM
Web (0)		File Folder	1/19/2011 6:39 PM

Files that are copied to CD are documented in a report along with their hash value and file path

FD-302 (Rev.10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/19/2011

Kiosk Name: Kiosk1
Kiosk ID: f727331b-56d5-42cc-baf5-4080fa54a6a5
Kiosk Location: Location1
Examiner Name: Bruce Kindley
User Name: bkindley
Field Office and Squad: HQ - Headquarters CART
Case Type: Homicide
Case Number: 269-HQ-00000
Exhibit Number: Two
Other Case Information:

Identifier_File Name	Md5 Hash	Category	File Path
1_ignore_my_docs	d41d8cd98f00b204e9800998ecf8427e	Misc	\ignore_my_docs
2_regapp.exe	135a590a1afd52919083714dc2d4d822	Executables	\regapp.exe
3_CE_DLL.dll	b8eb0623d32605935d69d78d7076252a	Executables	\CE_DLL.dll
4_Prince_of_Persia_Sands_of_Time[1].jpg	d0c0fb03ca93fbda50e507d803c21b9c	Pictures	\Prince_of_Persia_Sands_of_Time[1].jpg
5_Men_In_Black_3_Movie[2].jpg	6aec09e596775db3e5ec41a321b5419b	Pictures	\Men_In_Black_3_Movie[2].jpg
6_bg_reskin[1].jpg	17fe5383e3587e5b63ac299d1979c5b6	Pictures	\bg_reskin[1].jpg

FD-302 (Rev.10-6-95)

Identifier_File Name	Md5 Hash	Category	File Path
178_HostControl.pm	e78d2f9e666b784bb2e0eca3a4771156	Misc	\Treo_650_Simulator_GSM_Cingular-Consumer_MR3_EN_Rel_Build_350\TestAutomation\Perl\HostControl.pm
179_00029088.dll	2105f746e58ed1cae31dc00efe530a7f	Executables	*Recovered*
180_00000064.exe	5d653a5c60942ee9f0195108fb53bb0c	Executables	*Recovered*
181_00001632.exe	9dce94243f5bf07b25389d6416f836e2	Executables	*Recovered*
182_00000416.jpg	f1428e292ba6f2daf20eaf16b12ec6b0	Pictures	*Recovered*
183_00000544.jpg	0a8fff69da6745da961e0ba420d3b6cc	Pictures	*Recovered*
184_00000672.jpg	5de55c15579a90ae56abdac813b48c36	Pictures	*Recovered*
185_00000800.jpg	01b5f681b71090c4bf243a47c4c0cc69	Pictures	*Recovered*
186_00000928.jpg	7bc1733712891ef8f6b5fecce3a72c09	Pictures	*Recovered*
187_00001024.jpg	cd038b21ca62afc2a88119d8c99f864f	Pictures	*Recovered*
188_00042144.jpg	b0c6834cdfd52a1aa75ef58f7842bddb	Pictures	*Recovered*
189_00042784.jpg	87096e0c682ee42984217eb7b23f8dcf	Pictures	*Recovered*
190_00043520.jpg	dd535f4fe34b3fd1b7d742cd23010772	Pictures	*Recovered*
191_00043968.jpg	1bc5b77f3e50b7fbe12c792ee438da45	Pictures	*Recovered*
192_00044128.jpg	e5810dc95895eb5b80c163138970ec33	Pictures	*Recovered*
193_00004037.png	ea898c602ea73c60056ce273a3a1b1a1	Pictures	*Recovered*
194_00001664.zip	10df74ccf8ab27cd052fe3602282303e	Compressed	*Recovered*
195_00031296.zip	939917421c2298c9a491c220fdcbe923	Compressed	*Recovered*
196_00047136.zip	ac9a532c51fd55a64c7fc88c06c6764b	Compressed	*Recovered*