

CFSI Course Application

Thank you for your interest in the CFSI course. The first step in attending the course is to fill out this application and answer some questions about your knowledge and experience with forensics and Field Search.



Please complete all the fields in this document and save the document **renamed with your name added**. For example, if your name is Tom Wilson, you should rename this file “ **CFSI Application Tom Wilson.pdf**” when saving it.

Return the renamed application file **and a letter from your agency stating their support for you being an internal trainer** as attachments to an email directed to Sue Kaessner at sue.kaessner@nlectc-rm.org. The email should have a subject line that reads “CFSI application”

Applicant's Information

Applicant's Name _____

Agency: _____

Applicant's position in the agency: _____

Agency Address: _____
Street, City, State, Zip

Phone: _____

Email Address: _____
(We will notify you of your acceptance to the class at the above email address).

Location of class you are applying for: _____

Dates of class you are applying for: _____

Applicant's Experience with Field Search

Date of training: _____ Location of Training: _____

Instructor: _____ Sponsoring Agency: _____

If more than one training, please list others here.

How long have you been using Field Search?

In what capacity do you use Field Search? (i.e. probation compliance checks, Knock & Talks, etc.)

Please list any other forensic training you have.

Below you will find a series of questions about Field Search. Please answer the following questions by selecting **ONE** answer for each question and writing it in the space next to the question number.

Example Question:

0. _____C_____ FSWin will run on the following operating systems :
- A. Linux.
 - B. Mac OS X.
 - C. Windows.
 - D. Unix.
-
-

1. _____ FSWin collects information on which of the following items when it is first executed (you can review it BEFORE you start a scan)?
 - A. Recycle Bin.
 - B. Most Recently Used Files (MRUs).
 - C. Windows Install Date.
 - D. All of the above.

2. _____ Which of the following is **NOT** possible from within FSWin?
 - A. Saving images in zipped containers to external media.
 - B. Finding JPG images which are renamed.
 - C. Placing thumbnails of images in zipped containers in a final report.
 - D. Listing images in zipped containers in the Excel export.





3. _____ To speed up its search, FSWin
 - A. Examines the header data in files.
 - B. Ignores file extensions.
 - C. Only finds images within the sizes set in the filter settings.
 - D. Counts file hits instead of word hits when searching for keywords.

4. _____ In FSWin if you have captured frames from a video for inclusion in a report, how do you remove them from the report?
 - A. The media viewer, choose “selected” as the source, uncheck the frame.
 - B. The media viewer, uncheck the video.
 - C. The image gallery, choose “selected” as the source, uncheck the image.
 - D. The image gallery, right click on the image and select “remove from report”.

5. _____ What is the first thing you should do when launching FSWin?
 - A. Run the final report to check times and dates.
 - B. Go to the MRUs window to see where the computer has been.
 - C. Review URL histories.
 - D. Go to the image gallery.

6. _____ In a standard operating system configuration, scanning a drive with FSWin will change the Last Access Date on folders for which operating system(s)?
 - A. Windows ‘98
 - B. Windows XP
 - C. Windows Vista
 - D. B & C above.

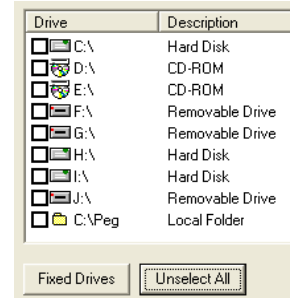
7. _____ One advantage of using the Zipping Tool to extract evidentiary files is:
 - A. It downloads every file listed in the report.
 - B. It downloads all files found on the drive.
 - C. It sorts the files by date/time.
 - D. It preserves the files’ paths.

8. _____ An image file with a modified date which is earlier than its created date suggests:
- A. The file was renamed on this volume.
 - B. The file was on another volume when it was last modified.
 - C. The file was deleted and then restored from the recycle bin.
 - D. The file was opened by the User on this volume.
9. _____ In FAT and NTFS systems, double clicking on anything in FSWin will generally
- A. Reveal the item's properties.
 - B. Change the modified date.
 - C. Change the created date.
 - D. Change the last access date.
10. _____ The most easily explained date/time stamp in the URL history view is generally:
- A. Record's last accessed.
 - B. Record's modified.
 - C. File's last accessed.
 - D. File's modified.
11. _____ Most of the date/time stamps in the URL history view are in what time setting?
- A. EST
 - B. UTC
 - C. GMT
 - D. MDT
12. _____ FSWin can extract which of the following from free space?
- A. URL records
 - B. Keywords
 - C. Recycle bin elements.
 - D. MRUs
13. _____ To get the contents of a file containing keywords into the final report you must:
- A. Right click and select "expand in report".
 - B. Check the box then run the Excel export tool.
 - C. Double click on the file then select "append".
 - D. Save the file and attach it as an appendix.
14. _____ Which of the following buttons captures a frame from a video?
- A. 
 - B. 
 - C. 
 - D. 

15. _____

If “Fixed Drives” is clicked on the computer shown at the right, how many devices will be scanned?

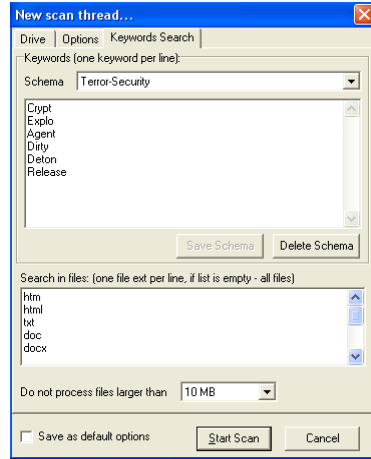
- A. 3
- B. 5
- C. 6
- D. 7



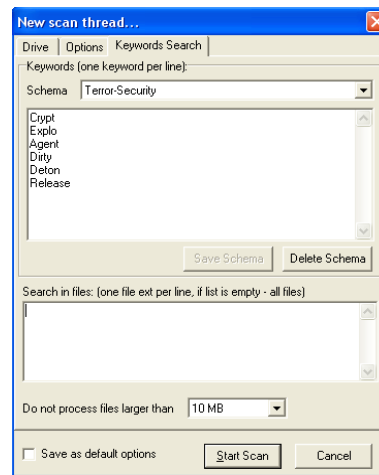
16. _____

Which scan will take the longest?

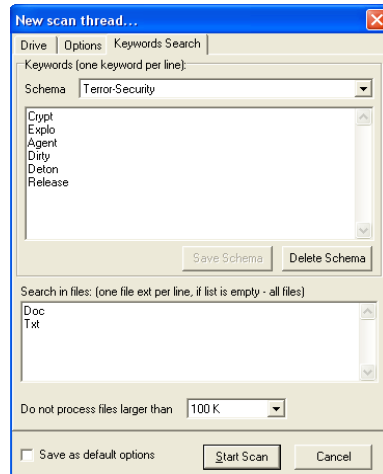
A.



B.



C.



D. All will be equal.

17. _____

File Name	Size	Created	Modified
<input type="checkbox"/> C:\Program Files\Mandiant\Memoryze	0	11/12/2008 11:27 AM	11/12/2008 11:37 AM
<input type="checkbox"/> C:\Program Files\Mandiant\Memoryze\Audits\JIMS\XPS\20081112183118\Bat...	7 KB	11/12/2008 11:31 AM	11/12/2008 11:31 AM
<input type="checkbox"/> C:\Program Files\Mandiant\Memoryze\Audits\JIMS\XPS\20081112183118\Iss...	321	11/12/2008 11:31 AM	11/12/2008 11:31 AM
<input type="checkbox"/> C:\Program Files\Mandiant\Memoryze\Audits\JIMS\XPS\20081112183118\Issu...	848 KB	11/12/2008 11:31 AM	11/12/2008 11:32 AM
<input type="checkbox"/> C:\Program Files\Mandiant\Memoryze\Audits\JIMS\XPS\20081112183118\m...	-95512...	11/12/2008 11:31 AM	11/12/2008 11:32 AM
<input type="checkbox"/> C:\Program Files\Mandiant\Memoryze\MIRAgent.0.log	249 KB	11/12/2008 11:31 AM	11/12/2008 11:31 AM

The above is from the MRU window. The highlighted object is:

- A. Included in the report
- B. Corrupted
- C. Deleted
- D. A folder.

Questions 18 and 19 refer to the following capture from the MRU window of FSWin.

File Name	Size	Created	Modified	Accessed
<input type="checkbox"/> K:\Tanner\TrueCrypt v BitLocker	0	-	-	-
<input type="checkbox"/> K:\Persinger	0	-	-	-
<input type="checkbox"/> J:\Picture 2.png	0	-	-	-
<input type="checkbox"/> I:\Power Point\Utah Inside Mind.ppt	12 MB	10/25/2008 10:55 AM	9/27/2008 12:41 PM	11/3/2008 12:00 AM
<input type="checkbox"/> I:\Power Point\Utah Deception Detection.PPT	903 KB	10/25/2008 10:55 AM	11/3/2008 8:24 AM	11/13/2008 12:00 AM
<input type="checkbox"/> I:\Power Point\Utah - Protecting self and family.ppt	12 MB	10/25/2008 10:55 AM	9/27/2008 1:11 PM	11/3/2008 12:00 AM
<input type="checkbox"/> I:\	0	-	-	-
<input type="checkbox"/> H:\Power Point\pptB9.tmp	0	-	-	-
<input type="checkbox"/> H:\Power Point\evolution.ppt	107 KB	3/18/2008 4:47 PM	3/18/2008 4:47 PM	11/10/2008 5:07 PM
<input type="checkbox"/> H:\Power Point\Yesterday, Today, and Tomorrow2.ppt	558 KB	7/7/2008 8:00 PM	7/8/2008 7:56 AM	11/8/2008 4:46 PM
<input type="checkbox"/> H:\Power Point\ITC 07-08 Arima Slide - TWO.ppt	0	-	-	-
<input type="checkbox"/> H:\Power Point\ITC 07-08 Arima Slide - TWO.ppt	0	-	-	-

18. _____

The “Utah Inside Mind.ppt” was:

- A. Created on Drive I:, then viewed, then moved elsewhere.
- B. Created elsewhere, then viewed, then moved to Drive I: and not viewed again.
- C. Created on Drive I:, moved elsewhere, then modified.
- D. Created elsewhere, then moved to Drive I: and then viewed.

19. _____

“ITC 07-08 Arima Slide - TWO.ppt”:

- A. Was deleted from Drive H:
- B. Is a folder on Drive H:
- C. Can be viewed by double clicking.
- D. Is in a zipped file.

20. _____

Something you have to remember about FSWin is:

- A. It cannot display the image gallery in some versions of Windows ‘98.
- B. It cannot print a report in some versions of Windows ME
- C. The keyword search windows always comes up blank until sorted.
- D. All the above.

Extra Credit: How do you see the contents of a Mozilla browser cache?

Extra-Extra Credit: Why do you have to take these actions to see the contents of a Mozilla browser cache?