

# AccessData Certified Examiner (ACE)

## Forensic Toolkit

For more information contact: [training@AccessData.com](mailto:training@AccessData.com)

The AccessData Certified Examiner (ACE) credential demonstrates your proficiency with AccessData's Forensic Toolkit technology. The exam is designed to test the proficiency of the user with the tool, and not necessarily forensic investigation workflows.

### Prerequisites

While there are no mandatory training prerequisites to take the ACE, it is recommended that the taker be a user of Forensic Toolkit or have taken relevant training courses. The course which will help the user best prepare for the ACE exam is Forensic Toolkit 101.

**Forensic Toolkit is required to take the exam.** Lab time may be purchased if the user does not have a copy of FTK, and is subject to availability.

### Exam Structure

The ACE exam is comprised of 25 questions, all requiring the taker to perform actions within a case. The exam will require the user to create a case, load and process evidence. The Image file and any associated support files will be provided by AccessData.

The exam answers are entered into the assessment page within the [training.accessdata.com](http://training.accessdata.com) webpage. The exam must be completed within three (3) hours. We suggest creating the case and doing some preliminary processing before starting the exam. Note: due to a limitation we cannot change, the idle timer for the exam is set for 10 minutes. If you are logged out for being idle on a question, the timer does not continue. Simply start back into the exam.

### Study Guide

Part of the exam is knowing which processing options to run to parse the files needed to answer the questions. Because of these the exact processing options are not given. Many times, the question will be written in a way to imply what processing option needs to be used, but ultimately is up to the user to know. It is recommended the larger "basic" processing options be run before actually starting the exam to minimize the impact on time allowed.

The exam includes various types of files, including documents, images, web history, and emails. The exam will cover topics such as filtering, searching, and the use of Known File Filter. Files may be allocated or unallocated.

The ACE is designed to be a test of the user's ability to work with FTK. The ACE is not a test of your forensic knowledge, nor does it require you to know any forensic attributes of a specific type of artifact. However, the questions within the ACE are typically based on the content of files and as such, any searches, filters, etc may require the user to view/read/examine the results for the answer.

The following page will give some topics to prepare for the exam.



# AccessData Certified Examiner (ACE)

## Forensic Toolkit

For more information contact: [training@AccessData.com](mailto:training@AccessData.com)

### Case Processing:

1. Understand Index Search options and how to change them.
2. Understand Expansion options. (Email, Documents, Images, Internet artifacts)
3. Understand how Data Carving is configured
4. What features can only be processed from within the case, outside of the Additional Analysis wizard.

### Interface:

1. Understand what data is held in the properties tab, and what is in the file list pane
2. Creating custom columns may help in the display of some data
3. Understand check marking and the impact that check marks can have.
4. Be able to configure the display time zone

### Filtering:

1. Single Rule Filter
2. Multi Rule Filters
3. Nested Filters

### Searching:

1. Index Searching
2. Field Searching
3. Operator Searching

### Known File Filter:

1. Understand how to create a KFF profile
2. Know how to run a KFF profile (required processing options, etc)
3. Know where to look for the results and how to filter those results

