

Training Manual

Academic Edition



AccessData®

AccessData Forensics

Instructor : S` VTaa]

Table of Contents

INTRODUCTION.....	2
ABOUT THIS HANDBOOK.....	3
INSTRUCTOR REQUIREMENTS	3
CONTACTING ACCESSDATA.....	3
TERMS AND CONDITIONS.....	4
CLASSROOM PREPARATION	5
System Recommendations.....	5
Software Installation.....	7
FTK INSTALLATION INSTRUCTIONS.....	8
Software Download & Preparation	8
Database Installation	9
FTK Application Installation.....	11
Install Additional Tools.....	14
NETWORK LICENSE SERVER (NLS)	15
Important NLS System Notes.....	15
NLS Client System Notes.....	16
NLS INSTALLATION INSTRUCTIONS.....	17
NLS Port Information.....	19
Managing NLS Licenses	19
Viewing NLS Licenses.....	20
CLASS USB IMAGE PREPARATION	21
ACCESSDATA CERTIFIED EXAMINER	23
ACE Study Guide.....	23
ACE Preparation Videos	23

INTRODUCTION

The AccessData Forensics Academic Training course provides the knowledge and skills necessary to install, configure and effectively use Forensic Toolkit (FTK), FTK Imager, Password Recovery Toolkit (PRTK), and Registry Viewer. Students will also use AccessData products to conduct forensic investigations on Microsoft Windows systems, learning where and how to locate Windows system artifacts.

The course is sectioned into 18 modules:

- Module 1 – Introduction
- Module 2 – Working with FTK Imager
- Module 3 – Working with FTK – Part 1
- Module 4 – Working with FTK – Part 2
- Module 5 – Processing the Case
- Module 6 – Narrowing your Focus
- Module 7 – Filtering the Case
- Module 8 – Regular Expressions
- Module 9 – Case Reporting
- Module 10 – Working with PRTK
- Module 12 – Registry Viewer
- Module 13 – ID Theft 1 Practical
- Module 14 – The Recycle Bin
- Module 15 – Link and Spool Files
- Module 16 – Encrypting File System
- Module 17 – Processing Information Lab
- Module 18 – ID Theft 2 Practical

Each of the Modules has hands-on instructor led labs and in some instances student practical's where the students should work through on their own.

The training package includes:

- 31 AccessData Forensic Academic Training manuals
- 30 AccessData Forensic Academic Training Student CD's
- AccessData Forensic Toolkit Software DVD's.
 - Disk 1 is the Application Installation DVD
 - Disk 2 is the Oracle Database Installation DVD
- 1 AccessData Forensic Academic Training Instructor CD
- 1 AccessData CodeMeter Network License Server dongle with 31 licenses

ABOUT THIS HANDBOOK

The AccessData Instructor handbook has been designed and developed to assist the instructors from academic institutions in setting up the classroom environment and to prepare materials that are needed during the classroom course.

INSTRUCTOR REQUIREMENTS

The requirements for the instructor are as follows:

1. The course instructor for the institution must be ACE Certified prior to the institution receiving course curriculum and materials.
2. The course instructor for the institution must maintain a current ACE certification at all times during course instruction.

CONTACTING ACCESSDATA

AccessData Corporation
384 South 400 West
Lindon, UT 84042
Phone: (801) 377-5410
Fax: (801) 377-5426
Web site: <http://www.accessdata.com>

Questions regarding the Academic Training Program or this manual, contact the Manager of Curriculum at academic@accessdata.com.

TERMS AND CONDITIONS

NOTICE: THE FOLLOWING GENERAL TERMS & CONDITIONS APPLY TO THE USE OF THE ACCESSDATA ACADEMIC PROGRAM MATERIALS AND SERVICES – JANUARY 1, 2010. USE OF THE ACADMEIC PROGRAM CONSTITUTES AN UNDESTANDING AND AGREEMENT BETWEEN THE PARTIES WITH RESPECT TO IT'S SUBJECT MATTER AND REPLACES AND SUPERSEDES ANY PRIOR WRITTEN OR VERBAL COMMUNICATIONS, REPRESENTATIONS, OR PROPOSALS.

1. The program will be available for one year from date of purchase and can be renewed annually. A new application will be needed annually for renewal of program.
2. The AccessData Academic Program is available only to higher education institutions.
3. The course instructor for the institution must be ACE Certified prior to the institution receiving course curriculum and materials.
4. The course instructor for the institution must maintain a current ACE certification at all times during course instruction.
5. AccessData must be notified if the institution changes instructor and furnish new instructor information to AccessData.
6. FTK installations must be stand alone only. Centralized Oracle installation cannot be used.
7. All course materials are the property of AccessData Corporation. No materials (i.e. manuals, presentations, software, student files) may be modified, copied, reproduced, republished, transmitted, sold, transferred, or distributed without written consent from AccessData Corporation.
8. The FTK NLS CodeMeter dongle can only be used for courses at the licensed academic institution during the license period and may not be used for commercial purposes.
9. The FTK NLS CodeMeter dongle remains the property of AccessData and must be returned once the institution no longer includes the Academic Program as part of their curriculum.

CLASSROOM PREPARATION

The classroom will need to have network accessibility for the Network License Server and should also have Internet access in order for the students to take the AccessData Certified Examiner (ACE) certification examination at the end of the course if they elect to do so.

System Recommendations

The following are the recommendations for classroom computers:

Hardware	Minimum	Recommended
Processor	<ul style="list-style-type: none"> • Intel Xeon, Core 2 Duo • AMD Athlon 64 X2 Dual Core 	<ul style="list-style-type: none"> • Intel Quad Core Processors • I7 Nehalem or AMD equivalent
RAM	4 GB	8 GB+
DVD drive	Yes	Yes
Hard disk space	250 GB plus space for your cases Warning! You will lose your case if you run out of free disk space while processing.	
Operating System	<ul style="list-style-type: none"> • Windows XP Pro 32 / 64-bit • Windows Vista Ultimate 32 / 64-bit • Windows 7 Ultimate 32 / 64-bit 	<ul style="list-style-type: none"> • Windows XP Pro 32 / 64-bit • Windows Vista Ultimate 32 / 64-bit • Windows 7 Ultimate 32 / 64-bit
USB	Two available USB ports for the security dongle and USB thumb drive	Two available USB ports for the security dongle and USB thumb drive

Any computers used in the classroom should have the following changes made:

Student user accounts need to have administrative privileges.

The computer systems should have the following changes made:

1. All systems on an internal network
2. Turn off UAC (Vista and Windows 7)
3. Firewall totally off in all profiles
4. Fully update and then turn off Auto Updates
5. From Windows Explorer, select and show –
 - File Details
 - Date Created
 - Date Modified
 - Date Accessed
6. Change the folder options to –
 - Show hidden files, folders, or drives
 - Uncheck – Hide empty drives in the Computer folder (Windows 7)
 - Uncheck – Hide extensions from known file types
 - Uncheck – Hide protected operating system files
7. In Internet Explorer, under Internet Options – Advanced, disable –
 - Script debugging (Internet Explorer)
 - Script debugging (Other)
8. Turn off simple file sharing
9. Download and install Microsoft .net 3.5 sp1
10. Install MagicDisk or other ISO mounting tool
11. Disable screen saver
12. Install all Language Packs
13. Install WinRAR or WinZip
14. Install Adobe Reader
15. Install Java
16. Install Microsoft Office 2003 or above or Open Office
17. Anti-Virus software is optional

Software Installation

Install the following software on each student and instructor computer:

- Oracle Database
- CodeMeter Dongle Driver
- Forensic Toolkit
- FTK Known File Filter
- FTK Imager
- FTK Registry Viewer
- Password Recovery Toolkit

Install the following software on the instructor computer or a system that will be accessible on the network:

- CodeMeter Dongle Driver
- NLS License Service
- License Manager

Important: As a reminder, the Academic installation of FTK must be stand alone only. Centralized Oracle installation cannot be used.

FTK INSTALLATION INSTRUCTIONS

This guide focuses on the more critical aspects of the installation and is not intended to cover every step or address all the installation possibilities. Refer to the User Guide for more extensive installation coverage.

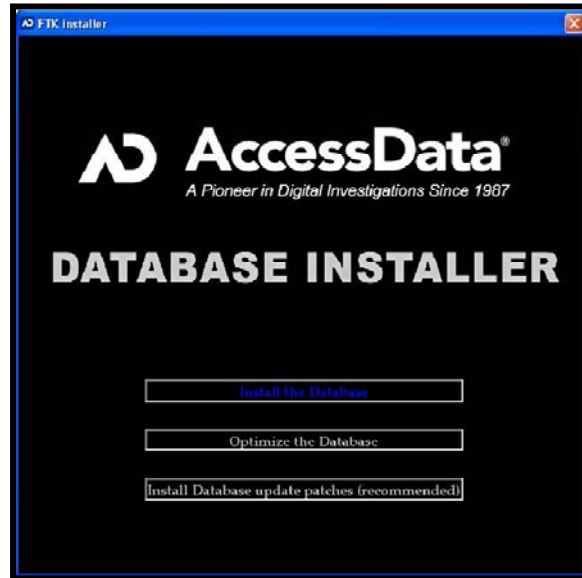
Software Download & Preparation

1. If you do not have install DVD's of the FTK software, you can download the ISO files from the AccessData website at <http://www.accessdata.com/downloads.html>:
 - a. FTK App Install.ISO
 - b. AD Database Install.ISO
2. Verify the MD5 hashes match what is posted on the main FTK download page to ensure there was no data corruption in the download process.
3. Either burn the ISO to a DVD or mount the ISO directly.

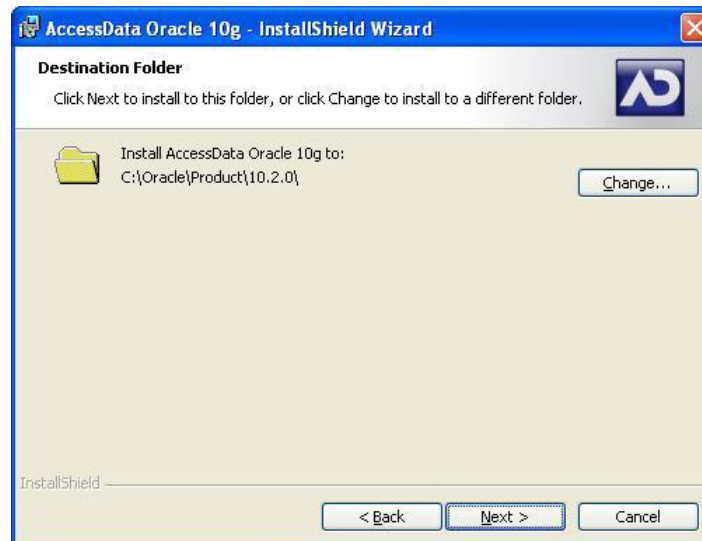
Important: If you install the database from a mounted ISO image, make sure there are no disks in the optical drives before starting the installation.

Database Installation

Install the Oracle database first. Insert the DB Install disk and launch Autorun.exe.



Step 1 – Select **Install the Database**. Keep the default install path. Hit **Next**.

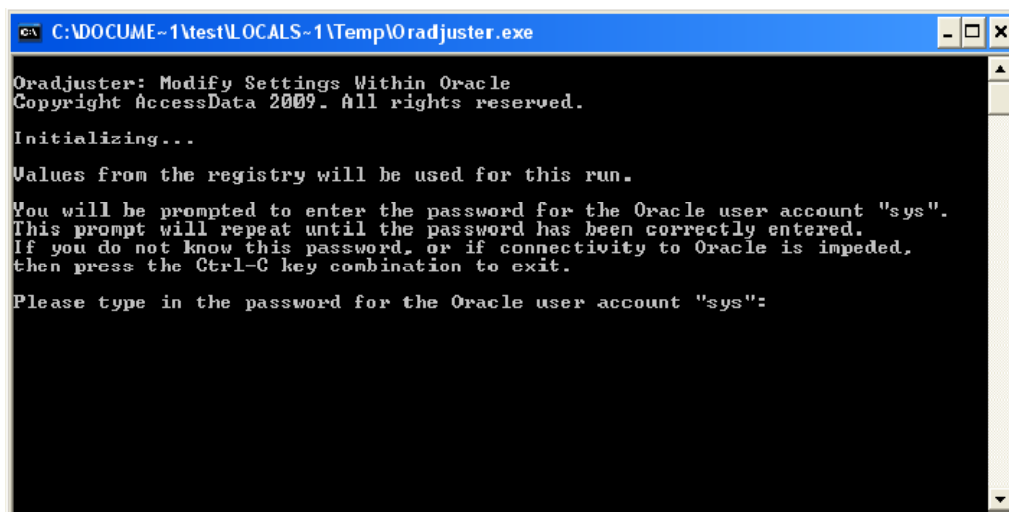


Step 2 – For the Setup Type, select **Typical**.



Step 3 – Accept the defaults and complete the installation.

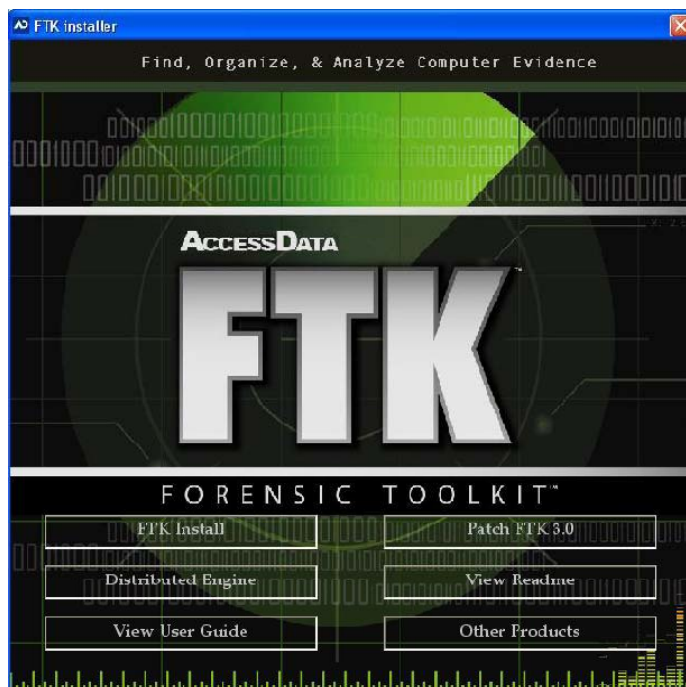
Step 4 - If you have installed Oracle on a 64 bit machine with more than 4 GB or RAM, select Optimize the Database from the Autorun menu. This will allocate more memory to Oracle for faster performance. This is not a required step, but will considerably speed up database operations.



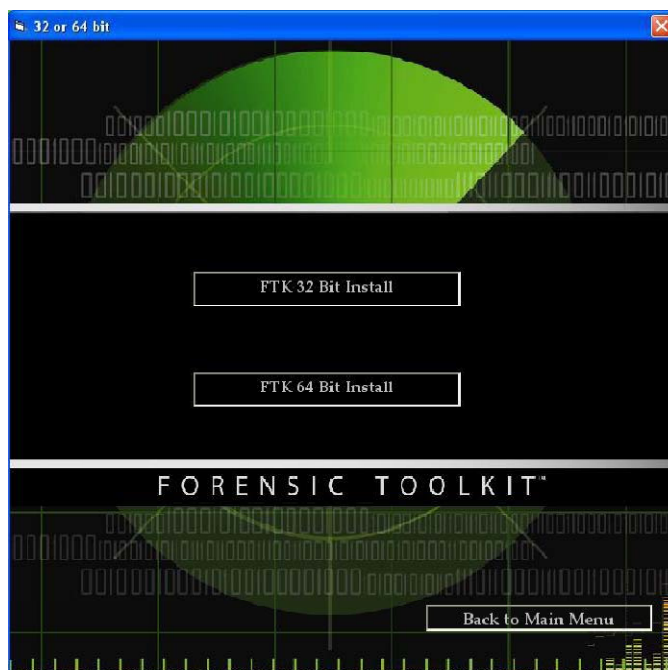
Step 5 –The latest Oracle Critical Patch Updates are provided for your convenience to patch the database. This is not a required step. If you wish to install these patches, Select **Install Database Update Patches** from the Autorun menu, and select **Patch the Database**.

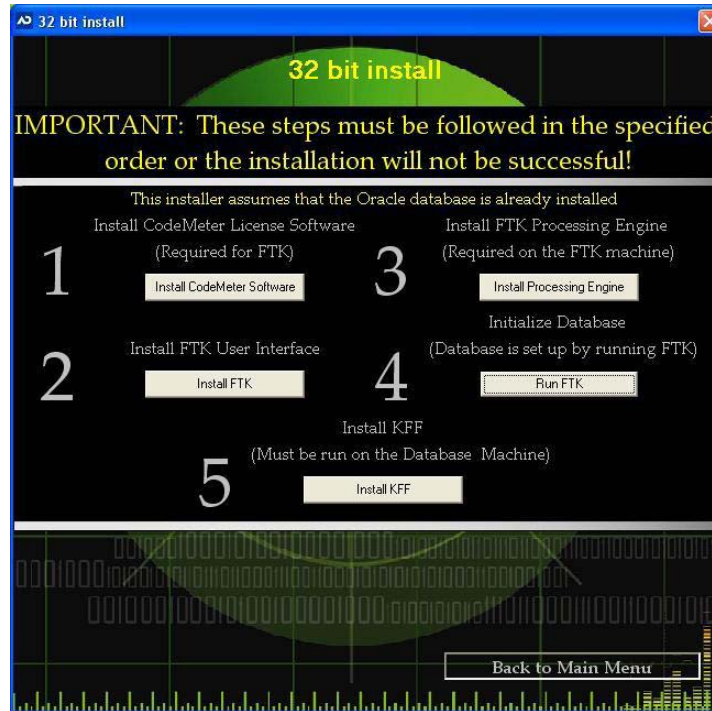
FTK Application Installation

Insert the App Install disk and launch Autorun.exe.



Select **FTK Install** and then select either the 32 bit install or 64 bit install.

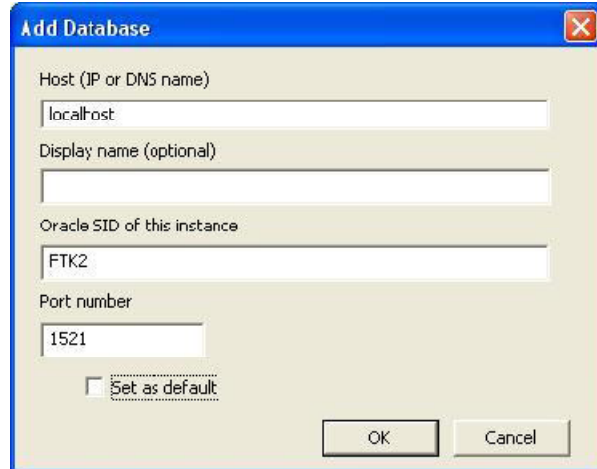




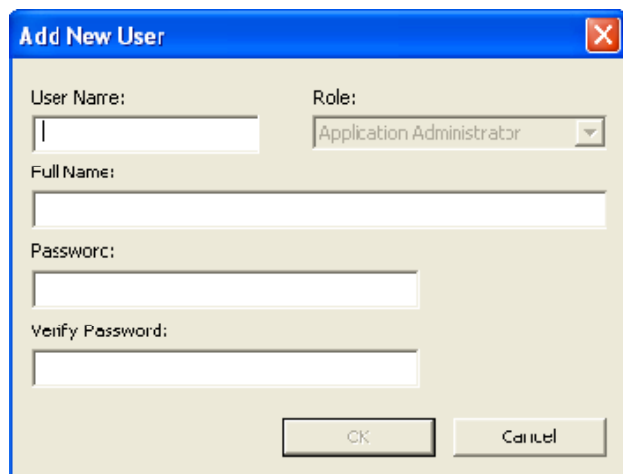
Step 1 – Install the CodeMeter dongle driver by selecting step 1 “**Install CodeMeter Software.**” Accept the defaults.

Step 2 – Install FTK by selecting step 2 “**Install FTK.**” Accept the defaults. After the install completes, a text file will open that explains some of the requirements for using distributed processing.

Step 3 - Install the Processing Engine by selecting step 3 “**Install Processing Engine.**” Accept the defaults.



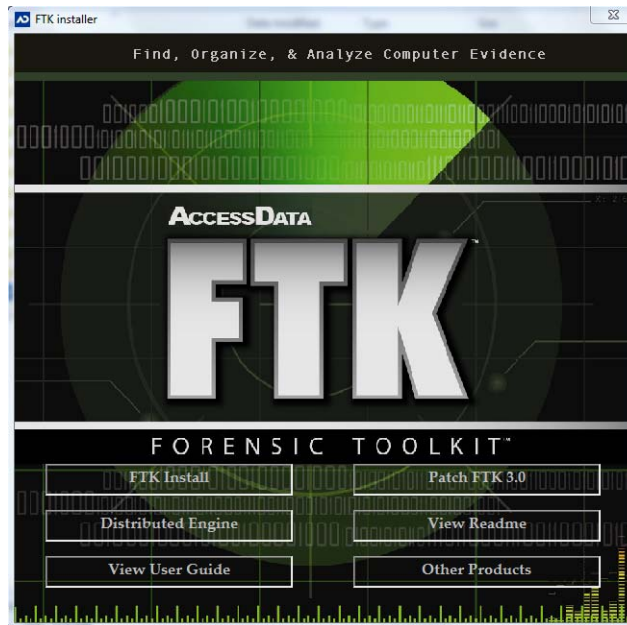
Step 4 – Run FTK 3.0 by selecting step 4 “**Run FTK.**” Accept the defaults. This will launch FTK for the first time and will create the database schema which is required before any case data can be loaded into the database.



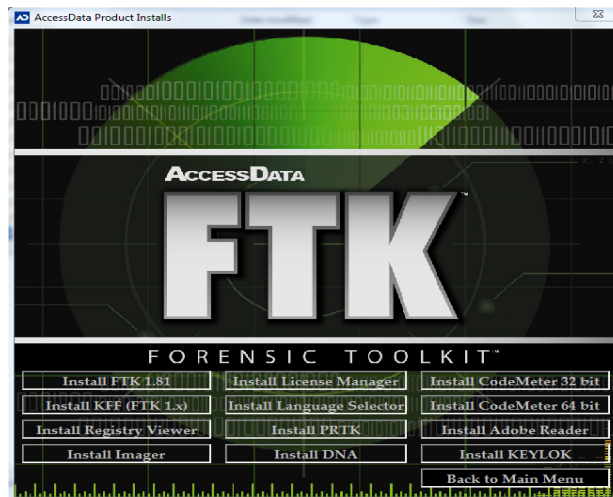
Step 5 – You will then be prompted to create the Application Administrator account for the FTK application. Do not create a user account at this time. Click **Cancel** and go to Step 6.

Step 6 – Install the KFF into the database by selecting “**Install FTK.**” Accept the defaults.

Install Additional Tools



Return to the FTK App Install main menu and select **Other Products**.



Install the following tools and accept the defaults during installation:

- Registry Viewer
- Imager
- PRTK

NETWORK LICENSE SERVER (NLS)

The AccessData (AD) Network License Service (NLS) extends the functionality of the WIBU* CmStick * and the licenses it carries across a network to allow multiple machines on the network to run AD software without each one requiring a physical, locally-installed CmStick. Install the following software on the system:

- CodeMeter Runtime 3.30a or newer
- License Manager 2.2.6 or newer
- Install NLS (Version 3.0.1) software. This version of NLS supports the following versions of Windows:
 - Windows XP 32/64 bit
 - Windows Server 2003 32/64 bit
 - Windows Vista 32/64 bit
 - Windows 7 32/64 bit
 - Windows Server 2008 32/64 bit

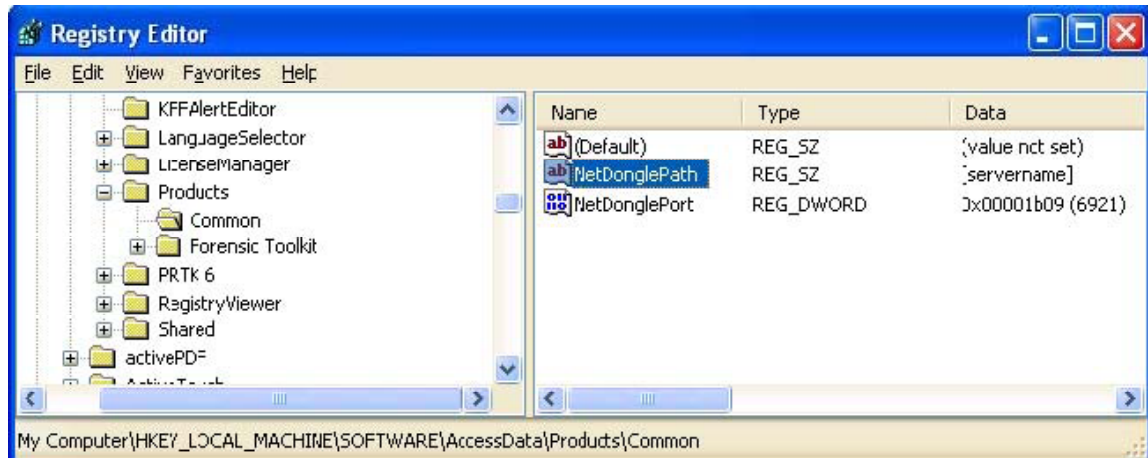
The NLS software can be found on the Instructor CD. If you do not have the Instructor CD or the software is not present, you can download it from <http://www.accessdata.com/downloads.html>.

Important NLS System Notes

- Make sure CodeMeter device is flagged as "network dongle" (i.e. License Manager will show the serial as "1181234N". To have this flag set on your CodeMeter device, please contact AccessData Technical Support)
- The system must be configured to not block incoming and outgoing traffic on TCP port 6921
- A web interface to view and revoke licenses all licenses is accessible at <http://localhost:5555> (this page can only be reached locally on the system)
- A "network dongle" cannot be used to run AccessData products locally unless the NLS server is running locally.
- Some versions of windows may not find a local NLS server when the DNS host-name of the server is provided. In those cases, it is recommended to use a static IP address.
- When using the NLS across domains, users must have permissions to access resources on both domains (either by dual-domain membership or cross-domain trust).
- When running NLS on Windows Server 2008, Terminal Services must be installed and accepting connections. If Terminal Services is not configured it will not open the port and share out the licenses correctly.
- The name of the service according to Windows is "AccessData Network License Service".

NLS Client System Notes

Any client system that needs to lease a license from the NLS server will automatically check for the License Server address information which is held in the client systems registry hive at: HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common



If the Registry key is not present, here is how to create/modify the NetDonglePath value data:

- Open Registry Editor (**Start** >> **Run** >> Type “**regedit**” >> Press **Enter**)
- Browse to the “Common” registry subkey listed above.
- If the key “NetDonglePath” does not exist, create a new key value.
- Right-click on “NetDonglePath” on the right hand side.
- Choose “**Modify**”
- Enter the [servername] value with the DNS hostname of the NLS server. (Do not include brackets)
- Close Registry Editor
- Client system must be configured to not block incoming and outgoing traffic on TCP port 6921
- If the NLS client application is having trouble reading a license either from the NLS server or from a security device (dongle), it is recommended to delete and recreate the NLS registry key located at HKEY_LOCAL_MACHINE\ SOFTWARE\AccessData\Products\Common in order to reset the licensing configuration to default.

NLS INSTALLATION INSTRUCTIONS

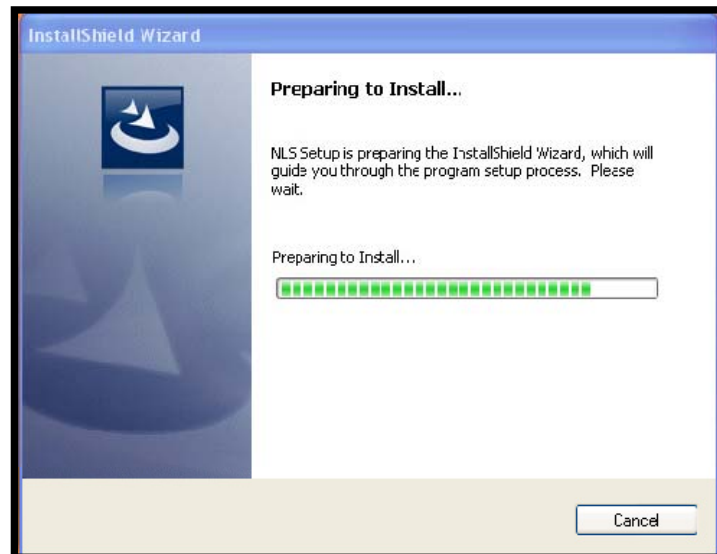
Important: You must have the CodeMeter Runtime software installed before you install the AD NLS software. The system gives you the following error message to remind you to do so:



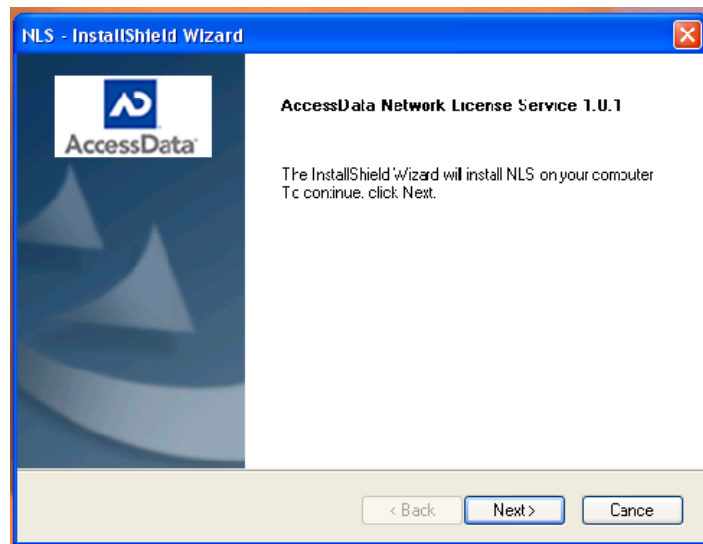
Note: The AD Network License Service CmStick ships from AccessData to serve solely as an AD network license device and will not function as a local service license CmStick. If you need to run a local copy of FTK be sure to have a local license CmStick installed. You can install both CmSticks on the same computer.

Before you can operate AD NLS, you need to set up a licensing server to serve as an AD NLS license check-out point. Perform the following steps:

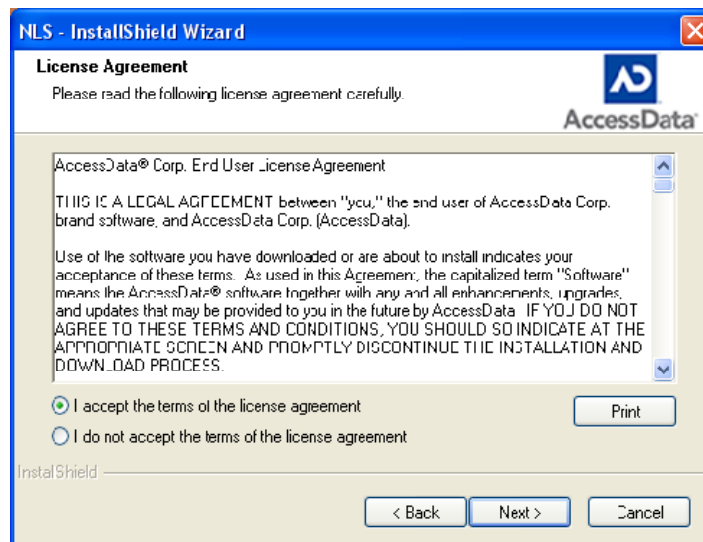
1. Open the NLS installer.



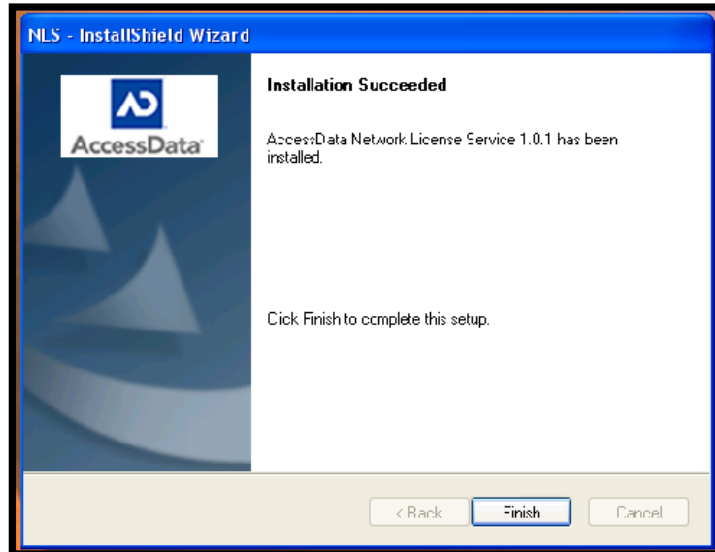
2. Click **Next** to install NLS.



3. Read through and choose to accept the agreement.



4. Wait for the installation to complete and click **Finish**.



NLS Port Information

AccessData NLS communicates on the following ports:

- **dataPort:** 6921
- **httpPort:** 5555

Note: The httpPort remains hard coded in the program.

Managing NLS Licenses

To operate an AD product such as FTK from the licensing server, you must lease a license from the NLS license server. The NLS license server keeps, on its CmStick, the network licenses available for FTK.

Viewing NLS Licenses

You can view the licenses available on your network CmStick by opening a browser window and entering <http://localhost:5555> into the address bar.

Leased licenses

	Locking Host	License product	License sub-product	License expiration date	Lease Time	Lease Expiration Time
<input type="button" value="Revoke licenses"/>						

Available licenses

License product	License sub-product	License expiration date	Count
Forensic Toolkit	Worker	05/31/2008	1
Forensic Toolkit	Worker	11/30/2008	2
Forensic Toolkit	Client	05/31/2008	1
Forensic Toolkit	Client	11/30/2008	4
eDiscovery	Worker	11/30/2008	1
eDiscovery	Client	11/30/2008	1
FTK Enterprise	Client	11/30/2008	1

Column	Information
Locking Host	The IP address of the host machine that currently leasing the license listed in the product information to the right.
License Product	The name of the licensed product the Locking Host has leased from the NLS license server. These include: <ul style="list-style-type: none"> •FTK 2.x •AD Enterprise
License Sub-Product	The element of the licensed product that is actually checked out, as from the following list: <ul style="list-style-type: none"> •Client •Worker
License Expiration Date	The date on which the license expires from usability, not the date of the lease expiration.
Lease Time	The remaining time on the lease for the current license.
Lease Expiration Time	The time at which the lease expires. The lease can be renewed up to this time.
Count	The number of each type of license available for lease

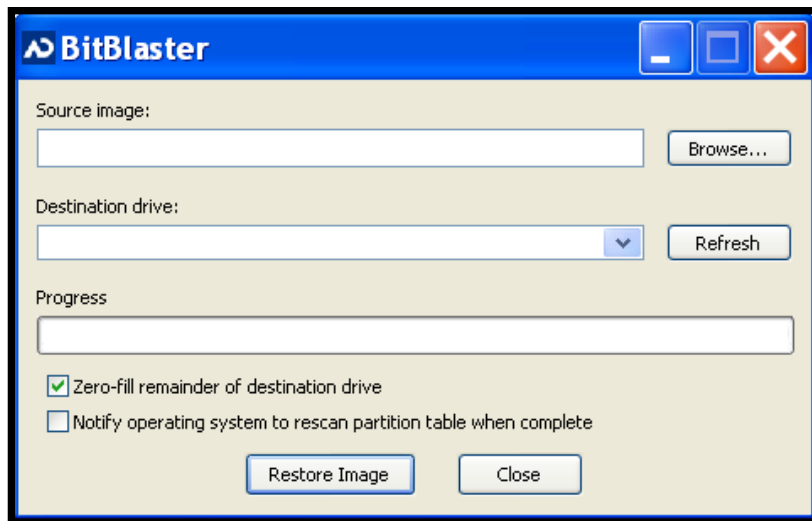
CLASS USB IMAGE PREPARATION

In module 2, Working with FTK Imager, the instructor will need to prepare USB thumb drives prior to class for the hands-on instructor led lab. In order to accomplish this task, the instructor will need sufficient USB drives for the students and the instructor. The drives should be USB 2 with a minimum of 256MB storage space.

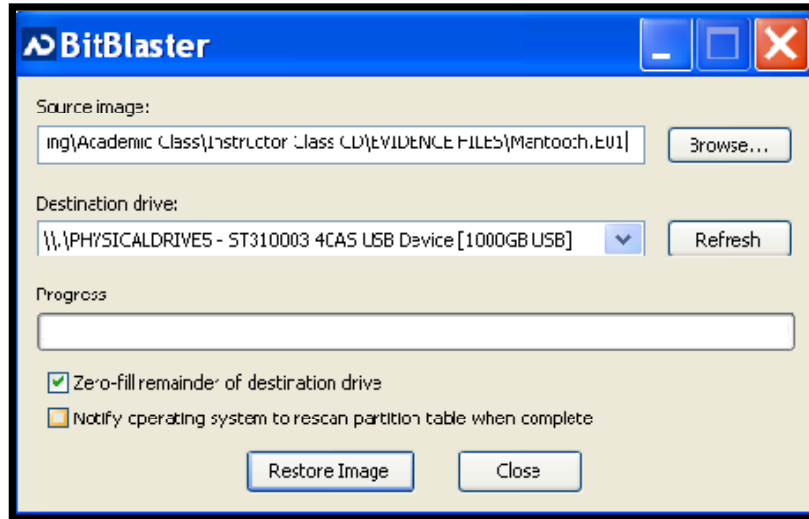
Note: These USB drives are not supplied by AccessData.

The instructor will also need the BitBlaster software located on the instructor CD. The instructor should complete the following steps:

1. Start the AccessData BitBlaster software. If you are using Windows Vista or Windows 7, the software will need to be run with Administrator rights. To accomplish this, right click on the software and select **Run as administrator** from the Windows drop down menu.



2. In the select Source Image, select the Mantoath.E01 image located in the Evidences Files folder on the instructor CD.
3. In the Destination drive box, select the USB drive from the pull-down list.
4. Ensure Zero-fill remainder of destination drive is checked.
5. Click **Restore Image**.



6. Upon completion of imaging the drive, you can remove the USB drive and insert a new one. When Windows completes recognizing the drive, click the **Refresh** button, from the pull down list under Destination drive, select the drive, and then click **Restore Image**.
7. Once the imaging process has been completed, close BitBlaster.

ACCESSDATA CERTIFIED EXAMINER



The AccessData Certified Examiner™ credential is obtained by completing a multiple choice exam which consists of Knowledge Based and Practical Based elements. Students will have 90 minutes to answer 37 multiple choice questions. 27 of the questions will be knowledge based and the remaining 10 questions will be practical based.

In preparation for the ACE program, it is recommended that students utilize their training manual focusing on the learning points and lab exercises from the course modules.

ACE Study Guide

In preparation for the process, candidates are encouraged to test their knowledge by downloading and reviewing the ACE Study Guide at [http://www.accessdata.com/downloads/media/ ACE_Study_Guide.pdf](http://www.accessdata.com/downloads/media/ACE_Study_Guide.pdf).

This study guide provides concept based questions that allow candidates to recognize areas that may need focus before beginning the ACE exam. The study guide also provides sample questions similar to what will be encountered in the Knowledge Based Assessment.

Please note the ACE credential encompasses the latest version of the following tools:

- Forensic Toolkit (FTK)
- Password Recovery Toolkit (PRTK)
- FTK Imager
- Registry Viewer


ACE Preparation Videos

The ACE Preparation Videos are also available for review for those comfortable with preparation outside of a structured environment. To access the videos, go to <http://www.accessdata.com/acePreparation.html>. The following videos may be streamed:

- Module #1 -- Overview and Imager
- Module #2 -- FTK (Part 1)
- Module #3 -- FTK (Part 2)
- Module #4 -- Registry Viewer
- Module #5 -- PRTK
- Module #6 -- Utility Integration and KBA Sample Questions

The course instructor may administer the ACE examination to students attending the class. The course is an open book/notes examination.

Step 1: Have all candidates complete the initial registration form at least one week before the examination is administered online at – <http://www.accessdata.com/ace>.

 **AccessData**
A Pioneer in Digital Investigations Since 1987

ACE CERTIFICATION REGISTRATION

If you would prefer, you may call your sales representative at 801-377-5410.

First Name	<input type="text" value="John"/>	*
Last Name	<input type="text" value="Smith"/>	*
Title	<input type="text" value="Student"/>	
Company	<input type="text"/>	*
Address	<input type="text" value="1234 N. Main Street"/>	*
City	<input type="text" value="Anyw here"/>	*
State/Province	<input type="text" value="UT"/>	
Zip	<input type="text" value="12345"/>	
Country	<input type="text" value="US"/>	*
Phone	<input type="text" value="555-555-5555"/>	*
Email	<input type="text" value="jsmith@online.com"/>	*
Organization Type	<input type="text" value="Educational Institution"/>	*
Language:	<input type="text" value="English"/>	
Comments	<input type="text" value="Student at the University of Learning."/>	

Step 2: At least two days prior to the examination, the instructor will need to obtain a passcode for the examination. This can be done by emailing the Manager of Curriculum at academic@accessdata.com.


Step 3: The ACE examination image file that will be needed for the practical portion of the examination can be found on the instructor CD.

Step 4: Students will pre-process the case evidence in FTK before beginning the examination.

Step 5: Once the processing has been completed, the instructor will direct students to the on-line examination website at:

<http://www.mytestcom.net/app/myTakeatestByCategory.cfm?accountLogin=AccessData123&GroupLoginCode=acestdrd>.

Step 6: Students will need to set up an account. From the home page, select **Need to create a new user account?**

 **AccessData**
A Pioneer in Digital Investigations Since 1987

In order to proceed, you need to log in. If the organization you're affiliated with is a Test.com customer, but you don't have a Test.com user account - you will first need to create a new user account that contains information such as your name and password. To create a new user account, select the appropriate link under the Log In button below or [click here](#).

Please log in using your username (or email), password, and account code.

Login Username:

Password:

Account Code:

[Did you forget your password?](#)

[Need to create a new user account?](#)

[Reset Account Log In](#)

Step 7: On the Account Setup page, students need to enter:

- Enter their Name
- Create a login name
- Enter their email address
- Create a password
- Select the time zone

The Join Passcode will be supplied to the students by the instructor once it is received.

Once completed, the student can hit **Create New User**.

Note: The student will need to remember their username and password to return to the exam in case of any problems.

The screenshot shows a registration form with the following fields and values:

- Account Code:** AccessData123
- Join Passcode:** AB77jf23Gq17 (required - this code should have been provided to you)
- Your Name:** John Smith (required)
- Login:** jsmith1010 (required - the name you would like to use when logging in)
- Email:** jsmith@online.com (required)
- Email (validate):** jsmith@online.com (enter the email again to validate)
- Password:** [masked with dots] (required - the password you would like to use when logging in)
- Password (validate):** [masked with dots] (enter the password again to validate)
- Time Zone Default:** Eastern with DST - US & Canada (set by defaults)
- Time Zone Override:** Ignore This Setting (dropdown menu) (choose Ignore This Setting to use the default)

Buttons and links at the bottom of the form:

- Create New User** (button)
- [Return to login screen](#) (link)
- [Reset Account Log In](#) (link)

Step 8: Once the registration has been completed, the student will be able to begin the examination.

Upon completion of the examination, the final grade will be displayed to the student. A minimum of 75% is required to pass the examination.

Note: If the student does not complete the examination within the 90 minutes allotted, the instructor can email the Manager of Curriculum at **academic@accessdata.com** and the exam will be graded manually and the results emailed to the student. All questions not answered will be counted as incorrect.

