AccessData

Forensic Toolkit

Installation Guide

Version: 4.2

AccessData®

A Pioneer in Digital Investigations Since 1987

Document date: January 28, 2013

Legal Information

AccessData Group, LLC makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, LLC reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, LLC makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, LLC reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, LLC.
588 W. 400 S.
Suite 350
Lindon, Utah 84042
U.S.A.

www.accessdata.com

AccessData Trademarks and Copyright Information

- AccessData® is a registered trademark of AccessData Group, LLC.
- Distributed Network Attack® is a registered trademark of AccessData Group, LLC.
- DNA® is a registered trademark of AccessData Group, LLC.
- Forensic Toolkit® is a registered trademark of AccessData Group, LLC.
- FTK® is a registered trademark of AccessData Group, LLC.
- Password Recovery Toolkit® is a registered trademark of AccessData Group, LLC.
- PRTK® is a registered trademark of AccessData Group, LLC.
- Registry Viewer® is a registered trademark of AccessData Group, LLC.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project .
- AFF® and AFFLIB® Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

- BSD License: Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Installing AccessData FTK

Contents

This guide details the installation of the components required for the operation of AccessData Forensic Toolkit (FTK).

Installation Information

AccessData FTK versions 2.2 and newer can be installed concurrently. Installation paths differ slightly from previous versions and registry entries are also different. This means you may not have to uninstall your earlier version of FTK 2.2 and later. You may not have to convert cases to the newest version to maintain compatibility with the database.

Note: You must run FTK under the authority of a local user account at least once to properly initialize the configuration.

Supported Operating Systems for FTK Installation

For a list of supported operating systems that you can install FTK on, see the bottom-right panel on the FTK download page:

http://www.accessdata.com/support/product-downloads/ftk-download-page.

Choosing a Database Application to Use

FTK requires using one of the following database applications:

PostgreSQL 9.0.x or 9.1.6	PostgreSQL is provided free of charge by AccessData. See Download & Preparation on page 10.
Microsoft SQL Server 2008 R2 or 2012	See Configuring Microsoft SQL Server on page 17.
Oracle 10.2.0.4	You can also use Oracle 11g if you have your own support contract for getting patches. See Best Practices for Using Oracle on page 16.

When you install FTK, you select which database application to use. If you are upgrading from a previous version of FTK, you are not required to use the same database. You can install and migrate cases to a new database application from a different database.

The database must be installed before installing FTK.

PostgreSQL is provided free of charge by AccessData. You can use your own installations of Microsoft SQL or Oracle,

Planning for a New Installation

Planning a New FTK Installation using PostgreSQL

- PostgreSQL 9.1.6 is available free of charge on the FTK download page.
  See Download & Preparation on page 10.
- You must install PostgreSQL before installing FTK.

Planning a New FTK Installation using Microsoft SQL Server

- You can use either Microsoft SQL Server 2008 R2 or 2012 with FTK.
- Before installing FTK, you must install SQL and configure it so that it will work with FTK.
  See Configuring Microsoft SQL Server on page 17.

Planning a New FTK Installation using Oracle

- You can use either Oracle 10.2.0.4 or 11g with FTK.
- You must install Oracle before installing FTK.
- When adding the database, you must configure the Oracle SID as FTK2.
  See Initializing the FTK Database on page 13.
- For information about obtaining and applying Oracle Critical Patch Updates, see Best Practices for Using Oracle (page 16).

Planning for an FTK Upgrade from a Previous Version

Verifying your version of CodeMeter

Before installing FTK, install the latest CodeMeter Runtime Kit.

See Click Install CodeMeter Software. under Installing the FTK Application (page 12)

About Upgrading and Migrating Cases

When you install a newer version of FTK, it does not replace the previous version of FTK and both versions are usable as stand-alone products. However, they do not share cases or instances of the database. When you install a newer version of FTK, it creates a new database and does not have any cases associated with it. You can upgrade or migrate cases from the previous database to work with the new version.

You can also change the database that FTK is using without changing the version of FTK.

Depending on the situation, you can do one of the following with your existing cases:

- Upgrade - You upgrade a case when you are upgrading to a new version of FTK and you are using the same type and version of the database.
- Migrate - You migrate a case when you are upgrading to a new version of FTK and you are using a different type or version of the database.
- Move - You move a case when you are using the same version of FTK and you are changing to a different type or version of the database.

When you upgrade or migrate a case to a newer version of FTK, the case is copied and the original case is still available for use with the previous version of FTK.

Planning an FTK 4.2 upgrade if you are using the same version of Oracle

- When adding the database, you must configure the Oracle SID as FTK2.
  See Initializing the FTK Database on page 13.
- If you have FTK 4.1, you can install FTK 4.2 and then upgrade your existing 4.1 cases.
  For more information, see the *Upgrading Cases* guide.
- If you have FTK 4.0 or earlier, you cannot upgrade your cases directly to 4.2. You must first upgrade them to 4.1.
  For more information, see the FTK 4.1 documentation.
- For information about obtaining and applying Oracle Critical Patch Updates, see Best Practices for Using Oracle (page 16).

Planning an FTK 4.2 upgrade if you are using PostgreSQL

- FTK 4.1 included PostgreSQL version 9.0.x while FTK 4.2 includes an updated version of PostgreSQL, 9.1.6.
  For information about PostgreSQL version 9.1.6, see the following link:
  http://www.postgresql.org/docs/current/static/release-9-1-6.html
  If you are upgrading from FTK 4.1 to 4.2, you are not required to upgrade to the new version of PostgreSQL. You can continue to use PostgreSQL 9.0.x with FTK 4.2.
  - Using PostgreSQL 9.0.x with FTK 4.2:
    - If you have FTK 4.1, you can install FTK 4.2 and then upgrade your existing 4.1 cases.
      For more information, see the *Upgrading Cases* guide.
    - If you have FTK 4.0, you cannot upgrade your cases directly to 4.2. You must first upgrade them to 4.1.
      For more information, see the FTK 4.1 documentation.
  - Using PostgreSQL 9.1.6 with FTK 4.2:
    - Install PostgreSQL 9.1.6 before installing FTK 4.2.
    - Do not uninstall PostgreSQL 9.0.x until you have backed up your cases so that you can migrate them to 4.2.
    - Do not uninstall PostgreSQL 9.0.x if you plan to continue using 4.1.
      FTK 4.1 will not run with PostgreSQL 9.1.6 and must use PostgreSQL 9.0.x.
    - If you choose to install both versions of PostgreSQL, you must use a new port when installing version 9.1.6. A new port will automatically be chosen during the installation. You should record the port that is used.
    - If you have FTK 4.1, you can install FTK 4.2 and then migrate your existing 4.1 cases.
      For more information, see the *Upgrading, Migrating, and Moving Cases* guide.
      If you have FTK 4.0, you cannot migrate your cases directly to 4.2. You must first upgrade them to 4.1.
      For more information, see the FTK 4.1 documentation.

Planning an FTK 4.2 upgrade if you are going to use Microsoft SQL Server

- In order to use Microsoft SQL Server with FTK, you must perform some SQL configuration tasks.
  See Configuring Microsoft SQL Server on page 17.

- If you have FTK 4.1, you can install SQL and FTK 4.2 and then migrate your existing 4.1 cases to SQL. For more information, see the *Upgrading, Migrating, and Moving Cases* guide.
- If you have FTK 4.0 or earlier, you cannot migrate your cases directly to 4.2. You must first upgrade them to 4.1.

For more information, see the FTK 4.1 documentation.

Prerequisites

The following prerequisites apply for installing and running FTK:

- CodeMeter Runtime software for the CodeMeter Virtual or USB CmStick.

  Note: For more information regarding the Virtual CmStick, see the Appendix "Managing Security Devices and Licenses" in the FTK User Guide.
- A WIBU-SYSTEMS CodeMeter USB or Virtual CmStick
- A supported database.
- Evidence Processing Engine

These additional AccessData programs are available to aid in processing cases:

- Known File Filter (KFF) Library
- Registry Viewer
- Language Selector
- LicenseManager

Hardware Considerations

The more powerful the available hardware, the faster FTK can analyze, process and prepare case evidence. Larger evidence files require more processing time than smaller evidence files. AccessData recommends that the various components be installed on separate machines to make more hardware resources available to the program. Thus, while the FTK and Oracle components can be installed on a single workstation, the ideal and recommended configuration uses two workstations connected by a Gigabit Ethernet connection, thus making more hardware resources available to each.

If the KFF Library is installed, it must be installed on the same computer as the database. Ideally, the latest CodeMeter Runtime, Language Selector, and LicenseManager software that AccessData provides should be installed on the same computer as the FTK application.

To further maximize performance, AccessData recommends the following:

- For both the single- and separate-workstation configurations, install the database to a large hard disk drive the database can use exclusively.
- Recommended RAM is 2 GB per processing core (e.g. an 8 core machine should have at least 16 GB of RAM). The minimum RAM must not be less than 1 GB per core.
- If your machine has less than 1 GB per core when processing multiple pieces of evidence under certain circumstances processing will fail and not recover. We recommend that the amount of RAM be 2 GB per processing core (e.g. an 8-core machine should have at least 16 GB of RAM).

  Note: AccessData has changed the way jobs are allocated to each engine based upon available resources. The new approach works by calculating the Number of Cores or hyperthreading times two (2), which determines the total number of processing threads the engine will use. Each job requires minimum of two threads plus one GB of FREE physical memory to start. So when the engine gets a request to process something, it looks at the total number of jobs it is already

working on. If it has at least two threads it can use on the new job, then it looks at free physical memory. If it also finds one GB free RAM available, then it will start up an **adprocessor.exe** to process the job.

- Do not run third-party applications on either the FTK or the database machine that will compete with FTK or the database for hardware resources.
- If you need PRTK or DNA, install it on the network, then copy any files for decryption to that machine.

Estimating Hard Disk Space Requirements

The FTK program requires a minimum of 500 megabytes of disk space for installation, although 5 gigabytes is recommended.

Oracle, where case data is stored, requires a minimum of 6 gigabytes (5 gigabytes for the basic installation) and plenty of additional room for case processing.

Additional space is required for the actual cases and for drive images and other evidence files that need to remain intact, separate from the database. These can be stored on other computers within the network.

Important: If disk space depletes while processing a case, the case data is corrupted.

To estimate the amount of hard drive space needed, apply these suggested guidelines:

- Data: every 500,000 items require one gigabyte of space in the Oracle storage location.
- Index: every 100 megabytes of text in the evidence requires 20 megabytes of space for processing in the case storage folder.

Configuration Options

FTK can be set up in three different configurations, each with its own benefits and advantages.

- Single Machine

  FTK and the database are both installed on the same box. It may be helpful in this scenario if the database is installed on a secondary drive to provide better throughput.
- Separate Machines with a new database install

  FTK and the databasecan be installed on separate boxes or on the same box. If both are installed on the same box, it is recommended that the database be installed either on a separate drive, or on a separate partition from FTK.
- Separate Machines with an existing database install

  If a compatible database is already installed, you may be able to use it with FTK. The installer runs a check for compatibility.

  Note: The database software should be installed to a physical system drive. Installing the database in a virtual machine is not supported. Installing the CodeMeter software in a virtual machine is not recommended.

  Note: AccessData recommends that you turn off firewalls and anti-virus software during installation.

  Important: If installation is being done using remote desktop to Server 2003, the remote connection needs to be established using either the **/admin** or the **/console** command.

Migration from FTK 2.2+ to FTK

FTK installs separately from an installation of FTK 2.2 so they can co-exist on one machine if you want them to; otherwise, just uninstall the previous version altogether before installing FTK.

FTK can convert any case processed using FTK 2.2 or newer to FTK through an option in the FTK UI.

For more information, see “Converting a Case From FTK 2.2+” in the FTK User Guide.

Uninstalling FTK

Important: Here are some things to remember when uninstalling FTK.

- Prompts to close running processes will not automatically close as indicated. When a user uninstalls FTK after they have been using the program and have since closed it, the dialog box on uninstall will notify the user that processes are still running and gives an option to close them automatically. If the user selects to have the process close them automatically, it cannot. The uninstall cannot work correctly until the user kills all running FTK processes manually.
- If you uninstall after a successful install, the pointer to the database will be left behind. If you want to re-install and point to a new Oracle location, you need to delete the **databases.xml** file found in the following path (in Vista):
[*drive*]:\ProgramData\AccessData\Products\Forensic Toolkit\FTK Databases.xml.

Installing AccessData Forensic Toolkit

There are two discs that ship with FTK: The FTK program install disc, and the database and KFF install disc. Each has an **Autorun.exe** to streamline the installation process.

The FTK Program can be installed on the same computer as the database. This is known as a one-box, or single-box, install. To perform a one-box install, perform the prescribed steps in the order presented, all on the same machine, switching out the DVDs as necessary.

FTK can be installed on two separate computers. The table below explains the recommended order for the installation tasks.

Table 1: Running a Two-box Install of FTK: What to do Where

Step	Machine	Task
1	Database	Install a supported database. See Installing the Database on page 10.
2	Oracle	If using Oracle, optimize Oracle Memory, by running Oradjuster.exe See Optimize the Oracle Database on page 11.
3	Oracle	If using Oracle, install Oracle Patches, if desired. See Best Practices for Using Oracle on page 16.
4	FTK	Install CodeMeter See Install CodeMeter on page 12.
5	FTK	Install FTK See Installing the FTK Application on page 12.
7	FTK	Run FTK to initialize the database See Initializing the FTK Database on page 13.
8	FTK	Install KFF See Install the KFF Library on page 14.

Important: For information regarding backup and restore for FTK when Oracle is installed on a separate box, see “Appendix F Back-up and Restore Case Data on a Two-Box Installation” on page 399 in the FTK User Guide.

Download & Preparation

Use the following procedure to download FTK from the AccessData website.

Note:

- The Exporting Emails to PST feature requires that you have either Microsoft Outlook or the Microsoft Collaboration Data Objects (CDO) installed on the same computer as the processing engine.

  If you don't have Outlook installed, you will need to install CDO manually.

  See http://www.microsoft.com/en-us/download/details.aspx?id=3671

  However, CDO does not support exporting Unicode email messages. Attempting to export Unicode messages to PST with CDO installed will result in errors and the resulting PST will be missing any Unicode email messages. To export Unicode email messages, you must install Outlook.

  You cannot have both CDO and Microsoft Outlook installed. If CDO is already installed, you must uninstall it before installing Microsoft Outlook. Likewise, you may receive an error from the FTK installer if you try to install CDO while you already have Microsoft Outlook installed.

  Microsoft Outlook 2003 and newer are supported.

1. Go to the AccessData website at: http://accessdata.com/support/adownloads#ForensicProducts.
2. On the *Product Downloads* page, expand *Forensic Toolkit (FTK)*, and click **Download**.
3. On the *Forensic Toolkit Download* page, click **Download Now** to download the following ISO files. (AccessData recommends using a download manager program such as Filezilla.)
   - For a new installation:
     - *FTK 4 Full Disk ISO Files*
     - (Optional) *Database Installation Disk* -- This disk contains the following:
       - PostgreSQL installation files if you need to install a database.
       - KFF Server and data installation files
   - For an upgrade
     - *FTK Upgrade* (32 or 64-bit)
     - (Optional) *Database Installation Disk* -- This disk contains the following:
       - PostgreSQL installation files if you need to install a database.
       - KFF Server and data installation files
4. 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.
5. Do one of the following:
   - Mount the ISO directly using a program like MagicDisc.

     AccessData recommends mounting an ISO image for the installation as it eliminates some of the problems associated with burning discs.
   - Burn the ISO to a DVD with a program such as ImgBurn.

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

Installing the Database

Before installing FTK, you must have a database installed.

See Choosing a Database Application to Use on page 4.

If you do not have one of the supported databases installed, you can install PostgreSQL, which is provided by AccessData.

If you already have a supported database installed, you can skip this section.

To Install PostgreSQL

1. Using the App Install disc or ISO, launch the Autorun.exe on the computer where FTK will reside.
2. On the *Database Installer* page, choose one of the following options:
   - 32 bit Install
   - 64 bit install
3. On the welcome screen, click **Next**.
4. Read the License Agreement. If you accept the terms of the licence agreement, select **I accept** and click **Next**.
5. In the *Destination Folder* dialog, define the location where you want to store the program files.

   You can either keep the default installation path or define a different path.

   To choose a different path, do the following:

   5a. Click **Change**.

   5b. In the *Change Current Destination Folder* dialog, either navigate to the folder or click the folder icon to create a new folder.
6. Click **Next**.
7. In the *Data Folder* dialog, define a location to store the database data files.

   To choose a different path, do the following:

   7a. Click **Change**.

   7b. In the *Change Current Destination Folder* dialog, either navigate to the folder or click the folder icon to create a new folder.
8. Click **Next**.
9. In the *PostgreSQL User Create* dialog, create a password for the PostgreSQL database system administrator.

Important: You are required to provide this password when performing certain database administrative tasks. Record this password. AccessData cannot recover this password if it is lost.

10. Click **Next**.
11. Click **Install**.
12. Click **Finish**.
13. Close the installer.

Optimize the Oracle Database

AccessData Oradjuster.exe optimizes Oracle's memory usage on your computer. This utility is particularly useful for 64-bit systems with large amounts of RAM installed. The Oradjuster utility is included on the FTK Application install disc. It can also be downloaded from the AccessData web site, www.accessdata.com/downloads. Look under Utilities.

For more information about Oradjuster, including its installation, configuration, and use, see "Appendix G AccessData Oradjuster" on page 405 of the FTK User Guide.

Choose **Optimize the Database** to run Oradjuster for the first time. During installation is the ideal time to run it because you will not have any processes running that will delay the optimization. Respond to the prompts as they appear.

Patch the Database

Choose to apply patches to the Oracle 10g database in preparation for the FTK schema to be laid down when you run FTK for the first time after all components are installed.

Note: Installing the patch can take as long as the original Oracle installation.

The FTK Application Install Disc

Place the FTK installation disc into the DVD drive and wait for the **Autorun.exe** to execute.

1. Choose the appropriate installation file for your system:
   - Click **FTK 32 Bit Install**
   - **FTK 64 Bit Install**.
2. In the Install menu, follow the steps in the order presented. For each product install, follow the prompts as they appear.

Install CodeMeter

Install the WIBU-SYSTEMS CodeMeter Runtime software for the USB CodeMeter (CmStick). The WIBU-SYSTEMS CodeMeter Runtime 4.20a is required if you are running with a Virtual CmStick. Click **Install CodeMeter Software** to launch the CodeMeter installation wizard. Follow the directions for installation, accepting all defaults, and click **Finish** to complete the installation.

If the user attempts to run FTK before installing the correct CodeMeter Runtime software and the WIBU-SYSTEMS CmStick, a message similar to the following will appear.

FIGURE 1-1 CodeMeter Error

If you are not using NLS for your security device configuration, after clicking **No,** you will see the following additional message.

FIGURE 1-2 Security Device Not Found

To remedy, click **OK**, then install the correct CodeMeter Runtime software, and connect the CmStick or run LicenseManager to generate your Virtual CmStick. Then, restart FTK.

For more information regarding CodeMeter Runtime, USB and Virtual CmSticks, and the management of Licenses, see “Appendix E Managing Security Devices and Licenses” in the FTK User Guide.

Installing the FTK Application

You must first install the database before you can install the FTK application.

1. Insert your license dongle into the computer you will be installing FTK on.
2. Using the App Install disc or ISO, launch the Autorun.exe on the computer where FTK will reside.
3. Select **FTK Install** and choose one of the following options:
   - FTK 32 Bit Install
   - FTK 64 Bit install
4. Click **Install CodeMeter Software**.

   Complete the Code Meter installation wizard and accept the default options in the installer.

   If you get prompted to change, repair, or remove CodeMeter, then you already have the current version installed and can click **Cancel, Yes**, and **Finish** and proceed to the next step.

5. Click **Install Processing Engine**.

   Complete the Evidence Processing Engine installation wizard and accept the default options in the installer.

   - The Exporting Emails to PST feature requires that you have either Microsoft Outlook or the Microsoft Collaboration Data Objects (CDO) installed on the same computer as the processing engine.

     If Microsoft Outlook is not currently installed, the Processing Engine installer will attempt to download and install CDO automatically. However, if the computer does not have an internet connection, you will need to install CDO manually.

     See http://www.microsoft.com/en-us/download/details.aspx?id=3671

     You cannot have both CDO and Microsoft Outlook installed. If CDO is already installed, you must uninstall it before installing Microsoft Outlook. Likewise, you may receive an error from the FTK installer if you try to install CDO while you already have Microsoft Outlook installed.

     Microsoft Outlook 2003 and newer are supported.

     CDO does not support exporting Unicode email messages. Attempting to export Unicode messages to PST with CDO installed will result in errors and the resulting PST will be missing any Unicode email messages. To export Unicode email messages, you must install Outlook.

   - If you are installing the processing engine on the same computer as FTK, do not select the **Install as distributed processing engine** option in the *Destination Folder* window,

6. Click **Install FTK**.

   Complete the Evidence Processing Engine installation wizard and accept the default options in the installer.

7. Click **Run FTK** to initialize the database.

   The database must already be installed prior to this step. The first time you launch FTK, it creates the database schema which is required before any case data can be loaded into the database. You will be prompted to give the location of the database you want FTK to use. This option allows a non-local database to be specified even if a local database is present.

   See Initializing the FTK Database on page 13.

8. (Optional) Click **Install KFF**. This step can only be done on the computer where the database resides. You must initialize the database before you do this step.

   See Install the KFF Library on page 14.

Initializing the FTK Database

1. Open FTK.
2. If FTK does not detect an existing database connection for that version of FTK, you will be prompted to *Add Database*.
3. In the *RDBMS* drop-down menu, select the brand of database to which you are connecting to FTK.
4. Specify the server hosting the database in the *Host* field. If the database is on the same computer as FTK, you can leave this field empty.
5. (Optional) Give the database connection a nickname in the *Display name* field.
6. Do one of the following:
   - If you are using Oracle, you must configure the *Oracle SID* to be FTK2.
   - If you are using PostgreSQL or MS SQL Server, for the *PostgreSQL dbname* or *mssql sa,* you can use the default values or enter your own value. If you enter your own value, make sure that you record it so that you know the database name.
7. Do not change the *Port number* fields unless you have a custom database configuration.
8. If you are using MS SQL Server, you can check **Use Integrated Security** to use your Windows authentication credentials.

9. Click **OK.**

   If the connection attempt to the database was successful, the database will be initialized.

10. Upon completion of the initialization process, you will be prompted to create the Application Administrator account for that version of the database schema. Enter the desired credentials for the account and click **OK**.

11. Log into the database using the Application Administrator account credentials via the *Please Authenticate* dialog.

12. A successful login enables you to use the *Case Manager* window. From here, you can create other user accounts and perform other administrative tasks.

Install the KFF Library

Starting with FTK 4.2, there are two distinct components of KFF:

- The KFF Server
- The KFF Data Libraries

Each component is installed separately. FTK The KFF database is no loner stored in the shared evidence database but on the file system in EDB format.

You do the following to install and add hash sets to KFF:

- Install the KFF Server

  When you install the KFF Server, you specify the location for the KFF Server and the data.

- Install or import KFF data
  - As part of the KFF installation, you can install pre-configured hash libraries.

    Starting with FTK 4.2, only the Hash Library from NIST NSRL (Feb 2012) is included in the installation. The NDIC HashKeeper and DHS libraries are available on the AccessData download site.

    For information about KFF libraries, see the FTK *User Guide*.

    After you install hash sets, you cannot delete them.

    You can import your own custom data.

If you are upgrading from FTK 4.1, you can use 4.1 to export your existing KFF groups and then import them into FTK 4.2.

For information about KFF libraries, see the FTK *User Guide*.

If you continue to use FTK 4.1, you will use the 4.1 version of KFF, not the new KFF version for 4.2.

To install KFF

Important: To install the KFF server, Microsoft .NET Framework 4 is required. If you do not have .NET installed, you will be prompted to install it. If you install .NET at this time, the computer must be restarted before installing KFF. On 32-bit computers, the installer will prompt you to do this, but on 64-bit computers, you are not prompted and the KFF Server Setup Wizard opens. You must cancel the wizard and restart the computer manually before restarting the KFF Server installation.

1. Using the Database installation disc or ISO, launch the Autorun.exe on the FTK computer.

   See Download & Preparation **on page 10.**

2. Install the KFF Server.

   2a. On the installation page, click KFF Install.

   2b. Click Install KFF Server.

   2c. Specify the location that you want to install FKK to

   2d. Complete the installation wizard.

3. Configure the KFF settings.
   - 3a. Specify the Storage Directory for KFF data.
   - 3b. Use the default interface port settings unless you want to use of different ports for your environment:
     - KFF Management Interface. (Default port is 3799)
     - KFF Lookup Interface. (Default port is 3798)
   - 3c. (Optional) If you want to encrypt the KFF data, specify a Management Communication Certificate.
   - 3d. Click Close.
4. (Optional) Install the KFF NSRL Data.

   After you install hash sets, you cannot delete them.
   - 4a. On the KFF installation page, click Install KFF Data.
   - 4b. Complete the wizard.

For more information about the KFF Library, see “Appendix D The KFF Library” on page 351 of the FTK User Guide.

AccessData Distributed Processing

This release of FTK supports Distributed Processing Engines (DPEs). Distributed Processing allows the installation of up to three additional processing engines to share the work load of processing evidence in a case

Additional Programs

The following AccessData programs may also be useful and are found on your product installation disc(s).

Language Selector

To change to another supported language other than the default English (United States) that ships with FTK, Language Selector must be installed.

Install Language Selector

To install Language Selector

1. From the FTK install disc Autorun Main Menu, click **Install Other Products**, then click **Install Language Selector.**
2. The Language Selector Installer runs. Click **Next** to continue.
3. Read and accept the License Agreement. Click **Next** to continue.
4. Click **Finish**.

Using Language Selector

Language Selector has a very simple interface.

To run Language Selector

1. Do one of the following:
   - Click **Start > All Programs > AccessData > Language Selector > Language Selector.**
   - Click the Language Selector Icon on your desktop.

2. Click the **Select Languages** drop-down to select the language to use. Languages to choose from are as follows: The “Products supporting this language” text box indicates the AccessData programs that will be affected by the language selection.

Table 2: Language Selector Supported Languages

• Chinese (Simplified, PRC)	• Korean (Korea)
• Dutch (Netherlands)	• Portuguese (Brazil)
• English (United States)	• Russian (Russia)
• French (France)	• Spanish (Spain, Traditional Sort)
• German (Germany)	• Swedish (Sweden)
• Italian (Italy)	• Turkish (Turkey)
• Japanese (Japan)	

   The File menu contains two choices:
   - Select Language
   - Exit

   The Help menu contains one choice:
   - About — Provides version and copyright information.

3. Click **Save Settings** to save selections and close Language Selector.

LicenseManager

If licenses need to be managed, LicenseManager must be installed. For more information on LicenseManager, see the FTK User Guide.

Also, make sure the current versions of any other programs required for the investigation are installed, including AccessData Registry Viewer, and AccessData Password Recovery Toolkit, or AccessData Distributed Network Attack.

Configuring and Managing Databases for FTK

This section provides information that you need to know to configure and manage the database for use with FTK.

For more information, see your SQL Server documentation or contact Technical Support.

Best Practices for Using Oracle

If you are using Oracle 10g, you should consider installing Oracle Critical Patch Updates. You can download the Oracle Critical Patch Update 38 and 45 (April 2011) from the AccessData Support Downloads web page:

http://www.accessdata.com/support/product-downloads > Utilities

For newer updates of Oracle 10, or to use Oracle 11g with its updates, you must have an Oracle support contract. You can upload updates from the Oracle web site (http://www.oracle.com/technetwork/topics/security/alerts-086861.html).

To install an Oracle Critical Patch Update, first back up the database, and then close all programs before you install the patch. (58583, 58248)

If you do not have an Oracle support contract, consider changing from an Oracle database to PostgreSQL, which is available at no cost on the FTK Download page. You can easily migrate your cases from Oracle to PostgreSQL. For more information, see the *Upgrading, Migrating, and Moving Cases* guide.

Configuring Microsoft SQL Server

If you are installing Microsoft SQL Server, perform the following configuration steps:

Configure SQL options during the SQL Installation

1. From the *Setup Role* page, choose **SQL Server Feature Installation**.
2. From the *Feature Selection* page, select the following features:
   - *Database Engine Services*
     - *Full-Text Search*
   - *Management Tools- Basic*
     - *Management Tools - Complete*
3. On the *Instance Configuration* page you can choose either **Default instance** or **Named instance**.
   If this SQL database is used exclusively by FTK, it is much simpler to choose default instance. If you choose named instance, remember the name that you give to the instance.)
4. On the *Server Configuration* page, do the following:
   4a. Click **Use the same account for all SQL Server services**.
   4b. Specify a username and password for all service accounts.
5. On the *Database Engine Configuration* page, choose the **Mixed Mode** authentication mode.

Configure SQL with the following collation

- "SQL_Latin1_General_CP1_CI_AS"

Enable TCP/IP for SQL Server

1. Open the SQL Server Configuration Manager.
   (Start > All Programs > Microsoft SQL Server > Configuration Tools > SQL Server Configuration Manager)
2. Expand *SQL Server Network Configuration*.
3. Select the SQL Instance to check or change.
4. Right-click Protocol Name **TCP/IP** and click **Enable**.
5. Stop and Start the SQL Service.

Configure Microsoft SQL Server authentication mode, remote connections, and default storage location settings

1. Open the SQL Server Management Studio (SSMS).
   (Start > All Programs > Microsoft SQL Server > Configuration Tools > SQL Server Configuration Manager.)
2. Enter the correct server name or servername/instance, authentication (Windows Authentication, SQL Authentication), and credentials.

3. Once connected to the SQL Server, in the *Object Explorer Pane*, right-click **Properties** of the server/instance that you want to configure.
4. To check or change the SQL authentication mode, do the following:
   4a. Click the **Security** tab.
   4b. Under *Server Authentication*, select **SQL Server and Windows**.
5. (Optional) To enable remote connections to the server, do the following:
   5a. Click the **Connections** tab.
   5b. Under *Remote Server Connections*, check **Allow remote connections to this server** is enabled.
6. To make changes to the database default storage locations, do the following:
   6a. Click the **Database Settings** tab.
   6b. Under *Database default locations*, change the *Data* and *Log* locations as desired.
7. Click **OK**.
8. Stop and restart the SQL service.

Maintaining and Optimizing Microsoft SQL Server

After you install FTK and initialize the database, you can do the following to manage and optimize SQL.

Configuring Case User Databases: Initial Size and Autogrowth

Case databases should be set to an estimated size based on the initial size of the data that will be ingested into it after the case is created. This can be found under the *Database Properties* > *Files* tab.

AccessData applications use files and filegroups. The files and data stored is within the following:

File (ex ADG53_####_TSf) in Filegroup (ex ADG53_####_TS)

This is what should be considered for changes to initial size and autogrowth settings.

A very rough rule is that the database will grow to 1/3 of the ingested data. This is not an exact estimate as multiple factors have to be taken into account regarding the data. Depending on the size and work being done in the case, Autogrowth should be considered as a percent or static size. Autogrowth for the case file can be initially set to 100 MB and 50 MB for the log file for the case database. These values should be monitored and changed as appropriate.

The database requiring growth during operation can hamper performance due to the server and disk activity required to grow the database as it becomes full.

To configure datafile and transaction log file settings

1. Open the SQL Server Management Studio (SSMS).
   (Start > All Programs > Microsoft SQL Server > Configuration Tools > SQL Management Studio.)
2. Enter the correct server name or servername/instance, authentication (Windows Authentication, SQL Authentication), and credentials.
3. Once connected to the SQL Server, in the *Object Explorer Pane*, right-click **Properties** on the FTK database.
   The default database name that FTK created is ADG. If you used a different name, select that database.
4. Click **Files**.
5. Under *Database* files, do the following:
   5a. For the datafile (first row), set the autogrowth setting from 1 MB to 100 MB.

5b. For the transaction log file (second row), set the autogrowth setting from 10% to 50 MB.

6. Repeat for all FTK databases.
7. Click **OK**.
8. Stop and restart the SQL service.

MS SQL Memory Allocation.

A general rule for memory allocation to the Windows OS is that for first 16 GB of Memory the operating system is allocated 4 GB. Afterwards for every additional 4 GB of memory the system gets 1 GB. SQL by default will take as much memory as possible. For Windows servers running only Microsoft SQL Server the following rule should be adhered to for Maximum memory allocated to the application subtracted by what will be required by the OS. Systems sharing memory with application other than MSSQL a maximum memory should be set as to not take away all available memory for the other applications.

Below is a T SQL script that set the max memory to the general rule or to set the memory based on a percent of the total available physical memory.

----------BEGIN COPY----------

```
USE [master]

--Rule: For the first 16 GB of ram in a system the operating system gets 4GB of it. After that for every 4GB the operating system gets 1GB.

DECLARE @PROC nvarchar (Max), @pmemMB INT, @subMB INT, @setMB INT, @setbypercent bit, @percentMB DECIMAL

SET @PROC = 'sp_configure ''show advanced options'', 1 '

EXEC SP_EXECUTESQL @PROC

SET @setbypercent = 0 --1 = set by percent , 0 = Based off rule (Recommend 0 if single instance of MSSQL is ONLY on server)

SET @percentMB = 50 -- allocate x percent of total CPU to SQL Max Memory

SET @PROC = 'RECONFIGURE'

EXEC SP_EXECUTESQL @PROC

select @pmemMB =  physical_memory_in_bytes/(1024*1024) from sys.dm_os_sys_info

IF @setbypercent = 0

BEGIN

    SET @subMB = 4096

    IF (@pmemMB > 16384)

        SET @subMB = (select (@subMB+(@pmemMB - 16384)/4))

    SET @setMB = @pmemMB-@subMB

END

ELSE

        SET @setMB =  @pmemMB* ( @percentMB/100)

SET @PROC = 'EXEC sys.sp_configure N''min server memory (MB)'', N''0'''

EXEC SP_EXECUTESQL @PROC

SET @PROC = 'EXEC sys.sp_configure N''max server memory (MB)'', N'''+CAST(CAST((@setMB ) AS INT)AS NVARCHAR(max))+''''
```

```
EXEC SP_EXECUTESQL @PROC
SET @PROC = 'RECONFIGURE WITH OVERRIDE'
EXEC SP_EXECUTESQL @PROC
```

----------END COPY----------

MS SQL Temp DB

SQL and the application use the tempdb database for storage of various temporary tables. Improved performance can be found with setting an increased size for the MDF file as well as having additional tempdb files allocated to the database.

Below is a script that increases the initial tempdb mdf file to 2 GB and Log file to 1 GB. It will also add additional tempdb mdf files, all 2 db in size for every physical core to a maximum of 8 total files.

----------BEGIN COPY----------

```
USE master
ALTER DATABASE [tempdb] MODIFY FILE ( NAME = N'tempdev', SIZE = 2097152KB )
GO
ALTER DATABASE [tempdb] MODIFY FILE ( NAME = N'templog', SIZE = 1048576KB )
GO

DECLARE @HTR int, @dflocation nvarchar(max), @PROC nvarchar(max)
SELECT @HTR =hyperthread_ratio
 FROM sys.dm_os_sys_info
 IF (@HTR > 8)
        SET @HTR = 8
 SET @dflocation = ( SELECT SUBSTRING(physical_name, 1, CHARINDEX(N'tempdb.mdf',
LOWER(physical_name)) - 1) DataFileLocation
         FROM master.sys.master_files
        WHERE database_id = 2 AND FILE_ID = 1 )
 DECLARE @CNT INT
 SET @CNT = 1
 WHILE (@CNT !=@HTR)
 BEGIN
    SET @PROC = N'ALTER DATABASE [tempdb] ADD FILE ( NAME = N''tempdb'+CAST(@CNT as
nvarchar(2))+''', FILENAME = N'''+@dflocation+'tempdev'+CAST(@CNT as nvarchar(2))+'.ndf'' , SIZE =
2097152KB , FILEGROWTH = 10%)'
    PRINT @PROC
    EXEC SP_EXECUTESQL @PROC
    SET @CNT =@CNT +1
 END
```

----------END COPY----------

Maintenance Jobs

You can create maintenance jobs to perform defragmentation and rebuilding of indexes, integrity and consistency checks, DBCC checkdb, backups, blocking sessions and database file monitor.

Maintenance jobs for backup, defragmentation and rebuild of indexes are default maintenance tasks that can be created via SSMS.

A rough estimate of a defragmentation job would be every day with a rebuild once a week. Actual expected rules are indexes with pages > 100 and fragmentation over 60 become rebuild and anything below to be re-org.

Maintenance jobs for Backups Full, Differential, Transaction should be based on your environment.These maintenance tasks can hamper performance as they can run into production hours depending on size of the database.

Other SQL Best Practices

Additional improvements can be made by setting the SQL Recovery Model to "Simple". This can result in less writes, providing less I/O to disk, and storage to the Log file (LDF). However, this can put you at risk as this disallows transaction backups and Tail Log restores.

DBCC, database file monitoring, and blocking sessions are advanced SQL items used to troubleshoot ad resolve issues that may be occurring. These are least likely to be needed for your system's day-to-day operation.