



AccessData[®]

Forensic Toolkit[®]

System Specifications Guide

March 2010

When it comes to performing effective and timely investigations, we recommend examiners take into consideration the demands the software, and specifically Oracle, will make on their hardware resources. Depending on the size and scope of a given investigation, Forensic Toolkit® 3 (FTK®) and AccessData Enterprise, will push hardware resources to their limits.

With FTK 3, examiners have several configuration options available to them during the installation process:

- 1) Install the FTK Client User Interface (UI), Client-side Processing Engine and Oracle database on a single machine.
- 2) Install the FTK Client UI and Client-side Processing Engine on one machine and the Oracle database on a second separate machine.
- 3) Install the FTK Client UI, Client-side Processing Engine and Oracle database on a single machine and the Distributed Processing Engine on separate drone machines.
- 4) Install the FTK Client UI and Client-side Processing Engine on one machine, Oracle on a separate machine and the Distributed Processing Engine on separate drone computers.

FTK Components and Their System Requirements

FTK is made up of four separate components/applications, each of which are installed separately and perform different functions. These components are the Oracle Database, the FTK Client UI, the Client-side Processing Engine and the Distributed Processing Engine. When configuring a system to run FTK, it is helpful to understand the hardware requirements of each of these components/applications and the strain these components each place on the hardware.

Oracle Database – The Oracle database is the foundation of the FTK application. Oracle stores the processed metadata, and performs all the queries, sorts, filters, file listing and other functions requested by the Client UI.

RAM: To achieve maximum product performance, especially during review, it is best to provide Oracle with as much RAM as possible. While it is possible for Oracle to operate on a system with only 4 gigs of RAM, the responsiveness of the FTK Client UI will be slow. 8 gigs of RAM is recommended for cases with up to 4 million record items. 12-16 gigs of RAM is recommended for cases with 4-8 million record items. Cases with over 8 million record items should be processed and analyzed on systems with 16 gigs of RAM or more.

OS: The Oracle database will run on all versions of Windows XP, 2003, Vista, 2008 and Windows 7. A 64-bit OS is not mandatory but is very strongly recommended, because Oracle's responsiveness is as much as 3-5 times faster on a 64-bit OS compared to a 32-bit OS.

CPU: Oracle will run on most processors that are core-2 duo or greater. A Quad processor is the recommended minimum CPU for a stand-alone forensic examiner machine. Oracle has been shown to run extremely well on the Intel i7. For dedicated Oracle boxes, hosting 4 or more simultaneous review sessions, an i7 or Dual Quad is recommended. Oracle can place a significant demand on the CPU during review. However, Oracle's demand on the CPU during image processing is relatively small.

CPU to Memory: AccessData recommends 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). The minimum RAM must not be less than 1 GB per core

Hard Disk, Storage Requirements and I/O Speed: The responsiveness of the UI is dependent on the responsiveness of Oracle. Oracle's responsiveness, especially during review, is affected most by the amount of RAM in the computer and secondly by the I/O read speed of the hard drive hosting the Oracle database. While hosting Oracle on a 7200 RPM drive is an option, the Client UI responsiveness and pre-processing times will suffer with these slower 7200 RPM drives, especially with larger cases. Single 10,000 or 15,000 RPM drives or a set of hardware RAIDed drives will provide much better performance. If using a hardware RAID, configure the Oracle box RAID0, RAID1 or RAID10. Avoid RAID5 for the Oracle database if possible. Solid state drives such as the Intel x25-M, x25-E series or Corsair P series will provide the highest level of Oracle performance and do not need to be RAIDed. (Note: Performance between different solid state drives varies dramatically. Make sure to research the drive performance data before making a purchase.)

For workstations, if the physical case allows for the space Oracle should have its own dedicated drive separate from the drive(s) used by the OS, or to store the E01 Image storage and case folder.

For laptops with a single internal hard drive, Oracle should be installed on the OS drive. If possible, laptop users should store the case folder and E01 image on an external drive. The connection to the external drive should be ESATA if available. Firewire and USB2 are viable second options, but will not be as fast as ESATA.

The storage requirements for the Oracle database are small relative to the storage requirements of the case folder and the E01 images. A case will usually take up only about 5 gigs for every million record items. The storage requirements are therefore directly dependent upon the number of active cases in the database. For most single Examiner machines 256 gigs of storage space for Oracle should be sufficient. For centralized Oracle servers 1 TB will usually be more than enough room.

Network Speed: 1 gig is recommended for distributed processing and remote review. 100Mbit is discouraged.

Database Optimization: Running Oradjuster to optimize the database is strongly recommended to achieve maximum database performance and the best FTK Client UI responsiveness. View this instructional webinar on how to use Oradjuster: [Oracle Adjuster Utility and UI Performance Tips](#)

FTK Processing Engine and FTK Distributed Processing Engine: The processing engine and distributed processing engines as their names suggest, perform the majority of the work when processing an image. The processing engine also performs live search during review.

CPU: When processing an image, usually the system is slowed down by either the capability of the CPU or the I/O speed of the drive hosting the image file. A Core-2 Quad processor is a good match for a system where the image file is stored on a 7200 RPM drive. If the image is stored on a RAID or high speed NAS then an i7 or dual Quad core would probably be a better CPU option. Having a slow CPU, such as a core-2 duo is not a problem, it just means the image will take longer to process.

RAM: The processing engine will adjust the number of threads based on the amount of RAM in the computer. 8 gigs or more is a suggested target but not mandatory. It is not recommended to run the processing engines on a machine with less than 4 gigs of RAM.

OS: The processing engines will run on all versions of Windows XP, 2003, Vista, 2008 and Windows 7. A 64-bit OS is not mandatory but strongly recommended. Vista and Windows 7 have much better memory management than Windows XP. Therefore, Vista-64 and Windows 7 are the manufacturer's recommended operating systems.

Hard Disk, Storage Requirements and I/O Speed: Many times the I/O access speed to the image will be the limiting factor when it comes to total processing time. Because most E01 images take up a lot of space, they are usually stored on large capacity, slower 7200 RPM drives. When connecting to an external hard drive, eSATA is going to provide faster response than USB or Firewire. While storing the image on a much faster drive such as a solid state drive (SSD) or a RAID array is an option, in many situations this may not cost effective. It is important not to store the image or case folder on the same drive as Oracle if at all possible, as performance will be significantly impacted.

Network Speed: 1 Gigbit network card or faster is necessary if using the Distributed Processing Engine or connecting to an image that is stored in a remote location such as a NAS.

FTK Client User Interface (UI): The Client user interface is an application that is used to manage the case, launch the Processing Engines and provide a user with a view into the metadata. The hardware requirements for the FTK Client User Interface are the least onerous of the four components. If the UI is slow and/or non-responsive it is usually a result of an issue with the Oracle database and not the UI machine.

CPU: When running the FTK Client UI, the CPU will rarely be taxed to its full capacity. Any system with a Core-2 duo or better should provide a reasonably fast UI experience. As stated above, the setup of the machine running the Oracle database is what has the greatest impact on UI performance.

RAM: The machine should have a minimum of 4 gigs of RAM.

OS: The FTK UI will run on all versions of Windows XP, 2003, Vista, Windows 2008 and Windows 7. A 64-bit OS is not mandatory but recommended. Vista and Windows 7 have much better memory management than Windows XP. Therefore, Vista-64 and Windows 7 are the manufacturer's recommended operating systems.

USB Slot: The FTK Client UI requires a security license. This license is usually stored on the CodeMeter dongle. If a USB slot is unavailable, the Network License Service (NLS) is an option.

There are two primary configurations that need to be considered when planning to install FTK 3.

- **Configuration 1:**
 - System 1: All components (GUI/Worker/Database) are on a single system
 - Systems 2-4: Distributed Processing Engine (optional)
- **Configuration 2:**
 - System 1: GUI/Worker
 - System 2: Database
 - System 3-5: Distributed Processing Engine (optional)

NOTE: All configurations will require one available USB slot for the hardware security device (CodeMeter/Dongle) unless using NLS (Network Licensing Services).

Specifications for FTK 3 with the Oracle Database, FTK UI and Processing Engine on the Same Machine

If installing Oracle, the UI, and the processing engine all on the same machine AccessData recommends one of the following hardware specifications:

	Recommended	Ideal
Processor	Intel® Quad Core or AMD equivalent	Intel® Dual Quad Core Xeon, i7 Nehalem or AMD equivalent
CD/DVD Drive	DVD	DVD
RAM	6 GB (DDR3) / 4-8 GB (DDR2)	12 GB (DDR3) / 16 GB (DDR2)
OS / Application drive	150 GB 10,000 – 15,000 RPM	150 GB 10,000 – 15,000 RPM
Storage for Oracle database	250 GB 10,000-15,000 RPM drive dedicated exclusively to running Oracle	125GB-250 GB Solid State Drive (SSD) dedicated exclusively to Oracle.
Network Card	Gigabit	Gigabit
Hard Drive Speed	7,200 RPM	10,000 - 15,000 RPM
HW RAID Controller	Highly recommended for Oracle database. Configure with RAID 0, 10, but avoid RAID5	Highly recommended for Oracle Database but not critical for SSD drives.
Drive Configuration	Drive Set 1: OS Drive Set 2: Oracle Database Drive Set 3: Case Folder and HD Image	Drive Set 1: OS (RAID 1) Drive Set 2: Oracle Database (SSD or HW RAID) Drive Set 3: Case Folder and HD Image
Operating Systems	MS Windows XP/Vista/2003/2008/Windows7 (64-bit)	MS Windows Vista/2008/Windows7 (64-bit)

Performance and Storage Considerations

- 1) The Oracle database should be on its own hard drive, Solid State Drive (SSD) or hardware RAID array, separate from the operating system. For hardware RAIDs RAID 0 gives the best performance but RAID 0 provides no recovery from drive failure. RAID 0 should only be considered if automatic scheduled backups are available. RAID 1+0 will provide similar performance as RAID 0 with the additional advantage of redundancy if a drive fails. RAID 5 should be avoided for use with databases.
- 2) It is strongly recommended to configure antivirus to exclude the Oracle database, temp, images, and index folders.
- 3) It is recommended to turn off indexing, compression and/or EFS encryption. (By default, indexing of files and folders is on.)
- 4) 10,000 RPM drives are recommended for the OS drive. A single 10,000 RPM drive will provide slightly better performance than two 7200 RPM drives configured with RAID 0 (software). A slightly faster option would be a 15,000 RPM SAS drive used for the OS, as it will provide the same performance as three 7200 RPM drives configured with RAID 0. The fastest drives are solid state drives, such as an Intel x25-M SSD drive, which will significantly outperform even 15,000 SAS drive.
- 5) Hardware RAID controllers will provide substantially better performance than an OS-based software RAID configuration. It is recommended to use a hardware RAID controller with at least 256MB of write-through cache. If activating the write-through cache,

it is strongly recommended to purchase a card with a backup-battery for the RAID controller and enabling the write-through cache. Enabling the write-through cache without the backup-battery creates the potential for database corruption in the event of a system crash or power failure.

- 6) For recommendations on hard drives and hardware RAID controllers please see:
 - a) Hard Drives: <http://www.tomshardware.com/charts/3-5-hard-drive-charts/benchmarks,24.html>
 - b) RAID Controllers: <http://www.maximumpc.com/sites/future.p2technology.com/files/imce-images/RAIDbenchmarksBIG.gif>
- 7) To estimate roughly the amount of storage space to support your processing load you should consider these estimates:
 - a) Database: Every 1 million record items requires roughly 5 GB of space on the Oracle drive.
 - b) Generally, the index will be about 25-30% the size of the compressed image.

Specification for FTK 3 UI and Processing Engine on one machine and Oracle on a Separate (2nd) Machine (2 Node Configuration)

Node 1: Specifications for GUI and Worker

If installing the embedded Oracle database on a second machine or using an existing Oracle infrastructure, AccessData recommends one of the following hardware specifications for the machine running the FTK UI and Processing Engine:

	Recommended	Ideal
Processor	Intel® Quad Core or AMD equivalent	Intel® Dual Quad Core, i7 or AMD equivalent
CD/DVD Drive	DVD	DVD
RAM	4 GB (32-bit) / 8GB (64-bit)	8 GB (64-bit)
OS/Application Drive Size	150GB	150 GB (10,000 RPM or better)
Network Card	Gigabit	Gigabit
Hard Drive Speed	7,200 RPM	10,000-15,000 RPM or SSD
Storage for Index and Images	As necessary	As necessary
Operating System	MS Windows XP/Vista (32bit) or Vista/Windows7(64-bit)	MS Windows Vista/Windows7/Windows 2008 (64-bit)
Drive Configuration	Drive Set 1: OS Drive Set 2: Hard Drive Image and Case Folder	Drive Set 1: OS (RAID 1) Drive Set 2: Hard Drive Image and Case Folder

Node 2: Stand-alone Database Specifications for Windows-based Oracle

If installing the embedded Oracle database on a second machine, AccessData recommends the following hardware specifications.

	Recommended	Ideal
Processor	Intel® Quad Core or AMD equivalent	Intel® Dual Quad Core Xeon, i7 Nehalem or AMD equivalent
CD/DVD Drive	DVD	DVD
RAM	6 GB (DDR3) / 4-8 GB (DDR2)	12 GB (DDR3) / 16 GB (DDR2)
OS / Application drive	150 GB 10,000 – 15,000 RPM	150 GB 10,000 – 15,000 RPM
Storage for Oracle database	250 GB 10,000-15,000 RPM drive dedicated exclusively to running Oracle	250+ GB Solid State Drive (SSD) dedicated exclusively to Oracle.
Network Card	Gigabit	Gigabit
HW RAID Controller	Highly recommended for Oracle database. Configure with RAID 0, 10, but avoid RAID5	Highly recommended for Oracle Database but not critical for SSD drives.
Drive Configuration	Drive Set 1: OS Drive Set 2: Oracle Database	Drive Set 1: OS (RAID 1) Drive Set 2: Oracle Database (SSD or HW RAID)
Operating Systems	MS Windows /Vista/2003/2008/Windows7 (64-bit)	MS Windows Vista/Windows7/2003/2008 Server (64-bit)

Distributed Processing Engine

If using a distributed processing engine, AccessData recommends the following hardware specifications.

	Recommended	Ideal
Processor	Intel® Core-2 Duo or AMD equivalent	Intel® Quad Core Xeon, i7 Nehalem or AMD equivalent
CD/DVD Drive	DVD	DVD
RAM	6 GB (DDR3) / 4-8 GB (DDR2)	12 GB (DDR3) / 8 GB (DDR2)
OS / Application drive	150 GB 7200 RPM	150 GB 10,000 – 15,000 RPM
Network Card	Gigabit	Gigabit
Operating Systems	MS Windows /Vista//2003/2008/Windows7 (64-bit)	MS Windows Vista/Windows7/Windows 2008 (64-bit)