SYSTEM SPECIFICATIONS GUIDE

FTK®

DIGITAL INVESTIGATIONS

v. 6.3

ACCESSDATA®

www.accessdata.com

Contents

AccessData® FTK Overview

When it comes to performing effective and timely investigations, we recommend examiners take into consideration the demands the software will make on their hardware resources. Depending on the size and scope of a given investigation, Forensic Toolkit® 5 (FTK®) will push hardware resources to their limits.

FTK is made up of four separate application components, each of which are installed separately and perform different functions. These components include a database, the FTK Client User Interface (UI), the Evidence Processing Engine (EP), and the optional Distributed Processing Engine (DPE). When configuring a system to run FTK, it is helpful to understand the hardware requirements of each of these components/applications and the impact each of them place on the hardware.

- **Database**—The database is a key component of the FTK application. It stores the processed metadata, performs all the queries, sorts, filters, file listings, and other functions requested by the FTK Client UI. PostgreSQL is included as the standard database. Oracle or MS SQL Server can be used as an alternative to PostgreSQL; however, AccessData only provides licensing for the included PostgreSQL database. For more information on using other database platforms, please see the FTK Install Guide on http://ftk.accessdata.com.
- **Evidence Processing Engine (EP) and Distributed Processing Engine (DPE)**—The processing engine and distributed processing engines, as their names suggest, perform the majority of the work when processing data.
- **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 the examiner with a view into the processed data.

General Considerations

AccessData strongly encourages the use of physical hardware platforms in any implementation of the AccessData Forensic Toolkit (FTK) solution. The support of any implementation which attempts to host one or more components on virtualized platforms is subject to the discretion of AccessData. AccessData reserves the right, during the troubleshooting of a support issue, to withdraw support on a specific issue if it is found to be induced by virtualization.

NOTE: VIRTUALIZATION USING MICROSOFT HYPER-V IS NOT SUPPORTED.

AccessData forbids the installation of any of the AccessData Forensic Toolkit solution's components on any system that hosts a Microsoft Domain Controller.

System Recommendations

It is strongly recommended that the Performance Guidelines KB article be followed closely when designing a system in preparation for installation of AccessData Forensic Toolkit. Disregarding these guidelines may result in poor performance, system hangs, and/or other issues that may render the product unusable.

The processing engine requires a temporary space with very fast I/O (read and write) and low fragmentation. This is referred to as "ADTemp" throughout this document. Among other things, the ADTemp is used by the engine to store data while it is being expanded, indexed, and prepared for insertion into the database (e.g., DtSearch indexes, thumbnails, compressed files, and metadata).

It is recommended that the database be on its own physical volume to minimize fragmentation and improve I/O. This volume should also be defragmented regularly to improve performance. However, defragmentation of this drive should not occur while processing or reviewing data.

When using distributed processing engines (DPE) there is absolutely no benefit to creating multiple virtual machines on the same system and putting distributed processing engines on those VM's.

It is important to note that when using DPE technology each DPE will be accessing the same evidence source which can quickly create an I/O bottleneck.

The PST export functionality requires Microsoft Outlook to be installed as it relies on libraries and program files contain therein.

For additional FTK resources and documentation, please visit http://ftk.accessdata.com.

Hardware / Software Requirements

AccessData FTK is based largely on Microsoft technologies and should, when possible, meet the following hardware specifications. Several additional software packages (e.g., .NET Framework 3.5.1, 4.0, Microsoft Visual C++, etc.) may be required during installation and will be installed as part of the component automatic pre-requisite check or manually from Microsoft's website. The performance of the system is directly related to the hardware used for each component and processing option selected.

(For a complete list of the operating systems (OS) supported, please see http://ftk.accessdata.com).

Single Server Install		
Component	**Basic**	**Recommended**
Processor	4 cores	48 cores
Memory	8GB RAM	96GB RAM (2GB/core min.)
Storage	• 7200 RPM / SSD - OS/Apps - ADTemp - Database - Evidence / Case Data)	• 7200 RPM disk (OS/Apps) • SSD – 256GB (ADTemp) • RAID 5 (Database) • RAID 5 (Evidence / Case Data)
	Windows 7 64-bit	Windows 7 x64 / Server 2008 R2
OS **Network**	1Gbit NIC minimum	10Gbit NIC
Other	USB interface for license dongle unless using soft dongle	

Laptop Install		
Component	**Basic**	**Recommended**
Processor	4 cores	8 cores
Memory	8GB RAM	16GB RAM (2GB/core)
Storage	7200 RPM	SSD
OS	Windows 7 64-bit	Windows 7 x64 / Server 2008 R2
Network	1Gbit NIC minimum	1Gbit NIC minimum
Other	USB interface for license dongle unless using soft dongle	

Distributed Install

Distributed Install— Evidence Processing Engine (EP) / FTK Client User Interface (UI)		
Component	**Basic**	**Recommended**
Processor	4 cores	8-32 cores
Memory	8GB RAM (2GB/core)	16-64GB RAM (2GB/core)
Storage	• Separate physical disks for OS and ADTemp files • 7200 RPM drives minimum	• Single Disk – OS/Apps • RAID 0 – ADTemp (SSD) • Hardware RAID controller
OS	Windows 7 64-bit	Windows 7 x64 / Server 2008 R2
Network	1Gbit NIC minimum	10Gbit NIC
Other	USB interface for license dongle unless using soft dongle	

Distributed Install— Database		
Component	**Basic**	**Recommended**
Processor	4 cores	8-16 cores
Memory	8GB RAM	16-64GB RAM
Storage	• Separate physical disks for OS and database files • 7200 RPM drives minimum	• RAID 1 – OS/Apps • RAID 10 – Database (10k or SSD) • Hardware RAID controller
OS	Windows 7 64-bit	Windows 7 x64 / Server 2008 R2
Network	1Gbit NIC minimum	10Gbit NIC

Distributed Install— Distributed Processing Engine (DPE)		
Component	**Basic**	**Recommended**
Processor	2 cores	4-16 cores
Memory	4GB RAM (2GB core)	8-32GB RAM (2GB/core)
OS	Windows 7 64-bit	Windows 7 x64 / Server 2008 R2
Network	1Gbit NIC minimum	10Gbit NIC

Considerations for Data Storage

Storage requirements for FTK are driven by case loads and retention policies. Here are a few considerations when determining the amount of storage needed:

- What is the typical number of evidence items processed for each case?
- What is the typical source image size?
- How long will processed case(s) be stored in the system?

ESI Storage Matrix				
Data Store	**Location**	**File Type**	**Size**	**Performance**
Evidence Files	Local, DAS device, or file server (SAN/NAS)	AD1, E01, Native	Driven by needs of organization	RAID 5 separate from case data
Case Data (Index of processed evidence)	Local, DAS device, or file server (SAN/NAS)	IDX, IX	Roughly 25-30% size of processed evidence image files	RAID 5 separate from evidence files
Metadata of Processed ESI	Local to database server	Various	Every 1 million items requires roughly 4-5GB of disk space in the database	RAID 5 or RAID 10 for redundancy and performance

Evidence files and case folders can be stored locally on the FTK system(s) or on a dedicated storage device, depending on the need. In larger environments with dozens of large cases, it is recommended that a dedicated storage device be used.

Whether it's for investigation, litigation or compliance, AccessData® offers industry-leading solutions that put the power of forensics in your hands. For 30 years, AccessData has worked with more than 130,000 clients in law enforcement, government agencies, corporations and law firms around the world to understand and focus on their unique collection-to-analysis needs. The result? Products that empower faster results, better insights, and more connectivity. For more information, visit www.accessdata.com

Visit us online:
www.accessdata.com

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com