



***FORENSIC TOOLKIT***<sup>®</sup>  
**PROCESSING PERFORMANCE TESTING  
AND SYSTEM CONFIGURATION**

**Table of Contents**

Performance Testing..... 1

FTK 2.2.1 Hardware Configuration Guide and Techniques for Achieving Better Processing Performance ..... 4

Hardware and Operating System Considerations .....4

How Much Does the Right System Cost? .....6

A great deal has been done to improve the performance of Forensic Toolkit (FTK®). A combination of factors affects the performance of this solution, but ultimately, hardware is the key. This next generation solution was engineered to take advantage of next generation hardware. In, the most recent round of testing — testing done both internally and with examiners in the field — has proven that FTK performs very well when recommended hardware specifications are met.

## Performance Testing:

Testing was conducted using a variety of hardware systems to clearly illustrate the dramatic difference in performance hardware can make on pre-processing times. Something as simple as putting the Operating System on a fast drive can save the investigator time with regard to processing a case.

Figure 1 below breaks up the carving, indexing and stream analysis (hashing, file signature analysis, drill down, Entropy) operations. You will notice that carving has the greatest impact on processing time. By performing the carving operation after the other processing or only when needed, you will save time and get to the analysis phase faster. This is of particular benefit to an investigator/analyst who is not able to upgrade his or her system or when time is of the essence.

The tests below all used the same 120GB image, containing 815,000 items...

FIGURE 1a

| Version - Computer - Database Location      | Product | CPU                    | # of Cores | RAM       | OS               | Oracle                            | Temp Space                    | Image                  | Case                        | Total Time Stream Analysis with Carving and Indexing | Total Time Stream Analysis with Indexing | Total Time Stream Analysis | Indexing | Carving | Total |
|---|---------|------------------------|------------|-----------|------------------|-----------------------------------|-------------------------------|------------------------|-----------------------------|--|--|----------------------------|----------|---------|-------|
| 1 i7 w/ 12 GB RAM - 5805 8 drive RAID10     | 1.18.3  | Intel i7               | 8          | 12 GB RAM | 10K Raptor       |                                   | Eight 15K SAS Drives RAID0    | Two - 10K Raptor       | Eight 15K SAS Drives RAID10 | 19.51  | 4.32                                     | 1.35                       | 2.97     | 15.19   | 19.51 |
| 3 Dual Quads 16GB RAM - Single Velociraptor | 1.18.3  | Dual Quad              | 8          | 16 GB RAM | 10K Velociraptor |                                   | 10K Velociraptor (Same as OS) | Two 7200 Dynamic Disks | Two 7200 Dynamic Disks      | 25.80  | 5.10                                     | 1.43                       | 3.67     | 20.70   | 25.80 |
| 5 Quad w/ 8GB RAM - 5405 4 drive RAID0      | 1.18.3  | Quad Q9450 2.66 Ghz    | 4          | 8 GB RAM  | 10K Raptor       |                                   | Four 7200 Drives RAID0        | Two - 10K Raptor       | Four 7200 Drives RAID0      | 28.70  | 5.45                                     | 1.50                       | 3.95     | 23.25   | 28.70 |
| 7 Quad 4GB RAM - Single 7200                | 1.18.3  | Quad Q9450 2.66 Ghz    | 4          | 4 GB RAM  | 10K Velociraptor |                                   | 10K Velociraptor (Same as OS) | NAS                    | Single 7200                 | 32.50  | 6.30                                     | 1.90                       | 4.40     | 26.20   | 32.50 |
| 9 Core2Duo 3GB RAM - USB 7200               | 1.18.3  | Core2Duo 2.5 Ghz       | 2          | 3 GB RAM  | Internal 7200    |                                   | Internal 7200 (Same as OS)    | USB 7200               | USB 7200                    | 38.25  | 8.45                                     | 2.10                       | 6.35     | 29.80   | 38.25 |
| 2 i7 w/ 12 GB RAM - 5805 8 drive RAID10     | 2.2.1   | Intel i7               | 8          | 12 GB RAM | 10K Raptor       | 5805 - Four 15K SAS Drives RAID10 | Four 15K SAS Drives RAID0     | Two - 10K Raptor       | Four 15K SAS Drives RAID10  | 5.32   | 3.01                                     | 1.35                       | 1.66     | 2.31    | 5.32  |
| 4 Dual Quads 16GB RAM - Single Velociraptor | 2.2.1   | Dual Quad E5405 2.0Ghz | 8          | 16 GB RAM | 10K Velociraptor | Intel x25-E SSD Drive             | 10K Velociraptor (Same as OS) | Two 7200 Dynamic Disks | Two 7200 Dynamic Disks      | 6.72   | 3.72                                     | 1.50                       | 2.22     | 3.00    | 6.72  |
| 6 Quad w/ 8GB RAM - 5405 4 drive RAID0      | 2.2.1   | Quad Q9450 2.66Ghz     | 4          | 8 GB RAM  | 10K Raptor       | 5405 -4 7200 Drives RAID0         | Four 7200 Drives RAID0        | Two - 10K Raptor       | Four 7200 Drives RAID0      | 11.29  | 4.27                                     | 1.55                       | 2.72     | 7.02    | 11.29 |
| 8 Quad 4GB RAM - Single 7200                | 2.2.1   | Quad Q9450 2.66Ghz     | 4          | 4 GB RAM  | 10K Velociraptor | Single 7200                       | 10K Velociraptor (Same as OS) | NAS                    | Single 7200                 | 14.01  | 5.40                                     | 2.60                       | 2.80     | 8.61    | 14.01 |
| 10 Core2Duo 3GB RAM - Internal 7200         | 2.2.1   | Core2Duo 2.5 Ghz       | 2          | 3 GB RAM  | Internal 7200    | Internal 7200                     | Internal 7200 (Same as OS)    | USB 7200               | USB 7200                    | 18.75  | 7.80                                     | 3.60                       | 4.20     | 10.95   | 18.75 |

FIGURE 1b

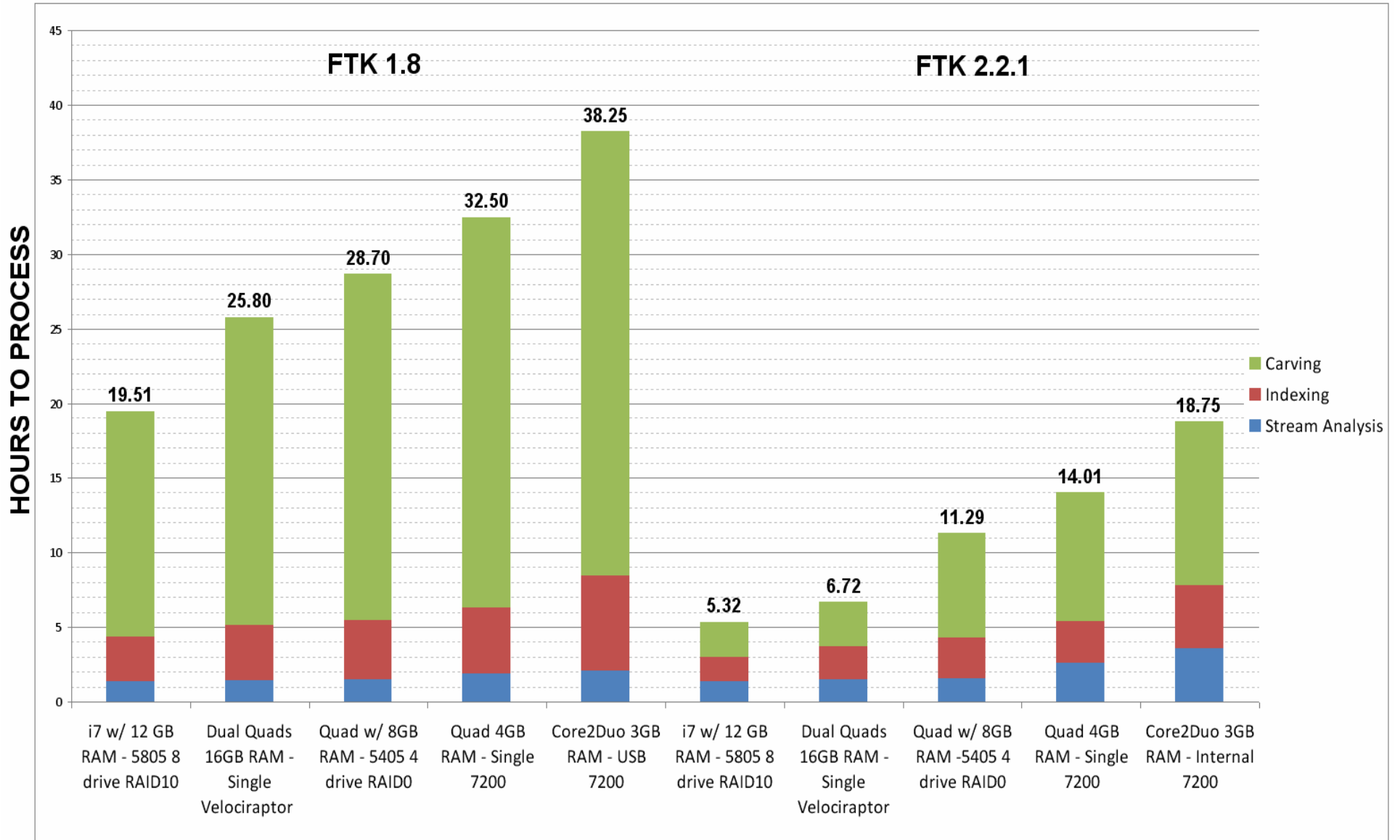
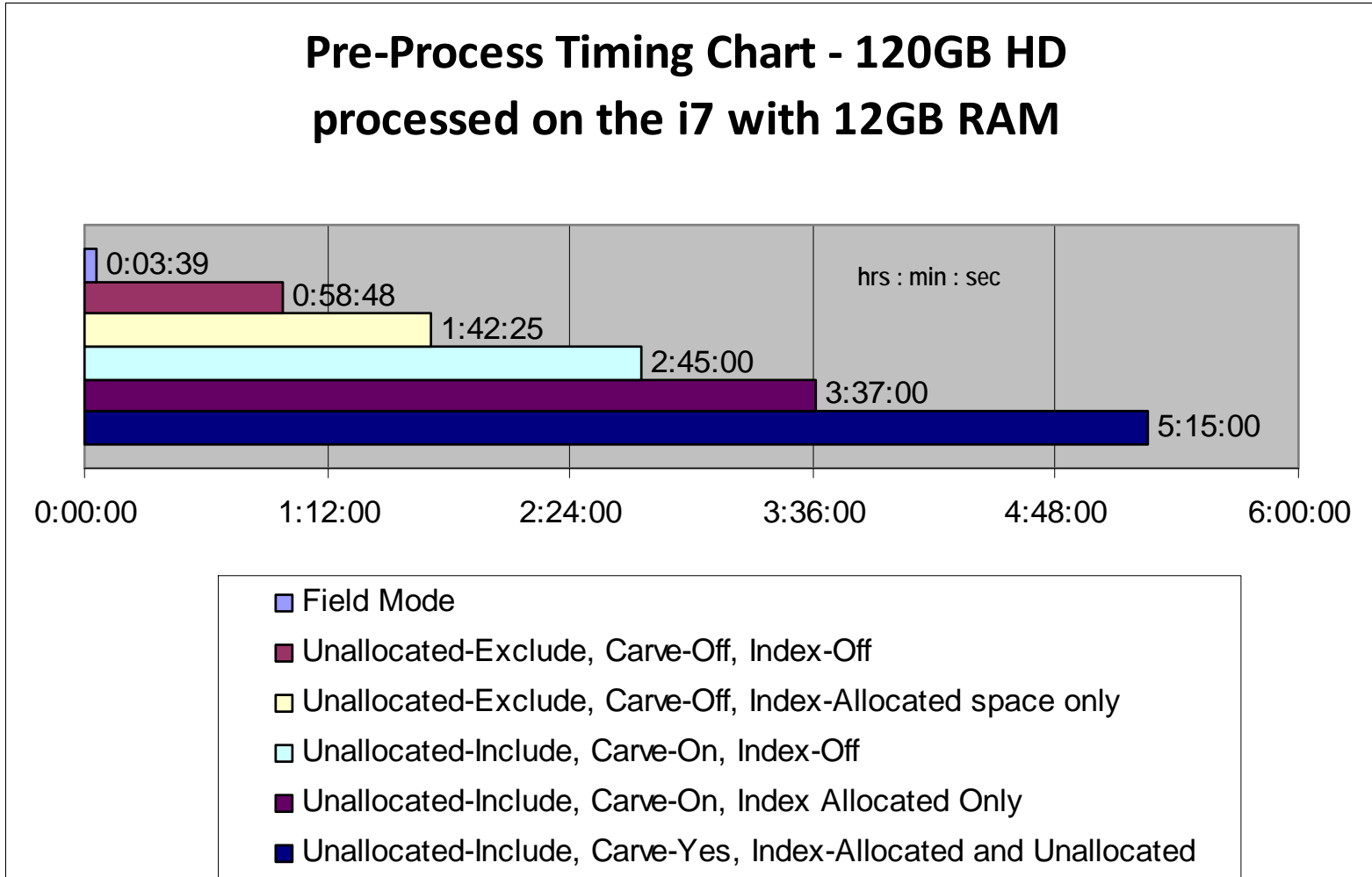


FIGURE 2



*Figure 2 metrics illustrate the impact various processing options have when using ideal system specifications (Intel i7 processor with 12 GB of RAM).*

## FTK 2.2.1 Hardware Configuration Guide and Techniques for Achieving Better Processing Performance

**Field Mode Images That Need to Be Quickly Reviewed** – Field Mode can usually fully enumerate a drive in 5-15 minutes. This is the single best way to quickly triage/examine the contents of a hard drive. Note that Field Mode allows you to access the data very quickly without the deeper processing operations. After reviewing the data in Field Mode, you can identify relevant data sets, on which to perform more advanced processing operations, using the “Additional Analysis” option. If you are using hardware with limited processing capabilities, Field Mode is an option that will save you a great deal of time, depending on the nature of your investigation.

**Full Text Index of Drive Free Space Usually Takes More than 50% of the Pre-Processing Time** – When processing a hard drive, in 95% of the cases, the key pieces of evidence are located in allocated space. Indexing drive free space and file slack is an important part of any forensics exam. However, if you need to reduce processing time, consider processing the hard drive WITHOUT indexing drive free space first. Drive free space can be indexed as a follow-up step by using the “Additional Analysis” feature.

**Oracle SGA Memory Settings** – Run AccessData’s “Oradjuster.exe” utility (available for download at [www.accessdata.com](http://www.accessdata.com) under “Support”) after installing FTK. It will adjust Oracles memory to more optimal values. The default setting for SGA RAM when FTK is first installed is very small. Increasing SGA RAM is the most effective way to increase UI performance.

**Backing Up Oracle** – Backing up Oracle can be problematic at times, because Oracle locks access to the database files. The two options are to either use the archive feature in the CasePortability.exe utility (available for download at [www.accessdata.com](http://www.accessdata.com) under “Support”) or stopping the Oracle service before running any backup utility.

**Regularly Archive Cases** – Use the utility “CasePortability.exe” (available for download at [www.accessdata.com](http://www.accessdata.com) under “Support”) to regularly archive the individual case database files. Try to keep only active cases in the Oracle database. Note: The “archive” function places a copy of the case DBF file in the case folder. Archiving a case is different from the “backup” function in that the backup function places a copy of the entire case folder, including the dtSearch index information and DBF file, into a zip container. Keeping the number of cases in the database to a minimum helps improve hard drive efficiency.

**Free Up Memory When Not Running FTK** – If Oracle is taking up memory that is needed for other applications and FTK is not in use, running the utility “Oradjuster.exe” and setting the SGA memory to 5–10% of the system RAM is the safest way to free up some RAM. Another option is to stop the Oracle service. However, stopping the service while the FTK Worker is processing a hard drive image can potentially corrupt any open/active cases.

## Hardware and Operating System Considerations

**64-bit Operating System** – FTK runs best in a 64-bit Windows operating system. Of the various operating systems, Windows Vista x64 has superior memory management and disk cache algorithms. FTK also runs well on Server 2003 x64 and Server 2008 x64. If possible try to avoid running FTK or Oracle on a 32-bit operating system.

**RAM** – The more RAM FTK/Oracle has to work with the better the performance during pre-processing and review. On 64-bit operating systems, 8 gigabytes of RAM is a recommended minimum and 12–16 gigs of RAM is preferable, especially when dealing with multi-million record item cases. Use quality gaming RAM when possible. Strongly avoid general purpose RAM.

**CPU Type, Speed and Number of Cores** – FTK is a multi-threaded application and as such will take advantage of the several cores available on many of the modern chips. Since FTK performance is usually bound by disk I/O, it is not necessary to spend top dollar to get the fastest, most expensive chips. Most of the Intel or AMD Quad core chips are good choices. Try to stay away from the dual core chip sets. The Intel i7 hyper threads up to 8 cores and is a very good choice for running FTK. The difference in performance between 4 cores and 8 cores is significant, especially when it comes to pre-processing speed. An 8-core system will outperform a 4-core system almost 3 to 1.

**Install Oracle on Its Own Hard Drive(s)** – Oracle runs best when it is on its own physical media. In a workstation environment, UI performance is greatly improved when Oracle is not sharing disk I/O resources with the OS or other applications. For backup consistency, consider assigning the drive to which Oracle is installed the letter “O:” In some situations,

such as running FTK on a laptop, there is not the option of installing Oracle on a separate drive. In those situations in which space for internal hard drives is limited, where possible, consider storing the image and the case folder on an external drive connected via eSATA.

**Installing Oracle on Faster Drives Will Improve UI Performance** – Oracle does not require a lot of space (a single case with one or two hard drives will usually only need 10–20GB of storage space). The speed of the UI is directly correlated to how fast Oracle can perform the various SQL queries. Try to avoid using Oracle on 7200 RPM drives, as the read seek latency makes Oracle run particularly slowly. Western Digital Velociraptor drives and the Intel x25-M are both particularly good choices when selecting hard drive(s) on which to run Oracle. One of the fastest and more reasonably priced options for achieving very fast drive performance for the Oracle database is to combine (span) an Intel x25-M 80Gig SSD drive with a 150GB WD VelociRaptor drive. Use the Windows disk manager to set the drives up as dynamic disks, span the drives (do not stripe) with the Intel x25-M SSD as the first drive and the WD VelociRaptor as the second/overflow drive. If budget is such that purchasing two or more of the Corsair P128 CMFSSD - 128GB SSDs is an option, consider striping the SSD drives and/or putting them behind a hardware RAID card.

**Using a Hardware RAID Card Can Significantly Improve UI Performance** – Hardware RAID cards can significantly improve the database performance. Try to stick with good quality cards that have a read/write cache, such as the Adaptec 5405 or 5805. It is strongly recommended to get a battery for the card to activate write-through cache. Set the stripe size to 1 MB or as large as the card will allow. When possible do NOT use RAID5 for the Oracle database. RAID5 will greatly impact Oracle's performance by more than 25%. RAID10 is best as it combines both performance and redundancy. RAID0 will provide very good performance, but since there is no redundancy, in case of drive failure, make sure to backup the cases regularly. The best possible performance is achieved by combining two or more x25-M or x25-E SSD drives with a hardware RAID card and activating the write-through cache. RAID5 works well as an option only for the drives holding the case folder, the HD images, and/or the OS.

**Turn Off Indexing, Compression, and EFS Encryption** – There is no reason to have either Microsoft indexing, or compression or EFS encryption running on the drive that hosts Oracle. Also make sure that Microsoft indexing and compression are turned off on the drive that hosts the case folder and images.

**Antivirus** – Make sure to exclude evidence, case folder and database from being scanned by antivirus. It can cause 25–50% performance degradation, depending on settings and antivirus client.

**OS Hard Drive and Page File** – The speed of the OS drive's most significant impact on the performance of an application deals with the speed of the page file. Fortunately, most of the time the OS drives can be small; 50–60 gigs for the OS is usually more than enough. For this reason the smaller, faster drives are great options for the OS drive. The x25-M drives are not usually the best option for an OS drive because of the slow write time. The x25-E SSD drive works spectacularly for the OS drive. However, if a system has only one x25-E SSD drive, it is best used for the Oracle database. The 10,000 RPM Raptor or VelociRaptor drives in the small form factor (74 gig or 150 gig) are a great choice for OS drives. For maximum OS performance, depending on the motherboard, try setting up two drives striped RAID0.

Incorrect settings for the Page File can also impact performance, but more importantly, page file problems can cause an application and even the OS to crash. Windows does not always do a great job at managing the page file. Because FTK pages a lot during image processing, it is usually a good idea to use the "Virtual Memory - Custom Size" option to manually increase the size of the main page file. The smallest the page file should be is 1x to 1.5x the amount of RAM on the computer. The maximum size should usually be around 2x or 3x the amount of RAM. Systems with smaller amounts of RAM require larger page files and systems with large quantities of RAM require relatively smaller page files.

**During Image Processing, the HD Image and the Case Folder Should be on a Different Drive than Oracle** – If the HD image or the case folder are on the same drive as Oracle, the image processing time can be as much as 75–100% longer than when Oracle has its own drive. Even having the image on a removable eSATA/USB drive is better than storing the HD image on the same drive(s) as Oracle.

## How Much Does the Right System Cost?

The following system pricing is estimated, based on our internal experience. Each system example below is designed to be a single-box solution, on which you can run both FTK and Oracle. This pricing is based on building the machines on your own, but it provides a good frame of reference, if you're looking at upgrade options.

However, for organizations in the US looking to purchase new hardware, companies such as Forensic Computers ([www.forensic-computers.com](http://www.forensic-computers.com)) and Digital Intelligence ([www.digitalintelligence.com](http://www.digitalintelligence.com)), provide state-of-the-art builds that are extensively tested and come pre-installed and configured with Forensic Toolkit®. They typically back their hardware with a 1 or 2 year guarantee and have great support if anything ever goes wrong. Going this route may well be worth the additional cost over trying to build a system from scratch.

*NOTE: In each example below the Case Folder and Image should be stored on a NAS or Removable 7200 Drives*

### Entry-Level FTK 2.x Forensics System

|   |                |
|---|----------------|
| CPU – i7 920 Nehalem 2.66 GHz LGA 1366                          | \$279          |
| RAM – 12 Gig 6 x 2GB OCZ Reaper DDR3 2000 (PC3 1600)            | \$290          |
| Motherboard – ASUS P6T Intel iX58 LGA 1366                      | \$249          |
| Case  | \$75           |
| Power Supply  | \$125          |
| Hard Drive for OS & Oracle – Western Digital Velociraptor 150GB | \$159          |
| Vista x64 Business  | \$125          |
| <b>Total</b>  | <b>\$1,302</b> |

---

### Mid-Level FTK 2.x Forensics System

|  |                |
|--|----------------|
| CPU – i7 920 Nehalem 2.66 GHz LGA 1366                 | \$279          |
| RAM – 12 Gig 6 x 2GB OCZ Reaper DDR3 2000 (PC3 1600)   | \$290          |
| Motherboard – ASUS P6T WS PRO LGA 1366                 | \$299          |
| Case   | \$125          |
| Removable Drive Tray                                   | \$100          |
| Power Supply   | \$125          |
| Hard Drive for Oracle - Corsair P128 CMFSSD-128GB SSD  | \$345          |
| Hard Drive for OS – Western Digital Velociraptor 150GB | \$159          |
| Vista x64 Business                                     | \$125          |
| <b>Total</b>   | <b>\$1,847</b> |

---

### Mid-High Level System

|  |                |
|--|----------------|
| CPU – i7 920 Nehalem 2.93 GHz LGA 1366   | \$550          |
| RAM – 12 Gig 6 x 2GB OCZ Reaper DDR3 2000 (PC3 1600)   | \$290          |
| Motherboard – ASUS P6T WS PRO LGA 1366   | \$299          |
| Case   | \$150          |
| Removable Drive Tray(s)  | \$200          |
| Power Supply   | \$125          |
| Adaptec 5405 RAID card   | \$379          |
| Battery for RAID card  | \$100          |
| (2) Hard Drive for Oracle - Corsair P128 CMFSSD - 128GB SSD<br>(connected to Adaptec Card either RAID0 or RAID1) | \$690          |
| (2) Hard Drive for OS – Western Digital Velociraptor 150GB   | \$320          |
| Vista x64 Business   | \$125          |
| <b>Total</b>   | <b>\$3,228</b> |

---

**Higher End System**

|  |                |
|--|----------------|
| CPU – Two Intel Xeon Quad E5520 2.26Ghz LGA 1366   | \$620          |
| RAM – 16 GB DDR3 1333  | \$290          |
| Motherboard – ASUS Z8PE-D12 Dual LGA 1366  | \$449          |
| Case   | \$175          |
| Removable Drive Tray(s)  | \$200          |
| Power Supply   | \$175          |
| Adaptec 5405 RAID card   | \$379          |
| Battery for RAID card  | \$100          |
| (2) Hard Drive for Oracle - Corsair P128 CMFSSD - 128GB SSD<br>(connected to Adaptec Card either RAID0 or RAID1) | \$690          |
| (2) Hard Drive for OS – Western Digital Velociraptor 150GB   | \$320          |
| Vista x64 Business   | \$125          |
| <b>Total</b>   | <b>\$3,868</b> |

---

**Top End System**

|  |                |
|--|----------------|
| CPU – Two Intel Xeon Quad E5540 2.4Ghz LGA 1366  | \$620          |
| RAM – 32GB DDR3 1333   | \$580          |
| Motherboard – ASUS Z8PE-D12 Dual LGA 1366  | \$449          |
| Case   | \$175          |
| Removable Drive Tray(s)  | \$200          |
| Power Supply   | \$175          |
| Adaptec 5805 RAID card   | \$525          |
| Battery for RAID card  | \$100          |
| (4) Hard Drive for Oracle - Corsair P128 CMFSSD - 128GB SSD<br>(connected to Adaptec Card either RAID10) | \$1,380        |
| (2) Hard Drive for OS – Western Digital Velociraptor 150GB   | \$320          |
| (1) Hard Drive for Page File – Corsair 128 SSD   | \$345          |
| Vista x64 Business<br>(for page file connect directly to motherboard)                                    | \$125          |
| <b>Total</b>   | <b>\$4,994</b> |

---