

## **Quantifying FTK 3.0 Performance with Respect to Hardware Selection**

### **Background**

A wide variety of hardware platforms and associated individual component choices exist that can be utilized by the Forensic Examiner to process computer based evidence. As the feature sets of current software tools expand, so do the hardware requirements of the forensic analysis systems. In order to maintain an acceptable level of performance, choosing the appropriate hardware is more important than ever. As the leading provider of Computer Forensic solutions, Digital Intelligence believes in the importance of helping the customer understand their hardware needs and provide the best choices available to meet those needs. In an effort to better quantify how hardware choices effect performance, a series of tests were developed using Digital Intelligence Intel i7 and Dual Xeon systems. These tests were used to quantify the performance of various CPU, Memory, and Storage configurations. It is anticipated that this information can be of significant value to the individual consumer when making hardware configuration decisions in the FTK 3.0 environment.

### **Approach**

A feature rich test case (hard drive) was developed that contained a variety of data of sufficient quantity to perform a meaningful examination. A representative set of operations to be performed by the examiner was identified and automated. The automation of these representative operations allowed detailed and reliable logging of the exact time required to perform each individual task. Simple hardware modifications were performed on the test platforms in order to quantify the changes in performance corresponding to individual hardware changes.

### **The Hardware**

Two test platforms were established. The platforms were set up using the base shipping configurations of DI equipment as follows.

Platform 1: An Intel i7 motherboard with an X58 chipset. The baseline platform was equipped with an Intel i7-965 CPU clocked at the factory speed of 3.2 GHZ. The board was outfitted with 6 GB of DDR3-1333 RAM. Three hard disk drives (HDD) were configured, one for the operating system (OS), one for the Oracle database and one for the evidence image and the case materials. The drives were stock 7200 RPM Seagate model ST3100340NS 1.0 TB capacity drives.

Platform 2: A dual Intel Xeon motherboard with a 5400 chipset. The baseline platform was equipped with dual Intel Xeon 5420 CPUs running at 2.5 GHZ. 8 GB of DDR2-667 Fully Buffered ECC RAM and three HDD completed the setup. The HDD were 7200 RPM Seagate ST31500341AS 1.5 TB drives configured as in Platform 1, one each for the OS, Oracle, and case.

## **The Software**

Microsoft Vista Ultimate (64 bit) was installed as the OS. Microsoft indexing and compression were turned off for all hard disk drives used for testing. In addition, there was no EFS encryption enabled on any drive. Page file size was manually adjusted on the OS drive to 2x the amount of RAM for the smallest size and 3x the amount of RAM as the largest. These adjustments to the OS are in line with recommendations made by AccessData in earlier performance testing. All manufacturer patches and updates were applied to the operating system. All hardware drivers (i.e. video, audio, etc) were also confirmed to be of the latest shipping version.

All software that is installed by Digital Intelligence by default on its shipping systems was included on the test platforms. AccessData Forensic Tool Kit, version 3.0 was installed on both platforms with the Oracle database on its own HDD. Using the included Oradjuster tool, Oracle was configured to use 32% of the RAM, the maximum setting allowed. FTK Imager was also installed. No other AccessData software was installed.

Using a free utility called AutoIT ([www.autoitscript.com/autoit3](http://www.autoitscript.com/autoit3)), a script was created to automate the benchmarking process. The script ran FTK and then ran the various benchmarking operations agreed upon (see Methodology). Additionally, the script created logs to time-stamp the various operations so comparisons between hardware configurations could be made.

## **The Test Data**

A test dataset was created on a 80GB hard drive consisting of one partition containing a Microsoft Windows OS and files on an NTFS file system, a second partition of files on a FAT32 file system and a third partition that was deleted after creation. The dataset contained approximately 815,000 items and the drive was physically imaged using FTK Imager version 2.2.5. The resulting image was called FTK3Bench; a raw (dd) image type was utilized.

## **Methodology**

Prior to beginning benchmarking, a case was created using the FTK3Bench image to determine what operations could be utilized in testing. The following procedures were accomplished:

- Opening the case
- Selecting Quick Pick at the top of the evidence on the Explore tab
- Re-sorting all items on the Explore tab from A-Z to Z-A, sort by MD5 hash value, sorting by SHA256 hash value, sorting by creation date
- Rendering all graphics in thumbnails on the Graphics tab

- Re-sorting all graphics on Graphics tab from A-Z to Z-A
- From the Overview tab, selecting File Types and then applying a global filter to hide KFF Ignorable, applying a tab filter for graphics greater than 1 MB in size
- Listing all Raster graphics from the Overview tab
- Closing the case

Routine functions of the User Interface (UI) such as the above had presented time challenges for versions of FTK from 2.0 through 2.2. However, with the release of version 3.0, the speed of the UI response was significantly improved to the point that there were negligible amounts of time from request to response. For example, the dataset contained almost 400,000 image files. They were rendered in the thumbnail view on the Graphics Tab in less than 3 seconds on initial display and then almost instantaneously thereafter. The same result was noted on display of all 815,000 items on the overview tab and then sorting all items.

Since the above operations did not seem provide meaningful data for hardware comparisons, our focus shifted to performing more intensive operations of initial case creation and performing additional analysis tasks.

The AutoIT script was modified to perform and log the times required to perform the following four benchmark tests. (The associated benchmark times for each of the tests associated with a given hardware configuration are listed in the tables which follow):

1. **“Pre-Processing”** benchmark: Create a case using the FTK3Bench.001 image. The case was created on the Case drive and used the MST (UTC-7) time zone. The initial case Detailed Options were set as follows:
  - a. Hashing (MD5, SHA1, SHA256)
  - b. Expand compound files
  - c. File signature analysis
  - d. Create thumbnails for graphics

Evidence Discovery Options, Evidence Refinement (Advanced), and Index Refinement (Advanced) choices were all left to their manufacturer default selections throughout the testing. The above configuration and options were used to perform the testing as documented in the “Pre-Processing” column of the spreadsheet.

After FTK created and processed the case to this point, a selection was made from the Evidence menu item to perform Additional Analysis. Three separate steps were performed with each step initiated only after the previous step had completed. In each step Target Items was set to All Items. The steps were:

2. **“dtSearch/Entropy”** benchmark: Index the case and perform the entropy test

3. "**Data/Meta Carving**" benchmark: Perform data and meta carving operations. All types of data were carved.
4. "**Known File Filter**" benchmark: All resulting files in the case were compared to the default Known File Filter (KFF) groups (AD\_Alert and AD\_Ignore)

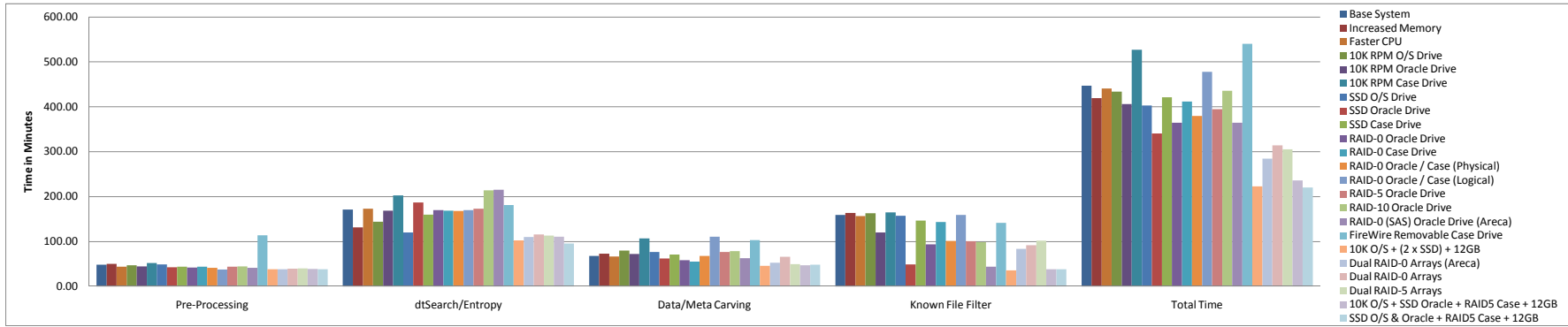
A baseline test was then conducted and the results were noted. After that, a single hardware variable was changed in each system and the test run again. For example, in the first test following the benchmark, memory was increased. In the next test, memory was restored to the baseline and the CPUs were altered. Next, the CPUs were returned to baseline and a faster OS drive was placed in each platform, and so on.

Prior to each run of the test, all created cases were removed from the FTK database. If the OS or Oracle drives were to be replaced, the replacement drive was provided with a standard GHOST disk image of the baseline drive in question that had been created by Norton Ghost version 11.5 (Ghost Solutions Suite 2.5).

The total time (in minutes) for each of the 4 tests, performed in each of the hardware configurations, can be seen in the benchmark tables. The hardware configuration for each set of tests is identified in the tables which follow.

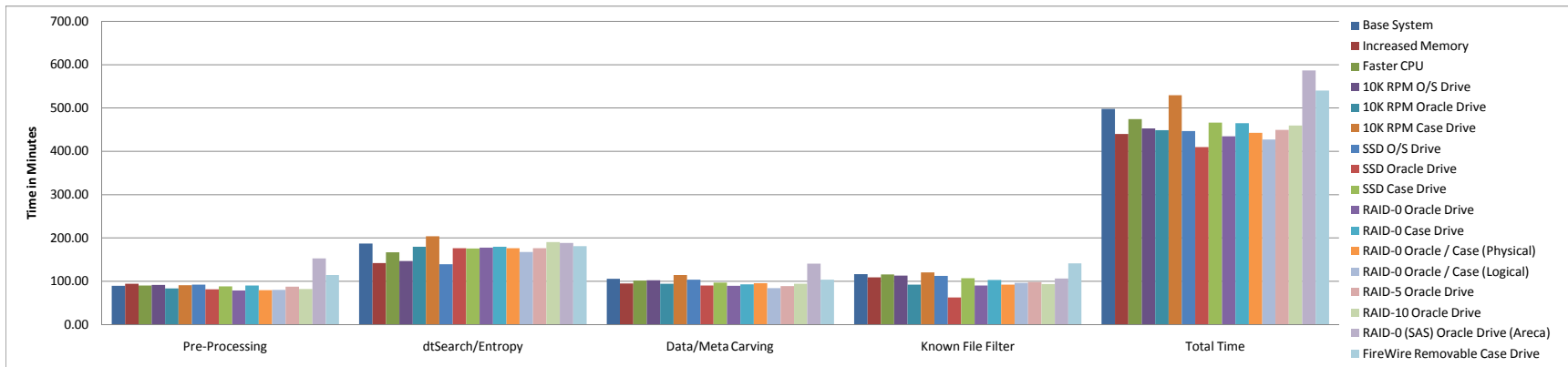
**i7 Benchmarks**

Benchmark Times	CPU	Memory	O/S Drive	Oracle Drive	Case Drive	Pre-Processing	dtSearch/Entropy	Data/Meta Carving	Known File Filter	Total Time
Base System	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	7200 RPM SATA	7200 RPM SATA	48.58	171.30	68.02	159.35	447.25
Increased Memory	i7 965 @ 3.2 GHZ	<b>12GB</b>	7200 RPM SATA	7200 RPM SATA	7200 RPM SATA	50.58	131.73	73.14	163.86	419.31
Faster CPU	<b>i975 Extreme @ 3.33 Ghz</b>	7200 RPM SATA	7200 RPM SATA	7200 RPM SATA	7200 RPM SATA	44.08	172.98	67.02	156.68	440.76
10K RPM O/S Drive	i7 965 @ 3.2 GHZ	6GB	<b>10K Raptor</b>	7200 RPM SATA	7200 RPM SATA	47.26	144.14	79.72	162.95	434.07
10K RPM Oracle Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>10K Raptor</b>	7200 RPM SATA	44.84	168.59	72.52	120.06	406.01
10K RPM Case Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	7200 RPM SATA	<b>10K Raptor</b>	52.26	202.78	107.09	164.79	526.92
SSD O/S Drive	i7 965 @ 3.2 GHZ	6GB	<b>X.25 SSD</b>	7200 RPM SATA	7200 RPM SATA	48.93	120.21	76.55	157.27	402.96
SSD Oracle Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>X.25 SSD</b>	7200 RPM SATA	42.57	186.79	62.61	48.93	340.90
SSD Case Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	7200 RPM SATA	<b>X.25 SSD</b>	43.84	159.78	70.85	146.83	421.30
RAID-0 Oracle Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>RAID-0 (5x1TB@7200)</b>	7200 RPM SATA	42.17	170.17	58.49	93.51	364.34
RAID-0 Case Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	7200 RPM SATA	<b>RAID-0 (5x1TB@7200)</b>	43.74	168.77	55.52	143.67	411.70
RAID-0 Oracle / Case (Physical)	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>RAID-0 (3x1TB@7200)</b>	<b>RAID-0 (2x1TB@7200)</b>	41.67	168.34	68.24	101.26	379.51
RAID-0 Oracle / Case (Logical)	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>RAID-0 (5x1TB@7200) w/Two Partitions</b>		37.90	169.86	111.04	159.35	478.15
RAID-5 Oracle Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>RAID-5 (5x1TB@7200)</b>	7200 RPM SATA	43.92	173.10	77.06	100.93	395.01
RAID-10 Oracle Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>RAID-10 (4x1TB@7200)</b>	7200 RPM SATA	44.51	213.95	78.85	98.61	435.92
RAID-0 (SAS) Oracle Drive (Areca)	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	<b>RAID-0 (5x1TB@15K SAS)</b>	7200 RPM SATA	41.58	215.49	63.08	44.18	364.33
FireWire Removable Case Drive	i7 965 @ 3.2 GHZ	6GB	7200 RPM SATA	7200 RPM SATA	<b>7200 RPM SATA (1394b)</b>	114.19	181.08	103.45	141.49	540.21
10K O/S + (2 x SSD) + 12GB	i7 965 @ 3.2 GHZ	<b>12GB</b>	<b>10K Raptor</b>	<b>X.25 SSD</b>	<b>X.25 SSD</b>	38.65	102.69	45.66	35.83	222.83
Dual RAID-0 Arrays (Areca)	i7 965 @ 3.2 GHZ	<b>12GB</b>	<b>10K Raptor</b>	<b>RAID-0 (5x1TB@7200)</b>	<b>RAID-0 (5x1TB@7200)</b>	38.15	109.94	52.85	83.49	284.43
Dual RAID-0 Arrays	i7 965 @ 3.2 GHZ	<b>12GB</b>	<b>10K Raptor</b>	<b>RAID-0 (5x1TB@7200)</b>	<b>RAID-0 (5x1TB@7200)</b>	39.73	115.95	66.38	91.91	313.97
Dual RAID-5 Arrays	i7 965 @ 3.2 GHZ	<b>12GB</b>	<b>10K Raptor</b>	<b>RAID-5 (5x1TB@7200)</b>	<b>RAID-5 (5x1TB@7200)</b>	40.00	113.61	49.67	102.10	305.38
10K O/S + SSD Oracle + RAID5 Case + 12GB	i7 965 @ 3.2 GHZ	<b>12GB</b>	<b>10K Raptor</b>	<b>X.25 SSD</b>	<b>RAID-5 (5x1TB@7200)</b>	39.00	111.01	47.44	38.50	235.95
SSD O/S & Oracle + RAID5 Case + 12GB	i7 965 @ 3.2 GHZ	<b>12GB</b>	<b>X.25 SSD</b>	<b>X.25 SSD</b>	<b>RAID-5 (5x1TB@7200)</b>	38.15	95.84	48.26	38.26	220.51



**Dual Xeon Benchmarks**

Benchmark Times	CPU	Memory	O/S Drive	Oracle Drive	Case Drive	Pre-Processing	dtSearch/Entropy	Data/Meta Carving	Known File Filter	Total Time
Base System	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	7200 RPM SATA	7200 RPM SATA	89.15	187.14	105.21	116.54	498.04
Increased Memory	Xeon E5420 @ 2.50 Ghz (x2)	<b>16 GB</b>	7200 RPM SATA	7200 RPM SATA	7200 RPM SATA	94.25	142.08	94.76	108.94	440.03
Faster CPU	<b>Xeon E5450 @ 3.00 Ghz (x2)</b>	8GB	7200 RPM SATA	7200 RPM SATA	7200 RPM SATA	89.73	166.83	101.77	115.78	474.11
10K RPM O/S Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	<b>10K Raptor</b>	7200 RPM SATA	7200 RPM SATA	91.24	146.34	102.33	112.79	452.70
10K RPM Oracle Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>10K Raptor</b>	7200 RPM SATA	83.40	179.30	94.16	91.84	448.70
10K RPM Case Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	7200 RPM SATA	<b>10K Raptor</b>	90.91	203.91	114.18	120.22	529.22
SSD O/S Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	<b>X.25 SSD</b>	7200 RPM SATA	7200 RPM SATA	92.07	138.90	103.52	112.46	446.95
SSD Oracle Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>X.25 SSD</b>	7200 RPM SATA	81.31	175.90	90.18	62.54	409.93
SSD Case Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	7200 RPM SATA	<b>X.25 SSD</b>	87.66	175.20	96.51	106.85	466.22
RAID-0 Oracle Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>RAID-0 (5x1TB@7200)</b>	7200 RPM SATA	78.47	177.71	89.03	89.75	434.96
RAID-0 Case Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	7200 RPM SATA	<b>RAID-0 (5x1TB@7200)</b>	89.81	179.65	92.51	102.77	464.74
RAID-0 Oracle / Case (Physical)	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>RAID-0 (3x1TB@7200)</b>	<b>RAID-0 (2x1TB@7200)</b>	79.14	175.92	95.32	92.08	442.46
RAID-0 Oracle / Case (Logical)	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>RAID-0 (5x1TB@7200) w/Two Partitions</b>		79.81	167.29	84.12	95.83	427.05
RAID-5 Oracle Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>RAID-5 (5x1TB@7200)</b>	7200 RPM SATA	86.98	176.08	88.84	97.75	449.65
RAID-10 Oracle Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>RAID-10 (4x1TB@7200)</b>	7200 RPM SATA	82.23	190.15	93.81	93.08	459.27
RAID-0 (SAS) Oracle Drive (Areca)	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	<b>RAID-0 (5x1TB@15K SAS)</b>	7200 RPM SATA	152.34	188.07	140.31	106.03	586.75
FireWire Removable Case Drive	Xeon E5420 @ 2.50 Ghz (x2)	8GB	7200 RPM SATA	7200 RPM SATA	<b>7200 RPM SATA (1394b)</b>	114.19	181.08	103.45	141.49	540.21



### **Benchmark Configuration Notes:**

The following are the details which corresponding to the hardware components identified in the benchmark tables:

#### Memory:

6GB / 12GB i7 Memory: DDR3-1333 RAM

8GB / 16 GB Xeon Memory: DDR2-667 Fully Buffered ECC RAM

#### Drives:

7200 RPM SATA Drive: Seagate ST3100340NS 1.0 TB 7200 RPM (i7&RAIDs)

7200 RPM SATA Drive: Seagate ST31500341AS 1.5 TB 7200 RPM (Xeon)

10K Raptor Drive: Western Digital WD300GLFS 300 GB 10,000 RPM

X25 SSD Drive: Intel X25 160 GB Solid State Disk

15K SAS Drive: Hitachi UltraStar HUS153030VLS300 15,000 RPM SAS

#### RAID Controllers:

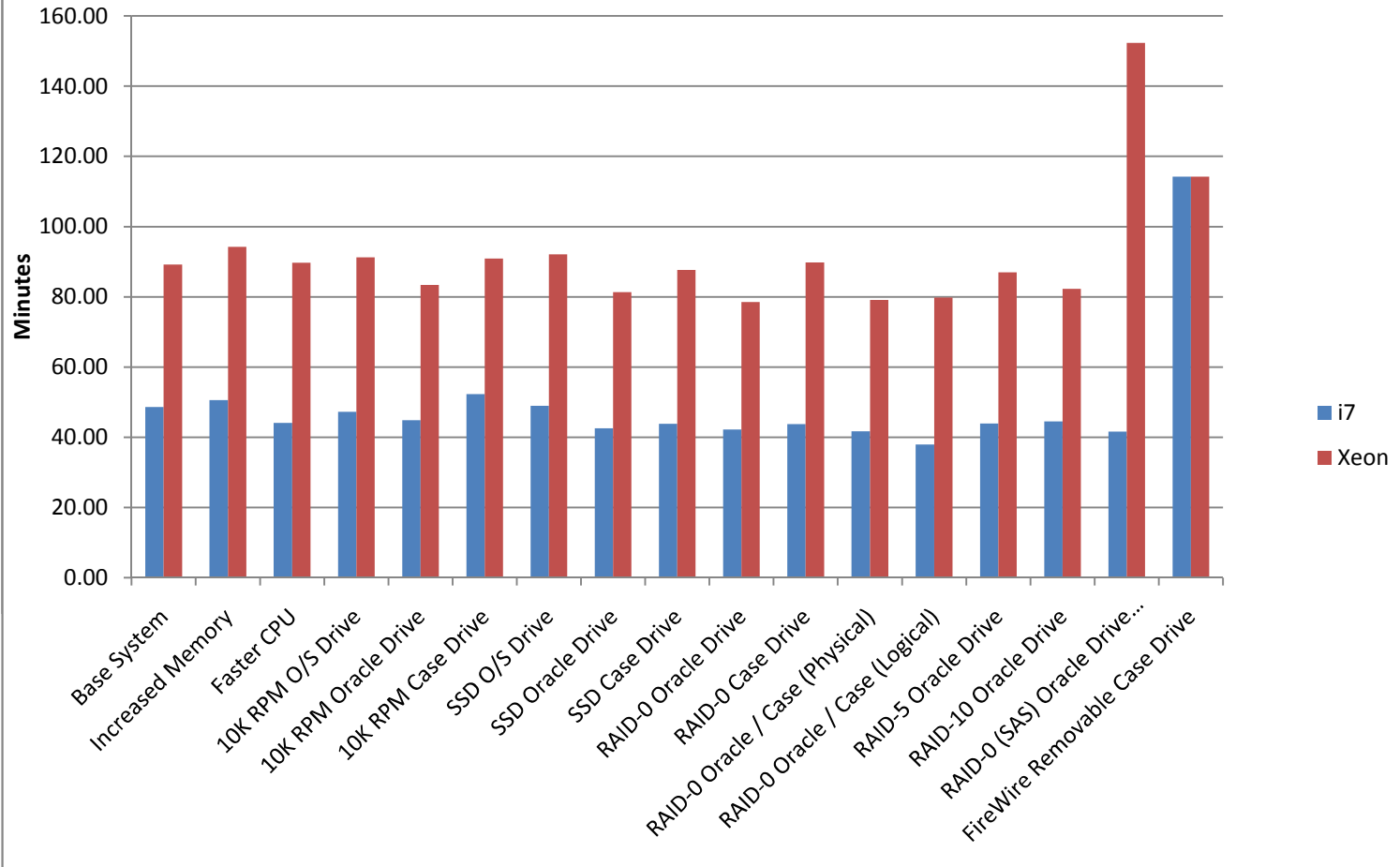
Single RAID Array Controller: Adaptec 3805 (8 Port / 128 MB RAM)

Dual RAID Arrays Controller: Adaptec 31205 (12 Port / 256 MB RAM)

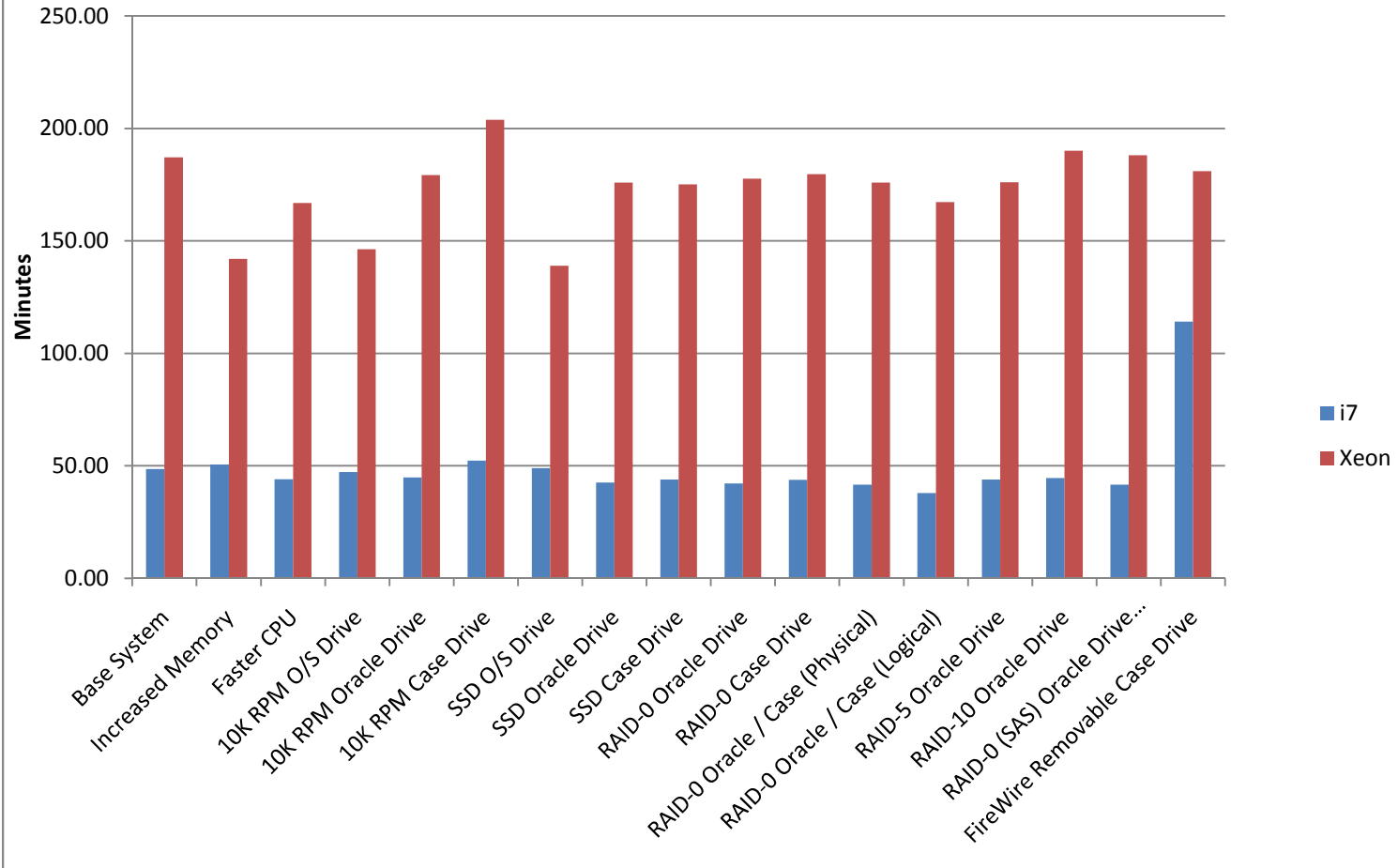
Areca RAID Controller: Areca ARC-1680ix-12 (12 Port / 4GB RAM)

Given the superior performance of the i7 system, a short series of additional tests were performed to quantify several hardware combinations on that platform only.

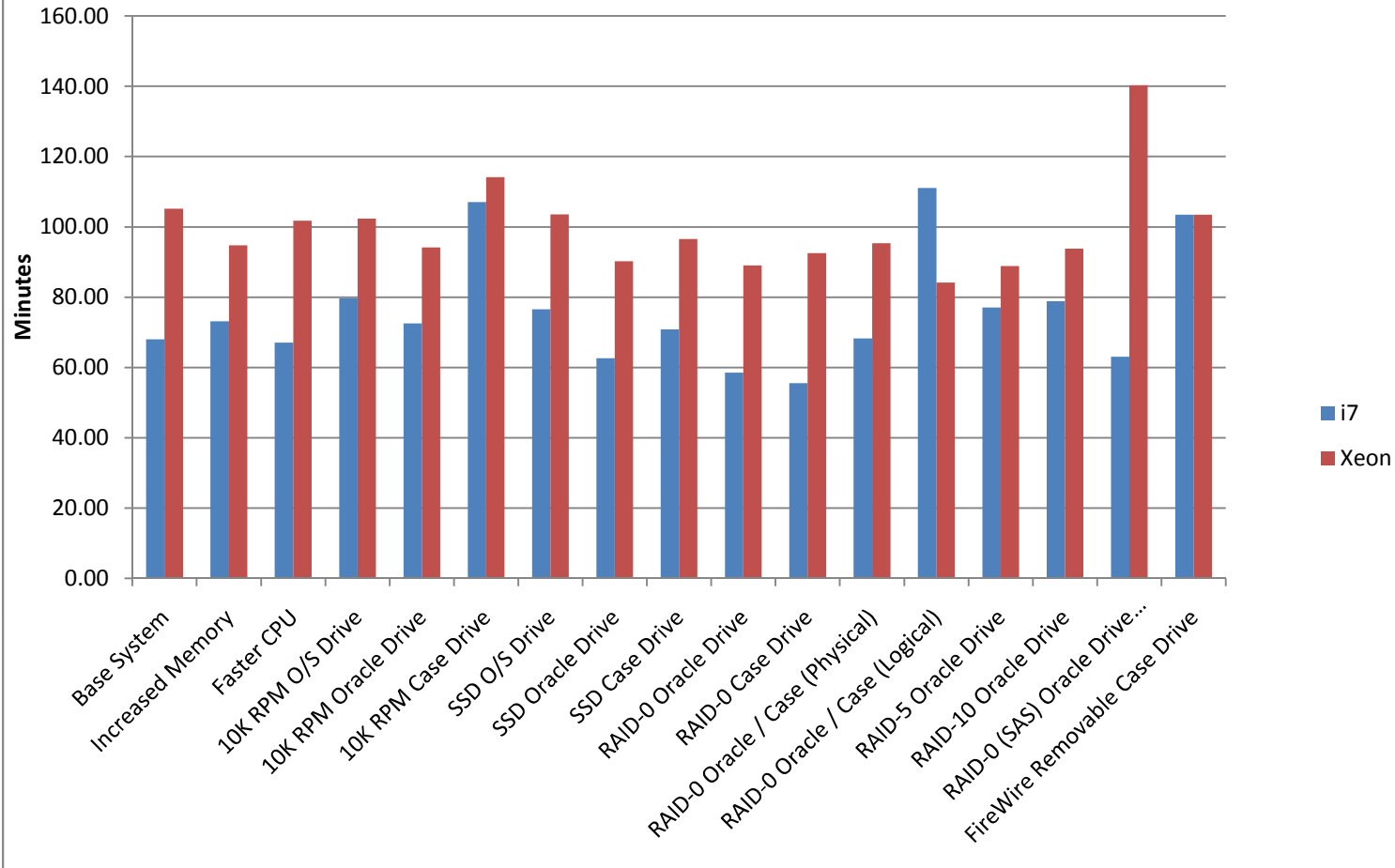
# Pre Processing



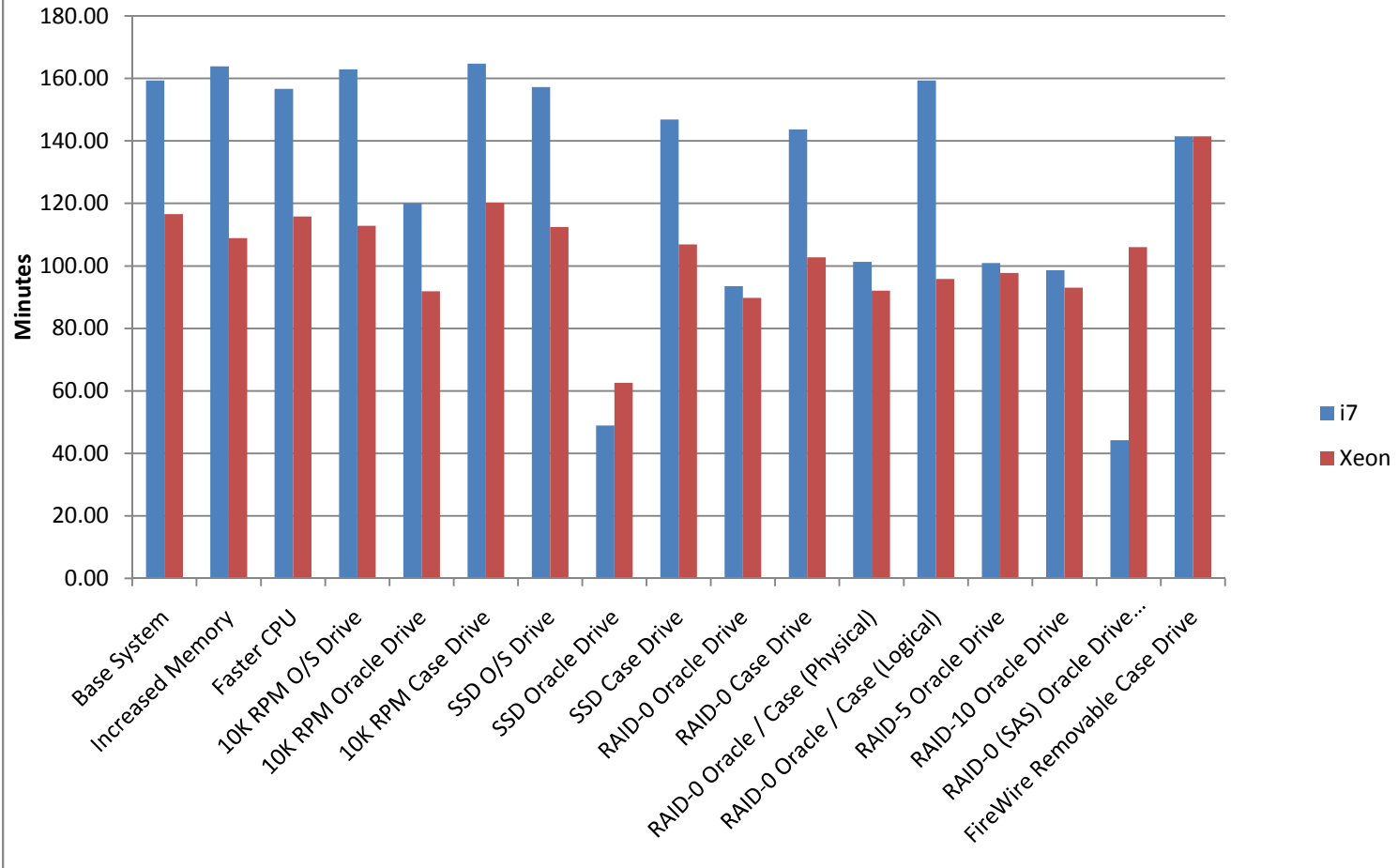
# dtSearch / Entropy



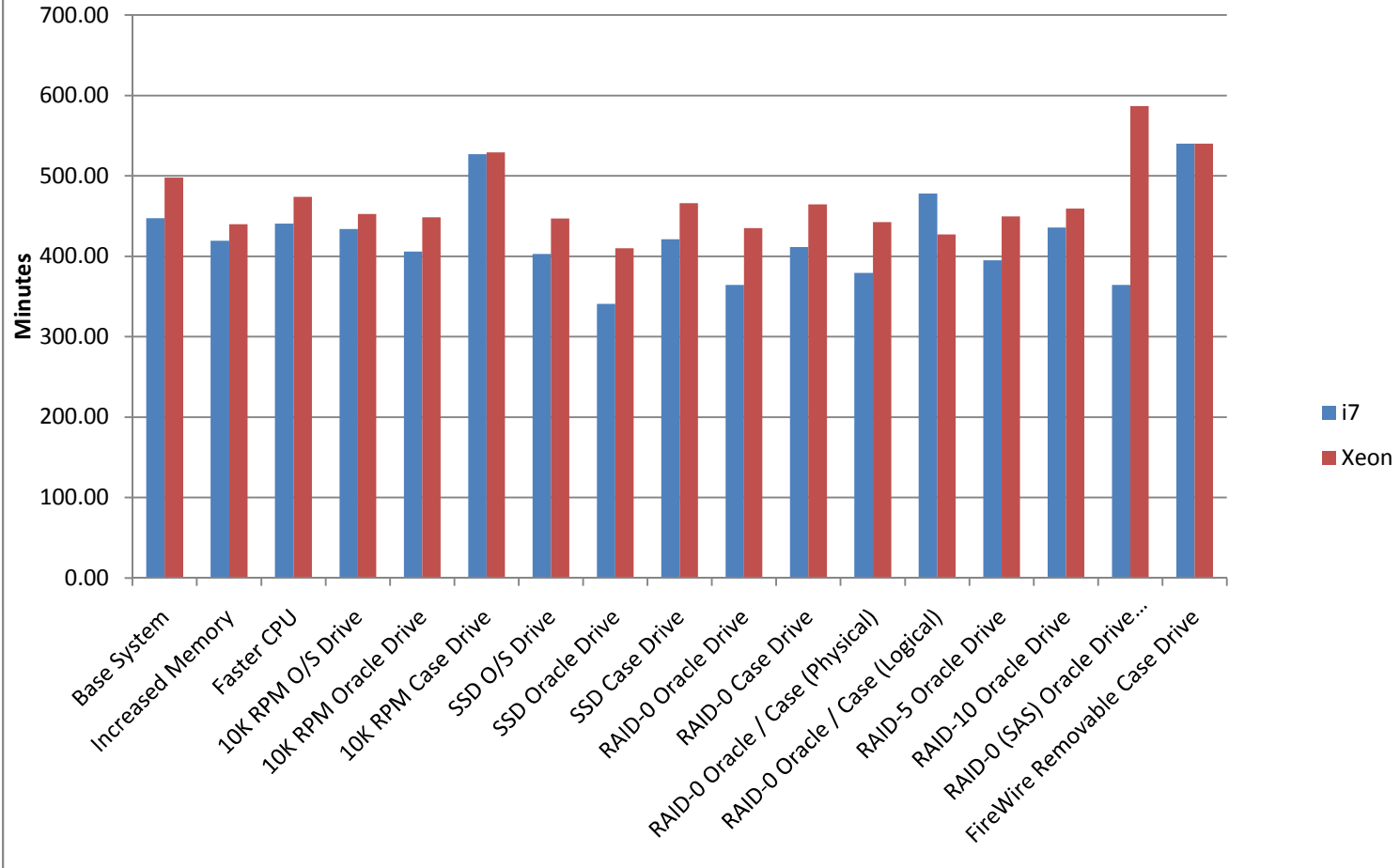
# Data/Meta Carving



# Known File Filter



# Total Time



## **Observations:**

The i7 outperformed the Dual Xeon system on almost every test. (The only exception to this was the Known File Filter benchmark). The increased i7 performance may be due to the more advanced I/O support subsystems on the i7 vs the Xeon platform (ICH9 vs ICH6 generations respectively). The i7 based platform has not only demonstrated superior performance but also results in a much less expensive platform for running FTK 3.0.

Increasing the speed of the system CPU has minimal effect. FTK 3.0 appears to benefit primarily by increasing I/O performance.

Increasing the amount of system memory is somewhat more effective than increasing the speed of the CPU but is still relatively marginal. Memory is relatively inexpensive however, and therefore most likely a worthwhile investment.

The “Oracle” drive appeared to benefit most by using a storage device capable of delivering rapid random I/O performance. Some of the fastest processing times were achieved when the SSD drive was used as the “Oracle” drive. It should be noted that putting an SSD in the O/S or Case drive position had minimal effect.

In testing the various RAID configurations RAID-0 was the fastest with RAID-5 close behind and RAID-10 (Mirrored RAID-0) a relatively distant 3<sup>rd</sup>.

The 4GB RAID controller (Areca) did not substantially outperform the 256MB RAID controller (Adaptec) in similar configurations. The 4GB RAID controller was also substantially more expensive.

While 1394b (Firewire 800) removable drives can stream data at fairly reasonable rates, they did not perform very well in these tests and do not make a good choice for use as the FTK3 case drive. Although it might be nice to store case information on removable drives, it does not appear to work very well for this particular application.

RAID-0 was only slightly faster than RAID-5. RAID-0 provides no data protection in the event of data loss. RAID-5 is a much better choice than RAID-0 due to increased data protection with only a minimal decrease in performance. Only 1 drive has to fail in a RAID-0 array to suffer complete data loss – and there are 5 points of potential failure in a 5 drive array.

RAID-10 (a mirrored RAID-0) was substantially slower than RAID-5 and RAID-0. Although RAID-10 does provide increased data protection (vs RAID-0), it is noticeably slower than RAID-5 in addition to being a relative waste of drive space.

RAID-5 appears to be the optimal RAID configuration for this application.

While the SSD drive generated outstanding performance in the “Oracle” drive position, it is a relatively expensive solution and could become a single point of failure in this configuration (vs RAID-5).

### **Considerations:**

The observations in these benchmarks are directly related to the implementation of a specific piece of software (FTK 3.0) and should not be interpreted to correlate to any other applications or uses.

These benchmarks were only performed using a single product (FTK 3.0) for a generalized test case. Although every effort was made to simulate realistic case data and processing operations, not every possible scenario, test case, operation, or hardware combination could be evaluated.

It is also expected that FTK 3.0 will not be the only application to run on the forensic workstation. With that in mind, the customer is encouraged to consider the requirements of other software products that may also be run on the system. Other applications may impose completely different demands of the CPU, Memory, Storage, Network, and Video sub-systems, etc.

The raw data is provided such that the reader can perform their own analysis and formulate personal conclusions based on individual criteria. Digital Intelligence is currently building systems which match almost all of these configurations (The Areca SAS RAID Controller is not currently an option) and our only goal is to help the customer make an informed decision.

### **Summary and Recommendations:**

With both CPU speed and memory size having a negligible effect on the performance of the analysis system we believe the greatest gain in performance can be achieved through the careful selection and configuration of the storage devices on the system.

The “10K O/S, SSD Oracle, and RAID-5 Case” drive configuration provided exceptional performance at a relatively reasonable price. This provides a massive amount of data-protected storage for the raw case information while providing impressive database performance. If you are comfortable with having your Oracle database on a single (unprotected) drive this is a very good option.

The “Dual RAID-5 Array” configuration provided very good performance while still providing data protection for both the Casework and Oracle volumes. While having the Oracle database on a RAID array is not as fast as having it on an SSD, this was the best performing combination that provided protection for both the database and raw casework data in the event of drive failure. While the Oracle database does not need all the space a 5 drive RAID-5 array can provide, it benefits from the increased performance that the

multiple spindles provide. The additional space on the Oracle RAID array could be used for other purposes as well (like database backups, exports, or archives).

FTK 3.0 appears to be I/O (not CPU) bound. The i7 platform also outperformed the more expensive dual Xeon platform for this application. Consider applying the money saved in purchasing a less expensive i7 platform toward a storage system performance upgrade (RAID or SSD).

Configuring a system with the fastest possible CPU(s) is typically a very expensive option. Again because FTK 3.0 does not appear to be CPU bound, consider purchasing a reasonably fast CPU. Testing indicates the fastest (and most expensive) CPU's do not make a big difference in FTK 3.0 performance.

Although memory did not appear to be a major factor in our benchmarks, all of the test systems were equipped with a fairly substantial amount of memory even in the baseline configurations. Memory is relatively inexpensive and can also play a major role in moving I/O around the system. Consider having the system configured to its full memory capacity. (Note: i7 memory is a lot less expensive than the Fully Buffered ECC memory used in the Xeon Systems).