Digital Intelligence®

Analyzing Hardware for EnCase v8 Optimization

Jim Borecki, Digital Intelligence Inc.

DIC 2017

My Background and Role

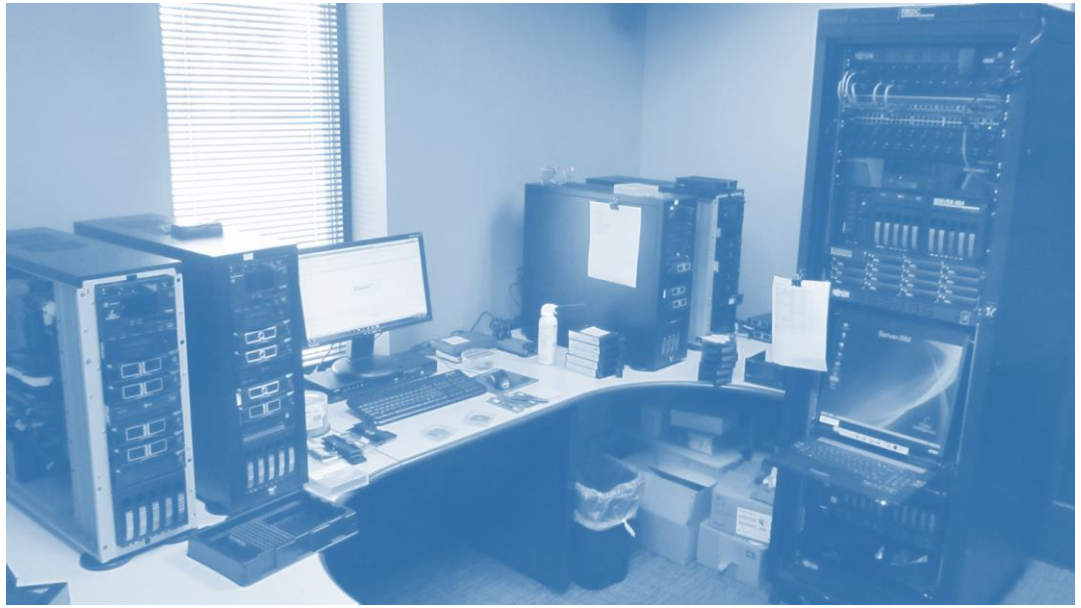
- Tableau Forensic Products – 2006 thru 2015
  - Based in Wisconsin, USA
  - Forensic Imaging Products – Duplicators, Write Blockers, & Tableau Imager
- Guidance Software – 2010 thru 2015
  - Vice President of the Forensic Business Unit
- Digital Intelligence – 2016 forward
  - Business Development
- Engineer and Business Manager by Education / Training

Who Performed The Testing?

- Jim Woodring
- Digital Intelligence Systems Engineer
- Test Workstations with various industry software
- Certify new versions
  - Hardware
  - Operating Systems
- FRED C Forensic Datacenter
  - R&D
  - Installation and Training
  - Support

Why We Test…

- System Compatibility and Stability
- Resource Requirements
  - CPU/Cores
  - Memory
  - Disk Subsystems
    - Rotational Media
    - SSD
    - NVMe
    - RAID and RAID configurations
- Result – we can provide INFORMED assistance during system selection and support!



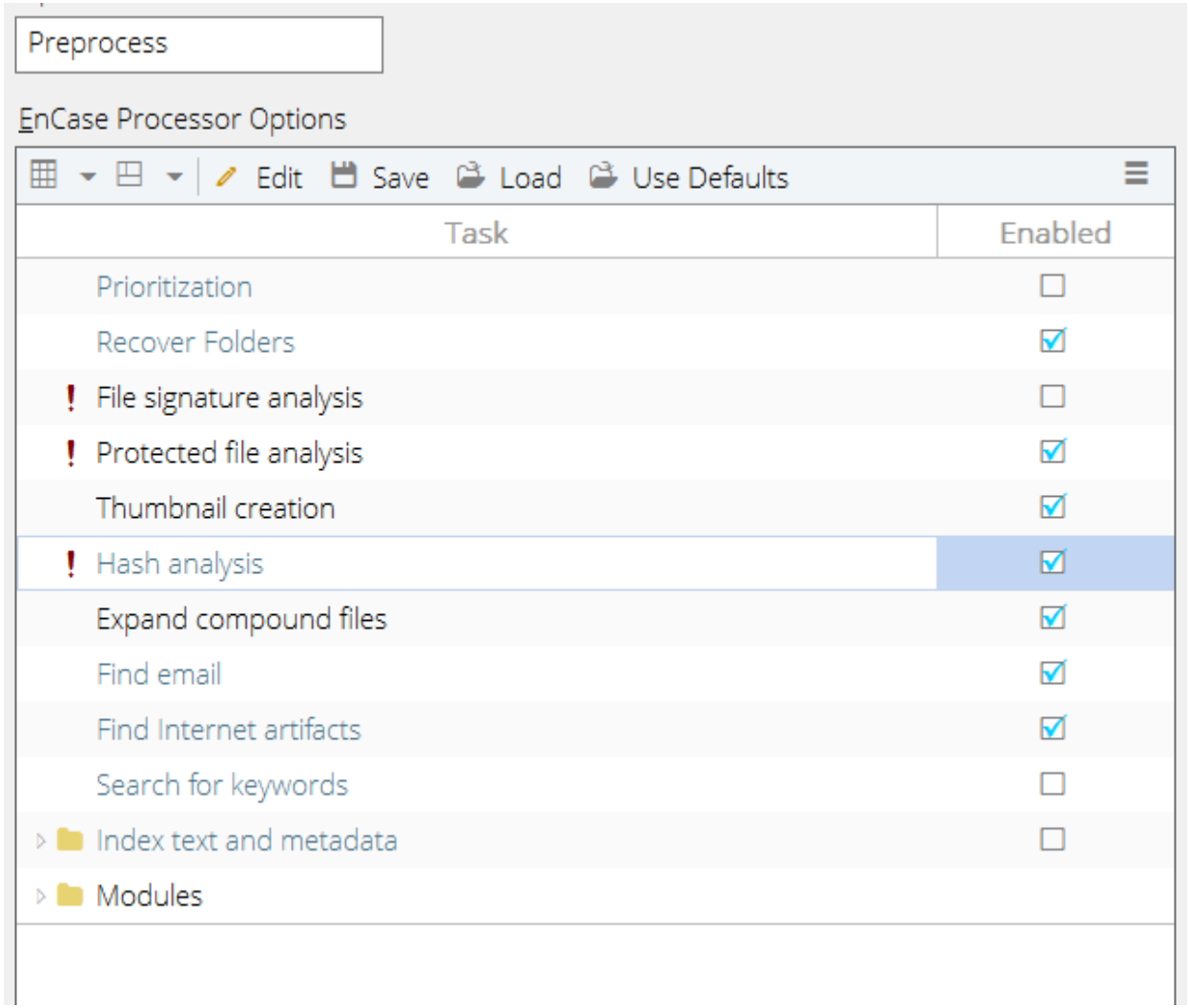
How We Test…

- Script Processes
  - Determine “typical” processing options
- “profile” of Application
  - Run test in phases to isolate the demands of each function
    - Evidence Verify
    - Pre-Processing
    - Indexing
    - Carving
- Select Baseline System
  - Typically entry-level FRED
  - Examine combined storage volumes
- Single Factor Tests
  - Alter one resource
- Multiple Factor Tests
  - Select “best” resources
  - Confirm Assumptions and Optimize

```
      $EnProcFile = @ScriptDir & $EnProcFile
   Else
      $EnProcFile = @ScriptDir & "\" & $EnProcFile
   EndIf

   If $Debug And MsgBox(4,$ProgramName, "Enproc file: " & $EnProcFile)=7 Then Exit 1

   WinActivate($LoadSettingsHandle)
   Send($EnProcFile & "{Enter}")
Else
   ; get x,y pairs and click on each
   _SplashMsg("Processing ini section: " & $Task)
   $XYArray = IniReadSection($ProgramName & ".ini", $Task)
   If $Debug Then _ArrayDisplay($XYArray,$Task & ".ini")
   If @Error = 0 Then; x,y values found
      If $Debug Then _ArrayDisplay($XYArray)
      For $x = 1 to $XYArray[0][0]
         If ($x = 1 And $RunRecoverFoldersFirst And $Task = "Index") Then ContinueLoop; skip turn off of Recover Folders - should already be off
         MouseClick("left",_GetField($XYArray[$x][1],1,$Comma),(_GetField($XYArray[$x][1],2,$Comma)*1)+$yOffset)
         _SplashMsg("Clicking on... " & $XYArray[$x][0])
         Sleep(2000)
      Next
      Switch StringUpper($Task)
      Case "INDEX"
         Send("!I{Down 2}{SPACE}"); Select East Asian Script Support
         Sleep(2000)
         Send("{TAB}")
         Sleep(2000)
         Send ("{ENTER}"); OK
      Case "CARVE"
         Send("!S{RIGHT}{RIGHT}")
         Sleep(2000)
         Send("!N")
         Sleep(2000)
         Send("{ENTER}"); OK
      EndSwitch
   Else; No Ini section found - skip
      If $Debug And MsgBox(4,$ProgramName, "No INI section found for " & $Task)=7 Then Exit 1
      $Skipping = True
   EndIf
EndIf
Sleep(5000)
Options_Label_Click();
Send($Task)

If $Debug And MsgBox(4,$ProgramName, "Ready to Proceed")=7 Then Exit 1
Sleep(1000)
MouseClick("left",590,957); click OK button
_SplashMsg("Processing " & $Task & " task....")

; check for "Warning - options have changed window
If WinExists(GetWinHandle2("Warning",2)) Then
   Send("!y")
```

Test Phases

- Verify – part of adding evidence
  - Checks the integrity of the E01 files
- Pre-Process
  - Start with “defaults”
  - Alter based on input from DI’s Services team
  - Add protected file analysis
    - Checks for file encryption



Test Phases - continued

- Index
  - De-select all current options
  - Select “Index text and metadata”
    - Select “East Asian Script Support”
- Carve
  - Select File Carver module
    - Note – carving utilizes the Hash Libraries

File Carver

Use this module to find file fragments in files, file slack, and unallocated space.

This module uses file signatures from the File Types table to identify file fragments.

Once identified, file fragments can be exported to a specified location.

Selected File Types

ZIP Compressed	Selected
JPEG Image Standard	Selected
TIFF Image	Selected

Search Options

Search All Files	Unselected
Search Unallocated	Selected
Search File Slack	Selected

Search Options

Carve HTML Files	Unselected
Carve Webmail Files	Unselected

Export Settings

Export Carved Files	Unselected

Evidence Repository

- Source http://digitalcorpora.org/corpora/files
  - courtesy of **Garfinkel, Farrell, Roussev and Dinolt, Bringing Science to Digital Forensics with Standardized Forensic Corpora, DFRWS 2009, Montreal, Canada**
- Build Repository
  - 1 million “random” files (GovDocs)
  - Enron dataset
  - Browsing History
- Process to create Test Disk
  - Sample files to get appropriate dataset size
  - Prepare base OS install (win10)
  - Make users w/”desktops” and other supporting structures
  - Copy files to user’s “documents” (round-robin)
    - Obfuscate by changing extension periodically
  - Copy and delete to “fragment” the drive – create carving challenge
  - Put sample Internet Activity into a single user’s browser history files
    - https://www.symantec.com/connect/articles/web-browser-forensics-part-1
- See also http://www.forensicfocus.com/images-and-challenges

“ImageDisk7”

- Windows 10x64
- 2 users
- 51 GB data/~96,000 user files
  - Split evenly between the 2 users
- 46 file extensions*
  - Note some may be obfuscated
- Baseline system test takes ~ 8 hours
- Internet history “injected” for one user
- Image with Tableau Imager/Digital Intelligence UltraBay 4
  - 29 E01 Files

Count	extension		Count	extension
21009	.PDF		17	.PST
19424	.HTML		14	.TEX
19395	.JPG		14	.TMP
7161	.TXT		13	.TROFF
6979	.DOC		7	.BMP
5782	.XLS		4	.PUB
4461	.PPT		4	.SGML
3298	.GIF		3	.GLS
1961	.PS		3	.XLSX
1668	.CSV		1	.BAT
1287	.GZ		14	.TMP
945	.LOG		13	.TROFF
491	.EPS		7	.BMP
…	…		4	.PUB

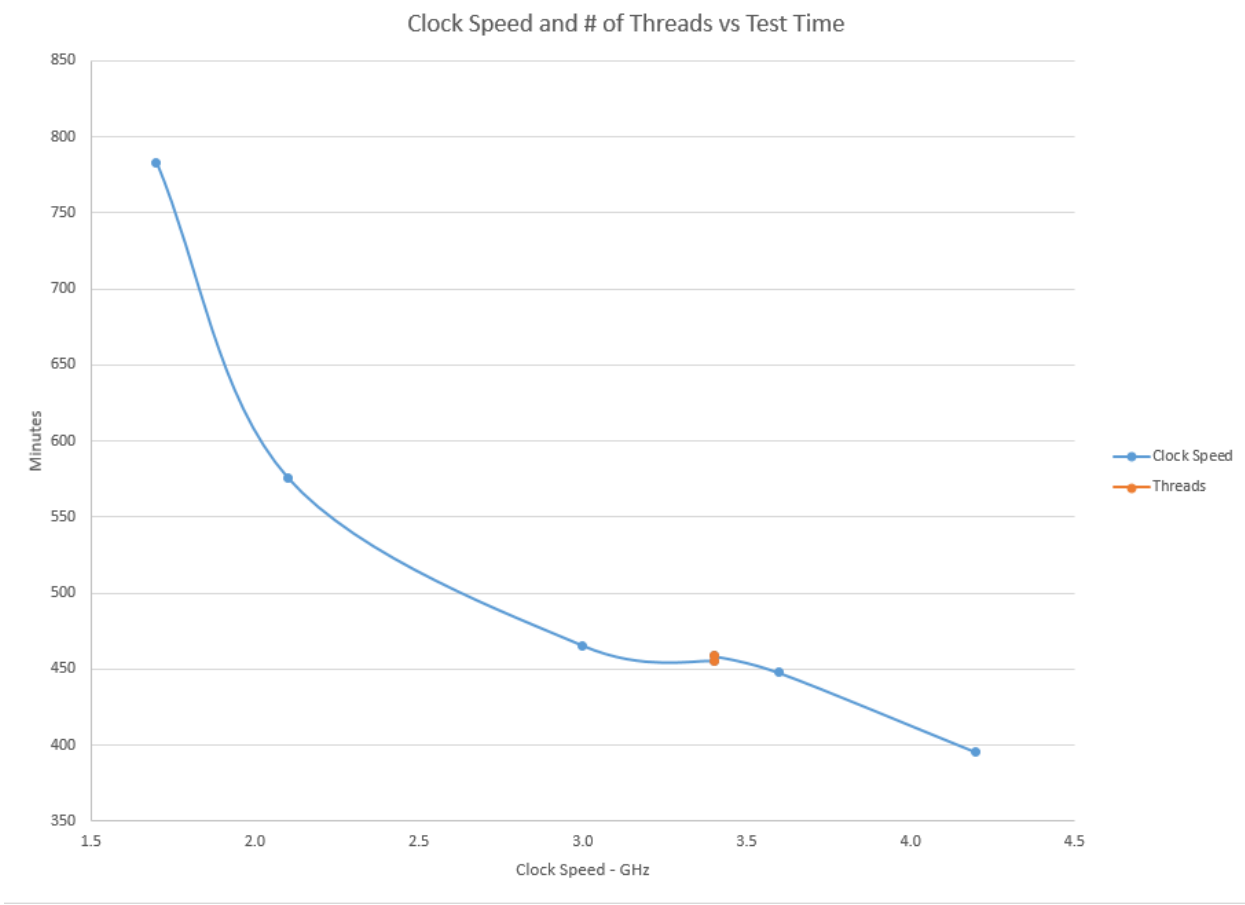
System Resources and Testing

- CPU/Cores
  - X99 (i7 6800K Family)
  - Z10 (Xeon E5-2600 Family)
- Memory
- I/O Subsystem Types and Architectures

- Single Factor Testing
  - Identifies the relative contribution of a specific resource
  - May have inter-dependencies
- Multi-factor Testing
  - Combines “best contributors” to obtain cumulative improvements
  - Helps identify and resolve inter-dependencies

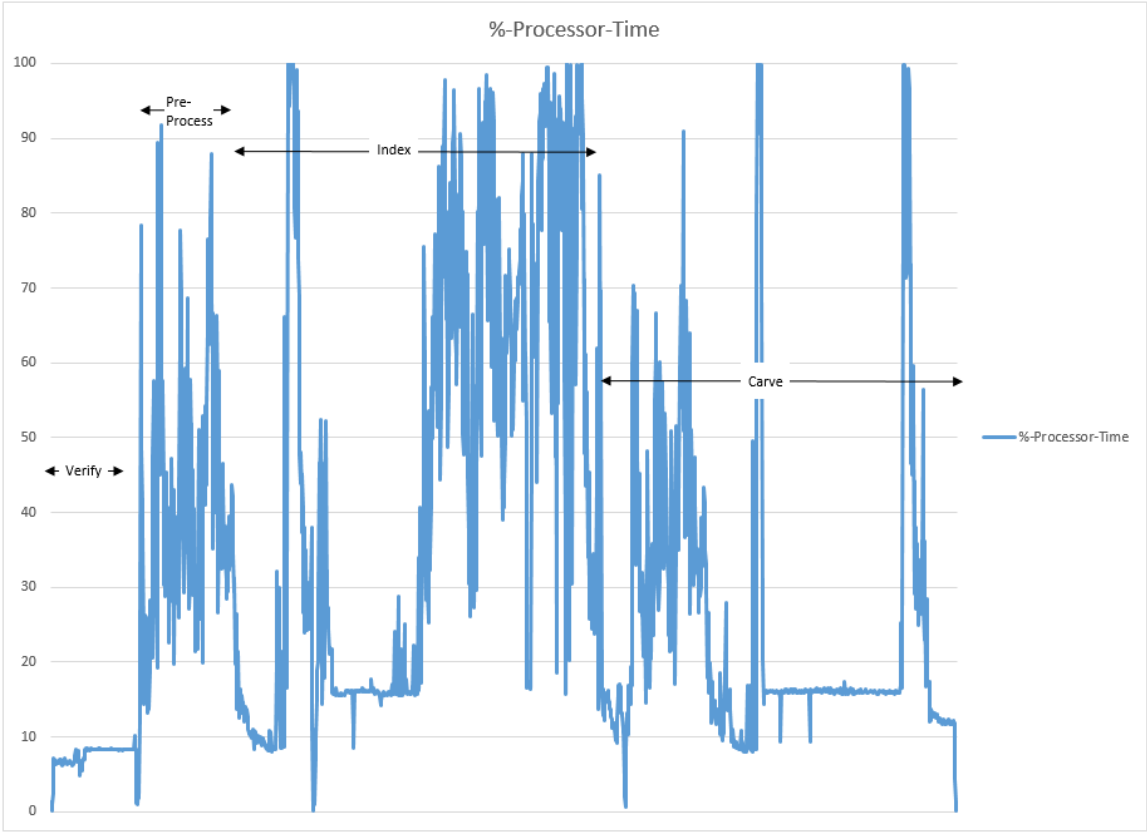
CPU Concepts

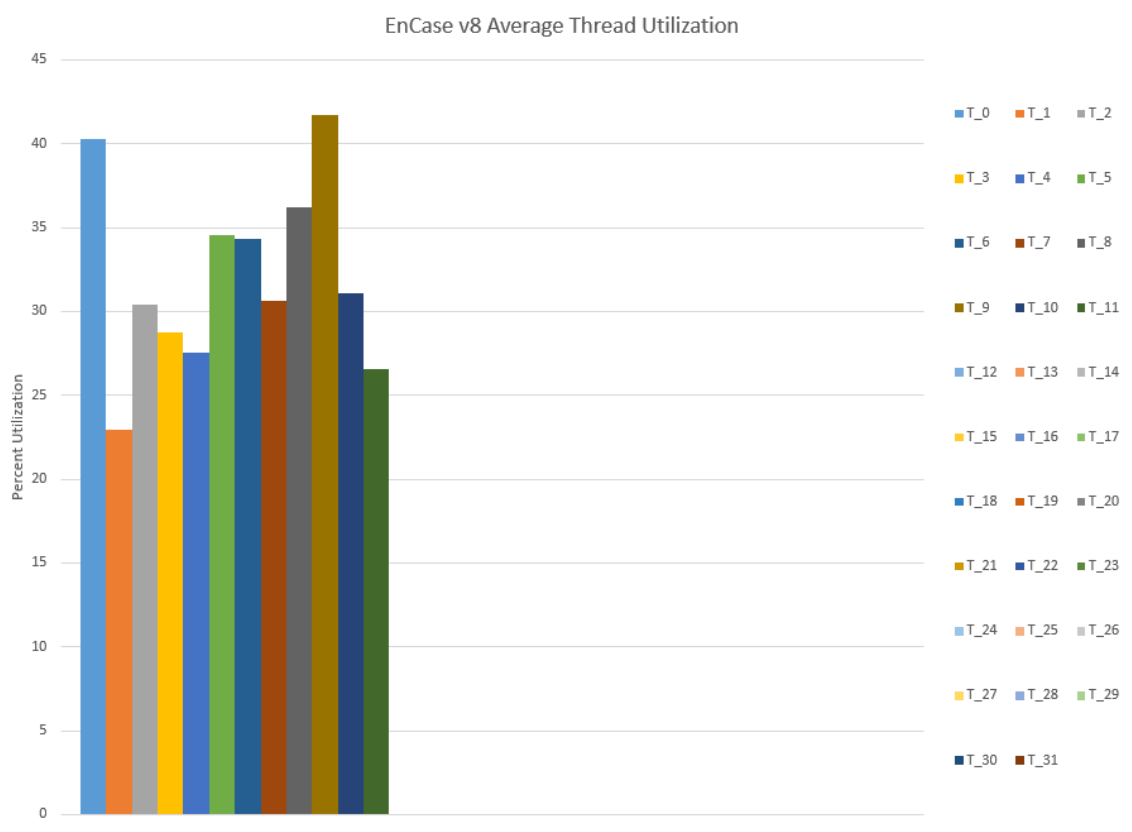
- Clock speed
  - Faster clock speed *can* yield Faster test times when:
    - There are “Single Threaded” processes like Validation
    - Either the application, specific workload, or just the forensic process in general doesn’t lend itself to multi-threading
- Threads (Hyper-threading = 2X cores)
  - Increased cores for the same clock speed doesn’t have much effect < 1%
  - More cores usually result in reduced clock speed due to thermal issues



CPU – i7

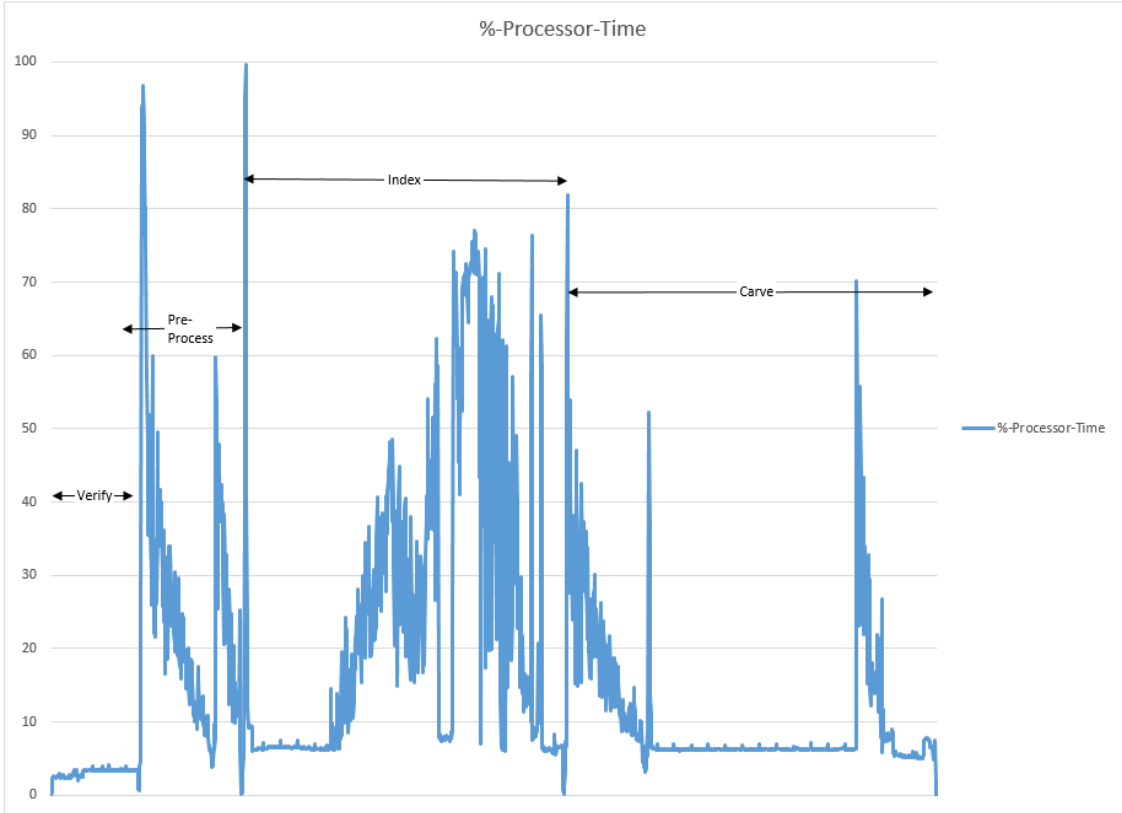
Intel(R) Core(TM) i7-6800K CPU @ 3.4 GHz – 6 cores – 12 Threads
Thread loads are well balanced – StdDev = 5.3
The average thread is 32% utilized

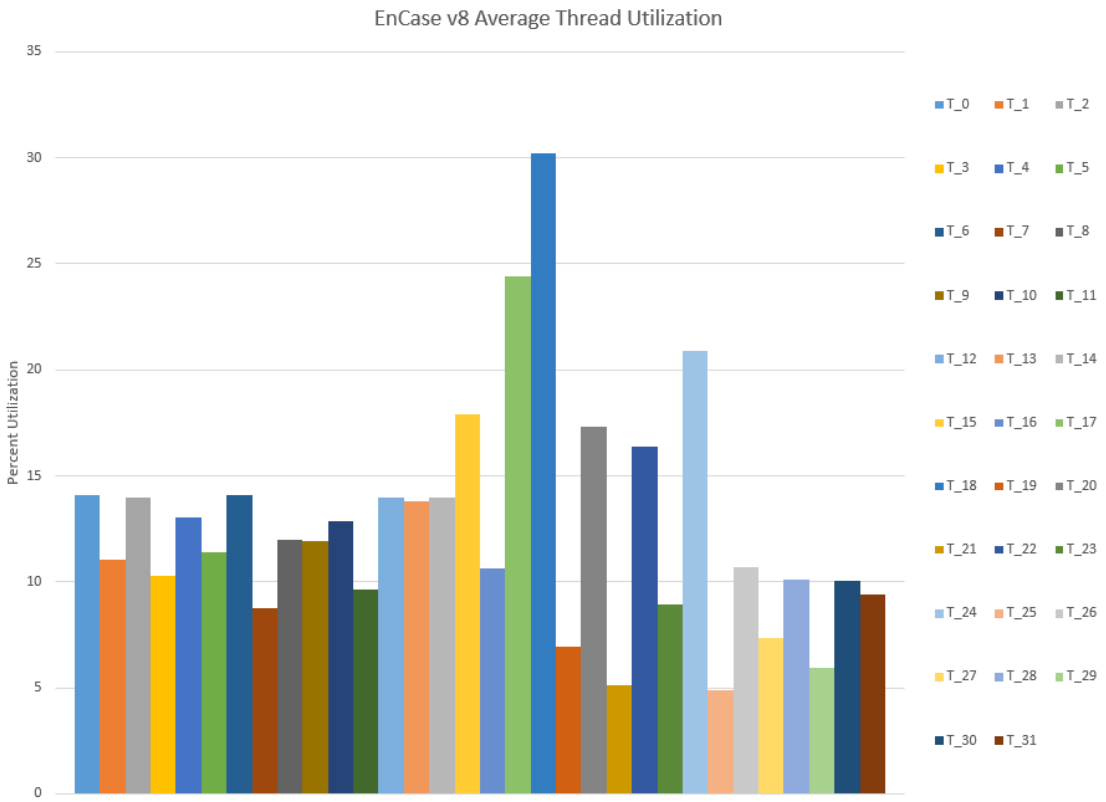




CPU – Xeon

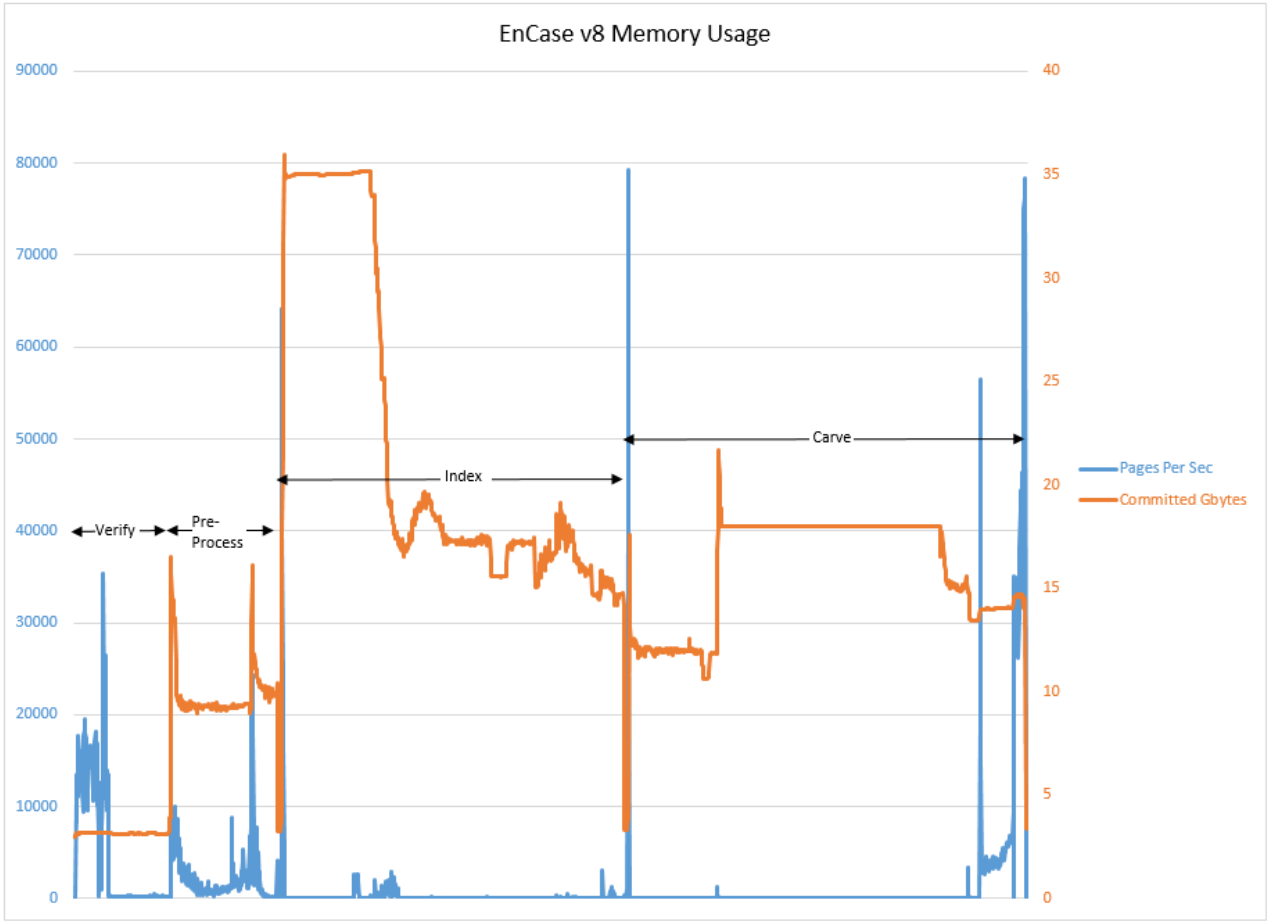
Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.1 GHz – 8 cores – 16 threads and 2 processors = 32 threads
Threads are well balanced – StdDev = 5.3
The average thread is 12.5% utilized





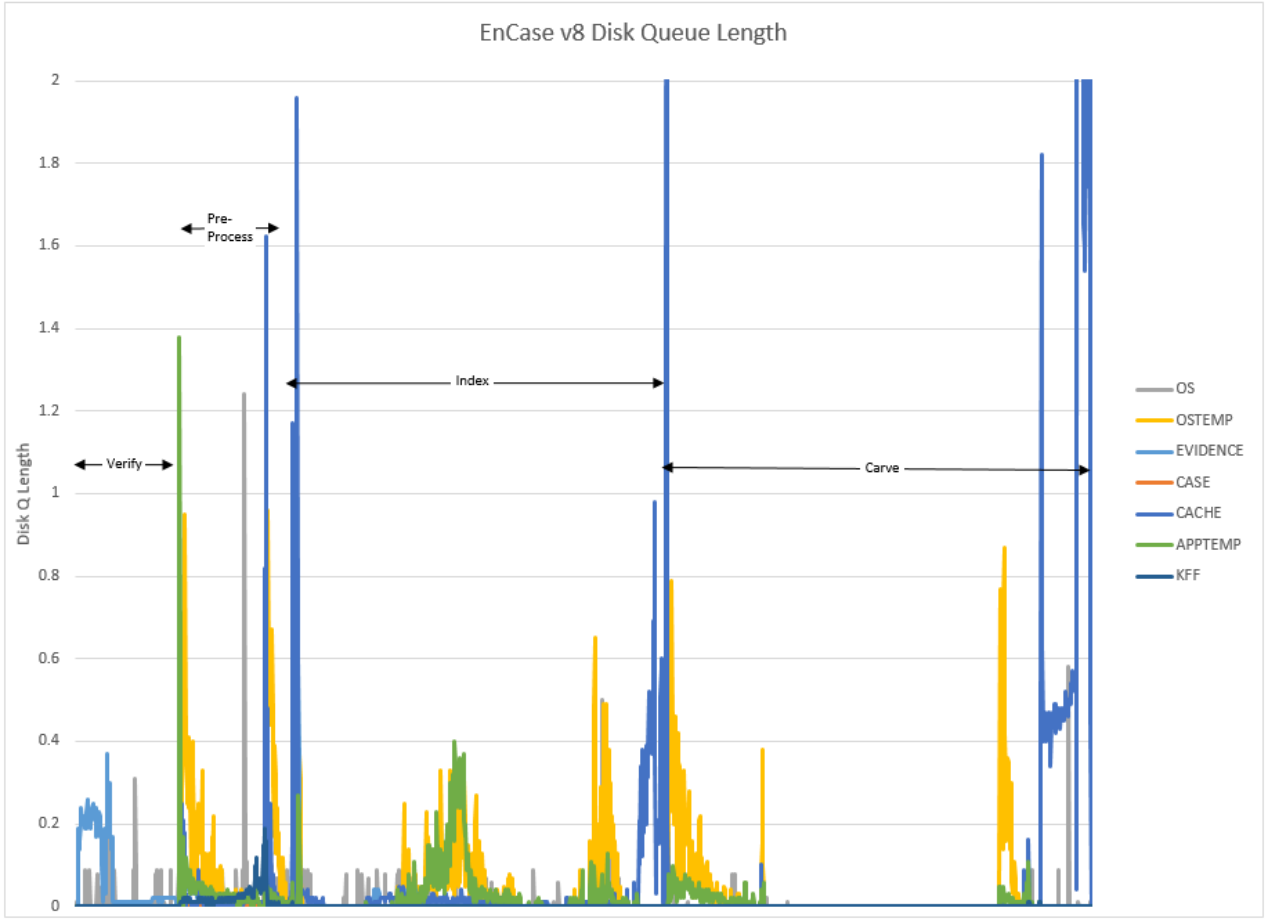
Memory

- Measures “Committed Memory”
  - Committed to application(s)
- Extremely sensitive to case contents and size
  - Large carving jobs need more memory
- Additional memory used by Operating System
  - I/O Buffering
  - “Background” processes/services
- The effects of memory changes are hard to predict – testing is required



Disk I/O

- 7 Different I/O Channels Identified
  - OS – Operating System
  - OSTEMP – TMP and TEMP environment variables
  - Evidence – E01 file storage
  - Case – Case file location
  - Cache – Cache file location
  - APPTEMP – “TEMP” sub-folder of Case file location
  - KFF – File signatures (NIST)
- Examine Throughput, I/O Operations, Disk Queue Length
- Example - Disk Q Length
  - Shows Channel Activity
  - Identifies “bottle necks”



Storage Channels and Application Demands

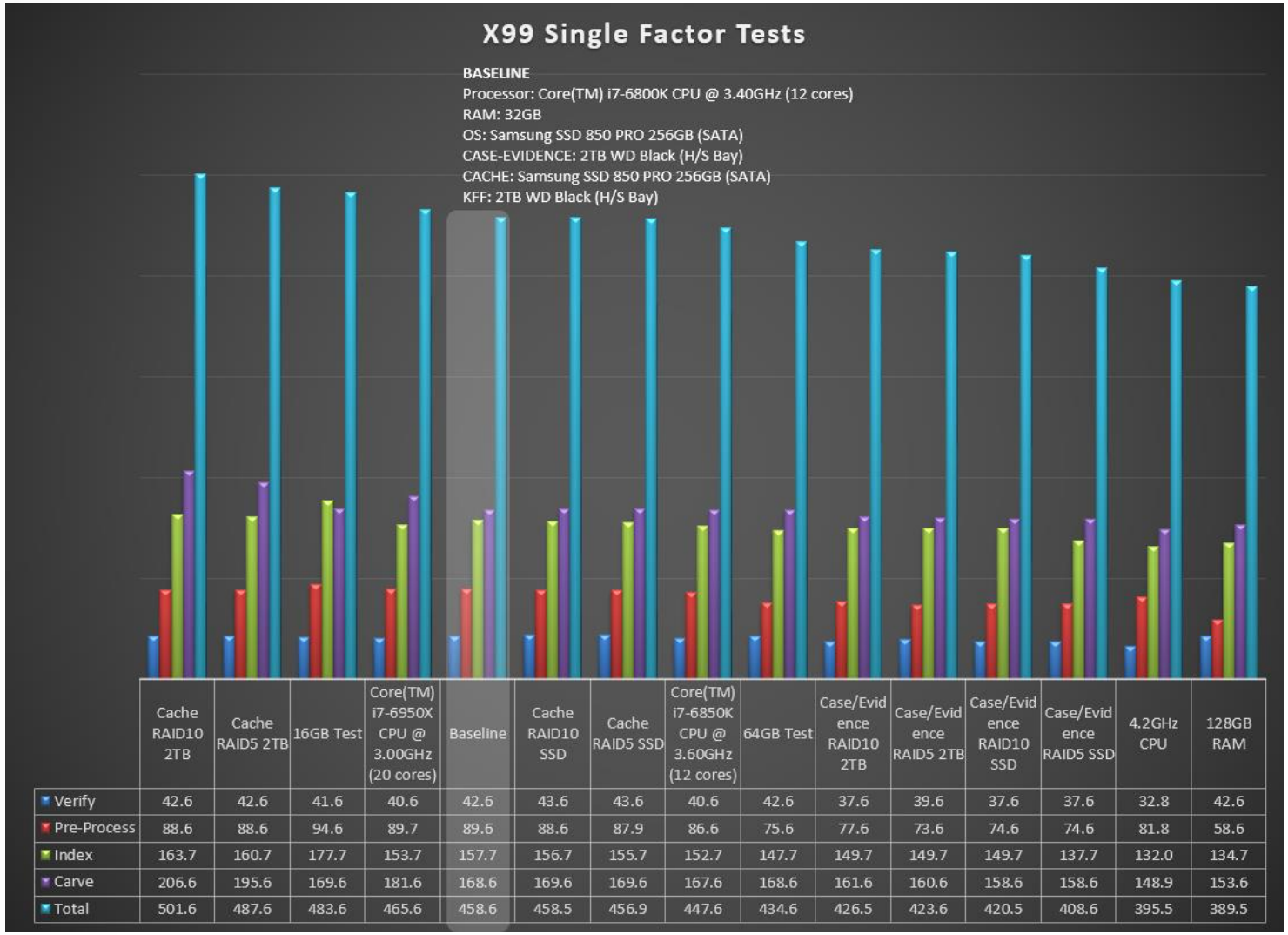
Location	Throughput	IOPS	Write Performance	Queue Depth	Storage Capacity (% of E01 size)	Desired Fault-Tolerance
OS	Low	Low	Low	Low	Low	Low
OSTEMP	Medium	Medium	High	Medium	Medium (100%)	None
EVIDENCE	High	High	None	High	High (100%)	High
CACHE	Medium	High	High	High	Very High (300%)	Medium
CASE	None	None	None	None	Low	Medium
APPTEMP	Medium	Low	Medium	Medium	Low (10%)	None
KFF	Low	Low	None	Low	Low (Fixed < 40GB)	None

Discussion of I/O Architectures

Type	IO Operations / Throughput	Strengths	Weaknesses
SATA Mechanical	Low/Low	Low $$ per GB, High Capacity	Slow, No Fault-tolerance
SATA SSD	Medium/Medium	Good IOPS and Throughput	No Fault-tolerance, Limited Capacity
RAID 5	Medium/High	Good Read Performance, Fault-tolerant, Good Capacity	Poor Write Performance, Increased Storage Overhead
RAID 10	High/High	Good Read/Write Performance, Fault-tolerant	High Storage Overhead
NVMe	Very High/High	Excellent IOPS and Good Read/Write Performance	No Fault-tolerance, Limited Capacity, High Cost

Single Factor Results

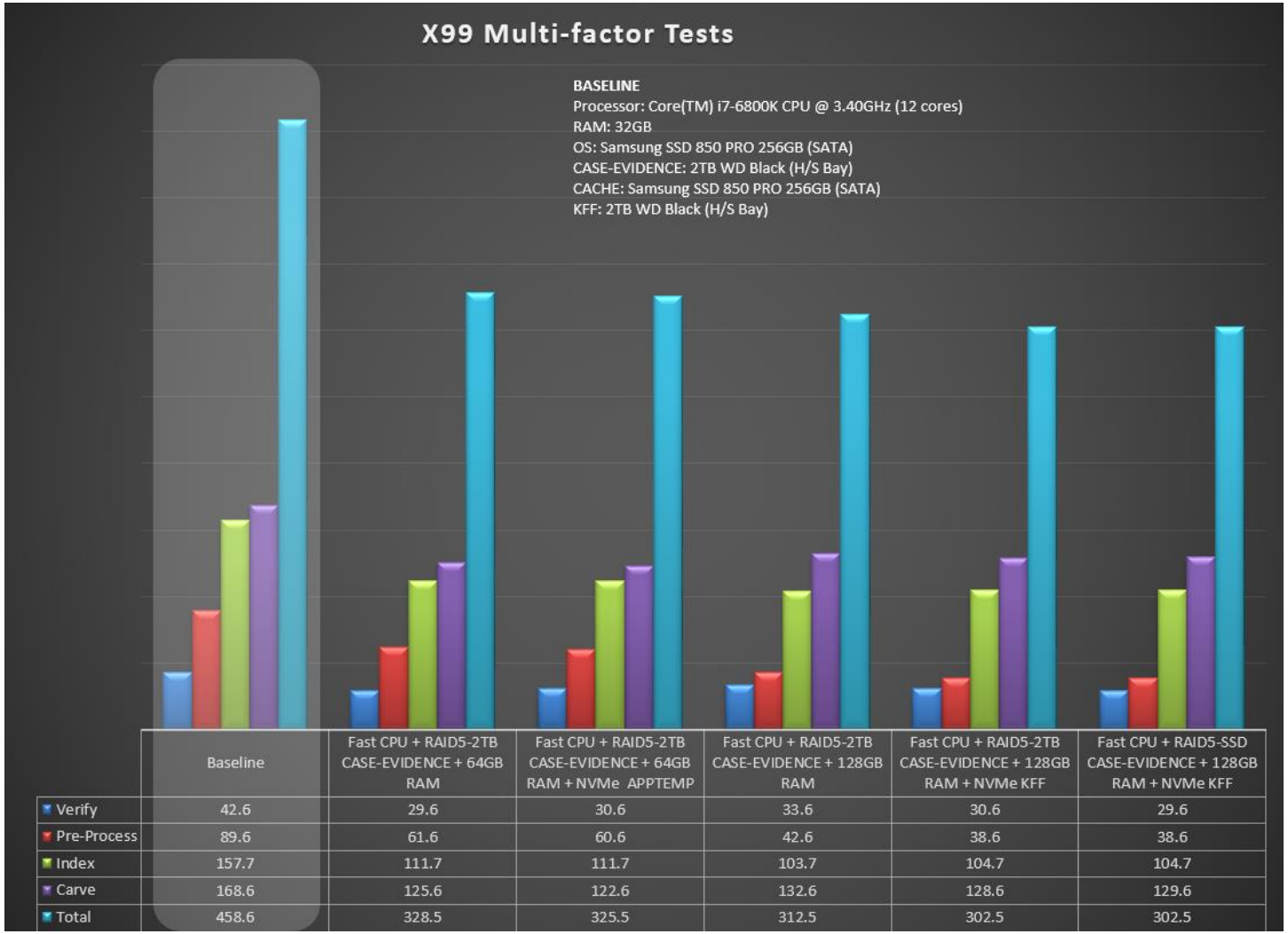
- Benefits
  - Maximum Memory
    - Affects Pre-Processing
  - Increased Clock Speed
    - Affects Verify, Indexing, and Carving
- Surprises
  - RAID-5 vs RAID-10
  - RAID CACHE Volume



	Cache RAID10 2TB	Cache RAID5 2TB	16GB Test	Core(TM) i7-6950X CPU @ 3.00GHz (20 cores)	Baseline	Cache RAID10 SSD	Cache RAID5 SSD	Core(TM) i7-6850K CPU @ 3.60GHz (12 cores)	64GB Test	Case/Evidence RAID10 2TB	Case/Evidence RAID5 2TB	Case/Evidence RAID10 SSD	Case/Evidence RAID5 SSD	4.2GHz CPU	128GB RAM
Verify	42.6	42.6	41.6	40.6	42.6	43.6	43.6	40.6	42.6	37.6	39.6	37.6	37.6	32.8	42.6
Pre-Process	88.6	88.6	94.6	89.7	89.6	88.6	87.9	86.6	75.6	77.6	73.6	74.6	74.6	81.8	58.6
Index	163.7	160.7	177.7	153.7	157.7	156.7	155.7	152.7	147.7	149.7	149.7	149.7	137.7	132.0	134.7
Carve	206.6	195.6	169.6	181.6	168.6	169.6	169.6	167.6	168.6	161.6	160.6	158.6	158.6	148.9	153.6
Total	501.6	487.6	483.6	465.6	458.6	458.5	456.9	447.6	434.6	426.5	423.6	420.5	408.6	395.5	389.5

Multi-factor Results

- Benefits
  - Confirms decision to combine CASE and EVIDENCE volumes
  - ~35% overall performance improvement
- Surprises
  - RAID w/SSD's does not differentiate itself



	Baseline	Fast CPU + RAID5-2TB CASE-EVIDENCE + 64GB RAM	Fast CPU + RAID5-2TB CASE-EVIDENCE + 64GB RAM + NVMe APPTEMP	Fast CPU + RAID5-2TB CASE-EVIDENCE + 128GB RAM	Fast CPU + RAID5-2TB CASE-EVIDENCE + 128GB RAM + NVMe KFF	Fast CPU + RAID5-SSD CASE-EVIDENCE + 128GB RAM + NVMe KFF
Verify	42.6	29.6	30.6	33.6	30.6	29.6
Pre-Process	89.6	61.6	60.6	42.6	38.6	38.6
Index	157.7	111.7	111.7	103.7	104.7	104.7
Carve	168.6	125.6	122.6	132.6	128.6	129.6
Total	458.6	328.5	325.5	312.5	302.5	302.5

Conclusions

- Increased Benefit
  - Maximize Memory
  - Maximize CPU clock speed
  - RAID for read-intensive volumes
    - Evidence
    - Case – little or no activity*
  - KFF on high IOPS volume

- Reduced Benefit
  - Increase # of Cores
    - Usually results in lower clock speeds due to thermal issues
  - RAID-10 vs RAID-5
    - Significant loss of storage capacity with no major performance improvement
  - RAID for write-intensive volumes
    - Cache

* APPTEMP has some impact

In Closing

- Your Mileage may vary….
  - Many factors are affected by evidence quantity and makeup
    - Image processing
    - Lotus Notes
    - Other “plug-ins”
  - Could vary by case or by discipline
  - Only you can determine what makes sense in your situation

Thank You!

- Questions?
- Coming Soon - Look for the full report on our website

  http://www.digitalintelligence.com