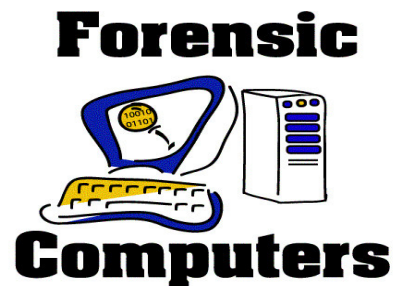


Equipping A Forensic Lab



Techno Forensics 2007

October 29, 2007

By

Greg Dominguez

Forensic



Computers

Overview

- ☞ What is a Lab
- ☞ Things to Consider
- ☞ Workstations
- ☞ Hardware Write Protection
- ☞ Software
- ☞ Training
- ☞ Tool Kits

The Computer Forensics Lab



Forensic



Computers

The Computer Forensics Lab

❏ What is a “Computer Forensics Lab”?

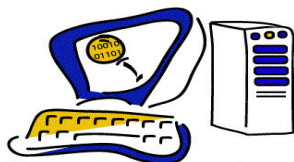
A Computer Forensics Lab or CFL is a designated location (permanent or mobile) for conducting computer based investigations.

The lab should be securable in order to prevent unauthorized access.



Things To Consider

Forensic



Computers

Forensic



Computers

Things To Consider

“Investigative Needs”

- ❏ In determining the type of forensic computer equipment needed, you should consider the following:
 - ❏ Type and volume of investigations being conducted
 - ⌚ Is the organization LE, or Corporate?
 - ⌚ If Corporate, are investigations internal only or internal and external.
 - ⌚ Organizations conducting external investigations may require a more broad range of capabilities than one that only does internal investigations.
 - ❏ Intended use of the machine:
 - ⌚ Will it be used only for imaging?
 - ⌚ Will it be used only as an analysis platform or will it be used for everything?
- ❏ Ultimately, and unfortunately the budget may override everything.

Forensic



Computers

Things To Consider

“Budget”

- ❯ Relatively few labs have an unlimited budget. So, there are a number of other things to consider:
 - ❯ How many investigators/examiners are assigned to the lab?
 - ❯ What equipment and software are already present?
 - ❯ What is the expected or known volume of work?
- ❯ The idea is to get as much for your money as you can. Purchasing from one source can often save you money as the company may be able to give larger discounts on volume purchases.

Forensic



Computers

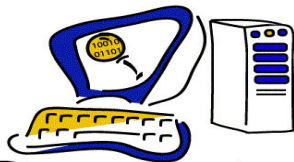
Things To Consider

“Space In The Lab”

- ❏ The facility or room you have for your lab may be out of your control.
 - ❏ The size of the lab should be major factor in the planning of furniture and how many systems you put in it.
 - ❏ If you have a closet for a lab, you will be limited if not crippled.
 - ❏ Do not forget to have a place to secure the original evidence.
 - ❏ Climate control (Heating & Air Conditioning)
 - ❏ Proper lighting
 - ❏ Does the lab have enough power for all you want to install?
 - ❏ Do not forget to plan for growth.

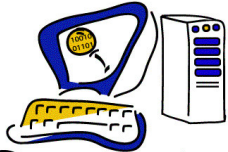
Workstations

Forensic



Computers

Forensic



Computers

Critical Hardware Choices

- ❏ One major decision point is whether to roll your own or purchase complete systems.
- ❏ Self-Built Forensic Systems
 - ❏ Great to do to learn hardware.
 - ❏ Initial purchase can be less expensive.
 - ❏ Investigator/Examiner must decide what parts to order.
 - ❏ Investigator/Examiner must integrate components from various suppliers and maintain purchase records in the event of product failure.
 - ❏ Investigator/Examiner is then responsible for all troubleshooting and repair.
 - ❏ The investment of time can be substantial which means a loss of investigative time.
- ❏ Commercially Purchased Forensic Systems
 - ❏ Vendor does all integrating and testing.
 - ❏ Vendor is responsible for warranty issues when problems occur and they will.
 - ❏ System arrives ready for use.
 - ❏ Investigator/Examiner can begin validation testing and investigating.

Forensic



Computers

Building Your Own

Critical choices are:

- ⌚ The case or enclosure
- ⌚ The processor(s)
- ⌚ The Motherboard
- ⌚ Power Supply
- ⌚ Memory (RAM)

🖱 Less Critical, yet still important choices are:

- ⌚ Hard drives for the OS and for data
- ⌚ Removable Drive Bays
- ⌚ Video Card
- ⌚ Monitor

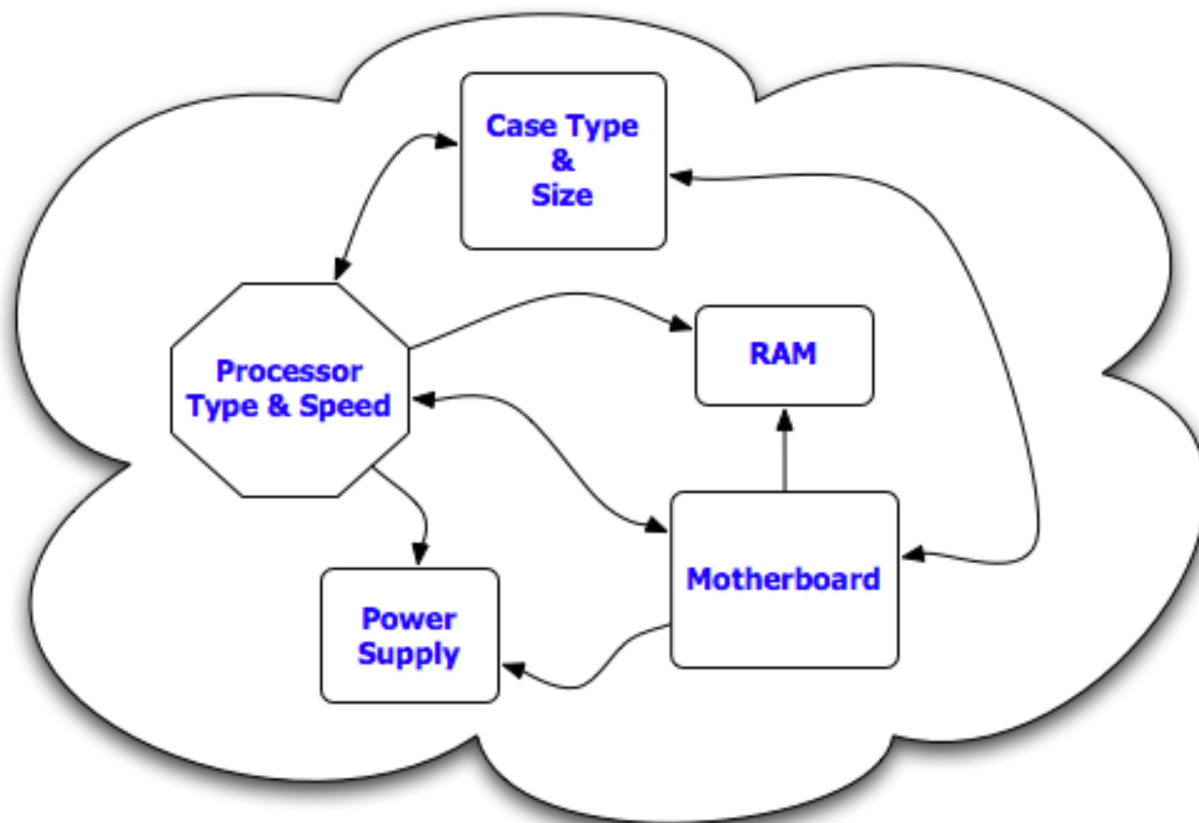
🖱 Consider the true needs versus the wants or nice to have items.

Forensic



Computers

Hardware Decisions



Forensic



Computers

Computer Cases

- ❏ The case you choose will depend on the intended use.
 - ❏ Do you need a full size tower or rackmount?
 - ❏ Does your system need to be portable?
 - ❏ Do you need multiple DVD/CDROM drives?
 - ❏ Do you need a RAID array in the case?
 - ❏ Does your chosen motherboard require a certain size case?
- ❏ Consider purchasing a case that can be used again when it is time to upgrade the motherboard/CPU/RAM combination.
- ❏ Consider a case that allows for expansion.
- ❏ Consider the construction quality as cases are not created equally.

Forensic



Computers

Cases/Enclosures

1 Square PC	Arrow Micro	Chenming	GearXS.com	MaPower	Seagate	Triumph
3COM	AsiaPro	Chiefmax	Generic	MASSCOOL	Shuttle	TTGI
3Dfx	Aspire	Chieftec	Genica	Media-To-Go	Sicuro	UML
3DO	Asus	CI DESIGN	Globalwin	Meritline	Silverstone	Vanguard
3Ware	Atadc	Cintre	Hewlett Packard	MGA Matrox	Sky	Vantec
Abiding	Athena Power	Codegen	HighPoint	MGC	Skyhawk	Vaster
ABS Computer	Athenatech	Codegen Group	Hi-Touch Imaging	MGE	Sony	ViPower
Acard	A-Top Technology	Compaq	House Brand	Modware	SOUNDCASE	WEGO
Adaptec	ATI	Compucase U.S.A	IBM	Morex	Soyo	Wytron
ADS Technology	Atrix	Cooler Master	iConcepts	NEC	Sparkle	Xcase
AeroCool	Avus	Cooler One	Impression	NHJ	Spire	XCLIO
Ahanix	AXIOMTEK	CoolerMax	In Focus Systems	Nikao	Star	XG
AIC	AXION	CoolMaster	Intel	nMediaPC	Stardom	XION
AiSI	BeanTech	Coolmax	Inwin	Norco Technologies Inc.	Startech.com	Yang Ming-Rackmountpro
Altec Lansing	Beyond Micro	CPU Solutions	IOGEAR	NZXT	Storage Country	Yeong Yang
American Power Conversion	BeyondMicro	Dell	i-Rocks	Overland	Storcase	Zalman
AMS	Biostar	Directron	I-Star Computer Co. Ltd	Palo Alto	Sunbeam	
ANGEL EYE	Broadway Com	Duramicro	JPAC computer	PC Case	Suntech	
Antec	Broadway Com Corp	DynapowerUSA	Just PC	PC Power and Cooling	Super Case	
Aopen	Bytecc	Echo Star	Kingston Technology	Penguin Gear	Super Flower	
Apacer	CABLES TO GO	eDigiByte	Kingwin	Platinum System	Super micro	
APC	Cabletron	Enermax	Koolance	Plumax	Super Talent	
Apex	Case Ace	Enhance Technology	Kroo	Power Magic	Supercase	
A-Power	CASE LOGIC	Enlight	LanReady	Powmax	Super-Flower	
Arctic Silver	Cabletron	EuroCom	LCT Technology	Proware	SuperMicro	
Argosy	Case Ace	Evercase	Lian-Li	PSI	Syba	
Broadway Com Corp	CASE LOGIC	Fong Kai USA	Linkword Technology	Raidmax	Tamrac	
Bytecc	CaseArts	Foxconn	Linkworld	Rainbow	Targus	
	Casedge	G-Alantic	Linkworld Electronics	Razor	ThermalRock	
	CASETRONIC	Galaxy	Lite-On	RealWorld	Thermaltake	
	Chenbro	Gateway 2000	Logisys	Rosewill	Tripp Lite	

Forensic



Computers

Cases/Enclosures



Forensic



Computers

Processors

- ☞ Two major manufacturers:
 - ☞ Intel
 - ☞ AMD
- ☞ Both manufacturer's make excellent processors.
- ☞ Do you want Single Core, Dual Core, Core 2 Duo, or Quad Core?
- ☞ AMD is toying with a triple Core.
- ☞ Choices range from the inexpensive older versions to the expensive bleeding edge.

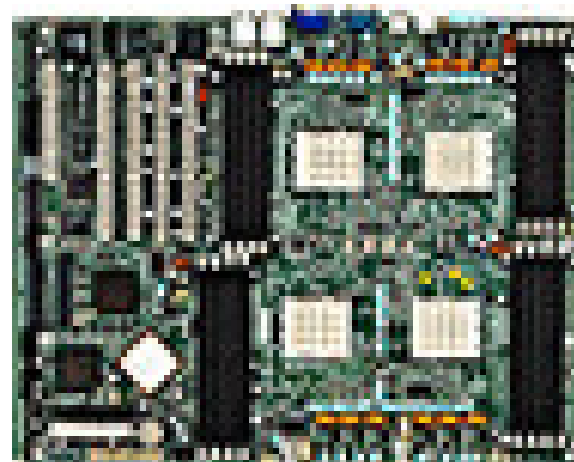
Forensic



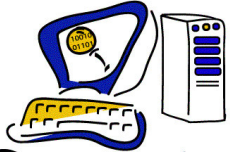
Computers

Motherboards

- ❏ Pricewatch.com lists 78 motherboard manufacturers.
- ❏ Prices range run from \$44.00 to well over \$2000.00
- ❏ Most boards could be used, however that does not mean they are all suited to forensic work.
- ❏ Consider the features on the board when deciding which board to purchase.
 - ❏ Does the board match your requirements for the case size, processor type, memory capacity, IDE buses, SATA/RAID, audio, NIC, USB, FireWire.....
- ❏ Consider staying with major board manufacturers like ASUS, Tyan, Gigabyte, Shuttle and even Intel.



Forensic



Computers

Power Supplies

- ❏ Not all power supplies will meet your needs.
- ❏ DO NOT go cheap here.
- ❏ Stay mainstream with companies like Antec, PC Power & Cooling, and Ultra.
- ❏ Make certain the Power Supply exceeds the minimum for the motherboard/processor combo you have selected.
- ❏ Consider large capacity units that are rated for 8 to ten hard drives.
- ❏ 550 watt to 1000 watt units will fits most forensic applications.
- ❏ Some cases/enclosures require multiple power supplies.

Forensic



Computers

Memory

- ❏ There are over 120 brands of RAM.
- ❏ The motherboard choice is going to drive the type of RAM you use.
- ❏ The amount of RAM you choose will in part be controlled by how much RAM the motherboard can hold and the intended Operating System.
- ❏ Consider 2GB of RAM the starting point for serious forensic work.
- ❏ The minimum amount of RAM should be no less than 1GB.
- ❏ Generally the more RAM the better systems perform.

Forensic



Computers

Hard Disk Drives

- ❏ Do you want your OS on a SCSI, IDE or SATA drive.
- ❏ SATA or Serial ATA drives are the current rage.
- ❏ SATA drives out perform IDE drives and they are generally larger and cheaper than SCSI drives.
- ❏ My preference is for the 74GB Raptor SATA drive for the OS.
- ❏ Typically your data drive sizes are governed by the size of the SUBJECT drives.
- ❏ When selecting the hard drives be aware the drives come with different warranties. Look for drives that are covered for 3 to 5 years.
- ❏ Cheaper drives may only be covered for 1 year.


Forensic





Computers






Purchasing Workstations

Commercially Purchased Systems – Selecting a vendor

 Commercial Companies like Dell, HP, IBM make good computers, but may have restrictions on customer repair and customization. Opening the case can void all warranties.

-  These companies do not design their systems with forensics in mind.
-  Has the company actually delivered forensic systems or are they just a website wonder?

 A company which specializes in forensic workstations should have:

-  The forensic experience to know what components are required, what the methodologies are and know how to use them.
-  A warranty policy that is “No Hassle” for the end user.
-  A policy that allows forensically qualified individuals to open the system. without voiding an warranty.
-  Test the systems to ensure they are forensically sound - not all computers are not created equal – test results must be repeatable.
-  The company should be responsive to customer needs and allow configuration changes based on customer specific needs.

Forensic



Computers

Workstations

- ☞ At the end of the day you want systems that will do the job.
- ☞ How fast the job gets done will in part depend on your budget.
- ☞ Is the system configured to accept the media routinely received in a investigation?
- ☞ Is the hardware easy to use?
- ☞ Do you need portable forensic systems?

Forensic



Computers

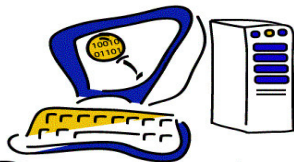
Portable Workstations

- ☞ Portables come in a verity of shapes and sizes.
- ☞ Some are built specifically for mobile forensics.
- ☞ Laptops can work well as long as you test before you buy or buy from a forensics company that has tested them.
- ☞ The portable solution you choose should give you the same basic capabilities as you lab systems.



Hardware Write Protection

Forensic



Computers

Forensic

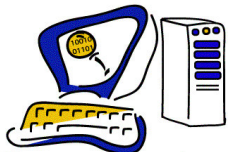


Computers

Hardware Write Protection

- ❏ Why use Hardware Write Protection?
- ❏ If you do not use Windows you may not need it, or do you?
- ❏ I say you do, you can never be too careful.
- ❏ Linux and Mac OS X can be configured so they do not automount hard drives and other media.
- ❏ Windows OS's will mount devices you attach.
- ❏ There are at least 5 companies manufacturing Hardware Write Protection devices or bridges.
- ❏ I prefer the Tableau products because of the quality and ease of use.

Forensic



Computers

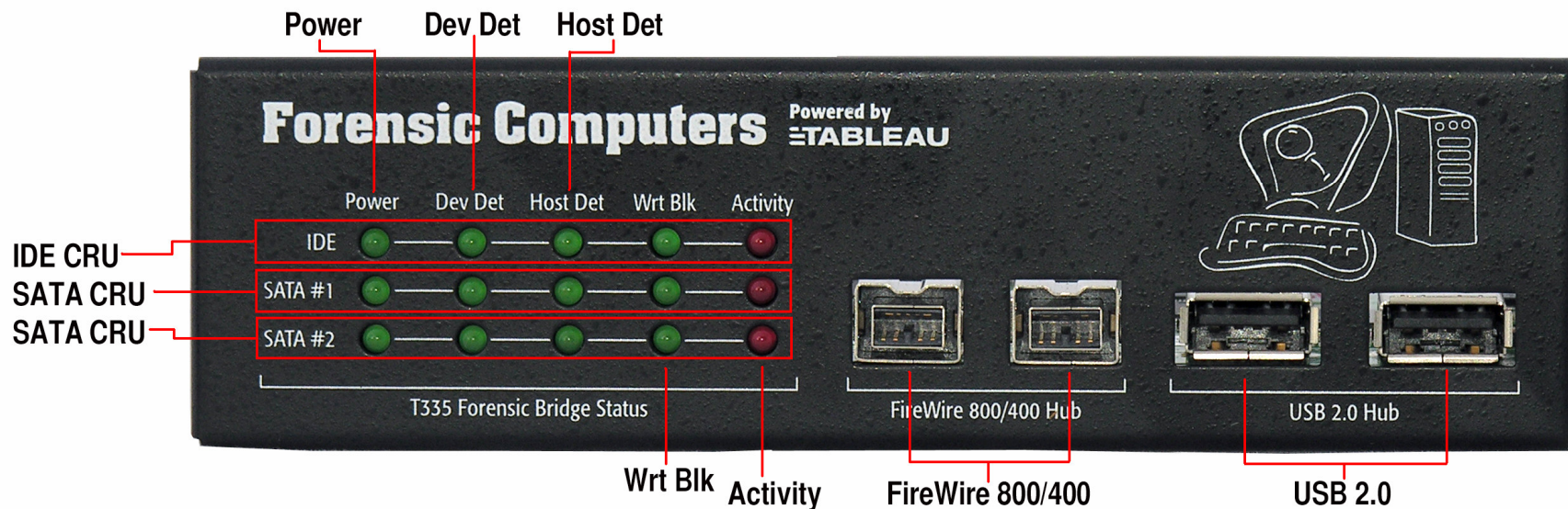
Hardware Write Protection

- ❏ There are bridges to write protect IDE, SATA, SCSI and USB devices.
- ❏ There are also bridges that will handle multiple types media.
- ❏ Tableau bridges as well as others have been tested by NIST and passed. The reports are published.
- ❏ There are 3 products by Tableau that are designed for installation in a 5.25" bay.
 - ❏ Tableau T35i (IDE and SATA)
 - ❏ Tableau T335 controls removable bays (IDE and SATA)
 - ❏ Tableau T345 (IDE, SATA, and SCSI – DI exclusive)



Hardware Write Protection

Tableau T335 Forensic Bay Controller



Forensic



Computers

Hardware Write Protection

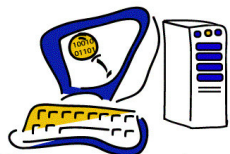
- ❏ Regardless which brand you choose you must run them through your own validation testing.
- ❏ A write blocker from one company (not Tableau) can be converted to READ WRITE if the user downloaded a firmware update and applied it. This could be bad for you case.....
- ❏ Just because a company makes write blockers does not mean everything they make is write protected.

IF IN DOUBT – ASK.....

Forensic Software & Training



Forensic



Forensic Software

Computers

- ❏ AccessData – Windows based Forensic Tool Kit and the Ultimate Tool Kit
<http://www.acesdata.com>
- ❏ ASRData – Linux based SMART
<http://www.asrdata.com>
- ❏ Blackbag Technologies – Mac OS X based Macintosh Forensic Suite and MacQuisition Boot disk
<http://www.blackbagtech.com>
- ❏ Guidance Software – Windows based EnCase
<http://www.encase.com>
- ❏ SubRosaSoft – Mac OS X, Linux and Windows based MacForensicsLab
<http://www.macforensicslab.com>
- ❏ Paraben – Windows based hard disk, PDA, and cell phone forensics software and hardware
<http://www.paraben.com>
- ❏ Technology Pathways – Windows based ProDiscover family of forensic and security software
<http://www.techpathways.com>

Forensic



Computers

Forensic Software

- ❏ There are other forensic packages out there that will the job and some of them are free or low cost:
 - ❏ Autopsy and Sleuth Kit (no cost)
 - ❏ Technology Pathways – ProDiscover Basic is free and they have a U3 version the runs from a USB Thumb Drive
 - ❏ WinHex – an excellent Hex editor also has a forensics package
 - ❏ Unix, Linux, and Mac OS X all have utilities included that work very well for forensics (dd, netcat, cryptcat, grep, strings, etc.)
 - ❏ There are also a number of “Live” or Bootable CDROMS that have been built by forensic investigators like Helix that are no cost.

Forensic



Computers

Forensics Training

- 🖱️ Get as much as you can.
- 🖱️ It is amazing how many people think one three day course on a software package makes them an expert.
- 🖱️ Also, get some hardware training like the A+ program.
 - 💻 Becoming A+ Certified is not a requirement, but it will not hurt.
 - 💻 A person conducting computer forensic exams should know what a jumper on an IDE drive is for and they should also know how to do simple things like format a hard drive.

Forensic



Computers

Reference Material

- 🖱 ***Techno Security's Guide to E-Discovery and Digital Forensics*** Lead Author Jack Wiles
🖱 ISBN 978-1-59749-223-2
- 🖱 ***How Computers Work*** by Ron White
🖱 ISBN 0-7897-2549-5
- 🖱 ***Upgrading and Repairing PCs*** (17th Edition) by Scott Mueller
🖱 ISBN 0-7897-2745-5
- 🖱 ***MAXIMUM PC Magazine***
🖱 A no nonsense publication.

Forensic



Computers

Tool Kits

☞ This is really a matter of individual preference

☞ For the Lab a good starting list is:

- ☞ High quality screwdriver set (small ones also) – I like Craftsman and Wiha
- ☞ Small Wire Cutters
- ☞ Small Needle Nose Pliers
- ☞ Assortment of Torx bits
- ☞ Assortment of Hex head bits
- ☞ Small flashlight
- ☞ Technicians Mirror (the kind you can adjust the mirror head)
- ☞ Hemostats (forceps - Radio Shack calls them as solder helpers)
- ☞ Static Wrist Strap
- ☞ Small Digital Multimeter
- ☞ Container of computer screws
- ☞ Spare Hard Disk Jumpers (large and small)
- ☞ Spare Cables (Floppy, IDE, SATA, SCSI)
- ☞ Assortment of Gender Changers
- ☞ Assortment of Molex Male and Female Cables
- ☞ Latex type gloves

Forensic



Computers

Last – But Not Least

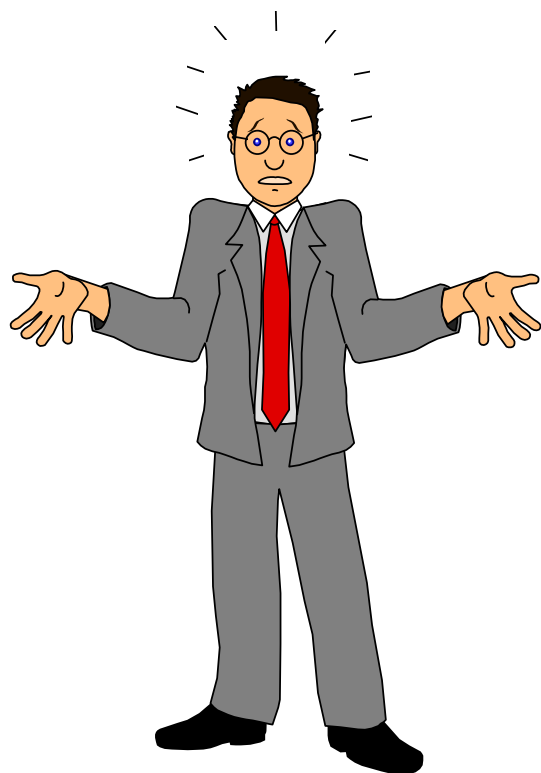
- ❏ Now you have it together, does it work?
- ❏ Is it forensically sound? Will it image and handle data without losing, dropping or changing data?
- ❏ Do the hashes match when known data is imaged?
- ❏ Your validation process should include the same procedures used in actual investigations.
- ❏ Verify your results with multiple programs and Operating Systems

Forensic



Computers

Questions and Comments



Forensic



Computers

Contact Information

**Greg Dominguez
Vice President
Forensic Computers**

**540-726-9530
greg@forensic-computers.com**