Executive Summary of key Digital Forensic Concepts

Presenter:
S. Robert Radus, CPA, CFE, PI
Our firm motto is:

Image Early

And

Analyze Later
Overview of this Presentation:

What you “Really” need to know about Digital Forensics.

Why use an Computer Forensic Expert.

Case Flow Management (Expert’s).

What is nice to know about Digital Forensics.
What you “Really” need to know about Digital Forensics

By S. Robert Radus, CPA, CFE, PI

ACTForensic.com, Inc.
California Licensed Private Investigators #25889
Email srr@ACTForensic.com
Call us @ 714 271 2865

02-17-2016
“Suspect Computer”

If the computer is **OFF**, leave it **OFF**.

If the computer is **ON**, leave it **ON**.

UNLESS you see the HDD light flashing. Then quickly pull the POWER PLUG.
If the computer is OFF: turning it back on can:

- Activate a dormant command: to wipe the HDD, send data out, or infect an entire network with malware.
- “Rummaging” around can
  - destroy data.
  - cause changes to dates and times.
  - Thus “destroying” the forensic value of any future investigation.
If the computer is ON:

disconnect it from the “outside world:” Mouse, Keyboard, Internet Cable

- The investigator can recover RAM which may contain valuable data and/or malicious programs which may have not been saved to the HDD yet.

- Once the RAM is recovered, the investigator can turn it off and make a “forensically sound” copy of the HDD.

- **ON or OFF, your investigator should NEVER examine the original HDD.**
Why use a Computer Forensic Expert.

By S. Robert Radus, CPA, CFE, PI
Using an Expert:

**ALWAYS prepare your expert.** Have your expert lay out the facts, describe their methods, support their findings, and give a clear opinion.

On the stand: Yes or No. “I cannot answer the question” is not an answer. On redirect go back over such replies and get a clear answer.

**ALWAYS prepare your expert.**

**Why?**
It is cost effective to have someone who has the training, expertise, and can testify. The opposition is going to review, duplicate your results. Then they will try to impeach them and your expert.

Or agree and move on.
The Expert's Report must:

Articulate the facts in a concise, plain English.

Lays out the facts, describes their methods, and supports their findings and opinions.

and NEVER embellish the facts.

Why? →
The consequences of not using Forensically Sound Procedures and a Well Written Report?

Having your testimony impeached in court.
Case Flow Management

By S. Robert Radus, CPA, CFE, PI
Pre-intake Documentation for computer cases:

- Where is the computer?
- Is the computer powered ON or OFF?
- Can the work be done off-site?
- Make, model, and Serial number of the computer.
- Size of HDD to be acquired.
- What is the project due date?
- What are the usernames and passwords?
Client Name: [Insert Client Name]
Address: [Insert Address]
City, State Zip: [Insert City, State, Zip]
Office Phone #: [Insert Office Phone Number]
Cell Phone #: [Insert Cell Phone Number]
Email: [Insert Email]

Re: [Insert Re:]

Make: [Insert Make]
Model: [Insert Model]
S/N: [Insert S/N]
BIOS: [Insert BIOS]
Date / / and Time:

Received From BY: Date/Time Received From

1. [Insert Instruction 1]
2. [Insert Instruction 2]
3. [Insert Instruction 3]
4. [Insert Instruction 4]

HDD Capture Instructions:
Investigator Initials: [Insert Initials]
Computer OFF or ON:
From your watch or cell phone: Date ________ and Time __________.

OFF:
1. Disconnect HDD Power and Data Cables.
2. Power Computer and enter SET UP for: BIOS Date ________ Time __________.

ON:
1. Take from Start Bar: Computer Date ________ Time ________
2. Insert USB FD, run these programs, save to Folder on FD:
   Helix: Run the RAM Capture program
   USBDview
   IHC
   Recent Docs
   Procedures do above: 1. exe for program. 2. Edit\SelectAll. 3. File\Save\save as .csv to folder. 4. Write report.
   Then Shut Down the computer Power off: Pull HDD, image, re-install, save image report.
Case enquiry comes into YOU

Contact ACTF so we can get the basic information and set a meeting with you and the client.

ACTF will meet with you and the client to discuss case: what they expect, what we can do, timing for delivery.

ACTF will prepare Engagement Letter, signed by all parties & RETAINER.
Work Flow:

Whether going to where computers are or taking HDD to our lab the flow is the same:

Original HDD

Protect with a "Write Block"

Field or Lab Acquisition Computer

Working Copy for use in forensic computer

Backup Copy

Output used for reports and exhibits

Secure Storage in case it is needed
Get your EXPERT in early:

Summary:
This is what we do and can Testify to. The longer you wait the less likely the Data can be recovered. (Overwritten or wipe out).
What is nice to know about Digital Forensics

By S. Robert Radus, CPA, CFE, PI

ACTForensic.com, Inc.
California Licensed Private Investigators #25889
Email srr@ACTForensic.com
Call us @ 714 271 2865
The three most important concepts in Computer Forensics:

- Write Block the Source Data.
- Hash the data.
- A well Written Report.
A Write Block Device:

Conceptually is a one-way road.

It allows data to flow from the source media through it to the target media.

Write Block Device is hardware or software which allows a computer to read the evidence media without altering the data thereon.
MD5 Hash

The Hash Algorithm Total is

An alpha numeric representation ("fingerprint") of consisting of 32 characters. It is the value of all of the bits in a file, folder, or total media.

An MD5 Hash is the 5th version of the Message Digest (alpha numeric representation). It is represented as 32 characters in 4 groups of 8.

Knowing this qualifies you to be a "GEEK"

MD5 Message-Digest Algorithm was designed in 1991.
Recap of Computer Forensics:

Knowing how the Operating System functions, writes, and stores data.

Having the proper hardware to secure the data.

Having the proper software to examine the data.

Having the experience and training to find the digital evidence AND be able to present those findings to your client and the Court.
Executive Summary of key Digital Forensic Concepts

The END

S. Robert Radus, CPA, CFE, PI

ACTForensic.com, Inc.
California Licensed Private Investigators #25889
Email srr@ACTForensic.com
Call us @ 714 271 2865