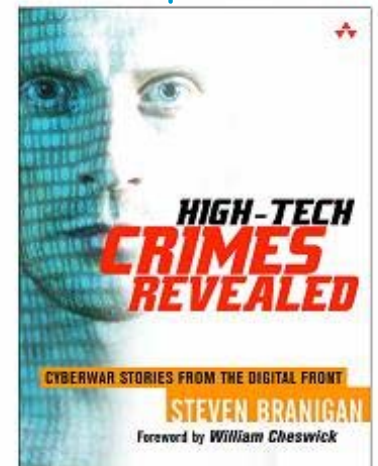


*High tech
investigations:
It ain't just
forensics...*

Steven Branigan, President

Excerpts from...



Cyan
Line

Overview

- My background...

Modules

- #1 Overview and basics. A *philosophy* for investigations.
- #2 Some tools and techniques to consider.
- #3 Evidence handling and metrics. (management)

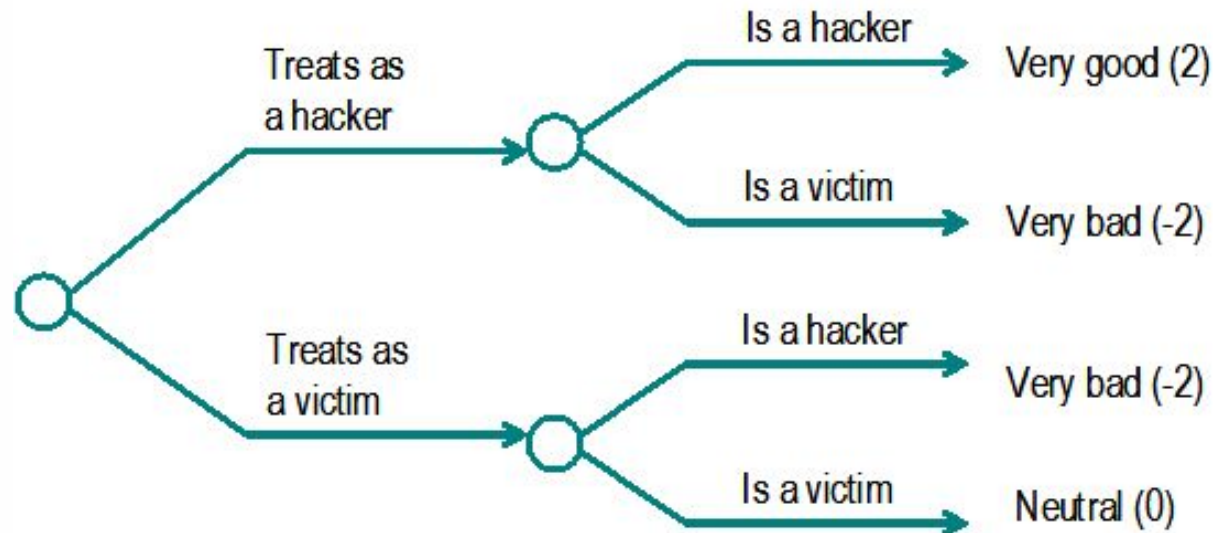
Module #1

- Overview and philosophy...

Principles:

- Innocent until proven guilty...
 - Ok to have suspects
 - Want to always be questioning whether you have the right suspect.
 - Beware of issues that might hinder you from seeing the whole truth.
- The psychology of investigations is very important.

Option matrix view



<http://www.cyanline.com>

Confirmation bias issue.

- An issue where people tend to ignore information that would disprove their theory.
- Example...

Cognitive dissonance

- Basically, it is our innate desire to justify a previous poor position.
- Example
 - When these results were announced, the head chiropractor turned to me and said, "You see, that is why we never do double-blind testing anymore. It never works!" At first I thought he was joking. It turned out he was quite serious. Since he "knew" that applied kinesiology works, and the best scientific method shows that it does not work, then -- in his mind -- there must be something wrong with the scientific method. (Hyman 1999)

The investigative cycle

- Discovery
 - Report
 - Witness
- Investigate
- Determination
- Prosecution

How do they start?

- Third party reports.
 - From an unsolicited report to the police
 - Through automated detection
- First hand reports
 - Police witnessing a crime
 - As a result of evidence uncovered in an investigation

The investigation

- Evidence collection process
- Maintain records!

When is it enough?

- Investigations lead to decisions.
 - Arrest/prosecute
 - Discipline/fire
 - Nothing

Investigative effort?

- Usually needs to match the crime.
 - A stolen floppy probably isn't worth much effort.
 - Unless it contains very valuable data.
 - However, big cases have been discovered with a small investigation.

Some rules..

- #1: Know what you are investigating. Don't be afraid to reach out for help when you are unsure about something.
- #2: Be calm and patient at all times. Rushing causes mistakes and time is usually on your side.
- #3: Don't jump to conclusions and then look for facts. Let the facts of the case tell you everything. Don't ignore the facts, even when they appear to go against your hunches.

More rules...

- #4: Miscommunication can adversely affect a case. Over-communicate with trusted team members, and under-communicate with those that really do not have a need to know.
- #5: Pay careful attention to the issues with high tech evidence, both its collection and storage.
- #6: Whenever possible, share new high tech criminal techniques that you have uncovered. Allow others to benefit from your discoveries to improve security for all of us.

Common mistakes

- **Mistake #1.** Do not make any investigative moves without the permission of the lead investigator, even if you are the boss. Your actions, even with the best of intentions, might set an investigation back.

Mistake #2

- Do not start any field forensic investigation unless you have a well thought-out plan and you record your steps. This move might tip off the suspect and, unless you record everything that you typed, you might destroy the value of any evidence collected.

Mistake #3

- **Mistake #3.** Don't scan a suspect's system with a computer labeled with a corporate security's name.

Mistake #4

- Do not act based upon old technical knowledge. High technology is a fast changing field.

Mistake #5

- Pressure usually adversely affects decisions. It is also best to have a plan for addressing contingencies in advance.

Bad Luck...

- Some examples....

Module #2

- Tools and techniques
 - Acquiring data forensically
 - Data analysis
 - Data reporting

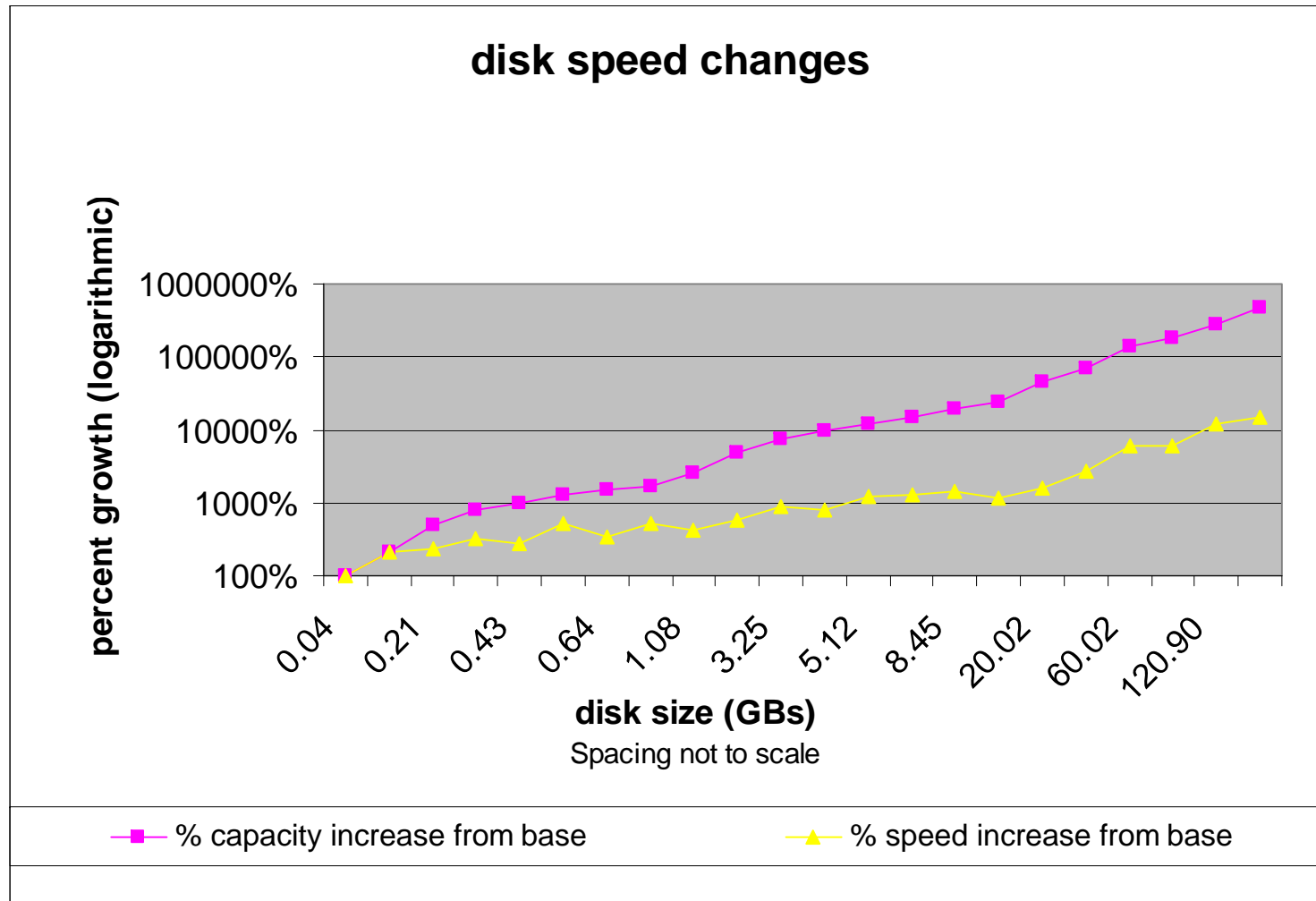
Forensic work

- 3 components
 - Data acquisition
 - Data analysis
 - Reporting/certification/testimony

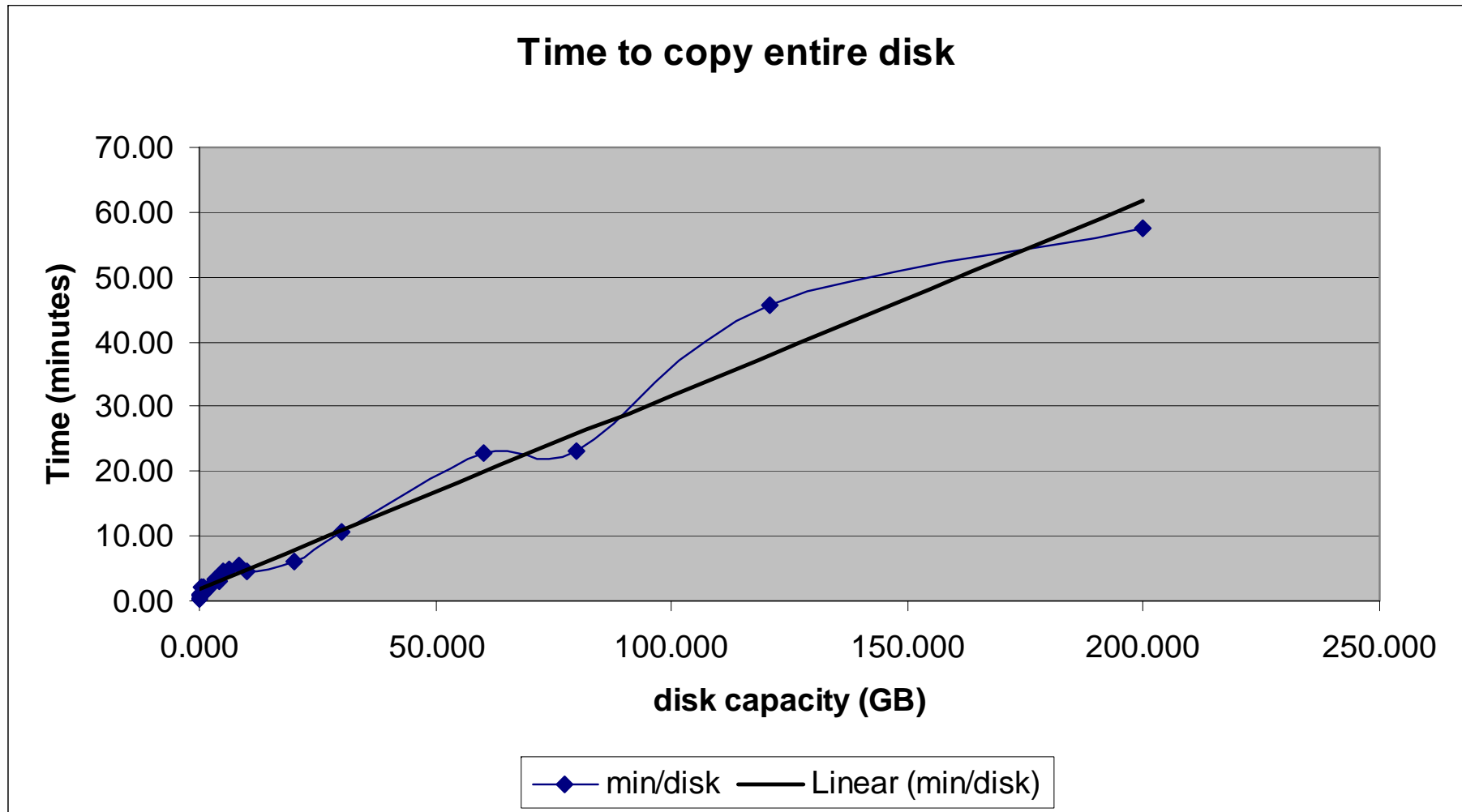
Hard drive

- Image single drives
- Imaging RAID drives

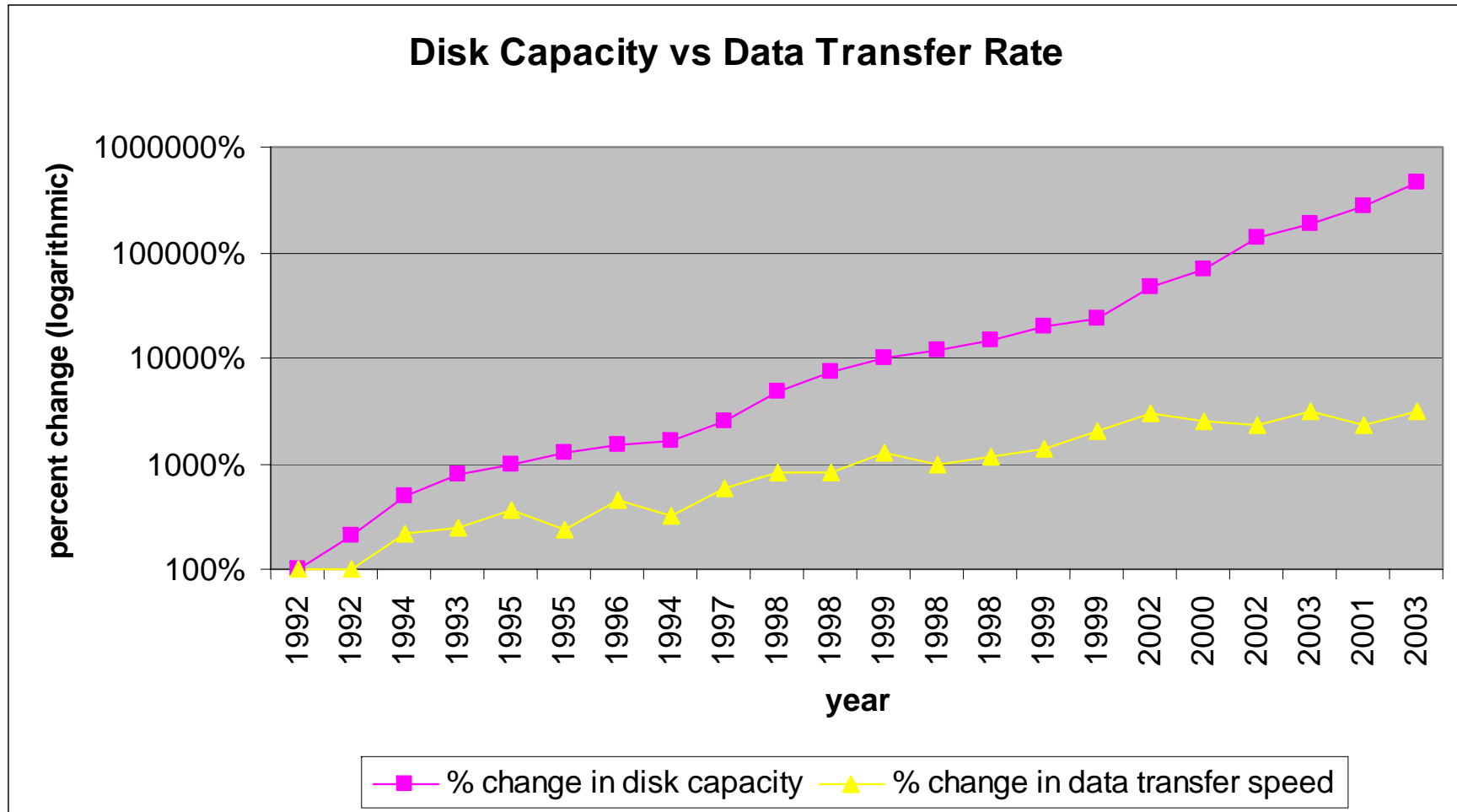
Trends: disk speed vs. size



Trends: time to copy entire disk



Trends: disk capacity vs. transfer rates



<http://www.cyanline.com>

Tools worthy of consideration

- Dcfldd (version 2.0)
 - Dd images a disk drive
 - This version is improved to hash the source media and report it in chunks.
- Loopback mounting
- Sleuthkit/autopsy
 - A reasonable analysis engine for examining images
- Knoppix/Helix
 - Great tools for examining a system.

Common practice

- Notes
- Photos

More information..

- www.cyanline.com/forensic
- Forensic tools
 - www.forensics.nl
- Victim Assistance Online
 - http://www.vaonline.org/internet_gen.html

Analysis

- Now that we have the data, what does it mean?
 - Usually, the toughest part of an investigation...
- Best to examine a couple of examples...

Email

- Focus of many investigations these days.
 - Contents of email messages.
 - 3rd parties reading email messages.

System tapped?

- A very common concern for people these days...
- Suggestions to attack this issue.

Open issues

- Imaging/analyzing databases?
 - Sql?
- Imaging running systems?
- Selected acquisitions of filesystems?
- Imaging phones/PDAs/digital cameras...
- How long to hold evidence? And what should be done with it once case is “over”.

Module #3

- Case management

Evidence handling

- There are only two ways to handle it
 - The right way...
 - All other ways...

Chain of custody

- In the electronic world, we usually take a copy of evidence.
- For this copy to be acceptable as a true copy, it must be well maintained.
 - Preferable, the evidence is never altered.
 - However, if it is, it must be NOTED!
- It is important to track the people that come in contact with the copy or copies.

Metrics?

- Manage by metrics.
 - But finding good metrics is difficult
- If you can measure it, hopefully you can manage it...

Investigator metrics

- Number of cases opened.
- Successful acquisitions?
- Successful analysis?
- Successful report?
- Types of cases.
- Client satisfaction with result.

Team metrics

- Client satisfaction with team.
- Comparison of individuals to group average.
- Look for lowest metrics, analyze why?
 - For example, acquisitions failing a lot.
Perhaps the technique needs to change.