

**CSI NetSec<sup>07</sup>**

June 11-13, 2007  
Scottsdale, AZ  
The Phoenician

# Up in Smoke ... Live Forensics, Here and Now

farmerdude

This document is protected by applicable copyright laws. You may not show, adapt, translate, or distribute this document or any part thereof without prior express written consent of the copyright holder. Copyright © 2007 farmerdude

[www.onlineforensictraining.com](http://www.onlineforensictraining.com)

[www.forensicbootcd.com](http://www.forensicbootcd.com)

- ◆ Ages 21+ only
- ◆ No photographs
- ◆ No audio/video recording
- ◆ Please MUTE cellular telephones, pagers, crackberries, whoopee cushions, etc.
- ◆ Heckling is very welcome ... cash, too ...

# Have YOU selected the right lecture?

“Every sixty seconds, thirty acres of rain forest are destroyed in order to raise beef for fast-food restaurants that sell it to people, giving them strokes and heart attacks, which raise medical costs and insurance rates, providing insurance companies with more money to invest in large corporations that branch out further into the Third World so they can destroy more rain forests.”

George Carlin

<http://www.sierraclub.org>

This document is protected by applicable copyright laws. You may not show, adapt, translate, or distribute this document or any part thereof without prior express written consent of the copyright holder. Copyright © 2007 farmerdude

- ◆ What's the point?
- ◆ Open Discussion
- ◆ Review, Questions and Answers (if you're lucky)

# There is **STILL** time to make another lecture!

NOTE: There was a graphic here. Those in attendance were able to view said graphic. Everyone else must wonder what this graphic was . . . And it was a good graphic!

This is what happens when you're a dork ... and when there's only **ONE Mt.** Dew left in the cooler ...

This document is protected by applicable copyright laws. You may not show, adapt, translate, or distribute this document or any part thereof without prior express written consent of the copyright holder. Copyright © 2007 farmerdude

- ◆ Background
  - ◆ Security Consultant
  - ◆ Red Hat, Inc.
  - ◆ THE FARMER'S BOOT CD
  - ◆ Forensics training
  - ◆ Case work

# What's the Point?

- ◆ You are here today because . . .
  - ◆ You have an interest in data forensics and/or incident response
  - ◆ You realize that there may be critical information available only while the computer system is up and running
  - ◆ Let's be honest ... you need a nap before the big golf outing
  - ◆ You are a glutton for punishment

# Open Discussion Overview

- ◆ Postmortem versus Live Analysis
- ◆ Live Analysis Requirements
- ◆ Live Analysis Targets
- ◆ Moving forward in 2007 and Beyond

This document is protected by applicable copyright laws. You may not show, adapt, translate, or distribute this document or any part thereof without prior express written consent of the copyright holder. Copyright © 2007 farmerdude

## ◆ Postmortem Analysis Benefits

- ◆ **Non-invasive** = The data is preserved in a read-only state, guaranteeing authenticity
- ◆ **Reproducible** = A static environment lends itself to reproducible results
- ◆ **Time** = A known time factor can lessen the potential for mistakes as well as provide focus
- ◆ **Minimal Mistakes** = Less mistakes are likely when you have a set amount of time and can work through a proven protocol
- ◆ **Correlation** = Given the capability to review other sources of information, you can typically correlate findings
- ◆ **Validation** = Validate your findings with a colleague

This document is protected by applicable copyright laws. You may not show, adapt, translate, or distribute this document or any part thereof without prior express written consent of the copyright holder. Copyright © 2007 farmerdude

- ◆ **Postmortem Analysis Limitations**
- ◆ **Missed system state** = What was the scene when you came upon it?
- ◆ **Missed network connections** = Who's on what port?
- ◆ **Missed process information** = Process state, process memory, process table
- ◆ **Missed memory** = Contents of RAM and caches
- ◆ **Missed file systems** = Specifically RAM file systems, but also network file systems
- ◆ **Missed users and user activity** = Who's logged in, doing what?
- ◆ **Where is the data** = off-loaded log files, wiping, encryption

This document is protected by applicable copyright laws. You may not show, adapt, translate, or distribute this document or any part thereof without prior express written consent of the copyright holder. Copyright © 2007 farmerdude

## ◆ Live Analysis Benefits

- ◆ Obtain RAM file systems
- ◆ Obtain contents of memory
- ◆ Obtain process information
- ◆ Obtain users and user activity
- ◆ Obtain network information
- ◆ Identify potential postmortem analysis limitations

## ◆ Live Analysis Limitations

- ◆ **Invasive** = What you do will impact the system, users, and/or applications/processes
- ◆ **Not trivial** = Dynamic and unique environments
- ◆ **Unknown time factor** = What's happening now, what's coming
- ◆ **More likely to make mistakes** = It's live – 'nuff said
- ◆ **Typically unable to correlate data** = Geographically and/or physically isolated
- ◆ **Often unable to validate** = Who is with you, for and against?

## ◆ Live Analysis Considerations

### ◆ Order of System Volatility

- Constant change
- What is your target?
- Act now before it's too late

### ◆ Legal challenges

- You're breaking the holy byte of data forensics
- Can you articulate A) What you did B) How you did it C) Why you did it D) What effect your actions had

### ◆ Technical

- Where to write the data
- Trusted Media Toolkit (TMT)

- ◆ **Live Analysis Requirements**
  - ◆ **Deep understanding and knowledge**
  - ◆ **Tools**
  - ◆ **Flexible protocol**
  - ◆ **Experience**

1. Turn off lights.
2. Turn off other electric things, like TVs, stereos, and radios when not in use.
3. Use rechargeable batteries.
4. Do things manually instead of electrically, like open cans by hand.
5. Use fans instead of air conditioners.
6. In winter, wear a sweater instead of turning up your thermostat.
7. Insulate your home so you won't be cold in winter.
8. Use less hot water.
9. Whenever possible, use a bus or subway, or ride your bike or walk.
10. Try to buy organic fruits and vegetables if you're concerned about pesticides. (Organic food is grown without man-made fertilizers and/or pesticides).
11. Don't waste products made from forest materials.
12. Use recycled paper and/or recycle it. Reuse old papers.
13. Don't buy products that may have been made at the expense of the rainforest.
14. Support products that are harvested from the rainforest but have not cut down trees to get it.
15. Plant trees, especially if you have cut one down.
16. Get other people to help you in your cause. Make and/or join an organization.
17. Avoid products that are used once, then thrown away.
18. Buy products with little or no packaging.
19. Encourage your grocery store sell environmentally friendly cloth bags for people to use when they shop, or bring your own.
20. REDUCE, REUSE, & RECYCLE.
21. Compost.
22. Buy recycled products.
23. Don't buy pets taken from the wild.
24. Cut up your six-pack rings before throwing them out.

This document is protected by applicable copyright laws. You may not show, adapt, translate, or distribute this document or any part thereof without prior express written consent of the copyright holder. Copyright © 2007 farmerdude

## ◆ Live Analysis Targets

- ◆ Memory

- ◆ Network

- ◆ Users

- ◆ Processes

- ◆ File systems

- ◆ Postmortem limitations

## ◆ Memory

- ◆ **Memory Mapped** = programs, device drivers, etc.
- ◆ **Cached** = passwords, clipboard contents, URLs, etc.
- ◆ **Process virtual memory**
- ◆ **Requires privilege to access memory**
- ◆ **Software dump** – Trusted Media Toolkit, such as FAU or memdump. Can be thwarted more easily because you rely on the operating system kernel (malicious) and it uses memory.
- ◆ **Hardware dump** – Direct memory access (DMA) or firewire/1394. The preferred method.

## ◆ Memory

- ◆ Ideal is to dump memory one page at a time if software tool is used
- ◆ /dev/mem represents physical address space on Linux system
- ◆ /dev/kmem represents virtual address space on Linux system
- ◆ \Device\PhysicalMemory for Win32

## ◆ Processes

- ◆ list
- ◆ state
- ◆ memory maps
- ◆ suspect processes = unknown, known bad, encryption, etc.

## ◆ File systems

- ◆ RAM
- ◆ hidden
- ◆ remote

- ◆ **Postmortem Limitations**
  - ◆ Wiping
  - ◆ Encryption

## ◆ Moving forward ... Tools

- ◆ Memparser for Win32:
  - process enumeration
  - dump process memory and strings
  - copies process environment information
  - lists DLLs loaded by each process
- ◆ KnTTools and KnTList for Win32:
  - dump physical memory
  - now commercial
- ◆ memfetch
- ◆ pcat, pmodump
- ◆ memdump


FORENSICBOOTCD.COM - Firefox

File Edit View History Bookmarks Tools Help

http://www.forensicbootcd.com/

contact | privacy

# forensicbootcd.com



- Home
- THE FARMER'S BOOT CD
- Screen Shots
- Comparison
- Online Store
- Calendar
- Support
- Services
- Training

Welcome to **forensicbootcd.com** - home of the ultimate Data Forensics preview boot CD.

## THE FARMER'S BOOT CD

(FBCD)

Because not all Linux bootable CDs are created equal, this is a valuable resource.

Done


Data Forensics Training - Firefox

File Edit View History Bookmarks Tools Help

http://www.onlineforensicttraining.com/

## online forensic training

home | courses | registration | forum | about



### data forensics training

Online Forensics Training is the premier provider of professional data forensics training in the unique distance learning format. Distance learning format allows you to learn wherever you are without requiring Internet access or a computer.

No Internet access? Power out? Computer being repaired? Whatever the scenario, our unique delivery allows you to learn at your pace, whenever and wherever. All that you need to learn are the course materials. Each educational course has an almanac that is written in a very verbose manner, providing you with the necessary information

### news

[Certified Computer Examiner](#)  
The CCE is emerging as the computer data forensics certification to obtain.

[THE FARMER'S BOOT CD](#)  
FBCD is the first bootable Linux CD

Done

farmerdude@crazytrain.com

This document is protected by applicable copyright law without prior express written consent of the copyright holder.

www.onlineforensict