

SANS WhatWorks in Forensics and  
Incident Response Summit 2008

Las Vegas, NV - October 10 - 20, 2008

# User Panel: Forensics & Incident Response It's important to have options!

Lance Mueller

CISSP, GCIH, GREM, EnCE, CCE, CFCE

[lance@bitsecforensics.com](mailto:lance@bitsecforensics.com)

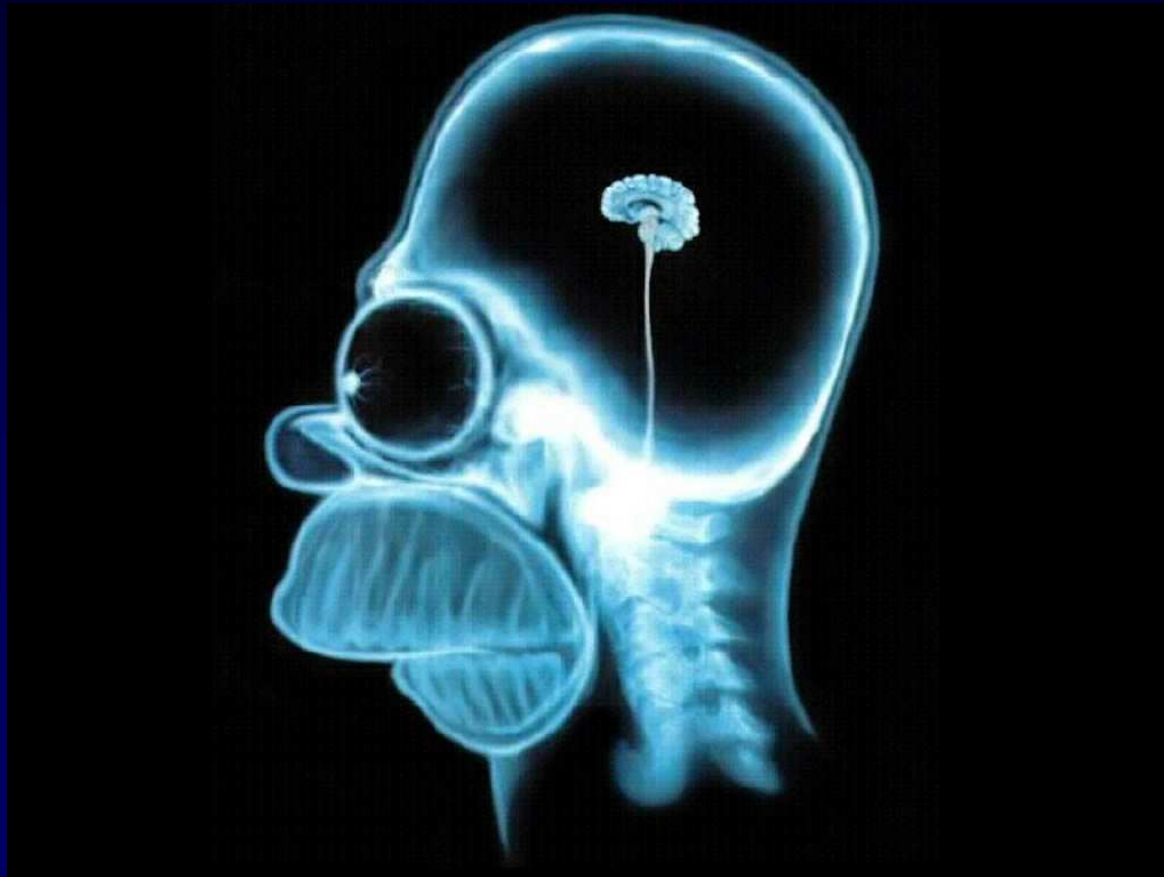


# SANS Forensic & Incident Response Summit

- Goals:
  - Discuss some important Incident Response & Forensic fundamentals
  - Highlight some methods, tools and equipment to assist

\*\*I have no special association with any vendors, the following views are strictly my own based on my experience of what has worked for me.

What's the most valuable Incident Response tool you own?



## SANS Forensic & Incident Response Summit

- You already own the most valuable tool you could ever use in Incident Response.
- The key is to harness it and think quickly
  - Medical industry uses the term “golden hour”
  - Law Enforcement uses a “24 hour” rule.

## SANS Forensic & Incident Response Summit

- The ability to connect the dots is a required skill in this field.
  - Difference between examiner and investigator/incident handler
- Industry tools are there to make your life easier, but the ability to “problem-solve” is invaluable.

## SANS Forensic & Incident Response Summit

- As the computing landscape changes, Incident Response techniques and tools are required to evolve and change.
- Operating System types, memory size, hard disk capacity and encryption are all examples of things that can effect our methods or processes.

## SANS Forensic & Incident Response Summit

- Incident handlers should prepare for the worst and have the ability to adapt to changes.
- Ability to “improvise, adapt & overcome”
- Having the necessary tools is paramount. We tend to stick with tools we know and are comfortable with.

# SANS Forensic & Incident Response Summit

- Corporate vs. Consultant environments
- Incident Response vs. Forensic environments

# SANS Forensic & Incident Response Summit

- What do you have in your toolkit?
- Are you prepared to deal with this?



# SANS Forensic & Incident Response Summit

- How about this?



# SANS Forensic & Incident Response Summit

- And this?



## SANS Forensic & Incident Response Summit

- Having a good toolkit can take some of the pain away.



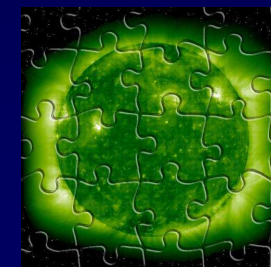
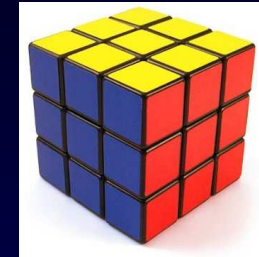
- SANS has excellent whitepapers on toolkit contents as an excellent starting point.

# SANS Forensic & Incident Response Summit

- Incident Response has several defined stages:
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned

# SANS Forensic & Incident Response Summit

- Typical process/methodology:
  - Triage involved machine(s)
  - Find identifying characteristics that can help direction
  - On enterprise, use those identifying characteristics to help identify additional compromised hosts.
  - Establish timelines and ingress direction



# SANS Forensic & Incident Response Summit

- The Forensic process can be broken down even further:
  - Preservation (identify it)
  - Collection (image it)
  - Analysis (process it)
  - Reporting (report it)

# SANS Forensic & Incident Response Summit

- Current trends in host-based forensics involve the collection of two main components:
  - Memory contents & Volatile data
  - Disk contents
- Remember order of volatility!

# SANS Forensic & Incident Response Summit

- Current Trends:
  - Memory collection is becoming more common for the masses.
  - Memory analysis is evolving at a fast pace and can seriously jump-start an investigation, or be the \*only\* way to get a big picture of what's going on.

# SANS Forensic & Incident Response Summit

- Several new tools have recently evolved to facilitate the collection of memory on current versions of Windows OS.
  - dd (may not work on all versions of OS)
  - mdd (Mantech)
  - Winen (EnCase)
  - KntTools (Garner)
  - Win32dd (Matthieu Suiche)
  - FastDump (HBGary)
  - F-Response (Agile, v2, creates possibility to use any imaging tool)

## SANS Forensic & Incident Response Summit

- Development of memory analysis tools like “Volatility” and “Voltage” allow the handler to parse captured image files or live, real-time memory.
- At a minimum, at least a collection allows a later analysis as tools evolve and skills increase.

## SANS Forensic & Incident Response Summit

- Collection of memory on a single machine is easy, how do you collect memory on remote machines?
- How do you collect memory on 5 or 20 or 100 machines in an enterprise quickly?

# SANS Forensic & Incident Response Summit

- Collection of other volatile data:
  - Helix
  - WFT
  - Coffee
  - Home-brewed
- Does not preserve original data for later analysis, just provides the results at that time.
- Trust issues with OS?

# SANS Forensic & Incident Response Summit

Image hard drive while live or dead?

- Production servers
- Encryption
- RAID Arrays
- OS Trust issues?
- Physical vs. Logical image?

# SANS Forensic & Incident Response Summit

- Hardware write blockers
  - All created equal?
    - Speed
    - Connectors
    - 1 to 1
    - 2 to 2
    - Image file vs. drive clone

# SANS Forensic & Incident Response Summit

- Drive Imaging tools:
  - dd (and various spin-offs)
  - FTK Imager
  - EnCase
  - SMART
  - Ghost

## SANS Forensic & Incident Response Summit

- How do you image machines remotely?
- How do you image 5 or 20 or 100 machines in an enterprise quickly (relatively speaking)?

## SANS Forensic & Incident Response Summit

- One of the most recent tools to be released is an amazingly small & simple solution to extend your current toolkit.
- The F-Response tool by Agile enables the Incident Handler/Investigator to use all the customary tools their familiar with, but enables them to be used over the network.

## SANS Forensic & Incident Response Summit

- By using the F-Secure Tool, you can “see” the remote memory and attached disk(s) as if they were connected to your local forensic machine.
- This enables you to use your traditional tools to image, view and analyze the remote disk(s).

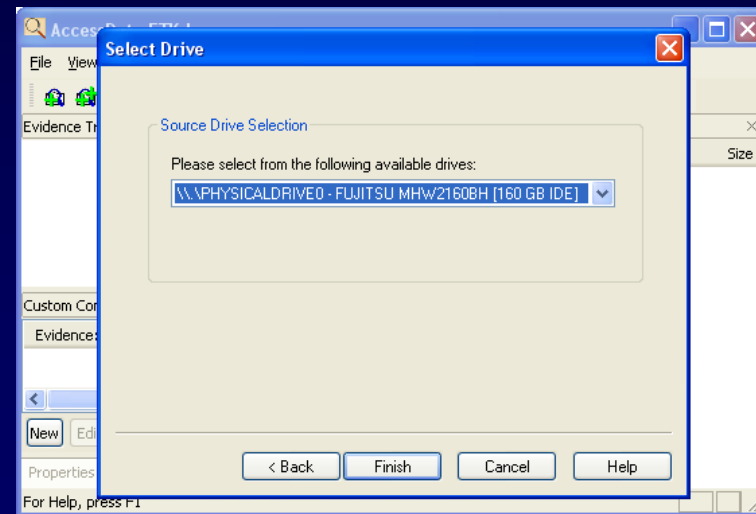
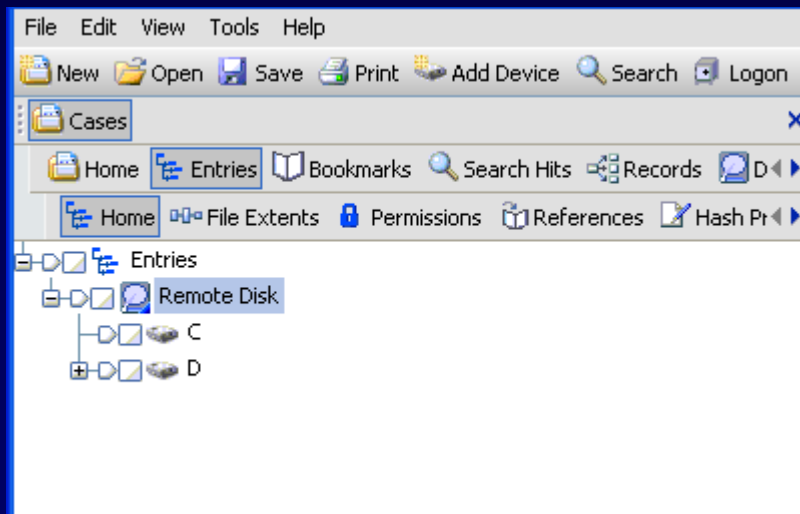
# SANS Forensic & Incident Response Summit

- Remote disk(s) now shows up on local forensic machine as a “locally” attached device.



# SANS Forensic & Incident Response Summit

- Use your favorite forensic tool to acquire, view and analyze:



# SANS Forensic & Incident Response Summit

- Well-known enterprise-class IR tools
  - Pro Discover (Technology Pathways)
  - EnCase Enterprise (Guidance)
  - MIR (Mandiant)
  - Access Data Enterprise (Access Data)

## SANS Forensic & Incident Response Summit

- Additional tools to help your analysis other than the obvious who, what, where questions:
  - Baselines or gold builds
  - Positive & negative hash sets
  - Packing detection/malware analysis
  - Antivirus (low-hanging fruit)
  - Network logs (device logs, netflow)

# Questions



Lance Mueller

[lance@bitsecforensics.com](mailto:lance@bitsecforensics.com)

<http://www.forensickb.com>