



**CJS 528**

**Module 12: Spring 2009**

# WRAP UP

## ○ Final Exams

- CIS 420 – 14 – May – 2009
- CJS 528 – 20 – May – 2009
- Exam is on Blackboard.
- There is a quiz on blackboard to ensure you have the ability to take the test. The quiz is **REQUIRED**. Please take the quiz **ASAP**.
- All cases must be submitted by May 20.
- Fisher is now available.



## ISSUES WITH FISHER

- Large File to download. (2 2Gb files).
- Just load the E01 file and the other will load with it.
- Requires dongle
  - Use Codemeter Files from [accessdata.com](http://accessdata.com)
  - Install codemeter file
  - Install KFF if you haven't done so
  - Then attach the dongle.
  - You may need to install license manager and refresh the dongle (under licenses tab).



# OVERVIEW OF AN EMAIL CASE

- Civil, corporate cases often have email components to them.
- Email comes in many forms
  - Local
  - Web Based
  - Server Side (Like Exchange)



# TACTICS

- Acquire both parties machines
- Examine the machines
  - If there is email installed
    - See if the emails are available
    - Else
      - Export the emails using a migration tool
      - Import the emails into a working machine and examine
  - Else
    - Examine the internet cache
    - Examine saved or deleted files
    - Examine swap files



## EMAIL TOOLS

- Mozbackup – will generate a file of all thunderbird email files for easy review.
- c:/Documents and Settings/<user>/Application Data/Thunderbird/Profiles/something.default/Mail/Local Folders
- Mbox files.
  - Search for these
  - They can be opened in another copy of thunderbird



# DEMO

- Looking at Davis again.



# SANS.ORG

- If you have funding consider
- SANS.ORG SEC 408 and SEC 508
  - Very intense courses but very good ones.
  - Preps for the GCFA certification
  - GCFA is a more infosec oriented cert than CCE.
- SANS Reading Room and Free Tools
- New Techniques to Keep in Mind
  - Live Memory Analysis
  - Use of Autopsy and Sleuthkit tools
  - Hyberfil.sys and shadow volumes



# LIVE MEMORY ANALYSIS

- This is a technique used to capture the contents of RAM while the machine is still running.
- Based on Rob Lee's presentation we have revised our protocol to always at least try this on operating machines we are seizing.
- Consider that RAM may be 4GB or greater and contains artifacts of cache and activity. This is a huge repository of information to lose.
- RAM may also contain encryption keys, passwords, and other information which will be lost and possibly unrecoverable.



## HOW TO DO THIS

- Live machines – you need to acquire a raw memory image
- There are problems with 64 bit machines
- Use
  - Win32dd.exe ([win32dd.msuiiche.net](http://win32dd.msuiiche.net))
  - Mdd.exe ([www.mantech.com/msma/mdd.asp](http://www.mantech.com/msma/mdd.asp))
  - Memoryze ([www.mandiant.com/software/memoryze.htm](http://www.mandiant.com/software/memoryze.htm))
- These tools basically acquire an image of RAM



# TOOLS TO ANALYZE MEMORY

- Memparser (by Chris Betz)
- Memoryze
- Volatility ([www.volatilesystems.com](http://www.volatilesystems.com))



# POLICY CHANGE

## ○ Old Policy

- Upon arrival
  - Determine machine is on or off
    - If Off:
      - Videotape scene including serial numbers
      - Photograph artifacts of interest
      - Photograph all setup and cables
    - If On
      - Assess Risk of off site attacks or damage
      - If off site risk seems high
        - Photograph Screen
        - Airgap networking
      - Then
        - Check drives for Media and remove
        - Videotape monitor screen



# POLICY CHANGE CONTINUED

- Old Policy
  - Else
    - Videotape Monitor Screen
    - Capture any screennames, usernames, or other activity
    - Examine any live screen artifacts (e.g. email) in plain sight
    - Validate RTC
    - Document time
    - Pull Plug



# POLICY CHANGE

- Revision
  - Else
    - ...
    - Validate RTC
    - Document Time
    - Insert cd with win32dd.exe
    - Insert 8gb or > USB Key
    - Capture memory to file
      - 2009ddmm-####M.img
    - Safely remove USB
    - Remove CD
    - Document Time
    - Pull Plug



# HIBERFIL.SYS

- One a dead machine you can look for this file
  - C:\hiberfil.sys
- This is the full memory of the machine saved in a disk file.
- Volatility will convert this file to a .dd type image
  - Find the registry hives System and SAM for each user
  - Dump the password hashes from S and S
  - Crack these password hashes with ophcrack or other rainbow tables cracks. (<http://bit.ly/WZDTg>)



# SHADOW VOLUMES

- Vista stores shadow volumes.
- These can be used to restore the system to earlier times.
- You may be able to do full analysis/imaging workups on each of these shadow volumes. (hope you're getting paid by the hour.)

