



**CJS 542/CIS 420**  
Module 11: Spring 2009

# GETTING A CASE

- Document the receipt and start a COC
- Enter this in your log
  - Received from Officer Molo
    - (1) Samsung WN321620A
      - SN == J4CH767081
      - Also labeled
        - 0040SAH7009147
  - Assigned case 20090005 – item 0001 (after as 5-1)
  - Gave receipt to O. Molo
  - Photograph Drive



## DETAILS

- Officer Molo tells you that there is no information about the drive just that it was found and is “of interest”. He tells you to examine it and see if anything stands out.



## TABLEAU CONNECTS

- Tableau write block was tested by writing to a sterile drive.
- Image created date and time.
- Second image created date and time
- All hashes checked
- Drive 5-1 returned to Officer Molo for evidence storage and receipt was obtained (receipt 20090035)



# IMAGES

- Image marked 2009-0005-0001a was burned to DVD, verified, and secured.
- Image marked 2009-0005-0001b was burned to DVD, verified, and used to begin examination.
- 84fd00392fa54388593d88325fdcf895
  - Hashed and matched.



# LOAD IN FTK

- Walk the tree
  - Note Volume has No Name
  - Volume is NTFS
  - Pretty quickly we see this is a data drive and not a system drive.
    - Pagefile.sys is the swap file (not here).
  - Looks like XP
  - We can identify the likely owner, emails, some photos and lots of web cache items.



## USING DAVIS 4G

- Another drive
- Volume Name Davis
- FAT-32 – common format for Win 98 and older hds.
- Win283.swp is on the main partition so this is a system drive.



# DATA CARVING SWAP FILES

- There is no telling what is in the swap file (if anything).
- Export the pieces of the swap file to a folder on your drive
- Use Simple Carver or some tool to carve the swap file and see what you find.
- This is the virtual memory of the machine so it's hard to say what will be here.



# QUICK OVERVIEW OF FULL VERSION OF FTK

- You need the codemeter drivers.
- You need a SILVER dongle to use with FTK for full.

