

**PURDUE**  
UNIVERSITY

CS526: Information Security  
Chris Clifton

December 4, 2003  
Forensics



## What is Computer Forensics?

- Understand what happened
  - Recovery
  - Prevention of future incidents
  - Sanctions / Law enforcement
- Often similar problems to Audit
  - But what if audit trail inadequate?*
  - Audit information incomplete/insufficient
  - Audit trail damaged
  - We don't own the computer



## What is the Challenge?

- Audit information incomplete/erased
  - Reconstruct deleted information
- “Acceptable” state of system unknown
  - Need to identify violation in spite of this
- Goal not obvious
  - Transformations may have been applied to data
- Strong burden of proof
  - Not enough to know what happened
  - Must be able to prove it (non-repudiation)

CS526, Fall 2003

3



## FBI List of Computer Forensic Services

- Content (what type of data)
- Comparison (against known data)
- Transaction (sequence)
- Extraction (of data)
- Deleted Data Files (recovery)
- Format Conversion
- Keyword Searching
- Password (decryption)
- Limited Source Code (analysis or compare)
- Storage Media (many types)

CS526, Fall 2003

4



## TCT – Tool Overview

- mactimes - report on times of files
- ils - list inode info (usually removed files)
- icat - copies files by inode number
- unrm - copies unallocated data blocks
- lazarus - create structure from unstructured data
- file - determine file type
- pcat - copy process memory
- grave-robber - captures forensic data

CS526, Fall 2003

5



## mactime

- mactime is shorthand reference to the three time attributes - mtime, atime, and ctime
  - atime - time of last access
  - mtime - time of last modification
  - ctime - time of last status change of inode
  - dtime - time of deletion (Linux only)
- Examples
  - # mactime -d /var/adm -y 1/1/1970
  - # mactime -R -d /var/log -y 1/1/1970
  - # mactime -R -d / -y 7/1/2001

CS526, Fall 2003

6



## mactime

- Examples

```
# mactime -d /var/adm -y 1/1/1970
# mactime -R -d /var/log -y 1/1/1970
# mactime -R -d / -y 7/1/2001
```



## ils

- ils lists inode information of removed files. Can be used to identify deleted files for possible attempt to undelete with icat. Specify a device file which contains a file system.
- Example

```
ils /dev/hdb1
```



## icat

- icat copies files by inode number from a device which contains a file system. Can be used to recover a deleted file (when intact)
- Example  
icat /dev/hdb1 17



## unrm

- unrm – copies unallocated data blocks  
Used to copy unallocated blocks to an output file in order to be processed by lazarus.

### Example

```
# unrm /dev/hdb1 > /tmp/unrm.of.hdb1
```



## lazarus

- lazarus – attempts to make sense out of raw data blocks
- Use to process the output from unrm. Saves blocks into files that lazarus thinks are associated in blocks directory
- Output controlled by lazarus.cf file
- Example
  - # lazarus /tmp/unrm.of.hdb1
- # lazarus -h /tmp/unrm.of.hdb1

CS526, Fall 2003

11



## Grouping Example

### File View

```

/* exploit.c */
/* Allows user to perform attack */
int main(int argc, char *argv [])
{
    evil_hack();
}

```

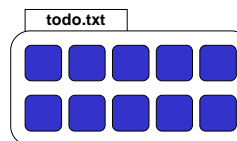
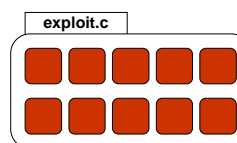
exploit.c: C source code

```

Things to Do:
- Give presentation
- Go to class
- Do laundry
- Write todo list


```

todo.txt: English text




CS526, Fall 2003

12



# Grouping Example

---



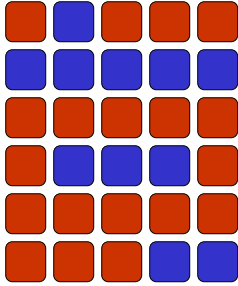
```

/* exploit.c */
/* Allows user to perform attack */
int main(int argc, char *argv [])
{
    evil_hack();
}

```

exploit.c: C source code

Block View




Things to Do:

- Give presentation
- Go to class
- Do laundry
- Write todo list

todo.txt: English text


CS526, Fall 2003

13



# lazarus

---



- Typical output looks something like  
atthttccccccppppptttttattcccpppttt  
otherwise output is in html files (-h option)
- See lazarus man page for translation of characters

CS526, Fall 2003

14



## file

- File – determine file type
- Similar to UNIX System V file command, but may generate better indication of file type



## pcat

- Pcat – copies process memory using ptrace or /proc file system. This is used to try to understand what a program is (doing), especially when the executable file has been deleted. (See Strangers in the Night article)
- Modern UNIX systems have a /proc filesystem that makes process information available in a convenient manner, including the executable file, current directory, and process memory.





## pcat

- Process attributes available in /proc
  - executable /proc/pid/exe
  - memory /proc/pid/mem
  - memory map /proc/pid/maps



## grave-robber

- grave-robber captures system forensic data
  - Runs many of TCT tools under the covers
- Three types of options
  - general options
    - where output goes, verbosity, etc
  - micro options
    - finer control over what data is collected
  - macro options
    - puts micro data collection into logical groups



## Law Enforcement Challenges

- Many findings will not be evaluated to be worthy of presentation as evidence.
- Many findings will need to withstand rigorous examination by another expert witness.
- The evaluator of evidence may be expected to defend their methods of handling the evidence being presented.
- The Chain of Custody may be challenged.



CS526, Fall 2003

19



## IDENTIFICATION – Technical Analysis

- Physical Context
- Logical Context
- Presentation/Use Context
- Opinion to support relevance of findings
- Handling and labeling of objects submitted for forensic analysis is key.
- Following a documented procedure is key.

CS526, Fall 2003

20



## Broader Picture: What to Do

- do not start looking through files
- start a journal with the date and time, keep detailed notes
- unplug the system from the network if possible
- do not back the system up with dump or other backup utilities
- if possible without rebooting, make two byte by byte copies of the physical disk
- capture network info
- capture process listings and open files
- capture configuration information to disk and notes
- collate mail, DNS and other network service logs to support host data
- capture exhaustive external TCP and UDP port scans of the host
- contact security department or CERT/management/police or FBI
- if possible freeze the system such that the current memory, swap files, and even CPU registers are saved or documented
- short-term storage
- packaging/labeling
- shipping