

Computer Forensics 2010
Computer Forensic Methodologies
Cell Phone Data Extraction

Detective Robby Godeaux
Austin Police Department
Computer Forensics Unit

Bachelors Degree Concordia University-
Criminal Justice Operations Management

Robby Godeaux- Bio

Austin PD since 1985
Detective since 1996

Assignments

Internal Affairs
Organized Crime
High Tech Investigations
Computer Forensics

IACIS-CFCE

International Association of Computer
Investigative Specialists
Certified Forensic Computer Examiner

EnCE

Guidance Software
EnCase Certified Examiner

ACE

Accessdata Corporation
Accessdata Certified Examiner

Common types of cases :

Child Pornography, Breach of Computer Security, Homicides, Sexual Assaults,
Robbery, Online Solicitation, Fraud, Theft, Counterfeiting, Identity Theft,
Narcotics, Human Trafficking, Prostitution, Gambling.

Surveillance Systems and Cell Phones.



Austin PD HTCF Unit

- High Tech Computer Forensics Unit
- 3 Detectives in Computer Forensics
 - Support Department-wide cases of all types
- 3 Detectives in "High Tech"
 - Work cases involving high tech crime

- 1 Sgt. Supervisor
- Mary Hesalroad 974-8526

Murphy's Top 10 Laws Of Computing

1. When computing, whatever happens, behave as though you meant it to happen.
2. When you get to the point where you really understand your computer, it's probably obsolete.
3. The first place to look for information is in the section of the manual where you'd least expect to find it.
4. When the going gets tough, upgrade.
5. For every action, there is an equal and opposite malfunction.
6. To err is human...to blame your computer for your mistakes is even more human, in fact its downright natural.
7. He who laughs last, probably has a back-up.
8. The number one cause of computer problems is computer solutions.
9. A complex system that doesn't work is invariably found to have evolved from a simpler system that worked just fine.
10. A computer program will always do what you tell it to do, but rarely what you want it to do

Differences between

Computer Examiners and Network Professionals

Network Professionals copy logical files
(evidence)

Computer Examiners copy physical files
(evidence)

Network Professionals

Disaster Prevention-Primary Focus

Disaster Recovery-Primary Focus

Network Security-Primary Focus

Computer Examiners

Evidence Preservation-Primary Focus

Evidence Analysis-Primary Focus

Courtroom Presentation of Evidence

Different Software Utilities
are used to accomplish each primary
focus

User Control- Absolute?

Operating Systems vs. File Systems
outside user control?

Allocated vs. Unallocated
outside user control?

Deleted vs. Deleted and Overwritten
outside user control?

Why is a physical acquisition necessary?

Scenario: US Constitution Conny.txt

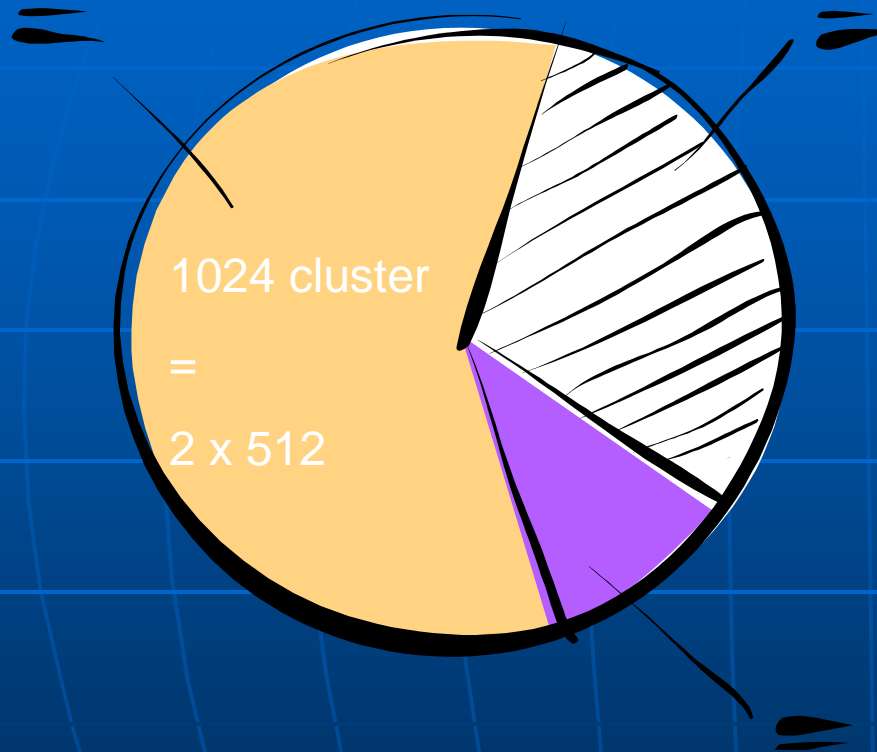
Sectors are grouped into clusters.

Windows writes to clusters.

Windows writes conny.txt to 1 cluster (two sectors) then is later deleted. A new file is written to the same cluster but is not nearly as large as Conny.txt.



File Slack (Cluster tips)



Conny.txt was a 400 byte file and is now deleted AND overwritten

the same cluster was used to write A new file, but this file is a 100 byte file.

If a simple and recognizable “stream” of data is visible-
What about other types?

Contiguous clusters vs Non-Contiguous Clusters

Acquisition 101

Use a forensic tool that captures everything on the hard drive.

Use a writeblocker to prevent accidental writes to the hard drive.
(Preserve the integrity of the evidence)

Beware of RAID volumes.

Hardware Writeblockers

