

CJS 528

Module 4: Spring 2009

Case Steps

- Scene Response
- Seizures and secure evidence
- Imaging and Storage of evidence
- Examination of images
 - ▣ Order by “interest”
 - ▣ Log and Notes
- Documentation
- Presentation to Parties involved
- Conclusion of Case
 - ▣ Return evidence

Writing a Good Case

- Peripheral Components
 - Table of Contents
 - Glossary
 - References (if any)
 - Policies
 - Evidence Handling and numbering
 - Chain of Custody documents
 - Sterile Media Management and Use
 - Software Licensing
 - Imaging Policy

Contents of a Case

- Depends on the case

- If the case asks a question

- E.g. – The suspect claims he was at home alone during the robbery and that he sent an email to a friend during that time. What should be in the summation?

- An answer to this question!

- If the case asks for production of all evidence

- Then you need to document what you found without going into great detail (see examples)

Writing a Good Case

- CV of examiners
- File Lists

Case 1 Steps

- Load the case into FTK
- Data Carve the Case (demo in class)
- Include any data carved items of relevance
- Examine the evidence and check mark any interesting items and document in your log.
- Revisit all checked items and bookmark them by category.
- Now revisit all your bookmarks and begin documenting the files relevant to the case.
- Screenshots, dates, times, hashes, etc.

Method for Case 1

- First start a log and keep up with what is happening
- Start a chain of custody document which shows the evidence at all times (number all evidence)
- Now, take the image and duplicate it (you don't really need to do this since you can download it as you need to from cisweb)
- Work on the duplicate

Case 1 Steps

- Write your analysis of the files with full explanations.
- Proof and reread your analysis
- Now write your draft summation
- Proof and re-read your summation for content.
- Document references with page and evidence numbers.
- Create all attachments etc.

DOS systems and knowledge

- ❑ DOS is often used because it is easier to understand and there are low level forensics tools available
- ❑ DOS is not required to take or pass the CCE examination
- ❑ DOS is not required for this course.
- ❑ The book does refer to DOS a lot.
- ❑ If you want to set up DOS, either get a boot disk for DOS or use vmware server (free) to run DOS under Windows.

Real Mode DOS

- Windows after WIN 98 stopped using Real mode dos
- Real Mode DOS means it is really running
- In WIN XP DOS is merely a shell emulation of DOS. Most forensics tools will not work in this environment.

OS and Disk Storage

- Different OS have had different approaches to storage of information.
- Some concepts are common
 - ▣ Bits – 0 or 1
 - ▣ Sectors – collection of things in a pie slice
 - ▣ Clusters – collection of sectors, the smallest writeable unit on the drive.
 - ▣ Tracks – Circular identifier on the platter
 - ▣ Cylinder – Column of tracks.
 - ▣ So it is common to see things referred by their sector

Partitions

- Partitions are made up of sectors and are sectors which are allocated to a logical structure.
- Partitions are typically logical drive structures (C, D, etc.)

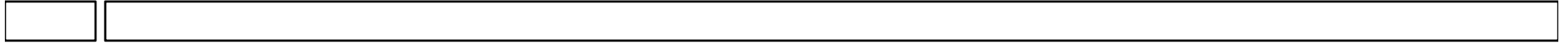
So how does a disk store things and find them again?

- Two main systems that were used
 - ▣ FAT (12, 16, 32)
 - ▣ NTFS
- Other systems
 - ▣ EXT2 and 3 (UNIX/Linux)
 - ▣ HTs (MAC)

FAT

- FAT is used for older drives and can still be used (FAT 32 or FAT 12).
- FAT writes two file allocation tables (one is a backup) to the disk
- A file allocation table contains pointers to the files location on the disk in terms of clusters
 - ▣ Clusters have a size in sectors which can be 512, 1024, etc. This is the smallest writeable unit on the disk.

FAT



- The file allocation table contains
 - ▣ Filename in text
 - ▣ File size in bytes
 - ▣ Starting cluster (where it is stored)
 - ▣ Date it was added and so on.
 - ▣ In FAT the data contents are stored out on the drive NOT in the FAT itself.

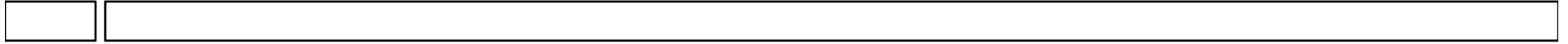
So how can you find anything?

- A pointer in the fat says that the file starts in cluster 85. If the file is 2090 bytes long and the cluster size is 512 then the file is 5 clusters long
 - $(2090 / 512 == 4.08)$.
- Each cluster on the disk has a pointer to the NEXT cluster so in a perfect world the clusters would look like
 - 85>>86>>87>>88>>EOF (in 89)
 - This is called a sequential file

An interesting artifact

- So think about that 4.08 clusters.
- In reality it looks like this
 - ▣ $512 == 512$ (85)
 - ▣ $512 == 512$ (86)
 - ▣ $512 == 512$ (87)
 - ▣ $512 == 512$ (87)
 - ▣ $512 > 2090 - 2048 == 42$ bytes
- So, there is really 470 bytes of unused (wasted) space in the cluster since it can't be written to.

Wasted Space



- This called Slack Space

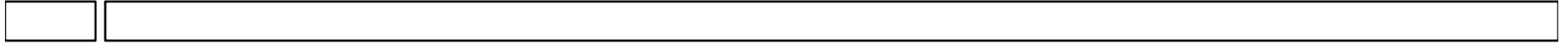
So what happens to a file when it is deleted?

- Create a text file on a floppy disk.
- The file contains:
 - ▣ The secret coordinates of the drop are 47N10 by 58W21.
 - ▣ This is 56 bytes. It is written to a cluster and thus the cluster looks like this
 - ▣ The secret coordinates of the drop are 47N10 by 58W21. f6f6f6f6f6f6f6f6f6 (and so on) to 512 bytes.
 - ▣ Now, let's delete this file.

Deleting a file

- In the FAT,
 - ▣ The first character of the file name is changed to δ (e5 hex).
 - ▣ That's it. The cluster is freed.
 - ▣ So now another file is written to the deleted space containing
 - ▣ My name is Mudd. 16 bytes.
 - ▣ Now the cluster looks like this
 - ▣ My name is Mudd.inates of the drop are 47N10 by 58W21. f6f6f6f6f6f66f6f6 (and so on) to 512 bytes.
 - ▣ Look how much info is still there!

Deleted Files

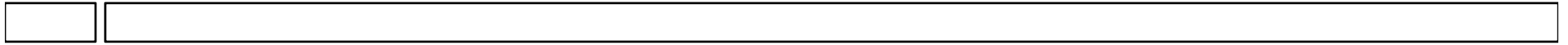


- So what happens is that over time, files pile up in this empty and sometimes create usable information.

Discussion of Data Carving

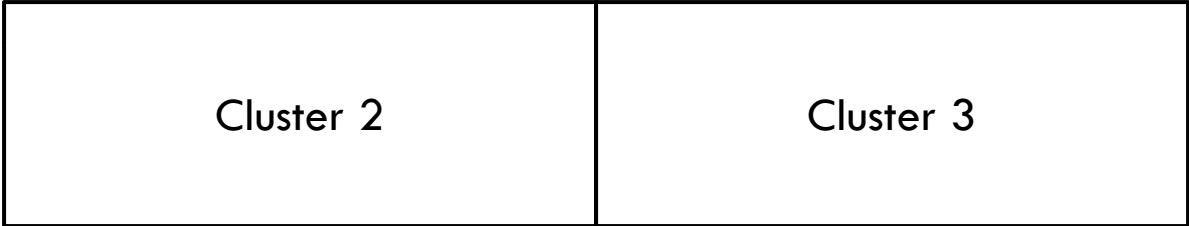
- Data carving involves simply examining multiple types of empty(?) space on media for content.
 - ▣ Slack Space
 - ▣ Unused Space (free space)
 - ▣ Unallocated Space (unpartitioned)
 - ▣ Multi-Sessions

Slack Space



- Disk formatting uses a unit called a cluster to allocate space (the smallest writeable unit) on the media.
- A cluster may be sized differently based on the system and formatting used
 - E.g. 512 bytes >> 4096 bytes

Slack Space

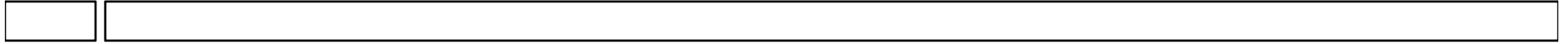


Byte 0

Byte 512

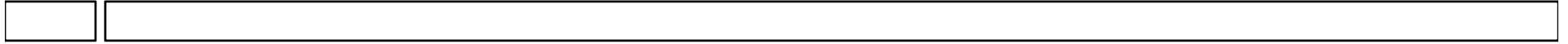
Byte
1024

Slack Space




- So if you have a file which is exactly 1024 bytes, it would fill these two clusters completely.
- If the file is only 865 bytes, then what happens?

So what can slack contain?



- ❑ Pieces of files
- ❑ Metadata
- ❑ Who knows?

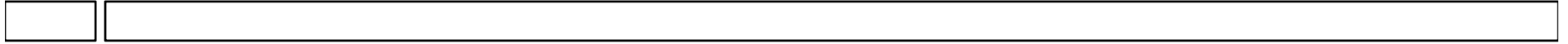
Unused Space

- 
- This is just free space on your logical disk.
 - When a file is deleted, it is only marked for deletion in the FAT or the MFT. The actual data remains on the disk until those clusters are overwritten by something else. Thus, pieces of files may be laying all over the disk and be able to be recovered.

Unused space which is used?!

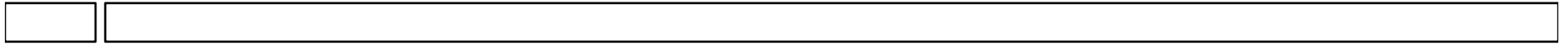
- Most OS can use “virtual memory” which is the use of contiguous clusters on the disk which are not in use.
- Virtual memory contains
 - ▣ Cache files (web pages, emails, chats)
 - ▣ Documents which were open on the screen
 - ▣ Almost anything.
- This may be recovered using techniques like data carving.

Unallocated Space



- This is unpartitioned space.
- When you partition a disk you are creating logical drives on the physical drive.
 - ▣ E.g. Drive C on Physical Drive 80.
- This partition can be deleted and its information is deleted from the partition tables but again, the space is untouched. This is great since now the OS cannot use this space and there may be all kinds of useful information here.

Unallocated



- Just because it is unallocated, doesn't mean it has no content.
- When a partition is deleted only the references to the partition are removed. The data in the partition is still there. You can delete and undelete partitions easily using partition magic, or other tools.

Understanding Data Carving

- This is the process of examining
 - ▣ slack,
 - ▣ Unused
 - ▣ Unallocated
- Space on the disk.

Disk fragmentation

- Remember the idea of the sequential clusters.
- In many cases, as files are written and deleted, the disk condition worsens and the total amount of sequential clusters declines to the point that there is simply not a space large enough to write an entire file. So now, the cluster list may look like this:
 - ▣ 85>>108>>2045>>76>>1012>EOF
 - ▣ This is called fragmentation (and this is pretty extreme).

Undeletes

- Undeletes happen by two things:
 - ▣ Change the E5 hex to an ! Or whatever
 - ▣ Relink the cluster chain which is all zeros
 - ▣ So, if you know a file starts in 85 and that it is 5 clusters, you can literally go on the disk and undelete this stuff by retyping the cluster addresses in.
 - ▣ But what happens when they are not sequential?
 - Good luck! You are going to need it.
 - ▣ Tools like FTK have algorithms that do this for you but it can be done manually!

The idea of data carving

- Data carving tools look for file headers
- When file headers are found in a cluster, the carving tool then makes a dramatic assumption:
 - ▣ That some number of clusters go with this header
- It then takes that number of sequential clusters and pulls together to see what is there.
- This approach can sometimes yield interesting results.

Carving Tools

- FTK data carving is not very good as it is very limited in file headers but it does work for some things.
- Carving is based on algorithms which attempt to figure out what is what and recover all the clusters from the space.
- Other tools
 - ▣ Datalifter
 - ▣ Simple Carver (requires a tool to extract the data)

Recommendation

- Data carving is an art form
- Some people start with large chunks and carve smaller and smaller until they get something.
- Others do the other way around.
- Best practice: It depends on what you are looking for.
- If you are searching for video, then larger file sizes are the norm.
- Having a good header list is important.

The smoking gun

- Forensics unfortunately doesn't always yield nice clean evidence which clearly indicts the suspect (or exonerates them).
- You may be forced to dig through slack space hoping to see a small portion of something that will give you what you need.
- Smoking guns are nice, but they may not happen.