Edinburgh Napier UNIVERSITY

CSN08101
Digital Forensics
Lecture 9: Data Analysis

Module Leader: Dr Gordon Russell
Lecturers: Robert Ludwiniak

Edinburgh Napier UNIVERSITY

Lecture Objectives

- File metadata
- Data hiding
- Data recovery
  - File signature
  - File carving

Edinburgh Napier
UNIVERSITY

METADATA

MFT List of possible attributes

Edinburgh Napier UNIVERSITY

- Defined in $AttrDef entry of MFT, but default is:
  - 0x10 STANDARD_INFORMATION
  - 0x20 $ATTRIBUTE_LIST
  - 0x30 $FILE_NAME0
  - 0x40 (NT) $VOLUME_VERSION (2K) $OBJECT_ID
  - 0x50 $SECURITY_DESCRIPTOR
  - 0x60 $VOLUME_NAME
  - 0x70 $VOLUME_INFORMATION
  - 0x80 $DATA
  - 0x90 $INDEX_ROOT
  - 0xA0 $INDEX_ALLOCATION
  - 0xB0 $BITMAP
  - 0xC0 (NT) $SYMBOLIC_LINK, (2K) $REPARSE_POINT
  - 0xD0 $EA_INFORMATION
  - 0xE0 $EA0xF0NT$PROPERTY_SET
  - 0x100 (2K) $LOGGED_UTILITY_STREAM

Edinburgh Napier UNIVERSITY

Date-Time Stamps Significance

- File Created
  - This date-time stamp usually shows when a file or folder was created
  - When an existing file is copied, the File Created date-time stamp of the new copy is set to the current time
  - When a file is moved onto a different volume using the Windows command line or drag-and-drop feature, the File Created date-time stamp of the new copy is set to the current time
  - When a file is moved onto a different volume using the Cut and Paste menu options, the File Created date-time stamp remains unchanged (the Last Accessed and Entry Modified date-time stamps would most likely change).

- Modified
  - This date-time stamp represents the last time the $DATA attribute of a file was altered.

Edinburgh Napier UNIVERSITY

Date-Time Stamps Significance

- Last Accessed
  - This date-time stamp represents the most recent time a file or folder was accessed by the file system. This date-stamp does not necessarily indicate that a file was opened; simply placing the mouse over the filename in Windows Explorer can update the last accessed date.

- SIA Modified
  - This date-time stamp represents the last time any attribute in the MFT record for the file or folder was modified. Reasons for an update to this date-time stamp can include changing a file's location on the disk, another data stream being added to the file, or a change in the file's name.

Edinburgh Napier UNIVERSITY

Metadata Analysis Considerations

- Directory Entry time Values
  - Times are stored with respect to time zones
  - Last access and created times are optional
    - Corroborate with Application-Level data

Edinburgh Napier UNIVERSITY

Metadata Analysis Considerations

- Create time
  - Resolution of 10 Milliseconds
- Write Time
  - Resolution of 2 Seconds
- Access Time
  - 1 Day

Edinburgh Napier
UNIVERSITY

METHODS OF HIDING DATA

Edinburgh Napier UNIVERSITY

Methods Of Hiding Data

- To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These are media exploited using new controversial logical encodings: steganography and marking.
  - **Steganography**: The art of storing information in such a way that the existence of the information is hidden.

Edinburgh Napier UNIVERSITY

Methods Of Hiding Data

- **T**o **h**uman **e**yes, **d**ata **u**sually **c**ontains **k**nown **f**orms, **l**ike **i**mages, **e**-mail, **s**ounds, **a**nd **t**ext. **M**ost **I**nternet **d**ata **n**aturally **i**ncludes **g**ratuitous **h**eaders, **t**oo**.** **T**hese **a**re **m**edia **e**xploited **u**sing **n**ew **c**ontroversial **l**ogical **e**ncodings: **s**teganography **a**nd **m**arking.

- ***The duck flies at midnight. Tame uncle Sam***
  - Simple but effective when done well

Edinburgh Napier UNIVERSITY

Methods Of Hiding Data

- **Watermarking**: Hiding data within data
  - Information can be hidden in almost any file format.
  - File formats with more room for compression are best
    - Image files (JPEG, GIF)
    - Sound files (MP3, WAV)
    - Video files (MPG, AVI)
  - The hidden information *may* be encrypted, but not necessarily
  - Numerous software applications will do this for you: Many are freely available online

Edinburgh Napier UNIVERSITY

Steganography Tools

- Steganos
- S-Tools (GIF, JPEG)
- StegHide (WAV, BMP)
- Invisible Secrets (JPEG)
- JPHide
- Camouflage
- Hiderman
- Many others…

Edinburgh Napier UNIVERSITY

Methods Of Hiding Data

- Hard Drive/File System manipulation
  - Slack Space is the space between the logical end and the physical end of file and is called the file slack. The logical end of a file comes before the physical end of the cluster in which it is stored. The remaining bytes in the cluster are remnants of previous files or directories stored in that cluster.
    - Slack space can be accessed and written to directly using a hex editor.
    - This does not add any “used space” information to the drive
  - Partition waste space is the rest of the unused track which the boot sector is stored on – usually 10s, possibly 100s of sectors skipped
    - After the boot sector, the rest of the track is left empty

Edinburgh Napier UNIVERSITY

Methods Of Hiding Data

- Hard Drive/File System manipulation cont…
  - Hidden drive space is non-partitioned space in-between partitions
    - The File Allocation Table (FAT) is modified to remove any reference to the non-partitioned space
    - The address of the sectors must be known in order to read/write information to them
  - Bad sectors occur when the OS attempts to read info from a sector unsuccessfully. After a (specified) # of unsuccessful tries, it copies (if possible) the information to another sector and marks (flags) the sector as bad so it is not read from/written to again
    - users can control the flagging of bad sectors
    - Flagged sectors can be read to /written from with direct reads and writes using a hex editor

Edinburgh Napier UNIVERSITY

Methods Of Hiding Data

- Hard Drive/File System manipulation cont…
  - Extra Tracks: most hard disks have more than the rated # of tracks to make up for flaws in manufacturing (to keep from being thrown away because failure to meet minimum #).
    - Usually not required or used, but with direct (hex editor) reads and writes, they can be used to hide/read data
  - Change file names and extensions – i.e. rename a .doc file to a .dll file

Edinburgh Napier UNIVERSITY

Alternate Data Streams

- (NTFS) New Technology File System allows for Alternate Data Streams
- One file can be a link to multiple Alternate Data Streams of files of any size.
- Important Note! – These Alternate Data Streams are Hidden!
- Allows for hiding of files and even directories!
- Difficult to detect
  - Doesn't show up when you run c:\dir

Edinburgh Napier UNIVERSITY

Alternate Data Streams

- C:\notepad mike.txt:mikehidden.txt
- This allows mikehidden.txt to be a hidden ADS

```
C:\dir
02/26/2004  02:29p         0  mike.txt
```

- Notice – no indication of mikehidden.txt
- Although a message was saved in the mikehidden.txt, the mike.txt shows 0 bytes!

Edinburgh Napier
UNIVERSITY

METHODS OF DETECTING/RECOVERING DATA

Edinburgh Napier UNIVERSITY

Methods Of Detecting/Recovering Data

- Steganalysis - the art of detecting and decoding hidden data
  - Hiding information within electronic media requires alterations of the media properties that may introduce some form of degradation or unusual characteristics
  - The pattern of degradation or the unusual characteristic of a specific type of steganography method is called a signature
  - Steganalysis software can be trained to look for a signature

Edinburgh Napier UNIVERSITY

Methods Of Detecting/Recovering Data

- Steganalysis Methods - Detection
  - Human Observation
    - Opening a text document in a common word processor may show appended spaces and “invisible” characters
    - Images and sound/video clips can be viewed or listened to and distortions may be found
      - Generally, this only occurs if the amount of data hidden inside the media is too large to be successfully hidden within the media (15% rule)
  - Software analysis
    - Even small amounts of processing can filter out echoes and shadow noise within an audio file to search for hidden information
    - If the original media file is available, hash values can easily detect modifications

Edinburgh Napier UNIVERSITY

Methods Of Detecting/Recovering Data

- Steganalysis Methods – Detection cont...
  - Disk analysis utilities can search the hard drive for hidden tracks/sectors/data
  - RAM slack is the space from the end of the file to the end of the containing sector. Before a sector is written to disk, it is stored in a buffer somewhere in RAM. If the buffer is only partially filled with information before being committed to disk, remnants from the end of the buffer will be written to disk. In this way, information that was never "saved" can be found in RAM slack on disk.
  - Firewall/Routing filters can be applied to search for hidden or invalid data in IP datagram headers

Edinburgh Napier UNIVERSITY

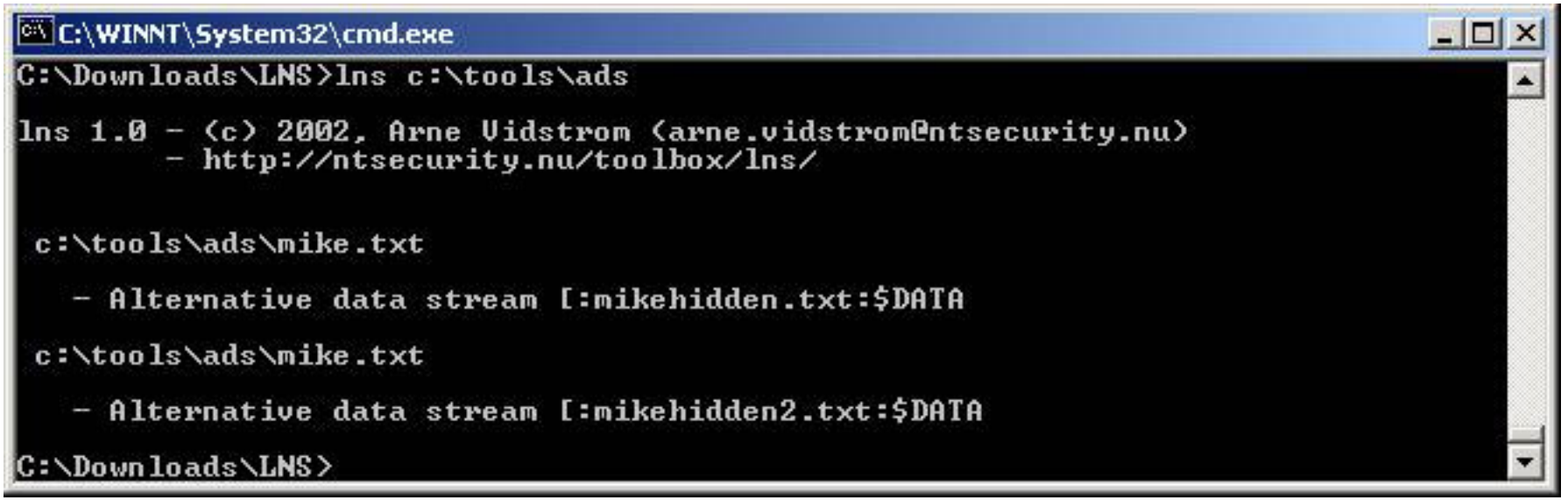
Methods Of Detecting/Recovering Data

- Steganalysis Methods – Recovery
  - Recovery of watermarked data is extremely hard
    - Currently, there are very few methods to recover hidden, encrypted data.
  - Data hidden on disk is much easier to find. Once found, if unencrypted, it is already recovered
  - Deleted data can be reconstructed (even on hard drives that have been magnetically wiped)
  - Check swap files for passwords and encryption keys which are stored in the clear (unencrypted)
  - Software Tools
    - Scan for and reconstruct deleted data
    - Break encryption

Edinburgh Napier UNIVERSITY

Alternate Data Streams

- Tools for Detecting Alternate Data Streams
  - LNS – www.ntsecurity.nu
  - LADS - www.heysoft.de
  - NTFS ADS Check - www.diamondcs.com.au



Edinburgh Napier
UNIVERSITY

FILE RECOVERY

Edinburgh Napier UNIVERSITY

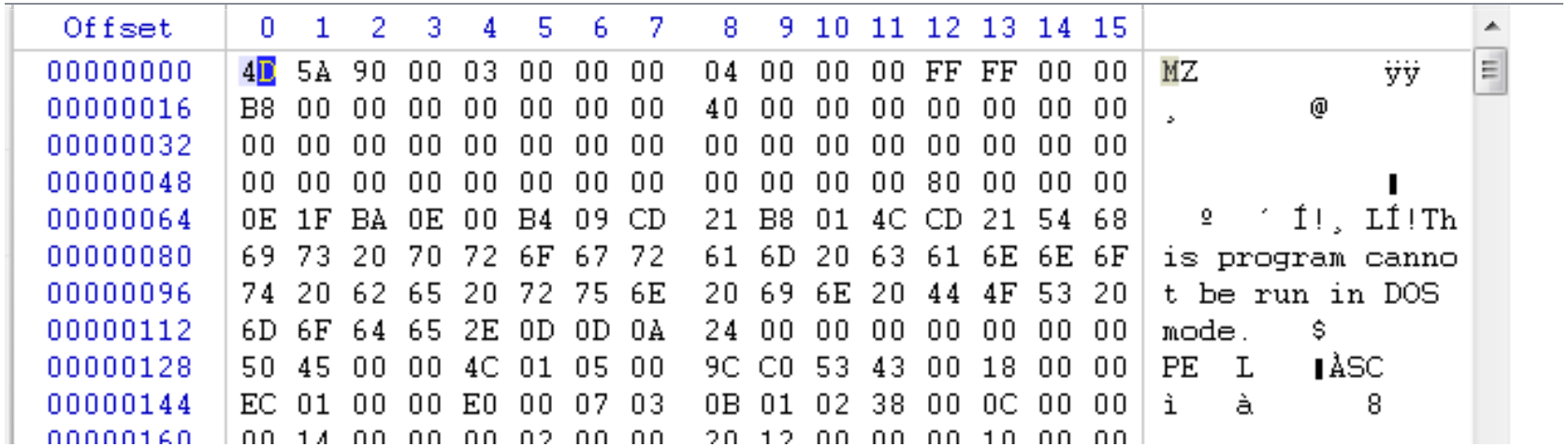
Files

- Windows uses file extensions to figure out how to open a file
  - e.g. .pdf
- However, files contain information inside them to allow other OS to process them
  - File Headers

Edinburgh Napier UNIVERSITY

File Header

- Example:
  - Executables have the header MZ (0x4D)



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ ÿÿ
00000016	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸ @
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000048	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	▌
00000064	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	º ´ Í!¸ LÍ!Th
00000080	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000096	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000112	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode. $
00000128	50	45	00	00	4C	01	05	00	9C	C0	53	43	00	18	00	00	PE L ▌ÀSC
00000144	EC	01	00	00	E0	00	07	03	0B	01	02	38	00	0C	00	00	ì à 8
00000160	00	14	00	00	00	02	00	00	20	12	00	00	00	10	00	00	

Edinburgh Napier UNIVERSITY

File Signatures

- Prime target for hiding data
  - E.g. hiding image files as dlls in a system folder
- Files also contain end regions, or footers
- A combination of file extension, headers and footers can be used for file recovery

Edinburgh Napier UNIVERSITY

File Signatures

4D 5A	MZ
COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS	Windows/DOS executable file
ACM	MS audio compression manager driver
AX	Library cache file
CPL	Control panel application
FON	Font file
OCX	ActiveX or OLE Custom Control
OLB	OLE object library
SCR	Screen saver
VBX	VisualBASIC application
VXD, 386	Windows virtual device drivers

25 50 44 46	%PDF
PDF, FDF	Adobe Portable Document Format and Forms Document file
	Trailers:
	0A 25 25 45 4F 46(.%%EOF)
	0A 25 25 45 4F 46 0A(.%%EOF.)
	0D 0A 25 25 45 4F 46 0D 0A(..%%EOF..)
	0D 25 25 45 4F 46 0D(.%%EOF.)

[512 byte offset] EC A5 C1 00	[512 byte offset] ì¥Á.
DOC	Word document subheader (MS Office)

Edinburgh Napier UNIVERSITY

File Signatures

49 44 33		ID3
	MP3	MPEG-1 Audio Layer 3 (MP3) audio file

52 49 46 46 xx xx xx xx		RIFF....
41 56 49 20 4C 49 53 54		AVI LIST
	AVI	Resource Interchange File Format -- Windows Audio Video Interleave file

[29,152 byte offset]		[29,152 byte offset]
57 69 6E 5A 69 70		WinZip
	ZIP	WinZip compressed archive

http://www.garykessler.net/library/file_sigs.html

Edinburgh Napier UNIVERSITY

File Hash Searching

- Databases of known “good” files or known “bad” files can be used to rapidly detect content
  - Goal is to easily identify “Known” files
  - Hashes of known files are calculated and stored
    - NIST NSRL (National Software Reference Library)
  - Search to identify “Known Bad” files
    - Hacking tools
    - Training manuals
    - Contraband photographs
  - Ignore “Known Good” files
    - Microsoft Windows files
    - Standard application files
    - Standard build files (corporate server deployments)

Edinburgh Napier UNIVERSITY

sorter

- Perl script that analyzes a file system to organize the allocated and unallocated files by file type.
- It runs the 'file' command on each file and organizes the files according to the rules in configuration files.
- Extension mismatching is also done to identify 'hidden' files.
- Work with hash databases for files that are known to be good and can be ignored and files that are known to be bad and should be alerted.

Edinburgh Napier UNIVERSITY

sorter

`-f fstype` - Specify the file system type of the image(s)
`-a hash_alert` - Specify the location a hash database with entries of known 'bad' files.
`-x hash_exclude` - Specify the location a hash database with entries of known 'good' files
`-d dir` - Specify the location of where all files should be written.
`-m mnt` - Specify the mounting point of the image being analysed.

sorter - sorter.sum

Edinburgh Napier UNIVERSITY

```
Files (282)

Files Skipped (33)
- Non-Files (33)
- Reallocated Name Files (0)
- 'ignore' category (0)

Hash Databases
- Hash Database Alerts (9)
- Hash Database Exclusions (226)

Extensions
- Extension Mismatches (5)
- Hash Database Exclusions with Extension Mismatch (0)

Categories (23)
- archive (0)
- audio (0)
- compress (1)
- crypto (0)
- data (9)
- disk (1)
- documents (1)
- exec (1)
- images (7)
- system (0)
- text (0)
- unknown (3)
- video (0)
```

Edinburgh Napier UNIVERSITY

hfind

- Looks up hash values in a database using a binary search algorithm.
- This allows to create a hash database and identify if a file is known or not.
- It works with the NIST National Software Reference Library (NSRL) and the output of ’md5sum’.

- Before the database can be used by ’hfind’, an index file must be created with the ’-i’ option.

Edinburgh Napier UNIVERSITY

hfind

`-i db_type` - Create an index file for the database.
`-f lookup_file` - Specify the location of a file that contains one hash value per line.
`db_file` - The location of the hash database file.
`[hashes]` - The hashes to lookup.

Example of hash database:

```
4f3f7bbc40bf854f8a3a8eb62ac8d2a1  Sac Bomb.htm
26821d2d7f896da0319590cbc661cb7b  geov2.js
4f59788bde58d15d541a9c116d0e850d  visit.gif
83ef14448bb235652e07e277460dc771  mc.js
87b690e217d6e7302d799ce6d4903a3e  glass_pipes.gif
325472601571f31e1bf00674c368d335  serv.gif
```

Edinburgh Napier UNIVERSITY

`md5deep`

- Suite of cross platform tools to compute and audit hashes for any number of input files.
- Similar to other hashing programs like md5sum.
- It can also recursively traverse directory structures, use a variety of algorithms, and use files of known hashes to perform both positive and negative matching.
- Another program in the suite `hashdeep` can conduct a computer forensics audit.

Edinburgh Napier UNIVERSITY

md5deep

`-c <alg1>[,<alg2>...]` - Computation mode. Compute hashes of FILES using the algorithms specified.

`-k` - Load a file of known hashes.

`-m` - Positive matching, requires at least one use of the -k flag.

`-x` - Negative matching. Same as the -m flag above, but does negative matching.

`-r` - Enables recursive mode.

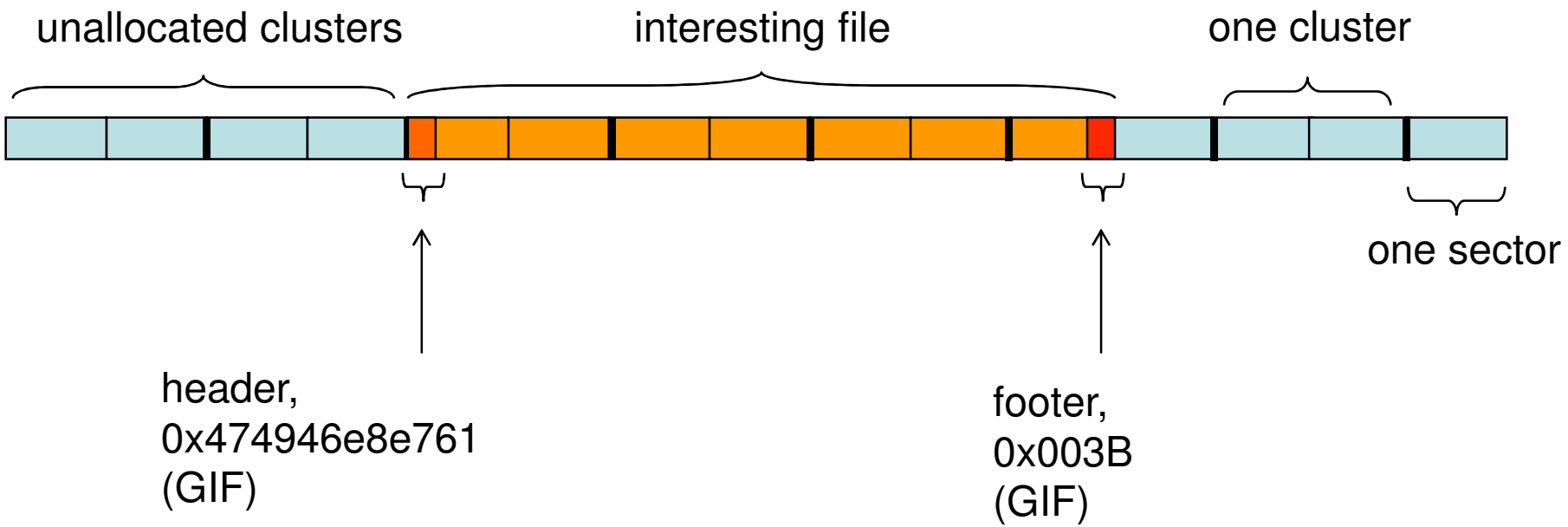
Edinburgh Napier UNIVERSITY

File Carving

- Carving is the process of discovering and extracting files based on their content, rather than using metadata.
- Most file carvers operate by looking for file headers and/or footers, and then "carving out" the blocks between these two boundaries.
- By using a database of headers and footers for specific file types, file carver can retrieve files from raw disk images, even if the file system metadata has been destroyed.

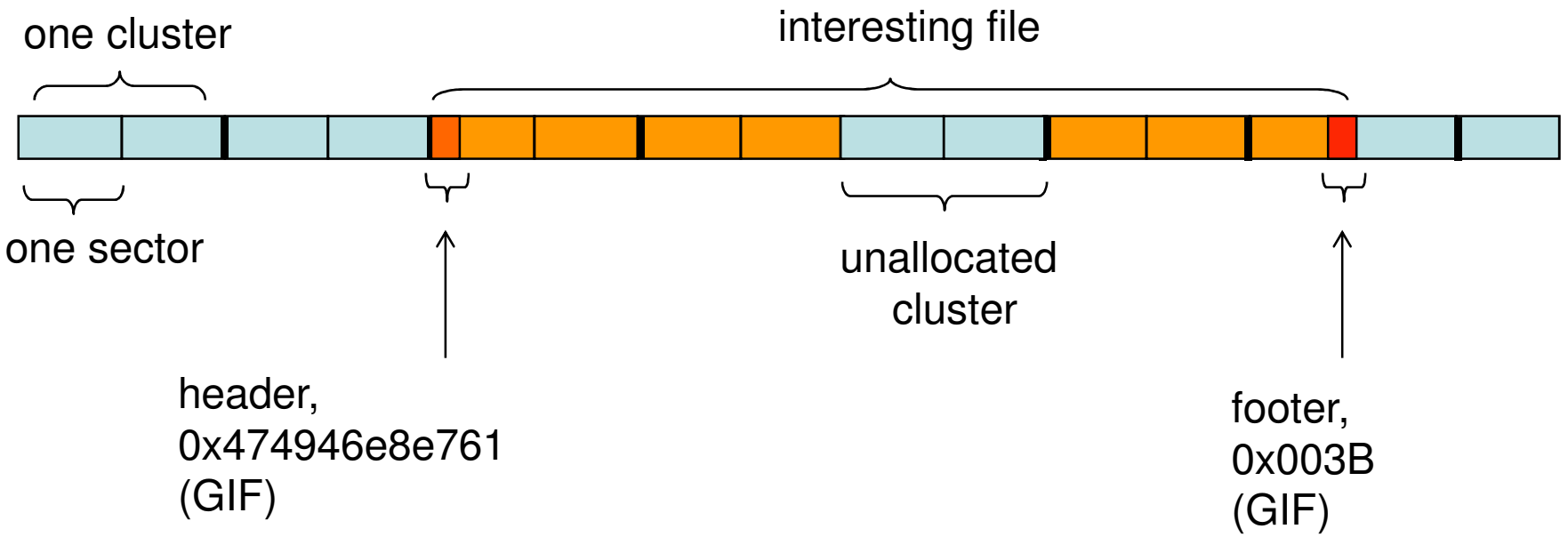
Edinburgh Napier UNIVERSITY

File Carving - Basic Idea



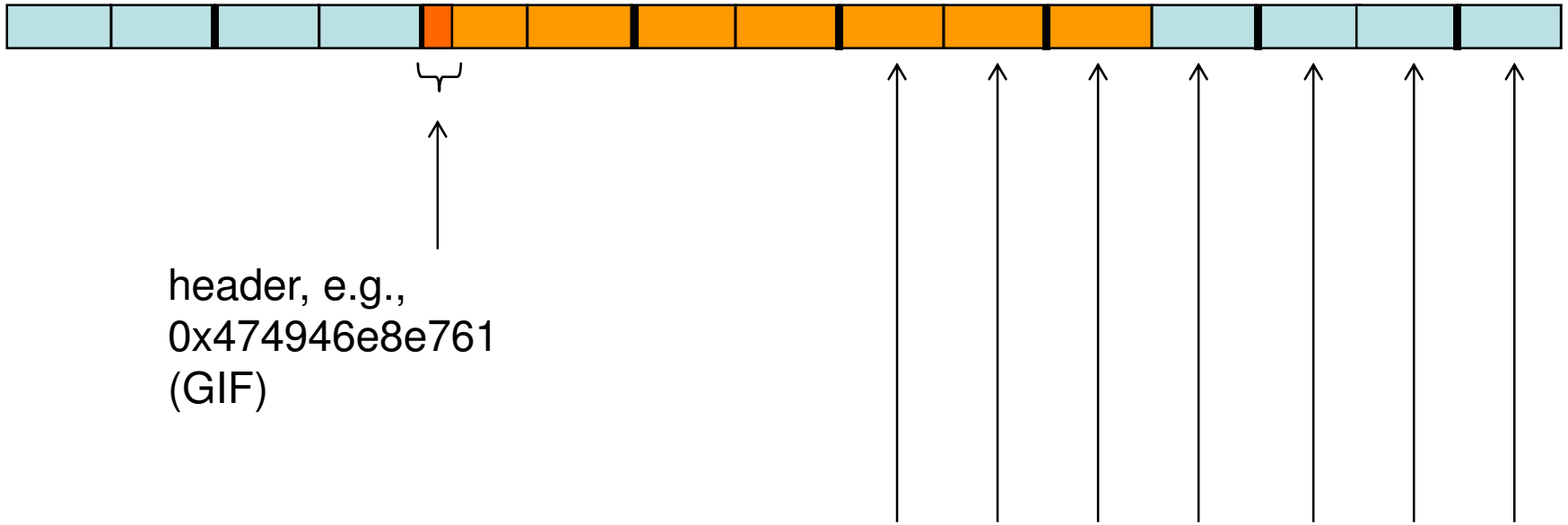
Edinburgh Napier UNIVERSITY

File Carving - Fragmentation



Edinburgh Napier UNIVERSITY

File Carving - Block Sniffing



header, e.g.,
0x474946e8e761
(GIF)

Do these blocks “smell” right?

- N-gram analysis
- entropy tests
- parsing

File Carving - Scalpel

Edinburgh Napier UNIVERSITY

- Two-pass design
  - Reads the entire disk image in large chunks (of user-definable size, with a default size of 10 MB).
  - Once the first pass complete, Scalpel has a complete index of header and footer locations, which is used to populate a set of work queues that control file carving operations .
- Minimizes:
  - Reads
  - Seeks
  - Writes
  - Data copying
  - Memory usage

G. G. Richard III, V. Roussev, "Scalpel: A Frugal, High Performance File Carver,"
Proceedings of the 2005 Digital Forensics Research Workshop (DFRWS 2005), New Orleans, LA.

Edinburgh Napier
UNIVERSITY

ANY QUESTIONS ...