Shadow Warriors

Lee Whitfield & Mark McKinnon

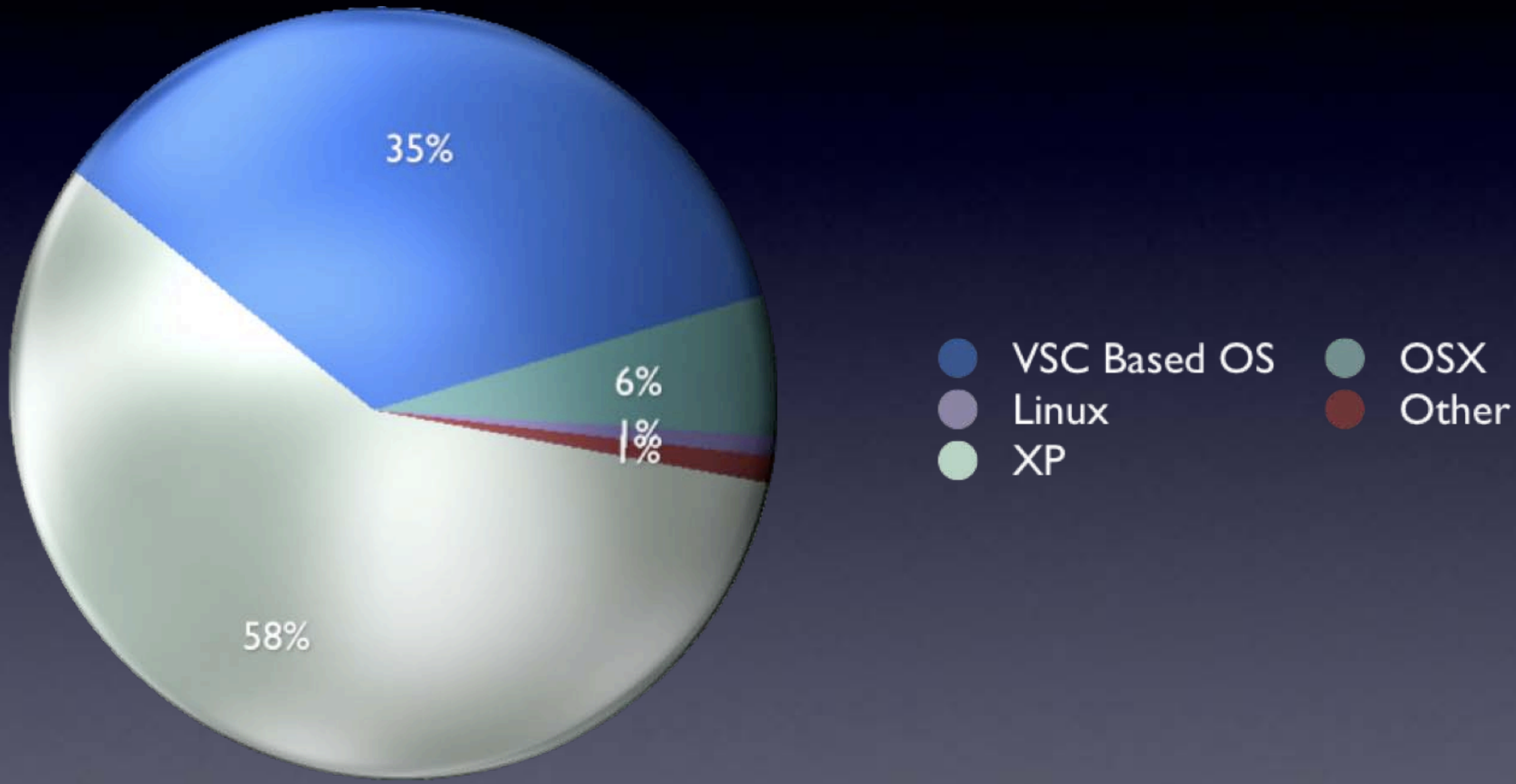
Lee Whitfield

- Responsible for Forensic Investigations at Disklabs in the UK
- 7 years in IT (4 in Forensics)
- Over 250 Investigations for Law Enforcement, Defence, and Corporate Clients
- BSC (Hons) Computing (Forensics)
- CCE
- GCFA (Do it)
- Founder of Forensic 4cast (http://forensic4cast.com)
- Twitter – @schizophreud

Mark McKinnon

- 19+ years in IT
- Masters of Science in Computer Science Emphasis in Software Engineering
- CCE
- GCFA
- Owner RedWolf Computer Forensics
  - Provide 15+ Programs used by Forensic Examiners around the world
    - Drive Prophet
    - Skype Log ParserChrome, Firefox, Flock Browser Parsers
    - Etc…
- Blog – http://cfed-ttf.blogspot.com
- Twitter – @markmckinnon

OS Usage



Numbers courtesy of StatCounter.com

What are Volume Shadow Copies?

System Volume Information

	Name
1	MountPointManagerRemoteDatabase
2	tracking.log
3	{3808876b-c176-4e48-b7ae-04046e6cc752}
4	{e04d024a-e56e-11de-bd6b-bbebb2745f6d}{3808876b-c176-4e48-b7ae-04046e6cc752}
5	{f1c5af7c-e581-11de-bb94-f1b60de5d687}{3808876b-c176-4e48-b7ae-04046e6cc752}
6	{6860adfb-e57e-11de-bdb0-cc551c307784}{3808876b-c176-4e48-b7ae-04046e6cc752}
7	SPP

What Does This Mean?

Useful Data

Wiped/Erased Files

File Movements

File Access

Link Files

Overwritten Files/Data

Older Versions of Files

Old Registry Entries

Etc

Shadow File Creation

Picture.jpg

16KB Block

16KB Block

= Occupied 4KB Cluster

= Deleted 4KB Cluster

= Unused 4KB Cluster

16KB Block

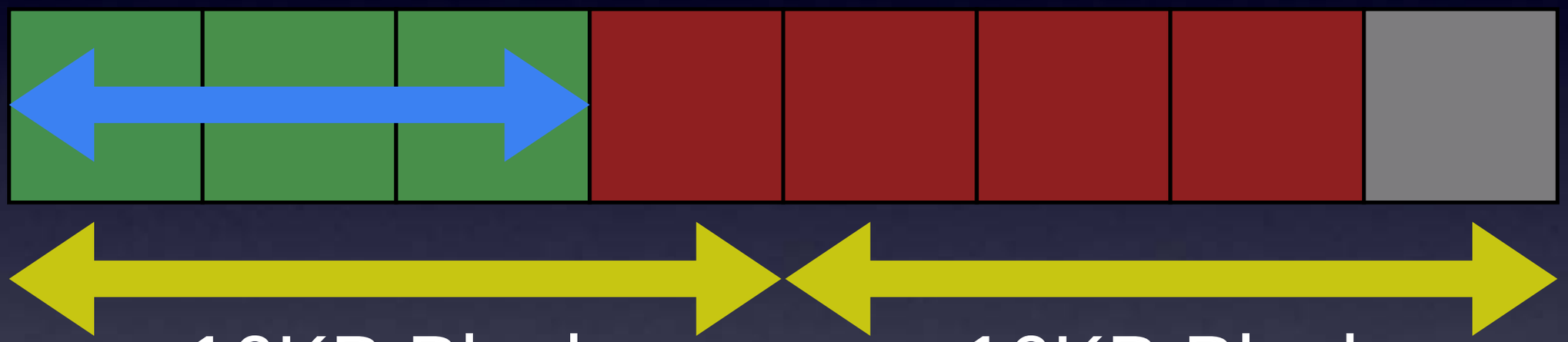
16KB Block

= Occupied 4KB Cluster

= Deleted 4KB Cluster

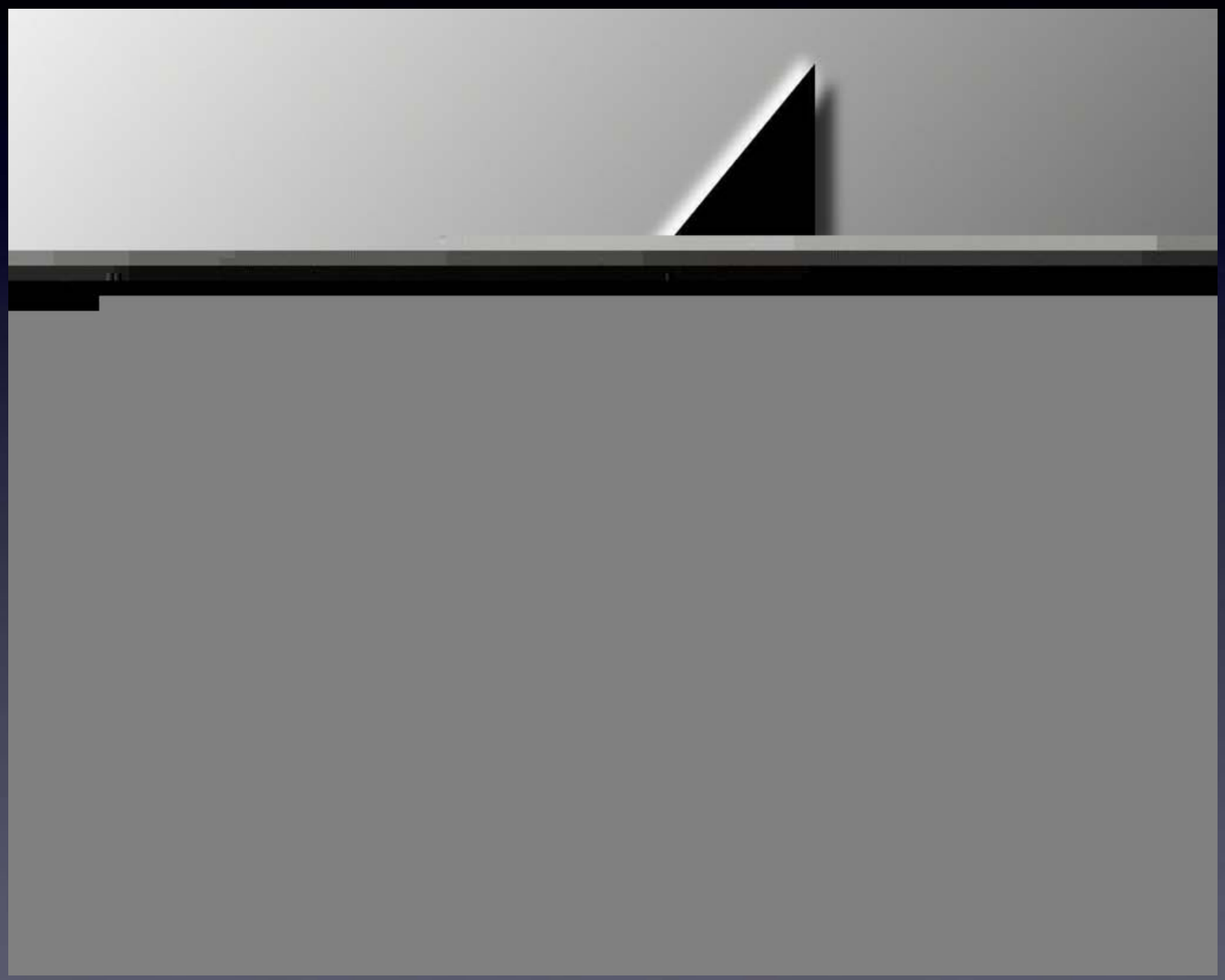
= Unused 4KB Cluster

Document.doc



= Occupied 4KB Cluster = Deleted 4KB Cluster = Unused 4KB Cluster

File Carve



Current Investigation Methods

?

Anatomy of Volume Shadow Copies

Data Blocks

Index Blocks

Index Blocks

Contain:

- volume logical offset of the original location
- difference file offset for original data
- volume logical offset of the original data within the difference file

6B 87 08 38 76 C1 48 4E B7 AE 04 04
6E 6C C7 52 01 00 00 00 04 00 00 00

8 bytes giving the index block's own file offset

8 bytes giving the index block's logical volume offset

8 bytes giving the logical volume offset for the next index block

Offset 128 of an index block

32 byte records referencing a data block

Made up of 4x 8 byte values

Bytes 0-7 contain the volume logical offset of the original location

Bytes 8-15 contain the file offset for original data

Bytes 16-23 contain the volume logical offset of the original data within the shadow file

Bytes 24-31 are more complicated...

Bytes 24-27 contain one of the following values:

00 - no meaning

02 - data mapping comes in to play

88 - currently unknown

Bytes 28-31

All zeroes unless preceded by 02

Each bit refers to a 512 byte chunk

Write on 1 leave on 0

Practical Application

$$4520914944\ \%$$

$$16384 = 12288$$

4520914944 - 12288

=

4520902656 (00 80 77 0D 01 00 00 00)

00 00 00 C0 15 00 00 00 00 80 77 0D 01 00 00 00

00 00 00 C0 18 00 00 00 00 00 00 00 00 00 00 00

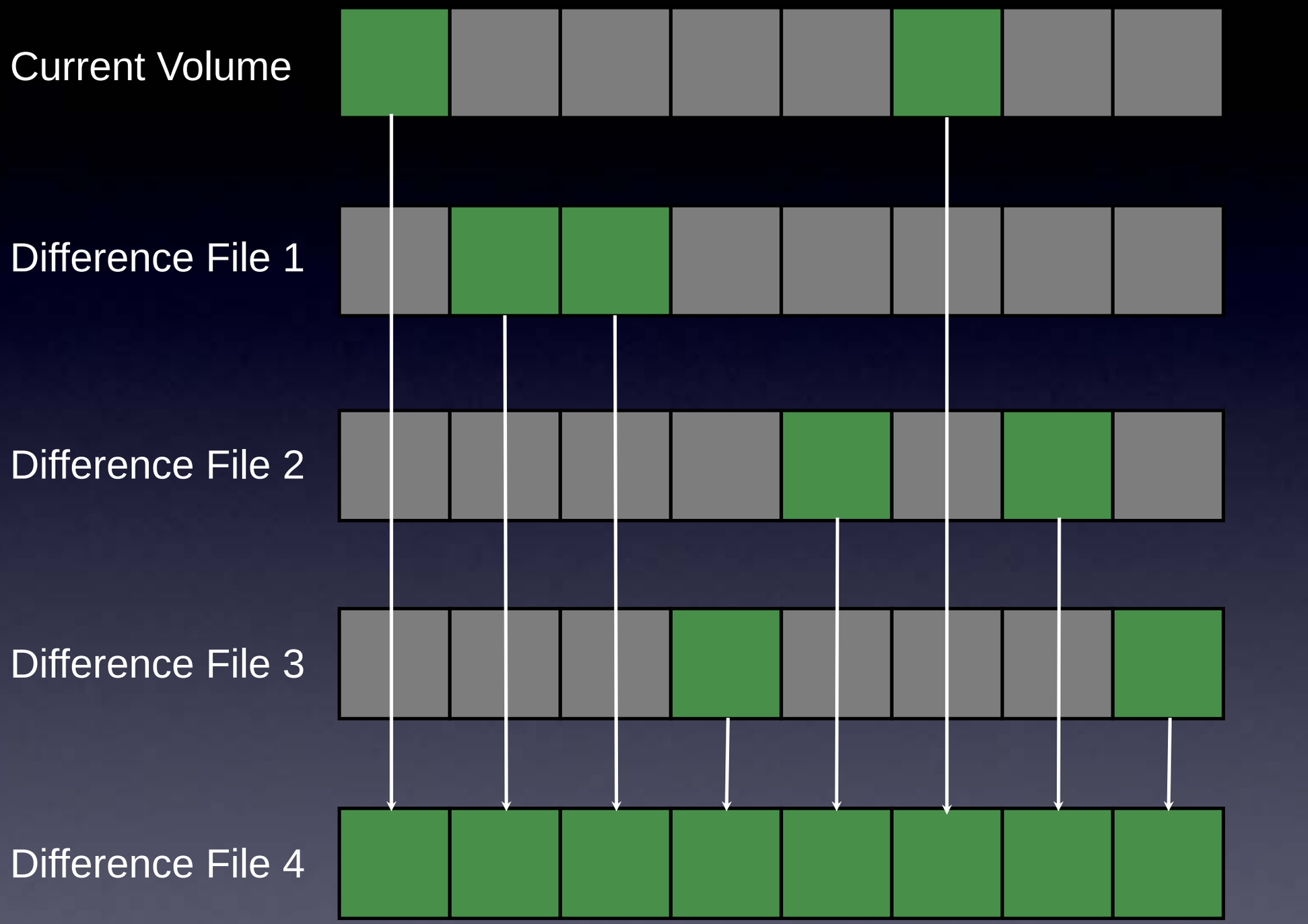
Logical Offset of Original Location

File Offset for Data Block (Search Hit)

Logical Offset of Original Data


4
cast

Complex File/Volume Recovery



Deleted, unallocated, and corrupt VSCs

00 00 00 C0 15 00 00 00 00 80 77 0D 01 00 00 00

00 00 00 C0 18 00 00 00 00 00 00 00 00 00 00 00

Logical Offset of Original Location

File Offset for Data Block (Search Hit)

Logical Offset of Original Data

Current Files

Excluded Files

shadow analyzer

Shadow Analyzer

- View the contents of the hard disk drive at a point in time.
- Recover deleted and erased files
- View older versions of current files
- View historic date and time information for all files, both live and deleted
- View changes to files across days, weeks, or even months
- Extract full files from volume shadow files.

Demo

Will run on XP upwards,
OS X, and Linux

Visit http://shadowanalyzer.com to register you interest and you'll be entered into a prize draw to win a free copy of Shadow Analyzer.

Thank you

twitter.com/shadowanalyzer

lee.whitfield@shadowanalyzer.com

mark.mckinnon@shadowanalyzer.com