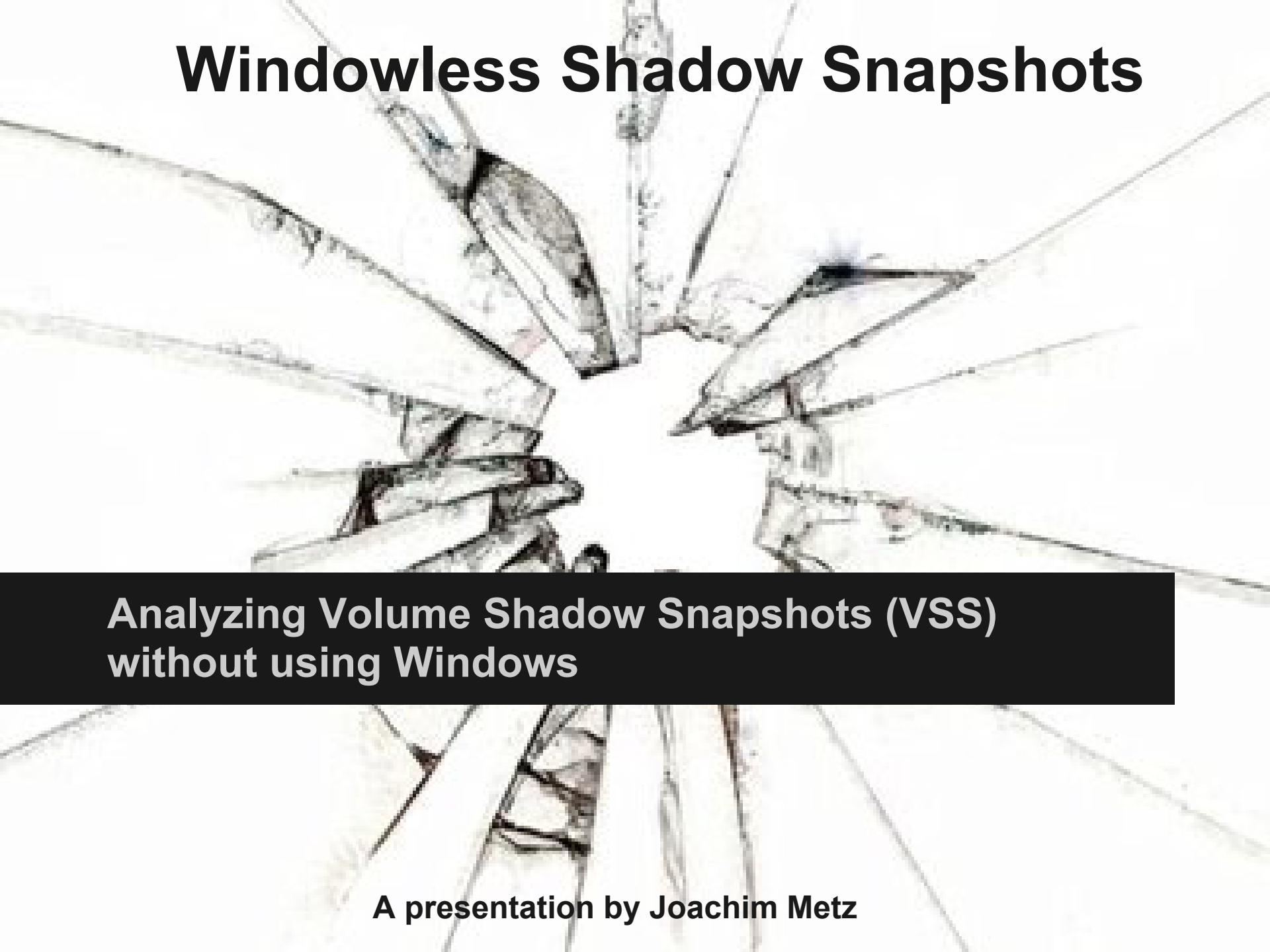
Windowless Shadow Snapshots



Analyzing Volume Shadow Snapshots (VSS) without using Windows

A presentation by Joachim Metz

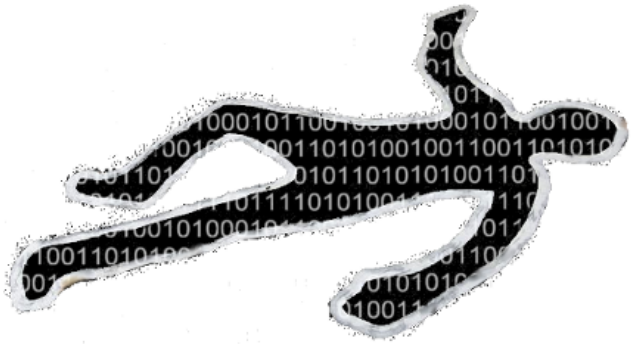
Hello, my name is ...

Joachim Metz <joachim.metz@gmail.com>

I work at ...

Google

Projects: libewf, libpff and more:
http://code.google.com/p/libyal/



What's in store

30 minutes of months of hexdump analysis.

Under the hood of Volume Shadow Snapshots (VSS)

Vshadow library and tools

Questions and discussion (at the end)

What's in a name

Volume Shadow Copy Service:

Extensive sub system in Windows to create shadow copies

Volume Shadow Snapshots:

On-disk snapshot volumes created by kernel driver volsnap.sys.
User-space API interfaces via IO control

Are you REALLY sure you deleted that file?

File system and content snapshot once a day (Windows Vista) or once a week (Windows 7), also used by System Restore Points.

History of system and application state

What about temporary files?

What about unallocated space?

Common practice

Windows analysis system

vssadmin, DiskShadow

VSS device files:
\\.\HarddiskVolumeShadowCopy#

http://www.forensicswiki.org/wiki/Windows_Shadow_Volumes

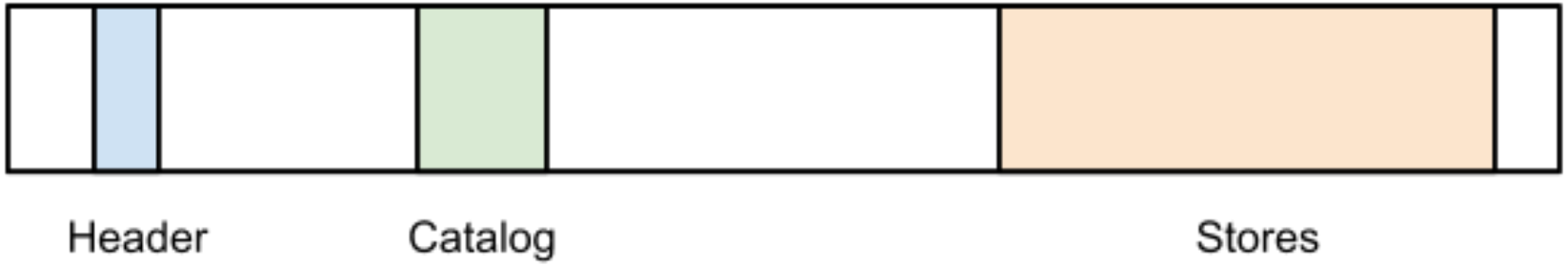
Did you know?

From MSDN:

If this bit flag (VSS_VOLSNAP_ATTR_EXPOSED_LOCALLY) and the VSS_VOLSNAP_ATTR_EXPOSED_REMOTELY bit flag are not set, the shadow copy is hidden.

http://msdn.microsoft.com/en-us/library/windows/desktop/aa385012(v=vs.85).aspx

VSS volume



Stand-alone, minor NTFS integration

Header points to the catalog

Catalog points to the store(s)

A store per snapshot-volume

The Store

"Basically bitmaps, block lists and data"

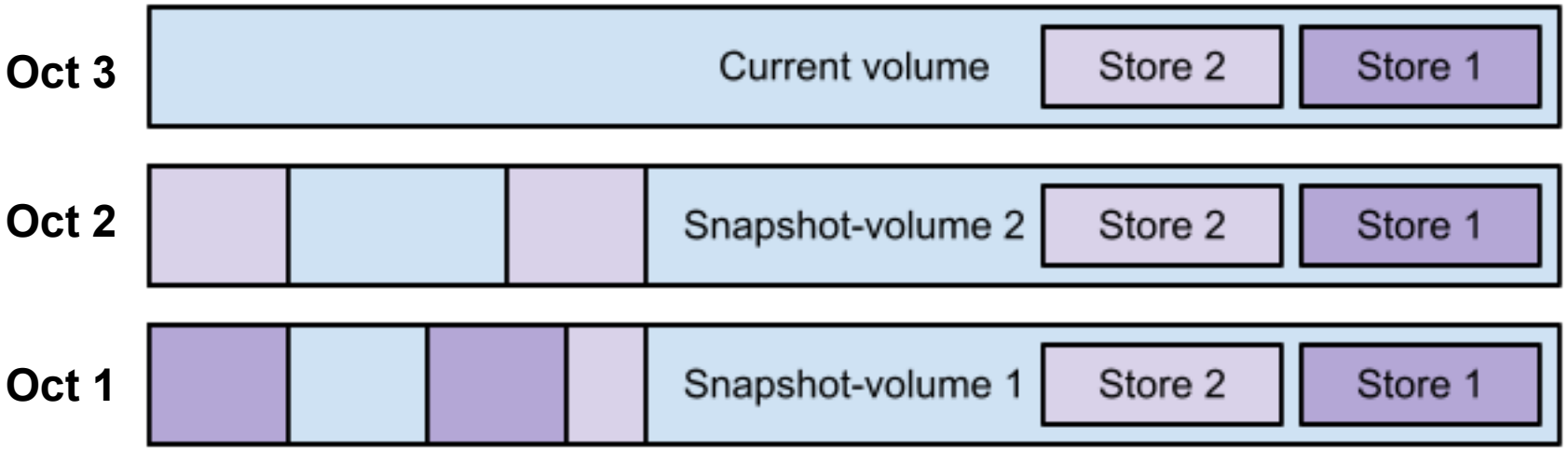
Store:

- information
- current bitmap
- previous bitmap
- block list
- block range list
- snapshot data

Block descriptor:

- original offset
- offset of the data
- flags
- bitmap

Stacking snapshots



Changes tracked in reverse

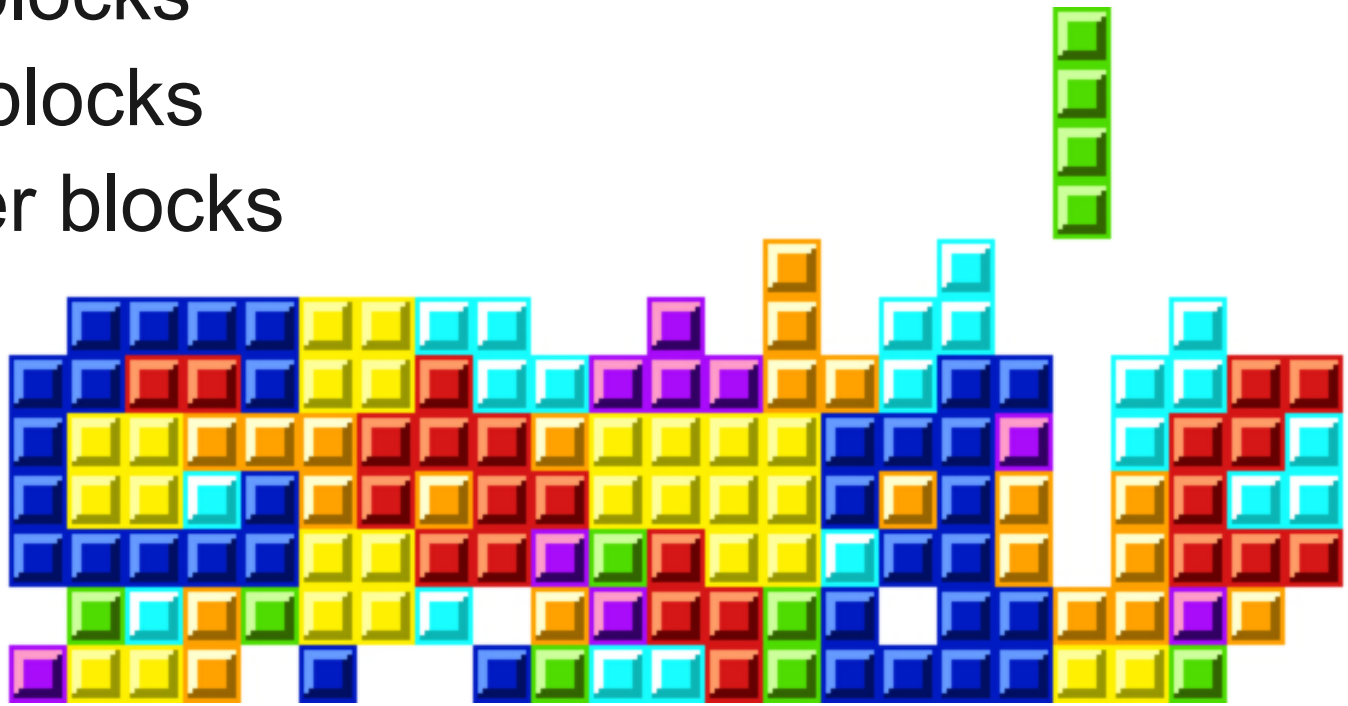
Bitmaps control data outside block list

Zero-fill or map to current volume

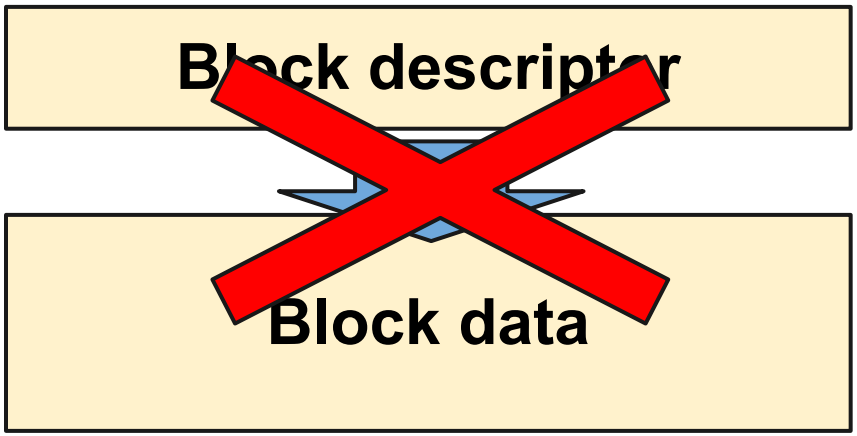
VSS is like playing Tetris

"Blocks all over the place and trying to place them somewhere that makes sense".

- normal blocks
- overlay blocks
- forwarder blocks

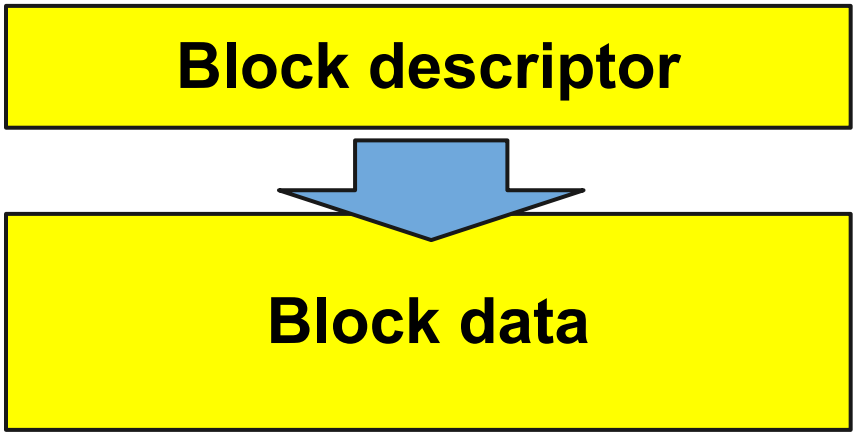


Normal blocks



Points to 16 KiB data

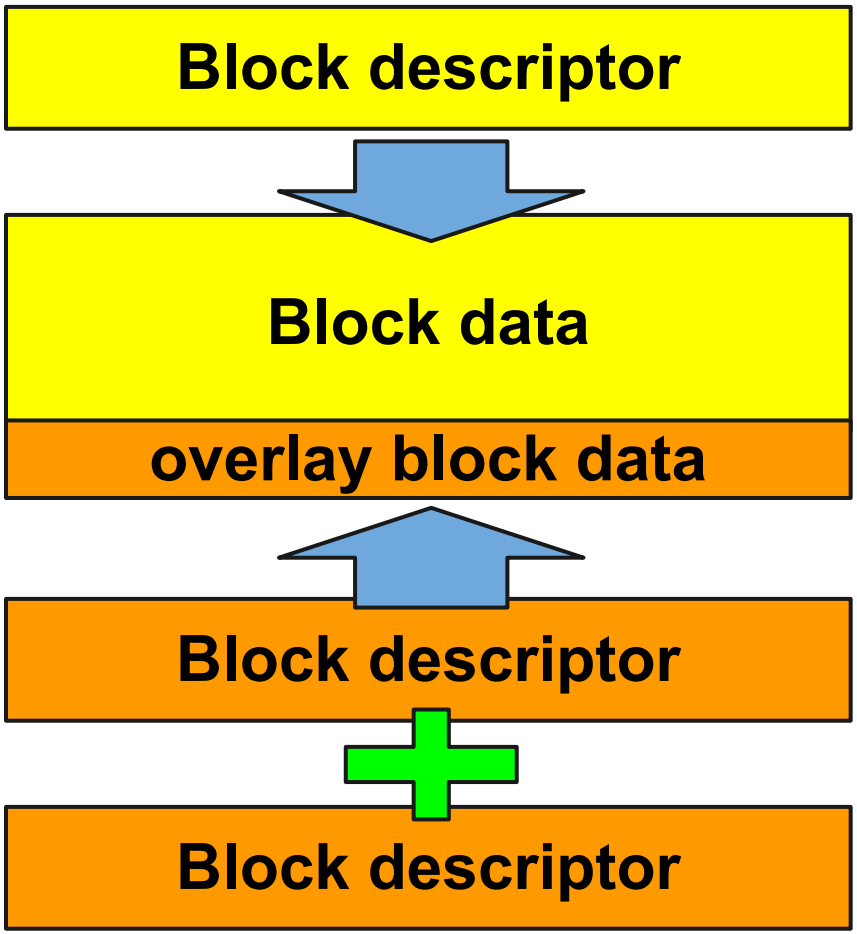
Any block except overlay or forwarder



Block order:

Most recent is used, including forwarder

Overlay blocks

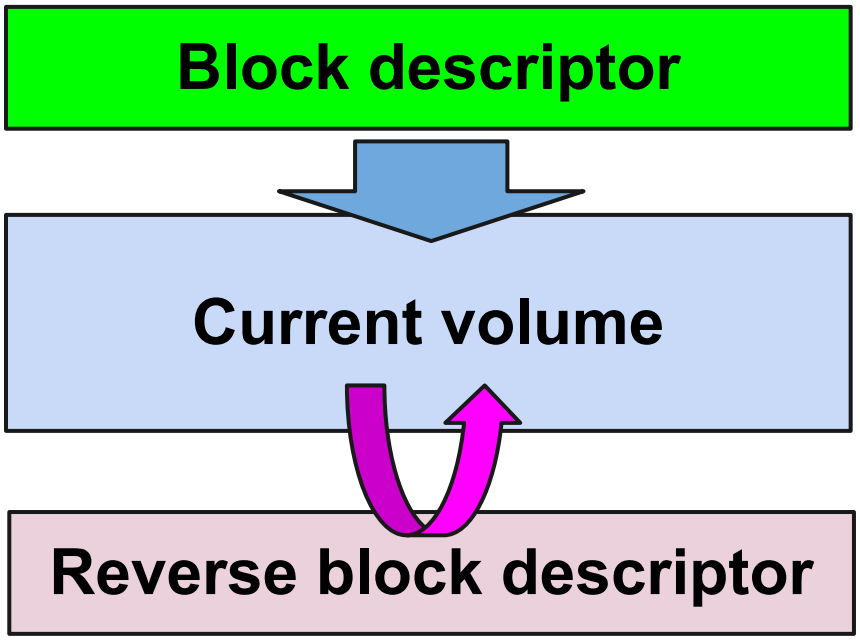


Overlays existing data

Controlled by bitmap
Granularity 512 bytes

Block order:
Multiple are combined
Separate from data

Forwarder blocks



Forward to offset

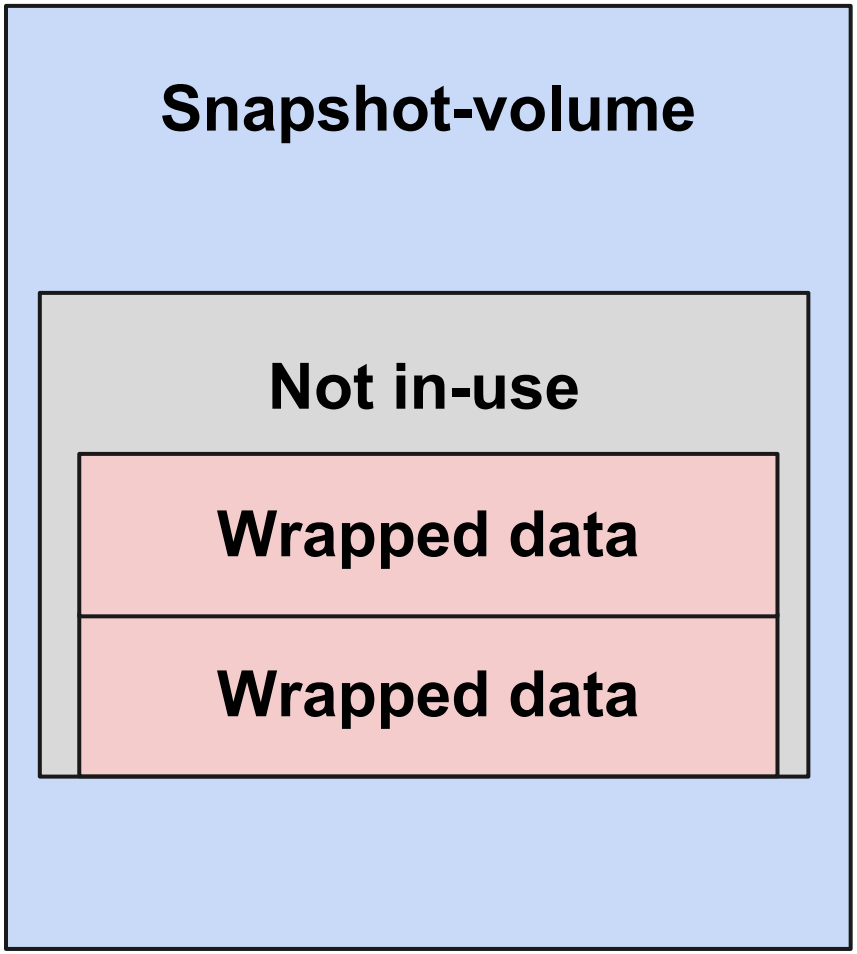
Block order:

Most recent is used

Adds reverse block descriptor

Offset swap

Block wrap: game over?



Mismatch between image and live device.

Data seems to be wrapped, but not consistent.

Implications for analyzing VSS

Let's recap

Stand-alone volume-layer
Stores: bitmaps, block lists and data
Blocks: normal, overlay and forwarder (reverse)
Changes tracked in reverse
Bitmaps control data outside block list
Block wrap: nasty side effect block not in-use

More detail: paper and format specification

libvshadow

Library and tools to support the Volume Shadow Snapshot (VSS) format.

Current state: experimental

Tools: vshadowinfo, vshadowmount

http://code.google.com/p/libvshadow/

vshadowinfo in action

```
vshadowinfo -o 1048576 image.raw
```

```
Volume Shadow Snapshot information:
    Number of stores:    2

Store: 1
    Identifier           : 93db9c47-bb19-4004-836d-c3c835550b9a
    Shadow copy set ID   : 8bc68d0b-9df4-49e0-be4b-725dceaaefc8
    Creation time        : May 19, 2012 14:20:35.765721000 UTC
    Shadow copy ID       : 04057e11-d2d5-4d9c-8914-aeba832e467b
    Volume size          : 30002905088 bytes
    Attribute flags      : 0x00420009

Store: 2
    ...
```

vshadowmount in action

```
vshadowmount -o 1048576 image.raw fuse/
```

```
fls fuse/vss1
r/r 35-128-1: file1
r/r 39-128-1: file2
```

```
fls fuse/vss2
r/r 35-128-1: file1
r/r 44-128-1: file3
```

```
icat fuse/vss1 39-128-1 > file2
```

What's next?

Tracking changes across snapshots

Inter-snapshot analysis

...

http://www.forensicswiki.org/wiki/Open_Research_Topics

Questions?