Unstuck in Time

STROZ FRIEDBERG 10/28/2015 strozfriedberg.com

Zack Weger, Jon Stewart

NTFS structures in play

- **$MFT**—primary filesystem metadata structure, maintains current state.
- **$Extend/$Usnjrnl**—$J alternate data stream records when changes were made to file.
- **$Logfile**—a traditional filesystem transactional journal, records very detailed changes but not always when the changes took place.
- **Volume Shadow Copies**—volume-level cluster snapshots of the filesystem, recorded periodically and on-demand.

$MFT

- Flat table of 1KB-sized records, each describing a file (<waves hands/>).
- Standard header, then list of “attributes” that contain metadata and sometimes file content.
  - You should know that I know that you know all this.
- This is what the Sleuthkit parses when working with an NTFS volume.

$UsnJrnl

- Main data stream is empty, “$J” stream is a log of filesystem changes as binary records.
- Instead of rolling to beginning of file, the beginning is clipped by using sparse data runs and new events are simply appended. *Tricksy,* NTFS, *very tricksy.*
  - If you copy out the sparse extents, you’ll have a *lot* of useless zeroes.
- Each event has timestamp of when the change occurred.
- Each event has the type of change.
- Each event notes the file that changed.
- There’s some other metadata, too.
- …But not much else about the change itself.

$UsnJrnl (cont'd)

```
typedef struct {
  DWORD          RecordLength;
  WORD           MajorVersion;
  WORD           MinorVersion;
  DWORDLONG      FileReferenceNumber;
  DWORDLONG      ParentFileReferenceNumber;
  USN            Usn;
  LARGE_INTEGER TimeStamp;
  DWORD          Reason;
  DWORD          SourceInfo;
  DWORD          SecurityId;
  DWORD          FileAttributes;
  WORD           FileNameLength;
  WORD           FileNameOffset;
  WCHAR          FileName[1];
} USN_RECORD_V2, *PUSN_RECORD_V2, USN_RECORD, *PUSN_RECORD;
```

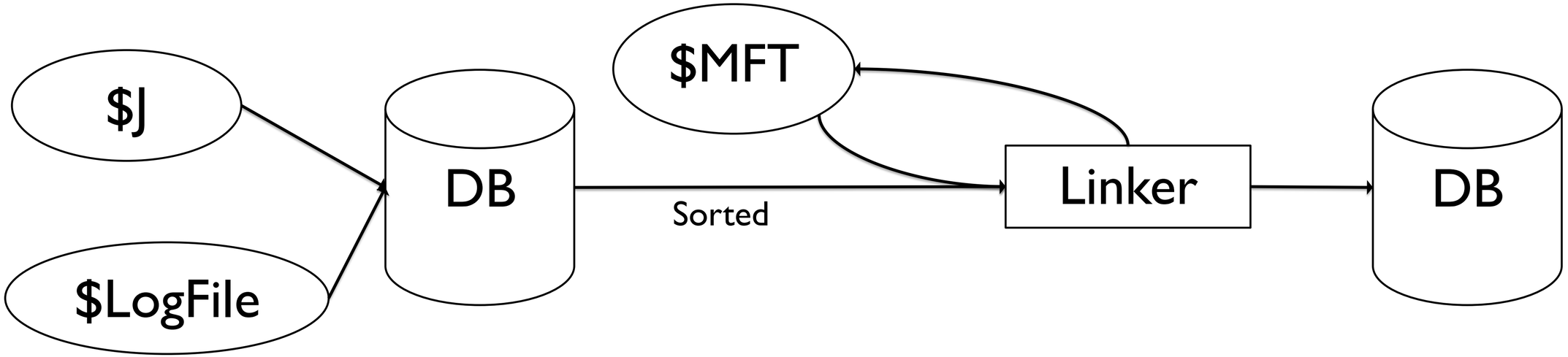
Source: MSDN

$logfile

- Circular log—wraps around to beginning. Sort events by LSN to restore order.
- Primary purpose: filesystem journaling, allow for repair & recovery.
- Binary log of changes made to files
  - Has a lot more data than $UsnJrnl. *A lot, a lot, a lot.*
  - *Fewer* events than $UsnJrnl, though.
- Records are in order, but no *event* timestamp is recorded about when changes occurred.
  - But some records will have timestamps we can use (e.g., created)

Linking the Data

- $UsnJrnl and $Logfile reference the $MFT, but over time.
- We typically only have the most recent version of $MFT.
- Therefore, one's conception of $MFT needs to change as $UsnJrnl/$Logfile are parsed.



Volume Shadow Copies

- Available in XP, enabled by default in Win7+. Defaults to weekly snapshots, but configurable.
- The raw clusters of the volume are snapshotted in a copy-on-write manner.
- Because it's so low-level, $MFT/$UsnJrnl/$Logfile are all snapshotted.
- Joachim Metz's libvshadow can parse VSCs
  - *No VSSAdmin required!*.

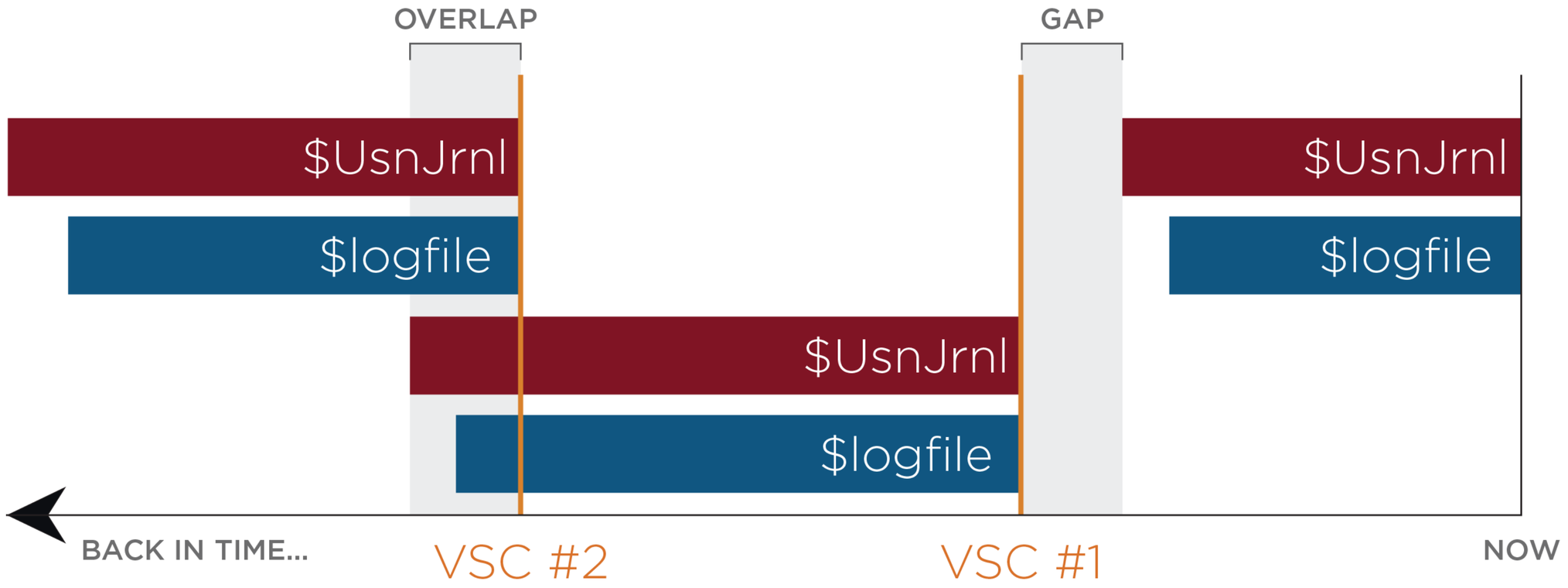
Introducing… NTFS-Linker!

- http://strozfriedberg.github.io/ntfs-linker
- Parses $MFT, $UsnJrnl, $Logfile
- Produces a uniform timeline of filesystem activity.
- Sqlite output.
- Open source, LGPLv3.
- C++
- *Alpha!*

Demo Time

<hold breath>

Reasoning Historically



Handling Overlaps

- Detect duplicate entries between different versions of $UsnJrnl/$Logfile
- Compare timestamps to VSC timestamp
- Delete events from more recent version; use the current VSC's version.

Mind the gap!

- If $UsnJrnl/$Logfile do not project back in time far enough to reach last VSC, there's a gap in our knowledge of the changes.
- $MFT from VSC allows for resync'ing, so that prevents parent folder errors from creeping in.
- But, there are windows of activity that cannot be accounted for. Don't assert something didn't happen just because it isn't present in the events.

Release Information

- Website: http://strozfriedberg.github.io/ntfs-linker
- Windows build
- Requires TSK 4.3 ☺
- Please report issues & feature requests on github.
- Remember: it’s alpha.

We're Hiring

Stroz Friedberg is hiring *Digital Forensics* & *Incident Response* professionals across the firm!

www.strozfriedberg.com/careers

@StrozCareers

- ✓ **DATA BREACH**
- ✓ **IP THEFT**
- ✓ **ADVANCED PERSISTENT THREAT**
- ✓ **MOBILE FORENSICS**
- ✓ **MALICIOUS CODE**
- ✓ **ELECTRONIC FORGERY**
- ✓ **SPYWARE**

T S R E U E T K H

THANK YOU

STROZ FRIEDBERG 10/28/2015 strozfriedberg.com