508.5 - Advanced Adversary and Anti-Forensics Detection

[Anti-Forensics Overview](#_Toc122086328) 5-6

[Common anti-forensics](#_Toc122086329) 5-6

[Recovery of Deleted files via VSS](#_Toc122086330) 9-17

[Overview/history](#_Toc122086331) 9

[Technical information](#_Toc122086561) 10

[ScopeSnapshots](#_Toc122086562) 10

[Volume shadow examination overview](#_Toc122086563) 11-16

[Overview](#_Toc122087138) 11-12

[‘vshadowinfo’ - List available snapshots](#_Toc122087139) 13

[‘vshadowmount’ - Mount VSS drive](#_Toc122087140) 14-15

[Auto mount snapshots remotely](#_Toc122087868) 16

[VSS Examination with log2timeline.py](#_Toc122087869) 17

[psort deduplication](#_Toc122087870) 17

[Advanced NTFS Tactics](#_Toc122088744) 21

[History](#_Toc122088745) 21-22

[NTFS features](#_Toc122088746) 23

[Master File Table (MFT)](#_Toc122088747) 25-34

[Overview](#_Toc122088748) 25

[MFT entries](#_Toc122088749) 26

[System files](#_Toc122088750) 26-29

[$Bitmap](#_Toc122088751) 26

[$MFT, $MFTMIRR, $LOGFILE, $VOLUME, $ATTRDEF, $BOOT, $BADCLAUS, $SECURE, $UPCASE, $EXTEND](#_Toc122088752) 27-29

[Allocated vs. unallocated](#_Toc122093325) 30

[Sequential MFT entries](#_Toc122093326) 31

[Typical MFT entry attributes](#_Toc122093327) 32

[MFT entry overview](#_Toc122093328) 33-34

[MFT Analysis](#_Toc122093329) 35-55

[‘istat’ - Sleuth Kit](#_Toc122093330) 35-37

[Analyzing filesystem metadata](#_Toc122093331) 35-36

[Analyzing header & $STANDARD\_INFORMATION](#_Toc122093616) 37-40

[Bit breakdown](#_Toc122093617) 38-39

[MFT file signature, Fixup array, $LogFile, Sequence number, Hard link count, FILE RECORD Size, Extended Records](#_Toc122093618) 38

[Next available ID, Fixup information](#_Toc122093619) 39

[$STANDARD\_INFORMATION Attribute](#_Toc122093620) 39-40

[MACB](#_Toc122093621) 40

[Attribute flags](#_Toc122093622) 40

[Tracking numbers ($Secure, $Quota, $UsnJrnl)](#_Toc122093623) 40

[Analyzing $FILE\_NAME & Attributes](#_Toc122094705) 41-43

[Summary](#_Toc122094706) 41

[$FILE\_NAME Attribute](#_Toc122094707) 41-43

[Time rules (Cheatsheets)](#_Toc122094708) 44-45

[$STANDARD\_INFORMATION](#_Toc122094709) 44

[$FILENAME](#_Toc122094710) 45

[Detecting timestamp manipulation](#_Toc122096763) 46-48

[Overview](#_Toc122096764) 46

[Techniques](#_Toc122096765) 47

[Example](#_Toc122096766) 48

[Analyzing $DATA](#_Toc122096767) 49-52

[Overview](#_Toc122096768) 49

[$DATA Attribute](#_Toc122096769) 50

[ADS – Alternate Data Streams](#_Toc122096770) 51-52

[‘icat’ – Extracting data from MFT](#_Toc122096771) 53

[Zone.Identifier ADS (evidence of download)](#_Toc122096772) 54-55

[Filename analysis layer](#_Toc122096773) 56-57

[Filenames & directory metadata](#_Toc122096774) 56-57

[$I30 – NTFS Directory Attributes](#_Toc122096775) 57

[Directory slack](#_Toc122096776) 56

[B-tree Index Searching](#_Toc122096777) 58-60

[Overview](#_Toc122096778) 58

[Index data carving](#_Toc122096779) 59

[$I30 Index Breakdown](#_Toc122096780) 59-60

[B-tree Index Rebalancing](#_Toc122096781) 61-62

[Parsing $I30 directory indexes](#_Toc122096782) 63-64

[Indx2csv, Indxparse.py, Velociraptor](#_Toc122096783) 63-64

[Filesystem journaling](#_Toc122096784) 65-81

[Overview](#_Toc122096785) 65

[$LogFile – Filesystem resilience](#_Toc122096786) 66-67

[$UsnJrnl – Change Tracking](#_Toc122096787) 68-69

[Common activity patterns](#_Toc122096788) 70-74

[Overview](#_Toc122096789) 70

[Patterns](#_Toc122096790) 71-72

[$UsnJrnl “Reason” codes](#_Toc122096791) 73

[$LogFile Operation Codes](#_Toc122096792) 74

[Useful filters and Searches](#_Toc122096793) 75-76

[LogFileParser.exe - $LogFile analysis](#_Toc122096794) 77-78

[‘MFTECmd.exe’ - $UsnJrnl analysis](#_Toc122096795) 79-80

[What happens when a file is deleted?](#_Toc122096796) 81

[Advanced Evidence Recovery](#_Toc122099088) 83-

[Overview](#_Toc122099089) 84

[File wiping](#_Toc122099090) 85-91

[SDelete example](#_Toc122099091) 85

[Other wipers](#_Toc122099092) 87-91

[BCWipe](#_Toc122099093) 88-89

[Eraser](#_Toc122099094) 90

[Cipher.exe](#_Toc122099095) 90-91

[Registry](#_Toc122099096) 92-93

[Record recovery](#_Toc122099097) 92

[Finding ‘fileless’ malware in registry](#_Toc122099098) 93

[File Recovery](#_Toc122099099) 94-98

[Metadata method vs. Carving method](#_Toc122099100) 94-95

[‘icat’ - Metadata method](#_Toc122099101) 96

[‘PhotoRec’ – Carving method](#_Toc122099102) 97-98

[Recovering Volume Shadows](#_Toc122099103) 99-102

[Overview](#_Toc122099104) 99

[Carving for VSS in SIFT](#_Toc122099105) 100-101

[‘vss\_carver’ – Example](#_Toc122099106) 102

[Event log & Filesystem stream carving](#_Toc122099107) 103-105

[‘Bulk extractor’ – Windows log carving](#_Toc122099108) 103-104

[‘blkls’ – Exctract/present unallocated clusters](#_Toc122099109) 104-105

[‘EVTXtract’ – Extract raw XML events](#_Toc122099110) 105

[Carving for strings](#_Toc122099111) 106-107

[Defensive Countermeasures](#_Toc122099112) 108-111

[Leverage filesystem history](#_Toc122099113) 109-110

[VSS](#_Toc122099114) 109

[$LogFile](#_Toc122099115) 109

[USN](#_Toc122099116) 110

[Monitoring admin tools](#_Toc122099117) 110

[Level up logging](#_Toc122099118) 111

# Anti-Forensics Overview

## Common anti-forensics

# Recovery of Deleted files via VSS

## Overview/history

## Technical information

### ScopeSnapshots

## Volume shadow examination

### Overview

### ‘vshadowinfo’ - List available snapshots

### ‘vshadowmount’ - Mount VSS drive

### Auto mount snapshots remotely

## VSS Examination with log2timeline.py

### psort deduplication

# Advanced NTFS Tactics

## History

## NTFS features

## Master File Table (MFT)

### Overview

### MFT entries

### System files

#### $Bitmap

#### $MFT, $MFTMIRR, $LOGFILE, $VOLUME, $ATTRDEF, $BOOT, $BADCLAUS, $SECURE, $UPCASE, $EXTEND

### Allocated vs. unallocated

### Sequential MFT entries

### Typical MFT entry attributes

### MFT entry overview

## MFT Analysis

### ‘istat’ - Sleuth Kit

#### Analyzing filesystem metadata

#### Analyzing header & $STANDARD\_INFORMATION

###### Bit breakdown

MFT file signature, Fixup array, $LogFile, Sequence number, Hard link count, FILE RECORD Size, Extended Records

Next available ID, Fixup information

$STANDARD\_INFORMATION Attribute

MACB

Attribute flags

Tracking numbers ($Secure, $Quota, $UsnJrnl)

#### Analyzing $FILE\_NAME & Attributes

##### Summary

##### $FILE\_NAME Attribute

### Time rules (Cheatsheets)

#### $STANDARD\_INFORMATION

#### $FILENAME

### Detecting timestamp manipulation

#### Overview

#### Techniques

#### Example

### Analyzing $DATA

#### Overview

#### $DATA Attribute

#### ADS – Alternate Data Streams

### ‘icat’ – Extracting data from MFT

### Zone.Identifier ADS (evidence of download)

## Filename analysis layer

### Filenames & directory metadata

#### $I30 – NTFS Directory Attributes

#### Directory slack

### B-tree Index Searching

#### Overview

#### Index data carving

#### $I30 Index Breakdown

### B-tree Index Rebalancing

### Parsing $I30 directory indexes

#### Indx2csv, Indxparse.py, Velociraptor

## Filesystem journaling

### Overview

### $LogFile – Filesystem resilience

### $UsnJrnl – Change Tracking

### Common activity patterns

#### Overview

#### Patterns

#### $UsnJrnl “Reason” codes

#### $LogFile Operation Codes

### Useful filters and Searches

### LogFileParser.exe - $LogFile analysis

### ‘MFTECmd.exe’ - $UsnJrnl analysis

### What happens when a file is deleted?

## Advanced Evidence Recovery

### Overview

### File wiping

#### SDelete example

#### Other wipers

##### BCWipe

##### Eraser

##### Cipher.exe

### Registry

#### Record recovery

#### Finding ‘fileless’ malware in registry

### File Recovery

#### Metadata method vs. Carving method

##### ‘icat’ - Metadata method

##### ‘PhotoRec’ – Carving method

### Recovering Volume Shadows

#### Overview

#### Carving for VSS in SIFT

#### ‘vss\_carver’ – Example

### Event log & Filesystem stream carving

#### ‘Bulk extractor’ – Windows log carving

#### ‘blkls’ – Exctract/present unallocated clusters

#### ‘EVTXtract’ – Extract raw XML events

### Carving for strings

## Defensive Countermeasures

### Leverage filesystem history

#### VSS

#### $LogFile

#### USN

#### Monitoring admin tools

### Level up logging