508.4 - Timeline Analysis

[Malware Discovery](#_Toc122441686) 5-17

[Anomaly detection](#_Toc122441687) 5-17

[Temporal analysis (timelining)](#_Toc122441688) 5

[YARA patterns](#_Toc122441689) 6-8

[Overview](#_Toc122441690) 6

[Example](#_Toc122441691) 7

[yara64.exe](#_Toc122441692) 8

[Density scout – Entropy analysis](#_Toc122441693) 9-11

[Overview](#_Toc122441694) 9

[Example](#_Toc122441695) 11

[sigcheck.exe – Signature checking](#_Toc122441696) 12-13

[Overview](#_Toc122441697) 12

[VirusTotal checking with sigcheck](#_Toc122441698) 13

[capa – Enumerate Malware Capabilities](#_Toc122441699) 14-16

[Overview](#_Toc122441700) 14

[Usage](#_Toc122441701) 15

[Example](#_Toc122441702) 16

[Putting it all together](#_Toc122441703) 17

[Timeline Analysis](#_Toc122441704) 19-116

[Timeline analysis overview](#_Toc122441705) 22-47

[Benefits](#_Toc122441706) 22

[Utopia vs. Reality](#_Toc122441707) 23-24

[Windows Forensic Trinity](#_Toc122441708) 25

[FS metadata, Windows artifacts, Registry](#_Toc122441709) 25

[Windows Forensics Artifact Review](#_Toc122441710) 26-42

[The pivot point](#_Toc122441711) 43-44

[Temporal proximity](#_Toc122441712) 43

[How do you find the pivot point?](#_Toc122441713) 44

[Timeline context clues](#_Toc122441714) 45

[Timeline tool capabilities](#_Toc122441715) 46

[fls, MFTECmd and Supertimeline](#_Toc122441716) 46

[Timeline analysis process](#_Toc122441717) 47

[Filesystem timelining](#_Toc122441718) 50-62

[MACB](#_Toc122441719) 50

[FAT time vs NFTS time](#_Toc122441720) 51

[Windows time rules cheatsheet](#_Toc122441721) 52

[Time rule exceptions](#_Toc122441722) 54

[Lateral movement time rule example](#_Toc122441723) 55

[Understanding filesystem timeline format](#_Toc122441724) 56-57

[How-to: Creating triage timeline](#_Toc122441725) 58-62

[Creating triage timeline step 1: Bodyfile](#_Toc122441726) 58-60

[MFTECmd.exe](#_Toc122441727) 58-59

[fls](#_Toc122441728) 60

[Creating triage timeline step 2: mactime](#_Toc122441729) 61-62

[Super Timeline](#_Toc122441730) 66-82

[Oveview](#_Toc122441731) 66

[Lateral movement example](#_Toc122441732) 68

[Malware installation example](#_Toc122441733) 70

[Plaso & log2timeline.py](#_Toc122441734) 72-82

[Overview](#_Toc122441735) 72

[Plaso parsers](#_Toc122441736) 73-79

[Windows parsers (win\_gen, winxp, win7)](#_Toc122441737) 73-74

[Registry parsers (winreg)](#_Toc122441738) 75-76

[Webhistory parsers (webhist)](#_Toc122441739) 77

[Linux/Android/Mac parsers](#_Toc122441740) 78-79

[log2timeline.py usage](#_Toc122441741) 80-82

[Overview](#_Toc122441742) 80

[Examples](#_Toc122441743) 82

[Targeted Super Timeline creation](#_Toc122441744) 85-91

[Overview](#_Toc122441745) 85-86

[log2timeline.py](#_Toc122441746) 87-89

[Parser presets](#_Toc122441747) 87

[Filter files](#_Toc122441748) 88-89

[Triage artifacts list](#_Toc122441749) 90

[Triage image timelining](#_Toc122441750) 91

[Filtering the Super Timeline](#_Toc122441751) 94-102

[‘pinfo.py’ – Plaso database info](#_Toc122441752) 94-98

[‘psort.py’ – Filtering timeline](#_Toc122441753) 99-100

[Web server intrusion example](#_Toc122441754) 101

[Remote timeline creation example](#_Toc122441755) 102

[Super Timeline analysis](#_Toc122441756) 105-116

[Timeline output (CSV)](#_Toc122441757) 105-108

[Recommended columns](#_Toc122441758) 109

[Timeline Explorer](#_Toc122441759) 111-112

[Timeline analysis process](#_Toc122441760) 113

[Scaling timeline analysis](#_Toc122441761) 116

[yara\_match.py](#_Toc122441762) 116

[Splunk](#_Toc122441763) 116

[ELK](#_Toc122441764) 116

# Malware Discovery

## Anomaly detection

### Temporal analysis (timelining)

### YARA patterns

#### Overview

#### Example

#### yara64.exe

### Density scout – Entropy analysis

#### Overview

#### Example

### sigcheck.exe – Signature checking

#### Overview

#### VirusTotal checking with sigcheck

### capa – Enumerate Malware Capabilities

#### Overview

#### Usage

#### Example

### Putting it all together

# Timeline Analysis

## Timeline analysis overview

### Benefits

### Utopia vs. Reality

### Windows Forensic Trinity

#### FS metadata, Windows artifacts, Registry

### Windows Forensics Artifact Review

### The pivot point

#### Temporal proximity

#### How do you find the pivot point?

### Timeline context clues

### Timeline tool capabilities

#### fls, MFTECmd and Supertimeline

### Timeline analysis process

## Filesystem timelining

### MACB

### FAT time vs NFTS time

### Windows time rules cheatsheet

### Time rule exceptions

### Lateral movement time rule example

### Understanding filesystem timeline format

### How-to: Creating triage timeline

#### Creating triage timeline step 1: Bodyfile

##### MFTECmd.exe

##### fls

#### Creating triage timeline step 2: mactime

## Super Timeline

### Oveview

### Lateral movement example

### Malware installation example

### Plaso & log2timeline.py

#### Overview

#### Plaso parsers

##### Windows parsers (win\_gen, winxp, win7)

##### Registry parsers (winreg)

##### Webhistory parsers (webhist)

##### Linux/Android/Mac parsers

#### log2timeline.py usage

##### Overview

##### Examples

## Targeted Super Timeline creation

### Overview

### log2timeline.py

#### Parser presets

#### Filter files

### Triage artifacts list

### Triage image timelining

## Filtering the Super Timeline

### ‘pinfo.py’ – Plaso database info

### ‘psort.py’ – Filtering timeline

### Web server intrusion example

### Remote timeline creation example

## Super Timeline analysis

### Timeline output (CSV)

### Recommended columns

### Timeline Explorer

### Timeline analysis process

### Scaling timeline analysis

#### yara\_match.py

#### Splunk

#### ELK