

508.4 – Timeline Analysis

Malware Discovery..... 5-17

Anomaly detection 5-17

Temporal analysis (timelining)5

YARA patterns..... 6-8

Overview6

Example.....7

yara64.exe.....8

Densityscout – Entropy analysis..... 9-11

Overview9

Example.....11

sigcheck.exe – Signature checking 12-13

Overview12

VirusTotal checking with sigcheck.....13

capa – Enumerate Malware Capabilities..... 14-16

Overview14

Usage15

Example.....16

Putting it all together.....17

Timeline Analysis..... 19-116

Timeline analysis overview 22-47

Benefits.....22

Utopia vs. Reality..... 23-24

Windows Forensic Trinity.....25

FS metadata, Windows artifacts, Registry.....25

Windows Forensics Artifact Review 26-42

The pivot point 43-44

Temporal proximity.....43

How do you find the pivot point?44

Timeline context dues.....45

Timeline tool capabilities46

fls, MFTECmd and Supertimeline.....46

Timeline analysis process47

Filesystem timelining.....50-62

MACB50

FAT time vs NFTS time.....51

Windows time rules cheatsheet.....52

Time rule exceptions54

Lateral movement time rule example.....55

Understanding filesystem timeline format..... 56-57

How-to: Creating triage timeline..... 58-62

Creating triage timeline step 1: Bodyfile.....58-60

MFTECmd.exe58-59

fls.....60

Creating triage timeline step 2: mactime61-62

Super Timeline..... 66-82

Overview.....66

Lateral movement example68

Malware installation example.....70

Plaso & log2timeline.py..... 72-82

Overview72

Plaso parsers.....73-79

Windows parsers (win_gen, winxp, win7).....73-74

Registry parsers (winreg).....75-76

Webhistory parsers (webhist).....77

Linux/Android/Mac parsers78-79

log2timeline.py usage80-82

Overview80

Examples82

Targeted Super Timeline creation 85-91

Overview..... 85-86

log2timeline.py..... 87-89

Parser presets87

Filter files.....88-89

Triage artifacts list.....90

Triage image timelining.....91

Filtering the Super Timeline.....94-102

‘pinfo.py’ – Plaso database info 94-98

‘psort.py’ – Filtering timeline 99-100

Web server intrusion example101

Remote timeline creation example.....102

Super Timeline analysis.....	105-116
Timeline output (CSV)	105-108
Recommended columns.....	109
Timeline Explorer.....	111-112
Timeline analysis process	113
Scaling timeline analysis.....	116
yara_match.py	116
Splunk	116
ELK.....	116