

IR Timeline Analysis

Walkthrough of the challenge room

Paweł Murdzek, Piotr Szewczyk

Warsaw University of Technology

January 26, 2026

Contents

Introduction	2
1. Lab Description	2
2. Timelines with Log2Timeline	2
2.1. Section Description	2
2.2. Analysis and Answers	2
3. Timeline Analysis with Timesketch	2
4. Timeline Analysis Practical	2
4.1. Conclusions	3

Introduction

This document constitutes a walkthrough for the "IR Timeline Analysis" challenge category on the Try-HackMe platform.

1. Lab Description

The lab aims to teach how to use tools for incident timeline analysis.

2. Timelines with Log2Timeline

2.1. Section Description

The task involved using the Log2Timeline tool to recreate basic information and the incident timeline.

2.2. Analysis and Answers

1. What option can be used with Log2Timeline to indicate the timeline output file?

Answer: -storage-file

2. Based on the Jimmy_timeline.plaso file, how many event sources are parsed after running pinfo.py against the storage file?

Command used: pinfo.py Jimmy_timeline.plaso | more

Answer: 4982

3. On the same timeline file, how many events were generated for the firefox_history?

Answer: 50

4. Based on the B4DM755 timeline, what time was the interview.txt file created? (hh:mm:ss)

Commands:

— log2timeline.py -storage-file Forensic_Image_b4dm755.plaso Forensic_Image_b4dm755.E01
— psort.py -o dynamic -w Forensic_Image_b4dm755.csv Forensic_Image_b4dm755.plaso

— grep -i "interview.txt" Forensic_Image_b4dm755.csv | grep "Creation Time"

Answer: 14:02:34

3. Timeline Analysis with Timesketch

— How many data types were in the Jimmy Supertimeline sketch?

Answer: 48

— How many entries were in the EVTX Gap Analysis under the Jimmy Supertimeline?

The EVTX analyzer report gives us:

Answer: 34870

— Which search engine did Jimmy Wilson use to search for "how to disappear without a trace?"

Answer: Bing

— What is the path of the program that was called to initiate Microsoft Antimalware Service?

Answer: C:\Program Files\Microsoft Security Client\MsMpEng.exe

4. Timeline Analysis Practical

— How many event sources were identified?

Command: pinfo.py Timeline_Challenge.plaso | more

Answer: 189100

— How many events were generated from the dpkg parser?

Answer: 14718

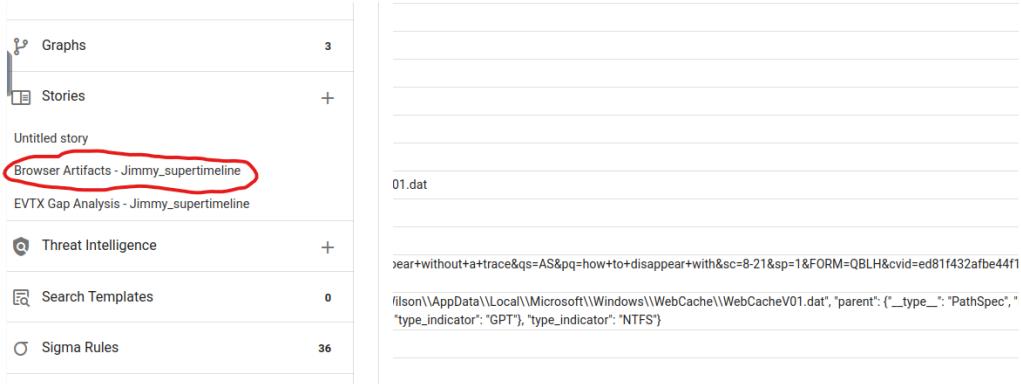


Figure 1: Browsing report.

- **How many total tags were set?**

Command: `psort.py -o null -analysis tagging -tagging-file tag_linux.txt Timeline_Challenge.plaso`
Answer: 5408

- **What is the highest tagged element?**

Answer: login_failed

- **Under which username does the cronjob that executes app.py run?**

Answer: smokey

- **What is the hash of the successful SSH login with the PID 1669?**

Answer: a2407e0f3c80d01d2369f15e2b8aa279e790eaa0b1d20ab71cd35c2c7f5aee71

4.1. Conclusions

During this lab, we learned how to read artifacts from a timeline using Log2Timeline, as well as other information using the Timesketch tool. Then we approached the challenge, where we applied the acquired skills in practice and found some information about SSH login.

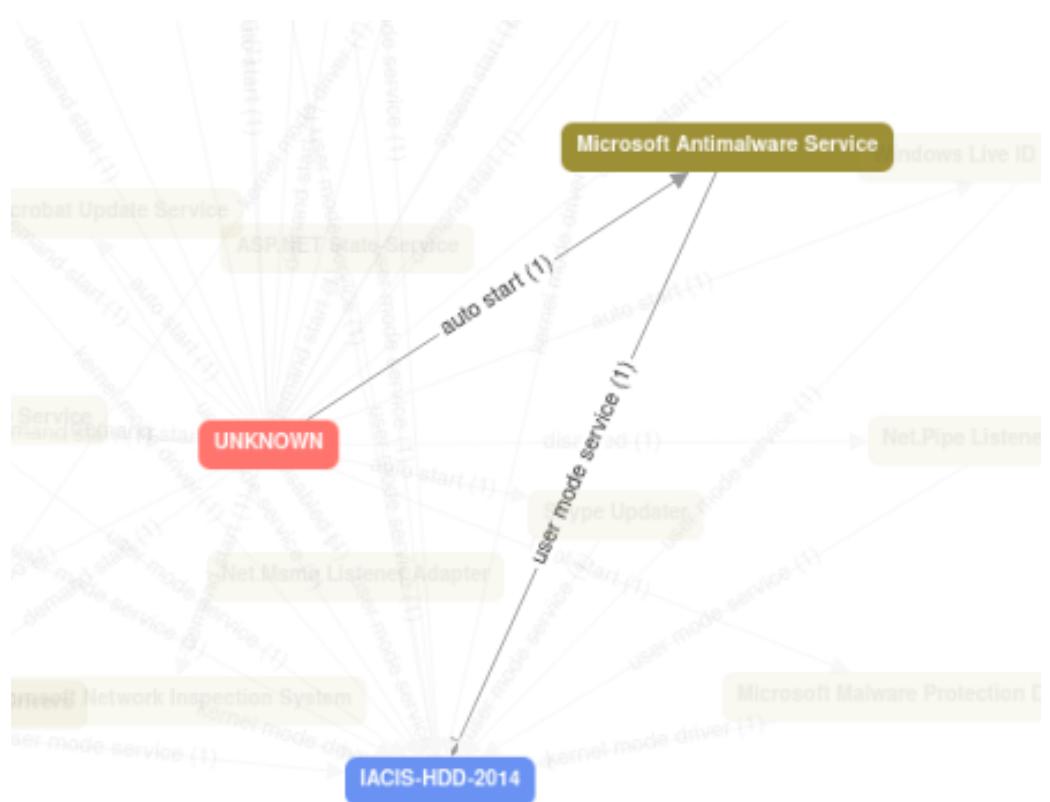


Figure 2: Graph with the service of interest.

```

analyst@ip-10-67-128-154: ~/Desktop/Timelines/Task6
File Edit View Search Terminal Help
Total          0          0          0          0
824802
Identifier      PID      Status      Memory      Events
Tags           Reports
Main           2975    finalizing    189.3 MiB    824802 (0)
5408 (0)        1 (0)
tagging         2978    completed     88.6 MiB    824802 (549)
5408 (6)        1 (1)

Processing completed.

***** Analysis report: tagging *****
Date and time : 2026-01-19T22:44:26.000000+00:00
Event filter : N/A
Results :
: application_execution: 82
: application_install: 1990
: boot: 26
: device_connection: 144
: device_disconnection: 16
: event_tags: 5408
: groupadd: 24
: groupdel: 4
: login: 190
: login_failed: 2454
: logout: 220
: runlevel: 24
: session_start: 120
: session_stop: 88
: shutdown: 2
: useradd: 20
: userdel: 4
-----
analyst@ip-10-67-128-154:~/Desktop/Timelines/Task6$ ^C

```

Figure 3: Result of Linux tags analysis.

Saved Searches 0

Data Types 8

- fs:stat (360.8K)
- syslog:line (21.9K)
- systemd:journal (20.3K)
- linux:dpkg_log:entry (7.2K)
- linux:utmp:event (1.7K)
- linux:apt_history_log:entry (36)
- syslog:sshd:login (29)
- syslog:cron:task_run (19)**

Tags 0

Graphs 3

Timeline Events (8.0002s)

Rows per page: 40 1-19 of 19

) ↓ message

2026-03-02T26:29.000Z Cron ran: /usr/bin/python3 /var/opt/app/app.py Timeline_Challenge

(smokey) CMD (/usr/bin/python3 /var/opt/app/app.py)
/usr/bin/python3 /var/opt/app/app.py
syslog:cron:task_run
2022-03-02T26:29.000000+00:00
EXT:/var/log/syslog.1
biblioteca
Cron ran: /usr/bin/python3 /var/opt/app/app.py for user **smokey** pid: 730

{
"__type__": "PathSpec", "inode": 19857, "location": "/var/log/syslog.1", "parent":
"__type__": "PathSpec", "volume_index": 0, "location": "/lvm1", "parent":
"__type__": "PathSpec", "location": "/p3", "parent": {"__type__": "PathSpec",
"parent": {"__type__": "PathSpec", "location": "/home/securitynomad/Desktop/
Forensics-Timeline/Timeline_Challenge.dd", "type_indicator": "OST"},
"type_indicator": "RAW"}, "type_indicator": "GPT"}, "type_indicator": "LVM"},

Figure 4: Finding the app.py call.

The screenshot shows a log analysis interface with a sidebar on the left containing various data types and search filters, and a main pane on the right displaying a specific log entry.

Left Sidebar (Data Types):

- Timelines: 1
- Saved Searches: 0
- Data Types: 8
 - fs.stat (560.8K)
 - syslog.line (21.9K)
 - systemd.journal (20.3K)
 - linux.dpkg_log_entry (7.2K)
 - linux.utmp.event (1.7K)
 - linuxapt_history.logentry (98)
 - syslog.ssh.login (29) (29)
 - syslog.cron.task_run (19)
- Tags: 0
- Graphs: 3
- Stories: +
- Threat Intelligence: +

Main Pane (Log Entry):

471 days	
2024-03-27T06:15:47.000Z	Successful login of user: smokey from 10.10.147.234 port 39802 using authentication method: password ssh pid: 669
authentication_method	password
body	Accepted password for smokey from 10.10.147.234 port 39802 ssh
data_type	syslog.ssh.login
datetime	2024-03-27T06:15:47.000000+00:00
display_name	EXT:/var/log/auth.log
hostname	biblioteca
ip_address	10.10.147.234
message	Successful login of user: smokey from 10.10.147.234 port 39802 using authentication method: password ssh pid: 1669
path_spec	{"_type_": "PathSpec", "inode": 6633, "location": "/var/log/auth.log", "parent": {"_type_": "PathSpec", "volume_index": 0, "location": "/lvm1"}, "path": "securitynomad/Desktop/Forensics-Timeline/Timeline_Challenge.dd", "type_indicator": "OS"}, "type_indicator": "RAW", "type_indicator": "GPT"}
pid	1669
port	39802
protocol	ssh2
reporter	sshd
sha256_hash	32407ed3c80d91d2369f15e2b8aa279e790eaab1d20ab71cc35c2c7f5ee71
source_long	SSH Log
source_short	LOG
tag	[]

Figure 5: Finding the SSH login hash with PID 1669.