Optimize Making The Timeline

and yet it does move
malware.co.kr

- dorumugs -

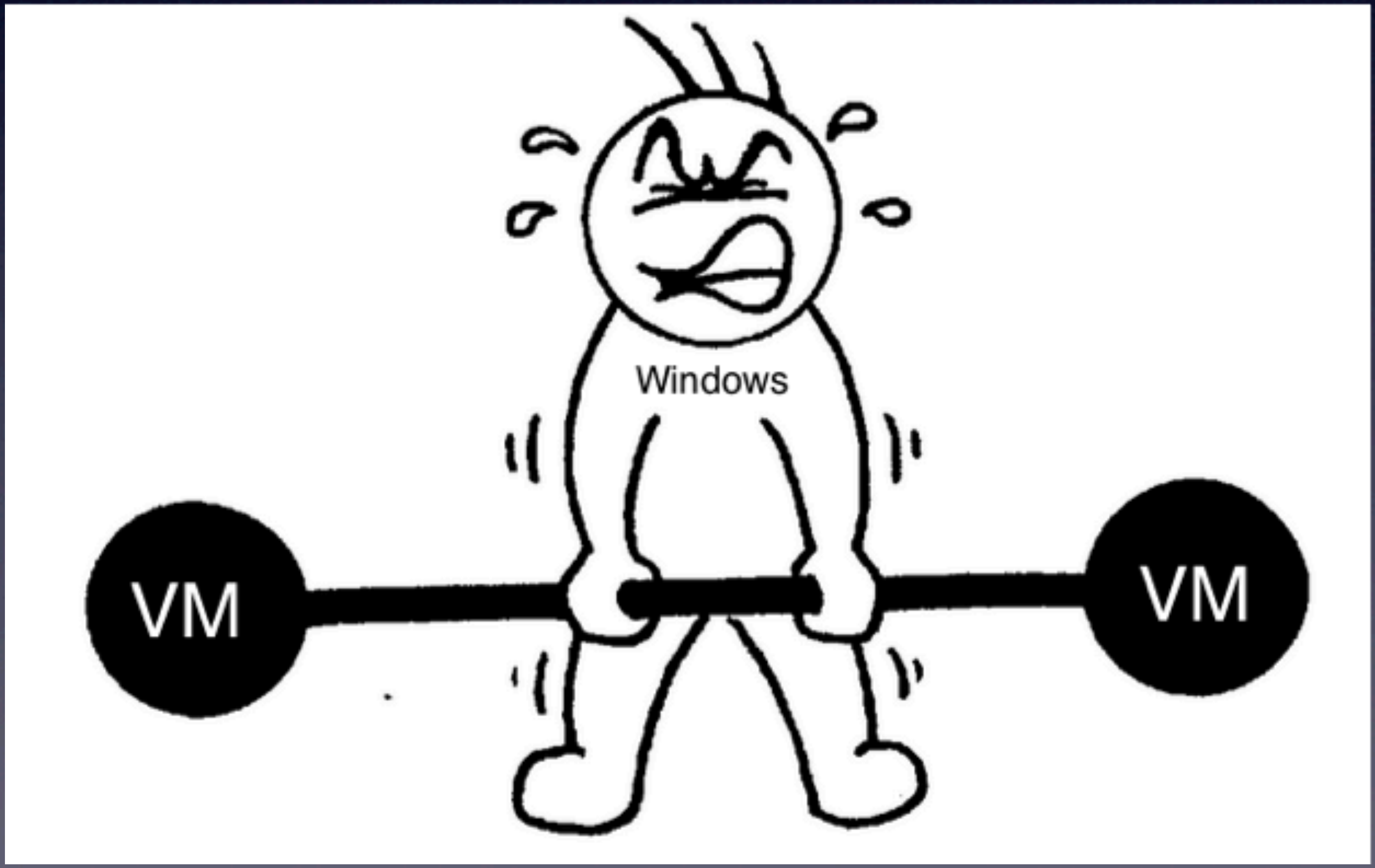
Log2Timeline

- The tool is written in Perl **for Linux**
- A framework for automatic creation of a super timeline.
- The main purpose is to provide a single tool to parse various log files and artifacts found on suspect systems.
- A timeline that can be analysed by forensic

Log2Timeline for Windows

Heavy

- When Examiner analyzes the images, VMware is heavy.



- http://katerawlings.com/2010/08/19/looking-for-heavy-metcons/

Windows Ver

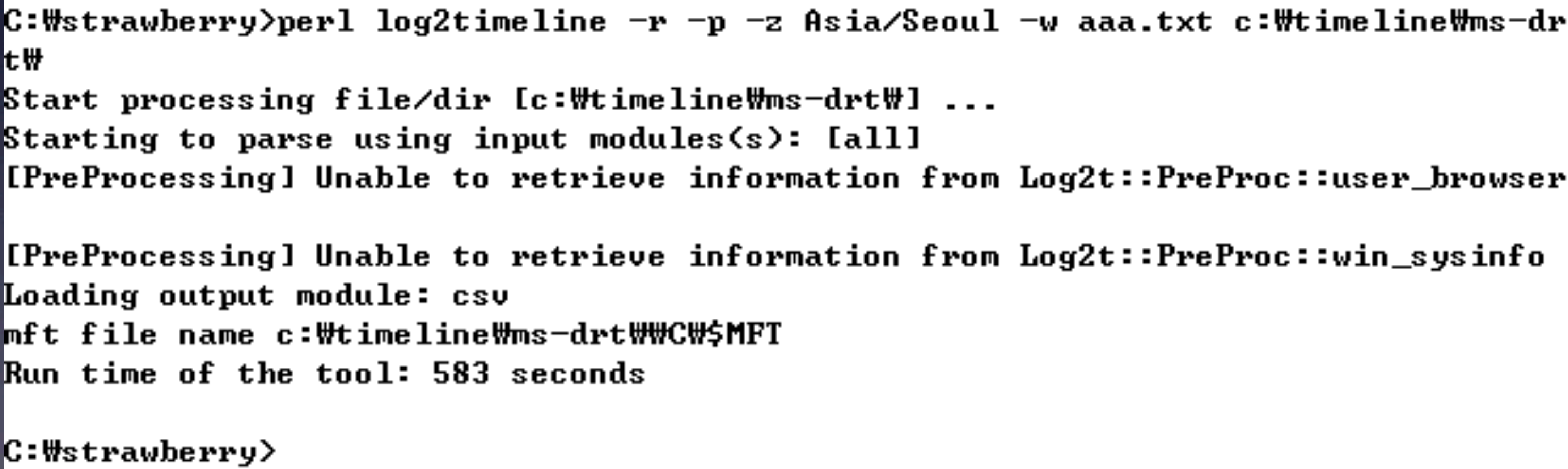
- But It is not working. because we use unicode(korean).
- http://log2timeline.net/INSTALL.txt

Fix Log2Timeline +_+

- http://fixthispcnow.webs.com/virusremovalservice.htm

Test! ^___^

- perl log2timeline.pl -r -p -z Asia/Seoul -w bodyfile c:\timeline\Image_name\



```
C:₩strawberry>perl log2timeline -r -p -z Asia/Seoul -w aaa.txt c:₩timeline₩ms-dr
t₩
Start processing file/dir [c:₩timeline₩ms-drt₩] ...
Starting to parse using input modules(s): [all]
[PreProcessing] Unable to retrieve information from Log2t::PreProc::user_browser

[PreProcessing] Unable to retrieve information from Log2t::PreProc::win_sysinfo
Loading output module: csv
mft file name c:₩timeline₩ms-drt₩₩C₩$MFT
Run time of the tool: 583 seconds

C:₩strawberry>
```

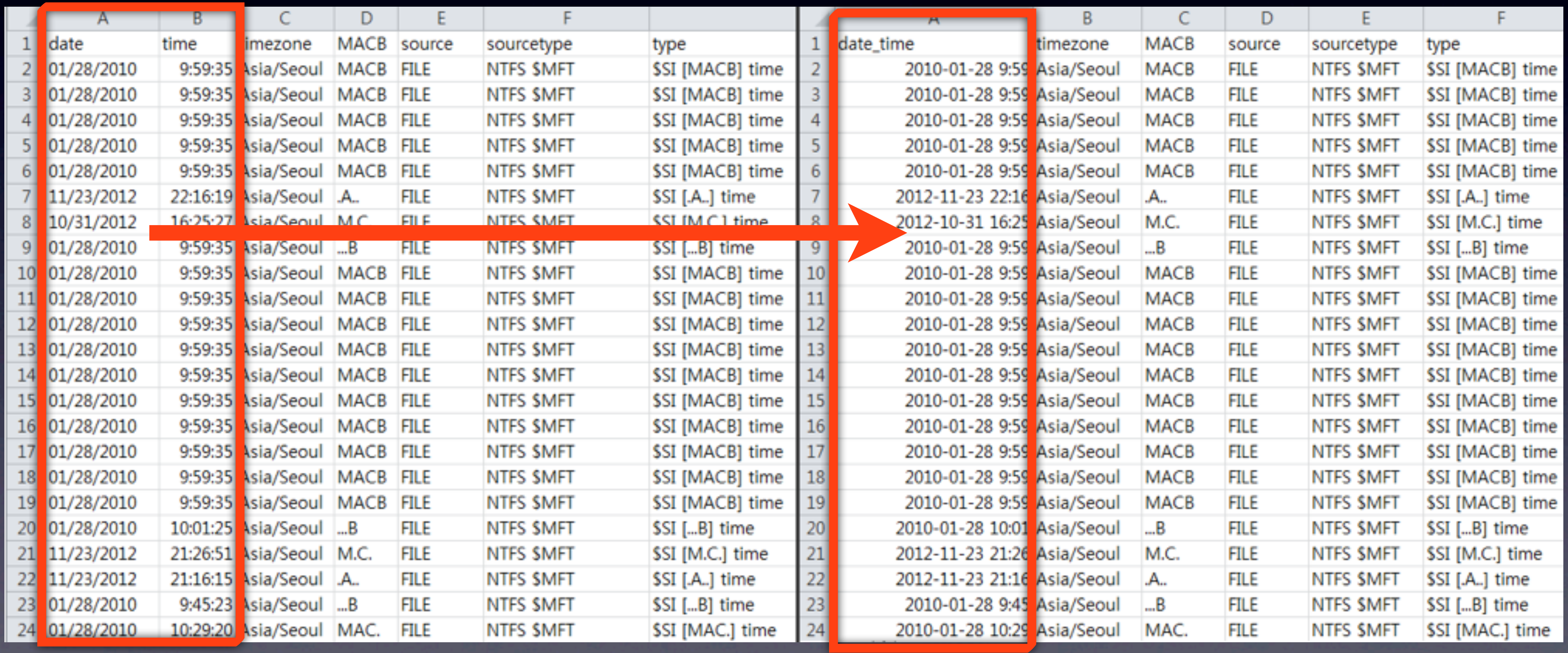
Sort T_T

l2t_process

- l2t_Process is boring. because it takes a lot of times.

- http://static4.businessinsider.com/image/4fbfb86becad044879000001-400-300/sleepy-tired-boring.jpg

Column(0) + Column(1)

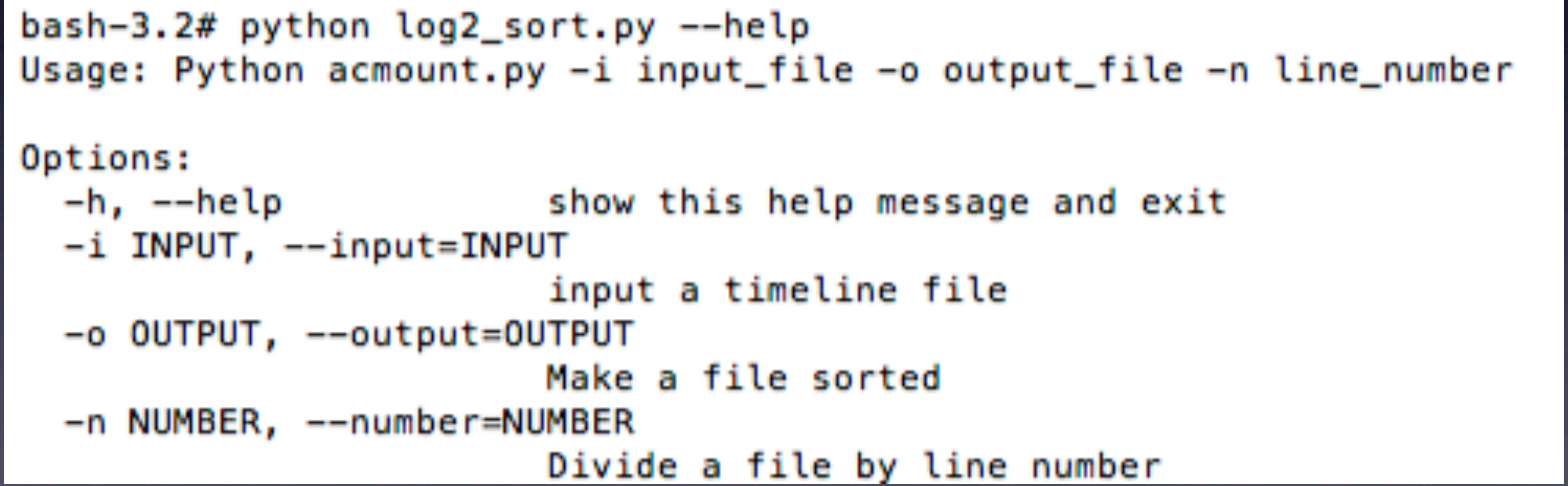


	A	B	C	D	E	F	
1	date	time	imezone	MACB	source	sourcetype	type
2	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
3	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
4	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
5	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
6	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
7	11/23/2012	22:16:19	sia/Seoul	.A..	FILE	NTFS $MFT	$SI [.A..] time
8	10/31/2012	16:25:27	sia/Seoul	M.C.	FILE	NTFS $MFT	$SI [M.C.] time
9	01/28/2010	9:59:35	sia/Seoul	...B	FILE	NTFS $MFT	$SI [...B] time
10	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
11	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
12	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
13	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
14	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
15	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
16	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
17	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
18	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
19	01/28/2010	9:59:35	sia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
20	01/28/2010	10:01:25	sia/Seoul	...B	FILE	NTFS $MFT	$SI [...B] time
21	11/23/2012	21:26:51	sia/Seoul	M.C.	FILE	NTFS $MFT	$SI [M.C.] time
22	11/23/2012	21:16:15	sia/Seoul	.A..	FILE	NTFS $MFT	$SI [.A..] time
23	01/28/2010	9:45:23	sia/Seoul	...B	FILE	NTFS $MFT	$SI [...B] time
24	01/28/2010	10:29:20	sia/Seoul	MAC.	FILE	NTFS $MFT	$SI [MAC.] time

	A	B	C	D	E	F
1	date_time	timezone	MACB	source	sourcetype	type
2	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
3	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
4	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
5	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
6	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
7	2012-11-23 22:16	Asia/Seoul	.A..	FILE	NTFS $MFT	$SI [.A..] time
8	2012-10-31 16:25	Asia/Seoul	M.C.	FILE	NTFS $MFT	$SI [M.C.] time
9	2010-01-28 9:59	Asia/Seoul	...B	FILE	NTFS $MFT	$SI [...B] time
10	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
11	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
12	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
13	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
14	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
15	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
16	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
17	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
18	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
19	2010-01-28 9:59	Asia/Seoul	MACB	FILE	NTFS $MFT	$SI [MACB] time
20	2010-01-28 10:01	Asia/Seoul	...B	FILE	NTFS $MFT	$SI [...B] time
21	2012-11-23 21:26	Asia/Seoul	M.C.	FILE	NTFS $MFT	$SI [M.C.] time
22	2012-11-23 21:16	Asia/Seoul	.A..	FILE	NTFS $MFT	$SI [.A..] time
23	2010-01-28 9:45	Asia/Seoul	...B	FILE	NTFS $MFT	$SI [...B] time
24	2010-01-28 10:29	Asia/Seoul	MAC.	FILE	NTFS $MFT	$SI [MAC.] time

Sort +_+

- Python log2_sort.py -i timeline.txt -o timelin.csv -n 1000000



```
bash-3.2# python log2_sort.py --help
Usage: Python acmount.py -i input_file -o output_file -n line_number

Options:
  -h, --help            show this help message and exit
  -i INPUT, --input=INPUT
                        input a timeline file
  -o OUTPUT, --output=OUTPUT
                        Make a file sorted
  -n NUMBER, --number=NUMBER
                        Divide a file by line number
```

Speed?

For More Speed

- Gather just necessary files
  - No change time information
  - No change folder information

Link

MFT

Prefetch

OS Artifacts

SysLog

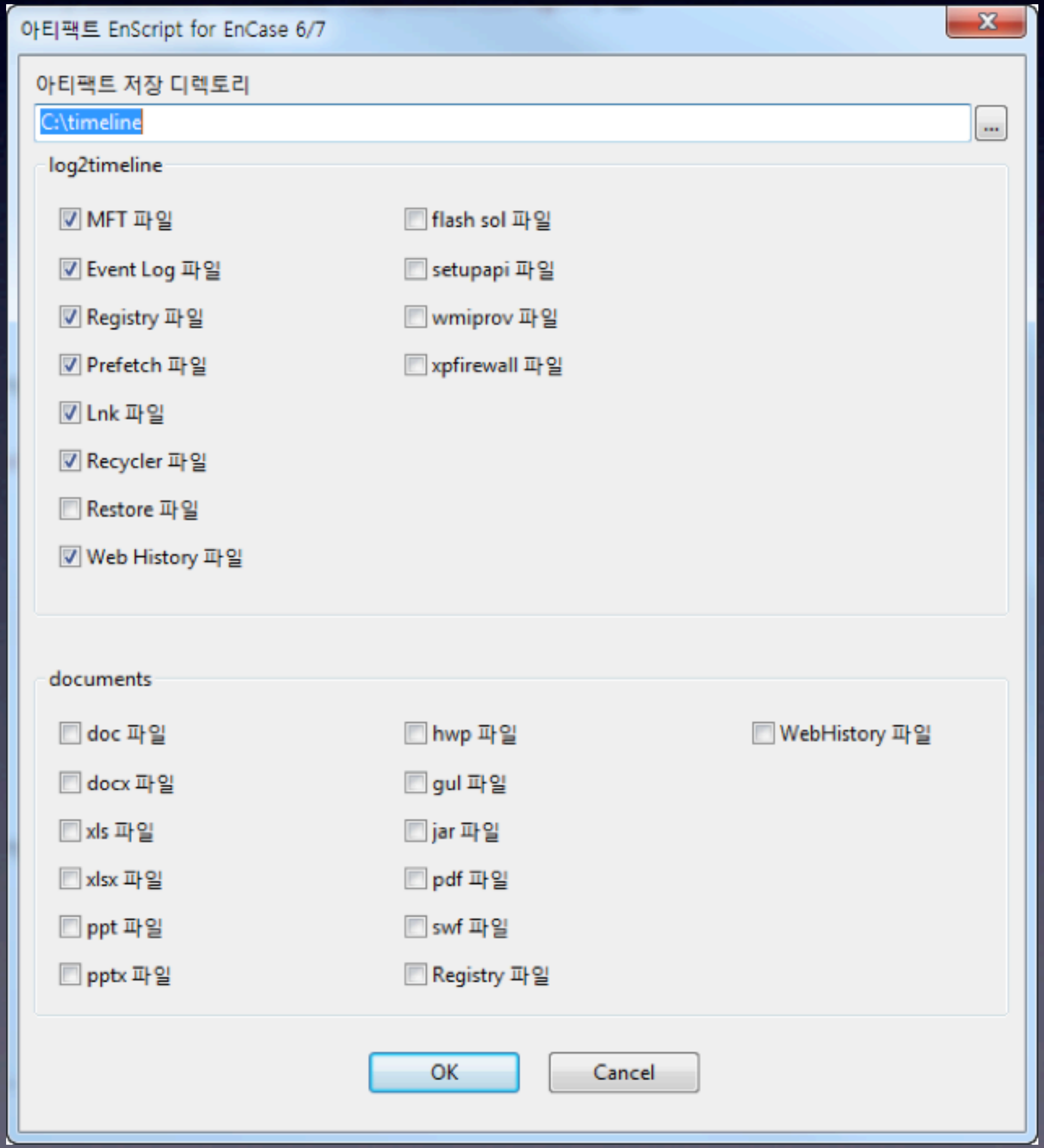
ETC

Event Log

Registry

HOW?

- EnScript is a perfect tool to gather OS artifacts.



아티팩트 EnScript for EnCase 6/7

아티팩트 저장 디렉토리

C:\timeline

log2timeline

☑ MFT 파일
☑ Event Log 파일
☑ Registry 파일
☑ Prefetch 파일
☑ Lnk 파일
☑ Recycler 파일
□ Restore 파일
☑ Web History 파일
□ flash sol 파일
□ setupapi 파일
□ wmiprov 파일
□ xpfirewall 파일

documents

□ doc 파일
□ docx 파일
□ xls 파일
□ xlsx 파일
□ ppt 파일
□ pptx 파일
□ hwp 파일
□ gul 파일
□ jar 파일
□ pdf 파일
□ swf 파일
□ Registry 파일
□ WebHistory 파일

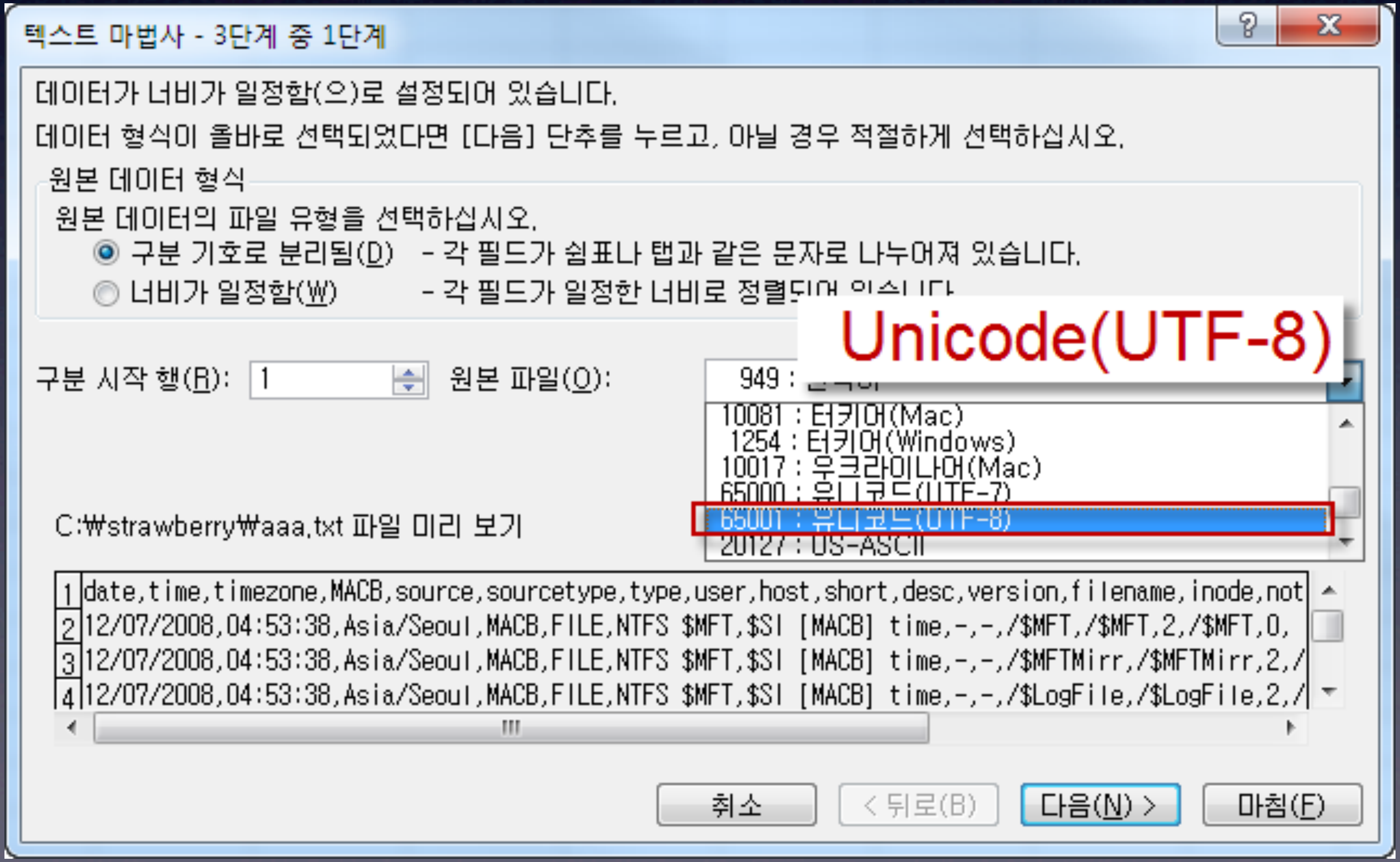
and then

- Run EnScript.
- Log2Timeline Windows ver
- Sort Bodyfile

Enjoy Timeline

But....

- If your timeline is crash, change the encoding from something to unicode.



텍스트 마법사 - 3단계 중 1단계

데이터가 너비가 일정함(으)로 설정되어 있습니다.

데이터 형식이 올바로 선택되었다면 [다음] 단추를 누르고, 아닐 경우 적절하게 선택하십시오.

원본 데이터 형식

원본 데이터의 파일 유형을 선택하십시오.

- ● 구분 기호로 분리됨(D) - 각 필드가 쉼표나 탭과 같은 문자로 나누어져 있습니다.
- ○ 너비가 일정함(W) - 각 필드가 일정한 너비로 정렬되어 있습니다.

구분 시작 행(R): 1 원본 파일(O): 949 : 한국어

Unicode(UTF-8)

C:₩strawberry₩aaa.txt 파일 미리 보기

```
date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,not
12/07/2008,04:53:38,Asia/Seoul,MACB,FILE,NTFS $MFT,$SI [MACB] time,-,-,/$MFT,/$MFT,2,/$MFT,0,
12/07/2008,04:53:38,Asia/Seoul,MACB,FILE,NTFS $MFT,$SI [MACB] time,-,-,/$MFTMirr,/$MFTMirr,2,/
12/07/2008,04:53:38,Asia/Seoul,MACB,FILE,NTFS $MFT,$SI [MACB] time,-,-,/$LogFile,/$LogFile,2,/
```

Thank you