



Extracting typing history in Unix Memory Image

forensic.nofate.com



Contents

- Introduction to bash history
- history management
- Extracting bash history
- Case study
- Conclusion



Bash

- Bourne-again shell
- GNU 프로젝트를 위해 Brian Fox가 작성한 유닉스 셸
- GNU OS, Linux, Mac OS X 기본 셸
- Cygwin이나 MinGW로 윈도우에서 사용 가능
- 명령 히스토리, 디렉터리 스택, \$RANDOM
POSIX 형식 명령어 치환, 명령어 자동 완성



Bash

- When started as an interactive login shell:
 - /etc/profile, ~/.bash_profile, ~/.bash_login, ~/.profile
- When a login shell exits : ~/.bash_logout
- When started as an interactive shell :
~/.bashrc



History Storage

- 사용자 명령어를 저장하여 추 후 해당 명령어를 바로 실행 시킬 수 있게 함
- **![HISTORY NUMBER]**
- 시간 값은 정의되어 있지 않으며, 실행한 명령어를 ~/.bash_history에 순차적으로 기록
- Mac OS X는 500개의 히스토리를 기록



History Storage

- The history list is an array of history entries

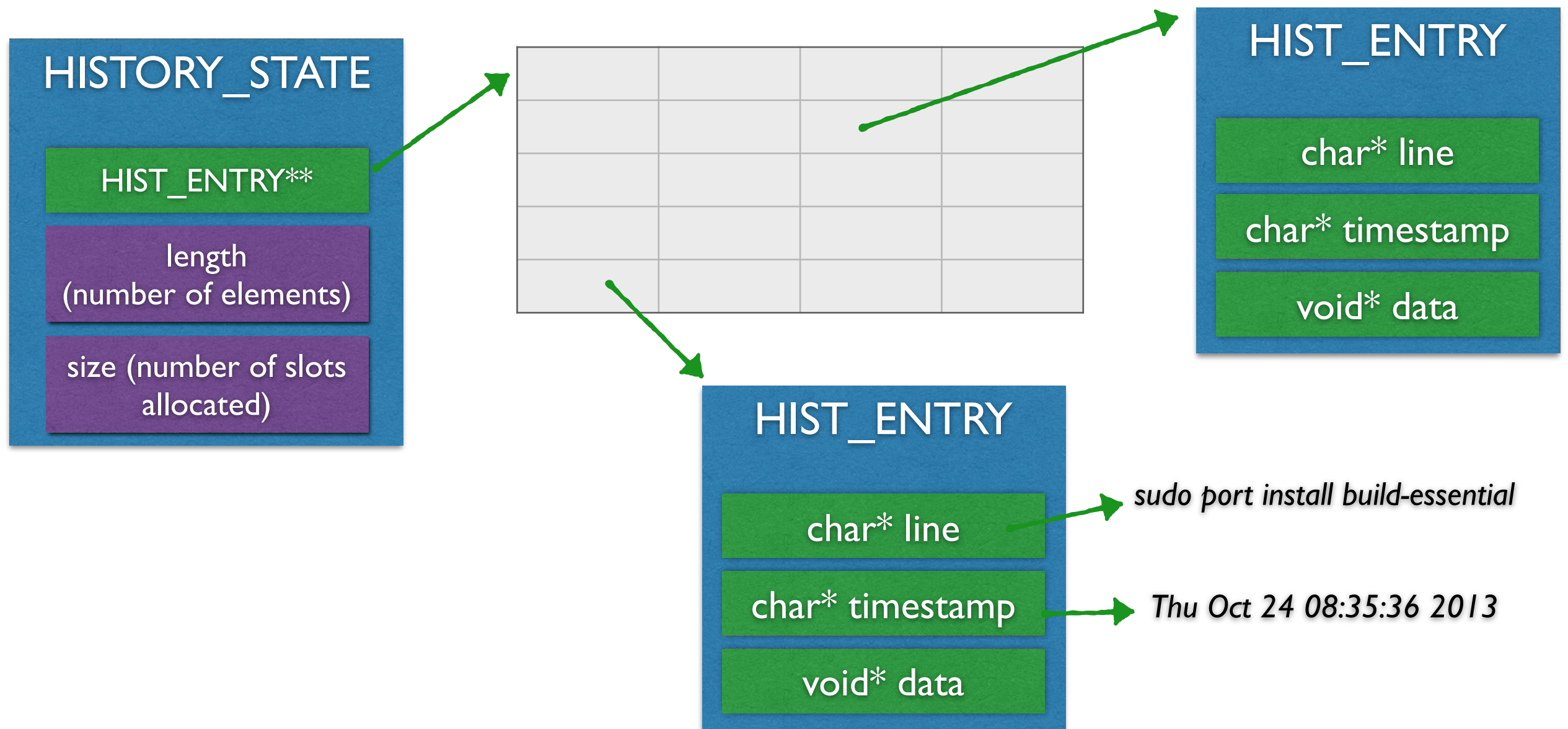
```
typedef void * histdata_t;  
  
typedef struct _hist_entry {  
    char *line;  
    char *timestamp;  
    histdata_t data;  
} HIST_ENTRY;
```

reference : <http://linux.die.net/man/3/history>

```
/*  
 * A structure used to pass around the current state of the history.  
 */  
typedef struct _hist_state {  
    HIST_ENTRY **entries; /* Pointer to the entries themselves. */  
    int offset;           /* The location pointer within this array. */  
    int length;           /* Number of elements within this array. */  
    int size;             /* Number of slots allocated to this array. */  
    int flags;  
} HISTORY_STATE;
```



History Storage

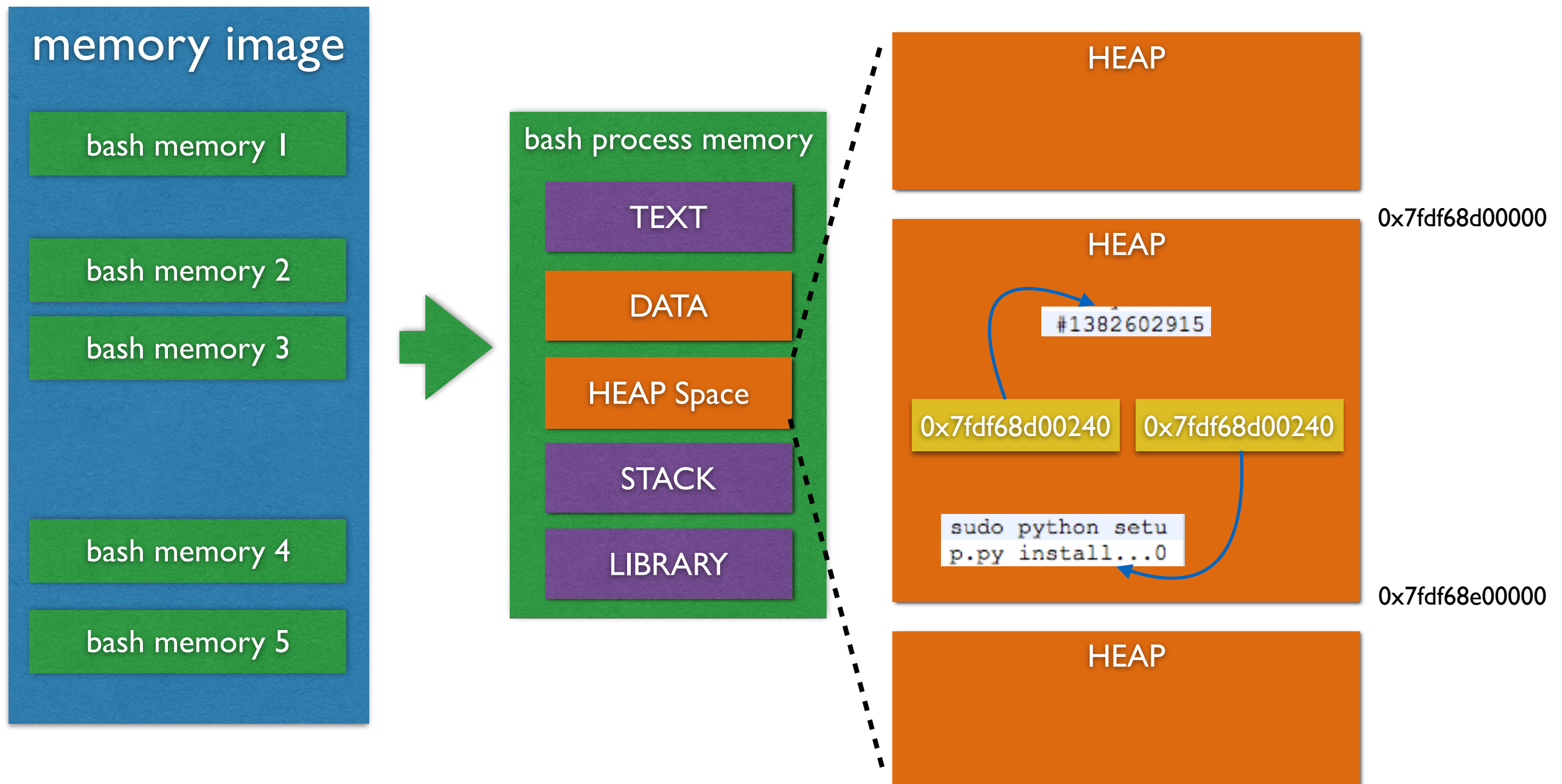




Extracting bash history

- 1. Live Forensics
 - ~/.bash_history 파일 추출
 - History Functions 이용 (GNU History library)
- 2. Memory Forensics
 - 맵핑된 history 파일 추출
 - bash 프로세스 영역에서 HIST_ENTRY 추출

Extracting bash history



Extracting bash history



- DEMO



Case Study

- 히스토리 타임스탬프 대부분이 동일한 이유
- `history -c` 명령 이 후에도 추출 가능한가
- 원격 접속 세션에서 `history -c` 실행



Case Study

- 히스토리 타임스탬프 대부분이 동일한 이유?
 - 히스토리 파일에 시간 정보가 없음
 - 프로세스가 히스토리 파일을 로드하고, 로드 시간으로 파일 내의 모든 히스토리 시간 정보를 저장
- 즉, 신규 입력된 명령어 이전의 히스토리의 시간 정보를 명령어 실행 시간으로 오해하면 안됨.



Case Study

- 히스토리 타임스탬프 대부분이 동일한 이유?

0x6DCB74A8	11746	1	255	0	com.apple.audio.	_netbios(501,20)	(501,20) Fri Nov 15 04:45:30 2013
0x161C0C9E8	11767	1	255	0	com.apple.WebKit	_netbios(501,20)	(501,20) Fri Nov 15 04:48:47 2013
0x163B0AA80	11935	247	255	0	Terminal	chainbreaker(501,20)	(501,20) Fri Nov 15 05:19:13 2013
0x1F8E8F000	11944	11935	255	0	login	chainbreaker(0,20)	(0,20) Fri Nov 15 05:19:22 2013
0x16110E950	11945	11944	255	0	bash	chainbreaker(501,20)	(501,20) Fri Nov 15 05:19:22 2013
0x8917D7E0	11987	303	255	0	mdworker	_spotlight(89,89)	(89,89) Fri Nov 15 05:23:47 2013
0x18E5ED000	11988	11945	255	0	sudo	chainbreaker(0,20)	(0,20) Fri Nov 15 05:23:48 2013
0x87DFF748	11989	11988	255	0	osxpmem	chainbreaker(0,0)	(0,0) Fri Nov 15 05:23:48 2013
0x8657E540	11990	8781	255	0	thnuclnt	chainbreaker(501,20)	(501,20) Fri Nov 15 05:24:06 2013

```
11945 bash Fri Nov 15 05:19:22 2013 python vol.py -i ../test.mem -o lsof
11945 bash Fri Nov 15 05:19:22 2013 python vol.py -i ../test.mem -o ps -x 1541
11945 bash Fri Nov 15 05:19:22 2013 ls
11945 bash Fri Nov 15 05:19:22 2013 file 1541-bash-
11945 bash Fri Nov 15 05:19:22 2013 file 1541-bash-*
11945 bash Fri Nov 15 05:19:22 2013 rm 1541-bash-*
11945 bash Fri Nov 15 05:19:22 2013 python vol.py -i ../test.mem -o ps | grep securityd
11945 bash Fri Nov 15 05:19:22 2013 python vol.py -i ../test.mem -o ps -x 14
11945 bash Fri Nov 15 05:19:22 2013 ls
11945 bash Fri Nov 15 05:19:22 2013 ls
11945 bash Fri Nov 15 05:19:22 2013 clear
11945 bash Fri Nov 15 05:19:22 2013 ls
```



Case Study

- history -c 명령어 이 후 추출 가능 여부
- 실험 방법
 - bash 프로세스 실행
 - 메모리 덤프 후 히스토리 추출
 - history -c 명령 실행 후, 히스토리 추출
- 결론 : 시간 정보만 존재하고 명령어 삭제



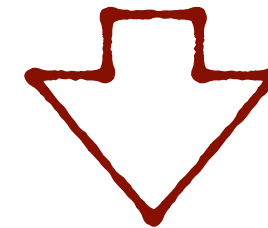
Case Study

- history -c 명령어 이 후 추출 가능 여부

```
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
11945 bash Fri Nov 15 05:19:22 2013
```

Good bye my history O_o

0040h:	23 31 33 38	34 34 39 32	38 30 35 00	00 00 00 00	#1384492805.....
0050h:	70 00 30 3A	B6 7F 00 00	40 00 30 3A	B6 7F 00 00	p.0:~...@.0:~...
0060h:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0070h:	73 75 64 6F	20 2E 2F 6F	73 78 70 6D	65 6D 20 2D	sudo ./osxpmem -
0080h:	66 20 72 61	77 20 64 75	6D 70 2E 62	69 6E 00 00	f raw dump.bin..



0040h:	23 31 33 38	34 34 39 32	38 30 35 00	00 00 05 00	#1384492805.....
0050h:	70 00 30 3A	B6 7F 00 00	40 00 30 3A	B6 7F 00 00	p.0:~...@.0:~...
0060h:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0070h:	00 00 00 00	00 00 00 80	00 00 00 00	00 00 00 80e.....e
0080h:	20 00 72 61	77 20 64 75	6D 70 2E 62	69 6E 00 00	.raw dump.bin..

```
11945 bash Fri Nov 15 05:23:41 2013 ./osxpmem -f raw historyc.bin
11945 bash Fri Nov 15 05:23:48 2013 sudo ./osxpmem -f raw historyc.bin
11945 bash Fri Nov 15 05:23:29 2013 ls
11945 bash Fri Nov 15 05:20:05 2013
```

Typing a new command

Certain points (input a 'history -c')



Case Study

- 원격으로 붙은 쉘에서 history -c 를 실행
- 실험 방법
 - bash 프로세스 여러 개 실행
 - 하나의 bash 프로세스에서 history -c 실행
 - 메모리 덤프 후 분석
- 결론 : 해당 bash history 내역만 삭제



Case Study

```
chainbreaker@testmachine:~/volafox$ python vol.py -i ../dump2.bin -o bash_history
```

```
[+] PID : 328, PROCESS: bash, HISTORY COUNT: 40
```

```
[+] PID : 586, PROCESS: bash, HISTORY COUNT: 19
```

```
[+] PID : 619, PROCESS: bash, HISTORY COUNT: 0
```

```
[+] PID : 769, PROCESS: bash, HISTORY COUNT: 4
```

```
PID PROCESS TIME (UTC+0) CMD
```

```
328 bash Fri Nov 15 06:11:12 2013 ls
328 bash Fri Nov 15 06:12:24 2013 python vol.py -i ../after.bin -o uname
328 bash Fri Nov 15 06:11:39 2013 cd volafox
328 bash Fri Nov 15 05:31:35 2013 cd /tmp/
328 bash Fri Nov 15 06:11:04 2013 ls
328 bash Fri Nov 15 05:32:27 2013 sudo ./osxpmem -f raw after.bin
328 bash Fri Nov 15 06:13:09 2013 clear
328 bash Fri Nov 15 06:11:07 2013 sudo mv after.bin ~
328 bash Fri Nov 15 05:31:27 2013 cat ~/.bash_history
328 bash Fri Nov 15 05:31:36 2013 ls
328 bash Fri Nov 15 06:11:39 2013 ls
328 bash Fri Nov 15 05:32:18 2013 ls -al
328 bash Fri Nov 15 06:11:20 2013 sudo chown n0fate:staff after.bin
328 bash Fri Nov 15 06:11:27 2013 sudo chown chainbreaker:staff after.bin
328 bash Fri Nov 15 05:31:11 2013 ls
328 bash Fri Nov 15 05:31:11 2013 ./osxpmem -f raw historyc.bin
328 bash Fri Nov 15 05:31:11 2013 sudo ./osxpmem -f raw historyc.bin
328 bash Fri Nov 15 05:31:11 2013 ls
328 bash Fri Nov 15 05:31:11 2013 ls -al
328 bash Fri Nov 15 05:31:11 2013 sudo mv *.bin ~
328 bash Fri Nov 15 05:31:11 2013 cd ~
328 bash Fri Nov 15 05:31:11 2013 sudo chown chainbreaker:staff *.bin
328 bash Fri Nov 15 05:31:11 2013 chmod 664 *.bin
328 bash Fri Nov 15 05:31:11 2013 ls -al
328 bash Fri Nov 15 05:31:11 2013 cd volafox
328 bash Fri Nov 15 05:31:11 2013 python vol.py -i ../dump.bin -o ps
328 bash Fri Nov 15 05:31:11 2013 python vol.py -i ../dump.bin -o bash_history
328 bash Fri Nov 15 05:31:11 2013 python vol.py -i ../historyc.bin -o bash_history
```

1. Type 'history -c'

```
328 bash Fri Nov 15 05:31:11 2013 sudo reboot
```

```
328 bash Fri Nov 15 06:11:12 2013 cd ~
```

```
328 bash Fri Nov 15 05:32:15 2013 ls
```

```
328 bash Fri Nov 15 05:32:11 2013 sudo chown -R root:wheel OSXPMem
```

```
328 bash Fri Nov 15 05:32:02 2013 chown -R root:wheel OSXPMem
```

```
328 bash Fri Nov 15 06:13:17 2013 history
```

```
328 bash Fri Nov 15 05:32:15 2013 cd OSXPMem/
```

```
328 bash Fri Nov 15 06:11:44 2013 python vol.py -i ../after.bin -o ps
```

```
328 bash Fri Nov 15 06:12:47 2013 python vol.py -i ../after.bin -o ps
```

```
328 bash Fri Nov 15 06:11:36 2013 sudo chmod 644 after.bin
```

```
328 bash Fri Nov 15 06:12:44 2013 python vol.py -i ../after.bin -o kextstat
```

```
328 bash Fri Nov 15 06:13:51 2013 history
```

```
586 bash Fri Nov 15 05:31:43 2013 cd Downloads/
```

```
586 bash Fri Nov 15 05:31:41 2013 cd ~
```

```
586 bash Fri Nov 15 05:31:41 2013 python vol.py -i ../dump.bin -o bash_history
```

```
586 bash Fri Nov 15 05:31:41 2013 cd volafox
```

```
586 bash Fri Nov 15 05:31:41 2013 python vol.py -i ../dump.bin -o ps
```

```
586 bash Fri Nov 15 05:31:41 2013 ls -al
```

```
586 bash Fri Nov 15 05:31:41 2013 sudo chown chainbreaker:staff *.bin
```

```
586 bash Fri Nov 15 05:31:41 2013 chmod 664 *.bin
```

```
586 bash Fri Nov 15 05:31:41 2013 ls
```

```
586 bash Fri Nov 15 05:31:41 2013 ls
```

```
586 bash Fri Nov 15 05:31:41 2013 sudo mv *.bin ~
```

```
586 bash Fri Nov 15 05:31:41 2013 ./osxpmem -f raw historyc.bin
```

```
586 bash Fri Nov 15 05:31:41 2013 sudo ./osxpmem -f raw historyc.bin
```

```
586 bash Fri Nov 15 05:31:43 2013 ls
```

```
586 bash Fri Nov 15 05:31:41 2013 python vol.py -i ../historyc.bin -o bash_history
```

```
586 bash Fri Nov 15 05:31:41 2013 sudo reboot
```

```
586 bash Fri Nov 15 05:31:41 2013 ls -al
```

```
586 bash Fri Nov 15 05:31:48 2013 tar xvf OSXPMem-RC1.tar
```

```
586 bash Fri Nov 15 05:31:54 2013 mv OSXPMem /tmp
```

```
769 bash Fri Nov 15 06:14:08 2013 cd OSXPMem/
```

```
769 bash Fri Nov 15 06:14:22 2013 sudo ./osxpmem -f raw dump2.bin
```

```
769 bash Fri Nov 15 06:14:01 2013 cd /tmp/
```

```
769 bash Fri Nov 15 06:14:01 2013 ls
```

```
chainbreaker@testmachine:~/volafox$
```

2. Start a new bash



Q & A

nofate@nofate.com