# Digital Forensics Report

Chip Holmes

Department and Organization: SCS

Investigation Number: 1

11/26/23

Contents

## 1. Executive Summary

This detailed report documents the forensic analysis of a university server, which was suspected to be compromised by a worm infection after spike in internet traffic detected by the University's Network Operations Center (NOC). This server in the early stages of setup and hosted accounts for Professor Bob and several students. The investigation involved examination of system logs, user accounts, and different activities to determine the cause of this spike in the internet traffic.

## 2. Purpose of the Investigation

The aim was to determine the cause of the traffic spike and whether the university server, flagged by the NOC for abnormal internet traffic behaviour, was compromised by a worm or any other form of malware, focusing on user activities and potential unauthorized access.

## 3. Methodology

The server's image was transferred to a Purple Kali Linux environment set up on VMware Station. In order to preserve the integrity of the original data, a hash check was performed when starting working and at the end of the investigation. A copy of the image was created in order to preserve the original image in an unaltered state.

A suite of forensic tools within the Kali Linux environment and UNIX commands and the Autopsy forensic tool in its Windows version was employed for the analysis. This analysis focused on user directories for any anomalies or signs of unauthorized access including detail review of user directories, bash histories, and system logs. Throughout the investigation, each step and finding were documented.

The investigation employed a comprehensive approach, including:

•System logs (including syslog, auth.log, wtmp, MySQL log, Faillog, Lastlog, and others) were examined for any signs of unauthorized access, manipulation, or anomalies.

•User account details, (passwd and group files), were checked to understand user privileges.

• A detailed review of user directories, bash history files, and deleted files was checked to identify any irregular activities or evidence of tampering.

## 4. Electronic Media Analyzed

The media analysed was a disk image of the university server (2.15GB in size). Key areas of focus included user home directories, bash history files, cron jobs, system log files and deleted files.

## 5. Report Findings

### *Malware and virus checking*

Clamscan was used to perform a full system scan. The database was updated to ensure the latest virus definitions were used as shown in figure 1.

## *Time zone*

The disk image was acquired on the 12th of November 2023, at 17:00, GMT+1 All actions mentioned in this report fall within the timeframe from November 12 to November 28, 2023.

## *Password and group file*

**Analysis of passwd File:**

The accounts Bob, Peter, Takeda, Kevin, and Eric are listed as users.

**Analysis of group File:**

• Both Bob and Takeda have administrative privileges, which means they have significant control over the server.

## *Logs Analysis*

- **syslog:** Showed Kevin editing the crontab. Also captured a 'shutdown -h now' command issued by Bob.
- **auth.log:** Recorded multiple rapid logins and logouts by Eric and standard logins by Kevin and Takeda.Bob executed a root-level command to shut down the system.
- **MySQL Log:** Indicated a normal shutdown of the MySQL service.
- **Wtmp Log:** System reboots and user sessions, including access by Bob, Takeda, Eric, and Kevin.
- **Faillog and Lastlog:** No significant entries were noted.

## *Deleted Files*

Examination for the deleted files within the system was done using **Autopsy** as shown in figure 2. A comparative analysis between active and deleted files did not reveal any signs of tampering, unexpected alterations, or abnormal activities.

## *User Directories*

Kevin's Activities*:* checking the **`.bash_history`** reveals kevin's activities on the system, including the setting up of cron jobs and SSH key generation as shown in the figure 3,4 . This led to further investigation to check the Kevin's cron jobs, focusing on the re syncing music from kevin.dynip.com to the server. links and music directories were checked also. Due to limitations in accessing real-time network traffic data, we were unable to directly observe the network activity generated by this rsync command.

•crontab -l: Displayed current crontab entries.

•echo "0 4 * * * rsync -aq --del --rsh="ssh" -e "ssh -l kevin" "kevin.dynip.com:My_Music/" "~/music"" | crontab -: Scheduled a cron job to sync music files from kevin.dynip.com to the local ~/music directory daily at 4 AM using rsync over ssh.

•The rsync command in the crontab used to sync a large music library could explain the unusual spike in network traffic reported by the NOC at 4 in the morning since is done at the same time.

### Bob's Activities

Server Shutdown: The server shutdown command was executed as shown in figure 4. This command is used to immediately halt the system. This command is used for safely turning off the system after Bob received the mail from the NOC.

### Eric's Activities

Repeated usage of 'mutt' shown in figure 5 after checking mutt we know that mutt is a text-based email client for Unix-like systems. Further checks and analyses of Eric's activities, including email log reviews revealed no indications of unauthorized or suspicious behaviours.

### Takeda's Activities

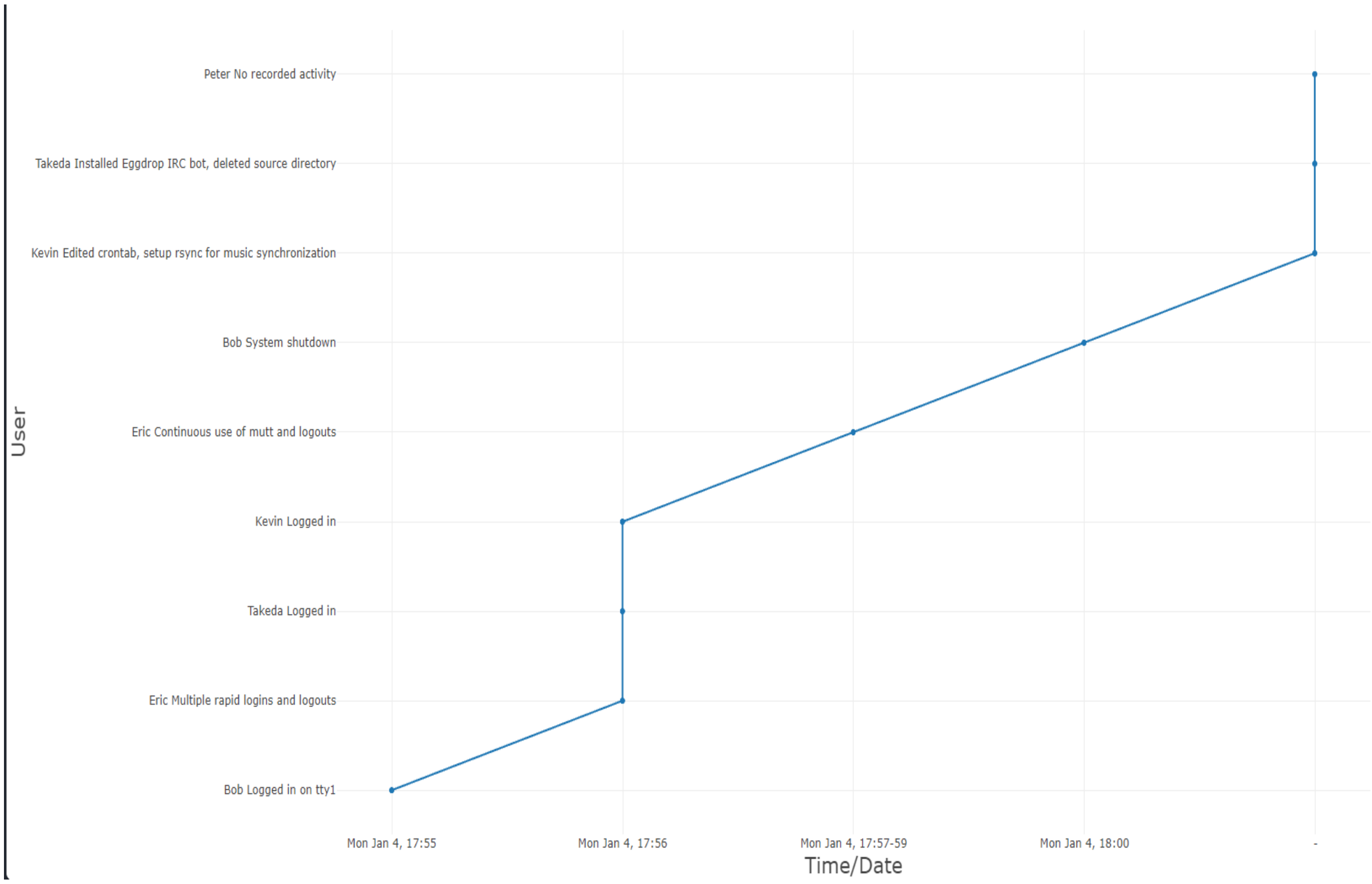
Reveals Takeda's commands for gathering system and network information and IRC bot installation activities (Eggdrop) as shown in the figure 6. This led to more investigation and in conclusion, the Eggdrop bot installed by the user "takeda" is a popular IRC bot commonly used for channel management, user interaction, and protection against spam and abuse on IRC networks. Our investigation and as we mentioned before revealed that Takeda have admin privileges and since the server in the early stages of setup so we suggest that the installation of Eggdrop by "takeda" does not appear to be malicious in nature.

### Peter's Activities

Investigation revealed that there is no .bash_history file for the user Peter, and a search through deleted files confirmed it was not erased. A potential explanation for this maybe indicating using of a different shell or absence of command history tracking.

## 6. Event Timeline

| Time/Date | User | Activity | Source |
|---|---|---|---|
| Mon Jan 4, 17:55 | Bob | Logged in on tty1 | wtmp |
| Mon Jan 4, 17:56 | Eric | Multiple rapid logins and logouts | wtmp |
| Mon Jan 4, 17:56 | Takeda | Logged in | wtmp |
| Mon Jan 4, 17:56 | Kevin | Logged in | wtmp |
| Mon Jan 4, 17:57-59 | Eric | Continuous use of mutt and logouts | .bash_history |
| Mon Jan 4, 18:00 | Bob | System shutdown | wtmp |
| Mon Jan 4 | Kevin | Edited crontab, setup rsync for music synchronization | .bash_history |
| Mon Jan 4 | Takeda | Installed Eggdrop IRC bot, deleted source directory | .bash_history |
| Mon Jan 4 | Peter | No recorded activity | - |
| Mon Jan 4 | - | MySQL Normal Shutdown | syslog |
| Mon Jan 4 | - | System reboot | wtmp |



## 7. Conclusion

**The investigation indicates no external compromise of the server.**

**Results:**

- The spike in network traffic was due to a cron job set up by Kevin for music synchronization.
- No violations were detected in the actions of Bob, Eric, and Peter.
- Takeda's installation of the Eggdrop IRC bot does not appear to be malicious.

**Recommendations:**

Consider removing Kevin's music synchronization cron job.

Conduct a thorough review of university policies to determine the permissibility of activities like music synchronization and Eggdrop installation.

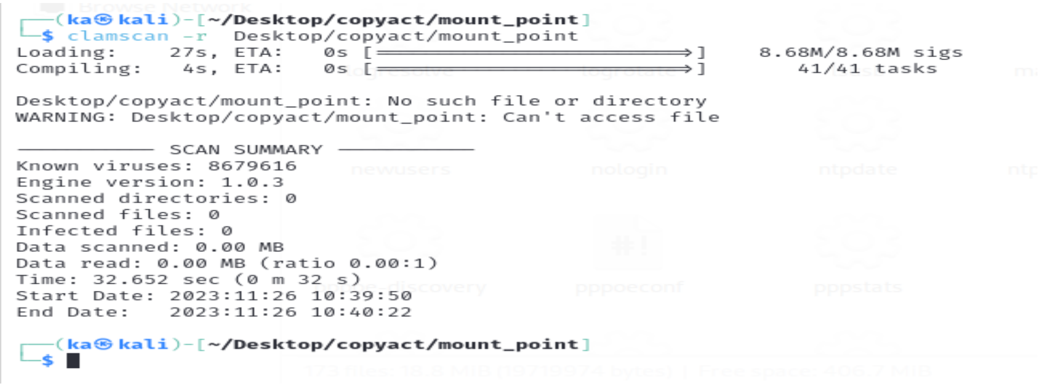
If Kevin's (music synchronization) and Takeda's activities (Eggdrop installation) are found to be in violation, appropriate measures should be considered, including formal warnings.

Arrange a meeting with Eric to discuss his frequent use of 'mutt', aiming to understand his activities.

Regular monitoring of network traffic.

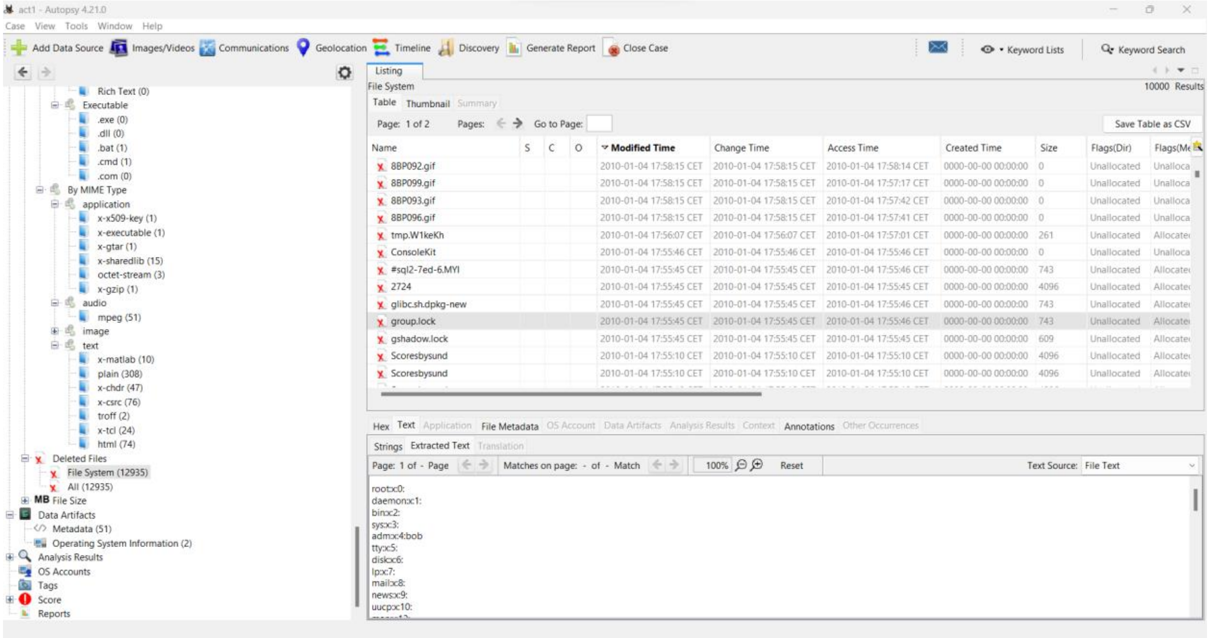
It is **very important** for the university to enforce server usage policies.

## 8. Exhibits



```
┌──(ka㉿kali)-[~/Desktop/copyact/mount_point]
└─$ clamscan -r  Desktop/copyact/mount_point
Loading:     27s, ETA:    0s [========================>]    8.68M/8.68M sigs
Compiling:    4s, ETA:    0s [========================>]      41/41 tasks

Desktop/copyact/mount_point: No such file or directory
WARNING: Desktop/copyact/mount_point: Can't access file

─────────── SCAN SUMMARY ───────────
Known viruses: 8679616
Engine version: 1.0.3
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 32.652 sec (0 m 32 s)
Start Date: 2023:11:26 10:39:50
End Date:   2023:11:26 10:40:22

┌──(ka㉿kali)-[~/Desktop/copyact/mount_point]
└─$ █
```

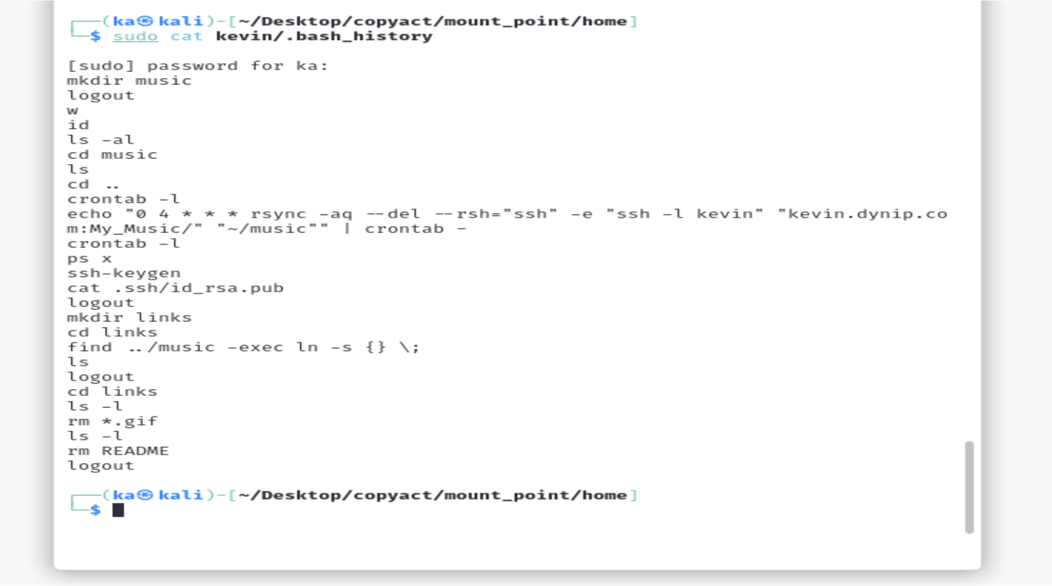
Figure 1: Shows scanning the image



| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Me |
|---|---|---|---|---|---|---|---|---|---|---|
| 8BP092.gif | | | | 2010-01-04 17:58:15 CET | 2010-01-04 17:58:15 CET | 2010-01-04 17:58:14 CET | 0000-00-00 00:00:00 | 0 | Unallocated | Unalloca |
| 8BP099.gif | | | | 2010-01-04 17:58:15 CET | 2010-01-04 17:58:15 CET | 2010-01-04 17:57:17 CET | 0000-00-00 00:00:00 | 0 | Unallocated | Unalloca |
| 8BP093.gif | | | | 2010-01-04 17:58:15 CET | 2010-01-04 17:58:15 CET | 2010-01-04 17:57:42 CET | 0000-00-00 00:00:00 | 0 | Unallocated | Unalloca |
| 8BP096.gif | | | | 2010-01-04 17:58:15 CET | 2010-01-04 17:58:15 CET | 2010-01-04 17:57:41 CET | 0000-00-00 00:00:00 | 0 | Unallocated | Unalloca |
| tmp.W1keKh | | | | 2010-01-04 17:56:07 CET | 2010-01-04 17:56:07 CET | 2010-01-04 17:57:01 CET | 0000-00-00 00:00:00 | 261 | Unallocated | Allocate |
| ConsoleKit | | | | 2010-01-04 17:55:46 CET | 2010-01-04 17:55:46 CET | 2010-01-04 17:55:46 CET | 0000-00-00 00:00:00 | 0 | Unallocated | Unalloca |
| #sql2-7ed-6.MYI | | | | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:46 CET | 0000-00-00 00:00:00 | 743 | Unallocated | Allocate |
| 2724 | | | | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:45 CET | 0000-00-00 00:00:00 | 4096 | Unallocated | Allocate |
| glibc.sh.dpkg-new | | | | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:46 CET | 0000-00-00 00:00:00 | 743 | Unallocated | Allocate |
| group.lock | | | | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:46 CET | 0000-00-00 00:00:00 | 743 | Unallocated | Allocate |
| gshadow.lock | | | | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:45 CET | 2010-01-04 17:55:45 CET | 0000-00-00 00:00:00 | 609 | Unallocated | Allocate |
| Scoresbysund | | | | 2010-01-04 17:55:10 CET | 2010-01-04 17:55:10 CET | 2010-01-04 17:55:10 CET | 0000-00-00 00:00:00 | 4096 | Unallocated | Allocate |
| Scoresbysund | | | | 2010-01-04 17:55:10 CET | 2010-01-04 17:55:10 CET | 2010-01-04 17:55:10 CET | 0000-00-00 00:00:00 | 4096 | Unallocated | Allocate |

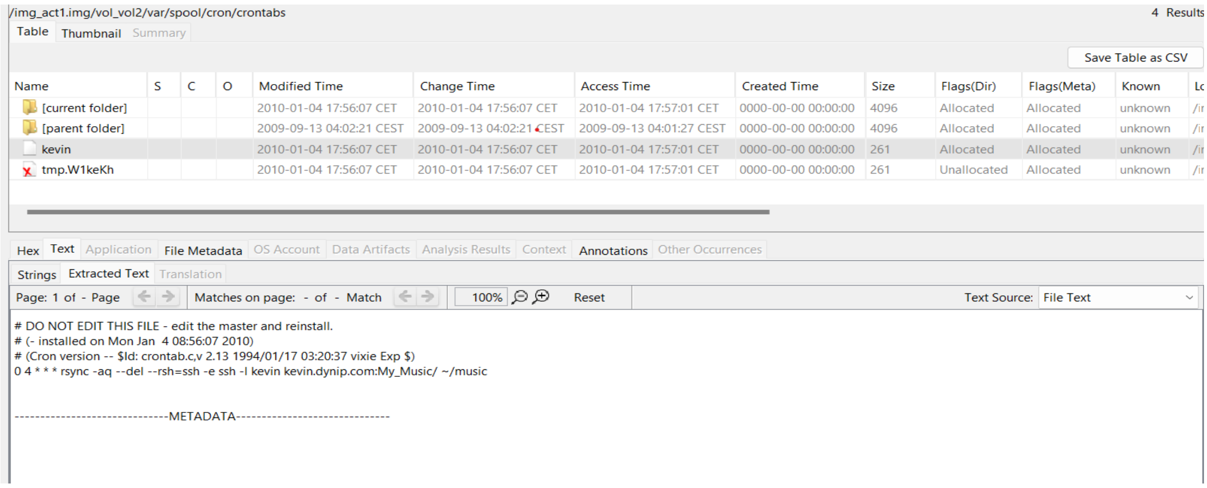
```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:bob
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
```

Figure 2:Shows using Autopsy to check the deleted files



```
┌──(ka㉿kali)-[~/Desktop/copyact/mount_point/home]
└─$ sudo cat kevin/.bash_history

[sudo] password for ka:
mkdir music
logout
w
id
ls -al
cd music
ls
cd ..
crontab -l
echo "0 4 * * * rsync -aq --del --rsh="ssh" -e "ssh -l kevin" "kevin.dynip.co
m:My_Music/" "~/music"" | crontab -
crontab -l
ps x
ssh-keygen
cat .ssh/id_rsa.pub
logout
mkdir links
cd links
find ../music -exec ln -s {} \;
ls
logout
cd links
ls -l
rm *.gif
ls -l
rm README
logout

┌──(ka㉿kali)-[~/Desktop/copyact/mount_point/home]
└─$ █
```

Figure 3:Shows Kevin bash_history



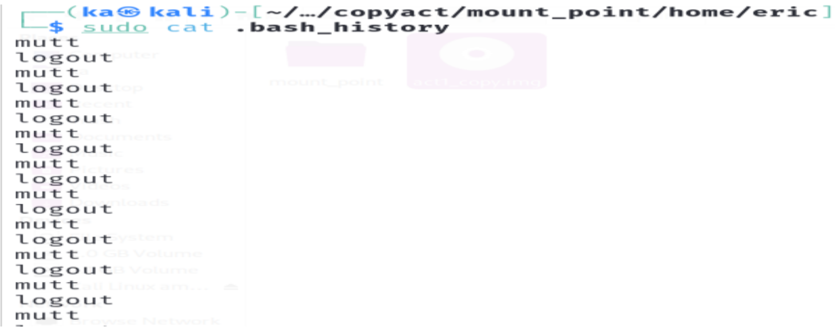
/img_act1.img/vol_vol2/var/spool/cron/crontabs 4 Results

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Lc |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [current folder] | | | | 2010-01-04 17:56:07 CET | 2010-01-04 17:56:07 CET | 2010-01-04 17:57:01 CET | 0000-00-00 00:00:00 | 4096 | Allocated | Allocated | unknown | /i |
| [parent folder] | | | | 2009-09-13 04:02:21 CEST | 2009-09-13 04:02:21 CEST | 2009-09-13 04:01:27 CEST | 0000-00-00 00:00:00 | 4096 | Allocated | Allocated | unknown | /i |
| kevin | | | | 2010-01-04 17:56:07 CET | 2010-01-04 17:56:07 CET | 2010-01-04 17:57:01 CET | 0000-00-00 00:00:00 | 261 | Allocated | Allocated | unknown | /i |
| tmp.W1keKh | | | | 2010-01-04 17:56:07 CET | 2010-01-04 17:56:07 CET | 2010-01-04 17:57:01 CET | 0000-00-00 00:00:00 | 261 | Unallocated | Allocated | unknown | /i |

Text Source: File Text

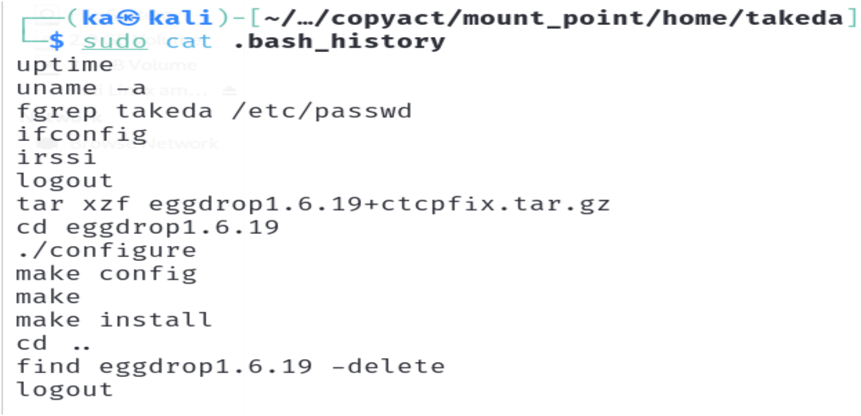
```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (- installed on Mon Jan  4 08:56:07 2010)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
0 4 * * * rsync -aq --del --rsh=ssh -e ssh -l kevin kevin.dynip.com:My_Music/ ~/music


-----------------------------METADATA-----------------------------
```

Figure 4:Shows Kevin crontab installed



```
┌──(ka㉿kali)-[~/…/copyact/mount_point/home/eric]
└─$ sudo cat .bash_history
mutt
logout
mutt
logout
mutt
logout
mutt
logout
mutt
logout
mutt
logout
mutt
logout
mutt
logout
mutt
logout
mutt
```

Figure 5:Show Eric bash_history



```
┌──(ka㉿kali)-[~/…/copyact/mount_point/home/takeda]
└─$ sudo cat .bash_history
uptime
uname -a
fgrep takeda /etc/passwd
ifconfig
irssi
logout
tar xzf eggdrop1.6.19+ctcpfix.tar.gz
cd eggdrop1.6.19
./configure
make config
make
make install
cd ..
find eggdrop1.6.19 -delete
logout
```

Figure 6:Shows Tekada bash_history

## 9. Glossary

**kali Linux**: A Debian-derived Linux distribution used for penetration testing, ethical hacking and network security assessment.

**Cron Job:** A scheduled task in Unix-based systems used to automate system maintenance or administration tasks at specified intervals.

**IRC Bot (Eggdrop):** An Internet Relay Chat (IRC) bot designed for channel management, user interaction, and protection against spam and abuse on IRC networks.

**Mutt:** A text-based email client for Unix-like systems.

**Syslog:** A standard for message logging in Unix systems, often used for system management and security auditing.

**Wtmp:** A Unix file that records login and logout activities.

**MySQL Log:** A log file generated by the MySQL database management system, recording database activities.

**Faillog:** A Unix file that records failed login attempts.

**Lastlog:** A Unix file that records the last login of each user.

**Autopsy:** A digital forensics platform and graphical interface used for digital forensics tools.

**Clamscan**: A command-line interface for the ClamAV antivirus software suite.

**Rsync**: A utility for efficiently transferring and synchronizing files across computer systems.

**Hash Check**: A process of using a hash function to verify data integrity.