Project 2: Hypervisor Disk Image Examination Report

Examination of Group 5 Disk Image - Andrew Chan

1. Case Overview

Our team (Team 7) received a compressed archive (`ToShare.zip`) containing a Linux virtual disk image (`ToShare.raw`) for forensic examination. The objective was to reconstruct user activity, identify structured artifacts, and evaluate potential cross-account behavior within the system. The image was analyzed using Autopsy, focusing on filesystem artifacts, user activity reconstruction, credential exposure, and session transitions between accounts.

```
andrewsushi@debian:~/Coding/uo/510-DF/2$ ls -la ToShare.zip ToShare.raw
-rw-rw-rw- 1 andrewsushi andrewsushi 21474836480 Feb  3 16:37 ToShare.raw
-rw-r--r-- 1 andrewsushi andrewsushi  2819974489 Feb 11 21:44 ToShare.zip
```

2. Evidence Handling & Integrity Preservation

Before we began the analysis, we extracted ToShare.raw from the provided archive and generated SHA-256 hashes for both the .zip file and the extracted .raw image. These hashes were recorded before any forensic examination began to preserve evidentiary integrity and maintain reproducibility. The raw disk image was ingested into Autopsy in a read-only forensic workflow. No modifications were made to the source image during analysis.

This process aligns with forensic best practices for:

- Integrity validation
- Chain-of-custody preservation
- Reproducibility of results

```
andrewsushi@debian:~/Coding/uo/510-DF/2$ cat evidence_hashes.txt
e09fbc2d5ac83b0624d6cc7a017d7b1b853ee2f9996804338ec9db81ff10e01b  ToShare.zip
1215efedc33651dc82d4f0bb31fc86a09ddc358293ea2d5e8a8240f072538853  extracted/ToShare.raw
extracted/ToShare.raw: DOS/MBR boot sector
```

3. System Identification

Analysis of /etc/debian_version and filesystem metadata confirmed:

- Operating System: Debian Linux
- Filesystem: EXT4 The EXT4 journaled filesystem is relevant because it preserves metadata timestamps (MAC times), which were used in timeline reconstruction.

FILE SYSTEM INFORMATION

File System Type: Ext4
Volume Name:
Volume ID: 4af188b610619ea9d9453c095e2f1f02

Last Written at: 2026-02-03 16:26:06 (PST)
Last Checked at: 2026-02-02 12:52:56 (PST)

Last Mounted at: 2026-02-03 16:26:10 (PST)
Unmounted properly
Last mounted on: /

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Needs Recovery, Extents, 64bit, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size

Journal ID: 00
Journal Inode: 8

4. User Accounts & System Structure

Inspection of /etc/passwd revealed two interactive user accounts

- user (UID 1000)
- squirrel (UID 1001) Both accounts were configured with /bin/bash, confirming interactive shell access. This established the foundation for evaluating cross-account behavior.

```
Debian-gdm:x:110:114:Gnome Display Manager:/var/lib/gdm3:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
squirrel:x:1001:1001:,,,:/home/squirrel:/bin/bash
```

5. Structured Content Creation – User Account

5.1 Image Artifacts

Within /home/user/Pictures/, multiple thematically named images were identified:

- salmon.jpeg
- salmon2.jpeg
- salmon3.jpeg
- salmon4.jpeg
- squirrel.jpeg

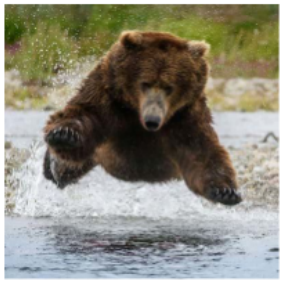
Timestamps clustered around February 2, 2026 (~13:40–13:43 PST), which suggests deliberate batch creation or collection.

Path: /home/user/Pictures/

salmon.jpeg

salmon2.jpeg

salmon3.jpeg



salmon4.jpeg

squirrel.jpeg

5.2 Document Artifacts

Under /home/user/Documents/, directories named salmon, salmon2, salmon3, salmon4, and squirrel contained text files describing types of salmon and squirrel. The timestamp clustering and consistent naming pattern indicate structured, intentional content creation rather than incidental storage.

```
andrewsushi@debian:~/Downloads/project 2 files/Documents$ ls
salmon  salmon2  salmon3  salmon4  squirrel
andrewsushi@debian:~/Downloads/project 2 files/Documents$ cat */*
Sockeye Salmon
Coho salmon
Chum Salmon
Atlantic Salmon
Squirrel
```

6. Application-Level Activity

Two key artifacts confirmed active user interaction:

- /home/user/.local/share/recently-used.xbel
- /home/user/.mozilla/firefox/.../places.sqlite

The recently-used.xbel file recorded that the image files were opened in Firefox ESR. This demonstrates:

- Files were not merely stored
- They were intentionally accessed and viewed

This corroborates filesystem timestamps and strengthens the behavioral timeline.

```
andrewsushi@debian:~/Downloads/project 2 files$ cat recently-used.xbel
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
>
  <bookmark href="file:///home/user/Pictures/salmon.jpeg" added="2026-02-02T21:40:11.715889Z" modified="2026-02-02T21:40:12.633083Z" visited="202
6-02-02T21:40:11.715891Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="image/jpeg"/>
        <bookmark:applications>
          <bookmark:application name="Firefox" exec="&apos;firefox-esr %u&apos;" modified="2026-02-02T21:40:12.633079Z" count="2"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
```

```
~~
      https://www.google.com/search?client=firefox-b-1-e&hs=r5bU&sca_esv=4d5059ca12558fc8&channel=entpr&udn=2&fbs=ADc_l-
aN0CWEZBOHjofHoaMMDiKpaEWjvZ2Py1XXV8d8KvlI3vWUtYx0DZdicpfE1faGYemg2KC4yuMPyQlIvlWqq2At2yMvCZgi_bWXXU0sv2NZz2VHRSLiUHmthAMk7QQB16edZH55kddu98F6SzcLZ80Qv3p7Jek2NCOv1aT3kzYIVOPY51ceQcaTHbHLdY8tgtkcgyzHKptKolEzuprR06e8TxGeHg&q=grizzly+bear&sa=
X&ved=2ahUKEwi_oeP84ruSAxULJkQIHWLyMa4QtKgLegQIExAB#sv=CAMSVhoyKh8lLMY2bmpDTmUzb3BMb2hNMg5mNm5qQ05lM29wTG9oTToV1E1d19rQlNf509VQU0gBCocCgztb3NhaWM5EGUtZjZuakNOZTNvcExvaE0YADA8GAcg7OeakQcwAkoKCAEQAhgCIAIoAggzrizzly bear - Google
Searchmoc.elgoog.www.d
TQ3MlTgoCIyfZ+
      https://wwfgifts-files.worldwildlife.org/wwfgifts/images/grizzly-bear-landing-photo.jpgsalmon4.jpggro.efildliwdlrow.selif-stfigfww.
f14k0wU5f0ys+
)E+
```

7. Shell & Editor Usage Corroboration

7.1 Bash History /home/user/.bash_history showed:

- Directory creation
- File renaming
- sudo usage
- su - invocation

The presence of su - is important, since it initiates a full login shell as another user, loading that user's environment.

Contents Of File: /1/home/user/.bash_history

```
ls
sudo apt update
su -
sudo -v
exit
ls
cd Videos/
ls
vim grizzly
ls
mkdir Grizzly Videos
ls
rmdir Grizzly Videos
ls
mkdir GrizzlyVideos
mv grizzly GrizzlyVideos/
ls
cd GrizzlyVideos/
ls
mkdir CrazyGrizzlyVideos
mv grizzly CrazyGrizzlyVideos/
ls
mkdir InsaneGrizzlyVideos
cd ..
ls
mkdir SalmonVideos
cd
exit
```

7.2 Vim Metadata Both /home/user/.viminfo and /home/squirrel/.viminfo contained file marks and jump lists confirming document editing activity

This independently verifies file modification beyond simple presence on disk.

```
# Jumplist (newest first):
-'  2  11  ~/Videos/grizzly
|4,39,2,11,1770069262,"~/Videos/grizzly"
-'  1  0  ~/Videos/grizzly
|4,39,1,0,1770069252,"~/Videos/grizzly"
-'  1  7  ~/Documents/squirrel/squirrel
|4,39,1,7,1770069051,"~/Documents/squirrel/squirrel"
-'  1  7  ~/Documents/squirrel/squirrel
|4,39,1,7,1770069051,"~/Documents/squirrel/squirrel"
-'  1  10  ~/Documents/salmon4/salmon4
|4,39,1,10,1770068969,"~/Documents/salmon4/salmon4"
-'  1  10  ~/Documents/salmon4/salmon4
|4,39,1,10,1770068969,"~/Documents/salmon4/salmon4"
-'  1  10  ~/Documents/salmon4/salmon4
|4,39,1,10,1770068969,"~/Documents/salmon4/salmon4"
-'  1  10  ~/Documents/salmon4/salmon4
|4,39,1,10,1770068969,"~/Documents/salmon4/salmon4"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  10  ~/Documents/salmon3/salmon3
|4,39,1,10,1770068952,"~/Documents/salmon3/salmon3"
-'  1  13  ~/Documents/salmon2/salmon2
|4,39,1,13,1770068936,"~/Documents/salmon2/salmon2"
-'  1  13  ~/Documents/salmon2/salmon2
|4,39,1,13,1770068936,"~/Documents/salmon2/salmon2"
-'  1  13  ~/Documents/salmon2/salmon2
```

8. Cleartext Credential Discovery

A significant artifact was discovered at:

/home/user/Videos/GrizzlyVideos/CrazyGrizzlyVideos/grizzly

This file contained plaintext credentials:

```
Username: squirrel
pw: squirrel
```

This indicates insecure credential storage and provides a plausible mechanism explaining how cross-account access may have occurred.

```
Contents Of File: /1/home/user/Videos/GrizzlyVideos/CrazyGrizzlyVideos/grizzly


Username: squirrel
pw: squirrel
```

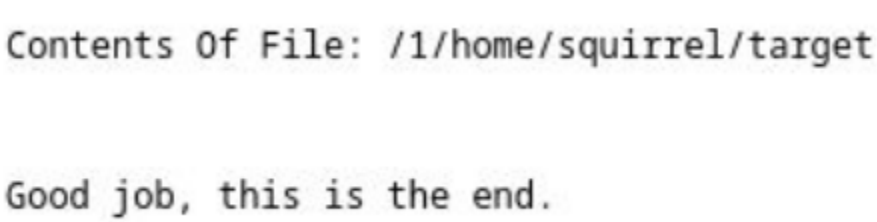
9. Confirmed Cross-Account Activity

9.1 Login Database Evidence /var/log/wtmp.db (SQLite login database) confirmed authenticated session

transitions **9.2 Target File Creation** Within /home/squirrel/target, an ASCII file containing:

“Good job, this is the end.”

was identified



squirrel’s .bash_history confirmed:

- Creation of temporary directories
- Editing of target using vim
- Subsequent removal of temporary directories

This sequence demonstrates deliberate, interactive use of the squirrel account.

Contents Of File: /1/home/squirrel/.bash_history

```
ls
mkdir Target
ls
cd Target
vim target
ls
cd
rmdir Target
ls
vim target
su - user
exit
```

/1/home/squirrel/.viminfo

```
# File marks:
'0  1  25  ~/target
|4,48,1,25,1770069201,"~/target"
'1  1  0  ~/Target/target
|4,49,1,0,1770069179,"~/Target/target"

# Jumplist (newest first):
-'  1  25  ~/target
|4,39,1,25,1770069201,"~/target"
-'  1  0  ~/Target/target
|4,39,1,0,1770069179,"~/Target/target"
-'  1  0  ~/Target/target
|4,39,1,0,1770069179,"~/Target/target"
```

10. Deleted Files & Unallocated Space

Deleted files and unallocated space were examined through Autopsy analysis. No additional suspicious or hidden artifacts were identified beyond the structured content described above.

11. Conclusion

This Debian EXT4 system contained two interactive user accounts. Analysis confirmed:

- Structured content creation under the user account
- Insecure storage of plaintext credentials
- Execution of su - privilege transition

- Authenticated cross-account session activity
- Deliberate content creation under squirrel
- Correlated evidence across multiple independent artifact sources
- The artifacts are consistent and reinforcing. No contradictory or anomalous evidence was identified.

Confidence Level: High