

Class activity

A hands-on exercise from the class-activities appendix. The full text also appears in Appendix A of the book.

Accompanies *Computer Security: The Foundations*, Krerk Piromsopa, Ph.D., 2026.
<https://www.cp.eng.chula.ac.th/~krerk/books/ComputerSecurity/>

Authorized use only

These exercises involve real attack techniques. Carry them out only against systems you own, or that you have written permission from the owner to test. Unauthorized access, scanning or interception is a criminal offence under Thailand's Computer Crime Act and its equivalents elsewhere, whether or not any damage results. If you are unsure whether a target is in scope, ask your instructor before you start.

Activity 9: Digital Forensics

Overview

Assume you are a digital forensics trainee. In this activity you will practice gathering digital evidence using tools available on Linux (Debian). Equivalent tools exist for Windows and macOS.

Exercises

1. **Where Is Your Home?** Your friend has sent you a photo taken at home. You want to determine the location by extracting the EXIF metadata.

Download the sample image:

```
https://www.cp.eng.chula.ac.th/~krerk/books/ComputerSecurity/files/
exif-sample.jpg
```

If ImageMagick is not installed:

```
$ sudo apt install imagemagick
```

Extract EXIF information with the `identify` command:

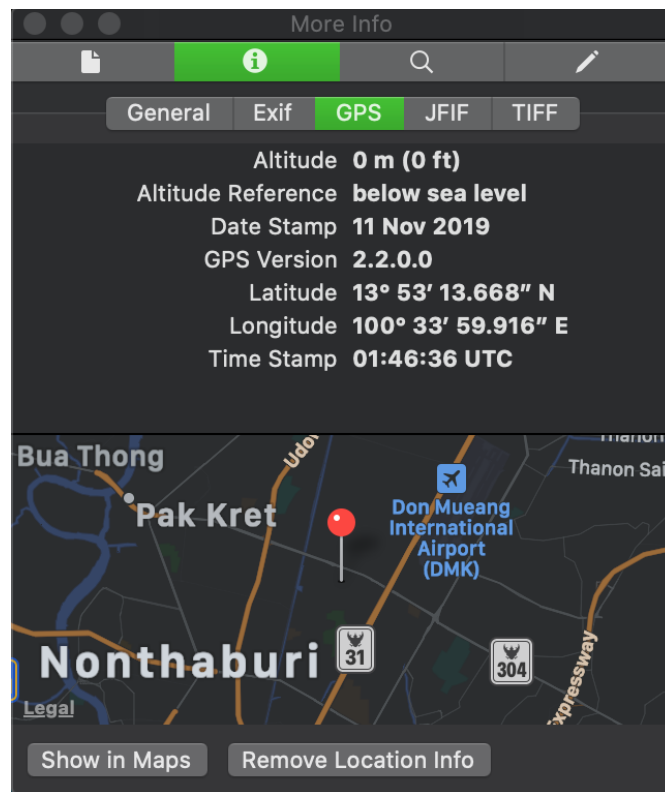
```
$ identify -verbose [img_file.jpg]
# or
$ identify -format '%[EXIF:]' [img_file.jpg]
```

Find the following information:

- Device that captured the image
- Date and time the image was taken
- GPS coordinates (latitude/longitude) of the location

With proper coordinate conversion, you can plot the location on Google Maps.

On modern operating systems (e.g. macOS), EXIF data can also be viewed directly from the file manager or image viewer (e.g. Preview on macOS).



Sample EXIF GPS data displayed in macOS Preview. The GPS tab shows latitude, longitude, and timestamp — enough to plot the location on a map.

2. **Recover a Deleted File.** You are given a USB drive that may contain a deleted evidence file. Recover the secret file on the disk.

Note: You may use the prepared disk image below and skip the Preparation and Steps 1–2. Download the ZIP archive and extract it with `unzip` to obtain `disk.img`.

<https://www.cp.eng.chula.ac.th/~krerk/books/ComputerSecurity/files/disk-sample.zip>

Preparation: Create a sample text file on your USB drive (e.g. `secret.txt`), then delete it.

Steps:

- (a) Plug in the USB drive. Use `lsblk` to identify the device and partition (e.g. `/dev/sdc2`).

```
$ lsblk
```

- (b) Clone the partition to an image file for offline forensics:

```
$ dd if=/dev/sdc2 of=disk.img bs=4M status=progress
```

- (c) Install TestDisk:

```
$ sudo apt install testdisk
```

- (d) Launch TestDisk on the image:

```
$ testdisk disk.img
```

TestDisk presents the disk and asks you to proceed. Select the disk entry and choose **Proceed**.

```
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk disk.img - 4294 MB / 4096 MiB

>[Proceed ] [ Quit  ]

Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

TestDisk — select disk.img and choose Proceed.

- (e) In TestDisk, navigate to **Advanced** → **Filesystem Utils**, list the files in the partition, select the deleted file, and copy it out.

*Because we imaged only the partition (not the whole disk), there is no partition map — select **None** when prompted.*

```
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk disk.img - 4294 MB / 4096 MiB

Please select the partition table type, press Enter when done.
[Intel  ] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Humax  ] Humax partition table
[Mac    ] Apple partition map
>[None  ] Non partitioned media
[Sun    ] Sun Solaris partition
[XBox   ] Xbox partition
[Return] Return to disk selection

Hint: None partition table type has been detected.
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a disk to be 'Non-partitioned'.
```

Select **None** — the image is a raw partition, not a whole disk.

```
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk disk.img - 4294 MB / 4096 MiB
  CHS 523 255 63 - sector size=512

[ Analyse ] Analyse current partition structure and search for lost partition
>[ Advanced ] Filesystem Utils
[ Geometry ] Change disk geometry
[ Options ] Modify options
[ Quit ] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

Main menu — choose **Advanced** for Filesystem Utils.

```
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk disk.img - 4294 MB / 4096 MiB - CHS 523 255 63

    Partition              Start          End      Size in sectors
>  P FAT32                 0  0  1  522  42 32    8388608 [NO NAME]

[ Type ] >[ Boot ] [Undelete] [Image Creation] [ Quit ]
                        Boot sector recovery
```

The FAT32 partition is detected. Select it and choose **Boot** to inspect the boot sector.

```

TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk disk.img - 4294 MB / 4096 MiB - CHS 523 255 63
  Partition          Start          End      Size in sectors
  P FAT32              0    0  1    522  42 32    8388608 [NO NAME]

Boot sector
OK

Backup boot sector
OK

Second sectors (cluster information) are not identical.

A valid FAT Boot sector must be present in order to access
any data; even if the partition is not bootable.

[ Quit ] >[ List ] [Org. BS] [Backup BS] [Rebuild BS] [ Dump ]
List directories and files, copy and undelete data from FAT

```

Boot sector is intact. Choose **List** to browse files (including deleted ones).

```

TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
  P FAT32              0    0  1    522  42 32    8388608 [NO NAME]
Directory /
>-rwxr-xr-x    0    0    89 15-Nov-2019 01:12 secret.txt

Next
Use Right to change directory, h to hide deleted files
q to quit, : to select the current file, a to select all files
C to copy the selected files, c to copy the current file

```

The deleted `secret.txt` is still recoverable. Press `c` to copy it out.

TestDisk supports several filesystem types and partition schemes. Experiment with your own system if you wish.

From *Computer Security: The Foundations*, Kerk Piromsopa, Ph.D.
Reproduce and adapt freely for non-commercial classroom instruction, with attribution. Full terms: LICENSE.txt in the student package.