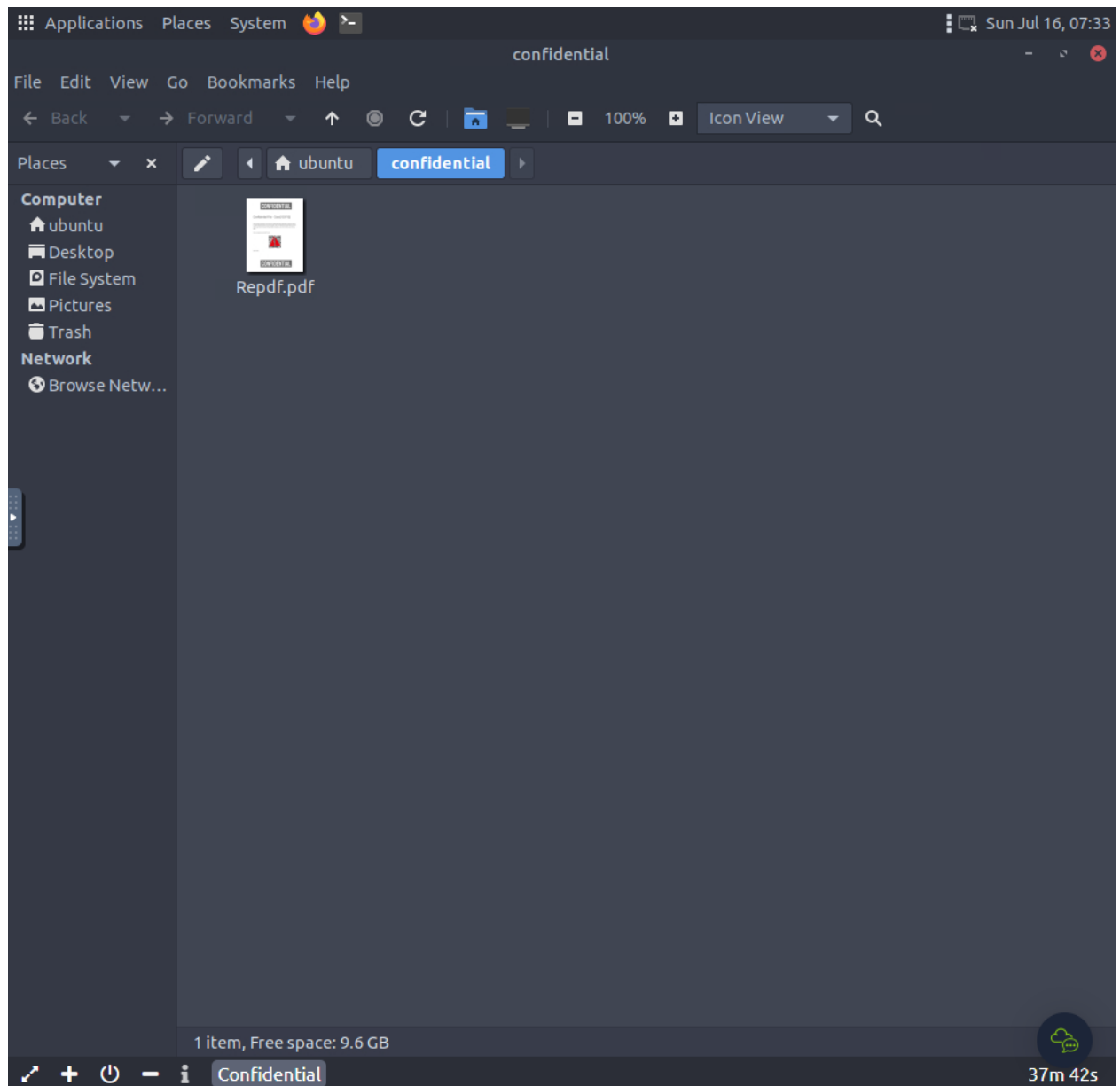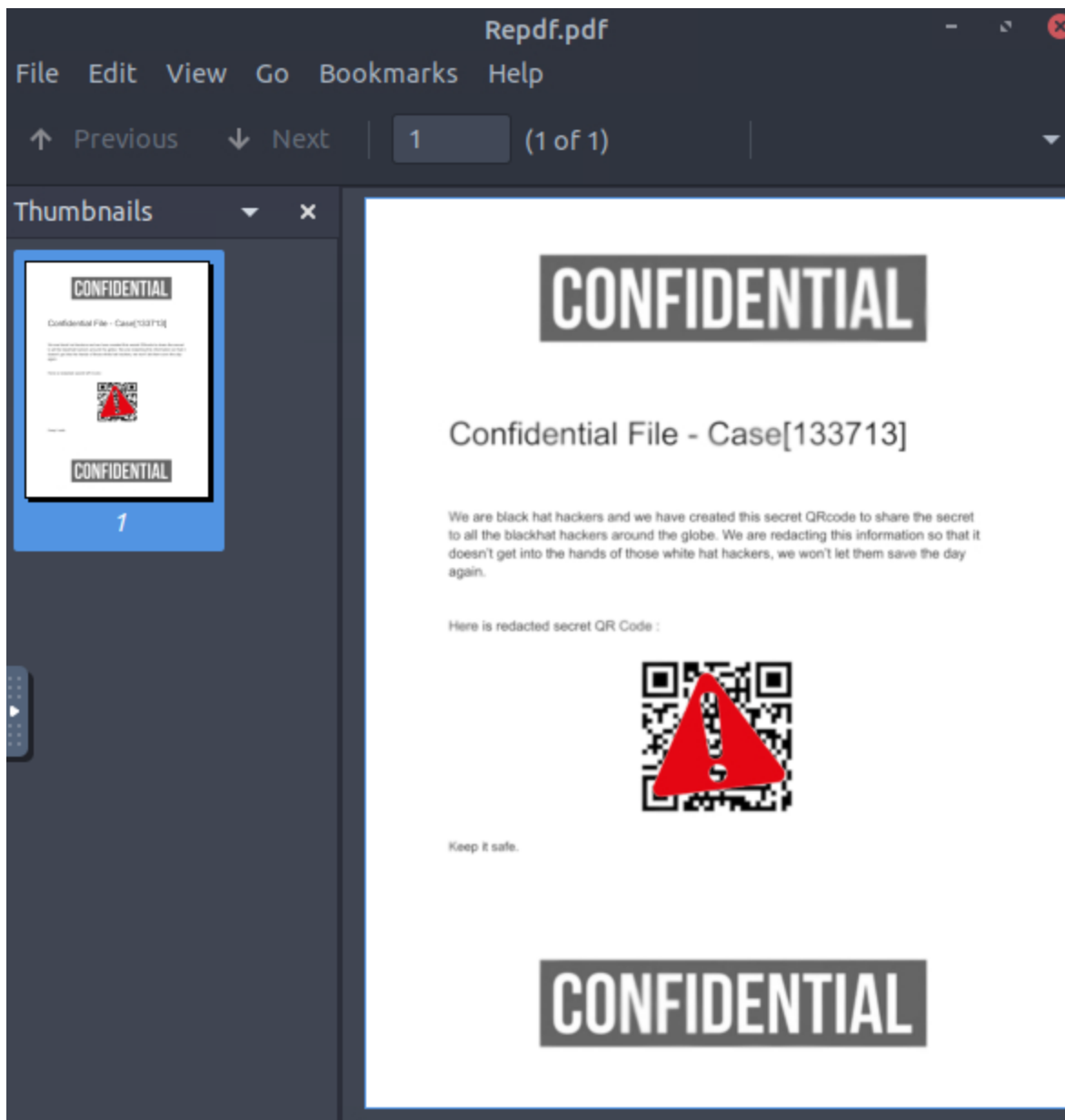# Confidential

> **Instruction**
>
> We got our hands on a confidential case file from some self-declared "black hat hackers"... it looks like they have a secret invite code available within a QR code, but it's covered by some image in this PDF! If we want to thwart whatever it is they are planning, we need your help to uncover what that QR code says!
>
> Access this challenge by deploying the machine attached to this task by pressing the green "Start Machine" button. This machine shows in Split View in your browser, if it doesn't automatically display you may need to click "Show Split View" in the top right. The file you need is located in /home/ubuntu/confidential on the VM.

The **Split View** Machine on web browser:

confidential

File   Edit   View   Go   Bookmarks   Help

← Back   → Forward   ↑ ◉ C | 🗁 ▬ | ■ 100% ⊞   Icon View   ▾   🔍

Places   ▾ ✕   ✎ ◄ 🏠 ubuntu   confidential ►

Computer
🏠 ubuntu
🖥 Desktop
🗄 File System
🖼 Pictures
🗑 Trash
Network
🌐 Browse Netw...

Repdf.pdf

1 item, Free space: 9.6 GB

⤢ ✛ ⏻ ━ ℹ   Confidential   37m 42s

Tools

- pdfinfo: display PDF file information

- pdfimage: extract images inside PDF file

- zbarimg: read the QR code in image

Transfer target file to local machine

The online machine does not contain the required tools for analyzing and is not allowed to install anything → The target PDF file must be transferred through the local machine for using the tools to analyze.

1. Start the HTTP.Server on the target machine

```
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

2. Download the file to local machine with the following command on the local machine:

```
$ wget http://<TARGET_MACHINE_IP>/Repdf.pdf
```

View file info

CONFIDENTIAL

Confidential File - Case[133713]

We are black hat hackers and we have created this secret QRcode to share the secret to all the blackhat hackers around the globe. We are redacting this information so that it doesn't get into the hands of those white hat hackers, we won't let them save the day again.

Here is redacted secret QR Code :

Keep it safe.

CONFIDENTIAL

```
$ pdfinfo Repdf.pdf
Producer:       cairo 1.17.4 (https://cairographics.org)
CreationDate:   Sat Feb  5 08:01:35 2022 EST
Custom Metadata: no
Metadata Stream: no
```

```
Tagged:          no
UserProperties:  no
Suspects:        no
Form:            none
JavaScript:      no
Pages:           1
Encrypted:       no
Page size:       849.894 x 1099.86 pts
Page rot:        0
File size:       102818 bytes
Optimized:       no
PDF version:     1.5
```

Extract images inside PDF

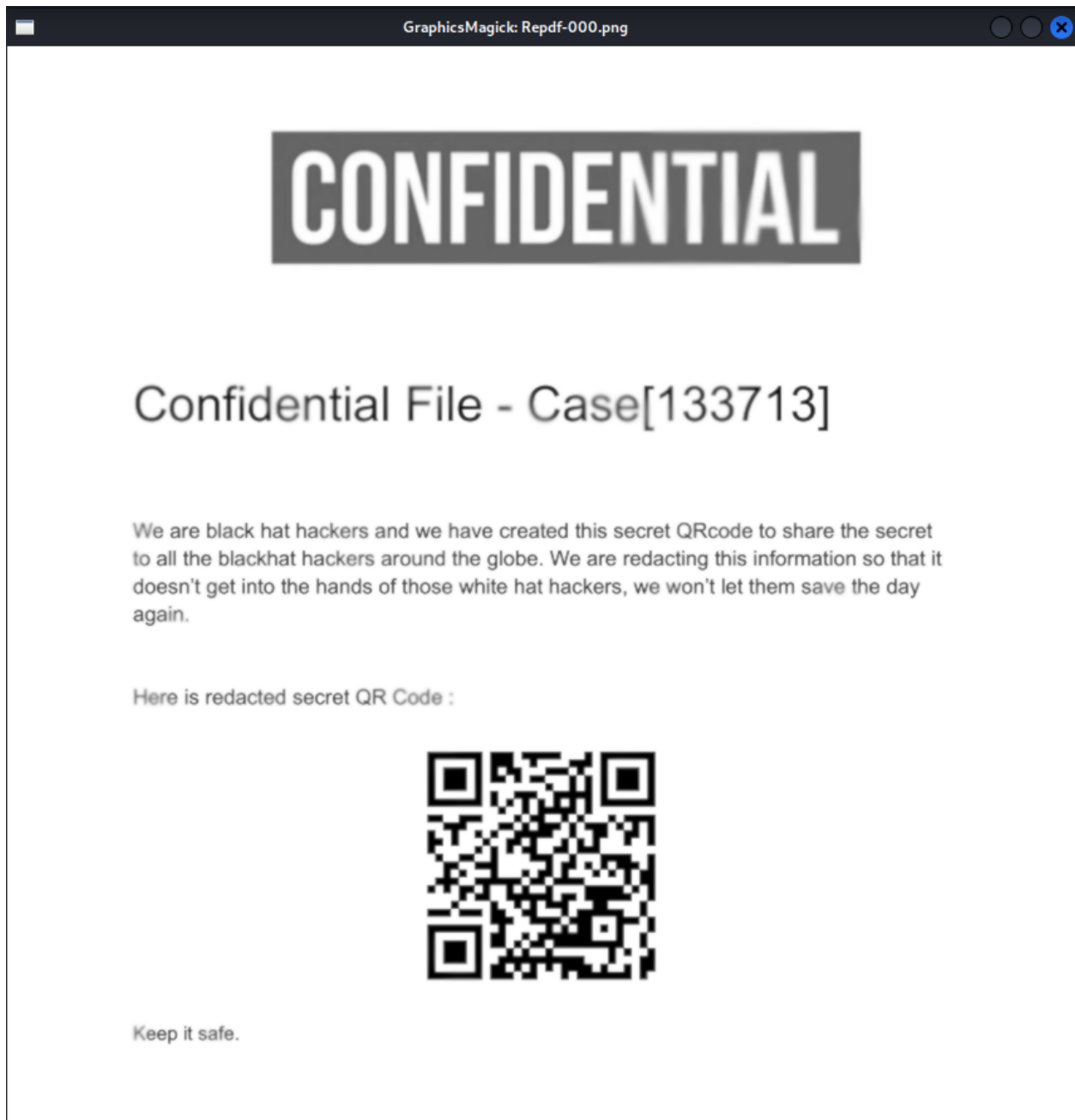As the view file above, the QR is covered by a red triangle. To view the original QR code
→ Extract the file into pieces by `pdfimage`

```
$ pdfimage -all Repdf.pdf Repdf

#Output:
Repdf-000.png
Repdf-001.png
Repdf-002.png
```

Display the **Repdf-000.png**

The **Repdf-001.png** and **Repdf-002.png** are the red triangle which covered the QR code.

Read the QR code → Get flag

```
$ zbarimg Repdf-000.png
```

```
#Output:
QR-Code:flag{HIDDEN}
scanned 1 barcode symbols from 1 images in 0.06 seconds
```