Qlocker

In this writeup we will go through the whole process of recovering and renaming your data.

You will need

- For Windows users: WSL (Windows subsystem for Linux)
- External HDD with a capacity of at least 2x your NAS, we recommend 3x bigger
- Connection to your NAS and to the internet
- the IP address of your PC (**`ipconfig /all`** on Windows cmd, **`ip address`** on Linux)

Let’s recover your data

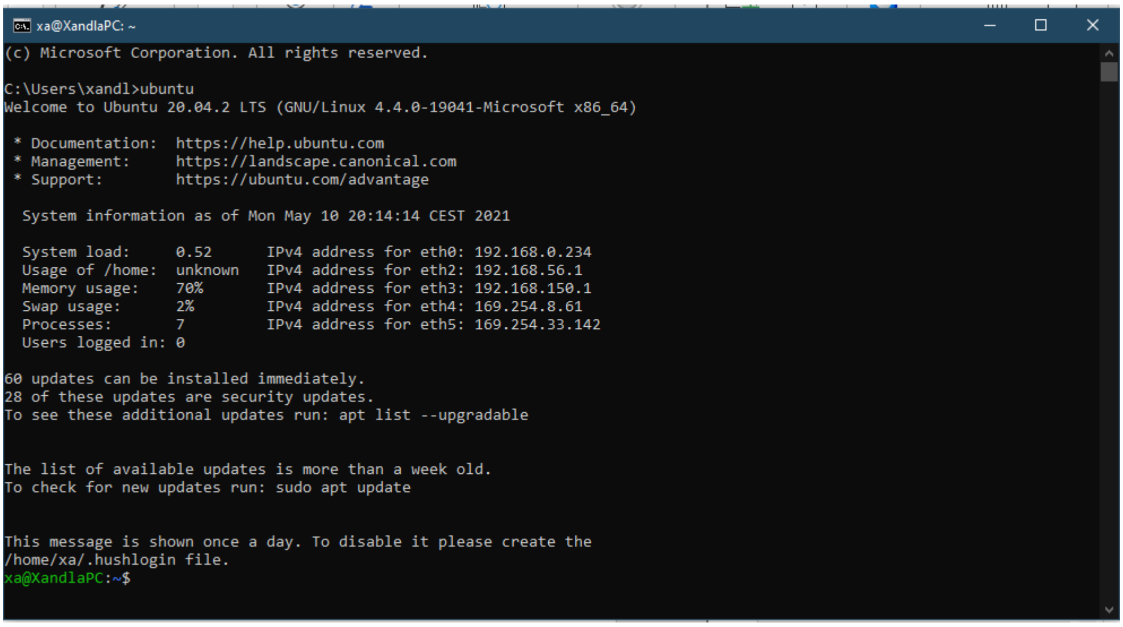
First, we need to install WSL

This will be our terminal where we will execute all commands.

Download it from the windows store and reboot after installation.
[Get Ubuntu - Microsoft Store]

Now open a command prompt by pressing **`Win+R`** and **`cmd`**, or just search for **`cmd`** in windows.

Type **`ubuntu`** in the command prompt which opened. It should look like this:



```
(c) Microsoft Corporation. All rights reserved.

C:\Users\xandl>ubuntu
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.4.0-19041-Microsoft x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon May 10 20:14:14 CEST 2021

  System load:     0.52      IPv4 address for eth0: 192.168.0.234
  Usage of /home:  unknown   IPv4 address for eth2: 192.168.56.1
  Memory usage:    70%       IPv4 address for eth3: 192.168.150.1
  Swap usage:      2%        IPv4 address for eth4: 169.254.8.61
  Processes:       7         IPv4 address for eth5: 169.254.33.142
  Users logged in: 0

60 updates can be installed immediately.
28 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


This message is shown once a day. To disable it please create the
/home/xa/.hushlogin file.
xa@XandlaPC:~$
```

1 Now run these three commands:

```
sudo apt-get update
sudo apt-get install rhash
sudo apt-get install p7zip-full
```

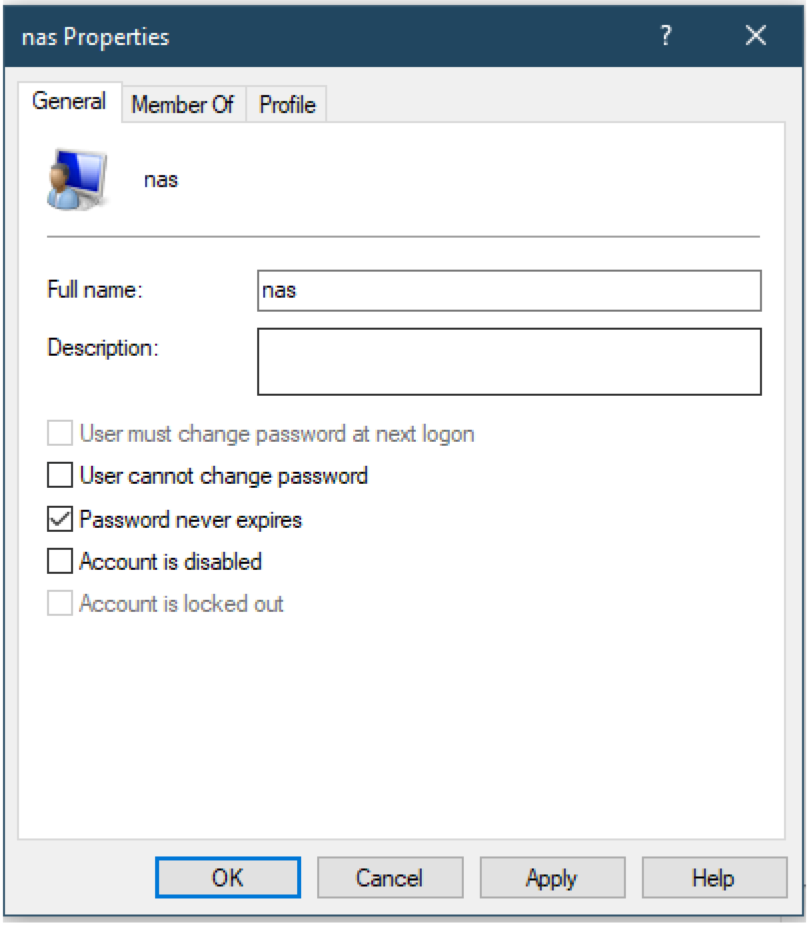
Recover the Deleted Data with PhotoRec

If you have already recovered your data with PhotoRec you can skip this part.

2 Connect an external hard drive to a PC which can be left turned on overnight. The size of the hard drive must be at least as big as the capacity of your NAS.

3 On the harddisk create a folder called **Share**

4 Create a new user called **nas** with the password **12345**:



nas Properties

nas

Full name: nas

Description:

□ User must change password at next logon

□ User cannot change password

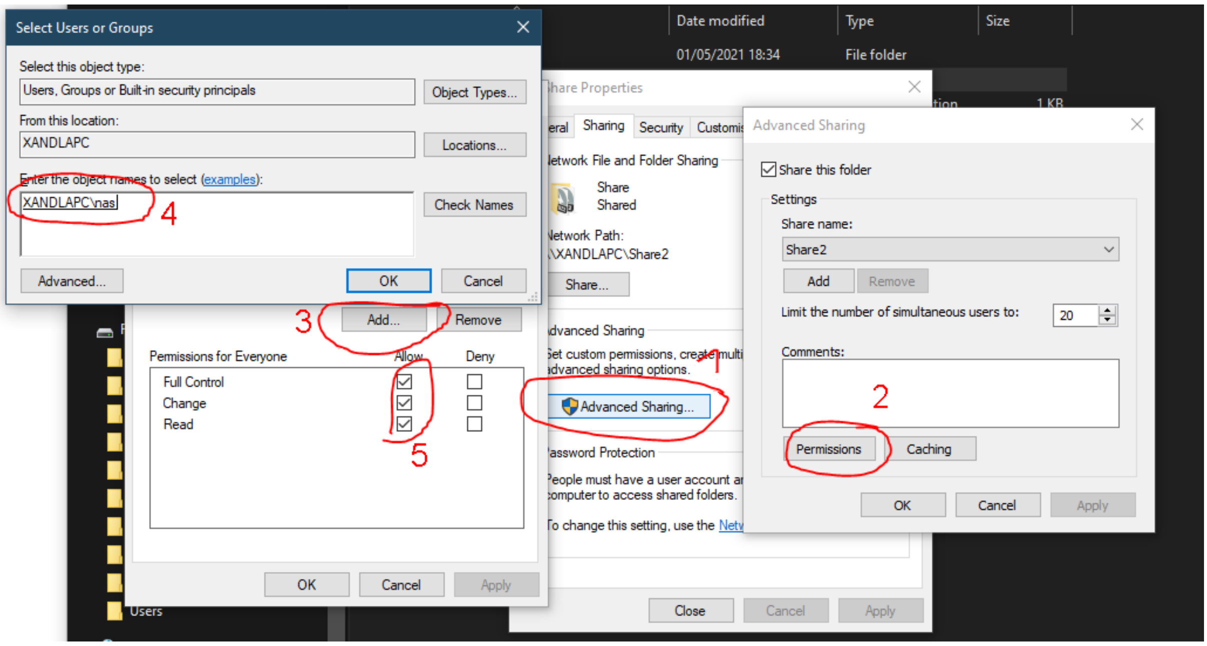
☑ Password never expires

□ Account is disabled

□ Account is locked out

Right click on **This PC -> Manage -> Local Users and groups -> Users-> new**

5 Go back to the share folder you just created
Right click on **Share -> Properties ->** go to sharing-tab **share -> advanced sharing -> permissions -> add ->** enter as user **nas**, password **12345** -> tick the box **full control**



Select this object type: Users, Groups or Built-in security principals
From this location: XANDLAPC
Enter the object names to select (examples): XANDLAPC\nas

Permissions for Everyone — Allow / Deny
Full Control ☑ □
Change ☑ □
Read ☑ □

01/05/2021 18:34 File folder

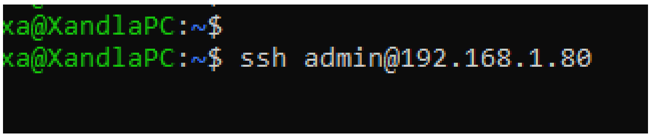
Share2
Shared
Network Path:
\\XANDLAPC\Share2

☑ Share this folder
Settings
Share name: Share2
Limit the number of simultaneous users to: 20
Comments:

6 Download the data recovery tool PhotoRec.
Note: There are two versions. We download both and determine later which one we need:
https://www.cgsecurity.org/testdisk-7.2-WIP.arm-none-linux-gnueabi.tar.bz2
Rename it to **`testdisk-i.tar.bz2`**
https://www.cgsecurity.org/testdisk-7.2-WIP.linux26-x86_64.tar.bz2
Rename it to **`testdiks-x.tar.bz2`**

7 Move them to the **Share** folder

8 Go to your terminal window where you started **`ubuntu`**
Connect to your NAS via SSH:
`ssh <user>@<IP-NAS>` (for example: **`ssh admin@192.168.1.80`**)
and enter the password of your user:



```
xa@XandlaPC:~$
xa@XandlaPC:~$ ssh admin@192.168.1.80
```

if successful this prompt should be visible:
`[~]#`
Maybe you have to leave the QNAP menu system by pressing **q** for quit and **y** for yes.

9 Enter the following commands on your NAS prompt:

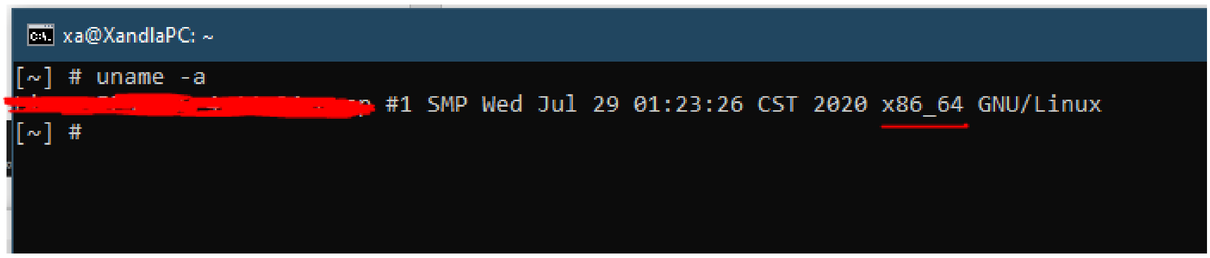
```
mkdir /mnt/rescue-share
sudo mount -t cifs -o user=nas //192.168.1.2/Share /mnt/rescue-share
```

(replace **`nas`** with your user from above, **`192.168.1.2`** with the IP address of your PC, and **`Share`** with the name of the share you created)

```
cd /mnt/rescue-share
```

10 Determine the version of PhotoRec you need:

```
uname -a
```



```
xa@XandlaPC: ~
[~] # uname -a
[redacted] #1 SMP Wed Jul 29 01:23:26 CST 2020 x86_64 GNU/Linux
[~] #
```

If the output is something with **x86_64**:

```
tar -xvf testdisk-x.tar.bz2
cd testdisk*
chmod +x ./photorec_static
sudo ./photorec_static
```

Else

```
tar -xvf testdisk-i.tar.bz2
cd testdisk*
chmod +x ./photorec
sudo ./photorec
```

11 Choose the **/dev/mapper/cachedev1** partition which should show up. Or choose the disk you stored your files at. Usually, it is the one with the highest capacity.
Choose **ext2/3/4** file format
Choose **ext2/ext3** option

12 Choose **Free** (In one instance it took about 24 hours. Don't be scared if it says 120hrs remaining during the process.)

13 Choose the **Shared** folder! Navigate to **..** (2nd from top). You could also create a new folder if you want to, but it must be within the Shared folder. Otherwise, it will not show up.
If you choose a folder on your NAS by accident, you will overwrite the files you are trying to backup! Take care!

14 After the undelete is completed, open your file explorer on windows and copy all encrypted files from your NAS to your external hard drive to the folder **Encrypted**. The folder has to be at the same level as your **Share** folder.

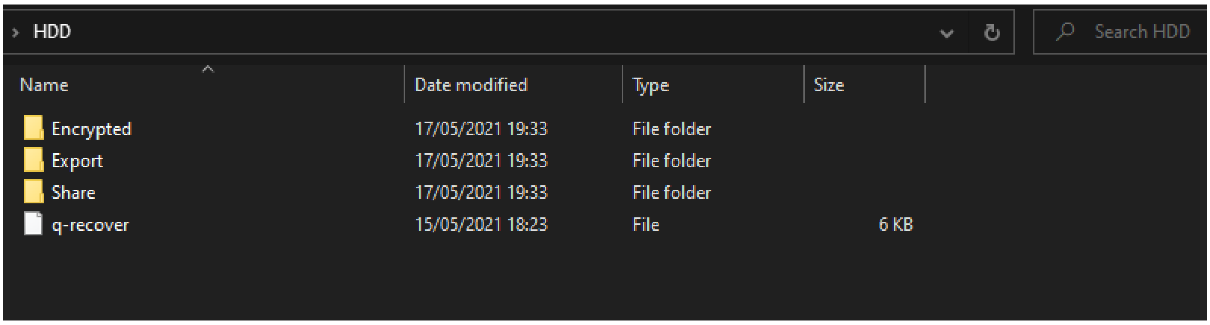
Rename your files by script

You need three folders. One called **Share**, where all the data from PhotoRec is stored, another one called **Encrypted**, where all your files from your NAS are (including the .7z ones) and you need to create a new one called **Export**.

15 You do not need to be connected to your NAS anymore. So you quit the ssh connection to return to the ubuntu shell:

```
exit
```

16 Download **q-recover.zip** and copy the content of the zip-file (= the **q-recover** script) to your external hard drive. It needs to be at the same level as your three folders:



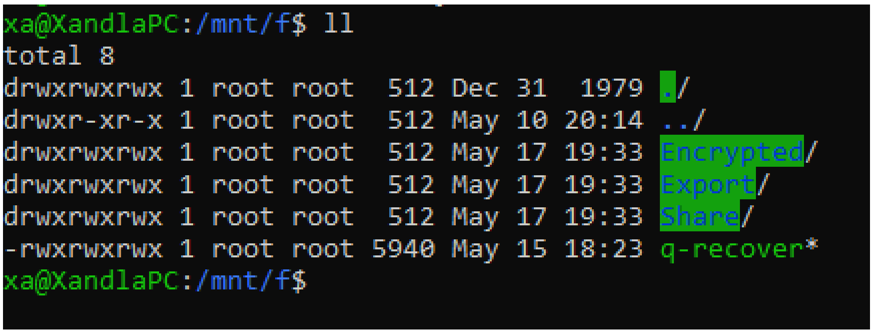
Name	Date modified	Type	Size
Encrypted	17/05/2021 19:33	File folder	
Export	17/05/2021 19:33	File folder	
Share	17/05/2021 19:33	File folder	
q-recover	15/05/2021 18:23	File	6 KB

17 Go to your ubuntu shell

18 Mount your external hard drive so ubuntu can see and access it
`sudo mkdir /mnt/f`
`sudo mount -t drvfs <letterOfDrive>: /mnt/f`
e.g.: **`sudo mount -t drvfs d: /mnt/f`**

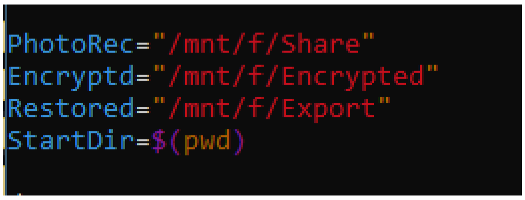
19 **`cd /mnt/f`**

20 Check if files are there
`ll` (or **`ls -la`**)



```
xa@XandlaPC:/mnt/f$ ll
total 8
drwxrwxrwx 1 root root  512 Dec 31  1979 ./
drwxr-xr-x 1 root root  512 May 10 20:14 ../
drwxrwxrwx 1 root root  512 May 17 19:33 Encrypted/
drwxrwxrwx 1 root root  512 May 17 19:33 Export/
drwxrwxrwx 1 root root  512 May 17 19:33 Share/
-rwxrwxrwx 1 root root 5940 May 15 18:23 q-recover*
xa@XandlaPC:/mnt/f$
```

21 Change the paths in the script if needed:
`vi q-recover`
Navigate with your arrow keys down where the paths are specified.



```
PhotoRec="/mnt/f/Share"
Encryptd="/mnt/f/Encrypted"
Restored="/mnt/f/Export"
StartDir=$(pwd)
```

If changes are needed press **`i`** to insert text. If you are done, press **ESC** and enter **`:wq`** and press the enter key.

22 After you closed the editor, type this to make the script executable
`chmod +x q-recover`

23 Execute the script by entering
`./q-recover`
It will take a while. The script will display progress in 10% steps.

24 After the first script is completed, the file structure will be recovered and there will be 6 other scripts on your drive. If you want only some functions you can call the scripts individually or just enter the command from step 31) to execute everything in order.

25 Renaming the files and moving them to their correct place.

```
./renamer
```

26 Giving the files their original date back. You will notice that all the PhotoRec files have the same creation date but with this script the original creation date will be applied.

```
./redater
```

27 QLocker does not encrypt large files like videos. For this, use the following script to copy unaffected files to the Export folder.

```
./notcryp
```

28 There will be files that our script will not find. But it will create a .csv file with all missing files which can be manually searched if wanted. Just import the file into a spreadsheet program.

```
notfound.csv
```

29 If you want to delete the .7z files from the hard drive run this. Only .7z files that were used for renaming are deleted.

```
./remover
```

30 If you want to look for the remaining files manually run this command because it will remove all files we already recovered and do not need to be looked at again.

```
./duplics
```

31 If you want to use all functions:

```
./renamer; ./redater; ./notcryp; ./remover; ./duplics
```

What remains to be done after running all the scripts:

- In the **PhotoRec** directory tree are recovered files that were already deleted before qlocker (maybe old but unencrypted versions). Maybe you can use them.
- In the **Encryptd** directory tree are .7z files for which there was no recoverable deleted file. Please keep a copy of those remaining (i.e. unrecoverable) .7z files because someday we might have the ability to decrypt them with a key. The file **notfound.csv** contains them without ending .7z (plus a count [usually 0], name [UTF-8], size, datetime).

Now all your data should show up in the folder **Export**.

We hope we could help you with this guide. If you have any questions, feel free to contact us at: qrecover.xandl@gmail.com