

QRescue handmatig installeren om door Qlocker versleutelde bestanden op een QNAP NAS te herstellen

Overzicht:

QRescue is het hulpprogramma voor het herstellen van gegevens in 7z-bestanden die door Qlocker zijn versleuteld. Het bevat:

- PhotoRec (open source-project/[GNU Algemene openbare licentie/Koppeling naar project](#)):
Software voor bestandsherstel die is ontworpen om kwijtgeraakte bestanden op harde schijven en cd-roms en kwijtgeraakte afbeeldingen (vandaar de naam 'Photo Recovery') op opslagmedia te herstellen.
- QRescue (ontwikkeld door QNAP):
Het script dat de bestandsstructuren in de versleutelde 7z-bestanden en PhotoRec-bestanden herstelt.

Vereisten:

- Download de QRescue-app via [deze koppeling](https://download.qnap.com/QPKG/QRescue.zip).
<https://download.qnap.com/QPKG/QRescue.zip>
- Maak een externe harde schijf klaar met een grotere capaciteit dan de totale gebruikte opslagruimte op uw NAS.
 - NB: Het is aan te bevelen om een externe HDD klaar te maken met 1,5 tot 2 keer zo veel vrije ruimte als de totale opslagruimte die op uw NAS wordt gebruikt. Tijdens het herstelproces is mogelijk extra ruimte nodig. Als er minder ruimte

beschikbaar is, kunnen er fouten en andere problemen optreden.



Demovideo:

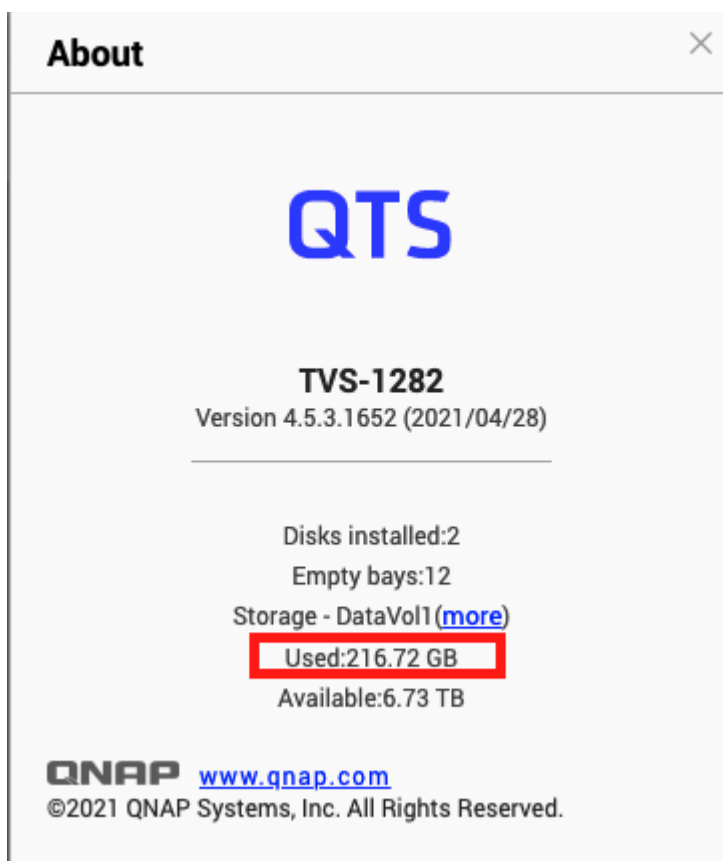
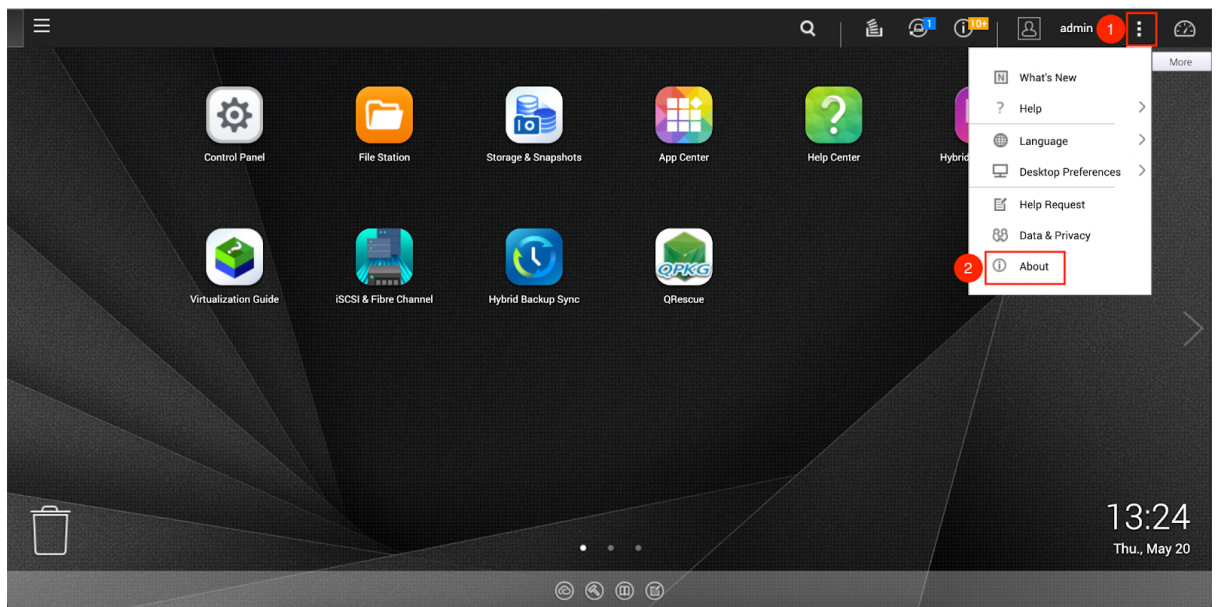
- Raadpleeg [deze koppeling](#).

Stappen:

Deel 1. Configureer een externe harde schijf met de naam 'rescue' en maak mappen met de naam 'recup1' voor herstel.

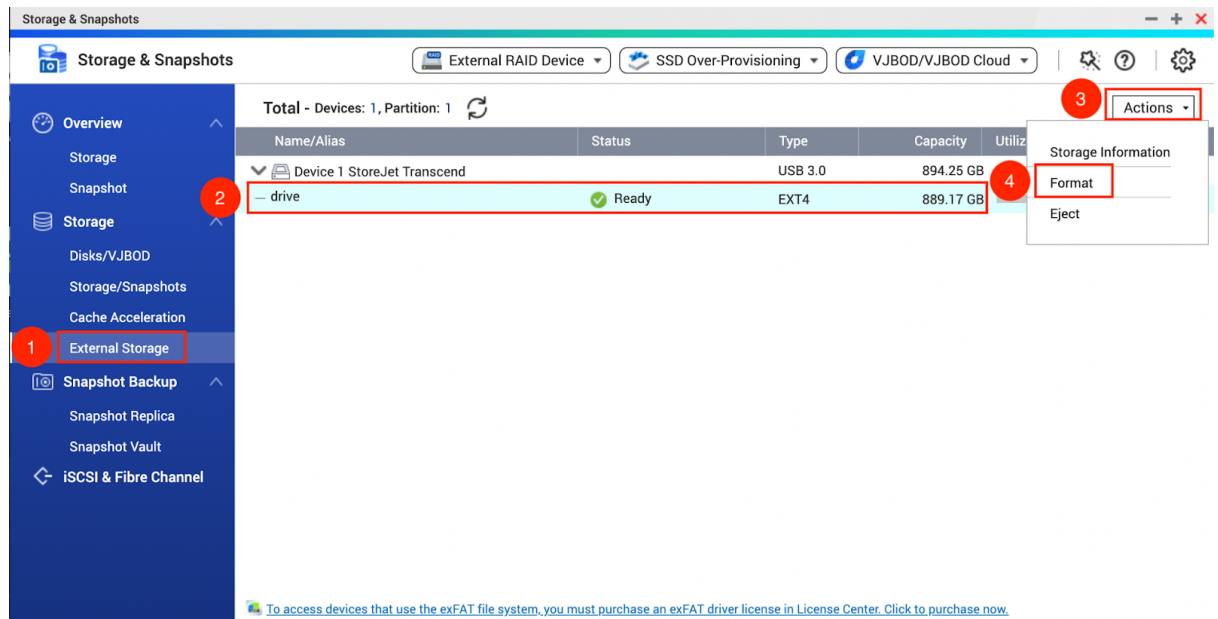
QRescue zal het herstelproces eerst naar de externe schijf uitvoeren. We moeten een aantal configuratiestappen voor dit herstelproces doorlopen en de specifieke doel- en mapnaam maken.

1. U moet een externe HDD klaarmaken met een bruikbare capaciteit die groter is dan de totale opslagruimte die op uw NAS wordt gebruikt. U moet namelijk eerst de bestanden naar het externe apparaat herstellen. Controleer vooraf uw gebruikte volume door op het bureaublad van QTS op **Meer > Over** te klikken;

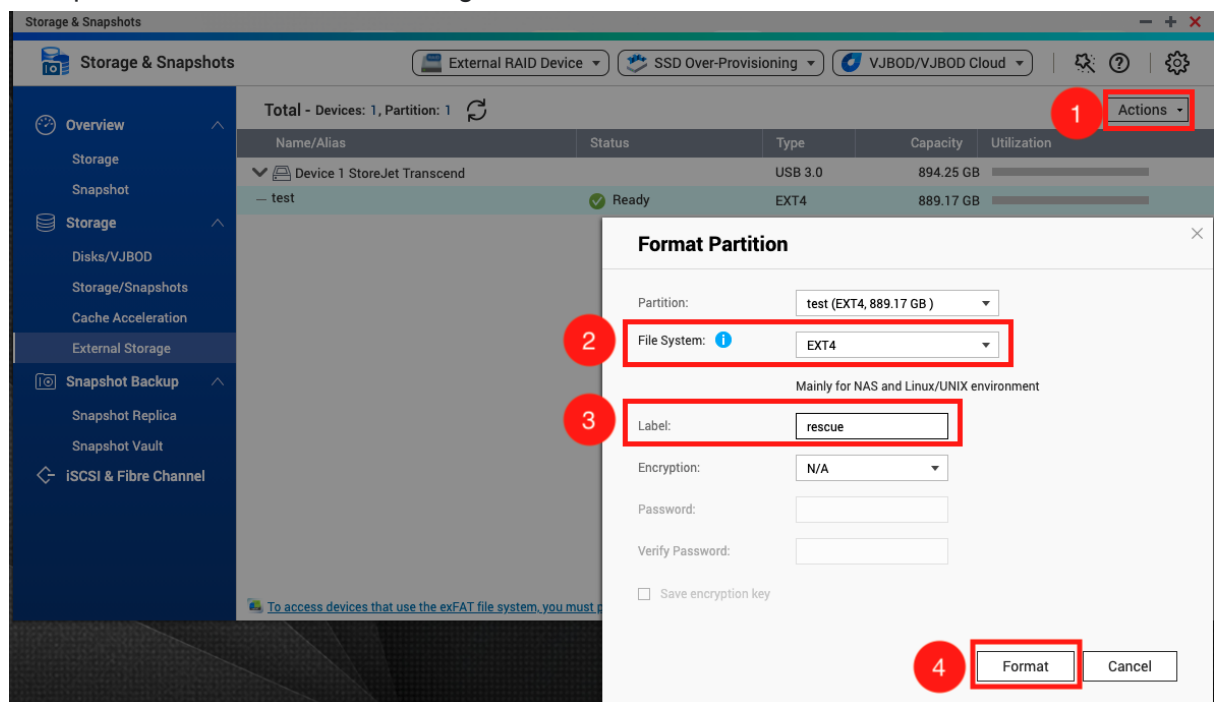


2. Sluit de externe schijf aan uw NAS aan. Ga naar **Opslagbeheer > Extern apparaat >** selecteer uw externe apparaat > klik op '**Acties**' > klik op '**Formatteren**' om de externe

schijf te formatteren;



3. Het bestandssysteem moet van het type 'EXT4' zijn en de labelnaam moet 'rescue' zijn. Klik op 'Formatteren.' als deze configuratie klaar is



NB:

De QRescue-app zal 'rescue' als naam voor de externe schijf gebruiken. Mogelijk mislukt het herstelproces als u een andere naam gebruikt;

4. (Optioneel) Als u het beheeraccount uitschakelt of u niet bij QTS aanmeldt als 'admin' ziet u de externe schijf mogelijk niet in File Station. Ga naar **Configuratiescherm > Machtigingen > Gedeelde map > Machtigingen voor gedeelde mappen bewerken** om lezen/schrijven-machtigingen voor de map 'resue' in te schakelen of te wijzigen en het account te selecteren waarmee u zich aanmeldt bij de NAS.
 - o Voorbeeld:
Een ander beheerdersgroepsaccount machtigen (voorbeeld: '_qnap_support' is het beheerdersgroepsaccount voor lezen/schrijven-machtigingen voor de externe

harde schijf met de naam 'rescue');

Control Panel

System

Users

User Groups

Shared Folders

Quota

Domain Security

Domain Controller

Virtualization Guide

Network & File

Applications

ControlPanel

Shared Folder

Advanced Permissions

Folder Aggregation

Create

Migrate to Snapshot Shared Folder

Remove

Restore Default Shared Folders

Folder Name	Size	Folders	Files	Hid...	Volume	Action
Container	1.03 GB	4489	28184	No	DataVol1	
Public	104.43 MB	15	21	No	DataVol1	
Web	247.88 MB	6	36	No	DataVol1	
Web2	75.83 MB	4	17	No	DataVol2	
homes	17.98 MB	31	87	No	DataVol1	
rescue	279.7 MB	305	3792	No	USB Disk 1	

Page 1 / 1

Display item: 1-6, Total: 6

Show 10 Item(s)

Edit Shared Folder Permission

Select permission type: Users and groups permission

Edit the user and group permissions for access from Windows, Mac, FTP, and File Station.

Shares

Container

Public

Web

Web2

homes

rescue

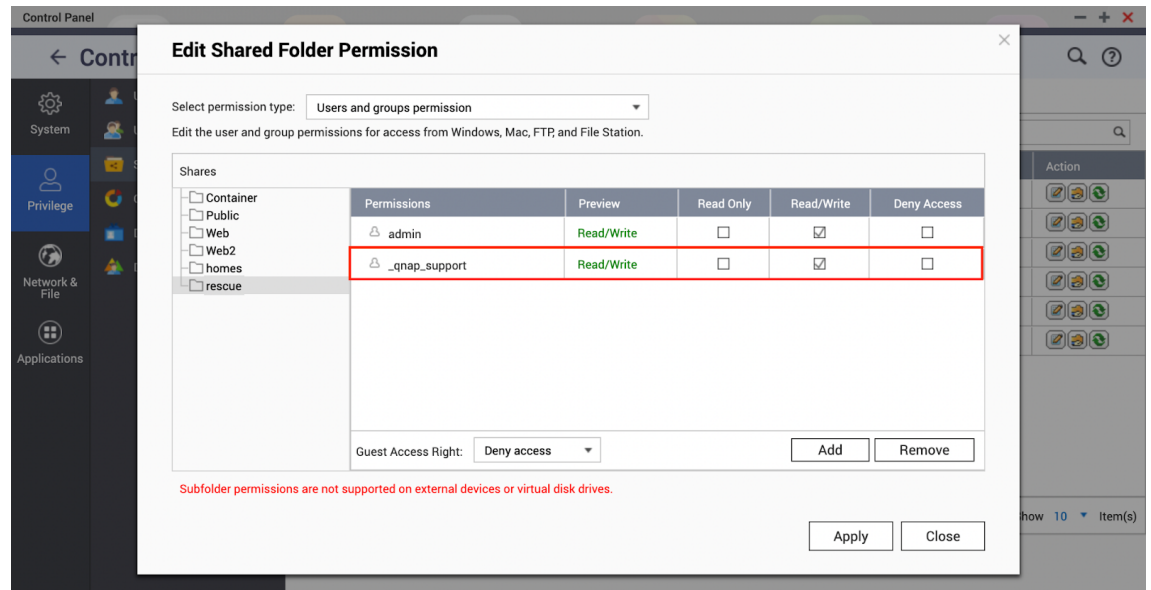
Permissions	Preview	Read Only	Read/Write	Deny Access
admin	Read/Write			

Guest Access Right: Deny access

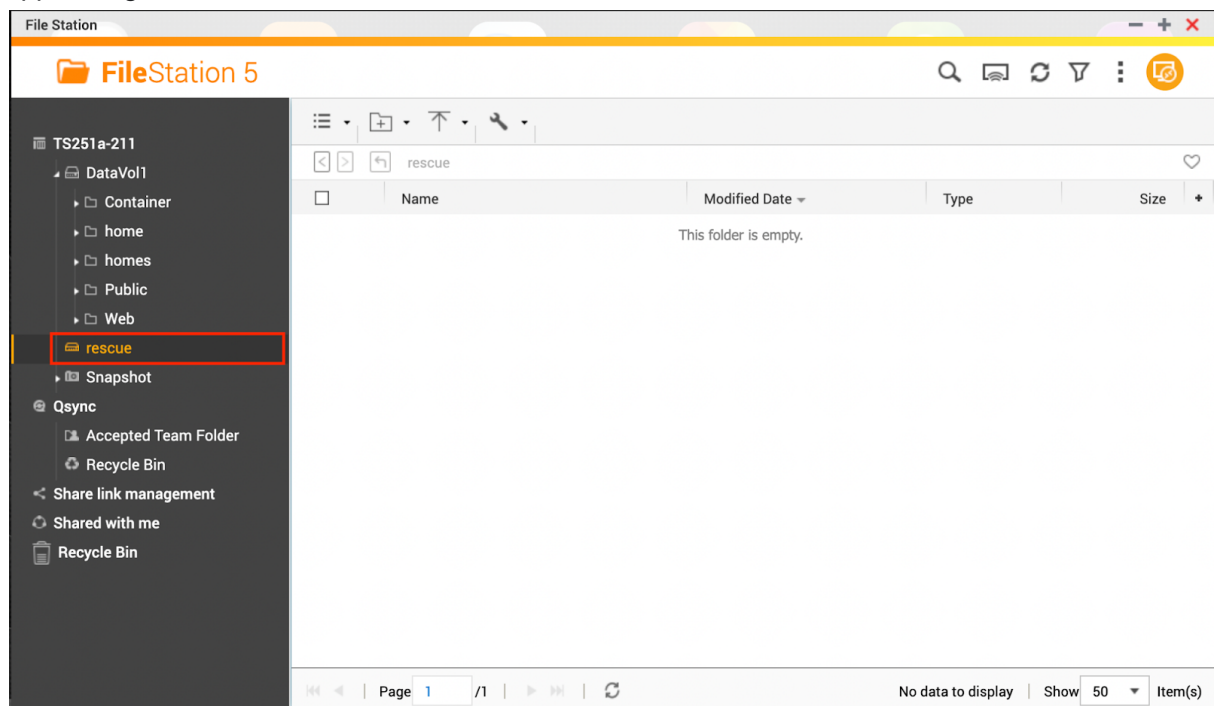
AddRemove

Subfolder permissions are not supported on external devices or virtual disk drives.

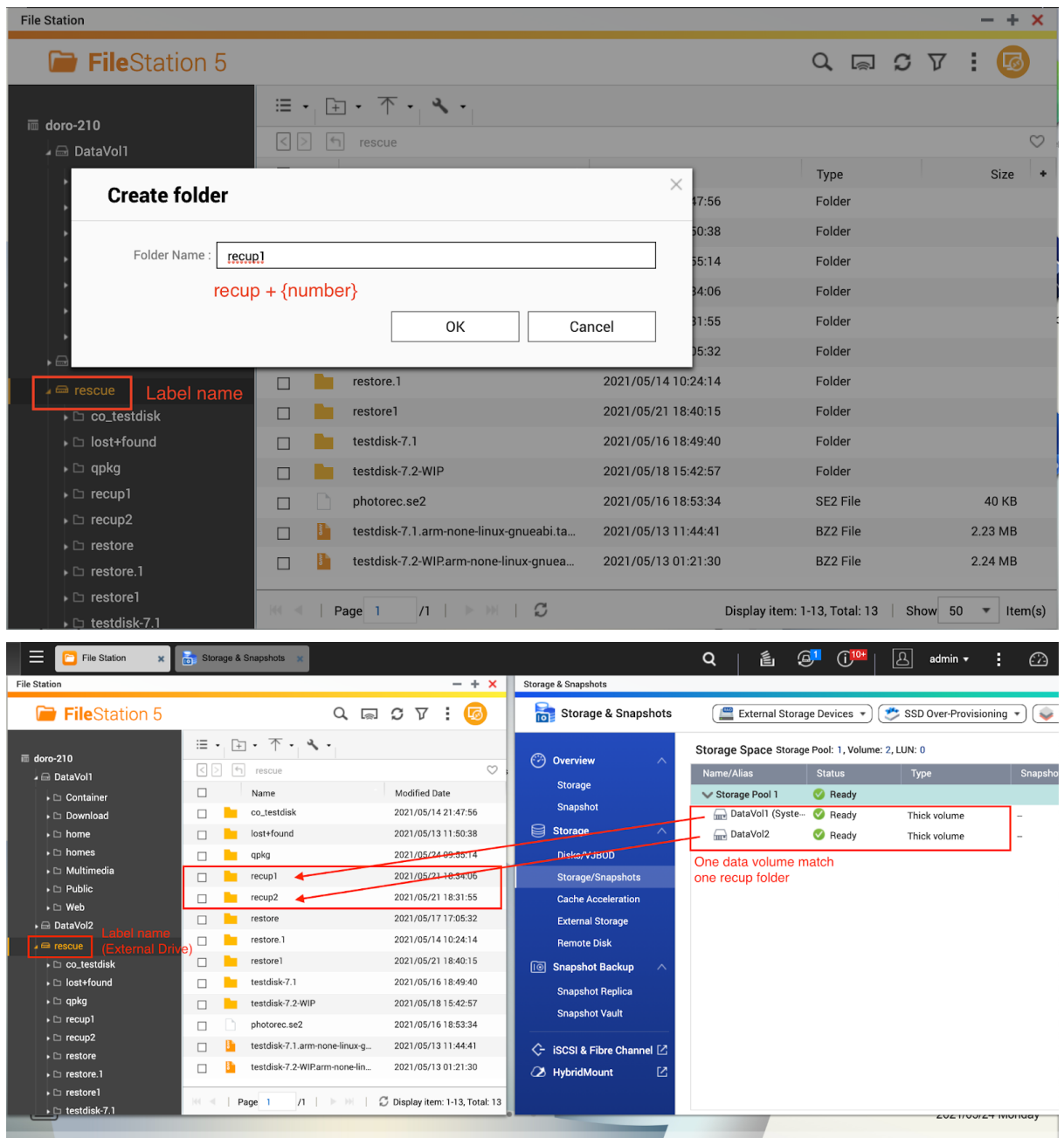
ApplyClose



5. Gebruik **File Station** om te controleren of het volume de juiste naam van het externe apparaat gebruikt;



6. Maak een nieuwe map en noem deze 'recup1' (indeling: recup+{getal}). Als u meer dan één opslagvolume hebt, moet u meer mappen toevoegen voor herstel.



NB:

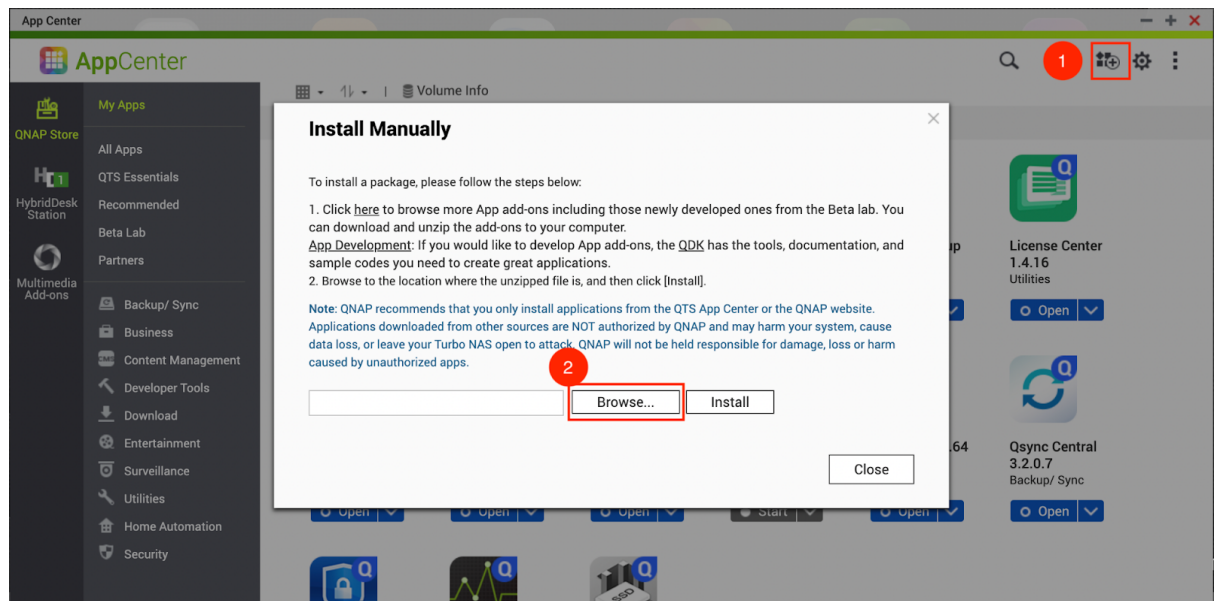
De QRescue-app zal 'recup+{getal}' als naam voor de map gebruiken. Mogelijk mislukt het herstelproces als u een andere naam gebruikt;

Deel 2. Download de QRescue-app en installeer deze handmatig

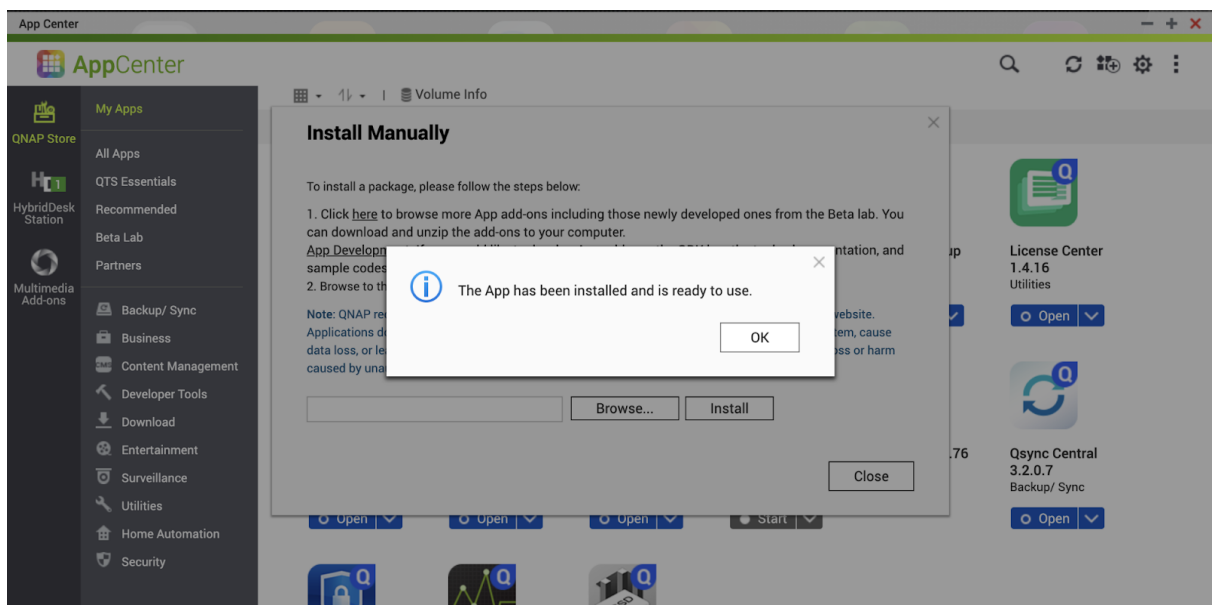
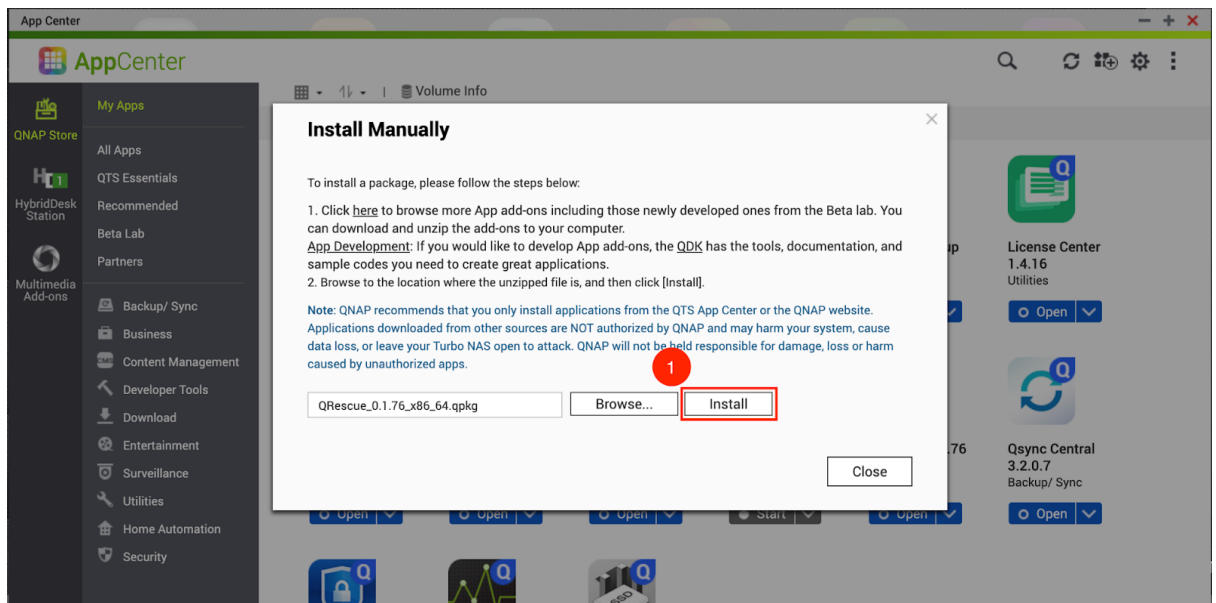
Deze QRescue-app is een speciale versie. Daarom moet u deze app handmatig installeren via het QTS App Center.

- Ga naar [deze koppeling](https://download.qnap.com/QPKG/QRescue.zip) om de QRescue-app te downloaden.

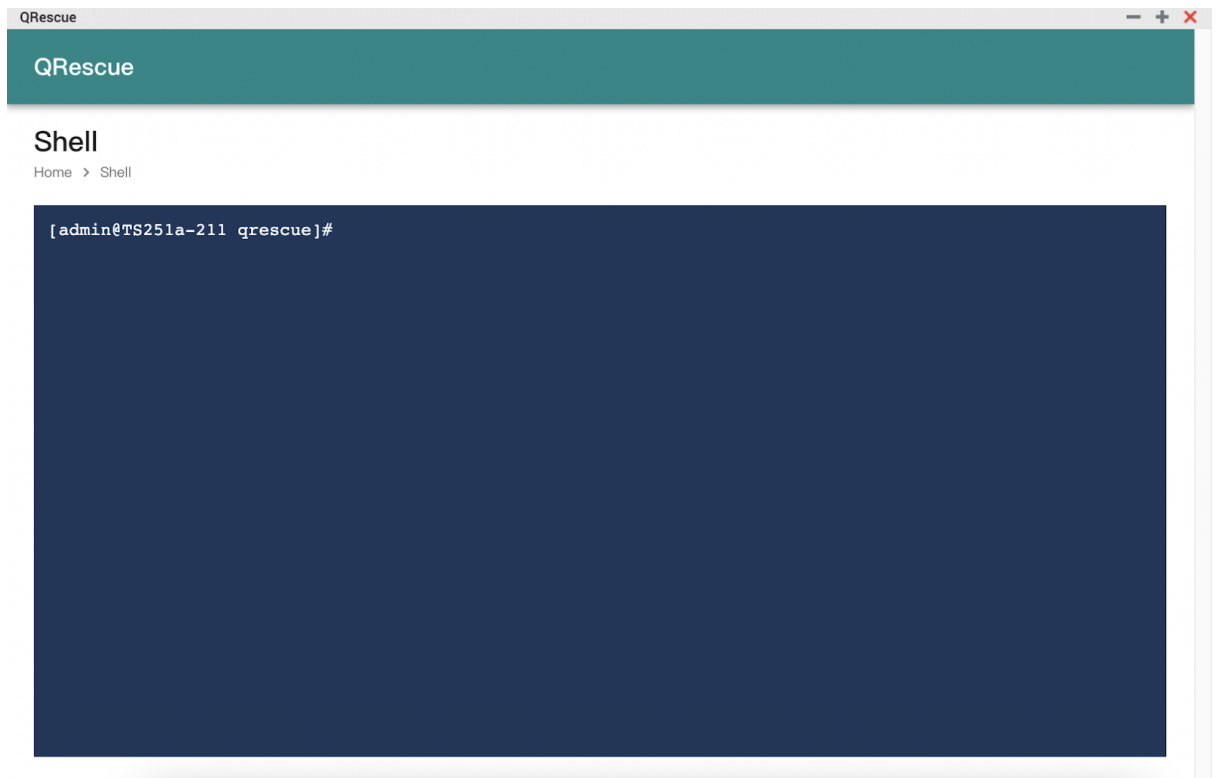
8. Ga naar **App-center** > klik op **Handmatig installeren** > klik op **Bladeren** om de locatie van de QRescue-app op uw computer te vinden;



9. Nadat u de app-locatie hebt geselecteerd, kunt u op **Installeren** klikken. Wacht tot de installatie is voltooid en open de **QRescue**-app op het bureaublad van QTS of in de zijbalk;



10. Als u de QRescue-app opent, wordt de webconsole weergegeven. Het kan helpen om PhotoRec en QRescue uit te voeren om uw bestanden te herstellen.



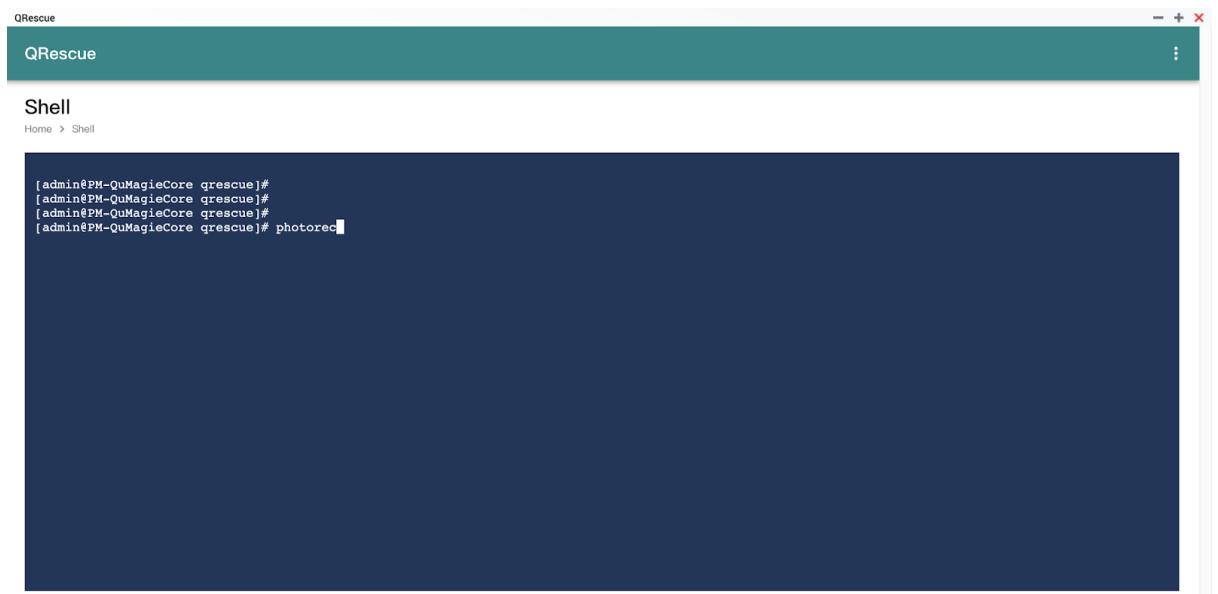
Deel 3. PhotoRec uitvoeren

Het uitvoeren van PhotoRec kan u helpen om de kwijtgeraakte bestanden op harde schijven te herstellen op de externe schijf. U herstelt de bestanden op de NAS nu naar de map 'recup1' (voorbeeld: recup+{nummer_van_schijf}) op de externe schijf.

11. Typ deze opdracht en druk op uw toetsenbord op Enter. **PhotoRec** wordt nu uitgevoerd. Opdracht:

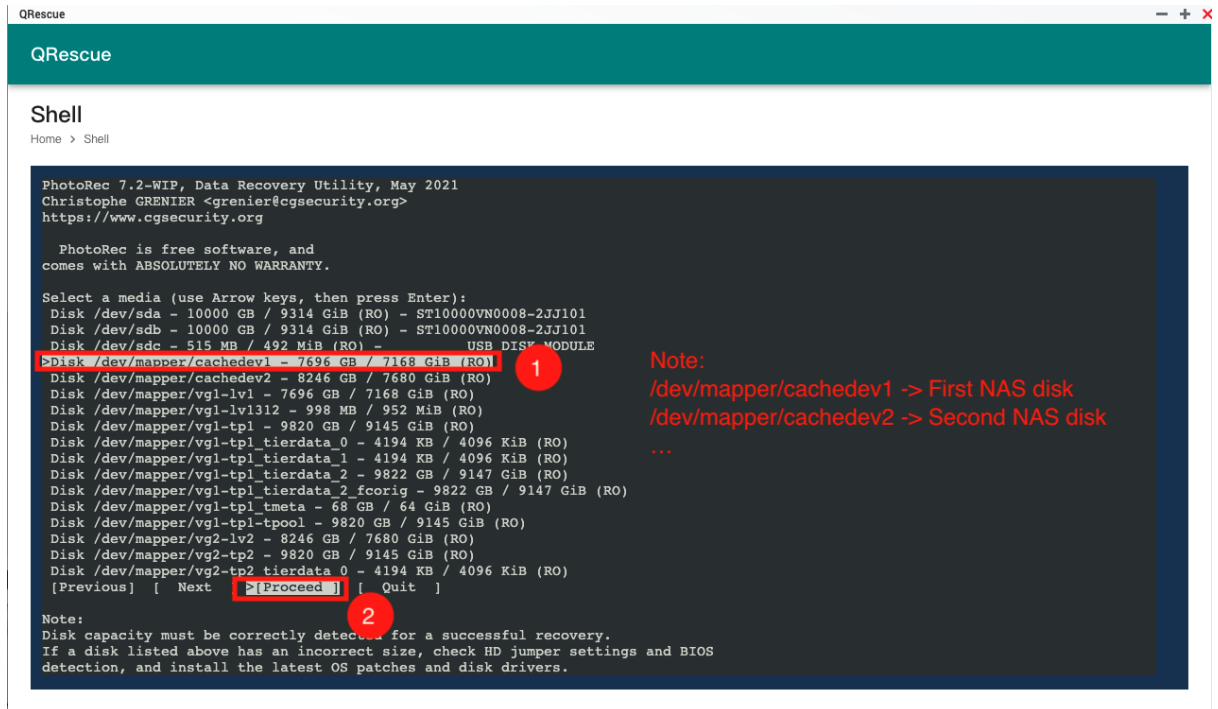
12. photorec

- 13.

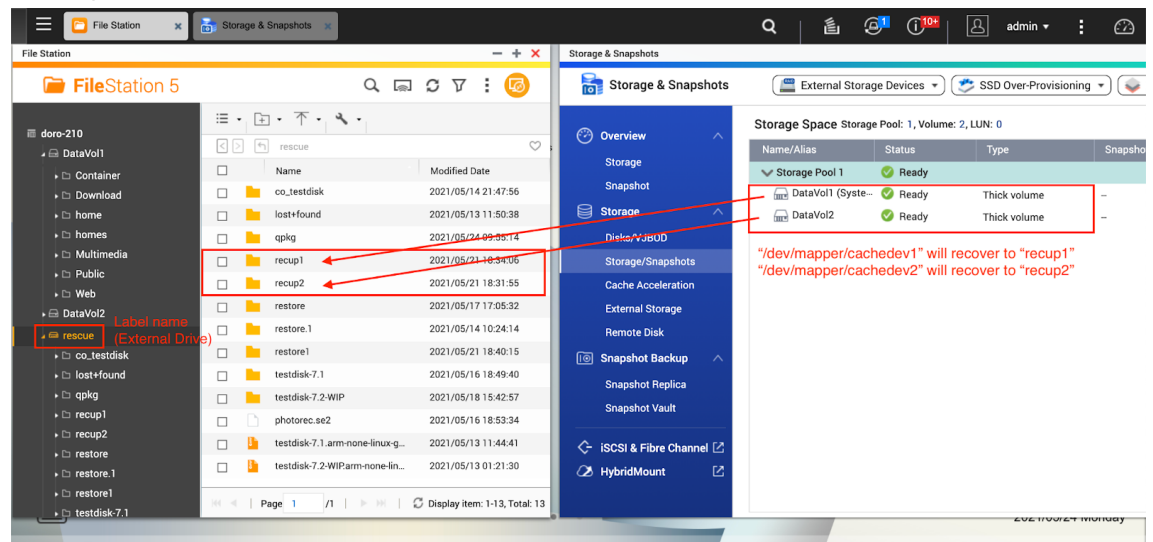


14. Gebruik de pijltjes omhoog en omlaag om de harde schijf te kiezen. Vervolgens kunt u de pijltjes naar links en rechts en 'Start' gebruiken om de schijf op de NAS te selecteren die

door **PhotoRec** moet worden hersteld;



- Voorbeeld:
 - /dev/mapper/cachedev1 als 1e gegevensvolume
 - /dev/mapper/cachedev2 als 2e gegevensvolume
 - ...
 - /dev/mapper/cachedev20 als 20e gegevensvolume
- NB:
U kunt het aantal gegevensvolumes controleren in 'Opslag en snapshots' > 'Opslag/snapshots';



15. Selecteer de 'ext4'-partitie en druk op **Enter**;

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/mapper/cachedev1 - 161 GB / 150 GiB (RO)

    Partition      Start      End      Size in sectors
    Unknown        0  0  1 314572799  0  1 314572800 [Whole disk]
> P ext4          0  0  1 314572799  0  1 314572800 [DataVol1]
```

>[Search] [Options] [File Opt] [Quit]
Start file recovery

16. Selecteer het bestandssysteem als [ext2/ext3] en druk op **Enter**;

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

P ext4          0  0  1 314572799  0  1 314572800 [DataVol1]

To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
>[ ext2/ext3 ] ext2/ext3/ext4 filesystem
[ Other      ] FAT/NTFS/HFS+/ReiserFS/...
```

17. Selecteer [**Whole**] voor de ruimte en druk op **Enter**;

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

P ext4          0  0  1 314572799  0  1 314572800 [DataVol1]

Please choose if all space needs to be analysed:
[ Free      ] Scan for file from ext2/ext3 unallocated space only
>[ Whole    ] Extract files from whole partition
```

18. We moeten nu de map met de bestemming voor het herstel op het externe apparaat selecteren;
- **Bron:** /share/external/DEV3301_01/qpkg/QRescue [QRescue qpkg]

- **Herstelbestemming:** /share/rescue/recup1 [extern apparaat]
- Klik op '..' om terug te gaan naar de bovenliggende map;

■ Voorbeeld van bestemming: Externe schijf in QRescue-app;

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /share/external/DEV3301_1/qpkg/QRescue/workspace
drwxr-xr-x  0  0      4096 22-May-2021 10:35 .
drwxr-xr-x  0  0      4096 21-May-2021 18:43 ..
lrwxrwxrwx  0  0        32 21-May-2021 18:21 1
lrwxrwxrwx  0  0        39 21-May-2021 18:21 photorec
-rw-r-----  0  0     40960 22-May-2021 10:35 photorec.se2
lrwxrwxrwx  0  0        42 21-May-2021 18:21 qrescue.pyc
lrwxrwxrwx  0  0        41 21-May-2021 18:21 qrescue.sh
lrwxrwxrwx  0  0        44 21-May-2021 18:21 sample_mem.sh
```

■ Voorbeeld: Extern apparaat (naam: 'rescue') > doelmap (naam: 'recup1');

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /share/rescue
drwxrwxrwx  0  0      4096 24-May-2021 09:55 .
drwxrwxr-x  0  0      580 21-May-2021 01:36 ..
drwxrwxrwx  0  0      4096 14-May-2021 21:47 co_testdisk
drwx-----  0  0     16384 13-May-2021 11:50 lost+found
drwxr-xr-x  0  0      4096 24-May-2021 09:55 qpkg
>drwxrwxrwx  0  0      4096 21-May-2021 18:34 recup1
drwxrwxrwx  0  0      4096 21-May-2021 18:31 recup2
drwxr-xr-x  0  0      4096 17-May-2021 17:05 restore
```

19. Klik op '**C**' op het toetsenbord als het doel '/share/rescue/recup1' is;

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /share/rescue/recup1
>drwxrwxrwx  0  0      4096 21-May-2021 18:34 .
drwxrwxrwx  0  0      4096 24-May-2021 09:55 ..
```


20. Start nu het herstelproces met PhotoRec. U kunt de geschatte tijd tot voltooiing zien;

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/mapper/cachedev1 - 64 GB / 60 GiB (RO)
  Partition      Start      End      Size in sectors
  P ext4          0    0  1 125829119    0  1 125829120 [DataVol1]

Destination /share/rescue/recup1/recup_dir

Pass 1 - Reading sector      1841344/125829120, 716 files found
Elapsed time 0h00m14s - Estimated time to completion 0h15m42
txt: 547 recovered
tx?: 74 recovered
elf: 58 recovered
mov: 11 recovered
mp3: 11 recovered
DS Store: 7 recovered
riff: 3 recovered
pdf: 2 recovered
png: 1 recovered
others: 2 recovered
Stop
```

21. Wanneer u het PhotoRec-proces voltooit, kunt u op Enter drukken wanneer u **[Quit]** selecteert of 'ctrl-c' typen om te stoppen.

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/mapper/cachedev1 - 161 GB / 150 GiB (RO)
  Partition      Start      End      Size in sectors
  P ext4          0    0  1 314572799    0  1 314572800 [DataVol1]

202724 files saved in /share/rescue/recup/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation

[ Quit ]
```

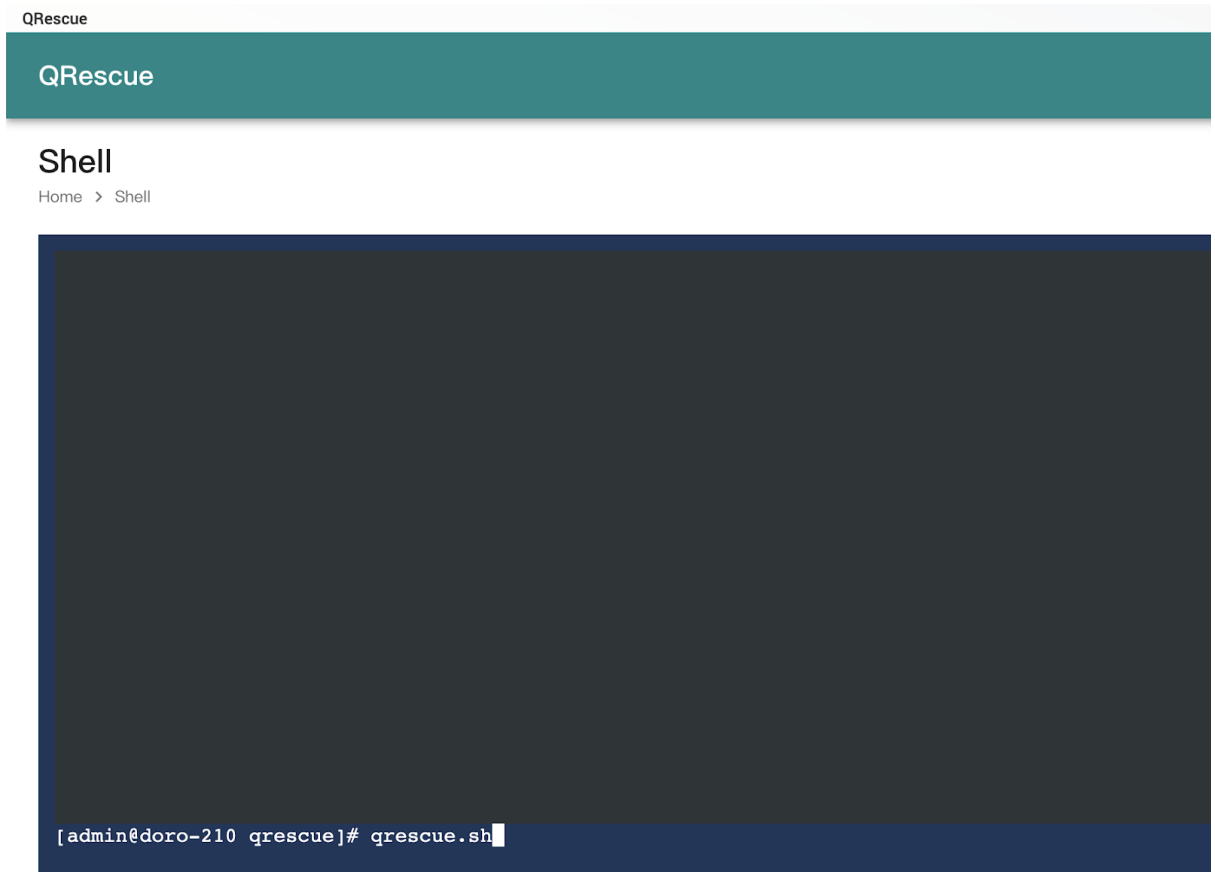
Deel 4. QRescue uitvoeren

Het uitvoeren van QRescue kan u helpen om de bestanden die PhotoRec heeft gevonden te herstellen. U herstelt de bestanden uit de map 'recup+{getal}' naar de map 'restore+{getal}', die automatisch op uw externe schijf wordt gemaakt.

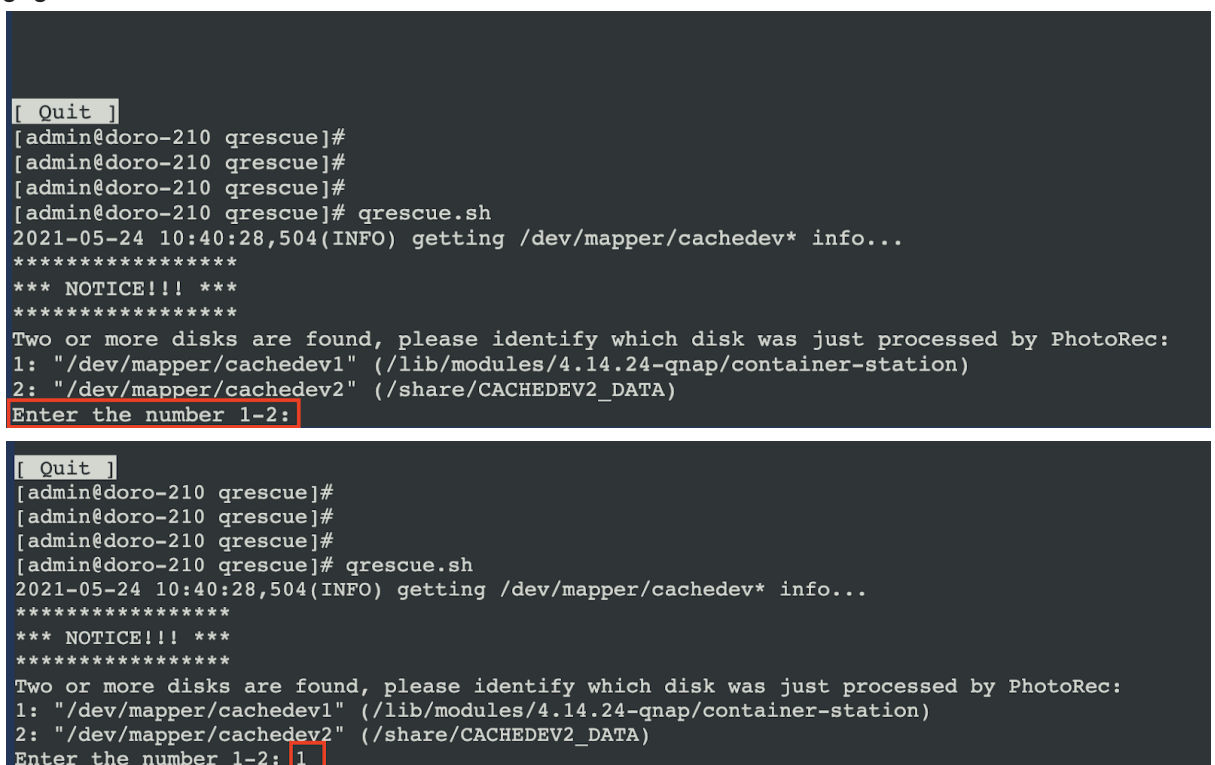
22. Typ deze opdracht en druk op uw toetsenbord op Enter. **QRescue** wordt nu uitgevoerd.
Opdracht:

23. qrescue.sh

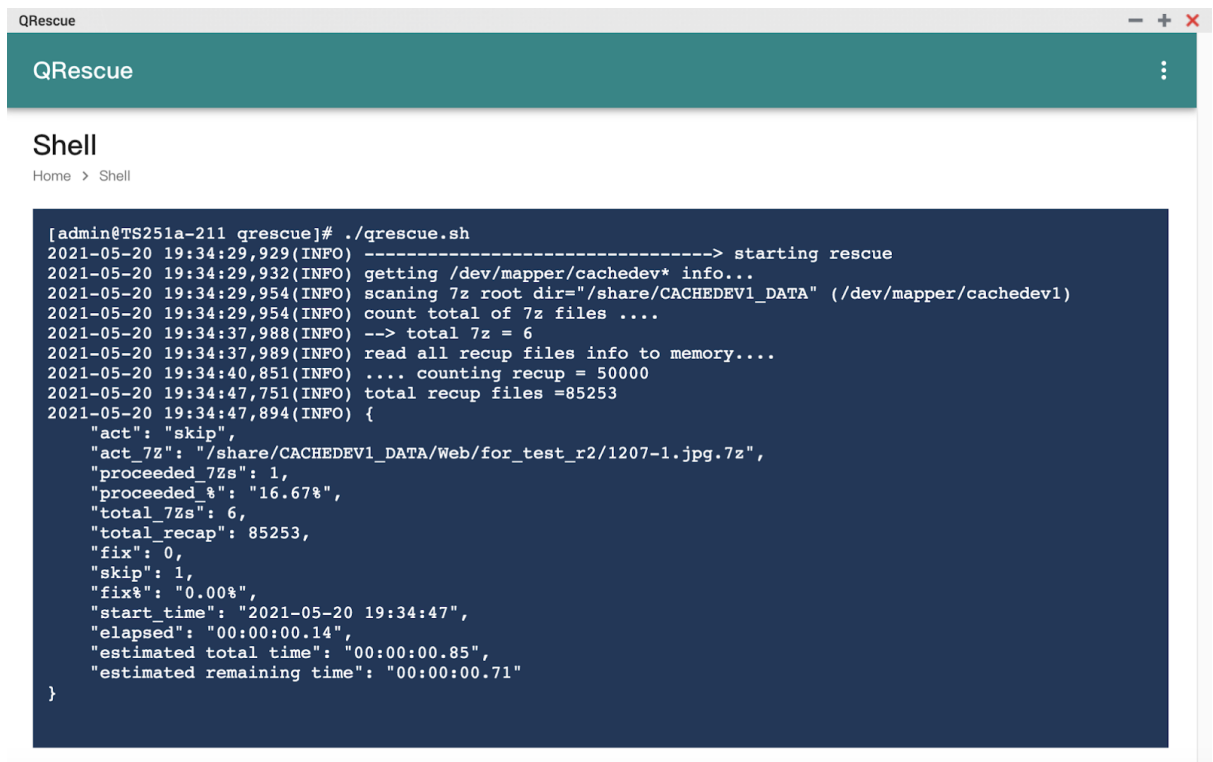
24.



25. (Optioneel) Als u minimaal twee gegevensvolumes op uw NAS hebt, kunt u op het scherm het gegevensvolume selecteren waarmee het proces wordt gestart. Typ het nummer en druk op Enter. Deze stap wordt mogelijk niet weergegeven als u maar één gegevensvolume hebt;

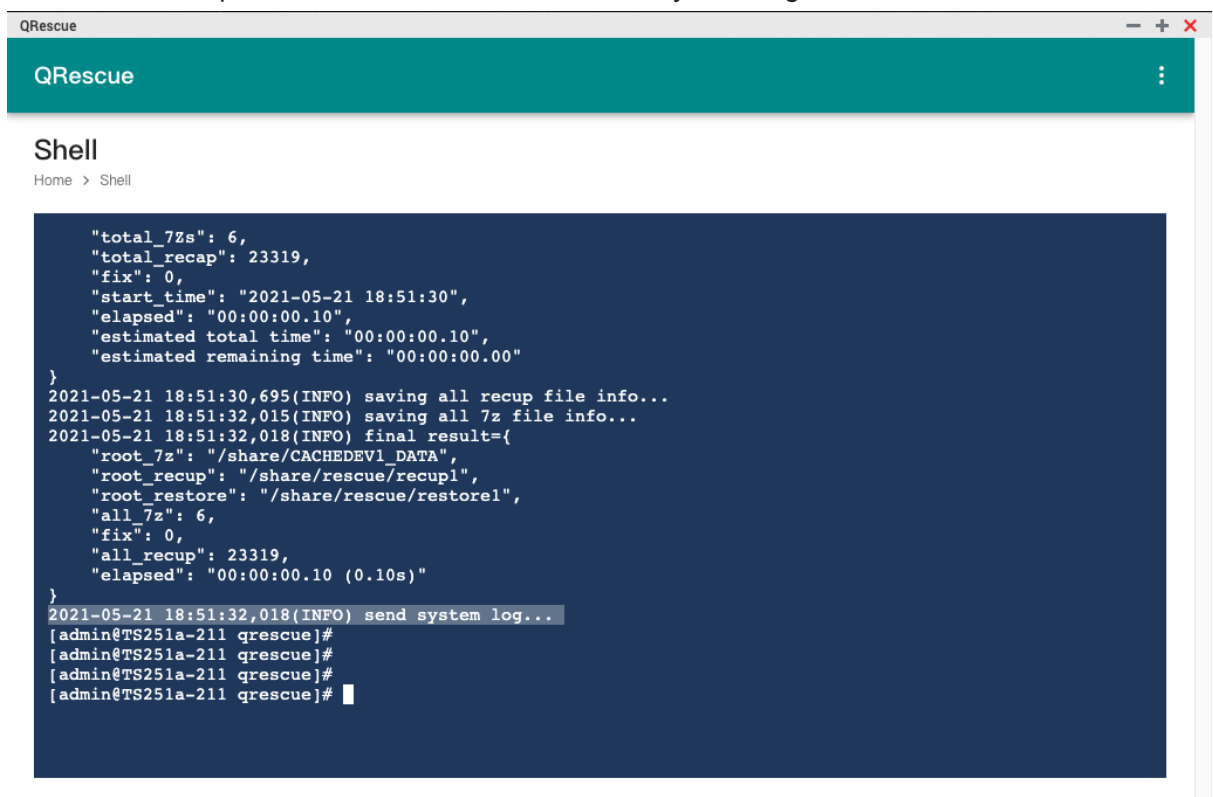


26. (Optioneel) U kunt nu de voortgang zien voor de bestanden die tijdens het herstelproces zijn voltooid;



```
[admin@TS251a-211 qrescue]# ./qrescue.sh
2021-05-20 19:34:29,929(INFO) -----> starting rescue
2021-05-20 19:34:29,932(INFO) getting /dev/mapper/cachedev* info...
2021-05-20 19:34:29,954(INFO) scanning 7z root dir="/share/CACHEDEV1_DATA" (/dev/mapper/cachedev1)
2021-05-20 19:34:29,954(INFO) count total of 7z files ....
2021-05-20 19:34:37,988(INFO) --> total 7z = 6
2021-05-20 19:34:37,989(INFO) read all recup files info to memory....
2021-05-20 19:34:40,851(INFO) .... counting recup = 50000
2021-05-20 19:34:47,751(INFO) total recup files =85253
2021-05-20 19:34:47,894(INFO) {
  "act": "skip",
  "act_7z": "/share/CACHEDEV1_DATA/Web/for_test_r2/1207-1.jpg.7z",
  "proceeded_7zs": 1,
  "proceeded_%": "16.67%",
  "total_7zs": 6,
  "total_recap": 85253,
  "fix": 0,
  "skip": 1,
  "fix%": "0.00%",
  "start_time": "2021-05-20 19:34:47",
  "elapsed": "00:00:00.14",
  "estimated total time": "00:00:00.85",
  "estimated remaining time": "00:00:00.71"
}
```

27. Als het gehele QRescue-proces is voltooid, toont het scherm u een samenvatting met de resultaten en het proces voor het verzenden van het systeemlogbestand.



```
"total_7zs": 6,
"total_recap": 23319,
"fix": 0,
"start_time": "2021-05-21 18:51:30",
"elapsed": "00:00:00.10",
"estimated total time": "00:00:00.10",
"estimated remaining time": "00:00:00.00"
}
2021-05-21 18:51:30,695(INFO) saving all recup file info...
2021-05-21 18:51:32,015(INFO) saving all 7z file info...
2021-05-21 18:51:32,018(INFO) final result={
  "root_7z": "/share/CACHEDEV1_DATA",
  "root_recup": "/share/rescue/recup1",
  "root_restore": "/share/rescue/restore1",
  "all_7z": 6,
  "fix": 0,
  "all_recup": 23319,
  "elapsed": "00:00:00.10 (0.10s)"
}
2021-05-21 18:51:32,018(INFO) send system log...
[admin@TS251a-211 qrescue]#
[admin@TS251a-211 qrescue]#
[admin@TS251a-211 qrescue]#
[admin@TS251a-211 qrescue]#
```

28. De QRescue-app stuurt tevens het gebeurtenislogbestand naar QuLog Center/System Log en informeert u als het gehele herstelproces is voltooid. Vergeet niet om feedback op

uw casus te geven als u een QNAP-ondersteuningsticket hebt geopend. Het QNAP-ondersteuningsteam helpt u dan met een extra controle. Heel erg bedankt.

Deel 5. Verplaats de herstelde gegevens naar uw NAS.

U kunt de herstelde gegevens naar uw NAS verplaatsen met behulp van File Station.

