

Qlocker で暗号化されてしまった QNAP NAS 上のファイルを回復させるために QRescue を手動インストールする

概要:

QRescueは、Qlockerで暗号化されてしまった7zファイルのためのデータ復元ツールです。次のものが含まれます。

- PhotoRec (オープンソースプロジェクト / [GNU一般公衆利用許諾書](#) / [プロジェクトへのリンク](#)):
ハードディスクやCD-ROMから失われてしまったファイル、およびストレージメディアから失われてしまった画像 (名称はPhoto Recovery) を復元するために設計されたファイル復元ソフトウェア。
- QRescue (QNAP開発):
暗号化されてしまった7zファイルとPhotoRecファイルから、ファイル構造を復元するスクリプト。

要件:

- QRescueアプリ、ダウンロードは[このリンク](#)。
<https://download.qnap.com/QPKG/QRescue.zip>
- お使いのNASの使用済の合計ストレージ領域より大きい容量の外部ハードディスクをご用意ください。
 - 注: お使いのNASの使用済の合計ストレージ領域より1.5倍～2倍の空き容量をもつ外部HDDを用意されることをお勧めします。復元処理中に追加の領域が必要になる場合があります。利用可能な領域が推奨値より小さい場合、エラーやその他の問題が発生する場合があります。

あります。



デモビデオ:

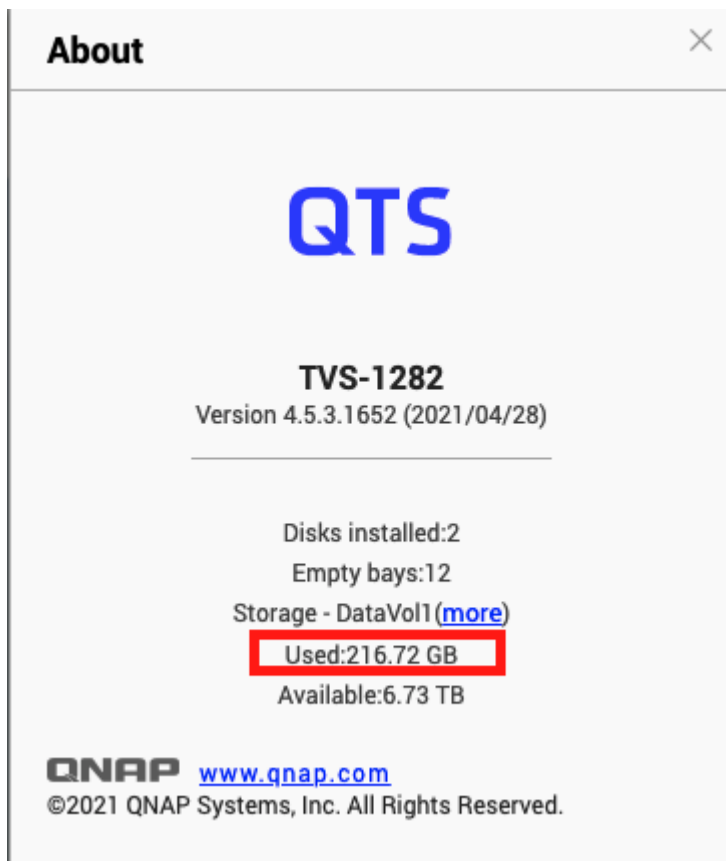
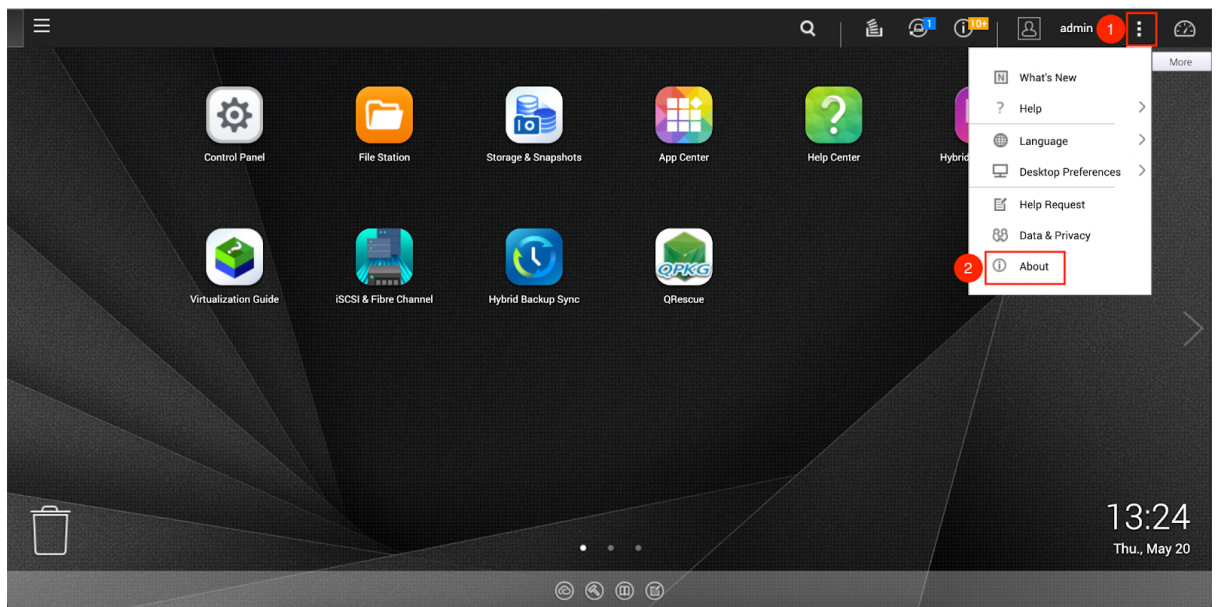
- [このリンク](#)をご参照ください。

手順:

パート1: 外部HDDに「rescue」という名前をつけ、「recup1」という名前の復元用フォルダーを作成します。

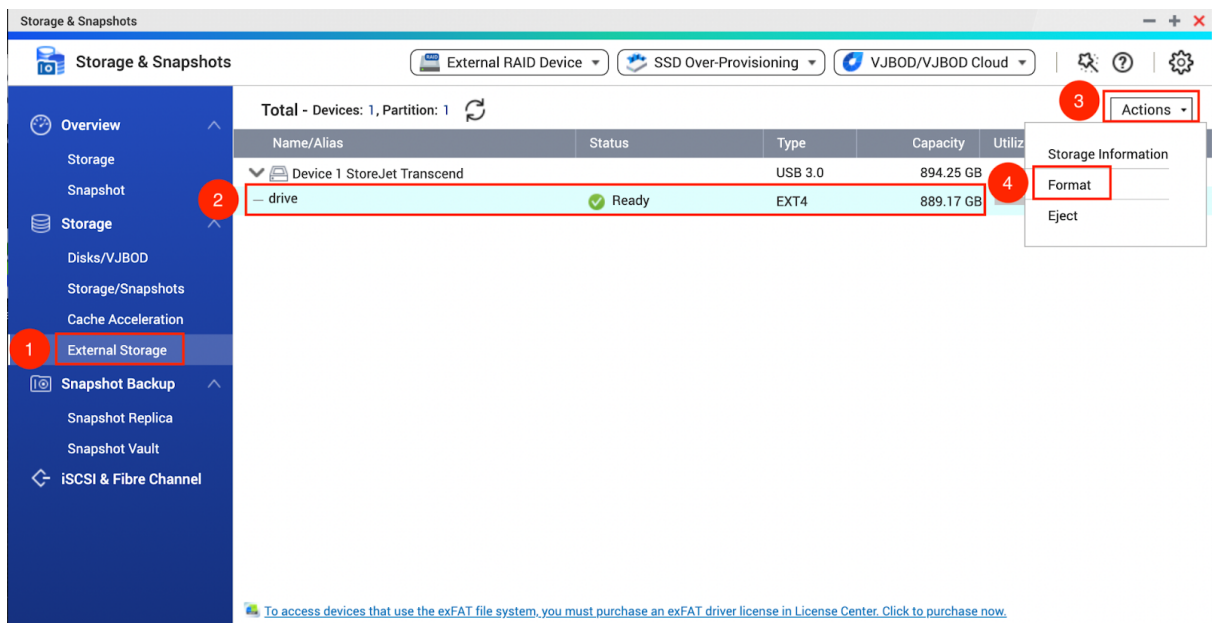
QRescueはまず外部ドライブへの復元処理を開始します。この復元処理ではいくつかの設定を行い、特定の宛先にフォルダーを作成します。

1. お使いのNASの使用済の合計ストレージのサイズよりも大きい空き容量が使用できる外部HDDを用意されることをお勧めします。これは、ファイルがまず外部HDDで復元されるためです。まずQTSデスクトップで[詳細] > [情報]をクリックし、使用済ボリュームサイズを確認してください。

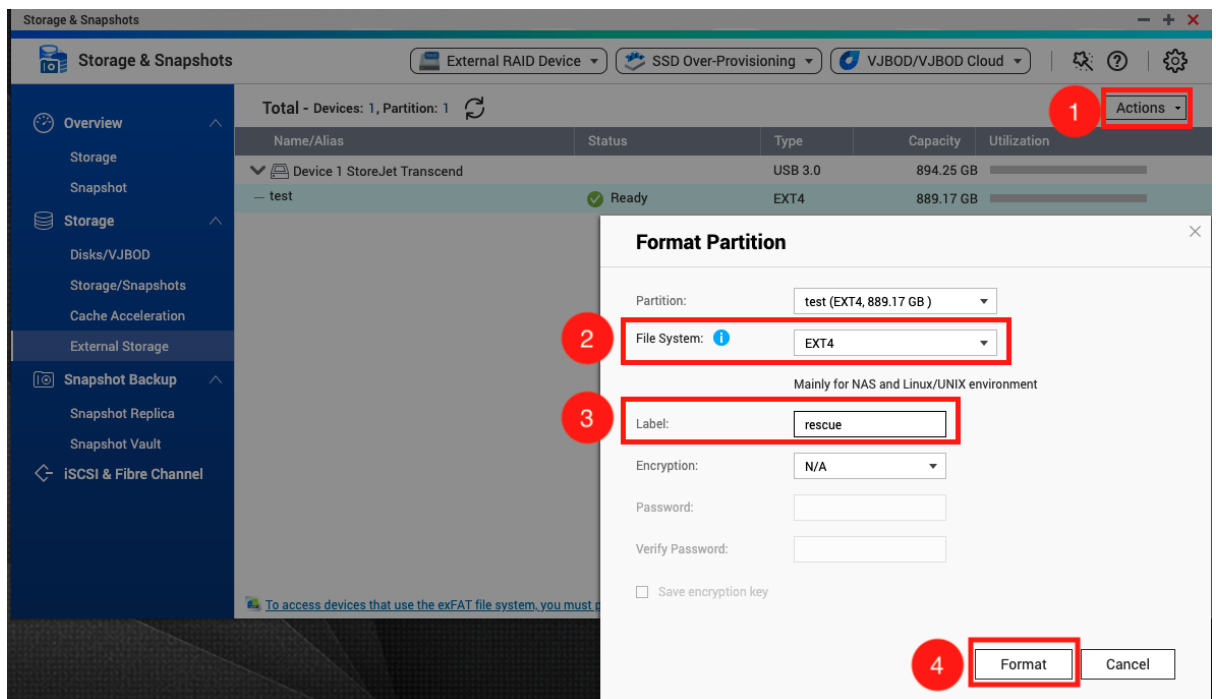


2. 外部ドライブをNASに挿入します。外部ドライブのフォーマットには、[ストレージマネージャー] > [外部デバイス] > [外部デバイスを選択] に進み、[アクション] をクリックし、[フォーマット] をクリックし

て外部ドライブをフォーマットします。



3. ファイルシステムは「EXT4」で、ラベル名は「rescue」を入力します。この設定ができれば、[フォーマット]をクリックします



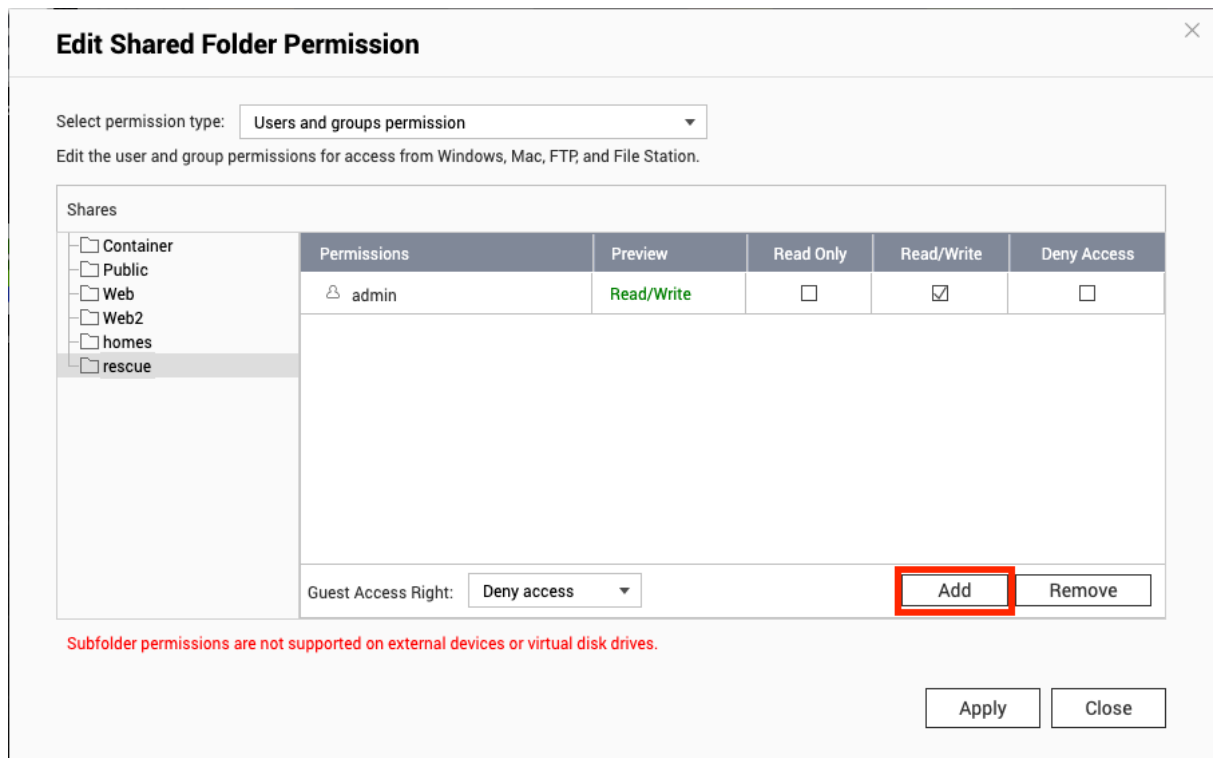
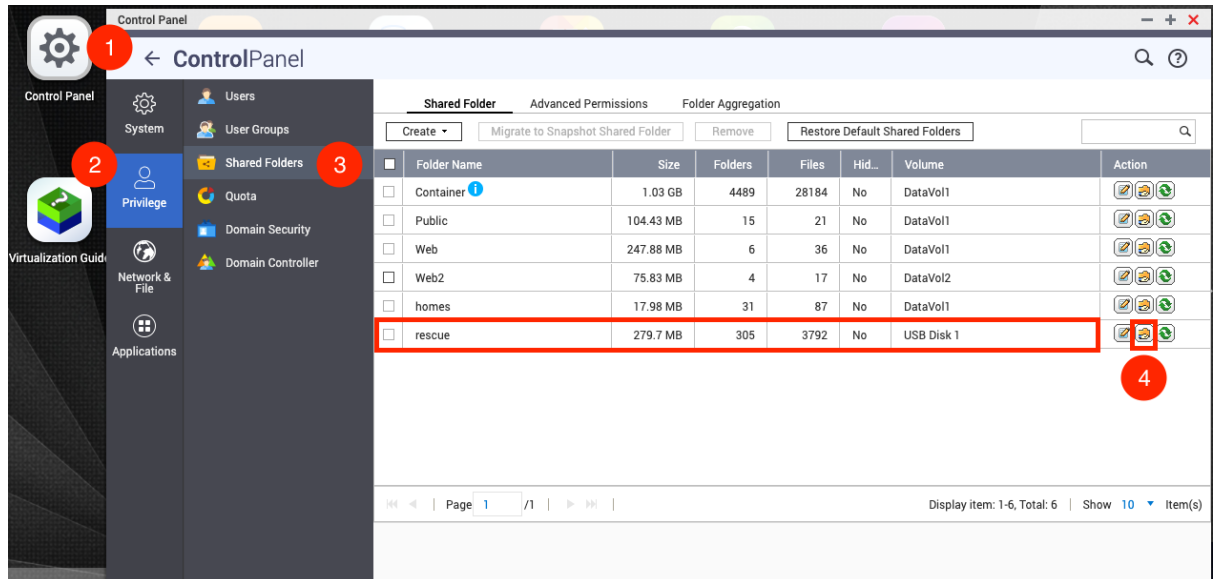
注意:

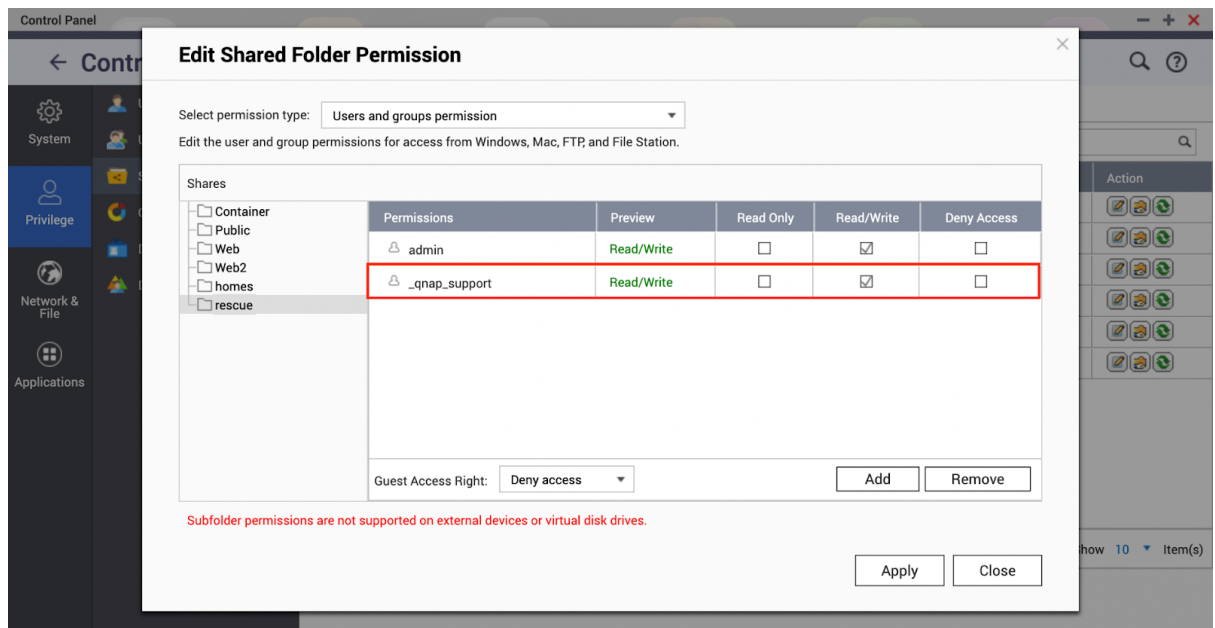
QRescueアプリは、外部ドライブ名として「rescue」を使用します。それ以外の名前を使用すると、復元処理が失敗することがあります。

4. (オプション) 管理者アカウントが無効になっていたり、QTSへのログインにadminを使用しないと、File Stationにその外部ドライブが表示されないことがあります。[コントロールパネル] > [rescue] > [共有フォルダー] > [共有フォルダー権限の編集]に進み、[rescue]フォルダーに対する読み取り/書き込み権限をNASにログインするアカウントと一致するように有効あるいは変更してください。

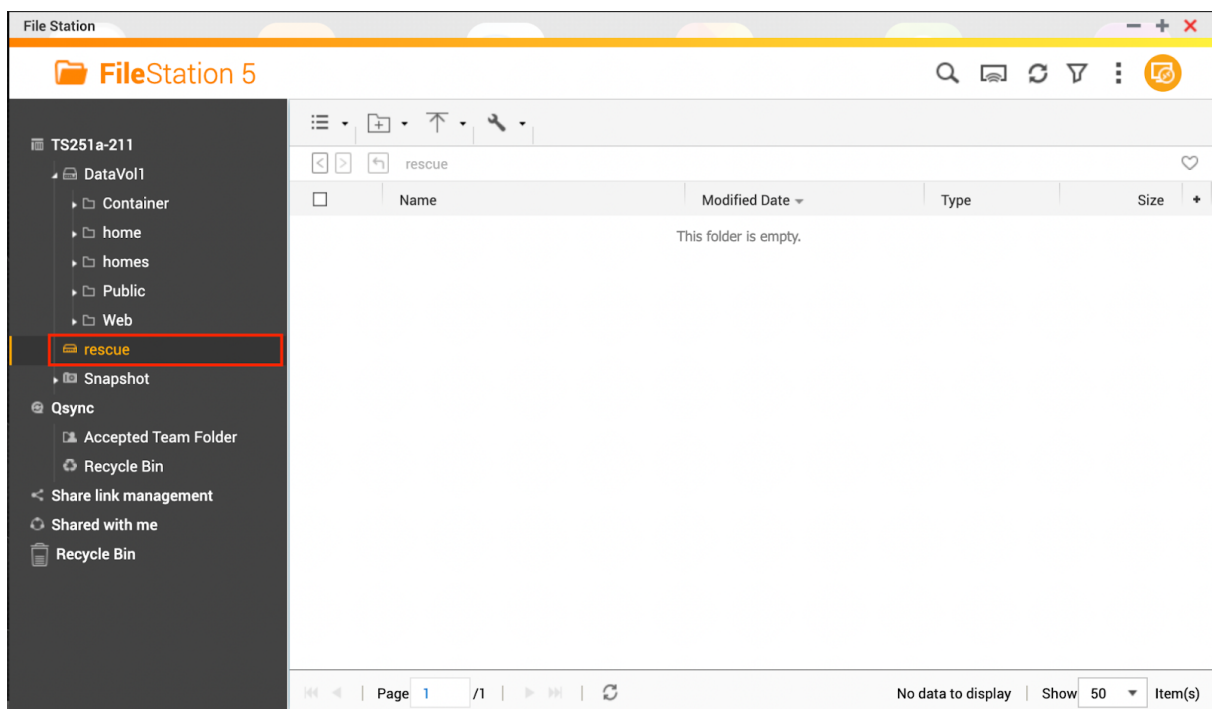
○ 例:

別の管理者グループアカウントを付与します (たとえば、「rescue」という名前の外部ハードドライブへの読み取り/書き込み権限のため「_qnap_support」が管理者グループアカウントであるなど)。

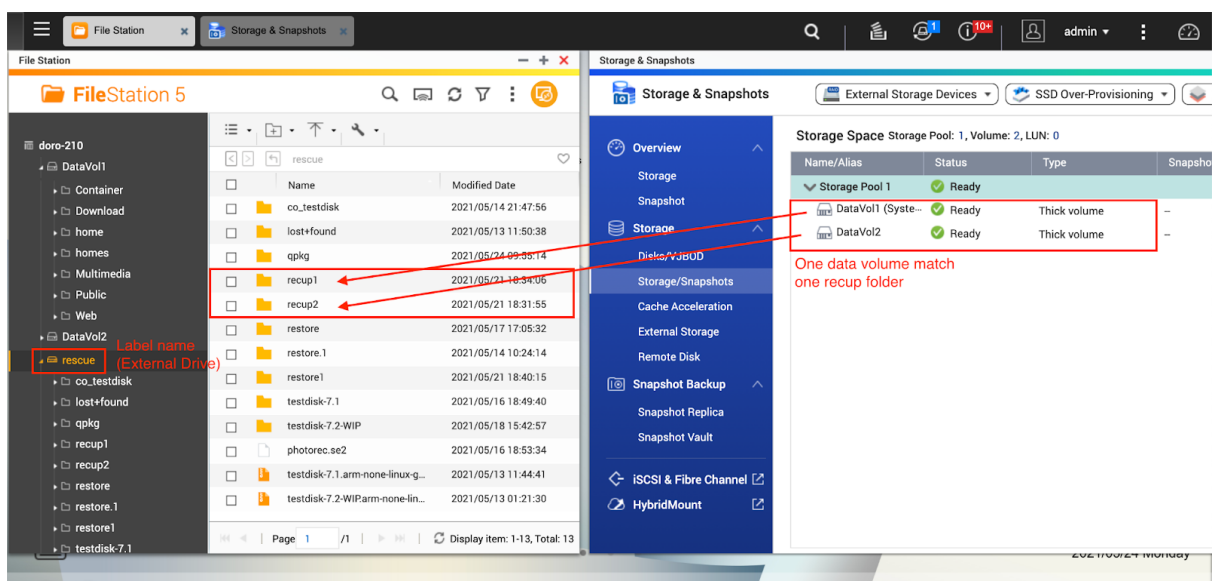
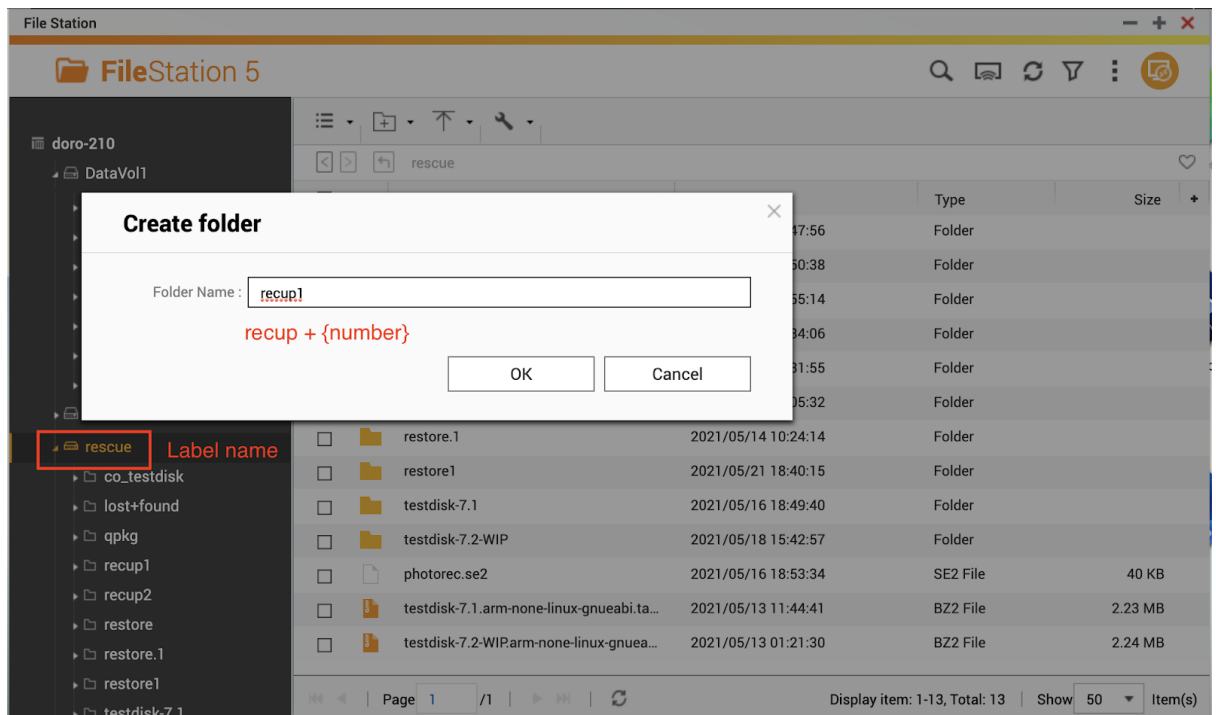




- File Stationを使って外部デバイス名が正しいことをボリュームで確認します。



- 新しいフォルダーを作成し、「recup1」という名前をつけます (形式:recup+{数字})。複数のストレージボリュームをもっている場合、復元にはさらに多くのフォルダーが必要です。



注記:

QRescueアプリは、フォルダー名として「recup+{数字}」を使用します。それ以外の名前を使用すると、復元処理が失敗することがあります。

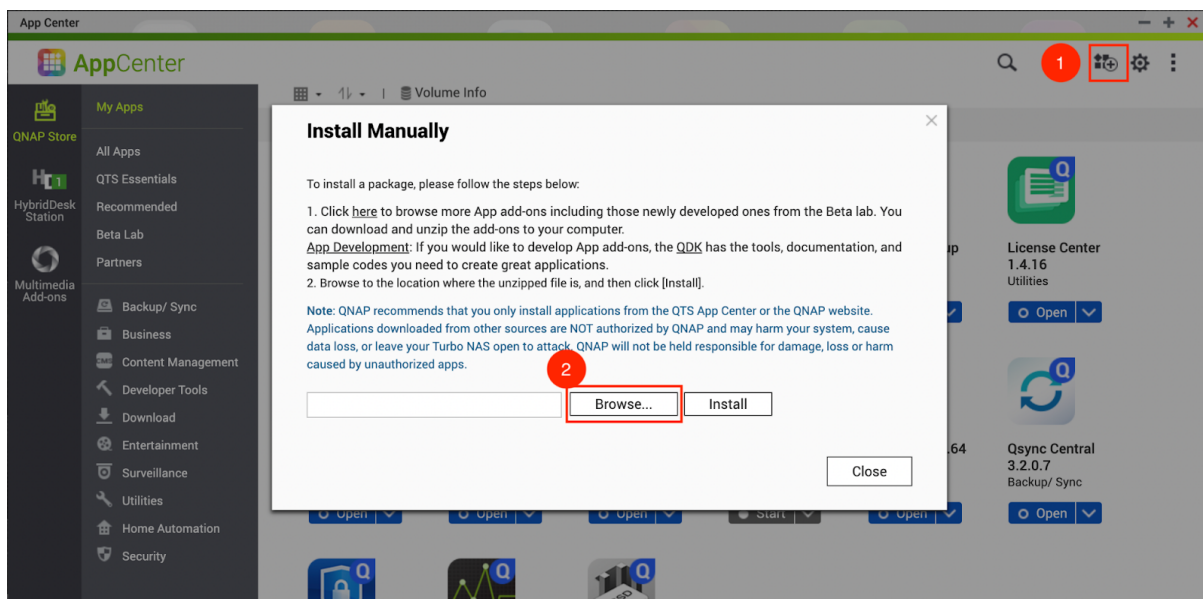
パート2: QRescueアプリをダウンロードし、手動でインストールする

このQRescueアプリは特別に作られたものです。そのため、このアプリはQTS App Centerから手動でインストールする必要があります。

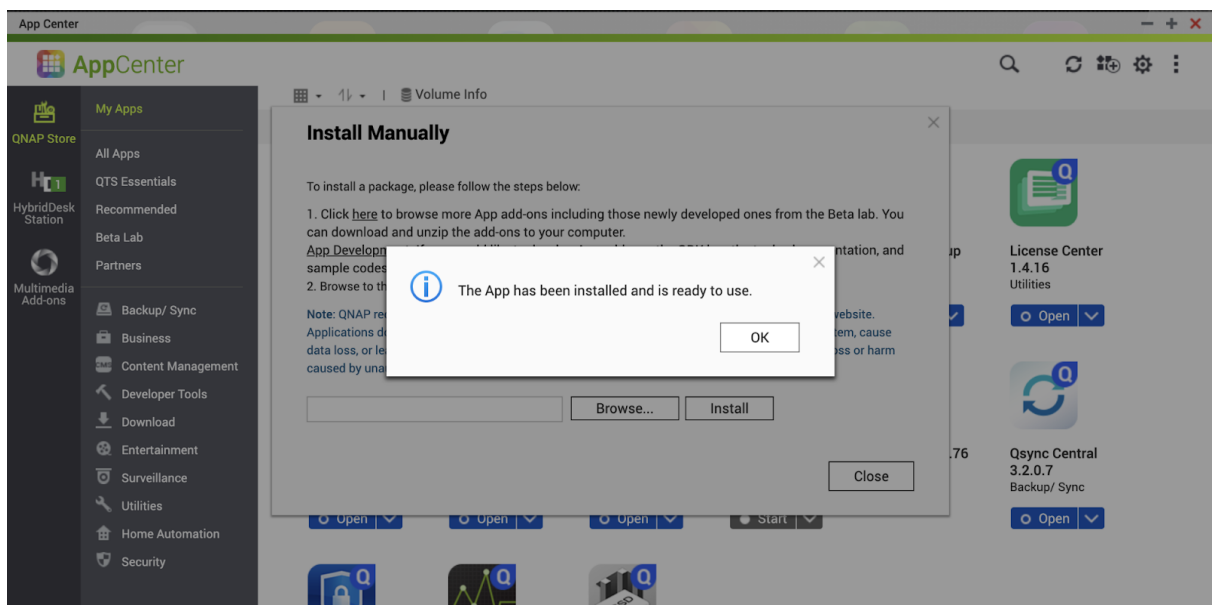
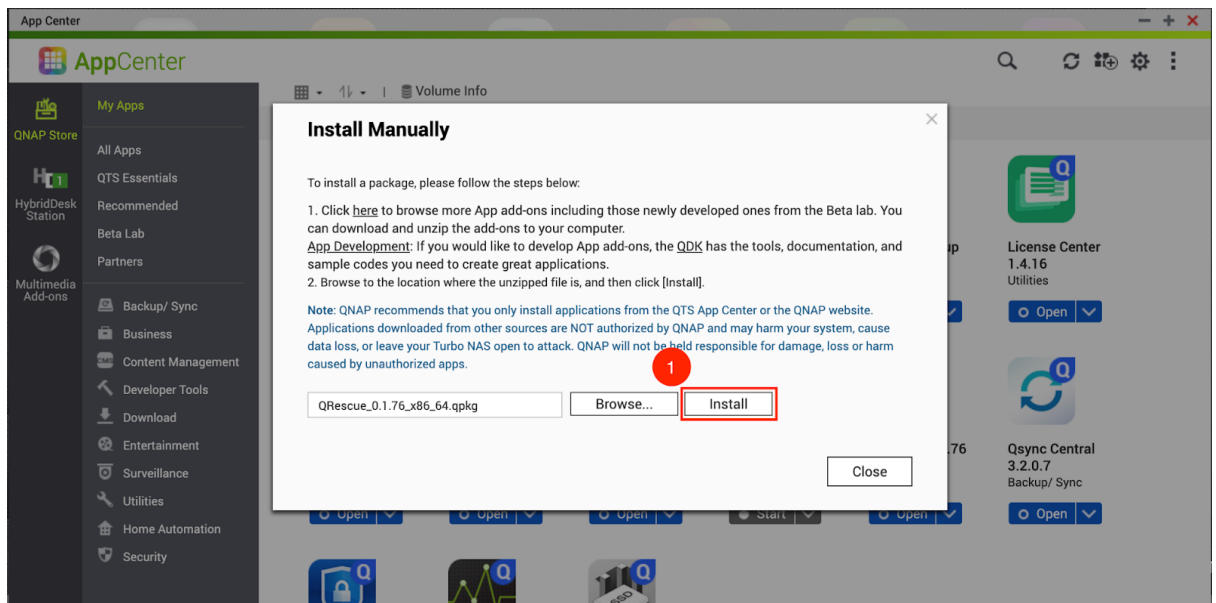
7. QRescueアプリをダウンロードするには、[このリンク](https://download.qnap.com/QPKG/QRescue.zip)に進んでください。

<https://download.qnap.com/QPKG/QRescue.zip>

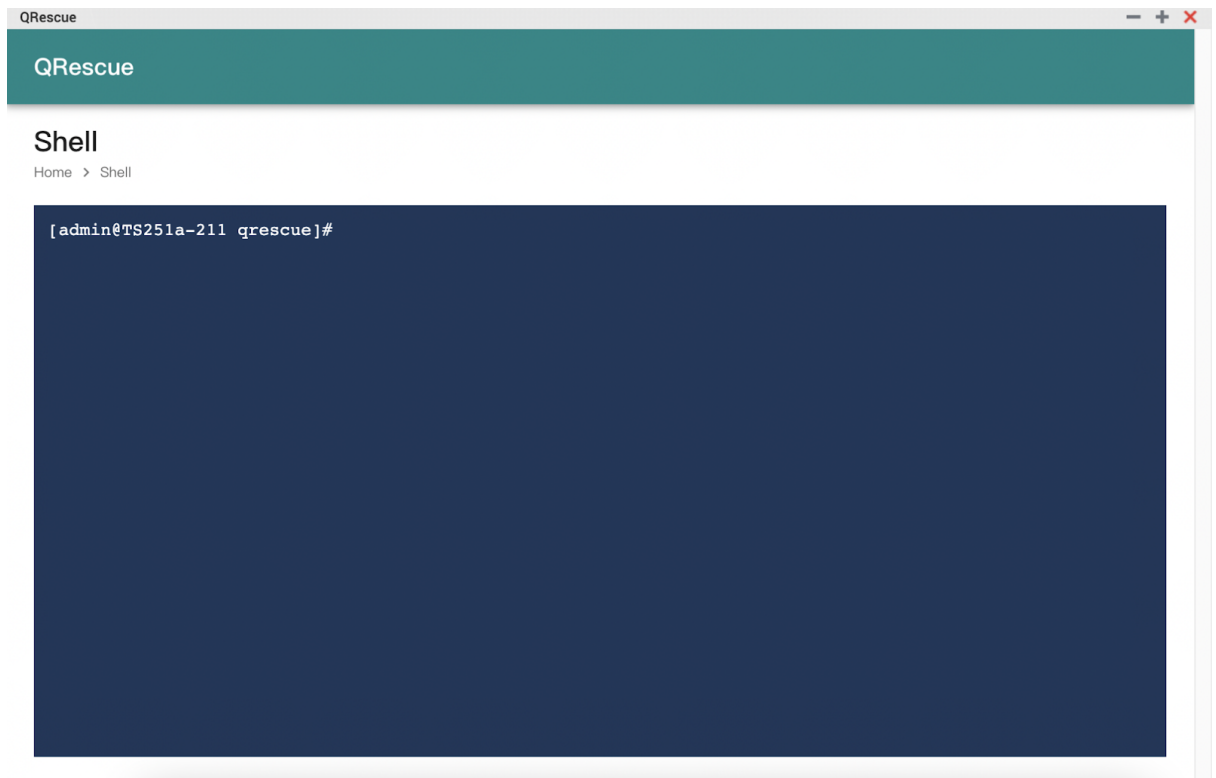
8. [App Center]に進み、[手動インストール]をクリックし、[表示]をクリックしてコンピューター上のQRescueアプリの場所を見つけます。



9. アプリの場所を選択した後、[インストール]をクリックします。インストールが終わるまで待ってから、QTSデスクトップまたはサイドバー上のQRescueアプリを開きます。



10. QRescueアプリを開くと、ウェブコンソールが表示されます。それはファイルを回復させるためのPhotoRecとQRescueを実行するのに役立ちます。



パート3: PhotoRecを実行

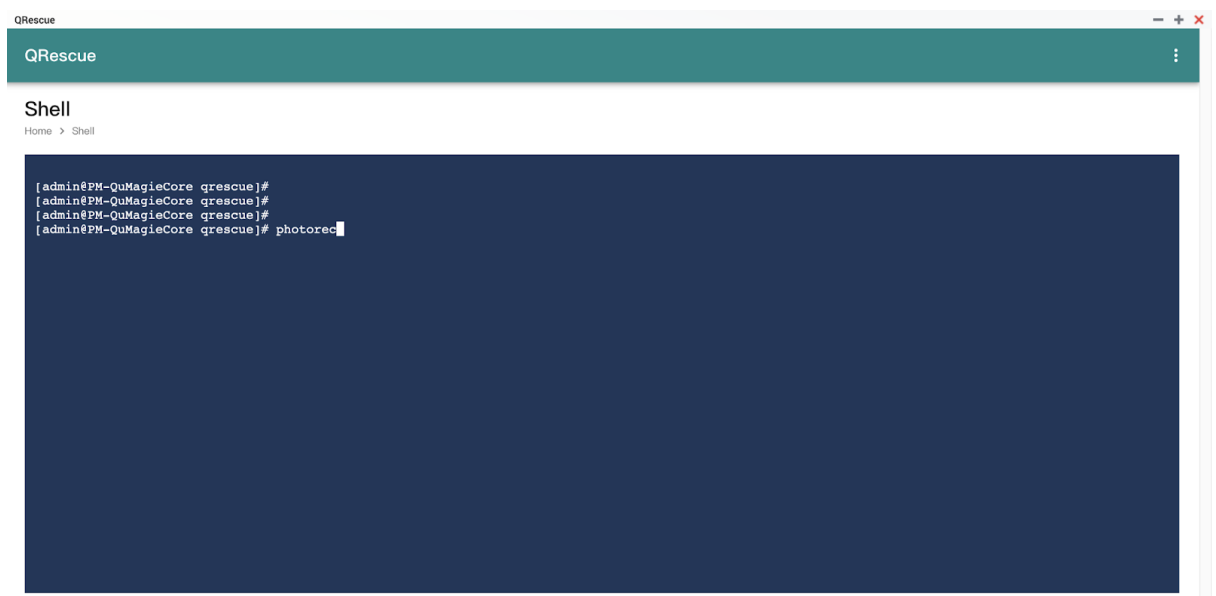
PhotoRecを実行することにより、失われてしまったファイルをハードディスクから外部ドライブに復元する作業に進みます。ここではNASファイルが、外部ドライブの「recup1」(たとえばrecup+{ディスク番号}) フォルダに復元されます。

11. このコマンドを入力し、キーボードの[Enter]を押します。**PhotoRec**を実行します。

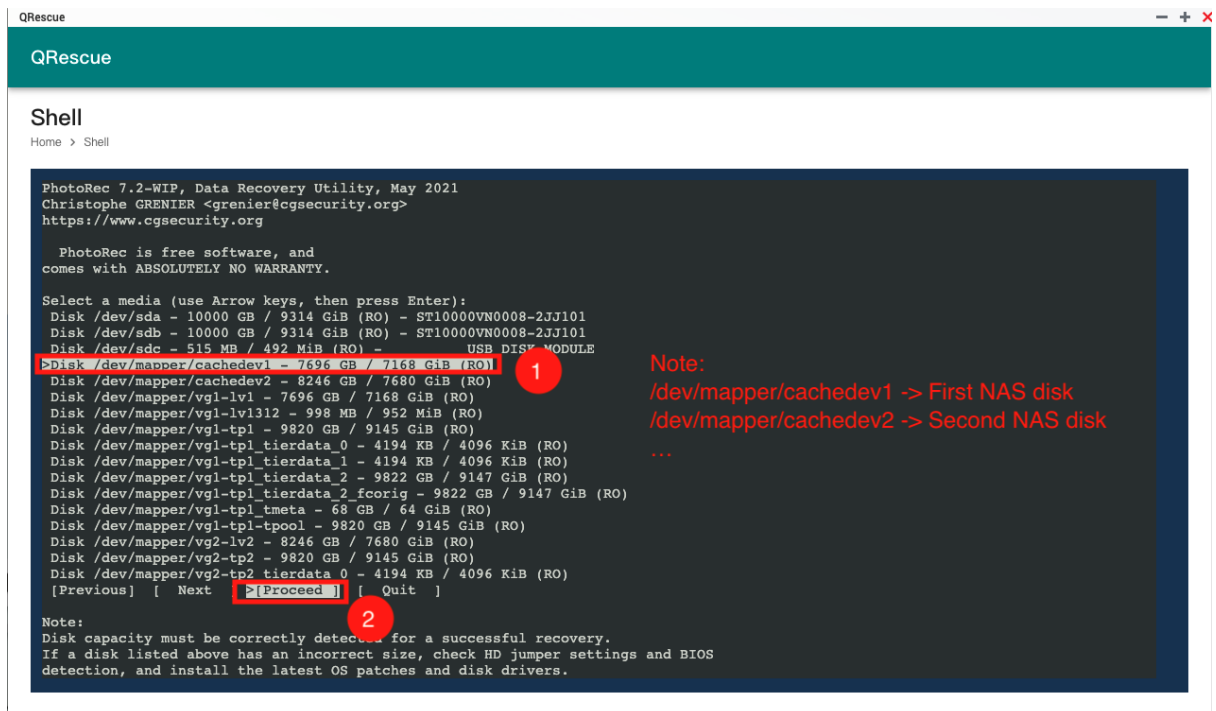
コマンド:

12. photorec

- 13.



14. 上下の矢印を使って外部ドライブを選択します。次に左右の矢印を使って**PhotoRec**が復元するNASディスクを選択します

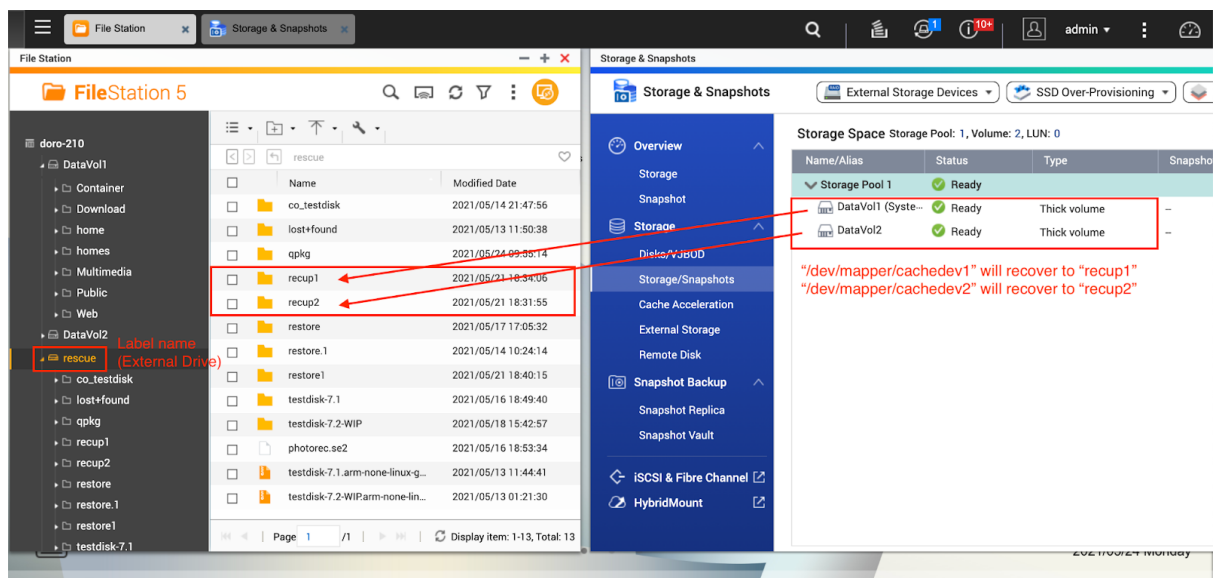


- 例:

- /Dev/mapper/cachedev1 (最初のデータボリューム)
- /dev/mapper/cachedev2 (2番目のデータボリューム)
- ...
- /dev/mapper/cachedev20 (20番目のデータボリューム)

- 注:

データボリュームの数は、[ストレージ&スナップショット] > [ストレージ/スナップショット]で確認できます。



15. [ext4]を選択して、[Enter]を押します。

```
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. ファイルシステムは[ext2/ext3]と選択し、[Enter]キーをクリックします。

```
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. 領域は[すべて]を選択し、[Enter]キーをクリックします。

```
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. ここでは、外部デバイスのフォルダーを復元先として選択する必要があります。

- ソース元/share/external/DEV3301_01/qpkg/QRescue [QRescue qpkg]
- 復元先: /share/rescue/recup1[外部デバイス]
- 上位レベルのフォルダーに戻るには[...]をクリックします。

■ デスティネーションの例: QRescueアプリ上の外部ディスク

```
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_01/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 l
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
```

■ 例: 外部デバイス (名前: rescue) > デスティネーションフォルダー (名前: 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. デスティネーションが[/share/rescue/recup1]の場合、キーボードのCをクリックします。

```
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. PhotoRecを実行して復元処理を開始します。完了までの予測時間が表示されます。

```
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. PhotoRecが終わった時点で、[Quit]を選択して押すか、または[ctrl + C:trl-c]を入力して終了します。

```
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 ]
```

パート4: QRescueを実行

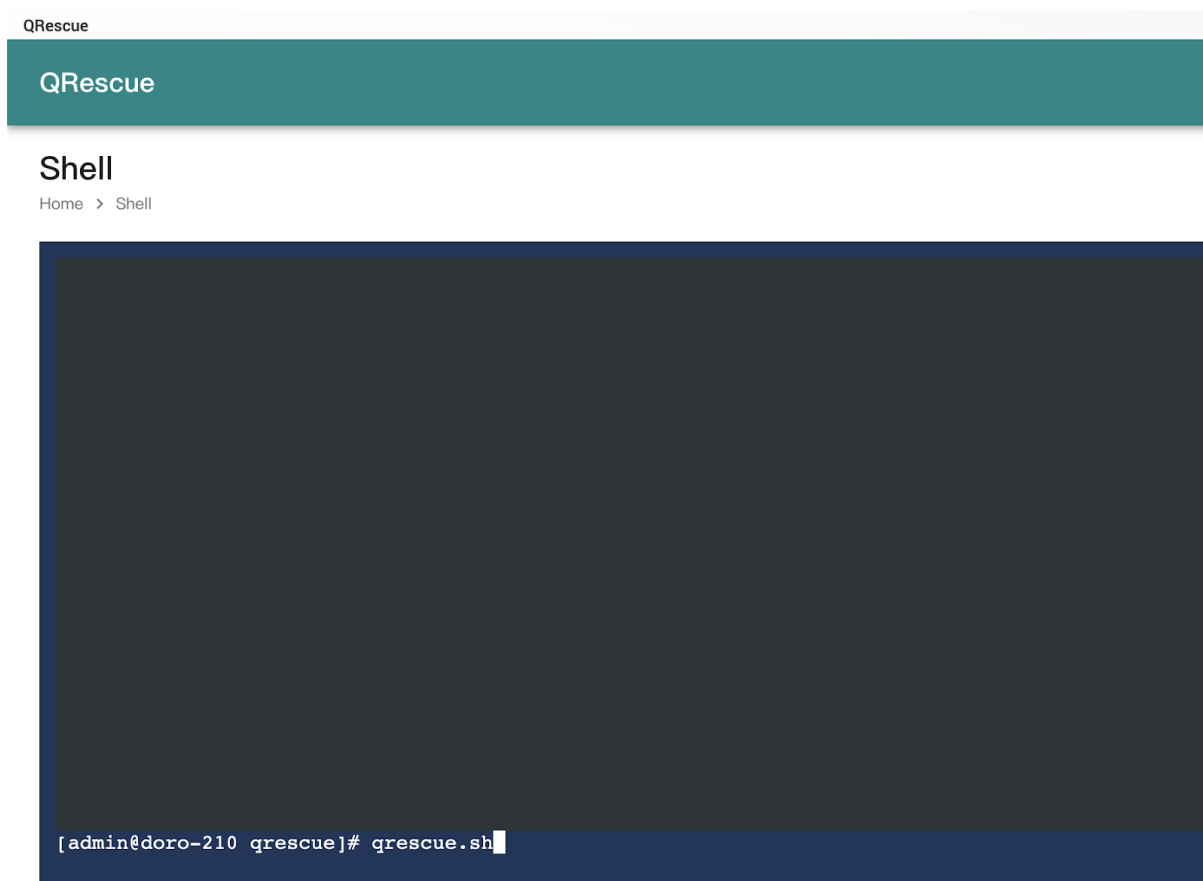
QRescueを実行し、PhotoRecで取り出されたファイルを復元する作業に進みます。ここでは、「recup+{数字}」フォルダーから外部ドライブ上に自動生成される「restore+{数字}」フォルダーにファイルを復元します。

22. このコマンドを入力し、キーボードの[Enter]をクリックします。QRescueを実行します。

コマンド:

23. qrescue.sh

24.

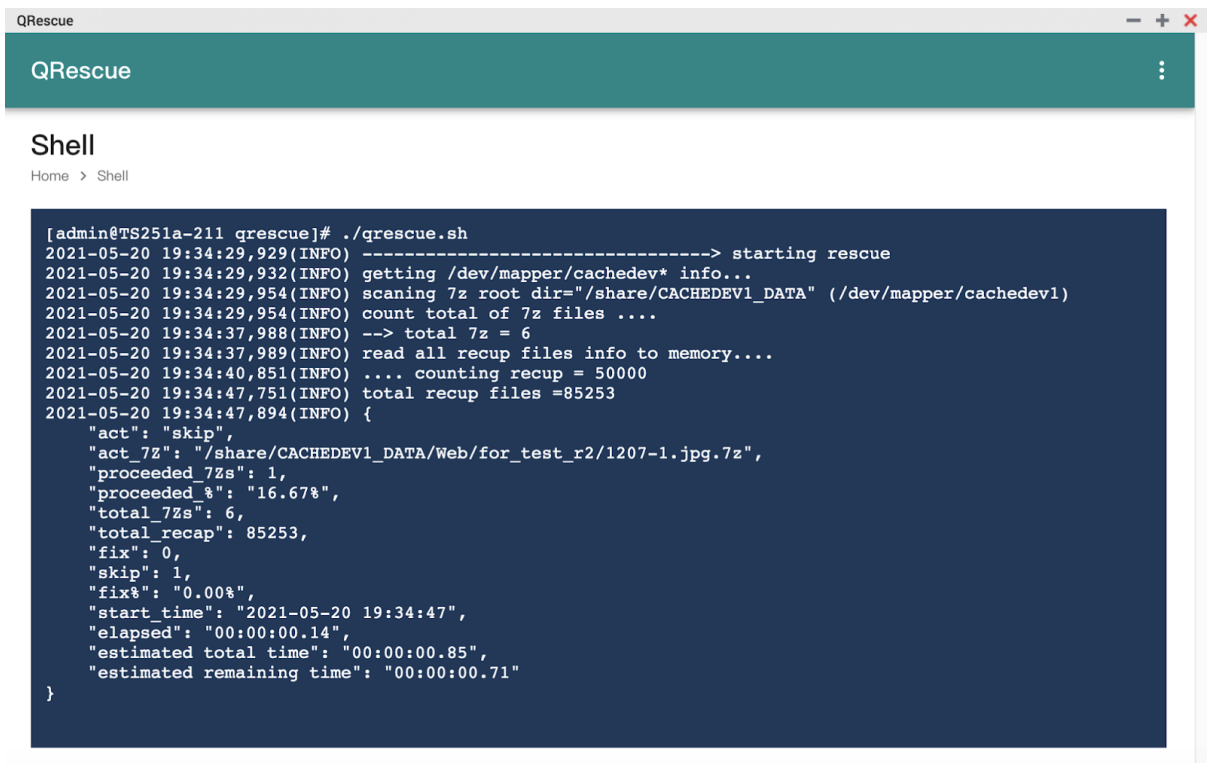


25. (オプション) お使いのNASに複数のデータボリュームがある場合、処理を開始するデータボリュームを選択する画面になります。数字を入力し、[Enter]を押します。データボリュームが1つの場合、この手順は現れません。

```
[ Quit ]
[admin@doro-210 qrescue]#
[admin@doro-210 qrescue]#
[admin@doro-210 qrescue]#
[admin@doro-210 qrescue]# qrescue.sh
2021-05-24 10:40:28,504(INFO) getting /dev/mapper/cachedev* info...
*****
*** NOTICE!!! ***
*****
Two or more disks are found, please identify which disk was just processed by PhotoRec:
1: "/dev/mapper/cachedev1" (/lib/modules/4.14.24-qnap/container-station)
2: "/dev/mapper/cachedev2" (/share/CACHEDEV2_DATA)
Enter the number 1-2:
```

```
[ Quit ]
[admin@doro-210 qrescue]#
[admin@doro-210 qrescue]#
[admin@doro-210 qrescue]#
[admin@doro-210 qrescue]# qrescue.sh
2021-05-24 10:40:28,504(INFO) getting /dev/mapper/cachedev* info...
*****
*** NOTICE!!! ***
*****
Two or more disks are found, please identify which disk was just processed by PhotoRec:
1: "/dev/mapper/cachedev1" (/lib/modules/4.14.24-qnap/container-station)
2: "/dev/mapper/cachedev2" (/share/CACHEDEV2_DATA)
Enter the number 1-2: 1
```

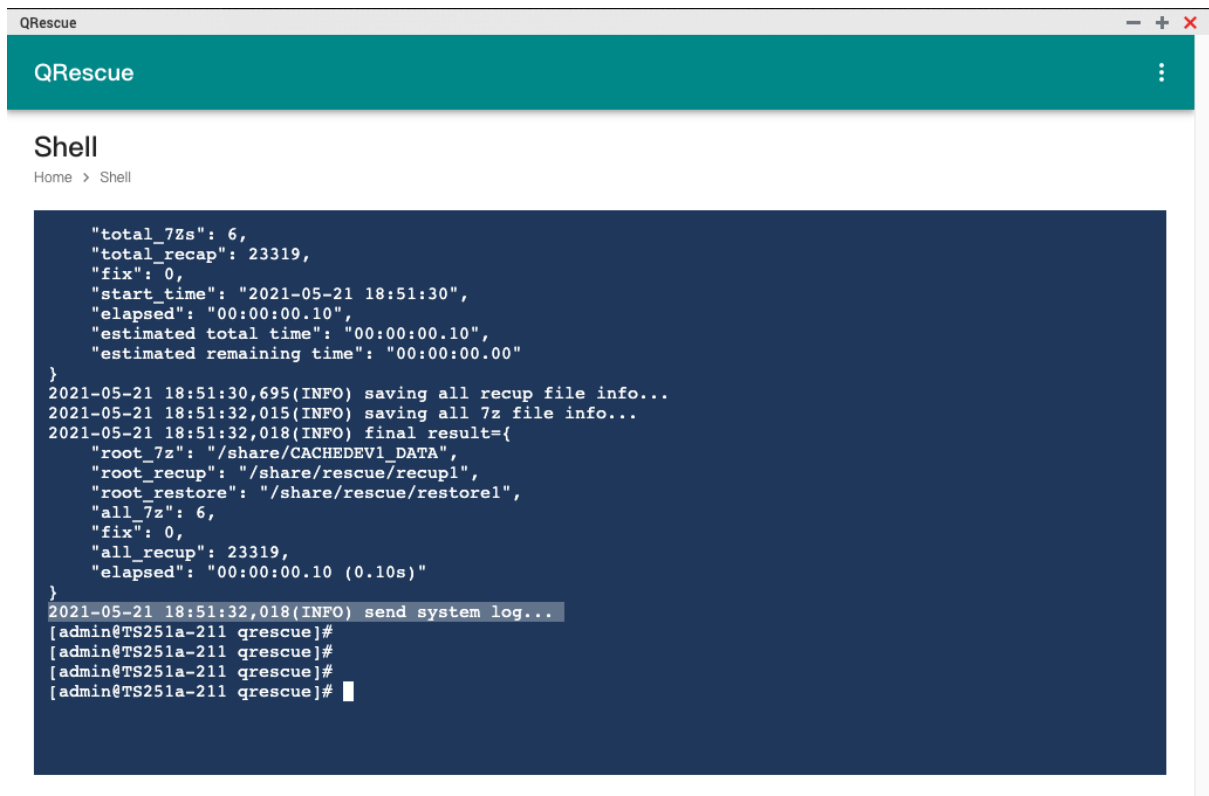
26. (オプション) 復元処理中にどのファイルが完了したかの進行状況が表示されます。



The screenshot shows the QRescue application window. The title bar is labeled "QRescue". Below the title bar is a teal header with the text "QRescue" and a menu icon. The main content area is titled "Shell" and shows a terminal window with the following output:

```
[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. QRescue処理のすべてが完了すると、画面には結果の要約とシステムログ送信処理が表示されます。



The screenshot shows a window titled "QRescue" with a teal header. Below the header, the text "Shell" is displayed, followed by a breadcrumb "Home > Shell". The main area is a dark blue terminal window showing the following output:

```
"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 recap 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. QRescueアプリはイベントログをQuLog Center / System Log に送信し、復元処理が終了したことを通知します。QNAPサポートチケットを開いている場合、ご自分のケースに対するフィードバックをすることを忘れないでください。QNAPサポートチームが再確認のためにご協力します。どうもありがとうございます。

パート5: NASにリカバリデータを移動します。

復元データはFile StationによってNASに移動することができます。

