

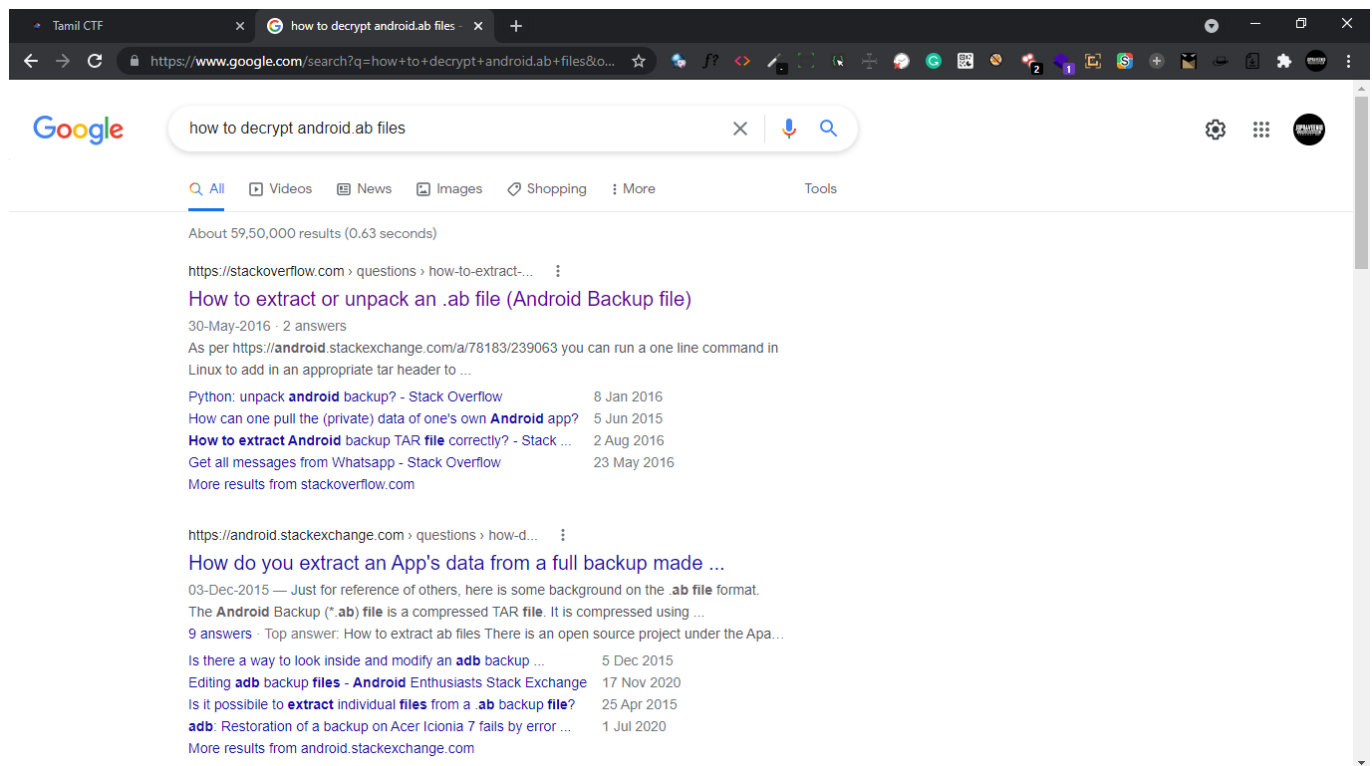
Hey I'm AB

Description

My phone got crashed and I took a backup of some important data

Challenge

- ▶ There's a download link let's download it
- ▶ we got a file named `android.ab`
- ▶ let's google how to decrypt this file



and got this

Stack Overflow question: <https://stackoverflow.com/questions/18533567/how-to-extract-or-unpack...>

2 Answers

92

Replace **backup.ab** with the path to your file.

Share Edit Follow

edited Apr 10 at 19:56 **StephenKing** 32k ● 9 ● 75 ● 108

answered Sep 30 '17 at 7:15 **Puddler** 1,915 ● 1 ● 14 ● 21

9 Seemed to work, though it ended with `gzip: stdin: unexpected end of file tar: Child returned status 1 tar: Error is not recoverable: exiting now` - assuming that's normal? - **tobek** Dec 27 '17 at 21:09

8 @tobek, yes, if you run the command as given it does complain, but produces the correct output. It is probably complaining because the backup.ab doesn't have the proper gzip file footer with CRC-32 checksum and length. - **hft** Feb 22 '18 at 3:46

10 Just a small annotation how to do it without Linux commandline. Open **backup.ab** with an HexEditor, and replace the first 24 Bytes (0x18) with `1F 8B 00 00 00 00 00 00` and save as **backup.tar.gz**. It can then be opened with WinRAR or any other extractor tool. - **Daniel Marschall** Oct 7 '18 at 1:22

Now working: `gzip: stdin: invalid compressed data--format violated tar: Child died with signal 13 tar: Error is not recoverable: exiting now` - **redanimalwar** Oct 21 '19 at 21:45

I believe none of the answers without using Java will work on encrypted phones. See my answer here: android.stackexchange.com/a/224474/95893 and more importantly nelenkov's app (github.com/nelenkov/android-backup-extractor) and answer - **alchemy** Apr 28 '20 at 22:40

Show 1 more comment

Hot Network Questions

- What is the contemporary translation of this quote from The Art of War?
- What is an expedience of sci-fi gliders? these machines flying near the very ground
- Increasing G force tolerance
- Should religious (or other kind of) titles be used when citing authors?
- Are there villains that wear a helmet in Star Trek?
- 'loose' cells on top tabular
- What is the "a" in "A donde vamos"?
- Taking a theorem as a definition and proving the original definition as a theorem
- Identify this late 1980's Peugeot

▶ Let's use this

```
> ( printf "\x1f\x8b\x08\x00\x00\x00\x00" ; tail -c +25 backup.ab )
| tar xfvz -
apps/com.example.devpack/_manifest
apps/com.example.devpack/r/app_flutter
apps/com.example.devpack/r/app_flutter/res_timestamp-1-1628219563788
apps/com.example.devpack/r/app_flutter/flutter_assets
apps/com.example.devpack/r/app_flutter/flutter_assets/isolate_snapshot_data
apps/com.example.devpack/r/app_flutter/flutter_assets/vm_snapshot_data
apps/com.example.devpack/r/app_flutter/flutter_assets/kernel_blob.bin

gzip: stdin: unexpected end of file
tar: Child returned status 1
tar: Error is not recoverable: exiting now
> ls
apps  backup.ab
```

- ▶ Here we got a folder named apps
- ▶ lets run tree and see all files

```
.
└─ com.example.devpack
    └─ _manifest
        └─ r
            └─ app_flutter
                └─ flutter_assets
                    ├── isolate_snapshot_data
                    ├── kernel_blob.bin
                    └─ vm_snapshot_data
└─ res_timestamp-1-1628219563788
```

`res_timestamp-1-1628219563788` is empty file

let's check other files

```
> strings kernel_blob.bin | grep TamilCTF
    title: Text('TamilCTF{1_l0v3_y0u_AB}'),
chunkStartbitinputCategorybinarySearchinsertionSortlowerBoundmergeSortp
kg.
```

▶ Just used strings and got the flag in `kernel_blob.bin` file

`TamilCTF{1_l0v3_y0u_AB}`