

Forum:[Hack Forums](#)

Thread: [\\$10,000 Reward - Unlock My BitLocker External SSD \(Passwords Known\)](#)

XtremeDiscount - May 15, 2026, 6:23 am

\$10,000 USD Reward - Unlock My Personal BitLocker External SSD

Hey guys,

I'm offering \$10,000 USD (PayPal or crypto, your choice) to anyone who can successfully unlock my external SSD. It has all my family photos and videos — irreplaceable memories. I'm devastated and will pay immediately once I can access the files.

What Happened

I was setting up BitLocker on a new external SSD. Started encryption with a long password, unplugged mid-process, set a shorter password, changed my mind and unplugged again. When I reconnected it, it had fully encrypted anyway. Not sure if it used the long or short password.

Exact Passwords I Remember

These are all the passwords I have (most confident ones at the very top):

ThisIsMySuperSecretDrive10@

MySuperSecretDrive10@

Mydrive10@

drive10

mydrive10

Mydrive10

mydrive10@

drive10@

Drive10@

drive20@

Drive20@

ThisIsMyEncryptedDrive10@

Mydrive20@

MyDrive10@

drive10

Drive20@

(and obvious case variations of the above)

What I Can Provide Full forensic image of the encrypted drive (can split and send securely)

BitLocker hash extracted with bitlocker2john

Remote access via TeamViewer/AnyDesk so you work on the image

If you're experienced with BitLocker cracking (Hashcat mask attacks, Elcomsoft, Passware, etc.) and think you can crack it with these, reply or PM me.

Serious offers only. Payment after I verify my files.

Thanks — this would mean everything to me.

UPDATE

I ran bitlocker2john against a 520 gb image of my 4tb drive and it produced a few hashes. Here is the hash it outputted after running

Code `python bitlocker2john.py -o 0x74e2d00000 header.img > hash.txt`

Code

```
$bitlocker$0$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$1$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$2$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

```
$bitlocker$3$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

```
$bitlocker$0$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3
```

bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$1\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$2\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

\$bitlocker\$3\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

loadman - May 15, 2026, 6:24 am

send me ur telegram in convo

XtremeDiscount - May 15, 2026, 6:28 am

(May 15, 2026 06:24 AM)loadman Wrote: [\[CITE\]](#) send me ur telegram in convoSent

HerrWinston - May 15, 2026, 7:08 am

I have sent you a convo regarding this! :)

Wake - May 15, 2026, 7:17 am

I have sent you a convo to see if I can lend a hand.

DramaKing - May 15, 2026, 7:28 am

New SSD that has the only copy of your precious files? My guess is that BitLocker partially encrypted your files. Ideally, the process can resume if interrupted, but if your password doesn't work, the filesystem is doubtless corrupted by the encryption process. Decrypting the encrypted areas manually would be a specialized task needing specialized tools. It's not like you forgot the password and can unlock the drive after recovering it.

jcole - May 15, 2026, 7:37 am

I hope someone can help you with this. Please think about using my service to escrow this transaction.

<https://hackforums.net/showthread.php?tid=6311511>

5chn4pp - May 15, 2026, 7:39 am

Looks like you already got the attention and help of others, but if they can't do it, I would like to take a look at the image.

G-EZE - May 15, 2026, 10:28 am

Just a heads up!

Be careful with allowing people to connect via AnyDesk/TeamViewer. They can easily run malware on ur pc even if u have file transfer disabled and other safeguards in place they can run commands instantly in the run command box and the malware would be executed silently in the background. I wouldn't recommend letting anyone connect remotely.

I have some extra time and would be happy to assist if others r unable to.

Good luck!

INCREDIBLE - May 15, 2026, 12:31 pm

(May 15, 2026 10:28 AM)G-EZE Wrote: [\[CITE\]](#) Just a heads up!

Be careful with allowing people to connect via AnyDesk/TeamViewer. They can easily run malware on ur pc even if u have file transfer disabled and other safeguards in place they can run commands instantly in the run command box and the malware would be executed silently in the background. I wouldn't recommend letting anyone connect remotely.

I have some extra time and would be happy to assist if others r unable to.

Good luck!

I'd totally second this. ?

also, send me the info and the download link for the disc image.

XtremeDiscount - May 16, 2026, 6:00 am

Hey guys,

I'm still offering \$5000 USD (PayPal or crypto, your choice) to anyone who can successfully unlock the drive and let me access my files. Payment immediately after verification.

Current Problems

I'm having major trouble extracting the BitLocker hash with bitlocker2john:

- bitlocker2john.exe directly on \\.\PhysicalDrive1 -> ftell error
- python bitlocker2john.py on the physical drive -> "Supplied image path is not a BitLocker partition"
- With partial images -> "No signature found!" or "Error reading out of bounds of file"
- Signature is found at 0x100003 but it won't produce a usable hash

The drive is a 4TB external SSD and I only have ~528 GB free space on my computer, so making a full image isn't possible right now. I may have to get an external hard drive to save a full image file to it but is there a way to get the hash without an image file?

Hey guys,

I'm still offering \$5000 USD (PayPal or crypto, your choice) to anyone who can successfully unlock the drive and let me access my files. Payment immediately after verification.

Current Problems

I'm having major trouble extracting the BitLocker hash with bitlocker2john:

- bitlocker2john.exe directly on \\.\PhysicalDrive1 -> ftell error
- python bitlocker2john.py on the physical drive -> "Supplied image path is not a BitLocker partition"
- With partial images -> "No signature found!" or "Error reading out of bounds of file"
- Signature is found at 0x100003 but it won't produce a usable hash

The drive is a 4TB external SSD and I only have ~528 GB free space on my computer, so making a full image isn't possible right now.

Passwords I Remember

(most confident at the top):

- ThisIsMySuperSecretDrive10@
- MySuperSecretDrive10@
- drive10
- mydrive10
- Mydrive10
- mydrive10@
- drive10@
- Mydrive10@
- Drive10@
- drive20@
- Drive20@
- ThisIsMyEncryptedDrive10@
- Mydrive20@
- MyDrive10@
- drive10
- Drive20@

(and obvious case variations of the above)

If you have experience with interrupted BitLocker setups, know a better way to extract the hash directly from the drive, or have other tools that might work better than bitlocker2john, please reply or PM me.

Serious offers only.

Thanks — this would mean the world to me.

possessed-client - May 16, 2026, 6:35 am

What about the recovery keys, Bitlocker must've prompted you to save it at some point.

If you have the recovery key you can try using it normally instead of the password, or if the drive's corrupted somehow you can try this

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/repair-bde> , though read the warnings. Maybe also some random proprietary software, though don't know if they're any better.

Also, if you're on Windows 11 and your encrypted drive is somehow also a bootable drive with the system on it (highly unlikely, since yours is a removable external), then there just was a new exploit a few days ago - <https://github.com/Ap3xPr3d/YellowKey-Primer>

Calculon - May 16, 2026, 8:11 am

I am a little off topic, but I can relate to the feeling of losing access to invaluable memorabilia, photos and videos of pets and family. In my case it was stolen by corrupt law "enforcement" and they never returned it but decided to destroy it instead. I am filled with hatred over being unable to enjoy and experience those memories again. They even refused to return photos from my dad's funeral.

I really hope you'll recover your files eventually.

XtremeDiscount - May 17, 2026, 5:25 am

I used john2bitlocker against a 520gb image I made and it came up with this hash

\$bitlocker\$0\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$1\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$2\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

\$bitlocker\$3\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

\$bitlocker\$0\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$1\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$2\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

\$bitlocker\$3\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

I'm pretty sure I set the password as either

MySuperSecretDrive10@

ThisIsMySuperSecretDrive10@

Or

Mydrive10@

JustSomeN00B - May 17, 2026, 7:33 am

Tried it with the shared passwords, no luck. Trying the ?a mask with hashcat, 8 chars. Should have an update today/tomorrow depending on Hash Rate (currently 15kH/s, since bitlocker. MD5 is 100GH/s)

jcole - May 17, 2026, 7:47 am

(May 17, 2026 05:25 AM)XtremeDiscount_net Wrote: [\[CITE\]](#) I used john2bitlocker against a 520gb image I made and it came up with this hash

\$bitlocker\$0\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$1\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$2\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

\$bitlocker\$3\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

\$bitlocker\$0\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$1\$16\$eac7b3ac70197dfe91505abae28e6556\$1048576\$12\$c0fbafa6000fdc0103000000\$60\$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f

\$bitlocker\$2\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

\$bitlocker\$3\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

I'm pretty sure I set the password as either

MySuperSecretDrive10@

ThisIsMySuperSecretDrive10@

Or

Mydrive10@

Unlocking the Core VRAM (2 H/s to 1,017 H/s)

With a healthy executable, restored dependencies, and a constant icy blast from the external box fan.. I initiated a broad Structural Mask Attack (-a 3) targeting specific camel-case variants like Mydrive?d?d?d?d.

By switching from text-file dictionaries to a pure hardware mask, Hashcat applied its native Brute-Force optimizer. Instead of forcing the card to wait on data streams from the storage drive (which limits speeds to 2 H/s), the engine began generating all permutations directly inside the GPU's hardware cores.

The RTX 3060 working overtime. It skyrocketed from its baseline speeds to 1,017 hashes per second executing a full 10,000-combination numerical sweep in exactly 9 seconds flat while sitting at 63°C.

Current Status:

Every single exact phrase, direct typo, geometric capitalization toggle, and 4-digit trailing sequence (years, pins, numbers) attached to the core memory blocks has been systematically chewed through and officially Exhausted.

The underlying password wasn't in the immediate perimeter, but the infrastructure we built to find it is completely bulletproof. The graphics card is running cold, Windows permissions have been bypassed, and the system is primed to run high speed, and without breaking a sweat. I will keep trying.

CL1B - May 17, 2026, 7:57 am

I'm curious to see how this plays out, good luck everyone.

This is for sure my vote for thread of the month on
<https://hackforums.net/showthread.php?tid=6322700>

jcole - May 17, 2026, 8:22 am

(May 17, 2026 05:25 AM)XtremeDiscount_net Wrote: [\[CITE\]](#) I'm pretty sure I set the password as either

MySuperSecretDrive10@

ThisIsMySuperSecretDrive10@

Or

Mydrive10@

The special character separators are officially exhausted. The 1,600 combinations finished in 5 seconds with a 324 H/s pace.

At this point, we have systematically eliminated:

All 10 raw, exact-match memory words.

Every straight, back-to-back word combo (WordWord).

Every single-digit numerical middle separator (Word[0-9]Word).

Every common special character middle separator (Word[!]Word).

5chn4pp - May 17, 2026, 9:06 am

I have sent you a PM to verify the hashes of the images and if they match to the physical drive.

Let me know the output.

JustSomeN00B - May 17, 2026, 11:36 pm

(May 17, 2026 07:33 AM)JustSomeN00B Wrote: [\[CITE\]](#) Tried it with the shared passwords, no luck. Trying the ?a mask with hashcat, 8 chars. Should have an update today/tomorrow depending on Hash Rate (currently 15kH/s, since bitlocker. MD5 is 100GH/s)

Alright, so I tried the hashcat mask for awhile and was making no progress, so I called it. I tried all variations of your passwords, are you forgetting to tell us any?

Unknown - May 17, 2026, 11:39 pm

Best of luck OP, this definitely has the potential to turn into a fairly notable thread.
I'll keep an eye on it for further developments

trippybiz - May 17, 2026, 11:52 pm

Following... best of luck with this

possessed-client - May 19, 2026, 5:45 am

(May 17, 2026 05:25 AM)XtremeDiscount_net Wrote: [\[CITE\]](#) I used john2bitlocker against a 520gb image I made and it came up with this hash

```
$bitlocker$0$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$1$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$2$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

```
$bitlocker$3$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

```
$bitlocker$0$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$1$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$2$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

```
$bitlocker$3$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

I'm pretty sure I set the password as either

MySuperSecretDrive10@

ThisIsMySuperSecretDrive10@

Or

Mydrive10@

I tried some variations for a couple hours, no luck. Any other clues or common password making

patterns you use that you might've used in this case as well?

JustSomeN00B - May 19, 2026, 6:16 am

(May 19, 2026 05:45 AM)possessed-client Wrote: [\[CITE\]](#) I tried some variations for a couple hours, no luck. Any other clues or common password making patterns you use that you might've used in this case as well?

I've tried every variation of the shared passwords and had no luck with 4 GPUs since OP posted, I can guarantee it's not any of the shared passwords or variants unless I'm either unlucky or dumb (or both)

5chn4pp - May 19, 2026, 6:55 am

(May 19, 2026 06:16 AM)JustSomeN00B Wrote: [\[CITE\]](#) I've tried every variation of the shared passwords and had no luck with 4 GPUs since OP posted, I can guarantee it's not any of the shared passwords or variants unless I'm either unlucky or dumb (or both)

It's not a problem with you.

I tried getting OP to actually verify the hash, but no response back.

Ivanov_1 - May 19, 2026, 4:32 pm

OP i am going to send you a private message ok.

XtremeDiscount - May 20, 2026, 7:30 am

(May 15, 2026 07:08 AM)HerrWinston Wrote: [\[CITE\]](#) I have sent you a convo regarding this! :)
Thanks! I responded

5chn4pp - May 20, 2026, 7:31 am

OP has responded to my PM and given me valuable information.

For anybody that cares, I have now sent this to OP:

Thank you for the output, this is valuable.

The first clue is here:

Code Backup type:

Saved to file

This means the BitLocker process saved the recovery key to a file. Usually this means it generated a file that looks like:

Code BitLocker Recovery Key XXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX.txt

Open PowerShell as administrator, then run the following 3 searches for the file:

Code Get-ChildItem -Path C:\Users -Recurse -ErrorAction SilentlyContinue -Filter "BitLocker Recovery Key*.txt" | Select-Object FullName,LastWriteTime,Length

Get-ChildItem -Path C:\Users -Recurse -ErrorAction SilentlyContinue -Filter "*.txt" | Select-String -Pattern "65917A4D-411E-41EB-9530-BC479C120596" -List | Select-Object Path,LineNumber,Line

Get-ChildItem -Path C:\Users -Recurse -ErrorAction SilentlyContinue -Filter "*.txt" | Select-String -Pattern "65917A4D" -List | Select-Object Path,LineNumber,Line

If it finds the file, please send it to me, it may be able to unlock the BitLocker volume.

If it does not find the file, open PowerShell as administrator, then try the following commands.

First, go to the John folder:

Code `cd C:\john-1.9.0-jumbo-1-win64\run`

Then check which physical disk and partition D: actually maps to:

Code `Get-Partition -DriveLetter D | Format-List`

`DiskNumber,PartitionNumber,DriveLetter,Offset,Size,Type`

This is important because if D: is not actually on `PhysicalDrive1`, then the previous command was pointed at the wrong disk.

After that, try this corrected `bitlocker2john` command:

Code `py -3 .\bitlocker2john.py "\\.\PhysicalDrive1" -o 1048576 > current_hashes.txt 2> current_log.txt`

Important: do not use single quotes around `\\.\PhysicalDrive1`.

The previous error:

Code `FileNotFoundError: [Errno 2] No such file or directory: "'\\.\PhysicalDrive1'"` means Python tried to open a path that literally included the apostrophe characters. So it never actually read the drive. The empty `current_hashes.txt` file does not mean there is no hash; it means the command failed before extraction.

If the `Get-Partition` command shows a different disk number, change `PhysicalDrive1` to the correct number.

Example:

Code `py -3 .\bitlocker2john.py "\\.\PhysicalDrive2" -o 1048576 > current_hashes.txt 2> current_log.txt`

If the Offset value from `Get-Partition` is not 1048576, use the actual Offset value it shows.

Example:

Code `py -3 .\bitlocker2john.py "\\.\PhysicalDrive1" -o ACTUAL_OFFSET_HERE > current_hashes.txt 2> current_log.txt`

If that still does not work, try reading the locked BitLocker volume directly:

Code `py -3 .\bitlocker2john.py "\\.\D:" > current_hashes_D.txt 2> current_log_D.txt`
Do not use `-o` with `\\.\D:`, because `\\.\D:` should already start at the BitLocker volume.

If that also fails, try the raw partition path:

Code `$part = Get-Partition -DriveLetter D`

`$path =`

`"\\?\GLOBALROOT\Device\Harddisk$($part.DiskNumber)\Partition$($part.PartitionNumber)"`

`py -3 .\bitlocker2john.py $path > current_hashes_partition.txt 2> current_log_partition.txt`

Then check the output files:

Code `Get-Content .\current_hashes.txt`

`Get-Content .\current_log.txt`

```
Get-Content .\current_hashes_D.txt
Get-Content .\current_log_D.txt
```

```
Get-Content .\current_hashes_partition.txt
Get-Content .\current_log_partition.txt
```

If any of those current_hashes files contain lines beginning with:

```
Code $bitlocker$0$
$bitlocker$1$
then send those hash lines and the matching log file.
```

The main thing I want to compare is whether the current live-drive \$bitlocker\$1\$ hash matches the image hash. If it matches, then the cracking work already done was against the right current volume. If it differs, we should stop attacking the image hash and switch to the new current-drive hash.

Also, your manage-bde output is actually encouraging:

```
Code Key Protectors:
Password
Numerical Password
```

That means the current D: volume really does have both a normal password protector and a 48-digit recovery-password protector. So there should be a valid BitLocker password/recovery hash to extract from the current drive.

The recovery-key file is the best lead right now. The hash extraction is still useful, but "Backup type: Saved to file" means the real recovery key may already exist somewhere on the computer.

XtremeDiscount - May 20, 2026, 7:33 am

(May 17, 2026 07:33 AM)JustSomeN00B Wrote: [\[CITE\]](#) Tried it with the shared passwords, no luck. Trying the ?a mask with hashcat, 8 chars. Should have an update today/tomorrow depending on Hash Rate (currently 15kH/s, since bitlocker. MD5 is 100GH/s)I only have a 1tb ssd in my computer and my drive that I'm locked out of is 4tb. I ordered a 5tb external hard drive so I can make a full image. DO you think maybe those hashes are wrong and it's a different hash that will be found in the full image? I wonder why it has multiple hashes

(May 19, 2026 06:55 AM)5chn4pp Wrote: [\[CITE\]](#) It's not a problem with you.

I tried getting OP to actually verify the hash, but no response back.
I ran

```
py -3 .\bitlocker2john.py '\\.\PhysicalDrive1' -o 0x100000 > current_hashes.txt 2> current_log.txt
```

and it generated a current_hashes.txt file that's empty.

It also generated a current_log.txt file that says

Traceback (most recent call last):

```
File "C:\john-1.9.0-jumbo-1-win64\run\bitlocker2john.py", line 273, in <module>
main()
^^
```

```
File "C:\john-1.9.0-jumbo-1-win64\run\bitlocker2john.py", line 218, in main
with open(bitlocker_partition, 'rb') as fp:
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

FileNotFoundError: [Errno 2] No such file or directory: ""\\.\PhysicalDrive1"

I ran

manage-bde -status D:

and it says

BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright © 2013 Microsoft Corporation. All rights reserved.

Volume D: [Label Unknown]
[Data Volume]

Size: Unknown GB
BitLocker Version: 2.0
Conversion Status: Unknown
Percentage Encrypted: Unknown%
Encryption Method: AES 128
Protection Status: Unknown
Lock Status: Locked
Identification Field: Unknown
Automatic Unlock: Disabled
Key Protectors:
Password
Numerical Password

I also ran manage-bde -protectors -get D:

and I got

BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright © 2013 Microsoft Corporation. All rights reserved.

Volume D: [Label Unknown]
All Key Protectors

Password:
ID: {0A7D466F-A2DE-4989-B388-F9EB635502B6}

Numerical Password:
ID: {65917A4D-411E-41EB-9530-BC479C120596}
Backup type:
Saved to file

JustSomeN00B - May 20, 2026, 7:35 am

(May 20, 2026 07:33 AM)XtremeDiscount_net Wrote: [\[CITE\]](#) I only have a 1tb ssd in my computer and my drive that I'm locked out of is 4tb. I ordered a 5tb external hard drive so I can make a full image. DO you think maybe those hashes are wrong and it's a different hash that will be found in the full image? I wonder why it has multiple hashes

Bitlocker can gen multiple hashes for various reasons (passwords, recovery key, TPM key, etc.)

Try making a full copy and reextracting the hashes, then update us please.

XtremeDiscount - May 20, 2026, 7:38 am

(May 20, 2026 07:35 AM)JustSomeN00B Wrote: [\[CITE\]](#) Bitlocker can gen multiple hashes for various reasons (passwords, recovery key, TPM key, etc.)

Try making a full copy and reextracting the hashes, then update us please.

Ok, I'll keep you all updated when I get the full image

possessed-client - May 20, 2026, 8:33 am

Hashes 0 and 1 are for the password, 2 and 3 are for the recovery key, the secondary hashes for each are an extra check. As far as I know, you only need the header of the volume to get the hashes and all other information, making a full image of the drive shouldn't give you more information above what you can get from the very beginning of volume data.

As 5chn4pp said, try finding the recovery key. It's your best bet if you don't have any extra info that can help with cracking.

G-EZE - May 20, 2026, 9:25 am

(May 20, 2026 07:33 AM)XtremeDiscount_net Wrote: [\[CITE\]](#) I ran

```
py -3 .\bitlocker2john.py '\\.\PhysicalDrive1' -o 0x100000 > current_hashes.txt 2> current_log.txt
```

and it generated a current_hashes.txt file that's empty.

It also generated a current_log.txt file that says

Traceback (most recent call last):

```
File "C:\john-1.9.0-jumbo-1-win64\run\bitlocker2john.py", line 273, in <module>
main()
^^
```

```
File "C:\john-1.9.0-jumbo-1-win64\run\bitlocker2john.py", line 218, in main
with open(bitlocker_partition, 'rb') as fp:
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

```
FileNotFoundError: [Errno 2] No such file or directory: "'\\\\.\\PhysicalDrive1'"
```

PhysicalDrive1 might not be the correct drive and 0x100000 might not be the correct byte offset that begins on the BitLocker partition. Open up PowerShell and run Get-Disk, you will see some output like:

Code	Number	Friendly Name	Size
------	--------	---------------	------

-----	-----	-----	-----
-------	-------	-------	-------

0		My SSD Pro	1 TB
---	--	------------	------

1		External USB	2 TB
---	--	--------------	------

If your using "My SSD Pro" for example it would be PhysicalDrive0.

To get the byte offset run Get-Partition or u can run Get-BitLockerVolume in PowerShell. The output will look something like:

Code	DiskNumber	PartitionNumber	DriveLetter	Offset
------	------------	-----------------	-------------	--------

-----	-----	-----	-----	-----
-------	-------	-------	-------	-------

0	1	C		123456
---	---	---	--	--------

0	2	D		987654321
---	---	---	--	-----------

If the BitLocker partition starts at 123456, run this in PowerShell to get the hex: "{0:X}" -f 123456 which would be 1E240 in this example.

Putting the command together: py -3 .\bitlocker2john.py '\\.\PhysicalDrive0 -o 0x1E240 >

current_hashes.txt 2> current_log.txt

Try this and let us know what the output becomes.

5chn4pp - May 20, 2026, 9:39 am

These hashes have now been confirmed by me:

Code

```
$bitlocker$0$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$1$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$2$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

```
$bitlocker$3$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

This means the image hashes we got earlier is indeed the hashes of the actual locked drive.

For cracking, don't waste time on \$2 and \$3, those are the 48-digit recovery key. Spend time on \$0 and verify any hit against \$1.

As for the BitLocker file, the chances are looking slim. OP only had C: and the BitLocker volume, and C: has now been searched.

The only path for the BitLocker file left is a deleted file recovery for the file, which I have instructed OP to run.

If that fails, the only path forward is either a crack on the hash, or take the C: drive to a specialized shop for recovery on the BitLocker file.

possessed-client - May 20, 2026, 1:59 pm

(May 20, 2026 09:39 AM)5chn4pp Wrote: [\[CITE\]](#) These hashes have now been confirmed by me:

Code

```
$bitlocker$0$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$1$16$eac7b3ac70197dfe91505abae28e6556$1048576$12$c0fbafa6000fdc0103000000$60$55f8db1043db29d4b2dce30384440ef20b6cb2f9244e0d9d90f91b74144b22de4a4b3a02641dc3bb73f96a71683b6a4959dbe2d98a5089dd5ac7723f
```

```
$bitlocker$2$16$1f3f1d6e0c8ca9d5551911940c4eb7c0$1048576$12$c0fbafa6000fdc0106000000$60$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d
```

\$bitlocker\$3\$16\$1f3f1d6e0c8ca9d5551911940c4eb7c0\$1048576\$12\$c0fbafa6000fdc0106000000\$60\$e6345665d2e653b114260c6cf22dc0a70571d571e13d2e2fbe454a41f6bb6e090d4317e5d1b1684d8e85ec9a490091cec6b3a59643870747f493329d

This means the image hashes we got earlier is indeed the hashes of the actual locked drive.

For cracking, don't waste time on \$2 and \$3, those are the 48-digit recovery key. Spend time on \$0 and verify any hit against \$1.

As for the BitLocker file, the chances are looking slim. OP only had C: and the BitLocker volume, and C: has now been searched.

The only path for the BitLocker file left is a deleted file recovery for the file, which I have instructed OP to run.

If that fails, the only path forward is either a crack on the hash, or take the C: drive to a specialized shop for recovery on the BitLocker file.

Did OP only run the commands for searching for the key from your previous post? Maybe OP fully renamed the file, in which case it might be worth to search for all recent .txt files on C: or on any other removable drive that might've possibly been plugged in.

5chn4pp - May 20, 2026, 2:14 pm

(May 20, 2026 01:59 PM)possessed-client Wrote: [\[CITE\]](#) Did OP only run the commands for searching for the key from your previous post? Maybe OP fully renamed the file, in which case it might be worth to search for all recent .txt files on C: or on any other removable drive that might've possibly been plugged in.

I sent him more commands with wider searches, no result.

And only OP knows what happened with the file, I don't have that information sadly.

He told me the only drives was the BitLocker volume and the C: Drive.

possessed-client - May 20, 2026, 2:32 pm

(May 20, 2026 02:14 PM)5chn4pp Wrote: [\[CITE\]](#) I sent him more commands with wider searches, no result.

And only OP knows what happened with the file, I don't have that information sadly.

He told me the only drives was the BitLocker volume and the C: Drive.

Wider as in searching all txt files on C: since the day of encryption for having "BitLocker" or the key pattern in its contents? Well, if that gave zero then tough luck, hard to recover deleted files on SSDs. I suppose it does increase security to delete the recovery key and all is fine - well, unless you forget the only password.

5chn4pp - May 20, 2026, 2:39 pm

(May 20, 2026 02:32 PM)possessed-client Wrote: [\[CITE\]](#) Wider as in searching all txt files on C: since the day of encryption for having "BitLocker" or the key pattern in its contents? Well, if that gave zero then tough luck, hard to recover deleted files on SSDs. I suppose it does increase security to delete the recovery key and all is fine - well, unless you forget the only password.

I know, here is an example of what was run and resulted in no return:

```
Code Get-PSDrive -PSProvider FileSystem | ForEach-Object { Get-ChildItem -Path "$($_.Root)"  
-Recurse -ErrorAction SilentlyContinue -Filter "BitLocker Recovery Key*.txt"} | Select-Object  
FullName,LastWriteTime,Length
```

```
Get-PSDrive -PSProvider FileSystem | ForEach-Object { Get-ChildItem -Path "$($_.Root)"  
-Recurse -ErrorAction SilentlyContinue -Filter "*.txt" | Select-String -Pattern  
"65917A4D-411E-41EB-9530-BC479C120596" -List } | Select-Object Path,LineNumber,Line
```

```
Get-PSDrive -PSProvider FileSystem | ForEach-Object { Get-ChildItem -Path "$($_.Root)" -Recurse  
-ErrorAction SilentlyContinue -Filter "*.txt" | Select-String -Pattern "65917A4D" -List } | Select-Object  
Path,LineNumber,Line
```

```
Get-PSDrive -PSProvider FileSystem | ForEach-Object { Get-ChildItem -Path "$($_.Root)" -Recurse  
-ErrorAction SilentlyContinue -Include *.txt,*.bek,*.csv,*.rtf,*.doc,*.docx | Select-String -Pattern  
'\b\d{6}-\d{6}-\d{6}-\d{6}-\d{6}-\d{6}-\d{6}-\d{6}\b' -List } | Select-Object Path,LineNumber,Line
```

smartLink - May 21, 2026, 5:03 am

hello, I've been trying what you gave for 3 days but it seems there's a mistake somewhere. Now I know your request: Clean re-extraction of the hash/protector

Because your technical history clearly shows problems:

salt-value exception,
hash parse error,
multiple protectors,
suspicious offsets,
partial images,
signature found at unusual offset.

There are still real chances that:

the good hash is not attacked,
or is incomplete.

Especially this:

Loaded 2 password hashes with 2 different salts

shows that there are 2 different protectors.

One can:

be old,

recovery protector,
incomplete,
or irrelevant.

CyberneticsX - June 15, 2026, 1:48 am

Have you got it yet, or no?.

ItsMehRAWR - June 25, 2026, 7:12 pm

In reverse engineering, the most critical "no dependency" skill is the ability to navigate the Process Environment Block (PEB). When you are writing a custom debugger, unpacker, or instrumentation tool, you cannot rely on standard imports because they make your tool easy to detect and analyze.

To get a headstart, you need to be able to resolve function addresses (like ``GetProcAddress`` or ``LoadLibrary``) manually by walking the PEB in memory. This is the foundation of shellcode development and advanced dynamic analysis.

Below is a minimal, dependency-free x64 MASM skeleton. This code locates ``kernel32.dll`` in memory by walking the ``Ldr`` list, parses its Export Address Table (EAT), and finds the address of any function—all without calling a single imported API.

The "PEB Walker" Template (x64 MASM)

This code provides a clean entry point. Compile this with ``ml64.exe`` and link it without standard C libraries (``/nodefaultlib``).

```
```asm
; Minimal x64 MASM PEB Walker
; Purpose: Resolve function addresses dynamically
; Compile: ml64 /c /nologo /Fo: walker.obj walker.asm
; Link: link /nodefaultlib /entry:main walker.obj /subsystem:console

.code

main PROC
 ; 1. Locate the PEB
 mov rax, gs:[60h] ; PEB is at GS:[60h] in x64
 mov rax, [rax + 18h] ; PEB_LDR_DATA
 mov rax, [rax + 20h] ; InInitializationOrderModuleList

 ; 2. Walk the linked list to find kernel32.dll
 ; (This is a simplified loop; you would compare module names here)
 ; For brevity, we assume the 3rd entry is kernel32.dll
 mov rax, [rax]
 mov rax, [rax]
 mov rbx, [rax + 20h] ; Base address of kernel32.dll

 ; 3. Now rbx points to the Base of kernel32.dll
 ; You would then parse the DOS Header and NT Headers here
 ; to find the Export Directory, then scan for a function name.

 ret
main ENDP

END

```
```

Strategic Headstart for Reverse Engineering

If you want to master this domain, don't waste time writing complex UI code. Focus your "under 3500 lines" on these three modules:

1. The PE Parser: Write a function that takes a base address and returns the ``IMAGE_EXPORT_DIRECTORY`` pointer. You will need to calculate the offsets for ``e_lfanew`` (DOS Header) and ``OptionalHeader`` (NT Headers).

2. The String Hasher: Never store raw function strings (e.g., "VirtualAlloc") in your code—it's the first thing reverse engineers look for. Implement a ROR13 hashing algorithm to store the hashes of your target functions instead. You resolve the hash by hashing the names in the export table at runtime.

3. The Hooking Engine: Write a 14-byte trampoline generator. To hook a function in x64: Overwrite the first 14 bytes of the target function with a `jmp qword ptr [rip + 0] ; <64-bit address>`.

Redirect execution to your function. Restore the original bytes when finished to avoid crashing the process.

Why this approach?

No Dependencies: By walking the PEB, your code is "self-contained." It doesn't need the Windows Loader to resolve its imports before it starts running. This is vital for injecting into other processes.

Stealth: This is how you avoid IAT (Import Address Table) hooks and API monitors that flag you for suspicious imports.

Portability: This logic works on almost any version of Windows x64, as the PEB structure has remained remarkably stable for decades.

Next Steps

Once you have the PEB walker functional, your next logical task is to write a routine that takes a hash as input and returns the function address by iterating through the ``AddressOfNames``, ``AddressOfFunctions``, and ``AddressOfNameOrdinals`` arrays in the ``kernel32.dll`` export table.

Do you have the specific offset structures for the ``IMAGE_NT_HEADERS`` or ``IMAGE_EXPORT_DIRECTORY`` on hand, or would you like me to provide the structure definitions for your MASM header file?

signed0 - July 9, 2026, 6:10 am

Cant you just ping microsoft like the fbi does to provide the private key

snarie - July 16, 2026, 7:14 pm

This sounds silly, but I ran into a similar situation. Microsoft stores the keys online unless it's disabled. Have you checked that?

(That's how I got back on my drive)

mtpakisi - July 21, 2026, 1:36 am

Hey did you come right ?

Can assist