

HDD ROCK **TIPS AND TRICKS**

Table of contents

Introduction

Getting Started to Unlock hard drive

Lock/Unlock Tab Tips

Erase Tab Tips

Password Removal Tab Tips

Atola Unlocker Tips

BRUTE-FORCE

3 Golden Rules

Starter Notes

Do It Smart

CharSet Rules

Q & A

[-Back On Top-](#)

Introduction

The HDD Rock is one of the few tools being used to find, recover, and remove ATA passwords on hard drives. It uses proprietary algorithms to extract passwords and unlock drives. In any case, if the hard drive is locked with a password, then the HDD Rock could find that password. However, there are restrictions, depending on the drive. For HDD Rock, time is the main issue. You could try to unlock an unknown hard drive with no background knowledge of the password, using the HDD Rock, and that is doable but it will take a long time. To cut down on the process time, you must try unlocking the drive systematically; think about the password you're trying before attempting them. This can cut down the operation time drastically.

[-Back On Top-](#)

Getting Started

There are many fields in the PasswordToolCase software that you need to pay attention to. These fields could save you countless hours of operation time when attempting to unlock your hard drive. Please carefully check them before attempting a drive.

[-Back On Top-](#)

Lock/Unlock Tab Tips

Purpose: Lock and/or Unlock your hard drive with a known password.

1. In section 5.2 of the HDD Rock manual, if the Security Level is on High then you should select to unlock your drive at High, and Maximum would set on Maximum. Setting this incorrectly, would result in twice the operation time.

2. Similarly, if you know a little bit about the password level either, user or master, then setting it accordingly would drastically decrease the operation time.

3. CodeSet field: use ASCII type because it will also include the KeyCode type. Only set to KeyCode if you have some idea about the password.

4. MD5 Hash Password: Advise not to check because having it checked will encrypt the password with a special encryption algorithm. Only check if you know the locked password had previously used MD5 Hash Password.

[-Back On Top-](#)

Erase Tab Tips

Purpose: Security Erase the hard drive with a generated word list, such as a dictionary list.

1. Some of the fields are similar to the Lock/Unlock tab, please read the Lock/Unlock Tab Tips.

2. Password Length: a critical field that could unlock your hard drive in a matter of minutes compared to hours, or even days. Each character will have 96 possible combinations (read more on alphanumeric).

3. Reset Count: being used to reset the hard drive after X failed password attempts. 5 will work with most drives, but if you notice your HDD locking up, lower this value.

4. Word List Option: select this option if you want to use a dictionary word list that you have generated. More knowledge on the input password would greatly help to reduce the time to unlock the password.

5. Charset Option: select this option to use rule on how HDD Rock will test the password. This option is mostly used on Brute-Force method (see Brute-Force Section)

[-Back On Top-](#)

Password Removal Tab Tips

Purpose: to remove the locked password with a word list and/or rule file, being used mostly with Brute-Force (see Brute-Force Section).

1. Mode Field: Word List, Incremental, and Vendor Unique are the 3 options to choose from. Again, choosing Word List will choose a dictionary list to run the unlock with. Incremental option yields to the Charset file with specific rule to run tests on. All available .chr file are provided in the rule folder. Unique Vendor is the option to choose with either some of the limited known hard drive vendor, such as Western Digital and Fujitsu.

[-Back On Top-](#)

Atola Unlocker Tips

Purpose: a special, and the fastest, way to unlock your hard drive. Atola Unlocker uses a proprietary method to unlock your hard drive on the Supported Drive List. Please contact your distributor for further information or updates on the Supported Drive List.

1. After getting the HDD information, the Atola Unlocker will display a message whether the hard drive can be unlock or not

[-Back On Top-](#)

BRUTE-FORCE

This method is an attack on the locked password with a large number of possible passwords. Mostly used by rules that are set on the .chr file. Brute-force can also use a combination of WordList and CharSet files to provide a quicker password attack.

[-Back On Top-](#)

3 GOLDEN RULES

Rule #1:
- Any HDD locked with a password is crackable*
Rule #2:
- Ony broken** HDDs are uncrackable.
Rule #3:
- Anything HDD that HDD ROCK cannot crack, see Rule# 2.

[-Back On Top-](#)

Starter Note:

1. There are total of 96 alphanumeric*** characters possible that a typical keyboard user would input for their password character, despite of any encryption on top of that.
2. For 1 character password, we need total of 96 combinations to test the entire possible crack. Hence, 2 characters password would require $96^2 = 9216$ **** combinations. And so forth for 3 characters password would require $96^3 = 884736$.
3. HDD ROCK can typically test 7000 combinational words in 1 hour. Some hard drives could require longer time to power on and off, and this issue affects greatly on the testing bench mark.

*Operation time varies widely, depending on HDD and password

**Hardware and mechanical problem.

***alphanumeric are number 0-9, lower case and upper case letter a-z A-Z, punctuation and special character such as ~!@#\$\$%^&*()_+{}|, etc.

**** $96 = 96$; $96 \times 96 = 9216$; $96 \times 96 \times 96 = 884736$.

[-Back On Top-](#)

Do It Smart

Understanding the locked password:

- If you know some background information about the password, this will greatly help how to attack using Brute-Force.

- Some of important fields:

1. Password Length: from 1 to 32. Each password character has 96 alphanumeric possibilities. Choosing the correct password length could reduce greatly on the time (see calculation on Password Length). Brute-Force without any knowledge about the hard drive will use all 32-byte characters.
2. Word List: a dictionary that is generated by some knowledge of the password. This text file could use together with the Rule file for better combination.
3. Rule: the set of instruction to apply either by itself or with a Word List to attack the password.

[-Back On Top-](#)

CharSet Rules

What is CharSet Rules? It establishes a rule of functions for attacking the locked password. You can create your own customized rule and control the HDD ROCK's behavior.

First: there are 32 characters. For each character, you can control the HDD ROCK to run tests on different alphanumeric and/or ASCII code.

Second: your rule must attack the whole 32 character password

Third: any background knowledge on the locked password would greatly reduce the time needed to unlock the drive.

Once you know what the CharSet rule is all about, you can try to create a rule and see the results. It is very simple once you've done it a couple of times.

Q & A

Q1: Does HDD ROCK support 64-bit machine?

A1: At this time, there is only a 32-bit USB driver available.

Q2: What is MD5 Hash Password? And how does one use it?

A2: MD5 Hash Password is an encrypted password algorithm that is used on top of the password, so the password output is not the actual raw password. If you have checked the MD5 Hash Password during the LOCK, then you must check it again for the UNLOCK.

Q3: If Atola Unlocker does not support my hard drive model, is there anything else I can try?

A3: The Atola Unlocker tab will only allow unlocking on drives on its supported hard drive models

(<http://yec-usa.com/products/hddrock.htm#LIST>) . If your hard drive model isn't on the supported list, then there are other possible ways, but the operation time will be much longer (brute-force).

Q4: What is HDD ROCK voltage's range?

A4: HDD ROCK is compatible with 110V (US). A voltage converter must be used to use it at a different voltage.

Q5: What is ASCII code?

A5: ASCII stands for American Standard Code for Information Interchange. It uses the character coding based on the English alphabet. Please note that I only refer on the printable characters (see Wikipedia for details http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters)

Q6: What is an alphanumeric code?

A6: Alphanumeric code is commonly used in computer terminology to represent machine code that is written so that it assembles into entirely readable ASCII characters such as "a" – "z", "A" – "Z", "1" – "9", "#", "!", and so on.

Q7: Sometimes the PassworldToolCase software hangs up, how do I fix this?

A7: Usually, this is caused by incorrect settings: the software is set to use SATA, instead of ATA, master instead of slave, etc. Please confirm your settings are correct before attempting to run an operation again.

[-Back On Top-](#)