- This is a modified version of Rotor-Cuda
- Huge thanks to kanhavishva and to all developers whose codes were used in Fialka M-125.

Quick start

- **How to create base addresses hex160Sort.bin**

Parametrs:

- -t ? amount of CPU cores (threads) to use?
- -r ? search mode number
- In any mode, you can use one of the options below:
- Bitcoin Single Addres use: `-m address --coin BTC 1PWCx5fovoEaoBowAvF5k91m2Xat9bMgwb`
- Bitcoin Multi Address use: `-m addresses --coin BTC -i test.bin`
- ETHEREUM Single Addres use: `-m address --coin eth 0xfda5c442e76a95f96c09782f1a15d3b58e32404f`
- ETHEREUM Multi Address use: `-m addresses --coin eth -i base160_eth_sorted.bin`
- Public key Single X Point use: `-m xpoint --coin BTC a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4`

- Public keys Multi X Points use: `-m xpoints --coin BTC -i Pubkeys0.1up.bin`
- Example Single Addres use: `Fialka.exe -t 6 -r 2 -s KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYzMHHGVe -n 11 -d 64 -m address --coin BTC 16jY7qd27Snurgjj5rumgHYBEuTSARVSf6`
- Example Single X Point use: `Fialka.exe -t 6 -r 2 -s KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYzMHHGVe -n 11 -d 64 -m xpoint --coin BTC cd6d186d8946f6baa4eca4bcd63deda1b0afe62939811f7ec202dc0007df16e0`
- Example Multi Address use: `Fialka.exe -t 6 -r 2 -s KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYzMHHGVe -n 11 -d 64 -m addresses --coin BTC -i hex160Sort.bin`
- Use old databases or a generator to create list of passphrases, minikeys, WIF, HEX
- The list of found passphrases is here and here
- There is a premade file test.bin 8 words of 3 letters can be found inside
- Uncomressed: cat, gaz, for, car
- Compressed: abc, cop, run, zip
- Make your own passphrase or minikeys for test
- There is a premade file test.bin 8 WIF can be found inside:
- 4 WIF uncomressed:
  5JiznUZskJpwodP3SR85vx5JKeopA3QpTK63BuziW8RmGGyJg81
  5KMdQbcUFS3PBbC6VgitFrFuaca3gBY4BJt4jpQ2YTNdPZ1CbuE
  5HwfeuhdFscL9YTQCLT2952dieZEtKbzJ328b4CR1v6YUVLu2D7
  5J9J63iW7s5p54T569qstediqNgBTLXpUmxUtQwsXTaHz3JCsKt
- 4 WIF compressed:
  L3UBXym7JYcMX91ssLgZzS2MvxTxjU3VRf9S4jJWXVFdDi4NsLcm
  L3BEabkqcsppnTdzAWiizPEuf3Rvr8QEac21uRVsYb9hjesWBxuF
  L31UCqx296TVRtgpCJspQJYHkwUeA4o3a2pvYKwRrCCAmi2NirDG
  KyiR31LZTQ2hk1DRxEticnsQCA8tjFZcgJiKNaRArZME5fpfAjWj
- Make your own WIF or HEX for test
- For searching for uncompressed WIF 5.. (51 length) use the **-b** parameter!

Mode 1

Find passphrases, minikeys and private keys from a text file

- Works only in CPU
- -t ? amount of cores (threads) to use? 1-11 max
- If CPU has 64 cores, you can run 6 copies of the program -t 10 with different dictionaries.txt
- For text files less than 100,000 use -t 1
- Maximun amount of lines in text file is 2,147,483,647 on a new line

- If the file is larger than that, cut into EmEditor chunks by 2,000,000,000 lines
- The last two lines in the file are **DISCARDED**!

To search for passphrases, for Uncompressed addresses use -u or -b

- For passphrases use only letters and symbols: A-Za-z0-9А-Яа-яёЁьЪЬъ `~!@#$&*()-_=+{}|;:'<>,./? others will be skipped!
- Run: `Fialka.exe -t 6 -r 1 -m addresses --coin BTC -s dictionary-words.txt -z Passphrases -i test.bin`

To search for BIP39 words

- For manual exact search of BIP39 word combinations
- Runs slowly on only one core! Use -t 1 If you need faster, use copies of the Fialka M-125 program with different text files
- Use a generator to generate BIP39 word combinations.
- Example: `Generator.exe --dictlist "in.txt,in2.txt" --rule "$0[_]?$1" -s " " out.txt`

- Run: `Fialka.exe -t 1 -r 1 -m address --coin BTC -s bips-list.txt -z BIP -n 5 1ASs2iVA1CCXoMGD98TDsdsoiFDDAbaqbd`

```
Администратор: Командная строка                                                    —  □  ×

C:\Users\BOSS>Fialka.exe -t 1 -r 1 -m address --coin BTC -s bips-list.txt -z BIP -n 5 1ASs2iVA1CCXoMGD98TDsdsoiFDDAbaqbd

    Fialka M-125 (10.01.2022)

    COMP MODE     : COMPRESSED
    COIN TYPE     : BITCOIN
    SEARCH MODE   : Single Address
    DEVICE        : CPU
    CPU THREAD    : 1
    SSE           : YES
    BTC ADDRESS   : 1ASs2iVA1CCXoMGD98TDsdsoiFDDAbaqbd
    OUTPUT FILE   : Found.txt

    Start Time    : Tue Jan 11 20:03:49 2022

    Mode          : 1
    Rotor         : Loading BIP39 WORDS from file: bips-list.txt ...ok
    Loaded        : 26 BIPs words
    Mode BIP      : BIP39 -> Bip32 -> Bip44
    Use words     : English 3,6,9,12,15,18,21,24
    BIP32         : Account 0 m/0/0 -> m/0/5
    BIP32         : Account 1 m/1/0 -> m/1/5
    BIP44         : Account 0 External 0 m/44'/0'/0'/0/0 -> m/44'/0'/0'/0/5
    BIP44         : Account 0 External 1 m/44'/0'/0'/1/0 -> m/44'/0'/0'/1/5
    BIP44         : Account 1 External 0 m/44'/0'/1'/0/0 -> m/44'/0'/1'/0/5
    BIP44         : Account 1 External 1 m/44'/0'/1'/1/0 -> m/44'/0'/1'/1/5
    Check         : 6 addresses for each account (Total addr. for each BIP 36)
    Rotor         : For files up to 100,000 use -t 1 For large file max to 2,147,483,647 lines use -t 1-11 max (For BIP -t 1 MAX)
    Site          : https://github.com/phrutis/Fialka
    Donate        : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9

    [00:00:19] [F: 0] [BIP: 23] [Addresses: 667] [CPU: 33.63/s] [Skip: 0] [word tonight have answer crop light] rip option burger]
    =============================== FOUND! ===============================
    BIP Words : enlist word mirror cable meat flag length symptom opinion
    BIP39 SEED: 0ae11d78675cfaa9f6132013df2dff2a6ef8dc7511550187e9cda13efaa369353fb1961ae08ef82068c3992cb25fd1eace14e720080fe37578202719745762fb
    Address    : 1ASs2iVA1CCXoMGD98TDsdsoiFDDAbaqbd
    Priv (WIF): p2pkh: L4Q5TKeUqHjXLCGj6zPcn5icSerhVUZe921im4p9MQGFjfEguf52
    Priv (HEX): D631DF38498435DDA30BD500A00D0A9E6CFB0C06C50607DABB1215A423B9F9F2
    PubK (HEX): 033E3545991D03C746F800F890C97FC7E66459BBB360AF363A12FDE5E37BCDADBC
    =============================================================================
    [00:00:22] [F: 1] [BIP: 26] [Addresses: 770] [CPU: 33.75/s] [Skip: 0] [release devote coffee habit battle mammal sound ankle exchange naive lion march]
    Search is Finish! Found: 1
```

To search for minikeys

- For minikeys S... (length 22) use -u parameter or S... (length 30) use -b parameter
- Run: `Fialka.exe -b -t 6 -r 1 -m address --coin BTC -s dictionary-minikeys.txt -z Passphrases 14VkDDuvFXs8sMhqznWzioMXKbPAuLofeb`

```
Администратор: Командная строка                                                    —  □  ×

C:\Users\BOSS>Fialka.exe -t 11 -r 1 -m address --coin BTC -s dictionary-minikeys.txt -z Passphrases 14VkDDuvFXs8sMhqznWzioMXKbPAuLofeb

    Fialka M-125 (10.01.2022)

    COMP MODE     : COMPRESSED
    COIN TYPE     : BITCOIN
    SEARCH MODE   : Single Address
    DEVICE        : CPU
    CPU THREAD    : 11
    SSE           : YES
    BTC ADDRESS   : 14VkDDuvFXs8sMhqznWzioMXKbPAuLofeb
    OUTPUT FILE   : Found.txt

    Start Time    : Tue Jan 11 20:11:30 2022

    Mode          : 1
    Rotor         : Loading Passphrases from file: dictionary-minikeys.txt ...ok
    Loaded        : 63994818 Passphrases
    Rotor         : Only letters and symbols: A-Za-z0-9└-■p- ¬и№▄·  `~!@#$&*()-_=+{}|;:'<>,./? others will be Skipped!
    Rotor         : For files up to 100,000 use -t 1 For large file max to 2,147,483,647 lines use -t 1-11 max (For BIP -t 1 MAX)
    Site          : https://github.com/phrutis/Fialka
    Donate        : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9

    [00:01:19] [c4b65af] [88795853F361F85E6E82C752714D9EB3C52509D7BB9C1E2E1C75CE28393AB272] [CPU: 278.21 Kk/s] [F: 0] [T: 9,966,257] [Skip: 0]
    =============================== FOUND! ===============================
    Address    : 14VkDDuvFXs8sMhqznWzioMXKbPAuLofeb
    Priv (WIF): p2pkh: L35KAApQrbsZYsD4tHHxeQZdpS8ao65R71KYab94tdVStuiANCMU
    Priv (HEX): AEB463CC8536279236A12F41259EA57D4E1459C696FE90DA4CB39A91D52B1844
    PubK (HEX): 02FCE38F2AA71DDF0F80345D1567E100F8D9C88A48D69B373F8077F444C072C1E2
    =============================================================================
    [00:04:57] [c074c168] [3875BD055FA7A54B822AEC121A3DB3B700B7D11EB2A83C4068EB3BCB1E87D874] [CPU: 280.04 Kk/s] [F: 1] [T: 70,992,770] [Skip: 0]
    Search is Finish! Found: 1
```

To search for private keys WIF

- For WIF **ONLY!** letters Base58 (ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz123456789)

- For WIF the first letter must be L... (length 52) and K... (length 52) or 5... (length 51) if 5.. WIF is listed use **-b**

- Run: `Fialka.exe -t 6 -r 1 -m addresses --coin BTC -s dictionary-WIF.txt -z WIF -i test.bin`

To search for private keys HEX

- For HEX use only 0,1,3,4,5,6,7,8,9,a,b,c,d,e,f length 1-64 max)

- Run: `Fialka.exe -t 6 -r 1 -m addresses --coin BTC -s private-keys-list.txt -z HEX -i test.bin`

Mode 2

Random search WIF from puzzle 64 bit

- VanitySearch search the prefix 16jY7qLJ from a puzzles 64 bits
- Example WIF out:
  KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYvQqYKVuZryGJLxfH1P
  KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYwJvoHMhmXgVkKmTcAx
  KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYwYTCAfXHKuFsZ2stFG
  KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYwyWFyQr5iVJkTvXccg
  KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYzMHHGVeYFPidEza7Td
  KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qZ3hA1yqkkqoyqype3pQ
  KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYzMHHGVeYFPidEza7Td
- We know that the private key corresponds to 64 bits. Therefore, set the -d 64 range bit limiter.
- If the output private key is more or less than 64 bits, skip...
- For 256 bit range use -d 256 or other ranges skip...
- -n ? amount of random letters. If prefix 41 letters 52-41 = -n 11
- Run: `Fialka.exe -t 6 -r 2 -s KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYzMHHGVe -n 11 -d 64 -m address --coin BTC 16jY7qd27Snurgjj5rumgHYBEuTSARVSf6`

Mode 3

Parallel search for WIF with continuation

How to use mode 3 + examples

Run: `Fialka.exe -t 6 -r 3 -d 64 -n 45 -m address --coin BTC 16jY7q2ZeFPaadZvdygopRURcXhwBWKsA4`

Mode 4

Parallel search for passphrases with continuation + filter

How to use mode 4 + examples

- Use the -u or -b parameter to find old passphrases
  Run: `Fialka.exe -t 6 -r 4 -m addresses --coin BTC -i test.bin -n 60`
  Run: `Fialka.exe -t 6 -r 4 -n 60 -m address --coin BTC 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2`

```
Администратор: Командная строка - Fialka.exe  -t 6 -r 4 -n 60 -m address --coin BTC 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2

C:\Users\BOSS>Fialka.exe -t 6 -r 4 -n 60 -m address --coin BTC 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2

 Fialka M-125 (05.01.2022)

 COMP MODE    : COMPRESSED
 COIN TYPE    : BITCOIN
 SEARCH MODE  : Single Address
 DEVICE       : CPU
 CPU THREAD   : 6
 SSE          : YES
 BTC ADDRESS  : 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2
 OUTPUT FILE  : Found.txt

 Start Time   : Fri Jan  7 14:39:45 2022

 Mode         : 4
 Rotor        : Paralleland sequential search Passphrases. MAX -t 64
 Rotor        : Save checkpoints every 5 minutes in NEXT-Passphrases.txt
 Rotor        : Activated filter-replacement of 3 identical letters (AAA->AAB) every ~60 seconds
 Letters      : (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz )
 Passphrase1  : Hello my friend
                ...
 Passphrase6  : Trussardi
 Site         : https://github.com/phrutis/Fialka
 Donate       : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9


 [00:00:01] [Hello my frjFFv] [B4B2B6C19022F579CFA4DD15422006A04E0A5650CB643038414CFAA95608FC1F] [CPU: 497.09 Kk/s] [F: 0] [T: 499,190] [Replaces: 0]
 =========================================================================================
 PubAddress: 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2
 Priv (WIF): p2pkh:L31UCqx296TVRtgpCJspQJYHkwUeA4o3a2pvYKwRrCCAmi2NirDG
 Priv (HEX): ACBA25512100F80B56FC3CCD14C65BE55D94800CDA77585C5F41A887E398F9BE
 PubK (HEX): 024D7F6D07FC4FD8DE5F08B8CF5B3C1B8A0B9C0B28F18EBEC39C6DC35E3AD22573
 =========================================================================================
 [00:00:40] [Hello my frxhgq] [8BC933B81F7BD16584C65E7B7C03070433244CAE444A3EFF06E4A011AB425189] [CPU: 270.43 Kk/s] [F: 1] [T: 11,564,758] [Replaces: 0]
```

Mode 5

Parallel search for passphrases with continuation + filter

How to use mode 5 + examples

- Use the -u or -b parameter to find old passphrases

  Run: `Fialka.exe -t 6 -r 5 -n 60 -m addresses --coin BTC -i test.bin`

  Run: `Fialka.exe -t 6 -r 5 -n 60 -m address --coin BTC`

  14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2


```
Filter 3 litters + Replace: TurboNuuU -> TurboNuuV

C:\Users\BOSS>Fialka.exe -t 6 -r 5 -n 60 -m address --coin BTC 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2

 Fialka M-125 (05.01.2022)

 COMP MODE    : COMPRESSED
 COIN TYPE    : BITCOIN
 SEARCH MODE  : Single Address
 DEVICE       : CPU
 CPU THREAD   : 6
 SSE          : YES
 BTC ADDRESS  : 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2
 OUTPUT FILE  : Found.txt

 Start Time   : Fri Jan  7 14:48:48 2022

 Mode         : 5
 Rotor        : Paralleland sequential search Passphrases. MAX -t 64
 Rotor        : Save checkpoints every 5 minutes in NEXT-Passphrases.txt
 Rotor        : Activated filter-replacement of 3 identical letters (AAA->AAB) every ~60 seconds
 Letters      : (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789 )
 Passphrase1  : Hello my friend
                ...
 Passphrase6  : Trussardi
 Site         : https://github.com/phrutis/Fialka
 Donate       : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9


 [00:00:02] [Hello my fri7ha] [67E0502DF780ACD2024A0375CD990CC50CB8E3E8866022A6E7613B9CC3266B69] [CPU: 379.72 Kk/s] [F: 0] [T: 763,460] [Replaces: 0]
 =========================================================================================
 PubAddress: 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2
 Priv (WIF): p2pkh:L31UCqx296TVRtgpCJspQJYHkwUeA4o3a2pvYKwRrCCAmi2NirDG
 Priv (HEX): ACBA25512100F80B56FC3CCD14C65BE55D94800CDA77585C5F41A887E398F9BE
 PubK (HEX): 024D7F6D07FC4FD8DE5F08B8CF5B3C1B8A0B9C0B28F18EBEC39C6DC35E3AD22573
 =========================================================================================
 [00:01:34] [Hello my fr2d5v] [8D57F6537525B75B91D70C8BF6DAE487A63C7374AC7DC47637876B42ED6B7326] [CPU: 265.95 Kk/s] [F: 1] [T: 25,778,864] [Replaces: 27]
```

Mode 6

Parallel search for passphrases with continuation + Filter

How to use mode 6 + examples

- Use the -u or -b parameter to find old passphrases
  Run: `Fialka.exe -t 6 -r 6 -n 60 -m addresses --coin BTC -i test.bin`
  Run: `Fialka.exe -t 6 -r 6 -n 60 -m address --coin BTC`
  15KqNGHFEViRS4WTYYJ4TRoDtSXH5ESzW9

```
Filter 3 litters + Replace: Trussueee -> Trussueef                                                    —   □   ×

C:\Users\BOSS>Fialka.exe -t 6 -r 6 -n 60 -m address --coin BTC 15KqNGHFEViRS4WTYYJ4TRoDtSXH5ESzW9

Fialka M-125 (05.01.2022)

COMP MODE     : COMPRESSED
COIN TYPE     : BITCOIN
SEARCH MODE   : Single Address
DEVICE        : CPU
CPU THREAD    : 6
SSE           : YES
BTC ADDRESS   : 15KqNGHFEViRS4WTYYJ4TRoDtSXH5ESzW9
OUTPUT FILE   : Found.txt

Start Time    : Fri Jan  7 14:56:14 2022

Mode          : 6
Rotor         : Paralleland sequential search Passphrases. MAX -t 64
Rotor         : Save checkpoints every 5 minutes in NEXT-Passphrases.txt
Rotor         : Activated filter-replacement of 3 identical letters (AAA->AAB) every ~60 seconds
Letters       : (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!#$&'()*+,-./:;<=>?@[]^_`{|}~  )
Passphrase1   : Hello my friend
              ...
Passphrase6   : Trussardi
Site          : https://github.com/phrutis/Fialka
Donate        : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9


[00:00:04] [Hello my fri5N3] [7C5AB3D1B75D608558FB5224C294C8A9390F53F52935CF4BDD00C672B5037836] [CPU: 356.23 Kk/s] [F: 0] [T: 1,430,306] [Replaces: 0]
===========================================================================
PubAddress: 15KqNGHFEViRS4WTYYJ4TRoDtSXH5ESzW9
Priv (WIF): p2pkh:L3BEabkqcsppnTdzAWiizPEuf3Rvr8QEac21uRVsYb9hjesWBxuF
Priv (HEX): B1C02B717C94BD4243E83B5E98BA37FB273BC035E4AD8FC438EA4D07A1043F56
PubK (HEX): 03ABC0DD6E7AFD2D884118807FB129C33ABA0AE28E075BF01346BBAF016F86DBD8
===========================================================================
[00:05:21] [Hello my fr2;]K] [FB268E1423C4E4B0D67959C872798FDCCB61526501E56A68E90A4246560A39BF] [CPU: 268.86 Kk/s] [F: 1] [T: 85,241,478] [Replaces: 49]
```

Mode 7

Parallel search for WIF with continuation (without range limiter -d)

Similar settings as in mode 3 without range limiter -d

Run: `Fialka.exe -t 6 -r 7 -n 45 -m address --coin BTC`
16jY7q2ZeFPaadZvdygopRURcXhwBWKsA4

Mode 8

Parallel search for minikeys S.. with continuation

Create file Minikeys.txt Add Minikeys S... (22) or S.. (30) on a new line. One line = 1 thread (-t 1) max -t 64

- For minikeys S... (length 22) use -u parameter or S... (length 30) use -b parameter
  Run: `Fialka.exe -t 6 -r 8 -m address --coin BTC 1KM1Wq1boMka4M4vavQX5Zyc281G8SbuCQ`

Mode 9

GPU Parallel WIF search

- Use WifSolverCuda

Mode 10

Random search for minikeys 22 S...

Run: `Fialka.exe -u -t 6 -r 10 -m addresses --coin BTC -i test.bin`

Mode 11

Random search for minikeys 30 S...

Run: `Fialka.exe -b -t 6 -r 11 -m addresses --coin BTC -i test.bin`

```
Администратор: Командная строка - Fialka.exe  -t 6 -r 11 -m addresses --coin BTC -i test.bin

C:\Users\BOSS>Fialka.exe -t 6 -r 11 -m addresses --coin BTC -i test.bin

   Fialka M-125 (05.01.2022)

   COMP MODE     : COMPRESSED
   COIN TYPE     : BITCOIN
   SEARCH MODE   : Multi Address
   DEVICE        : CPU
   CPU THREAD    : 6
   SSE           : YES
   BTC HASH160s  : test.bin
   OUTPUT FILE   : Found.txt

   Loading       : 100 %
   Loaded        : 75,471 Bitcoin addresses

   Bloom at      : 000001EAB92E6C70
   Version       : 2.1
   Entries       : 150942
   Error         : 0.0000010000
   Bits          : 4340363
   Bits/Elem     : 28.755175
   Bytes         : 542546 (0 MB)
   Hash funcs    : 20


   Start Time    : Fri Jan  7 15:40:42 2022

   Mode          : 11
   Rotor         : Random search Minikeys 30 litters. Ex. Sxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   Letters       : Base58 (ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz123456789)
   Site          : https://github.com/phrutis/Fialka
   Donate        : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9


   [00:00:30] [SFhLpfivFqAYFjirXyagg56PvtD3nx] [3AE6C358789BB31AFC8D84764B60D3F6515E079AED38CF4ED9C2DD28691ABE7E] [CPU: 294.74 Kk/s] [F: 0] [T: 8,826,482]
```

Mode 12

Random search for minikeys 22, 30 S...

- -s ? the first part of the key S.....
- -n ? how many letters to randomize?
- -z second part of the key (you can do without it)
- For minikeys S... (length 22) use -u parameter or S... (length 30) use -b parameter
  Run: `Fialka.exe -u -t 6 -r 12 -s SHwfehdFcL -n 3 -z 2ieZEtK -m address --coin BTC 1GWPWQNWdnYQYuo4DPzEhFCKhKq8dxGYSG`


```
Администратор: Командная строка - Fialka.exe  -t 6 -r 12 -s SHwfehdFcL -n 4 -z ieZEtK -m address --coin BTC 1GWPWQNWdnYQYuo4DPzEhFCKhKq8dxGYSG

C:\Users\BOSS>Fialka.exe -t 6 -r 12 -s SHwfehdFcL -n 4 -z ieZEtK -m address --coin BTC 1GWPWQNWdnYQYuo4DPzEhFCKhKq8dxGYSG

   Fialka M-125 (10.01.2022)

   COMP MODE     : COMPRESSED
   COIN TYPE     : BITCOIN
   SEARCH MODE   : Single Address
   DEVICE        : CPU
   CPU THREAD    : 6
   SSE           : YES
   BTC ADDRESS   : 1GWPWQNWdnYQYuo4DPzEhFCKhKq8dxGYSG
   OUTPUT FILE   : Found.txt

   Start Time    : Tue Jan 11 19:55:24 2022

   Mode          : 12
   Rotor         : Random search Minikeys
   Letters       : Base58 (ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz123456789)
   Rotor         : SHwfehdFcL[random 4 letters]ieZEtK
   Site          : https://github.com/phrutis/Fialka
   Donate        : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9


   [00:00:31] [SHwfehdFcLNmUsieZEtK] [7592361E2347548BEFCA5B556AE05463C9850B0BD523C68210ED5EC99BB03D53] [CPU: 265.57 Kk/s] [F: 0] [T: 9,212,533]
   ================================ FOUND! =================================
   Address    : 1GWPWQNWdnYQYuo4DPzEhFCKhKq8dxGYSG
   Priv (WIF): p2pkh: L21C3HoNLFpRd9sQ8efSh7bH9PEXuVApnS1obrhZma4bKS6QNJKb
   Priv (HEX): 8EBF11788B5AA5644350F44C7603712170275057D505D843A6BE94B3FFF94579
   PubK (HEX): 02C250685F7F3DFE85D58167923EB54DDF8B743086731137530E7BC41262904438
   =======================================================================
   [00:00:49] [SHwfehdFcLwcKiieZEtK] [9CE238634853C8555A8E52AF7F4AAA2FE8A5D9E7CBD76CD8F8CD9D7F7557C67F] [CPU: 261.93 Kk/s] [F: 1] [T: 13,985,369]
   ================================ FOUND! =================================
   Address    : 1GWPWQNWdnYQYuo4DPzEhFCKhKq8dxGYSG
   Priv (WIF): p2pkh: L21C3HoNLFpRd9sQ8efSh7bH9PEXuVApnS1obrhZma4bKS6QNJKb
   Priv (HEX): 8EBF11788B5AA5644350F44C7603712170275057D505D843A6BE94B3FFF94579
   PubK (HEX): 02C250685F7F3DFE85D58167923EB54DDF8B743086731137530E7BC41262904438
   =======================================================================
   [00:01:10] [SHwfehdFcLoCYSieZEtK] [AD1834FFE681567B52ADD4B22B3C713C401A324A03760DBE8B8DF440EFF3A37D] [CPU: 246.50 Kk/s] [F: 2] [T: 19,177,660]
```

Mode 13 (best performance)

Random search for minikeys 22, 30 S... (Analog mode 12)

- Checking minikays for validity "V" (? = 0x00...) If the mini-key is not valid then skip...
- -s ? the first part of the key S.....
- -n ? how many letters to randomize?
- -z second part of the key (you can do without it)
- For minikeys S... (length 22) use -u parameter or S... (length 30) use -b parameter
  Run: `Fialka.exe -u -t 1 -r 13 -s SYXqbKXyX -n 4 -z 3cSMV7Csa -m address --coin BTC 1KM1Wq1boMka4M4vavQX5Zyc281G8SbuCQ`

  if full random:

  Run: `Fialka.exe -u -t 6 -r 13 -s S -n 21 -m addresses --coin BTC -i test.bin`

Mode 14 (MAX -t 12)

Parallel search for WIF with continuation + filter AAA -> AAB + checksum check

-n ? ex. -n 38 = Movable part wif (38) + fixed part (13)

Example Create a text file WIF.txt with 6 WIF on a new line.

```
5JiznUZskJpwodP3SR85vx5JKeopA3QpTK13BuziW8RmGGyJg81
5KMdQbcUFS3PBbC6VgitFrFuaca3gBY4BJo4jpQ2YTNdPZ1CbuE
5HwfeuhdFscL9YTQCLT2952dieZEtKbzJ318b4CR1v6YUVLu2D7
L3BEabkqcsppnTdzAWiizPEuf3Rvr8QEac11uRVsYb9hjesWBxuF
L31UCqx296TVRtgpCJspQJYHkwUeA4o3a2avYKwRrCCAmi2NirDG
KyiR31LZTQ2hk1DRxEticnsQCA8tjFZcgJaKNaRArZME5fpfAjWj
```

Run: `Fialka.exe -b -t 6 -r 14 -n 38 -m addresses --coin BTC -i test.bin`

To turn on the AAA -> AAB filter, use: -s -s Filter

Run: `Fialka.exe -b -t 6 -r 14 -n 38 -s Filter -m addresses --coin BTC -i test.bin`

```
  C:\Users\BOSS>Fialka.exe -b -t 6 -r 14 -n 38 -m addresses --coin BTC -i test.bin

    Fialka M-125 (17.01.2022) v4.0

    COMP MODE    : COMPRESSED & UNCOMPRESSED
    COIN TYPE    : BITCOIN
    SEARCH MODE  : Multi Address
    DEVICE       : CPU
    CPU THREAD   : 6
    SSE          : YES
    BTC HASH160s : test.bin
    OUTPUT FILE  : Found.txt


    Loading      : 100 %
    Loaded       : 75,471 Bitcoin addresses

    Bloom at     : 000002733EFF7FC0
    Version      : 2.1
    Entries      : 150942
    Error        : 0.0000010000
    Bits         : 4340363
    Bits/Elem    : 28.755175
    Bytes        : 542546 (0 MB)
    Hash funcs   : 20



    Start Time   : Mon Jan 17 17:32:56 2022

    Mode         : 14
    Rotor        : Paralleland sequential search for WIF values. MAX -t 12, 1 core =
  1 line
    Rotor        : Save checkpoints every 5 minutes in NEXT-WIF.txt
    Rotor        : Activated filter-replacement of 3 identical letters (AAA->AAB)
  every 1 minute
    Rotor        : If the checksum (32 bit) does not equal the private key, skip...
    Rotor        : Movable part wif (38) + fixed part (13)
    Start WIF(1) : 5JiznUZskJpwodP3SR85vx5JKeopA3QpTK13Bu+[ziW8RmGGyJg81]
            ...
    Start WIF(6) : KyiR31LZTQ2hk1DRxEticnsQCA8tjFZcgJaKNaRArZME5fpfAjWj
    Site         : https://github.com/phrutis/Fialka
```

Valid WIF: 5HwfeuhdFscL9YTQCLT2952dieZEtKbzJ328b4CR1v6YUVLu2D7

=============================== FOUND! ===============================
Address   : 19JxMTT1YqVHAx16NdvgULNajRYvrbFjm1
Priv (WIF): p2pkh: 5HwfeuhdFscL9YTQCLT2952dieZEtKbzJ328b4CR1v6YUVLu2D7
Priv (HEX): 10C22BCF4C768B515BE4E94BCAFC71BF3E8FB5F70B2584BCC8C7533217F2E7F9
PubK (HEX):
04BEC831D2E490FB784CB48284E102B80FF84EC3E0F2F69806002134D166B1B998CD1A8043AEDFBC2D2C7

==

Valid WIF: L3BEabkqcsppnTdzAWiizPEuf3Rvr8QEac21uRVsYb9hjesWBxuF

=============================== FOUND! ===============================
Address   : 15KqNGHFEViRS4WTYYJ4TRoDtSXH5ESzW9
Priv (WIF): p2pkh: L3BEabkqcsppnTdzAWiizPEuf3Rvr8QEac21uRVsYb9hjesWBxuF
Priv (HEX): B1C02B717C94BD4243E83B5E98BA37FB273BC035E4AD8FC438EA4D07A1043F56
PubK (HEX): 03ABC0DD6E7AFD2D884118807FB129C33ABA0AE28E075BF01346BBAF016F86DBD8
==
[00:00:03] [5JiznUZskJpwodP3SR85vx5JKeopA3QpTK5UhdziW8RmGGyJg81] [CPU: 1.42
Mk/s] [F: 2] [V: 2] [Skip: 4,327,630]
Valid WIF: 5KMdQbcUFS3PBbC6VgitFrFuaca3gBY4BJt4jpQ2YTNdPZ1CbuE

=============================== FOUND! ===============================
Address   : 1ERNpuxsGB6ytQKTwtCSmeyBTzmyw3uQAG
Priv (WIF): p2pkh: 5KMdQbcUFS3PBbC6VgitFrFuaca3gBY4BJt4jpQ2YTNdPZ1CbuE
Priv (HEX): CADC8EDAB738C1DF2CE192AF17E7D35EBBDCAF075E32ED2CC86F6D97C160DBAE
PubK (HEX):
04AD0831DB6C686A67D03EC1087F05548B38EFA2E6225DC5DF317D901A312E133FC766AD786ABAE17EC1A

==
[00:00:04] [5JiznUZskJpwodP3SR85vx5JKeopA3QpTK6WEFziW8RmGGyJg81] [CPU: 1.36
Mk/s] [F: 3] [V: 3] [Skip: 5,510,681]
Valid WIF: 5JiznUZskJpwodP3SR85vx5JKeopA3QpTK63BuziW8RmGGyJg81

=============================== FOUND! ===============================
Address   : 162TRPRZvdgLVNksMoMyGJsYBfYtB4Q8tM
Priv (WIF): p2pkh: 5JiznUZskJpwodP3SR85vx5JKeopA3QpTK63BuziW8RmGGyJg81
Priv (HEX): 77AF778B51ABD4A3C51C5DDD97204A9C3AE614EBCCB75A606C3B6865AED6744E
PubK (HEX):
04A45EBC40F95CC06EF93A5F5E9DAA22774A5C9A120AC14D87C328B44C1158F81CDDD109246A4D8BFF5F9

==
[00:00:07] [5JiznUZskJpwodP3SR85vx5JKeopA3QpTK9i9hziW8RmGGyJg81] [CPU: 1.33
Mk/s] [F: 4] [V: 4] [Skip: 9,415,604]
Valid WIF: KyiR31LZTQ2hk1DRxEticnsQCA8tjFZcgJiKNaRArZME5fpfAjWj

=============================== FOUND! ===============================
Address   : 1Mfw1us14DXJ8ju88iewjt48tswqEshU62

```
    Priv (WIF): p2pkh: KyiR31LZTQ2hk1DRxEticnsQCA8tjFZcgJiKNaRArZME5fpfAjWj
    Priv (HEX): 4A70FE9AA6436E02C2DEA340FBD1E352E4EF2D8CE6CA52AD25D4B95471FC8BF2
    PubK (HEX): 03ED88FB3173D3ADCAABC0D49745E3946792B7CB92024E93966FB57511BFF853BE
    ============================================================================
    [00:00:12] [5JiznUZskJpwodP3SR85vx5JKeopA3QpTLFC1kziW8RmGGyJg81] [CPU: 1.30
  Mk/s] [F: 5] [V: 5] [Skip: 16,052,967]
    Valid WIF: L31UCqx296TVRtgpCJspQJYHkwUeA4o3a2pvYKwRrCCAmi2NirDG

    ============================== FOUND! ==================================
    Address    : 14Nmb7rFFLdZhKaud5h7nDSLFQfma7JCz2
    Priv (WIF): p2pkh: L31UCqx296TVRtgpCJspQJYHkwUeA4o3a2pvYKwRrCCAmi2NirDG
    Priv (HEX): ACBA25512100F80B56FC3CCD14C65BE55D94800CDA77585C5F41A887E398F9BE
    PubK (HEX): 024D7F6D07FC4FD8DE5F08B8CF5B3C1B8A0B9C0B28F18EBEC39C6DC35E3AD22573
    ============================================================================
    [00:00:36] [5JiznUZskJpwodP3SR85vx5JKeopA3QpTLhZE8ziW8RmGGyJg81] [CPU: 1.14
  Mk/s] [F: 6] [V: 6] [Skip: 46,706,108]
```

Mode 15

Random search part WIF + checksum check

- -s ? part1 (maybe without the first part)
- -n ? how many random letters
- -z ? part2 or checkeum (possible without the second part)

Run: `Fialka.exe -t 6 -r 15 -s L3UBXym7JYcMX91 -n 4 -z`

`ZzS2MvxTxjU3VRf9S4jJWXVFdDi4NsLcm -m addresses --coin BTC -i test.bin`

VanitySearch special edition for Fialka M-125

Example address [puzzle 64](#) **16jY7qLJnxb7CHZyqBP8qca9d51gAjyXQN**

The longer found prefix is, the more accurate is the WIF

You can specify the exact range for the WIF search.

Use start and finish options to randomize between them.

The output creates 2 files: Found.txt and NEW-WIF.txt (only WIF is sorted)